2400 series SecureSyncs

Table of Contents

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.

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

Safety for 2400 SecureSyncs

- Refer to Salesforce Cases such as: 282804 (though this particular case is pertaining to 1200 SecureSyncs-not 2400s)

  General Suggestions

  - Refer to the online Model 2400 SecureSync user guide:

    Safety: https://www.orolia.com/manuals/2400/Content/NC_and_SS/2400/INSTALL/Safety.htm?Highlight=safety

  - Refer to **RB oscillator MSDS datasheet and disposal docs:** I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Oscillators, rb material\Rb oscillator

  - Refer to **lithium battery replacement** in all SecureSyncs (note there is also a lithim battery for SAASM receiver, if installed): I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Battery replacement

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

  - Refer also to the "**UL and CE Testing / Declarations of Conformity**" section of the custserviceassistance doc for additional info: ..\CustomerServiceAssistance.pdf

- 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

Regulatory Compliance for 2400s: UL/CE Declaration of Conformity (DoC)

SecureSync CE approval/Declaration of Conformity (DoC0

- The SecureSync is CE compliant, so a Declaration of Conformity is available upon request.
- The "Declaration of Conformity" document (DEC-CONF-SecureSync 2400") is stored in Arena at
- DoC on our website: https://www.orolia.com/document/declaration-of-conformity-for-securesync-2400/
- DoC (in Arena attached to the DEC-CONF-SecureSync 2400 item):
- Refer to "Regulatory Compliance" in the 2400 online user guide: https://orolia.com/manuals/2400/Content/NC_and_SS/2400/INTRO/Compliance.htm

from Tom Richardson (15 May 18) BTW and for your information. 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.

Leakage current (current leakage)

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

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

LTA (Danny: Land Transport Authority) is looking for the a test report of current leakage of all equipment
The link below is an explanation of what they want to see.
http://carelabz.com/what-leakage-current-testing-measuring-how-leakage-current-testing-measuring-done/

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

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

Flammability testing/certifification

- Refer to the SecureSync IEC 60950-1 IT Equipment report ("31683550.001 CB Complete.pdf") : I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\EMC and CE Declaration of Conformity\CE testing
- Refer to reports (in Arena): https://app.bom.com/items/detail-spec?item_id=1216702411&version_id=10806087508&orb_msg_single_search_p=1

Fire retardent chemicals (bromine/Inorganic phosphorus material)

Q from a customer: Is there any about inorganic phosphorus material in SecureSyncs?
A Per Tom Richardson (6 Dec 17) "We have determined, according to our documentation, that there is no inorganic phosphorus material in the SecureSync. Bromine is the chemical used as the fire retardant in our boards."

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

EMI-Emissions/EMC/ESD testing

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

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

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

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

Fundamental frequency for SecureSyncs

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

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

UL Testing/ UL certificates

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

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

***Touch current

- Refer to Salesforce case 163902

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

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

RoHS compliancy statement for 2400 SecureSyncs

General info on RoHS / RoHS2 / RoHS3 Compliancy:

Refer to:

- https://www.rohsguide.com/
- "RoHS in: ..\CustomerServiceAssistance.pdf

RoHS 2 versus RoHS 2

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

RoHS 2 vs RoHS 3 (EU 2015/863)

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

RoHS compliancy for Model 2400 SecureSyncs

- Refer to the 2400 SecureSync data sheet and Declaration of Conformity
  - For a link to the current Dec of Confirmity, go to: I:\Customer Service\EQUIPMENT\SPECTRACOM

EQUIPMENT\SecureSync-2400 (Diamond)\CE Declaration of Conformity and EMI-EMC

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

Your question

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

GPS Clock Serial Card P/N 1204-02

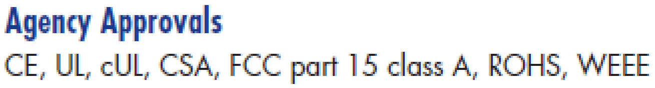
GPS Clock P/N

A reply from Keith (15 Mar 17)

My response

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

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



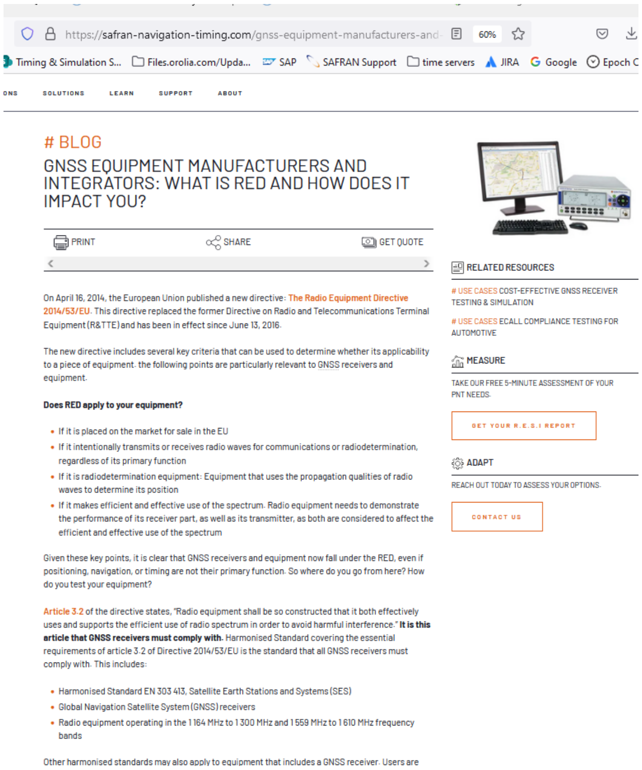
Agency Approvals

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

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

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

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



BLOG

GNSS EQUIPMENT MANUFACTURERS AND INTEGRATORS: WHAT IS RED AND HOW DOES IT IMPACT YOU?

On April 16, 2014, the European Union published a new directive: The Radio Equipment Directive 2014/53/EU. This directive replaced the former Directive on Radio and Telecommunications Terminal Equipment (R&TTE) and has been in effect since June 13, 2016.

The new directive includes several key criteria that can be used to determine whether its applicability to a piece of equipment. the following points are particularly relevant to GNSS receivers and equipment.

Does RED apply to your equipment?

- If it is placed on the market for sale in the EU
- If it intentionally transmits or receives radio waves for communications or radiodetermination, regardless of its primary function
- If it is radiodetermination equipment: Equipment that uses the propagation qualities of radio waves to determine its position
- If it makes efficient and effective use of the spectrum. Radio equipment needs to demonstrate the performance of its receiver part, as well as its transmitter, as both are considered to affect the efficient and effective use of the spectrum

Given these key points, it is clear that GNSS receivers and equipment now fall under the RED, even if positioning, navigation, or timing are not their primary function. So where do you go from here? How do you test your equipment?

Article 3.2 of the directive states, "Radio equipment shall be so constructed that it both effectively uses and supports the efficient use of radio spectrum in order to avoid harmful interference." **It is this article that GNSS receivers must comply with.** Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU is the standard that all GNSS receivers must comply with. This includes:

- Harmonised Standard EN 303 413, Satellite Earth Stations and Systems (SES)
- Global Navigation Satellite System (GNSS) receivers
- Radio equipment operating in the 1 164 MHz to 1 300 MHz and 1 559 MHz to 1 610 MHz frequency bands

Other harmonised standards may also apply to equipment that includes a GNSS receiver. Users are

RELATED RESOURCES

USE CASES COST-EFFECTIVE GNSS RECEIVER TESTING & SIMULATION

USE CASES ECALL COMPLIANCE TESTING FOR AUTOMOTIVE

MEASURE

TAKE OUR FREE 5-MINUTE ASSESSMENT OF YOUR PNT NEEDS.

ADAPT

REACH OUT TODAY TO ASSESS YOUR OPTIONS.

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

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

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

Such systems usually consist of:
1) A power transmitter, with additional communication capability to control the charge function, in conjunction with the receiving part. The power transmitter could also be named as base station.
2) A power receiver, which supplies the received energy to a mobile device and performs a control/supervision function for the mobile device status and charge operation. Both parts in combination are able to transmit and receive data in addition to the power transmission mode e.g. to control the mobile device status and to optimize the power transmission mode.
These radio equipment types are capable of operating in the permitted frequency bands below 30 MHz as specified in Table 1.
The present document covers fixed systems, mobile and portable systems.
Table 1: WPT systems within the permitted frequency bands below 30 MHz
WPT frequency range Frequency Bands Applications
Transmit and Receive 1 19 kHz to 21 kHz WPT systems
Transmit and Receive 2 59 kHz to 61 kHz WPT systems
Transmit and Receive 3 79 kHz to 90 kHz WPT systems
Transmit and Receive
4
100 kHz to 119 kHz WPT systems
Transmit and Receive 119 kHz to 140 kHz WPT systems

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

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

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

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

4.2.1 Background information

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

4.2.2 Wanted performance criteria

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

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

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

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

MIL-STD-461 (ELECTROMAGNETIC INTERFERENCE CHARACTERISTICS)

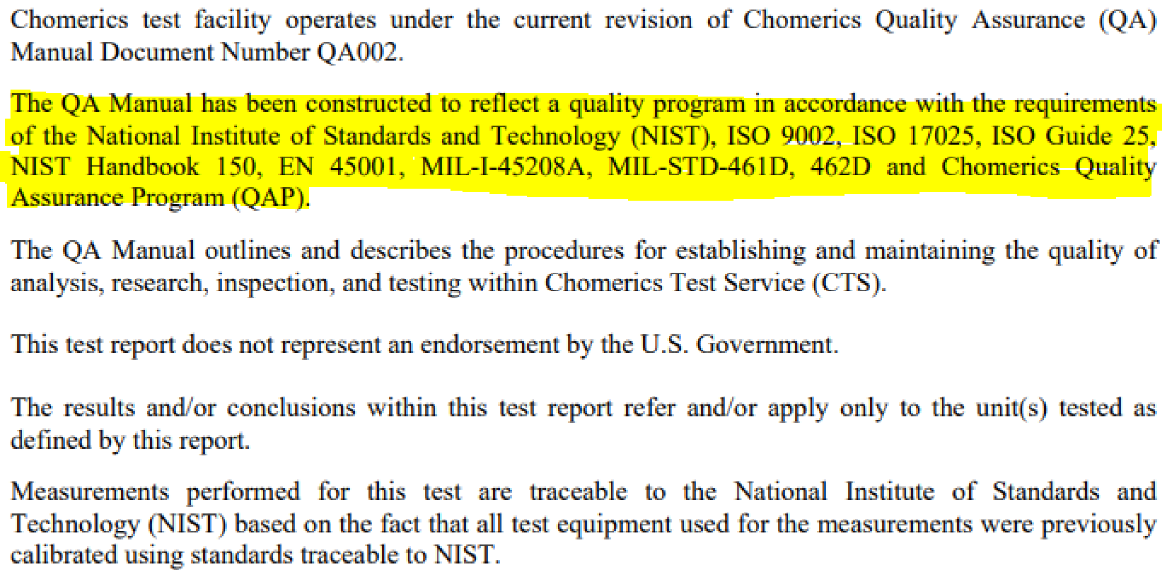
- Refer to sites such as: https://en.wikipedia.org/wiki/MIL-STD-461
- Refer to Salesforce Cases such as 196350

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

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

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

Q It is not mentioned in the Datasheet that SecureSync is compliant with MIL-STD-461. However, in every EMC Test reports available in Arena, it mentionned 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%5Flayouts%2Flanding%2Easpx%3FSource%3Dhttps%253A%252F%252Foroliagroupemeamicrosoftonlinecom%252D1%252Esharepoint%252Eemea%252Emicrosoftonline%252Ecom%252F%255Fforms%252Fdefault%252Easpx&lc=1033&id=500046&cbcxt=mai&wlidp=1&guest=1&bk=1333973817

Email from Paul Myers (3/5/12)

NOTE: We support NTP which is good.
NTP security has NOT been an issue so far, but I doubt we meet any STIG if it describes security.
Our NTP Supports security which includes Symmetric Keys and a single configuration of the AUTOKEY 'IFF protocol'.
Our AUTOKEY implementation is the most basic and supports IFF Group and Client Keys. We only support RSA keys and MD5 hash.
This is NOT likely the preferred method and we don't use a FIPS OpenSSL if that is require

Email from Paul Myers (3/5/12)

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

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

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

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

Apache

- FTP a file named cert.pem which means x509 PEM
- FTP a file named cert.der which means x509 DER
- FTP a file named certpem.p7c which means PKCS7 PEM
- FTP a file named certder.p7c which means PKCS7 DER

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 Wikipeda:
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 Wikipeda:
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, C**ommon 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-Securty-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.

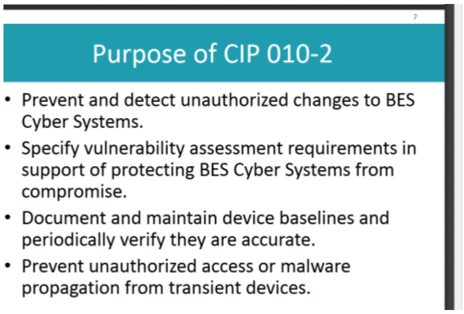
In general, we take in security vulnerability reports from our own scanning, from customers, and from vulnerability databases. Generally these are handled within our quarterly releases. We try to provide workarounds in the mean-time, however, if necessary we can do an out of band release to resolve.

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



Purpose of CIP 010-2

- Prevent and detect unauthorized changes to BES Cyber Systems.
- Specify vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise.
- Document and maintain device baselines and periodically verify they are accurate.
- Prevent unauthorized access or malware propagation from transient devices.

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 saveconfg<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.

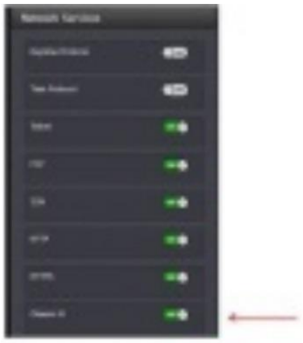
At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access.
Penetration of the cryptographic module enclosure from any direction has a very 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

Availale 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

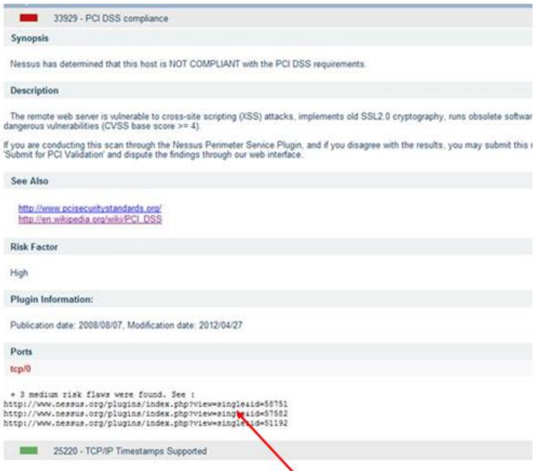
http://spectracom.com/Desktopmodules/Bring2Mind/DMX/Download.aspx?EntryId=1851&PortalId=0

E) **Salesforce cases, such as**

164874

A vulnerability scanner can detect/report PCI DSS Compliancy

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



🟥 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 softwar
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/0

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

🟩 25220 - TCP/IP Timestamps Supported

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

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

info on Services/deamons running in SecureSync

- refer to (in this doc): User accounts

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

- refer to (in this doc): User accounts

logging requirements for PCI-DSS compliancy:

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

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

Email from Morgan to Apps Engineering We have some questions on our support of the PCI-DSS (???) standards on the SecureSync product. Can you provide input to their concern and our support of the standard? https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

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

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

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

below info is From SF case 164874

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

- Access to sensitive and critical data (10.2.1)
- Action taken by user with administrative or root privileges (10.2.2)
- Invalid logical access attempts (I.e. Access denied) (10.2.4)
- Successful and Unsuccessful logons and logoffs (10.2.4)
    - 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 varius methodas 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.

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) Telecom Profile (Frequency sync)

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

C) Telecom Profile (Phase/Time Sync)

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

Per Dave Sohn (6 Oct 17) Our Rb SecureSyncs with GPS and the 1204-32 cards can be configured to operate according to the G.826x specs. We do not have compatibility with the G.827x specs

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.

"Indian Trusted Telecom Portal"

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

Scada Systems

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

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

Terms

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

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

- Refer to “Y2k38” in the Custserviceassistance document

SecureSync 2400

Links/Shortcuts:

Manuals/Guides:

- **Shortcut to SecureSync 2400 manual (2400-5000-0050) in Arena:** https://app.bom.com/items/list-main
- **Shortcut to Elta Special SecureSync 2400 manual (2400-5000-0050p) in Arena:** https://app.bom.com/items/list-main
- **Shortcut to Harris SecureSync 2400 manual (2400-5000-H050?) in Arena**:
- **Shortcut to SAASM receiver Manual Addendum (2400-5000-0056???) in Arena**

  Note: NOT in Arena as it's a FOUO document: U:\Documentation\Released\Manuals\1200-xxxx-xxxx
- **Shortcut to the SecureSync Service Manual (2400-5000-0056) not yet in Arena:**

  Please Note: The Service manual is not to be sent to customers/dealers
- **Option Card Install Guide for 2400 SecureSyncs (2400-5000-0052) in Arena**: https://app.bom.com/items/detail-spec?item_id=1271819535&version_id=11422521608&orb_msg_single_search_p=1
- **Shortcut to HOT SWAP guide for 2400s (2400-1000-0757) in Arena:** https://app.bom.com/items/detail-spec?item_id=1279181962&version_id=11650158118&orb_msg_single_search_p=1

Other shortcuts

- **Shortcut to SecureSync 2400 datasheet:** https://oroliagroup.sharepoint.com/sites/oroliasalesmarketing/
- **Shortcut to firmware upgrades:** I:\Customer Service\PSB, PSP software updates\2400 SecureSync
- **Shortcut to SecureSync Product Service Bulletins:** I:\Customer Service\PSB, PSP software updates\2400 SecureSync
- **Shortcut to pre-release candidate software updates:** S:\Engineering\Projects\Lafayette\200 Engineering Documents\Working Files\Releases
- **Shortcut to Engineering design Projects/test plans for SecureSync 2400:** S:\Engineering\Projects\Lafayette ??
- **Link to manual CD that we ship ( ) in Arena:**

Process Details/Schematics/Component Part Numbers

- **2400 top level Process Detail (240x-xxx) In Arena:** https://app.bom.com/items/detail-spec?item_id=1288342240&version_id=12207994608
- **2400-CNFG-PD: SecureSync,2400 Production Configuration Process Detail (In Arena)** https://files.bom.com/download/1zDERnnumw1An97rjY0Zl2USM9cV6ake/hchfefmkcqpefmzcnxebyfnfsfjapwwx/2400-CNFG-PD%20Rev%201.pdf
- **P/N for the 2400 series rack ears:** 2400-1000-0714
  - **Schematic for SecureSync 2400 CPU board (2400-1001-0200) in Arena:** https://app.bom.com/items/detail-spec?item_id=1239474681&version_id=11210585778&
  - **Schematic for SecureSync 2400 front panel PCB board: 2400-1001-0202 (in Arena):** https://app.bom.com/items/detail-spec?item_id=1247004315&version_id=11121828548&
    - **Front panel PCB FOO assembly: 2400-0000-F002 (in Arena):** https://app.bom.com/items/detail-spec?item_id=1232777518&version_id=11121828578&
- **2400 Extension board:**

➢ **Refer to ECO 1904 (in Arena):** https://app.bom.com/changes/detail-attach?change_id=2395273030

➢ **P/N for Extension board**: 2400-0000-F003 (in arena) https://app.bom.com/items/detail-spec?item_id=1232777535&version_id=11131235928&

➢ **Schematic for SecureSync 2400** Extension board: 2400-1001-0201 (in Arena): https://app.bom.com/items/detail-spec?item_id=1247673417&version_id=11210593828&

Spectracom Product roadmaps

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

Internatonal shipping (ECCN, CCATS and HTS codes)

CCATS Number for SecureSync

➢ Refer to "CCATS Numbers" Section in the Custserviceassist doc: ..\CustomerServiceAssistance.pdf

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

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

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

HTS and ECCN Numbers for all our products

➢ Refer to the "**Export Control**" section of the custserviceassist doc: ..\CustomerServiceAssistance.pdf

➢ Refer also to the latest version of the "US_Export_Controls_Matrix" (or order info in SAP)

I:\Trade Compliance\Export Control Matrix

I:\Customer Service\Export Control-HTS and ECCN numbers

A) (NO SAASM receiver installed, and no ITAR Specials installed) (carryover from 1200 SecureSyncs)

(Non-ITAR variants of SecureSync)

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

➢ Note: Regarding "letter of explanation" mentioed in email below, refer to the two docs at: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Intl Shipping - ECCN and HTS codes

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

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

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

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

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

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

Earlier Email from Dave L (19 Apr 17) I have a correction to the ECCN for Securesync. It is now 5A991.

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

B) With s SAASM receiver installed/ITAR Specials

ITAR variants of SecureSync

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

MTBF/MTTR

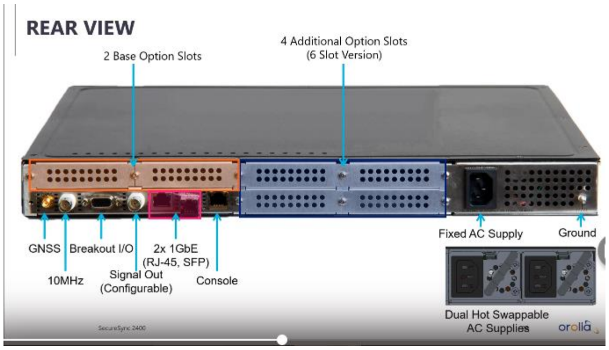
2400 SecureSync MTBF/MTTR

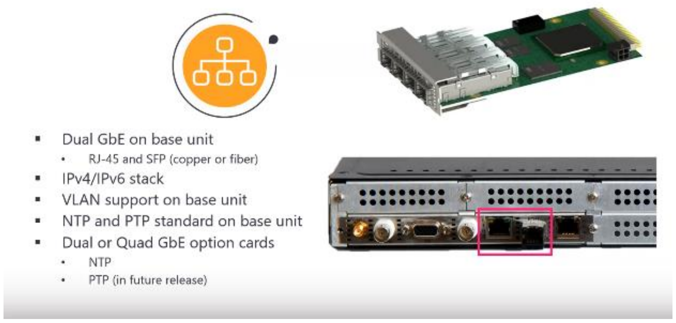
- See Alaysia/Quality team
- Refer to the MTBF/MTTR section in ..\CustomerServiceAssistance.pdf

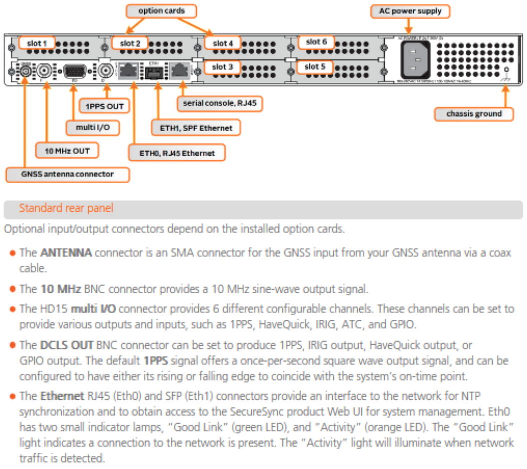
Rear panel/Slots-Slot Numberin

A) SecureSync rear panel/Base unit labeling

- Refer also to "**Unit Rear panel**" in online 2400 SecureSync user guide":
  https://www.orolia.com/manuals/2400/Content/NC_and_SS/2400/INTRO/Rear_Panel.htm?Highlight=rear%20panel




Dual GbE on base unit
RJ-45 and SFP (copper or fiber)
IPv4/IPv6 stack
VLAN support on base unit
NTP and PTP standard on base unit
Dual or Quad GbE option cards
NTP
PTP (in future release)



Standard rear panel

Optional input/output connectors depend on the installed option cards.

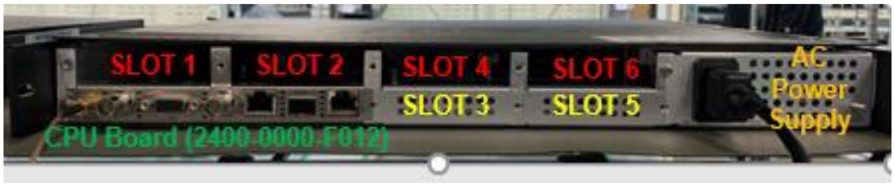
- The **ANTENNA** connector is an SMA connector for the GNSS input from your GNSS antenna via a coax cable.
- The **10 MHz** BNC connector provides a 10 MHz sine-wave output signal.
- The HD15 **multi I/O** connector provides 6 different configurable channels. These channels can be set to provide various outputs and inputs, such as 1PPS, HaveQuick, IRIG, ATC, and GPIO.
- The **DCLS OUT** BNC connector can be set to produce 1PPS, IRIG output, HaveQuick output, or GPIO output. The default **1PPS** signal offers a once-per-second square wave output signal, and can be configured to have either its rising or falling edge to coincide with the system's on-time point.
- The **Ethernet** RJ45 (Eth0) and SFP (Eth1) connectors provide an interface to the network for NTP synchronization and to obtain access to the SecureSync product Web UI for system management. Eth0 has two small indicator lamps, "Good Link" (green LED), and "Activity" (orange LED). The "Good Link" light indicates a connection to the network is present. The "Activity" light will illuminate when network traffic is detected.

BNC labeling on the base unit

- The **10 MHz output BNC** is silkscreened/labeled "**F**" (as in "Frequency)
- The **1PPS output BNC** is silkscreened/labeled "**D**" (as in "1PPS distribution")

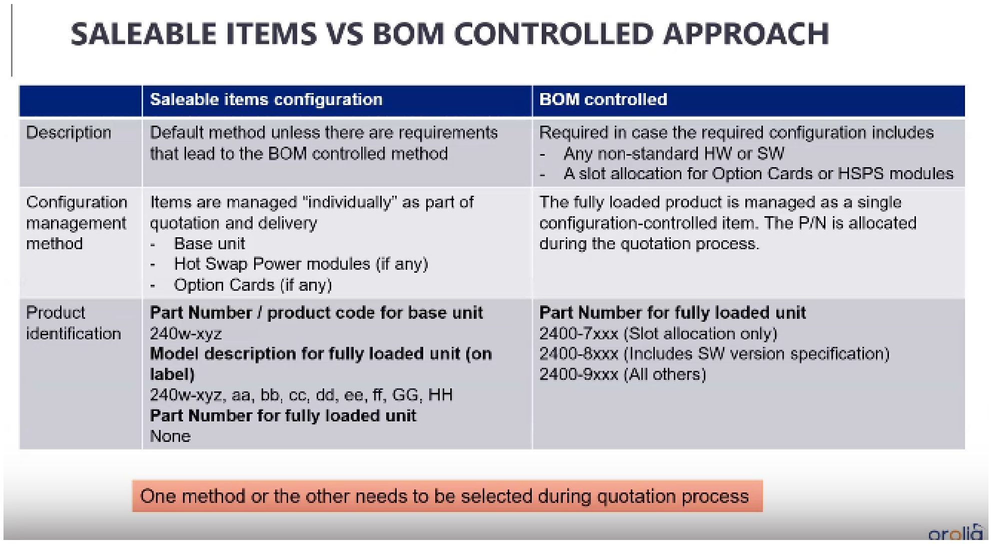
2400 SecureSyncs are available in two slot configurations

- **Two** Slots (2402-)
- **Six** Slots (2406-)



2400 Part Numbers (240W-XYZ)

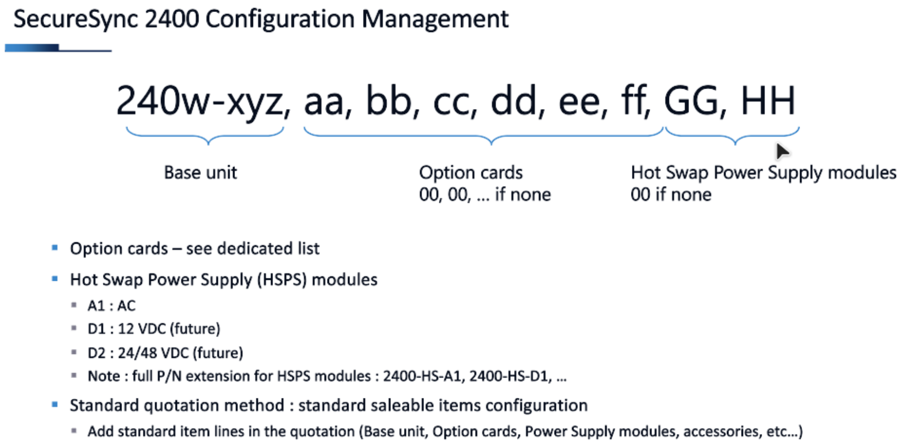
240w-xyz			
W: Expansion PCB	**x: Power**	**y: Oscillator**	**z: GPS/GNSS Receiver**
2 = 2 Option Cards (no expansion PCB	0 = AC only	0 = TCXO	1 = No Receiver installed
6 = 6 Option Cards (Expansion PCB)	2 = Single Hot Swap Power	1 = OCXO	3 = L1 Band Multi-GNSS (Commercial Receiver)
	3 = 12vdc	2 = LPN (High performace) OCXO	7 = L1/L2 band GB-GRAM SAASM GPS
	4 = 24/48vdc	3 = Standard RB	9 = M-Code SAASM Receiver
	6 = Dual Hot Swap Power	5 = LPN RB	



SALEABLE ITEMS VS BOM CONTROLLED APPROACH

	Saleable items configuration	BOM controlled
Description	Default method unless there are requirements that lead to the BOM controlled method	Required in case the required configuration includes - Any non-standard HW or SW - A slot allocation for Option Cards or HSPS modules
Configuration management method	Items are managed "individually" as part of quotation and delivery - Base unit - Hot Swap Power modules (if any) - Option Cards (if any)	The fully loaded product is managed as a single configuration-controlled item. The P/N is allocated during the quotation process.
Product identification	**Part Number / product code for base unit** 240w-xyz **Model description for fully loaded unit (on label)** 240w-xyz, aa, bb, cc, dd, ee, ff, GG, HH **Part Number for fully loaded unit** None	**Part Number for fully loaded unit** 2400-7xxx (Slot allocation only) 2400-8xxx (Includes SW version specification) 2400-9xxx (All others)

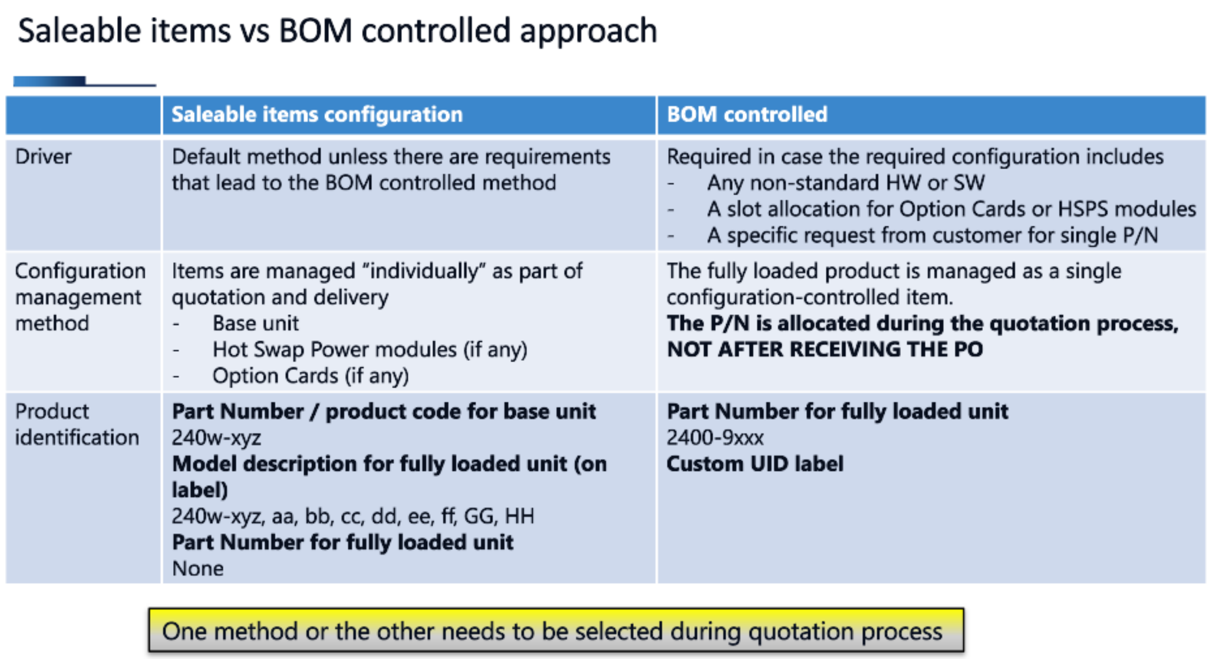
One method or the other needs to be selected during quotation process



SecureSync 2400 Configuration Management

240w-xyz, aa, bb, cc, dd, ee, ff, GG, HH

- Option cards – see dedicated list
- Hot Swap Power Supply (HSPS) modules
  - A1 : AC
  - D1 : 12 VDC (future)
  - D2 : 24/48 VDC (future)
  - Note : full P/N extension for HSPS modules : 2400-HS-A1, 2400-HS-D1, …
- Standard quotation method : standard saleable items configuration
  - Add standard item lines in the quotation (Base unit, Option cards, Power Supply modules, accessories, etc…)



Saleable items vs BOM controlled approach

	Saleable items configuration	BOM controlled
Driver	Default method unless there are requirements that lead to the BOM controlled method	Required in case the required configuration includes - Any non-standard HW or SW - A slot allocation for Option Cards or HSPS modules - A specific request from customer for single P/N
Configuration management method	Items are managed "individually" as part of quotation and delivery - Base unit - Hot Swap Power modules (if any) - Option Cards (if any)	The fully loaded product is managed as a single configuration-controlled item. **The P/N is allocated during the quotation process, NOT AFTER RECEIVING THE PO**
Product identification	**Part Number / product code for base unit** 240w-xyz **Model description for fully loaded unit (on label)** 240w-xyz, aa, bb, cc, dd, ee, ff, GG, HH **Part Number for fully loaded unit** None	**Part Number for fully loaded unit** 2400-9xxx **Custom UID label**

One method or the other needs to be selected during quotation process

In-house SecureSync references for Engineering

(Note: this info is from 1200 SecureSyncs)

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

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

Username: spadmin
Password: ~~Spadmin3~~

SecureSync 2400s on the Internet (outside of firewall)

(Note: this info is from 1200 SecureSyncs)

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

A) SecureSync on Internet for Sales demo:

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

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

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

User account for customers to login

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

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

Admin account
Username: **spadmin**
Password: **SPadmin4** (SP in caps - rest in lower-case letters)

B) SecureSync on Internet for Sales demo:

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

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

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

The correct login for the Model 9483/SecureSync is:

User account for customers
Username: **spadmin**
Password: **SPadmin3** (SP in caps - rest in lower-case letters)

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

Factory and spadmin

Visio Stencils/shapes

Link to the Visio graphic file referenced below: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Visio

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

Datasheet/Specs

(Note: this info is from 1200 SecureSyncs)

**IP rating (Ingress Protection)

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

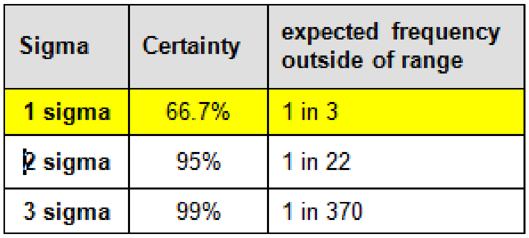
"One sigma" for the 1PPS specs (standard deviation)

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

http://en.wikipedia.org/wiki/Standard_deviation
http://en.wikipedia.org/wiki/68%E2%80%9395%E2%80%9399.7_rule
http://math.stackexchange.com/questions/320370/how-to-calculate-standard-deviation-and-use-three-sigma-rule-for-couple-variable

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

In statistics, the so-called **68–95–99.7 rule** is a shorthand used to remember the percentage of values that lie within a band around the mean in a normal distribution with a width of one, two and three standard deviations, respectively; more accurately, 68.27%, 95.45% and 99.73% of the values lie within one, two and three standard deviations of the mean,
In the empirical sciences the so-called **three-sigma rule of thumb** expresses a conventional heuristic that "nearly all" values are taken to lie within three standard deviations of the mean, i.e. that it is empirically useful to treat 99.7% probability as "near certainty"



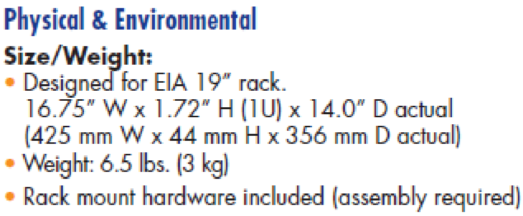
Sigma	Certainty	expected frequency outside of range
1 sigma	66.7%	1 in 3
2 sigma	95%	1 in 22
3 sigma	99%	1 in 370

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

Chassis dimensions/correct width

Chassis measurements (from the S/S datasheet)

see the note below this excerpt



Physical & Environmental

Size/Weight:

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

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

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

Chassis/top cover screws

(Note: this info is from 1200 SecureSyncs)

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

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

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

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

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

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

This video may help: https://www.youtube.com/watch?v=_mTFQbaT3Zc Hopefully in the future you will never have to change any option cards.

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

*Mercury in 2400 SecureSyncs?

- Refer to TOYO case 283704 for what I believe is the first Model 2400 SecureSync request for info on mercury.

*Asbestos in 2400 SecureSyncs?

- Refer to Case 300240 (May 2023)
- "Asbestos isn't currently mentioned/referenced in online user guide, previous to at least May 2023

Per Emmanuel (24 May 2023)

But you will find below answering elements

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

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

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

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

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

Status update (26 May 2023). Asbestos wasn't previously mentioned in the 2400 SecureSync Declaration of Conformity. With help from Emmanuel and Ryan Johnson, it has now been added to this document. Refer to the latest version of the Dec of Conformity at: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync-2400 (Diamond)\CE Declaration of Conformity and EMI-EMC\2400s\Declaration of Conformity for 2400s.

(Note: this info below is from 1200 SecureSyncs)

Conflict Minerals report

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

MSDS info

Hazardous materials/Rubidium material

A) Coin Battery for RTC

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

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

- Refer to the Spectratime PSDS (“Spectratime hazmat331.pdf”) on our website at:

  http://support.spectracom.com/articles/FAQ/Security-sheet-integrated-Spectratime-Rubidium-parts?retURL=%2Fapex%2FKnowledgeSiteHome&popup=false
- Refer also to the great webpage for info on Rb including health risks/measures: http://www.lenntech.com/periodic/elements/rb.htm

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

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

Mercury, lead, RoHs compliancy

Q. Any Mercury contained in the system such as LCD?
A Per Keith after talking with Dave Sohn The LCD display is RoHS compliant. We are not aware of it (nor the rest of the SecureSync) containing any mercury.

Q Any other hazardous materials such as Lead, RoHS complaint?
Keith’s response: The SecureSync is RoHS compliant. Also, the 1200-233 has a SpectraTime Rubidium oscillator installed. Attached you should find a PSDS Safety Data Sheet associated with this Rubidium oscillator.

Q Any specific safety warnings for operation and maintenance?
Keith’s response: Maintenance of the SecureSync in the field is really limited to the installation or removal of any Option Cards, which requires power be removed from the SecureSync and standard ESD practices be followed.

(Note: this info is below from 1200 SecureSyncs)

- For shock/vibe of antennas (such as Model 8230s), refer to the custservasssistdoc: ..\CustomerServiceAssistance.pdf

SecureSync has been tested against MIL-STD-810F

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

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

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

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

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

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

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

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

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

A Reply from Morgan (22 Sept 15) We vibration tested the SecureSync to a specific profile for a customer at the time of development. The limits of the profile are indicated on our spec without too much information on the customers profile as part of the NDA. The final installation was a naval shipboard environment. We have not tested the SecureSync to any other mobile environment up to this point.

Data sheet indicates “0.07g”

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

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

Data sheet indicates “0.53oz”

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

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

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

Q Also, in the stated shock and vibration limits, on the data sheet. You reference “10-55Hz/0.07g” and “55-500”/1.0g”. You mentioned before that this was a random test. Thus, do those values refer to PSD / ASD curve break points? Should they have units of g^2/Hz?

A Reply from Morgan (7 Oct 15) The 10 to 55Hz and the 55-500Hz tests were run separately. There were no break points in the profiles. Yes, the data sheets need to be updated and the units should be in g^2/Hz

Shock/vibe testing for Option Cards

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

Also, in the stated shock and vibration limits, on the data sheet. You reference “10-55Hz/0.07g” and “55-500”/1.0g”. You mentioned before that this was a random test. Thus, do those values refer to PSD / ASD curve break points? Should they have units of g^2/Hz?

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

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

PVC Plastics

- Any PVC plastics or electrical insulation?

A Wire/cable PVC insulation.

Shock/vibe (MIL-STD-810F)

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

(Note: this info is from 1200 SecureSyncs)

- Refer to sites such as: http://telecom-info.telcordia.com/site-cgi/ido/docs.cgi?ID=082705147D000542&KEYWORDS=&TITLE=&DOCUMENT=GR-63&DATE=&CLASS=&COUNT=1000
- Telcordia: NEBS (telecom) requirements for Physical Protection:
  - Criteria for equipment cooling air-inlet and exhaust locations are revised and clarified.
  - Operating temperature test conditions are now a function of the equipment-cooling air-inlet location.
  - A detailed heat dissipation calculation procedure is provided for frame and shelf-level equipment.
- **Fire resistance test methods are updated to address specific service provider requirements.**

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

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

"Zones" of eartquake testing (such as Zone 5, Zone 4, etc)
Per Tim T (from his email further below)
Zone 5 Earthquake esting is the worst case testing.
Zone 4 Equartquake would be pretty rough/

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

(Note: this info is from 1200 SecureSyncs)

Email from Tim Tetrault to Dave Sohn (7 Nov 2018) about Specials testing that has been performed
We did 2 sets of seismic testing. One on the AMDR chassis and one on the QEWR which was the 20" chassis. At the time, we wanted to be conservative so we ruggedized the 20" chassis. We RTV'd components and added a stiffening plate inside. We also used the full length rack ears that run the length of the chassis. We only had to do testing for the easiest of the zones. Zone 1.

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

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

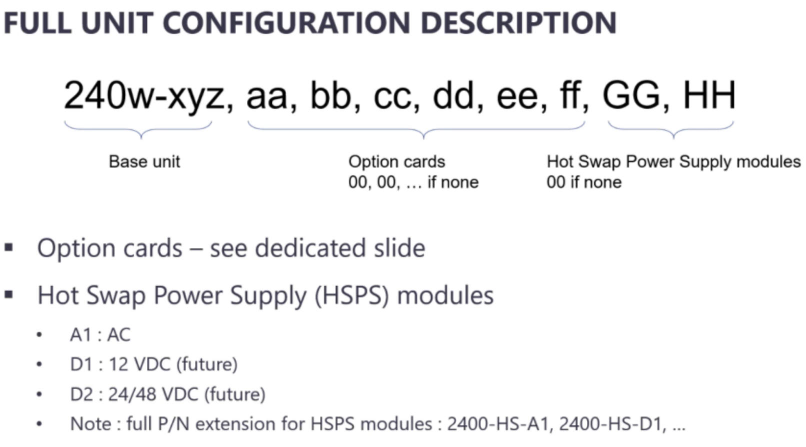
For the QEWR project, we only needed to operate through the seismic event, and meet spec once the event was done. Do we need to meet spec through the seismic event? Phase Noise? I see below that there is an operational vibration spec. Do we know what spec's we need to meet during the vibration?

CCATS Number for SecureSync

- Refer to "CCATS Numbers" Section in the Custserviceassist doc: ..\CustomerServiceAssistance.pdf

ECAT DS (ECATS) Number for SecureSync

2400 SecureSync Model Numbering scheme



FULL UNIT CONFIGURATION DESCRIPTION

$\underbrace{\text{240w-xyz}}_{\text{Base unit}}, \underbrace{\text{aa, bb, cc, dd, ee, ff}}_{\text{Option cards}}, \underbrace{\text{GG, HH}}_{\text{Hot Swap Power Supply modules}}$

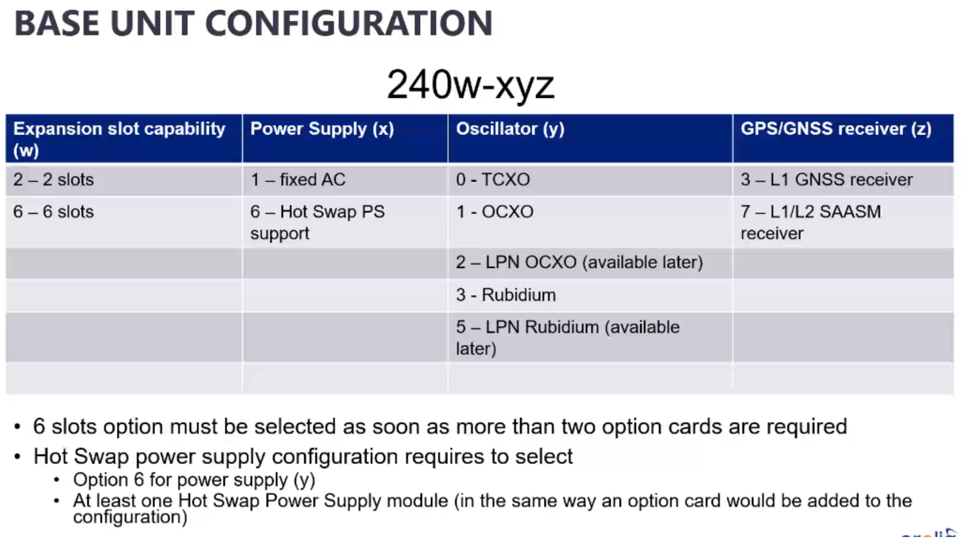
Base unit

Option cards
00, 00, … if none

Hot Swap Power Supply modules
00 if none

- Option cards – see dedicated slide
- Hot Swap Power Supply (HSPS) modules
  - A1 : AC
  - D1 : 12 VDC (future)
  - D2 : 24/48 VDC (future)
  - Note : full P/N extension for HSPS modules : 2400-HS-A1, 2400-HS-D1, …

Model 240w- xyz

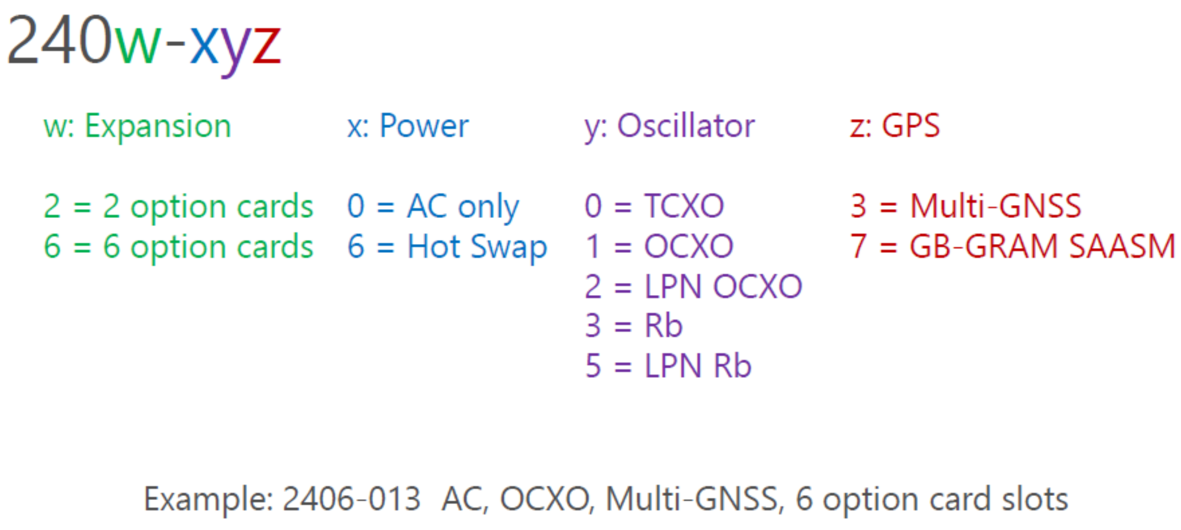


BASE UNIT CONFIGURATION

240w-xyz

Expansion slot capability (w)	Power Supply (x)	Oscillator (y)	GPS/GNSS receiver (z)
2 – 2 slots	1 – fixed AC	0 - TCXO	3 – L1 GNSS receiver
6 – 6 slots	6 – Hot Swap PS support	1 - OCXO	7 – L1/L2 SAASM receiver
		2 – LPN OCXO (available later)	
		3 - Rubidium	
		5 – LPN Rubidium (available later)	

- 6 slots option must be selected as soon as more than two option cards are required
- Hot Swap power supply configuration requires to select
  - Option 6 for power supply (y)
  - At least one Hot Swap Power Supply module (in the same way an option card would be added to the configuration)

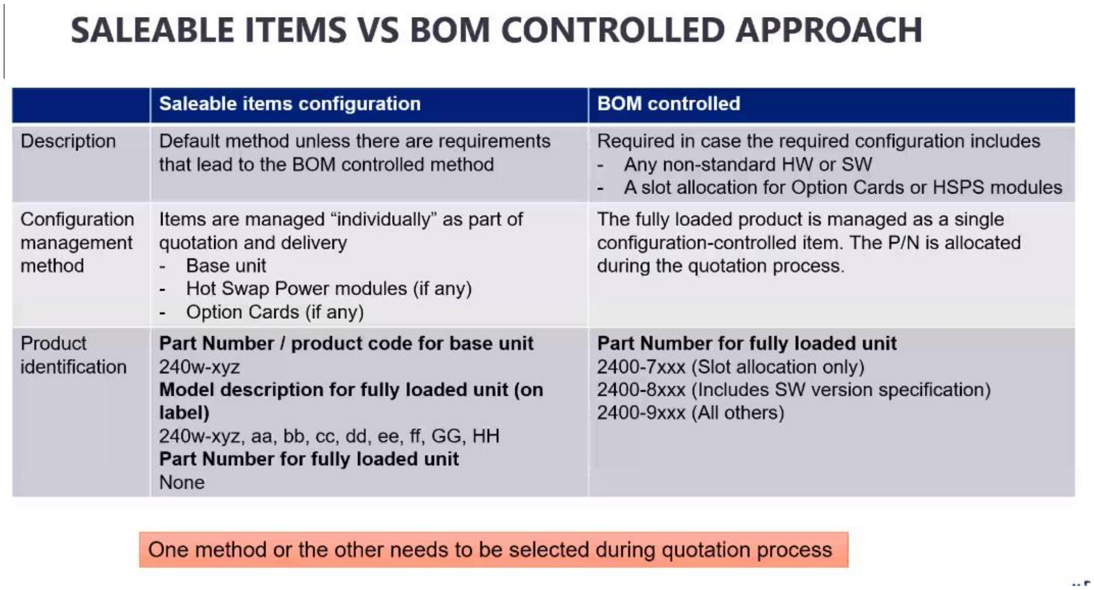


240w-xyz

w: Expansion	x: Power	y: Oscillator	z: GPS
2 = 2 option cards	0 = AC only	0 = TCXO	3 = Multi-GNSS
6 = 6 option cards	6 = Hot Swap	1 = OCXO	7 = GB-GRAM SAASM
		2 = LPN OCXO	
		3 = Rb	
		5 = LPN Rb	

Example: 2406-013 AC, OCXO, Multi-GNSS, 6 option card slots

Standard vs BOM Options (such as special software version)



SALEABLE ITEMS VS BOM CONTROLLED APPROACH

	Saleable items configuration	BOM controlled
Description	Default method unless there are requirements that lead to the BOM controlled method	Required in case the required configuration includes - Any non-standard HW or SW - A slot allocation for Option Cards or HSPS modules
Configuration management method	Items are managed “individually” as part of quotation and delivery - Base unit - Hot Swap Power modules (if any) - Option Cards (if any)	The fully loaded product is managed as a single configuration-controlled item. The P/N is allocated during the quotation process.
Product identification	**Part Number / product code for base unit** 240w-xyz **Model description for fully loaded unit (on label)** 240w-xyz, aa, bb, cc, dd, ee, ff, GG, HH **Part Number for fully loaded unit** None	**Part Number for fully loaded unit** 2400-7xxx (Slot allocation only) 2400-8xxx (Includes SW version specification) 2400-9xxx (All others)

One method or the other needs to be selected during quotation process

Fault tolerance

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

Enterprise-level Network Monitoring Tools (NMS)/ NRPE (such as Nagios, Zabbis Cacti, Splunk Integration, QRadar, etc)

(Note: this info is from 1200 SecureSyncs)

- Network Monitoring Systems (NMS) and Network Security Management platforms are tools for monitoring network devices.
- Some example NMS systems include Solarwinds, HP OpenView, Nagios, libreNMS,Zabbix and Cacti
- Refer also to the "Enterprise-level network monitoring tools" Section in the custserviceassistance doc for more info. I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf
- SecureSync/9400 series: As of at least software v5.5.1 (Jan 2017), SecureSync/0400 does not have any of these NMS systems installed, as needed for full compatibility (Denis Reilly was looking into this for future implementations).
    - But SecureSync does support SNMP, which is typically supported with the NMS systems (resulting in a partial compatibility with NMS systems).

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

- BMS and IBMS appear to be generic terms for various monitoring systems installed in a building .

"Integrated BMS is the key to 'intelligent buildings', equipped with a variety of monitoring devices and control systems, both automated and manned. Together they help regulate a long array of building services and utilities."

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

Examples of some available Network Monitoring tools/Network Security tools

A) HP OpenView (NNMi)

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

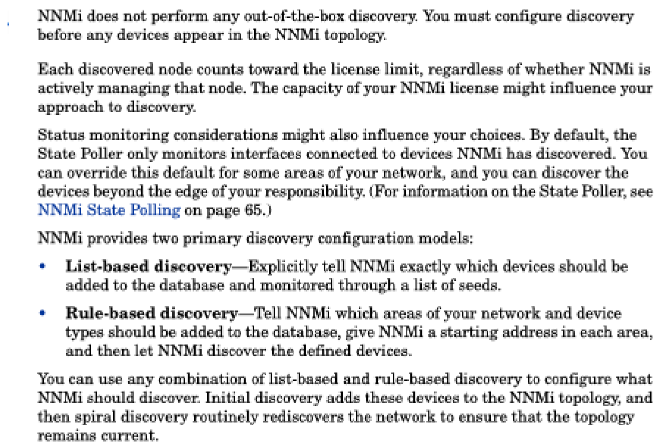
Network Node Manager i (*NNMi*) is a program that helps a network administrator view and manage the conditions in a computer network. *NNMi* is part of the OpenView suite of enterprise system management applications from HPE (Hewlett-Packard Enterprise), the company's business products and services division.

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

Example Unique OID numbers: .1.3.6.1.4.11.2.17.19.2.2.2

Need to configure OpenView not to use NNMI with SecureSyncs

(from the NNMI deployment guide at the link above)



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

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

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

NNMi provides two primary discovery configuration models:

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

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

B) Solarwinds Network Performance Monitor (NPM)

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

NCM 7.3.2
http://downloads.solarwinds.com/solarwinds/Release/OrionNCM/SolarWinds-NCM-v7.3.2-Eval.zip

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

C) Nagios software

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

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

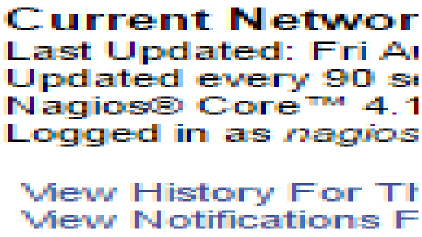
NRPE (Nagios Remote Plugin Executor)

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

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

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

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



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

View History For Th
View Notifications F

D) Zabbix software

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

E) Cacti software

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

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

F) Splunk Integration

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

G) IBM QRadar (Network Security Management platform)

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

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

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

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

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

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

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

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

- Refer to Salesforce case 171498

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

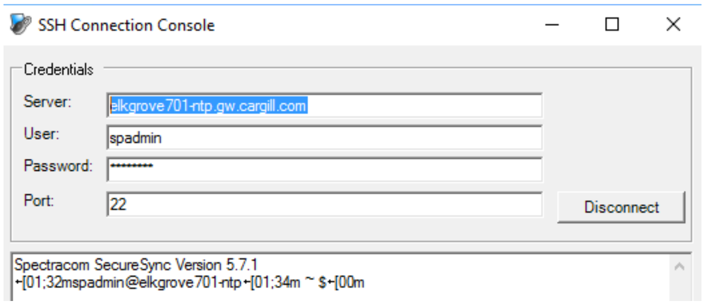
In the Privileged Access Management (PAM) market, buyers are seeking products that not only improve security and accountability, but also don’t impede their users in their day to day job tasks. Offering privileged session management and credential management as a solution from one company means that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

“Post login, it prompts with weird characters”

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

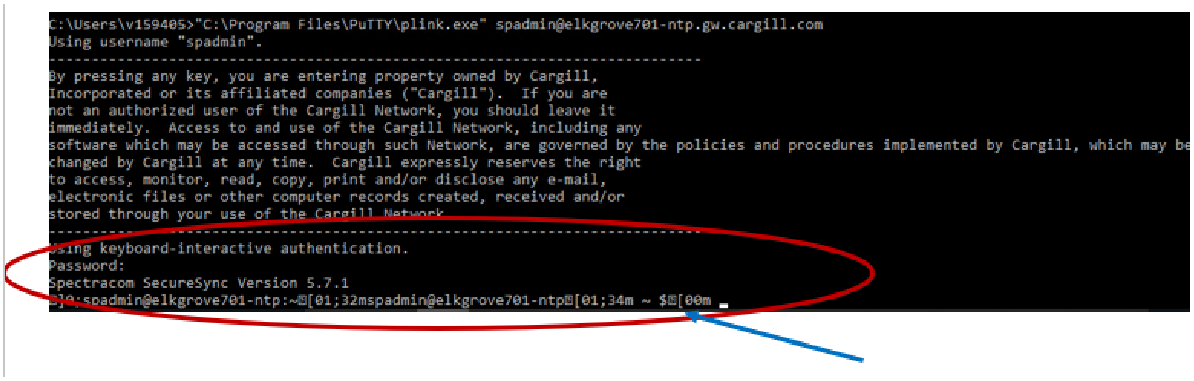
Customer Report (Aug 2018) We have SecureSync setup in our environment and we are integrating its local account password management to Lieberman tool. In pursuing doing this integration we are failing to change the password of the accounts and below is the update from the tools team. Please share your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

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



Server: elkgrove701-ntp.gw.cargill.com
User: spadmin
Password: ********
Port: 22

```
Spectracom SecureSync Version 5.7.1
←[01;32mspadmin@elkgrove701-ntp←[01;34m ~ $←[00m
```



```
C:\Users\v159405>"C:\Program Files\PuTTY\plink.exe" spadmin@elkgrove701-ntp.gw.cargill.com
Using username "spadmin".
---------------------------------------------------------------------------
By pressing any key, you are entering property owned by Cargill,
Incorporated or its affiliated companies ("Cargill").  If you are
not an authorized user of the Cargill Network, you should leave it
immediately.  Access to and use of the Cargill Network, including any
software which may be accessed through such Network, are governed by the policies and procedures implemented by Cargill, which may be
changed by Cargill at any time.  Cargill expressly reserves the right
to access, monitor, read, copy, print and/or disclose any e-mail,
electronic files or other computer records created, received and/or
stored through your use of the Cargill Network.
---------------------------------------------------------------------------
Using keyboard-interactive authentication.
Password:
Spectracom SecureSync Version 5.7.1
]0;spadmin@elkgrove701-ntp:~□[01;32mspadmin@elkgrove701-ntp□[01;34m ~ $□[00m _
```

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

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

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

Excerpt from the Lieberman Tool installation guide:

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

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

Veritas NetBackup (“OS NetBackup”)

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

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

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

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

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

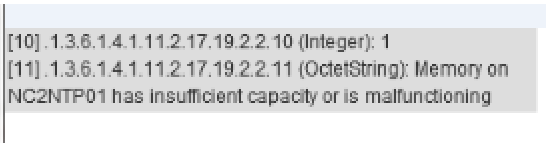
False alerts due to NMS/NNMi being enabled in the SNMP Manager

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

1) Virtual and physical memory has insufficient capacity or malfunctioning

- Refer to SF case 25091 for example

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

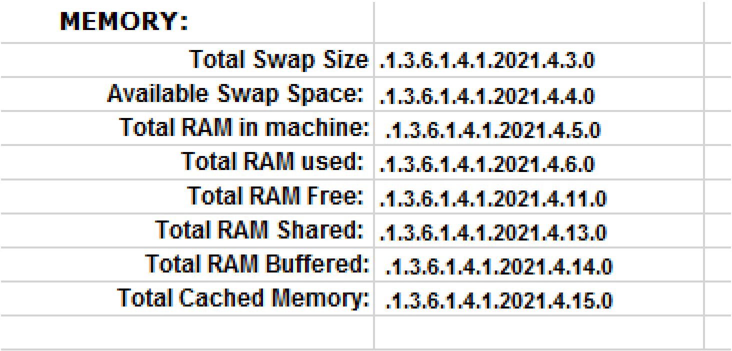


```
[10] .1.3.6.1.4.1.11.2.17.19.2.2.10 (Integer): 1
[11] .1.3.6.1.4.1.11.2.17.19.2.2.11 (OctetString): Memory on
NC2NTP01 has insufficient capacity or is malfunctioning
```

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

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

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



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

Thanks,

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

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

The SecureSync only supports the Spectracom MIBs and some generic MIBs (such as the RFC-1213 MIBS). The SecureSync can't respond to other objects that are unique to the NNMI module. our SecureSync is not responding at all to either of these objects. Since I wasn't sure what they even were, I googled them and found them in a guide for the NNMI module, which explains why I wasn't seeing a response to them. Since the SecureSync is not responding to these objects, it appears their NMS may be incorrectly handling the "no reply" to the objects, resulting in false alerts being asserted,
Even while I am confirming this info with the Engineer, you can go ahead and let your customer know that if their NMS system has configuration available to enable/disable NNMI for each device its monitoring, they should disable NNMI for the SecureSync(s), since the SecureSync does not support this functionally. I highly suspect this will then prevent the false alerts from being asserted.
I will get back to you, with any additional info I receive from the engineer, once he has reviewed it!

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

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

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

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

SecureSync Tech Brief: 1200 SecureSync to 2400 SecureSync Migration Guide

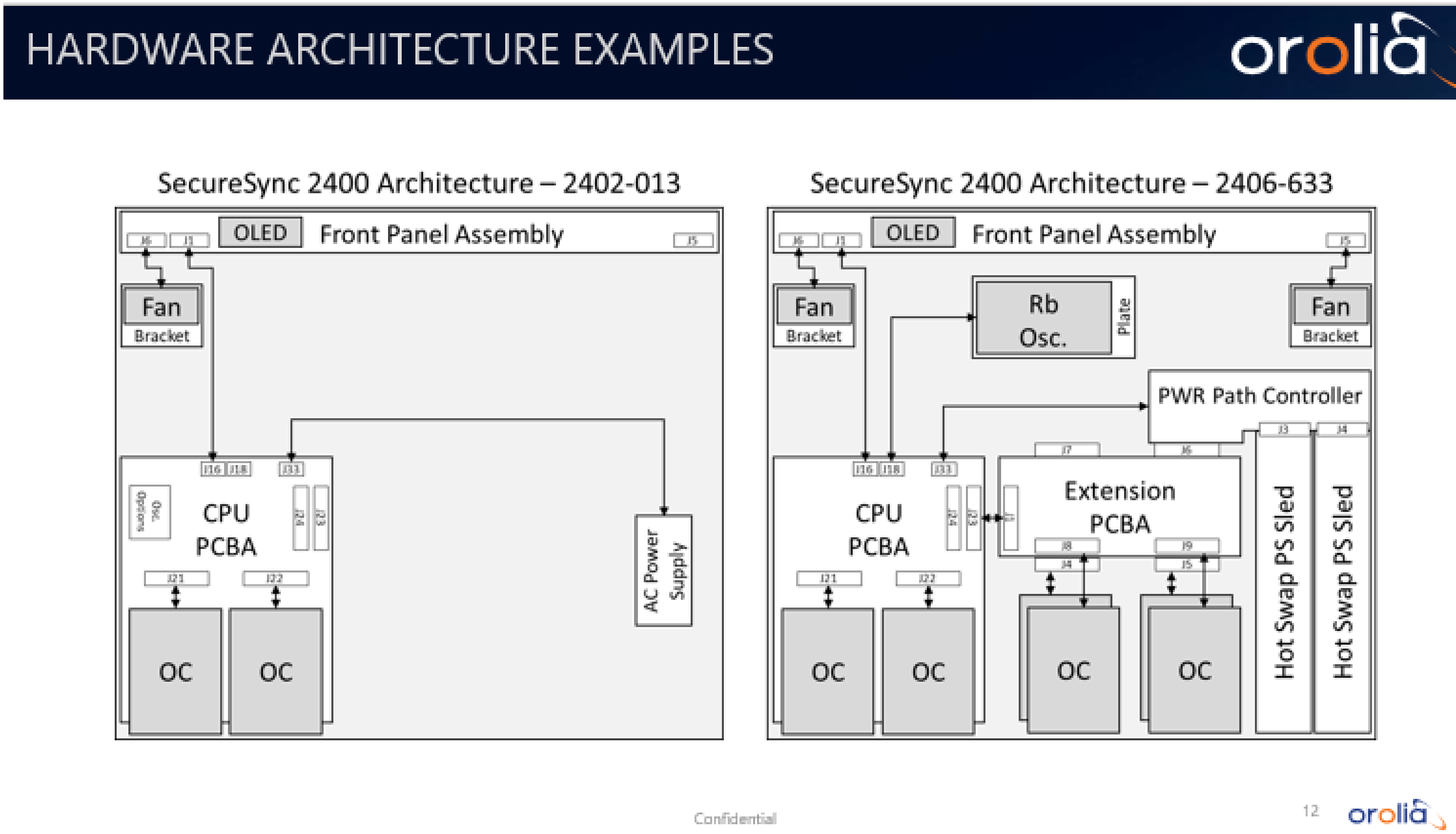
- Refer to our website: https://www.orolia.com/wp-content/uploads/2022/03/SecureSync-1200-to-2400-Migration-Guide_US_03-02-22.pdf

2400 Hardware architecture (CPU board, extension board, Oscillator, Input Power, eMMC Flash memory, etc)

ETX Module

- Unlike 1200 Series SecureSyncs, No ETX Module installed in 2400 series
- Unlike 1200 Series SecureSyncs, No CF card installed in 2400 series (CF card replaced by eMMC/ Micro SD FLASH)

For internal use only!

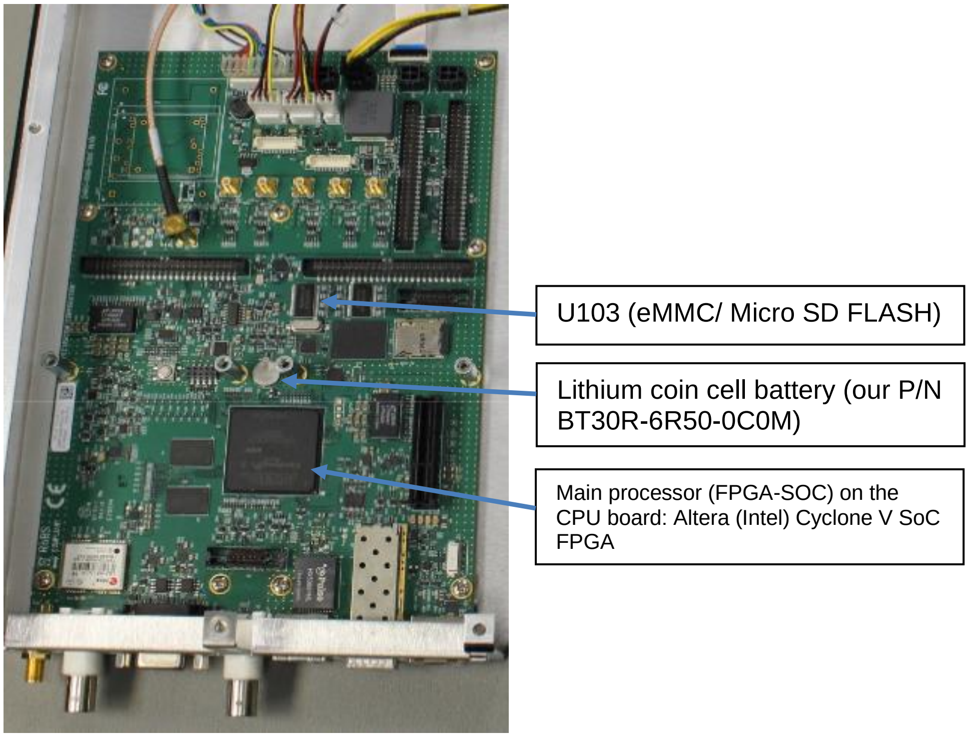


HARDWARE ARCHITECTURE EXAMPLES

SecureSync 2400 Architecture – 2402-013

SecureSync 2400 Architecture – 2406-633

*CPU board in 2400s (P/N 2400-0000-F001)



U103 (eMMC/ Micro SD FLASH)

Lithium coin cell battery (our P/N BT30R-6R50-0C0M)

Main processor (FPGA-SOC) on the CPU board: Altera (Intel) Cyclone V SoC FPGA

- **P/N 2400-0000-F001** In Arena at: https://app.bom.com/items/detail-spec?item_id=1232727526&version_id=11131593098
- **Schematic** for CPU PCBA (2400-1001-0212) in Arena at: https://app.bom.com/items/detail-spec?item_id=1278293579&version_id=11573082998&orb_msg_single_search_p=1
- Outsourced assembly
- Main processor (FPGA-SOC) on the CPU board: Altera (Intel) Cyclone V SoC FPGA
    - Specs: https://ark.intel.com/content/www/us/en/ark/products/210462/cyclone-v-5csxc6-fpga.html
        - Contains Dual-core ARM Cortex processor with up to 925 MHz maximum frequency.
- GNSS Receiver is attached to the CPU board.
- Component U103 (our P/N U060R-F8GB-010P): eMMC/ Micro SD FLASH (replaces CF card installed in 1200 SecureSyncs)

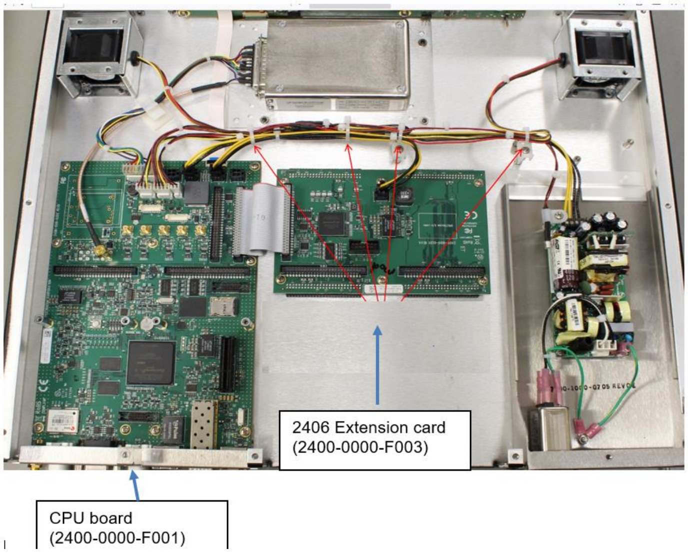
*(U103) eMMC/ Micro SD FLASH on CPU PCBA (replaces need for CF card) / micro-SD Card

- eMMC Flash memory (IC U103, our P/N U060-F8GB-010P in Arena at https://app.bom.com/items/detail-spec?item_id=1277510351&version_id=11572531398) mounted on the CPU board alleviates need for CF Card.
- Contains 8GB eMMC FLASH
- microSD card holder available to optionally install a micro-SD Card (Our P/N MP20R-0022-032)

1200 SecureSync CF card usage versus 2400 SecureSync eMMC usage

- Refer to Salesforce cases, such as especially Case 291205 (Nov 2022)

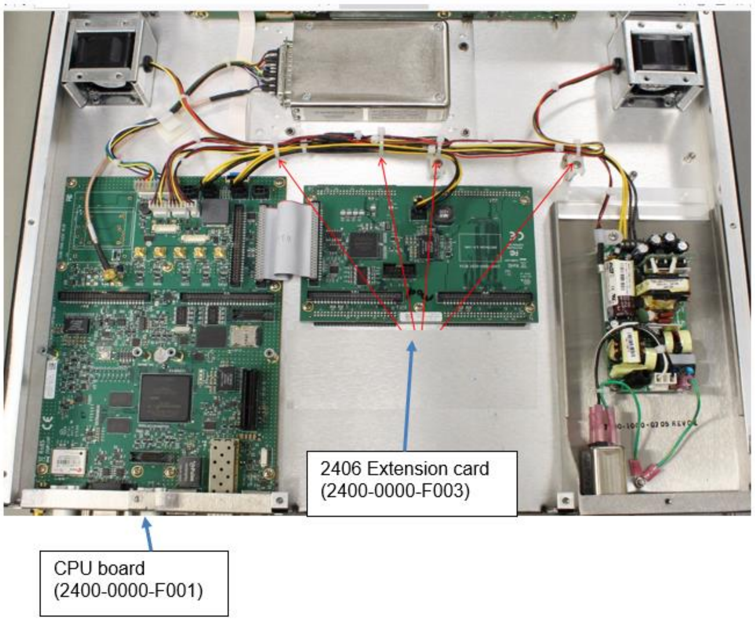
2406 Extension board (P/N 2400-0000-F003)



- Installed on 2406 SecureSyncs to allow up to four additional Option cards be installed (instead of just two)
  - **Two** Option cards can be attached to jack on bottom row
  - **Two** Option cards can be attached to top of board using ribbon cables
- Not installed in 2402 SecureSyncs
- In Arena at: https://app.bom.com/items/detail-spec?item_id=1232777535&version_id=11837183688

2400 series (2402 / 2406) SecureSync Top Assemblies

A) 2406 configs (six option card bays)



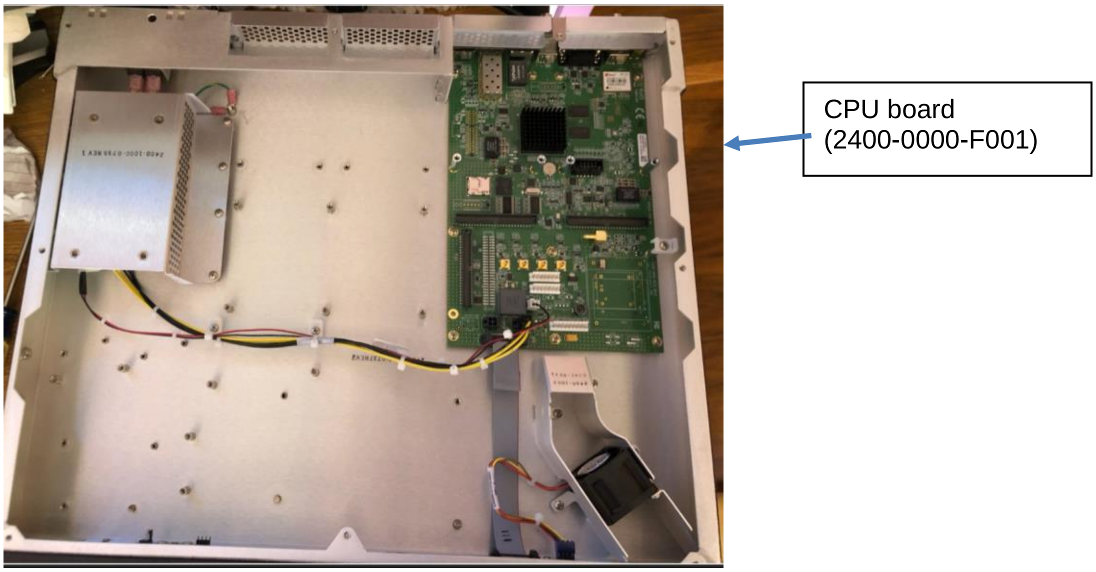
1. 2406-033

- **In SalesForce: (not yet in Salesforce, as of Jan 2019)**
- **In Arena:** https://app.bom.com/items/detail-bom-sourcing?item_id=1259608607&version_id=11319292528&&redirect_seqno=11786798505
- **Process detail (2400-X33-PD in Arena): SecureSync with Rb osc (in Arena)** https://app.bom.com/items/detail-spec?item_id=1262384882&version_id=11254179818&
- **First released to production ~7 March 2019 (refer to ECO-1946 in SAP)**

Configuration

- **SIX Option Card bays** (Up to Six Option Cards can be installed)
- **Power**=AC only (built-in. No hot swap modules available)
- Rb oscillator
- Commercial receiver (ublox)

B) 2402 configs (two option card bays)



2402 SecureSync with TCXO

1. **2402-033**
   - ○ In SalesForce: (not yet in Salesforce, as of Jan 2019)
   - ○ In Arena: https://app.bom.com/items/detail-spec?item_id=1233303800&version_id=10746377978&
   - ○ Process detail (2400-X33-PD in Arena): SecureSync with Rb osc (in Arena) https://app.bom.com/items/detail-spec?item_id=1262384882&version_id=11254179818&

Configuration

- ○ Up to two Option Cards can be installed
- ○ **Power**=AC only (built-in. No hot swap modules available)
- ○ Rb oscillator
- ○ Commercial receiver (ublox)

2. **2402-013**
   - **In SalesForce: (not yet in Salesforce, as of Jan 2019)**
   - **In Arena:** https://app.bom.com/items/detail-spec?item_id=1263043934&version_id=11263225738
   - **Process detail (240C-X13-PD in Arena):** https://app.bom.com/items/detail-spec?item_id=1233303800&version_id=10746377978&

Configuration

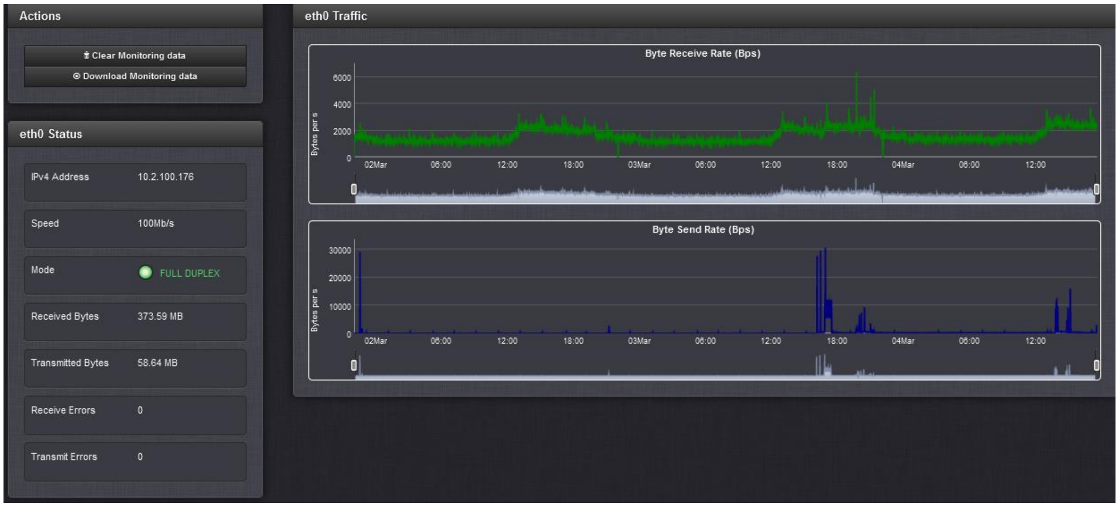
- ○ **Two Option Card bays** (Up to two Option Cards can be installed)
- ○ Power=AC only (built-in. No hot swap modules available)
- ○ OCXO oscillator
- ○ Commercial receiver (ublox)

Ethernet Monitor page and graphs

A) Eth0 only

***Tools* -> *Ethernet Monitor* page**

- ➢ Eth0 transmit/receive graphs are in the Tools -> Ethernet Monitor page

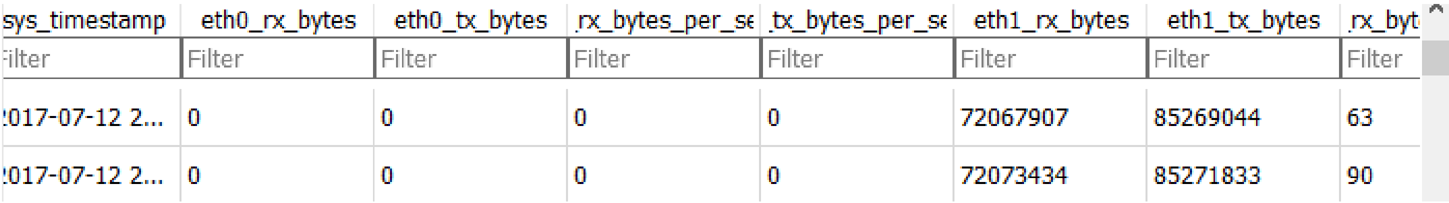


eth0 Status

IPv4 Address	10.2.100.176
Speed	100Mb/s
Mode	● FULL DUPLEX
Received Bytes	373.59 MB
Transmitted Bytes	58.64 MB
Receive Errors	0
Transmit Errors	0

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

- ➢ Sqlite database (“log_eth_mons” table) reports ethernet throughput (received/transmit)



sys_timestamp	eth0_rx_bytes	eth0_tx_bytes	rx_bytes_per_se	tx_bytes_per_se	eth1_rx_bytes	eth1_tx_bytes	rx_byt
ilter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
017-07-12 2...	0	0	0	0	72067907	85269044	63
017-07-12 2...	0	0	0	0	72073434	85271833	90

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

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

(Note: this info is from 1200 SecureSyncs)

- KTS Timing system microprocessor (U1) - the “inner” processor - CPU usage not available via either CLI or web browser.
  - KTS processor (U1) is for running the timing system.

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

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

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

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

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

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

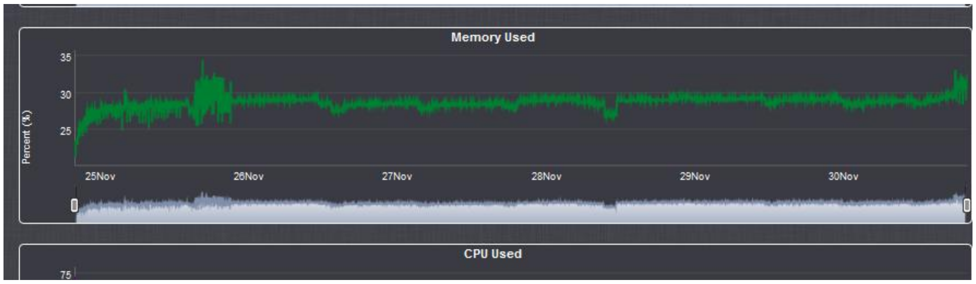
- Memory and CPU usage graphs and the Tools -> System Monitor page were added in v5.3.1

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

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

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

- This graph available starting in software update version 5.3.1



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

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

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

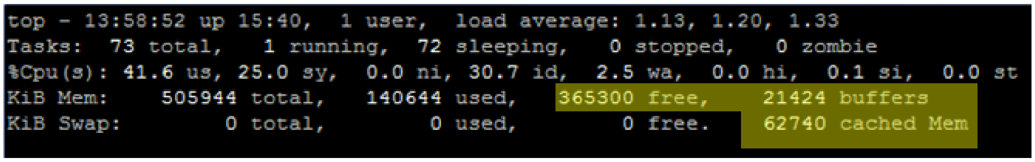
4. Reading the "outer" processor memory stats via CLI (telnet/SSH or serial)

- Can use CLI commands such as "top", "free", free -m , cat proc/meminfo or vmstat to read the CPU's free memory

- Note that free, top and vmstat all report the same memory values

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

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



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

"CPU" associated fields

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

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

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

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

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

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

- Starting in software update version 5.0.0, the Linux OS (Gentoo) grabs as much available RAM memory as possible and holds it until memory is requested. It then releases memory as needed. It is completely normal/ expected for free memory to continue to drop over time. Low/decreasing free memory (in versions 5.0.0 and above) is NOT a sign of a memory consumption issue. Memory is being reassigned as needed in these newer versions of software updates.

- Refer to knowledge base article on our site: http://support.spectracomcorp.com/articles/FAQ/free-cpu-memory?q=free%20mem&

- top automatically updates once every 5 seconds by default.

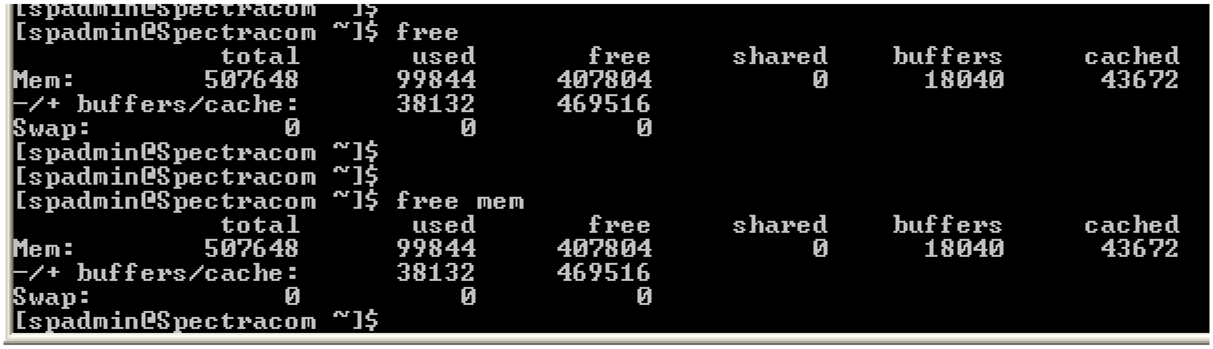
- Refer to Mantis case 3029.

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

A. Free, free mem, free -m commands

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

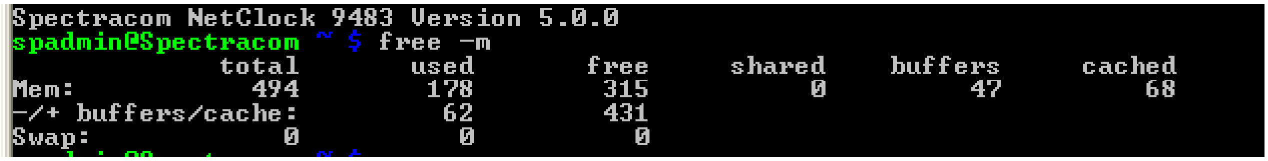
free -m (reports in Megabytes instead of kilobytes)



```
[spadmin@Spectracom ~]$
[spadmin@Spectracom ~]$ free
             total       used       free     shared    buffers     cached
Mem:        507648      99844     407804          0      18040      43672
-/+ buffers/cache:      38132     469516
Swap:            0          0          0
[spadmin@Spectracom ~]$
[spadmin@Spectracom ~]$
[spadmin@Spectracom ~]$ free mem
             total       used       free     shared    buffers     cached
Mem:        507648      99844     407804          0      18040      43672
-/+ buffers/cache:      38132     469516
Swap:            0          0          0
[spadmin@Spectracom ~]$
```

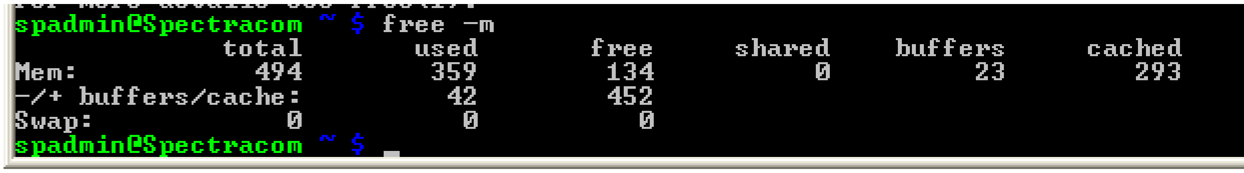
free -m (reports in Megabytes instead of kilobytes)

(With version 4.8.8 installed)



```
Spectracom NetClock 9483 Version 5.0.0
spadmin@Spectracom ~ $ free -m
             total       used       free     shared    buffers     cached
Mem:           494        178        315          0         47         68
-/+ buffers/cache:         62        431
Swap:            0          0          0
```

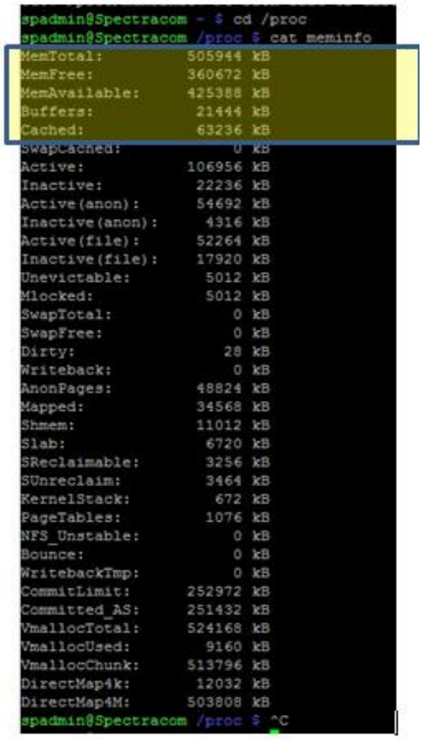
(With version 5.0.2 installed)



```
For more details see free(1).
spadmin@Spectracom ~ $ free -m
             total       used       free     shared    buffers     cached
Mem:           494        359        134          0         23        293
-/+ buffers/cache:         42        452
Swap:            0          0          0
spadmin@Spectracom ~ $ _
```

B. cat /proc/meminfo

- /proc/meminfo also reports info on free memory

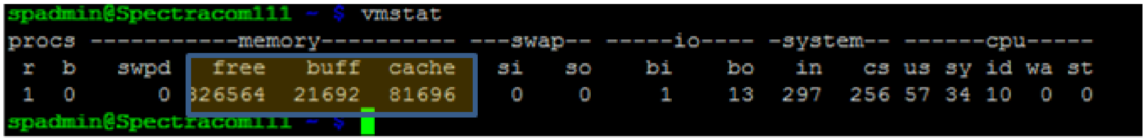


```
spadmin@Spectracom ~ $ cd /proc
spadmin@Spectracom /proc $ cat meminfo
MemTotal:         505944 kB
MemFree:          360672 kB
MemAvailable:     425388 kB
Buffers:           21444 kB
Cached:            63236 kB
SwapCached:            0 kB
Active:           106956 kB
Inactive:          22236 kB
Active(anon):      54692 kB
Inactive(anon):     4316 kB
Active(file):      52264 kB
Inactive(file):    17920 kB
Unevictable:        5012 kB
Mlocked:            5012 kB
SwapTotal:             0 kB
SwapFree:              0 kB
Dirty:                28 kB
Writeback:             0 kB
AnonPages:         48824 kB
Mapped:            34568 kB
Shmem:             11012 kB
Slab:               6720 kB
SReclaimable:       3256 kB
SUnreclaim:         3464 kB
KernelStack:         672 kB
PageTables:         1076 kB
NFS_Unstable:          0 kB
Bounce:                0 kB
WritebackTmp:          0 kB
CommitLimit:      252972 kB
Committed_AS:     251432 kB
VmallocTotal:     524168 kB
VmallocUsed:        9160 kB
VmallocChunk:     513796 kB
DirectMap4k:       12032 kB
DirectMap4M:      503808 kB
spadmin@Spectracom /proc $ ^C
```

C. Linux vmstat and vmstat 1 CLI commands

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

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



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

Field descriptions for the vmstat command

Memory

swpd: the amount of virtual memory used.
free: the amount of idle memory.
buff: the amount of memory used as buffers.
cache: the amount of memory used as cache.
inact: the amount of inactive memory. (-a option)
active: the amount of active memory. (-a option)

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

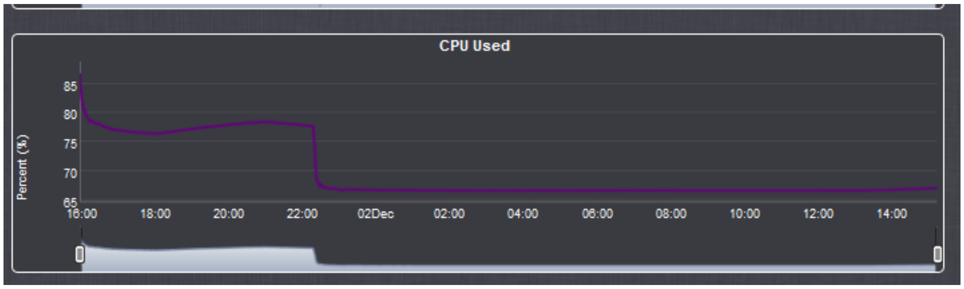
(Note: this info is from 1200 SecureSyncs)

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

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

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

- ➢ This graph available starting in update version 5.3.1

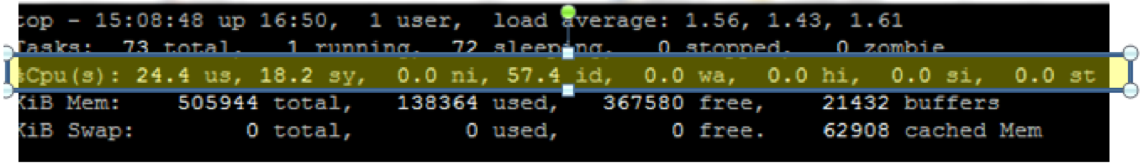


2. Reading the “outer” processor’s CPU usage stats via CLI (telnet/SSH or serial)

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

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

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



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

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

“CPU” associated fields

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

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

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

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

- ➢ “top” CLI command to retrieve the CPU usage is a standard linux command.
- ➢ top automatically updates once every 5 seconds by default.
- ➢ Refer to Mantis case 3029.
- ➢ CPU usage is a comparison of processor “use time” versus “rest time”.
- ➢ CPU usage is high in the SecureSync because ETX is a single core processor running multiple threads.
    - In version 5.2.0, CPU usage is running around 85 to 90%. After downgrade to version 5.1.2, similar values

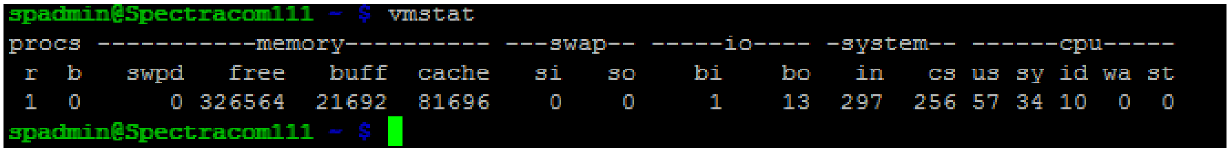
still being reported (around 91%).

- Though the usage is high, NTP is the one of the higher priority threads. So NTP performance is NOT affected in any way by the high CPU usage.

B) Linux vmstat and vmstat 1 CLI commands

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

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



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

Field descriptions for the vmstat command

CPU

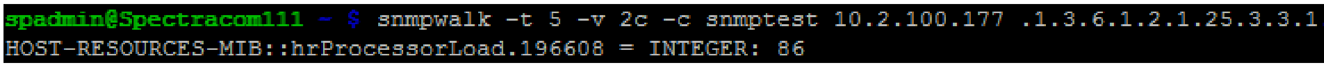
These are percentages of total CPU time.
us: Time spent running non-kernel code. (user time, including nice time)
sy: Time spent running kernel code. (system time)
id: Time spent idle. Prior to Linux 2.5.41, this includes IO-wait time.
wa: Time spent waiting for IO. Prior to Linux 2.5.41, shown as zero.

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

C) Reading the "outer" processor stats Via SNMP

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

SNMP object for reading "outer" CPU usage for all Versions of SecureSync software: .1.3.6.1.2.1.25.3.3.1.2



```
spadmin@Spectracom111 ~ $ snmpwalk -t 5 -v 2c -c snmptest 10.2.100.177 .1.3.6.1.2.1.25.3.3.1
HOST-RESOURCES-MIB::hrProcessorLoad.196608 = INTEGER: 86
```

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

percentage of user CPU time: .1.3.6.1.4.1.2021.11.9.0
raw user cpu time: .1.3.6.1.4.1.2021.11.50.0
percentages of system CPU time: .1.3.6.1.4.1.2021.11.10.0
raw system cpu time: .1.3.6.1.4.1.2021.11.52.0
percentages of idle CPU time: .1.3.6.1.4.1.2021.11.11.0
raw idle cpu time: .1.3.6.1.4.1.2021.11.53.0
raw nice cpu time: .1.3.6.1.4.1.2021.11.51.0

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

(Note: this info is from 1200 SecureSyncs)

Factors potentially adversely affecting CPU usage

- Having a more recent software version installed (versions 5.8.0 and above)

  Per Dave Sohn (7 Sept 2018) CPU utilization increase is due to patches required for Spectre/Meltdown vulnerability fixes. Removing/protecting speculative execution by the CPU does have an effect on processing efficiency.

- Having an earlier, less-efficient software version installed (**such as versions 5.4.0 or below**)
  - Having MANY NTP clients hitting the SecureSync at the same time (one or all interfaces)
  - Timekeeper option enabled and running (i.e. Morgan Stanley)
  - SNMP Manager(s) walking the SNMP MIB files (this can really increase usage)
  - FTP (especially when navigating to different directories) or telnet,ssh and HTTP/HTTPS browser connections (especially when there are many simultaneous cnn
  - Heavy network traffic

Recommended Suggestions

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

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

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

Many different conditions can affect the normal and periodic spikes in CPU usage valued, including SNMP operations (walking the SNMP MIBS has a large impact on this value) and heavy network traffic, for examples. For this reason, we recommend not walking the SNMP MIBS – we recommend polling individual values instead of walking the mib files. Is your SNMP Manager(s) walking the SecureSyncs' MIB files? If so, how often are the MIBs being walked (periodically or continuously)?

SSH and other logins can also increase the CPU usage above its typical values The typical "idle" CPU usage is around 60% to 70%. But SNMP Walks and other external connections can cause this to increase to around 90% to 95%. To prevent the normal operation of the SecureSync from causing superfluous high CPU usage alerts being sent, I recommend setting the alert threshold for CPU usage of the SecureSync in your SNMP Manager to a value such as 95% for instance (note that high CPU usage does not adversely affect the timing capabilities of the unit), If the alerts are continuing to be sent it wasn't just a one-time occurrence), find out if the SNMP Manager is walking the MIB files and was there one or more users logged into the SecureSync when the alert was sent? If the Manager is walking the MIB files, we recommend stopping the walks and then see if the alerts stop being sent.

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

My response

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

Before adjusting your CPU usage alert threshold levels accordingly for remotely monitoring the SecureSync, which version of software is currently installed in at least SecureSync NTPTTN32? And what is its typical CPU usage (note the CPU usage can be near, or at, 100% without adversely affecting the SecureSync's operation).

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

A) With the newer black background web browser (starting in software version 5.1.0), the System version is reported in the **Tools** -> **Upgrade/backup** page of the browser.

B) With a CLI command prompt (telnet, ssh or front panel RS-232 connection) type **version** <enter>. The response indicates the current version.

C) With earlier versions (which the web browser has a white/gray background) the Archive software version is reported at the top of the **Tools** -> **Versions** page.

Software version factors which can affect typical CPU usage observed:

A) Software Version 5.8.0 and above being installed: CPU utilization increase in newer versions of software is due to patches required for Spectre/Meltdown vulnerability fixes. Removing/protecting speculative execution by the CPU does have an adverse effect on processing efficiency.

B) Earlier software versions, such as versions 5.40 and 5.3.1 being installed: Software version 5.4.1 increased the efficiency of the software, thus allowing for a small decrease in the CPU usage typically observed,

Other Questions / suggestions for you:

1) Are you walking the SecureSync's SNMP MIB files from one or more SNMP Managers? If you are, try temporarily stopping this action and see what its usage drops to thereafter (walking its MIB files, instead of using SNMP Gets for particular object values, can significantly increase its CPU usage).

2) The **Management** -> **NTP Setup** page of the web browser includes "**NTP Throughput graphs**" of how often NTP in the SecureSync is responding to NTP requests (can you send us a screenshot of these two graphs for review)?

3) The SecureSync's log bundle records ethernet data, which we can use to see if periods of higher CPU usage correlate with higher network traffic. Further below is info on how to upload to us the unit's logs and configs bundles (two separate files), if you would like us to review these files for you, to see what they indicate.

4) Does the SecureSync have the Model 1204-06 GB Ethernet Option Card installed (adding three additional ethernet interfaces to the single ethernet interface, eth0, installed in all SecureSyncs)? If it does. how many of these three additional interface ports are connected to networks (just one, two of the three, or all three)? Or, is just the interface eth0 on the base chassis of all SecureSyncs (near the AC power connector) connected to a network?

5) How many computers are opening web browser or CLI connections to the SecureSync at the same time?

6) About how many computers/NTP clients are configured syncing to the SecureSync (tens of clients. or thousands of clients. for instance)? If you aren't sure how many clients/which clients are getting time from the SecureSync, this info can be obtained from a wireshark/tcpdump packet capture of UDP port 123 (the NTP port) on all ethernet interfaces of the SecureSync. Filter the capture using the "destination" address of the SecureSync (all NTP packets being sent to all SecureSync interfaces, eth0 thru eth3 which are connected to networks)

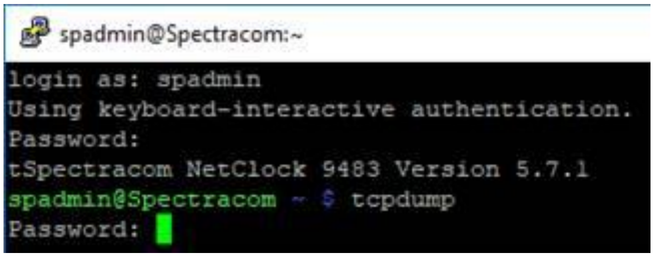
A) **Just interface eth0 connected to a network**, type: **tcpdump dst port 123**<enter>

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

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

Notes about TCPdump:

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



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

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

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

(Note: this info is from 1200 SecureSyncs)

Operating System

Name of Linux distribution we use in 2400s (as of at least versions 1.7.0 and below): "**Buildroot**" (as compared to the Model 1200 SecureSyncs running on "**Gentoo"** Linux)

Unrelated message from Ryan Johnson 6/1/2023: We did open a case with Tenable and their response was that the issue likely stems from the 2400 using **Buildroot as the Linux distribution and which Nessus doesn't know anything about** (as opposed to Gentoo Linux on the 1200 which Nessus does).

- SecureSync runs on (GNU/Linux)?

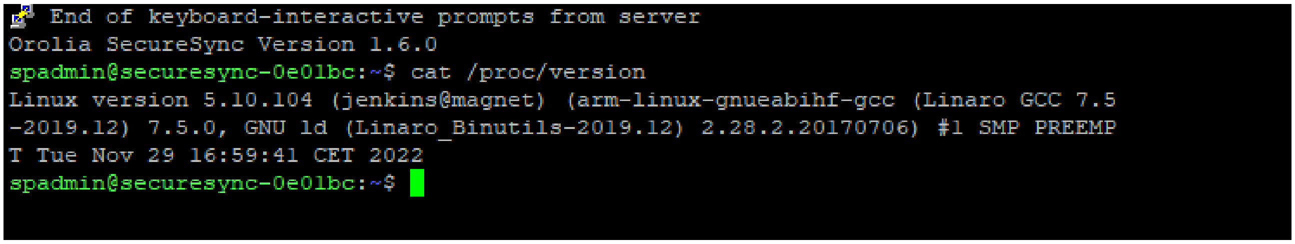
How is GNU different from Linux?

The GNU operating system is a complete free software system, upward-compatible with Unix. GNU stands for "**GNU's Not Unix**." It is pronounced as one syllable with a hard g. Richard Stallman made the Initial Announcement of the GNU Project in September 1983.

GNU is an operating system with different types of computer softwares, while Linux is a free and open-source software built around the Linux Kernel. It is one of the core differences between them. All the softwares of GNU is under the GNU project, while Linux is an GNU-based OS.

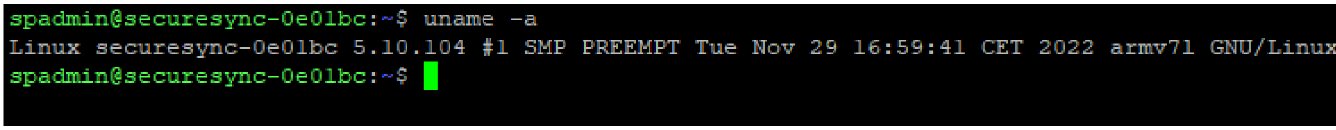
- **CLI commands to read Linux OS (kernel) version and distribution version:**

  cat /proc/version



```
 End of keyboard-interactive prompts from server
Orolia SecureSync Version 1.6.0
spadmin@securesync-0e01bc:~$ cat /proc/version
Linux version 5.10.104 (jenkins@magnet) (arm-linux-gnueabihf-gcc (Linaro GCC 7.5
-2019.12) 7.5.0, GNU ld (Linaro_Binutils-2019.12) 2.28.2.20170706) #1 SMP PREEMP
T Tue Nov 29 16:59:41 CET 2022
spadmin@securesync-0e01bc:~$
```

- **uname –a**



```
spadmin@securesync-0e01bc:~$ uname -a
Linux securesync-0e01bc 5.10.104 #1 SMP PREEMPT Tue Nov 29 16:59:41 CET 2022 armv7l GNU/Linux
spadmin@securesync-0e01bc:~$
```

Kernel versions

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

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

Software licenses of open source software

(Note: this info is from 1200 SecureSyncs)

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

1) NTP
2) OpenSSH
3) OpenSSL

Ability to view open source software licenses in the browser.

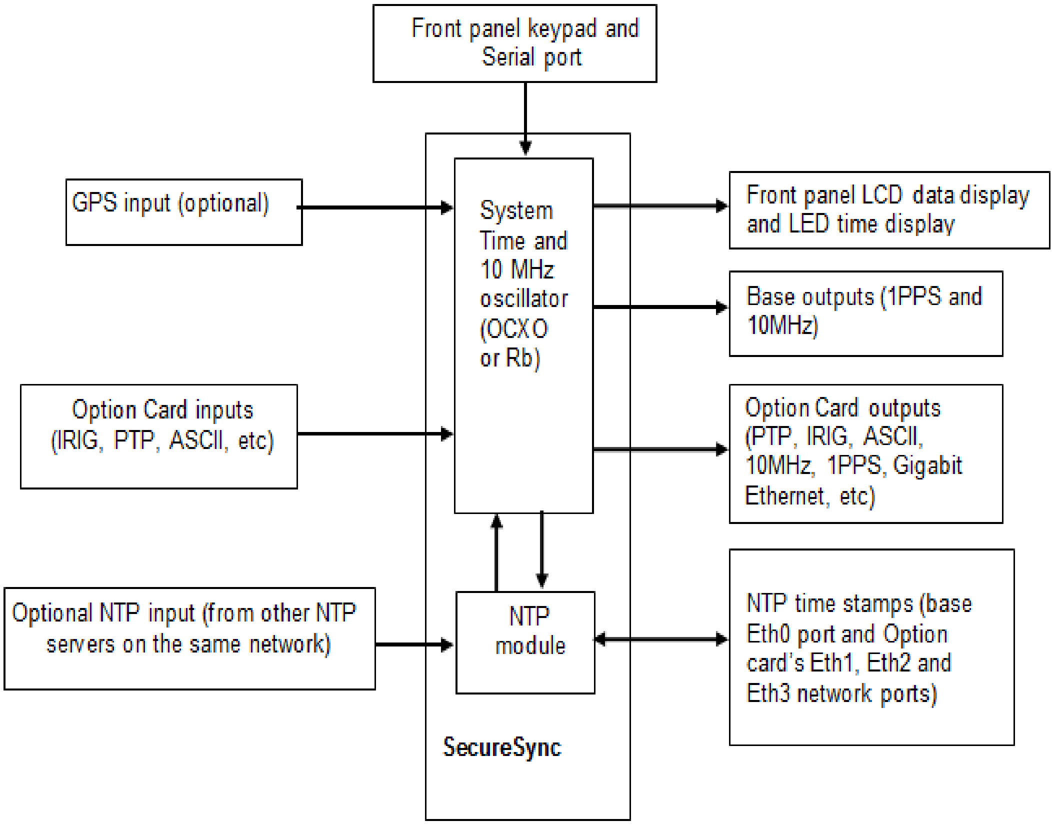
- ➢ Use the Browser's "Developer Tools" (shortcut: CTRL + Shift and the letter "i", and select "debugger") to view the Javascript files.
- ➢ For example, MIT license (for code such as dygraph) just requires a header be added to our code.

MIT's dygraph license for graphs.

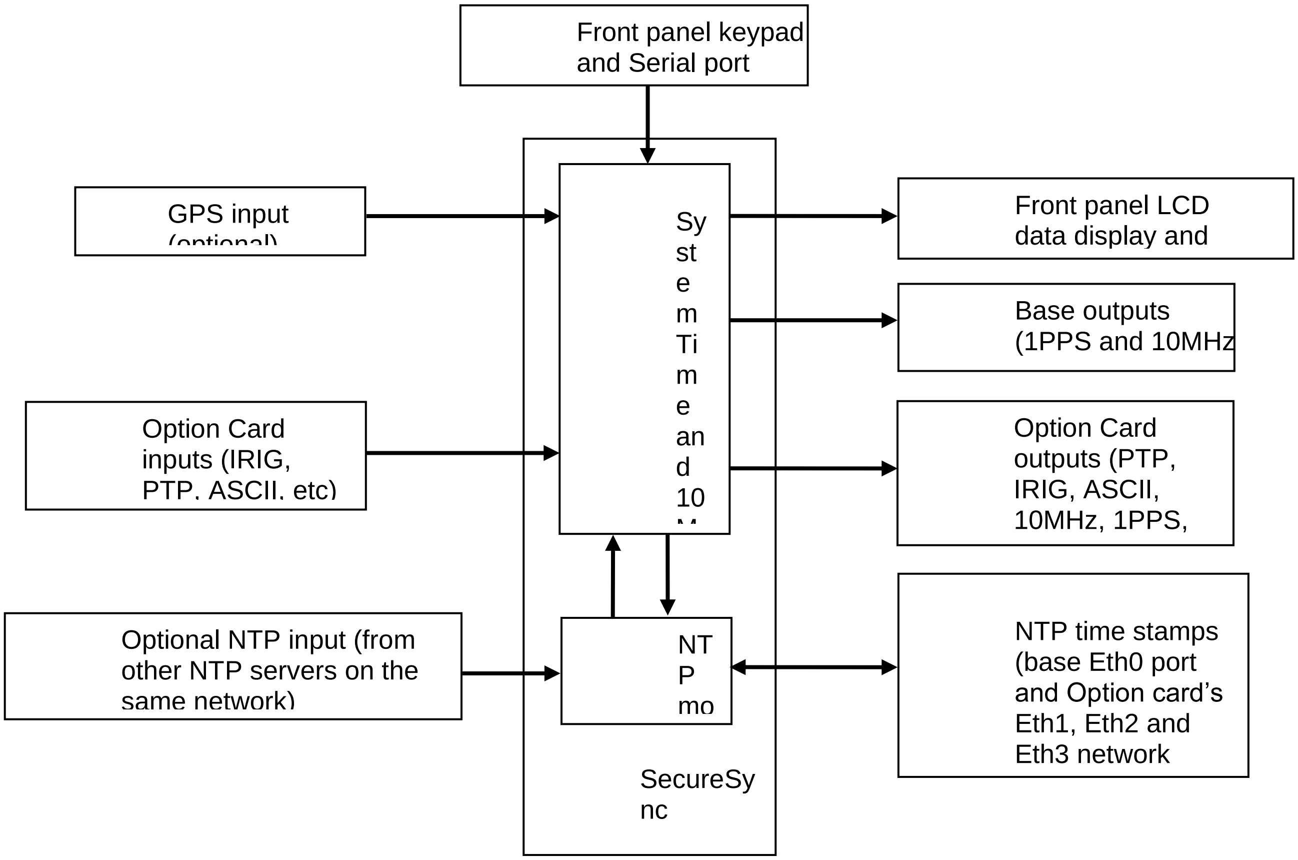
- ➢ Refer to steps above to view the dygraph.js file (Select "dygraph-combined.js") and the license is shown in the top line.

System operation block diagram (for internal use only)

(Note: this info is from 1200 SecureSyncs)


Front panel keypad and Serial port
GPS input (optional)
System Time and 10 MHz oscillator (OCXO or Rb)
Front panel LCD data display and LED time display
Base outputs (1PPS and 10MHz)
Option Card inputs (IRIG, PTP, ASCII, etc)
Option Card outputs (PTP, IRIG, ASCII, 10MHz, 1PPS, Gigabit Ethernet, etc)
Optional NTP input (from other NTP servers on the same network)
NTP module
NTP time stamps (base Eth0 port and Option card's Eth1, Eth2 and Eth3 network ports)
SecureSync

(for edits)

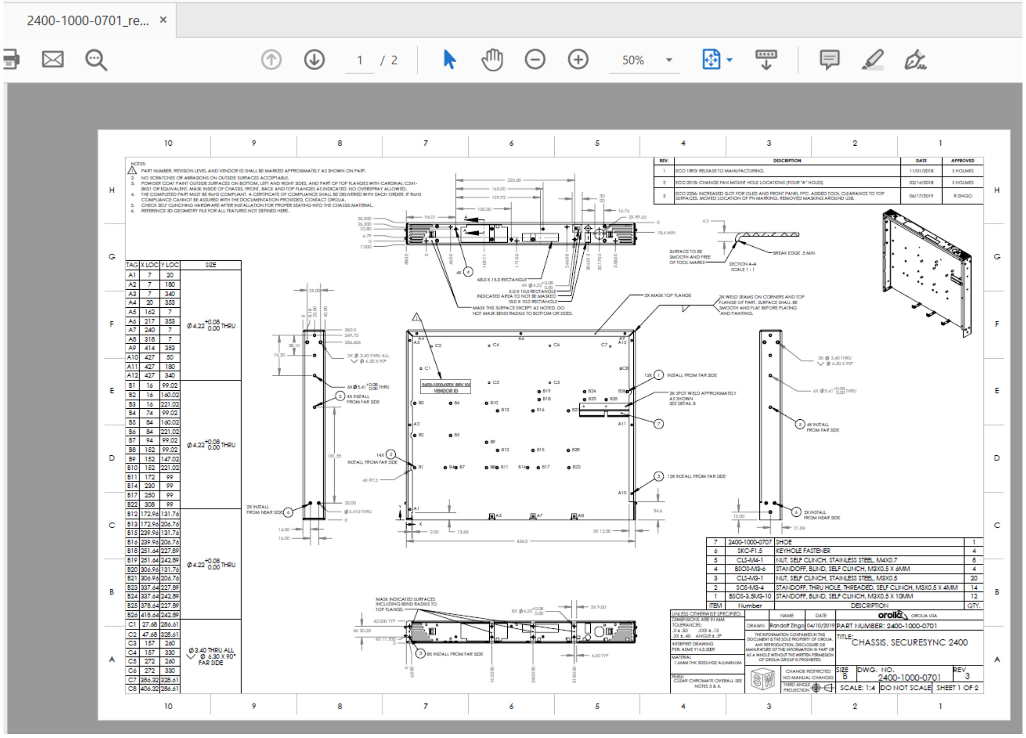

Front panel keypad and Serial port
GPS input (optional)
Sy st e m Ti m e an d 10 M
Front panel LCD data display and
Base outputs (1PPS and 10MHz
Option Card inputs (IRIG, PTP, ASCII, etc)
Option Card outputs (PTP, IRIG, ASCII, 10MHz, 1PPS,
Optional NTP input (from other NTP servers on the same network)
NT P mo
NTP time stamps (base Eth0 port and Option card's Eth1, Eth2 and Eth3 network
SecureSy nc

CAD/3D/Dimensional/Chassis mechanical drawings

- **Refer to:** I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync-2400 (Diamond)\CAD - 3D drawings

Dimensional drawings

- Refer to 2400 SecureSync online user guide at: https://www.orolia.com/manuals/2400/Content/NC_and_SS/2400/INTRO/Specs_MechEnv.htm
- Chassis mechanical drawing: 2400-1000-0701 (For much greater detail) excerpted below


2400-1000-0701_re... ×
1 / 2
50%
10
9
8
7
6
5
4
3
2
1
H
G
F
E
D
C
B
A
SURFACE TO BE SMOOTH AND FREE OF TOOL MARKS
BREAK EDGE .5 MIN
SECTION A-A SCALE 1 : 1
3X MASK TOP FLANGE
3X WELD SEAMS ON CORNERS AND TOP FLANGE OF PART. SURFACE SHALL BE SMOOTH AND FLAT BEFORE PLATING AND PAINTING.
12X INSTALL FROM FAR SIDE
2X INSTALL FROM NEAR SIDE
4X INSTALL FROM FAR SIDE
14X INSTALL FROM FAR SIDE
8X INSTALL FROM FAR SIDE

NOTES:
1. PART NUMBER, REVISION LEVEL AND VENDOR ID SHALL BE MARKED APPROXIMATELY AS SHOWN ON PART.
2. NO SCRATCHES OR ABRASIONS ON OUTSIDE SURFACES ACCEPTABLE.
3. POWDER COAT PAINT OUTSIDE SURFACES ON BOTTOM, LEFT AND RIGHT SIDES, AND PART OF TOP FLANGES WITH CARDINAL C241-BKD1 OR EQUIVALENT. MASK INSIDE OF CHASSIS, FRONT, BACK AND TOP FLANGES AS INDICATED. NO OVERSPRAY ALLOWED.
4. THE COMPLETED PART MUST BE RoHS COMPLIANT. A CERTIFICATE OF COMPLIANCE SHALL BE DELIVERED WITH EACH ORDER. IF RoHS COMPLIANCE CANNOT BE ASSURED WITH THE DOCUMENTATION PROVIDED, CONTACT OROLIA.
5. CHECK SELF CLINCHING HARDWARE AFTER INSTALLATION FOR PROPER SEATING INTO THE CHASSIS MATERIAL.
6. REFERENCE 3D GEOMETRY FILE FOR ALL FEATURES NOT DEFINED HERE.

REV.	DESCRIPTION	DATE	APPROVED
1	ECO 1893: RELEASE TO MANUFACTURING.	11/01/2018	S HOLMES
2	ECO 2018: CHANGE FAN MOUNT HOLE LOCATIONS (FOUR "A" HOLES)	02/14/2018	S HOLMES
3	ECO 2236: INCREASED SLOT FOR OLED AND FRONT PANEL FPC. ADDED TOOL CLEARANCE TO TOP SURFACES. MOVED LOCATION OF PN MARKING. REMOVED MASKING AROUND USB.	06/17/2019	R ZINGO

TAG	X LOC	Y LOC	SIZE
A1	7	20	Ø4.22 $^{+0.08}_{0.00}$ THRU
A2	7	180	
A3	7	340	
A4	20	353	
A5	162	7	
A6	217	353	
A7	240	7	
A8	318	7	
A9	414	353	
A10	427	50	
A11	427	180	
A12	427	340	
B1	16	99.02	Ø4.22 $^{+0.08}_{0.00}$ THRU
B2	16	160.02	
B3	16	221.02	
B4	74	99.02	
B5	84	160.02	
B6	84	221.02	
B7	94	99.02	
B8	152	99.02	
B9	152	147.02	
B10	152	221.02	
B11	172	99	
B14	230	99	
B17	250	99	
B22	308	99	
B12	172.96	131.76	Ø4.22 $^{+0.08}_{0.00}$ THRU
B13	172.96	206.76	
B15	239.96	131.76	
B16	239.96	206.76	
B18	251.64	227.89	
B19	251.64	242.89	
B20	306.96	131.76	
B21	306.96	206.76	
B23	337.64	227.89	
B24	337.64	242.89	
B25	378.64	227.89	
B26	418.64	242.89	
C1	27.68	286.61	Ø3.40 THRU ALL ⌵ Ø 6.30 X 90° FAR SIDE
C2	47.68	328.61	
C3	157	260	
C4	157	330	
C5	272	260	
C6	272	330	
C7	386.32	328.61	
C8	406.32	286.61	

ITEM	Number	DESCRIPTION	QTY.
7	2400-1000-0707	SHOE	1
6	SKC-F1.5	KEYHOLE FASTENER	4
5	CLS-M4-1	NUT, SELF CLINCH, STAINLESS STEEL, M4X0.7	8
4	BSOS-M3-6	STANDOFF, BLIND, SELF CLINCH, M3X0.5 X 6MM	4
3	CLS-M3-1	NUT, SELF CLINCH, STAINLESS STEEL, M3X0.5	20
2	SOS-M3-4	STANDOFF, THRU HOLE, THREADED, SELF CLINCH, M3X0.5 X 4MM	14
1	BSOS-3.5M3-10	STANDOFF, BLIND, SELF CLINCH, M3X0.5 X 10MM	12

UNLESS OTHERWISE SPECIFIED:
DIMENSIONS ARE IN MM
TOLERANCES:
.X ± .50 .XXX ± .15
.XX ± .40 ANGLE ± .5°

INTERPRET DRAWING PER: ASME Y14.5:2009

MATERIAL: 1.6MM THK 5052-H32 ALUMINUM

FINISH: CLEAR CHROMATE OVERALL SEE NOTES 3 & 4.

	NAME	DATE
DRAWN	Randolf Zingo	04/10/2019

orolia OROLIA USA

PART NUMBER: 2400-1000-0701

THE INFORMATION CONTAINED IN THIS DOCUMENT IS THE SOLE PROPERTY OF OROLIA. ANY REPRODUCTION, DISCLOSURE OR MANUFATURE OF THIS INFORMATION IN PART OR AS A WHOLE WITHOUT THE WRITTEN PERMISSION OF OROLIA GROUP IS PROHIBITED.

TITLE: CHASSIS, SECURESYNC 2400

CHANGE RESTRICTED NO MANUAL CHANGES

THIRD ANGLE PROJECTION

SIZE B | DWG. NO. 2400-1000-0701 | REV 3

SCALE: 1:4 | DO NOT SCALE | SHEET 1 OF 2

Hardware block diagram

Kramden Timing System (KTS)

(Note: this info is from 1200 SecureSyncs)

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

KTS consists of the following four components:

A. Microprocessor (U1):

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

to the micro.

B. FPGA (U40):

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

C. EEPROM (U2):

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

D. 10 MHz oscillator

Notes:

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

**Indications of KTS not running

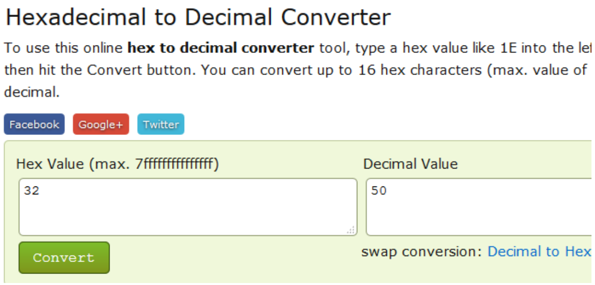
- ➢ Front panel LED time display frozen (not incrementing)
- ➢ Potentially- Several "KTS failed to read" log entries in the logs
- ➢ Potentially- difficulty with communicating with the browser/CLI due to ETX not being able to talk to KTS.

**ktsif file

- ➢ This KTS hardware configuration file is located in the home/spectracom/config directory
- ➢ It's like a batch file for hardware configuration at each boot-up.
- ➢ With the exception of the 1204-12 PTP card (which is the only card to internally store its own configs- so there won't be any listed PTR calls listed in this file), this file defines which cards are installed, and in which slots they are installed in (it will vary unit to unit, if the same cards aren't installed in the same slots).
- ➢ Defines other parameters such as Holdover timeout, System Timescale, etc.

Note: Option Cards are called by their hex number, but handled in the system by the corresponding decimal value

Example: The 1204-32 card in the sytem is actually "50" (refer to sites such as: http://www.binaryhexconverter.com/hex-to-decimal-converter)



Hexadecimal to Decimal Converter

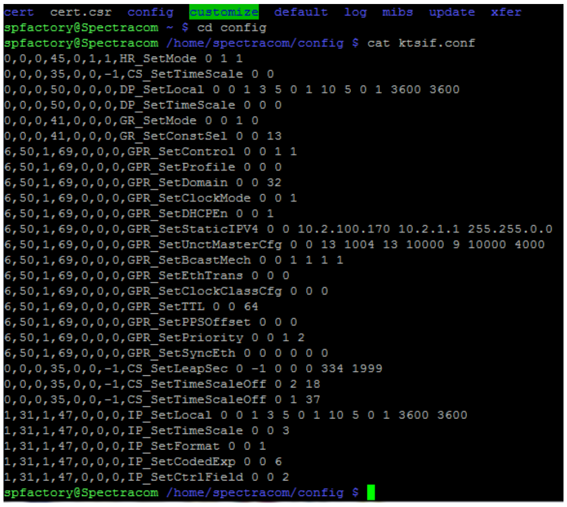
To use this online **hex to decimal converter** tool, type a hex value like 1E into the le
then hit the Convert button. You can convert up to 16 hex characters (max. value of
decimal.

Hex Value (max. 7fffffffffffffff): 32

Decimal Value: 50

swap conversion: Decimal to Hex

Internal note: this file is a great way to see syntaxes of various TSync calls (such as **IR_** calls for IRIG input, **IP_**calls for IRIG outputs for example), configure a particular Option Card as desired and then view the file to get the full api call (login to cli as spfactory, cd to config and then type **cat ktsif.conf**)/ Example screenshot below is from v5.6.0



```
cert  cert.csr  config  customize  default  log  mibs  update  xfer
spfactory@Spectracom ~ $ cd config
spfactory@Spectracom /home/spectracom/config $ cat ktsif.conf
0,0,0,45,0,1,1,HR_SetMode 0 1 1
0,0,0,35,0,0,-1,CS_SetTimeScale 0 0
0,0,0,50,0,0,0,DP_SetLocal 0 0 1 3 5 0 1 10 5 0 1 3600 3600
0,0,0,50,0,0,0,DP_SetTimeScale 0 0 0
0,0,0,41,0,0,0,GR_SetMode 0 0 1 0
0,0,0,41,0,0,0,GR_SetConstSel 0 0 13
6,50,1,69,0,0,0,GPR_SetControl 0 0 1 1
6,50,1,69,0,0,0,GPR_SetProfile 0 0 0
6,50,1,69,0,0,0,GPR_SetDomain 0 0 32
6,50,1,69,0,0,0,GPR_SetClockMode 0 0 1
6,50,1,69,0,0,0,GPR_SetDHCPEn 0 0 1
6,50,1,69,0,0,0,GPR_SetStaticIPV4 0 0 10.2.100.170 10.2.1.1 255.255.0.0
6,50,1,69,0,0,0,GPR_SetUnctMasterCfg 0 0 13 1004 13 10000 9 10000 4000
6,50,1,69,0,0,0,GPR_SetBcastMech 0 0 1 1 1 1
6,50,1,69,0,0,0,GPR_SetEthTrans 0 0 0
6,50,1,69,0,0,0,GPR_SetClockClassCfg 0 0 0
6,50,1,69,0,0,0,GPR_SetTTL 0 0 64
6,50,1,69,0,0,0,GPR_SetPPSOffset 0 0 0
6,50,1,69,0,0,0,GPR_SetPriority 0 0 1 2
6,50,1,69,0,0,0,GPR_SetSyncEth 0 0 0 0 0 0
0,0,0,35,0,0,-1,CS_SetLeapSec 0 -1 0 0 0 334 1999
0,0,0,35,0,0,-1,CS_SetTimeScaleOff 0 2 18
0,0,0,35,0,0,-1,CS_SetTimeScaleOff 0 1 37
1,31,1,47,0,0,0,IP_SetLocal 0 0 1 3 5 0 1 10 5 0 1 3600 3600
1,31,1,47,0,0,0,IP_SetTimeScale 0 0 3
1,31,1,47,0,0,0,IP_SetFormat 0 0 1
1,31,1,47,0,0,0,IP_SetCodedExp 0 0 6
1,31,1,47,0,0,0,IP_SetCtrlField 0 0 2
spfactory@Spectracom /home/spectracom/config $ 
```

Q The ktsif.conf file in the TU that was upgraded to 5.2.0 (with existing configuration) displays the following, but the ktisf.conf file in the manually configured file does not include the following:

```
0,0,0,37,0,0,-1,SS_SetHoldoverTO 0 432000
0,0,0,53,0,0,0,PP_SetSigCtrl 0 0 1
1,40,2,53,0,0,1,PP_SetSigCtrl 0 1 1
1,40,2,53,0,1,2,PP_SetSigCtrl 0 2 1
1,40,2,53,0,2,3,PP_SetSigCtrl 0 3 1
```

A **Keith's response:** these are internal hardware configurations that are dependent on which Option Cards are installed and what slots those cards are installed in. This info is updated upon each reboot and users don't have access to be able to edit this hardware configuration information.

SetHoldover to 432000 indicates Holdover was changed by a user to be 432,000 seconds

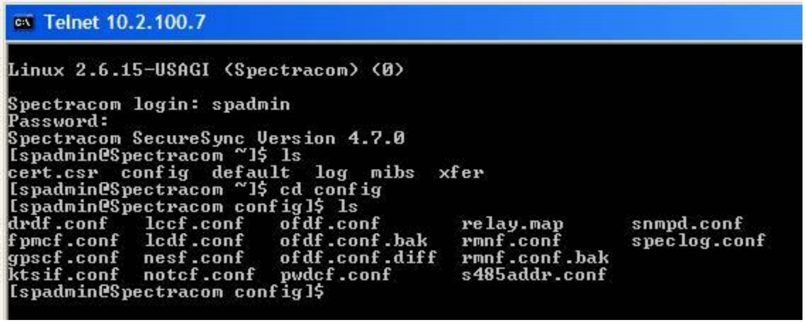
SetSigCtrl is related to Signature Control configuration for the various system/Option card outputs.

Multiple instances of the same type Option Card installed (like more than one IRIG card, for example)
If more than one of the same type Option Card is installed (such as more than one IRIG card, for example), the instance/name of that particular card (such as IRG 0, IRG 1, etc), will be based on the slot number order of the installed cards (starting with Slot 1). This is determined at start-up and provides consistently to the name of the cards. Unless the Option Cards are moved to a different slot or another same-type card is installed in a slot that is closer to Slot 1, each card will always be the same instance number.

Configuration settings of the Option Cards
The Option Card configurations are stored in the ktsif.conf file located in the home/spectracom/config directory. If a customer is having any problems with configuring Option Cards or settings not persisting through power cycles, have them FTP/SCP this file off the SecureSync and also send the System/timing logs for engineering review. Refer to Salesforce case 3918 for Open Access.

I have been working with one of our SecureSync engineers to try to determine why these IRIG output settings may not be persisting through power cycles on at least two of their SecureSyncs. To help us better analyze what may be causing this and when you get a chance, can you send me the following items from at least one of the two SecureSyncs exhibiting this reported symptom issue:

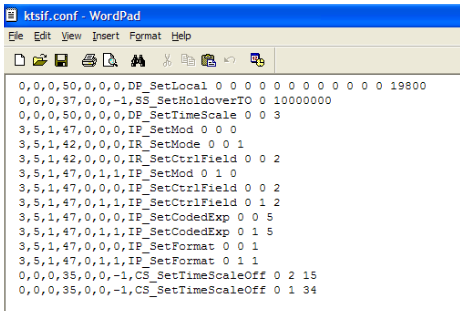
A copy/paste of the **System** and **Timing** logs (Tools/Logs page of web browser).
In the **Home/Spectracom/Config** directory, can you export (using FTP or SCP) the “ktsif.conf” file (as shown below):



```
Linux 2.6.15-USAGI (Spectracom) (0)

Spectracom login: spadmin
Password:
Spectracom SecureSync Version 4.7.0
[spadmin@Spectracom ~]$ ls
cert.csr  config  default  log  mibs  xfer
[spadmin@Spectracom ~]$ cd config
[spadmin@Spectracom config]$ ls
drdf.conf    lccf.conf   ofdf.conf        relay.map       snmpd.conf
fpmcf.conf   lcdf.conf   ofdf.conf.bak    rmnf.conf       speclog.conf
gpscf.conf   nesf.conf   ofdf.conf.diff   rmnf.conf.bak
ktsif.conf   notcf.conf  pwdcf.conf       s485addr.conf
[spadmin@Spectracom config]$
```

We will then analyze the data and get back to you with our findings!

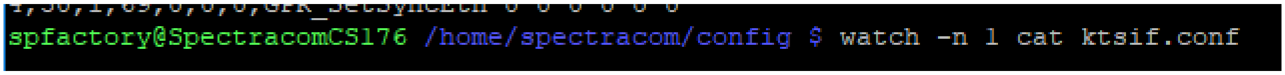
(View ktsif.conf with Notepad/wordpad) Example file from SecureSync is below:



```
0,0,0,50,0,0,0,DP_SetLocal 0 0 0 0 0 0 0 0 0 0 0 0 19800
0,0,0,37,0,0,-1,SS_SetHoldoverTO 0 10000000
0,0,0,50,0,0,0,DP_SetTimeScale 0 0 3
3,5,1,47,0,0,0,IP_SetMod 0 0 0
3,5,1,42,0,0,0,IR_SetMode 0 0 1
3,5,1,42,0,0,0,IR_SetCtrlField 0 0 2
3,5,1,47,0,1,1,IP_SetMod 0 1 0
3,5,1,47,0,0,0,IP_SetCtrlField 0 0 2
3,5,1,47,0,1,1,IP_SetCtrlField 0 1 2
3,5,1,47,0,0,0,IP_SetCodedExp 0 0 5
3,5,1,47,0,1,1,IP_SetCodedExp 0 1 5
3,5,1,47,0,0,0,IP_SetFormat 0 0 1
3,5,1,47,0,1,1,IP_SetFormat 0 1 1
0,0,0,35,0,0,-1,CS_SetTimeScaleOff 0 2 15
0,0,0,35,0,0,-1,CS_SetTimeScaleOff 0 1 34
```

Various ktsif.conf entries associated with specific Option Cards

To watch ktsif.conf file update once-per-second



```
1,50,1,69,0,0,0,GPR_SetSyncEth 0 0 0 0 0 0
spfactory@SpectracomCS176 /home/spectracom/config $ watch -n 1 cat ktsif.conf
```

D) 1204-32 (“GPR_” calls)

1,50,1,69,0,0,0,**GPR_SetControl** 0 0 1 1 (**0 0 1 0** = “**Enable PTP” not selected** or **0 0 1 1** = “**Enable PTP**” selected

1,50,1,69,0,0,0,**GPR_SetProfile** 0 0 **0** (0 0 0 = **default** profile or **0 0 1**= **Telecom** profile)

1,50,1,69,0,0,0,**GPR_SetDomain 0 0 10** (digits after 0 0 indicate domain value, in this case its domain “10”)

1,50,1,69,0,0,0,**GPR_SetClockMode** 0 0 **2** (last digit “**1**”= one step master or last digit “**2**” two step master

1,50,1,69,0,0,0,**GPR_SetDHCPEn** 0 0 **0** (**0 0 0** = **DHCP not enabled** or **0 0 1**= **DHCP enabled**)

1,50,1,69,0,0,0,**GPR_SetStaticIPV4** 0 0 192.168.253.17 192.168.253.18 255.255.255.252 (IP,.gateway mask)

1,50,1,69,0,0,0,**GPR_SetUnctMasterCfg** 0 0 1 **10000 1 10000 4 10000 4000**

1,50,1,69,0,0,0,**GPR_SetBcastMech** 0 0 **1 1 1 1** (**0 0 0** = or **0 0 1**=)

1,50,1,69,0,0,0,**GPR_SetEthTrans** 0 0 **0** (“**Transport protocol**” **0 0 0** = “**IPv4**” or **0 0 1** = **“802.3/Ethernet”**)

1,50,1,69,0,0,0,**GPR_SetClockClassCfg** 0 0 0 (0=“**PTP Clock Class**” “1” = “**Arbitrary**” “2” = “**ITUT G2865.1**”)

1,50,1,69,0,0,0,**GPR_SetTTL** 0 0 64 (digits after 0 0 indicate TTL value, in this case its TTL is “64”)

1,50,1,69,0,0,0,**GPR_SetPPSOffset** 0 0 **0** (last digit “0” =**1PPS offset** value, in this case its PPS offset is **“0**”)

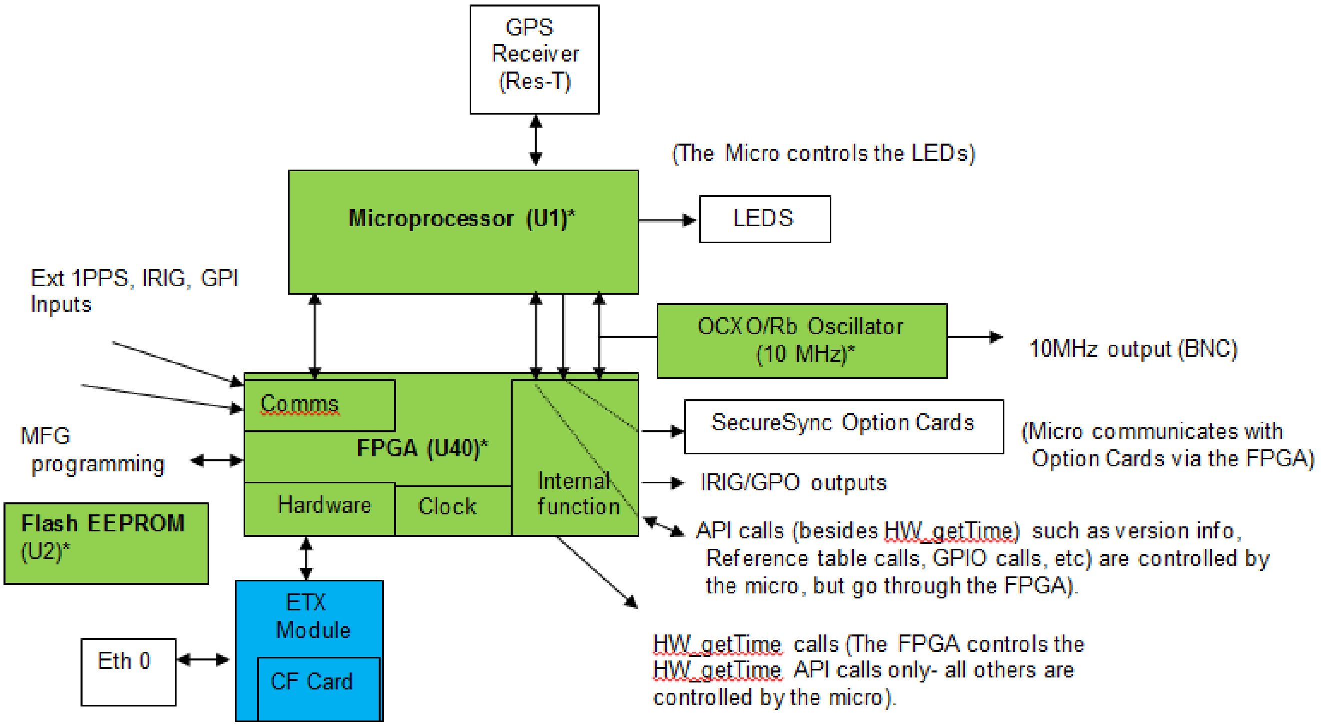
1,50,1,69,0,0,0,**GPR_SetPriority** 0 0 128 254 (digits after 0 0 indicate Priority 1 and Priority 2 values, in this case Priority 1 is “**128**” and Priority 2 is “**254**”)

1,50,1,69,0,0,0,**GPR_SetSyncEth** 0 0 **0 0 0 0** (0 0 0 0 0 0 indicates “**Enable SyncE**” and “**Enable ESMC**” are not selected, while

Network Processor software (NPS)

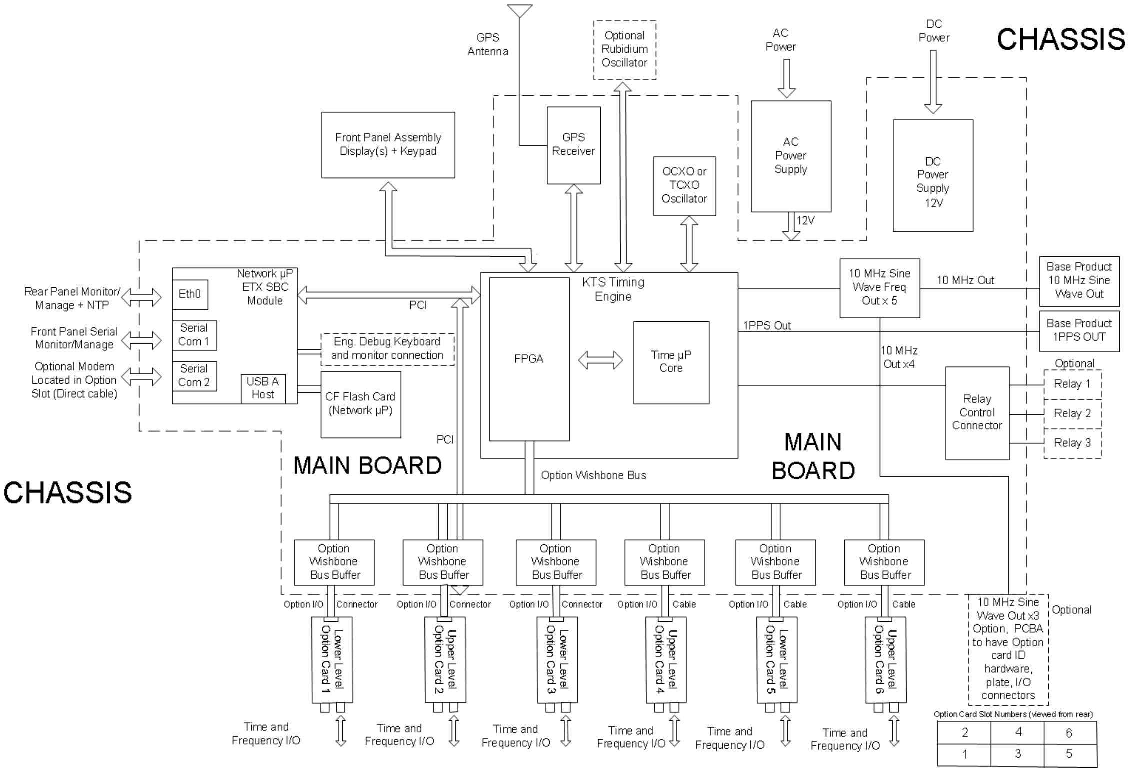
(Note: this info is from 1200 SecureSyncs)

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


GPS Receiver (Res-T)
(The Micro controls the LEDs)
Microprocessor (U1)*
LEDS
Ext 1PPS, IRIG, GPI Inputs
OCXO/Rb Oscillator (10 MHz)*
10MHz output (BNC)
Comms
FPGA (U40)*
MFG programming
SecureSync Option Cards
(Micro communicates with Option Cards via the FPGA)
Internal function
IRIG/GPO outputs
Hardware
Clock
Flash EEPROM (U2)*
API calls (besides HW_getTime) such as version info, Reference table calls, GPIO calls, etc) are controlled by the micro, but go through the FPGA).
ETX Module
Eth 0
CF Card
HW_getTime calls (The FPGA controls the HW_getTime API calls only- all others are controlled by the micro).

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

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


CHASSIS
GPS Antenna
Optional Rubidium Oscillator
AC Power
DC Power
CHASSIS
Front Panel Assembly Display(s) + Keypad
GPS Receiver
OCXO or TCXO Oscillator
AC Power Supply
12V
DC Power Supply 12V
Rear Panel Monitor/ Manage + NTP
Front Panel Serial Monitor/Manage
Optional Modem Located in Option Slot (Direct cable)
Eth0
Network µP ETX SBC Module
Serial Com 1
Serial Com 2
USB A Host
PCI
Eng. Debug Keyboard and monitor connection
CF Flash Card (Network µP)
PCI
KTS Timing Engine
FPGA
Time µP Core
10 MHz Sine Wave Freq Out x 5
10 MHz Out
Base Product 10 MHz Sine Wave Out
1PPS Out
Base Product 1PPS OUT
10 MHz Out x4
Optional
Relay Control Connector
Relay 1
Relay 2
Relay 3
MAIN BOARD
MAIN BOARD
Option Wishbone Bus
Option Wishbone Bus Buffer
Option Wishbone Bus Buffer
Option Wishbone Bus Buffer
Option Wishbone Bus Buffer
Option Wishbone Bus Buffer
Option Wishbone Bus Buffer
Option I/O
Connector
Option I/O
Connector
Option I/O
Connector
Option I/O
Cable
Option I/O
Cable
Option I/O
Cable
10 MHz Sine Wave Out x3 Option, PCBA to have Option card ID hardware, plate, I/O connectors
Optional
Lower Level Option Card 1
Upper Level Option Card 2
Lower Level Option Card 3
Upper Level Option Card 4
Lower Level Option Card 5
Upper Level Option Card 6
Time and Frequency I/O
Time and Frequency I/O
Time and Frequency I/O
Time and Frequency I/O
Time and Frequency I/O
Time and Frequency I/O
Option Card Slot Numbers (viewed from rear)
2
4
6
1
3
5

Halt/Halt-Shutdown performed

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

SecureSync 2400 Ancillary kits (Anc kits/rack ears/brackets, etc)

List of standard SecureSync Anc Kits

A) 2400-0000-0701:

"ANC KIT, 2400 SecureSync, N. AMERICA, AC ONLY (in Arena) https://app.bom.com/items/detail-spec?item_id=1252020550&version_id=11079191208

B) 2400-0000-0702

"ANC KIT 2400 SECURESYNC, N.AMER, AC & DC OPT" (in Arena) https://app.bom.com/items/detail-spec?item_id=1252020575&version_id=11079191608

SMA to Type N adapter cable
CABLE,N JACK,SMA PLUG,RG-316,12in CA01R-0NSA-8001

SecureSync chassis material/mounting brackets/rack ears

(Note: this info is from 1200 SecureSyncs)

Mounting info in the online SecureSync user guide:
http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/Mounting.htm?Highlight=bracket

FAQs about chassis material and mounting

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

Q. What type of plating/ conformal coating is used on the part?
A. No conformal Coating. Rohs Compliant Clear Iridite and Black Annodize.

Email from Scott Holmes (1/11/12)
We specify Cardinal C241-BK01 or equivalent powder coat paint on our products that are painted black.

Note: Responses to questions below in red are from Scott Holmes (3 Dec 2015)
Q What is the material of the unit chassis? Material is 5052-H32 aluminum alloy

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

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

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

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

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

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

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

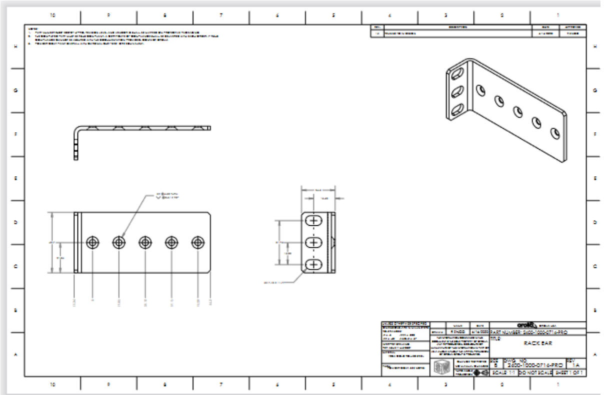
- Refer to "SecureSync M and 0_2.stp" at: I:\Customer Service\EQUIPMENT\SPECTRACOM

EQUIPMENT\SecureSync\CAD - 3D drawings)

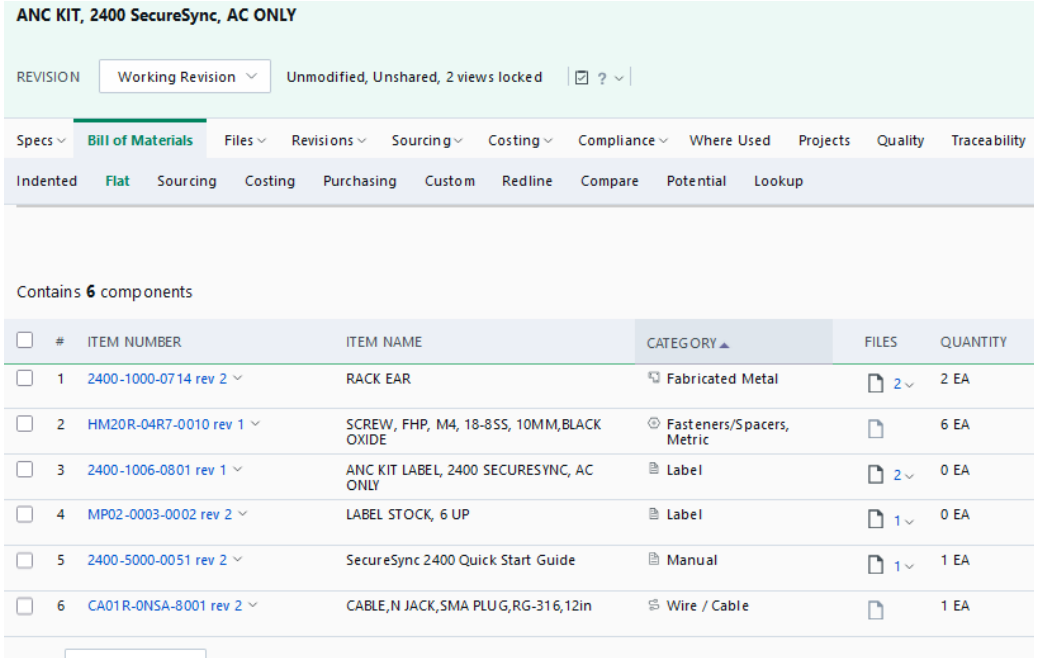
Rack ears/mounting brackets

- Unlike 1200 SecureSyncs/Model 9300 series NTP time servers, 2400 SecureSyncs don't come with a front panel handle (wwhich can be attached to their rack ears)

- 2400 SecureSyncs use DIFFERENT rack ear hardware than the 1200 SecureSyncs/Model 9300 series NTP time servers
- Mechanical drawing of rack ears for 2400 SecureSyncs: Refer to drawing "**2400-1000-0714**" (in Arena) at: https://app.bom.com/items/detail-spec?item_id=1285276681&version_id=11681089288



- We only provide screws to mount the ears to the chassis and the handles to the rack ears. We don't provide the rack screws for attaching the ears to the rack
- The hardware is included in the ancillary kit. The Orolia Part Numbers for the rack ears/hardware are shown in the list below (the full anc kit for North America, AC power only, which includes the rack hardware, is "2400-0000-0701" as shown below):



ANC KIT, 2400 SecureSync, AC ONLY

REVISION Working Revision Unmodified, Unshared, 2 views locked

Contains **6** components

□	#	ITEM NUMBER	ITEM NAME	CATEGORY ▲	FILES	QUANTITY
□	1	2400-1000-0714 rev 2	RACK EAR	Fabricated Metal	2	2 EA
□	2	HM20R-04R7-0010 rev 1	SCREW, FHP, M4, 18-8SS, 10MM,BLACK OXIDE	Fasteners/Spacers, Metric		6 EA
□	3	2400-1006-0801 rev 1	ANC KIT LABEL, 2400 SECURESYNC, AC ONLY	Label	2	0 EA
□	4	MP02-0003-0002 rev 2	LABEL STOCK, 6 UP	Label	1	0 EA
□	5	2400-5000-0051 rev 2	SecureSync 2400 Quick Start Guide	Manual	1	1 EA
□	6	CA01R-0NSA-8001 rev 2	CABLE,N JACK,SMA PLUG,RG-316,12in	Wire / Cable		1 EA

- The **(6) HM20R-04R7-0010** (Metric, 10MM long. 18-8 SS. Flat Head Phillips) screws are for attaching the rack ears.

In Arena at: https://app.bom.com/items/detail-spec?item_id=1202836827&version_id=10221213778&orb_msg_single_search_p=1&redirect_seqno=7791476254

McMaster Carr: http://www.mcmaster.com/#catalog/121/3018/=zfsfk2

Stress testing/ Type of material used for the rack ears

(Note: this info is from 1200 SecureSyncs)

- Refer to Salesforce case 15341

Q What is the material of the mounting brackets?
A. Reply from Scott Homes (3 Dec 2015) 12 Ga Cold Rolled Steel (1018)

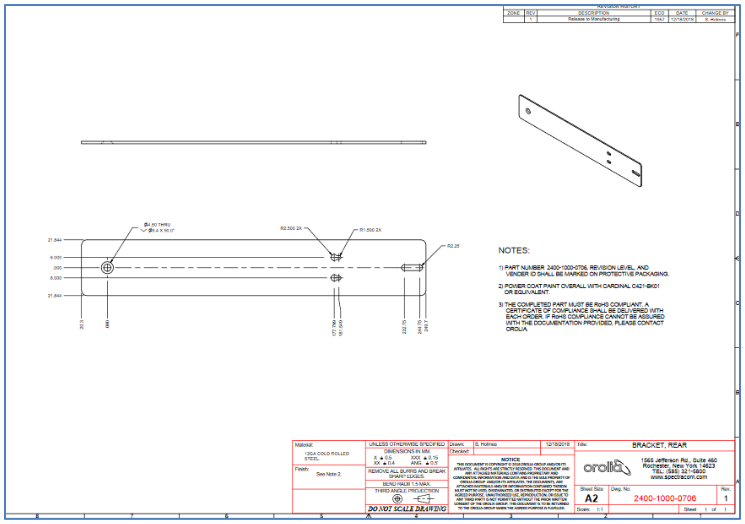
A Raytheon engineer is performing mechanical stress testing on a SecureSync and was asking about the mounting brackets. He wanted to know specifically what material these were made of.

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

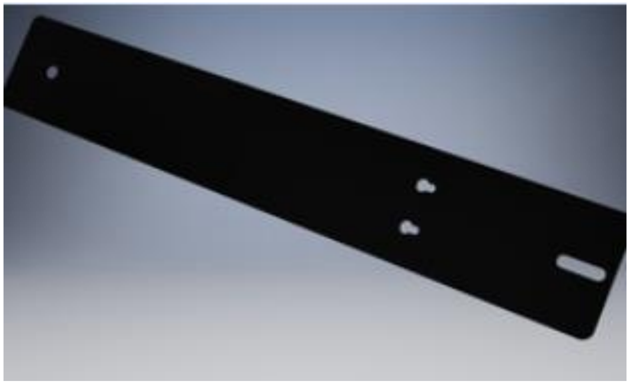
Therefore the brackets could be made from any steel the manufacturer has on hand. So to be safe I would calculate based on the weakest or most common 12Ga cold rolled steel.

Optional rear support mounting bracket ("rear bracket") for 2400 SecureSyncs

Note: this info has been updated already for 2400 SecureSyncs



21.844
8.000
.000
8.000
21.844
Ø4.50 THRU
Ø9.4 X 90.0°
R2.500 2X
R1.500 2X
R2.25
20.3
.000
177.799
181.559
232.75
244.75
249.7
NOTES:
1) PART NUMBER 2400-1000-0706, REVISION LEVEL, AND VENDER ID SHALL BE MARKED ON PROTECTIVE PACKAGING.
2) POWER COAT PAINT OVERALL WITH CARDINAL C421-BK01 OR EQUIVALENT.
3) THE COMPLETED PART MUST BE RoHS COMPLIANT. A CERTIFICATE OF COMPLIANCE SHALL BE DELIVERED WITH EACH ORDER. IF RoHS COMPLIANCE CANNOT BE ASSURED WITH THE DOCUMENTATION PROVIDED, PLEASE CONTACT OROLIA.
Material: 12GA COLD ROLLED STEEL.
Finish: See Note 2.
UNLESS OTHERWISE SPECIFIED
DIMENSIONS IN MM.
X ± 0.5 XXX ± 0.15
XX ± 0.4 ANG. ± 0.5°
REMOVE ALL BURRS AND BREAK SHARP EDGES.
BEND RADII 1.5 MAX.
THIRD ANGLE PROJECTION
DO NOT SCALE DRAWING
Drawn: S. Holmes 12/18/2018
Checked:
NOTICE
Title: BRACKET, REAR
orolia
1565 Jefferson Rd., Suite 460
Rochester, New York 14623
TEL: (585) 321-5800
www.spectracom.com
Sheet Size A2
Dwg. No. 2400-1000-0706
Rev. 1
Scale: 1:1
Sheet 1 of 1



Summary: Customers can purchase the standard rear support bracket (**2400-1000-0706**) by purchasing the "**SecureSync Anc Kit, Rugged Installation**" (**2400-0000-**) ????

Note from Dave S: "The brackets we ship provide mounting features to support brackets that can be used depending on the depth of their racks. **They will still need to source the actual rear mounts**."

More details for the info above:

- Our P/N for the bracket: 2400-1000-0706
- **Mechanical drawing above** (**2400-1000-0706**) in Arena: https://app.bom.com/items/detail-spec?item_id=1263580793&version_id=11273375818&
- This bracket is included in anc kit P/M ???
- This bracket attaches to the two vertical holes right next to the AC power connector ??? (*this note is carry-over from 1200 SecureSync)*
- The thread size for these two holes in the chassis M3 (not M3.5). ??? (*this note is carry-over from 1200 SecureSync)*

Rack-mount slides (rackmount slides) for 2400 SecureSyncs

*(**Note**: info below is carryover from the 1200 SecureSyncs)*

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

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

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

Frequently Asked Questions (FAQs)

note all info below is carryover from 1200 SecureSyncs

1) EMI/EMC STANDARD: MIL STD 461F for submarine or STANAG 4370 does it match with SecureSync unit?
We tested the SecureSync for FCC part 15 and CE. We did not test against 461F or STANAG 4370, and have not done any analysis between the standards.

2) **Gravity Center of the equipment:** The SecureSync unit will have a RB option, 4 option boards and the fan will be replaced in the rear-left side of the unit (near GPS connector): Do you think I can say that the center of gravity stay in the center of the unit with this configuration or would you have some more precise answers on this subject ?

The SecureSync center of gravity changes with the options. With the AC power supply and Rb installed but no option cards. It will be forward of center and a little to the right (facing the front panel). If it's a DC only unit, it will be approximately in the center of the unit. Each option card added will move the center of gravity more to the left. The location of the fan will not significantly change the center of gravity, regardless of options.

Important Note: If mechanical/electrical modifications are made to the SecureSync appliance (such as relocating the fan) we can't guarantee compliance to our specifications. The specifications are generated based on the factory configuration of the equipment. Any modifications to the equipment may affect the specifications we provide.

3) **Regulation of the front panel lightning**: Is there any automatic regulation (for example against temperature variations) of the lightning of the front panel?
There is no automatic regulation of the front panel.

4) Material, is it fungus resistant? : do you have some information about the paint of the equipment (for example) that can allow us to say if the unit is well protected against moistures and fungus.
I have found a standard (MIL-V-173C), may be the customer wants some approached elements…
The SecureSync is not protected against condensing moisture and fungus at all. We would need to find anti fungus coatings for the boards and mechanical parts. These parts would have to be manufactured special for this order.

5) Ingress rating: Refer to "IP rating/Ingress rating (for all products)" in the CustomerServiceAssistance document.

Any hazardous material internally? None
Do you have a material substance report? No

Fuses/Grounding / Input power (AC and DC) / Current

note info below is carryover from 1200 SecureSyncs

Power Fuses

A) DC input fuses

- Refer to “DC input power” further below

B) AC input power

- F010R-0002-000E, FUSE, 2A,SB, IEC SURGE,GLASS,250V,5X20M, Fuses for AC power entry module
- MFG P/N Littlefuse 0213002.MXP

The AC fuses (Spectracom P/N F010R-0002-000E) used in the SecureSync are from a company called Littelfuse and their P/N is 0213002.MXP. They are available through Digikey. They can refer to http://parts.digikey.com/1/parts/692754-fuse-250v-iec-slo-5x20mm-2a-0213002-mxp.html for replacements.

NATO code for the AC power fuse

Email from Sylvain (9 June 2015) I think I have found at least the little fuse NSN ref on the web site.

So it should be this one:

5920015888770 NSN CAGE 5FWY4
http://buyaircraftparts.com/manufacturers/5FWY4

Previous issues with fuses (ECN changes)

AC Fuses in SecureSync units sold before about 8/27/10:
ECN 2486 (~7/26/10) - SecureSync units were initially shipped with 4A instead of 2A fuses. This ECN changed the fuse to 2A. PSB2486 and new fuses were sent to all customers as of this time frame.

ECN 2517 (8/27/10) - SecureSync units with 208VAC input were popping the new 2A fuses. This ECN changed the two AC fuses to P/N F010R-0002-0000E. Only customers that reported the fuse blowing were sent replacements. No PSB was sent out. Units with the 2A fuse may see the fuses pop in the future because of too many power cycles. Then, supply customer with the fuses incorporated in ECN 2517.

Note: The correct fuses are small, 2 amp Slo Blow fuses. Manufacturer is “**Littlefuse**”. Their MFG P/N is **0213002.mxp**

Grounding

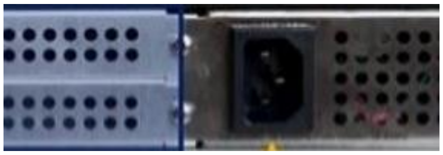
Unlike NetClocks and Model 8195 series Master Oscillators, there is no dedicated rear panel grounding lug. Earth grounding is provided through the AC power cord or the DC connector (depending on which connectors are available and used).

Input power/Power supply bays

- Refer to **online 2400 SecureSync** user guide at: https://safran-navigation-timing.com/manuals/2400/Content/NC_and_SS/2400/INSTALL/DC_pwr2
- Refer to **2400 SecureSync datasheet** (on our website): https://www.orolia.com/product/securesync-time-and-frequency-reference-system/

**Available 2400 SecureSync input power configurations

A) AC only (hard-set at time of manufacture)



B) DC only (hard-set at time of manufacture)

Two DC input power Ranges:

- **12vdc (12vdc to 17vdc, at 10A maximum)**
  - **Two**-pin connector

- **24vdc/48vdc** (21 to 60VDC at 5.5A maximum)
  - **Three**-pin connector

.

C) Single or Dual AC (via dual hotswap modules)

- **2400-HS-A1**: 100-240 VAC
  - Dual AC input alleviates the need to use an external AC to DC converter (like used with 1200 SecureSyncs) for dual AC input)

D) Single or Dual DC (via dual hotswap modules)

Two DC input power Ranges available:

- **2400-HS-D1**: **12 VDC** Hot Swap Power module. (**12vdc to 17vdc, at 10A maximum)**
- **2400-HS-D2: 24/48 VDC** Hot Swap Power module (**21vdc to 60VDC at 5.5A maximum**)

E) AC + DC (via dual hotswap modules)

Two DC input power Ranges available:

- **2400-HS-D1**: **12 VDC** Hot Swap Power module. (**12vdc to 17vdc, at 10A maximum)**
- **2400-HS-D2: 24/48 VDC** Hot Swap Power module (**21vdc to 60VDC at 5.5A maximum**)

blank cover for an unused power supply bay

- **P/N** 2400-1000-0746 (COVER,HOT SWAP,SS2400) ??? In Arena: https://app.bom.com/items/detail-whereused?item_id=1277033197&version_id=11756527778

Q. When a customer orders the 2400 hot swap chassis but only orders one power supply is there a blank cover to protect the opening for the second supply?

A. from David Dasson with Sales team (4 April 2022) YES. there is a blank cover for an unused power supply bay.

Additional details about available hotswaps- futher below

AC input power specs

- Refer to 2400 datasheet (on our website): https://www.orolia.com/document/securesync-2400-datasheet/

Per online 2400 SecureSync user guide https://safran-navigation-timing.com/manuals/2400/Content/NC_and_SS/2400/INTRO/Specs_InputPower.htm?Highlight=ac%20power%20source

AC power source: 100 to 240 V AC, 50/60 Hz, ±10 %

Opportunity that requires 88 ~ 264Vac.

- Refer to Salesforce Case 266604

Per Danny Loke "Can you confirmed the usable input AC voltage range for fixed AC 2400.
http://manuals.spectracom.com/2400/Content/NC_and_SS/2400/INTRO/Specs_MechEnv.htm
I know the specs says 100-240 VAC: up to 13120 ft (3999 m)

However, we have an opportunity for a open tender that requires 88 ~ 264Vac.
I know it is no big deal but tender's specs is tender's specs and we want to displace the incumbent Microchip S650 here.

SFDC link is here:
https://orolia.lightning.force.com/lightning/r/Opportunity/0060h00001Ef9mRAAR/view"
Reply from Ryan Johnson (15 July 2021) Hi Danny, I think the below opportunity is with you. I checked with the team and the answer is:

"AC power supply operates 88VAC to 264VAC, as does product. The safety specs require that whatever the voltage range on the label is, the product must operate to +/-10% of the labeling. 100VAC at 10% low is 90VAC, but AC power supply is rated to operate down to 88VAC." So there's no issue with these requirements.

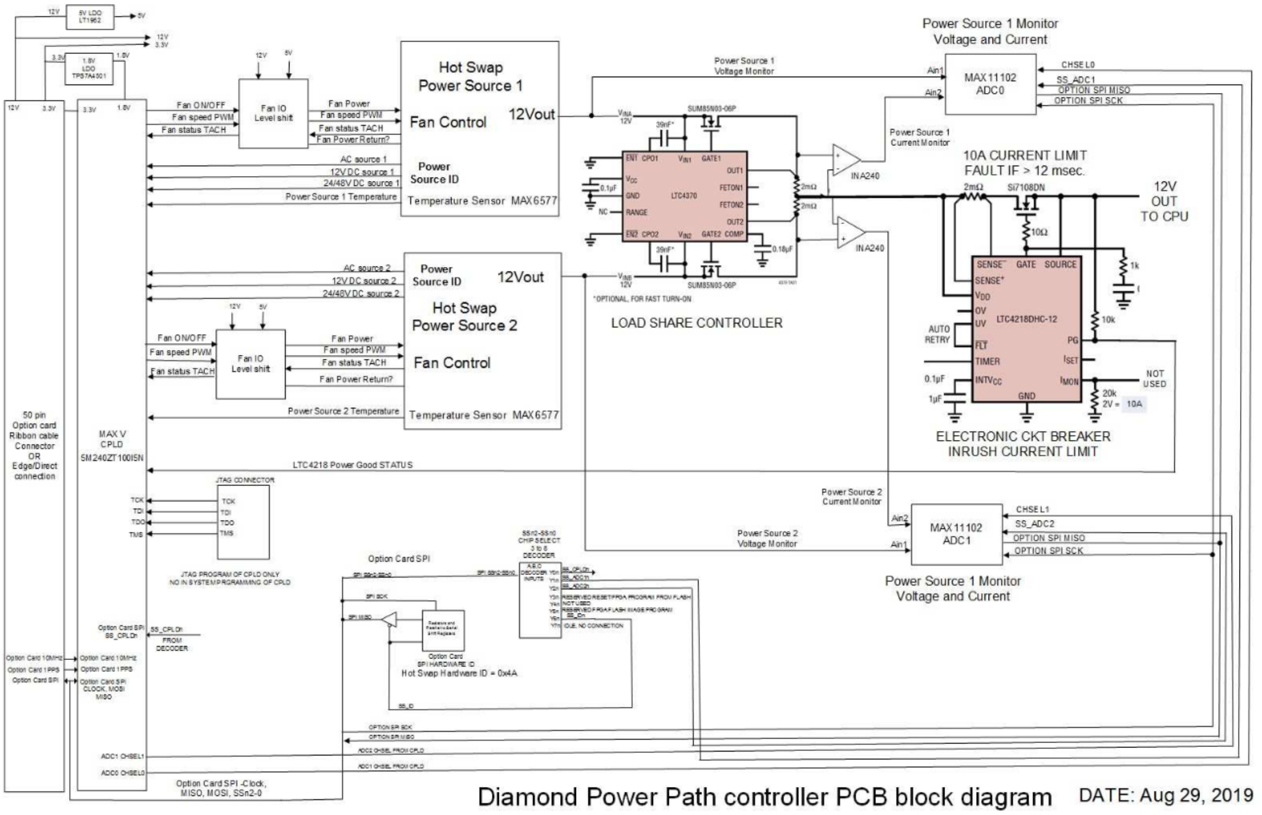
(“2400-HS-*) Hotswap Bays/Hot swap Power Supply modules (“SLEDs”)

Hot Swap Bays /electrical info on Hot Swap Bays / “Power Path Controller” in Chassis

Power path Controller board (combiner for the two hot swaps):

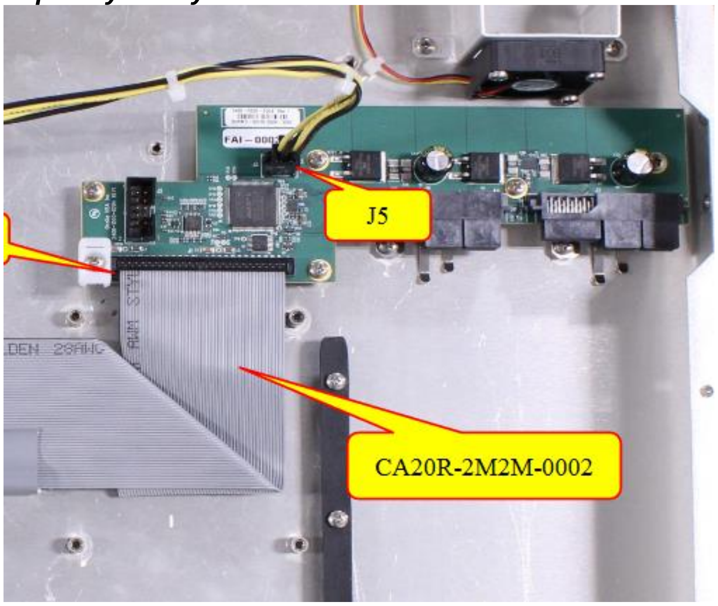
- P/N 2400-0000-F006
- PCB in arena at: https://app.bom.com/items/detail-spec?item_id=1271740949&version_id=12403961858
- Schematic (2400-1001-0204) https://files.bom.com/download/M2tCbLGDE4gSCWwtGKvOf6OhI0IyI8E3/qyvutwypinojipkldblqypemawefqwag/2400-1001-0204%20Rev%202%20DNP%202400-0000-F006.pdf

  (Block diagram excerpt below. Do not send out to anyone)

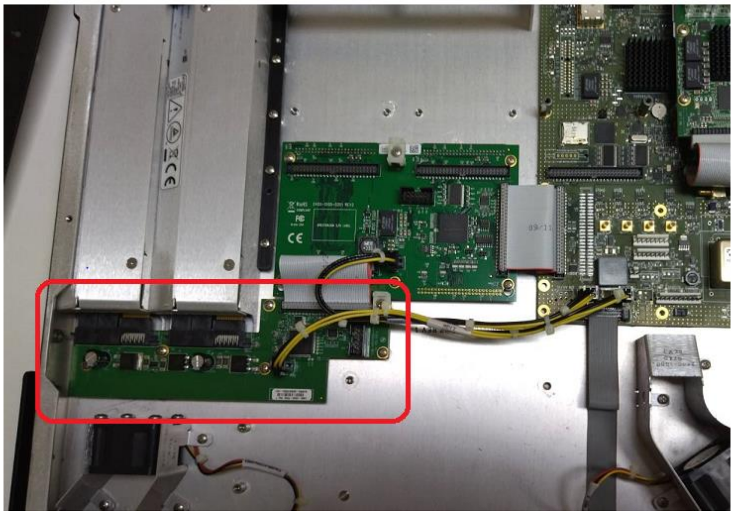


Diamond Power Path controller PCB block diagram DATE: Aug 29, 2019

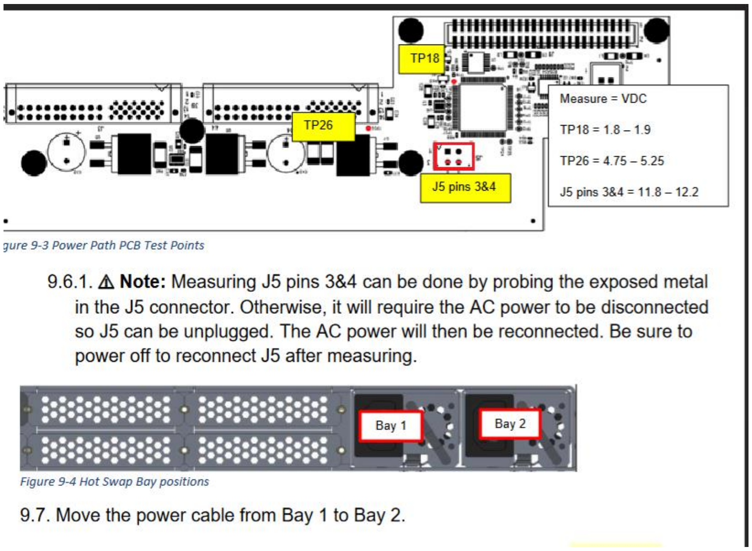
Hot swaps bays not yet installed



Two Hot swaps bays installed



DC voltage test points (from test procedure)



Measure = VDC

TP18 = 1.8 – 1.9

TP26 = 4.75 – 5.25

J5 pins 3&4 = 11.8 – 12.2

gure 9-3 Power Path PCB Test Points

9.6.1. ⚠ **Note:** Measuring J5 pins 3&4 can be done by probing the exposed metal in the J5 connector. Otherwise, it will require the AC power to be disconnected so J5 can be unplugged. The AC power will then be reconnected. Be sure to power off to reconnect J5 after measuring.

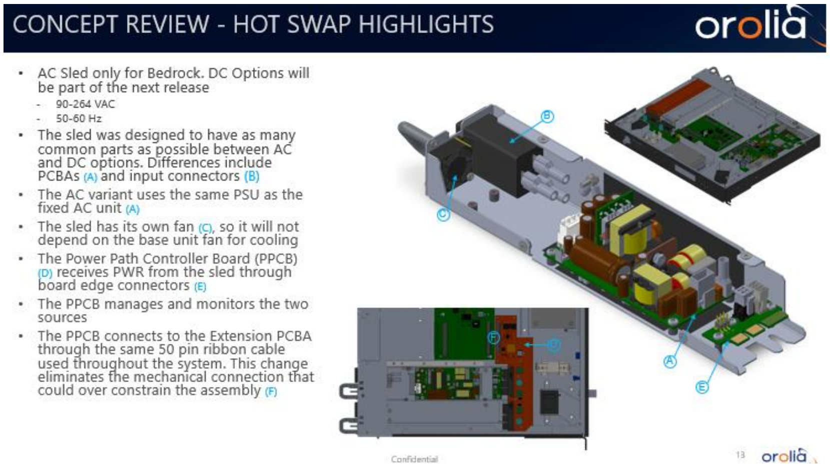
Figure 9-4 Hot Swap Bay positions

9.7. Move the power cable from Bay 1 to Bay 2.

AC and DC Hot Swap SLEDS

- Refer to Model 2400 SecureSync online user guide at: https://orolia.com/manuals/2400/Content/NC_and_SS/2400/INTRO/HotSwapPower.htm
- Manufactured by ~~Orolia~~/Safran (not just purchased/resold)
- Warranty period for Hot Swap modules: 5 years (they are individually serialized)

(**Note**: slide below is company confidential. Do not release)



CONCEPT REVIEW - HOT SWAP HIGHLIGHTS

- AC Sled only for Bedrock. DC Options will be part of the next release
  - 90-264 VAC
  - 50-60 Hz
- The sled was designed to have as many common parts as possible between AC and DC options. Differences include PCBAs (A) and input connectors (B)
- The AC variant uses the same PSU as the fixed AC unit (A)
- The sled has its own fan (C), so it will not depend on the base unit fan for cooling
- The Power Path Controller Board (PPCB) (D) receives PWR from the sled through board edge connectors (E)
- The PPCB manages and monitors the two sources
- The PPCB connects to the Extension PCBA through the same 50 pin ribbon cable used throughout the system. This change eliminates the mechanical connection that could over constrain the assembly (F)

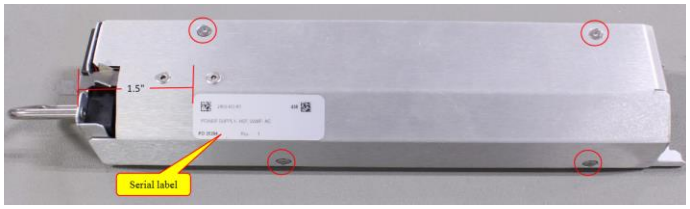
Confidential

13

EU/CE Mark Declaration of Conformity approval for hotswaps

- Refer to linked Salesforce cases **287404/ 287479**
- Refer to I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync-2400 (Diamond)\CE Declaration of Conformity and EMI-EMC

A) Model 2400-HS-A1 (AC Power Hot swap):



- **In Salesforce:** https://orolia.lightning.force.com/lightning/r/Product2/01t0h000005ouhuAAA/view

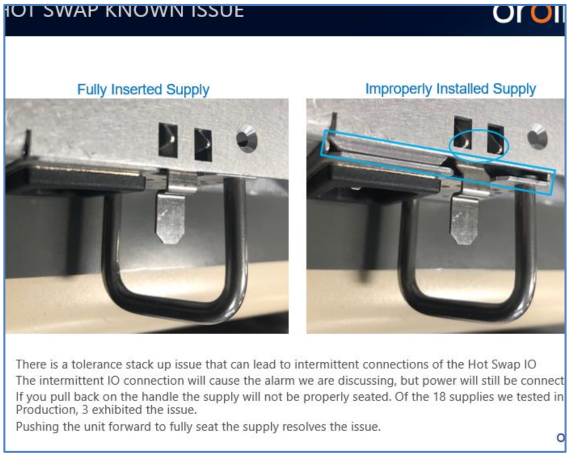
  Per Salesforce: *Hot Swappable AC Power Supply 100-240 VAC 50/60 Hz - IEC60320 connector ; Compatible only with SecureSync 2400 configuration with Hot Swap power supply support. Limit 2 per system.*

- **Our P/N:** 2400-HS-A1 (In Arena) https://app.bom.com/items/detail-spec?item_id=1283347094&version_id=11883904638

**Potential "mechanical" issue with hotswap (hot swap) SLED not being completely inserted upon receipt of device

- ➢ Refer to details ("*AC Hot swap alarm training*") in: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync-2400 (Diamond)\Alarms and logs
- ➢ In summary, tolerance issue can allow hotswap to become not fully seated during shipment, resulting in Power Supply-associated alarms ("*Timing system hardware Error*").

  Note pictures below, excerpted from documentation at link above, are for internal use. There is a dedicated document in the same folder, which is for customers.



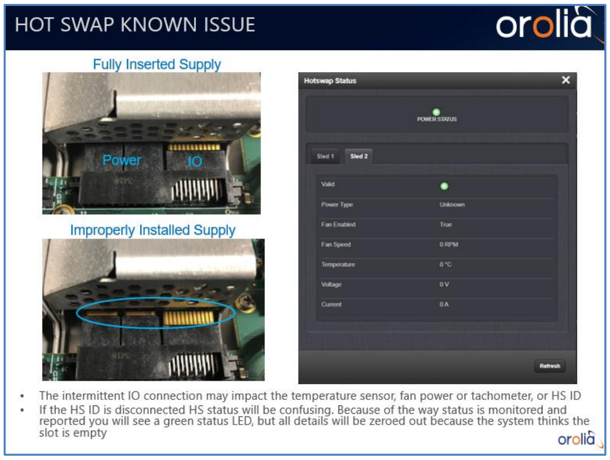
HOT SWAP KNOWN ISSUE

There is a tolerance stack up issue that can lead to intermittent connections of the Hot Swap IO

The intermittent IO connection will cause the alarm we are discussing, but power will still be connect

If you pull back on the handle the supply will not be properly seated. Of the 18 supplies we tested in Production, 3 exhibited the issue.

Pushing the unit forward to fully seat the supply resolves the issue.



HOT SWAP KNOWN ISSUE

Valid	●
Power Type	Unknown
Fan Enabled	True
Fan Speed	0 RPM
Temperature	0 °C
Voltage	0 V
Current	0 A

- The intermittent IO connection may impact the temperature sensor, fan power or tachometer, or HS ID
- If the HS ID is disconnected HS status will be confusing. Because of the way status is monitored and reported you will see a green status LED, but all details will be zeroed out because the system thinks the slot is empty

---

B) DC Power Hot swaps:

B.1 Model 2400-HS-D1 (12vdc DC Power Hot swap)

B.2 Model 2400-HS-D2 (24vdc/48vdc DC Power Hot swap)

Software support for DC hotswaps

- **DC Hotswap software support added in update version 1.4.1 (April 2022)** Per version 1.4.1 (April 2022) Release Notes **"Added software support for DC fixed and Hot Swap power supply options."**

Hot Swap Power Management (Software support) in 2400 SecureSync Web Browser

DC Hot Swap software support

Per version 1.4.1 (April 2022) Release Notes "Added software support for DC fixed and Hot Swap power supply options."

A) Via CLI interface

To read the current Alarm status (determine if each individual Alarm is active or inactive)

To read an alarm status, type: **LS_GetAlarm 0 x** (where x is one of the following values)

8 = **BAY 1 hot swap** alarm

9 = **BAY 1 hot swap** alarm

B) Via web browser interface

Management* -> *Hot Swap status page of browser (not available in 1.4.1 and below. Added in v1.6.0 update?)

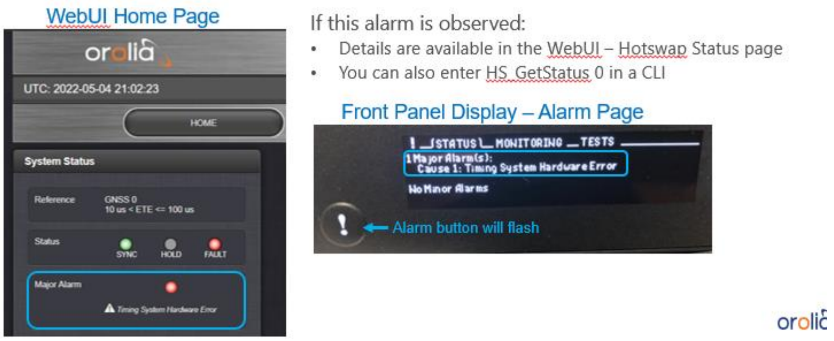
➢ Refer to online 2400 SecureSync user guide: (info hasn't been added yet, as of at least Oct 2022, for 1.4.3)

1. Update Versions 1.6.0 and above

2. Update Versions 1.4.3 and 1.4.1

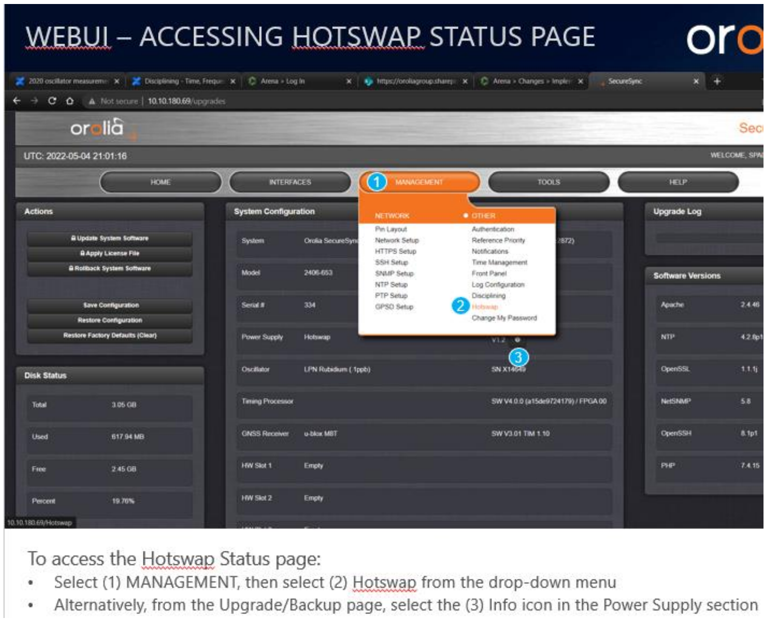
Below info from Powerpoint slides in ("AC Hot swap alarm training"): I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync-2400 (Diamond)\Alarms and logs

- A new HS Alarm was introduced with SecureSync 2400 SW v1.4.1/v1.4.1a. It is displayed in the WebUI and Front Panel OLED display as a Major Alarm with the text "Timing System Hardware Error"
- Alarm Conditions - Each Hot Swap Supply monitored individually:
  - Voltage out of range
  - Current over threshold
  - Temperature over threshold
  - Fan speed out of range or disabled
- This Alarm is the first (quick and dirty) step towards Hot Swap Monitoring, so it does not provide any useful details. Much more comprehensive and detailed monitoring will be available in upcoming releases.



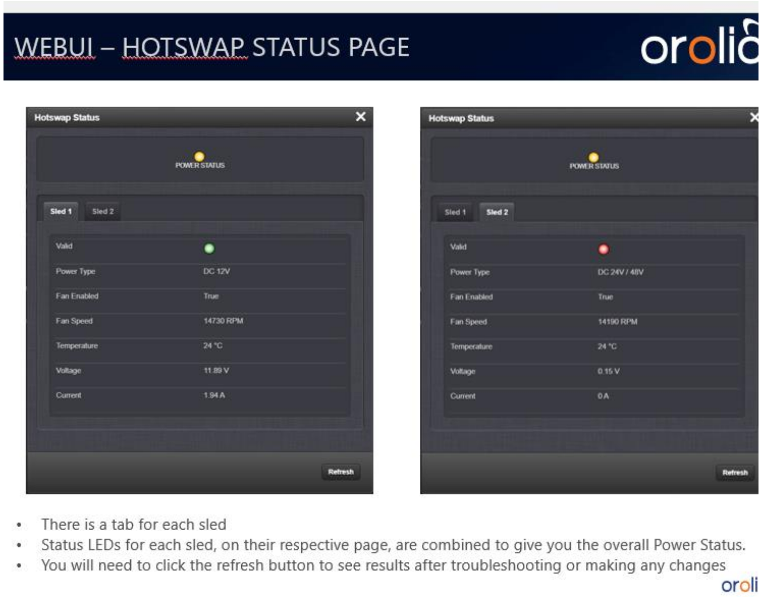
If this alarm is observed:

- Details are available in the WebUI – Hotswap Status page
- You can also enter HS GetStatus 0 in a CLI



To access the Hotswap Status page:

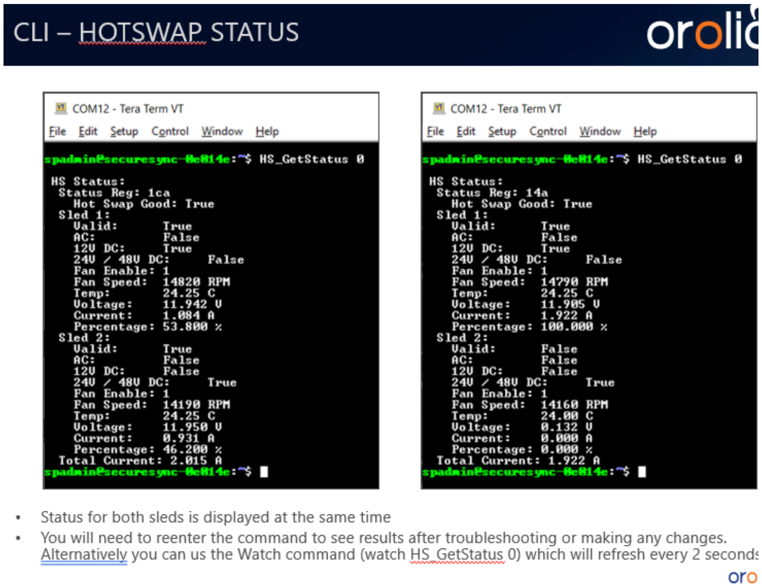
- Select (1) MANAGEMENT, then select (2) Hotswap from the drop-down menu
- Alternatively, from the Upgrade/Backup page, select the (3) Info icon in the Power Supply section



WEBUI – HOTSWAP STATUS PAGE

	Sled 1	Sled 2
Valid	🟢	🔴
Power Type	DC 12V	DC 24V / 48V
Fan Enabled	True	True
Fan Speed	14730 RPM	14190 RPM
Temperature	24 °C	24 °C
Voltage	11.89 V	0.15 V
Current	1.94 A	0 A

- There is a tab for each sled
- Status LEDs for each sled, on their respective page, are combined to give you the overall Power Status.
- You will need to click the refresh button to see results after troubleshooting or making any changes


orolia
COM12 - Tera Term VT
File Edit Setup Control Window Help
COM12 - Tera Term VT
File Edit Setup Control Window Help
oro

CLI – HOTSWAP STATUS

```
spadmin@securesync-0e014e:~$ HS_GetStatus 0

 HS Status:
  Status Reg: 1ca
    Hot Swap Good: True
  Sled 1:
    Valid:      True
    AC:         False
    12V DC:     True
    24V / 48V DC:     False
    Fan Enable: 1
    Fan Speed:  14820 RPM
    Temp:       24.25 C
    Voltage:    11.942 V
    Current:    1.084 A
    Percentage: 53.800 %
  Sled 2:
    Valid:      True
    AC:         False
    12V DC:     False
    24V / 48V DC:     True
    Fan Enable: 1
    Fan Speed:  14190 RPM
    Temp:       24.25 C
    Voltage:    11.950 V
    Current:    0.931 A
    Percentage: 46.200 %
  Total Current: 2.015 A
spadmin@securesync-0e014e:~$
```

```
spadmin@securesync-0e014e:~$ HS_GetStatus 0

 HS Status:
  Status Reg: 14a
    Hot Swap Good: True
  Sled 1:
    Valid:      True
    AC:         False
    12V DC:     True
    24V / 48V DC:     False
    Fan Enable: 1
    Fan Speed:  14790 RPM
    Temp:       24.25 C
    Voltage:    11.905 V
    Current:    1.922 A
    Percentage: 100.000 %
  Sled 2:
    Valid:      False
    AC:         False
    12V DC:     False
    24V / 48V DC:     True
    Fan Enable: 1
    Fan Speed:  14160 RPM
    Temp:       24.00 C
    Voltage:    0.132 V
    Current:    0.000 A
    Percentage: 0.000 %
  Total Current: 1.922 A
spadmin@securesync-0e014e:~$
```

- Status for both sleds is displayed at the same time
- You will need to reenter the command to see results after troubleshooting or making any changes. Alternatively you can us the Watch command (watch HS_GetStatus 0) which will refresh every 2 seconds

Software versions prior to v.1.4.1
Q Missing **Power Supply status display** on home page. Below are pictures from old units (power status display on home page): and also was displayed in Dual power AC-DC model:

A (per Dave Sohn May 2021) This display is missing on new unit's home page. However, we have power supply status available in new screen (Management-> Hot Swap) on GUI that shows power supply status for both PS, but it is better to also show the status on Home page.

This is good feedback and will likely be incorporated. Likely just the high level power status will be presented with further details on the hot-swap status page.

"Load Module": (Which power supply or which hot swap SLED is currently powering the unit, power supply selections)

Inquiry Keith sent to Engineering, while 1,6.0 is in development (6 Oct 2022) along the same topic of 2400 hot swaps: I don't see it yet in beta, but think it would be nice to see this available eventually. Have you considered reporting in the browser (Home page for instance) which power source is actively selected/powering the unit? Whether its Sled 1 or Sled 2, or AC vs DC, etc? Just a thought...

Reply from William Comly (6 Oct 2022)

As for what power supply is powering the unit: the answer is both. The unit has a load module that makes it so that the power supplies usually share the responsibility for providing power, no one module is providing all the power at once.

Fixed AC power connector: Unit has C14 inlet connector

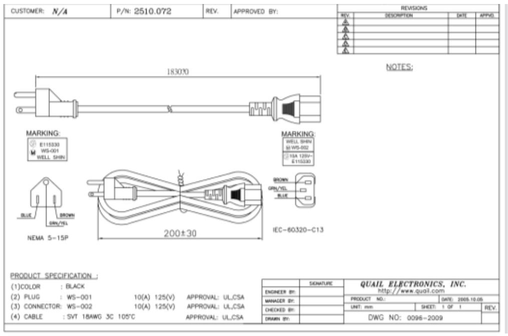
AC line cords for 240VAC input to the C14 connector on back of the 1200 SecureSyncs

- Refer to Salesforce Case 285021 (for 1200 SecureSyncs)
- As of at least May 2022, I don't believe we offer any 240VAC input line cords.
- Customers need to 'locally obtain' a 240VAC to C13 line cord. Some suggested Sources/Part Numbers below:
  - Mouser Electronics (https://www.mouser.com/c/?q=AC%20line%20cords)
  - Quail Electronics, inc (https://www.quail.com/typesearch.htm?type=plugreceptaclematrix&gclid=CjwKCAjwp7eUBhBeEiwAZbHwkW56yg9zYZdkifvJC0cKGKX4KqLd33egbQr6lDeiTphmWwPIYLrXwBoC4z8QAvD_BwE)
  - Walmart (confirm with Eng) : https://www.walmart.ca/en/ip/Tripp-Lite-P032-007-7-Feet-AC-Power-Cord-10A-100-240V-12Awg-C13-C20/PRD6SHG20D8DNUP

AC power cable included in ancillary kit (either US or Euro) ?

A) US version (120VAC)

- Our P/N: CA06R-1513-0001
- Refer to: (Arena) https://app.bom.com/items/detail-spec?item_id=1202841923&version_id=10257870238



Approved Vendors/Vendor P/Ns

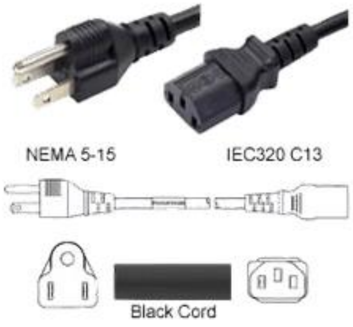
A) King Cord P/N: K01031BF201NB (https://www.mymectronic.com/part-search/all/K01031BF201BR/0/0)

1) Volex P/N: 17758 10 B1

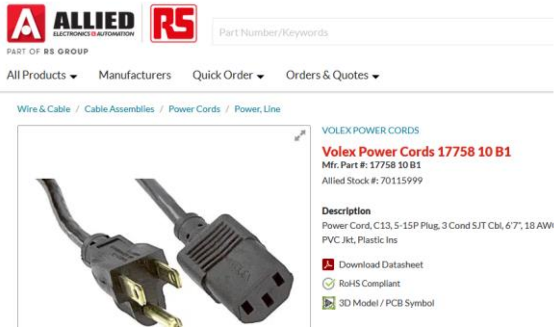
link to Allied Electronics datasheet (https://www.alliedelec.com/product/volex-power-cords/17758-10-b1/70115999/?gclid=CjwKCAjwp7eUBhBeEiwAZbHwkSk4xcGkzvKE9iGF0di3XZ4lFT86C6ZX9LTtC2P6zY6U-QPCis1NfBoCOTkQAvD_BwE&gclsrc=aw.ds)

- **Cable length**: 6 ft 7 inches (2032 millimeters)

Standard (supplied) "detached" power cable is C13 to NEMA 5-15P (this cable is not attached to the back of the unit- it's detachable from the power connector).



- ➢ RoHS compliancy of the AC line cord
  - ○ Refer to Salesforce Case 285022 (for 1200 SecureSyncs)
  - ○ Volex P/N: 17758 10 B1 link to Allied Electronics datasheet (https://www.alliedelec.com/product/volex-power-cords/17758-10-b1/70115999/?gclid=CjwKCAjwp7eUBhBeEiwAZbHwkSk4xcGkzvKE9iGF0di3XZ4lFT86C6ZX9LTtC2P6zY6U-QPCis1NfBoCOTkQAvD_BwE&gclsrc=aw.ds)



Wire & Cable / Cable Assemblies / Power Cords / Power, Line

VOLEX POWER CORDS

Volex Power Cords 17758 10 B1

Mfr. Part #: 17758 10 B1

Allied Stock #: 70115999

Description

Power Cord, C13, 5-15P Plug, 3 Cond SJT Cbl, 6'7", 18 AW

PVC Jkt, Plastic Ins

Download Datasheet

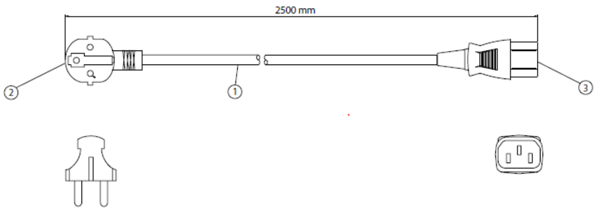
RoHS Compliant

3D Model / PCB Symbol

  - ○ Refer to "*RoHS compliancy statement for SecureSyncs*" in this same document

B) Euro version

- ➢ Our P/N: CA06R-EU13-0001 (in Arena) https://app.bom.com/items/detail-spec?item_id=1203165790&version_id=10257870248
- ➢ **Description:** AC CORD,EU to C13,18AWG,10A,250V, 70C
- ➢ **Cable length**: 8.2 feet (2500 millimeters)



PLUG: CONTINENTAL EUROPEAN CEE 7 RIGHT ANGLED
Connector: IEC 60320 C13 (to SecureSync)

Note: As of at least March 2015, we don't offer any alternate AC power cables (such as a C13 to C14 cable for example) and Dave Sohn doesn't want to get into supporting various other power cables. The C13 to xxx cables should be readily available locally.

Power cords for Les Ulis that will work with SecureSync if one is not specified and shipped with the order Per Tom Richardson - cord for STA or CNT-90 would work.

Input power signal characteristics/requirements (Sinusoidal power/ square wave power)

- Refer to: Power interruption tolerance: UPS backup to AC input for SecureSyncs/9400s

Input AC current (amps) (Note: this info is from 1200 SecureSyncs)

Email from Mark McGregor

The amps drawn depends on the input voltage, that is why power draw is specified.

The amps drawn will be roughly the power drawn divided by the AC line voltage (P=VI, I=P/V). For example, we specify 40W normal for an OCXO. If the AC power is 115VAC, the current draw is 40W/115VAC~=0.35Amp. This would only be when the customer had all six option cards installed; it should typically be less than that.

The AC input is rated for 1A maximum, but that is at low AC voltage of 90VAC, and the 1A has at least 20% margin over what the box actually draws, to ensure the maximum is never exceeded, as it is a safety parameter.

Another Email from Mark McGregor (17 Jan 2013)

Note: Mark also included MFG data sheets for the TDK-Lambda and TDK Lamba LS100 evaluation test dat **Refer to:** I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Input power

It is really just taken from the specification of the AC to DC power supply, as a maximum. It also depends on the AC line voltage and the AC fuses and the chassis wiring. The AC to DC power supply specifies it as 60A maximum with 277VAC input voltage. SecureSync uses an LS100-12 power supply. See attached data sheet and evaluation test data.

I think that the actual value would be lower due to the SecureSync chassis wiring and the slow blow AC fuses that are IEC surge rated.

We also do not have equipment to measure it. We would have to rent equipment, or send a unit somewhere, or take it somewhere that does have that equipment to know what the actual number is.

Q "I'm looking for some technical data on the SecureSync GPS (P/N 1200-003). Can you provide me with the following information:

- Maximum Current draw for 115VDC and 220VDC voltage sources.
  2) Maximum Power Consumption for 220VDC voltage sources.
  3) Heat Dissipation for 115VDC and 220VDC voltage sources.

A Reply from Tom R (15 sept 17)

Hi Data Sheet Page 3
TCXO: 40W normal (50W startup)

1) Maximum Current draw for 115VDC and 220VDC voltage sources.
2) Maximum Power Consumption for 220VDC voltage sources. 50 Watts
3) Heat Dissipation for 115VDC and 220VDC voltage sources. 50 Watts

Watt = 1VRMS * 1A therefore Amp = Watt/VRMS
50 Watts/115VRMS = 0.43 A
50W/220V = 0.23 A

AC Power Factor/ Power draw

(Note: this info is from 1200 SecureSyncs)

AC Power Factor

- Refer to case 24906
- measured Power Factor of an AC unit in the lab was + 0.83 (valid range for power factory is from -1 to +1).

from https://en.wikipedia.org/wiki/Power_factor
In electrical engineering, the **power factor** of an AC electrical power system is defined as the ratio of the real power flowing to the load to the apparent power in the circuit, and is a dimensionless number in the closed interval of −1 to 1. A power factor of less than one means that the voltage and current waveforms are not in phase, reducing the instantaneous product of the two waveforms (V × I).

Q Email Keith sent to Tom Richardson: In reference to our Salesforce case 24906 (submitted by Jim Rayhill with Harris), he is asking for the "Power Factor" for SecureSync's AC input…
I looked in my notes and the SecureSync online manual, but wasn't surprised it's not mentioned in either place (believe this is the first time I've heard it asked for this product)
A (response from Tom Richardson, 31 Mar 17) I measured Power Factor of an AC unit in the lab and got 0.83.

Volt-amps (VA)

Q Could you please give us the requirement of following specification?
Unit: 1200-033
Spec: Apparent electric power (VA)

According to the datasheet, the SecureSync(033) need 80W at bootup, and 50W at actual use.
The customer wants to know also VA values to calculate load of their power supply.

A Reply from Josh (based on info he received from Jean-Arnold) 16 Jan 18: The Apparent electric power for the SecureSync is as follow :
55.5VA at actual use
88.9VA at boot up.

Power draw (excerpt below from 2400 SecureSync online manual at http://manuals.spectracom.com/2400/Content/NC_and_SS/2400/INTRO/Specs_InputPower.htm

Maximum power draw:

- TCXO/OCXO oscillator installed: 40 W normal (50 W start-up)
- Rubidium (Rb) oscillator installed: 50 W normal (80 W start-up)
- Low-Phase Noise (LPN) Rubidium oscillator installed: 52 W normal (85 W start-up)

Attached you should find a copy of the SecureSync data sheet. Page 3 (second to last page) contains the "Power Draw" specs for SecureSync. The power draw that will exist with SecureSync is primarily based on which type of oscillator is installed in the appliance (the TCXO, OCXO or Rubidium oscillator).

The oscillators inherently draw more current when they are cold, so the start-up wattage is higher than is during normal operation (as shown in the above specs). Once the oscillators have become internally warm again, the power draw by the oscillator is able to drop.

Not only will the type of oscillator affect the power draw, the specific configuration of the installed Option Cards will also affect the amount of power draw, as well. These specs in the datasheet are the maximum power expected in any configuration of the option cards. I spoke to one of our engineers that performed the measurements for these specs and he said the power draw difference between the AC input and DC input is negligible (as your customer is asking about).

The engineer also mentioned that when powering SecureSync with both AC and DC input power (for automatic failover upon loss of AC power to DC power), even though the DC power is not being used when AC power is present, there is still a few watts drawn on the DC power as its used by the DC to DC converter.

Two Emails from Mark McGregor:
We do not/did not measure the current draw for each option card configuration. It will be less than the data sheet maximum of 1A. I came up with the data sheet value using 20W of option card power draw with power resistors to simulate the option cards, and I am sure it is less than that.
I measured about 0.7A for the Rubidium (033) at start-up with 20W simulated option card load, and added some margin to get 1A.
I can't say how much less, as I don't know what a 1204-05 option card draws, as that is a SAASM option card we are not allowed to have. I do not know how much power a 1204-06 Ethernet card draws.

I found the data I took. It was on 11/23/2009. I used a low AC line voltage of 95V (draws more current than 115V) in a model 033 Rubidium with AC power SecureSync, with 20W of extra load to simulate option cards
At start up, the current draw was 0.75A at 95VAC.
After 3 minutes the current dropped to 0.5A at 95VAC
After 20 minutes, the current was 0.47A at 95 VAC.
With AC line at 115V, current drop rflowers@murphymedical.org ed to 0.40A.
The unit shipped to the customer will be somewhat less than this.

208 VAC input with both being hot with respect to ground

Email from Mark McGregor (5/23/11)
The SecureSync will run OK from 208VAC, two phases of the three phase power, but they must still supply an earth ground on the third pin of the AC power connection for the SecureSync to remain safe per UL60950-1 and CE EN60950-1 safety standards. The SecureSync is rated for 100-240VAC up to 2000 meters of altitude. As long as Tony's customer is not going to operate the product above 2000m, then 208VAC is OK when an earthed ground is supplied on the third pin of the SecureSync AC power inlet.

FYI - The 208V is derived from using two lines of the 120V three phase power. Each phase voltage is 120VAC, but when two of them are used together, due to them being 1/3 of a cycle (120 degrees) out of phase with each other, the result is 208VAC. This is what the IT data centers are doing that were blowing the AC fuse that did not have a high enough surge rating.

In order to comply with UL and CE safety both AC lines must be treated as being potentially hot. Neither AC line can go directly to earth ground.

The reason for the double pole/neutral line fusing, is that if one of the incoming AC lines can't be reliably identified as an earthed neutral, then both sides of the AC line must be fused, if fusing is used for overcurrent protection. In the US consumer 120V outlets, the one AC slot being wider than the other identifies the earthed neutral, so only one fuse is required in the known "hot" line. In Europe, they don't have this kind of outlet, so you can't guarantees that one of the two lines is an earthed neutral, so both must be fused.

Power interruption tolerance: UPS backup to AC input for SecureSyncs/9400s

(Note: this info below is from 1200 SecureSyncs)

- Current draw of the oscillator should be considered when selecting a UPS to use with SecureSync
- Refer to the following about email below: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\UPS for SecureSync

- The SecureSync can operate for up to 20 msec. after AC input power is lost with no negative effects.

Q They are planning to prepare some measures for instantaneous interruption of their power supply.Could you please tell us how much variation can the power unit of the time server allow?
They want to confirm following specifications of the time server:
- Allowable voltage drop threshold [V]

- Allowable instantaneous interruption period [sec]

A Email from Dave L (14 Feb 18) Per the user manual, the SecureSync can operate for up to 20 msec. after AC input power is lost with no negative effects

Questions from SF case 126365

1. We are trying to support a SecureSync unit on a UPS. One UPS we have in mind would have a brief power interruption when switching from primary power to battery power, rated to be between 4 and 8 milliseconds. Question is this: What are the capabilities of the SecureSync unit to ride through such a power interruption? What power interruption can it ride through without losing time (under the assumption that GPS is not available, and the unit is running on an internal Rb standard)?

1a. Does the unit require sinusoidal power? Or is it OK with square wave power some UPS's output?

A Reply from Mark McGregor (7 Feb 18) The AC power supply internal to SecureSync is a TDK-Lambda LS100. It has a hold up time specification, which is how long it can operate after loss of AC power. LS100 hold up time is 25 msec typical with 115 VAC input, and 150 msec. typical for 230VAC input. That being the case I would tell the customer that SecureSync can operate for 20 msec. after AC input power is lost since the TDK spec is “typical”, not minimum. If power is restored less than 20 msec after it is lost, the SecureSync should not experience a power cycle, restart.

As far as the AC input waveform, it is not specified for the TDK-Lambda LS-100. The AC input is specified as 88VAC to 264VAC RMS at 47-63 Hz frequency. It can operate with DC input from 125V to 373V DC. I think that a square wave would work if its AC RMS voltage is within 88 to 264 VAC, at 47 to 63 Hz frequency. An inquiry could be made to TDK-Lambda local sales rep to try to get an answer from TDK-Lambda.

Q from Mike Messina to Tom Richardson referring to FAA: Any idea of what they can use as a UPS now with SecureSync?

A Reply from Tom R (30 May 17) A 12 to 36 VDC backup supply should work. Try this.
http://www.technologydynamicsinc.com/dc-ups/tdrsp-1urk-bbu12-50.php

Q Site where Time Server is located has regular testing where they fail over from one power source to another. Since the Time Server only has one power supply, this will take the Time Server down regularly. Do you have an option for a secondary power supply that can be plugged into a separate PDU? or do you supply/recommend a small UPS for short power outages?

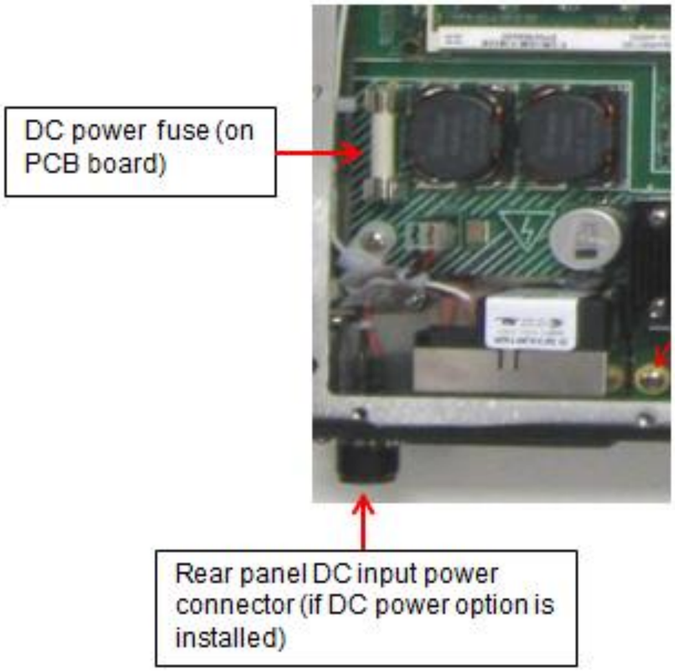
A (reply from DL 16 Feb 18) Answer:
The Securesync does have a dual power option but this must be ordered at the time of purchase. It is not installable afterwards.
The best method of protection from power outages for this Securesync is to use a UPS system.

The size of the UPS depends on what the oscillator option is on your Securesync

- **TCXO**: 40W normal (40W start-up)
- **OCXO**: 40W normal (50W start-up)
- **Rb**: 50W normal (80W start-up)

C) DC input power

(Note: this info is from 1200 SecureSyncs)


DC power fuse (on PCB board)
Rear panel DC input power connector (if DC power option is installed)

1. 24/48vdc input power

- Spectracom Fuse P/N F030R-0005-010E, FUSE, 5A, FB, CERAMIC CART,250V,3AB, 24/48VDC power fuse
- MFG P/N Littlefuse 0314005.HXP or 0314005.MXP
- DC power jack (included in “DC” and “AC/DC” anc kits: our P/N P240r-0032-002f (in Arena) at :https://app.bom.com/items/detail-spec?item_id=1202844982&version_id=10221223528
- DC ripple:

2. 12vdc input power

- Spectracom Fuse P/N F030R-0010-000E, FUSE, 10A, FB, CERAMIC CART,250V,3AB, 12VDC power fuse
- MFG P/N Littlefuse 0314010.HXP or 0314010.MXP
- DC power jack (included in “DC” and “AC/DC” anc kits: our P/N P240R-0032-002f (in Arena) at :https://app.bom.com/items/detail-spec?item_id=1202844982&version_id=10221223528
- DC ripple:

Secure locking DC input connector (attaches to DC input jack on rear panel)

- (included in “DC” and “AC/DC” anc kits: our P/N P240R-0032-002F (in Arena) at: https://app.bom.com/items/detail-spec?item_id=1202844982&version_id=10221223528
- Refer to “Secure locking device” further below for additional info on this connector

Desire to convert a DC only unit to AC input power

(Note: this info is from 1200 SecureSyncs)

Highly recommend considering to purchase and use the Spectracom Model PS06R-2Z1M-DT01 (Available AC to 24VDC converter for redundant AC input) instead of retrofitting the time server. This external AC to DC converter will alleviate the need for the equipment to be returned to us for hardware modifications.

Q. **(from Scott Holmes to Mark McGregor**) There is a 10A fuse located on the SecureSync main board near the DC supply area. Do we consider that a "field replaceable" part?
A. Reply from Mark McGregor (10/24/12) The 10A fuse is only used for the 12V DC option. There is a 5A fuse that goes in the same spot for the 24/48V DC option. That fuse is not populated if no DC input option is present.

I am fairly sure that none of the parts inside the box are considered to be field replaceable for UL safety. (Keith's edit- Refer to the SecureSync manual for more info).

D) AC and DC Input power

Altitude limitations for the internal power supply (AC and DC)

- Refer to the SecureSync data sheet
- SecureSync Data Sheet lists both 100-240 VAC to 6,560 feet and 100-120 VAC to 13,123 feet
- Per Dave Sohn- Max altitude for DC power is same as 100-120 VAC… 13,123 feet.

E) DC input power

- Note: AC input, if supplied, is selected over DC input (AC input is primary. DC input is backup).

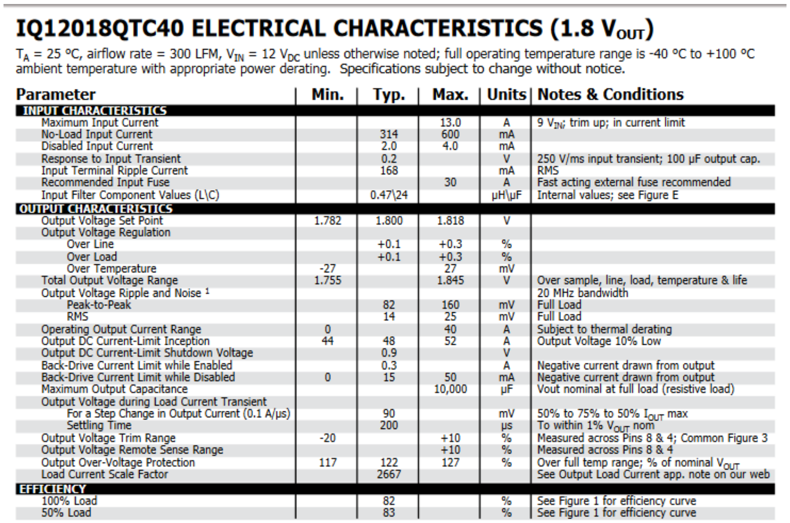
DC to DC converter installed

(Note: this info is from 1200 SecureSyncs)

1. **12Vdc Option range: 10- 17vdc (Uses DC to DC converter P/N PS03R-0J0J-PC00) (8 Amps)**
   - Note: This DC to DC converter can actually handle 10 to 22vdc input, but we specify 10 to 17vdc with a tolerance for UL requirements

Our P/N: PS03R-0J0J-PC00 (in Arena at https://app.bom.com/items/detail-spec?item_id=1202845980&version_id=10221213338&orb_msg_single_search_p=1)

MFG and P/N: SYNQOR IQ12120QTC10NRS-G



IQ12018QTC40 ELECTRICAL CHARACTERISTICS (1.8 V_{OUT})

T_A = 25 °C, airflow rate = 300 LFM, V_{IN} = 12 V_{DC} unless otherwise noted; full operating temperature range is -40 °C to +100 °C ambient temperature with appropriate power derating. Specifications subject to change without notice.

Parameter	Min.	Typ.	Max.	Units	Notes & Conditions
INPUT CHARACTERISTICS					
Maximum Input Current			13.0	A	9 V_{IN}; trim up; in current limit
No-Load Input Current		314	600	mA	
Disabled Input Current		2.0	4.0	mA	
Response to Input Transient		0.2		V	250 V/ms input transient; 100 µF output cap.
Input Terminal Ripple Current		168		mA	RMS
Recommended Input Fuse			30	A	Fast acting external fuse recommended
Input Filter Component Values (L\C)		0.47\24		µH\µF	Internal values; see Figure E
OUTPUT CHARACTERISTICS					
Output Voltage Set Point	1.782	1.800	1.818	V	
Output Voltage Regulation					
Over Line		+0.1	+0.3	%	
Over Load		+0.1	+0.3	%	
Over Temperature	-27		27	mV	
Total Output Voltage Range	1.755		1.845	V	Over sample, line, load, temperature & life
Output Voltage Ripple and Noise [1]					20 MHz bandwidth
Peak-to-Peak		82	160	mV	Full Load
RMS		14	25	mV	Full Load
Operating Output Current Range	0		40	A	Subject to thermal derating
Output DC Current-Limit Inception	44	48	52	A	Output Voltage 10% Low
Output DC Current-Limit Shutdown Voltage		0.9		V	
Back-Drive Current Limit while Enabled		0.3		A	Negative current drawn from output
Back-Drive Current Limit while Disabled	0	15	50	mA	Negative current drawn from output
Maximum Output Capacitance			10,000	µF	Vout nominal at full load (resistive load)
Output Voltage during Load Current Transient					
For a Step Change in Output Current (0.1 A/µs)		90		mV	50% to 75% to 50% I_{OUT} max
Settling Time		200		µs	To within 1% V_{OUT} nom
Output Voltage Trim Range	-20		+10	%	Measured across Pins 8 & 4; Common Figure 3
Output Voltage Remote Sense Range			+10	%	Measured across Pins 8 & 4
Output Over-Voltage Protection	117	122	127	%	Over full temp range; % of nominal V_{OUT}
Load Current Scale Factor		2667			See Output Load Current app. note on our web
EFFICIENCY					
100% Load		82		%	See Figure 1 for efficiency curve
50% Load		83		%	See Figure 1 for efficiency curve

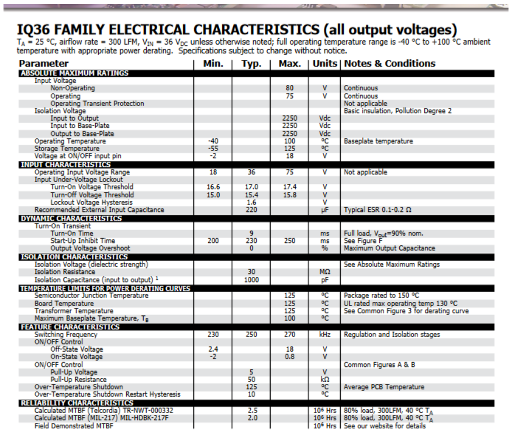
24/48Vdc Option range: 21-60vdc (Uses DC to DC converter P/N PS03R-1U0J-PC00) (10 Amps)

(Note: this info is from 1200 SecureSyncs)

- Note: This DC to DC converter can actually handle 18 to 75 vdc input, but we specify 21 to 60vdc with a tolerance for UL requirements

Our P/N: PS03R-1U0J-PC00 (in Arena at: https://app.bom.com/items/detail-spec?item_id=1202845981&version_id=10228388768&orb_msg_single_search_p=1

MFG and P/N: SYNQOR IQ36120QTC10NRS-G



IQ36 FAMILY ELECTRICAL CHARACTERISTICS (all output voltages)

T_A = 25 °C, airflow rate = 300 LFM, V_{IN} = 36 V_{DC} unless otherwise noted; full operating temperature range is -40 °C to +100 °C ambient temperature with appropriate power derating. Specifications subject to change without notice.

Parameter	Min.	Typ.	Max.	Units	Notes & Conditions
ABSOLUTE MAXIMUM RATINGS					
Input Voltage					
Non-Operating			80	V	Continuous
Operating			75	V	Continuous
Operating Transient Protection					Not applicable
Isolation Voltage					Basic insulation, Pollution Degree 2
Input to Output			2250	Vdc	
Input to Base-Plate			2250	Vdc	
Output to Base-Plate			2250	Vdc	
Operating Temperature	-40		100	°C	Baseplate temperature
Storage Temperature	-55		125	°C	
Voltage at ON/OFF input pin	-2		18	V	
INPUT CHARACTERISTICS					
Operating Input Voltage Range	18	36	75	V	Not applicable
Input Under-Voltage Lockout					
Turn-On Voltage Threshold	16.6	17.0	17.4	V	
Turn-Off Voltage Threshold	15.0	15.4	15.8	V	
Lockout Voltage Hysteresis		1.6		V	
Recommended External Input Capacitance		220		µF	Typical ESR 0.1-0.2 Ω
DYNAMIC CHARACTERISTICS					
Turn-On Transient					
Turn-On Time		9		ms	Full load, V_{out}=90% nom.
Start-Up Inhibit Time	200	230	250	ms	See Figure F
Output Voltage Overshoot		0		%	Maximum Output Capacitance
ISOLATION CHARACTERISTICS					
Isolation Voltage (dielectric strength)					See Absolute Maximum Ratings
Isolation Resistance		30		MΩ	
Isolation Capacitance (input to output) [1]		1000		pF	
TEMPERATURE LIMITS FOR POWER DERATING CURVES					
Semiconductor Junction Temperature			125	°C	Package rated to 150 °C
Board Temperature			125	°C	UL rated max operating temp 130 °C
Transformer Temperature			125	°C	See Common Figure 3 for derating curve
Maximum Baseplate Temperature, T_B			100	°C	
FEATURE CHARACTERISTICS					
Switching Frequency	230	250	270	kHz	Regulation and Isolation stages
ON/OFF Control					
Off-State Voltage	2.4		18	V	
On-State Voltage	-2		0.8	V	
ON/OFF Control					Common Figures A & B
Pull-Up Voltage		5		V	
Pull-Up Resistance		50		kΩ	
Over-Temperature Shutdown		125		°C	Average PCB Temperature
Over-Temperature Shutdown Restart Hysteresis		10		°C	
RELIABILITY CHARACTERISTICS					
Calculated MTBF (Telcordia) TR-NWT-000332		2.5		10^6 Hrs	80% load, 300LFM, 40 °C T_A
Calculated MTBF (MIL-217) MIL-HDBK-217F		2.0		10^6 Hrs	80% load, 300LFM, 40 °C T_A
Field Demonstrated MTBF				10^6 Hrs	See our website for details

DC Ripple spec (for 21- 60vdc input): 260 mA RMS

Amps/Watts for 48vdc

Q ….We are working on putting together some information in a bid that requires details surround the Securesync 48V electrical specs. Your website provides details on the AC, 120V side.

Could you provide me the following specs for the 48V DC operations:

-DC Amps
-DC Power
-Recommended DC breaker size (if you have one)
-Thermal contribution (in BTU)

Email from Tom Richardson (25 Sept 17) The information you have is correct as far as I know.
DC amps would be calculated as the Watts divided by the Voltage.
We have no recommended DC breaker size.
We have not measured or calculated the Thermal contribution in BTU.

A Reply from Jodi to Customer

Here are the answers, below, to your questions about the SecureSync.
DC input (option):

- 12-17 V_{DC} -15%, +20%, or
- 21-60 V_{DC} -15%, +20%, secure locking device

Maximum power draw:

- TCXO/OCXO oscillator installed: 40 W normal (50 W start-up)
- Rubidium (Rb) oscillator installed: 50 W normal (80 W start-up)
- Low-Phase Noise (LPN) Rubidium oscillator installed: 52 W normal (85 W start-up)

We have no recommended DC breaker size and we have not measured or calculated the Thermal contribution in BTU. I do have some information on the cooling fan and thermal dissipation that may help, however:

- Rb oscillator: 50W normal (80W start-up) 170.60708165 BTU/hr normal, (272.97133064 BTU/hr startup) Startup time is 30 minutes.

The cooling fan: **Air flow:** 1.30 CFM

SecureSync Chassis Cooling: The cooling fan, while running (it is temperature controlled), pulls ambient air in through the right side of the front panel. The chassis was intentionally designed to have holes only on the back of the left side of the chassis, so air is essentially "ducted" to and across the back end of the chassis for cooling (drawing heat away from the components located towards the front of the chassis).

Second reply from Jodi (25 Sept 17)
I also have this information. Let me know if it's what you're looking for.

For a TCXO oscillator: 40W normal (50W startup)

1) Maximum Current draw for 115VDC and 220VDC voltage sources.
2) **Maximum Power Consumption for 220VDC voltage source**= 50 Watts
3) **Heat Dissipation for 115VDC and 220VDC voltage sources**= 50 Watts

Watt = 1VRMS * 1A therefore Amp = Watt/VRMS
50 Watts/115VRMS = 0.43 A
50W/220V = 0.23 A

"Secure locking device" (as stated in the manual)

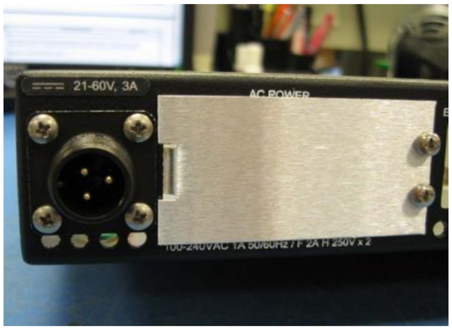
(Note: this info is from 1200 SecureSyncs)

- The mating connector is included with the unit.
- Included in the "DC" and "AC/DC" Anc kits:
- Our P/N for the mating connector is P240R-0032-002F (in Arena) at :https://app.bom.com/items/detail-spec?item_id=1202844982&version_id=10221223528
- Amphenol P/N: DL3106A10SL-3S

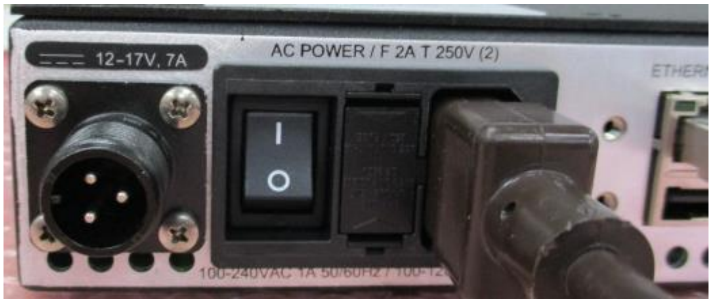
This comment is referring to the available DC input power connector for the SecureSync. The AC input is a standard IEC line cord. The DC connector is threaded so that the mating connector can be physically and positively attached with a metal threaded nut. Though not necessarily recommended, the SecureSync could theoretically be picked up by its mating DC power connector without the plug falling off the back of the SecureSync and thereby causing the unit to lose input DC power.
Below are two pictures of the DC connector. It's a little difficult to see from this picture, but the outer circle of the

connector is threaded:

DC power only

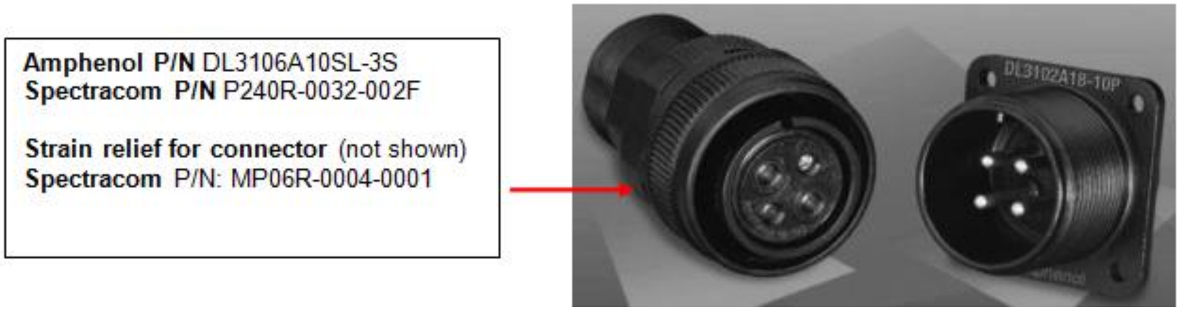


DC and AC power



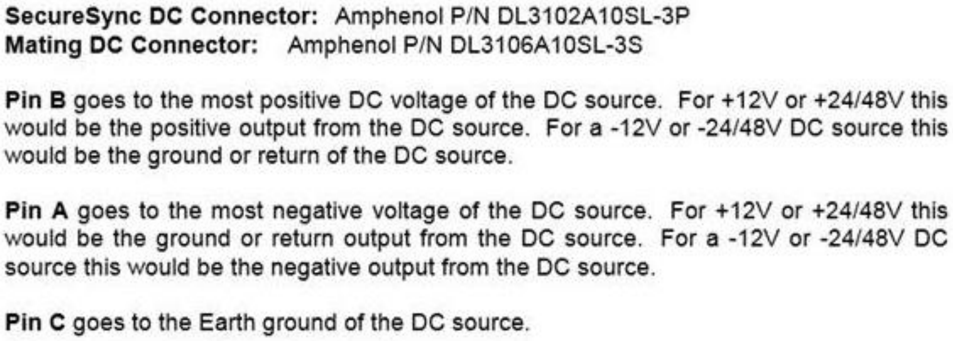
The DC mating connector is an “**Amphenol**” connector. Their Part Number is “**DL3106A10SL-3S**”. The Spectracom P/N is P240-0032-002F. The connector has solder cups for soldering wires to the connector pins.

Below is a better picture of both connectors together (the one on the back of the SecureSync is on the right and the mating connector is on the left). This picture shows the threads better than the above picture.



Amphenol P/N DL3106A10SL-3S
Spectracom P/N P240R-0032-002F

Strain relief for connector (not shown)
Spectracom P/N: MP06R-0004-0001

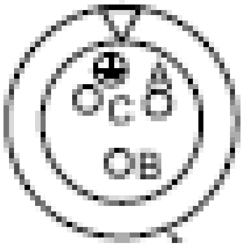


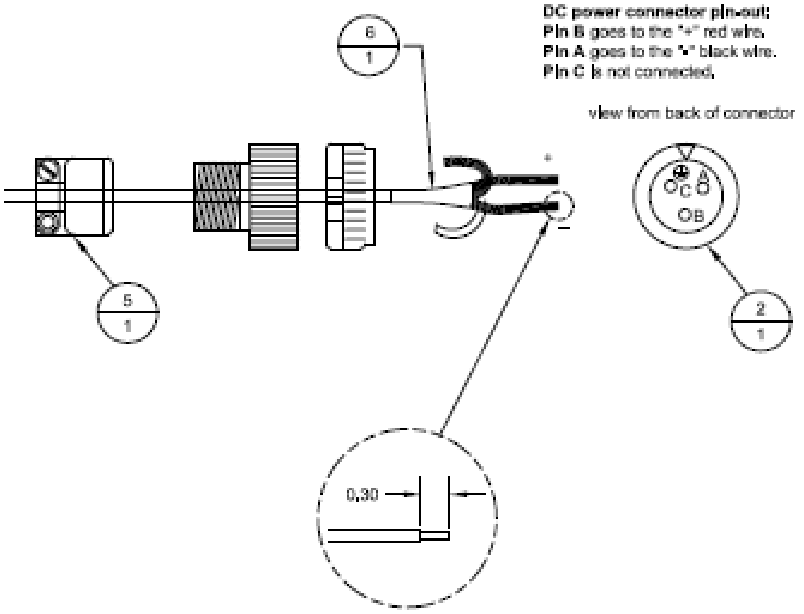
SecureSync DC Connector: Amphenol P/N DL3102A10SL-3P
Mating DC Connector: Amphenol P/N DL3106A10SL-3S

Pin B goes to the most positive DC voltage of the DC source. For +12V or +24/48V this would be the positive output from the DC source. For a -12V or -24/48V DC source this would be the ground or return of the DC source.

Pin A goes to the most negative voltage of the DC source. For +12V or +24/48V this would be the ground or return output from the DC source. For a -12V or -24/48V DC source this would be the negative output from the DC source.

Pin C goes to the Earth ground of the DC source.




DC power connector pin-out:
Pin B goes to the "+" red wire.
Pin A goes to the "-" black wire.
Pin C is not connected.

DC power wiring

- A cable of 6 feet or less, using 16AWG wire, with adequate insulation for the DC voltage source should be used with this connector.
- The 6 feet or less cable is due to inrush current causing voltage drop. Refer to email below.

Specific to 24/48vdc input

Email from Sam Otto: I checked with design engineer (Mark McGregor) who recommends a **24**VDC, **6.25** Amp, **150** watt power supply using **16** gauge wire less than 1 meter from out unit. The reason for this is the inrush current causes the voltage to drop which results in an under voltage lockout preventing your SecureSync from powering on.

Pin B goes to the most positive DC voltage of the DC source. For +12V or +24/48V this would be the positive output from the DC source. For a -12V or -24/48V DC source this would be the ground or return of the DC source.

Pin A goes to the most negative voltage of the DC source. For +12V or +24/48V this would be the ground or return output from the DC source. For a -12V or -24/48V DC source this would be the negative output from the DC source.

Pin C goes to the Earth ground of the DC source.

Important! SecureSync is earth grounded through the DC power connector. Ensure that the SecureSync is connected to a DC power source that is connected to earth ground via the grounding pin C of the SecureSync DC power plug supplied in the ancillary kit.

Leakage current (current leakage)

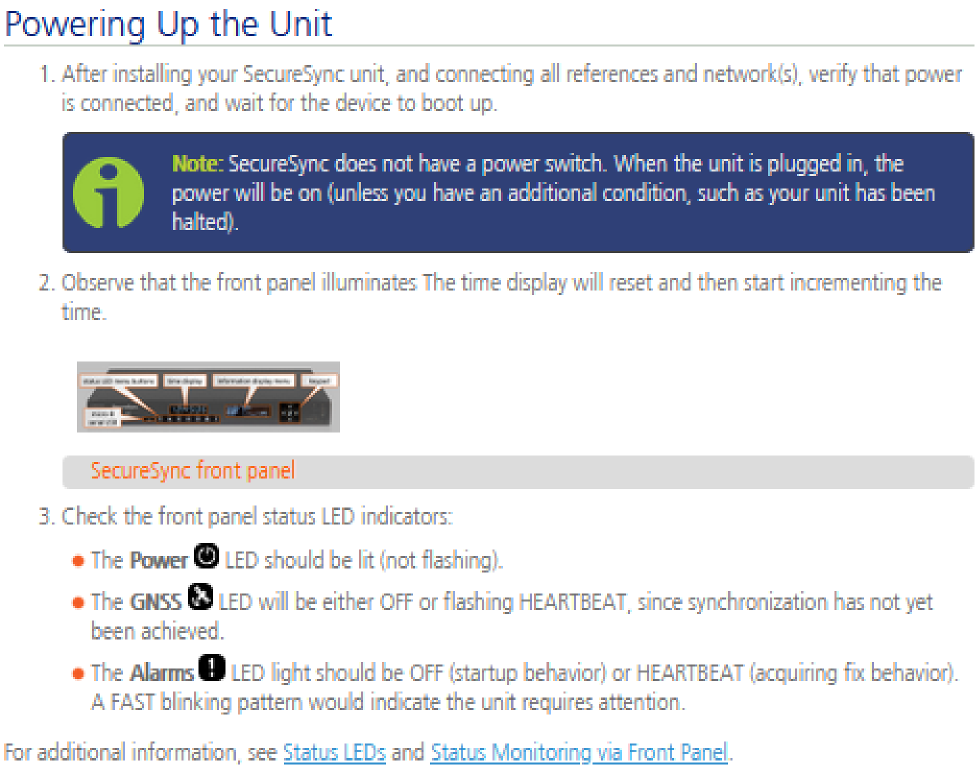
- Refer to Salesforce case 163902

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

External Power OFF/ON (Powering-up/power-down)

2400 SecureSyncs have no power switch

- Refer to online 2400 user guide (excerpt below at: http://manuals.spectracom.com/2400/Content/NC_and_SS/2400/INSTALL/Power_Up.htm



Powering Up the Unit

1. After installing your SecureSync unit, and connecting all references and network(s), verify that power is connected, and wait for the device to boot up.

> **Note:** SecureSync does not have a power switch. When the unit is plugged in, the power will be on (unless you have an additional condition, such as your unit has been halted).

2. Observe that the front panel illuminates The time display will reset and then start incrementing the time.

SecureSync front panel

3. Check the front panel status LED indicators:
   - The **Power** ⏻ LED should be lit (not flashing).
   - The **GNSS** 🛰 LED will be either OFF or flashing HEARTBEAT, since synchronization has not yet been achieved.
   - The **Alarms** ! LED light should be OFF (startup behavior) or HEARTBEAT (acquiring fix behavior). A FAST blinking pattern would indicate the unit requires attention.

For additional information, see Status LEDs and Status Monitoring via Front Panel.

Q (per Hughes eval demo) Unit does not have Power ON/OFF switch/button, older units have the button. Is there somewhere one could fit if “we must”?

A (per Dave Sohn) Due to space restrictions, especially on our hot-swap variants the physical on/off switch was removed from the 2400. Full shut down of the system is achieved through removal of the power cords.

There are many pieces of equipment within infrastructure that do not have power switches themselves. Most routers and switches that they utilize within their systems probably don’t have independent power switches.

This is different than the 1200 but is it acceptable to Hughes?

**Power monitor / alarms / traps

- An alarm is asserted when both AC and DC input connectors are present, but one of the two inputs is not present.
- For more info, refer to: **Front panel status LEDs/ (AC and DC power monitoring) in this document.

Alert notification (such as SNMP traps) for loss of redundant power

- As of at least update versions 1.2.1 and below, no alerts available

Q (May 2021, from Hughes while demoing the 2400s) It remained powered ON when one power supply is down, but does not send alarm/trap when one power supply is down.

A (per Dave Sohn) Notifications including alarming are on our roadmap for future releases. likely slated for Q3 (2021) release.

"Timing System Hardware Error" alarms versus "Hot Swap Major"/ "Hot Swap Minor" alarms

- Starting in update 1.6.0 (~Dec 2022) all Hot Swap/power associated alerts no longer assert "**Timing System Hardware Erro**r"
  - Note that if a Hot Swap is installed, but no power is applied to that Hot Swap, the "Timing System Hardware Error alarm is asserted. To clear this particular condition, either supply power to the Hot Swap, or simply remove the Hot Swap.

- Update 1.6.0 changes power issues to either **Hot Swap Major**" and/or "**Hot Swap Minor**" alarms

---

**Humidity/Power/BTU specs (Heat dissipation) ????

(Note: this info is from 1200 SecureSyncs)

Humidity: 10% - 95% relative humidity, non-condensing @ 40 C

Power Draw / Heat dissipation (BTU/hr)

- • TCXO: 40W normal (40W start-up) 136.48566532 BTU/hr
- • OCXO: 40W normal (50W start-up) 136.48566532 BTU/hr normal (170.60708165 BTU/hr startup)
- • Rb: 50W normal (80W start-up) 170.60708165 BTU/hr normal (272.97133064 BTU/hr startup)

BTU disbursement rating/ Heat dissipation

Email from Tom Richardson

A BTU (British Thermal Unit) is the amount of heat necessary to raise one pound of water by 1 degree Fahrenheit (F).
1 Watt is the power from a current of 1 Ampere flowing through 1 Volt.
1 kWh = 3413 BTU
Using how many Watts the unit takes to warm up and neglecting the hours part, 50 Watthours = 171 BTU, 80 Watthours = 273 BTU
This is sort of like apples and applesauce because BTUs are usually used in cooling and Watts are energy. Customer probably really wants to know how many BTUs it takes to cool a unit.

Email from Scott Holmes

Tom's explanation is a good one.
Just a few definitions that might help.
Power is the rate energy is consumed and can be expressed in watts, kilowatts, etc.

Energy is the amount of power consumed, expressed in watt-hours, kilowatt-hours, BTU, etc.

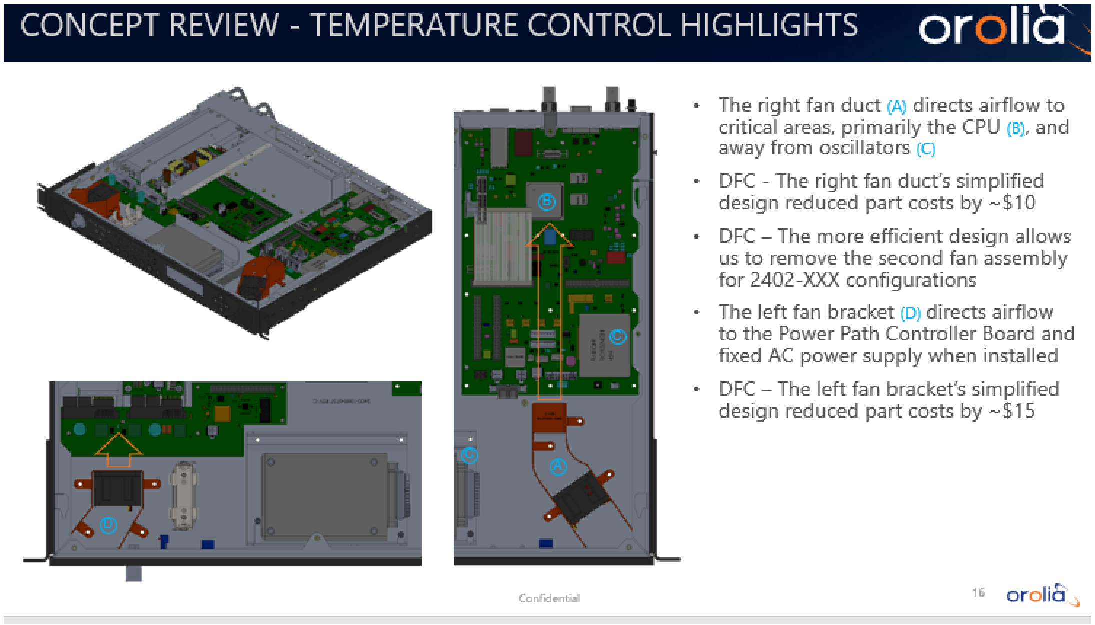
So, as Tom says it's apples to applesauce. The watt is an SI unit of power and the BTU an Imperial unit of energy.

Just to add to Tom's 1kWh = 3413 BTU, you can also say 1W = 3.41 Btu/hr, if this makes it a bit clearer.

Email from Mark McGregor:

There should be two BTU ratings. The ones Tom gave (above) are for while the OCXO and Rb units are warming up. If you have the unit running for more than 30 minutes, the rating will drop a bit to the 40W max for OCXO and 50W max for Rb. If they are using it for cooling fan rating, I would just give them the warm up power numbers, as it will have them choose a larger fan.

**Cooling fan/Temperatures



CONCEPT REVIEW - TEMPERATURE CONTROL HIGHLIGHTS

- The right fan duct (A) directs airflow to critical areas, primarily the CPU (B), and away from oscillators (C)
- DFC - The right fan duct's simplified design reduced part costs by ~$10
- DFC – The more efficient design allows us to remove the second fan assembly for 2402-XXX configurations
- The left fan bracket (D) directs airflow to the Power Path Controller Board and fixed AC power supply when installed
- DFC – The left fan bracket's simplified design reduced part costs by ~$15

Confidential

16

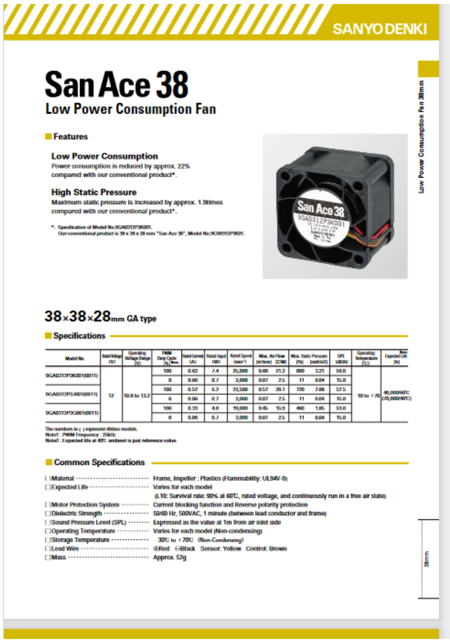
Fan control

Q (From Hughes eval demo) Fan Configuration/Settings (System Status) screen missing, we have seen this option on some of the older units (manufactured after January 2016)
A (Per Dave Sohn ~May 2021) The cooling infrastructure of the 1200 and 2400 are different. The 1200 included more basic control functions with single speed fans, which were improved after a HW change around 2016 to allow more user control of the on/off state. The 2400 includes variable speed fans, so are controlled completely by the system without user configuration.

We are doing the temperature maintenance in the new systems differently and the variable control removes the need for more strict control that we give directly to the customer. Temperature is monitored in various locations internal to the system to drive the fans. This is different than the 1200 but is it acceptable to Hughes?

Cooling fan for 2400 SecureSync

➢ **Our P/N for the 2400 cooling fan**: **B338R-0016-000J** (in Arena) https://app.bom.com/items/detail-spec?item_id=1233304132&version_id=10746383248



SANYO DENKI

San Ace 38

Low Power Consumption Fan

Low Power Consumption Fan 38mm

■ Features

Low Power Consumption
Power consumption is reduced by approx. 22% compared with our conventional product*.

High Static Pressure
Maximum static pressure is increased by approx. 1.9times compared with our conventional product*.

*: Specification of Model No.9GA0312P3K001.
Our conventional product is 38 x 38 x 28 mm "San Ace 38", Model No.9GV0312P3K01.

38×38×28mm GA type

■ Specifications

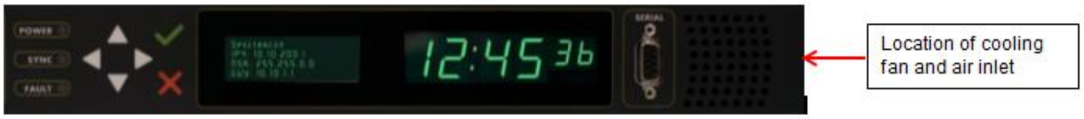
Model No.	Rated Voltage [V]	Operating Voltage Range [V]	PWM Duty Cycle [%] Note1	Rated Current [A]	Rated Input [W]	Rated Speed [min⁻¹]	Max. Air Flow [m³/min]	Max. Air Flow [CFM]	Max. Static Pressure [Pa]	Max. Static Pressure [inchH2O]	SPL [dB(A)]	Operating Temperature [°C]	Expected Life Note2 [h]
9GA0312P3K001(0011)	12	10.8 to 13.2	100	0.62	7.4	25,000	0.60	21.2	800	3.21	59.0	−10 to +70	40,000/60°C (70,000/40°C)
			0	0.06	0.7	3,000	0.07	2.5	11	0.04	15.0		
9GA0312P3J001(0011)			100	0.52	6.2	23,500	0.57	20.1	720	2.89	57.5		
			0	0.06	0.7	3,000	0.07	2.5	11	0.04	15.0		
9GA0312P3G001(0011)			100	0.33	4.0	19,000	0.45	15.9	460	1.85	53.0		
			0	0.06	0.7	3,000	0.07	2.5	11	0.04	15.0		

The numbers in ( ) represent ribless models.
Note1 : PWM Frequency : 25kHz
Note2 : Expected life at 40°C ambient is just reference value.

■ Common Specifications

□Material	Frame, Impeller : Plastics (Flammability: UL94V-0)
□Expected Life	Varies for each model (L10: Survival rate: 90% at 60°C, rated voltage, and continuously run in a free air state)
□Motor Protection System	Current blocking function and Reverse polarity protection
□Dielectric Strength	50/60 Hz, 500VAC, 1 minute (between lead conductor and frame)
□Sound Pressure Level (SPL)	Expressed as the value at 1m from air inlet side
□Operating Temperature	Varies for each model (Non-condensing)
□Storage Temperature	−30°C to +70°C (Non-Condensing)
□Lead Wire	⊕Red ⊖Black Sensor: Yellow Control: Brown
□Mass	Approx. 52g

- **Mfg**: SANYO DENKI AMERICA, INC.
- **MFG P/N:** 9GA0312P3G001
- Link to Digikey info: **1688-1533-ND** (https://www.digikey.com/en/products/detail/sanyo-denki-america-inc/9GA0312P3G001/6192249?utm_adgroup=Fans%20%26%20Thermal%20Management&utm_source=google&utm_medium=cpc&utm_campaign=Dynamic%20Search_EN_RLSA&utm_term=&utm_content=Fans%20%26%20Thermal%20Management&gclid=Cj0KCQjws-OEBhCkARIsAPhOkIZ1cnushROzbq4HZDQfSgoNU5S49SPd-jrj93_s3wMAt39XTHOc8PsaAvHHEALw_wcB)



Life expectancy of the fan, from Mfg. Data sheet): 40000 Hrs @ 60°C

(about 7 years of continuously on) ???

Air flow: 15.9 CFM (0.445m^3/min)

Power: 4 W

~~**SecureSync Chassis Cooling:** The cooling fan, while running (it is temperature controlled), pulls ambient air in through the right side of the front panel. The chassis was intentionally designed to have holes only on the back of the left-side of the chassis, so air is essentially "ducted" to and across the back end of the chassis for cooling (drawing heat away from the components located towards the front of the chassis).~~

~~**Per Dave Sohn (7 Nov 2018)** SecureSync has a single fan on the front of the unit (right side as you look at it). Airflow is designed from front to rear. There is venting in the rear, side rear, and top rear. The side and top vent holes are not required to be clear for correct temperature control.~~

Storage Temperature: -40° to 85°C storage range

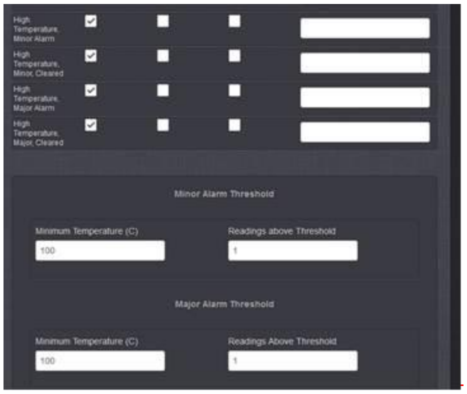
Indications of the fan operation/fan has failed

~~Q. If the fan is left in the 'always on' function what is the expected time before it may stop working and will the SecureSync indicate a failure of the fan in anything other than the logs?~~

~~**A Keith's response (10 Feb 16):** the life expectancy for the fan when always running is 60000 hrs @ 40°C (about 7 years). As there is no feedback from the fan indicating whether or not it's actually spinning, there isn't a direct indication of the fan's operation (log entries, alarms or alerts) available for the SecureSync.~~

~~However, software version 5.3.1 also added SNMP traps and gets and Minor/Major alarms associated with the internal temperature. If the cooling fan was to fail and this resulted in the internal temperature exceeding a user-specified threshold, a Minor and/or Major alarm can be optionally asserted and an optional SNMP trap can be sent to an SNMP Manager.~~

~~Alarms and SNMP Trap alerts for high/low temperatures are configured in the Management -> Notifications page of the browser (with version 5.3.1 or above installed), System tab (as shown below)~~



High Temperature, Minor Alarm	☑	□	□	
High Temperature, Minor, Cleared	☑	□	□	
High Temperature, Major Alarm	☑	□	□	
High Temperature, Major, Cleared	☑	□	□	

Minor Alarm Threshold

Minimum Temperature (C): 100

Readings above Threshold: 1

Major Alarm Threshold

Minimum Temperature (C): 100

Readings Above Threshold: 1

~~checkboxes in this tab allow the associated temperature traps to be enabled to be sent, and the user-configurable temperature thresholds are configured in the fields towards the bottom of this tab. "Readings above threshold" allows a delay (in seconds) between each insertion of this alarm (for instance, set it to "5" for a 5 second delay between each insertion of the condition, if the temperature remains above the specified value for a length of time. this prevents it from being continuously inserted as the temp remains above the threshold).~~

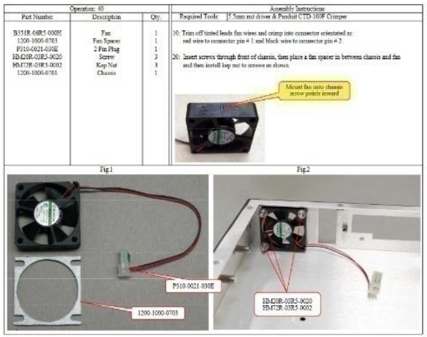
Replacing fan in the field

- Refer to Salesforce case 159470

Email from Dave L (18 Apr 18) It is not impossible to replace the fan, just not really easy. You would need to disassemble the front panel a bit to prevent the fan screws from turning if they will not loosen or tighten. If they are manageable you would not need to remove the front panel.

Here are a few photos of the product. Please have a look and see if this is something you would want to tackle or if you would like to RMA the Securesync. I can send you a fan with the connector already installed.

Here is a view of the inside showing the screw locations, this should help.



Operation: 40

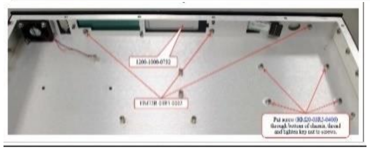
Part Number	Description	Qty.
B351R-06R5-000H	Fan	1
1200-1000-0703	Fan Spacer	1
P310-0021-030E	2 Pin Plug	1
HM20R-03R5-0020	Screw	3
HM72R-03R5-0002	Kep Nut	3
1200-1000-0701	Chassis	1

Assembly Instructions

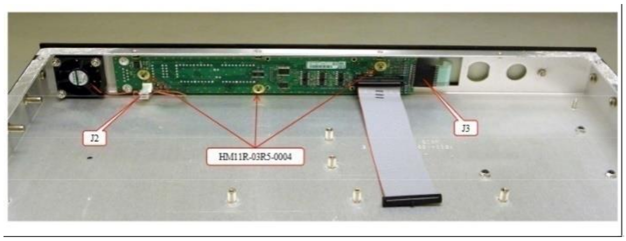
Required Tools: 5.5mm nut driver & Panduit CTD-100F Crimper

10: Trim off tinted leads fan wires and crimp into connector orientated as: red wire to connector pin # 1 and black wire to connector pin # 2.

20: Insert screws through front of chassis, then place a fan spacer in between chassis and fan and then install kep nut to screws as shown.



Put screw (HM20-03R5-0400) through bottom of chassis, thread and tighten kep nut to screws.

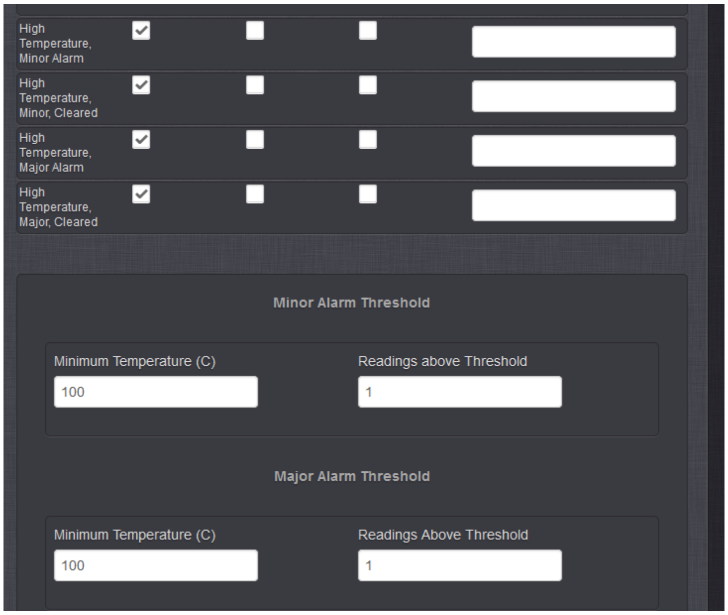


Operating (internal) Temperature:

- -20°C to 65°C operating range with the two OCXOs (Standard and high performance)
- -20°C to 55°C operating range with the Rubidium oscillator (KW Note: as of 11/11/11, this upper-end spec changed some time ago. It used to be only +50°C, instead. ~~We're not sure exactly when this spec change occurred~~) Per the note below, it appears this change occurred in Aug, 2010.

Alarms/SNMP traps/email alerts for high temperatures

- Version 5.3.1 also added SNMP alerts for high temperatures (Management -> Notifications page, System tab)



High Temperature, Minor Alarm	☑	□	□	
High Temperature, Minor, Cleared	☑	□	□	
High Temperature, Major Alarm	☑	□	□	
High Temperature, Major, Cleared	☑	□	□	

Minor Alarm Threshold

Minimum Temperature (C): 100
Readings above Threshold: 1

Major Alarm Threshold

Minimum Temperature (C): 100
Readings Above Threshold: 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.~~

Recommended temperature settings

~~Q ...in Securesync there are three temperature value which are CPU, board and oscillator. I would like to know what is the threshold or max operational temp level. For the temp alarm monitoring the default value is 100°C and it is referring to what. CPU, board or oscillator ? What is the recommended value for temp. setting?~~

~~**A . Reply from Jodi (30 Mar 17**) Please see the below excerpt from the SecureSync online user manual:~~

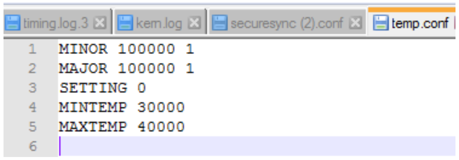
~~*The default temperature threshold value for both Minor, and Major Alarms is 100°C. With simultaneous alarm triggerings, the Major Alarm will override the Minor Alarm, i.e. you will be notified only about the Major Alarm. If you want to be notified early about a rise*~~

~~*in temperature, a recommended setting for the Minor Alarm temperature would be 90°C. Please note that it is not advisable to set the Major Alarm temperature to a value higher than 100°C.*~~

~~We do not have a range of recommended temperature for the unit, but we do have a recommendation of NOT exceeding 90 degrees C.~~

~~Storage of the temperature monitor settings~~

- These settings are stored in the /home/spectracom/config folder - temp.conf file



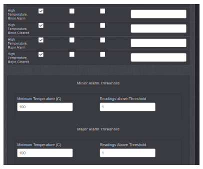
```
MINOR 100000 1
MAJOR 100000 1
SETTING 0
MINTEMP 30000
MAXTEMP 40000

```

~~Q. If the fan is left in the always on function what is the expected time before it may stop working and will the SecureSync indicate a failure of the fan in anything other than the logs?~~

~~**A. Keith's response (10 Feb 16) :** the life expectancy for the fan when always running is 60000 hrs @ 40°C (about 7 years). As there is no feedback from the fan indicating whether or not it's actually spinning, there isn't a direct indication of the fan's operation (log entries, alarms or alerts) available for the SecureSync.~~

~~However, software version 5.3.1 also added SNMP traps and gets and Minor/Major alarms associated with the internal temperature. If the cooling fan was to fail and this resulted in the internal temperature exceeding a user-specified threshold, a Minor and/or Major alarm can be optionally asserted and an optional SNMP trap can be sent to an SNMP Manager.~~

~~Alarms and SNMP Trap alerts for high/low temperatures are configured in the **Management** -> **Notifications** page of the browser (with version 5.3.1 or above installed), **System** tab (as shown below)~~



High Temperature, Minor Alarm ☑ □ □
High Temperature, Minor, Cleared ☑ □ □
High Temperature, Major Alarm ☑ □ □
High Temperature, Major, Cleared ☑ □ □

Minor Alarm Threshold

Minimum Temperature (C): 100
Readings above Threshold: 1

Major Alarm Threshold

Minimum Temperature (C): 100
Readings Above Threshold: 1

~~Checkboxes in this tab allow the associated temperature traps to be enabled to be sent, and the user-configurable temperature thresholds are configured in the fields towards the bottom of this tab. "Readings above threshold" allows a delay (in seconds) between each insertion of this alarm (for instance, set it to "5" for a 5 second delay between each insertion of the condition, if the temperature remains above the specified value for a length of time. this prevents it from being continuously inserted as the temp remains above the threshold).~~

~~Software versions 5.3.0 and below~~

- All original as well as all units shipped Oct 2014 until 5.3.1 was released (~Dec 2015) hardware caused cooling fan to turn on at 40C.
- Units shipped between ~Feb 2014 and ~Oct 2014: Hardware (resistor change) caused the cooling fan to turn on at 50C (instead of 40C).
- Until version 5.3.1 was cut-in to manufacturing (~Dec 2015) Temperature reading for the cooling fan operation was based on a temperature sensor located on the front panel assembly of all units. As of at least Dec 2015, this sensor's temperature reading is NOT reported anywhere (it's not one of the three temperatures reported in the browser with later software versions, for example). It just turned the fan on and off (version 5.3.1 with an EEPROM change incorporated moved fan control to software, based on CPU temp or fan always running).

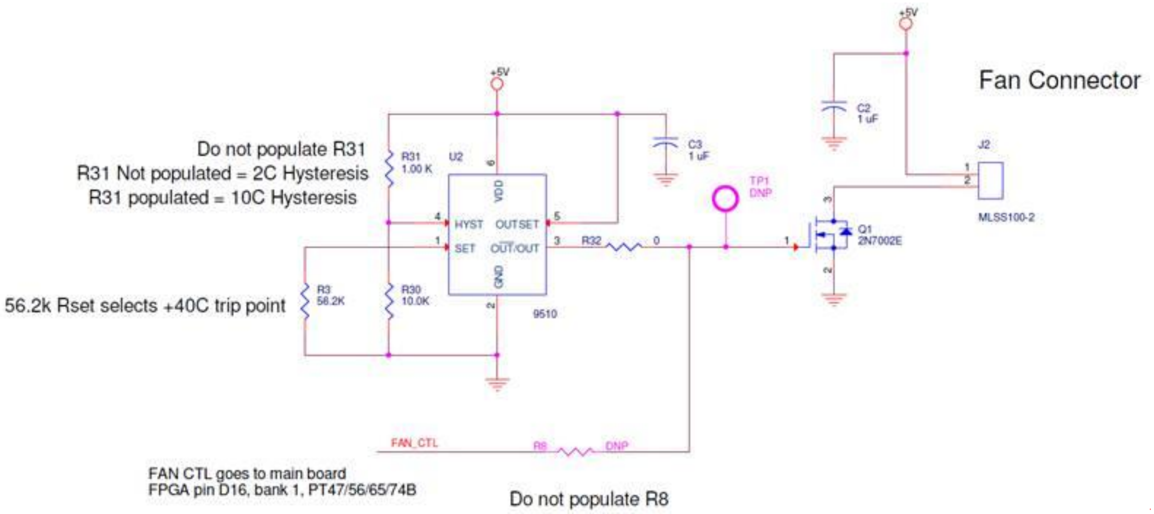
Hysteresis

- Used to turn the fan off, once it's on.
- The Temperature must drop by the set Hysteresis value to off, once it is on, in order for fan to turn off.

- ~~**Example**: If Hysteresis is set to 10C, the temperature must drop by 10C from what it was when the fan turned on, before the fan turns off again.~~

~~**Email from Mark McGregor (12 Oct 2015)** There was a period of time when the SecureSync fan control located on the front panel was changed from its original settings of fan turn on at 40C and 10C Hysteresis (for hysteresis, temperature must drop 10C to turn fan off once it is on). This will be present only on the newer front panels with bare PCB 1200-1000-0300 Rev. C. The 1200-1000-0300 Rev. C have an SMT connector to the front panel overlay, J3, rather than a through hole connector.~~

~~The 50C turn on, 2C hysteresis was done by making front panel resistor R3 to 48.7k and new resistor R31 not populated, DNP.~~



~~When the Harris high RB failure rate investigation was done, it was discovered that the change to have the fan run less was not good for Rb units and later for the ETX as well.~~

~~So, some time last year, the newer front panels fan control has been changed to be back to the original 40C turn on, with 10C hysteresis to try to keep the RB and ETX as cool as possible.~~

~~The original 40C turn on, 10C hysteresis was restored by making front panel resistor R3 back to the original 56.2k and new resistor R31 populated, R116R-1001-YF0b, 1k-ohm.~~

~~**Note (3 Feb 2014 KW) Per Mark McGregor** - ECN 3381 is changing the temp for fan operation. Added changes to decrease fan switch temperature delta for on to off from **10C to 2C.** Also changed fan turn on temperature from 40C to 50C. This was to minimize the frequency shift of the oscillator getting pushed around when the fan cycles and drives the temperature inside the box from 45C to 35C faster than the control loop can follow.~~

Automatic thermal shut-down/operating in an “overtemp” condition

Operating temperature spec change

Email from Tony Difloirio to Hughes network (1/13/12)

This temperature spec was first changed in August 2010 – see attached datasheet from Aug 17, 2010 (rev F). Which is well before HNS selected Spectracom for the Jupiter project. Also, our engineers have informed me that the unit will operate at +70C, however, due to UL certification requirements the metal surfaces in the unit are not allowed to get above +70C and thus the reason for the change.

Q. Also can you provide information about what can be expected if the units are run beyond these limits? We do not intend to run them outside the range but we need to know the impact to the performance if the units are run beyond the limits.

(Email from Dave Sohn) Initially as the unit is heated above the temperature specification, the oscillator driving the timing system will become unstable. This instability will affect our timing performance and all output performance. As the unit continues to be heated, the unit will become unstable and unresponsive. On the low end, the first failure will be the front panel display failing to operate, and then the remainder of the unit will become unstable and unresponsive.

~~Per your other questions, the SecureSync does not have an automatic shutdown on over-temperature condition.~~ However, it does have a temperature-operated cooling fan which turns on and off the cooling fan, based on the internal temperature. The temperature data calculated by the internal temperature sensor is not available to be reported by the SecureSync, so the internal temperature cannot be obtained from the appliance. The sensor is just used to control the cooling fan.

Email from Dave Sohn 3/28/11

The unit will always feel warm after a period of operation.
The fan should come on when the sensor is at +40C and shut off when the sensor is at +30C.

Note (3 Feb 2014 KW) Per Mark McGregor - ECN 3381 is changing the temp for fan operation added changes to decrease fan switch temperature delta for on to off from **10C to 2C.** Also changed fan turn on temperature from 40C to 50C. This was to minimize the frequency shift of the oscillator getting pushed around when the fan cycles and drives the temperature inside the box from 45C to 35C faster than the control loop can follow.

Note: Clarification to the SecureSync manual- the fan may not energize at power-up, if the unit wasn't running for about an hour or so prior to power-cycle. If the unit is cold at power-up, the fan won't run at start-up. But if it's warm, it will. (The internal temperature needs to be elevated above 30 Deg C to have the fan come on at startup).

To test the cooling fan operation, follow this procedure:

1) Power up the unit and allow it to warm up for about 30 minutes. This will raise the internal temperature to the operating range of the fan.
2) Turn off the power for about 5 seconds
3) Turn on the power and listen for the fan to come on. It will the turn off after a short period of time unless the internal temp is above the fan shutoff level.

Issue with SecureSync booting back up again at the same temperature it was while it was running (observed long before Sept 2015/version 5.3.0 update) erratic front panel display observed

- Occurs if the temperature is near 55°C when the SecureSync is rebooted.
- If the ETX module has a chance to first cool down a few degrees, it will boot-up normally

Email from Dave Sohn (21 Sept 2015) This appears to be an issue with the ETX modules where they can run at high temperatures, but there is something restricting them from starting up at the same temperature. After the processor cools down for some short period, the system will start up again. We started talking with the manufacturer, Advantech, but I don't believe we have gotten far with that yet. It may also be worsened by some of the changes with the front panel fan operation that were shipping for a few months. This caused the fan to run less often.

As far as fixes, we are looking at changing the heat dissipation technique for the ETX. Currently we have a heat sink applied directly to the processor chip on the ETX, but a heat spreader is also available from the manufacturer that will pull the heat from the chip and spread it over a larger area. Operating at my desk, the overall temperature of the processor and ETX were lower by more than 5 degrees with the heat spreader. Whether we would work with just the heat spreader, or in combination with a heat sink remains to be seen. Alternatively, we are also looking at a newer ETX module from the vendor as well.

Example log entries from a unit with a CPU temp of 100 deg

- Refer to salesforce case 24138

Email from Dave L to Engineering (12 Jan 17) Here is a report of a Securesync that was updated from v 5.1.4 to 5.5.1 that has a high CPU Temp of 100 Deg. Also the GNSS 0 Reference keeps switching between Green and Dark on the HOME page. It should be going Green / Red,   I see some of these strange messages in the System.log:

```
Jan 12 17:22:56 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed:
log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 17:23:23 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:24:35 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:28:30 DC-NTP1 last message repeated 2 times
Jan 12 17:30:25 DC-NTP1 last message repeated 2 times
Jan 12 17:31:02 DC-NTP1 DC-NTP1: [webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetPhaseErrorLim
0   (KTSAL)
Jan 12 17:32:42 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:33:54 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:35:18 DC-NTP1 last message repeated 2 times
Jan 12 17:37:01 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:38:25 DC-NTP1 last message repeated 2 times
Jan 12 17:40:09 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:41:34 DC-NTP1 last message repeated 2 times
Jan 12 17:44:19 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:45:31 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:47:13 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 17:47:43 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed:
log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 17:59:42 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed:
log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 18:06:43 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed:
log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 18:16:44 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed:
log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 18:18:47 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed:
log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 18:51:43 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed:
log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 19:03:32 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 19:05:55 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed:
log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 19:05:56 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
Jan 12 19:11:00 DC-NTP1 DC-NTP1: [webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetMode 0   (KTSAL)
Jan 12 19:13:44 DC-NTP1 DC-NTP1: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 19 NOT NULL constraint failed:
log_ref_mon_statuses.ref2_phase (WEB)
Jan 12 19:15:33 DC-NTP1 DC-NTP1: [WEB] Failed TSYNC_RS_getState: 30003 (admin)
```

Reading/obtaining/storing internal temperatures

(Note: this info is from 1200 SecureSyncs)

Regarding the front panel cooling fan

The Temperature reading for the cooling fan’s operation is based on a temperature sensor located on the front panel assembly of all units. As of at least Oct 2015, this sensor’s temperature reading for the fan operation is NOT reported anywhere (it’s not one of the three temperatures reported in the browser with later software versions, for example). It just turns the fan on and off.

In summary: The temp sensors/read-outs discussed below are not associated with the cooling fan operation.

Storage of and obtaining reported/displayed temperatures/

Storage of the temperature data

Length of time Temperature data is stored for:

- refer to (in the SecureSync online user guide, then scroll down to “**Deleting Temperature Data**”) http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm

Email from Ron D (28 Mar 18) The temperature monitor graph page in the online manual states it. It should probably be added to all of the graph sections that it applies to.

Note- not edited to be directly sent to a customer- except

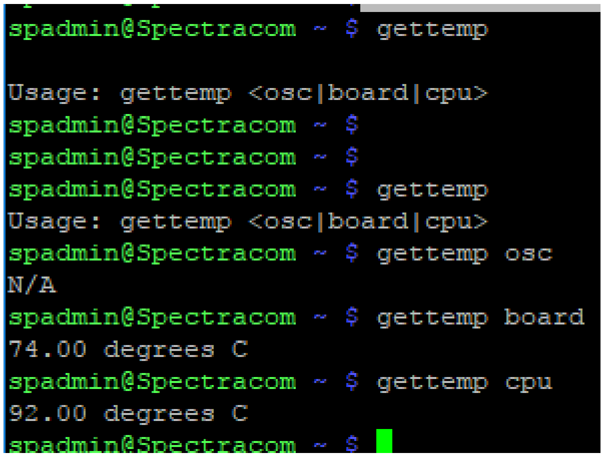
“Temperature graphs (and other graphs as well) will display up to approximately 10000 readings, which are generated at a 1/min. rate, i.e. the data displayed covers about 7 days. Thereafter, the oldest data gets overwritten.”

http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm

A) Via the CLI interface:

**Obtain Oscillator, board and CPU temperature readings via CLI (applicable to versions 5.4.5 and above only)

- Version 5.4.5 added the **gettemp** command to allow reading of temperatures.



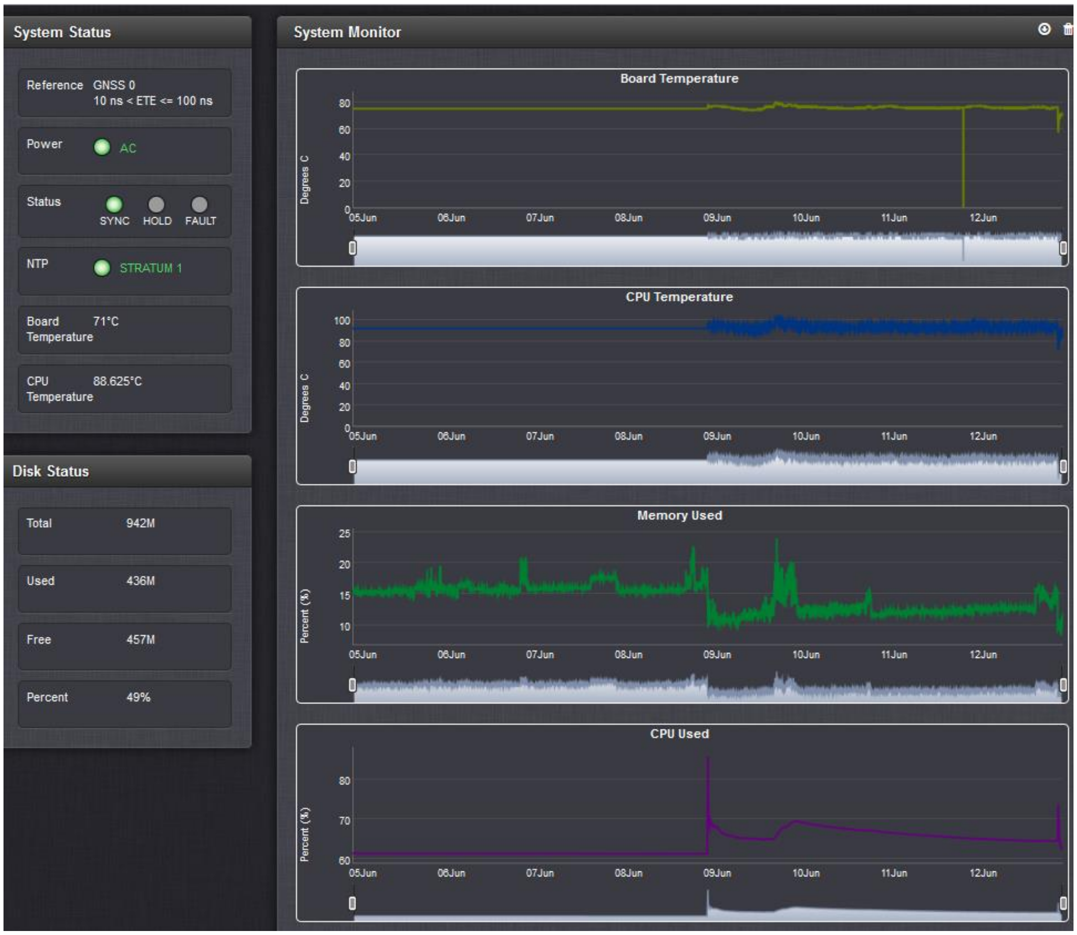
```
spadmin@Spectracom ~ $ gettemp

Usage: gettemp <osc|board|cpu>
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $ gettemp
Usage: gettemp <osc|board|cpu>
spadmin@Spectracom ~ $ gettemp osc
N/A
spadmin@Spectracom ~ $ gettemp board
74.00 degrees C
spadmin@Spectracom ~ $ gettemp cpu
92.00 degrees C
spadmin@Spectracom ~ $
```

Q We would like a system status command via the CLI which gives up the temperature ("sensors" command on a Linux box)

A Email from Dave Sohn to Matt Loomis (8 Mar 16) "cat /sys/class/hwmon/hwmon0/temp*_input" run from the command line will provide the raw temperature monitor information from the processor board and CPU in that order. Divide by 1000 for degrees Celsius.

B) Via the web browser

- ***Tools*** -> ***System Monitor*** page of the browser



System Status

Reference	GNSS 0 10 ns < ETE <= 100 ns
Power	● AC
Status	● SYNC ● HOLD ● FAULT
NTP	● STRATUM 1
Board Temperature	71°C
CPU Temperature	88.625°C

Disk Status

Total	942M
Used	436M
Free	457M
Percent	49%

NOTE: from talking with Dave Sohn (22 oct 15 KW). These reported temperatures (in Celsius) may initially appear to be very hot to some customers. They need to understand that these are not ambient temperatures inside the chassis. They are the actual die temperature for the processor (Processor temp and CPU temp) or very close to the ovenized oscillator (Oscillator temp). These higher temps are expected for the specific components they are monitoring.

Note: all temperatures are calculated and reported in **Celsius**

A) "Oscillator temperature" (sensor "U60" located on the PCB very near the oscillator- not inside the oscillator. This was the first available temp readout - starting in software version 5.1.7)

Notes:

- The oscillator temp is not located inside any of the Wentzel oscillators, or any of our oscillators. It's an ambient sensor located on the main board NEAR the oscillator. Ambient temp changes wil inherenelty affect this temperature reading.
- Requires a hardware thermostat that started being installed on Rev B main boards back in 2012. Units purchased prior to Rev B (starting sometime in 2012) will not see these additions.
- This was the first temperature read-out available in the SecureSync.
- Per Paul Myers (in Mantis case) 9489s do not have the temperature sensor installed. Only SecureSyncs and 9483 purchased after sometime in 2012 have the sensor installed.
- Software version 5.1.7 and below don't provide the means to report internal temperature (even if the sensor is installed)
- Software update version 5.2.0 added internal "temperature" readout (software support for an earlier hardware change of adding a thermostat that occurred sometime in 2012 with Rev B main boards)
- Typical temperature reading is around 50 degrees C.
- This temperature is measured near the oscillator, so its labeled changed from "*Temperature*" to "*Oscillator Temperature*" in later software versions.

Email Keith sent to a customer concerned about a .4 degree OI spoke to one of engineers about what you are observing. He reminded me that it was important for you to understand that the reported Oscillator Temperatures are not obtained from a sensor within the oscillator itself. These readings are instead obtained from a sensor located on the main PCB board, near where the oscillator is located. So this sensor readings are affected by any ambient temperature changes to the internal air flow inside the unit. They are not a report of temperature fluctuations from within the oscillator itself (The oscillators used in the SecureSync do not report their internal temperatures. We just refer to this ambient air temperature reading as the "Oscillator temperature" because of where this sensor is located within the SecureSync).

The Wetzel oscillator in the Hughes SecureSync (and also the standard OCXO and Rubidium oscillators which can also be installed in SecureSyncs), is an ovenized oscillator, which helps it compensate for ambient air temperature changes. Changes in the oscillator's DAC values are completely expected as its internal oven operates to keep the temperatures within the oscillator as stable as possible. The DAC changes are needed to steer the oscillator to 10 MHz as the internal temperatures waiver.

In summary, the "oscillator temp" is an ambient temperature reading taken near the oscillator. Changes of a few tenths of a degree in the ambient temperature are not at all unexpected and the oscillator's internal over works to help dampen out the temperature changes inside the oscillator.

Storage/output of the three temperatures (and oscillator data) (via either a ".csv" or ".json" file)

All three available temperatures are stored in MySQL database and can be downloaded as either a. "**.csv**" file (for raw data that can be opened in excel) or a "**.json"** file (for raw graphing).

Download of raw temperate data as a ".csv" file (can be opened in excel)

- A ".csv" file with the three available temperatures can be downloaded in one of either two different methods

1. Download button available in the Management -> Disciplining page of the browser

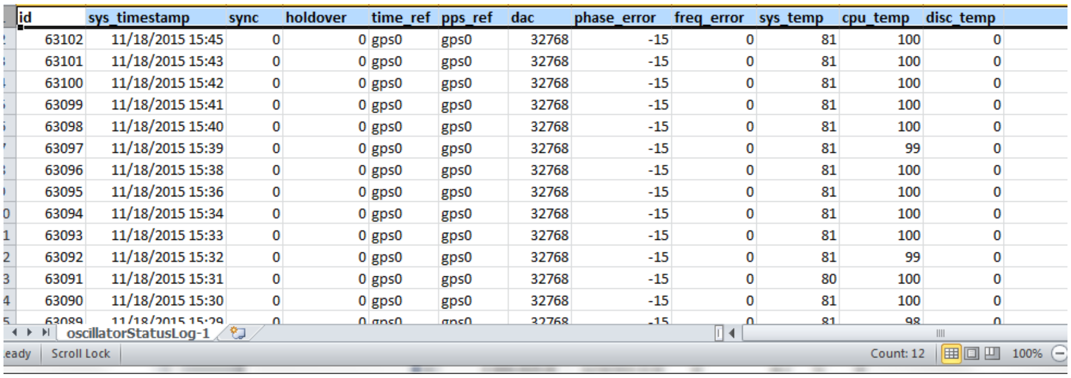
From the ***Management*** -> ***Disciplining*** page of the browser (click on the "**down arrow**" icon on the right side of the page to download the .csv file. Press the garbage can icon to delete all of the oscillator and temperature data used to display the graphs)

2. Manually enter the link to the OscillatorStatuslog

If you manually enter **/logs/OscillatorStatusLog.csv** after the URL of the SecureSync in the web browser it will download a csv file that can be opened in Excel with the GPS status log data.

Example: http://10.10.128.1/logs/OscillatorStatusLog.csv (change address as applicable)

Example output below ("Sys temp" and "CPU temp" fields were added in software version 5.3.0)



id	sys_timestamp	sync	holdover	time_ref	pps_ref	dac	phase_error	freq_error	sys_temp	cpu_temp	disc_temp
63102	11/18/2015 15:45	0	0	gps0	gps0	32768	-15	0	81	100	0
63101	11/18/2015 15:43	0	0	gps0	gps0	32768	-15	0	81	100	0
63100	11/18/2015 15:42	0	0	gps0	gps0	32768	-15	0	81	100	0
63099	11/18/2015 15:41	0	0	gps0	gps0	32768	-15	0	81	100	0
63098	11/18/2015 15:40	0	0	gps0	gps0	32768	-15	0	81	100	0
63097	11/18/2015 15:39	0	0	gps0	gps0	32768	-15	0	81	99	0
63096	11/18/2015 15:38	0	0	gps0	gps0	32768	-15	0	81	100	0
63095	11/18/2015 15:36	0	0	gps0	gps0	32768	-15	0	81	100	0
63094	11/18/2015 15:34	0	0	gps0	gps0	32768	-15	0	81	100	0
63093	11/18/2015 15:33	0	0	gps0	gps0	32768	-15	0	81	100	0
63092	11/18/2015 15:32	0	0	gps0	gps0	32768	-15	0	81	99	0
63091	11/18/2015 15:31	0	0	gps0	gps0	32768	-15	0	80	100	0
63090	11/18/2015 15:30	0	0	gps0	gps0	32768	-15	0	81	100	0
63089	11/18/2015 15:29	0	0	gps0	gps0	32768	-15	0	81	98	0

Definition of fields

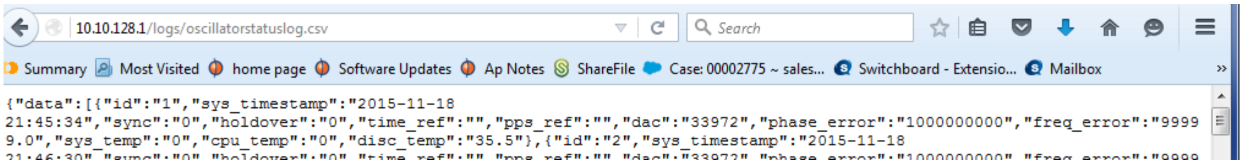
- **Sync** and **Holdover**: 1 is true, 0 is false
- **Time ref** and **PPS ref:** Selected input reference at that time
- **DAC:** Oscillator's DAC value
- Phase Error: 1PPS Phase Error
- **Freq Error:** Oscillator's Frequency Error
- Temps: Board, CPU and Oscillator
- **Notes**:
  1. **Oscillator** temp is only available if sensor is installed on the main PCB
  2. **Board** and **CPU** temps were added in software version 5.3.0

Output of graphable temperature and oscillator data (.json file)

➢ Same process as downloading.csv file, but replace ".csv" with ".json" instead.

If you manually enter **/logs/OscillatorStatusLog.json** after the URL of the SecureSync in the web browser it will download a csv file that can be opened in Excel with the GPS status log data.

Example: http://10.10.128.1/logs/OscillatorStatusLog.json (change address as applicable)



10.10.128.1/logs/oscillatorstatuslog.csv
Search
Summary
Most Visited
home page
Software Updates
Ap Notes
ShareFile
Case: 00002775 ~ sales...
Switchboard - Extensio...
Mailbox

```
{"data":[{"id":"1","sys_timestamp":"2015-11-18
21:45:34","sync":"0","holdover":"0","time_ref":"","pps_ref":"","dac":"33972","phase_error":"1000000000","freq_error":"9999
9.0","sys_temp":"0","cpu_temp":"0","disc_temp":"35.5"},{"id":"2","sys_timestamp":"2015-11-18
21:46:30","sync":"0","holdover":"0","time_ref":"","pps_ref":"","dac":"33972","phase_error":"1000000000","freq_error":"9999
```

Processor board and CPU temperature graphs

(Note: this info is from 1200 SecureSyncs)

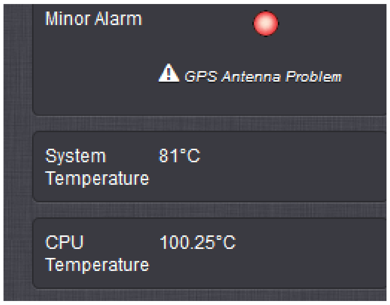
Note about refernces to "temp sensor": "Oscillator" temp is only available if the temperature sensor (U60) is installed on the main PCB (very close to the oscillator). Refer to ECN 2807 (5 Dec,2011)

- Software version 5.3.0 (Sept 2015) also added Board (System) Temperature and CPU temperature (three different temperatures are now available, for newer units that have the temp sensor installed)
- The CPU and board temperatures are not stored in discstats. All three temperatures are stored in MySQL database and can be downloaded as part of a csv or json file. See the information further above about how to export this raw data that is used for graphing.

- **CPU Temperature** and **Board Temperature** readouts added on the left side of the **Management** -> **Disciplining** page:
  - **System/Board Temperature** and **CPU temperature** readouts were added on the left side of the **Home** page, as well as the left side of the **Management** -> **Disciplining** page

- **Home** page of browser

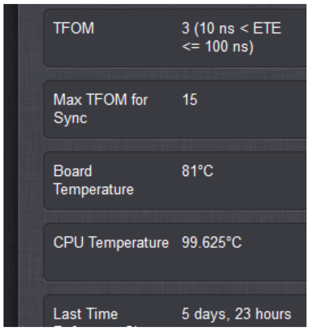
Management -> **Disciplining** page of browser



Minor Alarm

GPS Antenna Problem

System Temperature	81°C
CPU Temperature	100.25°C



TFOM	3 (10 ns < ETE <= 100 ns)
Max TFOM for Sync	15
Board Temperature	81°C
CPU Temperature	99.625°C
Last Time	5 days, 23 hours

Summary of temperature readings:

(Note: this info is from 1200 SecureSyncs)

- **"Temperature"** / "**Oscillator Temperature"** = temperature sensor on PCB, near the oscillator (~ 50 deg c) (this was the first sensor reported - reported temperature was added in software versions 5.2.0/5.2.1, if the temp sensor is installed)
- **"CPU Temperature"** = Processor temperature based on sensor near the KTS CPU processor (~100 deg C) (available in versions 5.3.0 and above)
- **"Board Temperature" / "System Temperature"** = **ETX module** temperature (~80 deg C) (available in versions 5.3.0 and above) via temp sensor within the ETX module (die temperatire of the ETX module).

Temperature(s) displayed/reported/recorded:

- Only the temp sensor on the main board (if installed) is recorded in discstats (end of each entry)

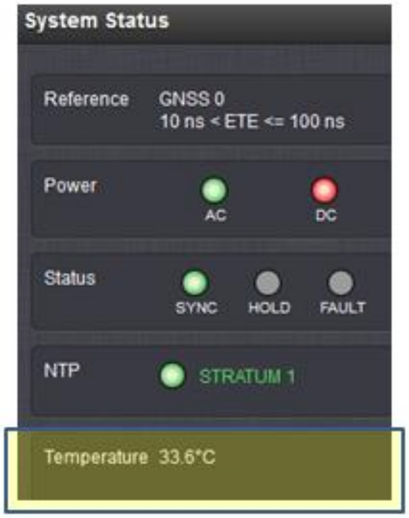
```
16591,194,1,0,ird0,ird0,33384,15,8.94e-14,59.597710
```

- The CPU and board temperatures are not stored in discstats. All three temperatures are stored in MySQL database and can be downloaded as part of a csv or json file. See the information further above about how to export this raw data that is used for graphing.
  - **Report via SNMP**: As of at least v5.2.0, temperature doesn't appear to be available via SNMP.
  - **Note**: Refer to Mantis case 1857.

- Displayed on the Home page of the newer browser (under “System Status” in the upper left corner)

Note: Temperature reports are not available in the classic interface browser

Versions 5.2.0 and 5.2.1 (if the temp sensor is installed)



System Status

Reference GNSS 0
10 ns < ETE <= 100 ns

Power AC DC

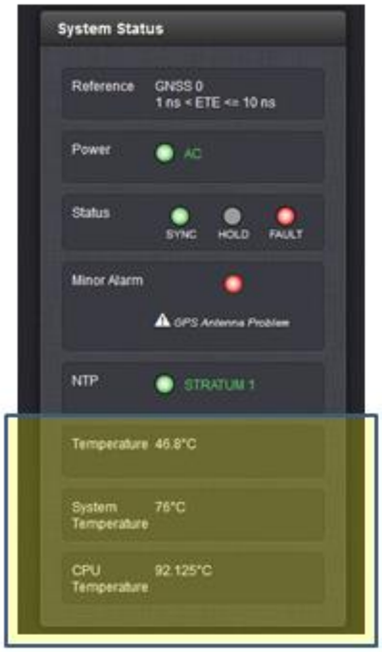
Status SYNC HOLD FAULT

NTP STRATUM 1

Temperature 33.6°C

“Temperature” = temperature near the oscillator

Versions 5.3.0 and above (if the temp sensor is installed)



System Status

Reference GNSS 0
1 ns < ETE <= 10 ns

Power AC

Status SYNC HOLD FAULT

Minor Alarm GPS Antenna Problem

NTP STRATUM 1

Temperature 46.8°C

System Temperature 76°C

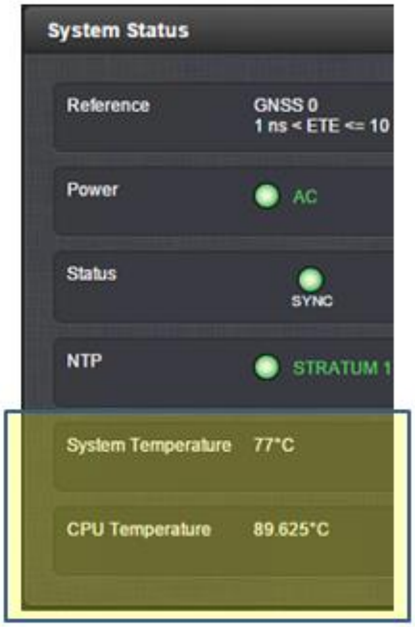
CPU Temperature 92.125°C

“Temperature” = temperature near the oscillator

“**System Temperature**” = ETX module temperature

“**CPU Temperature”** = Processor temperature

Software was updated to versions 5.3.0 and above (temp sensor was not installed)



System Status

Reference GNSS 0
1 ns < ETE <= 10

Power AC

Status SYNC

NTP STRATUM 1

System Temperature 77°C

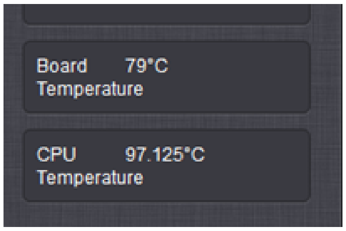
CPU Temperature 89.625°C

Temperature near the oscillator not available without sensor installed

“**System temperature**” = ETX module temperature

“**CPU Temperature**” = Processor temperature

Version 5.3.1 (if the temp sensor isn’t installed)



Board Temperature 79°C

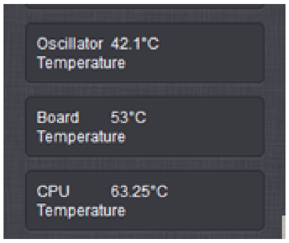
CPU Temperature 97.125°C

“**Board Temperature**”= ETX Module Temperature

“**CPU Temperature**” = Processor Temperature

Note: “Oscillator Temperature” not available without sensor installed

Version 5.3.1 (if the temp sensor is installed)



Oscillator Temperature 42.1°C

Board Temperature 53°C

CPU Temperature 63.25°C

“Oscillator Temperature” = Temperature near the oscillator

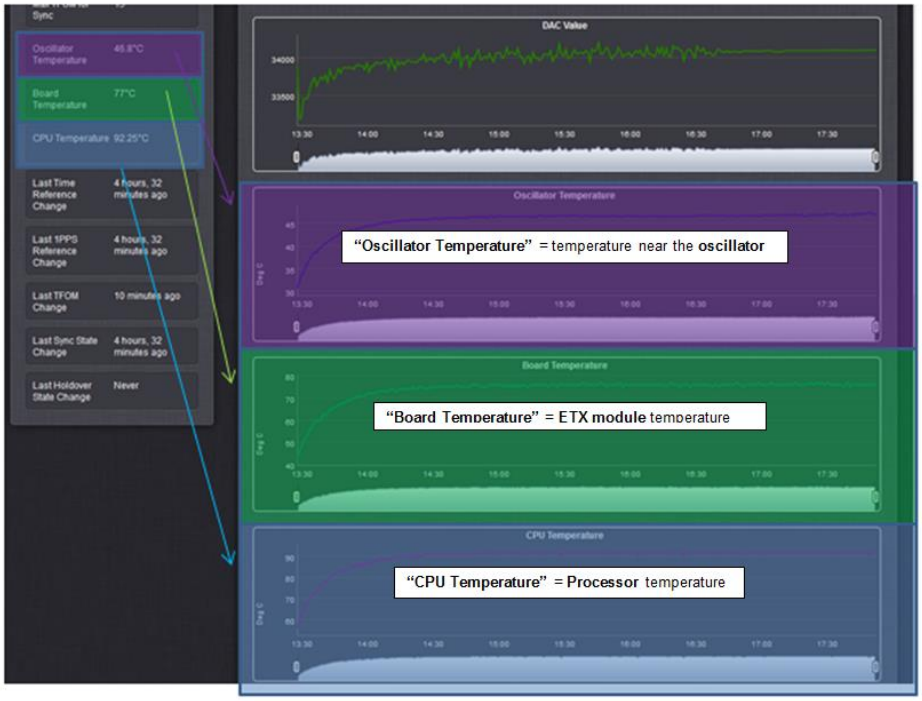
“**Board Temperature**”= ETX Module Temperature

“**CPU Temperature**” = Processor Temperature

Temperature-over-time graph (**Management -> Disciplining** page)

(Note: this info is from 1200 SecureSyncs)

- Reports Oscillator, board (ETX Module) and CPU (Processor) temperatures



Sync	
Oscillator Temperature	46.8°C
Board Temperature	77°C
CPU Temperature	92.25°C
Last Time Reference Change	4 hours, 32 minutes ago
Last 1PPS Reference Change	4 hours, 32 minutes ago
Last TFOM Change	10 minutes ago
Last Sync State Change	4 hours, 32 minutes ago
Last Holdover State Change	Never

"Oscillator Temperature" = temperature near the oscillator

"Board Temperature" = ETX module temperature

"CPU Temperature" = Processor temperature

Length of time the temperature data is stored for:

- refer to (in the SecureSync online user guide, then scroll down to "**Deleting Temperature Data**") http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm

Email from Ron D (28 Mar 18) The temperature monitor graph page in the online manual states it. It should probably be added to all of the graph sections that it applies to.

"Temperature graphs (and other graphs as well) will display up to approximately 10000 readings, which are generated at a 1/min. rate, i.e. the data displayed covers about 7 days. Thereafter, the oldest data gets overwritten."

http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm

Q. I'm trying to find out of the SecureSync has a SNMP MIB variable to provide temperature? I have searched our SecureSync and Spectracom MIBs without finding anything so to be sure, I am asking

Update to the answer below (9 Dec 2015 KW). Software update v5.3.1 added objects for providing temperatures of the Oscillator, CPU and board (temp sensor on the front panel for the cooling fan isn't available via SNMP).

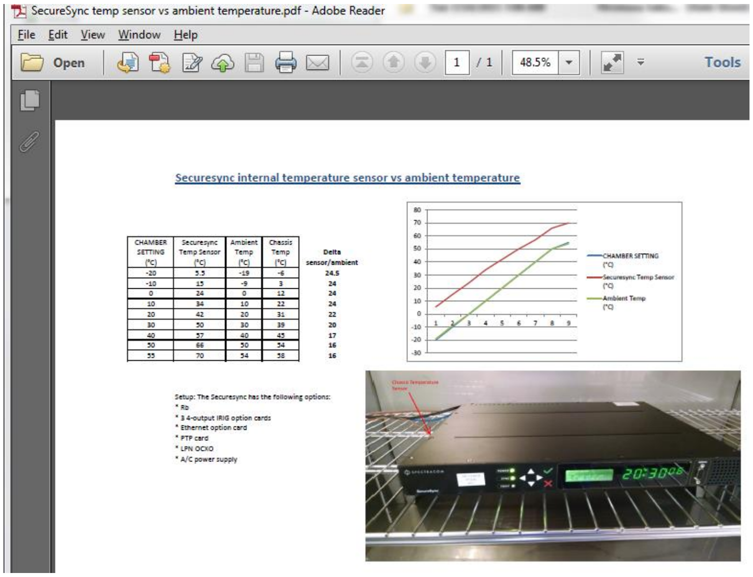
A (KW 11/8/12) with at least Archive versions 4.8.7 and prior, there is no way to read the internal temperature. Prior to Rev B of the main circuit board, there was no thermostat in the SecureSyncs. Rev B of the board adds a thermostat, but the software is not currently inter-operating with this component. Someday, we may integrate it into software. If we do, customers that apply the software update will have this capability available, if they have a rev B (or higher) circuit board installed.

Test data on the internal temperature sensor of the SecureSync vs ambient temperature

(Note: this info is from 1200 SecureSyncs)

Q (from Raytheon) “for the temperature, I noticed that the probe is for internal to the system. At what reading would the temperature be considered critical? How does the operating temperature range in the spec correlate to the temp reading on the system?”

A Reply from Tim Tetreault (13 Jul 2015) Here is the test data on the internal temperature sensor of the SecureSync vs ambient temperature. The testing was done with a SecureSync that had the same configuration as the SecureSync’s in the AMDR units.


SecureSync temp sensor vs ambient temperature.pdf - Adobe Reader
File
Edit
View
Window
Help
Open
1 / 1
48.5%
Tools
80
70
60
50
40
30
20
10
0
-10
-20
-30
1
2
3
4
5
6
7
8
9
CHAMBER SETTING (°C)
Securesync Temp Sensor (°C)
Ambient Temp (°C)
Chassis Temperature Sensor

Securesync internal temperature sensor vs ambient temperature

CHAMBER SETTING (°C)	Securesync Temp Sensor (°C)	Ambient Temp (°C)	Chassis Temp (°C)	Delta sensor/ambient
-20	5.5	-19	-6	24.5
-10	15	-9	3	24
0	24	0	12	24
10	34	10	22	24
20	42	20	31	22
30	50	30	39	20
40	57	40	45	17
50	66	50	54	16
55	70	54	58	16

Setup: The Securesync has the following options:
* Rb
* 3 4-output IRIG option cards
* Ethernet option card
* PTP card
* LPN OCXO
* A/C power supply

Lithium Battery (or batteries) that may be installed / battery change intervals/ Shelf life

1. **There is one Lithium battery in all SecureSyncs for the RTC (Real Time Clock) to keep it incrementing each second when the unit's primary power is lost.**
   - Refer to the lithium coin celll battery section further below for details on this battery:
2. **If a GB-GRAM Receiver (Model 1204-1A Option Card) is installed, it also has one lithium battery installed**
   - Refer to the separate "Model 1204-1A GB-Gram Option card 12" document for details on this battery: U:\Engineering\SAASM-FOUO\CustomerService\SecureSync

In summary of the info above:

Either one or two batteries are installed in SecureSync:

- There is just one lithium battery is installed if GB-Gram SAASM receiver is not installed (the lithium battery for the RTC)
- Two batteries are installed if GB-GRAM SAASM receiver is installed (one lithium battery for the RTC and the other lithium battery is for the receiver)

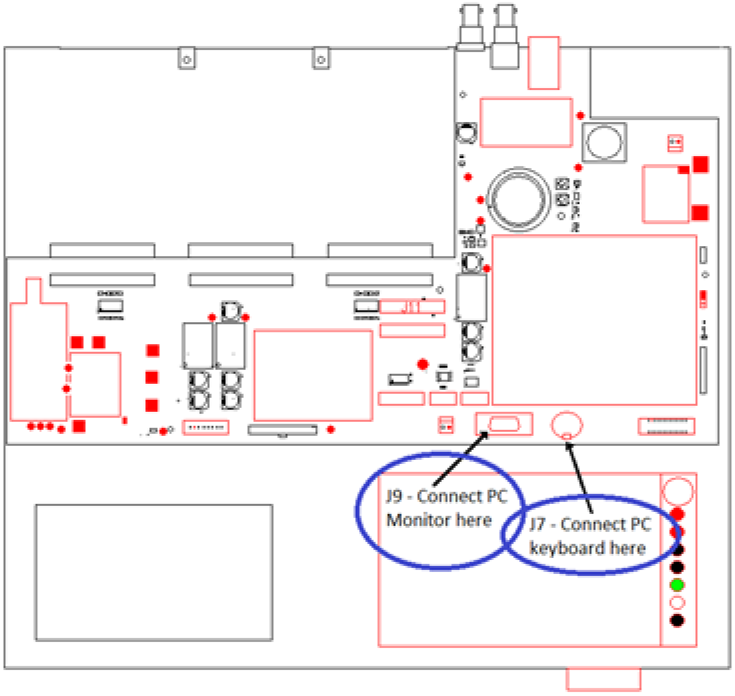
BIOS/ CF Card/ RTC (Real Time Clock) / kernel time at boot-up/ RTC coin cell battery / Shelf Life

NO ETX module installed in 2400 SecureSyncs

(Note: this info is from 1200 SecureSync)

Desire to view the BIOS

Email from /Dave Lorah- These items are you standard VGA cable and Keyboard cable, I have attached the jpegs for your review



BIOS protection against viruses

Q. Do we protect BIOS from potential viruses and possible corruption?
A Reply from Mark Goodlein (3/21/12) Our system is running Linux and the permissions have been locked down for security to protect it from viruses. In order for a virus to attack the BIOS, it would require superuser access, which has been locked down.

Q. Do you support a Secure BIOS Ecosystem?

- Digital signature that ensures Firmware/BIOS/Image authenticity.
- Root of trust for updates. contains signature verification algorithm and a key store that includes a public key to verify the signature or include a hash of the public key if a copy of the public key is provided with the BIOS update image
- Authentication BIOS mechanism.

- Do you have a protection mechanism?

Local Updates

- Ensures authenticity and integrity of the update image by requiring physical presence
- Supply chain ensures a secure, trusted or attested to BIOS
- The supply chain and custody process is documented
- Restriction of remote upgrades via a network

A Reply from Mark Goodlein (3/21/12)
Our BIOS is flashed by the vendor then configured here in manufacturing. We do not currently support updates to the BIOS nor have we ever needed to. I do not believe we have a “Secure BIOS Ecosystem” or any specific protection mechanisms in place.

For ETX BIOS configuration, refer to: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\ETX BIOS settings

NOTE: SecureSync boots-up using the ETX BIOS settings for its starting Time/Date values (BIOS time is “loosely” maintained by the RTC in the ETX module, as described further below).

Default BIOS settings: 2003/1/1 00:00. (year 2003)

Note: If the default BIOS date/time are displayed after each power-up:

- BIOS (coin cell) battery may be bad. TP69 should be around 3 vdc with a good battery installed. Refer to: Shelf Life/Internal coin cell battery further down in this document.
- ETX module was removed/reinstalled without the BIOS being correctly configured.
- The BIOS was not set correctly at the factory prior to shipment.

Q. If the power is turned OFF and ON, the date and time of SecureSync are reset. Is it possible to make a setting so that SecureSync recovers with the date and time close to the time when the power was turned OFF?
A. SecureSync will load the system time from a battery backed clock each time it powers up. The unit will still not be in sync until a valid reference is applied, however. We are going to be adding a feature that will allow a user to select a mode where that battery backed time write also synchronizes the unit.
(**update 10/28/12**-Battery Backed time was added in V4.8.0).

RTC backup battery (BT1 on top side of the CPU board)

- Refer to model 2400 SecureSync user guide at: https://safran-navigation-timing.com/manuals/2400/Content/NC_and_SS/2400/INTRO/Specs_InputPower.htm?Highlight=ac%20power%20source (excerpt below)

  - **Backup Battery:** *SecureSync has an internal battery to support the Real Time Clock. The battery is a small recharging 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. There is one rechargeable lithium battery installed on the CPU board in 2400 SecureSyncs (This is for the BIOS/RTC clock. A BATTERY,SM,LITHIUM RECHARGEABLE,3V,MS920T COIN,6.5MAH, Lithium coin cell battery)*

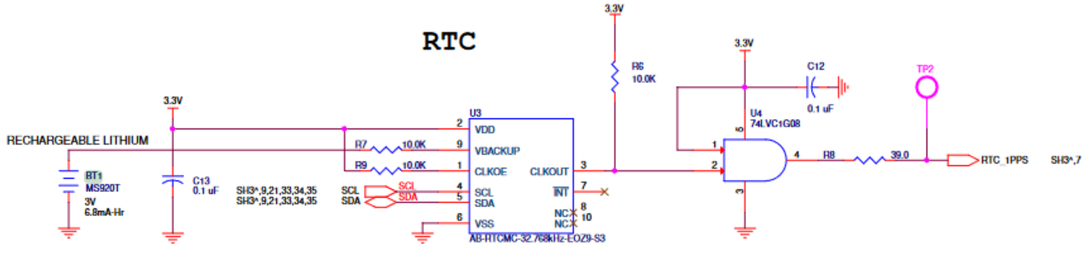
    - Our P/N for the battery: **BT30R-6R50-0C0M** (in Arena at: https://app.bom.com/items/detail-spec?item_id=1217515334&version_id=10547142528&orb_msg_single_search_p=1)
    - **MFG and MFG P/N**: SEIKO INSTRUMENTS INC: MS920T-FL27E
    - **Digi-Key P/N** 728-1077-ND
    - **Link to datasheet** (obtained from Digi-Key page for their P/N 728-1077-ND): https://www.seiko-instruments.de/fileadmin/Editors/COMP/PDF/MicroBattery_catalogue_E_2018A_forWeb.pdf

Datasheet provides environmental info (such as)

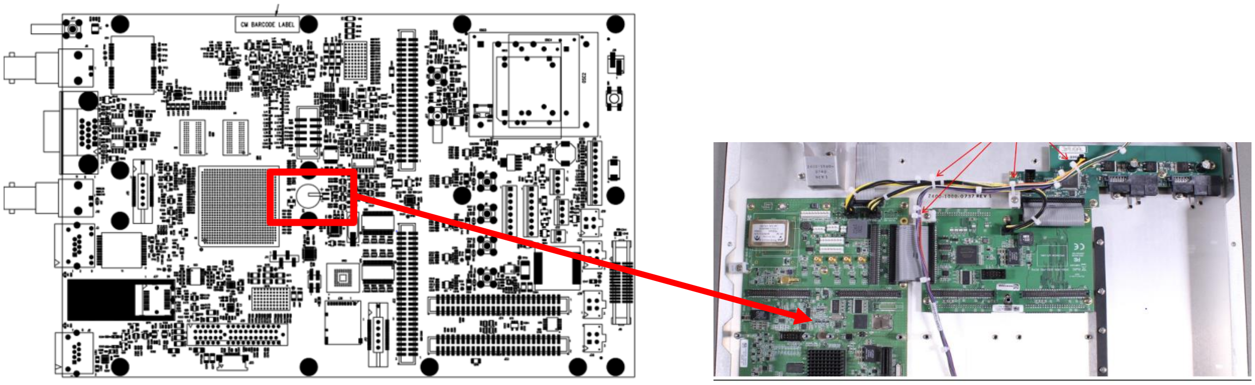
- Mercury-free
- Battery is not applied to RoHS Directives. Our battery products do not contain any substances restricted by RoHS Directive.
- Approved by UL (Underwriters Laboratories Inc.)

    - **Battery is installed on the 2400 SecureSync's CPU board** (P/N 2400-0000-F012 in arena at: https://app.bom.com/items/detail-bom?item_id=1278293557&version_id=11813815178)

Schematic for CPU board: 2400-1001-0212 in arena: https://app.bom.com/items/detail-spec?item_id=1278293579&version_id=11573082998
(note: excerpt below is for internal reference only)



200uA maximum charge current, SHOULD SET RTC for 5k Trickle Charge Resistor enabled, ~60uA charge with RTC 5k plus external 10k.



(Note: this info below is from 1200 SecureSyncs) need to see if applies to 2400

- Info/Document for replacing the RTC battery in SecureSync (P/N ~~1200-5000-0055)~~ ~~Refer to manuals in Released drive:~~ ~~EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Battery replacement~~

- There is one lithium battery installed on the main PCB in all SecureSyncs. This is for the RTC clock (A 3vdc - 500mAh, Lithium coin cell battery)
- The battery just allows the RTC clock to keep incrementing the time while input power is not available. It isn't used to store the time at all.
- The battery only discharges when input power is removed.
- If the battery is removed or its voltage drops too low, the worst thing that happens is the RTC doesn't increment while power is removed. So it will power-up with whatever the time/date was when it was last set. The amount of initial error is about the amount of elapsed time it was powered-down. If it was powered-down for 10 minutes, the time would be about 10 minutes or so off at power-up. It doesn't prevent the time from being changed from the incrementing 0's at start-up.

Recommended RTC battery voltage range (minimum voltage)

Per Tom Richardson (Oct 2014)

I found it in one of the design guides.

BATT Input=
3V backup cell input from carrier to SOM-ETX module for RTC operation and storage register non-volatility in the absence of system power. (BATT=2.4V-3.3V)

So it looks like 2.4 is the minimum.

Methods to tell if the RTC battery needs to be replaced

Q. how does the operator/maintainer know the battery needs to be replaced? Is there a way to use the software to check the battery levels?

A. reply from Keith (Oct 2014) To answer your question, there are really only two ways to tell if the Lithium coin cell RTC battery needs to be replaced. The first is the System Time will be incorrect at each power-up, with the amount of error being about the length of time it was powered-down for, until an external reference corrects the time and the SecureSync goes into Sync. The second way is to measure the voltage on the battery with the cover removed (there is also a test point on the main board for this voltage, TP69).

The battery has an expected life of about 5 years of cumulative unit power-down time (it only discharges when input power is removed from the SecureSync). As long as power is normally applied, I would recommend that the battery just be routinely replaced like every 5 years or so to prevent it from starting to become too low.

FYI- the coin cell BIOS battery is not considered critical to the SecureSync's operation. Its only function is to keep the Real Time clock incrementing when power is removed. The Real Time Clock is the start-up time reference for the system until an external time reference becomes present and valid to correct any time errors, before SecureSync goes into sync.

~~**Note**~~: ~~With the exception of the ETX module and battery/socket, the rest of the components associated with the coin battery are attached to the bottom of the main SecureSync PCB. The stand-offs need to be removed to allow access to the bottom of the PCB board.~~

C62 is a Bypass Capacitor for Noise. It is also for charge storage to keep the battery voltage up while the batter is being changed if the battery is not dead.

The battery is present to keep the ~~ETX single board computer~~ internal clock/date in stored memory should SecureSync power cycle. After power has returned the SecureSync will display BIOS time. The unit will update (+/- adjusted seconds) the displayed time upon normal GPS reception. A battery circuit failure will not affect GPS and/or Oscillator and Sync functions.

Please inform the customer that the SecureSync is not broken if the battery fails. It will operate properly without the battery. The SecureSync is still functional even with the ETX backup battery failed. The battery is only used when power goes down and the SecureSync has no power applied. The only effect of the failed ETX backup battery will be that it will take longer to Sync after power is re-applied. It will also not remember the time and date, etc., but will get it from the GPS.
The battery being dead is not a critical failure as if the SecureSync won't operate because the backup battery is dead.
Does the customer connect the SecureSync power into an Uninterruptible power supply**?**

Effects on the system if RTC battery is removed

- The only setting lost when the battery is removed is the RTC clock (date/time). All other BIOS Settings and System Settings (network, NTP, Reference Priority) are stored in Flash memory and are not lost when the battery is removed.

Q. If we remove and reseat "button battery" on the SecureSync and re-set clock by configuring the BIOS settings, will each setting(ex, IP address, NTP setting, reference setting etc,) be initialized?

A. **Reply from Keith (11 Nov 2014)** The very short answer to your question is "no". Each setting (ex, IP address,NTP setting,reference setting etc,) will not be initialized after removing/reinstalling this battery.

I confirmed with our Engineering team what the effects are of removing the ETX's Real Time Clock coin cell battery. The only setting lost when this battery is removed is the approximate date/time for the next time the unit is booted-up. The BIOS date/time can be reprogrammed after re-installing the battery if you wish. If this setting isn't reprogrammed with a keyboard and monitor attached to the main board, it will take a little longer for the SecureSync to power-up and sync just the next time its powered-up and synced to GPS. And it will power-up the first time with the incorrect date and time. However, within about 10 minutes or so of the SecureSync resyncing to GPS, NTP or other external time reference, the Real Time Clock for the ETX module will be automatically updated with the correct time/date (just as if the BIOS had been updated with a keyboard and monitor). All other settings for the unit besides the time/date at next power-up (such as the network and NTP settings, Reference Priority table, etc) are stored in a CF flash card that doesn't rely on this coin cell battery to remain installed at all times. Removing the battery will not cause any of these other settings to be lost because they are stored in flash memory.

So in summary, the ONLY setting affected by the removal of the coin cell battery is the boot-up time/date, after each power-up. And if it's resynced to an external time reference after the battery is reinstalled, the RTC is automatically corrected for future power-ups to have the approximately correct time/date.

Shelf life for RTC battery

- Shelf life is how long the device can remain unused before placing into service
- Shelf life is 5 years, limited by an on-board replaceable battery (for BIOS). See info below.

Email from Mark McGregor on 9/2/10:

The SecureSync appliance contains one internal battery (A 3vdc -500mAh, Lithium coin cell battery, P/N BR3032). This battery is used as backup power to the ETX microprocessor (for functions such as saving the BIOS settings and for the RTC -yearReal Time Clock functionality, etc). The SecureSync battery is specified to operate over a wide temperature range of -30C to 80C.

The backup battery life is based on the current draw of the ETX module when the SecureSync power is off. Battery life= Battery capacity (A-hr)/battery current (A). The BR3032 capacity is 0.5 A-hr. The ETX draws 12.5 uA when off. This results in 4.57 years of backup time/off time. Battery is not drained when power is on.

For the 93xx (NetClocks), a CR2032 is used, 0.22A-Hr. It uses the same ETX with 12.5uA of current draw when off. This results in 2 years of backup time/off time for the 93xx, so the SecureSync is an improvement over the 93xx. The SecureSync battery is also specified to operate over a wider temperature range of -30C to 80C, whereas the 93xx is a -30C to 60C battery.

The battery is a socketed component, but changing of the battery needs to be performed at the factory, in order to reset the ETX BIOS settings once the battery has been replaced.

Note: Because the backup time/off time is a cumulative time, based on how the customer normally operates the equipment, we cannot put an exact “expiration time” on the battery. We can’t just say the battery is good for 10 years, for example.

Document for replacing the battery in SecureSync (P/N 1200-5000-0055) Refer to manuals in Released drive

- **Also refer to:** EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Battery replacement

Email from Dave Lorah to Masataka with TOYO (10/3/12)

You are correct to think the battery has failed and isn’t backing up the time. It could also be the time was not set properly when the BIOS was first configured or the ETX module was removed and the time not set after ETX was reinstalled. The default date for the ETX module is Jan 1, 2003.

If the battery has failed it could be due to a high current draw. I have seen this happen once where the battery was drained by a damaged capacitor C62. There also could be a problem anywhere in the path between the battery and the ETX module.

Aluminum capacitors in SecureSync

(Note: this info is from 1200 SecureSyncs)

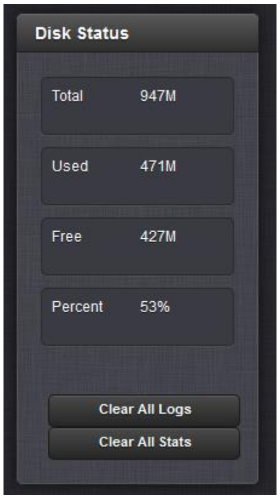
Q are there any aluminum capacitors in SecureSync?

A reply from Dave Lorah (18 Jan 16) The answer is yes, there are capacitors constructed with aluminum in the Securesync. I am curious why the customer would want to know this?

Report of Disk/Memory status

(Note: this info is from 1200 SecureSyncs)

- ***Tools*** -> ***Upgrade/Backup*** page of the browser



Disk Status

Total	947M
Used	471M
Free	427M
Percent	53%

RTC (Real Time Clock) / Linux kernel time

(Note: this info is from 1200 SecureSyncs)

Linux Kernel time (summary of time at each start-up)

- When the SecureSync is powered down, the RTC gets its battery power from the ETX coin cell battery.
- The coin cell battery doesn't allow RTC to store the time. The battery just allows the RTC to keep incrementing the time while input power is removed.
- Refer to Mantis case 0001704 for more info:
- The battery-backed Real Time Clock (RTC) is read upon each boot-up in order to set the Linux kernel time.
- The kernel time then sets the KTS time.
- The kernel time is adjusted by NTP during synchronization to other references.
- Fcron (scheduler program) runs every 10 minutes to write the linux time to the RTC.
- Upon a Reboot or halt being performed, the kernel time is set into the RTC.

Note: If the time is manually set, KTS is set to this time. If the time is set backwards by any amount, Fcron may stop running until time catches up, and therefore it may not set the RTC. If the unit is then power cycled (not Rebooted or Halted), the manual set time is lost upon reboot. In order for the manual set time to be retained for the next power-up, a Reboot or Halt needs to be performed.

Update: this issue was fixed in the version 5.0.0 software update. Refer to Mantis case 2091 (http://cvsmantis.int.orolia.com/mantis/view.php?id=2091)

Note: the TSync-PCIe boards do not have an RTC, so this info does not apply to the timing boards.

Sample log entries associated with RTC (note there may be others, also)

(Note: this info is from 1200 SecureSyncs)

From cron.log

Time saved to RTC (should be logged every 10 minutes:

```
fcron[3565]: Job /etc/init.d/Cronhwclock save started for user root (pid 3566)
```

From kern.log

After system reboot: `rtc_cmos rtc_cmos: setting system clock to 2014-09-09 22:15:57 UTC (1410300957)`

RTC "accuracies" while SecureSync is powered down

(Note: this info is from 1200 SecureSyncs)

- The BEST that the BIOS can set the SecureSync's time at start-up is 0.5 seconds (it sets the time to the closest ½ second)
- The RTC uses a very low quality oscillator to maintain the time. This time will inherently drift off of the correct time, the longer that SecureSync is powered-down (the BIOS time is updated when the SecureSync powers down, but it then drifts from there).
- We do not currently have any specs for the drift of the RTC (when power is not applied) see email below from Tom.

SecureSync RTC drift can't predicted because the RTC is on the ETX single board computer. Spectracom does not know what the RTC/crystal is on the ETX. An inquiry could be made to the ETX board manufacturer, Advantech about RTC time drift during power loss. It also depends on the RTC crystal and environmental conditions, change of temperature, etc. I do not know the SecureSync software, but I think the ETX time, NTP and RTC time, is updated from KTS timing system when the unit achieves synchronization. I do not know how often this time is refreshed.

There are no specifications given for the RTC because it is provided for "coarse maintenance" of the time base when a SecureSync that was in Sync powers off. The idea is that the date will be correct, and the time will be "close" to correct when power is restored, which is better than starting up and waiting up to 12 minutes for GPS to become in sync to get time and date. I do not believe it was ever intended for the customer to depend on the RTC time accuracy/drift over a power outage. It is outside the scope of the product specifications/requirements.

In order to answer this persons RTC question an inquiry to Advantech should be made, or maybe a SecureSync could be tested to get a typical value for room ambient temperature, but I don't know the resolution of the time a user can get from the system or what methods the user has available to get the time from the system. Maybe a software guy or Ron might know this information

FYI – The Rb does not get time or keep time, ever. The Rb disciplines its 10MHz output to a 1PPS reference. The Rb 10 MHz is the input to the KTS hardware clock. KTS hardware clock is what loads time from the RTC at power up and keeps time. This time will be updated when the unit again achieves time sync, at that point the RTC time is over written in KTS and the KTS time is sent to the ETX to update the RTC as well. After a power cycle the RB has to go through warm up of about 7 minutes before the Rb 10 MHz is good enough to use.

Q I the user reference guide "Document Part No.: 1200-5000-0050 Revision: 25 Date: 28-Aug-2017" there are references to a battery backed internal Real Time clock, but no specifications on the accuracy of this clock. On page 151, it states:

"The Accuracy of the Battery Backed Time depends on the accuracy of the hand-set time if the time is set manually in an autonomous system. In a non-autonomous system (i.e, when using external reference(s)) SecureSync's System lock will regularly update the battery-backed time. Another factor impacting the accuracy of the battery-backed time is how long a SecureSync unit is powered off: Any significant amount of time will cause the battery-backed RTC to drift, i.e. the battery-backed time will become increasingly inaccurate. The battery used for the RTC is designed to last for the lifetime of the product."

I am interested in the case where the unit is operating, receiving GPS time, and keeping the real time clock updated. Then, power is lost, recovers a few hours later, and GPS is no longer available. (At that point I expect the Rb standard starts and loads from the Real Time Clock.)

I need to know the accuracy of the real time clock so I can calculate how much drift might occur if the unit lost power and GPS was not available when repowered a few hours later.   I am looking to achieve and project accuracy down to milliseconds levels

A. **Reply from Mark McGregor (7 Feb 8)** SecureSync RTC drift can't be predicted because the RTC is on the ETX single board computer. Spectracom does not know what the RTC/crystal is on the ETX. An inquiry could be made to the ETX board manufacturer, Advantech about RTC time drift during power loss. It also depends on the RTC crystal and environmental conditions, change of temperature, etc. I do not know the SecureSync software, but I think the ETX time, NTP and RTC time, is updated from KTS timing system when the unit achieves synchronization. I do not know how often this time is refreshed.

There are no specifications given for the RTC because it is provided for "coarse maintenance" of the time base when a SecureSync that was in Sync powers off. The idea is that the date will be correct, and the time will be "close" to correct when power is restored, which is better than starting up and waiting up to 12 minutes for GPS to become in sync to get time and date. I do not believe it was ever intended for the customer to depend on the RTC time accuracy/drift over a power outage. It is outside the scope of the product specifications/requirements.

In order to answer this persons RTC question an inquiry to Advantech should be made, or maybe a SecureSync could be tested to get a typical value for room ambient temperature, but I don't know the resolution of the time a user can get from the system or what methods the user has available to get the time from the system. Maybe a software guy or Ron might know this information

FYI – The Rb does not get time or keep time, ever. The Rb disciplines its 10MHz output to a 1PPS reference. The Rb 10 MHz is the input to the KTS hardware clock. KTS hardware clock is what loads time from the RTC at power up and keeps time. This time will be updated when the unit again achieves time sync, at that point the RTC time is over written in KTS and the KTS time is sent to the ETX to update the RTC as well. After a power cycle the RB has to go through warm up of about 7 minutes before the Rb 10 MHz is good enough to use.

Email from Tom Richardson (20 Dec 2012)

AMD CS 5536 companion chip.

32 KHz Input. This input is used for the real-time clock (RTC), GPIOs, MFGPTs, and power management functions. This input may come from either an external oscillator or one side of a 32.768 KHz crystal. If an external oscillator is used, it should be powered by VIO_VSB. This signal takes approximately one second to lock after power-up.

I found a crystal on the board looks something like this. Marked “C3N7C”. Can’t find any specs but it probably isn’t worse than 100 PPM.

100 ppm x 24 hours is 8 seconds.
25 ppm for 24 hours is about 2 seconds.
0.5 seconds in 24 hours is 5 ppm
I took a quick look at Digikey and they have 20 ppm stock, about 1.7 seconds per day.
As in anything your mileage may vary.

Keith’s email to TOYO (20 Dec 12): Yes. The SecureSync does maintain an estimate of the current time/date while the SecureSync is powered down. This is to allow the approximated time/date to be displayed at start-up (or starting in Archive software version 4.8.0, SecureSync can be configured to use this time/date for its initial synchronization, even though it’s not very accurate. This is configured by enabling the “Battery backed Time” checkbox on the Setup -> Reference Priority page of the browser, as shown below).

The time/date during equipment power-down is not maintained by the SecureSync’s 10MHz oscillator (which is not operational without input power applied to the SecureSync). Instead, the start-up time is simply maintained by the Real Time Clock (RTC) inside the system’s ETX embedded CPU module. This RTC is powered by the internal coin cell battery and estimates the start-up time/date to within no better than 0.5 seconds of the actual time (this 0.5 second time error does not account for inherent oscillator drift- only the ability for the time to be set at start-up. Inherent drift of the RTC while power is removed will affect the overall accuracy of this time).

The RTC in the ETX module uses a very low quality oscillator to maintain the BIOS time while the SecureSync is powered-down. As this crystal is inherently not very stable, the RTC time will continue to drift off of the correct time, the longer the SecureSync is powered down. We do not have any specifications on the time drift. However, if its desired to maintain the SecureSyncs time as accurately as possible, the SecureSync should be operated with an uninterruptable power source (UPS), in order to prevent the SecureSync from being powered-down (and therefore, the SecureSync’s time can be maintained by GPS, instead of via the RTC clock).

To prevent the chance of inaccurate time at startup from being used by external devices for their synchronization, the Synchronize to Battery Backed Time on Startup” checkbox in the **Setup** -> **Reference Priority** page should not be enabled (it is not checked by factory default), if the “User” reference is enabled in the Reference Priority table. With this checkbox not enabled, the SecureSync will not automatically use the RTC clock as a time reference for its synchronization (manual intervention via the web browser is required after each boot-up, before the RTC time can be used for SecureSync’s synchronization (thereby allowing a user to be able to update the SecureSync’s startup time, before it can declare sync using the BIOS backed time).

500ms error in versions 4.8.5 and below (fixed in v4.8.6)

Email from Paul Myers (2/28/12)

Note on reboot after an update the time is exactly 500 msec off. The RTC estimates to within a half second.

Note: 127.127.1.0 in the table above is the local system clock (the kernel time, as set by the RTC at power-up) The RTC error that Paul was referring to in his email above is the time difference between 127.127.1.0 and an external reference (in this case NTP server 96.9.150.154) the time difference is 500 ms (in the offset field).

RTC being set when manually setting the System time backwards into the past

- When System Time is advanced into the future, RTC is updated every 10 minutes.
- When System Time is set back into the past, RTC isn't updated the first time for about 3 to 4 hours. Then it's updated every 10 minutes again.

The system is not intended to be a simulator. It especially does not like being set backwards to an earlier time. This causes Cron to completely stop running, until time has caught up to the correct time.

If the time is set backwards and then power cycled without a several minute delay, it will not power-up with the time that it was manually set to. It takes several minutes for NTP to change the kernel time, once it's been manually set. Then Cron, which is used to periodically set the RTC stops running until time catches up to the kernel time. If the time is set backwards, a delay of several minutes (like 20 to 30 minutes) should occur between setting the time and power cycling the unit.

Email Keith sent to Masataka (18 Feb 15) Thanks for your email. Our Applications Engineering team has reviewed the information you provided us with regards to the SecureSync's RTC being saved. I am happy to pass along to you their findings.

To begin, when manually setting the time of the SecureSync, there is a one particular scenario that will allow the RTC to be automatically saved within 10 minutes of setting the time. There is another scenario which prevents the System Time from being able to be automatically saved to the RTC for a few hours, unless a reboot or halt of the SecureSync is commanded.

If the System Time/date is manually set by a user to a time/date ahead of the current System Time, the SecureSync continues to be able to automatically set the time into the RTC every 10 minutes (on a 10 minute schedule). However, if a user manually sets the date/time to an earlier date/time than the System Time was set to, the System Time can't be automatically set into the RTC for about 3 to 4 hours, unless a *reboot* or *halt* command is performrned.

If the date/time is set by a user to a date/time in the past and its desired to save this "new" date/time into the RTC without waiting the 3 to 4 hours for it to be automatically saved, the SecureSync should be commanded to be either rebooted or halted (not just power cycled) after setting the date/time backwards. Note the RTC is not updated upon a power cycle of the SecureSync. However, the RTC is updated with the System Time upon either a reboot or a halt command being issued. The SecureSync can be either rebooted or halted via the front panel menus, the web browser, the CLI command line interface or via SNMP.

Please be aware that the RTC taking a few hours to be set when a user sets the date/time into the past is not a software bug and Spectracom has no intentions at this time of changing how this operates. If it's desired to manually set the time of the SecureSync backwards to a previous date/time for some reason, the SecureSync should be either rebooted or halted (via its user interfaces) in order to alleviate the need to wait the 3 to 4 hours that is needed for the RTC to be updated with this earlier System Time. Note that the RTC is updated with each reboot or halt command, whether the date/time was set forward or backwards from the starting System Time. The reboot/halt command alleviates any need to wait for the RTC to be updated, as the RTC update occurs before the SecureSync is brought down with either command being performed.

Site acceptance testing / performance testing

Refer to: \\Rocfnp01\idrivedata\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Acceptance tests

SecureSync Options

Options/License files available for SecureSync (besides Option Cards)

- Refer to the 2400 SecureSync datasheet: https://www.orolia.com/product/securesync-time-and-frequency-reference-system/

Generating license files

A) 2400 SecureSync License Bundle creator

- ➢ See Dan Pashina/Will Comly

B) 1200 SecureSync License Bundle Creator

- ➢ refer to: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\License Files Updates

Per Ron Dries (25 Jan 18) The updated License creator tool is being kept in Arena.

The item number for the tool is SS_LIC_PROG_CS. It can be found here: https://app.bom.com/items/detail-spec?item_id=1242672189&version_id=10893367128&orb_msg_single_search_p=1

It can be run by downloading it to your PC and extracting it. The executable is called **bundleCreator.exe.**

Enter the model and serial number into the GUI and then check the licenses you would like to include in the bundle for the specified model and serial number.

After pressing submit the file is created in the directory C:\ManufacturingProgrammingFiles\ on your PC.

Associated response from Dave L: I have placed the new update file in **I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Software Update- license fil**es.
I have also updated the license file creation instruction to reflect this new procedure.

Installing licenses

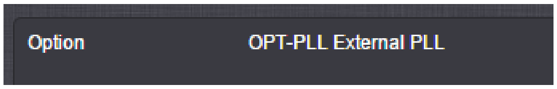
- ➢ Specific process to install license can vary based on installed software version.
  - For example, version 5.2.1 has a dedicated button to upgrade License File (installing license is not the same process as updating the software)

Process for updating a SecureSync customer unit in the field (email from Tom Richardson)

1) Sales/Customer service gets order for update license from customer. Customer supplies required serial number(s).
2) Order Entry enters order and adds serial number(s) as a line note. Notifies Customer Service.
3) Customer Service creates license update file following the license file creation process.
4) License file and installation instructions sent to Customer through Salesforce.
5) Unit notes in Salesforce are updated to reflect serial number change in status.
6) Customer service notifies Operations that item has shipped and Shipping update transaction in Visual.

Browser report of installed license files

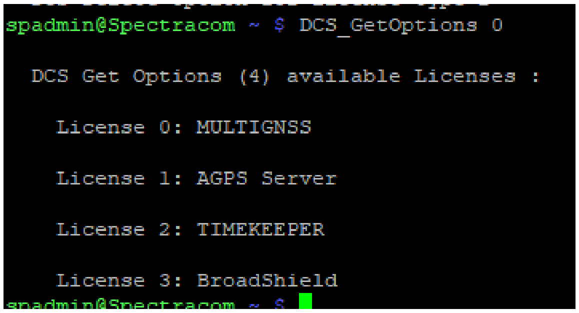
- The license status is visible on the **TOOLS** -> **Upgrade/Backup** page in the web user interface. It should be listed under the “System Configuration” section at the bottom like below:



Option OPT-PLL External PLL

Deleting installed Option Licenses:

- **DCS_GetOptions 0** lists the installed licenses (example below)



```
spadmin@Spectracom ~ $ DCS_GetOptions 0

  DCS Get Options (4) available Licenses :

    License 0: MULTIGNSS

    License 1: AGPS Server

    License 2: TIMEKEEPER

    License 3: BroadShield
spadmin@Spectracom ~ $
```

  - **DCS_CheckOption**

- **DCS_DeleteOption 0 #** deletes the options (where # is the Option Number desired to be removed)

  Caution: Always verify the desired Options Number first, before deleting an Option, as the assigned Option number may be different in each unit (based on what other options were installed prior for installed)

  Example: With TimeKeeper being Option 2, the command to remove it is **DCS_DeleteOption 0 2**

(SS-Opt-BSH and SS-Opt-JADE) IDM software (BroadShield Talen-X /embedded BroadShield interference and Spoofing detection software) for 2400 SecureSyncs

Current status of Opt-BSH and Opt-Jade in 2400 SecureSyncs

Per Dave Sohn (26 Apr 2021) **“**SS-OPT-BSH IDM Suite is functional and tested within our current release of 2400. SS-OPT-JADE is not yet available on 2400”

> **Update on JADE from Keith (7 Oct 2021)** As of at least v1.2.2, Opt-JADE still not available for 2400s. Per Sadie, Opt-Jade is very low on the Engineering Priority list for 2400s.

Links/shortcuts

- **Refer to the BroadShield datasheet on our website:** https://www.orolia.com/product/broadshield/
- **Refer to SecureSync IDM suite on our site**: https://www.orolia.com/solution/interference-detection-and-mitigation/

Link to press release on a web page

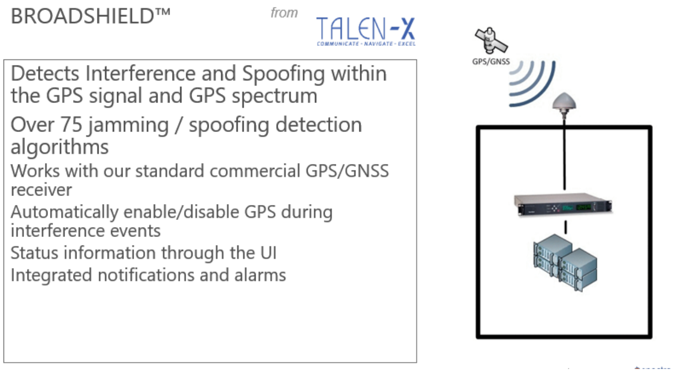
Link to SecureSync with Broadshield information page

- **Link to Broadshield datasheet on our site:** Refer to the BroadShield datasheet on our website: https://www.orolia.com/product/broadshield/

Link to Salesforce (pricing/ordering):
https://orolia.lightning.force.com/lightning/r/Product2/01t0h000006Bi28AAC/view

Link to info about Broadshield in online 2400 SecureSync manual:
http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/TIME/Broadshield.htm

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

Detects Interference and Spoofing within the GPS signal and GPS spectrum

Over 75 jamming / spoofing detection algorithms

Works with our standard commercial GPS/GNSS receiver

Automatically enable/disable GPS during interference events

Status information through the UI

Integrated notifications and alarms

Details: Spectracom and Talen-X have aligned hardware and software development efforts to jointly develop, market and sell the most advanced PNT solutions, combining the strengths of leading **Spectracom Resilient PNT** products with Talen-X’s **BroadShield** interference and spoofing detection suite.

The Spectracom SecureSync will take full advantage of BroadShield algorithms, which are known for meeting the requirements for Critical Infrastructure published by the US Department of Homeland Security (DHS). Beyond complying with DHS best practices, Talen-X has further enhanced the BroadShield algorithms to go beyond simply detecting various threats, also providing Spectracom SecureSync operators with detailed threat characteristics, real-time situational awareness and recorded data for post event forensic analysis.

System requirements

- Strong GPS signal strengths
- **uBlox M8T GNSS receiver** (doesn't work with Trimble Res-T, or RES-SMT-GG receiver)
- For 2400 SecureSyncs: Software **versions 1.1.0A** (Feb 2020) or higher.

SecureSync Software changes associated w/BroadShield (in ascending order)

pseudod: daemon to pass ublox messages to the Broadshield option

ECO-FAI-002849 (1 Sept 2021): Release Broadshield 1.2.1 into production for 2400

- This releases version 1.2.1 of Broadshield into production. This version of Broadshield is needed for 1.2.1 2400 software.

V1.6.0 2400 SecureSync update = BroadShield version 5.8.0

Two available Modes of operation for BroadShield

- 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.**

broadshield.ini file/Configuration of BroadShield

- Refer to online SecureSync manual: http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/TIME/Broadshield.htm

broadshield.ini file

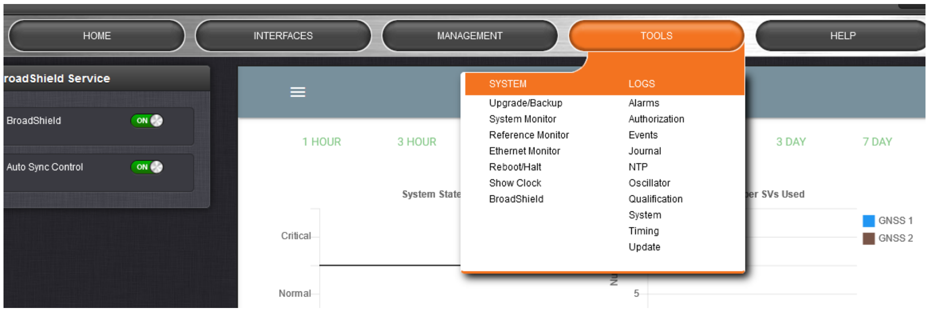
path to the broadshied.ini file: home/spectracom/config/Talen-X/BroadShield.ini

"Talen-X/BroadShield.ini: Permission denied"

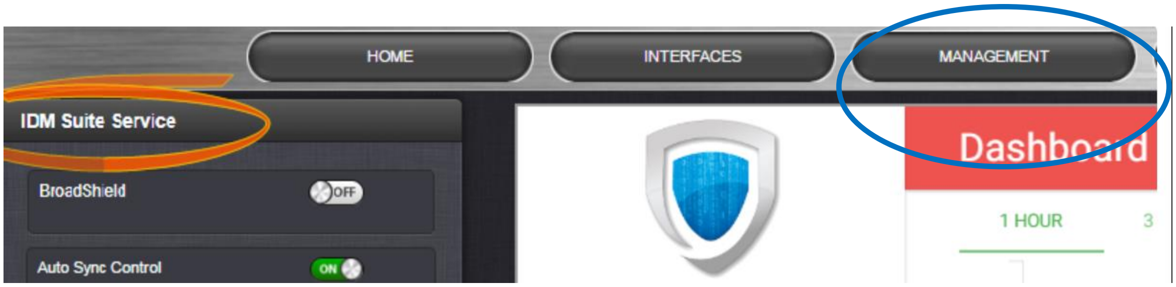
- refer to Salesforce case 172828

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

Note: Unlike the 1200 SecureSyncs having BroadShield under a separate main "**Monitoring**" button at the top of the browser, in the 2400 SecureSyncs, BroadShield is available via the "**Management**" menu (in at least v1.6.0, its now in the Tools menu, as shown directly below).



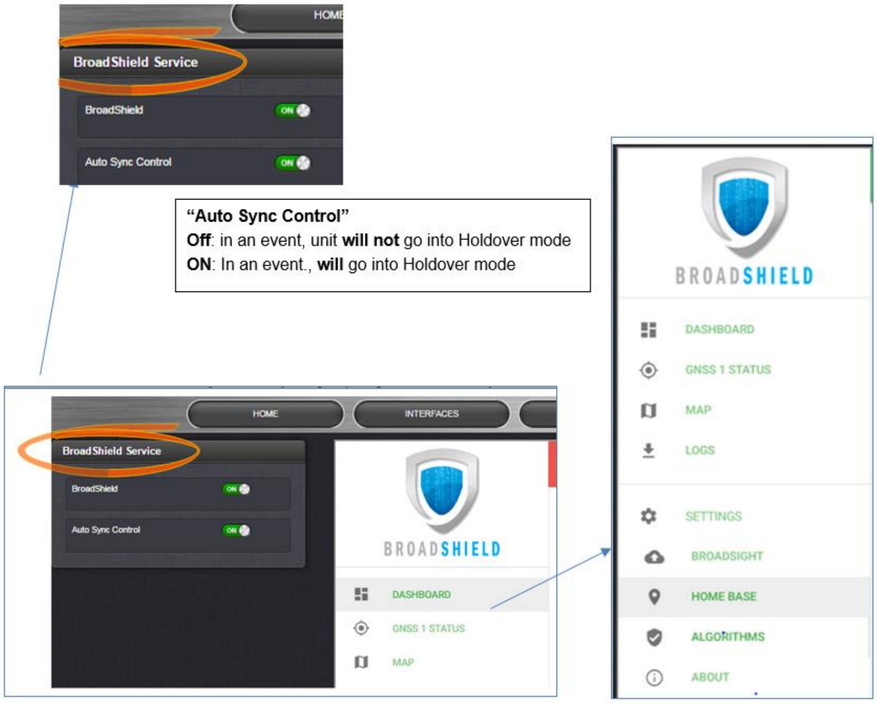
Screenshot below from the 2400 SecureSync user guide



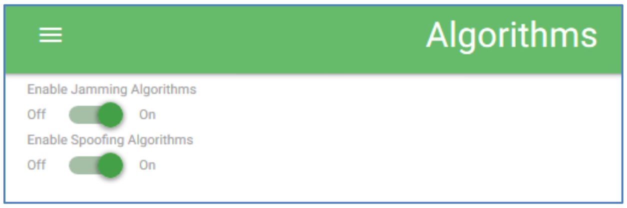
A) To configure the mode of operation

1. Navigate to ***Management*** > ***BroadShield***. (or ***Tools*** -> ***BroadShield*** in at least 1.6.0)
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.


"Auto Sync Control"
Off: in an event, unit **will not** go into Holdover mode
ON: In an event., **will** go into Holdover mode

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



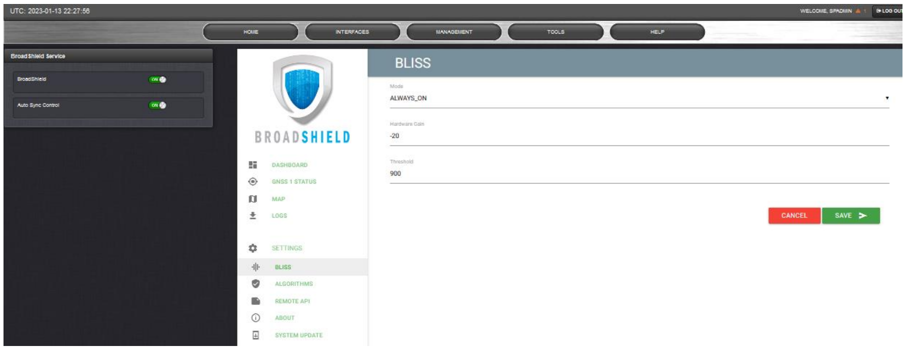
Enable Jamming Algorithms

Off On

Enable Spoofing Algorithms

Off On

B) Bliss



UTC: 2023-01-13 22:27:56

BroadShield Service

BroadShield ON

Auto Sync Control ON

BLISS

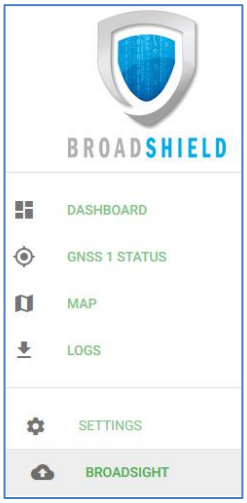
Mode
ALWAYS_ON

Hardware Gain
-20

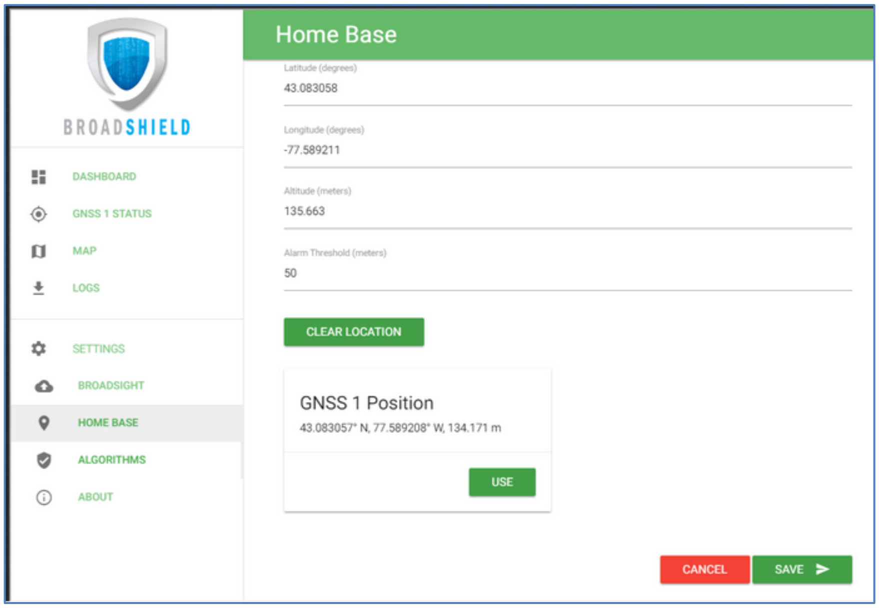
Threshold
900

C) BroadSight

- ➢ not supported for SecureSync (apparently has been removed from earlier versions of BroadShield)



D) “Home Base” position (optional- (apparently has been removed from earlier versions of BroadShield)



Home Base

Latitude (degrees)
43.083058

Longitude (degrees)
-77.589211

Altitude (meters)
135.663

Alarm Threshold (meters)
50

GNSS 1 Position
43.083057° N, 77.589208° W, 134.171 m

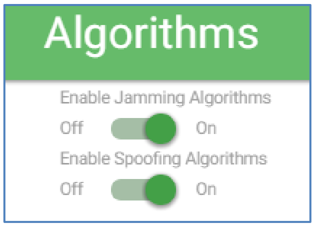
- By setting the HOME BASE position you allow BroadShield to use this location as a reference position for spoofing detection:
  - Should BroadShield detect that the geographic position reported by SecureSync's GPS receiver seems to move beyond the set Alarm Threshold (even though SecureSync does not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

The standard use case is to make your GNSS 1 Position your HOME BASE:

1. Should the position fields be populated (other than the Alarm Threshold), click **CLEAR LOCATION** (this will prevent BroadShield from issuing an alarm once you SAVED the new position.)
2. Click **USE** in the GNSS 1 Position box to apply the settings.
3. The default Alarm Threshold is 50 m, i.e. any detected position shift beyond a 50-m circle around the HOME BASE position will cause an alarm. You can change this setting to adjust the sensitivity.
4. Click SAVE to accept the entered values.

A less common use case may be that you want to pre-set the unit's position for later use e.g., if the SecureSync unit will be deployed in a different location: Set a position manually by entering lat/long (format: xx.xxxxxx degrees) and alt. Note, however, that this may cause a spoofing alarm, since BroadShield detects a difference between the HOME BASE position and the GNSS position.

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



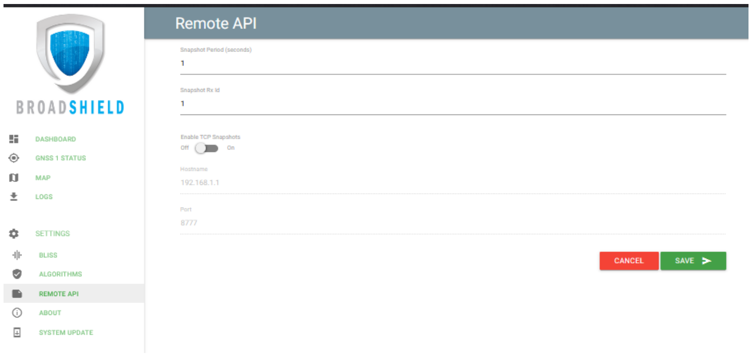
Algorithms

Enable Jamming Algorithms: On

Enable Spoofing Algorithms: On

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.

F) Remote API



Remote API

Snapshot Period (seconds)
1

Snapshot Rx Id
1

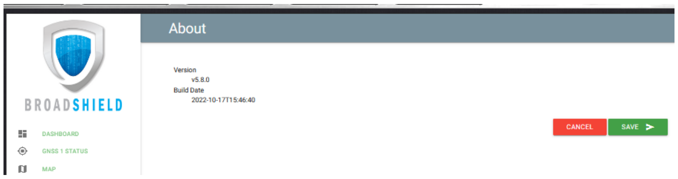
Enable TCP Snapshots
Off On

Hostname
192.168.1.1

Port
8777

G) About

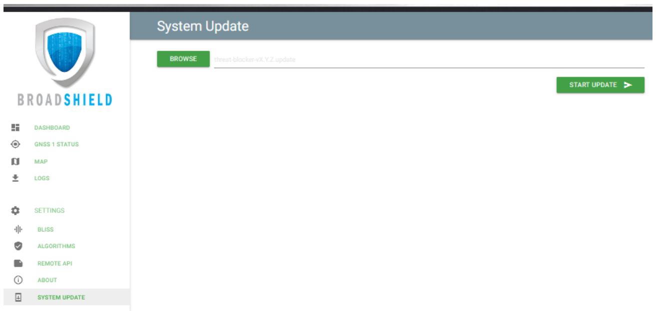
- ➢ Displays Version and Build Date of the BroadShield software.



About

Version
v5.8.0
Build Date
2022-10-17T15:46:40

H) System Update



System Update

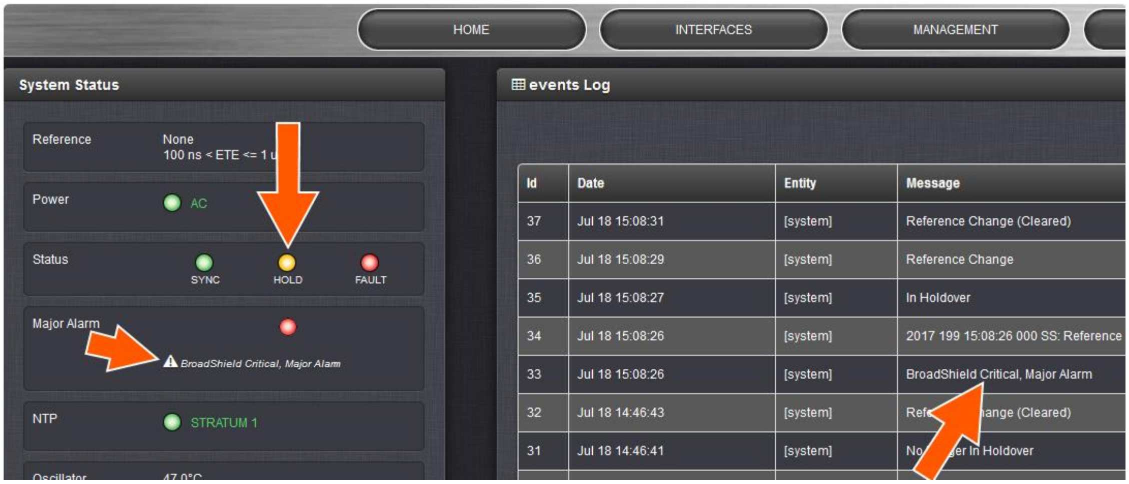
threat-blocker-vX.Y.Z.update

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).



System Status

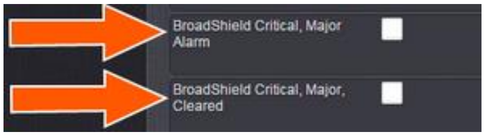
Reference	None 100 ns < ETE <= 1 u
Power	● AC
Status	● SYNC ● HOLD ● FAULT
Major Alarm	● ⚠ BroadShield Critical, Major Alarm
NTP	● STRATUM 1
Oscillator	47.0°C

events Log

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]	Refe ange (Cleared)
31	Jul 18 14:46:41	[system]	No ger In Holdover

Available Broadshield notifications

Management -> **Notifications** page of the browser



BroadShield Critical, Major Alarm □

BroadShield Critical, Major, Cleared □

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.)

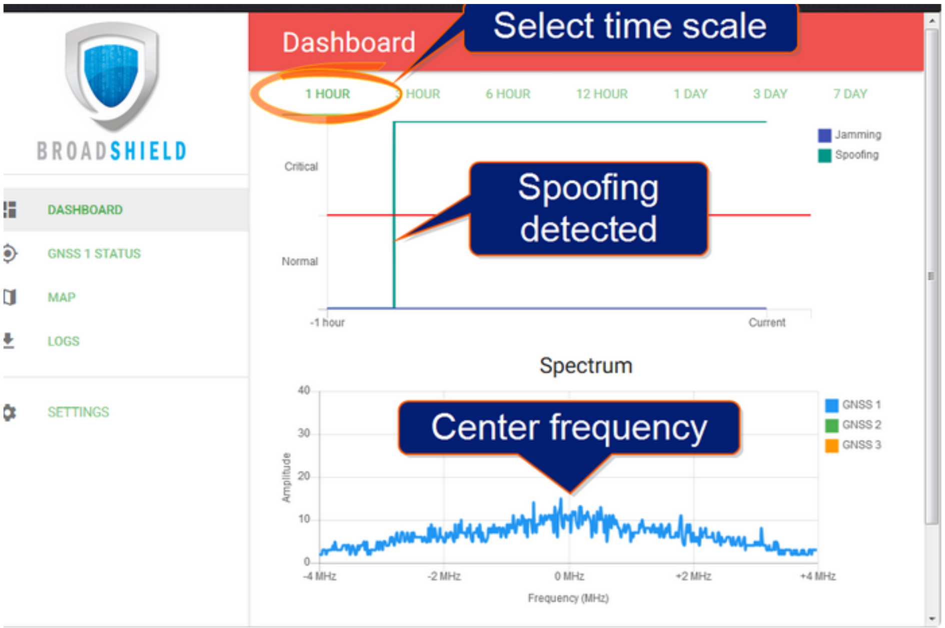
The embedded Broadshield Web UI will open, displaying the Dashboard and providing access to the following panels:

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;

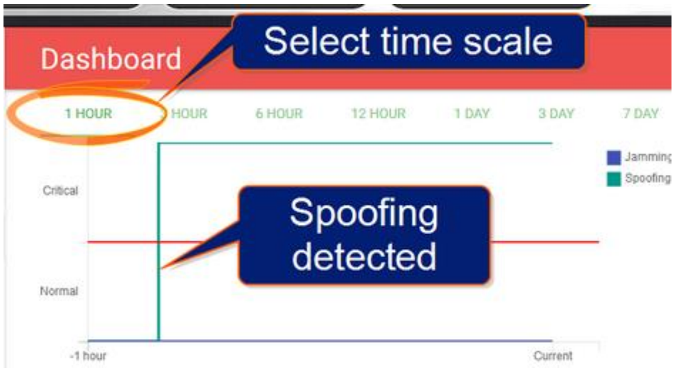
green = no alarms at this time



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

Note:

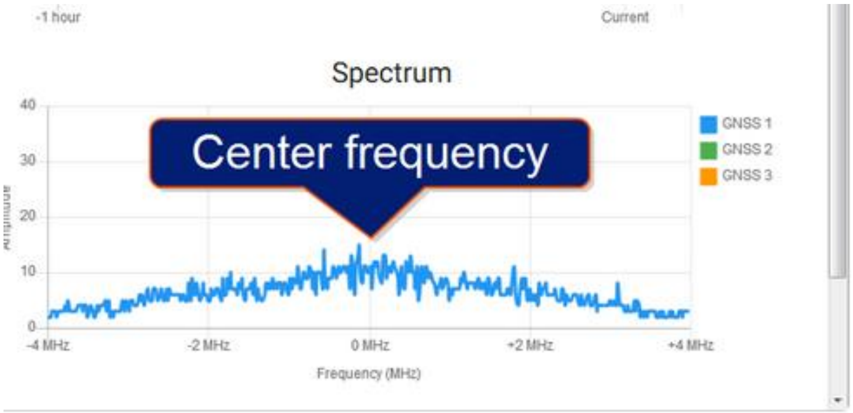
○ You can **change the time scale** by clicking on any of the labels at the top (between "**1 hour**" and "**7 days**"



- Displays the past signal level over time, divided into a Normal and a Critical signal level (separated by a red line).
  - A blue line in the Critical zone indicates a potential jamming incident, while
  - A green line indicates that SecureSync may be subject to a spoofing attack.

Note: A SecureSync reboot will reset all history data (it can still be retrieved via LOGS.)

B) Bottom graph of the dashboard (labeled "Spectrum") (shows current signal over the GPS band)

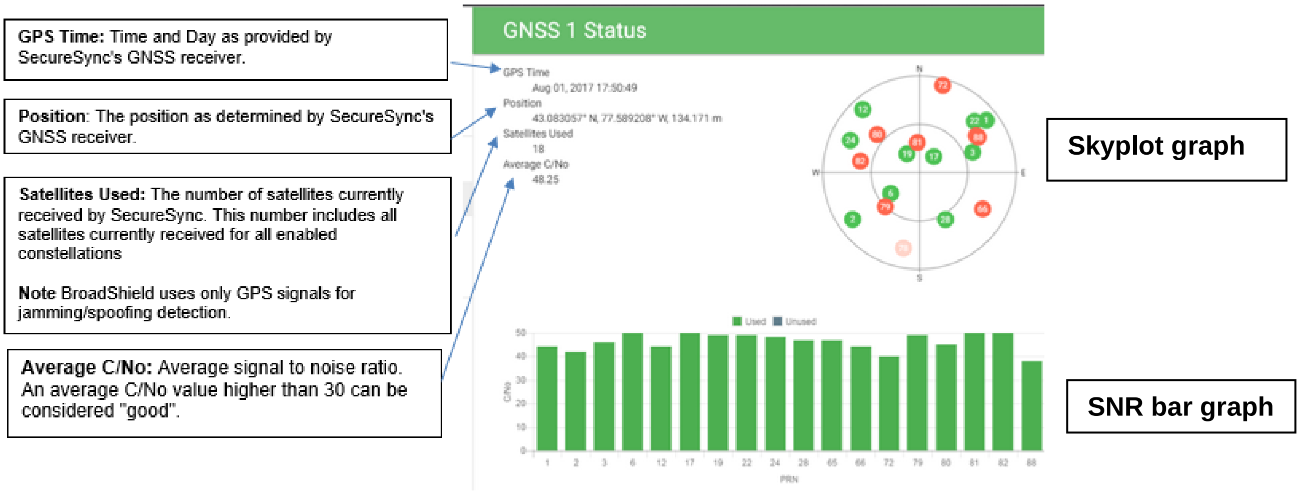


- Visualizes the current signal over the GPS frequency band.
- Unusual amplitude spikes indicate a potential threat.
    - ~~If your system is equipped with more than one GNSS receiver, a green and an orange graph will indicate the signal level for additional receivers.~~

GNSS 1 Status (Skyplot graph)

- ➢ This graph visualizes the signal-to-noise ratio for up to 20 received satellites in real time. The satellites are numbered by their NMEA ID's (as in the skyplot mentioned above).

GNSS 1 Status



GPS Time: Time and Day as provided by SecureSync's GNSS receiver.

Position: The position as determined by SecureSync's GNSS receiver.

Satellites Used: The number of satellites currently received by SecureSync. This number includes all satellites currently received for all enabled constellations

Note BroadShield uses only GPS signals for jamming/spoofing detection.

Average C/No: Average signal to noise ratio. An average C/No value higher than 30 can be considered "good".

GNSS 1 Status

GPS Time
Aug 01, 2017 17:50:49
Position
43.083057° N, 77.589208° W, 134.171 m
Satellites Used
18
Average C/No
48.25

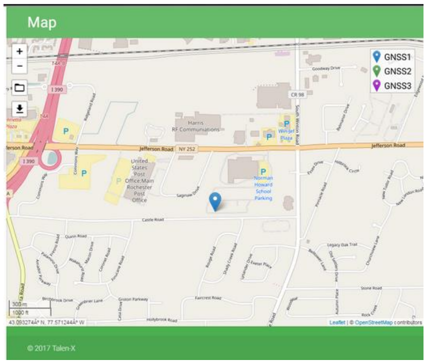
The center of the skyplot represents the antenna position. The skyplot shows all GPS satellites currently being tracked and – if enabled (under INTERFACES: REFERENCES > GNSS Reference: GNSS 0 > Edit button > Selected Constellations) – will also display all GLONASS satellites (numbered 65 and higher).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

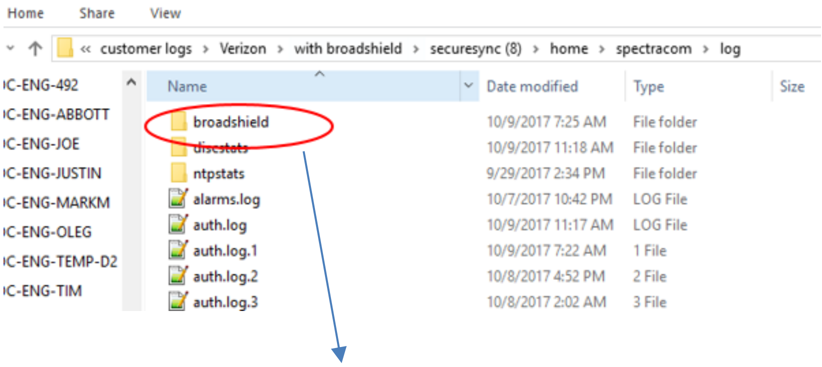


Note: the map data is not part of the BroadShield software, but is downloaded from the Internet. Hence, this feature is only available if your SecureSync unit is connected to the Internet.

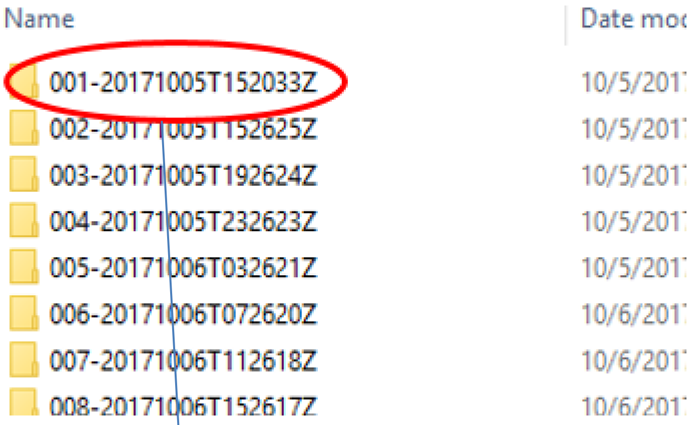
- ➢ The map displays your current position, as reported by the GPS receiver.
- ○ Should the displayed position differ from the actual antenna position, the GPS signal is likely spoofed.

BroadShield's dedicated Logs (SystemStatus.csv files) (note these are separate from the SecureSync's other available "System" logs)

Home -> Spetracom -> Log -> broadshield directory

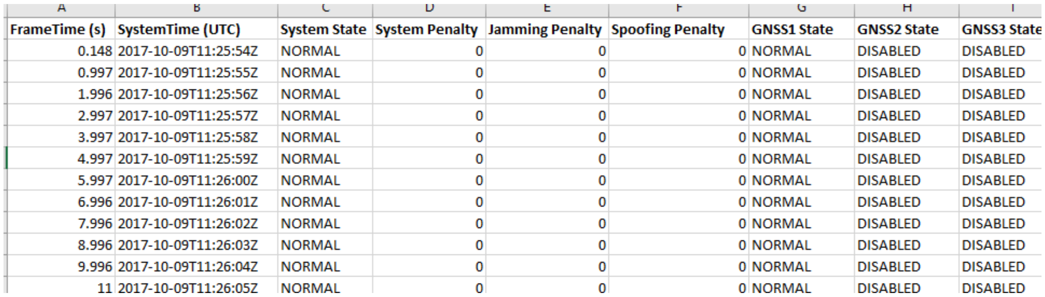


Name	Date modified	Type	Size
broadshield	10/9/2017 7:25 AM	File folder	
discstats	10/9/2017 11:18 AM	File folder	
ntpstats	9/29/2017 2:34 PM	File folder	
alarms.log	10/7/2017 10:42 PM	LOG File	
auth.log	10/9/2017 11:17 AM	LOG File	
auth.log.1	10/9/2017 7:22 AM	1 File	
auth.log.2	10/8/2017 4:52 PM	2 File	
auth.log.3	10/8/2017 2:02 AM	3 File	



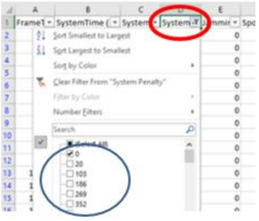
Name	Date mod
001-20171005T152033Z	10/5/201
002-20171005T152625Z	10/5/201
003-20171005T192624Z	10/5/201
004-20171005T232623Z	10/5/201
005-20171006T032621Z	10/5/201
006-20171006T072620Z	10/6/201
007-20171006T112618Z	10/6/201
008-20171006T152617Z	10/6/201

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 scrollong 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

amming Penalty: count of jamming penalties

Spoofing Penalty count of Spoofing penalties

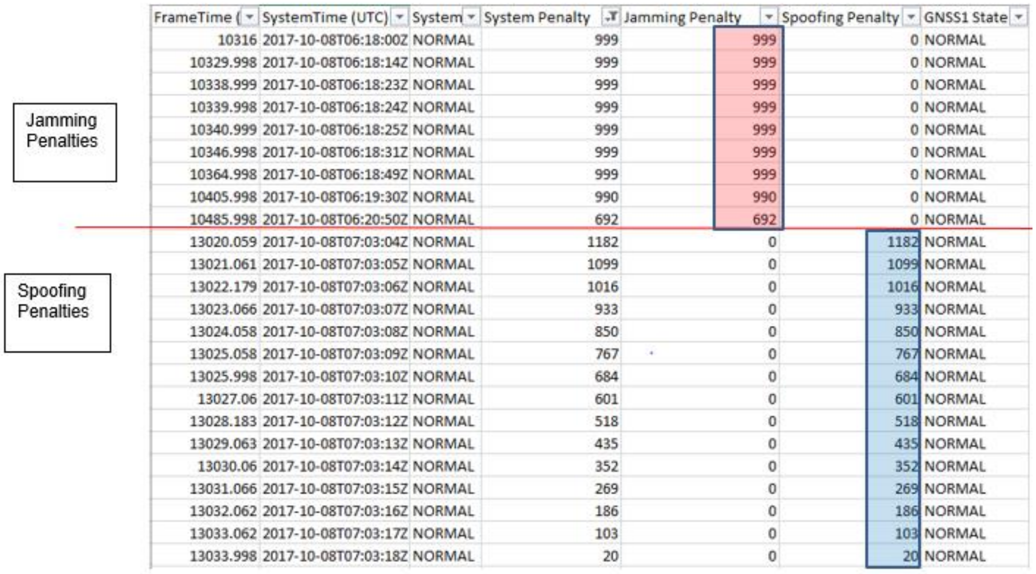
GNSS1 State: (“Home Base” position)

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



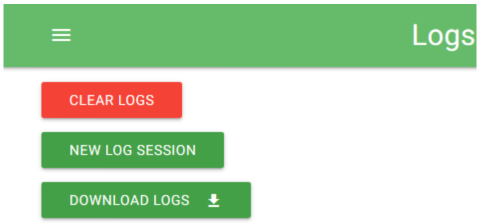
Jamming Penalties
Spoofing Penalties

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

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

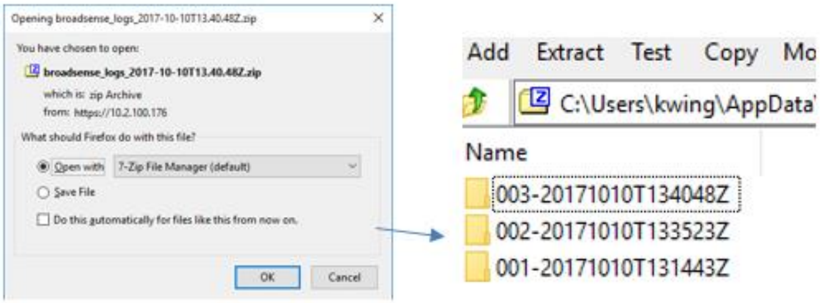
➢ Per Paul M (9 Oct 17) If CF card usage is greater than 70%, Broadshield logs are deleted.

Clear/download logs (SystemStatus.csv files)



- ○ **To clear all current logs (SystemStatus.csv fles) stored on SecureSync**, click CLEAR LOGS.
- ○ **To start a new log session**, click NEW LOG SESSION.

- **To download current logs**, click DOWNLOAD LOGS.



Opening broadsense_logs_2017-10-10T13.40.48Z.zip

You have chosen to open:

broadsense_logs_2017-10-10T13.40.48Z.zip

which is: zip Archive

from: https://10.2.100.176

What should Firefox do with this file?

● Open with 7-Zip File Manager (default)

○ Save File

□ Do this automatically for files like this from now on.

OK Cancel

C:\Users\kwing\AppData'

Name

003-20171010T134048Z

002-20171010T133523Z

001-20171010T131443Z

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 ohcnntpz2 ohcnntpz2: [system] BroadShield Critical, Major, Cleared
Oct  5 15:20:35 ohcnntpz2 ohcnntpz2: [system] BroadShield Warning, Minor, Cleared
Oct  5 15:20:35 ohcnntpz2 ohcnntpz2: [system] BroadShield Critical, Major, Cleared
```

A) Alarms.log

- Example entry Oct 8 02:41:02 ohcnntpz2 ohcnntpz2: [system] BroadShield Critical, Major Alarm

B) Events.log

- Example entries

```
Oct  5 15:20:33 ohcnntpz2 ohcnntpz2: [system] BroadShield Critical, Major, Cleared
Oct  5 15:20:35 ohcnntpz2 ohcnntpz2: [system] BroadShield Warning, Minor, Cleared
Oct  5 15:20:35 ohcnntpz2 ohcnntpz2: [system] BroadShield Critical, Major, Cleared
Oct  5 15:26:25 ohcnntpz2 ohcnntpz2: [system] BroadShield Critical, Major, Cleared
Oct  8 02:41:02 ohcnntpz2 ohcnntpz2: [system] BroadShield Critical, Major Alarm
Oct  8 02:41:02 ohcnntpz2 ohcnntpz2: [system] In Holdover
Oct  8 02:41:02 ohcnntpz2 ohcnntpz2: [system] 2017 281 02:41:02 000 SS: Reference changed to Time Ref: none PPS Ref:
none
Oct  8 02:41:03 ohcnntpz2 ohcnntpz2: [system] Reference Change
Oct  8 02:41:04 ohcnntpz2 ohcnntpz2: [system] Reference Change (Cleared)
Oct  8 02:42:05 ohcnntpz2 ohcnntpz2: [system] BroadShield Critical, Major, Cleared
Oct  8 02:42:06 ohcnntpz2 ohcnntpz2: [system] Reference Change
Oct  8 02:42:06 ohcnntpz2 ohcnntpz2: [system] 2017 281 02:42:06 000 SS: Reference changed to Time Ref: gps0 PPS Ref:
gps0
Oct  8 02:42:07 ohcnntpz2 ohcnntpz2: [system] No Longer In Holdover
Oct  8 02:42:08 ohcnntpz2 ohcnntpz2: [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 untiljamming 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 ohcnntpz2 ohcnntpz2: [system] 2017 278 07:00:46 000 XO: Ref Changed: old=gps0 new=none
Oct  5 07:00:46 ohcnntpz2 ohcnntpz2: [system] 2017 278 07:00:46 000 XO: Phase Reference Invalid.
Oct  5 07:00:48 ohcnntpz2 ohcnntpz2: [system] 2017 278 07:00:47 000 XOS: Rb track off -- free run
Oct  5 07:00:54 ohcnntpz2 ohcnntpz2: [system] 2017 278 07:00:54 000 XO: Ref Changed: old=none new=gps0
Oct  5 07:00:54 ohcnntpz2 ohcnntpz2: [system] 2017 278 07:00:54 000 XO: Phase Reference Valid.
Oct  5 07:02:28 ohcnntpz2 ohcnntpz2: [system] 2017 278 07:02:28 000 XOS: Rb synchronized
Oct  5 07:03:00 ohcnntpz2 ohcnntpz2: [system] 2017 278 07:03:00 000 XOS: Frequency error recalculated: -00.000023 (-2.337x10^-12)
Oct  5 07:31:31 ohcnntpz2 ohcnntpz2: [system] 2017 278 07:31:31 000 XO: Ref Changed: old=gps0 new=none
Oct  5 07:31:31 ohcnntpz2 ohcnntpz2: [system] 2017 278 07:31:31 000 XO: Phase Reference Invalid.
Oct  5 07:31:32 ohcnntpz2 ohcnntpz2: [system] 2017 278 07:31:32 000 XOS: Rb track off -- free run
Oct  5 07:31:39 ohcnntpz2 ohcnntpz2: [system] 2017 278 07:31:39 000 XO: Ref Changed: old=none new=gps0
Oct  5 07:31:39 ohcnntpz2 ohcnntpz2: [system] 2017 278 07:31:39 000 XO: Phase Reference Valid.
Oct  5 07:33:14 ohcnntpz2 ohcnntpz2: [system] 2017 278 07:33:13 000 XOS: Rb synchronized



Oct  5 10:21:08 ohcnntpz2 ohcnntpz2: [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^-
```

Special software patches / Specials for SecureSync

Special software patches for particular customers

SPECIALS

- Refer to: U:\Engineering\Projects

Option Cards

- **Option Card Install Guide for 2400 SecureSyncs (2400-5000-0052) in Arena**: https://app.bom.com/items/detail-spec?item_id=1271819535&version_id=11422521608&orb_msg_single_search_p=1

- **Schematics for the Option Cards:** (Refer to the 1204-xxxx) \\rocfnp01\idrivedata\Engineering\Archive\New Released\PCB Documentation

- For **additonal information** on SecureSync Option cards, refer also to:

  - **Table/list of Option Cards**: ..\SecureSync Option Card table.pdf
  - **Details for each card**: ..\SecureSync Option Card information.pdf
  - **Folder**: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Option Cards
  - **Sharepoint site**: https://oroliagroup-portal1.sharepoint.com/Spectracom/customer_service/Shared%20Documents/Forms/AllItems.aspx

API calls for Option Cards/Slots

- Refer to Tim Tetreault's "cheat sheet" at: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\Timing boards\TSync family\Tsync driver calls cheat sheet
- These are examples - additional calls may have since been added

Option Card commands
DCS_GetCardInfo
DCS_GetFeatByIdx
DCS_GetInstance
DCS_GetOptions
DCS_GetSlot

**Slot Numbers

**Installing or relocating Option Cards

(Note: this info is from 1200 SecureSyncs)

Installing Option Cards

Metal bracket screws and stand-offs used on the Option Cards

Email from Scott Holmes (4/2/12)

The material we specify is 0.81mm (20 ga) thick aluminum alloy 5052-H32. Before screening we plate it with RoHS compliant clear plating. The plating is electrically conductive.

Screws and standoffs

Email from Dave Lorah (5/10/12)

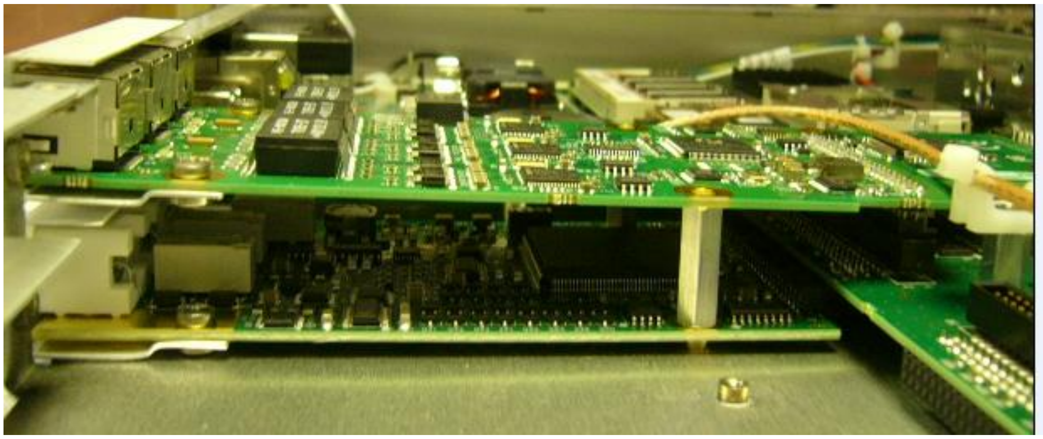
The mounting bracket screws are a M4, Flathead Phillips, 10MM black machine screw, stainless steel. I think these are all fine thread.

The option card standoffs are a Hex spacer, M3x18mm, zinc plated brass. These are pretty soft metal. I have broken some myself.

Standoff lengths

Q. (Email from Sylvain)…we have noticed an important bending of the 1204-06 card when it is mounted with another board below. It seems the pillar is too high. The pillar can be OK when there is no board below but not for a "sandwich mode" …

Here are the pictures of the 1204-06 mounting. The 892,3,4 show mounting with card in bottom slot and 895,6 show mounting with no card underneath (no additional spacer in place of PCB). I used a thin nylon spacer (0.5mm) + the supplied 19mm pillar to give the correct height. I think that the supplied pillars are 1mm too long.



Reply from Scott Holmes (10/26/12) There are two standoffs we use for the option cards. One is longer and allows a card to be installed in an upper slot with no card below. The other is shorter and used when there are cards in both upper and lower slots. It looks like the longer standoff was used. Did they move the cards around and mix up the standoffs or was the mistake made on our production floor?

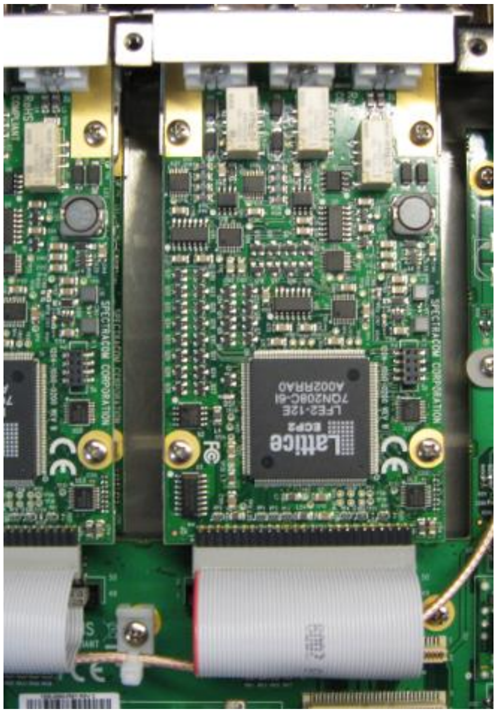
- Option Cards on bottom plug straight into rear connector.
- Option Cards on top are connected to the main board via a 50 pin ribbon cable **(CA20R-R200-0R21**)

➢ Refer to the SecureSync Option Card Installation Guide (1200-5000-0052) I:\New Released\Manuals\1200-xxxx-xxxx.

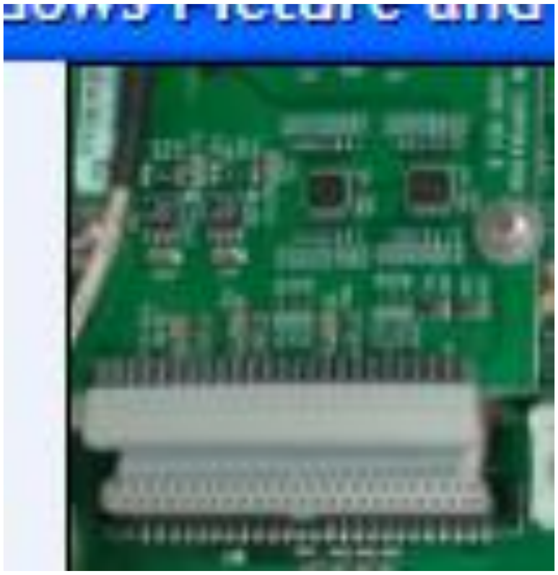
Ribbon cable for top row

- When we send new Option Cards to be installed in the field, a kit that includes a 50 pin ribbon cable (ribbon cable is our P/N CA20R-R200-0R21) and the Install guide mentioned above, is provided with each card. This ribbon cable provided is only used when installing an Option card in the top row (Bays 2, 4 and 6). The ribbon cable is not used with the bottom row of Option Cards (Bays 1, 3 and 5).

Ribbon cable should be "looped outward"

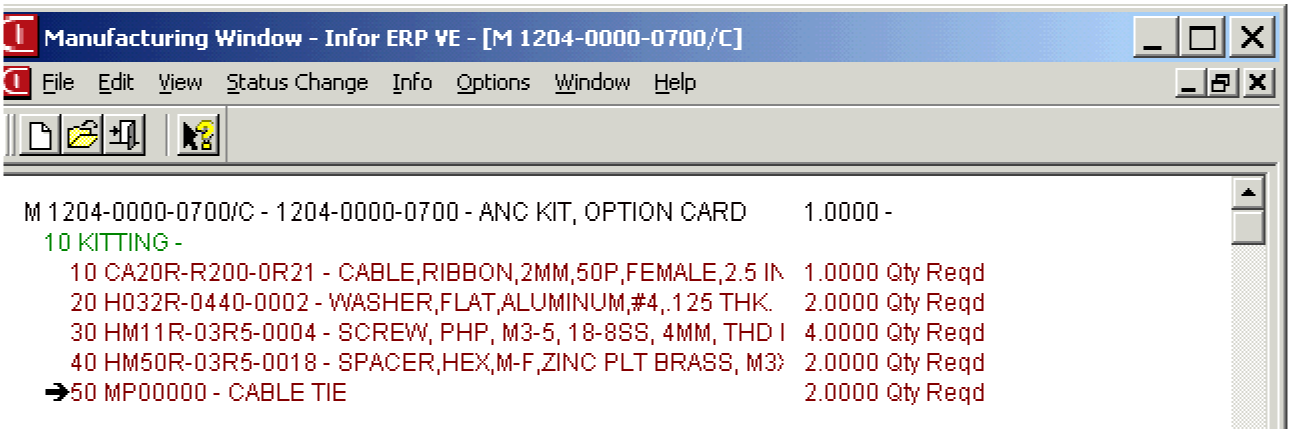


Don't install the cable "looped inward"



Ancillary kit included with Option Card purchases

- The P/N for the ancillary kit is 1204-0000-0700. This ancillary kit includes:



```
M 1204-0000-0700/C - 1204-0000-0700 - ANC KIT, OPTION CARD        1.0000 -
  10 KITTING -
    10 CA20R-R200-0R21 - CABLE,RIBBON,2MM,50P,FEMALE,2.5 IN   1.0000 Qty Reqd
    20 H032R-0440-0002 - WASHER,FLAT,ALUMINUM,#4,.125 THK.    2.0000 Qty Reqd
    30 HM11R-03R5-0004 - SCREW, PHP, M3-5, 18-8SS, 4MM, THD I 4.0000 Qty Reqd
    40 HM50R-03R5-0018 - SPACER,HEX,M-F,ZINC PLT BRASS, M3X   2.0000 Qty Reqd
  ➔50 MP00000 - CABLE TIE                                      2.0000 Qty Reqd
```

- If a customer desires to move a card that is installed when the SecureSync was purchased, from the bottom row to the top row, they will need the kit above (which includes the ribbon cable to connect the Option Card to the main board).

System Memory (SecureSync and Option Cards) / Sanitization

(Note: some of this info is from 1200 SecureSyncs)

**GPS receiver memory and CF Card/System memory in SecureSync *(need to update for 2400 SecureSyncs)*

Refer to: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Memory\SecureSync memory.pdf

Note: Manufacturer's names and P/Ns subject to change. Do not release to customers, though memory sizes can be released as appropriate.

Note: This document has an FAQ that refers to the **"/dev/hda1"** file. This is the name of the mounted installed CF card in its entirety. So the FAQ is referring to all files on the CF card itself.

Q. What is the capacity of the Main Memory? (Ex.: 256 MB)
A. The 2400 SecureSync has 8GB eMMC memory onboard.

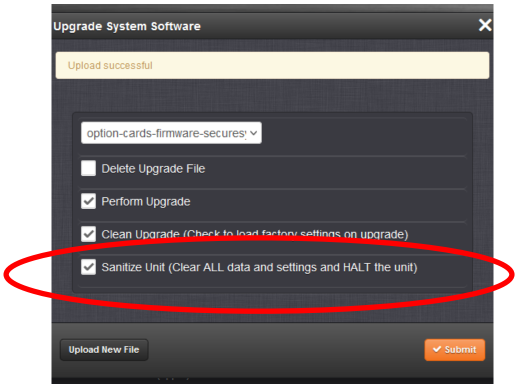
**Certificate of Volatility (COV) / Letter of Volatility (LOV)

- **Refer to**: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync-2400 (Diamond)\Memory
- **Refer to**: **JIRA Ticket CAR-2122** (request Keith submitted to Engineering on 12 December 2022, for them to release a COV for 2400s)

Procedure to Sanitize/Sanitization of the Model 2400 SecureSync (versions 1.6.0 and above)

- Refer to the 2400 SecureSync online user guide at: (not yet in user guide as of 21 Dec 2022)

1) Upload the same as already installed, or newer version of software via FTP/SCP (such as load 1.6.0., if 1.6.0 is already installed.
2) (Starting in Versions 1.6.0 and above, as shown below) Perform a "**Sanitize Unit (Clear ALL data and Settings and HALT the unit)"**



Upgrade System Software

Upload successful

option-cards-firmware-secures

□ Delete Upgrade File

☑ Perform Upgrade

☑ Clean Upgrade (Check to load factory settings on upgrade)

☑ Sanitize Unit (Clear ALL data and settings and HALT the unit)

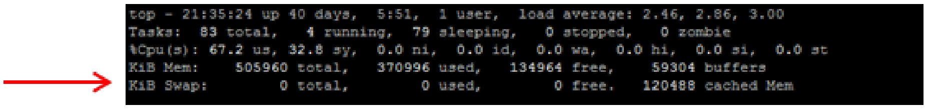
Added in version 1.6.0 (~Dec 2022)

- 1st select "Perform Upgrade". Then select the "**Sanitize Unit**" checkbox
- Selecting the "**Sanitize Unit"** checkbox automatically selects "**Clean Upgrade**" checkbox

Clean upgrade (Such as first performing a Forced upgrade from 4.8.8 to 4.8.9, for example. Then automatically resetting the NTP server back to factory default settings and deleting all log files): "**sysupgrade clean**" followed by the upgrade file name (Example: **sysupgrade clean update489.tar.gz**).

Report of swap memory usage

- May be monitored by solar winds (solarwinds) for example.
- Swap is reported at the beginning of the non-spectracom specific "**top**" cli command.
- Swap is reported as "0 total", since there is no swap memory in the system:



```
top - 21:35:24 up 40 days,  5:51,  1 user,  load average: 2.46, 2.86, 3.00
Tasks:  83 total,   4 running,  79 sleeping,   0 stopped,   0 zombie
%Cpu(s): 67.2 us, 32.8 sy,  0.0 ni,  0.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem:    505960 total,   370996 used,   134964 free,    59304 buffers
KiB Swap:        0 total,        0 used,        0 free.   120488 cached Mem
```

Q. (from George Siaw with Hughes) SNMP monitor of the spectracom GPS keeps telling us this. (Swap Memory has exceeded threshold: (60%) currently (100%))
A (from Dave Sohn) This should be ignored. There isn't any swap memory to exceed, or be below, a threshold.

Sanitization

- Refer to: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Memory\SecureSync memory.pdf

Email from Denis Reilly:

Customers can apply upgrades, provided by us, that upgrade the functional logic of the FPGA. Customers can't put arbitrary data in the Option Card FPGA EEPROM, and no user data ever goes into the FPGA EEPROM: the only data the customer puts there is data that we provide. (either the initial image that ships with the unit, or any other data we provide as part of the upgrade process.)

The only exception is the PTP card, as I have described.

Applying a forced upgrade to the unit will ensure that the option card FPGA images get reverted to a known state, which may be what the customer is going for.

Model and Serial Number

(Note: this info is from 1200 SecureSyncs)

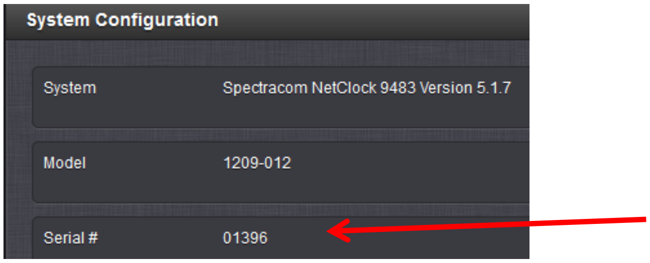
- CLI command to get the Model and Serial number: **model** <enter>
- Per Denis Reilly, the unit's Serial Number is stored in the EEPROM on the main logic board.

Obtaining Model and Serial Number remotely

A) Via web browser

1. Newer black web browser:

Tools -> **Upgrade/Backup** page of the browser (under "System Configuration")



System Configuration

System	Spectracom NetClock 9483 Version 5.1.7
Model	1209-012
Serial #	01396

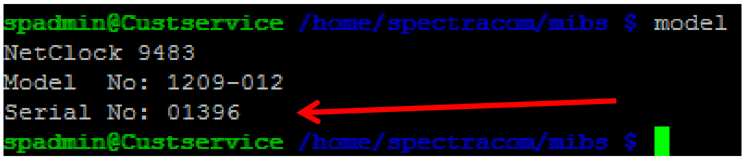
2. Classic interface browser

Note: Post version 4.4.0 updates should have the Model/Serial Number at the top of the **Tools** -> **Versions** page.

Note that the reported "Archive Version" is the "common reference" for all the various software versions installed in the SecureSync. The "Archive version" defines all 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.

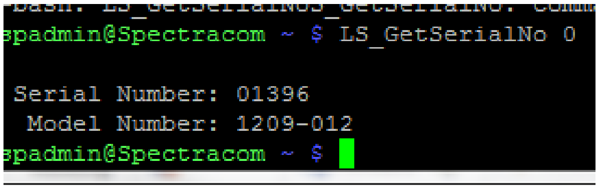
A) Via CLI (telnet, ssh or serial connection)

- Use the CLI command of **model** <enter> (lower-case)



```
spadmin@Custservice /home/spectracom/mibs $ model
NetClock 9483
Model  No: 1209-012
Serial No: 01396
spadmin@Custservice /home/spectracom/mibs $
```

Note: Can also use the command: **LS_GetSerialNo 0**



```
-bash: LS_GetSerialNo3_GetSerialNo: comm
spadmin@Spectracom ~ $ LS_GetSerialNo 0

 Serial Number: 01396
  Model Number: 1209-012
spadmin@Spectracom ~ $
```

B) Model/Serial Number Via SNMP **(info below is from 1200s)**

- Serial Number via SNMP was added in version 5.2.1 software update.
    - The Model and Serial Number are not available via SNMP in version 5.2.1 and below, refer to Mantis Case 1855).

Q. Is the Serial Number and Hardware Version available via SNMP? If so, what OIDs should we use? We've looked through the provided MIBS, but didn't find anything.
A. At this time, the Serial Number and Hardware Version information are not available via SNMP. The unit's Serial Number can be found on the Serial Number tag affixed to the appliance. We do not provide any "Hardware version" information. However, the "Software versions" for the various SecureSync modules can be obtained from the Tools/Versions page of its web browser.

C) Model/Serial Number via the logs

- Version 5.2.1 update (Apr 2015) added Model and Serial Number to the **System Log** at each start-up.

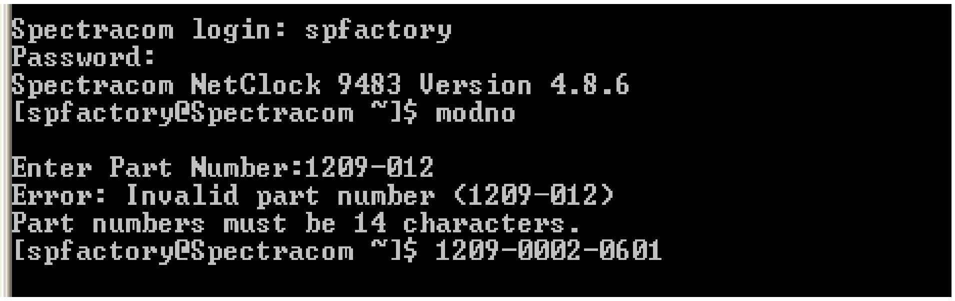
Programming Model Number/Power configuration and Serial Number

(Note: this info is from 1200 SecureSyncs)

- The programmed Model Number (Part Number) affects the software power configuration. A missing or incorrect Part Number will result in the unit thinking the input power configuration is different than the actual input power input configuring, resulting in an alarm being asserted.
- The unit's Serial Number (Tools ->Versions page) can be entered, if it was inadvertently not programmed or if it was programmed incorrectly when the SecureSync was shipped.

Programming a missing or incorrect Model/Part Number (which affects the AC/DC input power configuration)

1) telnet or ssh into the unit (can't change values via the web browser)
2) login as "**spfactory**".
3) type: **modno** <enter> Response will prompt for the desired unit's Model Number.
4) Enter the correct 14 digit Part Number and press <enter> (Note: this is the 12 digit P/N and counts the two dashes): **Example**: **1200-0237-0601** <enter> (the example consists of 12 digits and two dashes)
5) Reboot/power cycle the unit for changes to take effect.

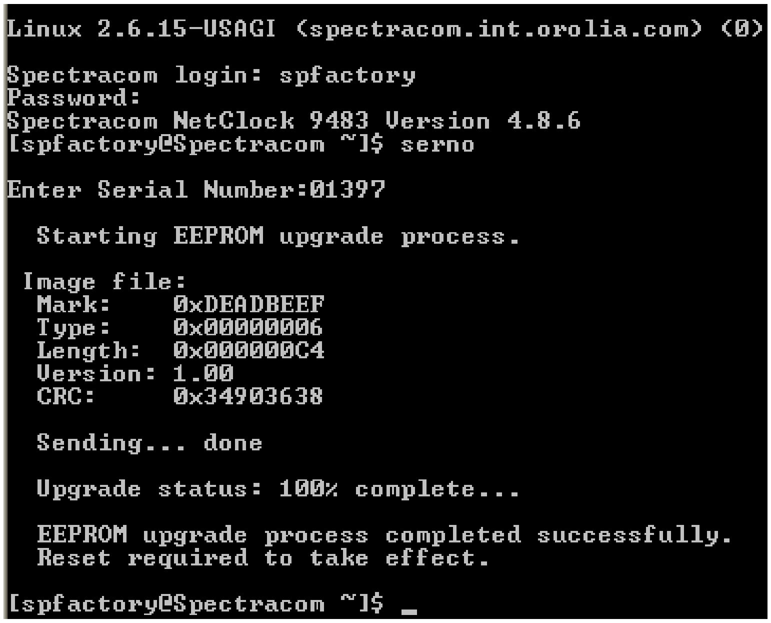


```
Spectracom login: spfactory
Password:
Spectracom NetClock 9483 Version 4.8.6
[spfactory@Spectracom ~]$ modno

Enter Part Number:1209-012
Error: Invalid part number (1209-012)
Part numbers must be 14 characters.
[spfactory@Spectracom ~]$ 1209-0002-0601
```

Programming a missing or incorrect unit's Serial Number

1) telnet or ssh into the unit.
2) login as “**spfactory**”.
3) type: **serno** <enter> Response will prompt for the desired unit’s Serial Number.
4) Enter correct Serial Number and press <enter>
5) Reboot/power cycle the unit for changes to take effect.

Note: After rebooting/power cycling to have the Model Number or Serial Number change take effect, the web browser may display “**the web browser encountered an unexpected error…”.** Refer to Mantis case 1982.



```
Linux 2.6.15-USAGI (spectracom.int.orolia.com) (0)

Spectracom login: spfactory
Password:
Spectracom NetClock 9483 Version 4.8.6
[spfactory@Spectracom ~]$ serno

Enter Serial Number:01397

  Starting EEPROM upgrade process.

 Image file:
  Mark:     0xDEADBEEF
  Type:     0x00000006
  Length:   0x000000C4
  Version:  1.00
  CRC:      0x34903638

  Sending... done

  Upgrade status: 100% complete...

  EEPROM upgrade process completed successfully.
  Reset required to take effect.

[spfactory@Spectracom ~]$ _
```

**SecureSync calibration service

(Note: this info is from 1200 SecureSyncs)

- There is no calibration required/available for the SecureSync or its Option Cards
- The SecureSync is self-calibrated to an external input reference (such as GPS)

Email Keith sent to Hongbo (16 Jan 2013) Is this regarding a SecureSync that has already been purchased and shipped to your customer? Or is this regarding an order that the customer will be submitting to us sometime in the future?

I don’t believe we have provided any customer yet with a Calibration Certificate for SecureSync. We can supply Certificates of Conformance for this unit, but note that there really isn’t anything in SecureSync to actually “calibrate”.

SecureSync is a self-calibrating device (when locked to GPS, IRIG, etc). The oscillator calibrates itself and there are no tunable items in the unit (no potentiometers or other adjustable components). Calibration service would really be limited to the same items included in the certificate of Conformance, which covers the tests normally performed during factory production. The calibration service would essentially entail verifying voltage measurements and also the normal operation of the unit, since there are really no adjustable items in the unit.

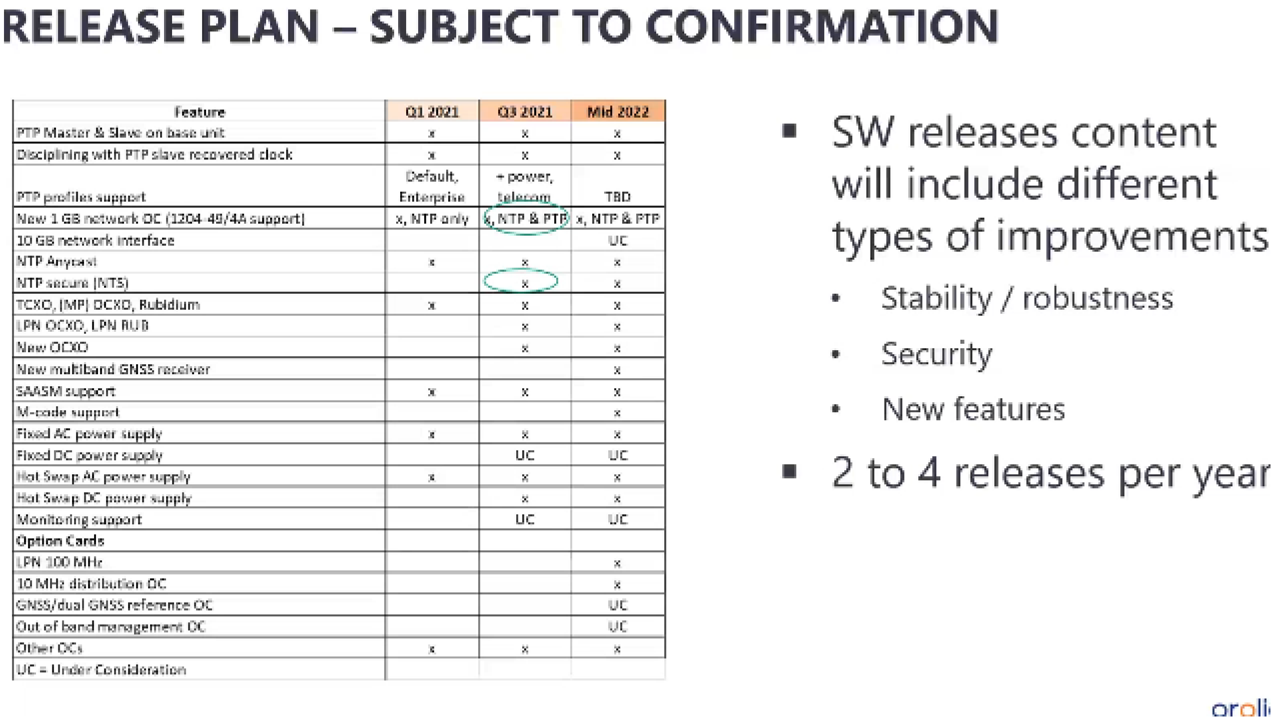
If your customer requires this calibration sticker, we will need to come up with a price for this service. Also, the SecureSync would need to be returned to us (if this is for a unit that has already been purchased from us and shipped to the customer, it would need to be returned for the first calibration and then every year thereafter, if they wished to renew the calibration certificate). All shipping fees and the established calibration service fee (the minimum cost for the calibration service fee will be at least $200.00 USD as this is the minimum evaluation fee for all non-warranty returns).

If your customer still wants to have the unit re-tested as it was during the manufacturing process for a certificate, we will establish an actual cost for this service. But as there are no adjustable items in this unit, I would like to first verify your customer still wants this test performed, with this understanding.

Please let me know if this is for a new order that has not yet shipped to the customer, and if they still want this calibration service performed, with the understanding there really isn’t anything to “adjust” in this particular unit, as it’s designed to be self-calibrating. Then, we can go from there!

Software version/Software update/Software downgrade

(Note: much of this info is from 1200 SecureSyncs)



RELEASE PLAN – SUBJECT TO CONFIRMATION

Feature	Q1 2021	Q3 2021	Mid 2022
PTP Master & Slave on base unit	x	x	x
Disciplining with PTP slave recovered clock	x	x	x
PTP profiles support	Default, Enterprise	+ power, telecom	TBD
New 1 GB network OC (1204-49/4A support)	x, NTP only	x, NTP & PTP	x, NTP & PTP
10 GB network interface			UC
NTP Anycast	x	x	x
NTP secure (NTS)		x	x
TCXO, (MP) OCXO, Rubidium	x	x	x
LPN OCXO, LPN RUB		x	x
New OCXO		x	x
New multiband GNSS receiver			x
SAASM support	x	x	x
M-code support			x
Fixed AC power supply	x	x	x
Fixed DC power supply		UC	UC
Hot Swap AC power supply	x	x	x
Hot Swap DC power supply		x	x
Monitoring support		UC	UC
Option Cards			
LPN 100 MHz			x
10 MHz distribution OC			x
GNSS/dual GNSS reference OC			UC
Out of band management OC			UC
Other OCs	x	x	x
UC = Under Consideration			

- SW releases content will include different types of improvements
  - Stability / robustness
  - Security
  - New features
- 2 to 4 releases per year

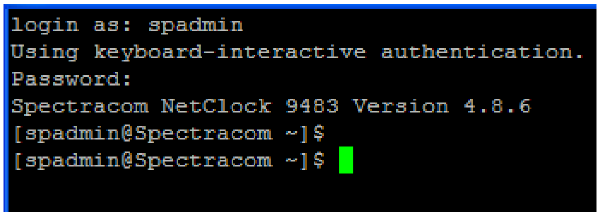
Link to info on all available software versions for 2400 SecureSyncs
Refer to: ..\..\PSB, PSP software updates\2400 SecureSync\2400 SecureSync Software updates

Obtaining currently installed version information

- ➢ Update software version 5.2.0 enhanced the version info being reported in the Tools -> Upgrade/Backup page of the browser.
- ➢ Now reports versions of Apache, NTP, OpenSSL, NetSNMP, OpenSSH, PHP (for newer black/charcoal browser), KTS version, etc.

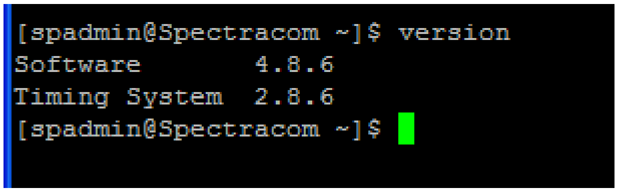
Obtaining the currently installed Archive / Timing System software versions:

- ➢ Reported in the ***Tools*** -> ***Versions*** page of the web browser.
- ➢ Automatically reported when logging in with telnet/ssh (displayed after entering the correct password). Refer to: Command line interface (CLI) further down.



```
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 4.8.6
[spadmin@Spectracom ~]$
[spadmin@Spectracom ~]$
```

- Login via telnet/SSH and type “version” (Version command returns Archive and Timing System version) Refer to: Command line interface (CLI) further down.



```
[spadmin@Spectracom ~]$ version
Software        4.8.6
Timing System   2.8.6
[spadmin@Spectracom ~]$ 
```

Obtaining the versions of the installed software packages (such as Apache, GPS, SNMP, NTP, etc):

There are “**version**” commands available for the installed packages, via the CLI interface. Refer to: Command line interface (CLI) further down.

**Performing software updates

- ➢ All versions of software support updating the software via the web browser.

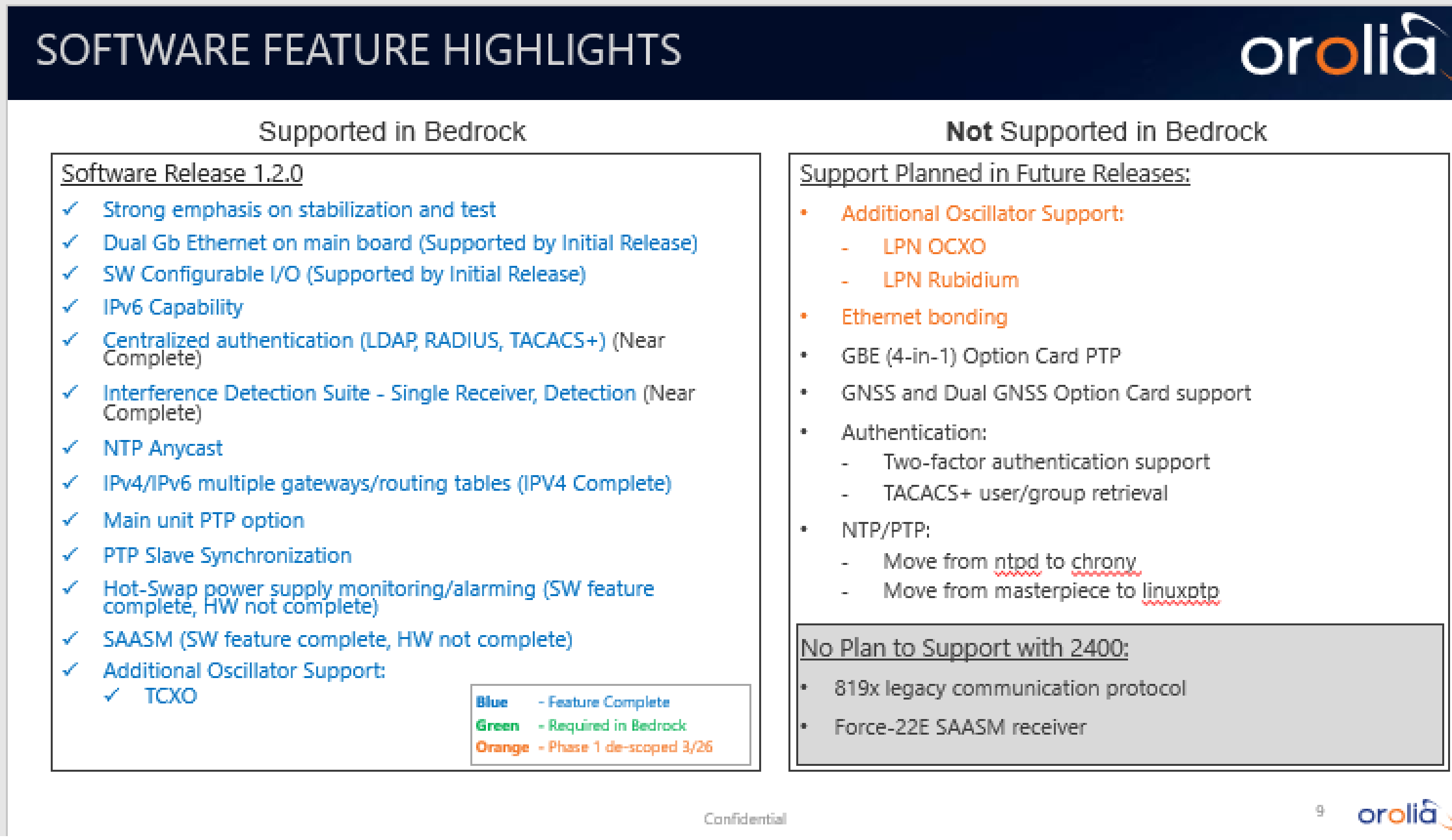
(at least v1.2.1 and below) Incorrectly applying 1200 SecureSync software update bundle to Model 2400 SecureSync

- ➢ Created JIRA ticket DMND-1599 to help prevent this from happening again.
- ➢ Refer to Salesforce Case 270459 (applied 5.9.1 to 2400 SecureSync)

Excerpt report from Customer (2 Aug 2021) SecureSync 2400 and tried to perform firmware upgrade to 5.9.1 (update591.tar.gz). However, the upgrade status said - "upgrade failed" and asked me to reboot the unit. However, it didn't reboot itself and I no longer can log into it via the web browser. I tried ssh into it using spadmin and a password that was set before (I am pretty sure the password is correct!) but failed. I tried to ssh into it using spadmin and a default password but still no luck.

Specific software version notes (info not necessarily in release notes)

Version 1.2.0 upgrade



SOFTWARE FEATURE HIGHLIGHTS

Supported in Bedrock

Software Release 1.2.0

- ✓ Strong emphasis on stabilization and test
- ✓ Dual Gb Ethernet on main board (Supported by Initial Release)
- ✓ SW Configurable I/O (Supported by Initial Release)
- ✓ IPv6 Capability
- ✓ Centralized authentication (LDAP, RADIUS, TACACS+) (Near Complete)
- ✓ Interference Detection Suite - Single Receiver, Detection (Near Complete)
- ✓ NTP Anycast
- ✓ IPv4/IPv6 multiple gateways/routing tables (IPV4 Complete)
- ✓ Main unit PTP option
- ✓ PTP Slave Synchronization
- ✓ Hot-Swap power supply monitoring/alarming (SW feature complete, HW not complete)
- ✓ SAASM (SW feature complete, HW not complete)
- ✓ Additional Oscillator Support:
  - ✓ TCXO

Blue - Feature Complete
Green - Required in Bedrock
Orange - Phase 1 de-scoped 3/26

Not Supported in Bedrock

Support Planned in Future Releases:

- Additional Oscillator Support:
  - LPN OCXO
  - LPN Rubidium
- Ethernet bonding
- GBE (4-in-1) Option Card PTP
- GNSS and Dual GNSS Option Card support
- Authentication:
  - Two-factor authentication support
  - TACACS+ user/group retrieval
- NTP/PTP:
  - Move from ntpd to chrony
  - Move from masterpiece to linuxptp

No Plan to Support with 2400:

- 819x legacy communication protocol
- Force-22E SAASM receiver

Confidential 9

Update log/entries

- ➢ Update log is not displayed in browser, but captured in the standard log bundle.
- ➢ Update log can be viewed via CLI (logs directory).

- ➢ Updates that are performed are reported in the Tools -> Versions page of the web browser.
- ➢ Logs record when the update was performed, version it was updated to, etc.
- ➢ If “Restore Factory Configuration” update was also selected (or if the clean command was used when performing the update a via a CLI command) when the update was performed, all logs (and configs) are cleared. There will be no Update log entries after the update is performed.

software update, especially when there have been no software updates applied in a very long time.

A) SIGTERM entry in the logs (such as Error_log, SNMPD log, etc

Update log entry

```
Jun  9 13:02:10 s43u1clk s43u1clk: [sw-upgrade] Upgrade Initiated, Reboot Required: /home/spectracom/update54A.tar.gz
(SWUAL)
```

Associated Error_log entries during a software update or halt

```
[Thu Jun 09 13:02:06 2016] [warn] [client 10.144.97.236] -authlogic- authtype is currently Pamacea (for /index.php), referer:
https://s43u1clk.vida.local/Upgrades
Reboot required to complete upgrades.
[Thu Jun 09 13:02:27 2016] [notice] caught SIGTERM, shutting down
[Thu Jun 09 13:20:02 2016] [notice] Graceful restart requested, doing restart
```

Associated SNMPD log entries during a software update or halt

```
Received TERM or STOP signal...  shutting down...
```

Associated SNMPD log entries during a software update

```
Jun  9 13:02:30 s43u1clk exiting on signal 15
```

B) power cycling the unit (inadvertently or intentionally) before update is complete

Email from Dave Sohn on 11/2/11, regarding a customer power cycling SecureSync apparently before the update process had completed:

Remember that upgrade actually involves two reboots of the system. The first reboot is done into memory to rebuild the CF card with the new upgraded version. The unit then reboots again to start running from that newly built CF. During the first reboot, the front panel LCD will be blank, and the console is not available. If they power cycled before that process is complete, I would be concerned that something might not have been performed properly in the process. They may want to “force” another update at the same version to ensure that the upgrade completed fully and successfully.

Software update when Skylight installed: The upgrade process is the same, but they can only upgrade to other Skylight versions.

Ability to perform software updates via CLI interface (for scripting updates)

- ➢ Version 4.8.8 (Dec 2012-ECN 3099) Added sysupgrade CLI command to perform software updates.

Ability to perform a software upgrade via CLI command (instead of using the web browser), such as for scripting software updates

Starting in Archive software version 4.8.8, the software update can be initiated using a CLI command (issued via telnet, SSH or the front panel Serial port), instead of using the web browser, if desired. This entails performing an FTP/SCP transfer of the software update file into the SecureSync’s */home/spectracom* directory **and then issuing the**

sysupgrade CLI command to initiate the software upgrade.

Steps to upgrade the software using CLI interface

1) After extracting the .tar.gz update file from the file downloaded from our website, transfer the updatexxx.tar.gz update file into the time server's **/home/spectracom** directory using an FTP program (such as Core FTP for instance)

2) Perform the **sysupgrade** command to initiate the update process.

   The syntax for issuing the *sysupgrade* command is (where the "updatexxx.tar.gz" is the specific version upgrade bundle desired to be applied).

   - Standard upgrade (Such as upgrading versions 4.8.8 to 4.8.9 for example): "sysupgrade" followed by the upgrade file name (Example: **sysupgrade update489.tar.gz**).
   - Forced upgrade (Such as downgrading versions 4.8.9 to 4.8.8 for example, but can also be used with Standard upgrades, also): "sysupgrade force" followed by the upgrade file name (Example: **sysupgrade force update489.tar.gz**).
   - Clean upgrade (Such as first performing a Forced upgrade from 4.8.8 to 4.8.9, for example. Then automatically resetting the NTP server back to factory default settings and deleting all log files): "sysupgrade clean" followed by the upgrade file name (Example: **sysupgrade clean update489.tar.gz**).

Updating 2400 SecureSync versions prior to v1.4.1 (such as 1.3.0) to v1.4.1 or above (tar.gz to squashfs)

Email from Michael Pratt (Engineer) to Dave L (April 2022): When upgrading a 2400 unit from a version prior to 1.4.1 (i.e., 1.3.0 or earlier), please use the file update-securesync-1.4.1.tar.gz. When upgrading a unit from 1.4.1 or later (including any release candidate versions), please use the file securesync-1.4.1.squashfs.

Please also be aware that if your current software is on version 1.1.0a or earlier, a direct upgrade to 1.4.1 will fail unless the clean option is selected. To prevent configuration loss, users are advised to save and download a configuration bundle, perform a clean upgrade to 1.4.1, and apply the saved config file.

- If your current software is on **version 1.1.0a or earlier**, a direct upgrade to 1.4.1 will fail unless the clean option is selected. To prevent configuration loss, users are advised to save a configuration bundle, perform a clean upgrade to 1.4.1, and apply the saved config file.

"Force update" (available in 1200s, not available in 2400s)

Q from Keith to Will Comly (4 Jan 2023)

Quick 2400 1.4.x / 1.6.0 software update question for you. As 2400s don't have force update checkbox, when applying the same version already installed, will everything update, or does the updater skip assemblies already at that version (do we still need to add a force button at some point, or is force upgrade of everything inherent when applying same version over itself?

[10:16 AM] William Comly (4 Jan 2023)
When updating from 1.6.0 to 1.6.0, for example, you are upgrading everything, but since everything should already be the proper firmware versions paired with 1.6.0, nothing will be forced to update and the customer configurations will be transferred to the new installation. If you do a clean upgrade to 1.6.0 from 1.6.0, then it WILL force everything to update but wipe out the configuration. Essentially, we rolled that force functionality only into the clean upgrades.

The best way to "force" update would be to save the 1.6.0 configuration, do a clean upgrade to 1.6.0, then reapply the configuration on the new installation.

Some extra info, the sanitized upgrade forces like a clean one does, but is more comprehensive in what it clears. It will wipe out data from both partitions, so a rollback won't be useful since all of the previous data was cleared.

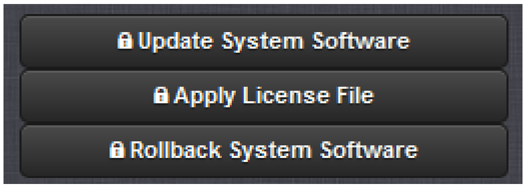
[10:20 AM] William Comly
Also, the upgrading on 1200 was much more atomic than it is on Versa and 2400.

Currently, the only things that are updated separately from the base system are the option cards. The timing system isn't really "upgraded" anymore as it's loaded from the unit sw and will always match the version it's paired with. Also, we haven't had a new version of the UBlox firmware since we released 2400, so I'm not sure if that's really handled by our upgrades yet.

Rollback System software (Software downgrade/upgrade capability in 1.4.1 and above)

- In at least versions 1.3.0 and below, Force upgrade is not available
- Versions prior to v1.4.1 can't be downgraded (in the field) to any earlier version (have to be returned to downgrade)
- The ability to Rollback to an earlier version (downgrade)/Rollback again to the newer version (up was added in v1.4.1
- Can only downgrade back to v1.4.1 (no earlier versions are available)
- Configs are independent/confined to the particular selected partition- they don't follow the rollover to the opposite partition

***Tools* -> *Upgrade/Backup* page**



Performing more than one Rollback: It can continue to switch back and forth between the two installed versions

Configuration files when performing Rollbacks

- Config files are specific to which of the two partitions is currently selected (configs are not shared by the two partitions)
- If a rollback occurs, configs will be based on the previous configuration. If a change is made and then another rollback occurs to the more recent version, the config change won't persist with the rollback.

[10:07 AM] Keith Wing
The other question which came up is about configs during rollback. I assume the configs are shared? so if you rollback and change a config, then rollback again, that config change will remain with the rollback?

[10:08 AM] Keith Wing
so the configs are not "version dependant" they will remain the same, no matter which partition?

[10:10 AM] William Comly
configs are version dependent and a customer will not have configurations persist after rollback, since configs are stored on the specific partitions.

[10:10 AM] William Comly
in short, configs are not shared
like 1

[10:10 AM] Keith Wing
Got it!! Thanks much!!!
like 1

[10:11 AM] William Comly
though if you rollback from 1.6.0 to 1.4.3, the configs from the 1.6.0 partitions will still be there if you rollback again from 1.4.3 to 1.6.0
like 1

[10:12 AM] Keith Wing
Makes sense! So the configs would be back to the way there were before the first rollback?

[10:13 AM] William Comly
right, all rollback does is switch the currently active partition. So except for some bugs concerning some stuff stored on the eeprom (which we have tickets for), all configs will remain on their partition for when you switch back and forth since they're just files stored in the linux filesystems

Log entries associated with Rollback

- In at least updated1.6.0 and below, if a rollback is performed, standard reboot/boot-up logs are asserted. But there is no specific “rollback occurred” type entry asserted in partition that it was rolled back to (going from 1.6.0 to 1.4.3, no rollback entries will be present while in the 1.4.3 partition. It also appears there aren’t any specific “rollback” entries asserted in the original partition, either (after rolling back from the initial Rollback),
- Refer to CAR-2157 (Jan 2023) for request to see if any entries can also be asserted in at least the active partition to show a user initiated a rollback...

Sanitization upgrade (v1.6.0 and above)

- Refer to: Procedure to Sanitize/Sanitization of the Model 2400 SecureSync (versions 1.6.0 and above)

Software upload Failures (failure uploading the upgrade file into the server)

(Note: this info is from 1200 SecureSyncs)

1. **Displayed error message of “500, internal server error” / “internal server error 500”**
   - Refer to Mantis case 3092 (Increase maximum speed Apache limits file download/upload)
   - Has been observed with update versions 5.3.0 and 5.3.1.
   - Likely partially caused by slow transfer rates due to encryption of data when logged in as HTTPS and Apache throttling back uploads so that it can still also be used as a browser during the upload.
   - Recommendation when this issue occurs- login with HTTP (instead of HTTPS) or manuallu upload the file using FTP/SFP (instead of using the browser to upload the file). Then use the browser (or the CLI) to initiate the upgrade.
   - v5.4.0 is lengthening the Apache timeout (30 seconds to 150 seconds) so that once 5.4.0 has been installed, this won’t be a potential issue for subsequent updates.

Draft email Keith uses:

Some customers have observed a general error message when using the web browser to upload the software upgrade bundle file into the time server.

The error message is due a combination of a couple of factors, including the size of the upgrade bundles, the Apache browser limiting the speed of the file upload so it can continue being a “browser” at the same time and the strengths of the cyphers algorithms that are encrypting the file as its being uploaded into the NTP server. So the file transfer is timing out in the browser before it can be fully uploaded.

There are a couple of easy work-arounds available for this condition. After rebooting the unit to clean out its /tmp directory (after each time the file doesn’t fully upload, it leaves files behind in this directory):

1) If you don’t need to have a secure connection to the SecureSyncs browser to upload the file (closed network for instance), login to the browser using HTTP instead of HTTPS (note that this may require HTTP be enabled in th e server if it’s currently disabled. Then the file will be transferred faster, and no longer time-out.
2) If you need a secure connection to upload the file, use an SCP file transfer program to put the full update file int o the **home/spectracom** directory. Then use the browser as normal to initiate the update itself. Unlike the Apa che upload, SFP/FTP don’t throttle back the file transfer. These programs keep sending it as fast as possible wi

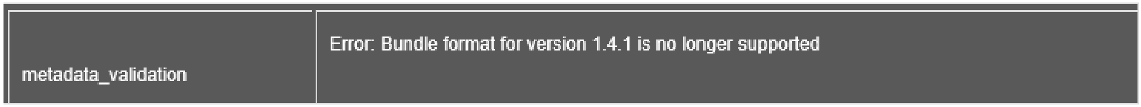
thout concerns of also having to “allot” resources for other simultaneous functions. This will also allow the file to be transferred before timing out.

With the file update file now successfully uploaded without timing out, initiate it using the browser – just like normal!! Among other changes implemented in the version 5.3.1 upgrade, it has lengthened the Apache timeout for file ploads to help with future updates that may be applied.

**Software Upgrade Failures (failures after starting the update process)

A) Specific failures

2. metadata_validation   Error: Bundle format for version 1.4.1 is no longer supported



metadata_validation	Error: Bundle format for version 1.4.1 is no longer supported

Email from Michael Pratt (Engineer) to Dave L (April 2022): When upgrading a 2400 unit from a version prior to 1.4.1 (i.e., 1.3.0 or earlier), please use the file update-securesync-1.4.1.tar.gz. When upgrading a unit from 1.4.1 or later (including any release candidate versions), please use the file securesync-1.4.1.squashfs.

Please also be aware that if your current software is on version 1.1.0a or earlier, a direct upgrade to 1.4.1 will fail unless the clean option is selected. To prevent configuration loss, users are advised to save and download a configuration bundle, perform a clean upgrade to 1.4.1, and apply the saved config file.

B) Other failures

➢ **Review update log via either browser or the CLI interface**

Possible reasons for upgrade failure:

- Corrupt update file (verify the md5 checksum of the file using a utility such as md5checker)
- CF card is too full (**df -h** command’s response is greater than about 72%)
- Too many previous update files retained (try deleting all previous files)

  Via CLI interface

  ✓ To check for any previous updatexxx.tar.gz bundles via CLI: in the home/spectracom directory, type **ls -l** <enter>

  ✓ **To delete an update bundle** in the home/spectracom directory. type **rm <filename>** <enter>

  for example: >**rm update502.tar.gz** <enter>

- Not selecting “**Force Update**” when downgrading to an earlier version,
- Temp directory has lots of files in it (such as due to past failed software updates or using TCPDump). Either Reboot or power cycle to clean out this directory.

Update log entry indicates “[sw-upgrade] Upgrade Initiated, Reboot Required: home/spectracom/update517.tar.gz (SWUA**)”**

➢ Observed with 5.1.4 to 5.1.7 update

➢ Should be fixed with 5.1J beta/ version 5.2.0 software update.

➢ Refer to Salesforce case 16749 (Jump Trading)

➢ Unit doesn’t complete the upgrade because it can’t reboot.

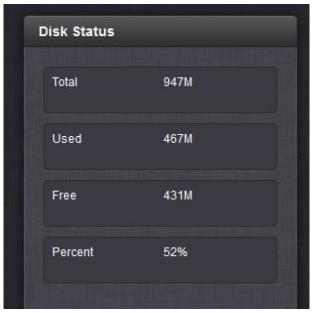
- Reboot commands via browser/CLI don't work.
- Requires a hard power cycle of the unit to finish the update.
- Dave Sohn noted this has been observed with Verizon likely due to the potential pipe software command issue in 5.1.7 and below. "This sounds similar to the Verizon issue as well. I believe when we had an issue with one of the units, the hung process prevented the reboot. In that case, it took a hard power cycle to recover it."

General troubleshooting of a failed software update (specific failures futher below)

- View the Update and System logs to see what they show (both can be viewed in the browser).

If "**Upgrade Failure**" is displayed during the update process or for some reason the upgrade/downgrade process doesn't work:

1) If updating from versions 4.8.9 and below, what upgrade version is being applied? Note there is a check to ensure 5.0.2 has been installed before going to any versions beyond v5.1.2 (If you try applying 5.1.2 to 4.8.9 for example, the update will fail).
2) Look at the entries in the Update log (**Tools** -> **Logs** page of the browser). They will likely indicate why the update didn't take.
3) Perform a **dh -h** CLI command with telnet or ssh (or look at the **"Disk Status"** menu in the browser starting in version 5.2.1 (bottom-left corner of the **Tools** -> **Upgrade/Backup** page)



Disk Status

Total	947M
Used	467M
Free	431M
Percent	52%

4) If the CF card usage is greater than about 72%, delete the logs and NTP starts, delete previous update bundle files, reboot or power cycle to clear out the temp directory. Verify the usage drops.

- To check for any previous updatexxx.tar.gz bundles via CLI, type **ls -l** <enter> (in the home/spectracom directory)
- To delete an update bundle type **rm <filename>** <enter> (for example: >**rm update5.0.2.tar.gz** <enter>

1) With versions 5.1.5 and below, need to use the cleaner patch to make space:

- Engineering has created a patch called "updatecleaner.tar.gz" (17 Feb 15) that cleans out unnecessary files.
- Link to this patch in Arena: https://app.bom.com/files/detail-summary?file_master_id=1236440967&file_id=1748872341&orb_msg_single_search_p=1&redirect_seqno=6242513546
- This patch is intended for update versions 5.0.0 and above only.

A) Two different locations to delete the logs in web browser.

1. Delete just the logs displayed in browser (Qual, Update, etc) but not the system logs in the background (such as kern.log, sys.log, etc)

Management -> **Log Configuration** page. Click the "**Clear All Logs**" button in the upper-left corner).

Notes

1. The Clear All Logs" and "buttons were added in 5.2.1 (I believe). (bottom-left of the **Tools** -> **Upgrade/Backup page)**
2. But with at least software versions 5.2.1 and below, these two buttons in the browser don't work (was fixed in 5.3.0). Have to use the cli **clearlogs** command to delete these items with 5.2.1 and below.

2. Delete all of the logs (both the ones in the background and the ones in the browser)

above- via the bottom-left corner of the **Tools** -> **Upgrade/Backup** page (click the "**Clear All Logs**" button).

Notes:

1. The clearlogs command clears all logs (ones displayed in the browser and the "system" logs in the background. But it doesn't clear the ntpstats and discstats. (refer to clearstats).

Software issue associated with deleting logs and NTP stats via the browser

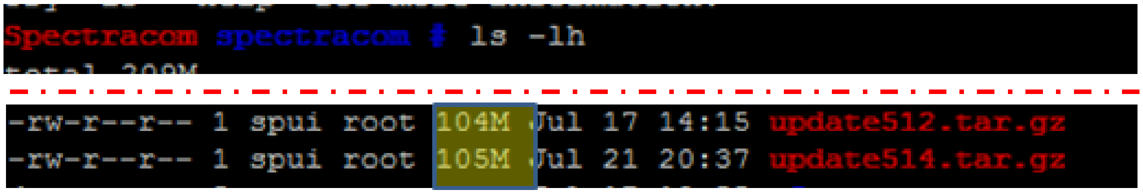
- With software versions 5.2.1 and below, the "Clear All logs" button and Clear Statistics button didn't work
- Note the associated CLI commands work fine in both Models.
- Refer to Mantis case 3049. http://cvsmantis.int.orolia.com/mantis/view.php?id=3049
- Fixed in the version 5.3.0.

B) Delete logs via CLI interface (telnet or ssh)

- clearlogs command via and cli was added in version 5.1.5 (I believe).
- Verify the checksum of the update bundle in the directory it's being uploaded from (not a directory it was downloaded to, prior to moving it to another directory).
- View the size of the update bundle in the home/spectracom directory and make sure it's the same size as the original update bundle (if it's smaller, antivirus may have stripped some of the file).

In the default **home/spectracom** directory, type "**ls -lh**" at the command prompt (note there is a space between the "s" and the "-lh").

The total size of the update bundle is reported (in MB) to the left of the date in the "**updatexxx.tar.gz**" row (as shown below):



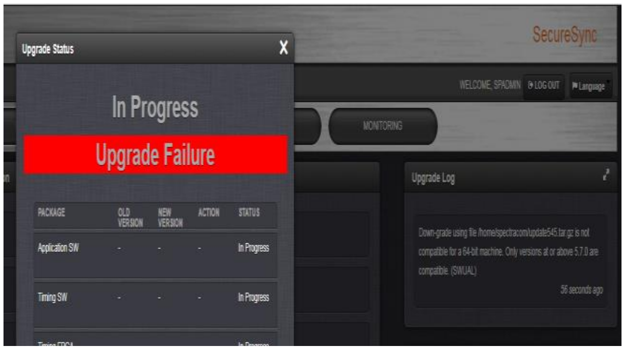
```
Spectracom spectracom # ls -lh
total 209M
-rw-r--r-- 1 spui root 104M Jul 17 14:15 update512.tar.gz
-rw-r--r-- 1 spui root 105M Jul 21 20:37 update514.tar.gz
```

Specific examples of Upgrade Failure:

1. Trying to install a version prior to v5.7.0 (in order to downgrade to an earlier version) when a newer Model ETX module is installed (started shipping Sept 2017) results in the following error in the Upgrade log:

"Down-grade using the file /home/spectracom.update545/tar/gz is not compatible for a 64-bit machine. Only versions at or above 5.7.0 are compatible. (SWUAL)"

- Starting in software version 5.70 software, Paul M added a check to see if a newer ETX is installed, and if an arlier version of software is attempted to be applied, the updater will fail with an error message. The upper-right corner of the screenshot shows this error message!!



Upgrade Status

In Progress

Upgrade Failure

PACKAGE	OLD VERSION	NEW VERSION	ACTION	STATUS
Application SW	-	-	-	In Progress
Timing SW	-	-	-	In Progress
Timing FPGA				In Progress

Upgrade Log

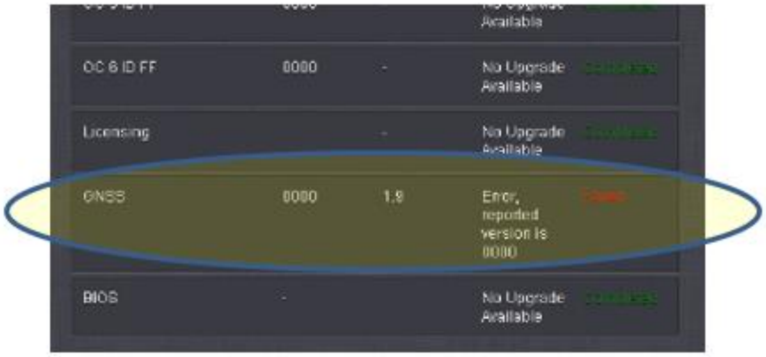
Down-grade using file /home/spectracom/update545.tar.gz is not compatible for a 64-bit machine. Only versions at or above 5.7.0 are compatible. (SWUAL)

56 seconds ago

2. **“Starting up System” remains indefinitely displayed on front panel LCD during (and after) attempted update**

   ➢ Refer to Salesforce case 25112 (occurred during v5.6.0 update)

3. **“Error, reported version is 0000, Status: Failed” appears “Upgrade Status” ‘In Progress’ window (for “GNSS”)**



[illegible]	[illegible]		[illegible] Available	[illegible]
OC 6 ID FF	0000	-	No Upgrade Available	[illegible]
Licensing		-	No Upgrade Available	[illegible]
GNSS	0000	1.9	Error, reported version is 0000	[illegible]
BIOS	-		No Upgrade Available	[illegible]

➢ This Error message is due to having a Res-T GPS receiver (first Model used in SecureSync/9400s) installed when the v5.6.0 and above updater checks to see if a Res-SMT-GG or ublox is installed.

➢ No further actions required. There are no available/expected updates for the Res-T receivers.

➢ Hendrik intends to add note starting in the v5.7.0 update instructions.

Email from Paul (18 Apr 17 after a v5.6.0 update attempt) Thanks, I did not catch that … You are right, the receiver does NOT support update is a Trimble Resolution T (RES T) not SMT.We can try to squelch that in a future release but it is not a priority now.

SWUAL_Lock: lockfile exists

Q I have been trying to "clean update" and Securesync unit but the software update is stalling part way through ... I have left it for days and it never finishes.I've power-cycled the unit and tried to update again (to 5.5.1) but the updater complains "Lock file exists"

I have been trying to "clean update" and SecureSync unit but the software update is stalling part way through ... I have left it for days and it never finishes. I've power-cycled the unit and tried to update again (to 5.5.1) but the updater complains "Lock file exists.   Is there a way to clear-out the lock file and get the update going again?

```
spadmin@pptp201 ~ $ sysupgrade clean update551.tar.gz
Background upgrade process is running...
The process may take some time based on system configuration.
The system will reboot to complete the upgrade process.
```

Check the update log for status.
spadmin@pptp201 ~ $ SWUAL_Lock: lockfile exists

A Refer to Salesforce case 24121. Likely due to a full CF card. Perrform a **df -h** CLI command

(note from Keith) Seems even more likely the unit just needs to be rebooted (a reboot fixed the issue with a later customer). Perhaps this is related to the /tmp file getting full due to earlier update attempts failing.

---

4. **CF card too full to perform a software update (especially with earlier versions such as 5.0.2, 5.1.2, 5.1.4, etc)**

   - Engineering has created a patch called "updatecleaner.tar.gz" (17 Feb 15) that cleans out unnecessary files.
   - Link to this patch in Arena: https://app.bom.com/files/detail-summary?file_master_id=1236440967&file_id=1748872341&orb_msg_single_search_p=1&redirect_seqno=6242513546
   - This patch is intended for update versions 5.0.0 and above only.

---

5. **Can telnet/ssh in after update, but can't access the web browser**

   - Refer to Mantis 2795 http://cvsmantis.int.orolia.com/mantis/view.php?id=2795
   - First try just restarting Apache with **servset 6 on** / **servset 6 off**. Then try logging in again.
   - If still not working, try resetting the HTTPS certificate using either the **defcert** or **defcert -sha1** cli command.
     - Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
     - An example defcert CLI syntax (5.6.0 and above only) is **defcert -sha256**
     - V5.6.0 also changed the default algorithm to **SHA256** for better security (the default in 5.5.1 and below was SHA1) .
     - As IE8 and below do not support SHA-256, in versions 5.6.0 and above, use **defcert -sha1** to regenerate a new certitficate using SHA1 to gain access to IE8 and below

   Email from Keith (20 Jul KW) One thing to keep in mind is that, depending on the current software version installed in the SecureSync, the **defcert** command will create its new default certificate using either a **SHA1** cipher or a **SHA256** cipher.

   With software **versions 5.6.0 and above** installed in the SecureSync, the more secure SHA256 encryption cipher will be used to generate its new certificate (with version 5.5.1 and below, the defcert command used the SHA1 cipher).

   The issue with the more secure SHA256 cipher is **Internet Explorer versions 8** and below can't use this newer cipher. With these more recent versions of software installed in the SecureSync (5.6.0 and above), and when using IE8 or below to access the SecureSync, instead of using the CLI command of **defcert** to replace the existing certificate, issue instead the following CLI command to generate a new certificate using the earlier SHA1 cipher: **defcert -sha1** <enter>. Then try accessing the web browser again.

---

6. **Downgrading to an earlier version of software without select the "Force Update" checkbox, in addition to selecting the "Update System.**

   - Software downgrades or to same version require "Force Update" to also be selected.

---

7. **Not enough room in CF card**

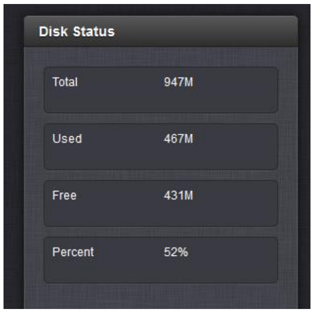
   - Issue CLI command **df -h** to determine CF card disk usage.

CF card usage is now reported in the browser (alleviating need to have to use CLI command)

Note: Update version 5.2.0 added CF card memory status to the newer web browser (not available in classic interface).

Note: Also added ability to delete logs and Statistics from the same location

Tools -> **Upgrade/Backup** page of the browser (under "Disk Status")



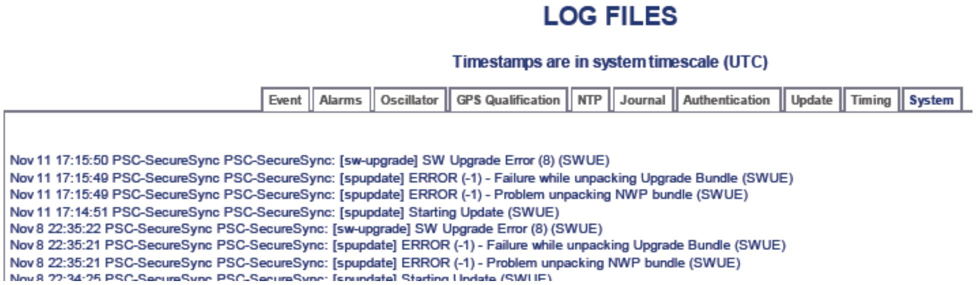
Disk Status

Total	947M
Used	467M
Free	431M
Percent	52%

Note: In general, disk usage should be **less than** around **70%** or so usage to prevent issues with the update process. Logs and previous update bundles may be taking up too much space.

- ➢ Delete previous update bundles (such as update489, for instance) to free space
- ➢ Delete logs to free up space.
- ➢ Reboot/power cycle to clear out the temp directory (just in case it has lots of files in it)
- ➢ May or may not cause "Error (-1) Failure while unpacking Upgrade Bundle" / "Problem unpacking NWP bundle" to be asserted.

Update log entries "Error (-1) Failure while unpacking Upgrade Bundle" / "Problem unpacking NWP bundle"



LOG FILES

Timestamps are in system timescale (UTC)

```
Nov 11 17:15:50 PSC-SecureSync PSC-SecureSync: [sw-upgrade] SW Upgrade Error (8) (SWUE)
Nov 11 17:15:49 PSC-SecureSync PSC-SecureSync: [spupdate] ERROR (-1) - Failure while unpacking Upgrade Bundle (SWUE)
Nov 11 17:15:49 PSC-SecureSync PSC-SecureSync: [spupdate] ERROR (-1) - Problem unpacking NWP bundle (SWUE)
Nov 11 17:14:51 PSC-SecureSync PSC-SecureSync: [spupdate] Starting Update (SWUE)
Nov 8 22:35:22 PSC-SecureSync PSC-SecureSync: [sw-upgrade] SW Upgrade Error (8) (SWUE)
Nov 8 22:35:21 PSC-SecureSync PSC-SecureSync: [spupdate] ERROR (-1) - Failure while unpacking Upgrade Bundle (SWUE)
Nov 8 22:35:21 PSC-SecureSync PSC-SecureSync: [spupdate] ERROR (-1) - Problem unpacking NWP bundle (SWUE)
Nov 8 22:34:25 PSC-SecureSync PSC-SecureSync: [spupdate] Starting Update (SWUE)
```

Likely causes:

A) Corrupt update file. Run MD5 checker to verify file integrity

B) Too many Update Bundles stored in unit.

1. **Issue CLI command df -h to determine CF card disk usage.**

   In general, disk usage should be less than around70% usage to prevent issues with the update process. Logs and previous update bundles may be taking up too much space.

2. **Delete previous update bundles (such as update489, for instance)**

   To delete earlier update file, select each one in the drop-down, check only the "**Delete Update File**" checkbox in the screen where you normally select “Update File”. Then press Submit.

3. **Then select “Update System”.**

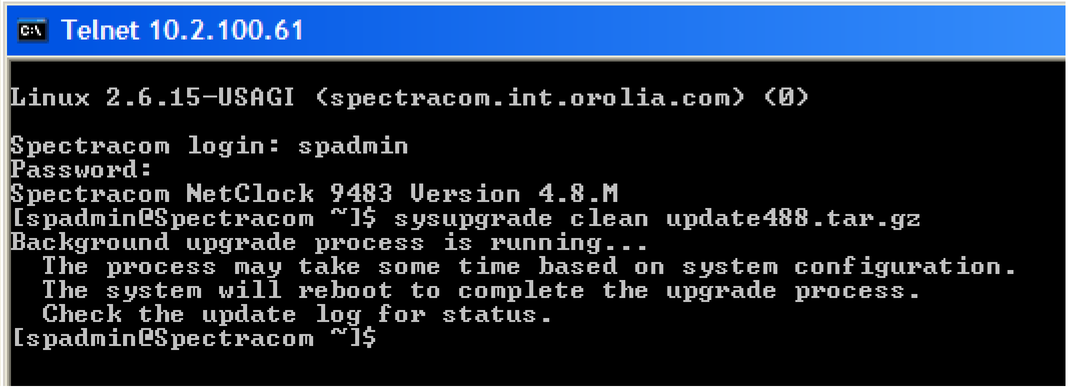
See if it proceeds through the process this time (as I suspect it will).

A) **Downgrading from 4.8.M to earlier version**

- Update log contained” “Spectracom Spectracom: [sw-upgrade] Downgrades require clean update: /home/spectracom/update488.tar.gz (SWUAL)

Email from Dave Sohn (15 May 13) “In any case, the upgrade failed because 4.8.M to 4.8.8 is considered a downgrade and as of 4.8.9 (or M) downgrade requires the clean setting:

Note: “clean update” is not available in web browser, login using telnet/ssh and perform a **sysupgrade clean 4xx.tar.gz** command (where xx is the “downgrade to” version) as shown below:



```
Linux 2.6.15-USAGI (spectracom.int.orolia.com) (0)

Spectracom login: spadmin
Password:
Spectracom NetClock 9483 Version 4.8.M
[spadmin@Spectracom ~]$ sysupgrade clean update488.tar.gz
Background upgrade process is running...
  The process may take some time based on system configuration.
  The system will reboot to complete the upgrade process.
  Check the update log for status.
[spadmin@Spectracom ~]$
```

[spupdate] ERROR (-1) - Failure while unpacking Upgrade Bundle (SWUE)

- Likely due to a problem with the update file in the unit- not likely a problem with the update process.
  1) Check the MD5 file checksum to ensure the file wasn’t corrupted when it was downloaded.
  2) Make sure that if the file is being transferred in using FTP/SCP (instead of using the browser), that the file is transferred using “**binary**” mode. Otherwise, the file can be altered/corrupted during the file transfer.

Known Software issues

- ➢ Refer to/Search the latest Release Notes document. The document contains a section for known issues
- ➢ 2400 Release notes available from: I:\Customer Service\PSB, PSP software updates\2400 SecureSync\2400 SecureSync Software updates

Known issues from the Release Notes, sorted by version (note this list may not be complete)

Known Issues (from v1.4.3 release notes)

• Option cards 1204-49 and 1204-4A are limited to install on slots 1 & 2 only.
• This software version DOES NOT ALLOW downgrades before version 1.4.1.
• ASCII time code format ICD-153c is supported only on the -02 and -1F option cards, and only if the unit has a SAASM receiver installed. This format is not supported on the main board interface (from 1.3.0).
• The `clean` command does not reset the GNSS position. It is recommended to unplug the receiver, reset the receiver in the Web UI, and then run the `clean` command in order to reset the GNSS position (from 1.3.0).
• PTP over a VLAN interface is not currently functional (from 1.4.1).
• The SFP fiber link-state on models AVAGO AFBR-5710PZ and FTLF8519P2BNL are not working properly (from 1.4.1).
• The restore factory defaults function `clean` does not currently reset the Network Access control rule (from 1.4.1).
• PTP Power Profile (IEEE C37.238) is unable to pass the Alternate Time Offset Indicator and Total Time Inaccuracy TLVs through the system when PTP interfaces are configured as both a master and a slave (from 1.4.1).
• PTP Power Profile (IEEE C37.238) is only able to sync to an EdgeSync master when set to mixed Unicast mode (from 1.4.1).
• The tcpdump command has incorrect ownership, blocking all users from deleting files. To remove files, the user can update to the same or a newer version. To prevent this scenario, you can execute tcpdump as `sudo tcpdump -Z <user> ...`, (for example: `sudo tcpdump -Z spadmin -i eth0 -w file.pcap)`. This will cause the captured file to be created with ownership of the specified user, allowing said user to delete (from 1.4.1).
• DHCPv6 may not perform as expected. It is recommended to use either static or stateless (SLAAC) IPv6 addressing, particularly with network time distribution.

Known Issues (from v1.4.1 release notes)

• Option cards 1204-49 and 1204-4A are limited to install on slots 1 & 2 only.
• This software version DOES NOT ALLOW downgrades. If you put this software on your system, and later need to return your unit to a software version that came before version 1.4.1, it will be necessary to return your unit to Orolia for reprogramming (from 1.3.0).
• ASCII time code format ICD-153c is supported only on the -02 and -1F option cards, and only if the unit has a SAASM receiver installed. This format is not supported on the main board interface (from 1.3.0).
• The `clean` command does not reset the GNSS position. It is recommended to unplug the receiver, reset the receiver in the Web UI, and then run the `clean` command in order to reset the GNSS position (from 1.3.0).
• PTP over a VLAN interface is not currently functional.
• The SFP fiber link-state on models AVAGO AFBR-5710PZ and FTLF8519P2BNL are not working properly.
• The restore factory defaults function `clean` does not currently reset the Network Access control rule.
• Upgrade warnings for loss of or altered configurations: o On software versions before 1.3.0, SNMP, GPSD, and LDAP settings are preserved on upgrade but not correctly transferred in configuration bundles. These services will need to be re-enabled following the application of a configuration bundle.
o On software versions before 1.3.0, certain front panel settings for the Local Clock and the Lock Keyboard function do not persist after upgrade.
o Upon upgrading to 1.4.1 or applying a configuration bundle from an earlier version, the System Time Message feature will be set to ON, regardless of previous setting. Following a Clean upgrade to 1.4.1, the System Time Message, Daytime Protocol, and Time Protocol features will be configured to OFF (the new default state).
o If your current software is on 1.1.0a or earlier, a direct upgrade to 1.4.1 will fail unless the clean option is selected. To prevent configuration loss, users are advised to save a configuration bundle, perform a clean upgrade to 1.4.1, and apply the saved config file.

• PTP Power Profile (IEEE C37.238) is unable to pass the Alternate Time Offset Indicator and Total Time Inaccuracy TLVs through the system when PTP interfaces are configured as both a master and a slave.
• PTP Power Profile (IEEE C37.238) is only able to sync to an EdgeSync master when set to mixed Unicast mode.
• The tcpdump command functionality was found to have incorrect ownership, thereby preventing users from deleting files, even with admin rights. To remove these files, the user can update to the same or a newer version. To prevent this scenario, you can execute tcpdump as `sudo tcpdump -Z <user> ...`, (for example: `sudo tcpdump -Z spadmin -i eth0 -w file.pcap)`. This will cause the captured file to be created with ownership of the specified user, allowing said user to delete the file.

Known Issues (from v1.3.0 release notes)

• Option cards 1204-49 and 1204-4A are still limited to install on slots 1 & 2 only.
• This software version DOES NOT ALLOW downgrades. If you put this software on your system, and later need to return your unit to a software version that came before version 1.3.0, it will be necessary to return your unit to Orolia for reprogramming.
• When configured as a slave, the on-unit PTP will sometimes incorrectly remain in a Sync state when the Master has gone out of sync.
• ASCII time code format ICD-153c is supported only on the -02 and -1F option cards, and only if the unit has a SAASM receiver installed. This format is not supported on the main board interface.
• The 4A/49 option card user configurations will be lost when performing an upgrade that is not “clean”. The card can be reconfigured and will function, but any new configuration will not persist after a power cycle of the unit. Cleaning the unit configuration (or performing a clean upgrade) will allow new configuration to persist correctly. An applied configuration bundle saved from an earlier software version will encounter the same difficulty.
• The `clean` command does not reset the GNSS position. It is recommended to unplug the receiver, reset the receiver in the Web UI, and then run the `clean` command in order to reset the GNSS position.
• Any changes to the Logging Configuration (for instance, turning on Local Logging) will not take effect without restarting the unit.
• If a user configures the time zone via the front panel, the configuration will be lost after upgrade or config bundles are applied.
• The Reference Priority configuration is sometimes not restored properly from configuration bundles and will have to be reconfigured following upgrades or application of a config bundle from pre-1.3.0 software.
• When multiple major or minor alarms are present, the front panel LED alarm status light will not activate. All other alarm behavior, including notifications, operates as expected.

Known Issues (from v1.2.2 release notes)

• In version 1.2.2, the 2400 cannot be configured to operate as both a PTP slave and NTP client.
• When switching PTP configuration between master and slave, occasionally the change will not take effect unless manually disabling/reenabling PTP on that interface.

Known Issues (from v1.2.0 release notes)

• The following option cards are currently limited in use to only slots 1 & 2: 1204-2F, 1204-13, 1204-23, 1204-49, 1204-4A, and 1204-30.
• On units that have manually-set time as a PTP Master and then are switched to using a valid reference, the Slave time does not correctly switch to the reference but will instead stay on manual time. If switching between manually-set time and an external reference, the PTP master must be restarted for the slaves to properly follow the new time source.
• When restoring configurations, the GNSS Constellations configuration is on rare occasions not loading correctly.

**License files (for Purchased Options)

(Note: this info is from 1200 SecureSyncs)

- License Install instructions: Refer to [..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\License Files Updates](..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\License Files Updates)
- License Files allow options such as Glonass, Skylight and Rinex server to be added in the field.
- The same license file that is used to enable Glonass is the same file used to enable Skylight phase 2/

Creating license files

1) See Dave Lorah or Ron Dries for process to create files.
2) Licenses are **Model** and **Serial Number** specific:
   - Make sure Serial Number is verbatim of what is programmed into the unit (**Tools**-> **Upgrade/backup** page). If here are no leading 0s in the Serial Number, do not use a leading 0 when creating the license file.

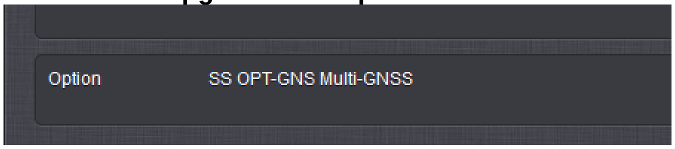
Viewing installed license files

Note:, the "**manifest**" command will show all the system information in more detail.

To view installed licenses/options:

A) Via web browser

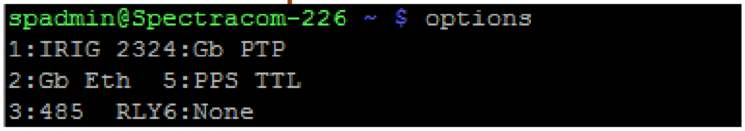
Go to **Tools** -> **Upgrade/Backup.** Scroll down to the bottom of the **System Configuration** table.



Option	SS OPT-GNS Multi-GNSS

B) Via CLI

The CLI command is "**options**"



```
spadmin@Spectracom-226 ~ $ options
1:IRIG 2324:Gb PTP
2:Gb Eth  5:PPS TTL
3:485   RLY6:None
```

Deleting license file

Deleting license file from the browser doesn't remove the Option- just the file used to enable the Option.

Troubleshooting license file install

- Licenses are Model and Serial Number specific:
- Model Number (2400) matters (as reported in the **Tools** -> **Upgrade/Backup** page)

Leading "0" in Serial Number matters (as reported in the Tools 0> Upgrade/Backup page)

- If there is one or two leading 0s in the Serial Number, the license has to be created with the 0.
- If there is no leading 0s in the Serial Number, the license has to be created without the 0.

***SC037 ("Trade and Industry Department Cryptography Questionaire")/Blowfish

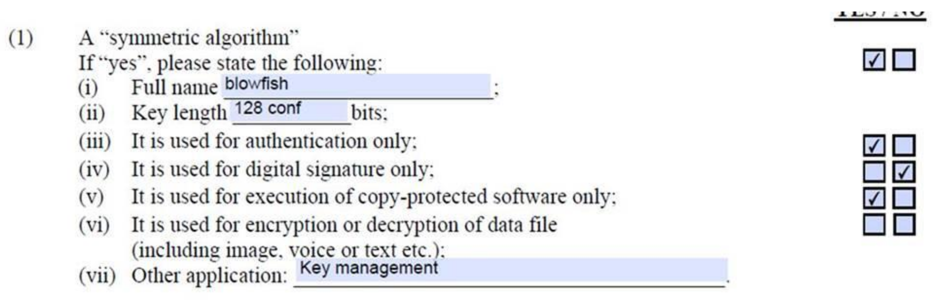
SC037 (“Trade and Industry Department Cryptography Questionaire”)/

- Refer to: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Cryptography questionanaire

Blowfish (part of the Crytography questionnaire referred to above)

Email from Paul Myers (29 Jun 17) “BlowFish is in OpenSSL but I don’t know how we use it.

Why is blowfish marked specifically.
I don’t remember what uses it.



YES / NO

(1) A “symmetric algorithm” ☑ □
If “yes”, please state the following:
(i) Full name blowfish;
(ii) Key length 128 conf bits;
(iii) It is used for authentication only; ☑ □
(iv) It is used for digital signature only; □ ☑
(v) It is used for execution of copy-protected software only; ☑ □
(vi) It is used for encryption or decryption of data file (including image, voice or text etc.); □ □
(vii) Other application: Key management.

System initialization after each boot-up

(Note: this info is from 1200 SecureSyncs)

System outputs default time of 00:00:00 (incrementing) year 2000 while initializing

Q. (From Jennifer Trotta with Raytheon) I have a question about time code output when the SecureSync is rebooted due to a configuration or other change. Does the IRIG output ever put out all zeroes when the system is going through a reboot? What happens to the IRIG signal upon reboot?

We are seeing some squirrely behavior on one of our units downstream that is receiving the IRIG signal. It thinks that the year rollover has occurred when we do a reboot.

A Reply From Keith Wing (7 Aug 2014)

To answer your question, as the SecureSync is booting-up and loading, it will initially output the time as all 0’s (and the year as the default of 2000), and then start to increment the seconds value from there, each second. The estimated time is typically loaded into the timing system for it to update the outputs (such as IRIG) within about a minute or so after applying power, or after performing a reboot.

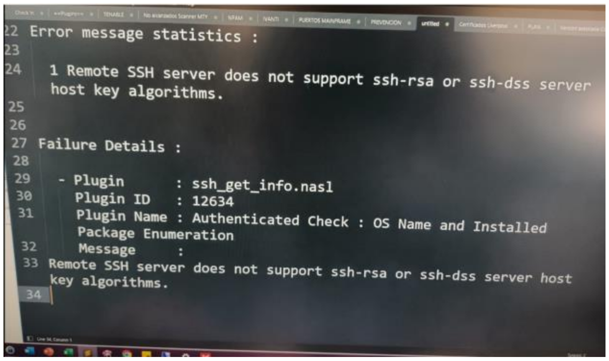
This start-up initialization of the system can be viewed very easily by power cycling the SecureSync and then watch the green LED clock on the front panel. Moments after power up, the time will be displayed (such as 00:00:02, by the point it can be displayed) and then it increments the seconds once-per-second. This continues for just over a minute. Then the System clock (which controls the date/time to the outputs such Perf as IRIG) is corrected by the Real Time Clock, which continues to maintain an estimate of the time/date while the system is powered down. The front panel time display and the system outputs such as IRIG, will jump to this estimated time, until an input reference (such as GPS) becomes present and valid, at which time the date/time is corrected as needed and the Sync LED turns green.

The method to prevent the initialization of the SecureSync from needing to occur is to keep it continuously powered-up.

Network Vulnerability Scans/Tenable Nessus Credentialed Security Scans

Error message "Remote SSH server does not support ssh-rsa or ssh-dss server host key algorithms" displayed when scanning Model 2400 SecureSync (not displayed when scanning Model 1200 SecureSyncs)

- Refer to Salesforce Case 294835
- Associated with Plugin named: "ssh_get_info.nasl"



```
Error message statistics :

  1 Remote SSH server does not support ssh-rsa or ssh-dss server
  host key algorithms.


Failure Details :

  - Plugin      : ssh_get_info.nasl
    Plugin ID   : 12634
    Plugin Name : Authenticated Check : OS Name and Installed
    Package Enumeration
    Message     :
Remote SSH server does not support ssh-rsa or ssh-dss server host
key algorithms.
```

Message from Ryan Johnson "We did open a case with Tenable and their response was that the issue likely stems from the 2400 using **Buildroot as the Linux distribution and which Nessus doesn't know anything about** (as opposed to Gentoo Linux on the 1200 which Nessus does).

Email Keith sent to our dealer (12 June 2023) We are also observing the same condition of the failed plug-in. As we also observed it, we were able to ask Tenable about it and they explained why it's being observed while successfully scanning a Model 2400 SecureSync, but not observed when scanning a Model 1200 SecureSync.

There are several different distributions of Linux, the Operating Systems for the Models 1200 and 2400 SecureSyncs. These two Models do not run on the same distribution of Linux.

Tenable Nessus is fully aware of the distribution of linux that the 1200 SecureSync operates on. But it's not familiar with the distributions of Linux that the Model 2400s operate on. Because it's not familiar with the linux distribution that the Model 2400 SecureSyncs operates on, its scan of the OS operates a little differently than it does when it's fully familiar with the linux distribution (but the scan is still successful). This is the reason for the plugin message as its scanning the Model 2400 SecureSyncs.

This is not an issue with (in any way), or a limitation of the Model 2400 SecureSyncs. Tenable has mentioned to our Engineering team they don't intend on changing Nessus software to be fully aware of this distribution of Linux. However, if by chance they one day decide to be fully aware of this particular distribution of Linux, the message about the plugin can be prevented from being displayed.

As we observed, the scan of the Model 2400 is still successful, and your customer's scan results matched ours. Again, the plug-in message is strictly due to Tenable Nessus software not being familiar with the linux distribution intended to continue being used with the Model 2400 SecureSyncs. Though it's a different distribution in the Model 2400 SecureSyncs, than in the Model 1200s, the scan is still successful.

Third-party software packages used/not used in 2400 SecureSyncs

(Note: this info is from 1200 SecureSyncs)

A) systemd

- Per https://en.wikipedia.org/wiki/Systemd

  systemd is an init system used in Linux distributions to bootstrap the user space and manage all processes subsequently, instead of the UNIX System V or Berkeley Software Distribution (BSD) init systems. It is published as free and open-source software under the terms of the GNU Lesser General Public License (LGPL) version 2.1 or later.[5] One of systemd's main goals is to unify basic Linux configurations and service behaviors across all distributions.[6]

- Per Dave Sohn (5 July 17, pertaining to CVE-2017-445) "We do not currently use systemd on SecureSync"

Anti-virus software (antivirus software)

Q (from TOYO) Our customer NTT East who are considering introducing your time servers newly, they have a question about anti-virus policy of the product. Could you please answer their questions below?

1. What measures are prepared against threat of computer viruses in the SecureSync?

2. Is it possible to install an anti-virus software to the SecureSync?
(If yes, do you have any recommendation?)

3. If the SecureSync has no specific measures, please tell us your policy and the grounds.

A **Reply from Dave Sohn (28 Jul 17)** The SecureSync is not a general application server. It is a purpose-built appliance. While it utilizes a standard operating and file system, it is not susceptible to viruses in a similar way as a general purpose machine, and as such does not include anti-virus SW or provisions to run anti-virus SW. Vulnerabilities are minimized through the security mechanisms built-in. The ability to inadvertently load and execute malicious code that can compromise the system is limited based on customer privilege levels (no root access). In addition, system SW updates are verified through hashing and checksums to prevent manipulation of update images.

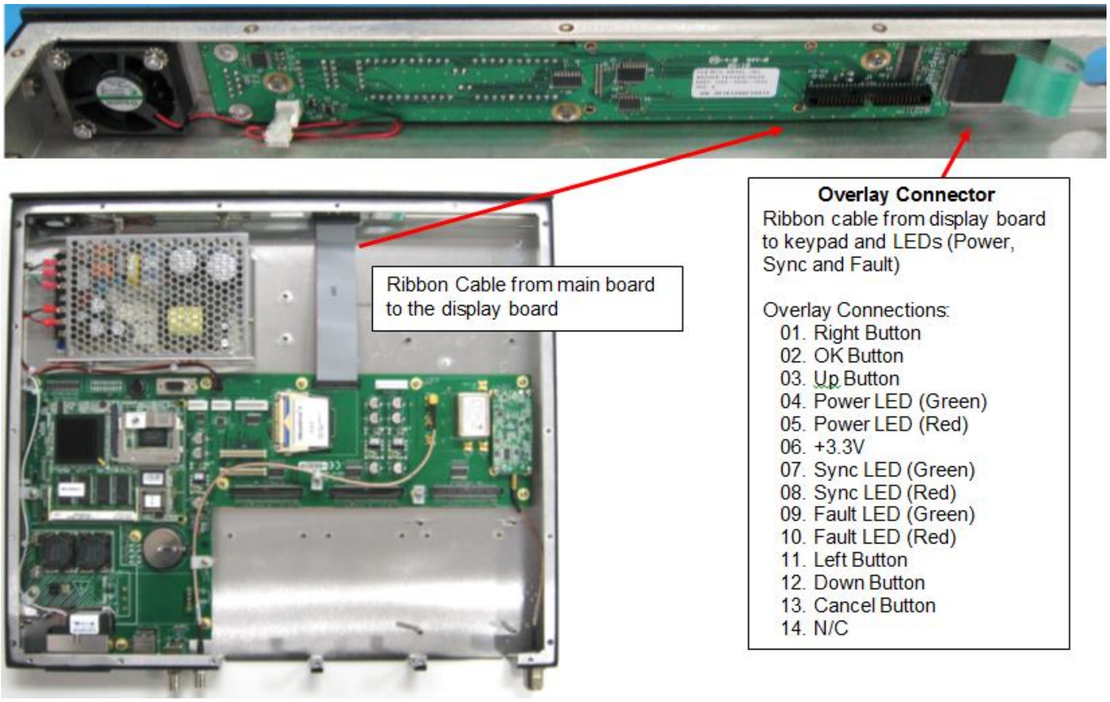
Front Panel / keypad

****Front panel connections**

Schematic for SecureSync

(Note: this info is from 1200 SecureSyncs)

- front panel PCB board (1200-1001-0300) (in 1200-0000-F004) in Arena: https://app.bom.com/items/detail-spec?item_id=1202839909&version_id=10299091328&orb_msg_single_search_p=1&redirect_seqno=8027520292
- main SecureSync PCB board (1200-1001-0200) (in 1200-0000-F003) In Arena: https://app.bom.com/items/detail-spec?item_id=1202839908&version_id=10290528958&orb_msg_single_search_p=1&redirect_seqno=8027522349

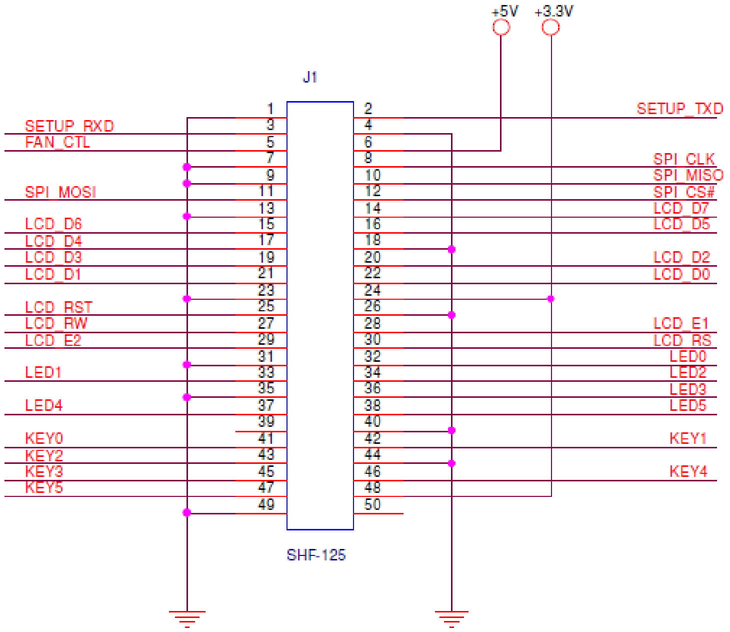


Ribbon Cable from main board to the display board

Overlay Connector
Ribbon cable from display board to keypad and LEDs (Power, Sync and Fault)

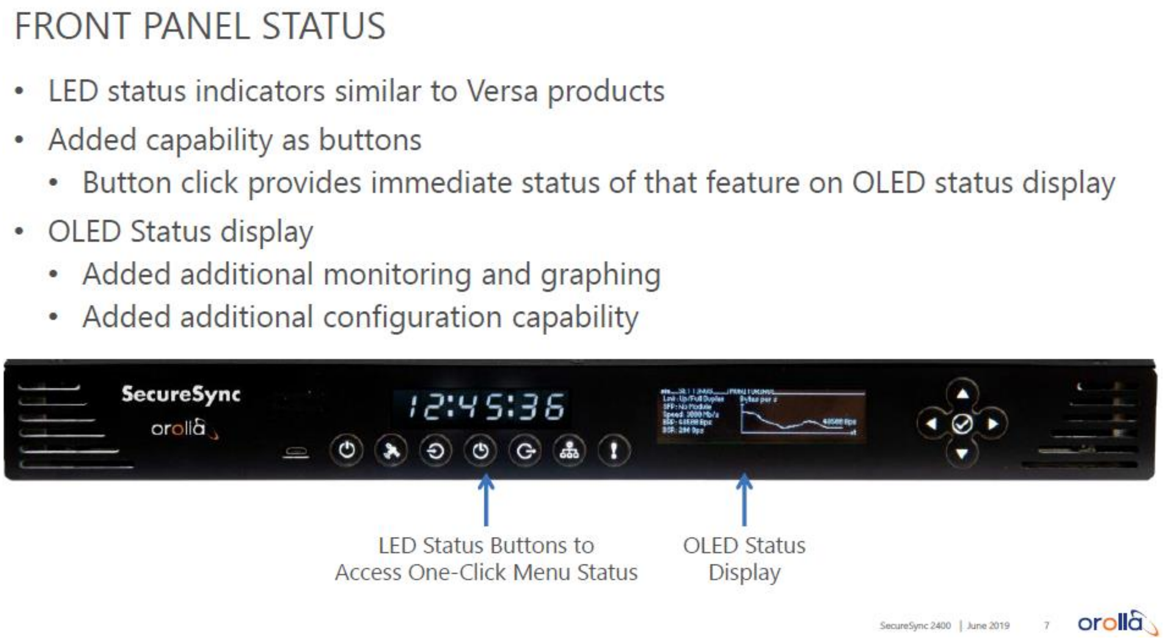
Overlay Connections:
01. Right Button
02. OK Button
03. Up Button
04. Power LED (Green)
05. Power LED (Red)
06. +3.3V
07. Sync LED (Green)
08. Sync LED (Red)
09. Fault LED (Green)
10. Fault LED (Red)
11. Left Button
12. Down Button
13. Cancel Button
14. N/C

Main Board I/O



**2400 Front Panel OLED / time display / keypad

- Refer to online 2400 User guide at: http://manuals.spectracom.com/2400/Content/NC_and_SS/2400/INTRO/Front_Panel.htm



FRONT PANEL STATUS

- LED status indicators similar to Versa products
- Added capability as buttons
  - Button click provides immediate status of that feature on OLED status display
- OLED Status display
  - Added additional monitoring and graphing
  - Added additional configuration capability

SecureSync
orolia
12:45:36

LED Status Buttons to Access One-Click Menu Status

OLED Status Display

SecureSync 2400 | June 2019 7 orolia

A) **LED Display**

(Note: this info is from 1200 SecureSyncs)

LED Time display while the system is initially booting-up (after power cycle, reboot or clean)

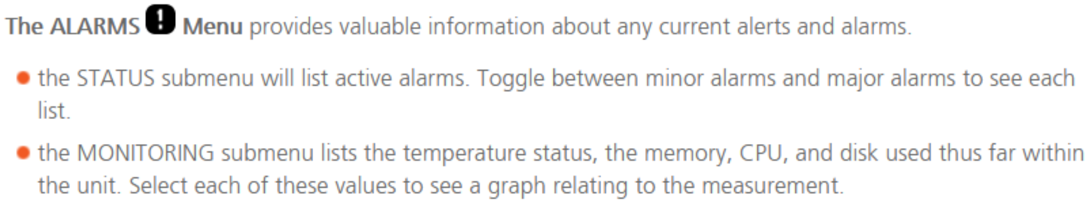
During boot-up (power-up or reboot), or after a clean, the displays are initially all blank. After a few moments, the LED display goes to all 0's for several seconds. Then, it displays the time read from the RTC (which should be fairly accurate). Then later, the LCD will start displaying data, also (unless the front panel is configured for "None" in the front panel "Display Content" field).

- The front panel time display, like other outputs such as IRIG and ASCII, will initially output the default year 2000 and the time as 00:00:00 (incrementing each second) for about the first minute or so after power -up. Then the time/date is applied.
- For more details, refer to: System initialization after each boot-up in this document

Status LEDs (Power, Sync and Fault) on 1200 SecureSyncs not present on 2400 SecureSyncs

1200 SecureSyncs (Power Sync Fault)

2400 SecureSyncs


The ALARMS ❗ Menu provides valuable information about any current alerts and alarms.

- the STATUS submenu will list active alarms. Toggle between minor alarms and major alarms to see each list.
- the MONITORING submenu lists the temperature status, the memory, CPU, and disk used thus far within the unit. Select each of these values to see a graph relating to the measurement.

API calls associated with Front panel display

(Note: this info is from 1200 SecureSyncs)

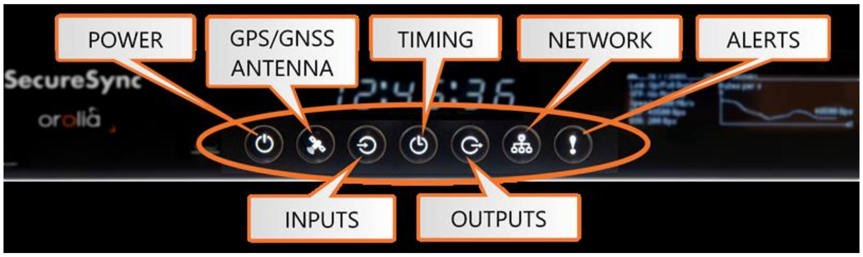
- Refer to Tim Tetreault's "cheat sheet" at: ..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\Timing boards\TSync family\Tsync driver calls cheat sheet
- These are examples - additional calls may have since been added

Front panel display commands
DP_GetFormat
DP_GetLocal
DP_GetNumInst
DP_GetTimeScale
DP_SetFormat
DP_SetLocal
DP_SetTimeScale

LED CONTROL Commands
EC_GetMode
EC_GetState
EC_SetMode
EC_SetState

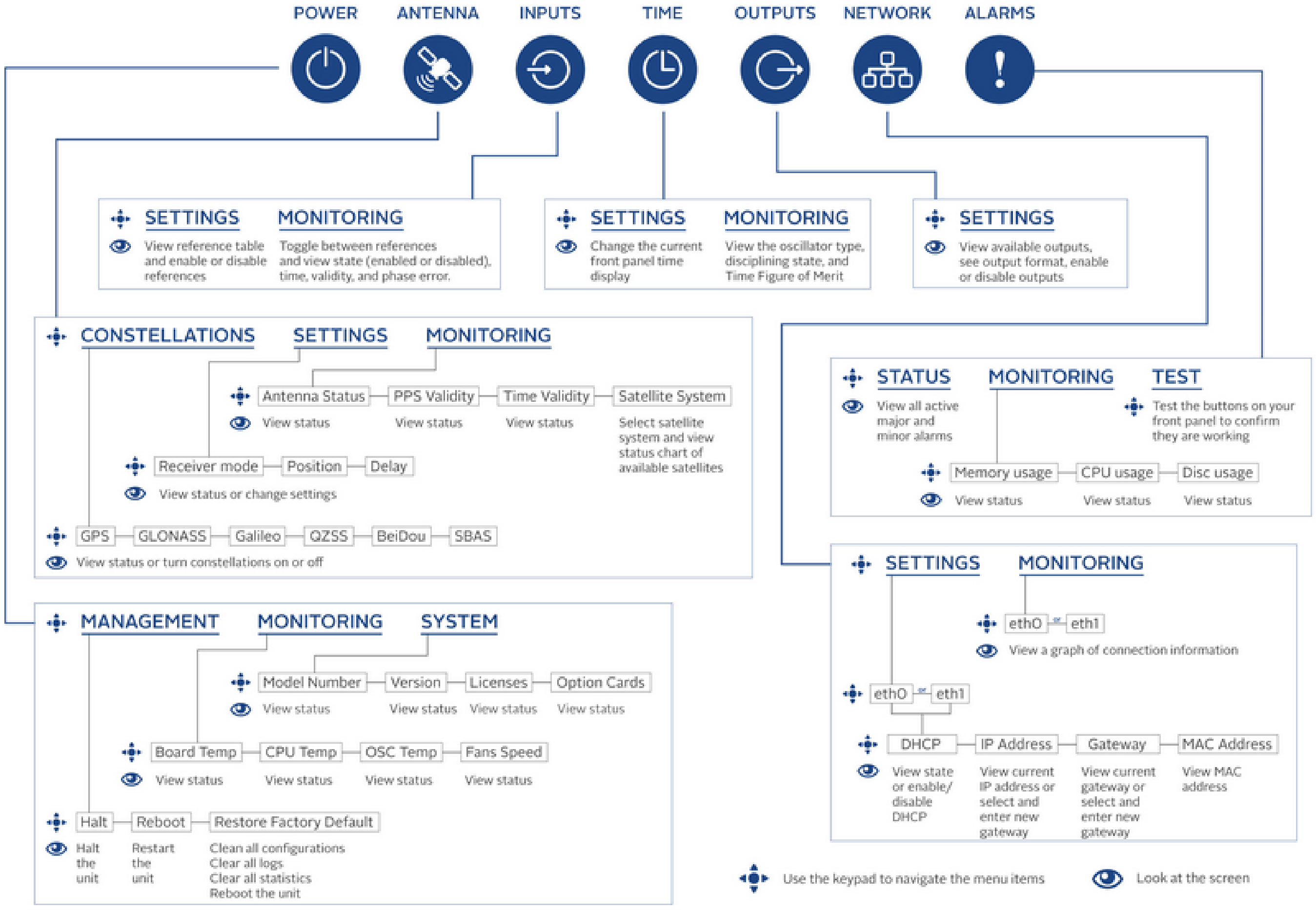
OLED/keypad

- Refer to online 2400 User guide at http://manuals.spectracom.com/2400/Content/NC_and_SS/2400/INTRO/Keypad_Usage.htm
- Buttons perform the same functions as the VersaSync indicators



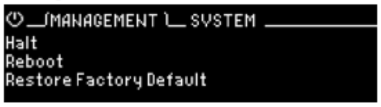
Front Panel Display: Menu Tree

The illustration below shows how the menu is organized, and which functions can be accessed via the front panel (i.e. without using the Web UI):


POWER
ANTENNA
INPUTS
TIME
OUTPUTS
NETWORK
ALARMS
SETTINGS
View reference table and enable or disable references
MONITORING
Toggle between references and view state (enabled or disabled), time, validity, and phase error.
SETTINGS
Change the current front panel time display
MONITORING
View the oscillator type, disciplining state, and Time Figure of Merit
SETTINGS
View available outputs, see output format, enable or disable outputs
CONSTELLATIONS
SETTINGS
MONITORING
Antenna Status
PPS Validity
Time Validity
Satellite System
View status
View status
View status
Select satellite system and view status chart of available satellites
Receiver mode
Position
Delay
View status or change settings
GPS
GLONASS
Galileo
QZSS
BeiDou
SBAS
View status or turn constellations on or off
STATUS
View all active major and minor alarms
MONITORING
TEST
Test the buttons on your front panel to confirm they are working
Memory usage
CPU usage
Disc usage
View status
View status
View status
MANAGEMENT
MONITORING
SYSTEM
Model Number
Version
Licenses
Option Cards
View status
View status
View status
View status
Board Temp
CPU Temp
OSC Temp
Fans Speed
View status
View status
View status
View status
Halt
Reboot
Restore Factory Default
Halt the unit
Restart the unit
Clean all configurations
Clear all logs
Clear all statistics
Reboot the unit
SETTINGS
MONITORING
eth0
or
eth1
View a graph of connection information
eth0
or
eth1
DHCP
IP Address
Gateway
MAC Address
View state or enable/ disable DHCP
View current IP address or select and enter new gateway
View current gateway or select and enter new gateway
View MAC address
Use the keypad to navigate the menu items
Look at the screen

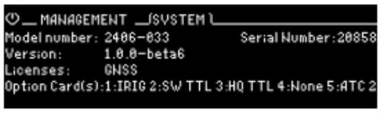
A) POWER Menu

- Management



```
Halt
Reboot
Restore Factory Default
```

  - halt
  - reboot
  - restore factory defaults
- System

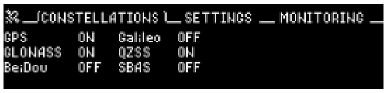


```
Model number: 2406-033          Serial Number:20858
Version:      1.0.0-beta6
Licenses:     GNSS
Option Card(s):1:IRIG 2:SW TTL 3:HQ TTL 4:None 5:ATC 2
```

  - view model number
  - view serial number
  - view software version
  - view licenses
  - view option cards installed

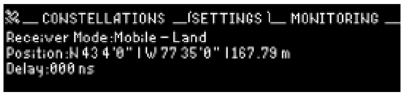
B) GNSS ANTENNA Menu (Constellations, Settings, Monitoring antnenna status, validity)

- Constellations



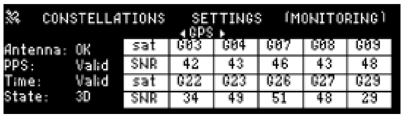
```
GPS       ON    Galileo  OFF
GLONASS   ON    QZSS     ON
BeiDou    OFF   SBAS     OFF
```

  - view power status for GPS, GLONASS, BeiDou, Galileo, QNSS, and SB
  - turn reception OFF or ON to any satellite system by selecting the stat
- Settings



```
Receiver Mode:Mobile - Land
Position:N 43 4'0" | W 77 35'0" |167.79 m
Delay:000 ns
```

  - view or change receiver position mode
  - view or set position
  - view or change delay
- Monitoring



```
Antenna:  OK
PPS:      Valid
Time:     Valid
State:    3D
```

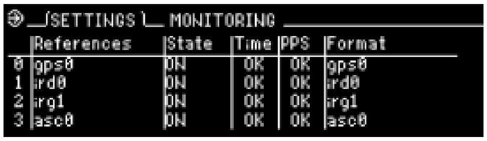
sat	G03	G04	G07	G08	G09
SNR	42	43	46	43	48
sat	G22	G23	G26	G27	G29
SNR	34	49	51	48	29

  - view antenna status
  - view for each satellite system:
    - chart of all visable satellites
    - PPS validity
    - time validity

C) INPUTS Menu

Inputs Menu:

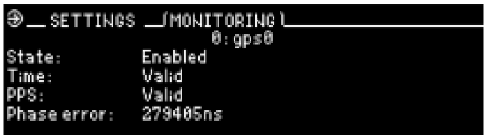
- Settings



```
  SETTINGS   MONITORING
   References      State  Time PPS  Format
 0 gps0            ON      OK   OK  gps0
 1 ird0            ON      OK   OK  ird0
 2 irg1            ON      OK   OK  irg1
 3 asc0            ON      OK   OK  asc0
```

  - view reference table
  - enable or disable references

- Monitoring

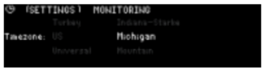


```
  SETTINGS   MONITORING
                 0: gps0
State:         Enabled
Time:          Valid
PPS:           Valid
Phase error:   279405ns
```

  - view each input reference
  - view reference state, time, validity, and phase error

D) TIME Menu (Settings, Monitoring -Osc type, disc state, TFOM)

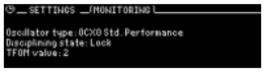
- Settings:



```
  SETTINGS   MONITORING
           Turkey      Indiana-Starke
Timezone:  US          Michigan
           Universal   Mountain
```

change the current time display

- Monitoring:

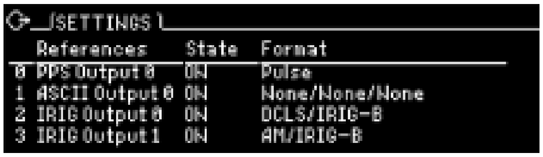


```
  SETTINGS   MONITORING

Oscillator type: OCXO Std. Performance
Disciplining state: Lock
TFOM value: 2
```

view the oscillator type, disciplining state, and TFOM value

E) OUTPUTS Menu

- Settings

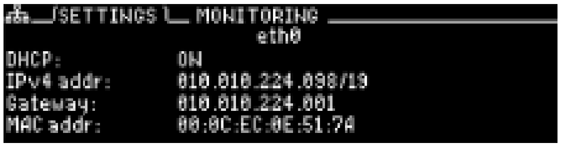


```
  SETTINGS
   References      State   Format
 0 PPS Output 0    ON      Pulse
 1 ASCII Output 0  ON      None/None/None
 2 IRIG Output 0   ON      DCLS/IRIG-B
 3 IRIG Output 1   ON      AM/IRIG-B
```

  - view list of outputs available
  - see and change outputs format
  - enable or disable outputs

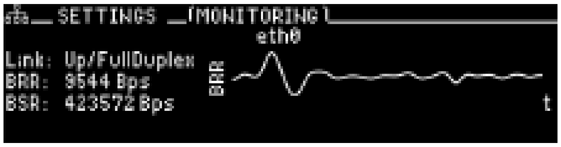
F) NETWORK Menu

- Settings: For each ETH connection:



```
SETTINGS  MONITORING
                 eth0
DHCP:          ON
IPv4 addr:     010.010.224.098/19
Gateway:       010.010.224.001
MAC addr:      00:0C:EC:0E:51:7A
```

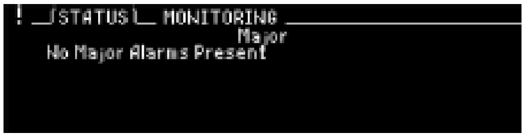
  - enable or disable DHCP
  - view or set IP address
  - view or change gateway
  - view MAC address
- Monitoring: View a graph for each ETH connection



```
SETTINGS  MONITORING
                 eth0
Link:  Up/FullDuplex
BRR:  9544 Bps
BSR:  423572 Bps
```

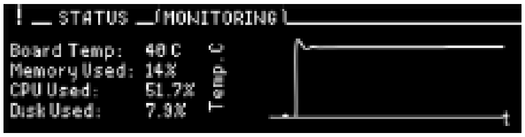
G) ALERTS Menu (Status, Monitoring, Test)

- Status



```
! STATUS  MONITORING
                    Major
   No Major Alarms Present
```

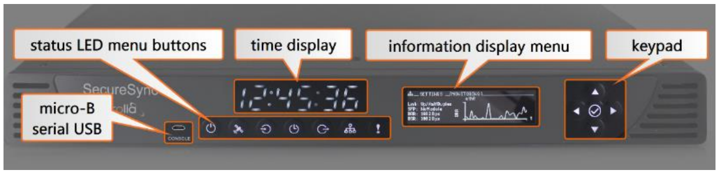
  - show current major or minor alarms and descriptions
- Monitoring



```
! STATUS  MONITORING
Board Temp:    40 C
Memory Used:  14%
CPU Used:      51.7%
Disk Used:     7.9%
```

  - view board temperature and graph
  - monitor memory and view graph
  - monitor CPU and view graph
  - monitor disk used and view graph

***Configure front panel time display for local time *(Management* -> *Front Panel*)



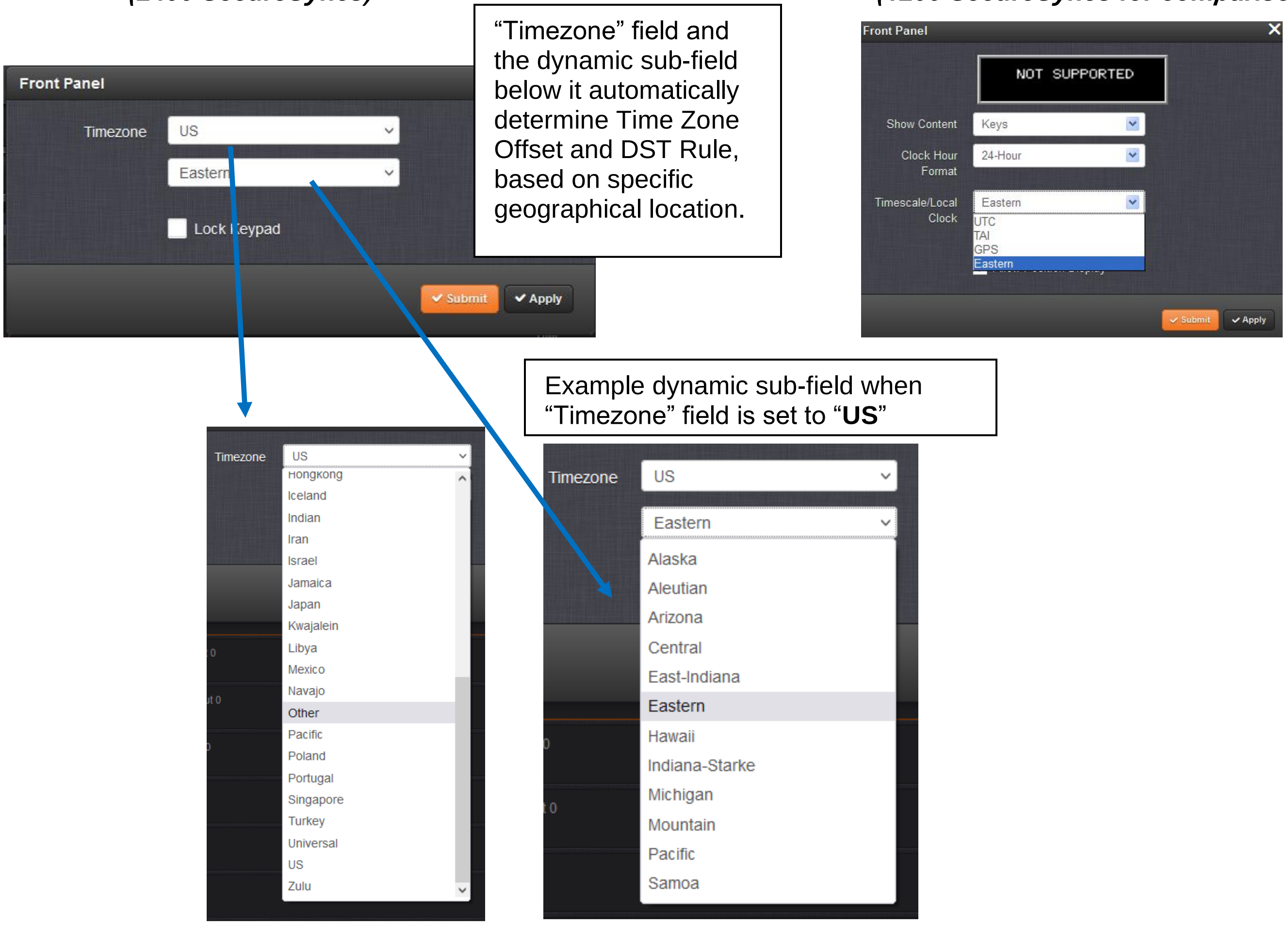
Note: As of at least v1.4.1 and below, and unlike 1200 SecureSyncs, Local Clocks (*Time Management* page) are not used for front panel configuration. Instead, two fields in the *Front Panel* page are used to configure a particular geographical location. A database in the background (refer to: https://www.iana.org/time-zones) then determines/applies to the front panel time display the applicable Time Zone Offset and DST rules for that location.

Note (as also mentioned further below): As of at least v1.4.1 and below, and unlike 1200 SecureSyncs, the browser doesn't display Local Time, whether or not the front panel is displaying local time.

A) web browser

Mangement -> *Front Panel* page

(2400 SecureSyncs) ***(1200 SecureSyncs for comparison)***



"Timezone" field and the dynamic sub-field below it automatically determine Time Zone Offset and DST Rule, based on specific geographical location.

Example dynamic sub-field when "Timezone" field is set to "**US**"

Front Panel

Timezone: US

Eastern

☐ Lock Keypad

Front Panel (1200)

NOT SUPPORTED

Show Content: Keys

Clock Hour Format: 24-Hour

Timescale/Local Clock: Eastern

- Refer to "**Configuring the Front Panel**" in the online 2400 SecureSync user guide at: https://www.orolia.com/manuals/2400/Content/NC_and_SS/2400/INSTALL/Front_Panel_Config.htm (excerpt below)

To change the time display on the front panel:

1. Log on to the Web UI
2. Navigate to ***MANAGEMENT*** > ***Front Panel.***
3. Select your general region, and the specific time zone. The listed time regions and zones are based on the zones found here.
4. Click Submit

Changing this time display does not affect any internal clocks or create a local clock within the system.

****Local Time display in the web browser

- Refer to Salesforce Case **285179** / JIRA DMND-1794
- Apparently, in at least versions 1.6.0. and below, there is no way to get a local time display in the browser (unlike in the 1200 SecureSyncs):
  - Local Clocks (***Management*** -> ***Time Management*** page) don’t apply to the Front panel time display (like it does in 1200 SecureSyncs). Local Clocks are for use with interfaces such as Option Cards for instance.
  - ***Management*** -> ***Front panel*** page has two fields which determine what local time should be.
  - **These fields do not apply to the web browser time display-** only to the front panel display. Even though the front panel is showing local time, the browser will continue showing UTC time ONLY.

Show content field

- Not present in in 2400 SecureSyncs

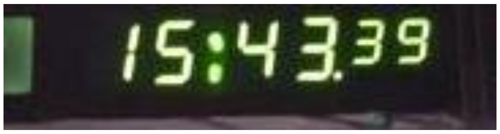
Q (from Hughes 2400 demo) Management-Front panel screen not showing front panel display. Following front panel display on UI on the new unit: Older units shows additional information:

A (per Dave Sohn May 2021) The front panel on the 2400 went through a large redesign in comparison to the 1200. This included removal of the constant content display, which is configured via the “Show Content” selection. As the constant content display was removed from the front panel functionality it was also removed from the web user interface area. This information is already available in various other areas of the user interface, so this is unlikely to be duplicated in the front panel configuration interface

This is different than the 1200 but is it acceptable to Hughes?

Two different decimal points in front panel LED time display (when it’s configured to display local time)

(Note: this info is from 1200 SecureSyncs)



- **DST indicator:** The decimal point to the **right of the minutes** indicates the front panel clock is showing a Local Clock time AND Daylight Savings Time in in affect. This is a Daylight Savings Time indicator.
- **PM indicator:** The decimal point to the right of the Hours portion of the clock display means the front panel is showing a Local Clock time in 12 hour mode AND the time is PM. When the time transitions to AM the decimal point will extinguish.

Q I have noted since installation of release 5.8.0 a new LED symbol illuminates after the SecureSync is up and running. Note the separator decimal point lower right of the minutes digit lit. I contacted Dave Lorah at Spectracom and he noticed this as well on his rack. A search of the manual does not reveal any answers.

A reply from Dave L (4 Jun 18) I have found the decimal point to the right of the minutes characters in the clock display indicates the front panel clock is showing a Local Clock time AND Daylight Savings Time in in affect. This is a Daylight Savings Time indicator.

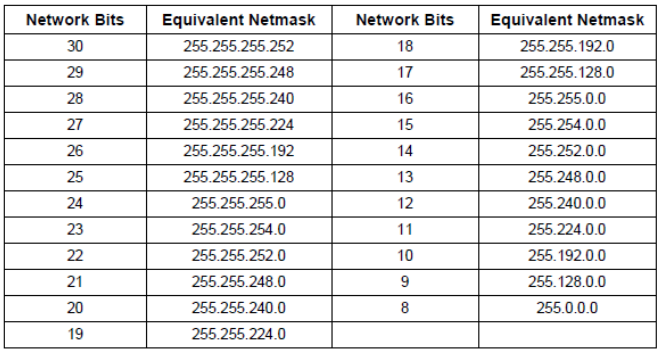
When we transition out of Daylight Savings Time in November the decimal point will extinguish.

The decimal point to the right of the Hours portion of the clock display means the front panel is showing a Local Clock time in 12 hour mode AND the time is PM. When the time transitions to AM the decimal point will extinguish.

I was able to locate this information in our online User Manual. So this will be included in the next pdf revision of the manual

Note: With Timescale configured as “Local” and during DST (Daylight Saving Time, as configured in the Local Clock), a “DST indicator” (decimal point) will be displayed to the bottom-right of the minutes portion of the LED time display. The “DST indicator” extinguishes during “Standard” time. If the Local Clock is configured as “No DST/Always Standard Time”, the DST indicator won’t ever be lit.

***Configure/display network settings using the front panel keypad/LCD



Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
30	255.255.255.252	18	255.255.192.0
29	255.255.255.248	17	255.255.128.0
28	255.255.255.240	16	255.255.0.0
27	255.255.255.224	15	255.254.0.0
26	255.255.255.192	14	255.252.0.0
25	255.255.255.128	13	255.248.0.0
24	255.255.255.0	12	255.240.0.0
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		

Table 3-3: Subnet mask values

**Front panel keypad lock/unlock

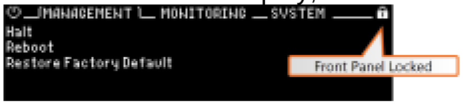
- ➢ Refer to the online Model 2400 user guide at: https://www.orolia.com/manuals/2400/Content/NC_and_SS/2400/INSTALL/Front_Panel_Config.htm

Excerpt below from the user guide

To lock or unlock the front panel:

1. Log on to the Web UI
2. Navigate to MANAGEMENT > Front Panel.
3. Check the box next to Lock Front Panel to lock. To unlock, verify that the box is unchecked.
4. Click Submit

The front panel information display will lock at the last viewed screen. A small padlock icon will appear in the upper right hand corner of the display, and will flash brighter if any buttons are pressed on the front panel.



Locked Front Panel Display

The front panel will remain locked until it is unlocked through the Web UI or via CLI commands.
To lock or unlock the front panel via the CLI, use the **fp_lock** and **fp_unlock** commands (admin access is required).

Indication on the front panel that the front panel is locked

Hi Dan, Will and Ryan, I am so sorry for the false alarm on the front panel not responding after the update. I forgot until just now (checking all configs remained the same upon completion of update) that I had selected the front panel lock button, while also setting it to local time 🙁 I can…
Q (from Ron Dries) I s there a way on the front panel to see that it is locked? If not it may be a good future nice to have feature.
A. (per Will Comly, engineer 14 Sept 2022) Yes, when locked, a lock icon appears in the upper right hand corner of the OLED and flashes when you attempt to press a button

Desire for more secure locking mechanism (carry over from 1200s)

Q This brings a security problem as anybody can force the unit manually though the keypad and modify the network properties for example…

A Per Dave S (1 Jun 17) The keypad lockout is to prevent accidental and casual changes using the front panel. Our view is that the customer is responsible for physical security.

Front panel FAQs

Q Does the front panel have any sort of security/protection such as entry of credentials or password to gain access to certain functions?

A. The front panel does not utilize credentials or password. The keypad can be locked, but can be unlocked via the web UI or CLI

Q Is the GPS lock status displayed on the front panel? Is it possible to determine whether or not the GPS receiver is operating in SAASM mode via the front panel (specifically, indication of using PPS versus SPS)?

A GPS status can be displayed on the front panel. It will display PPS vs SPS mode.

**Front panel status LEDs/ (AC and DC power monitoring)

Status/Power page of the web browser

POWER LED flash pattern

the Power LED will indicate status of input power

If the Power Indication is Off: Both AC and DC Input Power are disconnected. Or, SecureSync's AC input switch is turned off and DC input is not present.

If the Power Indication is Green, but blinking Orange once per second; Indicates power error condition; general power configuration fault.

- GREEN w/ ORANGE BLINKING: Power fault; Power inputs don't match configuration
- ORANGE SOLID – DC ONLY – DC only power detected; AC & DC supported
- ORANGE SOLID – AC ONLY – AC only power detected; AC & DC supported
- GREEN SOLID: All configured power is present

Note: Green/amber flashing indicates the SecureSync was not originally programmed as the correct Model type during the manufacturing process (indicates configuration issue).

Email from Dave Sohn (3/16/12)
If the SecureSync is setup for dual power (AC / DC power) with firmware **version 4.8.2** or higher, the power LED only flashes orange if the unit isn't configured properly. If there is a failure on a power supply, the power LED will be solid orange.

Email Keith sent to a customer (2 Jan 2013) - I saw your email to Jeremy regarding the blinking orange Power LED on the SecureSync and have some information for you that I hope will help!

FYI- During the manufacturing process, the SecureSync is programmed with its particular input power configuration (such as AC only, or AC and DC input, for examples). This particular SecureSync was likely inadvertently programmed with the incorrect power configuration, resulting in the blinking orange that you are observing. When programmed correctly and with an input power not applied, the LED will be solid orange, instead of blinking orange. Blinking orange only occurs if the power configuration isn't programmed correctly.

In archive versions prior to version 4.8.2 (as reported in the **Tools** - > **Versions** page of the browser), there were no alarms associated with input power being present or not present. So even if the SecureSync happened to be programmed incorrectly, there was no visible indicator for this condition. However, if a SecureSync is updated to a version of 4.8.2 or higher, since version 4.8.2 adds an indication of lost power via the Power LED, an incorrect programming will then become apparent.

This blinking power LED does not affect the operation of the SecureSync. If this is a demo SecureSync that you currently have, thanks for bringing this to our attention. We will fix it when its returned to us. However, if this is a SecureSync you have already purchased, please let me know. if you can connect the SecureSync to the internet, outside of a firewall, and provide us with the IP address (and enable all Services) we can reprogram it remotely for you, to resolve this issue. If it can't be temporarily placed on the Internet, we can also assign an RMA Number for it to be returned for a reprogramming. Or, we may be able to work with our engineering team to provide you with a special upgrade file that can also reprogram it in the background.

***Ability to mask/override the Power LED/Power alarm (if backup power is not connected)

(5 Apr 2013 KW) Currently (as of at least versions 5.6.0 and below), there is no way to mask/override the Power LED alarm pattern if SecureSync has both AC and DC input configuration, but only one power source is connected.

- Refer to Salesforce case 9038 and Mantis case 1983.

Available work-around to inherently clear this alarm condition (if AC is supplied and no DC power is applied)

- Purchase from us and connect the available external AC to DC converter (Our P/N "PS06-2Z1M-DT01") to the DC connector on the back of the SecureSync (thereby applying power to both connectors).
- Refer to (in this document) "PS06-2Z1M-DT01" for more info on this available power adapter.

Q On some GPS-CLock, we did not connect the DC Power, on the GPS-CLock, the DC Power appears in red and monitoring system generates an alarm. Is there a way to configure the Spectracom GPS-Clock to inform it that the DC Power is simply not plugged in (look like a check box)? Currently we have an unjustified alarm and we don't want to handle exceptions.

A reply from Keith (2 Feb 17) There is no way to clear/mask the DC power alarm with a SecureSync having either of the two input power connections not having power applied.

However, if a customer purchased a unit with both AC and DC input, but isn't planning on applying DC input power, we offer an available AC to DC converter, that can act as a redundant AC input (and thereby inherently clearing the Power alarm indication, when its connected). This external AC to DC converter has a DC connector that mates with the DC connector on the back of the time server, for convenience (as shown below). Our P/N for this available adapter is PS06-2Z1M-DT01:

Sync LED

If the Sync Indication is **Red**; Time Sync alarm. 1) SecureSync has powered up and has not yet achieved synchronization with its inputs. 2) SecureSync was synchronized to its selected input references, but has since lost all available inputs (or the inputs were declared invalid) and the Holdover period has since expired.

If the Sync Indication is **Green**; SecureSync has valid time and 1PPS reference inputs present and is synchronized to its reference.

If the Sync Indication is **Orange**; In Holdover mode. SecureSync was synchronized to its selected input references, but has since lost all available inputs (or the inputs are not declared valid). SecureSync's outputs will remain useable until at least the Holdover period expires.

Fault LED

If the Fault Indication is **Blinking orange**; GPS antenna problem alarm has been asserted and is currently active. A short or open has been detected in the GPS antenna cable. The light will automatically turn off when the alarm condition clears

If the Fault Indication is **Solid orange**; A Minor alarm condition (other than an antenna problem alarm) has been asserted and is currently active

If the Fault Indication is **Red**; A Major alarm condition has been asserted and is currently active

Known Issues/Conditions with front panel LCD/ LED time display

A) (Oct/Nov 2014) LED time display is frozen. Seconds not incrementing

- Communications (HTTPS, SSH, etc) may be sluggish as a factor of KTS not responding.
- Indicates KTS (Timing System) is frozen/locked-up.

- Network processor software likely still OK.
- Likely due to loss of/glitch in 10MHz OCXO oscillator output adversely affecting the FPGA.

Refer to "**LED time not counting up. LCD is fine (OCXO glitching causes lockup**)" in the oscillator section of this document (Mantis case 2916)

- Review System log for KTS failed to read log entries (examples below). In versions 5.2.1 and above also look for "possible oscillator error" or "probably FPGA Failure" entries. These are associated with 10 MHz glitching issue mentioned above.

```
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true GR_GetMfrMdl 0 0 (KTSAL)
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetState 0 (KTSAL)
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetOscType 0 (KTSAL)
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetSerialNo 0 (KTSAL)
```

- Bring back for oscillator evaluation.

B) Front panel LCD window and Time display intensity matching (one unit compared to another)

Notice: The LCD protective film issue described further below only applies to the LCD window display. If the LCD window AND the Time display are at a different intensity than another unit, the issue further below does not apply.

Differences with both the LCD and Time display as compared to other units are due to tolerances in electronic components and the front panel filter.

Below is a (now modified) email Keith sent to Mark Day in the UK about this (may need to be edited before sending to anyone else)

Initially, there is a protective film on the front panel components that needs to be removed before the front panel assembly is placed in the front panel portion of the chassis. The intensity difference between two units may likely be due to this film inadvertently not being removed from one of the two units (one has this film removed and the other unit has the film still applied –resulting in one display being darker in appearance than the other.

To begin, the display intensities are not adjustable and we don't perform any side-by-side intensity matching of the front panel displays. However, typically the display intensity from one SecureSync to another is fairly similar. Any intensity differences between them are normally limited to tolerances of the electronic components (such as the intensity setting resistors) and the filtering of the front panel overlay.

Your customer can either remove the cover and the power supply that inhibits the front panel assembly from being removed, to see if the film is still applied to these components (if the film is still applied to one of the two, the bottom unit in the picture appears to be the one with the film still applied). OR, they can send the SecureSyncs back to us for evaluation.

C) Front panel LCD protective film still installed when unit is received

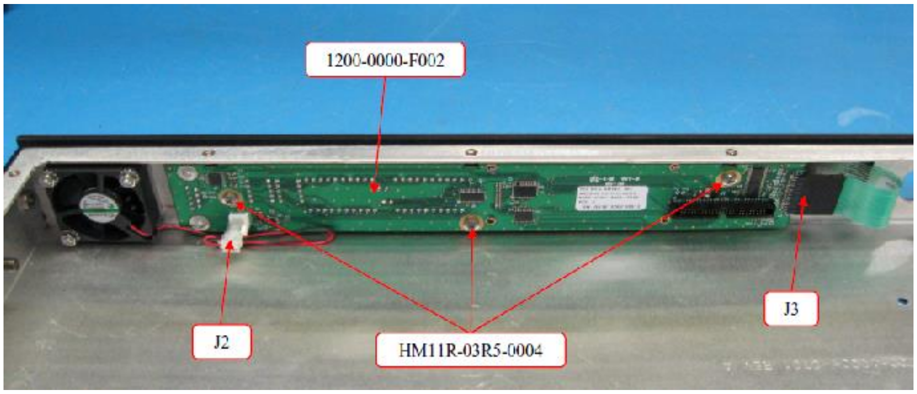
Email from Dave Lorah to customer (6/12/12)

We apologize for the problem with your new SecureSync unit. This has been recorded and preventive action is being addressed by our QA department.

Fortunately this can be easily fixed in the field. The front panel assembly will need to be detached from the Cd and chassis. All you need is a medium Phillips screwdriver.

Here is what to do:

1) Remove the 20 screws from the top cover and remove the cover.
2) Remove the fan connection shown as (J2) below.
3) Remove the three screws attaching the front panel PCB to the chassis. You may not need to remove the J3 or ribbon cable to get to the film.
4) The protective film on the LCD Display will peel off easily.
5) Reassembly is the reverse of disassembly.



If you have any questions or need assistance, please let me know.

D) LCD display dark after booting-up a cold unit (cold LCDs)

Email from Sylvain to Dave Sohn We recently made a experimentation outside on site and I had a little issue on SecureSync that I would like to share with you :

This was in the early morning, it was cold outside and the unit has spent the night in the back side of our car.
At the first starting up time, I couldn't see the front panel display working normally : LCD remaining Black and LEDs Power Green only (others OFF) – I just could see the clock display keeping running then taking the RTC time after more than a minute. Then nothing else.
After a second reboot (power OFF action): the SecureSync started as well.

My question is: as the firmware + software of my Securesync doesn't include the last BIOS configuration changing the threshold parameters for temperature limits, can it be corrected by this setting ?
I assume it is not link to the high temperature this time but in cold status context….

Reply from Dave Sohn (18 Mar 16) LCDs at cold temperature may be blank and sluggish for updates. If the time display was running, LEDs were lit, and the time was updated from the RTC then I would say the SecureSync was running. When we do our tests that is what we see, but the LCD comes back after it warms up.

A) LED time not counting up. LCD is fine (OCXO glitching causes lockup)

B) Only the Power LED is lit (LED time is NOT displayed and nothing is displayed in LCD either)

1. Issue with the oscillator/10 MHz into KTS Timing System

(email from Dave Lorah to a customer, 23 Jun 16) If the clock is not working then I believe the oscillator has failed. That is the symptom of a failed oscillator, just the power LED and nothing else on the front panel.

- Refer to Salesforce case 21277 (Google saw this on a very-early RB-based SecureSync)
- Only indicator on the front panel was the power LED (even after reboot).

C) Front panel keypad not responsive

- Keypad may be locked. Try unlocking it via either the web browser or from the front panel using the unlock sequence.

- If the front panel isn’t locked, try power cycling the time server. May need to be returned due to issue related to the ETX or could be a software issue.
- This one isn’t related to the 10MHz oscillator (which can affect the LED time display).

**out-of-band management (front panel micro USB/rear panel console Setup port

Out of band management

From Wikipedia (https://en.wikipedia.org/wiki/Out-of-band_management) In computer networks, **out-of-band management** involves the use of a dedicated channel for managing network devices. This allows the network operator to establish trust boundaries in accessing the management function to apply it to network resources. It also can be used to ensure management connectivity (including the ability to determine the status of any network component) independent of the status of other *in-band* network components.

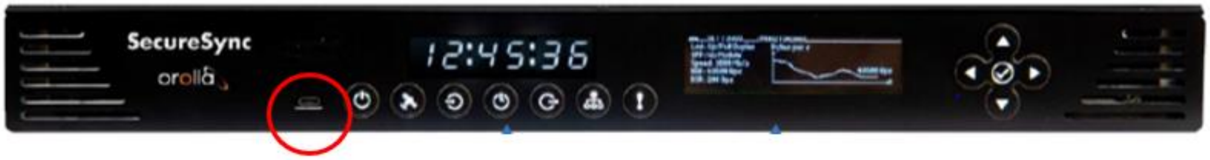
- ➢ SecureSync provides the front panel (micro USB) and rear panel (DB9F) RS-232 Serial port for serial/terminal server connections to the CLI interface (see below for more info)

Two available "Serial Console" connectors for 2400s (one on front panel and one on rear panel)

DB9 port: Unlike 1200 SecureSyncs, 2400 SecureSyncs do not have a DB9 connector on front or rear panel

A) FRONT panel micro USB port/Terminal server connection

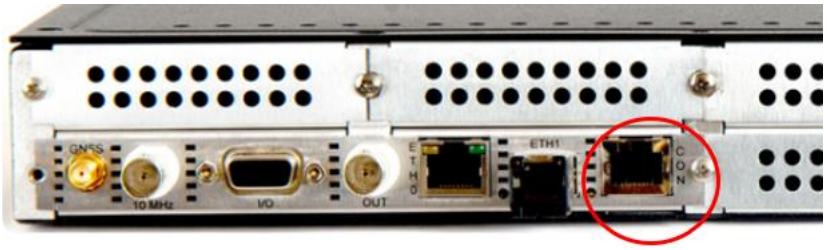
The 2400 front panel connector is **now a micro USB connection (no longer a DB9F connector on front panel as it is on 1200 SecureSyncs)**.



- **Connector**: micro-B USB (requires installed driver; if your driver does not automatically install, visit: https://www.ftdichip.com/Drivers/VCP.htm)
- **Character structure**: ASCII, 115200 baud, 1 start, 8 data, 1 stop, no parity

- ➢ This front panel Serial port is password protected (must login).
- ➢ Refer to CLI section directly below for info on commands
- ➢ Login user names and passwords are same as used to login to the web browser

B) REAR panel RJ-45 Terminal server connection (Labeled "CON")



Refer to the Model 2400 user guide at https://www.orolia.com/manuals/2400/Content/NC_and_SS/2400/INTRO/Rear_Panel.htm

Note: This rear panel is **similar to the DB9F connector on the front of the 1200 SecureSyncs**

- The rear Serial Console accepts serial commands to locally configure the unit via CLI.
- The RJ45 serial port on the rear of the 2400 is **designed to work with a standard Cisco console cable**
- This Rear panel Serial "**CON**" port is password protected (must login).
- Refer to CLI section directly below for info on commands.
- Login user names and passwords are same as used to login to the web browser.

Interface Serial port with a Terminal Server/Cisco router's ASYNC/Console port (DTE device)

Note this info from 1200 SecureSyncs

- Refer to SR 5457
- Refer to http://www.cisco.com/c/en/us/support/docs/dial-access/asynchronous-connections/5466-comm-server.html and http://www.cisco.com/c/en/us/support/docs/routers/1600-series-routers/46789-port-pinout.html

Settings
9600, 8 bit, 1 stop bit, no parity, flow control off (must disable hand-shaking on their end)

6 foot DB-9 to RJ45 Serial Console Cable

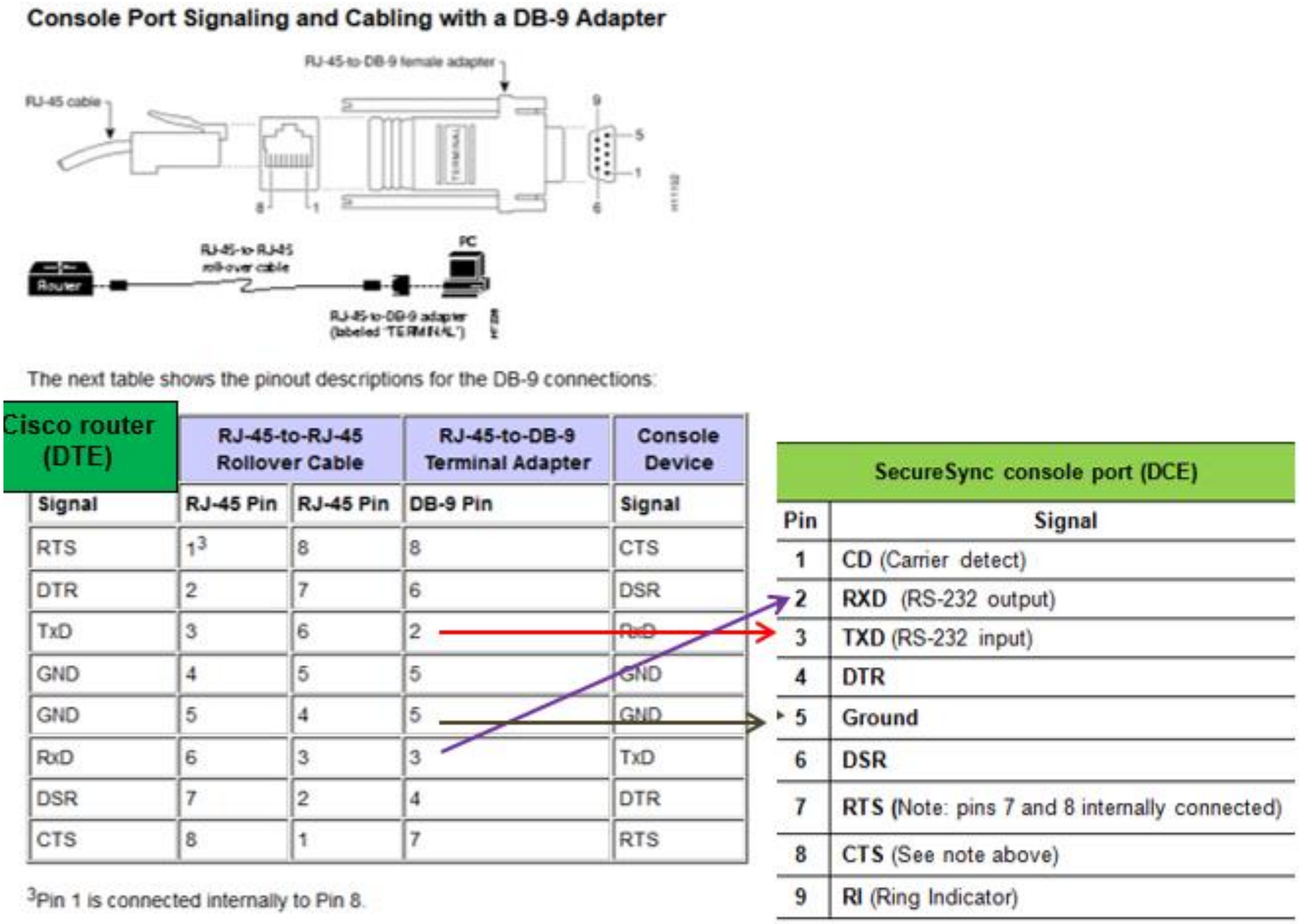
- Cisco Compatible DB9 to RJ45 Console Cable, 6ft
- **Our P/N** CA21R-D945-0001 (in Arena) https://app.bom.com/items/detail-spec?item_id=1270476743&version_id=11397430388

Cable Pin-out

Notes

- When using an RJ-45 to DB9M, pins 2 and 3 need to be reversed on one of the DB9 cable (as shown below)
- On our end, we only care about pins 2, 3 and 5

From: http://www.cisco.com/c/en/us/support/docs/routers/1600-series-routers/46789-port-pinout.html#db9


RJ-45 cable
RJ-45-to-DB-9 female adapter
9
5
1
6
8
1
TERMINAL
Router
RJ-45-to-RJ-45 roll-over cable
PC
RJ-45-to-DB-9 adapter (labeled "TERMINAL")

Console Port Signaling and Cabling with a DB-9 Adapter

The next table shows the pinout descriptions for the DB-9 connections:

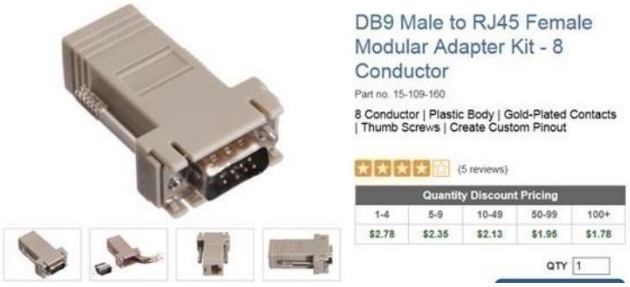
Cisco router (DTE)	RJ-45-to-RJ-45 Rollover Cable		RJ-45-to-DB-9 Terminal Adapter	Console Device
Signal	RJ-45 Pin	RJ-45 Pin	DB-9 Pin	Signal
RTS	1[3]	8	8	CTS
DTR	2	7	6	DSR
TxD	3	6	2	RxD
GND	4	5	5	GND
GND	5	4	5	GND
RxD	6	3	3	TxD
DSR	7	2	4	DTR
CTS	8	1	7	RTS

[3] Pin 1 is connected internally to Pin 8.

SecureSync console port (DCE)	
Pin	Signal
1	CD (Carrier detect)
2	RXD (RS-232 output)
3	TXD (RS-232 input)
4	DTR
5	Ground
6	DSR
7	RTS (Note: pins 7 and 8 internally connected)
8	CTS (See note above)
9	RI (Ring Indicator)

Example RJ-45 to DB9 converter

- Refer to: http://www.showmecables.com/product/DB9-Male-RJ45-Female-Modular-Adapter-Kit.aspx?utm_source=google&utm_medium=cse&utm_campaign=15-109-160&gclid=Cj0KEQjwnIm7BRDSs42KxLS8-6YBEiQAfDWP6JQVqlbSm2rD5plReLTI5IMD4gU4B5UbDeLofAMQ8cIaAul_8P8HAQ


DB9 Male to RJ45 Female Modular Adapter Kit - 8 Conductor

Part no. 15-109-160

8 Conductor | Plastic Body | Gold-Plated Contacts | Thumb Screws | Create Custom Pinout

★★★★☆ (5 reviews)

Quantity Discount Pricing				
1-4	5-9	10-49	50-99	100+
$2.78	$2.35	$2.13	$1.95	$1.78

QTY 1

CLI (Command Line Interface)

- Our CLI is proprietary. Spectracom created it specifically for our application.
- Type Helpcli or clihelp for list and descriptions of the available CLI commands.

Notes:

1) Type **Q** to exit help.
2) Typing **help cli** or **cli help** (two words instead of one) will respond with "**permission denied**"
3) Commands and API calls are cap letter sensitive. Typing any character in the wrong case will cause the command to respond with "**command not found**".

Hint: to highlight desired letters or words

1) Press the " **/** " key.
2) Type the letters or word to highlight and press enter.

"vi" text file viewer/editor

- Refer to: https://www.cs.colostate.edu/helpdocs/vi.html

Example to edit a file: Type **vi /etc/sysconfig/network-scripts/ifcfg-eth0**

To exit vi:

First press *shift* + *colon* (**:**) to move to the bottom of the file. Then either…

To save and exit type **x** <enter> after the colon
To exit without save (quit) type **q!** <enter> after the colon

Press *shift* and Type **visual** to edit the file again.

GNU Bash

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

Alternate interface to using the limited CLI commands

- Refer to the REST API section of this doc: ****secure REST API

**Security with the CLI interface (Ability to connect out using FTP, SCP/SFTP, etc)

Q. We recently purchased two SecureSync NTP appliances. How locked down is the default user account when they log into the cli? (The product appears to be running on Linux.)

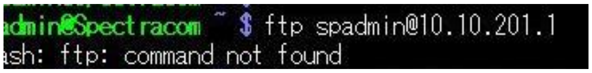
A. From Sam Otto (11 Jul 2013) The user cannot change configuration files or run most executables. Users must use Spectracom Web UI or CLI commands to configure the system.

To prevent any modifications from the CLI both the Telnet Service and SSH Service can be disabled via Network Services / Network Setup / Services and submitting, refer to the following Picture.

Security concerns with the Model 1204-06 Option Card installed (FTP/SFTP out for instance)

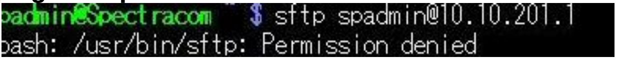
- Due to security concerns across Ethernet ports, **version 5.1.2** disabled user-level permissions from being able to perform services such as telnet, ssh, FTP and sftp/scp from the command line interface.
- Can still SCP into the SecureSync. This change prevents scp'ing out from the box.
- Can still ping out from within the SecureSync.
- Refer to Salesforce case 13444 and Mantis 2757 for an SCP issue this changed ended up causing

Trying to FTP from the CLI



```
dmin@Spectracom ~ $ ftp spadmin@10.10.201.1
ash: ftp: command not found
```

Trying to sftp from the CLI



```
padmin@Spectracom ~ $ sftp spadmin@10.10.201.1
bash: /usr/bin/sftp: Permission denied
```

Email from Dave Sohn (4 March 2014) We have removed local user access to these to prevent security vulnerabilities allowing a user to login from one network and potentially have these accesses to the additional networks that may be connected to the SecureSync. They can still scp to/from the unit, but they need to run it from another machine.

"su" command to switch users (such as su spfactory) (for internal use only)

- To switch from **spadmin** to **spfactory**, type: **su spfactory** <enter>. Then typye the spfactory password
  - Refer to: [hCTL (Https://www.tecmint.com/su-vs-sudo-and-how-to-configure-sudo-in-linux/](Https://www.tecmint.com/su-vs-sudo-and-how-to-configure-sudo-in-linux/)
- To switch from **spfactory back to spfactory**, type: **su - spfactory** <enter> (with a space before and after the hyphen), Then type the spadmin password
  - Refer to: https://www.tecmint.com/difference-between-su-and-su-commands-in-linux/

Available CLI calls (API calls)

CTL linux commands (journalctl, systemctl)

A) 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.

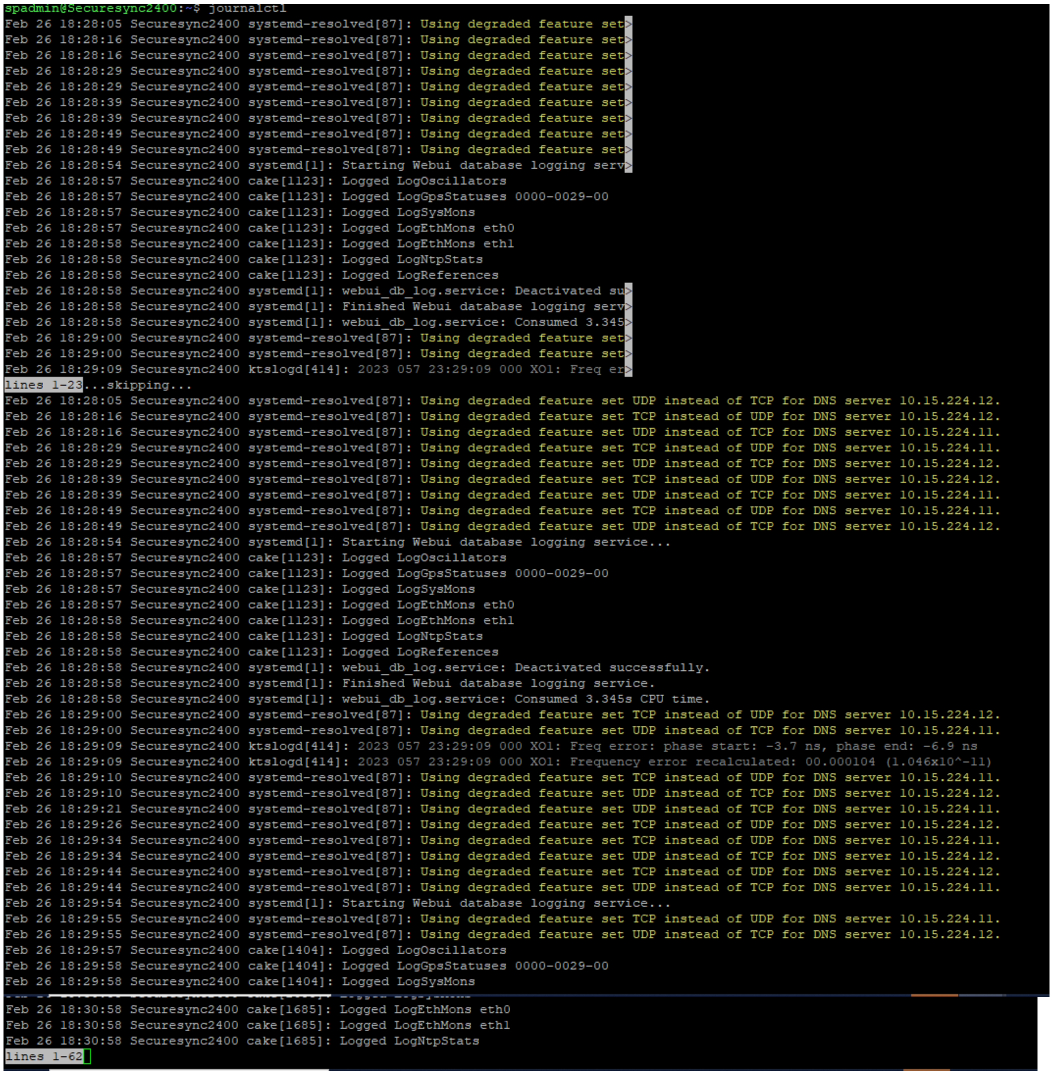
B) What is Systemctl used for?

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

journalctl

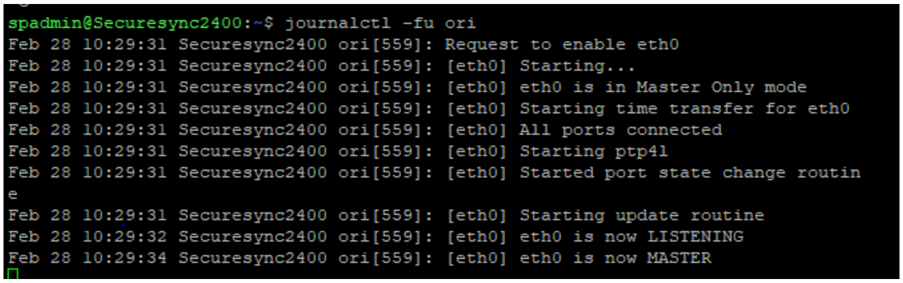
(*screenshot below from SecureSync at v1.6.0)*



```
spadmin@Securesync2400:~$ journalctl
Feb 26 18:28:05 Securesync2400 systemd-resolved[87]: Using degraded feature set>
Feb 26 18:28:16 Securesync2400 systemd-resolved[87]: Using degraded feature set>
Feb 26 18:28:16 Securesync2400 systemd-resolved[87]: Using degraded feature set>
Feb 26 18:28:29 Securesync2400 systemd-resolved[87]: Using degraded feature set>
Feb 26 18:28:29 Securesync2400 systemd-resolved[87]: Using degraded feature set>
Feb 26 18:28:39 Securesync2400 systemd-resolved[87]: Using degraded feature set>
Feb 26 18:28:39 Securesync2400 systemd-resolved[87]: Using degraded feature set>
Feb 26 18:28:49 Securesync2400 systemd-resolved[87]: Using degraded feature set>
Feb 26 18:28:49 Securesync2400 systemd-resolved[87]: Using degraded feature set>
Feb 26 18:28:54 Securesync2400 systemd[1]: Starting Webui database logging serv>
Feb 26 18:28:57 Securesync2400 cake[1123]: Logged LogOscillators
Feb 26 18:28:57 Securesync2400 cake[1123]: Logged LogGpsStatuses 0000-0029-00
Feb 26 18:28:57 Securesync2400 cake[1123]: Logged LogSysMons
Feb 26 18:28:57 Securesync2400 cake[1123]: Logged LogEthMons eth0
Feb 26 18:28:58 Securesync2400 cake[1123]: Logged LogEthMons eth1
Feb 26 18:28:58 Securesync2400 cake[1123]: Logged LogNtpStats
Feb 26 18:28:58 Securesync2400 cake[1123]: Logged LogReferences
Feb 26 18:28:58 Securesync2400 systemd[1]: webui_db_log.service: Deactivated su>
Feb 26 18:28:58 Securesync2400 systemd[1]: Finished Webui database logging serv>
Feb 26 18:28:58 Securesync2400 systemd[1]: webui_db_log.service: Consumed 3.345>
Feb 26 18:29:00 Securesync2400 systemd-resolved[87]: Using degraded feature set>
Feb 26 18:29:00 Securesync2400 systemd-resolved[87]: Using degraded feature set>
Feb 26 18:29:09 Securesync2400 ktslogd[414]: 2023 057 23:29:09 000 XO1: Freq er>
lines 1-23...skipping...
Feb 26 18:28:05 Securesync2400 systemd-resolved[87]: Using degraded feature set UDP instead of TCP for DNS server 10.15.224.12.
Feb 26 18:28:16 Securesync2400 systemd-resolved[87]: Using degraded feature set TCP instead of UDP for DNS server 10.15.224.12.
Feb 26 18:28:16 Securesync2400 systemd-resolved[87]: Using degraded feature set UDP instead of TCP for DNS server 10.15.224.11.
Feb 26 18:28:29 Securesync2400 systemd-resolved[87]: Using degraded feature set TCP instead of UDP for DNS server 10.15.224.11.
Feb 26 18:28:29 Securesync2400 systemd-resolved[87]: Using degraded feature set UDP instead of TCP for DNS server 10.15.224.12.
Feb 26 18:28:39 Securesync2400 systemd-resolved[87]: Using degraded feature set TCP instead of UDP for DNS server 10.15.224.12.
Feb 26 18:28:39 Securesync2400 systemd-resolved[87]: Using degraded feature set UDP instead of TCP for DNS server 10.15.224.11.
Feb 26 18:28:49 Securesync2400 systemd-resolved[87]: Using degraded feature set TCP instead of UDP for DNS server 10.15.224.11.
Feb 26 18:28:49 Securesync2400 systemd-resolved[87]: Using degraded feature set UDP instead of TCP for DNS server 10.15.224.12.
Feb 26 18:28:54 Securesync2400 systemd[1]: Starting Webui database logging service...
Feb 26 18:28:57 Securesync2400 cake[1123]: Logged LogOscillators
Feb 26 18:28:57 Securesync2400 cake[1123]: Logged LogGpsStatuses 0000-0029-00
Feb 26 18:28:57 Securesync2400 cake[1123]: Logged LogSysMons
Feb 26 18:28:57 Securesync2400 cake[1123]: Logged LogEthMons eth0
Feb 26 18:28:58 Securesync2400 cake[1123]: Logged LogEthMons eth1
Feb 26 18:28:58 Securesync2400 cake[1123]: Logged LogNtpStats
Feb 26 18:28:58 Securesync2400 cake[1123]: Logged LogReferences
Feb 26 18:28:58 Securesync2400 systemd[1]: webui_db_log.service: Deactivated successfully.
Feb 26 18:28:58 Securesync2400 systemd[1]: Finished Webui database logging service.
Feb 26 18:28:58 Securesync2400 systemd[1]: webui_db_log.service: Consumed 3.345s CPU time.
Feb 26 18:29:00 Securesync2400 systemd-resolved[87]: Using degraded feature set TCP instead of UDP for DNS server 10.15.224.12.
Feb 26 18:29:00 Securesync2400 systemd-resolved[87]: Using degraded feature set UDP instead of TCP for DNS server 10.15.224.11.
Feb 26 18:29:09 Securesync2400 ktslogd[414]: 2023 057 23:29:09 000 XO1: Freq error: phase start: -3.7 ns, phase end: -6.9 ns
Feb 26 18:29:09 Securesync2400 ktslogd[414]: 2023 057 23:29:09 000 XO1: Frequency error recalculated: 00.000104 (1.046x10^-11)
Feb 26 18:29:10 Securesync2400 systemd-resolved[87]: Using degraded feature set TCP instead of UDP for DNS server 10.15.224.11.
Feb 26 18:29:10 Securesync2400 systemd-resolved[87]: Using degraded feature set UDP instead of TCP for DNS server 10.15.224.12.
Feb 26 18:29:21 Securesync2400 systemd-resolved[87]: Using degraded feature set UDP instead of TCP for DNS server 10.15.224.11.
Feb 26 18:29:26 Securesync2400 systemd-resolved[87]: Using degraded feature set TCP instead of UDP for DNS server 10.15.224.12.
Feb 26 18:29:34 Securesync2400 systemd-resolved[87]: Using degraded feature set TCP instead of UDP for DNS server 10.15.224.11.
Feb 26 18:29:34 Securesync2400 systemd-resolved[87]: Using degraded feature set UDP instead of TCP for DNS server 10.15.224.12.
Feb 26 18:29:44 Securesync2400 systemd-resolved[87]: Using degraded feature set TCP instead of UDP for DNS server 10.15.224.12.
Feb 26 18:29:44 Securesync2400 systemd-resolved[87]: Using degraded feature set UDP instead of TCP for DNS server 10.15.224.11.
Feb 26 18:29:54 Securesync2400 systemd[1]: Starting Webui database logging service...
Feb 26 18:29:55 Securesync2400 systemd-resolved[87]: Using degraded feature set TCP instead of UDP for DNS server 10.15.224.11.
Feb 26 18:29:55 Securesync2400 systemd-resolved[87]: Using degraded feature set UDP instead of TCP for DNS server 10.15.224.12.
Feb 26 18:29:57 Securesync2400 cake[1404]: Logged LogOscillators
Feb 26 18:29:58 Securesync2400 cake[1404]: Logged LogGpsStatuses 0000-0029-00
Feb 26 18:29:58 Securesync2400 cake[1404]: Logged LogSysMons
Feb 26 18:30:58 Securesync2400 cake[1685]: Logged LogEthMons eth0
Feb 26 18:30:58 Securesync2400 cake[1685]: Logged LogEthMons eth1
Feb 26 18:30:58 Securesync2400 cake[1685]: Logged LogNtpStats
lines 1-62
```

journalctl -fu ori

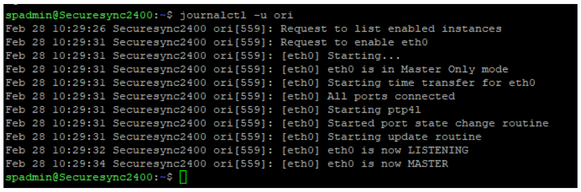
(*screenshots below from SecureSync at v1.6.0)*



```
spadmin@Securesync2400:~$ journalctl -fu ori
Feb 28 10:29:31 Securesync2400 ori[559]: Request to enable eth0
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Starting...
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] eth0 is in Master Only mode
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Starting time transfer for eth0
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] All ports connected
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Starting ptp4l
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Started port state change routin
e
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Starting update routine
Feb 28 10:29:32 Securesync2400 ori[559]: [eth0] eth0 is now LISTENING
Feb 28 10:29:34 Securesync2400 ori[559]: [eth0] eth0 is now MASTER
```

journalctl -u ori

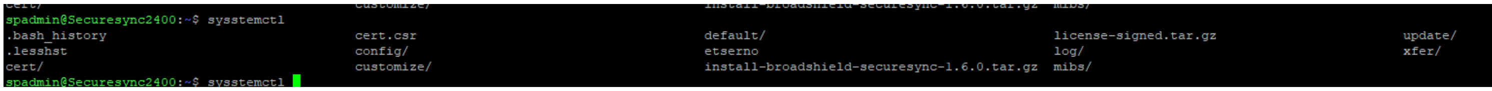
(*screenshot below from SecureSync at v1.6.0)*



```
spadmin@Securesync2400:~$ journalctl -u ori
Feb 28 10:29:26 Securesync2400 ori[559]: Request to list enabled instances
Feb 28 10:29:31 Securesync2400 ori[559]: Request to enable eth0
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Starting...
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] eth0 is in Master Only mode
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Starting time transfer for eth0
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] All ports connected
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Starting ptp4l
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Started port state change routine
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Starting update routine
Feb 28 10:29:32 Securesync2400 ori[559]: [eth0] eth0 is now LISTENING
Feb 28 10:29:34 Securesync2400 ori[559]: [eth0] eth0 is now MASTER
spadmin@Securesync2400:~$
```

systemctl

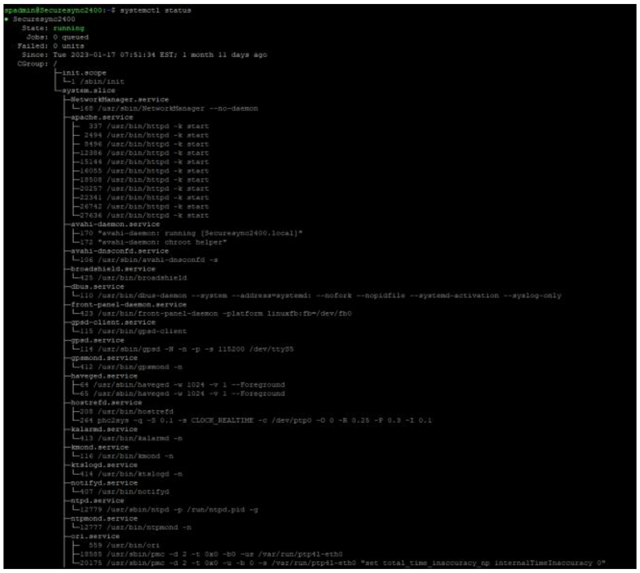
(*screenshot below from SecureSync at v1.6.0)*



```
spadmin@Securesync2400:~$ sysstemctl
.bash_history          cert.csr          default/                                    license-signed.tar.gz    update/
.lesshst               config/           etserno                                     log/                     xfer/
cert/                  customize/        install-broadshield-securesync-1.6.0.tar.gz  mibs/
spadmin@Securesync2400:~$ sysstemctl
```

systemctl status

(*screenshot below from SecureSync at v1.6.0)*

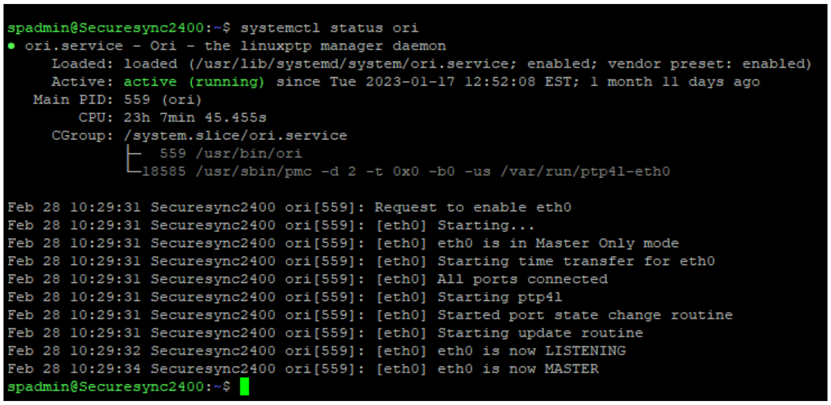


```
spadmin@Securesync2400:~$ systemctl status
● Securesync2400
    State: running
     Jobs: 0 queued
   Failed: 0 units
    Since: Tue 2023-01-17 07:51:34 EST; 1 month 11 days ago
   CGroup: /
           ├─init.scope
           │ └─1 /sbin/init
           └─system.slice
             ├─NetworkManager.service
             │ └─168 /usr/sbin/NetworkManager --no-daemon
             ├─apache.service
             │ ├─  337 /usr/bin/httpd -k start
             │ ├─ 2494 /usr/bin/httpd -k start
             │ ├─ 8496 /usr/bin/httpd -k start
             │ ├─12386 /usr/bin/httpd -k start
             │ ├─15144 /usr/bin/httpd -k start
             │ ├─16055 /usr/bin/httpd -k start
             │ ├─18508 /usr/bin/httpd -k start
             │ ├─20257 /usr/bin/httpd -k start
             │ ├─22341 /usr/bin/httpd -k start
             │ ├─26742 /usr/bin/httpd -k start
             │ └─27636 /usr/bin/httpd -k start
             ├─avahi-daemon.service
             │ ├─170 "avahi-daemon: running [Securesync2400.local]"
             │ └─172 "avahi-daemon: chroot helper"
             ├─avahi-dnsconfd.service
             │ └─106 /usr/sbin/avahi-dnsconfd -s
             ├─broadshield.service
             │ └─425 /usr/bin/broadshield
             ├─dbus.service
             │ └─110 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
             ├─front-panel-daemon.service
             │ └─423 /usr/bin/front-panel-daemon -platform linuxfb:fb=/dev/fb0
             ├─gpsd-client.service
             │ └─115 /usr/bin/gpsd-client
             ├─gpsd.service
             │ └─114 /usr/sbin/gpsd -N -n -p -s 115200 /dev/ttyS5
             ├─gpsmond.service
             │ └─412 /usr/bin/gpsmond -n
             ├─haveged.service
             │ ├─64 /usr/sbin/haveged -w 1024 -v 1 --Foreground
             │ └─65 /usr/sbin/haveged -w 1024 -v 1 --Foreground
             ├─hostrefd.service
             │ ├─208 /usr/bin/hostrefd
             │ └─264 phc2sys -q -S 0.1 -s CLOCK_REALTIME -c /dev/ptp0 -O 0 -R 0.25 -P 0.3 -I 0.1
             ├─kalarmd.service
             │ └─413 /usr/bin/kalarmd -n
             ├─kmond.service
             │ └─116 /usr/bin/kmond -n
             ├─ktslogd.service
             │ └─414 /usr/bin/ktslogd -n
             ├─notifyd.service
             │ └─407 /usr/bin/notifyd
             ├─ntpd.service
             │ └─12779 /usr/sbin/ntpd -p /run/ntpd.pid -g
             ├─ntpmond.service
             │ └─12777 /usr/bin/ntpmond -n
             ├─ori.service
             │ ├─  559 /usr/bin/ori
             │ ├─18585 /usr/sbin/pmc -d 2 -t 0x0 -b0 -us /var/run/ptp4l-eth0
             │ └─20175 /usr/sbin/pmc -d 2 -t 0x0 -u -b 0 -s /var/run/ptp4l-eth0 "set total_time_inaccuracy_np internalTimeInaccuracy 0"
```

(last entry in response)

systemctl status ori

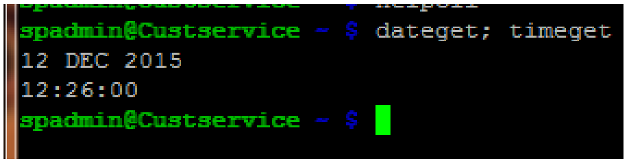
(*screenshot below from SecureSync at v1.6.0)*



```
spadmin@Securesync2400:~$ systemctl status ori
● ori.service - Ori - the linuxptp manager daemon
     Loaded: loaded (/usr/lib/systemd/system/ori.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2023-01-17 12:52:08 EST; 1 month 11 days ago
   Main PID: 559 (ori)
        CPU: 23h 7min 45.455s
     CGroup: /system.slice/ori.service
             ├─  559 /usr/bin/ori
             └─18585 /usr/sbin/pmc -d 2 -t 0x0 -b0 -us /var/run/ptp4l-eth0

Feb 28 10:29:31 Securesync2400 ori[559]: Request to enable eth0
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Starting...
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] eth0 is in Master Only mode
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Starting time transfer for eth0
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] All ports connected
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Starting ptp4l
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Started port state change routine
Feb 28 10:29:31 Securesync2400 ori[559]: [eth0] Starting update routine
Feb 28 10:29:32 Securesync2400 ori[559]: [eth0] eth0 is now LISTENING
Feb 28 10:29:34 Securesync2400 ori[559]: [eth0] eth0 is now MASTER
spadmin@Securesync2400:~$
```

Desire to perform more than one CLI command with a single response

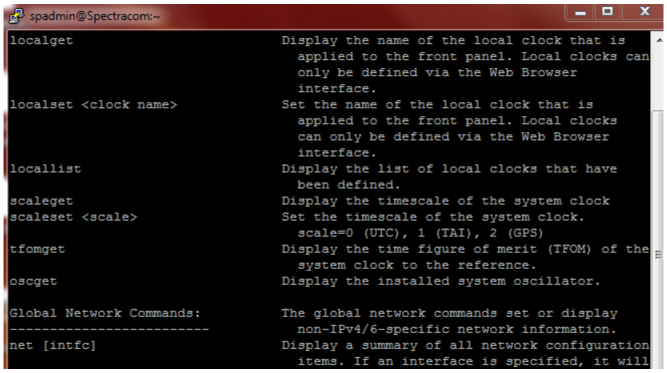
- Separate multiple commands with a semi-colon (“;”) to have just one response.



```
spadmin@Custservice ~ $ dateget; timeget
12 DEC 2015
12:26:00
spadmin@Custservice ~ $
```

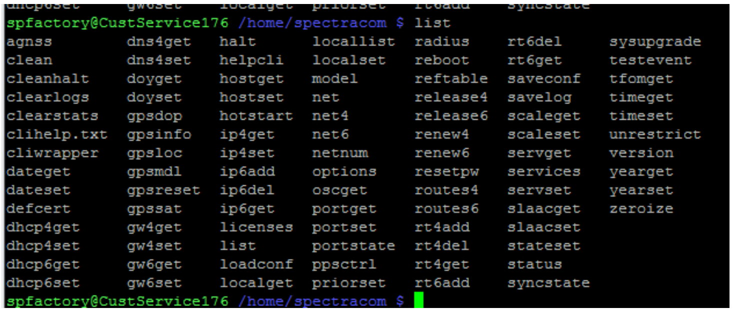
A) “Documented” CLI calls

- Type **helpcli** for a list of call, descriptions and syntaxes (shift and “q” to exit out)



```
localget                          Display the name of the local clock that is
                                    applied to the front panel. Local clocks can
                                    only be defined via the Web Browser
                                    interface.
localset <clock name>             Set the name of the local clock that is
                                    applied to the front panel. Local clocks
                                    can only be defined via the Web Browser
                                    interface.
locallist                         Display the list of local clocks that have
                                    been defined.
scaleget                          Display the timescale of the system clock
scaleset <scale>                  Set the timescale of the system clock.
                                    scale=0 (UTC), 1 (TAI), 2 (GPS)
tfomget                           Display the time figure of merit (TFOM) of the
                                    system clock to the reference.
oscget                            Display the installed system oscillator.

Global Network Commands:          The global network commands set or display
-------------------------           non-IPv4/6-specific network information.
net [intfc]                       Display a summary of all network configuration
                                    items. If an interface is specified, it will
```

- Type “**list**” or help in the home/spectracom directory to display a list of all available CLI calls



```
spfactory@CustService176 /home/spectracom $ list
agnss        dns4get   halt      locallist  radius     rt6del    sysupgrade
clean        dns4set   helpcli   localset   reboot     rt6get    testevent
cleanhalt    doyget    hostget   model      reftable   saveconf  tfomget
clearlogs    doyset    hostset   net        release4   savelog   timeget
clearstats   gpsdop    hotstart  net4       release6   scaleget  timeset
clihelp.txt  gpsinfo   ip4get    net6       renew4     scaleset  unrestrict
cliwrapper   gpsloc    ip4set    netnum     renew6     servget   version
dateget      gpsmdl    ip6add    options    resetpw    services  yearget
dateset      gpsreset  ip6del    oscget     routes4    servset   yearset
defcert      gpssat    ip6get    portget    routes6    slaacget  zeroize
dhcp4get     gw4get    licenses  portset    rt4add     slaacset
dhcp4set     gw4set    list      portstate  rt4del     stateset
dhcp6get     gw6get    loadconf  ppsctrl    rt4get     status
dhcp6set     gw6set    localget  priorset   rt6add     syncstate
spfactory@CustService176 /home/spectracom $
```

- The entire list of documented CLI calls is provided in Chapter 5 of the SecureSync manual
  - **Online SecureSync manual at**: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/APPENDIX/CLICommands.htm?Highlight=cli%20interface
  - **Shortcut to SecureSync manual (1200-5000-0050) in Arena:** https://app.bom.com/items/detail-attach?item_id=1203165562&version_id=10381283008

Remember: All commands and API calls are capital letter sensitive. Typing any character in the wrong case will cause the command to respond with “command not found”.

B) “Undocumented”/unsupported CLI calls (calls associated with the TSync boards)

- Refer to the cheat sheet Tim Tetreault created (API for KTS): ..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\CLI -API calls
- Undocumented calls allow “gets” but not “sets” (not available to use for configuration, for example. But can be used to obtain data/settings).

Remember: All commands and API calls are capital letter sensitive. Typing any character in the wrong case will cause the command to respond with “command not found”.

The SecureSync’s web browser needs to perform “Get” and “Set” API calls to KTS, in order to show or change information in the system. All of these API calls exist in the background and the “**Get**” calls are available to users, via the CLI interface (the **Set** commands require root account permissions to perform and therefore are not available for customer use).

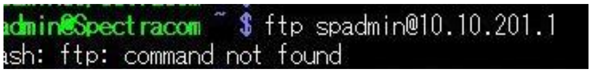
Note that the Get API calls are “not supported”, but customers can be informed of them and can use them if they wish.

(9/21/12) As of at least 5.8.2 and below, users can only access the “**get**” API calls. They do not have permission to access the “**set**” API calls.

Unsupported CLI commands (such as FTP/SCP/SFTP etc) due to potential Security concerns

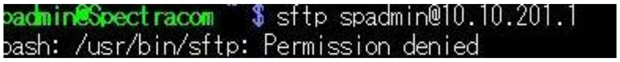
- Due to potential security concerns across Ethernet ports, version 5.1.2 disabled user-level permissions from being able to perform services such as telnet, ssh., FTP and sftp/scp from the command line interface.
- Can still SCP into the SecureSync. This change prevents scp’ing out from the box.
- Can still ping out from within the SecureSync.
- Refer to Salesforce case 13444 and Mantis 2757 for an SCP issue this changed ended up causing

Example trying to FTP from the CLI



```
dmin@Spectracom ~ $ ftp spadmin@10.10.201.1
sh: ftp: command not found
```

Example trying to sftp from the CLI



```
padmin@Spectracom ~ $ sftp spadmin@10.10.201.1
bash: /usr/bin/sftp: Permission denied
```

Email from Dave Sohn (4 March 2014) We have removed local user access to these to prevent security vulnerabilities allowing a user to login from one network and potentially have these accesses to the additional networks that may be connected to the SecureSync. They can still scp to/from the unit, but they need to run it from another machine.

Display lists of available SecureSync CLI Commands and “Get” API calls

A) To display a list of ALL available Commands and “Get” API calls

To see a list of all available API calls and available CLI commands, at the CLI command line, hit the TAB key two times. Type a letter “**Y**” at the prompt that is displayed. ALL available SecureSync commands and KTS **Get** API calls that users can use will be listed. Hit any key to proceed to the next page of listed commands.

Note” This does not list any “**Set”** API calls. Set API calls are not permissible via the SPadmin or user accounts. Only root has permissions to perform Set calls.

Example: at the command prompt, press the TAB key two times to see all of available commands:

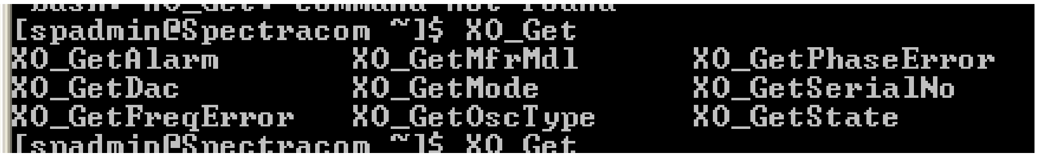
Note: If no response is shown after hitting the TAB key twice, this is likely due to one or more letters for the call being typed in the wrong case (upper or lower). Re-enter the command using the correct case for each letter.

B) To display a list of all commands and Get calls for a particular function (such as all available IRIG gets)

To see a list of all available “**Get**” calls for a particular function, at the command line, **type the first two characters of the call, followed by the underscore symbol, followed by the word “Get**”. Then, hit the TAB key two times. This will show only the particular API Get calls of that type of call.

Note” This does not list any “**Set”** API calls. Set API calls are not permissible via the SPAdmin or user accounts. Only root can perform set calls.

Example: Type “**XO_Get”** and then press the **TAB** key three times to see all of available XO_Get type commands:



```
bash: XO_Get: command not found
[spadmin@Spectracom ~]$ XO_Get
XO_GetAlarm          XO_GetMfrMdl         XO_GetPhaseError
XO_GetDac            XO_GetMode           XO_GetSerialNo
XO_GetFreqError      XO_GetOscType        XO_GetState
[spadmin@Spectracom ~]$ XO_Get
```

Note: If no response is shown after hitting the TAB key twice, this is likely due to one or more letters for the call being typed in the wrong case (upper or lower). Re-enter the command using the correct case for each letter.

*Specific available CLI commands/API calls/ functions

exit to logout

Note: The Device ID value for each call (the first number entered after each command) should always be 0 (such as IR_GetMode **0**).

CLI Commands which no longer available

Mgmt (mgmtget/mgmtset)

Email from Keith to Mark Day (23 May 13) I JUST recalled, **mgmt** was a planned command to be able to manage Ethernet ports, but it was then decided not to be used. So it has since been removed in a newer version of software. There is no functionality assigned to it, in earlier versions of software.

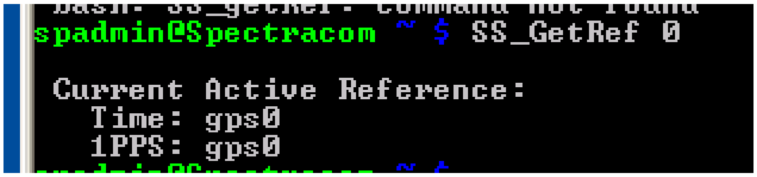
Note: Refer to Mantis case 1423 (the two “mgmt” commands were removed from the CLI and front panel LCD in Archive version 4.5.0).

Refer to the following section for more information about Management control:**VLANs/Network ports/Management/Network Access restriction (Access control)

System status

Obtain the currently selected Time and PPS references (SS_GetRef 0)

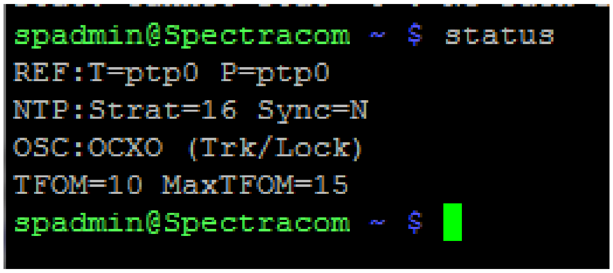
SS_GetRef 0 Gets the currently selected time and 1PPS reference.



```
bash: SS_getRef: command not found
spadmin@Spectracom ~ $ SS_GetRef 0

 Current Active Reference:
   Time: gps0
   1PPS: gps0
spadmin@Spectracom ~ $
```

Status

- ➢ Reports selected references, NTP Stratum, Osc status, TFOM and MaxTFOM)



```
spadmin@Spectracom ~ $ status
REF:T=ptp0 P=ptp0
NTP:Strat=16 Sync=N
OSC:OCXO (Trk/Lock)
TFOM=10 MaxTFOM=15
spadmin@Spectracom ~ $
```

Email from Keith (The **status** command is the best CLI command to observe, and to also assume, normal operation of the SecureSync. The NTP status reporting Stratum 1 (or Stratum 2) means the SecureSync is synced to a reference such as GPS (or NTP from another NTP server). Therefore, NTP and PTP are in a state that their associated Slaves can use for their synchronization.

If instead, NTP is Stratum 16, this means there is a problem with the SecureSync's synchronization to its inputs, or there is a problem associated with NTP itself,

Add an additional check for the state of the Fault LED (summary of both Minor/Major alarm states)

Where (note the Power LED is only one color, while Fault/Sync can be bi-color, requiring two controllers each)

Fault LED = LED 0 + LED 1 (EC_GetState 0 0 + EC_GetState 0 1) ??

Sync LED = LED + LED 2/4 (EC_GetState 0 2 + EC_GetState 0 4) ??

Power LED = Just LED 5 (EC_GetState 0 2 + EC_GetState 0 4) ??

In sync	Holdover (binking green/red)	no sync
0 blink	**blink**	**on**
1 blink	**blink**	**off**
2= off	**on**	**on**
3 = on	**on**	**off**
4 off	**off**	**off**
5	**on**	**on**

- **Fault LED: EC_GetState 0 0 + EC_GetState 0 1** (if Fault reports “ON” or “Blinking”, the Minor and/or Major Alarms are active): Blinking/Blinking indicates GPS antenn Probem alarm is asserted???

To read individual status indicators

- **Sync Status = SS_GetSync 0**
- **Holdover = SS_GetHoldover 0**
- **Freerun status = SS_GetFreeRun 0**

To read the current Alarm status (determine if each individual Alarm is active or inactive)

To read an alarm status, type: **LS_GetAlarm 0 x** (where x is one of the following values)

0 = **Sync** alarm

1 = **Holdover** alarm

2 = **Frequency** Error alarm

3 = **Freerun** alarm

4 = **Software error** alarm

5 = **1PPS Specification** alarm

6 = **Reference Change** alarm

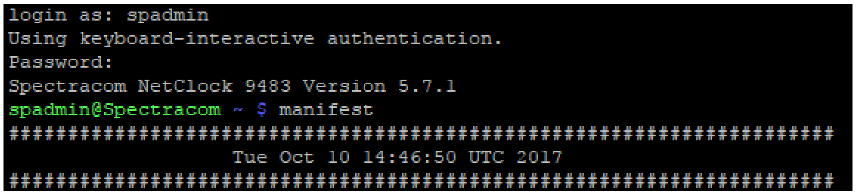
7 = **Hardware error** alarm

8 = **BAY 1 hot swap** alarm

9 = **BAY 1 hot swap** alarm

CLI command to display the entire manifest.log

- Command added in version 5.7.1
- Type: **manifest**



```
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 5.7.1
spadmin@Spectracom ~ $ manifest
######################################################################
                   Tue Oct 10 14:46:50 UTC 2017
######################################################################
```

Note: For more info on the manifest log, refer to (in this document): manifest.log file /manifest.config file

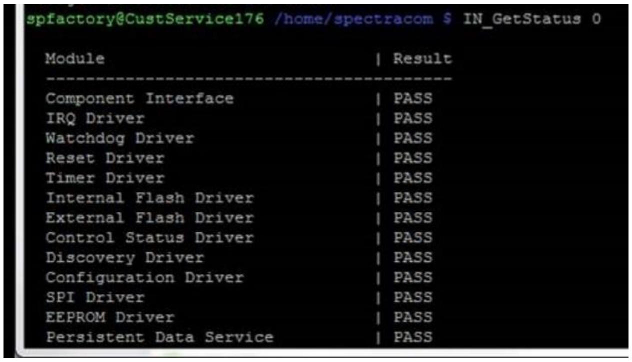
Email from Dave L (10 Oct 17) Also, starting on the version 5.7.0 firmware there is a new CLI command “manifest” you can use to identify the exact Option cards installed on the system. In earlier versions the “options” command would identify the cards but the descriptions were rather generic so the exact model of the options cards was a little vague.

CLI command for KTS initialization test results (IN_GetStatus 0)

- Can find KTS related problems such as an issue with an Option Card at boot-up.
- This command is available to customers in the spadmin account.

Email from Paul Myers (7 Jun 16): Can you have the customer run "**IN_GetStatus 0**" on the command line and look for any initialization failures?

This command prints all the initialized drivers, services and components. If something failed in startup it would show here. (Note the screenshot below is only a partial list)



```
spfactory@CustService176 /home/spectracom $ IN_GetStatus 0

  Module                                | Result
  -----------------------------------------
  Component Interface                   | PASS
  IRQ Driver                            | PASS
  Watchdog Driver                       | PASS
  Reset Driver                          | PASS
  Timer Driver                          | PASS
  Internal Flash Driver                 | PASS
  External Flash Driver                 | PASS
  Control Status Driver                 | PASS
  Discovery Driver                      | PASS
  Configuration Driver                  | PASS
  SPI Driver                            | PASS
  EEPROM Driver                         | PASS
  Persistent Data Service               | PASS
```

Examples of CLI commands for particular situations:

1) Commands regarding the Ethernet ports: Refer to: CLI Commands for the Ethernet ports
2) Apache Web browser no longer accessible, but can still ping, telnet etc. Refer to "free" or "free mem" commands below.
3) Available CLI commands for network troubleshooting within SecureSync

Note (Update to the info below) This info appears to have changed with the Gentoo version 5.0.0 and above release. I don't believe these tools were added in with 5.0.0 and above.

Starting in SecureSync software version 4.8.0, customers will be able to troubleshoot network issues from within SecureSync (instead of just external to the SecureSync). There are several tools being added to provide standard Linux commands for troubleshooting the network traffic. These commands are only available in the CLI port (not on the web browser) and are intended for experienced users only.

The added commands are:

Ping, ifconfig, arp, rarp, route, netstat, domainname, dig, host, nslookup, traceroute

For these commands, refer to: **Network troubleshooting from within SecureSync (ping, arp, traceroute, etc)

Deleting/removing a file (such as an ugrade bundle) where permissions allow: **rm <filename>** <enter>

- To check for any previous updatexxx.tar.gz bundles via CLI, type **ls -l** <enter> (in the home/spectracom directory)
- To delete an update bundle type **rm <filename>** <enter> (for example: >**rm update5.0.2.tar.gz** <enter>

**CLI commands enable/disable/, display, configure the Ethernet ports (DNS, DHCP, IP

address, Subnet mask, Static routes)

Enable/Disable network interfaces via CLI commands (portstate?portset command)

Note: since the ports can't be enabled via the keypad in versions prior to v5.5.1, they can only be enabled via either CLO command or via the web browser using eth0

For more infon on enabling ports via keypad or via the browser, refer to (in this doc): [Desire to Enable/Disable the Gigabit interfaces (eth1, eth2 and/or eth3)]()**

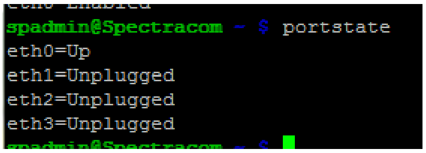
Port state

- Display the port state of all Ethernet ports (port up, port down, cable unplugged)

portstate command

Note: To obtain port state for SMNP instead of CLI, refer to the "**ifOperStatus**" SNMP object in the SNMP section of this document.

- Displays status of all installed Ethernet ports, including Eth0.



```
eth0 Enabled
spadmin@Spectracom ~ $ portstate
eth0=Up
eth1=Unplugged
eth2=Unplugged
eth3=Unplugged
spadmin@Spectracom ~ $
```

portset command

- This command was implemented starting with the new web browser design in Archive version 5.1.2 (not available with earlier versions)
- The CLI command: **portset x on** enables the interface number specified by the "x".
- The CLI command: **portset x off** disable the interface number specified by the "x
- CLI command to retrieve current port state: **portget x** <enter>

Enable /disable link negotiation and ability to hard-set port settings

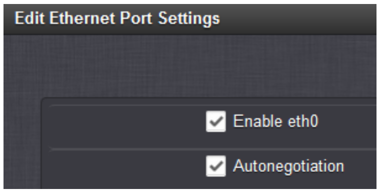
Q (7 May 2021 fromHughes demoing 2400 v1.2.0?) It doesn't have option to set Speed/Duplex Ethernet settings, which was available in older units.

A Per Dave Sohn This feature didn't make the initial release, but is already in our roadmap for future releases likely slated for Q3 (2021) release.

Below is from 1200 SecureSyncs

A) Via web browser

1. Navigage to the ***Management*** -> ***Network Setup*** page.
2. Unselect the "**Autonegotiation**" checkbox (selected on all interfaces by factory default)

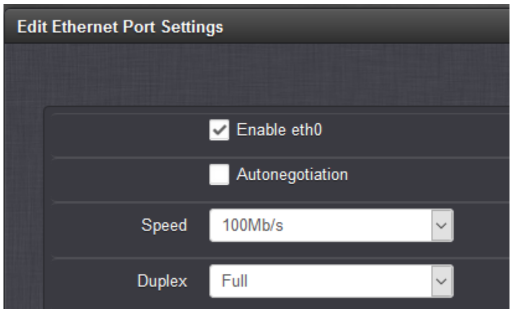


Edit Ethernet Port Settings

☑ Enable eth0

☑ Autonegotiation

->



Edit Ethernet Port Settings

☑ Enable eth0

□ Autonegotiation

Speed: 100Mb/s

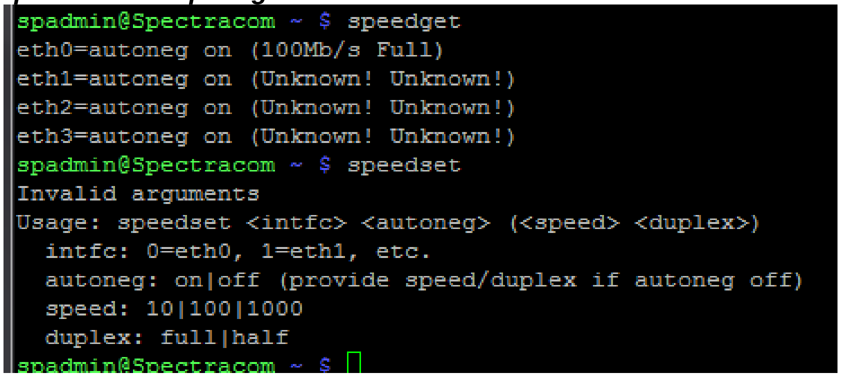
Duplex: Full

3. Configure desired speed and duplex
4. Press Submit

B) Via CLI interface (info below from 1200 secureSyncs)

speedget and speedset commands (???)

One of the new features in the next firmware release version 5.8.0 is the ability to control the port settings through the ***speedset*** and ***speedget*** CLI commands.

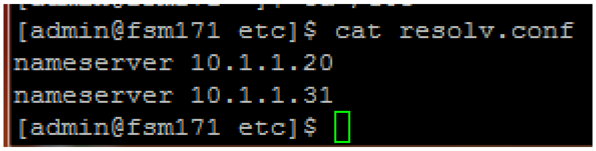


```
spadmin@Spectracom ~ $ speedget
eth0=autoneg on (100Mb/s Full)
eth1=autoneg on (Unknown! Unknown!)
eth2=autoneg on (Unknown! Unknown!)
eth3=autoneg on (Unknown! Unknown!)
spadmin@Spectracom ~ $ speedset
Invalid arguments
Usage: speedset <intfc> <autoneg> (<speed> <duplex>)
  intfc: 0=eth0, 1=eth1, etc.
  autoneg: on|off (provide speed/duplex if autoneg off)
  speed: 10|100|1000
  duplex: full|half
spadmin@Spectracom ~ $
```

DNS servers ("resolv.conf" file)

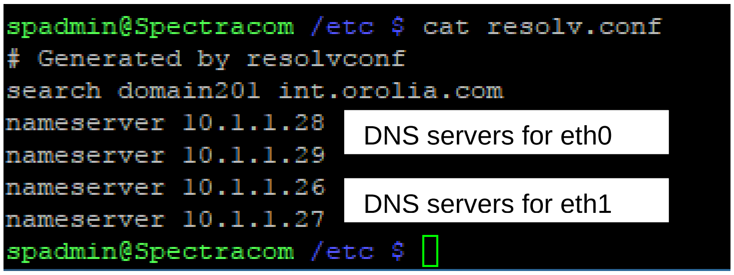
- **/etc/resolv.conf** file stores all DNS server addresses (for all interfaces)

resolv.conf file with only one interface configured for DNS



```
[admin@fsm171 etc]$ cat resolv.conf
nameserver 10.1.1.20
nameserver 10.1.1.31
[admin@fsm171 etc]$
```

resolv.conf file with two different nterfaces (eth0 and eth1) configured for different DNS servers

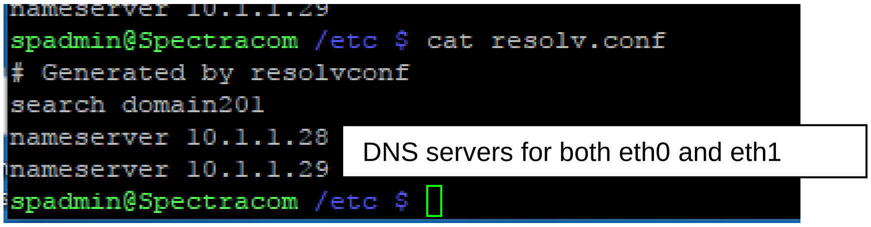


```
spadmin@Spectracom /etc $ cat resolv.conf
# Generated by resolvconf
search domain201 int.orolia.com
nameserver 10.1.1.28
nameserver 10.1.1.29
nameserver 10.1.1.26
nameserver 10.1.1.27
spadmin@Spectracom /etc $
```

DNS servers for eth0

DNS servers for eth1

resolv.conf file with two different nterfaces (eth0 and eth1) configured for the same two DNS servers



```
nameserver 10.1.1.29
spadmin@Spectracom /etc $ cat resolv.conf
# Generated by resolvconf
search domain201
nameserver 10.1.1.28
nameserver 10.1.1.29
spadmin@Spectracom /etc $
```

DNS servers for both eth0 and eth1

CLI commands to Display/Retrieve/Set DNS server settings for each Ethernet interface

- The CLI command: **dns4get x** retrieves the DNS setting (for the port specified by the "x".
- The CLI command: **dns4set x <primary dns> <secondary dns>** configures the DNS setting for he Ethernet interface port number specified by the "x". (note the secondard dns address is optional/not required)

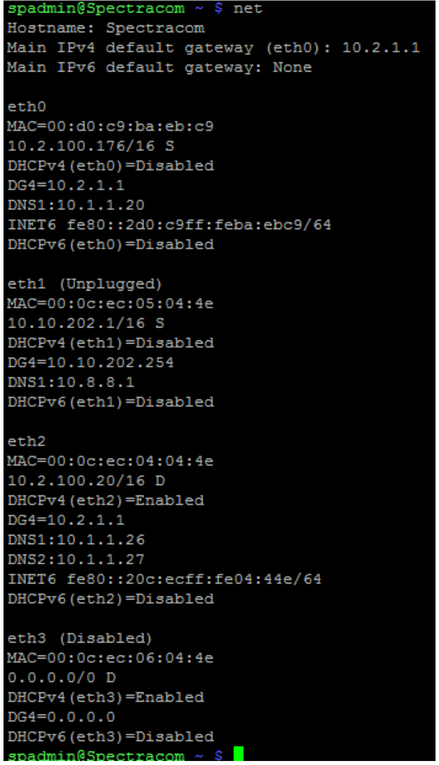
Example journal.log entries associated with DNS

Adding two new DNS servers for eth1 via the browser

Oct 19 14:37:42 Spectracom Spectracom: [webui] set DNS for eth1 to 10.1.1.28.
Oct 19 14:37:42 Spectracom Spectracom: [webui] set DNS for eth1 to 10.1.1.29.

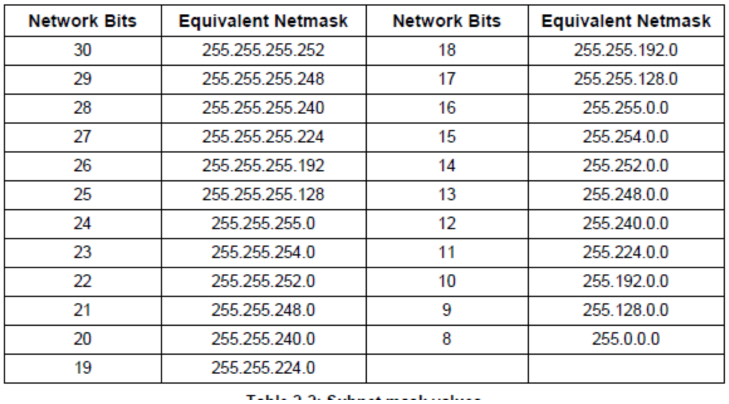
Display/retrieve network settings (IP address, subnet mask)

net <enter> shows all network settings for all ports



```
spadmin@Spectracom ~ $ net
Hostname: Spectracom
Main IPv4 default gateway (eth0): 10.2.1.1
Main IPv6 default gateway: None

eth0
MAC=00:d0:c9:ba:eb:c9
10.2.100.176/16 S
DHCPv4(eth0)=Disabled
DG4=10.2.1.1
DNS1:10.1.1.20
INET6 fe80::2d0:c9ff:feba:ebc9/64
DHCPv6(eth0)=Disabled

eth1 (Unplugged)
MAC=00:0c:ec:05:04:4e
10.10.202.1/16 S
DHCPv4(eth1)=Disabled
DG4=10.10.202.254
DNS1:10.8.8.1
DHCPv6(eth1)=Disabled

eth2
MAC=00:0c:ec:04:04:4e
10.2.100.20/16 D
DHCPv4(eth2)=Enabled
DG4=10.2.1.1
DNS1:10.1.1.26
DNS2:10.1.1.27
INET6 fe80::20c:ecff:fe04:44e/64
DHCPv6(eth2)=Disabled

eth3 (Disabled)
MAC=00:0c:ec:06:04:4e
0.0.0.0/0 D
DHCPv4(eth3)=Enabled
DG4=0.0.0.0
DHCPv6(eth3)=Disabled
spadmin@Spectracom ~ $
```

Subnet mask conversion table for quick-reference



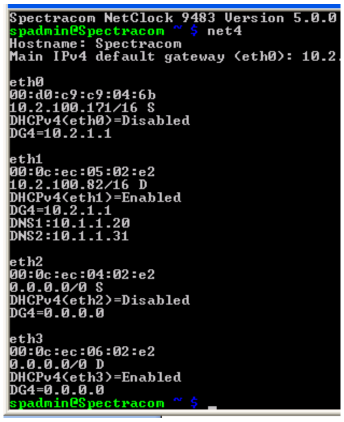
Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
30	255.255.255.252	18	255.255.192.0
29	255.255.255.248	17	255.255.128.0
28	255.255.255.240	16	255.255.0.0
27	255.255.255.224	15	255.254.0.0
26	255.255.255.192	14	255.252.0.0
25	255.255.255.128	13	255.248.0.0
24	255.255.255.0	12	255.240.0.0
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		

Table 2-2: Subnet mask values

net show and **net4** commands (net4 is equivalent to net show command in earlier Models)

Displays All IPv4 settings for all Ethernet port

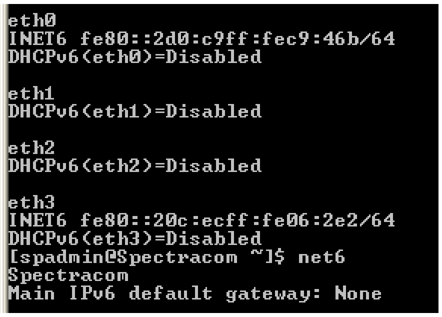
- The command: **net4** displays or gets the network settings/MAC addresses for each of the network ports.
- IPv4 settings only (no IPv6 settings)



```
Spectracom NetClock 9483 Version 5.0.0
spadmin@Spectracom ~ $ net4
Hostname: Spectracom
Main IPv4 default gateway (eth0): 10.2.

eth0
00:d0:c9:c9:04:6b
10.2.100.171/16 S
DHCPv4(eth0)=Disabled
DG4=10.2.1.1

eth1
00:0c:ec:05:02:e2
10.2.100.82/16 D
DHCPv4(eth1)=Enabled
DG4=10.2.1.1
DNS1:10.1.1.20
DNS2:10.1.1.31

eth2
00:0c:ec:04:02:e2
0.0.0.0/0 S
DHCPv4(eth2)=Disabled
DG4=0.0.0.0

eth3
00:0c:ec:06:02:e2
0.0.0.0/0 D
DHCPv4(eth3)=Enabled
DG4=0.0.0.0
spadmin@Spectracom ~ $ _
```

Display IPv6 settings only (no IPv4 settings)

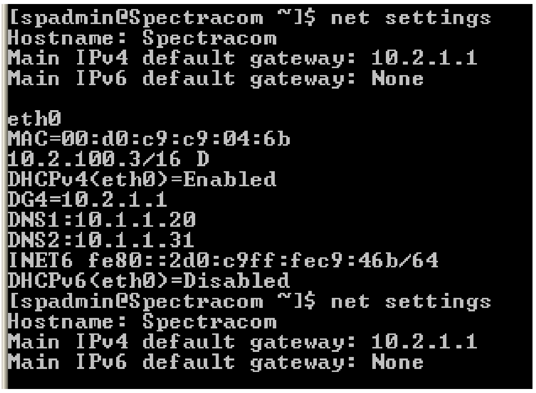
- The command: **net6** displays the network settings/IPv6 addresses for each of the network ports.



```
eth0
INET6 fe80::2d0:c9ff:fec9:46b/64
DHCPv6(eth0)=Disabled

eth1
DHCPv6(eth1)=Disabled

eth2
DHCPv6(eth2)=Disabled

eth3
INET6 fe80::20c:ecff:fe06:2e2/64
DHCPv6(eth3)=Disabled
[spadmin@Spectracom ~]$ net6
Spectracom
Main IPv6 default gateway: None
```

Display Eth0 settings only (Both IPv4 and IPv6 settings)

- **net settings** command displays only Eth0's IPv4 and IPv6 network port configurations
- Shows no info on Eth1, Eth2, Eth3



```
[spadmin@Spectracom ~]$ net settings
Hostname: Spectracom
Main IPv4 default gateway: 10.2.1.1
Main IPv6 default gateway: None

eth0
MAC=00:d0:c9:c9:04:6b
10.2.100.3/16 D
DHCPv4(eth0)=Enabled
DG4=10.2.1.1
DNS1:10.1.1.20
DNS2:10.1.1.31
INET6 fe80::2d0:c9ff:fec9:46b/64
DHCPv6(eth0)=Disabled
[spadmin@Spectracom ~]$ net settings
Hostname: Spectracom
Main IPv4 default gateway: 10.2.1.1
Main IPv6 default gateway: None
```

DHCP (V4 and V6)

A) DHCP4

Get all current DHCP settings: **dhcp4get**

Get current DHCP setting for one particular port: **dhcp4get <interface>** (such as **dhcp4get 0**)

- **Enable DHCP setting**: **dhcp4set <interface> on** (such **as dhcp4set 0 on**)
- **Disable DHCP setting: dhcp4set <interface> off** (such as **dhcp4set 0 off**)

B) DHCP6

➢ To set a static IPv6 address, you must first turn off DHCP for IPv6

- **dhcp6get** Display whether DHCP is enabled. Get all current DHCP settings
- **dhcp6set 1 off** turning off dhcp on port eth1.

Get current DHCP setting for one particular port: **dhcp4get <interface>** (such as **dhcp4get 0**)

- **Enable DHCP setting**: **dhcp4set <interface> on** (such **as dhcp4set 0 on**)
- **Disable DHCP setting: dhcp4set <interface> off** (such as **dhcp4set 0 off**)

- **dhcp6get** – Display whether DHCP is enabled.
- **dhcp6set 1 off** – turning off dhcp on port eth1.

****Assigning network settings

- **IP4get** <interface> (such as IP4get 0)
- **IP4set** <interface> <address> <mask> (such as **IP4set 0 10.10.200.1 255.255.255.0**)

IP Address

- **Get current IPv4 address** (can't display all at once): **IP4get** <interface> (such as **IP4get 0**)
- **Set IP address: IP4set** <interface> <address> <mask> (such as **IP4set 0 10.10.200.1 255.255.255.0**)

Gateway addresses (Main default gateway as well as the gateway address for each port)

A) IPv4 gateway

Get current gateway address:

- **gw4get** Displays gateway address for all Ethernet ports.
- **gw4get <interface>** (such as **gw4get 0**) for one particular gateway address

  Note <interface> is 0, 1, 2, 3 or m for main default gateway.

Enable and set gateway address: **gw4set <interface>** <'**gateway address>** (example **gw4set m 10 10.10.200.1**)

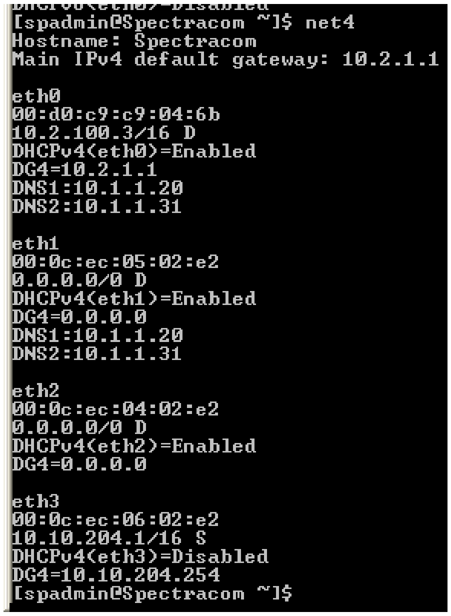
Get (read)

- ○ CLI command to read which port is the main default gateway: **gw4get m** <enter> (where m is for main)
- ○ CLI command to read the gateway address for a particular Ethernet port (eth2 for example): **gw4get 2** <enter>

Set

- ○ CLI command to set which port is the main default gateway: **gw4set m x y** <enter> (where **m** is for “main”, **x** is the gateway address and **y** is the port number.

  Example to make the default port 2: **gw4set m 10.2.1.1 2 <enter>**



```
DHCPv6<eth0>=Disabled
[spadmin@Spectracom ~]$ net4
Hostname: Spectracom
Main IPv4 default gateway: 10.2.1.1

eth0
00:d0:c9:c9:04:6b
10.2.100.3/16 D
DHCPv4<eth0>=Enabled
DG4=10.2.1.1
DNS1:10.1.1.20
DNS2:10.1.1.31

eth1
00:0c:ec:05:02:e2
0.0.0.0/0 D
DHCPv4<eth1>=Enabled
DG4=0.0.0.0
DNS1:10.1.1.20
DNS2:10.1.1.31

eth2
00:0c:ec:04:02:e2
0.0.0.0/0 D
DHCPv4<eth2>=Enabled
DG4=0.0.0.0

eth3
00:0c:ec:06:02:e2
10.10.204.1/16 S
DHCPv4<eth3>=Disabled
DG4=10.10.204.254
[spadmin@Spectracom ~]$
```

B) IPv6 gateway address

NOTICE: IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 netwok while configuring. Otherwise the config changes won’t be accepted.

➢ Refer also to: **Interface gateway addresses (IPv4/IPv6)

gw6set 1 xxx.xxx.xxx.xxx – sets the IPv6 gateway address

Usage: gw6set <on|off> [addr]
  addr: IPv6 address, ie. fe80::230:64ff:fe04:3ef8

Email from Ron D (19 Sep 17) about the IPv6 link-local address, in software version 5.7.1 the functionality to set the IPv6 gateway to the link-local address was only added to the CLI.

To set the IPv6 gateway to the link-local address the gw6set command needs to be used.
The command usage is: “gw6set <on|off> [addr] <intfc>”

Where “addr” would be the link-local address and “intfc” is the Ethernet interface to apply it to. So an example of the command to set the link-local address as the gateway for eth0 would be “gw6set on fe80:: 0”.

- ip6add 1 (IP xxx.xxx.xxx.xx) (subnet address xxx.xxx.xxx.xxx) (gateway address xxx.xxx.xxx.xxx)
  - ○ ip6add 1 xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx (adds IPv6 IP address, subnet and gateway for eth1)

Issues with configuring IPv6 gateway address (such as not being able to use a link-local address)

- Refer to: **Interface gateway addresses (IPv4/IPv6)

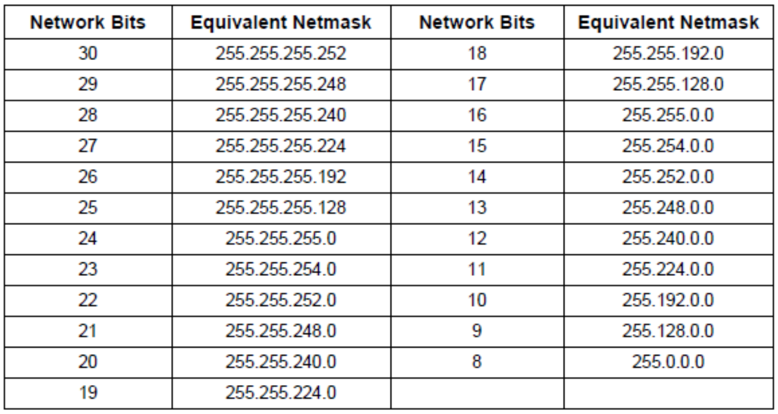
Ifconfig / ip addr

- just type "**ifconfig**" or "**ip addr**"

Function: allows the operating system to setup network interfaces and allow the user to view information about the configured network interfaces.

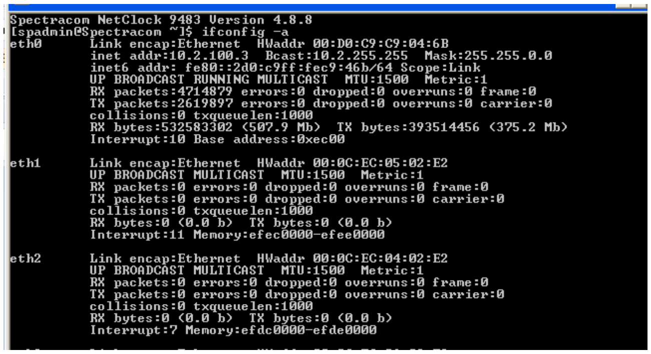
Displays: all IP addresses, subnet masks, MAC addresses, received/transmitted packets, dropped packets, packet collisions, etc

Netmask conversion table for quick-reference



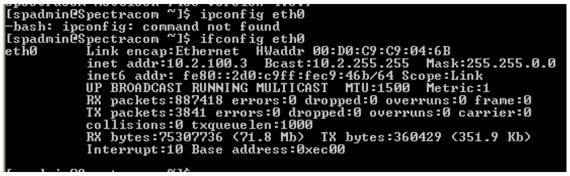
Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
30	255.255.255.252	18	255.255.192.0
29	255.255.255.248	17	255.255.128.0
28	255.255.255.240	16	255.255.0.0
27	255.255.255.224	15	255.254.0.0
26	255.255.255.192	14	255.252.0.0
25	255.255.255.128	13	255.248.0.0
24	255.255.255.0	12	255.240.0.0
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		

Ifconfig -a (Shows status of all network ports) (example below just shows a couple of the Ethernet ports)



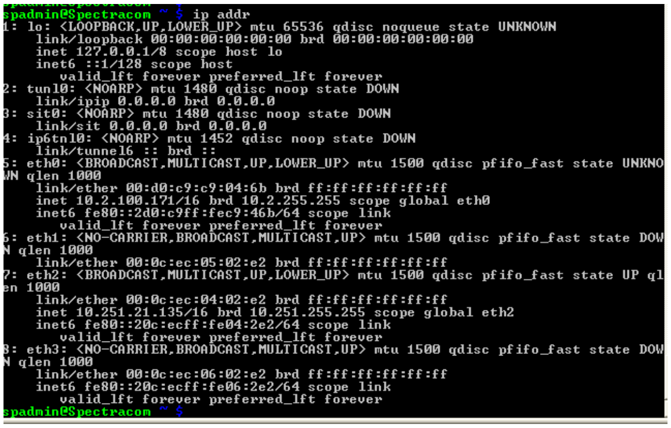
```
Spectracom NetClock 9483 Version 4.8.8
[spadmin@Spectracom ~]$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:D0:C9:C9:04:6B
          inet addr:10.2.100.3  Bcast:10.2.255.255  Mask:255.255.0.0
          inet6 addr: fe80::2d0:c9ff:fec9:46b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4714879 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2619897 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:532583302 (507.9 Mb)  TX bytes:393514456 (375.2 Mb)
          Interrupt:10 Base address:0xec00

eth1      Link encap:Ethernet  HWaddr 00:0C:EC:05:02:E2
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:11 Memory:efec0000-efee0000

eth2      Link encap:Ethernet  HWaddr 00:0C:EC:04:02:E2
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:7 Memory:efdc0000-efde0000
```

ifconfig etho (Shows only Eth0 status) – same for Eth1, Eth2 or Eth3



```
[spadmin@Spectracom ~]$ ipconfig eth0
-bash: ipconfig: command not found
[spadmin@Spectracom ~]$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:D0:C9:C9:04:6B
          inet addr:10.2.100.3  Bcast:10.2.255.255  Mask:255.255.0.0
          inet6 addr: fe80::2d0:c9ff:fec9:46b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:887418 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3841 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:75307736 (71.8 Mb)  TX bytes:360429 (351.9 Kb)
          Interrupt:10 Base address:0xec00
```

IP addr (IP Address)



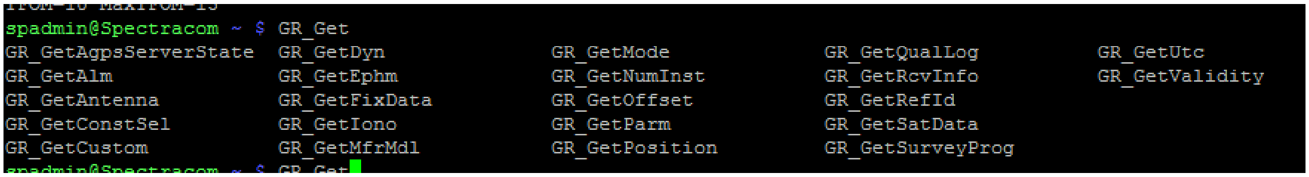
```
spadmin@Spectracom ~ $ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: tunl0: <NOARP> mtu 1480 qdisc noop state DOWN
    link/ipip 0.0.0.0 brd 0.0.0.0
3: sit0: <NOARP> mtu 1480 qdisc noop state DOWN
    link/sit 0.0.0.0 brd 0.0.0.0
4: ip6tnl0: <NOARP> mtu 1452 qdisc noop state DOWN
    link/tunnel6 :: brd ::
5: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNO
WN qlen 1000
    link/ether 00:d0:c9:c9:04:6b brd ff:ff:ff:ff:ff:ff
    inet 10.2.100.171/16 brd 10.2.255.255 scope global eth0
    inet6 fe80::2d0:c9ff:fec9:46b/64 scope link
       valid_lft forever preferred_lft forever
6: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOW
N qlen 1000
    link/ether 00:0c:ec:05:02:e2 brd ff:ff:ff:ff:ff:ff
7: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql
en 1000
    link/ether 00:0c:ec:04:02:e2 brd ff:ff:ff:ff:ff:ff
    inet 10.251.21.135/16 brd 10.251.255.255 scope global eth2
    inet6 fe80::20c:ecff:fe04:2e2/64 scope link
       valid_lft forever preferred_lft forever
8: eth3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOW
N qlen 1000
    link/ether 00:0c:ec:06:02:e2 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::20c:ecff:fe06:2e2/64 scope link
       valid_lft forever preferred_lft forever
spadmin@Spectracom ~ $
```

Configure Static Routes

Refer to “Static Routes” (Static Routing) in the “Network” section further below in this document

GPS info (“GR_” commands)

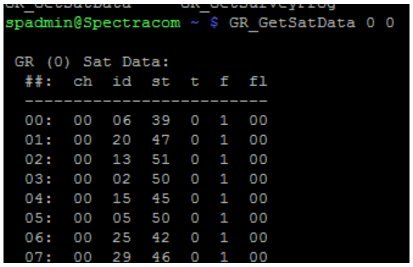
Refer also to the GPS section of this document: GPS input



```
spadmin@Spectracom ~ $ GR_Get
GR_GetAgpsServerState  GR_GetDyn        GR_GetMode       GR_GetQualLog    GR_GetUtc
GR_GetAlm              GR_GetEphm       GR_GetNumInst    GR_GetRcvInfo    GR_GetValidity
GR_GetAntenna          GR_GetFixData    GR_GetOffset     GR_GetRefId
GR_GetConstSel         GR_GetIono       GR_GetParm       GR_GetSatData
GR_GetCustom           GR_GetMfrMdl     GR_GetPosition   GR_GetSurveyProg
spadmin@Spectracom ~ $ GR_Get
```

Specific examples

Signal strengths and number of satellites being tracked



```
spadmin@Spectracom ~ $ GR_GetSatData 0 0

 GR (0) Sat Data:
  ##:  ch  id  st  t  f  fl
  -------------------------
  00:  00  06  39  0  1  00
  01:  00  20  47  0  1  00
  02:  00  13  51  0  1  00
  03:  00  02  50  0  1  00
  04:  00  15  45  0  1  00
  05:  00  05  50  0  1  00
  06:  00  25  42  0  1  00
  07:  00  29  46  0  1  00
```

Reading/ manually setting Date and Time (via cli or browser)

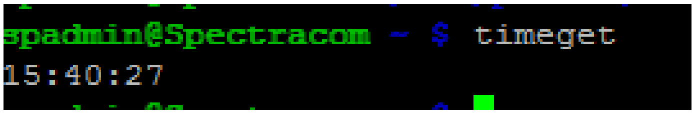
IMPORTANT NOTE: USER/USER input reference **MUST** be enabled in the reference priority table in order to be able to manually change the date/time via the web browser, CLI interface (such as dateset or doyset) or front panel. If USER/USER is not enabled, the time/date will not be changed.

- Note: If any inputs are present and valid with a higher priority than the user/user reference, the higher priority reference will override the manual set time.

A) timeget/timeset (System Time)

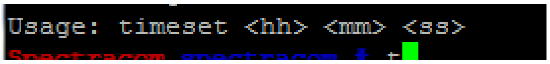
In addition to the time being displayed in the browser, the SecureSync's UTC time can also be queried using a CLI command (via a telnet or SSH session). The CLI command to read the current time is "**timeget**" as shown below:

timeget



```
spadmin@Spectracom ~ $ timeget
15:40:27
```

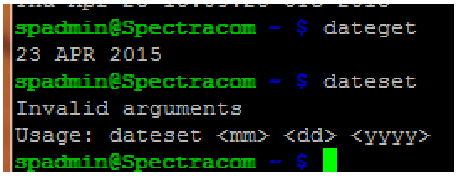
timeset



```
Usage: timeset <hh> <mm> <ss>
```

B) dateget/dateset (System Date)

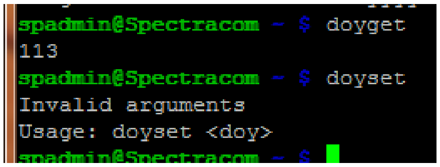
- **dateget** retrieves the System Date
- **dateset** is used to set the System Date



```
spadmin@Spectracom ~ $ dateget
23 APR 2015
spadmin@Spectracom ~ $ dateset
Invalid arguments
Usage: dateset <mm> <dd> <yyyy>
spadmin@Spectracom ~ $
```

C) Doyset/doyget (System Day of Year)

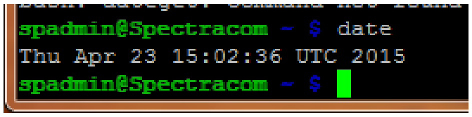
doyget and **doyset**



```
spadmin@Spectracom ~ $ doyget
113
spadmin@Spectracom ~ $ doyset
Invalid arguments
Usage: doyset <doy>
spadmin@Spectracom ~ $
```

D) Date (Linux OS date and time)

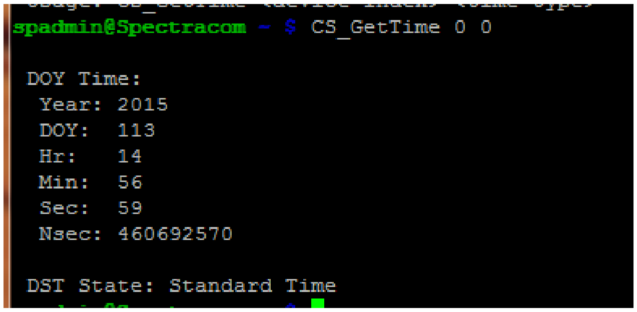
The **date** command reads the Linux OS date and time (not the System Time's date). The proper CLI command to read the current System Date is instead "**date**" as shown above:



```
spadmin@Spectracom ~ $ date
Thu Apr 23 15:02:36 UTC 2015
spadmin@Spectracom ~ $
```

E) CS_GetTime 0 0 <enter>

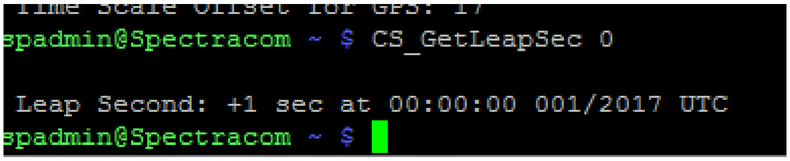
- ➢ This KTS call reads the System Date and Time and is also used in the system to update the front panel.



```
spadmin@Spectracom ~ $ CS_GetTime 0 0

 DOY Time:
  Year: 2015
  DOY:  113
  Hr:   14
  Min:  56
  Sec:  59
  Nsec: 460692570

 DST State: Standard Time
```

F) **Obtaining the next scheduled leap second**

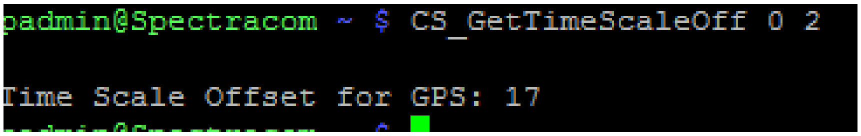
CS_getLeapSec 0



```
spadmin@Spectracom ~ $ CS_GetLeapSec 0

 Leap Second: +1 sec at 00:00:00 001/2017 UTC
spadmin@Spectracom ~ $
```

G) **Get the offset (in seconds) between GPS time and UTC time**

CS_GetTimeScaleOff 0 2 (where the "2" indicates the offset for GPS time scale)

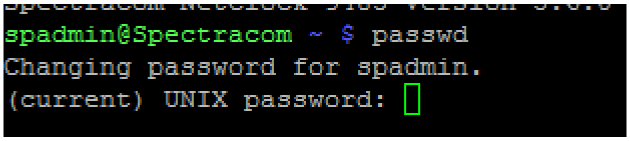


```
padmin@Spectracom ~ $ CS_GetTimeScaleOff 0 2

Time Scale Offset for GPS: 17
```

Change the spadmin account password via CLI

passwd

- Per the note futher below, in at least versions 5.7.0 and below, the rules for passwords being created/changed in the browser are not being applied to passwords being changed via the CLI.
  - **Per JIRA-SSS-259:** See info further below about a post 5.7.0 update intending on the ability to configure the password via CLI being forbidden. Due to the password rules only being available via the browswer, this intention is to prevent anyone from using the cli to change a password, with no restrictions on the intended password.



```
spadmin@Spectracom ~ $ passwd
Changing password for spadmin.
(current) UNIX password:
```

Note about the available "Password Security" Rules in the browser (Management -> Authentication page)

- Per Salesforce case 25067, and in at least versions 5.7.0 and below, the Password Security rules that can be custom configured in the browser (such as special characters, min length, expiry, etc) don't currently apply to the passwd command. These available 'rules' ONLY apply when creating/changing passwords via the BROWSER.
  - Reference **JIRA ticket SSS-259** (https://spectracom.atlassian.net/browse/SSS-259)
  - For more info on Password Security rules: Password Security" (Available minimum password requirements that can be enforced, if desired)

Follow-up status from Engineering/Product Management on this condition

Email from Paul Myers (4 Aug 17, referring to a planned change in post v5.7.0) JIRA-SSS-259 is changed to FORBID use of passwd command to change passwords for any users other than spfactory or root.

User's must change passwd and passwd rules form Web UI.Change approved by Product Management for SecureSync: David Sohn.

Model and Unit's Serial Number

model

```
spadmin@setimex1 /usr/cli $ model
        SecureSync
        Model No: 1200-233
        Serial No: 05861
```

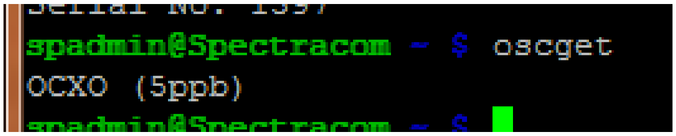
Note: To change the Model Number, login as **spfactory** and type **modno**

Oscillator type and Serial Number

Type of osc installed

Oscget (or **XO_GetOscType 0**)

```
spadmin@setimex1 /usr/cli $ oscget
```



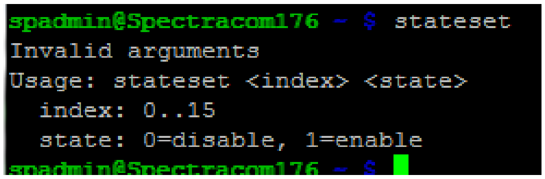
```
Serial No: 1397
spadmin@Spectracom ~ $ oscget
OCXO (5ppb)
spadmin@Spectracom ~ $
```

Rubidium (**.1ppb**)

Osc Serial Number:

XO_GetSerialNo 0

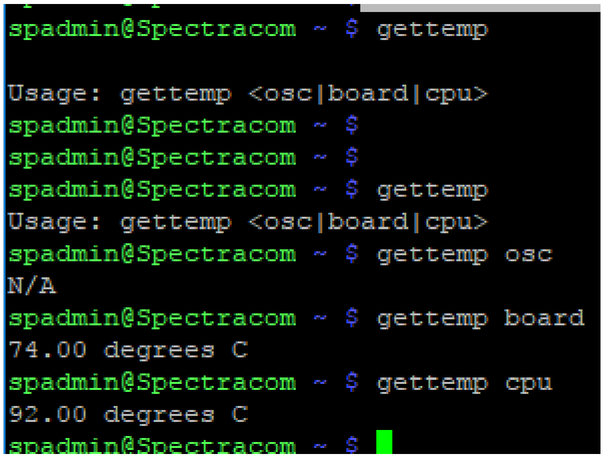
Enable/disable entries already in the Reference Priority table (changes the "State")
stateset



```
spadmin@Spectracom176 ~ $ stateset
Invalid arguments
Usage: stateset <index> <state>
  index: 0..15
  state: 0=disable, 1=enable
spadmin@Spectracom176 ~ $
```

****Obtain Oscillator, board and CPU temperature readings via CLI (applicable to versions 5.4.5 and above only)**

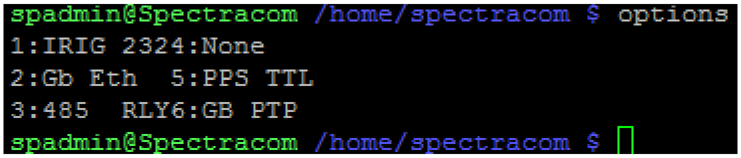
- Version 5.4.5 added the **gettemp** command to allow reading of temperatures.



```
spadmin@Spectracom ~ $ gettemp

Usage: gettemp <osc|board|cpu>
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $ gettemp
Usage: gettemp <osc|board|cpu>
spadmin@Spectracom ~ $ gettemp osc
N/A
spadmin@Spectracom ~ $ gettemp board
74.00 degrees C
spadmin@Spectracom ~ $ gettemp cpu
92.00 degrees C
spadmin@Spectracom ~ $
```

CLI command to list all installed Option Cards

options



```
spadmin@Spectracom /home/spectracom $ options
1:IRIG 2324:None
2:Gb Eth  5:PPS TTL
3:485  RLY6:GB PTP
spadmin@Spectracom /home/spectracom $
```

Note: Also in newer firmware version 5.7.1 and higher units, the "**manifest**" command will show all the system information in more detail.

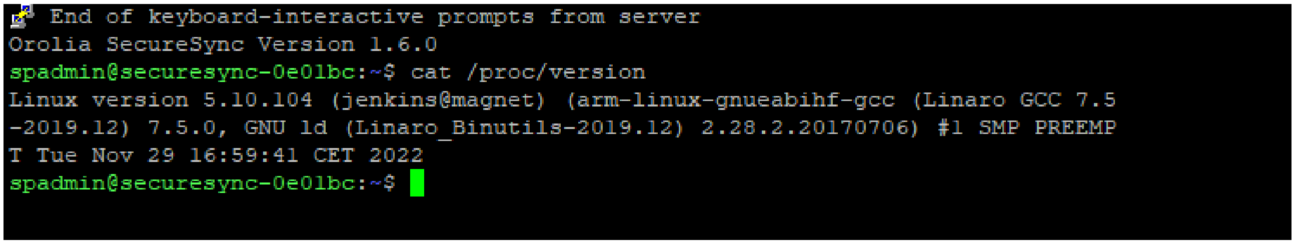
**Version commands (Linux OS and SecureSync software)

A) Read the current version of Linux OS

- 2400 SecureSync runs on a Linux OS.

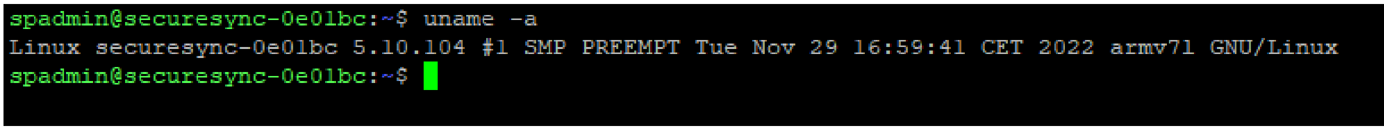
CLI commands to read Linux OS version:

cat /proc/version



```
End of keyboard-interactive prompts from server
Orolia SecureSync Version 1.6.0
spadmin@securesync-0e01bc:~$ cat /proc/version
Linux version 5.10.104 (jenkins@magnet) (arm-linux-gnueabihf-gcc (Linaro GCC 7.5
-2019.12) 7.5.0, GNU ld (Linaro_Binutils-2019.12) 2.28.2.20170706) #1 SMP PREEMP
T Tue Nov 29 16:59:41 CET 2022
spadmin@securesync-0e01bc:~$
```

uname –a



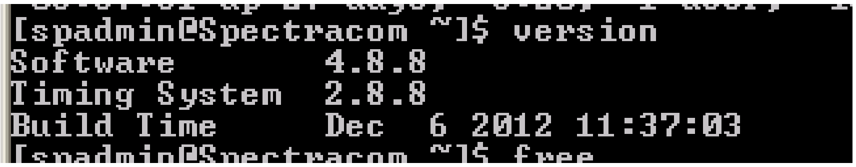
```
spadmin@securesync-0e01bc:~$ uname -a
Linux securesync-0e01bc 5.10.104 #1 SMP PREEMPT Tue Nov 29 16:59:41 CET 2022 armv7l GNU/Linux
spadmin@securesync-0e01bc:~$
```

B) SecureSync software version

available version command ("**Version xxx**") in the CLI to query for the versions of the different modules (SNMP, GPS, Apache, SSH, SSL, etc). (These values not planned to be added to the browser display). Below is a list of specific commands (with a space in between the word "version" and the module name:

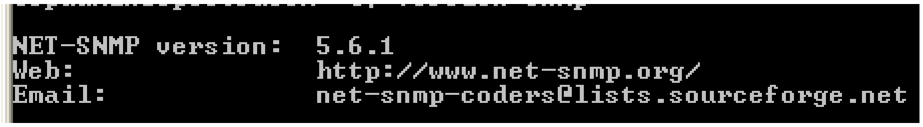
Note: First letter “version” has to be lower-case.

“**version**” (with nothing after it) reports the Archive and Timing System versions



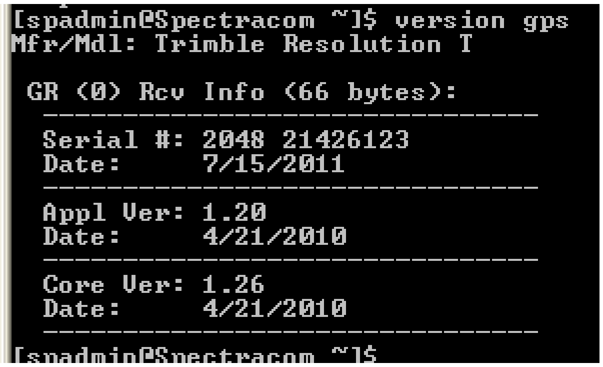
```
[spadmin@Spectracom ~]$ version
Software        4.8.8
Timing System   2.8.8
Build Time      Dec  6 2012 11:37:03
[spadmin@Spectracom ~]$ free
```

version SNMP (shown with 4.8.8 installed)



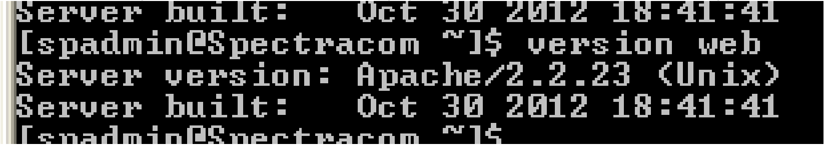
```
NET-SNMP version:  5.6.1
Web:               http://www.net-snmp.org/
Email:             net-snmp-coders@lists.sourceforge.net
```

version GPS



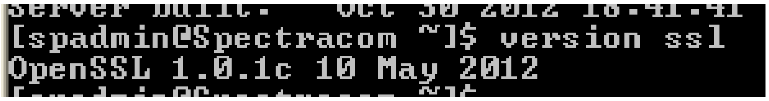
```
[spadmin@Spectracom ~]$ version gps
Mfr/Mdl: Trimble Resolution T

 GR (0) Rcv Info (66 bytes):
  ---------------------------------
  Serial #: 2048 21426123
  Date:     7/15/2011
  ---------------------------------
  Appl Ver: 1.20
  Date:     4/21/2010
  ---------------------------------
  Core Ver: 1.26
  Date:     4/21/2010
  ---------------------------------
[spadmin@Spectracom ~]$
```

version web (not “version apache”) (shown with 4.8.8 installed)



```
Server built:   Oct 30 2012 18:41:41
[spadmin@Spectracom ~]$ version web
Server version: Apache/2.2.23 (Unix)
Server built:   Oct 30 2012 18:41:41
[spadmin@Spectracom ~]$
```

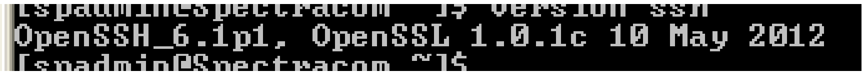
version SSL (shown with 4.8.8 installed)



```
Server built:   Oct 30 2012 18:41:41
[spadmin@Spectracom ~]$ version ssl
OpenSSL 1.0.1c 10 May 2012
[spadmin@Spectracom ~]$
```

version SSH (shown with 4.8.8 installed)

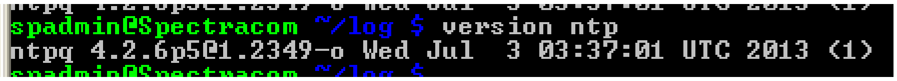
(or ssh -v)



```
[spadmin@Spectracom ~]$ version ssh
OpenSSH_6.1p1, OpenSSL 1.0.1c 10 May 2012
[spadmin@Spectracom ~]$
```

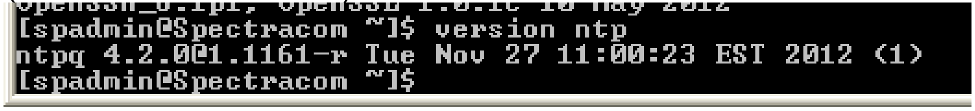
version NTP

(***shown with 5.0.2 installed***)



```
spadmin@Spectracom ~/log $ version ntp
ntpq 4.2.6p5@1.2349-o Wed Jul  3 03:37:01 UTC 2013 (1)
```

(*shown with 4.8.8 installed*)



```
[spadmin@Spectracom ~]$ version ntp
ntpq 4.2.0@1.1161-r Tue Nov 27 11:00:23 EST 2012 (1)
[spadmin@Spectracom ~]$
```

defcert or defcert -sha1 (delete the HTTPS certificate)

- The only CLI command associated with certificates is the **defcert** command (to reset the certificate back to default)
  - Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
  - An example defcer CLI syntax (5.6.0 and above only) is **defcert -sha256**
  - As IE8 and below do not support SHA-256, in versions 5.6.0 and above, use **defcert -sha1** to regenerate a new certitficate using SHA1 to gain access to IE8 and below

Email from Keith (20 Jul KW) One thing to keep in mind is that, depending on the current software version installed in the SecureSync, the **defcert** command will create its new default certificate using either a **SHA1** cipher or a **SHA256** cipher.

With software **versions 5.6.0 and above** installed in the SecureSync, the more secure SHA256 encryption cipher will be used to generate its new certificate (with version 5.5.1 and below, the defcert command used the SHA1 cipher).

The issue with the more secure SHA256 cipher is **Internet Explorer versions 8** and below can't use this newer cipher. With these more recent versions of software installed in the SecureSync (5.6.0 and above), and when using IE8 or below to access the SecureSync, instead of using the CLI command of **defcert** to replace the existing certificate, issue instead the following CLI command to generate a new certificate using the earlier SHA1 cipher: **defcert -sha1** <enter>. Then try accessing the web browser again.

GNU Bash

- SecureSyncs have GNU Bash installed
- The CLI command to obtain the Bash version is: bash -version ("dash, dash" before "version").

CLI CMMANDS FOR 1204-3D Satelles STL receiver (versions 5.6C and above only)

STR_GetSubscription 0 0

- Reports end of subscription.

```
Spectracom SecureSync Version 5.6.C
spadmin@Spectracom ~ $ STR_GetSubscription 0 0

  RESPONSE  End of Subscription: 01/06/1980
```

“STR_” error messages in System log (Versions 5.8.0 and above only)

"ERROR in KTSAL_Get:SPEC_KTSAL_EN=true STR_GetSubscription 0.0 (KTSAL)"

- Refer to SF cases such as 171405
- Caused by “**STL INFO**” menu being displayed on front panel (or rotate menus selected) with no 1204-3D/1204-3E STL card installed in the syste,
- Version 5.8.0 added the STL Info menu in all units, even if 1204-3D/3E is installed, If the unit is downogradred to below 5.8.0. this STL menu is no longer exists so the issue no longer occurs.
- if STL card isnt installed the request by the front panel to display STL data causes an error message to be asserted.

email from Keith (1 Nov 18) This “GetSubscription” entry is associated with a purchasable feature we now offer for SecureSyncs, called “STL”. In case you aren’t familiar with it, it’s a satellite signal, similar to GPS, but since these satellites are closer to the earth than the GPS constellation, their signals are stronger. There are other benefits to it, as well.

STL is available with an STL receiver Option Card and a subscription to the service. The version 5.8.0 software update added a new front panel LCD display menu which shows the signal strength of this STL signal. The error message just means that someone was scrolling through the various menu screens, which include the STL menu. But without the STL receiver/option being installed, there was no communications available to report the expected value.

This “errant” entry is expected to be no longer reported if the STL menu is selected, or scrolled thru, via a future software update. There should be no operational concerns if this entry is observed! Thanks again for asking about it, just to be sure it didn’t indicate a problem!!

**reviewing/saving/deleting logs via CLI interface

Viewing the logs in the web browser

A) Newer browser

In versions 5.1.2 to at least 5.3.1 (this is expected to be changed in 5.4.0, ~ Jan 2016) the newer (black/charcoal) browser only displays the most current set of entries (the file with no number). This is being changed to allow the newer browser to display all the logs. In the earlier versions, “all” log entries can only be displayed in the classic interface or via a cli connection.

Ability to view the logs (log entries) with the CLI interface

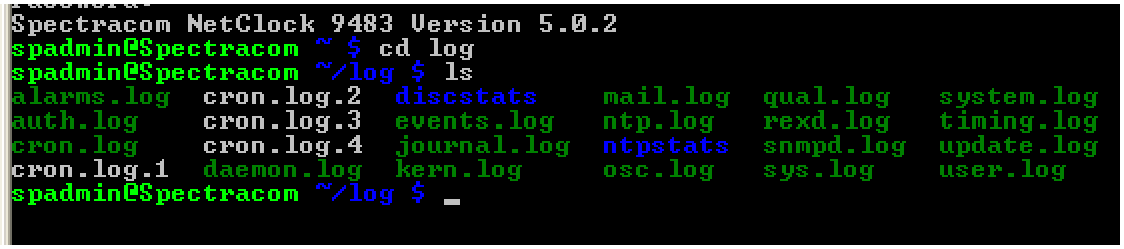
A) Login with **telnet**/ssh

B) Type **cd log** to change to the log directory

C) Type **ls** to list all log file names

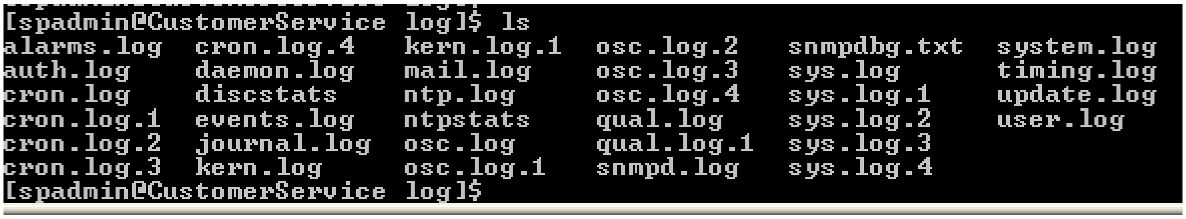
D) Type **cat** followed by the name of the log (including the file extension).

With versions 5.0.2 or higher installed



```
Spectracom NetClock 9483 Version 5.0.2
spadmin@Spectracom ~ $ cd log
spadmin@Spectracom ~/log $ ls
alarms.log   cron.log.2  discstats     mail.log  qual.log    system.log
auth.log     cron.log.3  events.log    ntp.log   rexd.log    timing.log
cron.log     cron.log.4  journal.log   ntpstats  snmpd.log   update.log
cron.log.1   daemon.log  kern.log      osc.log   sys.log     user.log
spadmin@Spectracom ~/log $ _
```

With versions 4.8.9 or prior installed



```
[spadmin@CustomerService log]$ ls
alarms.log   cron.log.4   kern.log.1   osc.log.2    snmpdbg.txt   system.log
auth.log     daemon.log   mail.log     osc.log.3    sys.log       timing.log
cron.log     discstats    ntp.log      osc.log.4    sys.log.1     update.log
cron.log.1   events.log   ntpstats     qual.log     sys.log.2     user.log
cron.log.2   journal.log  osc.log      qual.log.1   sys.log.3
cron.log.3   kern.log     osc.log.1    snmpd.log    sys.log.4
[spadmin@CustomerService log]$
```

Viewing the log bundle file on a linux box or Windows PC

Q What linux command line argument can I use to “untar” the log files so I can read them?

A Keith’s response (12 Jan 17) : The log bundle is a tar.gz file. You can use “**tar**” in linux to examine the log bundle. Or, you can also use either Winzip or 7-zip in a Windows PC to open the bundle.

Ability to Save/backup logs via CLI

- Version 4.8.8 (Dec 2012-ECN 3099) Added **savelog** CLI command to handle log backup.
- Versions 4.8.7 and below- not available

savelog <file name> <enter>

- This command saves the system log bndle to the following directory: /Home/Spectracom/Xfer/Log
- Then the user can manually FTP/SCP the log bundle file from this directory.

Note:

- **FTP port is port 21**
- **SCP port is port 22**

Ability to delete the logs via CLI

- Version 5.1.5 introduced the **clearlogs** CLI command
- Can’t delete the logs via CLI before version 5.1.5

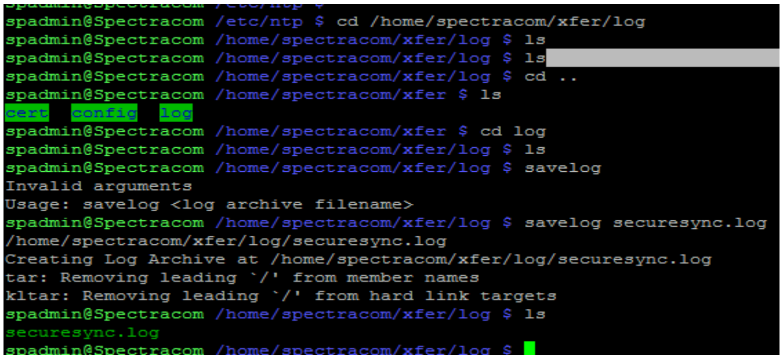
Saved log bundle way too small (only ~15kb) when downloaded using browser and only contains HTML code when opened

- Update to bullet directly below (11 Dec 15 KW) it now appears this condition is caused by the log bundle file being too large to download using the web browser. This particular conditon was noticed again with another unit and Ron Dries had the customer look at the size of the log file while still in the SecureSync. It was a valid size, even though it was only 15kb when downloaded using the browser. Log bundle was also confirmed f fine after extracting it via the CLI (FTP/SFP

Email from Ron to Eric Girard (11 Dec 15) Could you have him check the log bundle on the SecureSync in the /home/spectracom/xfer/log directory?
Check to make sure that the bundle was created around the time that he clicked the save and download logs button, and the file size.

To do this have him issue the following command in the directory: “ls –la” and send us the screenshot, and if the bundle is there have him send us that as well.
I had this happen to me, and what it looked like is we were saving the log bundle on the system but it was too large to download from the web UI.

Temporary work-around if this condition happens: After saving/creating the log bundle in the browser (or performing a **savelog** CLI command) manually extract the bundle using FTP or SCP (instead of using the browser to download it). The securesync.log bundle file is located in the following directory: /home/spectracom/xfer/log



```
spadmin@Spectracom /etc/ntp $
spadmin@Spectracom /etc/ntp $ cd /home/spectracom/xfer/log
spadmin@Spectracom /home/spectracom/xfer/log $ ls
spadmin@Spectracom /home/spectracom/xfer/log $ ls
spadmin@Spectracom /home/spectracom/xfer/log $ cd ..
spadmin@Spectracom /home/spectracom/xfer $ ls
cert  config  log
spadmin@Spectracom /home/spectracom/xfer $ cd log
spadmin@Spectracom /home/spectracom/xfer/log $ ls
spadmin@Spectracom /home/spectracom/xfer/log $ savelog
Invalid arguments
Usage: savelog <log archive filename>
spadmin@Spectracom /home/spectracom/xfer/log $ savelog securesync.log
/home/spectracom/xfer/log/securesync.log
Creating Log Archive at /home/spectracom/xfer/log/securesync.log
tar: Removing leading `/' from member names
kltar: Removing leading `/' from hard link targets
spadmin@Spectracom /home/spectracom/xfer/log $ ls
securesync.log
spadmin@Spectracom /home/spectracom/xfer/log $
```

- Per Ron and Paul (9 Nov 15) they believe this is a factor of the SecureSync still being in an abnormal state when the logs were bundled.
    - They recommend rebooting the unit and then try saving the logs again.

Example entries below, when this condition has occurred

```
!DOCTYPE html>
<html>
<head>
  <!-- Always force latest IE rendering engine or request Chrome Frame -->
  <meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible">
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />    <!--nocache-->
    <title>
        MEY-MNC02    </title>
    <!--/nocache-->
    <link href="/favicon.ico" type="image/x-icon" rel="icon" /><link href="/favicon.ico" type="image/x-icon" rel="shortcut icon" /><link rel="stylesheet" type="text/css" href="/css/lafayette.css" /><script type="text/javascript" src="/js/lafayette.js"></script><script type="text/javascript" src="/js/helper.js"></script>
    <!--[if lt IE 9]>
    <script type="text/javascript" src="/js/html5shiv.js"></script><script type="text/javascript" src="/js/excanvas.js"></script><script type="text/javascript" src="/js/iefix.js"></script><link rel="stylesheet" type="text/css" href="/css/iefix.css" />    <![endif]-->

    <script type="text/javascript" src="/util/dygraph-combined.js"></script>
   <meta name="viewport" content="width=device-width, maximum-scale=1, initial-scale=1, user-scalable=0">

  </head>
<body>

<div class="container-fluid page-container">
    <!--nocache-->
    <script type="text/javascript">$(document).ready( function() {});</script>    <!--/nocache-->
        <div id="banner">
        <div class="row-fluid">
            <div id="bannerTop" class="span12">
                <div class="row-fluid">
                    <div id="bannerLogo" class="logo span5 pull-left"></div>
                    <div id="bannerDeviceName" class="Devicename span4 pull-right">
                        <div class='elem_DeviceName'>
    <span> <a href="/">SecureSync</a>    </span>

              </div>
```

Desire to automatically delete the logs on a periodic schedule

Q Can we automate (or setup) log cleaning on the Spectracom GPS-Clock for a predetermined period ?

A Keith's response: The short answer is the logs cannot be automatically deleted/cleaned based on a predetermined period. Instead, each log file (such as the Alarms log, Events log, Qualification log, etc) is independently cleared as necessary, based on a defined log file size (the logs are rotated to delete the oldest entries first).

The longer answer: When the unit's logs are configured to be stored within the time server (this is the factory default configuration, as configured in the **Management** -> **Log Configuration** page of the browser. Note most of the logs can be optionally sent to a syslog server and configured not to be stored in time server at all) each individual log file is automatically rotated and cleared, when each file has reached a certain size. After the earliest log entices have been rotated to a fourth log file of a similar name, the oldest entries of that particular log file are deleted.

Besides configuring the logs to not be stored in the server- they can instead just be sent to a remote Syslog server (and the factory default hard-set log rotation in the software) there is no other way to internally automate the logs being deleted on a specified/periodic basis.

However, there is a CLI command that will delete the logs (the logs can be commanded to be cleared/deleted via either the browser or CLI). If desired, they can create a custom script that logs into the CLI interface (telnet or SSH) when desired and then performs the CLI command: clearlogs <enter> (this command is available in software versions 5.2.1 and above).

Testing SNMP traps and email alerts (testevent and sendtrap commands)

- Refer to (in this document): **Testing/Verifying SNMP/Email alerts are enabled and working inside the SecureSync

System Start-Up sequence/boot-up and intial effects of Signature Control on outputs

Special patch modifying start-up sequence of GPS sync (~Jun 2018)

- Reference Salesforce Case 164267
- Refer also to emails/patch located at: ..\..\PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates\Previous-debug SecureSync updates\1-patches not changing version\SF Case 164267 startup sequence

Reported issue: AS we discussed yesterday we have a customer, **EF Johnson having issues with the Securesync power on sequence. Their Securesyncs with signature control set for “Enabled in Holdover” will continuously output the 10 MHz and 1PPS upon startup. The Securesync will go right into Holdover mode and the outputs remain on, which causes major problems for their radio transmitter when the Securesync syncs to GPS and the timing shifts.**
We discussed writing a script or modifying the config file to allow the system to startup with no references available for sync.

Another email from Dave L (4 Jun 18) They have updated to v5.8.0 and their system is continuously powering up and going immediately into Holdover mode. The desired operation is to output only good timing using Signature Control in Sync and Holdover modes after the Securesync has synchronized and stabilized. Having the Securesync go into Holdover mode before the timing is good negatively affects their radio transmitters.

Sometimes it comes up In Holdover right away and other times it comes up Out of Sync and operates as expected. The Securesync is not consistent.

Start-up Questions/Answers

Note: Customer questions and answers in red below from Keith (18 Jan 2017)

1. **Upon application of 28VDC power, how soon do each of the output signals (IRIG, 10MHz) appear?**

   Keith’s response: The SecureSync’s 10 MHz output will be present moments after input power is applied. The 10 MHz output will be disciplined/aligned to GPS 1PPS within about 10 minutes or so, once the Sync LED has turned green (indicating the SecureSync is synced to GPS). Once the oscillator has locked to GPS, the Frequency Error alarm will clear, and the associated front panel red Fault LED will also extinguish (indicating all asserted alarms have now been cleared).

   The IRIG output will be present within about one minute or so after applying power (once the software is up and running).

2. **Is the appearance of these signals dependent on GPS receiver lock?**

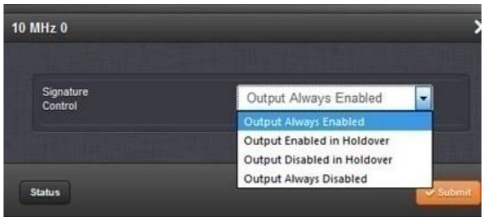
   Keith’s response: Unless “**Signature Control**” has been enabled for each of these outputs, the 10 MHz and IRIG outputs will be present, regardless of GPS receiver lock/sync state. Signature Control (which is disabled by factory default settings) is an available configuration for each individual output, which can start squelching each output (once the software is up and running) until GPS input is valid and the SecureSync has gone into sync. Signature Control is used to also squelch each output if the SecureSync loses all input references after it has achieved sync, since it was last booted-up (either right then or after a period of time of having no references available).

   Note the 10 MHz output (a hardware output, not requiring the software to be running before being provided) will be present some time before the software (and therefore the Signal Control function, if enabled) can squelch this output. Once the software is up and running (and therefore Signature Control has “kicked-in”), this signal will be squelched until the SecureSync has achieved sync.

   The IRIG output requires software to be up and running before it can be provided. Initially after the software is running, it will be configured using all of its default settings (IRIG B, 1kHz, Signature Control not enabled) and the output will be present. Then very shortly after the software is running, the unit will have all of its user-configurations applied (replacing the default configs as applicable). If the IRIG output’s Signature Control setting has been changed from the default value (Output always enabled) to either “**Output Enabled in Holdover**” or “**Output Disabled in Holdover**” the IRIG output will be squelched at that point until sync has been achieve to an input reference.

Below for your reference are two screenshots from the web browser, just so you can see the Signature Control settings I am referring to above"

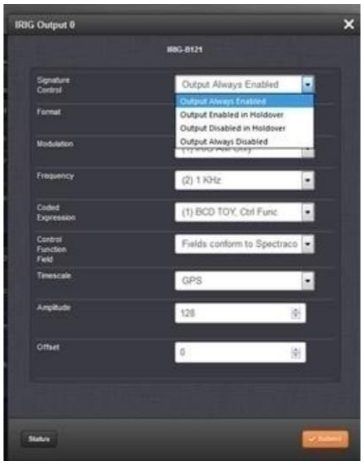
10 MHz output (Interfaces -> 10 MHz 0 page of the browser)



10 MHz 0

Signature Control: Output Always Enabled

IRIG output (Interfaces -> IRIG output 0 page)



IRIG Output 0

IRIG-B121

Signature Control: Output Always Enabled

Format

Modulation

Frequency: (2) 1 KHz

Coded Expression: (1) BCD TOY, Ctrl Func

Control Function Field: Fields conform to Spectraco

Timescale: GPS

Amplitude: 128

Offset: 0

Note about the available selections for Signature Control

The factory default Signature Control setting for all outputs is: **"Output Always Enabled"** (no Signature Control/squelching of this particular output occurs).

"**Output enabled in Holdover**" means this particular output is present while the SecureSync is in sync to an input reference, and also for a user-configurable allotted amount of tine after losing all input references (this allotted period of time is called "Holdover"). The default allotted amount of time is 2 hours after losing all input references and then sync is completely lost if no references have been restored. This value is configured in the **Management -> Disciplining** page of the browser with a range of 1 second to 5 year). While in Holdover mode, the SecureSync remains "in sync".

"**Output Disabled in Holdover**" means this particular output is only present while an input reference is actively present/valid. If the SecureSync goes into Holdover mode due to losing all input references, this particular output will be squelched at that point, until at least one input reference has been restored. With this setting selected, this particular output is not present while in Holdover mode.

2) What is the range of time it can take for the GPS receiver to lock?

Keith's response: It can take up to about 13 minutes for the SecureSync to go into GPS lock. The GPS satellites transmit a particular value (the GPS to UTC offset value) every 12.5 minutes, which needs to be received by the SecureSync's receiver before the SecureSync can achieve sync. The length of time it takes to sync is dependent on how long before the GPS satellites transmit this value again, in relation to when the SecureSync and its receiver are powered-up.

For example, if the receiver powers up two minutes before this data is transmitted, and as long as the receiver is tracking at least four satellites (as required for a 3-D fix) it will only take 2 minutes to sync.

3) What happens if we don't issue a HALT command when powering down?

Keith's response: This is a very good question, and I have some information for you that I hope will help alleviate any concerns that you may have about this:

Like any other computer, it is always best to stop the programs that are currently running before just pulling the power cord out of the computer. Otherwise, there is always that small chance that you could corrupt a program this was running at power down. So, computers usually internally stop all processes before they power-down, just to be safe. The HALT command is the method used to stop all processes in the SecureSync before powering power.

The Halt Command is provided to promote file system stability. It does take time to preserve data in the file system. Using halt to shut-down the SecureSync rather than just removing power ensures log data, and configuration information being written to the file system is successfully stored. Also, it avoids any issues of file system corruption. The file system can recover from corruption and errors. However, to avoid file system corruption the use of Halt is recommended. Also if a file error was to occur, the file system will try to fix it the next time the unit is booted up. This process could cause the power-on to take longer than normal.

**Configs/configurations (Save configs /Backup and restore configs/Clean Configs)

Security considerations/default and recommended configurations

- Refer to: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Security- Vulnerabilities

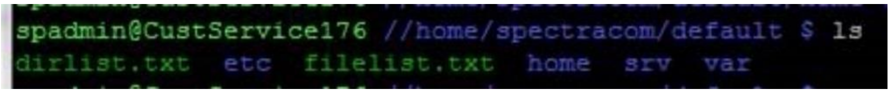
Note: The best source of info about securing/hardening the SecureSync for security is the "**Default and Recommended Configurations**" section of the online 2400 SecureSync user guide: https://orolia.com/manuals/SS/Content/NC_and_SS/Com/Topics/ADMIN/Conf_Def_Recom.htm

Factory default settings/default configs

- Refer to "**Default and Recommended Configurations**" section of the online 2400 SecureSync user guide: https://orolia.com/manuals/SS/Content/NC_and_SS/Com/Topics/ADMIN/Conf_Def_Recom.htm

The factory default configurations, for "Restore Factory Defaults(Clean)" are stored in a separate directory (amongst four different directores, in this main directory).

? All the factory default settings are stored in the **home/spectracom/default** directory. As shown below, the default settings are stored in the etc, home, srv and var directories as applicable (as defined by the dirlist.txt and filelist.txt files in the same default dectory).



```
spadmin@CustService176 //home/spectracom/default $ ls
dirlist.txt  etc  filelist.txt  home  srv  var
```

Easily finding potential configuration issues with a customer's unit

Instead of side-by-side, line-by-line comparing a customer's file to one of our files, use a third part "diff" program for Windows (such as either WinMerge or KDiff) to compare their file to a default config file. It will show all of the config changes that have been made.

*Desire to change configs that aren't directly accessible to the user.

- Example: desire to alter the list of ciphers we support. Customers don't have "access" to this via the browser.

Steps

1) Perform a config save.
2) Edit the config save.
3) Perform a config restore.

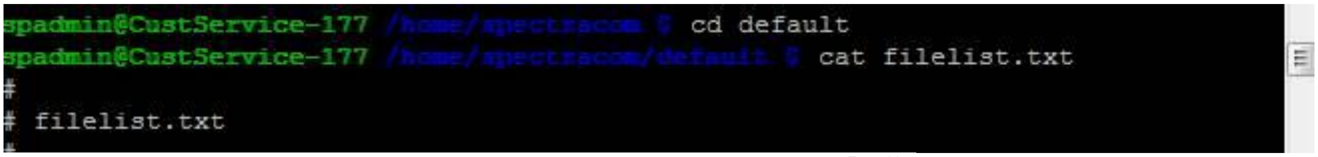
Note: the changed file(s) will be reset back to factory default if a clean is ever performed.

**Backup/restore configs (configuration files)

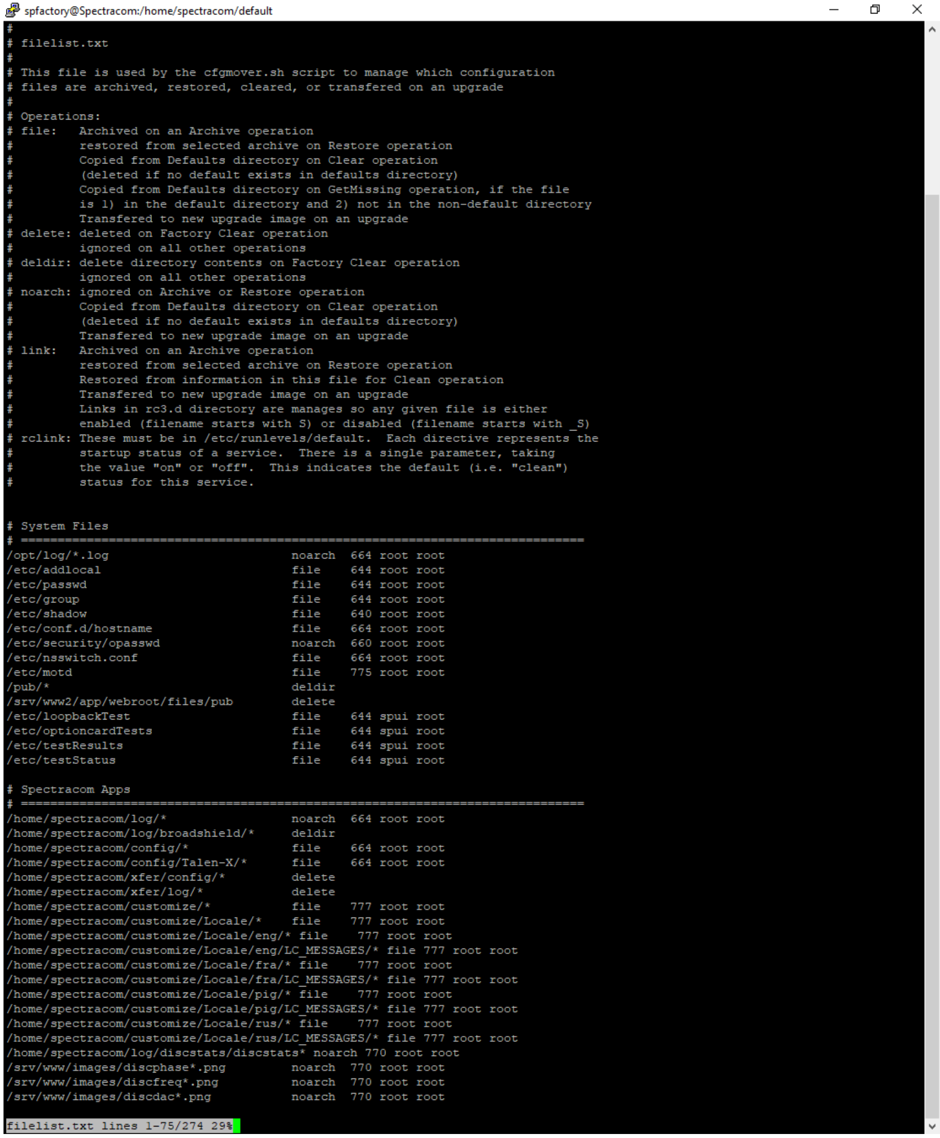
- Refer to the Config backup/restore Tech Note: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Backup-restore configs

List of all files/configs that are backed-up to the saved .conf file (as spfactory account)

- In the **home/spectracom/default** directory –> cat or less “filelist.txt”
- “**file**” items in this list are backed up to the saved.conf file. “**noarch**” and “**delete**” items are not backed-up into the saved .conf file.
- “q” to exit out



```
spadmin@CustService-177 /home/spectracom $ cd default
spadmin@CustService-177 /home/spectracom/default $ cat filelist.txt
#
# filelist.txt
#
```



spfactory@Spectracom:/home/spectracom/default

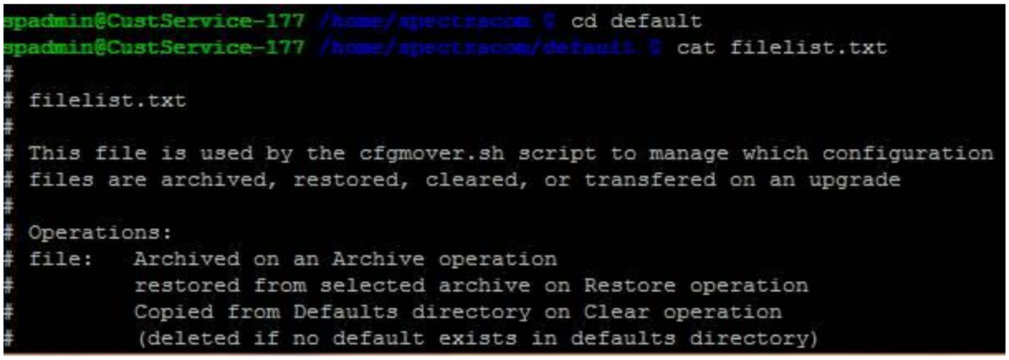
```
#
# filelist.txt
#
# This file is used by the cfgmover.sh script to manage which configuration
# files are archived, restored, cleared, or transfered on an upgrade
#
# Operations:
# file:   Archived on an Archive operation
#         restored from selected archive on Restore operation
#         Copied from Defaults directory on Clear operation
#         (deleted if no default exists in defaults directory)
#         Copied from Defaults directory on GetMissing operation, if the file
#         is 1) in the default directory and 2) not in the non-default directory
#         Transfered to new upgrade image on an upgrade
# delete: deleted on Factory Clear operation
#         ignored on all other operations
# deldir: delete directory contents on Factory Clear operation
#         ignored on all other operations
# noarch: ignored on Archive or Restore operation
#         Copied from Defaults directory on Clear operation
#         (deleted if no default exists in defaults directory)
#         Transfered to new upgrade image on an upgrade
# link:   Archived on an Archive operation
#         restored from selected archive on Restore operation
#         Restored from information in this file for Clean operation
#         Transfered to new upgrade image on an upgrade
#         Links in rc3.d directory are manages so any given file is either
#         enabled (filename starts with S) or disabled (filename starts with _S)
# rclink: These must be in /etc/runlevels/default.  Each directive represents the
#         startup status of a service.  There is a single parameter, taking
#         the value "on" or "off".  This indicates the default (i.e. "clean")
#         status for this service.


# System Files
# =============================================================================
/opt/log/*.log                         noarch  664 root root
/etc/addlocal                          file    644 root root
/etc/passwd                            file    644 root root
/etc/group                             file    644 root root
/etc/shadow                            file    640 root root
/etc/conf.d/hostname                   file    664 root root
/etc/security/opasswd                  noarch  660 root root
/etc/nsswitch.conf                     file    664 root root
/etc/motd                              file    775 root root
/pub/*                                 deldir
/srv/www2/app/webroot/files/pub        delete
/etc/loopbackTest                      file    644 spui root
/etc/optioncardTests                   file    644 spui root
/etc/testResults                       file    644 spui root
/etc/testStatus                        file    644 spui root

# Spectracom Apps
# =============================================================================
/home/spectracom/log/*                 noarch  664 root root
/home/spectracom/log/broadshield/*     deldir
/home/spectracom/config/*              file    664 root root
/home/spectracom/config/Talen-X/*      file    664 root root
/home/spectracom/xfer/config/*         delete
/home/spectracom/xfer/log/*            delete
/home/spectracom/customize/*           file    777 root root
/home/spectracom/customize/Locale/*    file    777 root root
/home/spectracom/customize/Locale/eng/* file    777 root root
/home/spectracom/customize/Locale/eng/LC_MESSAGES/* file 777 root root
/home/spectracom/customize/Locale/fra/* file    777 root root
/home/spectracom/customize/Locale/fra/LC_MESSAGES/* file 777 root root
/home/spectracom/customize/Locale/pig/* file    777 root root
/home/spectracom/customize/Locale/pig/LC_MESSAGES/* file 777 root root
/home/spectracom/customize/Locale/rus/* file    777 root root
/home/spectracom/customize/Locale/rus/LC_MESSAGES/* file 777 root root
/home/spectracom/log/discstats/discstats* noarch 770 root root
/srv/www/images/discphase*.png         noarch  770 root root
/srv/www/images/discfreq*.png          noarch  770 root root
/srv/www/images/discdac*.png           noarch  770 root root

filelist.txt lines 1-75/274 29%
```

Email Keith sent to Hughes after talking with Oleg (17 Nov 2014)

As far as the network configurations are concerned, these configs can be removed from one or more saved .conf files to allow cloning of SecureSyncs. This alleviates the risk of having duplicate IP address. Static values can also be changed if desired.

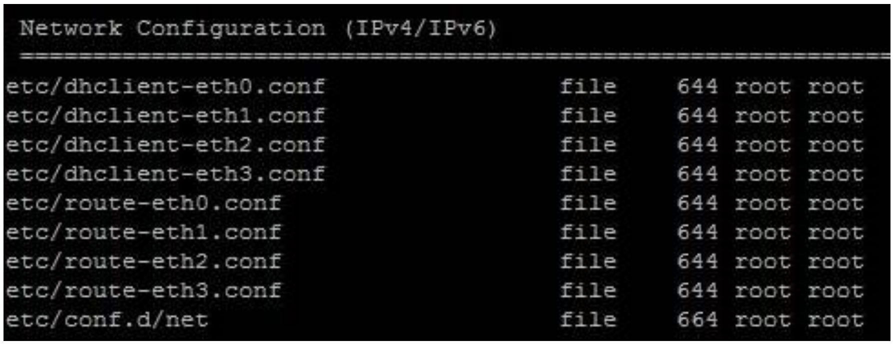
Otherwise, the .conf file is not intended to be edited by a user as a method to configure the SecureSyncs. One or more config files can be created from pre-configured SecureSyncs as a method to configure other SecureSyncs with similar settings. In general, the generated config file is not intended to be edited by customers. The .conf files consist of both config files as well as many rows of comma-delimited values. Incorrect editing of these non-network values can result in the need to clean the unit of call settings, resetting it back to a default state. Hardware configurations also affect the creation of the saved .conf file. If you wish to have various configurations of the SecureSync, we recommend you configure the SecureSync as desired and create a different .conf file for each desired configuration.

FYI: There is a list of all files that are placed in the .conf file. This list can be viewed via a CLI connection. To view this list cd to default directory (from home/spectracom) and then either "cat" or "less" the file of "filelist.txt":



```
spadmin@CustService-177 /home/spectracom $ cd default
spadmin@CustService-177 /home/spectracom/default $ cat filelist.txt
#
# filelist.txt
#
# This file is used by the cfgmover.sh script to manage which configuration
# files are archived, restored, cleared, or transfered on an upgrade
#
# Operations:
# file:   Archived on an Archive operation
#         restored from selected archive on Restore operation
#         Copied from Defaults directory on Clear operation
#         (deleted if no default exists in defaults directory)
```

Each file placed in the .saved con file is annotated with "file". Files not saved in the saved .conf are indicated with "noarch" or "delete". As an example, below from this list are all the files associated with network settings. These files are in the .conf file.



```
 Network Configuration (IPv4/IPv6)
 ==============================================================
etc/dhclient-eth0.conf                file    644 root root
etc/dhclient-eth1.conf                file    644 root root
etc/dhclient-eth2.conf                file    644 root root
etc/dhclient-eth3.conf                file    644 root root
etc/route-eth0.conf                   file    644 root root
etc/route-eth1.conf                   file    644 root root
etc/route-eth2.conf                   file    644 root root
etc/route-eth3.conf                   file    644 root root
etc/conf.d/net                        file    664 root root
```

Limitations of config restore

- Config files created with software versions 4.8.9 or below installed cannot be restored to any software version of versions 5.0.0 or above (due to MOTD being needed. More on this further below).
- Config files created with software versions 5.0.0 or above installed cannot be restored to any previous version of software (for example, a version 5.1.5 backup file can't be applied to version 5.1.4 software).

Note: Trying to apply a saved config file saved from a newer version than the target unit may result in a "**Version is not found**" entry in the Update log.

Potential loss of configurations: The Config file "Transfer engine" has a "20 version step" limit

- Applicable to at least software versions 5.8.2 and below. (not certain if/when a change will be incorporated, but likely it wil be in 5.8.3 or 5.8.4 if a change is possible)
- Applicable to both the software update process and to config file restores.
- Loss of configurations can occur if there are more than a total of 20 software updates (both updates released to production as well as all Engineering releases not released to production- such as versions 5.4.A and 5.7A for examples) between the start version (such as v5.0.2 for instance) and the version the configs are being restored to

(such as 5.8.2

Email Keith sent to Eric Girard (13 Nov 2018) I wanted to make sure you are aware of something that the rest of us JUST learned, pertaining to SecureSync/9400 configs. When either performing software updates, or when installing an earlier version configuration backup bundle to a newer installed version, there is (at least currently) a "**20 version step**" limit of the configs actually being restored.

The "version steps" in between the version the configs are being restored from (such as upgrading from version 5.0.2, or restoring a config bundle which was saved at version 5.0.2 to a unit now running 5.8.2) includes all full releases, and all engineering only releases (such as version 5.4.A for instance) from that point forward to the newly installed version. If there are more than 20 total software versions between the starting version and the newer version, the config transfer engine won't restore the configs to the newer version.

But if a "step" / interim software update is first performed (which is no more than 20 versions away from the starting/current version) before updating to the latest version of software, the configs will transfer to the "step" interim version. An example of this step is to update v5.0.2 to 5.4.0 first and not just update it directly to 5.8.2.

If there are only 20 versions between the one step/interim version and the final desired version, it can then be updated from the one step to the latest version with all configs being retained. With a very early starting version (such as v5.0.2 for example) a total of like three or four software updates to interim versions is required, if its desired to retain configs being restored during an update to version 5.8.2 (as Dave Lorah just had reported to him from a customer☹)!!!!!!

If a customer updates a SecureSync/9400 directly from v5.0.2 to 5.8.2 for instance, v5.8.2 will still be applied OK. But because there are many more than 20 versions in between, the current settings/configs will be lost when it has been upgraded to 5.8.2 (the customer will need to manually restore their desired configs)

Engineering will be looking into changing/removing this "20 step" limit on the transfer engine. But this won't be incorporated until update version 5.8.3 at the earliest. So, this 20 step limit will be in place until the change has been added into a newer version.

The biggest potential condition is if a customer is updating a remotely installed unit, from an earlier version. Then during a software update process, they then lose the settings which allow them to access it remotely.

I have asked that Dave Sohn add a notice on the same web page where customers download the software update bundles, that advises our customers that they may potentially lose configurations when applying a software update, especially when there have been no software updates applied in a very long time.

etc/MOTD file (Config files for software versions 5.0.0 and above)

- Starting in software version 5.0.0, the config bundles now contain an MOTD file in the /etc folder which indicates the version of software the config file was archived from.
- (search config file for "motd") Example below:

Spectracom SecureSync Version 5.1.5

- If there is no MOTD file in the ETC folder, the backup was saved prior to version 5.0.0 and cannot be applied to units running versions 5.0.0 and above.
- If there is a MOTD file in the ETC folder, the backup was saved from a version 5.0.0 or higher unit and can be applied to units running versions 5.0.0 and above. Open the file to see the version of software it was pulled from.

Note: You can restore from an earlier version to a newer version (5.1.4 configs onto a 5.1.5 unit). But you can't restore from a newer version to an earlier version (5.1.5 configs onto a 5.1.4 unit). This is because any config changes that have since been incorporated aren't recognized in the earlier version. (It can actually be done, but it requires "hacking" of the backup file to make it compatible with the earlier version). I recommend updating the earlier version to 5.1.5, instead of needing to modify the backup file.

A) Save and restore configs using the web browser

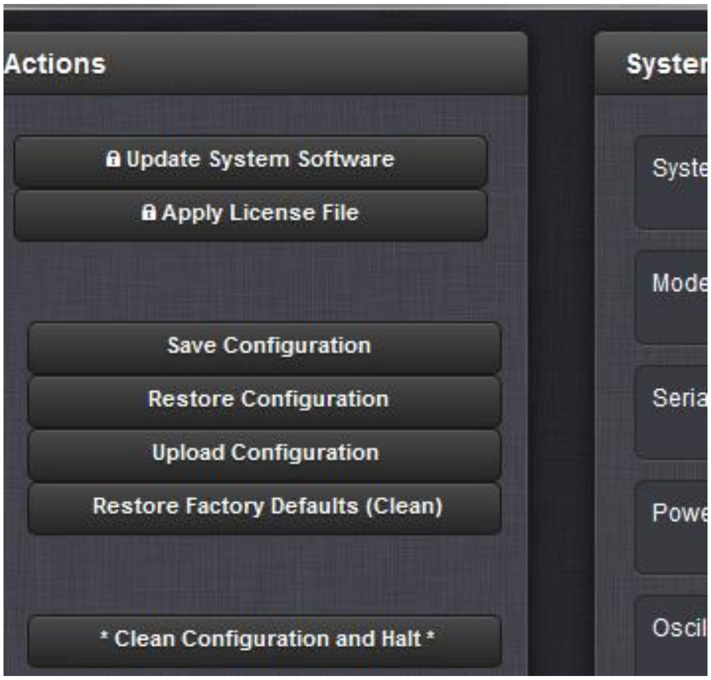
Limitations of config restore

- ➢ Config files created with software versions 4.8.9 or below installed cannot be restored to any software version of versions 5.0.0 or above (due to MOTD being needed. More on this further below).
- ➢ Config files created with software versions 5.0.0 or above installed cannot be restored to any previous version of software (for example, a version 5.1.5 backup file can’t be applied to version 5.1.4 software).

Note: Trying to apply a saved config file saved from a newer version than the target unit may result in a “**Version is not found**” entry in the Update log.

1. Newer black/charcoal browser (v5.1.2 and above)

Left side of the Tools -> Upgrade/Backup page of the browser:



A) To create a new config backup file:

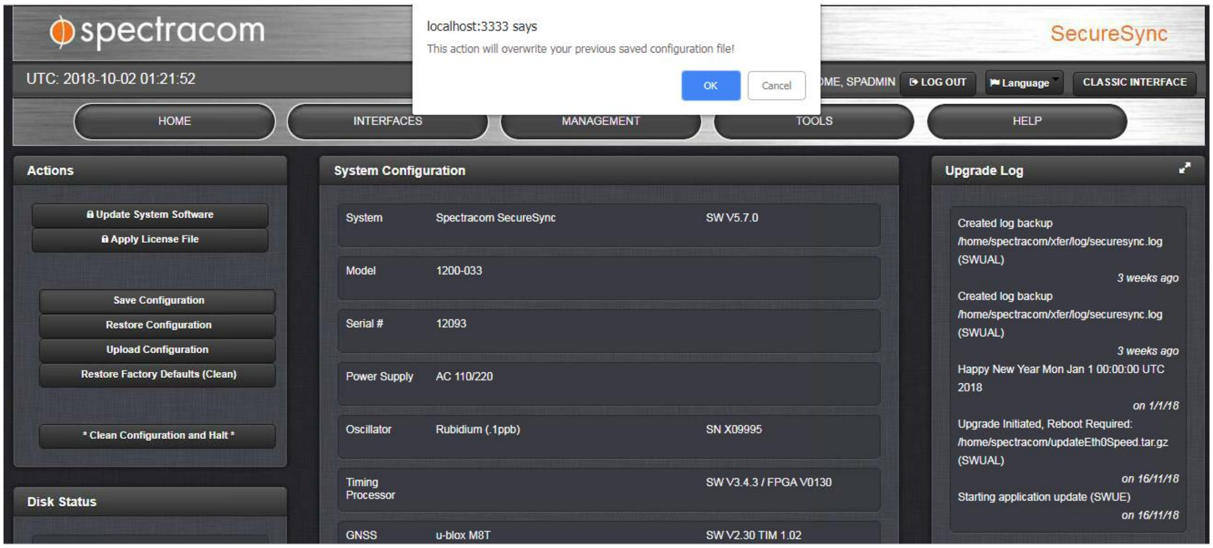
1. Press the “**Save Configuration”** buttion on the left side of the **Tools** -> **Upgade/Backup** page

B) To restore a previously saved config bundle:

1. First press the **Upload Configuration** button, to load the config bundle from the PC onto the servers
2. Then press the **“Restore Configuration**” button to apply the configs, and then the unit will automatically reboo to start using the restored configs.

“Localhost: 3333 says This action will overwrite your previous saved configuration file!”

Email from a customer: While saving configuration, I'm getting following message. I'm guessing it should be fine as it will probably overwrite previously downloaded configuration, but I need your confirmation that it won't impact any current configuration/settings on the unit. As the units are deployed at client sites with live operation and I don't want to take any risk.



localhost:3333 says

This action will overwrite your previous saved configuration file!

System	Spectracom SecureSync	SW V5.7.0
Model	1200-033	
Serial #	12093	
Power Supply	AC 110/220	
Oscillator	Rubidium (.1ppb)	SN X09995
Timing Processor		SW V3.4.3 / FPGA V0130
GNSS	u-blox M8T	SW V2.30 TIM 1.02

```
Created log backup
/home/spectracom/xfer/log/securesync.log
(SWUAL)
                                    3 weeks ago
Created log backup
/home/spectracom/xfer/log/securesync.log
(SWUAL)
                                    3 weeks ago
Happy New Year Mon Jan 1 00:00:00 UTC
2018
                                        on 1/1/18
Upgrade Initiated, Reboot Required:
/home/spectracom/updateEth0Speed.tar.gz
(SWUAL)
                                      on 16/11/18
Starting application update (SWUE)
                                      on 16/11/18
```

Reply from Dave L (2 Oct 18) This message is normal and informs you the Securesync will be creating a new saved Config file based on the current settings. If there was a previously saved config file it will be overwritten by this new config file.
This will not interrupt services and it will not change any setting on the Securesync.

2. Classic interface browser

- Refer to the Config backup/restore Tech Note: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Backup-restore configs

C) Ability to perform remote configuration save and restore configurations via CLI interface

saveconf and loadconf

- Versions 4.8.7 and below- not available
- Version 4.8.8 (Dec 2012-ECN 3099) Added saveconf and loadconf CLI commands to handle configuration backups.

saveconf <file name>: Saves config file to **/Home/Spectracom/Xfer/Config**

****Manually transferring the config file (instead of using the browser to save file to Windows computer, available with the new browser starting in version 5.1.2)**

- Config file must be transferred out of the SecureSync using BINARY mode. Transferring the file using ASCII mode instead will corrupt the config file, resulting in a “Version not found” error being asserted in the Update log.
- Refer to the “Update.log” section for additional info on this error message and how to verify the config file to see if it’s corrupted.

loadconf <file name>: Restores config file from **/Home/Spectracom/Xfer/Config** (First FTP/SCP a saved config file to this directory and then run this command).

Limitations of config restore

- Config files created with software versions 4.8.9 or below installed cannot be restored to any software version of versions 5.0.0 or above (due to MOTD being needed. More on this further below).
- Config files created with software versions 5.0.0 or above installed cannot be restored to any previous version of software (for example, a version 5.1.5 backup file can’t be applied to version 5.1.4 software).

Note: Trying to apply a saved config file saved from a newer version than the target unit may result in a "**Version is not found**" entry in the Update log.

Note:

- **FTP port is port 21**
- **SCP port is port 22**

Desire to perform script/scripting for automating the config backup process

- In at least 5.7.1 and below, automatically Saving/restoring configs via the SecureSync itelf is not available.
- Web browser connection scripting isn't feasible to download/restore configs. But connection to the CLI (sftp/scp and telnet/ssh) can be scripted to download/upload config bundles.

Summary: Since the web browser interface (the normal interface used to backup or restore the configs) can't easily be scripted for automation, a user can create a custom script which logs into the CLI interface, performs a CLI command which bundles all of the configuration files into a single bundle file. Then, this bundle file can be downloaded from the time server using an FTP/SCP (file transfer) connection to the unit's CLI interface.

Custom scripts to connect to the CLI, generate the config bundle file via a CLI command, and to download the file (as well as to upload and restore a config bundle) are the responsibility of the customer.

As for the SecureSync, these are the functions that need to be performed to download the configs using the CLI interface (and to upload/restore a config bundle), instead of using the web browser to perform these functions.

- All the configuration files can be bundled together into a single file, which can then be exported out of the unit using an FTP/SCP client.
- A config bundle file can be uploaded into the SecureSync(s) using an FTP/SCP client. Then this config file can be restored and the unit automatically rebooted to start using its new configuration file.

Note: If you need a free FTP client to perform the file transfers we often use CoreFTP lite (http://www.coreftp.com/).

- The CLI command to generate the config backup file ("securesync.conf" is **saveconf** <enter>.
- The 'securesync.conf' file is generated/stored in the following directory: /home/spectracom/xfer/config

Q (forwarded from Eric Girard) We would like to know the possibilities to automate the configuration backup of subjected devices.

A (modified) Email Keith sent it Eric Girard (20 Jan 16) As for the configuration backups of the SecureSyncs / NetClocks (Models 9383 and 9483), the SecureSyncs and NetClocks themselves do not have the ability to automate this desired function. The NetClock Model 9383s require the use of a GUI program to save or restore config files (our Specup utility that is also used to perform software updates). So this process can't be automated outside of the NetClock, either. This is a manual function.

However, the NetClock Model 9483s can perform a save configuration via the CLI interface (using the 'saveconf' CLI command) instead of using the web browser. And then, this saved configuration bundle file can be downloaded from the SecureSync or NetClock using FTP/SCP (Secure Copy), instead of needing to use the web browser.

You may be able to create your own custom script that can login to the CLI interface of the Model 9483 using SSH, run the **saveconf** CLI command to save the config file and then FTP into to the NetClock to download this file (the config file is created/stored in the **/home/spectracom/xfer/config** directory).

~~I have copied in Dave Sohn just so that he is aware your customer requested the capability to automate this process, and to see if he happens to have any additional info he can provide you with, that I'm not aware of.~~

Q Thanks for the procedure. So there's no way we can generate and copy out the config from our Linux server, meaning we cannot issue the "saveconf" command remote and then scp the output without any human intervention right?

A per Dave S (2 May 17) If you have a server that can run automated scripts, you could generate a script on that machine to periodically run the saveconf command remotely, and remotely scp that saved configuration from the unit.

A) Below are the steps to automate/script generating and exporting the config bundle file from one or more SecureSyncs

Generate the config bundle file (using a CLI command)

- Login to the SecureSync's CLI interface via a telnet/ssh connection (ex. PutTTY, HyperTerminal, etc.).

- At the command prompt type saveconf and then press <Enter> to generate the config bundle

Download the log file from the NetClock (using an FTP/SCP client)

- Connect to the SecureSync via a FTP/SCP client (such as CoreFTP lite for instance, a freeware program)
- Navigate to the /home/Spectracom/xfer/config directory and download the securesync.conf file to your computer.

B) Below are the steps to automate/script uploading and restoring a config bundle into one or more SecureSyncs

Upload the config bundle file into the SecureSync (using an FTP/SCP client)

- Connect to the SecureSync via a FTP/SCP client (such as CoreFTP lite for instance, a freeware program)
- Navigate to the /home/Spectracom/xfer/config directory, and upload the securesync.conf config bundle file from your computer into the SecureSync.

Restore the config bundle file (using a CLI command)

- Login to the SecureSync's CLI inteface via a telnet/ssh connection (ex. PutTTY, HyperTerminal, etc.).
- At the command prompt type loadconf and then press <Enter> to restore the config bundle (shortly thereafter, the unit will automatically reboot to start using the configs that were in the uploaded bundle file. It should be accessible again, within a couple minutes thereafter.

Download the log file from the SecureSync (using an FTP/SCP client)

- Connect to the **SecureSync** via a FTP/SCP client (such as CoreFTP lite for instance, a freeware program)
- Navigate to the /home/Spectracom/xfer/config directory and download the securesync.conf file to your computer.

Email from Keith to Eric Girard As for the configuration backups of the SecureSnc

NetClocks themselves do not have the ability to automate this desired function, The NetClock Model 9383s require the use of a GUI program to save or restore config files (our Specup utility that is also used to perform updates). So this process can't be automated outside of the NetClock, either. This is a manual function.

However, the Model 9483s can perform a save configuration via the CLI interface (using the saveconf CLI command) instead of using the web browser. And then this saved configuration file can be downloaded from the NetClock using FTP, instead of needing to use the browser.

Your customer may be able to create their own custom script that can login to the CLI interface of the Model 9483 using SSH, run the **saveconf** CLI command to save the config file and then FTP into to the NetClock to download this file (the config file is created/stored in the **/home/spectracom/xfer/config** directory).

I have copied in Dave Sohn just so that he is aware your customer requested the capability to automate this process, and to see if he happens to have any additional info he can provide you with, that I'm not aware of.

Note Tech Notes for SecureSync backup/cloning. Refer to the applicable link below:

- Link to SecureSync config/cloning: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Backup-restore configs

Note: The file (netclock.conf) is stored in: home/spectracom/xfer/config/

The Information below is the original info, before the two Tech Notes were released:

NOTE: The file names are different for the SecureSync and for Model 9400 series.

1. Refer to “A” below for SecureSync.
2. Refer to “**B”** below for Model 9400 series.

Note: If you need a free FTP client, we often use CoreFTP Lite (http://www.coreftp.com/).
Note:

3. **FTP port** is port 21
4. **SCP port** is port 22

C) SecureSync only:

Note: This process does not backup any installed certificates/keys.

Important note: The save and backup files should be transferred on and off in **BINARY** file format. With SCP, this is automatic. With FTP, must select Binary transfer mode!!

Note:

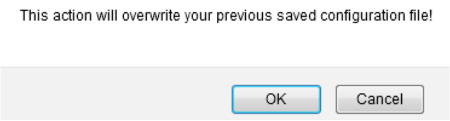
1. FTP port is port 21
2. SCP port is port 22

T**ools -> “Upgrade/Backup**” page of the web browser

D) To Store/ Download configuration file for storage on a PC

1. Via CLI interface (versions 4.8.8 and above only)
   1. Type **saveconf** <enter>
   2. Then FTP/SCP the file from the directory **home/spectracom/xfer/config/SecureSync.conf**):

2. Via newer web browser (v5.1.2 and above)
   1. Navigate to the **Tools** -> **Upgrade/Backup** page
   2. Download the config bundle by pressing “**Save Configuration”** (on the left side of the page)
   3. The following message will be displayed



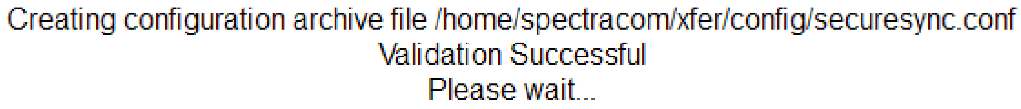
This action will overwrite your previous saved configuration file!

   4. Press **OK** to download
   5. Save the file to the desired location on the PC.

3. Via classic interface web browser: Change “Save Configuration” to “Enabled” and press Submit.

One file containing all configuration files is first generated in the SecureSync, using **Tools** -> **Upgrade/Backup**”, page, **Configuration** tab.

The screenshot below is displayed after performing a “Store Configuration” the path to this file is displayed in this screenshot (**home/spectracom/xfer/config/SecureSync.conf**):



Creating configuration archive file /home/spectracom/xfer/config/securesync.conf
Validation Successful
Please wait...

E) To Restore a Configuration file:

4. Via CLI interface (versions 4.8.8 and above only)
   1. Manually FTP/SCP the saved confit file to the directory **home/spectracom/xfer/config/SecureSync.conf**):
   2. Type **loadconf** <enter>
   3. The unit will automatically reboot to start using the new configs.

1. Via the newer web browser (versions 5.1.2 and above)

1. Navigate to the **Tools** -> **Upgrade/Backup** page
2. Upload config bundle into the unit by pressing : **Upload Configuration**
3. Select the location of the saved config file.
4. Press the **Restore Configuration** button to start using new configs.
5. The unit will automatically reboot to start using new configs.

2. Via classic interface web browser:

1. One file containing all configuration files is first generated in the SecureSync, using **Tools** -> **Upgrade/Backup**”, page, **Configuration** tab.
2. Change “**Save Configuration**” to “Enabled” and press Submit

When a Store configuration is performed, a file is placed in the following directory:
home/spectracom/xfer/config/SecureSync.conf.

The User can restore from this file in the directory, or they can FTP/SCP transfer the desired SecureSync.conf file from a PC into this specified SecureSync directory (such as the desire to clone or backup from an archived file).

Note: If performing a “Restore Configurations” before a “Store Configurations” has been performed (or a SecureSync.conf file is not present in the right directory, as described above), a validation error will occur. A “Store configuration” has to be performed first, before performing a “Restore Configuration”.

Email I sent to Richard Fox about “Restore configuration” (8/23/11). He had received a validation error because he hadn’t first performed a “Store Configuration” before performing a “Store Configuration”:

Q. I tried your first option to restore the configuration but failed at the validating process when I hit the Submit button. Do I have to be in a certain mode to do it?

Hi Richard,
The “Restore Configuration” restores configurations as they are placed in one bundled file located in the

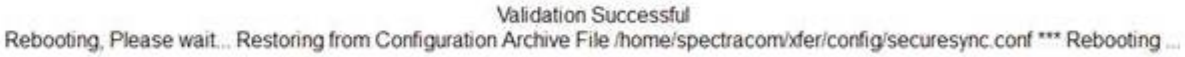
Home/Spectracom directory inside the SecureSync. Before you can perform a “Restore Configuration”, there has to be a configuration file (config) in this directory.

The first step is to perform a “Save Configuration”. This places a config file (with all configuration files bundled together in a single file) into the Home/Spectracom directory inside SecureSync. Then, if it’s desired to save this file onto a computer, you can then manually FTP (or SCP) in to this directory and copy this config file to your computer.

To “Restore Configuration” you can either restore from the file that was initially saved on that same SecureSync, or you can transfer the bundled file to the same or any other SecureSync via FTP (transfer the file using FTP to the home/spectracom directory). Then, perform a “Restore Configuration”. It will then reconfigure itself to the values that are inside the bundled file.

If you try to perform a “Restore Configuration” before performing a “Save Configuration”, there is no file to restore from, so a validation error occurs. This bundled file has to be either first created using a “Store Configuration” or the file first has to manually transferred into this directory using FTP (or SCP).

This time, it will display (I duplicated exactly what you were seeing- before performing a “Store Configuration”. I got the validation error. After performing a Store and then a Restore, I got:



Validation Successful

Rebooting, Please wait... Restoring from Configuration Archive File /home/spectracom/xfer/config/securesync.conf *** Rebooting ...

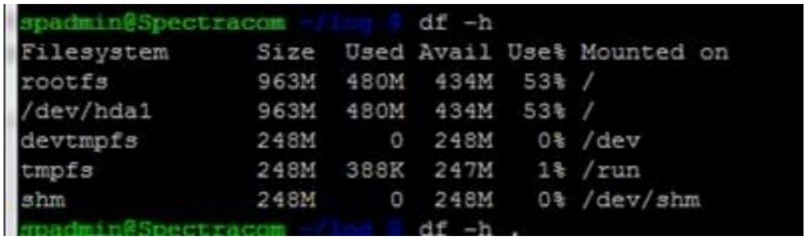
After performing Save Configs, Backup Config file isn’t created in the “home/spectracom/xfer/config/” directory

- CF card may be full or quite full.
- Use the df -h CLI command to check disk usage

Email Keith sent to a customer (7 Aug 2014)

There is no indication displayed that the bundle file has been created. You should be able to FTP into the **home/spectracom/xfer/config/** directory, see the bundle file and transfer it out to your PC.

If by chance the file isn’t in this directory, the Compact Flash card might be quite full of logs and previous update bundles. To determine what percent of the CF card is being used, connect to the CLI interface using telnet or ssh. After logging in type the following at the command prompt: **df –h** (as shown below).



```
spadmin@Spectracom ~/log $ df -h
Filesystem      Size  Used Avail Use% Mounted on
rootfs          963M  480M  434M  53% /
/dev/hda1       963M  480M  434M  53% /
devtmpfs        248M     0  248M   0% /dev
tmpfs           248M  388K  247M   1% /run
shm             248M     0  248M   0% /dev/shm
spadmin@Spectracom ~/log $ df -h .
```

If the “**Use%**” in the “**/dev/hda1**” row is greater than around 70%, it may have a lot of logs and previous update bundles stored in the flash card. I haven’t seen this usage ever cause a reboot to be needed, but it’s good to look at this anyways before applying software updates. If it’s greater than around 70% or so, let me know and I will provide you with info on how to delete past update files that remain stored in the unit after each updated.

While performing Save Configs via CLI command, “tar: Removing leading `/' from member names” messages are displayed

Q. What do these messages mean?

A. The backup config process is able to truncate the full path name to the location of config files.(it doesn't need to store the full path route). These entries just indicate the path was shortened. They are not an indication of a problem!

While performing Save Configs with CLI command, "Cannot stat: No such file or directory" and "Exiting with failure status due to previous errors messages" displayed.

Example:

```
tar: /etc/route-eth0.conf: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
```

Email from Oleg: Because they do not have routes and radius activated, so the files do not exist on their system. Save configs is looking for all known possible configs and tries to copy them, some may not exist.

- The Backup process looks for specific config files to copy.
- If it can find specified files because a particular function hasn't been configured yet (such as Radius or network static routes for examples), an error message is asserted to indicate the file could not be found and then the process moves on to looking for the next file in the list.
- The "/etc/" path indication at the beginning of the "Cannot stat" message indicates which function isn't configured, resulting in the error condition being asserted

Examples

  - **/etc/route** is referring to static routes.
  - **etc/raddb/server** is referring to static routes

- These messages and error condition do not prevent the file from being built,

Q. When attempting to do it via the CLI I get the following errors…

```
admin@time ~ $ saveconf backup1
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: /etc/route-eth0.conf: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
tar: Removing leading `/' from member names
tar: /etc/route-eth1.conf: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
tar: Removing leading `/' from member names
tar: /etc/route-eth2.conf: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
tar: Removing leading `/' from member names
tar: /etc/route-eth3.conf: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
tar: /etc/raddb/server: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
admin@time ~ $
```

A. **Reply from Keith after talking to Oleg (7 Aug 14)** After talking with one of our software engineers, I have some additional info for you that should help.

The Config save process looks for specific configuration files to copy into the backup bundle file. If the process doesn't find a specified file because that particular function has not yet been configured (such as Radius authentication and network routes, based on the logs you sent) it generates an error to indicate there were no files to save and moves on to the next file in the list to look for. The error should not prevent the bundle from being created.

There is no indication displayed that the bundle file has been created. You should be able to FTP into the **home/spectracom/xfer/config/** directory, see the bundle file and transfer it out to your PC.

Error message when trying to "Save Configs" again

FAQs about backup/restore configs

This backup process does not backup any installed certificates/keys. LDAP certificates are now backed-up.

1) It does save static assigned network settings but does not store DHCP assigned settings (it just stores the setting of DHCP being enabled.
2) Passwords are saved and restored/cloned.

FYI: For security and operational reasons, the save and clone configurations functions do not save or restore/clone any SSH/SSL certificates or keys. It will save and restore/clone the network settings (such as the IP address, subnet mask and gateway settings), if these are set to static values (DHCP not enabled). However, if DHCP is enabled, it will save/clone the setting of DHCP being enabled, but it won't save/clone the specific network settings. These network values will be assigned by the DHCP server when that SecureSync unit is connected to the network.   Also, login passwords are stored and restored/cloned.

The reason it doesn't store/restore certificates or keys is to prevent a compromise of the private keys. The reason it doesn't store/restore DHCP assigned values is because even if the network settings were saved for either cloning of units or future restoring, it's entirely possible/likely that the DHCP server would reassign new network values anyways (especially if the values are cloned into a different unit which will have a different MAC address). So there's no benefit to saving/cloning DHCP assigned addresses.

If custom SSL certificates have been created or imported into the SecureSync, they will need to be re-created in the original or cloned SecureSync after the configuration file have been restored (or cloned into another unit). However, if no custom certificates were created or imported, the default Spectracom certificates that are present will allow operation of a cloned or configuration restored SecureSync.

(red responses below are email responses from Mike Sander, on 3/9/11 as applicable to v4.4.0 and below)

Q. Is there any way to back-up the settings using the Terminal services?
A. The first question is easy, the steps of moving the configuration archive on and off the unit are terminal based, but the creation of the configuration archive, or the action of applying an archived configuration can only be done from the web UI.

Q. Also I see that in section 3.7 it says this backups all but network settings. Does this include the services like DHCP and such?
A. The manual is incorrect about the second question. The network configuration is saved and restored. Users and passwords are also saved and restored. Security certificates are not saved and restored. We will be updating that configuration. (KW summary after talking to Mike S- not at this time)

The save/restore feature has two uses. The first is to make a backup of the configuration of a single unit. The second is to clone the configuring of one unit and apply it to many. The implementation is designed to meet both goals.

If the customer is using static IP addresses and they want to clone the configuration and apply it to multiple units there are several approaches they can take. The first is to clone the configuration and then change the IP addresses from the front panel to prevent multiple machines from having the same IP address. Or they could temporarily set the unit to DHCP, save that configuration, and then, after cloning that configuration onto a unit, set each one to a static IP.

(KW summary after talking to Mike Sander):   Doesn't store DHCP settings but will store static values. The reason it doesn't store DHCP is because DHCP server could still reassign it, even if the settings were stored/restored).

Known issues with config save

A) IPSec configs not being saved

- Refer to Mantis case 1853

**Clean command (reset logs and configs)

- Clean and Cleanhalt commands were added to the front panel "Serial" port in Archive software version 4.4.0.
- Clean and Cleanhalt commands were added to the front panel keypad in version 4.7.0

To perform a Clean via the front panel keypad

To clean the unit from the front panel Keypad/LCD:

1) First press the front panel green check mark to see the Home menu.
2) Use the white directional keys to highlight the System menu and press the green check mark.
3) Use the white directional keys to highlight the Cmd menu and press the green check mark.
4) Use either the up or down keys until "clean" is displayed. Then, hit the green check key, to select it and then hit it again to apply the command. Note: An automatic reboot is performed when performing a clean command.

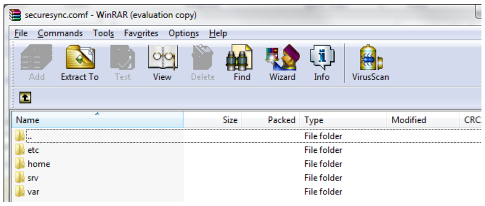
To perform a Clean via a serial connection

To reset all of the configs and logs back to factory default values, perform a "**clean**" CLI command. A "clean" command can be performed by connecting a PC running HyperTerminal (or other terminal emulator software) to the front panel SERIAL port with a straight-thru DB9F to DB9M serial cable. The settings for HyperTerminal are 9600, N, 8 1 (the "flow control" setting does not matter).

Once connected, type: **clean** <enter>. Note that this same command can also be sent with a telnet or an SSH connection (as long as these services are still enabled in the web browser). Either telnet or ssh into the NTP server and then type: **clean** <enter>. After issuing this command via RS-232, telnet or SSH, the logs and configurations will be reset and the web browser should be accessible again. Then just configure the SecureSync as desired. **Note**: An automatic reboot is performed when performing a clean command.

Breakdown of all the various config files

A) securesync.conf file



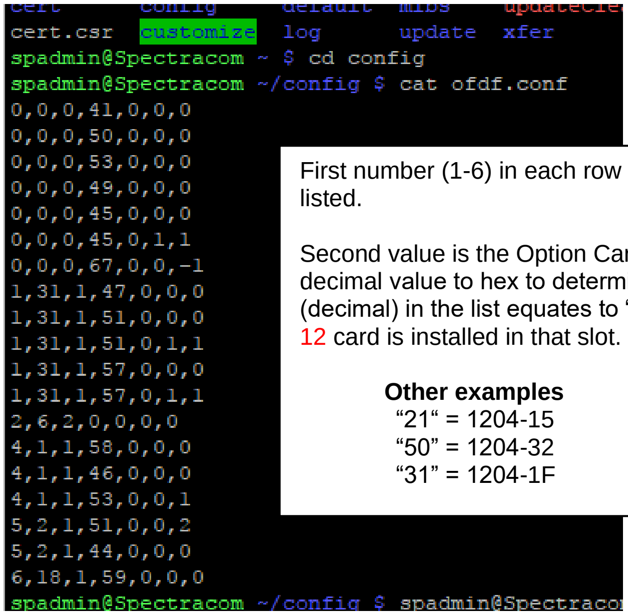
Name	Size	Packed	Type	Modified	CRC
..			File folder		
etc			File folder		
home			File folder		
srv			File folder		
var			File folder		

B) home/spectracom/config configuration files

Config file name	Configurations for:	Notes
access.conf	Network Access Restriction	(**Management**-> **Network page**, Access Control button
cagps.conf	A-GPS (Assisted GPS)	**Interfaces** -> **GNSS 0** page Rinex file, YUMA data
drdf.conf	Local Clock configurations	**Management** -> **Time Management** page, Local Clocks
fpmcf.conf	Front panel LCD	**Management** -> **Front Panel** page Content of LCD, keypad lock, menu rotation enable/number of seconds to display each menu
gpscf.conf	GPS Receiver	**Interfaces** -> **GNSS 0** page Rcvr mode, constellations, offset
gpsrinexd.conf	A-GPS Server	Generation of Rinex files (if AGPS Server license has been purchased/installed
ktsif.conf	MaxTFOM, Holdover, phase error limit, UTC and TAI Timescale offset	**Management** -> **Disciplining** page **Management** -> **Time Management** page
lccf.conf	Local Clock	Local Clock settings
lcdf.conf	Front panel configs	**Management** -> Front panel page
nesf.conf	Current active alarm	Values for active minor and major alarms
notcf.conf	Trap and email notifications/ mask alarms	**Management** -> **Notifications** page
ofdf.conf (see addional info further below)	Option Cards	Feature mapping
pdcf.conf		
pwdcf.conf	Password complexity	
relay.map	Relays	Model 9483 only
remove.conf	Remove **TCPdump** from the system	
rmif.cond		
rmnf.conf	Reference Priority table settings	**Management** -> **Reference Priority** page

rmsf.conf	Enable battery-backed time button	**Startupsync 0:** button is not selected **Startupsync 1:** button is selected
snmpd.conf	SNMP configs	
speclog.conf	Log configuration/mapping (Syslog facility and Severity codes)	
rs485addr.conf	Model 1204-0B Option Card configs	
stmd.conf/ stcermd.conf	NTP Anycast mode configurations	
temp.conf	Temperatue monitoring for alarms/traps	v5.3.1 and above only
temperature.conf	Temperature monitor for thresholds	v5.3.1 and above only (I believe)
webif.conf	Browser time-out in minutes (from first accessed) I believe	Example entry “cookieTimeout 15”

ofdf.conf file



```
cert        config      default   mibs     updatecle
cert.csr    customize   log       update   xfer
spadmin@Spectracom ~ $ cd config
spadmin@Spectracom ~/config $ cat ofdf.conf
0,0,0,41,0,0,0
0,0,0,50,0,0,0
0,0,0,53,0,0,0
0,0,0,49,0,0,0
0,0,0,45,0,0,0
0,0,0,45,0,1,1
0,0,0,67,0,0,-1
1,31,1,47,0,0,0
1,31,1,51,0,0,0
1,31,1,51,0,1,1
1,31,1,57,0,0,0
1,31,1,57,0,1,1
2,6,2,0,0,0,0
4,1,1,58,0,0,0
4,1,1,46,0,0,0
4,1,1,53,0,0,1
5,2,1,51,0,0,2
5,2,1,44,0,0,0
6,18,1,59,0,0,0
spadmin@Spectracom ~/config $ spadmin@Spectracoi
```

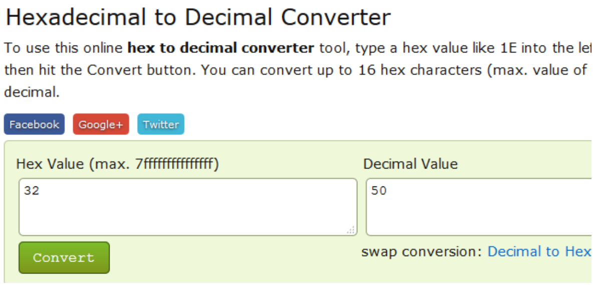
First number (1-6) in each row is the slot number. If a slot is empty, its slot number is not listed.

Second value is the Option Card Model Number (reported in decimal). Convert this decimal value to hex to determine the actual Model Number. For example, an “18” (decimal) in the list equates to “12” in hex. An “18” reported in a slot means a Model 1204-12 card is installed in that slot. (See note and dec/hex converter below the screenshot)

Other examples
“21“ = 1204-15
“50” = 1204-32
“31” = 1204-1F

Note: Option Cards are called by their hex number, but handled in the system by the corresponding decimal value

Example: The 1204-32 card in the sytem is actually “**50**” (refer to sites such as: http://www.binaryhexconverter.com/hex-to-decimal-converter)



Hexadecimal to Decimal Converter

To use this online **hex to decimal converter** tool, type a hex value like 1E into the lef
then hit the Convert button. You can convert up to 16 hex characters (max. value of
decimal.

Hex Value (max. 7fffffffffffffff): 32

Decimal Value: 50

swap conversion: Decimal to Hex

C) home/spectracom/customize

➢ For Customization of the newer browser

- For more details refer to (in this doc): Customization of the newer browser
- Newer browser can be customized with a custom logo(“**logo.png**” file) custom language (“**Locale**” directory) and or custom contact info (“**contact-example.html**” file)
- Custom items such as a logo, locale or contact info are plced in the **home/spectracom/customize** folder (spadmin has access to this folder)

D) /etc configuration files

Config file name	Configurations for:
conf.d folder	See table futher below (hostname and Ethernet interface settings)
dhclient.conf-eth number (such as “dhclient-eth0.conf”	Ethernet port config files
group	Account info
host.conf	
ldap.conf	LDAP
logrotate	Log rotation
motd	Date (“of the day”)
nail.rc	Nail (email settings)
nssswitch.conf	
passwd	
policy.conf	
racoon.conf	
resolv.conf	Two DNS server addreses
shadow	User accounts and Passwords

syslog.conf	Syslog configuration
tacacs_pam.conf	Tacacs config file
timekeeper.conf	Timekeeper
udhcpd.conf	Static routes??
xinetd.conf	xinetd?

E) /etc/apache2/

Config file name	Configurations for:	Some example parameters
sites-enabled.conf	List of supported ciphers for connection	
ssl.conf	SSL support for Apache	
httpd.conf	Apache config	PHP, languages, browser error messages, network access restrictions.

F) /etc/conf.d

Config file name	Configurations for:
hostname	hostname
net	Ethernet interface settings

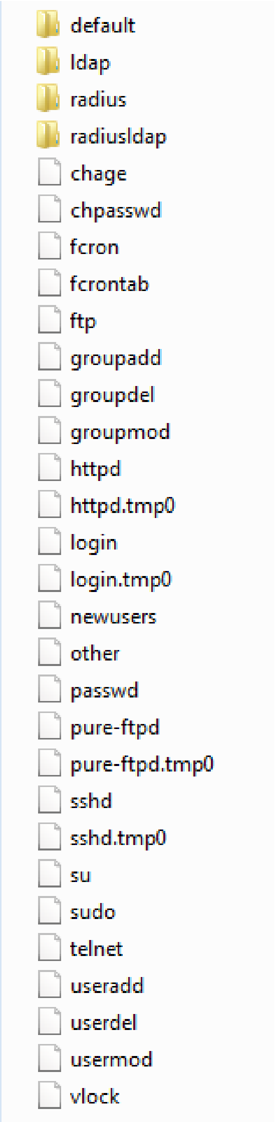
G) /etc/local.d

Config file name	Configurations for:
logrotate.conf	Log rotations

H) /etc/ntp

Config file name	Configurations for:
ntp.conf	NTP
ntp.keys	NTP auth keys

I) etc/pam.d



```
default
ldap
radius
radiusldap
chage
chpasswd
fcron
fcrontab
ftp
groupadd
groupdel
groupmod
httpd
httpd.tmp0
login
login.tmp0
newusers
other
passwd
pure-ftpd
pure-ftpd.tmp0
sshd
sshd.tmp0
su
sudo
telnet
useradd
userdel
usermod
vlock
```

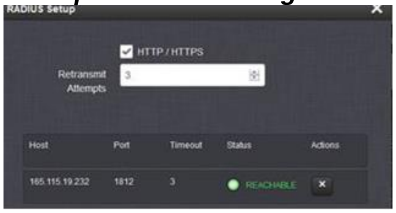
J) /etc/quagga

Config file name	Configurations for:
ospfd.conf	OSPF for NTP over Anycast
bgpd.conf	BGP for NTP over Anycast
zebra.conf	Associated with NTP over Anycast

K) /etc/raddb/

Config file name	Configurations for:
server	Retries and Server adress
rc.conf	Radius

Example Radius config file

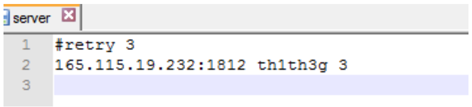


RADIUS Setup

☑ HTTP / HTTPS

Retransmit Attempts: 3

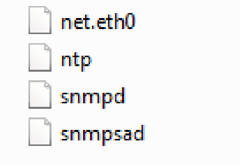
Host	Port	Timeout	Status	Actions
165.115.19.232	1812	3	● REACHABLE	×



server

```
#retry 3
165.115.19.232:1812 th1th3g 3

```

L) /etc/runlevels



- net.eth0
- ntp
- snmpd
- snmpsad

M) /etc/security

Config file name	Configurations for:
access.conf	Access control for CLI
group.conf	
dclimits.conf	User permissions
pam_env.conf	
time.conf	PAM-Time module

N) /etc/ssh

Config file name	Configurations for:
sshd_config	SSH
sshd_config.expert	SSH (but not currently used)

O) /etc/xinetd.d/

Config file name	Configurations for:

	Daytime protocol
ftp	FTP
ssh	ssh
telnet	telnet
time	Time protocol

**CLI commands to display / configure / disable the Ethernet ports (DNS, DHCP, IP address, Subnet mask, Static routes)

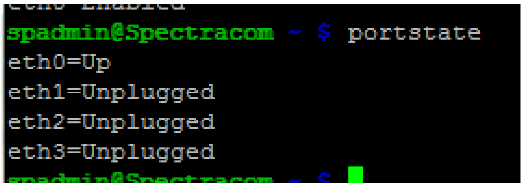
Port state

- Desire to display port state of all Ethernet ports (port up, port down, cable unplugged)

portstate command

Note: To obtain port state for SMNP instead of CLI, refer to the "**ifOperStatus**" SNMP object in the SNMP section of this document.

- CLI command is **portstate**
- Displays status of all installed Ethernet ports, including Eth0.



```
eth0 Enabled
spadmin@Spectracom ~ $ portstate
eth0=Up
eth1=Unplugged
eth2=Unplugged
eth3=Unplugged
spadmin@Spectracom ~ $
```

Enable/Disable the Gigabit interfaces (eth1, eth2 or eth3)

A) Via the front panel keypad (available in versions 5.6.0 and above)

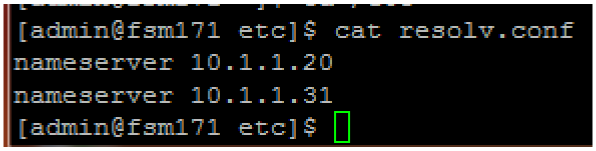
- **Refer to (in this doc):** Configure/display network settings using keypad

B) Via the CLI interface (required in versions 5.5.1 and below)

portset command (available in versions 5.1.2)

- This command was implemented starting with the new web browser design in Archive version 5.1.2 (not available with earlier versions)
- The CLI command: **portset x on** enables the interface number specified by the "x".
- The CLI command: **portset x off** disable the interface number specified by the "x
- CLI command to retrieve current port state: **portget x** <enter>

DNS servers ("resolv.conf" file)



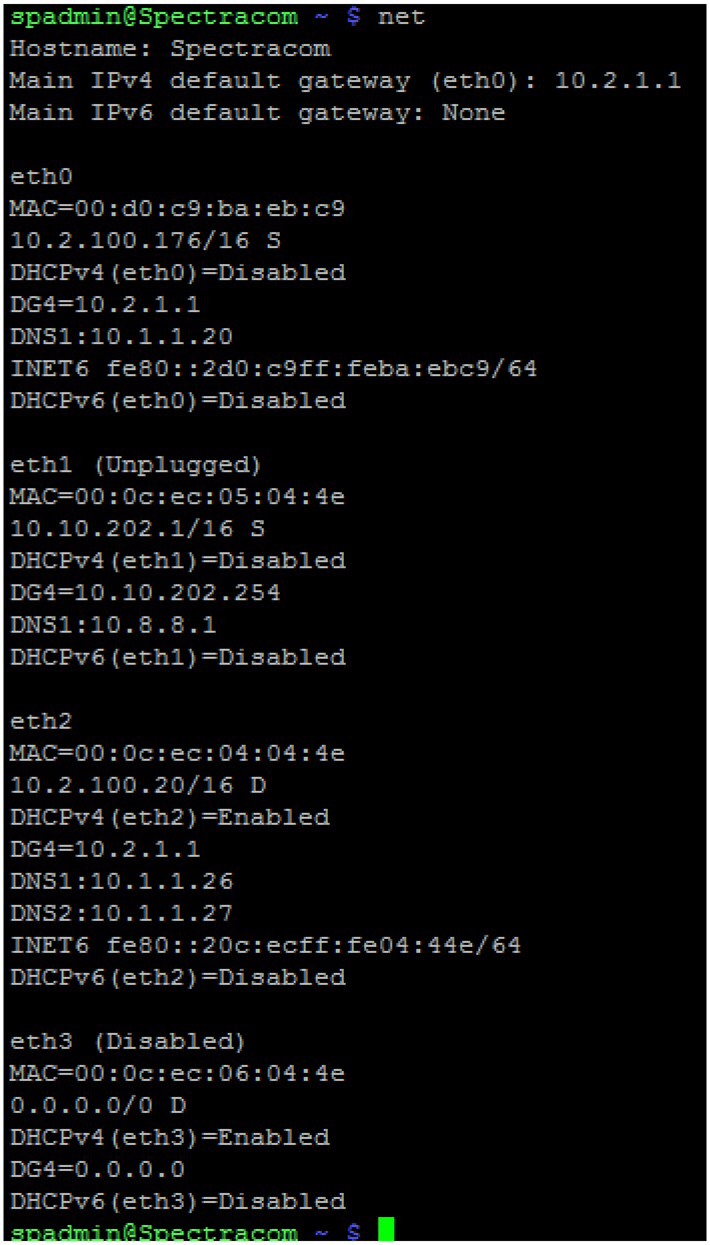
```
[admin@fsm171 etc]$ cat resolv.conf
nameserver 10.1.1.20
nameserver 10.1.1.31
[admin@fsm171 etc]$
```

Display/retrieve/set DNS server settings for each Ethernet interface

- The CLI command: **dns4get x** retrieves the DNS setting (for the port specified by the "x".
- The CLI command: **dns4set x <primary dns> <secondary dns>** configures the DNS setting for he Ethernet interface port number specified by the "x". (note the secondard dns address is optional/not required)

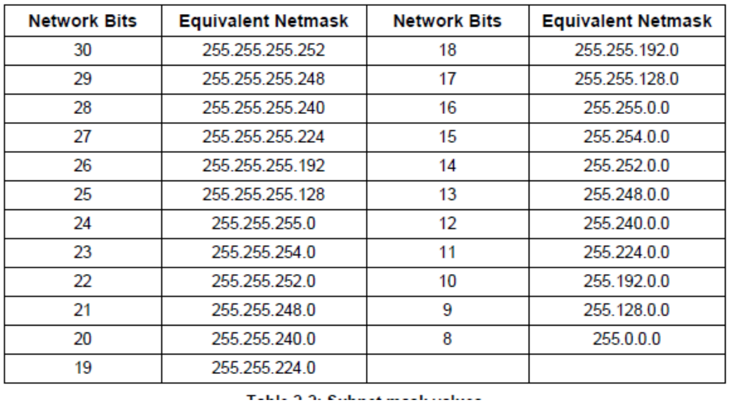
Display/retrieve network settings (IP address, subnet mask)

net <enter> shows all network settings for all ports



```
spadmin@Spectracom ~ $ net
Hostname: Spectracom
Main IPv4 default gateway (eth0): 10.2.1.1
Main IPv6 default gateway: None

eth0
MAC=00:d0:c9:ba:eb:c9
10.2.100.176/16 S
DHCPv4(eth0)=Disabled
DG4=10.2.1.1
DNS1:10.1.1.20
INET6 fe80::2d0:c9ff:feba:ebc9/64
DHCPv6(eth0)=Disabled

eth1 (Unplugged)
MAC=00:0c:ec:05:04:4e
10.10.202.1/16 S
DHCPv4(eth1)=Disabled
DG4=10.10.202.254
DNS1:10.8.8.1
DHCPv6(eth1)=Disabled

eth2
MAC=00:0c:ec:04:04:4e
10.2.100.20/16 D
DHCPv4(eth2)=Enabled
DG4=10.2.1.1
DNS1:10.1.1.26
DNS2:10.1.1.27
INET6 fe80::20c:ecff:fe04:44e/64
DHCPv6(eth2)=Disabled

eth3 (Disabled)
MAC=00:0c:ec:06:04:4e
0.0.0.0/0 D
DHCPv4(eth3)=Enabled
DG4=0.0.0.0
DHCPv6(eth3)=Disabled
spadmin@Spectracom ~ $
```

Subnet mask conversion table for quick-reference



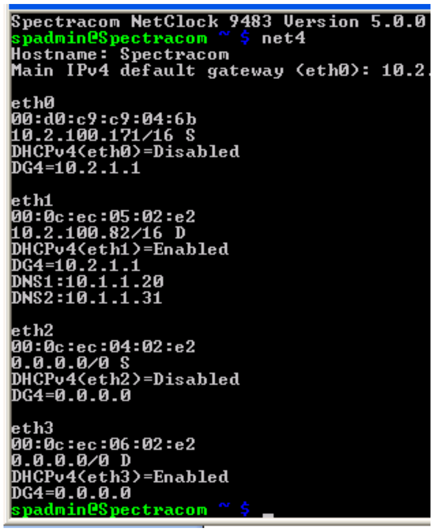
Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
30	255.255.255.252	18	255.255.192.0
29	255.255.255.248	17	255.255.128.0
28	255.255.255.240	16	255.255.0.0
27	255.255.255.224	15	255.254.0.0
26	255.255.255.192	14	255.252.0.0
25	255.255.255.128	13	255.248.0.0
24	255.255.255.0	12	255.240.0.0
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		

Table 3-3: Subnet mask values

net show and **net4** / **net 6** commands (net4 is equivalent to net show command in earlier Models)

Net show displays All IPv4 settings for all Ethernet interfaces

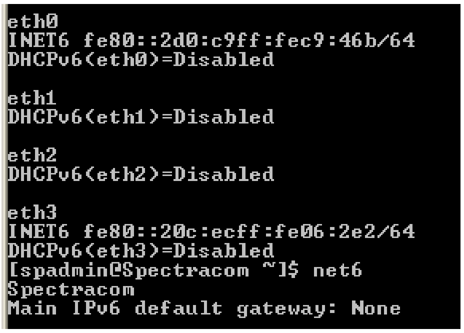
- **net4** displays or gets the network settings/MAC addresses for each of the network ports.
- IPv4 settings only (no IPv6 settings)



```
Spectracom NetClock 9483 Version 5.0.0
spadmin@Spectracom ~ $ net4
Hostname: Spectracom
Main IPv4 default gateway (eth0): 10.2.

eth0
00:d0:c9:c9:04:6b
10.2.100.171/16 S
DHCPv4(eth0)=Disabled
DG4=10.2.1.1

eth1
00:0c:ec:05:02:e2
10.2.100.82/16 D
DHCPv4(eth1)=Enabled
DG4=10.2.1.1
DNS1:10.1.1.20
DNS2:10.1.1.31

eth2
00:0c:ec:04:02:e2
0.0.0.0/0 S
DHCPv4(eth2)=Disabled
DG4=0.0.0.0

eth3
00:0c:ec:06:02:e2
0.0.0.0/0 D
DHCPv4(eth3)=Enabled
DG4=0.0.0.0
spadmin@Spectracom ~ $ _
```

Display IPv6 settings only (no IPv4 settings)

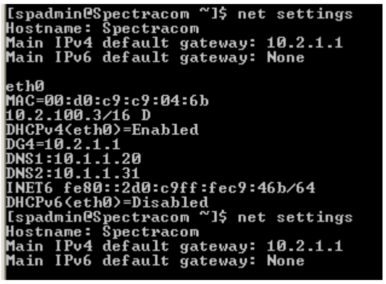
- **net6** displays the network settings/IPv6 addresses for each of the network ports.



```
eth0
INET6 fe80::2d0:c9ff:fec9:46b/64
DHCPv6(eth0)=Disabled

eth1
DHCPv6(eth1)=Disabled

eth2
DHCPv6(eth2)=Disabled

eth3
INET6 fe80::20c:ecff:fe06:2e2/64
DHCPv6(eth3)=Disabled
[spadmin@Spectracom ~]$ net6
Spectracom
Main IPv6 default gateway: None
```

Display Eth0 settings only (Both IPv4 and IPv6 settings)

- ➢ Net settings command displays only Eth0 IPv4 and IPv6 network port configurations
- ➢ Shows no info on Eth1, Eth2, Eth3



```
[spadmin@Spectracom ~]$ net settings
Hostname: Spectracom
Main IPv4 default gateway: 10.2.1.1
Main IPv6 default gateway: None

eth0
MAC=00:d0:c9:c9:04:6b
10.2.100.3/16 D
DHCPv4(eth0)=Enabled
DG4=10.2.1.1
DNS1:10.1.1.20
DNS2:10.1.1.31
INET6 fe80::2d0:c9ff:fec9:46b/64
DHCPv6(eth0)=Disabled
[spadmin@Spectracom ~]$ net settings
Hostname: Spectracom
Main IPv4 default gateway: 10.2.1.1
Main IPv6 default gateway: None
```

Ipv4 Configure/show network settings

DHCP

Get all current DHCP settings: **dhcp4get**

Get current DHCP setting for one particular port: **dhcp4get** <**interface**> (such as **dhcp4get 0**)

- **Enable DHCP setting**: **dhcp4set** <**interface**> **on** (such **as dhcp4set 0 on**)
- **Disable DHCP setting**: **dhcp4set** <**interface**> **off** (such as **dhcp4set 0 off**)

****Assigning network settings via CLI

- **IP4get** <interface> (such as IP4get 0)
- **IP4set** <interface> <address> <mask> (such as **IP4set 0 10.10.200.1 255.255.255.0**)
- **ip6get 1** get the IPv6 address for eth1

NOTICE: IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 netwok while configuring. Otherwise the config changes won't be accepted.

IP Address (IPv4 and IPv6)

- **Get current IP address** (can't display all at once): **IP4get** <interface> (such as **IP4get 0**)
- **Set IP address: IP4set** <interface> <address> <mask> (such as **IP4set 0 10.10.200.1 255.255.255.0**)
- **ip6add 1** (IP xxx.xxx.xxx.xx) (subnet address xxx.xxx.xxx.xxx) (gateway address xxx.xxx.xxx.xxx)
    a. ip6add 1 xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx – Adds IPv6 IP address, subnet and gateway for eth1.

NOTICE: IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 netwok while configuring. Otherwise the config changes won't be accepted.

Gateway (Main default gateway as well as the gateway address for each port)

Get current gateway address:

- **gw4get** Displays gateway address for all Ethernet ports.
- **gw4get <interface>** (such as **gw4get 0**) for one particular gateway address

  Note <interface> is 0, 1, 2, 3 or m for main default gateway.

Enable and set gateway address: **gw4set** <**interface**> <'**gateway address>** (example **gw4set m 10 10.10.200.1**)

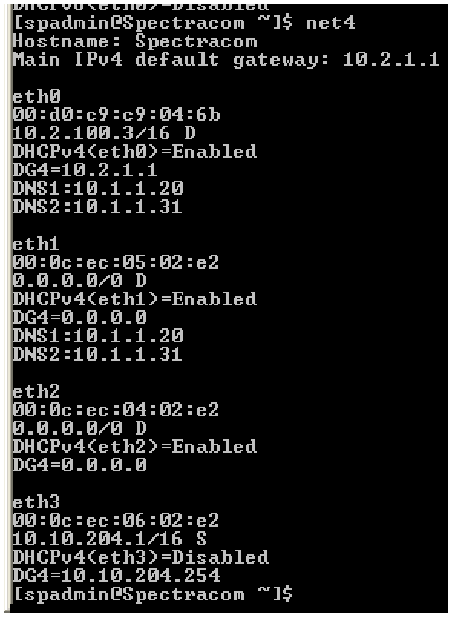
Get (read)

- CLI command to read which port is the main default gateway: **gw4get m** <enter> (where m is for main)
- CLI command to read the gateway address for a particular Ethernet port (eth2 for example): **gw4get 2** <enter>

Set

- CLI command to set which port is the main default gateway: **gw4set m x y** <enter> (where **m** is for "main", **x** is the gateway address and **y** is the port number.

Example to make the default port 2: **gw4set m 10.2.1.1 2 <enter>**



```
DHCPv6(eth0)=Disabled
[spadmin@Spectracom ~]$ net4
Hostname: Spectracom
Main IPv4 default gateway: 10.2.1.1

eth0
00:d0:c9:c9:04:6b
10.2.100.3/16 D
DHCPv4(eth0)=Enabled
DG4=10.2.1.1
DNS1:10.1.1.20
DNS2:10.1.1.31

eth1
00:0c:ec:05:02:e2
0.0.0.0/0 D
DHCPv4(eth1)=Enabled
DG4=0.0.0.0
DNS1:10.1.1.20
DNS2:10.1.1.31

eth2
00:0c:ec:04:02:e2
0.0.0.0/0 D
DHCPv4(eth2)=Enabled
DG4=0.0.0.0

eth3
00:0c:ec:06:02:e2
10.10.204.1/16 S
DHCPv4(eth3)=Disabled
DG4=10.10.204.254
[spadmin@Spectracom ~]$
```

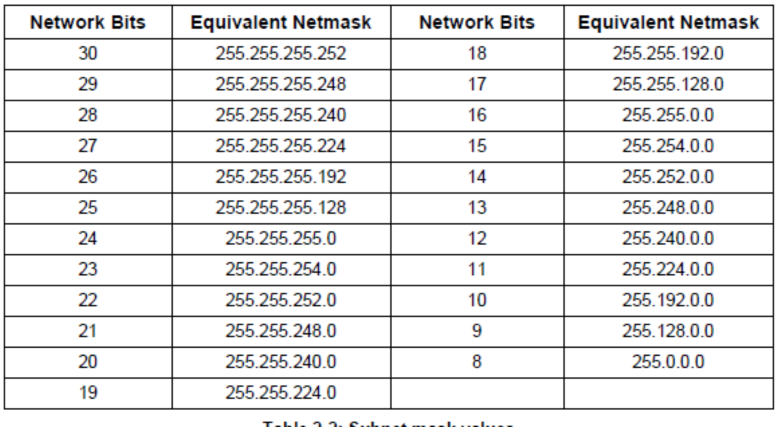
Ifconfig / ip addr

- just type "**ifconfig**" or "**ip addr**

Function: allows the operating system to setup network interfaces and allow the user to view information about the configured network interfaces.

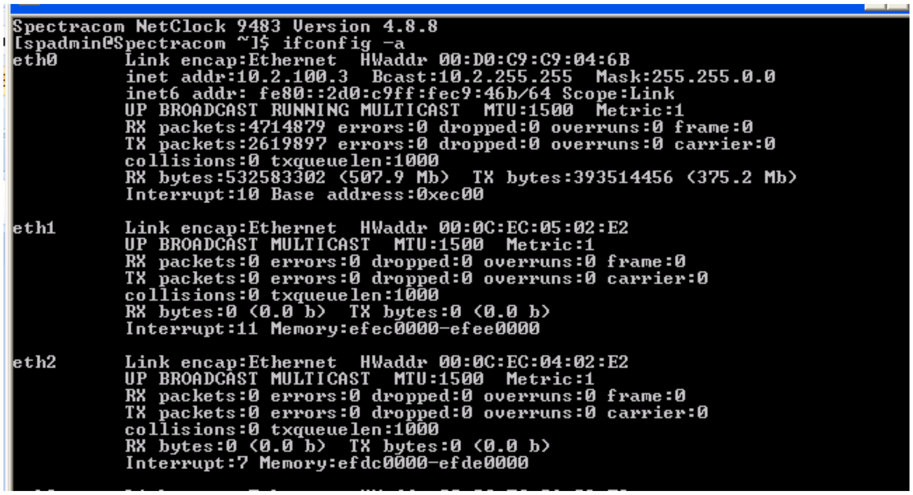
Displays: all IP addreses, subnet masks, MAC addresses, received/transmitted packets, dropped packets, packet collisions, etc

Netmask conversion table for quick-reference



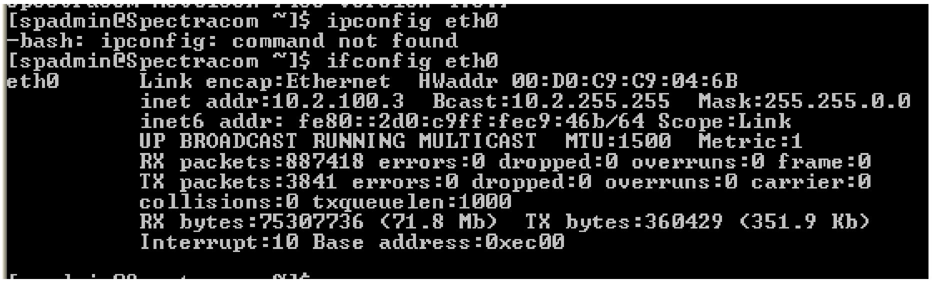
Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
30	255.255.255.252	18	255.255.192.0
29	255.255.255.248	17	255.255.128.0
28	255.255.255.240	16	255.255.0.0
27	255.255.255.224	15	255.254.0.0
26	255.255.255.192	14	255.252.0.0
25	255.255.255.128	13	255.248.0.0
24	255.255.255.0	12	255.240.0.0
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		

Ifconfig -a (Shows status of all network ports) (example below just shows a couple of the Ethernet ports)



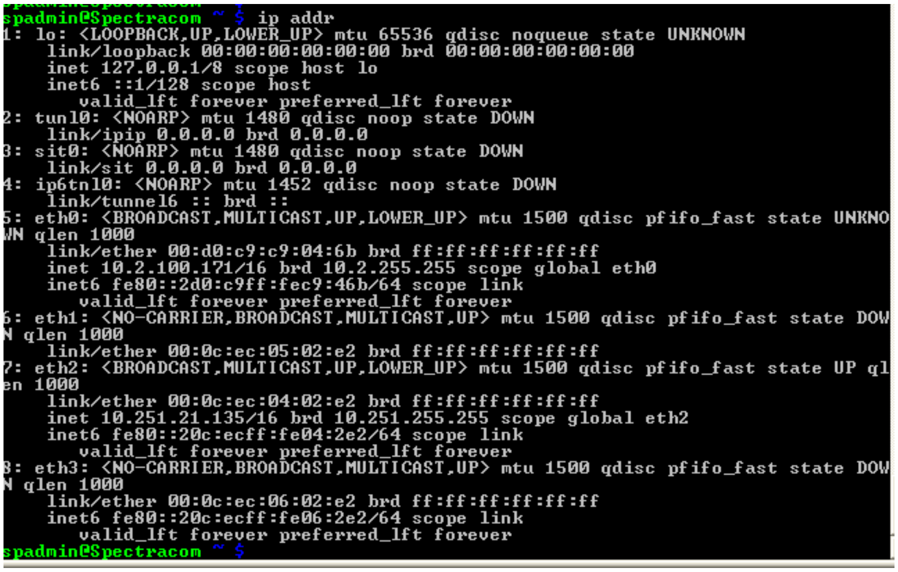
```
Spectracom NetClock 9483 Version 4.8.8
[spadmin@Spectracom ~]$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:D0:C9:C9:04:6B
          inet addr:10.2.100.3  Bcast:10.2.255.255  Mask:255.255.0.0
          inet6 addr: fe80::2d0:c9ff:fec9:46b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4714879 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2619897 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:532583302 (507.9 Mb)  TX bytes:393514456 (375.2 Mb)
          Interrupt:10 Base address:0xec00

eth1      Link encap:Ethernet  HWaddr 00:0C:EC:05:02:E2
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:11 Memory:efec0000-efee0000

eth2      Link encap:Ethernet  HWaddr 00:0C:EC:04:02:E2
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:7 Memory:efdc0000-efde0000
```

ifconfig etho (Shows only Eth0 status) – same for Eth1, Eth2 or Eth3



```
[spadmin@Spectracom ~]$ ipconfig eth0
-bash: ipconfig: command not found
[spadmin@Spectracom ~]$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:D0:C9:C9:04:6B
          inet addr:10.2.100.3  Bcast:10.2.255.255  Mask:255.255.0.0
          inet6 addr: fe80::2d0:c9ff:fec9:46b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:887418 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3841 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:75307736 (71.8 Mb)  TX bytes:360429 (351.9 Kb)
          Interrupt:10 Base address:0xec00
```

IP addr (IP Address)



```
spadmin@Spectracom ~ $ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: tunl0: <NOARP> mtu 1480 qdisc noop state DOWN
    link/ipip 0.0.0.0 brd 0.0.0.0
3: sit0: <NOARP> mtu 1480 qdisc noop state DOWN
    link/sit 0.0.0.0 brd 0.0.0.0
4: ip6tnl0: <NOARP> mtu 1452 qdisc noop state DOWN
    link/tunnel6 :: brd ::
5: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNO
WN qlen 1000
    link/ether 00:d0:c9:c9:04:6b brd ff:ff:ff:ff:ff:ff
    inet 10.2.100.171/16 brd 10.2.255.255 scope global eth0
    inet6 fe80::2d0:c9ff:fec9:46b/64 scope link
       valid_lft forever preferred_lft forever
6: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOW
N qlen 1000
    link/ether 00:0c:ec:05:02:e2 brd ff:ff:ff:ff:ff:ff
7: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql
en 1000
    link/ether 00:0c:ec:04:02:e2 brd ff:ff:ff:ff:ff:ff
    inet 10.251.21.135/16 brd 10.251.255.255 scope global eth2
    inet6 fe80::20c:ecff:fe04:2e2/64 scope link
       valid_lft forever preferred_lft forever
8: eth3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOW
N qlen 1000
    link/ether 00:0c:ec:06:02:e2 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::20c:ecff:fe06:2e2/64 scope link
       valid_lft forever preferred_lft forever
spadmin@Spectracom ~ $
```

Static Routes

- Refer to "Static Routes" (Static Routing) in the "Network" section further below in this document :

Holdover timeout

- Read current Holdover value: **SS_GetHoldoverTO 0** <enter>
- Change Holdover value: **SS_SetHoldoverTo 0 xxxx** <enter> (entered in 'seconds')

Note: available range is 1 second to 5 years

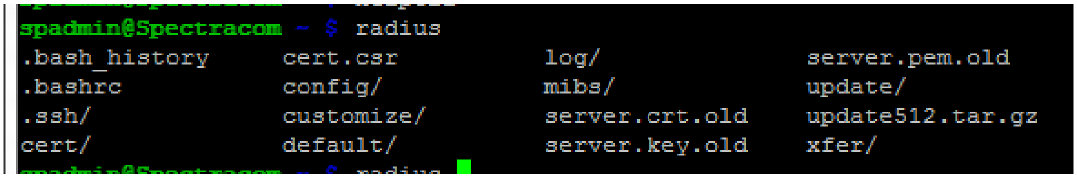
Holdover timeout is configured in "seconds"

Desired Holdover Length	Holdover Length (in seconds) to be entered
2 hours	7200 seconds (default value)
24 hours	86400
7 days	604,800
30 days	2,419,200
1 year	29,030,400
5 years	10.450,944,010

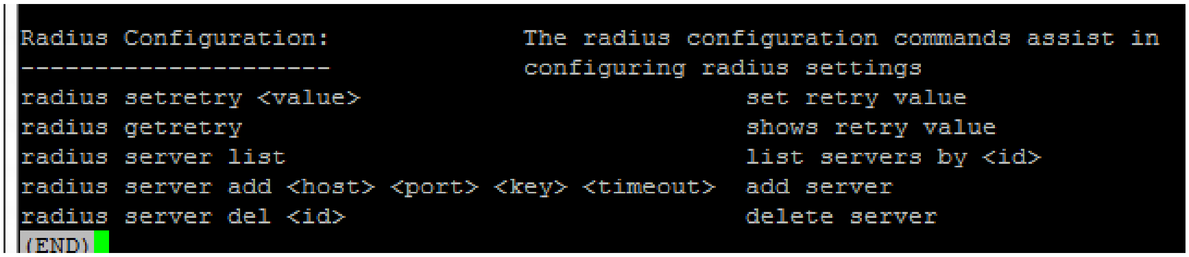
LDAP and Radius configuration

Radius CLI

- Not sure what software version these commands were added in.
- Type **radius** followed by the **tab** key to view the list of all radius commands



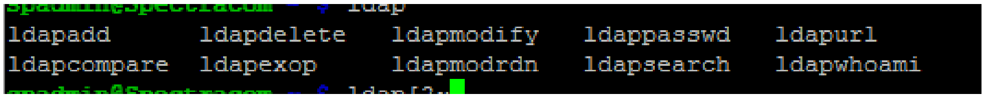
```
spadmin@Spectracom ~ $ radius
.bash_history      cert.csr          log/              server.pem.old
.bashrc            config/           mibs/             update/
.ssh/              customize/        server.crt.old    update512.tar.gz
cert/              default/          server.key.old    xfer/
spadmin@Spectracom ~ $ radius
```



```
Radius Configuration:                 The radius configuration commands assist in
---------------------                 configuring radius settings
radius setretry <value>                              set retry value
radius getretry                                      shows retry value
radius server list                                   list servers by <id>
radius server add <host> <port> <key> <timeout>      add server
radius server del <id>                               delete server
(END)
```

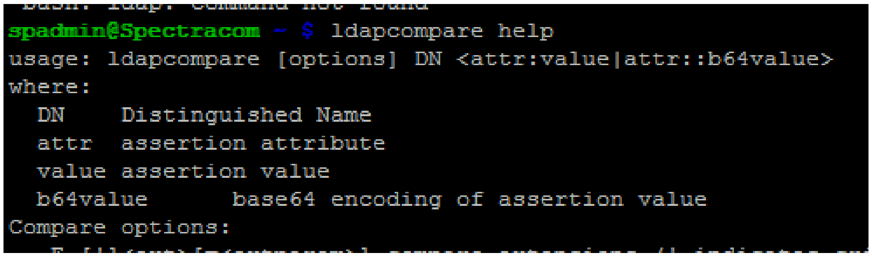
LDAP CLI

- Not sure what software version these commands were added in.
- Type ldap followed by the tab key to view the list of all ldap commands



```
spadmin@Spectracom ~ $ ldap
ldapadd       ldapdelete    ldapmodify    ldappasswd    ldapurl
ldapcompare   ldapexop      ldapmodrdn    ldapsearch    ldapwhoami
```

- Type a specific ldap command followed by a space and then the word help to see info about that command :

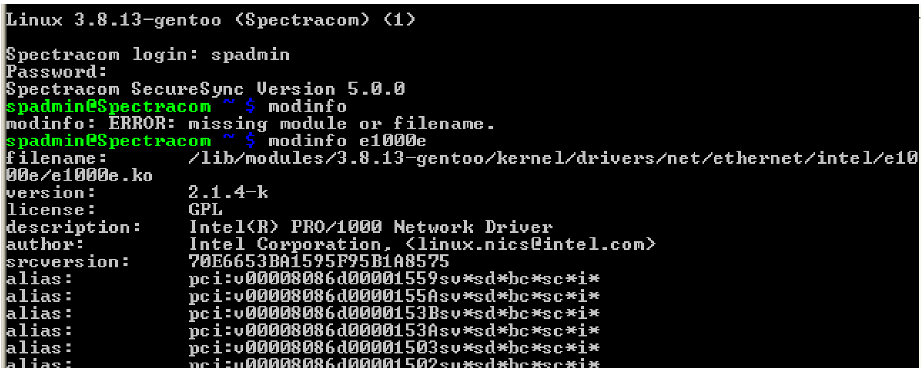


```
bash: ldap: command not found
spadmin@Spectracom ~ $ ldapcompare help
usage: ldapcompare [options] DN <attr:value|attr::b64value>
where:
  DN    Distinguished Name
  attr  assertion attribute
  value assertion value
  b64value      base64 encoding of assertion value
Compare options:
```

ldapurl:
 example response: ldap://:389 (I suspect ldap server address will be reported inside the two slashes, if it has been configured

"modinfo" Installed module/driver info(such as the e1000e network driver

- CLI command to see current version of E100e driver: **modinfo e1000e**

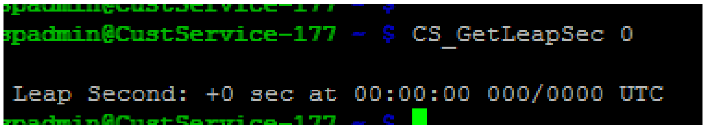


```
Linux 3.8.13-gentoo (Spectracom) (1)

Spectracom login: spadmin
Password:
Spectracom SecureSync Version 5.0.0
spadmin@Spectracom ~ $ modinfo
modinfo: ERROR: missing module or filename.
spadmin@Spectracom ~ $ modinfo e1000e
filename:       /lib/modules/3.8.13-gentoo/kernel/drivers/net/ethernet/intel/e10
00e/e1000e.ko
version:        2.1.4-k
license:        GPL
description:    Intel(R) PRO/1000 Network Driver
author:         Intel Corporation, <linux.nics@intel.com>
srcversion:     70E6653BA1595F95B1A8575
alias:          pci:v00008086d00001559sv*sd*bc*sc*i*
alias:          pci:v00008086d0000155Asv*sd*bc*sc*i*
alias:          pci:v00008086d0000153Bsv*sd*bc*sc*i*
alias:          pci:v00008086d0000153Asv*sd*bc*sc*i*
alias:          pci:v00008086d00001503sv*sd*bc*sc*i*
alias:          pci:v00008086d00001502sv*sd*bc*sc*i*
```

"free", "free mem" (free -m) and "cat/proc/meminfo" memory commands

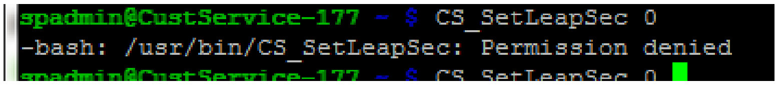
Scheduled leap second

- Command to get the next scheduled leap second: **CS_GetLeapSec 0**



```
spadmin@CustService-177 ~ $
spadmin@CustService-177 ~ $ CS_GetLeapSec 0

 Leap Second: +0 sec at 00:00:00 000/0000 UTC
spadmin@CustService-177 ~ $
```

Note: User doesn't have permission to schedule the next leap second via the cli. It needs to be scheduled via the browser



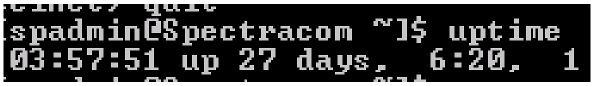
```
spadmin@CustService-177 ~ $ CS_SetLeapSec 0
-bash: /usr/bin/CS_SetLeapSec: Permission denied
spadmin@CustService-177 ~ $ CS_SetLeapSec 0
```

System "Uptime"

CLI commands which report the system uptime

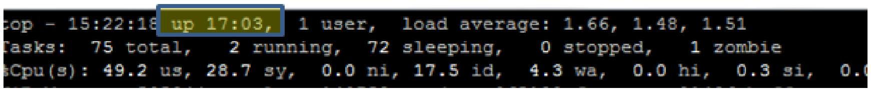
1. **SS_GetUptime**

2. **uptime**



```
telnet> quit
spadmin@Spectracom ~]$ uptime
03:57:51 up 27 days,  6:20,  1
```

3. **"top" command**



```
top - 15:22:18 up 17:03,  1 user,  load average: 1.66, 1.48, 1.51
Tasks:  75 total,   2 running,  72 sleeping,   0 stopped,   1 zombie
Cpu(s): 49.2 us, 28.7 sy,  0.0 ni, 17.5 id,  4.3 wa,  0.0 hi,  0.3 si,  0.0
```

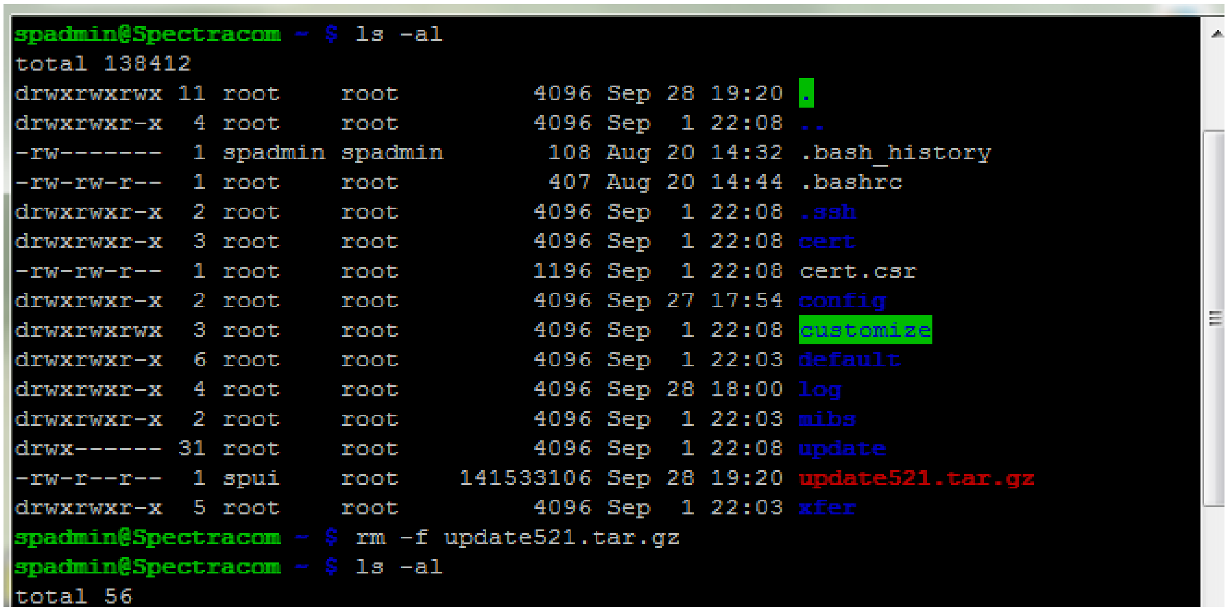
- The "top" command also reports the uptime (at the top of the response)
- Refer to http://linux.about.com/od/commands/l/blcmdl1_top.htm

Command to reset the Network Access table

- Version 4.4.0 (possibly before) adds a new CLI command (“**unrestrict**”) to clear the Access table. In units with 4.4.0 or higher installed, no longer need to clean all configurations. This can be performed via the CLI- it’s not available via the keypad (it’s not in the Front panel “Cmd” menu).

Manually delete an update file (if can’t delete it via the browser)

1) Type **rm -f xxxxxx** (where xxxxxx is the file name to be deleted)



```
spadmin@Spectracom ~ $ ls -al
total 138412
drwxrwxrwx 11 root    root          4096 Sep 28 19:20 .
drwxrwxr-x  4 root    root          4096 Sep  1 22:08 ..
-rw-------  1 spadmin spadmin        108 Aug 20 14:32 .bash_history
-rw-rw-r--  1 root    root           407 Aug 20 14:44 .bashrc
drwxrwxr-x  2 root    root          4096 Sep  1 22:08 .ssh
drwxrwxr-x  3 root    root          4096 Sep  1 22:08 cert
-rw-rw-r--  1 root    root          1196 Sep  1 22:08 cert.csr
drwxrwxr-x  2 root    root          4096 Sep 27 17:54 config
drwxrwxrwx  3 root    root          4096 Sep  1 22:08 customize
drwxrwxr-x  6 root    root          4096 Sep  1 22:03 default
drwxrwxr-x  4 root    root          4096 Sep 28 18:00 log
drwxrwxr-x  2 root    root          4096 Sep  1 22:03 mibs
drwx------ 31 root    root          4096 Sep  1 22:08 update
-rw-r--r--  1 spui    root     141533106 Sep 28 19:20 update521.tar.gz
drwxrwxr-x  5 root    root          4096 Sep  1 22:03 xfer
spadmin@Spectracom ~ $ rm -f update521.tar.gz
spadmin@Spectracom ~ $ ls -al
total 56
```

Ability to perform software updates via CLI interface (for scripting updates)

- Version 4.8.8 (Dec 2012-ECN 3099) Added sysupgrade CLI command to perform software updates.

Ability to perform a software upgrade via CLI command (instead of using the web browser), such as for scripting software updates

Starting in Archive software version 4.8.8, the software update can be initiated using a CLI command (issued via telnet, SSH or the front panel Serial port), instead of using the web browser, if desired. This entails performing an FTP/SCP transfer of the software update file into the SecureSync's */home/spectracom* directory **and then issuing the *sysupgrade*** CLI command to initiate the software upgrade.

The syntax for issuing the *sysupgrade* command is:

- Standard upgrade (Such as upgrading versions 4.8.8 to 4.8.9 for example): "sysupgrade" followed by the upgrade file name (Example: *sysupgrade update489.tar.gz*).
- Forced upgrade (Such as downgrading versions 4.8.9 to 4.8.8 for example, but can also be used with Standard upgrades, also): "sysupgrade force" followed by the upgrade file name (Example: *sysupgrade force update489.tar.gz*).
- Clean upgrade (Such as first performing a Forced upgrade from 4.8.8 to 4.8.9, for example. Then automatically resetting the NTP server back to factory default settings and deleting all log files): "sysupgrade clean" followed by the upgrade file name (Example: *sysupgrade clean update489.tar.gz*).

Note:

- **FTP port** is port 21
- **SCP port** is port 22

Base 1PPS output Enable /Disable control using "ppsctrl" command

- Version 4.8.7 (~Sept 2012) added **ppsctrl** command to enable or disable the 1PPS output on the rear panel

Q from BAE systems- Our requirement is to be able to Enable\Disable the 1PPS outputs programmatically. To do so, I use the CLI command ppsctrl. The question is, can the resultant output level of a disabled 1PPS control be programmatically set? Most times, when disabled it is 0V which is what we need. Sometimes though, it is 10V which is bad for us. It seems the level depends on where in the 1PPS pulse the output transitions to disabled.

A Per Dave Sohn 19 Mar 15: "We currently freeze the output at the current level, I believe, and is played out according to your report. There isn't a way to do what you want programmatically. However, depending on the responsiveness for your disable, you could perform the disable half way through the second, which would ensure that the 1PPS is already in its inactive state.

Use of REST API to control 1PPS output(s)

Per Dave Sohn (12 Apr 17) These configurations can also be adjusted via the REST API that we are continuing to document. Any 1PPS or 10MHz in the system could be controlled in this way.

Base 10MHz output Enable / Disable output control

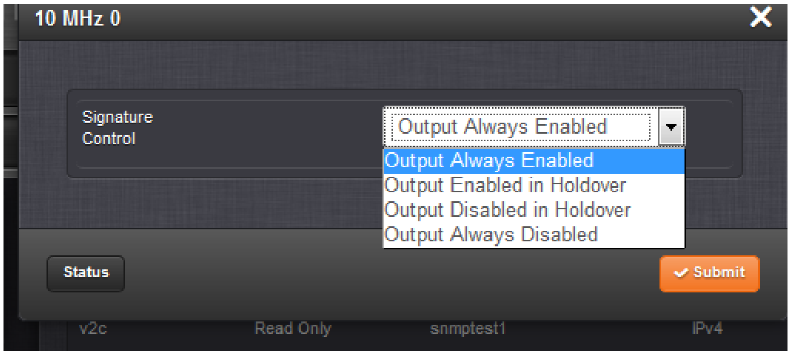
- As of at least Apr 2017 (v5.6. 0 and below), 10 MHz output is not configurable with CLI call.
- Per Dave Sohn (~9/21/12), may consider adding it with an NRE fee (or likely with very large purchase).
- Per Dave Sohn (12 Apr 17)

Use of REST API to control 10 MHz output(s)

Per Dave Sohn (12 Apr 17) These configurations can also be adjusted via the REST API that we are continuing to document. Any 1PPS or 10MHz in the system could be controlled in this way.

Use of web browser to control 10 MHz

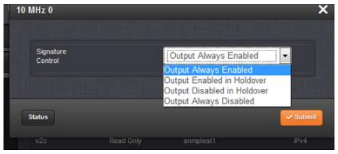
- As of at least v5.6.0, the 10 MHz output can only be disabled via the browser (set Signature Control to “Output Always Disabled” in the **Interfaces** -> **10 MHz 0** page of the browser):



10 MHz 0

Signature Control: Output Always Enabled

Partial email from Keith (12 Apr 17 and added to on 17 May 17) …Currently, the 10 MHz output can only be disabled by changing the configuration of the 10 MHz Signature Control in the web browser. Signature Control for just the 10Mhz output can be set to “Output Always disabled” for as long as its desired to squelch this particular output (no effects on the other outputs/functions of the system) as shown below:



10 MHz 0

Signature Control: Output Always Enabled

However, we could consider adding a serial/CLI interface command which would also allow the output to be controlled remotely, or these settings could also be adjusted via the REST API interface.

Wade Sober can work with our SecureSync Product Manager to see what may be required (such as any associated NRE fees/minimum orders, etc) to have either a CLI command and/or REST API interface added, which can also allow the 10 MHz output to be enabled/disabled, in addition to being able to using the web browser

Commands to zeroize SAASM receiver (when installed)

- Version 4.8.8 (Dec 2012-ECN 3099) Added **zeroize** command to CLI to support emergency zeroize and zeroize keys.

CF card memory usage / “du” command

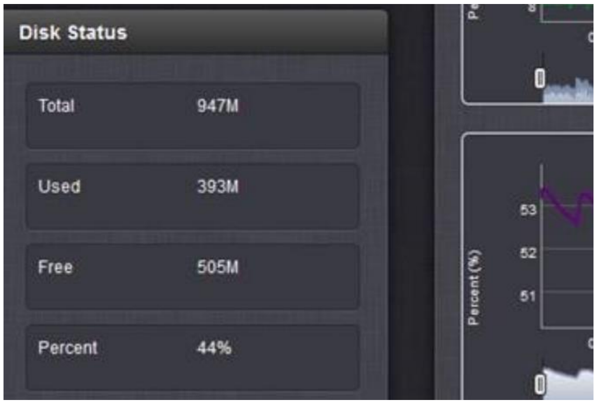
- Percent of Cf card usage can be checked using any of the following:

1) Web browser

Note: not available in classic interface

- **Tools** –> **System Monitor** page of the web browser (versions **5.3.1 and above**)

  Refer to the “**Percent**” field at the bottom of this section.



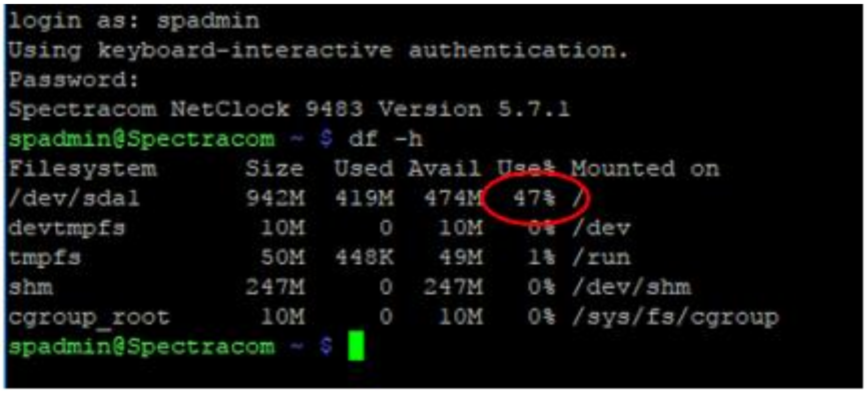
Disk Status

Total	947M
Used	393M
Free	505M
Percent	44%

- **Tools** -> **Upgrade/backup** page (versions 5.2.0 to 5.3.0) (under “**Disk Status**”)

2) CLI interface

- Type “**df**” or “**df -h**” at the command prompt (note there is a space between the “f” and the “-h”)



```
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 5.7.1
spadmin@Spectracom ~ $ df -h
Filesystem        Size  Used Avail Use% Mounted on
/dev/sda1         942M  419M  474M  47% /
devtmpfs           10M     0   10M   0% /dev
tmpfs              50M  448K   49M   1% /run
shm               247M     0  247M   0% /dev/shm
cgroup_root        10M     0   10M   0% /sys/fs/cgroup
spadmin@Spectracom ~ $
```

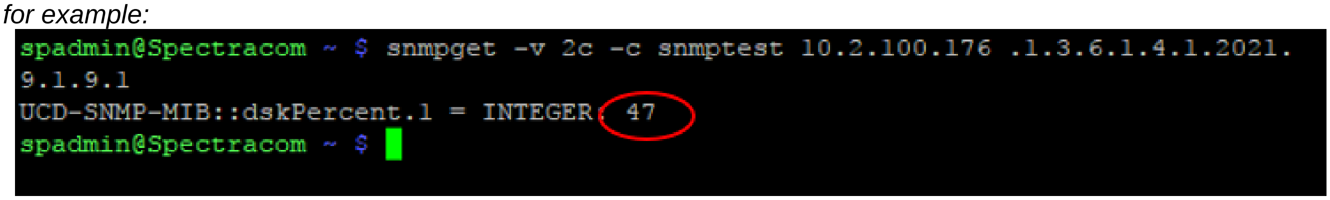
If the “**Use%”** in the **“/dev/hda1**” row is greater than around 70%, it may have a lot of logs and previous update bundles stored in the flash card. If it’s greater than around 70% or so, let me know and I will provide you with info on how to delete past update files that remain stored in the unit after each updated.

3) Using SNMP

- disk usage can be also be checked via SNMP by performing an SNMP get of OID: .1.3.6.1.4.1.2021.9.1.9.1

snmpget -v 2c -c snmptest 10.2.100.176 .1.3.6.1.4.1.2021.9.1.9.1

for example:



```
spadmin@Spectracom ~ $ snmpget -v 2c -c snmptest 10.2.100.176 .1.3.6.1.4.1.2021.
9.1.9.1
UCD-SNMP-MIB::dskPercent.1 = INTEGER: 47
spadmin@Spectracom ~ $
```

Notes if the CF card is full or nearly full:

1) With Versions 5.2.0 (and above) **clear all logs** and **clear all stats** (bottom-left of the **Tools** -> **Upgrade/Backup** page, bottom-left corner).

    1) **clearlogs** and **clearstats** commands via and cli were added in version 5.1.5 (I believe). The **Clear All Logs**" and "**Clear all Stats**" buttons were added in 5.2.1 (I believe). (bottom-left of the **Tools** -> **Upgrade/Backup** page)

    2) But with at least software versions 5.2.1 and below, these two buttons in the browser don't work (should be fixed in 5.30). Have to use the cli commands only to delete these items with 5.2.1 and below.

    3) The Temp directory may have lots of info in it. Reboot or power cycle to clear the temp directory. Run the **df –h** command again to see if the usage number has dropped because temp was cleared out.

    4) Run the first "du" command below to show contents of different parts of the CF card to see what Section is higher than normal. The largest directories are at the top of the list.

    5) Refer to the "SecureSync logs" and "SecureSync web browser" sections of this document for more information on a full CF card.

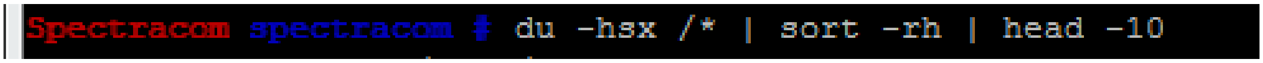
"du" commands (Use if the CF card is quite or completely full, such as with nullmailer tidbits)

- Refer to http://www.cyberciti.biz/faq/how-do-i-find-the-largest-filesdirectories-on-a-linuxunixbsd-filesystem/

Note: If the card is full or nearly full, to see the top 10 largest directories (and each file, in "MB) perform the first "du" command below to see the entire CF card contents. Or, go to a particular directory and perform the second "du" command to see the contents of just that directory.

Entire contents of the CF card

At the prompt (home/spectracom directory), type the following: **du -hsx /* | sort -rh | head -10** <enter> (where the vertical line "pipe" is SHIFT and the key under the **backspace** key)



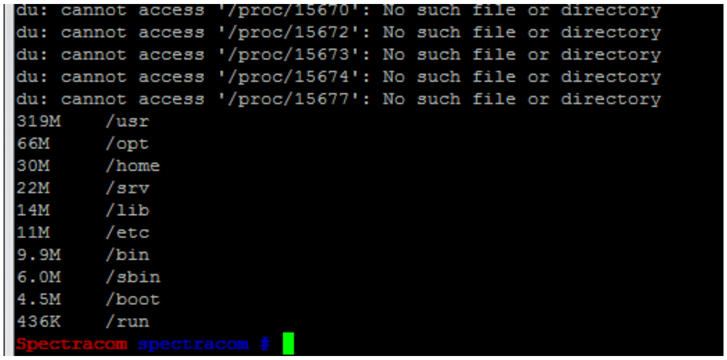
```
Spectracom spectracom # du -hsx /* | sort -rh | head -10
```

Note it may take a fee moments for the full response to be displayed.

Scroll down to the bottom (past all of the **"permission denied**" entries) to see the directories and their sizes. Refer to "C" below to list the content/sizes of the large directories below (such as /usr or /tmp for instance)

(Example entry below is from version 5.3.0) you can use these directory sizes to help determine which of their directories are larger than normal.

These are the directories to look at more closely (by switching to that directory and typing **ls -lh** (as discussed in more detail a little further down).



```
du: cannot access '/proc/15670': No such file or directory
du: cannot access '/proc/15672': No such file or directory
du: cannot access '/proc/15673': No such file or directory
du: cannot access '/proc/15674': No such file or directory
du: cannot access '/proc/15677': No such file or directory
319M    /usr
66M     /opt
30M     /home
22M     /srv
14M     /lib
11M     /etc
9.9M    /bin
6.0M    /sbin
4.5M    /boot
436K    /run
Spectracom spectracom #
```

Steps to determine CF card usage:

1) Type **du -hsx /* | sort -rh | head -10**
2) Disregard “permission denied”
3) Scroll down to bottom of the response to see the top 10 largest directories
   - These are the directories to look at more closely (by switching to that directory and typing **ls -lh** (as discussed in more detail a little further down).
4) If /var/nullmailer is in the list, nullmailer is taking up too much space and needs to be cleared out.
5) See if sqlbackup is listed – it can be removed (**rm sqlbackup.** command
6) If /tmp is one of the larger directories in the list- reboot/power cycle the unit to clean this directory. The likely reason for a large /tmp directory is due to using tcpdump.

Steps to clean nullmailer while logged in as spfactory

Gotomeeting

1) Open Gotomeeting
2) Sending invite to email address (add meeting in outlook)
3) Download “desktop” (not lite, becase lite can’t provide mouse and keyboard
4) Share keyboard and mouse
5) Make customer the presenter
6) Make sure to exit twice at the end to ensure out of roor user and spfactory acounts

1. Login as, or switch to, spfactory user:
   - To swich from spadmin to spfactory, type: **su -l spfactory** <enter> (letter L- not i) and then enter spfactory password.
2. Switch to root user: type: **sudo su** <enter>
3. type **cd /var**<enter>
4. in /var directory, type **du -s /* | sort -nr | head** <enter>
5. if **nullmailer** directory looks jarge, navigate to (type) **cd /var/nullmailer/queue** <enter>
6. **type rm *** <enter> **(while in the var/nullmailer/queue directory)!!!!**
7. **Look for sqlbackup file in any listed directory. Delete it with rm sqlbackup. <enter> mmand**
8. **Type df -h** <enter>

9. **Type** exit <enter> to logout of root

10. **Again, type** exit <enter> to logout of spfactory

Check just the contents of the current directory (such as the default directory of home/spectracom)

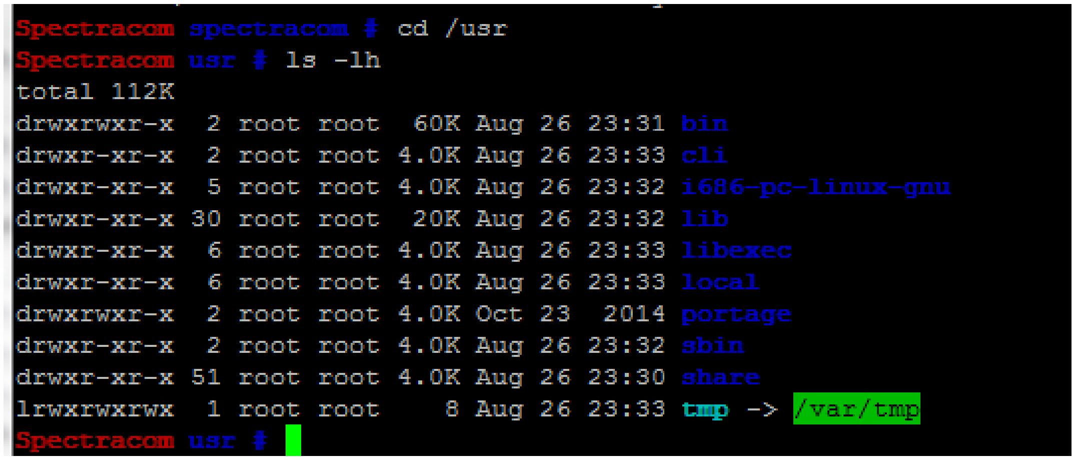
Note: it appears this no longer works in at least 5.3.0??

- In the desired directory, type the following: **du –s * | sort –nr** <enter> (where the vertical line "pipe" is CTRL and the key under backspace)
- Note: to see just the contents of the entire CF card (not just the current directory, see the other "du" command above).

List the logs and their file sizes

Show the total size of the "Spectracom" logs (such as GPS Qual, Oscillator, etc)

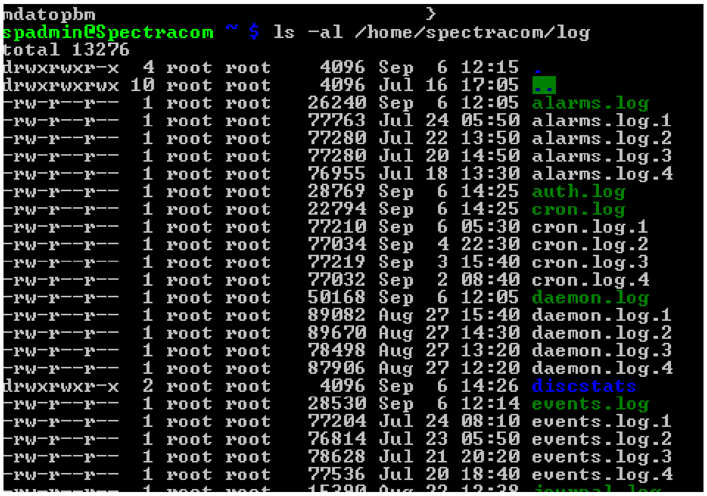
1) Type "**ls -lh** " at the command prompt (note there is a space between the "s" and the "-lh")
2) The total size of the Spectracom logs is in the "log" row.



```
Spectracom spectracom # cd /usr
Spectracom usr # ls -lh
total 112K
drwxrwxr-x  2 root root  60K Aug 26 23:31 bin
drwxr-xr-x  2 root root 4.0K Aug 26 23:33 cli
drwxr-xr-x  5 root root 4.0K Aug 26 23:32 i686-pc-linux-gnu
drwxr-xr-x 30 root root  20K Aug 26 23:32 lib
drwxr-xr-x  6 root root 4.0K Aug 26 23:33 libexec
drwxr-xr-x  6 root root 4.0K Aug 26 23:33 local
drwxrwxr-x  2 root root 4.0K Oct 23  2014 portage
drwxr-xr-x  2 root root 4.0K Aug 26 23:32 sbin
drwxr-xr-x 51 root root 4.0K Aug 26 23:30 share
lrwxrwxrwx  1 root root    8 Aug 26 23:33 tmp -> /var/tmp
Spectracom usr #
```

Show the total size of each of the "Spectracom" logs (such as GPS Qual, Oscillator, etc) individually

1) Type: **ls –al /home/spectracom/log** <enter>

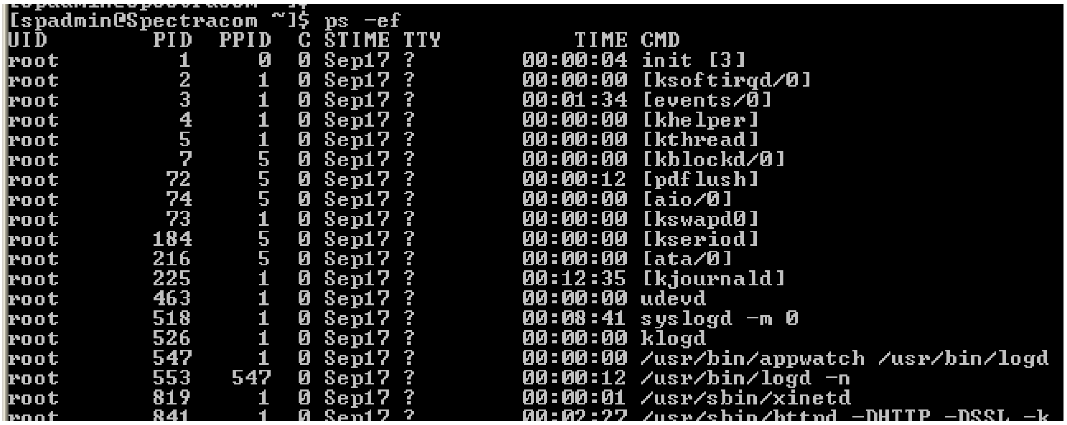


```
mdatopbm                                      }
spadmin@Spectracom ~ $ ls -al /home/spectracom/log
total 13276
drwxrwxr-x  4 root root    4096 Sep  6 12:15 .
drwxrwxrwx 10 root root    4096 Jul 16 17:05 ..
-rw-r--r--  1 root root   26240 Sep  6 12:05 alarms.log
-rw-r--r--  1 root root   77763 Jul 24 05:50 alarms.log.1
-rw-r--r--  1 root root   77280 Jul 22 13:50 alarms.log.2
-rw-r--r--  1 root root   77280 Jul 20 14:50 alarms.log.3
-rw-r--r--  1 root root   76955 Jul 18 13:30 alarms.log.4
-rw-r--r--  1 root root   28769 Sep  6 14:25 auth.log
-rw-r--r--  1 root root   22794 Sep  6 14:25 cron.log
-rw-r--r--  1 root root   77210 Sep  6 05:30 cron.log.1
-rw-r--r--  1 root root   77034 Sep  4 22:30 cron.log.2
-rw-r--r--  1 root root   77219 Sep  3 15:40 cron.log.3
-rw-r--r--  1 root root   77032 Sep  2 08:40 cron.log.4
-rw-r--r--  1 root root   50168 Sep  6 12:05 daemon.log
-rw-r--r--  1 root root   89082 Aug 27 15:40 daemon.log.1
-rw-r--r--  1 root root   89670 Aug 27 14:30 daemon.log.2
-rw-r--r--  1 root root   78498 Aug 27 13:20 daemon.log.3
-rw-r--r--  1 root root   87906 Aug 27 12:20 daemon.log.4
drwxrwxr-x  2 root root    4096 Sep  6 14:26 discstats
-rw-r--r--  1 root root   28530 Sep  6 12:14 events.log
-rw-r--r--  1 root root   77204 Jul 24 08:10 events.log.1
-rw-r--r--  1 root root   76814 Jul 23 05:50 events.log.2
-rw-r--r--  1 root root   78628 Jul 21 20:20 events.log.3
-rw-r--r--  1 root root   77536 Jul 20 18:40 events.log.4
-rw-r--r--  1 root root   15390 Aug 22 12:38 journal.log
```

Show all processes that are currently running (PIDs)

Type "**ps -el**" at the command prompt (note there is a space between the "s" and the "-ef")

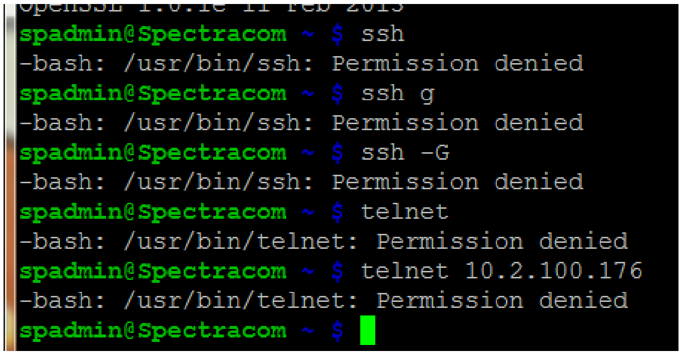
Note: Can also type "**ps -elf**" at the command prompt for even more data



```
[spadmin@Spectracom ~]$
[spadmin@Spectracom ~]$ ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 Sep17 ?        00:00:04 init [3]
root         2     1  0 Sep17 ?        00:00:00 [ksoftirqd/0]
root         3     1  0 Sep17 ?        00:01:34 [events/0]
root         4     1  0 Sep17 ?        00:00:00 [khelper]
root         5     1  0 Sep17 ?        00:00:00 [kthread]
root         7     5  0 Sep17 ?        00:00:00 [kblockd/0]
root        72     5  0 Sep17 ?        00:00:12 [pdflush]
root        74     5  0 Sep17 ?        00:00:00 [aio/0]
root        73     1  0 Sep17 ?        00:00:00 [kswapd0]
root       184     5  0 Sep17 ?        00:00:00 [kseriod]
root       216     5  0 Sep17 ?        00:00:00 [ata/0]
root       225     1  0 Sep17 ?        00:12:35 [kjournald]
root       463     1  0 Sep17 ?        00:00:00 udevd
root       518     1  0 Sep17 ?        00:08:41 syslogd -m 0
root       526     1  0 Sep17 ?        00:00:00 klogd
root       547     1  0 Sep17 ?        00:00:00 /usr/bin/appwatch /usr/bin/logd
root       553   547  0 Sep17 ?        00:00:12 /usr/bin/logd -n
root       819     1  0 Sep17 ?        00:00:01 /usr/sbin/xinetd
root       841     1  0 Sep17 ?        00:02:27 /usr/sbin/httpd -DHTTP -DSSL -k
```

"SSH", telnet, "FTP"

- For security reasons, starting in version 5.1.3, can no longer go "outbound" with service commands (can't telnet /ssh FROM this time server to another device. Can only telnet into this time server from another device).
- Reports "Permission denied" if attempted.



```
OpenSSL 1.0.1e 11 Feb 2013
spadmin@Spectracom ~ $ ssh
-bash: /usr/bin/ssh: Permission denied
spadmin@Spectracom ~ $ ssh g
-bash: /usr/bin/ssh: Permission denied
spadmin@Spectracom ~ $ ssh -G
-bash: /usr/bin/ssh: Permission denied
spadmin@Spectracom ~ $ telnet
-bash: /usr/bin/telnet: Permission denied
spadmin@Spectracom ~ $ telnet 10.2.100.176
-bash: /usr/bin/telnet: Permission denied
spadmin@Spectracom ~ $
```

Status of Services (such as Apache, for instance)

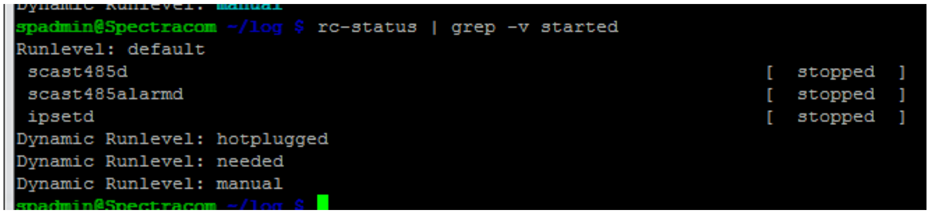
rc-status command

Note: Run this command using SSH (not telnet). Telnet doesn't display the left side of the response, which are the names of all the corresponding Services.

- This command checks if the previous command (i.e. the start/restart/stop of a service) executed successfully and sets the "status value".

Checking for just all STOPPED services

- With grep. "**-v**" causes it to search for the "opposite"
- Type **rc-status | grep started**

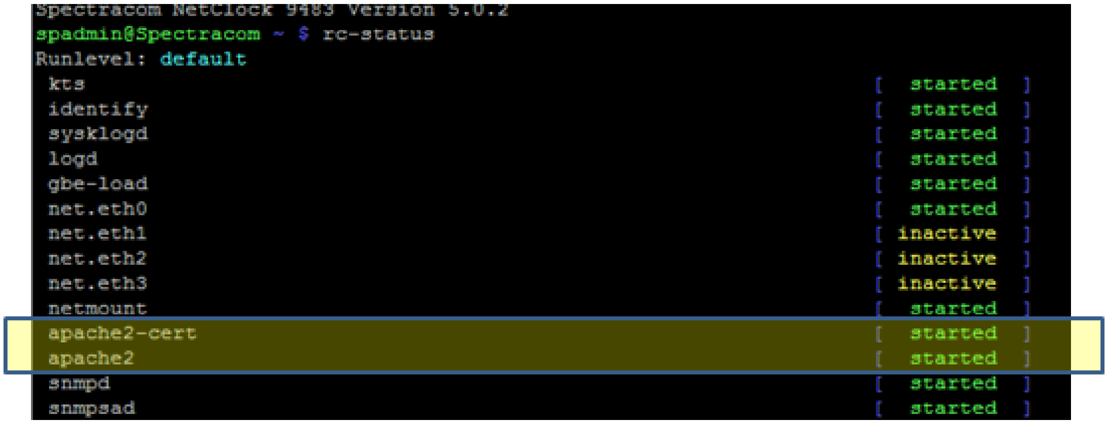


```
Dynamic Runlevel: manual
spadmin@Spectracom ~/log $ rc-status | grep -v started
Runlevel: default
 scast485d                                                         [  stopped  ]
 scast485alarmd                                                    [  stopped  ]
 ipsetd                                                            [  stopped  ]
Dynamic Runlevel: hotplugged
Dynamic Runlevel: needed
Dynamic Runlevel: manual
spadmin@Spectracom ~/log $
```

Checking for Apache (HTTP/HTTPS)

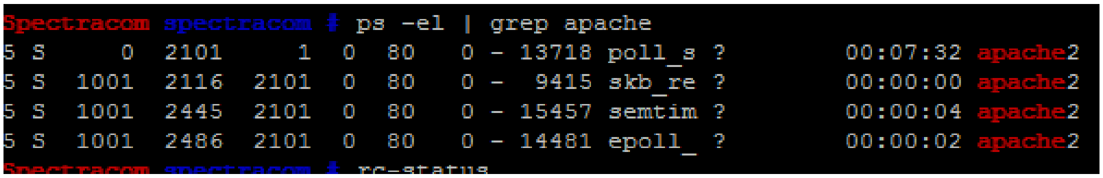
Note: To check for Apache, browser must be open (login screen displayed or logged into the browser)

1. Make sure Apache2 is "started" (not "stopped", "crashed" or "scheduled")



```
Spectracom NetClock 9483 Version 5.0.2
spadmin@Spectracom ~ $ rc-status
Runlevel: default
 kts                                                         [  started  ]
 identify                                                    [  started  ]
 sysklogd                                                    [  started  ]
 logd                                                        [  started  ]
 gbe-load                                                    [  started  ]
 net.eth0                                                    [  started  ]
 net.eth1                                                    [ inactive  ]
 net.eth2                                                    [ inactive  ]
 net.eth3                                                    [ inactive  ]
 netmount                                                    [  started  ]
 apache2-cert                                                [  started  ]
 apache2                                                     [  started  ]
 snmpd                                                       [  started  ]
 snmpsad                                                     [  started  ]
```

2. Make sure “**Apache2**” is listed (**ps -el | grep apache**)



```
Spectracom spectracom # ps -el | grep apache
5 S     0  2101     1  0  80   0 - 13718 poll_s ?        00:07:32 apache2
5 S  1001  2116  2101  0  80   0 -  9415 skb_re ?        00:00:00 apache2
5 S  1001  2445  2101  0  80   0 - 15457 semtim ?        00:00:04 apache2
5 S  1001  2486  2101  0  80   0 - 14481 epoll_ ?        00:00:02 apache2
Spectracom spectracom # rc-status
```

“Out-bound” network troubleshooting commands

- Refer to the following section further down for more info: Network troubleshooting from within SecureSync

Version 4.8.0 (ECN 2802) Added “out-bound” network tools to the command line interface for troubleshooting network issues associated with the SecureSync’s network.
Added the following network troubleshooting tool commands: ifconfig, arp, rarp, route, netstat, domainname, dig, host, nslookup and traceroute.

These commands can only be used from the front panel SERIAL port, telnet, SSH etc. They are not in the web browser.

Sync/Holdover status via CLI command

'syncstate' command: (Added in software version **4.8.6)** It prints one of three responses: **Sync**, **Holdover** or **Free Run.**

KW as of at least 2/9/12) the SecureSyncs Sync /Holdover state is not directly available via the CLI commands. It is only available via SNMP or web browser (The Status command shows Sync, but it’s the NTP sync state, not the System’s sync status).

Update to note above: Version 4.8.6 adds new CLI call ‘**syncstate’** which provides sync status.

Email to Justin Tabeling with RT Logic (2/9/12)

I just spoke to the engineer that implemented the front panel LCD/Keypad design and the CLI interface commands. The primary purpose of the front panel CLI interface is to provide the data to and from the front panel keypad/LCD display. The CLI was never meant to be a primary means of remotely monitoring or configuring the SecureSync. The primary method for performing these functions is via either the web browser or SNMP.

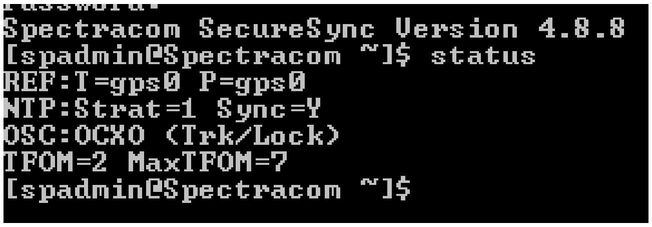
As the SecureSync’s sync state is directly displayed with the state of an LED on the front panel, there was no need for a CLI command to read the sync state. So, there is no Sync/Holdover state reported via the CLI interface. However, the current Sync and Holdover states can be obtained remotely using the SNMP get functionality. If you have one of more SNMP Managers on the network, these status values can be read by the SNMP Manager, after compiling the SecureSync mib files.

Attached you should find a document that discusses the SNMP functionality of the SecureSync, in much greater detail than the user manual.

Status via CLI command

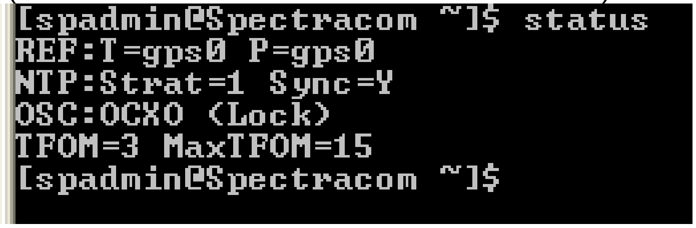
‘status’ command**:** Shows NTP Sync status, TOM/MaxTFOM and NTP stratum level. (In software versions prior to 4.8.6, Sync state of the box is not available via CLI. Information about this is below. The fix is to upgrade to v4.8.6 or above and then use the **syncstate** CLI call (mentioned above).

(Archive Version 4.8.8 and above - see note below)



```
Spectracom SecureSync Version 4.8.8
[spadmin@Spectracom ~]$ status
REF:T=gps0 P=gps0
NTP:Strat=1 Sync=Y
OSC:OCXO (Trk/Lock)
TFOM=2 MaxTFOM=7
[spadmin@Spectracom ~]$
```

(Archive Version 4.8.7 and below - see note below)



```
[spadmin@Spectracom ~]$ status
REF:T=gps0 P=gps0
NTP:Strat=1 Sync=Y
OSC:OCXO (Lock)
TFOM=3 MaxTFOM=15
[spadmin@Spectracom ~]$
```

Note: Reported Oscillator lock State name changed (changed from “Lock” to “Trk/Lock”)
“Osc” value in this status command

(**Mantis Case 1880)** Version **4.8.8** update changed the reported state name, to also account for the newest Low Phase Noise Rb oscillator, also.

Note in this Mantis case from Dave Sohn: The new disciplining states associated with the low phase noise rubidium changed the lock state to track/lock to cover all oscillator cases. The procedure should be updated to reflect that.

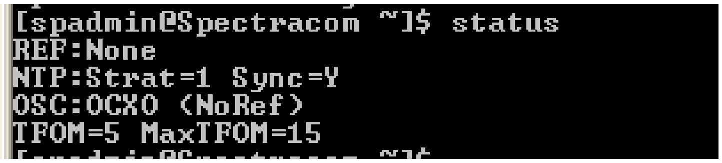
“**REF**” value in the first line of the status command:

- When a value other than “Ref: None” is displayed, the SecureSync is either in full sync mode or in the Holdover mode (treated like full sync mode).
- If SecureSync is not in Sync, both these values will change to “REF: None”.
- (Versions 4.8.7 and above) If NTP is the time reference, the REF line will show BOTH he selected NTP NTP server as well as the selected PPS reference (Version 4.8.6 and below- as shown further below - only reported the selected Time Reference but not the PPS reference

```
[spadmin@fe01pdei08 cli]$ ./status
REF:T=ntp  P=epp0
NTP:Strat=2 Sync=Y
OSC:Rb (Trk/Lock)
TFOM=2 MaxTFOM=15
```

(**Versions 4.8.6 and below**) If NTP is the selected time reference, the REF line will only show the selected NTP server (as shown in example below)

In the screenshot below, I disabled GPS (and all other input references) and made Holdover mode last only one second. This shows the result of the status message when SecureSync is out of sync (lost all references and Holdover mode expired):

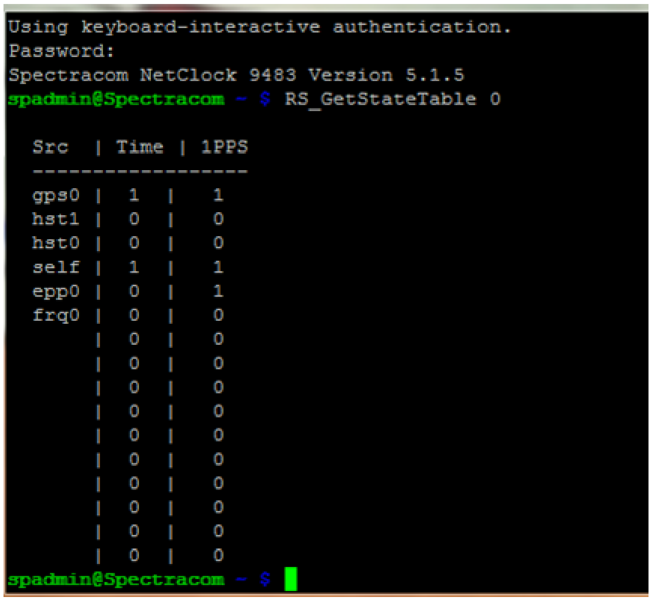


```
[spadmin@Spectracom ~]$ status
REF:None
NTP:Strat=1 Sync=Y
OSC:OCXO (NoRef)
TFOM=5 MaxTFOM=15
```

Reference Status table via CLI

- ➢ Though limited Reference Status is available via SNMP (as of at least version 5.1.5), the status of all references can be polled via CLI interface.

- At command prompt, type: **RS_GetStateTable 0** <enter>



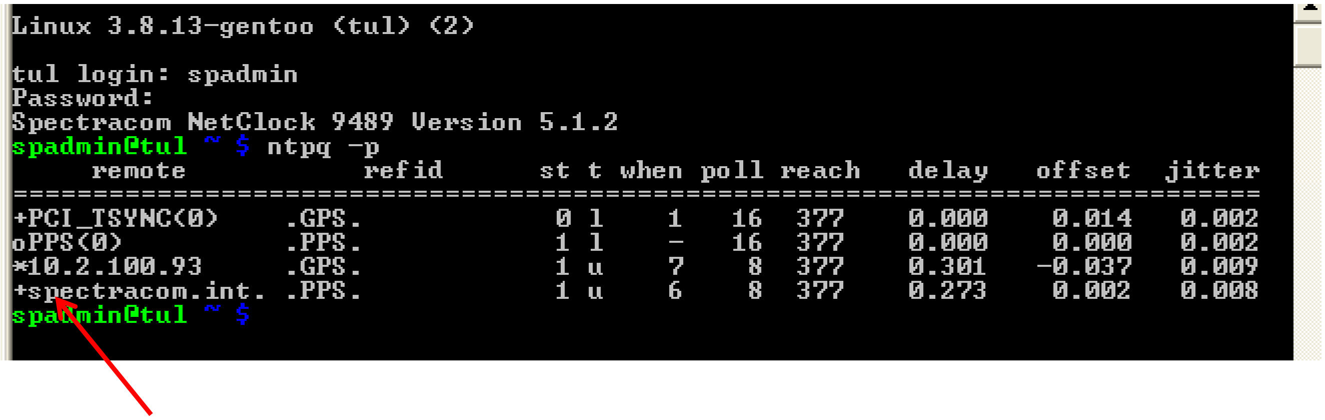
```
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 5.1.5
spadmin@Spectracom ~ $ RS_GetStateTable 0

  Src   | Time | 1PPS
  ------------------
  gps0 |   1   |   1
  hst1 |   0   |   0
  hst0 |   0   |   0
  self |   1   |   1
  epp0 |   0   |   1
  frq0 |   0   |   0
       |   0   |   0
       |   0   |   0
       |   0   |   0
       |   0   |   0
       |   0   |   0
       |   0   |   0
       |   0   |   0
       |   0   |   0
       |   0   |   0
       |   0   |   0
spadmin@Spectracom ~ $ 
```

- Refer to Tim Tetreault's "cheat sheet" at: ..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\Timing boards\TSync family\Tsync driver calls cheat sheet
- These are examples - additional calls may have since been added

REF MONITOR commands
RS_AddEntry
RS_DeleteEntry
RS_GetBestRef
RS_GetEnable
RS_GetEntry
RS_GetPriority
RS_GetStateTable
RS_GetTable
RS_SaveUserDef
RS_SetEnable
RS_SetFactDef
RS_SetPriority
RS_SetUserDef
RS_AddEntry

NTP peers command

- At command prompt, type: **ntpq –p** <enter> (or for IP addresses only , type **ntpq –pn)**



```
Linux 3.8.13-gentoo (tul) (2)

tul login: spadmin
Password:
Spectracom NetClock 9489 Version 5.1.2
spadmin@tul ~ $ ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+PCI_TSYNC(0)    .GPS.            0 l    1   16  377    0.000    0.014   0.002
oPPS(0)          .PPS.            1 l    -   16  377    0.000    0.000   0.002
*10.2.100.93     .GPS.            1 u    7    8  377    0.301   -0.037   0.009
+spectracom.int. .PPS.            1 u    6    8  377    0.273    0.002   0.008
spadmin@tul ~ $
```

Sync ("Tally Code"): a symbol that indicates if the listed reference is available for selection as a reference. The following table below indicates the symbols and their meanings.

Sync column symbols

Symbol	Indication
*	The Selected **Time** reference
O	The Selected **PPS** reference
+	A high quality candidate for NTP reference input that can be selected by NTP as its time reference (Good reference, but not selected)
X	"**Falseticker**" Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference).
-	"**Outlyer**" Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference).
(blank)	**Source discarded**: Failed Sanity check

GPS SAASM receiver API calls/ SAASM receiver key status (only for SAASM receivers)

gpsinfo:

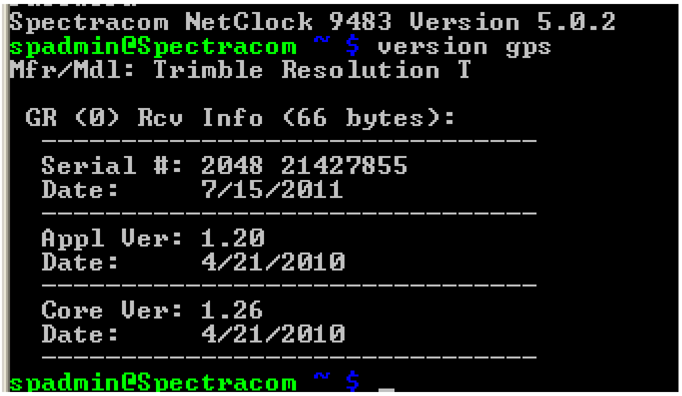
- Reports if the SAASM receiver is zeroized or keyed.
- Reports "NOT SUPPORTED" in commercial receivers

zeroize: **Used to zeroize the receiver of any loaded keys (same as using the front panel toggle switch)**

GPS reception status/troubleshooting API calls

GPS receiver firmware version

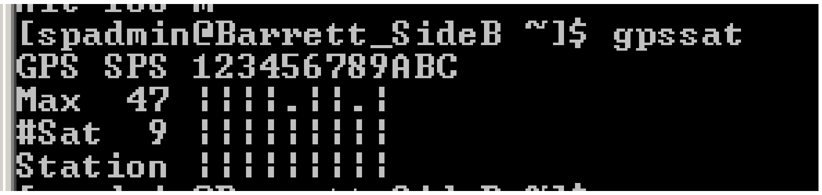
- CLI commands: **version gps** or **gpsmdl** or **GR_GetMfrMdl 0 0**



```
Spectracom NetClock 9483 Version 5.0.2
spadmin@Spectracom ~ $ version gps
Mfr/Mdl: Trimble Resolution T

 GR (0) Rcv Info (66 bytes):
  --------------------------------
  Serial #: 2048 21427855
  Date:     7/15/2011
  --------------------------------
  Appl Ver: 1.20
  Date:     4/21/2010
  --------------------------------
  Core Ver: 1.26
  Date:     4/21/2010
  --------------------------------
spadmin@Spectracom ~ $ _
```

GPS signal strengths (as displayed on the front panel and with the gpssat command)

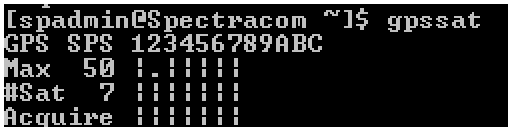
- CLI command: **gpssat** (in Standard/Stationary mode)
  - Will report "GNS" with a RES-SMT receiver installed
  - Will report "GPS" with a RES-T receiver installed



```
[spadmin@Barrett_SideB ~]$ gpssat
GPS SPS 123456789ABC
Max  47 ¦¦¦¦.¦¦.¦
#Sat  9 ¦¦¦¦¦¦¦¦¦
Station ¦¦¦¦¦¦¦¦¦
```

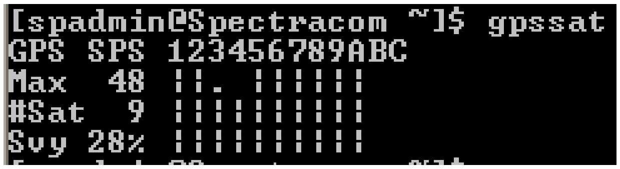
Standard/Stationary mode

- "Acquire" (not yet tracking any satellites while either in Mobile Mode, or Standard mode with survey complete)



```
[spadmin@Spectracom ~]$ gpssat
GPS SPS 123456789ABC
Max  50 ¦.¦¦¦¦¦
#Sat  7 ¦¦¦¦¦¦¦
Acquire ¦¦¦¦¦¦¦
```

- CLI command: in Standard/Stationary mode and GPS survey is in progress
- While performing GPS survey, shows how far along the survey is ("Svy")



```
[spadmin@Spectracom ~]$ gpssat
GPS SPS 123456789ABC
Max  48 ¦¦. ¦¦¦¦¦¦
#Sat  9 ¦¦¦¦¦¦¦¦¦¦
Svy 28% ¦¦¦¦¦¦¦¦¦¦
```

CLI command: in Standard/Stationary mode, GPS survey is complete, tracking at least one satellite

- When survey has been completed, and tracking 0 satellites ("Acquire")
- When survey has been completed, and tracking at least one satellite ("Station")

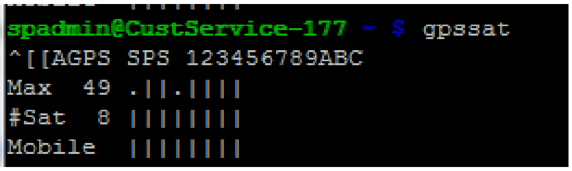
Mobile mode

- Change to gpssat command: Software version 5.0.0 changed *gpssat* command by removing the display of the dynamics code in Mobile mode.

1) Software versions 5.0.0 and above, (while tracking satellites)

- In mobile mode, “Acquire” means the receiver is either not tracking any satellites or is tracking less than four satellites.
- In mobile mode , “Mobile” being displayed means the receiver is now tracking at least four satellites

The last line of the response indicates selected GPS mode When in Mobile mode, because the Dynamics code for Mobile mode was removed in version 5.0.0 and above. So with versions 5.0.0 and above installed, the last line of response now just indicates “**Mobile**” when in Mobile mode and tracking at least four satellites.



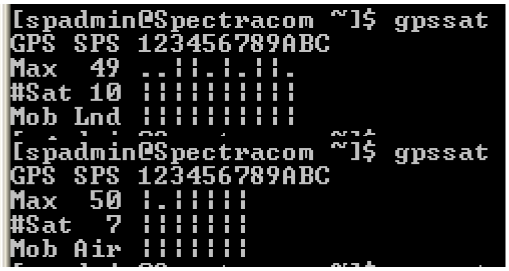
```
spadmin@CustService-177 ~ $ gpssat
^[[AGPS SPS 123456789ABC
Max  49 .||.||||
#Sat  8 ||||||||
Mobile  ||||||||
```

Software versions 4.8.9 and below only (while tracking satellites)

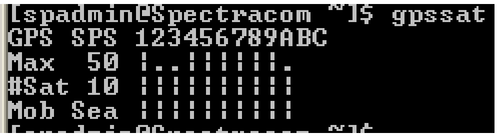
- In Mobile mode, Dynamics code “Land”, “Sea” or “Air” being reported means the receiver’s now tracking satellites.
- Reports “Acquire” instead, when not tracking any satellites

The last line of the response indicates selected GPS mode (When in Mobile mode, also reports Dynamics code” “Station” is “Stationary” “Mob Lnd” is Mobile/Land

In Mobile mode or Standard mode (and while in position Hold) will display “Acquire” while tracking 0 satellites.



```
[spadmin@Spectracom ~]$ gpssat
GPS SPS 123456789ABC
Max  49 ..¦¦.¦.¦¦.
#Sat 10 ¦¦¦¦¦¦¦¦¦¦
Mob Lnd ¦¦¦¦¦¦¦¦¦¦
[spadmin@Spectracom ~]$ gpssat
GPS SPS 123456789ABC
Max  50 ¦.¦¦¦¦¦
#Sat  7 ¦¦¦¦¦¦¦
Mob Air ¦¦¦¦¦¦¦
```



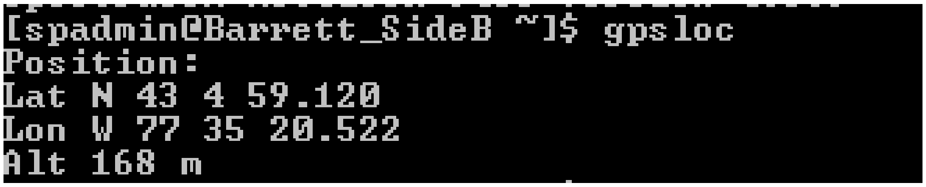
```
[spadmin@Spectracom ~]$ gpssat
GPS SPS 123456789ABC
Max  50 ¦..¦¦¦¦¦¦.
#Sat 10 ¦¦¦¦¦¦¦¦¦¦
Mob Sea ¦¦¦¦¦¦¦¦¦¦
```

Email from Dave Lorah to customer (9 July 13) The gpssat command indicates there are 9 satellites being tracked with a maximum signal strength of 47. This is a kind of a crude bar graph showing the individual signal strengths of each tracked satellite. This particular unit has good reception from one of our rooftop antennas. You should see anywhere from 5 to 9 satellites for good reception. The unit should track at least four satellites for best timing.

You can get the same information as gpssat using the front panel display. Press the green check button and then navigate to the “Display” selection. Then using the down arrow key, select “GPS INFO” and “Apply”. Use the red X key to back out to the main screen and it will show the GPS information.

GPS location (as displayed on the front panel)

CLI command: gpsloc

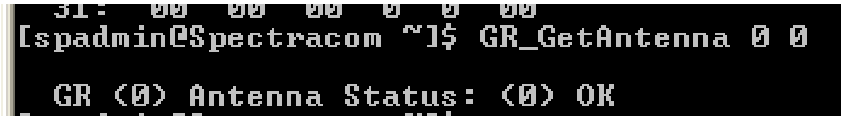


```
[spadmin@Barrett_SideB ~]$ gpsloc
Position:
Lat N 43 4 59.120
Lon W 77 35 20.522
Alt 168 m
```

GPS receiver Antenna Sense

GR_GetAntenna 0 0 <enter>

"<0> OK" indicates the GPS antenna is successfully connected to the GPS receiver (with no opens or shorts being detected in the antenna cable).

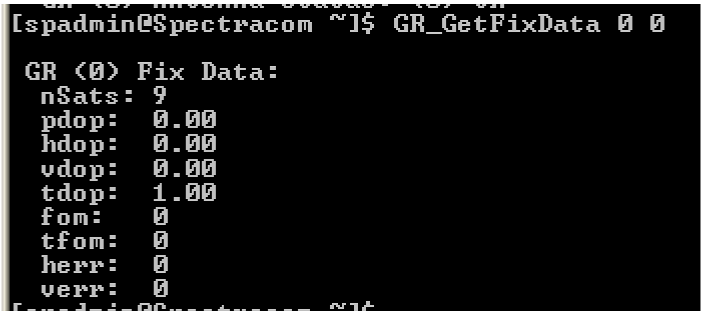


```
  31:  00  00  00  0  0  00
[spadmin@Spectracom ~]$ GR_GetAntenna 0 0

  GR (0) Antenna Status: (0) OK
```

Reported Number of satellites being tracked

GR_GetFixData 0 0 <enter>
nSats= Number of GPS satellites the GPS receiver is using to calculate its time and positional information

Note: "nSats" should normally be between 4 and 12, with typical being 6-10 satellites being tracked at all times.

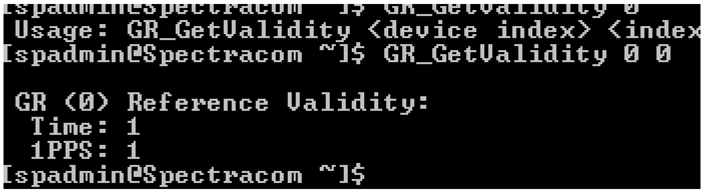


```
[spadmin@Spectracom ~]$ GR_GetFixData 0 0

 GR (0) Fix Data:
  nSats: 9
  pdop:  0.00
  hdop:  0.00
  vdop:  0.00
  tdop:  1.00
  fom:   0
  tfom:  0
  herr:  0
  verr:  0
```

GPS validity (indicates if the GPS receiver's reception is qualified):

GR_GetValidity 0 0 <enter>

- Time and 1PPS=1 indicates GPS reception is fully qualified (desired values)
- Time and 1PPS=0 indicates GPS is not qualified (GPS survey not completed yet, or receiver is not tracking at least one satellite).



```
[spadmin@Spectracom ~]$ GR_GetValidity 0
 Usage: GR_GetValidity <device index> <index
[spadmin@Spectracom ~]$ GR_GetValidity 0 0

 GR (0) Reference Validity:
  Time: 1
  1PPS: 1
[spadmin@Spectracom ~]$
```

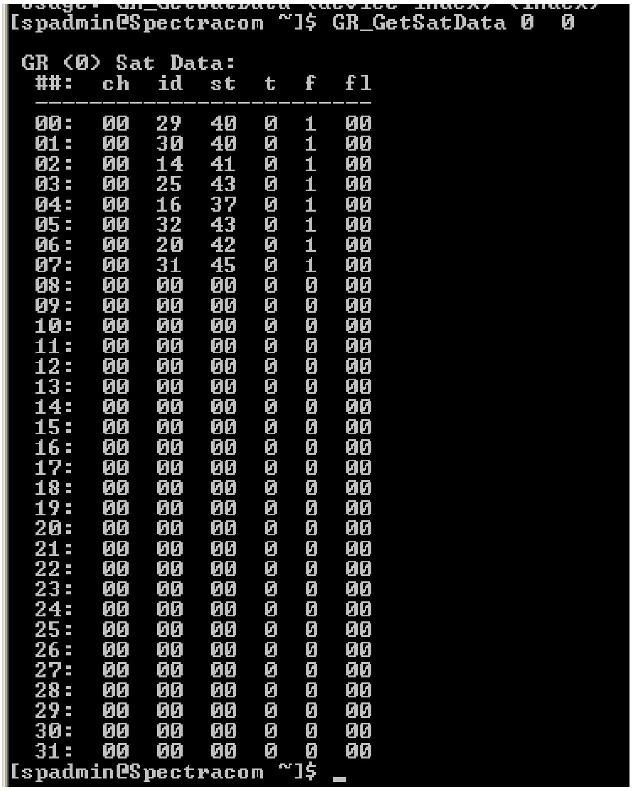
Satellites being tracked, signal strengths

GR_GetSatData 0 0 <enter>

ID= Satellite identifier each channel is assigned to track (there are 12 individual channels in the GPS receiver, so only "**ch**" values 0 through 11 are used)

ST=Signal strength of that particular satellite (not 0 when satellite being tracked. Expected values 30 to 55)

Note: Typically, between four and 12 rows of this table should have a number other than 0 in the "**st**" field.
In this example below, the GPS receiver is tracking 8 satellites.



```
Usage: GR_GetSatData <device index> <index>
[spadmin@Spectracom ~]$ GR_GetSatData 0  0

 GR (0) Sat Data:
  ##:  ch  id  st  t  f  fl
  -------------------------
  00:  00  29  40  0  1  00
  01:  00  30  40  0  1  00
  02:  00  14  41  0  1  00
  03:  00  25  43  0  1  00
  04:  00  16  37  0  1  00
  05:  00  32  43  0  1  00
  06:  00  20  42  0  1  00
  07:  00  31  45  0  1  00
  08:  00  00  00  0  0  00
  09:  00  00  00  0  0  00
  10:  00  00  00  0  0  00
  11:  00  00  00  0  0  00
  12:  00  00  00  0  0  00
  13:  00  00  00  0  0  00
  14:  00  00  00  0  0  00
  15:  00  00  00  0  0  00
  16:  00  00  00  0  0  00
  17:  00  00  00  0  0  00
  18:  00  00  00  0  0  00
  19:  00  00  00  0  0  00
  20:  00  00  00  0  0  00
  21:  00  00  00  0  0  00
  22:  00  00  00  0  0  00
  23:  00  00  00  0  0  00
  24:  00  00  00  0  0  00
  25:  00  00  00  0  0  00
  26:  00  00  00  0  0  00
  27:  00  00  00  0  0  00
  28:  00  00  00  0  0  00
  29:  00  00  00  0  0  00
  30:  00  00  00  0  0  00
  31:  00  00  00  0  0  00
[spadmin@Spectracom ~]$ _
```

Breakdown of the Satellite Data table:

ch: Receiver channel Number

Id: (aka "SVN" - Space Vehicle Number) ID Number of the satellite being tracked

Distinguishing between GPS satellites and Glonass satellites, when the Glonass Option is enabled (ID field)

To determine if each bar represents a GPS or a Glonass satellite, Mouse-hover each bar to see a report of three values (two letters, the Satellite ID number and the signal strength value for that satellite).

- **GPS satellites** are indicated with the two letters of "**GP**" and have a Satellite ID Number of **0 to 59**
- **Glonass satellites** are indicated with an:

  "**R**" (v5.3.0 and above) or

  the two letters of "**GP**" (v5.2.1 and below)

  the two letters of "**GL**" and have a Satellite ID Number of 60 and above.
- **QZSS** (Japan) satellite(s) are indicated with a "J". Note these satellites are only available insoftware versions v5.3.0 and above and if the Glonass option is enabled.
- **Beideu satellite(s)** are indicated with a " " Note these satellites are only available in softwave versions 5.4.0 or above, with a u-blox Model M8T receiver installed and Opt-GNS license enabled (Started shipping this ublox receiver ~17 March 2016 with approximate Serial Numbers 11718 and above).
- **Galileo** satellites (Europe) are identified with an "**E**"

st: signal strength of the satellite being tracked (reported in dB/Hz, as provided by the receiver).

t: TRAIM (aka "**bTraim**") Is this satellite accepted by the receiver's TRAIM algorithm? (always reported as "00" with RES-T, RES-SMT and RES-SMT-GG receivers).

f: Fix status (aka "**bInfix**") Is the receiver using this satellite in its positional fix? ("0" if not in fix, "1" if satellite is being used in fix)

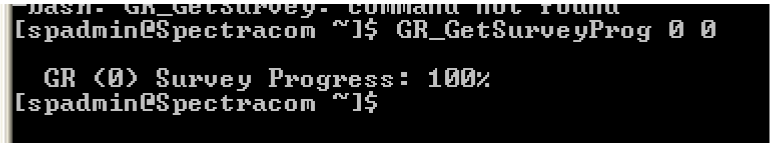
fl: Flags reported by the receiver (always reported as "00" with RES-T, RES-SMT and RES-SMT-GG receivers. Used only with SAASM receivers)

Status of the GPS survey

GR_ GetSurveyProg 0 0 <enter>

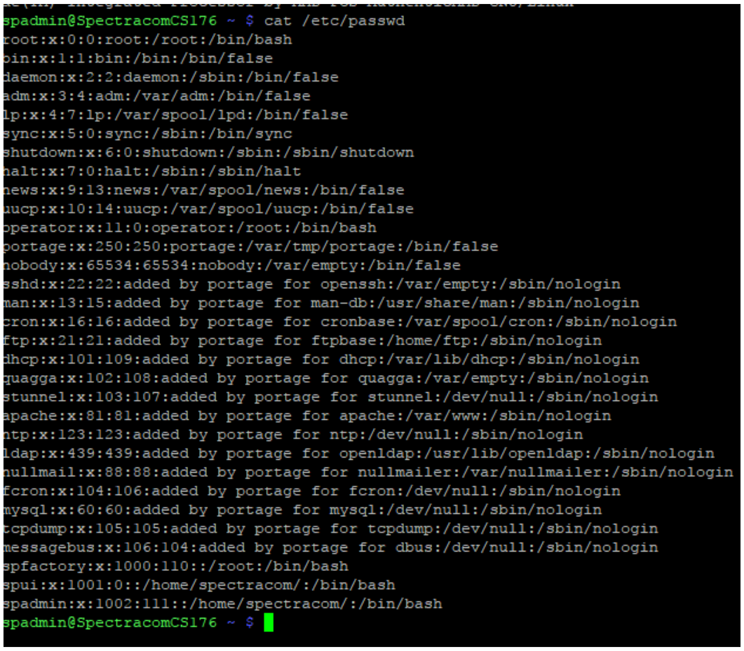
If the GPS receiver has been reset, a new GPS survey will start to be performed once the receiver is tracking at least four satellites. It takes about 34 minutes for survey to complete, once the GPS receiver is tracking (and continues to track) at least 4 satellites. The reported percent complete provides an estimate of how much longer before the survey completes and the SecureSync will then go back into sync (example 50% indicated about 17 minutes remain before SecureSync syncs to GPS again.

100% indicates the survey has completed successfully.



```
-bash: GR_GetSurvey: command not found
[spadmin@Spectracom ~]$ GR_GetSurveyProg 0 0

  GR (0) Survey Progress: 100%
[spadmin@Spectracom ~]$
```

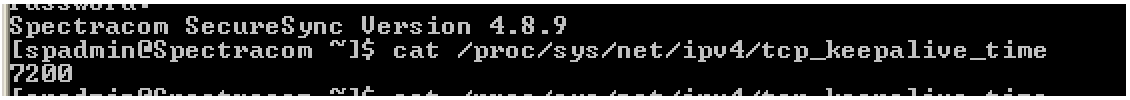
List of all user account (user account list): (cat /etc/passwd)



```
spadmin@SpectracomCS176 ~ $ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
adm:x:3:4:adm:/var/adm:/bin/false
lp:x:4:7:lp:/var/spool/lpd:/bin/false
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
news:x:9:13:news:/var/spool/news:/bin/false
uucp:x:10:14:uucp:/var/spool/uucp:/bin/false
operator:x:11:0:operator:/root:/bin/bash
portage:x:250:250:portage:/var/tmp/portage:/bin/false
nobody:x:65534:65534:nobody:/var/empty:/bin/false
sshd:x:22:22:added by portage for openssh:/var/empty:/sbin/nologin
man:x:13:15:added by portage for man-db:/usr/share/man:/sbin/nologin
cron:x:16:16:added by portage for cronbase:/var/spool/cron:/sbin/nologin
ftp:x:21:21:added by portage for ftpbase:/home/ftp:/sbin/nologin
dhcp:x:101:109:added by portage for dhcp:/var/lib/dhcp:/sbin/nologin
quagga:x:102:108:added by portage for quagga:/var/empty:/sbin/nologin
stunnel:x:103:107:added by portage for stunnel:/dev/null:/sbin/nologin
apache:x:81:81:added by portage for apache:/var/www:/sbin/nologin
ntp:x:123:123:added by portage for ntp:/dev/null:/sbin/nologin
ldap:x:439:439:added by portage for openldap:/usr/lib/openldap:/sbin/nologin
nullmail:x:88:88:added by portage for nullmailer:/var/nullmailer:/sbin/nologin
fcron:x:104:106:added by portage for fcron:/dev/null:/sbin/nologin
mysql:x:60:60:added by portage for mysql:/dev/null:/sbin/nologin
tcpdump:x:105:105:added by portage for tcpdump:/dev/null:/sbin/nologin
messagebus:x:106:104:added by portage for dbus:/dev/null:/sbin/nologin
spfactory:x:1000:110::/root:/bin/bash
spui:x:1001:0::/home/spectracom/:/bin/bash
spadmin:x:1002:111::/home/spectracom/:/bin/bash
spadmin@SpectracomCS176 ~ $
```

Network Services (FTP/Telnet/SSH/HTTP/HTTPS/Time/Daytime)

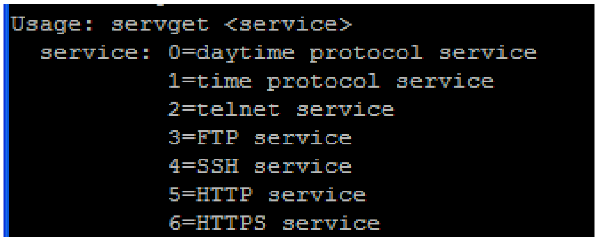
- ➢ View the current TCP connection timeout



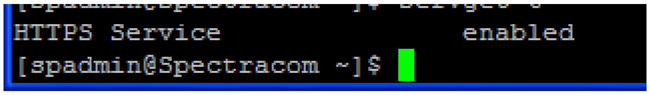
```
Spectracom SecureSync Version 4.8.9
[spadmin@Spectracom ~]$ cat /proc/sys/net/ipv4/tcp_keepalive_time
7200
```

Enable/disable Services (such as HTTPS)

- ➢ Configured in the Network/General Setup page of the browser, “Services” tab
- ➢ **servget** command displays status of all Services

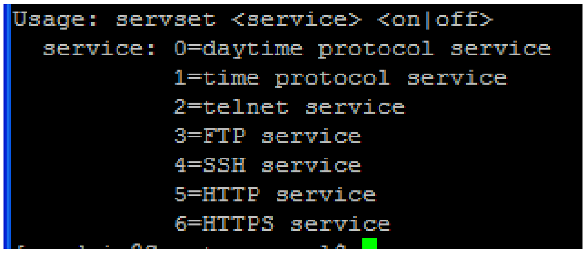


```
Usage: servget <service>
  service: 0=daytime protocol service
           1=time protocol service
           2=telnet service
           3=FTP service
           4=SSH service
           5=HTTP service
           6=HTTPS service
```

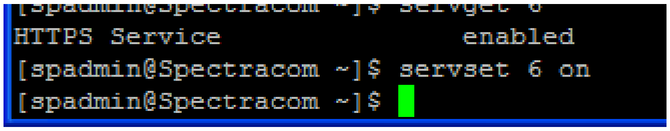


```
HTTPS Service                    enabled
[spadmin@Spectracom ~]$
```

- ➢ **servset** command displays status of all Services

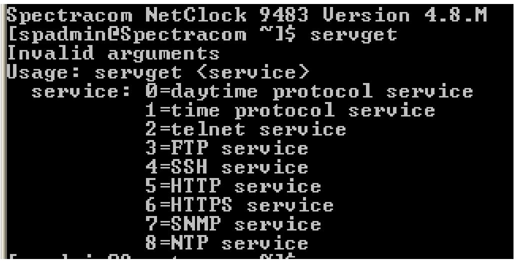


```
Usage: servset <service> <on|off>
  service: 0=daytime protocol service
           1=time protocol service
           2=telnet service
           3=FTP service
           4=SSH service
           5=HTTP service
           6=HTTPS service
```



```
HTTPS Service                    enabled
[spadmin@Spectracom ~]$ servset 6 on
[spadmin@Spectracom ~]$
```

Note: ECN 3173 (March 2013) adds NTP and SNMP to the list of Services that can be stopped/started or running status viewed using these two CLI commands.

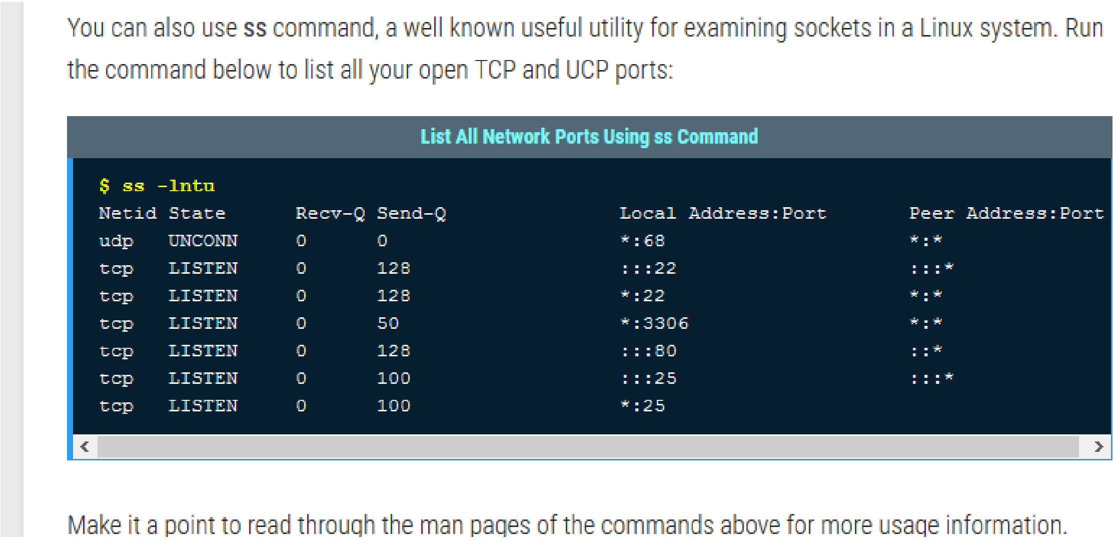


```
Spectracom NetClock 9483 Version 4.8.M
[spadmin@Spectracom ~]$ servget
Invalid arguments
Usage: servget <service>
  service: 0=daytime protocol service
           1=time protocol service
           2=telnet service
           3=FTP service
           4=SSH service
           5=HTTP service
           6=HTTPS service
           7=SNMP service
           8=NTP service
```

Enable/Disable HTTPS

The CLI “Serial” port on the front of the SecureSync has an available command for verifying if HTTPS was somehow disabled and also provides the ability to re-enable any service that has been disabled. All of the available CLI commands are listed in Section 11 of the SecureSync manual (pages 11-1 through 11-3).

After connecting a straight-thru serial cable between this port and a PC running HyperTerminal, login to this port using the spadmin account and the same password used to login to the browser.   Once logged in, type ***services*** <enter>. This command lists the services and whether or not each service is enabled. In addition to this command, **servget** <enter> can display each service one at a time and **servset** <enter> is used to re-enable or disable a particular service.



You can also use **ss** command, a well known useful utility for examining sockets in a Linux system. Run the command below to list all your open TCP and UCP ports:

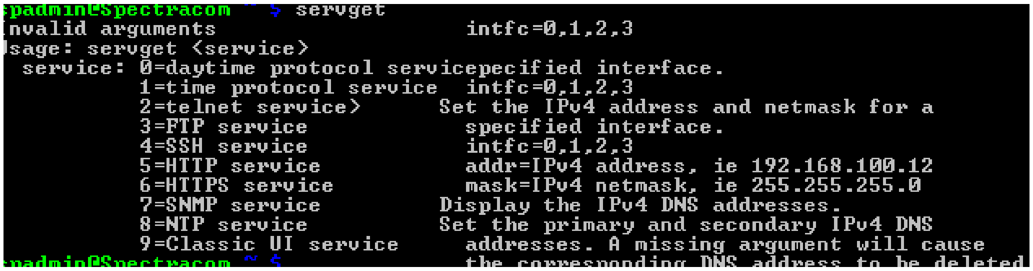
List All Network Ports Using ss Command

```
$ ss -lntu
Netid State      Recv-Q Send-Q                Local Address:Port          Peer Address:Port
udp   UNCONN     0      0                     *:68                        *:*
tcp   LISTEN     0      128                   :::22                       :::*
tcp   LISTEN     0      128                   *:22                        *:*
tcp   LISTEN     0      50                    *:3306                      *:*
tcp   LISTEN     0      128                   :::80                       ::*
tcp   LISTEN     0      100                   :::25                       :::*
tcp   LISTEN     0      100                   *:25
```

Make it a point to read through the man pages of the commands above for more usage information.

Enable/disable the Classic interface browser via CLI (v5.5.0 and above)

- **servget** command displays status of all Services
- **servset 9 on** command enables the classic interface
- this variant of the servget/servset commands was added in version 5.5.0 update



```
spadmin@Spectracom ~ $ servget
Invalid arguments                          intfc=0,1,2,3
Usage: servget <service>
  service: 0=daytime protocol servicepecified interface.
           1=time protocol service   intfc=0,1,2,3
           2=telnet service>       Set the IPv4 address and netmask for a
           3=FTP service             specified interface.
           4=SSH service             intfc=0,1,2,3
           5=HTTP service            addr=IPv4 address, ie 192.168.100.12
           6=HTTPS service           mask=IPv4 netmask, ie 255.255.255.0
           7=SNMP service          Display the IPv4 DNS addresses.
           8=NTP service           Set the primary and secondary IPv4 DNS
           9=Classic UI service      addresses. A missing argument will cause
spadmin@Spectracom ~ $               the corresponding DNS address to be deleted
```

Services

SSH (OpenSSH)

- Refer to the Model 2400 online user guide at: https://orolia.com/manuals/2400/Content/NC_and_SS/Com/Topics/SETUP/SSH_Configuration.htm
- Also refer to: "**SSH (for all products)" in ..\CustomerServiceAssistance.pdf

Network ports used

- **Telnet**: uses TCP **port 23**
- **SSH**: uses TCP **port 22**

SSH login password

SSH effects on 1204-49/1204-4A Option Card GB ports, when PTP has been enabled on that interface

- spadmin/spfactory account passwords won't allow SSH login to 1204-49/1204-4A Option Card interfaces, if PTP has been enabled on that interface.
- Refer to Salesforce Case 272881

Per Ryan Johnson (8 Sept 2021) This unit came into service and I took a look at it. And… there doesn't seem to be anything wrong with it. I was able to log into the unit fine with both spadmin/spfactory. But I have a hunch what happened. If they had been attempting to log into the device via the **IP address of one of the 1204-49 (PTP) ports** they would see the problem they did. When trying to connect to the 49/4A cards via ssh it will let the user attempt to connect, but the credentials are completely different from the standard console interface and so spadmin/spfactory/etc will not work.

I did make a ticket (**O4-118**) to disable the ssh service on these cards since 1) it's confusing and 2) a (minor) security risk.

limit of failed login attempts/retries for telnet/ssh

- Refer to (in this same document): Limit number of web browser/ssh login attempts/re-tries (entering incorrect password several times in a row)

SSH hostkeys supported (RSA or DSA)

C) RSA, DSA

D) ED25519 (versions 1.4.1 and above only)

- **Per Update version 1.4.1 (April 2022) release notes:** "Added support for the ED25519 host key algorithm for SSH"

SSH (openSSH) software version installed

- Via CLI command **version ssh** <enter>
- Via newer web browser: **Tools**-> **Upgrade/Backup** page (starting in update version 5.2.0)
- Via the SecureSync software version installed

- Refer to the “Software Release Date” spreadsheet at : I:\Customer Service\PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates

libssh

- We do not instal/use this package in SecureSyncs/VersaSync or VelaSyncs.
  - per Ron Dries, 24 Oct 2018 ”I have asked engineering and they have confirmed that we use openssh and not libssh in SecureSync, VersaSync, and VelaSync”

SSH protocol versions supported (such as v1, v2, v3, etc)

- As of at least March 2018, the supported versions of SSH are not in data sheet or online user guide
- Per Dave Sohn/Ron Dries (29 Mar 2018, for at least to version 5.8.0)
  - We support **SSH v2** (SSH version 2) only
  - We **do not support SSHv1** (SSH version 1). It is considered “unsafe”
  - we **do not yet support SSHv3** (SSH version 3)

Q I am currently doing network hardening of a Spectracom SecureSync 12xx NTP server to DoD standards. The listed specifications list SSH support but can you please confirm for us the SSH version? Does it support SSHv1 or SSHv2? I'm hoping it defaults to SSHv2 and that SSHv1 is not even available on your NTPs, as DoD considers SSHv1 as unsafe.

A reply from Keith (29 Mar KW) Thanks very much for your email and (Great) question about the Spectracom SecureSync. I just confirmed with one of our Applications Engineers and the SecureSync Product Manager (fortunately, they were standing next to each other) that the SecureSync ONLY supports SSH v2. It does not support SSH v1 at all (we consider it unsafe, as well! I believe this was the answer you were hoping to hear 😊!!

Much earlier question/answer (long before March 2018)

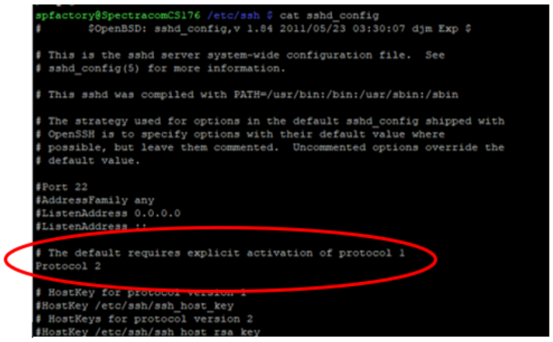
Q. What is the version of the current SSH that it can support (1, 2 or both)?

A. The SecureSync only supports SSH version 2. It does not respond to SSH version 1 (I just confirmed this by trying to connect using “V1 only”).

SSH version enabling in the sshd_config file

(note per Keith- I believe this is correct but confirm with Eng/Apps eng)

```
cd /etc/ssh

cat sshd_config
```



```
spfactory@SpectracomCS176 /etc/ssh $ cat sshd_config
#       $OpenBSD: sshd_config,v 1.84 2011/05/23 03:30:07 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

# The default requires explicit activation of protocol 1
Protocol 2

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
```

Version 1.99 (sshv1) detected in v5.8.0 Nessus scan

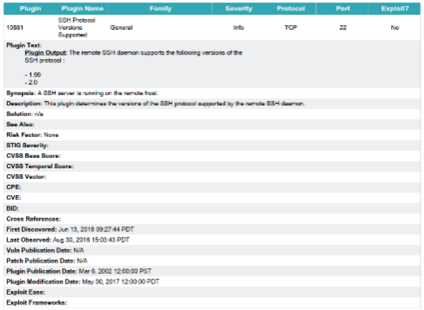
reported by the customer, this "false alert (since v1 is not enabled) can happen in SSH versions prior to 7.6 (version 5.8.1 has SSH version 7.5p1 implemented)

I think 1.99 is an indication of backwords compatibility (i.e. support for SSH v1 & 2), so another way to ask is: Is SSH version 1 allowed? If so, can we disable it so that only SSH v2 is allowed.

Followed by…

"Looking closer, I'm thinking when you implement SSH >7.6, the SSH 1.99 issue will go away.

Here is a screen grab of our Nessus scan:



Plugin	Plugin Name	Family	Severity	Protocol	Port	Exploit?
10881	SSH Protocol Versions Supported	General	Info	TCP	22	No

Plugin Text:
Plugin Output: The remote SSH daemon supports the following versions of the SSH protocol :

- 1.99
- 2.0

Synopsis: A SSH server is running on the remote host.

Description: This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution: n/a

See Also:

Risk Factor: None

STIG Severity:

CVSS Base Score:

CVSS Temporal Score:

CVSS Vector:

CPE:

CVE:

BID:

Cross References:

First Discovered: Jun 13, 2018 09:27:44 PDT

Last Observed: Aug 30, 2018 15:03:43 PDT

Vuln Publication Date: N/A

Patch Publication Date: N/A

Plugin Publication Date: Mar 6, 2002 12:00:00 PST

Plugin Modification Date: May 30, 2017 12:00:00 PDT

Exploit Ease:

Exploit Frameworks:

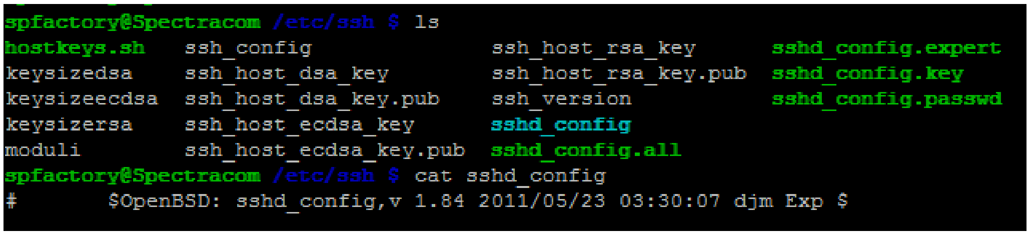
****View the openssh config file (sshd_config)

- ➢ Customers have permission to view this file via the spadmin account

SSH specs/SSH configs (in the background- not available to customers)

SSHd configuration files/SSHd Expert mode

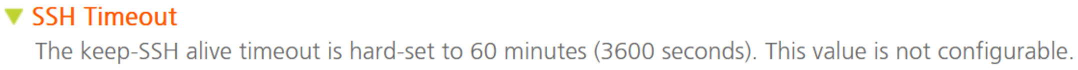
- ➢ There are three separate sshd config files:
  - **sshd_config**: The standard configuration file for ssh
  - **sshd_config.all:** Spectracom-created file that Paul created back in the 9100s to allow the browser to easily update the sshd_config with the user change to select login with keys and/or password. Note that the **sshd_config.all** and **sshd_config files** may not be exactly the same, but should be functionally the same
  - **sshd_config.expert:** not currently used. Added in case we ever add an expert mode in future (we may just remove this file in the future to alleviate confusion).
- ➢ These three similar sshd config files are all located in the **/etc/ssh** directory



```
spfactory@Spectracom /etc/ssh $ ls
hostkeys.sh    ssh_config              ssh_host_rsa_key      sshd_config.expert
keysizedsa     ssh_host_dsa_key        ssh_host_rsa_key.pub  sshd_config.key
keysizeecdsa   ssh_host_dsa_key.pub    ssh_version           sshd_config.passwd
keysizersa     ssh_host_ecdsa_key      sshd_config
moduli         ssh_host_ecdsa_key.pub  sshd_config.all
spfactory@Spectracom /etc/ssh $ cat sshd_config
#       $OpenBSD: sshd_config,v 1.84 2011/05/23 03:30:07 djm Exp $
```

2400 SecureSync SSH timeout for login (ssh idle timeout, “keepalive”, inactivity timeout)

- ➢ refer to online 2400 SecureSync user guide: https://safran-navigation-timing.com/manuals/2400/Content/NC_and_SS/Com/Topics/SETUP/SSH_Configuration.htm
  - scroll down and select “**SSH Timeout**” (screenshot below is for at least v1.7.0 and below)



▼ SSH Timeout

The keep-SSH alive timeout is hard-set to 60 minutes (3600 seconds). This value is not configurable.

(below info copy/pasted from 1200 SecureSyncs)

“The SSH configuration is fairly standard.” Default values we change:

- ➢ **LoginGraceTime 30s**: The login grace period is 30 seconds (you have 30 seconds to enter password after being prompted
- ➢ **MaxAuthTries 4:** The number of password attempts is 4. (max of four failed password attempts)
- ➢ **MaxStartups 3 (“3:30:10”):** Specifies the maximum number of concurrent unauthenticated connections to the sshd daemon. Additional connections will be dropped until authentication succeeded, or the **LoginGraceTime** expires for a connection (The default is 10.   We change this value to 3)

Defaults values we don’t currently change

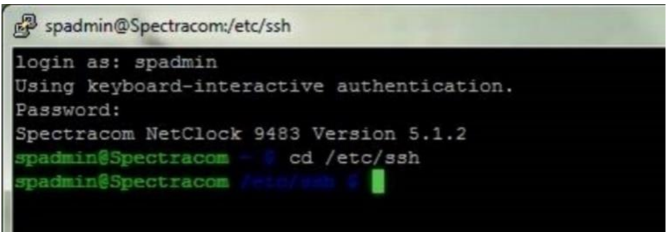
- ➢ **Rate limiting**: SSH limits successful connection to 5 in 60 seconds.

  Note (3/9/12) US Army has requested this value be increased in a future update. We will likely increase this value in a future release.

  Update to this (8/31/12): The pending version 4.8.7 release addresses this.
  FYI- Regarding the desire to view the SecureSync's ssh_config and sshd_configs, these can be viewed from the SecureSync via a DB9 Serial or CLI connection.

To view these configs, either connect to the SecureSync's front panel Serial port using a DB9M to DB9F serial cable pinned straight-thru, or via a CLI connection (via either telnet or SSH).   The login credentials for the CLI interfaces is the same as the web browser. Attached is a document that discusses how to use HyperTerminal (or other terminal emulator program) to communicate with the front panel Serial port.

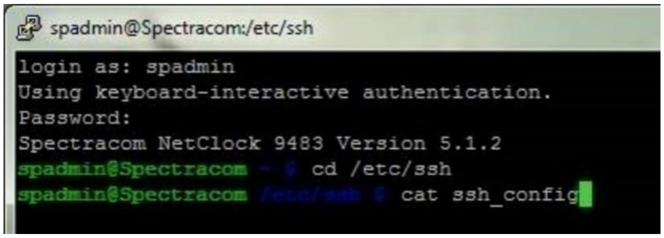
Then, change to the /etc/ssh file.   Then you can "cat" the **sshd_config** file. Refer to the screenshots below for an example:



spadmin@Spectracom:/etc/ssh

```
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 5.1.2
spadmin@Spectracom ~ $ cd /etc/ssh
spadmin@Spectracom /etc/ssh $
```

`



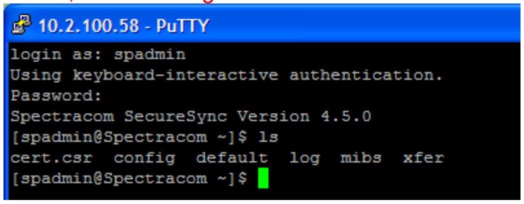
```
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 5.1.2
spadmin@Spectracom ~ $ cd /etc/ssh
spadmin@Spectracom /etc/ssh $ cat ssh_config
```

Hi Richard,
Good morning. I hope you had a great weekend!

Regarding SecureSync SSH, this is not a normal means to monitor the operation of the SecureSync. SSH (Secure telnet) provides the ability to offload/upload the SecureSync's security certificates (such as the HTTPS certificate), configuration files, the unit's log files and the SNMP MIB files.   It provides the same limited functionality as telnet. But with SSH, the login password is encrypted, unlike telnet which sends the password in the clear.

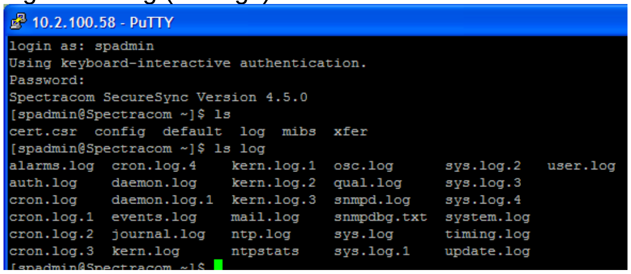
If you don't already have an SSH client on your PC, we typically use the PuTTY SSH client software for Windows (I believe this is still a freeware program). SSH uses network packets to communicate with the SecureSync.

As shown below, the following items are available via SSH:



```
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom SecureSync Version 4.5.0
[spadmin@Spectracom ~]$ ls
cert.csr  config  default  log  mibs  xfer
[spadmin@Spectracom ~]$
```

Performing an LS log (list logs) command results in:



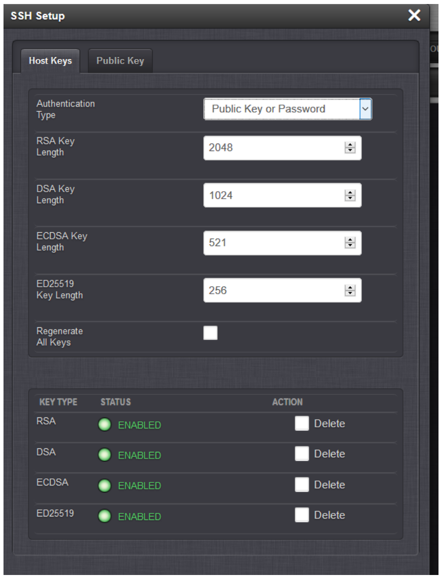
```
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom SecureSync Version 4.5.0
[spadmin@Spectracom ~]$ ls
cert.csr  config  default  log  mibs  xfer
[spadmin@Spectracom ~]$ ls log
alarms.log  cron.log.4    kern.log.1  osc.log      sys.log.2   user.log
auth.log    daemon.log    kern.log.2  qual.log     sys.log.3
cron.log    daemon.log.1  kern.log.3  snmpd.log    sys.log.4
cron.log.1  events.log    mail.log    snmpdbg.txt  system.log
cron.log.2  journal.log   ntp.log     sys.log      timing.log
cron.log.3  kern.log      ntpstats    sys.log.1    update.log
[spadmin@Spectracom ~]$
```

SSH configurations available to users

A) SSH configuration via the newer (black/charcoal) interface browser.

refer to online SecureSync user guide:
http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/SSH_Configuration.htm

- Configured in the **Management** -> **SSH Setup** page of the browser, **Host Keys** tab



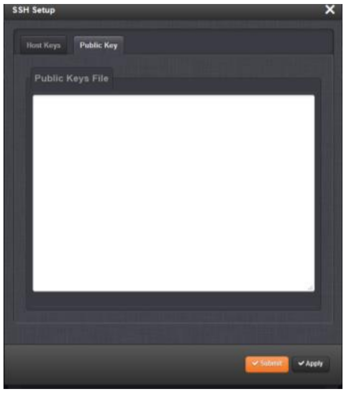
Authentication Type	Public Key or Password
RSA Key Length	2048
DSA Key Length	1024
ECDSA Key Length	521
ED25519 Key Length	256
Regenerate All Keys	□

KEY TYPE	STATUS	ACTION
RSA	● ENABLED	□ Delete
DSA	● ENABLED	□ Delete
ECDSA	● ENABLED	□ Delete
ED25519	● ENABLED	□ Delete

- Can login using Public Key Only, Password only, or either Public Key or Password
- When using password to connect via SSH. Account and password is either the spadmin account/password or a user account that has been created.

Note: User accounts that are created with user rights can still connect to SSH (does not have to be assigned to the admin group)

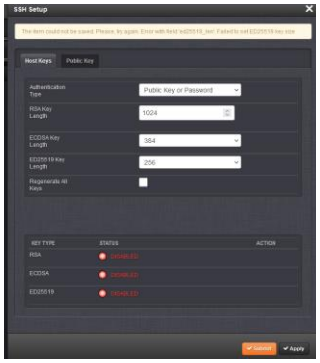
“**Public Key Tab**: Paste the public key from each computer that wishes to access the NTP server via SSH into this field (if there are four computers, paste four keys into the table and then change “View or Edit” to Enabled. Press Submit). Each key goes into a new line in this field).



Note: Private keys remain on the computers.

Issues associated with the ‘ED25519’ key type

1. ED25519 key type drop-down is limited to just “256” bit (unlike the other key types)
2. Error message displayed at top of page when trying to regenerate the keys:



The item could not be saved. Please, try again. Error with field 'ed25519_len': Failed to set ED25519 key size

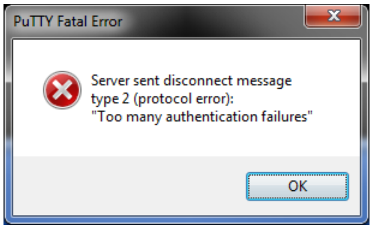
Authentication Type	Public Key or Password
RSA Key Length	1024
ECDSA Key Length	384
ED25519 Key Length	256
Regenerate All Keys	□

KEY TYPE	STATUS	ACTION
RSA	● DISABLED	
ECDSA	● DISABLED	
ED25519	● DISABLED	

- Refer to Salesforce Case 278362/JIRA ticket DMND-1728 (Jan 2022)
- Associated with at least version 1.4.0, beta 3.

Limit number of login Telnet/SSH re-tries (entering incorrect password several times in a row)

In summary, 3 “retries” are allowed, before a 60 second timeout period has to occur, before a successful login can occur. The following message will be displayed after the third failed login attempt (“**server sent disconnect message type 2 (protocol error): Too many authentication failures”**)



Server sent disconnect message type 2 (protocol error): "Too many authentication failures"

Note: web browser login re-tries is not the same. Refer to the web browser section of this document for more info.

Example of a similar error message response

```
$ ssh spadmin@sv02pdmi33
Password:
Received disconnect from UNKNOWN: 2: Too many authentication failures
```

Reply from Dave Lorah (12 May 16) I believe this is a factor of too many wrong password entries when trying to connect via SSH. I get the same error if I enter the password wrong three times in a row using Putty. Try closing the SSH viewer and reopen it.

Telnet socket issues/Bash Shell (Reported by Walt Washington, 22 Aug 2013

Q We are not using ssh. Our software works through this same Telnet protocol on another GPS so I know the code works. I believe the problem is the fact that your GPS runs the bash shell. We are not using a command line interface so the shell script doesn't have anywhere to run. We are simply creating a socket and connecting it through Telnet and sending ASCII characters. The connection is successful and we can see that in the GPS logs. We do not receive prompts on the Telnet connection after the connection is made like we do when we are in the command line.
Bash scripts do not return values according to my research and it is my belief that the shell is causing a disconnect since it doesn't have anywhere to run.

Second email from Walt

The program we are using is a simple socket program written in ADA. This program was written solely for testing communication with the GPS, because once we get this working will be able to integrate it into our software product.

The socket is setup as a client and connects to the GPS server socket on port 23. There is no command line interface using this method. We have the Username and Password in separate commands. We start by connecting the socket. We then manually click the Username button to send the username. We then manually click the Password button to send the password. Then we click the Send command to attempt to get time. At any point in this process we have a receive button that we can click to see what information has been received from the GPS. When we click Connect and then receive we get some jibberish instead of a prompt for the Username. Then if we attempt to send the Username or password or the time command and then hit receive, we do not receive any information at all.

When we connect to the server, we expect to receive a prompt from the GPS for a Username. We do not receive this prompt, we only receive jibberish. We know that the program is correctly connecting to the server because the GPS logs show that the session was started and a connection was made. After that point, no matter what commands we send to the GPS, we do not get any login failures or successes.   The GPS simply does not acknowledge anything we send it. Nothing changes in the logs except when we close the program it shows the session ending. We know the information is being successfully sent, because the program has error checking built in. If it tries to send the information and it does not get sent, we would get a send error.

The software version we are running is 4.8.7.

Also, using the same software, if I change the port to the FTP port (port 21) or the SSH port (port 22) we receive a welcome message from the GPS. We do not get jibberish like we do on the telnet line.

We would prefer to not use SSH or any third party software to be able to connect to the GPS.

The other GPS that we can successfully use this software with does not use the Linux Shell commands. When a telnet session is opened only simple communication back and forth occurs.

Last email from Walt

The "gibberish" that is coming from the SecureSync is connection codes from the telnet server running on that port. It requires some response codes from their client in order to proceed further with the connection to get the username/password prompt. The links below are a discussion on a telnet vs raw socket connection, and a resource on the telnet commands/options. From a high level, the telnet server is asking the client, or socket connection in this case, to do certain things. If the client says it won't do that, it will still continue to make the connection.
http://archive.iprodeveloper.com/forums/aft/52910
http://www.networksorcery.com/enp/protocol/telnet.htm

I've attached a python script I wrote as an example showing a "WON'T" response to all of the "DO" commands, logging in, and running the HW_GetTime command. Below is the output from the SecureSync from running the python script. The \xff\xfd\x18 is an example of a "DO" command. The script would send back \xff\xfc\x18 as the "WON'T" response.

Python script output:

```
"\xff\xfd\x18\xff\xfd \xff\xfd#\xff\xfd'"
'\xff\xfb\x03\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x05\xff\xfd!'
'\xff\xfb\x01\r\nLinux 3.8.13-gentoo (Spectracom) (1)\r\n\r\n'
'Spectracom login: '
'spadmin\r\nPassword: '
'\r\nSpectracom SecureSync Version 5.0.0\r\nspadmin@Spectracom ~ $ '
HW_GetTime 0

DOY Time:
  Year: 2013
  DOY:  235
  Hr:   18
  Min:  19
  Sec:  47
  Nsec: 423202970
  Sync: TRUE
spadmin@Spectracom ~ $
```

Troubleshooting telnet/SSH issues

1) SSH doesn't appear to be running, even though it's enabled

- SSH daemon is not always running. It only starts running if it has detected a connection attempt is being made. Otherwise, it's not running. It can only be detected when it's actually running.

Q. sshd on one of ntp appliance is not up, reboot does not fix it.
A (email from Keith, with input from Paul Myers, 8 Nov 2012) lo note, SSH cannot be detected unless it's actually running. And SSH is not a continuously running daemon. It doesn't continue to run, while waiting for a SSH connection to start. SSH is only started if it detects a connection attempt is in process.   If you don't see SSH running, it's because SecureSync has not detected an attempt to login is now occurring.   If you are trying to SSH into a SecureSync, but it's failing to connect (not even getting a login prompt), there may be a firewall blocking the SSH port, for instance. You may need to perform a wireshark packet sniff to see where the SSH packets are being lost.

Email from Keith (9 Feb 16) When you try connecting via ssh, does it display any error messages (such as "connection **refused**" for example)? Do you get to the login prompt but it's not taking your credentials to get past login? Or does it stop after logging in?

There are no known issues associated with SSH in version 5.2.1. With the unit still being accessible via its browser, as long as SSH is still enabled and as long as no entries have been added to the Network Access Restriction table, there shouldn’t be any reason with the server itself that the ssh wouldn’t be working in the SecureSync. External to the SecureSync, make sure that TCP port 22 is open on any firewalls in between and on your PC.

To verify SSH is still enabled in the server, login to the SecureSync’s browser and then, navigate to the **Management -> Network** page of the browser. In the lower-left corner, make sure the “SSH” slider switch is set to “ON” (with a green fill), If it’s still enabled, I suspect there is a firewall on your PC or between the SecureSync and your PC which is now blocking port 22.

Let me know what you find and then we can go from there!!

2) “Network error: Connection refused” displayed

Possible causes/suggestions

1. SSH/telnet is disabled in the list of Services (Newer browser: Management -> Network page, bottom left-corner)
2. Make sure TCP port 22 is open for SSH (or TCP port 23 for Telnet) on ay firewalls

3) “Access denied” reported

Possible causes:

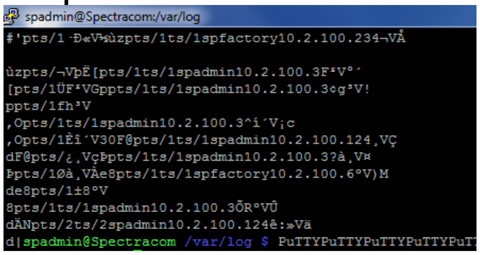
- Invalid password entered (local, LDAP or Radius/Tacacs account with versions 5.6.0 or above installed)
- Invalid account name entered (local, LDAP or Radius/Tacacs account with versions 5.6.0 or above installed)
- Network Access Restriction table has at least one entry in it and this computer is not allowed to connect to telnet or ssh.

The /var/log/wtmp.log filemay be full

- Refer also to wtmp.log in this doc
- Refer to Salesforce case 21031 (for Jane Street)
  - Initially reported that the browser and SSH had stopped working in 5.2.1. He responded back with: “It appears we've had the same issue before and wtmp is full.”
- The newer version of the cleaner patch (~Dec 2015) cleans out this file. Perform the cleaner to reduce this file size (I don’t believe a reboot will clean out this file).

What is the wtmp file refer to (http://linux.die.net/man/5/wtmp)
“The *wtmp* file records all logins and logouts. Its format is exactly like *utmp* except that a null username indicates a logout on the associated terminal”

Example from our server



```
#'pts/1 ·Ð«V¾ùzpts/1ts/1spfactory10.2.100.234¬VÅ

ùzpts/¬VþË[pts/1ts/1spadmin10.2.100.3F²V°´
[pts/1ÜF²VGppts/1ts/1spadmin10.2.100.3¢g³V!
ppts/1fh³V
,Opts/1ts/1spadmin10.2.100.3^í´V¡c
,Opts/1Èî´V30F@pts/1ts/1spadmin10.2.100.124¸VÇ
dF@pts/¿¸VçÞpts/1ts/1spadmin10.2.100.3?à¸V¤
Þpts/1Øà¸VÀe8pts/1ts/1spfactory10.2.100.6°V)M
de8pts/1±8°V
8pts/1ts/1spadmin10.2.100.3ÕR°VÛ
dÄNpts/2ts/2spadmin10.2.100.124ê:»Vä
d|spadmin@Spectracom /var/log $ PuTTYPuTTYPuTTYPuTTYPuT
```

4) no matching key exchange method found” displayed in the SSH program OR “Could not load host key” log entries in time server

no matching key exchange method found

```
$mparvath009383:~ mparvath$ ssh spadmin@kynudcsts001
ssh_dispatch_run_fatal: Connection to 10.65.224.170: no matching key exchange method found
mparvath009383:~ mparvath
```

Report from customer “There are these messages in the auth.log”

```
Jan 27 00:16:57 nt01pdmi107 sshd[7256]: error: Could not load host key: /etc/ssh/ssh_host_ed25519_key
Jan 27 00:16:57 nt01pdmi107 sshd[7256]: Did not receive identification string from 144.14.193.108
Jan 27 00:16:57 nt01pdmi107 xinetd[2927]: EXIT: ssh pid=7256 duration=41(sec)
```

Email from Dave L (15 Feb 27) What we believe is happening is you are using an older or NEWER SSH version and there is key negotiation issues where it tries key different types and it is timing out before getting a connection.

We updated OpenSSH in nearly every past version and there was usually an issue with the supported key types.

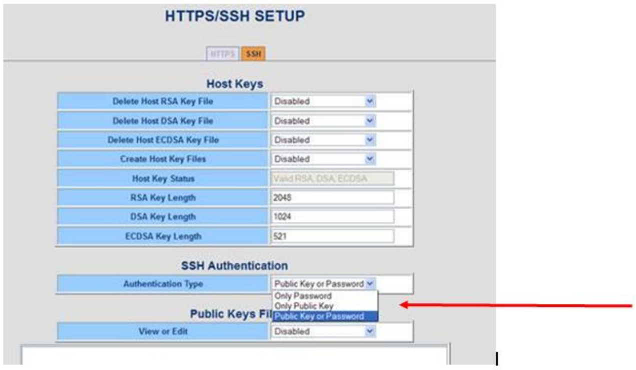
I would recommend you evaluate which version of SSH you and the Securesync are using, and pick a compatible key type on each side that works. Updating the firmware to current version 5.5.1 should also resolve the problem.

Keith sent to Danny Loke (16 May 13) Please note that there were no changes to either Radius or SSH (that I’m aware of anyways- I’m double-checking with our Engineers just to be sure) in either the versions 4.8.8 or 4.8.9 software updates.

SSH with Radius login hasn’t been available in any version of the SecureSync software. Radius login has always been limited to strictly the web browser (HTTP/HTTPS) login. So your customer wouldn’t have been able to login to SSH using the Radius password even before updating the software beyond 4.8.7.

First, SSH has to be enabled in SecureSync in order to be able to use it. Have your customer navigate to the **Network** -> **General Setup** page of the browser and click on the “**Services**” tab. Make sure SSH Service is set to “**Enabled**”. If it’s set to “Disabled, enable it and press Submit.

SSH has specific configurations for login (As configured in the **Network** -> **HTTPS/SSH Setup** page of the browser, **SSH** tab). The “**SSH Authentication**” field determines if the SSH connection requires no login password- just the correct public key, only a password with no public key, or if it needs either one in order to connect (as shown below):



HTTPS/SSH SETUP

Host Keys

Delete Host RSA Key File	Disabled
Delete Host DSA Key File	Disabled
Delete Host ECDSA Key File	Disabled
Create Host Key Files	Disabled
Host Key Status	Valid RSA, DSA, ECDSA
RSA Key Length	2048
DSA Key Length	1024
ECDSA Key Length	521

SSH Authentication

Authentication Type	Public Key or Password

Public Keys Fil

View or Edit	Disabled

Have your customer verify the current settings in this page of the SecureSync. At least for test purposes, temporarily set it to “Only Password” so that it can only connect with the proper password. This can be changed later, as desired.

With version 4.8.8 software installed in a SecureSync, I just created two local login accounts, one with user rights and one with admin rights. I was then able to connect to SSH using both of these two accounts with no problems (the rights don’t restrict the ability to connect to SSH). If your customer still can’t login to SSH with any User accounts, please have them verify that Port 22 is open on any firewalls on the PC or in between the PC and the NTP server.

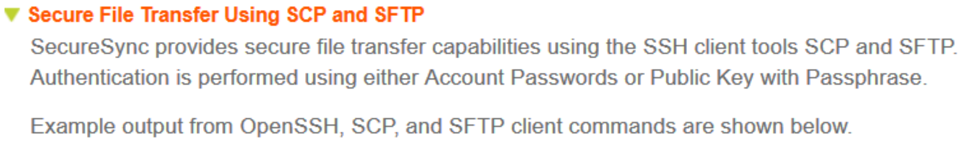
Please let me know what they find was preventing the SSH connection, so that I know they are all set- Thanks

FTP and SFTP/SCP (Secure Copy Program)

A) FTP (File Transfer Program)

B) SFTP/SCP (SecureSync Copy Program)

- Refer to online SecureSync user guide: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/SSH_Configuration.htm
  - Select "File Transfer Using SCP and SFTP"



▼ Secure File Transfer Using SCP and SFTP

SecureSync provides secure file transfer capabilities using the SSH client tools SCP and SFTP. Authentication is performed using either Account Passwords or Public Key with Passphrase.

Example output from OpenSSH, SCP, and SFTP client commands are shown below.

SFTP/SCP (Secure Copy Program) is a secure means of copying files from one system to another, using the underlying Secure Shell.

**tcpforwarding (TCP forwarding)

- tcpforwarding is disabled in all software versions

Email from Paul Myers (15 Jan 2014)

The SSHD Configuration files have "AllowTcpForwarding no" by default. I think this has been this configuration for some time. It is either the default or I turned it off since the NetClock 93xx. NetClock 93xx has it turned off as well.

User Rights/Permissions

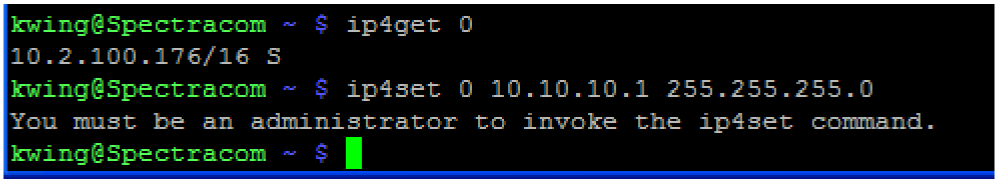
- Permissions / rights are determined by the Group (user or admin) setting of the local account created in the SecureSync.

"user" group limitations include:

- Being able to read but not change network settings.
- Being able to read but not change the state of Services (such as telnet,ftp ssh)

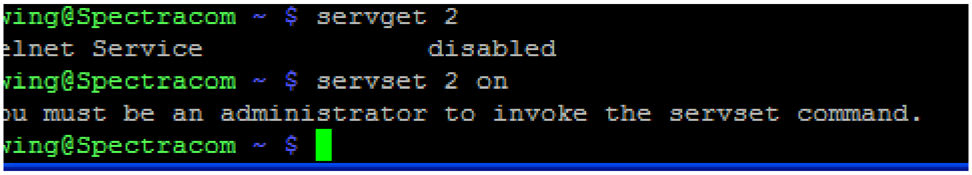
If a "user" is logged in with ssh/telnet and they try to perform an admin-only task, "**you must be an administrator to invoke the xxxxx command"** is displayed.

Below, I can view whether or not DHCP is enabled on Eth2, but I cannot change it (because I am a user group member):
Below, I can view the current static IP address of Eth0. but I cannot change it (because I am a user Group member):



```
kwing@Spectracom ~ $ ip4get 0
10.2.100.176/16 S
kwing@Spectracom ~ $ ip4set 0 10.10.10.1 255.255.255.0
You must be an administrator to invoke the ip4set command.
kwing@Spectracom ~ $
```

I also mentioned that users cannot change the state of services (such as telnet, ssh, http, etc). Changes to the state of each Service (such as telnet) require an account with admin rights. Below, I can view that telnet is not enabled. But I cannot enable it (because I am a user Group member):



```
ving@Spectracom ~ $ servget 2
elnet Service              disabled
ving@Spectracom ~ $ servset 2 on
ou must be an administrator to invoke the servset command.
ving@Spectracom ~ $ 
```

Security Algorithms (such as RC4)

**RC4 (also known as ARC4 or ARCFour)

- Refer to: http://en.wikipedia.org/wiki/RC4
- Refer to Mantis case 2293 http://cvsmantis.int.orolia.com/mantis/view_all_bug_page.php
- ARCFour consists of ARCFour, ARCFour 128 and ARCFour 256
- ARCFour is known to be weak. ARCFour 128 and ARCFour 256 improve these ciphers by removing the less secure portion of the cipher.
- ARCFour was enabled, but at the bottom of the cipher selection list, in at least version 5.0.0 and below
- ARCFour was disabled in version 5.2.1 update.

Q. We need to disable RC4 for SSH. Can you folks tell me how that can be done?

A. Reply from Paul Myers to Wade Sober (8 July 2013)

If SSH users do NOT want RC4, Please have Keith collect the customer requirements and enter a Mantis case.

Does the customer have a security reason why RC4 should be removed?
If it is generally applicable, we can consider removing it for all customers in a subsequent release.
I think this would require rebuilding of OpenSSL or less likely OpenSSH.
I don't recall an OpenSSH configuration operation to disable RC4.
For HTTP there might be such an option but they are referring to SSH correct?

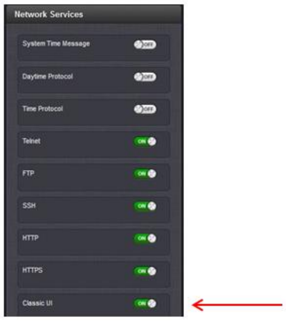
Update for questions below:

- RC4 was initially removed in update version 5.0.1 (Refer to Mantis case 2293)
- RC4 was then brought back into the software with version 5.1.5 (Refer to Mantis case 2918). It is also confirmed to be enabled in versions 5.1.7. 5.1J and 5.2.0 as well. It was added in to help address a vulnerability issue that was more severe.
- RC4 was then removed in version 5.2.1, as it was no longer needed in order to mitigate another vulnerability issue.

Note: In at least versions 5.2.1 through 5.3.1, RC4 cipher is only being used with the earlier "classic interface" web browser. It's not used with the newer black/charcoal browser

- If network scanner is detecting RC4 cipher is present, we recommend disabling the classic interface browser and just using the newer browser.

The classic interface web browser on port 8080 can be disabled in the bottom-left corner of the **Management** -> **Network** page of the newer black browser. It's the last slide switch in the "**Network Services**" list, labeled as "**Classic UI**" (as shown below). Note there is no need to reboot the SecureSync after sliding this switch to the OFF position.



Network Services

System Time Message	OFF
Daytime Protocol	OFF
Time Protocol	OFF
Telnet	ON
FTP	ON
SSH	ON
HTTP	ON
HTTPS	ON
Classic UI	ON

Q. We need to disable RC4 for SSH (in SecureSync). Can you folks tell me how that can be done?

A. Reply from Paul Myers to Wade Sober (8 July 2013)

If SSH users do NOT want RC4, Please have Keith collect the customer requirements and enter a Mantis case.

Does the customer have a security reason why RC4 should be removed?
If it is generally applicable, we can consider removing it for all customers in a subsequent release.
I think this would require rebuilding of OpenSSL or less likely OpenSSH.
I don't recall an OpenSSH configuration operation to disable RC4.

For HTTP there might be such an option but they are referring to SSH correct?

Email from Paul Myers

It seems like SSH2 is GOOD with ARCFOUR

http://www.openssh.org/security.html

OpenSSH was not vulnerable to the RC4 cipher password cracking, replay, or modification attacks. At the time that OpenSSH was started, it was already known that SSH 1 used the RC4 stream cipher completely incorrectly, and thus RC4 support was removed.

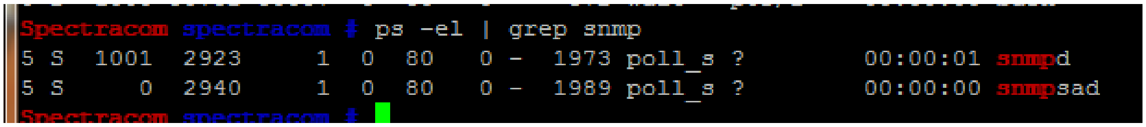
http://linux.die.net/man/5/sshd_config
ciphers described here

http://csce.uark.edu/~kal/info/private/ssh/ch03_09.htm
Restates RC4 is not useable with SSH1

Services/Processes/daemons which may be running

To check what processes are currently running

- All processes: At the CLI prompt, type **ps -el** <enter> (Note: **ps -elf** provides even more info)
- To see if a particular process (such as SNMPD and SNMPSAD, our sub-agent) is running, type **ps -el | grep snmp** <enter> (where it will list everything with the name typed after "grep)



```
Spectracom spectracom # ps -el | grep snmp
5 S  1001  2923     1  0  80   0 -  1973 poll_s ?        00:00:01 snmpd
5 S     0  2940     1  0  80   0 -  1989 poll_s ?        00:00:00 snmpsad
Spectracom spectracom #
```

Note: when the SNMP enable/disable switch is off, both snmpd and snmpsad should be stopped (not listed)

List of various daemons/services/processes which may be enabled/running in the unit

Note: Not all processes in this list below (such as Broadshield for instance) apply to all SecureSyncs- the list of services actually running in each SecureSync is likely to vary from one unit to the next. Also note there may be others not listed below (such as any that were added after this list was compiled, ~June 2018, for instance)

list below was from Mike Sutton (28 June 2018)

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

Controlling Services as spfactory (internal use only)

Kill a particular process that is currently running (such as snmpsad from above screenshot)

- Type: **kill** followed by the **pid number** (“2940” in the above screenshot). Example: **kill 2940** <enter>.

Start or stop services (such as SNMP, NTP etc)

1) Change to /etc/init.d
2) Type the name of service (such as **snmpd**) followed by **start** or **stop** or **zap**

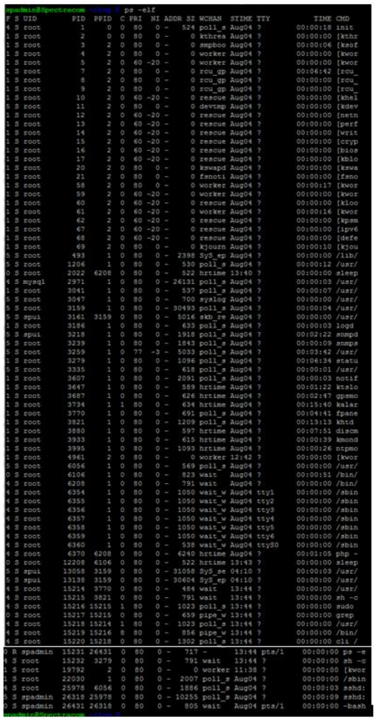
3) Zap (zap is for stopping a crashed service such as SNMP, NTP etc)

4) Change to /etc/init.d

5) Type the name of service (such as *snmpd*) followed by **zap. Example: snmpd zap**

6) Type the name of service (such as *snmpd*) followed by **start. Example: snmpd start**

Example ps -elf command from a v5.2.1 unit operating normally:



```
spadmin@Spectracom [illegible] ps -elf
F S UID          PID  PPID  C PRI  NI ADDR SZ WCHAN  STIME TTY          TIME CMD
4 S root           1     0  0  80   0 -   524 poll_s Aug04 ?        00:00:18 init
1 S root           2     0  0  80   0 -     0 kthrea Aug04 ?        00:00:00 [kthr
1 S root           3     2  0  80   0 -     0 smpboo Aug04 ?        00:00:06 [ksof
1 S root           4     2  0  80   0 -     0 worker Aug04 ?        00:00:00 [kwor
1 S root           5     2  0  60 -20 -     0 worker Aug04 ?        00:00:00 [kwor
1 S root           7     2  0  80   0 -     0 rcu_gp Aug04 ?        00:06:42 [rcu_
1 S root           8     2  0  80   0 -     0 rcu_gp Aug04 ?        00:00:00 [rcu_
1 S root           9     2  0  80   0 -     0 rcu_gp Aug04 ?        00:00:00 [rcu_
1 S root          10     2  0  60 -20 -     0 rescue Aug04 ?        00:00:00 [khel
5 S root          11     2  0  80   0 -     0 devtmp Aug04 ?        00:00:00 [kdev
1 S root          12     2  0  60 -20 -     0 rescue Aug04 ?        00:00:00 [netn
1 S root          13     2  0  60 -20 -     0 rescue Aug04 ?        00:00:00 [perf
1 S root          14     2  0  60 -20 -     0 rescue Aug04 ?        00:00:00 [writ
1 S root          15     2  0  60 -20 -     0 rescue Aug04 ?        00:00:00 [cryp
1 S root          16     2  0  60 -20 -     0 rescue Aug04 ?        00:00:00 [bios
1 S root          17     2  0  60 -20 -     0 rescue Aug04 ?        00:00:00 [kblo
1 S root          20     2  0  80   0 -     0 kswapd Aug04 ?        00:00:00 [kswa
1 S root          21     2  0  80   0 -     0 fsnoti Aug04 ?        00:00:00 [fsno
1 S root          58     2  0  80   0 -     0 worker Aug04 ?        00:00:17 [kwor
1 S root          59     2  0  60 -20 -     0 worker Aug04 ?        00:00:00 [kwor
1 S root          60     2  0  60 -20 -     0 rescue Aug04 ?        00:00:00 [kloo
1 S root          61     2  0  60 -20 -     0 worker Aug04 ?        00:00:16 [kwor
1 S root          62     2  0  60 -20 -     0 rescue Aug04 ?        00:00:00 [kpsm
1 S root          67     2  0  60 -20 -     0 rescue Aug04 ?        00:00:00 [ipv6
1 S root          68     2  0  60 -20 -     0 rescue Aug04 ?        00:00:00 [defe
1 S root          69     2  0  80   0 -     0 kjourn Aug04 ?        00:00:10 [kjou
5 S root         493     1  0  80   0 -  2398 SyS_ep Aug04 ?        00:00:00 /lib/
5 S root        1206     1  0  80   0 -   530 poll_s Aug04 ?        00:00:12 /usr/
0 S root        2022  6208  0  80   0 -   522 hrtime 13:40 ?        00:00:00 sleep
4 S mysql       2971     1  0  80   0 - 26131 poll_s Aug04 ?        00:00:03 /usr/
1 S root        3041     1  0  80   0 -   537 poll_s Aug04 ?        00:00:07 /usr/
5 S root        3047     1  0  80   0 -   700 syslog Aug04 ?        00:00:00 /usr/
5 S root        3159     1  0  80   0 - 30493 poll_s Aug04 ?        00:00:04 /usr/
5 S spui        3161  3159  0  80   0 -  5016 skb_re Aug04 ?        00:00:00 /usr/
1 S root        3186     1  0  80   0 -   633 poll_s Aug04 ?        00:00:03 logd
5 S spui        3218     1  0  80   0 -  1918 poll_s Aug04 ?        00:02:22 snmpd
5 S root        3239     1  0  80   0 -  1843 poll_s Aug04 ?        00:00:09 snmps
5 S root        3259     1  0  77  -3 -  5033 poll_s Aug04 ?        00:03:42 /usr/
1 S root        3279     1  0  80   0 -  1096 poll_s Aug04 ?        00:06:34 statu
5 S root        3335     1  0  80   0 -   618 poll_s Aug04 ?        00:00:01 /usr/
1 S root        3607     1  0  80   0 -  2091 poll_s Aug04 ?        00:00:03 notif
1 S root        3647     1  0  80   0 -   589 hrtime Aug04 ?        00:01:22 ktslo
1 S root        3687     1  0  80   0 -   626 hrtime Aug04 ?        00:02:47 gpsmo
1 S root        3734     1  1  80   0 -   634 hrtime Aug04 ?        00:15:40 kalar
1 S root        3770     1  0  80   0 -   691 poll_s Aug04 ?        00:04:41 fpane
1 S root        3821     1  0  80   0 -  1209 poll_s Aug04 ?        00:13:13 khtd
1 S root        3880     1  0  80   0 -   597 hrtime Aug04 ?        00:07:51 discm
1 S root        3933     1  0  80   0 -   615 hrtime Aug04 ?        00:00:39 kmond
1 S root        3995     1  0  80   0 -  1093 hrtime Aug04 ?        00:00:26 ntpmo
1 S root        4961     2  0  80   0 -     0 worker 12:42 ?        00:00:00 [kwor
5 S root        6056     1  0  80   0 -   569 poll_s Aug04 ?        00:00:00 /usr/
0 S root        6106     1  0  80   0 -   823 wait   Aug04 ?        00:00:51 /bin/
4 S root        6208     1  0  80   0 -   791 wait   Aug04 ?        00:00:00 /bin/
4 S root        6354     1  0  80   0 -  1050 wait_w Aug04 tty1     00:00:00 /sbin
4 S root        6355     1  0  80   0 -  1050 wait_w Aug04 tty2     00:00:00 /sbin
4 S root        6356     1  0  80   0 -  1050 wait_w Aug04 tty3     00:00:00 /sbin
4 S root        6357     1  0  80   0 -  1050 wait_w Aug04 tty4     00:00:00 /sbin
4 S root        6358     1  0  80   0 -  1050 wait_w Aug04 tty5     00:00:00 /sbin
4 S root        6359     1  0  80   0 -  1050 wait_w Aug04 tty6     00:00:00 /sbin
4 S root        6360     1  0  80   0 -   538 wait_w Aug04 ttyS0    00:00:00 /sbin
4 S root        6370  6208  0  80   0 -  6240 hrtime Aug04 ?        00:01:05 php -
0 S root       12208  6106  0  80   0 -   522 hrtime 13:43 ?        00:00:00 sleep
5 S spui       13058  3159  0  80   0 - 31058 SyS_se 04:10 ?        00:00:03 /usr/
5 S spui       13138  3159  0  80   0 - 30604 SyS_ep 04:10 ?        00:00:00 /usr/
4 S root       15214  3770  0  80   0 -   484 wait   13:44 ?        00:00:00 /usr/
4 S root       15215  3821  0  80   0 -   791 wait   13:44 ?        00:00:00 sh -c
4 S root       15216 15215  1  80   0 -  1023 poll_s 13:44 ?        00:00:00 sudo
0 S root       15217 15215  0  80   0 -   659 pipe_w 13:44 ?        00:00:00 grep
4 S root       15218 15214  1  80   0 -  1023 poll_s 13:44 ?        00:00:00 /usr/
4 S root       15219 15216  8  80   0 -   856 pipe_w 13:44 ?        00:00:00 /bin/
4 S root       15220 15218  0  80   0 -  1302 poll_s 13:44 ?        00:00:00 cli /
0 R spadmin    15231 26431  0  80   0 -   717 -      13:44 pts/1    00:00:00 ps -e
4 S root       15232  3279  0  80   0 -   791 wait   13:44 ?        00:00:00 sh -c
1 S root       19792     2  0  80   0 -     0 worker 11:38 ?        00:00:00 [kwor
1 S root       22030     1  0  80   0 -  2007 poll_s Aug04 ?        00:00:00 /sbin
4 S root       25978  6056  0  80   0 -  1886 poll_s Aug04 ?        00:00:03 sshd:
5 S spadmin    26318 25978  0  80   0 - 10255 poll_s Aug04 ?        00:00:09 sshd:
0 S spadmin    26431 26318  0  80   0 -   805 wait   Aug04 pts/1    00:00:00 -bash
spadmin@Spectracom [illegible]
```

Network related (network settings/Network Setup/DNS/Port enabling)

Network Discovery/Network Auto Discovery/Auto-Discovery

- for general info, refer also to associated "**Network Discovery**" in: ..\CustomerServiceAssistance.pdf

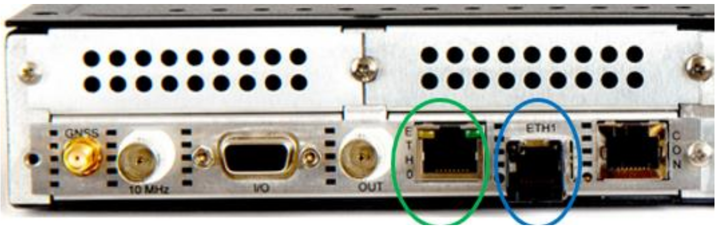
per https://www.bing.com/search?q=auto+discover+network&qs=SC&pq=autodiscover+network&sk=AS1&sc=6-20&cvid=E0055639B243408EA04BC4283BC25288&FORM=QBRE&sp=2

"Based on the **network** location you choose, Windows will **automatically** assign a **network discovery** state to the **network** and opens the appropriate Windows Firewall ports for that state. **Network discovery** is a **network** setting that affects whether your computer can find other computers and devices on the **network** and whether other computers on the **network** can find your computer"

Specific to Model 2400 SecureSyncs

- Don't believe Model 2400 SecureSyncs do currently support this capability, as of **at least** version 1.0.1 (first production release, Sept 2019)
- Refer to Salesforce cases such as 209596 (requesting it be available in 1200 SecureSync)

Base Ethernet interfaces (eth0/eth1) / Option Card interfaces (such as 1204-49/1204-4A)



- **ETH0** 1GB Ethernet (RJ45 connector)
- **ETH1** Ethernet (SFP connector)

- The **Ethernet** RJ45 (Eth0) and SFP (Eth1) connectors provide an interface to the network for NTP synchronization and to obtain access to the SecureSync product Web UI for system management. Eth0 has two small indicator lamps, "Good Link (green LED), and "Activity" (orange LED). The "Good Link" light indicates a connection to the network is present. The "Activity" light will illuminate when network traffic is detected.

1204-49/1204-4A Ethernet Option Cards to add additional network interfaces

- ➢ For more info, refer to Option Card Tech Note and Option Cards in online 2400 User guide: http://manuals.spectracom.com/2400/Content/NC_and_SS/SS/Topics/OCs/OC_Id.htm

List below is for current examples (List subject to change)

- ○ **Model 1204-49**: (2 SFPs) **Dual** GBE (Gigabit Ethernet) interface

  - **Inputs/Outputs**: (2) Gigabit Ethernet
  - **Connectors**: SFP Ports (2x)
  - **Management**: Enabled or Disabled (NTP server only)
  - **Maximum Number of Cards**: 1
  - **Ordering Information**: 1204-49: Dual Gigabit Ethernet

- ○ **Model 1204-4A**: (4 SFPs) **Quad** GBE (Gigabit Ethernet) interface

  - **Inputs/Outputs**: (4) Gigabit Ethernet
  - **Connectors**: SFP Ports (4x)
  - **Management**: Enabled or Disabled (NTP server only)
  - **Maximum Number of Cards**: 1
  - **Ordering Information**: 1204-4A: Quad Gigabit Ethernet

Management -> Network Setup page (for base eth0/eth1 and 1204-49/1204-4A Option Cards)

A) Base ethernet interfaces (eth0 and 1)

- Base ethernet interfaces are configured in ***Management*** -> ***Network Setup***

Issue: Report of *Management* -> *Network Setup* page not displaying eth0/eth1

Refer to Case 274942

Was due to being logged in as a USER account (instead of an admin account). User account doesn't have rights to view or change network settings.

Reply from Dave Lorah (9 Nov 2021) The reason you are seeing only the one Icon instead of three on the Network Setup screen is because you are logged in with an account that has only User privileges, which is read only. The configuration Icons are not visible if logged in with a User Account.

You can either login to the spadmin account or change your User Account privileges to Admin instead of User.

The front panel doesn't have a login and is always capable of setting the Network parameters.

B) Network Interface Setup of 1204-49 and 1204-4A expansion cards

- Refer also to the Option Card Assistance document in I:\Customer Service\1- Cust Assist documents\Word documents for more info on these cards

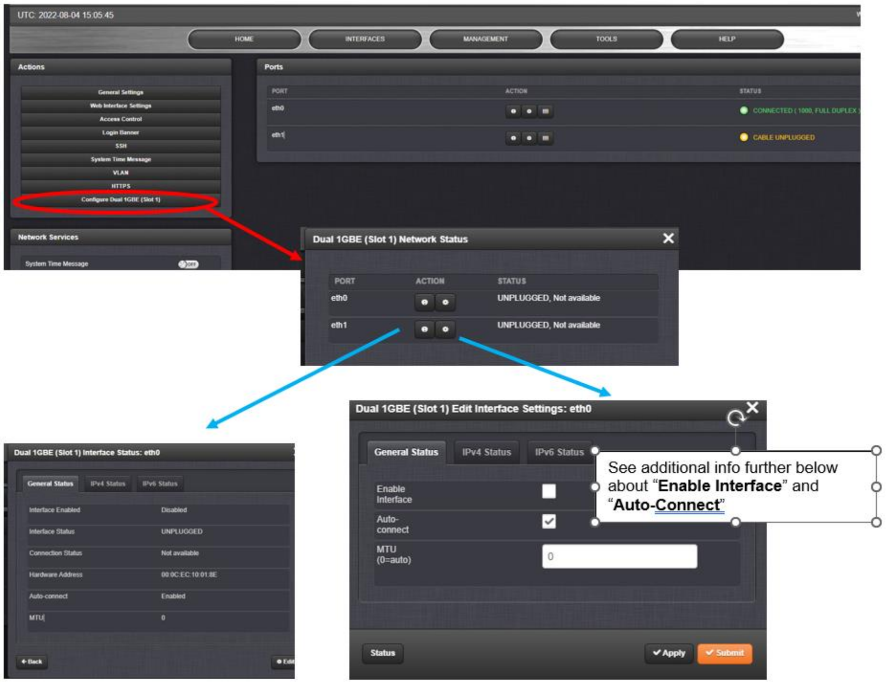
Important Note: These Option Cards are only compatible with **Slots 1 and 2** of the 2400 SecureSyncs. This is not a potential issue with Model 2402 SecureSyncs (which only has Slots 1 and 2), But can potentially be an issue with Model 2406 SecureSyncs (having 6 slots).

On 6/14/2023, Jon Brand mentioned that OPA automated tested has since started verifying these Option Cards are only installed in Slots 1 or 2, and has also become more thourough at verifying operation of these cards. Earlier shipped 2400 SecureSyncs have had these cards installed in at least slot 6, if not also 4 or 5 as well.

Symptoms of these cards being installed in a slot other than 1 or 2 include the Option Card being installed. But the Card's version is reported as "N/A".

Note: Network settings for the GB expansion cards are only available when starting from the "**Configure 1GBE**" button in the ***Management*** -> ***Network Setup*** page of the browser. The Network Settings won't be displayed/available if clicking on the **Configure 1GBE**" button in the ***Management*** -> ***NTP Setup*** page.

Management -> ***Network Setup*** page



UTC: 2022-08-04 15:05:45

Ports

PORT	ACTION	STATUS
eth0		CONNECTED (1000, FULL DUPLEX)
eth1		CABLE UNPLUGGED

Dual 1GBE (Slot 1) Network Status

PORT	ACTION	STATUS
eth0		UNPLUGGED, Not available
eth1		UNPLUGGED, Not available

Dual 1GBE (Slot 1) Interface Status: eth0

Interface Enabled	Disabled
Interface Status	UNPLUGGED
Connection Status	Not available
Hardware Address	00:0C:EC:10:01:8E
Auto-connect	Enabled
MTU	0

Dual 1GBE (Slot 1) Edit Interface Settings: eth0

Enable Interface	☐
Auto-connect	☑
MTU (0=auto)	0

See additional info further below about “**Enable Interface**” and “**Auto-Connect**”

Info about “General Status” (“Enable interface” and “Auto-connect”)

Whether a network cable is connected to an installed SFP (and the other end of the cable connected to another network device) DOES determine whether the Enable button can remain selected. Please have the customer connect a cable to the SFP, and their observation should disappear.

Having an SFP installed in a network interface, but no cable connecting the SFP to a network device, will not allow the interface to be “enabled”. An SFP needs to be installed, and a network cable needs to be connecting the SFP to another network device (such as a switch), in order for the port to be able to be enabled/remain enabled.

If the “**Auto-connect”** button (under the “Enable” Button) remains selected (enabled by default) the Enable button will be selected automatically, once a cable connects the SFP to another device, and the web page is refreshed. Then, if the Enable button is unchecked by a user, while the cable remains selected, the port switches from “**active**” state to “**inactive**” state.

Display network (UDP/TCP) network ports open/Network port assignments (such as port 123 is for NTP)

Netstat commands

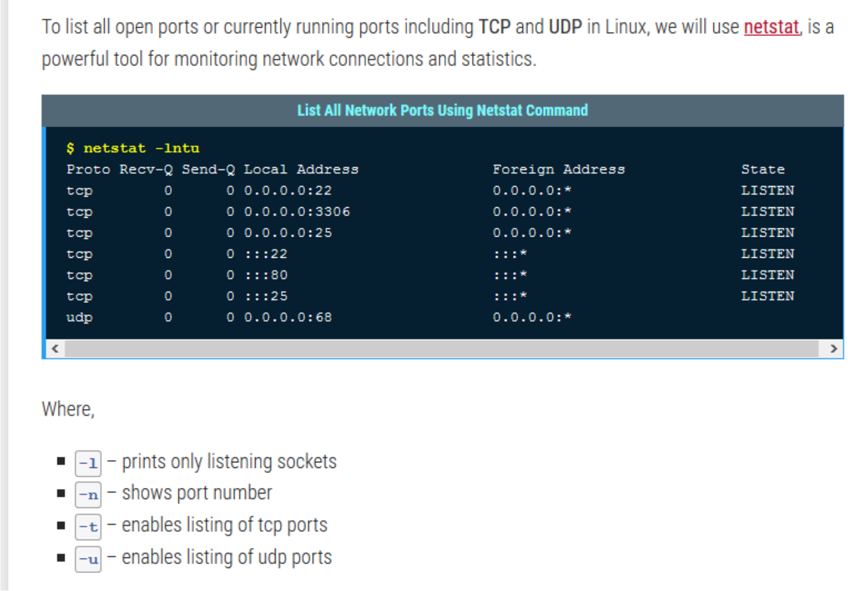
- Refer to netstat section in this doc: netstat and ss commands

“To list all open ports or currently running ports including **TCP** and **UDP** in Linux, we will use netstat, is a powerful tool for monitoring network connections and statistics.”

Available variants of the netstat command

- refer to sites such as: https://www.tecmint.com/20-netstat-commands-for-linux-network-management/

https://www.tecmint.com/find-open-ports-in-linux/



To list all open ports or currently running ports including **TCP** and **UDP** in Linux, we will use netstat, is a powerful tool for monitoring network connections and statistics.

List All Network Ports Using Netstat Command

```
$ netstat -lntu
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:3306                0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:25                  0.0.0.0:*                   LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
tcp        0      0 :::80                       :::*                        LISTEN
tcp        0      0 :::25                       :::*                        LISTEN
udp        0      0 0.0.0.0:68                  0.0.0.0:*
```

Where,

- `-l` – prints only listening sockets
- `-n` – shows port number
- `-t` – enables listing of tcp ports
- `-u` – enables listing of udp ports

netstat -tuln | grep :::

tcp6 0 0 :::8080 :::* LISTEN port **8080** is used for **Timekeeper option (if license file installed)**

tcp6 0 0 :::80 :::* LISTEN port **80** is used for **HTTP** web U/I

tcp6 0 0 :::21 :::* LISTEN port **21** is used for **FTP**

tcp6 0 0 :::22 :::* LISTEN port **22** is used for **SSH, SCP**

tcp6 0 0 :::23 :::* LISTEN port **23** is **Telnet**, unencrypted text communications to the unit

tcp6 0 0 :::443 :::* LISTEN port **443** is used for **Https, SSL**

udp6 0 0 :::57543 :::*

udp6 0 0 :::161 :::*

spadmin@Spectracom ~ $

In addition to the list above, port **123** is for NTP packets, and port **161** is for SNMP packets

ss -lntu command to find a list of all open ports
refer to L https://www.tecmint.com/find-open-ports-in-linux)

RFCs

The Internet Engineering Task Force website (has a section titled "RFC pages". RFC's (Request For Comments) provide a breakdown of the many protocols used by computers and networks. Refer to http://www.ietf.org/rfc.html to query for a specific RFC.

MIB-2 is officially defined in RFC1213. Type in "**1213"** where it asks for the RFC number. This will give you Management Information Base for Network Management protocol for TCP/IP-based Internets (MIB-II).

For a "complete" list of **ports**, refer to: http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

UDP/TCP Ports for the 2400 SecureSync

Protocol	Port	Description	Associated service (for listening)	Notes
TCP or UDP	**13**	**Daytime**	**Xinetd** (although this will launch daytime upon connection)	Daytime protocol (RFC 867)
TCP	**22**	**SCP/SFTP**	**Xinetd** (although this will launch **sshd** upon connection) see example log entry to the right	SSH (Secure Shell) Apr 13 17:37:14 Spectracom **xinetd**[2383]: **START: ssh** pid=18927 from=::ffff:10.2.100.52
TCP	**37**	**TIME**	**Xinetd** (although this will launch time protocol upon connection)	Time protocol (RFC 868)
UDP	**53**	**DNS**		Domain Name System
TCP	**80**	**HTTP**	HTTP	Optional, if HTTPS is normally used)
UDP	**123**	**NTPD**	NTPD	Network Time Protocol (NTP)
UDP	**161**	**SNMP**	snmpd	(Factory default is 161, but is user-configurable)
UDP	**162**	**SNMP TRAPS**	snmpd	(Factory default is 162, but is user-configurable)
TCP	**443**	**HTTPS/SSL**	Apache2	Associated with the Apache browser
UDP	**514**	**syslog**	syslogd	Remote Shell, Factory default is port **514**. Can be changed in versions 5.7.1 and above,
UDP	**319**	**ptpv2**	ptpd	PTP protocol
UDP	**320**	**ptpv2**	ptpd	PTP protocol

xinetd (per https://en.wikipedia.org/wiki/Xinetd)
xinetd listens for incoming requests over a network and launches the appropriate service for that request.[5] Requests are made using port numbers as identifiers and xinetd usually launches another daemon to handle the request. It can be used to start services with both privileged and non-privileged port numbers.

CLI Command to report port statuses

Per Eric Girard (June 2022) grep <service name > etc/services **will report each used port for each protocol**

**2400 Port speeds/duplex settings (hard-set vs auto-negotiate) selections (eth0/eth1)

Customer desire to Hard-set network speed/duplex settings in 2400 SecureSync v1.2.2

- Refer to Case 285987 / JIRA ticket CAR-1815
- Ability to hard-set port not available in at least v1.6.0 and below (Nov 2022)

NOTE: Info further below is from 1200 SecureSyncs

Current info for 2400 SecureSyncs
As of even at least v1.6.0 and below (expected around Nov 2022) ability to hard-set port speed/duplex settings is not available!

CAR-1815 was created by Ryan Johnson as a feature request to add hard-set speed/duplex settings

(Status update as of 2 Nov 2022)

rdries 3 hours ago
Hi @Girard Eric, there is currently no way for a customer to disable auto-negotiation in 2400. Engineering has a ticket to add this in a future release.

Girard Eric 2 hours ago
Thanks @rdries So i guess it is scheduled for 1.7.0, expected for Q1 2023?

rdries 2 hours ago
I am not sure when this feature is planned for. @Mike Pratt @ryanj could you provide Eric this information?

Mike Pratt 2 hours ago
@Girard Eric @rdries That feature is tentatively planned for 2400 version 1.8.0, which is two versions from now. That's Q2 2023 at best, but I absolutely don't guarantee that right now (edited)

A) Configuring via CLI (speedget and speedset commands)

(Not currently available in 2400s. Needs to be edited in the future)

B) Configuring via web browser

Management -> ***Network Setup*** page,
Click the middle icon (pencil) for each interface (eth0 thru eth3)

"Autonegotiation" enabled (default) **Autonegotiation" disabled**

(Not currently available in 2400s. Needs to be edited in the future)

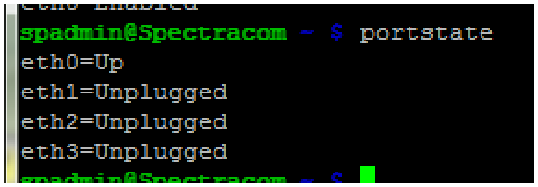
Logging of associated port settings in the kern.log

(Not currently available in 2400s. Needs to be edited in the future, once speed/duplex settings can be hard-set)

- Port speeds (such as 10Mbps, 100Mbs or 1000Mbps) and duplex selection (half duplex or full duplex) for the Ethernet interfaces are logged in the kern.log
  - Example kern.log entry:

**Desire to display port state of all Ethernet ports (port up, port down, cable unplugged)

- CLI command is **portstate**
- Displays status of all installed Ethernet ports, including Eth0

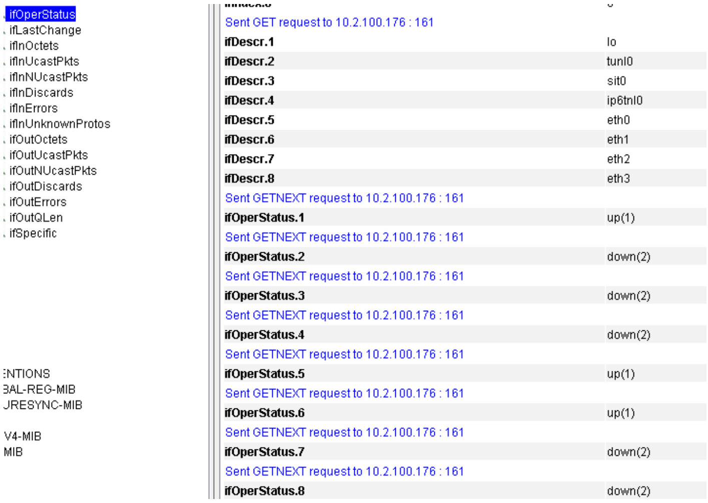


```
spadmin@Spectracom ~ $ portstate
eth0=Up
eth1=Unplugged
eth2=Unplugged
eth3=Unplugged
spadmin@Spectracom ~ $
```

Ethernet port states via SNMPGets

Note that in addition to the port states being available via the **portstate** CLI command, they are also available via SNMPGets in the generic (not Spectracom-specific) RFC-1213 MIB. The name of the object for the states of each port in the RFC1213 MIB is **ifOperStatus** (as shown below):

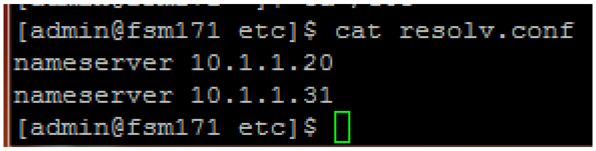
The **ifDescr** object lists all of the available interfaces in the time server and reports the “assigned name” for each one.



```
Sent GET request to 10.2.100.176 : 161
ifDescr.1                                   lo
ifDescr.2                                   tunl0
ifDescr.3                                   sit0
ifDescr.4                                   ip6tnl0
ifDescr.5                                   eth0
ifDescr.6                                   eth1
ifDescr.7                                   eth2
ifDescr.8                                   eth3
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.1                              up(1)
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.2                              down(2)
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.3                              down(2)
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.4                              down(2)
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.5                              up(1)
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.6                              up(1)
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.7                              down(2)
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.8                              down(2)
```

DNS servers settings (Primary and Secondary DNS servers)/LLMNR

Configuration (“etc/resolv.conf” file)



```
[admin@fsm171 etc]$ cat resolv.conf
nameserver 10.1.1.20
nameserver 10.1.1.31
[admin@fsm171 etc]$
```

- Users do not have permission to edit resolv.conf file directly.
- The two DNS Server fields are only displayed in the browser if DHCP is disabled (they are hidden when DHCP is enabled)
- DNS settings should be automatically configured if the port is configured as DHCP enabled
- Manual configuration if DHCP is disabled on that Ethernet interface
- For detailed info on the etc/resolv.conf file, refer to http://man7.org/linux/man-pages/man5/resolv.conf.5.html

The Link-Local Multicast Name Resolution (LLMNR)

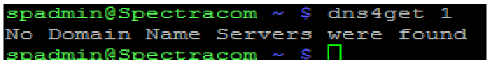
- Refer to Salesforce Case 301047 (for 1200 but likely also applies to 2400s)
- refer to https://en.wikipedia.org/wiki/Link-Local_Multicast_Name_Resolution#:~:text=The%20Link%2DLocal%20Multicast%20Name,on%20the%20same%20local%20link

  “The Link-Local Multicast Name Resolution (LLMNR) is a protocol based on the Domain Name System (DNS) packet format that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link.”

A) Via CLI command

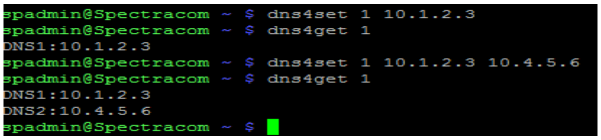
Display/retrieve/set DNS settings for each Ethernet interface

- The CLI command: **dns4get x** retrieves the DNS setting (for the port specified by the “x”.



```
spadmin@Spectracom ~ $ dns4get 1
No Domain Name Servers were found
spadmin@Spectracom ~ $
```

- The CLI command: **dns4set x <primary dns> <secondary dns>** configures the DNS setting for the Ethernet interface port number specified by the “x”. (note the secondary DNS address is optional/not required)

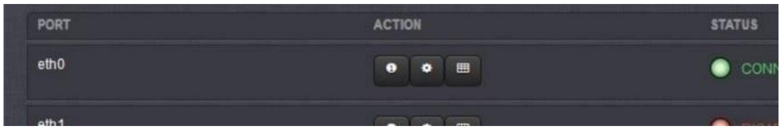


```
spadmin@Spectracom ~ $ dns4set 1 10.1.2.3
spadmin@Spectracom ~ $ dns4get 1
DNS1:10.1.2.3
spadmin@Spectracom ~ $ dns4set 1 10.1.2.3 10.4.5.6
spadmin@Spectracom ~ $ dns4get 1
DNS1:10.1.2.3
DNS2:10.4.5.6
spadmin@Spectracom ~ $
```

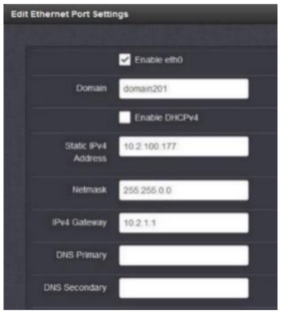
B) Via New browser (Management -> Network page of the browser)

Email from Keith (25 Jun 15) FYI- the only reason you should have to configure DNS servers is if you are using static network settings. If you are using DHCP, the DHCP server should have configured these settings for you.

For static network settings, the DNS settings are located in the **Management** -> **Network** page of the web browser. Then click on the middle of the three icons (the gear icon) for the Ethernet interface that you wish to configure.



With the Ethernet interface enabled (top of the pop-up window) and as long as the "**Enable DHCPv4**" checkbox is not selected, you will see the DNS server fields (these fields are not displayed if the "Enable DHCPv4" checkbox is selected) as shown below:



Edit Ethernet Port Settings

☑ Enable eth0

Domain: domain201

□ Enable DHCPv4

Static IPv4 Address: 10.2.100.177

Netmask: 255.255.0.0

IPv4 Gateway: 10.2.1.1

DNS Primary:

DNS Secondary:

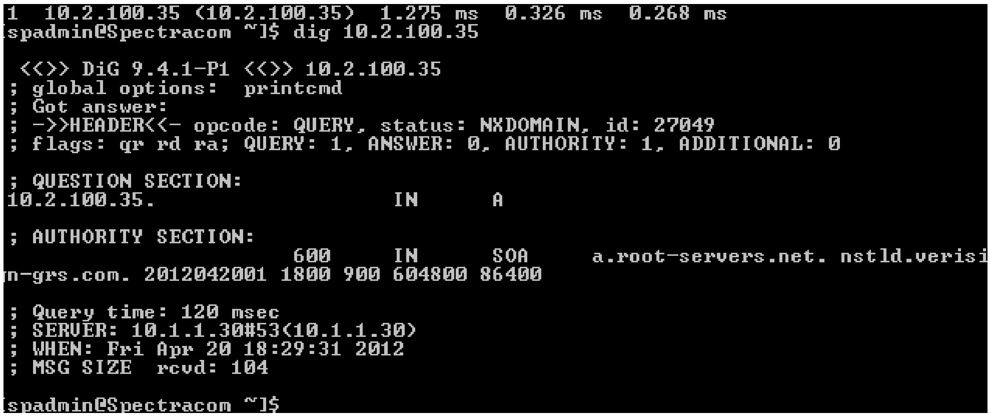
Available CLI ("dig") command to help troubleshoot DNS issues

Note (24 Jan KW) Appears dig may have removed (or disabled for spadmin)

dig: (Domain Information Groper)

- At the command prompt. type "**dig**"

  Function: a flexible tool for interrogating **DNS name servers**. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.



```
1  10.2.100.35 (10.2.100.35)  1.275 ms  0.326 ms  0.268 ms
[spadmin@Spectracom ~]$ dig 10.2.100.35

 <<>> DiG 9.4.1-P1 <<>> 10.2.100.35
; global options:  printcmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 27049
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

; QUESTION SECTION:
10.2.100.35.                   IN      A

; AUTHORITY SECTION:
                       600     IN      SOA     a.root-servers.net. nstld.verisi
n-grs.com. 2012042001 1800 900 604800 86400

; Query time: 120 msec
; SERVER: 10.1.1.30#53(10.1.1.30)
; WHEN: Fri Apr 20 18:29:31 2012
; MSG SIZE  rcvd: 104

[spadmin@Spectracom ~]$
```

**DNS Host name/ Fully Qualified Domain Name (FQDN)/ (hostname/host name)/LLMNR

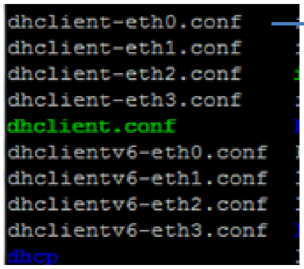
Notice about using DNS host names: When listing DNS hostnames (instead of IP addresses) to peer NTP servers together, the FQDN (Fully Qualified Domain Name) may need to be used, especially when the devices are not on the same domain.

Rules for hostnames in linux (Refer to RFCs 952 https://tools.ietf.org/html/rfc952 and Section 2 of RFC 1123: https://tools.ietf.org/html/rfc112)

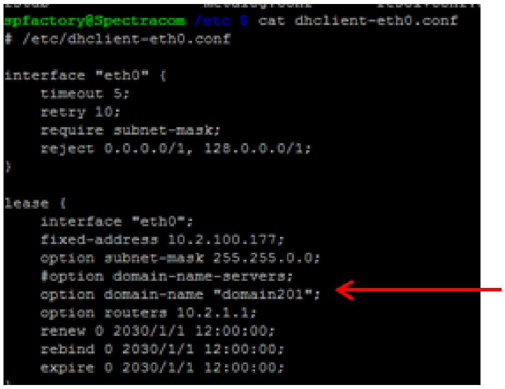
A "name" (Net, Host, Gateway, or Domain name) is a text string up to 24 characters drawn from the alphabet (A-Z), digits (0-9), minus sign (-), and period (.). Note that periods are only allowed when they serve to delimit components of "domain style names". (See RFC-921, "Domain Name System Implementation Schedule", for background). No blank or space characters are permitted as part of a name. No distinction is made between upper and lower case. The first character must be an alpha character. The last character must not bea minus sign or period. A host which serves as a GATEWAY should have "-GATEWAY" or "-GW" as part of its name. Hosts which do not serve as Internet gateways should not use "-GATEWAY" and "-GW" as part of their names. A host which is a TAC should have "-TAC" as the last part of its host name, if it is a DoD host. Single character namesor nicknames are not allowed.

Domain Name storage

- The domain name for each Ethernet port is stored in the associated “dhclient-eth” config file located in the /etc file (for example, the IPv4 domain name for eth0 is stored in the dhclient-eth0.conf file



```
dhclient-eth0.conf
dhclient-eth1.conf
dhclient-eth2.conf
dhclient-eth3.conf
dhclient.conf
dhclientv6-eth0.conf
dhclientv6-eth1.conf
dhclientv6-eth2.conf
dhclientv6-eth3.conf
dhcp
```



```
spfactory@Spectracom /etc $ cat dhclient-eth0.conf
# /etc/dhclient-eth0.conf

interface "eth0" {
    timeout 5;
    retry 10;
    require subnet-mask;
    reject 0.0.0.0/1, 128.0.0.0/1;
}

lease {
    interface "eth0";
    fixed-address 10.2.100.177;
    option subnet-mask 255.255.0.0;
    #option domain-name-servers;
    option domain-name "domain201";
    option routers 10.2.1.1;
    renew 0 2030/1/1 12:00:00;
    rebind 0 2030/1/1 12:00:00;
    expire 0 2030/1/1 12:00:00;
```

- If NTP peering isn’t working when using hostnames, may need to use FQDN (Fully Qualified Domain Name). Or, setup the domain name on the network interface setup page of the time server for each port, which should allow the single name rather than needing to use the FQDN.

SecureSyncs/9400s support just ONE Domain name per Ethernet interface (can’t list more than one)

- As of least version 5.6.0 (Apr, 2017), can’t list more than one domain name per Ethernet interface.

Q We were adding some additional domains under below location. We tried adding domains separated by comma, space, semicolon but received error “Invalid domain name”

Management -> Network Setup - > Go to “eth*” interface –> Click on gear box -> Under domain field add domains < ofi.com ny.ofi.com den.ofi.com tri.ofi.com roc.ofi.com oppenheimerfunds.com >

A Reply from Dave L (14 Mar 17) These parameters are limited in the Securesync configuration.The Securesync cannot have more than one Domain name per Ethernet port. Each port can have up to two DNS server addresses.

Configuration of hostnames (excerpted from 1200s)

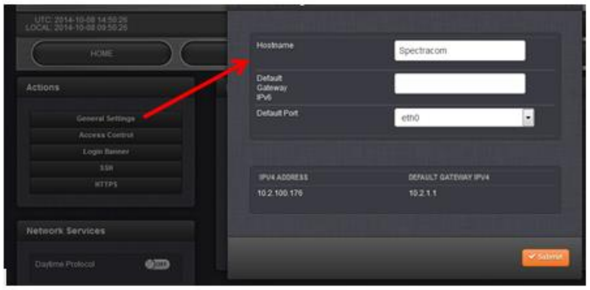
Factory default hostnames

- **Eth0**: domain201
- **Eth1**: domain202

Via web browser

A) Management -> Network page, General Settings **button on the left**

- ➢ To view the current value: click on the left of the three icons (i) for the particular port
- ➢ To change the current value: click on the middle of the three icons (gear icon) for the particular port. It's the "Domain" field.



UTC: 2014-10-08 14:50:26
LOCAL: 2014-10-08 09:50:26

Hostname: Spectracom

Default Gateway IPv6:

Default Port: eth0

IPV4 ADDRESS	DEFAULT GATEWAY IPV4
10.2.100.176	10.2.1.1

Newer browser interface only:

SecureSyncs/9400s accept:

- ➢ Over 40 total characters total in length (not sure exact limit)
- ➢ First character can be any number or letter (lower or upper-case)
- ➢ Hyphens/minus sign (-) (except as the first character)
- ➢ Dots "." (except as the first character)

Note (about dots): In order to use any dots in the hostname, it can only be entered via the newer browser. The classic interface doesn't accept any dots.

Does not accept:

- ➢ Can't be left blank.
- ➢ Spaces in the name. However, you can you a hyphen ("-") in place of the space. Note that you can't use an underscore ("_") in between.
- ➢ Does NOT accept as first or any other character: either parenthesis sign (either "(" or ")") the "and" sign (&) or quote mark ("),colon (:), apostrophe ('), or semicolon (;) or backslash (\), or pound sign ("#") or a plus sign (+),asterisk (*),underscore (_), percent sign (%), tilde (~), question mark (?), ampersand (@), (^) exclamation (!), brackets ([or]) or ({) or (}),or comma (,) forward slash (/)
- ➢ Does not accept less than or greater than signs (< or >) anywhere in the string.
- ➢ Does not accept dollar sign (random numbers may be returned in its place).

The Link-Local Multicast Name Resolution (LLMNR)

- Refer to Salesforce Case 301047 (for a 1200 but likely also applies to 2400s)
- Refer to https://en.wikipedia.org/wiki/Link-Local_Multicast_Name_Resolution#:~:text=The%20Link%2DLocal%20Multicast%20Name,on%20the%20same%20local%20link

"The Link-Local Multicast Name Resolution (LLMNR) is a protocol based on the Domain Name System (DNS) packet format that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link."

Troubleshooting NTP peering

- Use the **Status** -> **NTP** page and NTP log entries to help troubleshoot
- When using hostname to define other NTP servers:

  A) If they SSH or telnet to the SecureSync, can they ping the hostname of the other NTP server from the command line?

  B) If just the single name of the hostname (example "spectracom") has the full domain name been configured in the Interfaces page of the browser? This will need to be done.

  C) Are the other NTP servers on the same domain? If not, the FQDN (not just the single name) will need to be used.

**ARPS / ARP CACHING

Issue: ARP messages keep going out around every 35 seconds. (Acts like arp caching issue - not able to store the arps properly).

- Refer to Salesforce case 11297 (https://na8.salesforce.com/500C000000TDnFi)
- Paul Myers said this is likely due to adding NTP peers or NTP servers, and this NTP server can't find one or more of the NTP servers on the network due to network or routing issue. So it keeps sending ARP messages to find it.

**TCP connection/TCP session timeouts

Note: To see the timeout value, as any user, type "**cat /proc/sys/net/ipv4/tcp_keepalive_time**"

- **Factory default TCP timeout is 7200** seconds (as verified in versions 5.2.1, 5.3.1 and 5.4.1)
- **Factory default TCP timeout is 7200** seconds (with at least versions 4.8.9 and below).

- I entered Mantis case 2060 to make this timeout value user-configurable (as requested by Joel Polleta with Northrop Grumman). Refer to Salesforce Case 10072 for more info

References for TCP User Timeout:
The relevant standards are:

- http://tools.ietf.org/html/rfc5482
- http://tools.ietf.org/html/rfc793

Note: this info doesn't appear to apply to SSH (or at least SSH in Gentoo-versions 5.0.0 and above anyways)

In at least versions 5.3.1 and below, the TCP timeout value is hard-coded and can't be edited by a user.

Email from Paul Myers
SHORT ANSWER:
The default value is 7200 seconds
To see as any user type "**cat /proc/sys/net/ipv4/tcp_keepalive_time** " from the command line.
We could control the value via software if we so chose.

LONG ANSWER WITH THEORY BELOW:

In regards to the TCP User Timeout
The relevant standards are:
http://tools.ietf.org/html/rfc5482
http://tools.ietf.org/html/rfc793

How to change:
http://stackoverflow.com/questions/15484906/change-the-tcp-timeout-for-a-linux-network-device

http://www.cyberciti.biz/tips/linux-increasing-or-decreasing-tcp-sockets-timeouts.html

Excerpted from above link: (Credit given)

Some time it is necessary to increase or decrease timeouts on TCP sockets. You can use **/proc/sys/net/ipv4/tcp_keepalive_time** to setup new value.

The number of seconds a connection needs to be idle before TCP begins sending out keep-alive probes. Keep-alives are only sent when the SO_KEEPALIVE socket option is enabled. The default value is 7200 seconds (2 hours).
For example set value to 2400 seconds:
echo 2400 > /proc/sys/net/ipv4/tcp_keepalive_time
You can make changes to /proc filesystem permanently using /etc/sysctl.conf

Half-Open TCP sessions

- From wikipedia The term half-open refers to TCP connections whose state is out of synchronization between the two communicating hosts, possibly due to a crash of one side. A connection which is in the process of being established is also known as embryonic connection. The lack of synchronization could be due to malicious intent.
- Both questions below were regarding Salesforce case 16300

Q. Does the SecureSync network stack drop half open TCP sessions after a timeout period? If so, what is the timeout? Is it adjustable?
A. Keith's response (from Dave Sohn, 30 Oct 2014): Yes, after ~3 minutes. It is not currently adjustable.

Q. Does the SecureSync network stack set a limit as to the maximum number of half-open TCP sessions allowed? If so, what is the limit?
A. Keith's response (from Dave Sohn, 30 Oct 2014): Yes, 128 half-open connections.

**FIPS compliancy / Network Isolation/Network security

- For FIPS: Refer to: FIPS compliancy (FIPS 140-2) for all Spectracom NTP servers

Q. Email from Jeremy Thomas (10/13/11) "They site CSG security accreditation (EL4 and above) no doubt we have similar US alternatives"
A. Reply from Dave Sohn: We don't have any security accreditations for the SecureSync

Q. Email from Jeremy Thomas (10/13/11): The question is the separation and security of SecureSync network timing signals as each test room must ensure absolute security
A. Reply from Dave Sohn: Network isolation is handled within the SW via routing tables and rules.

***IEEE 802.3

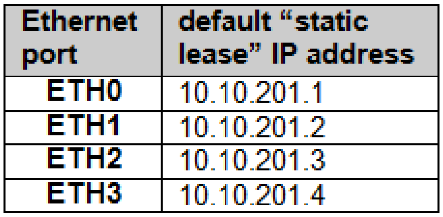
- ➢ Refer to http://en.wikipedia.org/wiki/IEEE_802.3
- ➢ IEEE 802.3 is a working group and a collection of IEEE standards produced by the working group defining the physical layer and data link layer's media access control (MAC) of wired Ethernet.

IEEE 802.3ad/ IEEE 802.1ax (Link Aggregation Control Protocol"- LACP)

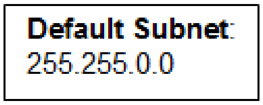
- ➢ Link aggregation is a computer networking term to describe various methods of combining (aggregating) multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links fail.
  - 802.1ax (back in 2008)
  - 802.3ad (initial release back in 2000)
- ➢ Refer to http://en.wikipedia.org/wiki/Link_aggregation#Initial_release_802.3ad_in_2000
- ➢ As of at least software version 5.5.0 software, SecureSync is not 802.3ad or 802.1ax compliant

DHClient (“Static lease” default IP addresses for the Ethernet interfaces)

- ➢ Assigned “Static” IP addresses are actually “static lease” dynamic address
- ➢ Note: The NTP server’s default subnet mask is “16” (255.255.0.0) Not 255.255.255.0. Since 255.255.255.0 is fairly common, a PC directly connected to the network ports may need to be reconfigured as 255.255.0.0 to allow a connection.



Ethernet port	default “static lease” IP address
ETH0	10.10.201.1
ETH1	10.10.201.2
ETH2	10.10.201.3
ETH3	10.10.201.4



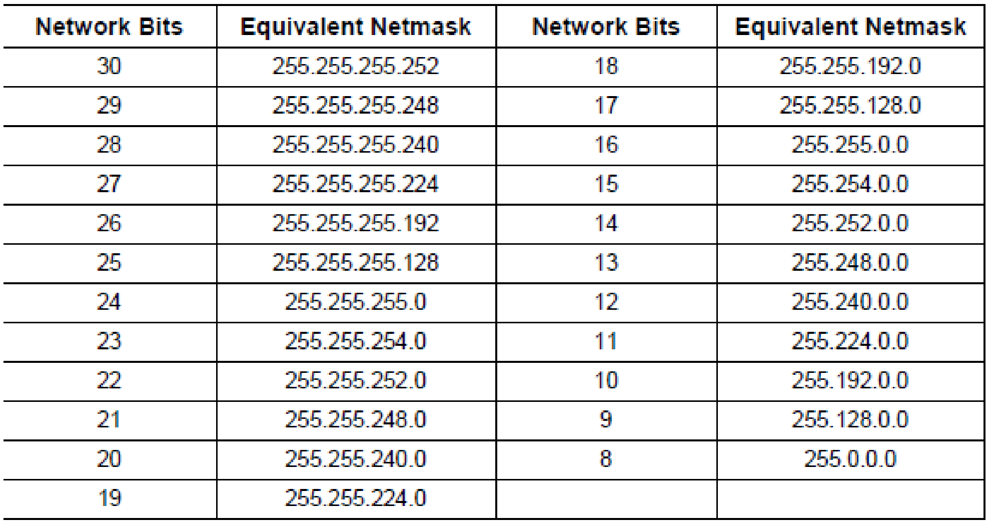
Default Subnet:
255.255.0.0

Email from Mark Goodlein to Morgan Stanley (7/11/12)

The product may have up to 4 interfaces, each of which may be configured differently (with or without DHCP) but must share some of the same network configuration files (eg. resolv.conf). Because of this, we utilize dhclient for interfaces regardless of whether they are configured for DHCP or static. Each interface has a dhclient.conf file that contains a “static lease” for that interface, which specifies the IP address, mask, DNS servers, domain, etc. When the static parameters are configured on the Web UI or from the command line, they are written into this saved in the static lease in the config file.

When dhclient is invoked to obtain or renew a lease, it will broadcast a request then wait for a response. If no acceptable response is received before some timeout (10 seconds), it will default to using the static lease from the config file. When you configure an interface to be ‘static’ on the SecureSync, what this does is it modifies the dhclient configuration file for that interface by telling it to reject responses to its dhcp request that come from any IP address. This forces dhclient to timeout and use the static lease. When DHCP is ‘enabled’ the interface is configured to allow DHCP responses and it will accept the first valid response it receives from a DHCP server.

When a new DHCP lease is used, a script is run which re-creates the resolv.conf file, pulling together all the domains and DNS servers from each interface. Note: that because we allow 2 DNS servers per interface and may have 4 interface, our system has been modified to support a maximum of 8 DNS servers, instead of the default 3.



Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
30	255.255.255.252	18	255.255.192.0
29	255.255.255.248	17	255.255.128.0
28	255.255.255.240	16	255.255.0.0
27	255.255.255.224	15	255.254.0.0
26	255.255.255.192	14	255.252.0.0
25	255.255.255.128	13	255.248.0.0
24	255.255.255.0	12	255.240.0.0
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		

Ethernet Bonding (two IP addresses assigned to same port) /Link Aggregation (LACP)

- 803.2ad / Load balancing / Ethernet Bonding/ LACP (Link Aggregation Control Protocol) Aggregate addresses are NOT supported in SecureSync or Model 9400 series. These are all names for a network function that allows more than one network port to have the same IP address for network redundancy.
- Refer to Mantis case 3091 for a request for us to support Ethernet Bonding.
- The IP addresses for Eth0-Eth3 CAN be on the same subnet but CANNOT be set to the same IP address as another one of the ports (two different ports can't both be 10.10.2.1 for instance).
- Refer to NTP over Anycast as an alternate solution:

(11 Aug 15 KW) Per Dave Sohn, Bonding in SecureSync is feasible. It's just lower in priority right now.

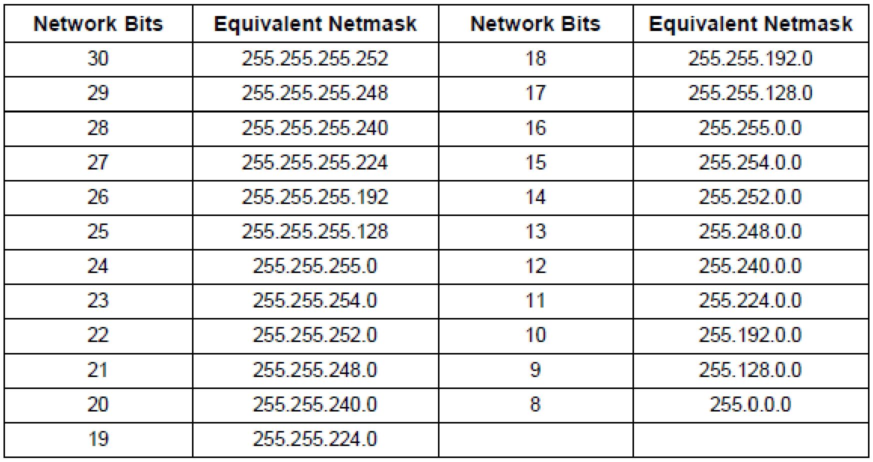
Duplicate IP addresses

If you duplicate an IP address, network connectivity stops as soon as the IP address has taken ("**please wait**" is shown on the front panel for about 10 seconds while the changes take effect. Once the message clears, no longer able to ping, access the web browser on any of the ports with the same IP address.

Note (per Dave Sohn): if more than one network port is on the same subnet as other network ports, the routing tables and routing rules will allow response packets to go out the same port that the incoming packets were received on (not just the first port on the subnet).

Example: If Eth0 and Eth1 are on the same subnet and NTP request is received on Eth1, the packet will also go back out on Eth1 (not Eth0, even though it's the first port in the routing table). This is established by the routing rules, which "flag" which specific routing table to use for the return, when the packet is initially received.

Netmask settings



Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
30	255.255.255.252	18	255.255.192.0
29	255.255.255.248	17	255.255.128.0
28	255.255.255.240	16	255.255.0.0
27	255.255.255.224	15	255.254.0.0
26	255.255.255.192	14	255.252.0.0
25	255.255.255.128	13	255.248.0.0
24	255.255.255.0	12	255.240.0.0
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		

Auto-MDIX

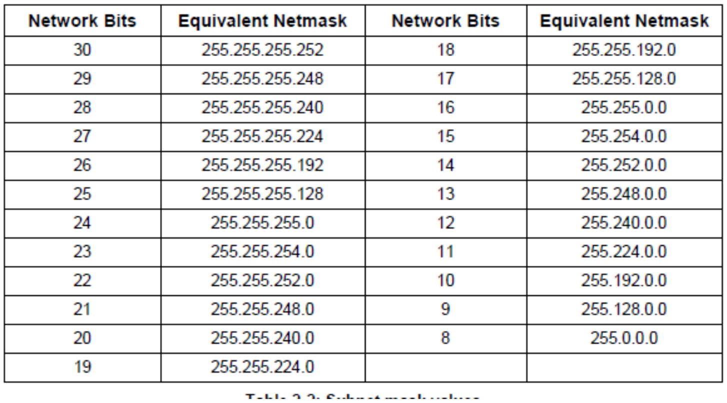
Ethernet ports Eth1, Eth2 and Eth3 (when the Model 1204-06 Gigabit Option Card is installed) are **auto-MDIX** network ports. This allows a PC to be connected directly to these Ethernet ports without the need for a network cross-over cable.

Note: eth0 (the base Ethernet port) is not auto-MDIX, a crossover cable needs to be used when connecting a PC directly to this Ethernet port.

Connecting a PC directly to one of the Ethernet ports

When connecting a PC directly to ETH0, a network cross-over cable is required:

1) When connecting a PC directly to ETH1, ETH2 or ETH3, since these ports are auto-MDIX, either a straight-thru OR standard network cable can be used.
2) Most PCs default to DHCP enabled. The PC needs to be configured with a STATIC IP address with the same subnet mask as the NTP Server.
3) The NTP server's default subnet mask is "16" (255.255.0.0) Not 255.255.255.0. Since 255.255.255.0 is fairly common, a PC directly connected to the network ports may need to be reconfigured as 255.255.0.0 to allow a connection.



Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
30	255.255.255.252	18	255.255.192.0
29	255.255.255.248	17	255.255.128.0
28	255.255.255.240	16	255.255.0.0
27	255.255.255.224	15	255.254.0.0
26	255.255.255.192	14	255.252.0.0
25	255.255.255.128	13	255.248.0.0
24	255.255.255.0	12	255.240.0.0
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		

Table 2-2: Subnet mask values

Status LEDs for the network ports (Eth0- Eth3)

- Note the status LEDs next to Eth0 are dim by design.
- Eth1-Eth3 do not have status LEDs next to Ethernet jacks due to space limitations on Option Cards. But each port has an internal status LED that can be viewed through the slot next to each connector of through holes in the back of the top cover.

Q. I noticed ALL the SecureSync GPS receivers LAN port LED's do not light when connected. I was troubleshooting some connectivity issues here and when I saw no LED's on the receiver I couldn't ping, I thought it was a physical issue until about a half hour later realized None of the SecureSync LAN ports light even when all is OK.

A (Keith's reply 11/6/12) For your information, the base Ethernet network port (which is installed in the left-side of the chassis of all SecureSyncs and is called "Eth0") does have an external green Good Link LED and an amber activity LED. These LEDs are always enabled on all SecureSyncs, with no ability to disable them.

However, due to space/footprint limitations on the optional three network port "Gigabit" Option Card (Spectracom Model 1204-06), when installed in a rear panel Option Bay, these three network ports (Eth1, Eth2, and Eth3) do not have external network status LEDs available. But each of these three ports does have its own internal link status LED which is lit when a network cable is connected to the network ports on this Option Card (the link LED being lit can be viewed either right beside each network connector or through the holes in the back of the top cover. These LEDs are always enabled on all SecureSyncs, with no ability to disable them.

This is why you are not seeing any enable/disable boxes associated with the network LEDs in the web browser.

**Troubleshooting issues with network configuration/operation

A) Desire to know if a network interface (eth0, eth1, eth2 or eth3) is up or down

- Refer to “Desire to know if a network port is up or down” in the SecureSync Option Card document ..\SecureSync Option Card information.pdf

B) Network settings aren’t being restored correctly after reboot (going back to default??)

A customer reported that after each reboot, Eth0 was losing its IP address and all three Gb Option card ports (eth1, eth and eth3) were disabled again (all are enabled before the reboot).

Conclusion/resolution: Dave Sohn indicated the factory default settings are eth 0 set to DHCP enabled and all of the Gb ports being disabled. So it appeared they are going to defaults at start-up. Dave S recommended performing a software update to the latest version while also performing a restore to factory default settings. Suspected something may have happened to the configs.

Note: Don’t restore from a backup file or it the issue could happen again.   Manually reconfigure as desired.

IPTABLES (desire to filter packets from getting into the SecureSync/9400s)

- Ability to edit IPtables was added in update version 5.4.0
- Configuration is only available via the CLI (not available via the web browser)
- Can only make security stronger than factory default (can't make security less restrictive than factory default)

Prior to version 5.4.0 update: IPtables couldn't be edited as spadmin

- Email Keith sent to Dave Sohn: "This SecureSync customer wants to access the SecureSync's IPTables to block access to malicious IPs".

A. reply from Dave Soihn (6 Jan 2016) "Access to IPTABLES is not available to a customer in the SecureSync. The access control feature blocks access to the unit services, but doesn't filter the packets."

From Wikipedia: iptables is a user-space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall (implemented as different Netfilter modules) and the chains and rules it stores. Different kernel modules and programs are currently used for different protocols; *iptables* applies to IPv4, *ip6tables* to IPv6, *arptables* to ARP, and *ebtables* to Ethernet frames.

Permissons to edit IPTables

Note: Customers can't type "**sudo su iptables**" (which will prompt for login to root).

need to type "sudo" before each command

A) Versions 5.4.5 and above:

- Starting in v5.4.5, spadmin now has rights to run iptables. No longer need to type "sudo" in front of "iptables" to edit the tables (now just type **iptables xxxx**)

B) Versions 5.4.1 and below:

- As of at least v5.4.0, only spadmin account (not custom user accounts) has permission to edit.

Saving changes to the IPtables

- In at least versions 5.5.1 and below, the IPtables are not saved/do not persist through a reboot/power cycle. The changes need to be re-configured after each boot-up.
- This is expected to be addressed in a future release – as of 20 March 17, it has not yet been determined when the saving of changes will be implemented. Refer to JIRA cases **SSS-523** and **SSS-238** for details

Work-around to save changes to IPTables

email from Pritam to Morgan (10 Sept 2018) There is workaround for users to save the iptable rules permanently and have it run when the system reboots:

1. Customer can create a shell script that contains the desire iptables rules.
2. Save this scripts as file in the home directory and give the user executable permission to the file.
3. Run this script via cron, whenever the system gets rebooted, with crontab entry of something like below:

```
@reboot /home/spectracom/firewall.bash
```

Let me know if I can assist you with the how-to process in person.

Operation of editing IPtables

- Consists of editing tables containing of chains of rules for the treatment of packets
- Each table is associated with a different kind of packet processing.
- Packets are processed by sequentially traversing the rules in chains. A rule in a chain can cause a goto or jump to another chain, and this can be repeated to whatever level of nesting is desired. (A jump is like a “call”, i.e. the point that was jumped from is remembered.) Every network packet arriving at or leaving from the computer traverses at least one chain.
- Each rule specifies what to do with a packet that matches. This is called a `target', which may be a jump to a user-defined chain in the same table.

The five indivual tables are as follows:

filter: This is the default table (if no -t option is passed). It contains the built-in chains INPUT (for packets destined to local sockets), FORWARD (for packets being routed through the box), and OUTPUT (for locally-generated packets).

nat: This table is consulted when a packet that creates a new connection is encountered. It consists of three built-ins:

PREROUTING (for altering packets as soon as they come in)

OUTPUT (for altering locally-generated packets before routing), and

POSTROUTING (for altering packets as they are about to go out).

mangle: This table is used for specialized packet alteration. Until kernel 2.4.17 it had two built-in chains: PREROUTING (for altering incoming packets before routing) and OUTPUT (for altering locally-generated packets before routing). Since kernel 2.4.18, three other built-in chains are also supported: INPUT (for packets coming into the box itself), FORWARD (for altering packets being routed through the box), and POSTROUTING (for altering packets as they are about to go out).

raw: This table is used mainly for configuring exemptions from connection tracking in combination with the NOTRACK target. It registers at the netfilter hooks with higher priority and is thus called before ip_conntrack, or any other IP tables. It provides the following built-in chains: PREROUTING (for packets arriving via any network interface) OUTPUT (for packets generated by local processes)

security: This table is used for Mandatory Access Control (MAC) networking rules, such as those enabled by the SECMARK and CONNSECMARK targets. Mandatory Access Control is implemented by Linux Security Modules such as SELinux. The security table is called after the filter table, allowing any Discretionary Access Control (DAC) rules in the filter table to take effect before MAC rules. This table provides the following built-in chains: INPUT (for packets coming into the box itself), OUTPUT (for altering locally-generated packets before routing), and FORWARD (for altering packets being routed through the box).

TARGETS

A firewall rule specifies criteria for a packet and a target. If the packet does not match, the next rule in the chain is the examined; if it does match, then the next rule is specified by the value of the target, which can be the name of a user-defined chain or one of the special values ACCEPT, DROP, QUEUE or RETURN.

ACCEPT means to let the packet through.
DROP means to drop the packet on the floor.
QUEUE means to pass the packet to userspace. (How the packet can be received by a userspace process differs by the particular queue handler. 2.4.x and 2.6.x kernels up to 2.6.13 include the ip_queue queue handler. Kernels 2.6.14 and later additionally include the nfnetlink_queue queue handler. Packets with a target of QUEUE will besent to queue number '0' in this case. Please also see the NFQUEUE target as described later in this man page.)

RETURN means stop traversing this chain and resume at the next rule in the previous (calling) chain. If the end of a built-in chain is reached or a rule in a built-in chain with target RETURN is matched, the target specified by the chain policy determines the fate of the packet.

Configuration of iptables

Note: Can lock yourself out if not careful.   If this happens, can either:

- (in at least versions 5.5.1 and below), since the changes to IPtables don't persist through reboots, just reboot the unit to restore the original configurations and regain access.
- Perform a standard **Clean** or **use the front panel Serial port** to edit the tables back to the default configuration (IPtables don't affect the serial port conerction).

This function uses the standard linux commands to edit the table. Refer to sites such as:
http://ipset.netfilter.org/iptables.man.html or
https://fedoraproject.org/wiki/How_to_edit_iptables_rules

IPtables is located in the **/sbin** directory (cd to this directory)

iptables -h returns iptables help menu

(versions 5.4.1 and below, need to type Sudo at the beginning of each command

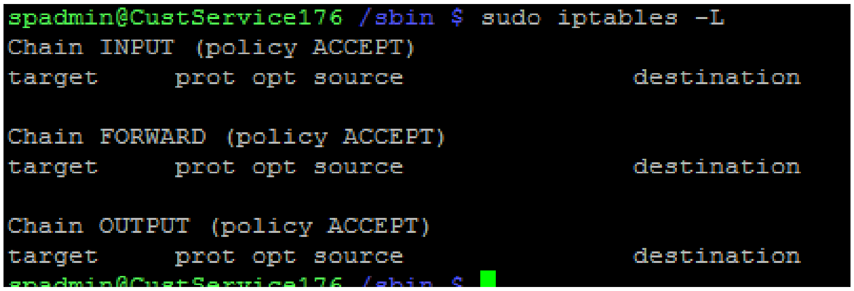
A) Software versions 5.4.5 and above:

- No longer need to type *sudo* in each command (spadmin was give the right to edit iptables starting in update version 5.4.5).
- For example, to list all the current Rules, type: **iptables -L** **(**or **iptables -list**)

B) Software versions 5.4.1 and below:

- have to type **sudo** before each command to have root priveledge

To list all the current Rules, type: **sudo iptables -L** **(**or **sudo iptables -list**)



```
spadmin@CustService176 /sbin $ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
spadmin@CustService176 /sbin $
```

Format for Adding a rule (Note: info below shows "**sudo**" in front of all commands. This word only needs to be typed in versions 5.4.1 and below. Omit this word in versons 5.4.5 and above)

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

(**Append** to Input chain a rule that **accepts** TCP port 80 packets)

Where:

-A is to **Append** a new rule to the chain

INPUT is the chain to be edited

-dport defines the port

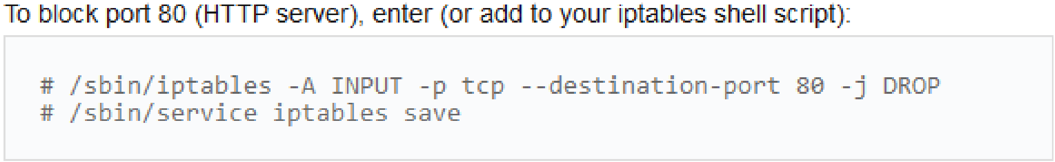
-j indicates the target (can be: ACCEPT DROP QUEUE or RETURN)

Now display the new rules: **sudo iptables -L**

Blocking an incoming or outgoing port (such as port 80 for HTTP, or 123 for NTP) on a particular interface (such as just eth0)

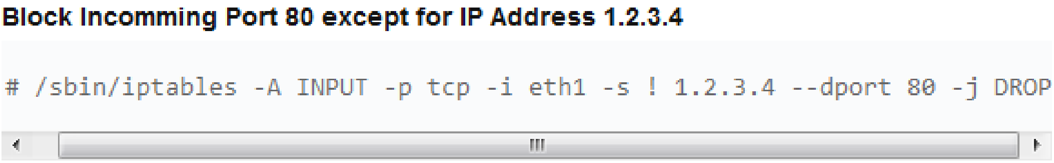
1. Refer to: http://www.cyberciti.biz/faq/iptables-block-port/ (also below)

A) Block incoming packets



To block port 80 (HTTP server), enter (or add to your iptables shell script):

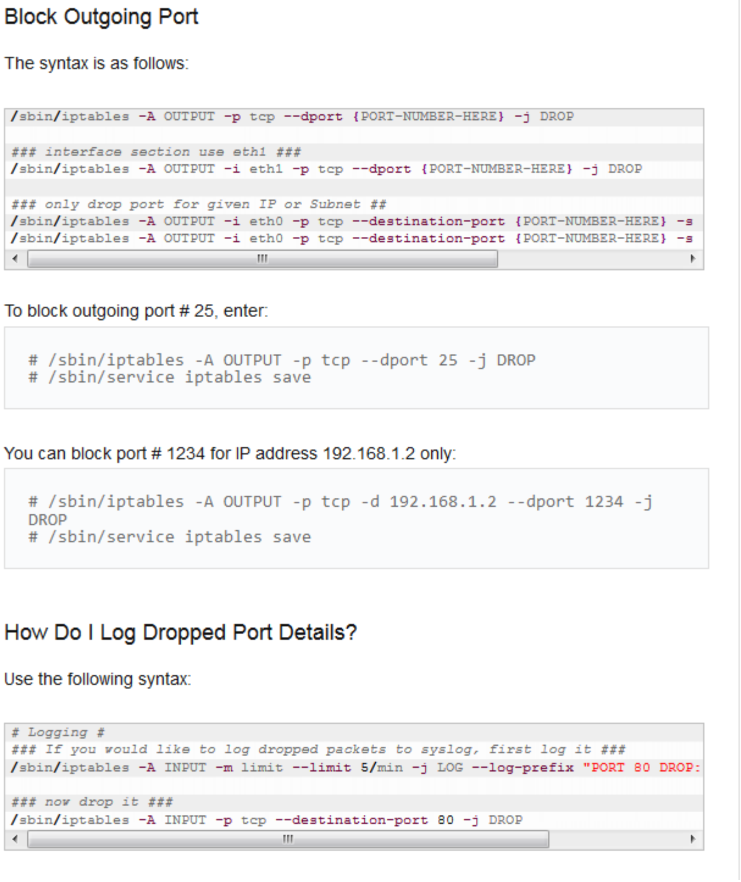
```
# /sbin/iptables -A INPUT -p tcp --destination-port 80 -j DROP
# /sbin/service iptables save
```



Block Incomming Port 80 except for IP Address 1.2.3.4

```
# /sbin/iptables -A INPUT -p tcp -i eth1 -s ! 1.2.3.4 --dport 80 -j DROP
```

B) Block outgoing packets



Block Outgoing Port

The syntax is as follows:

```
/sbin/iptables -A OUTPUT -p tcp --dport {PORT-NUMBER-HERE} -j DROP

### interface section use eth1 ###
/sbin/iptables -A OUTPUT -i eth1 -p tcp --dport {PORT-NUMBER-HERE} -j DROP

### only drop port for given IP or Subnet ##
/sbin/iptables -A OUTPUT -i eth0 -p tcp --destination-port {PORT-NUMBER-HERE} -s
/sbin/iptables -A OUTPUT -i eth0 -p tcp --destination-port {PORT-NUMBER-HERE} -s
```

To block outgoing port # 25, enter:

```
# /sbin/iptables -A OUTPUT -p tcp --dport 25 -j DROP
# /sbin/service iptables save
```

You can block port # 1234 for IP address 192.168.1.2 only:

```
# /sbin/iptables -A OUTPUT -p tcp -d 192.168.1.2 --dport 1234 -j
DROP
# /sbin/service iptables save
```

How Do I Log Dropped Port Details?

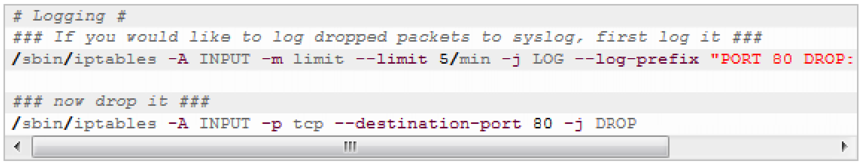
Use the following syntax:

```
# Logging #
### If you would like to log dropped packets to syslog, first log it ###
/sbin/iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "PORT 80 DROP:

### now drop it ###
/sbin/iptables -A INPUT -p tcp --destination-port 80 -j DROP
```

C) Logging dropped port details

How Do I Log Dropped Port Details?

Use the following syntax:



```
# Logging #
### If you would like to log dropped packets to syslog, first log it ###
/sbin/iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "PORT 80 DROP:

### now drop it ###
/sbin/iptables -A INPUT -p tcp --destination-port 80 -j DROP
```

**IPv6 addresses (such as SLAAC address / Link-Local address. Global unicast address)

- **Refer to** “IPv6 addresses (for all products that support IPv6)” in custserviceassst doc: I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf
  - Contains info on the four types of IPv6 addresses (Global unicast, Link-local, unique local addresses, and Special addresses)

IPv6 status

(23 Jan 2013): there are a few Mantis cases open regarding the support of IPv6 addresses. These include:

1722: Issues with IPv6 addresses not being stored and no current support for IPV6 Radius

Update to this case (4 Apr 2013) Per Dave Sohn: The pam_auth_radius module we use does not support IPv6. There is an IPv6 patch for it that would need to be tested. So the answer is we do not support IPv6 RADIUS at this time.

1849/1897: Syslog not working with IPv6 addresses.
Status update per Dave Sohn (8 Mar 2013): “Our current syslog package does not support IPv6. Either a new package/version or patch are required.” (This is recorded in Mantis case 1897)

1897/1937: Does the **gateway address** IPv6 Default Gateway”, support IPv6? Update- Starting in v4.8.9, the main default gateway does support IPv6 addresses. 1937 is now resolved.

1937 -> 1963: IPv6 static routes, “desire to configure the IPv6 addresses on the NTP server to ping to another device using different IPv6 subnet

Update:

- Mantis 1937 was split off to 1963 to be able to close 1937.
- Mantis 1963 for static routes is still open as of Nov 5. 2014.

Summary of IPv6 status as of Archive software version 4.8.9

Note (Sept 2014 Update to the info below) Version 5.1.2 added ipv6 DHCP functionality and SLAAC address

Email Keith sent to Matt Loomis (16 Apr 2013) and OK’d by Dave Sohn:

1) All **four available network ports** can be assigned IPv4 and/or IPv6 addresses (all of the ports support simultaneous IPv4 and IPv6 addressing).
2) With the exception of NTP Autokey, **NTP** supports IPv6.
3) The main **default gateway** can be IPv4 or IPv6 (added in v4.8.9 software update). However**, we don’t currently support IPv6 static routes** (likely added later this year- Q3 or Q4 expected). Until these are implemented, if the IPv6 network(s) are connected directly to the SecureSync, they are all set. But if they are on subnets not directly connected, we will send unsolicited traffic out on Eth0 instead of to the Ethernet port that routes to the subnet. If they send a packet to the NTP server, we can route back to the correct network port that the packet was received on.
4) **Syslog** does not support IPv6. This will require either a patch or a new version of the package that we use for this function. Probally not going to be available for a while.
5) Cannot disable IPv6 Auto configuration.

Additional Note (not included in email to Matt): We do not support IPv6 Radius at this time.

**Main Default port/main default Gateway address

This tab of the browser is used to configure network settings for when network traffic originates inside of the SecureSync (instead of responding to traffic that was received. Examples of this include NTP broadcast mode or SNMP traps).

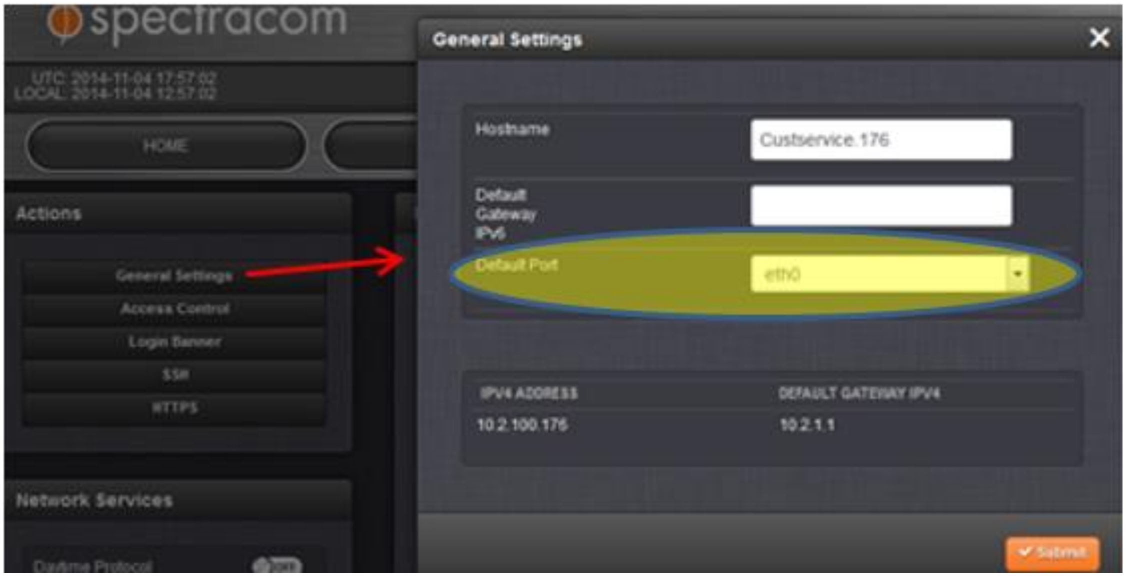
Main Default Gateway address is configured in the:

A) Classic Interface browser

Network -> **General Setup** page of the browser, **General** tab

B) Newer black/charcoal browser (v5.1.2 and above):

- **Management** -> **Network** page of the browser, "**General Settings**" button (on the left side of the screen):



Hostname: Custservice 176

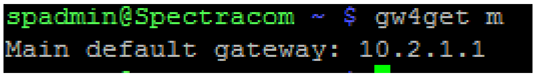
Default Gateway IPv6:

Default Port: eth0

IPV4 ADDRESS	DEFAULT GATEWAY IPV4
10.2.100.176	10.2.1.1

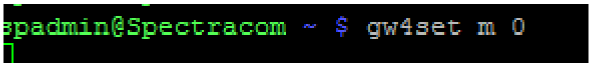
C) Configuring the main default gateway via the CLI interface

- **CLI command** to read which port is the main default gateway: **gwget <enter>** (the response is inside the parenthesis)



```
spadmin@Spectracom ~ $ gw4get m
Main default gateway: 10.2.1.1
```

- **CLI command** to set which port is the main default gateway: **gw4set m x <enter>** (where **m** is for "main" w and **x** is the Ethernet interface port number configured withthe desired main default gateway addres)



```
spadmin@Spectracom ~ $ gw4set m 0
```

Example to make the default gateway port as port 2: **gw4set m 2 <enter>**

- **CLI command** to set the default gateway for a particular port (not the main default gateway) the command is **gw4set m 2 <enter>** (where **x** specifies the main default gateway port is being configured, and **2 is** the interface having the desired gateway address.

Difference between the global gateway address and the interface gateway addresses

(9/27/12 Email from Dave Sohn to Sylvain) The gateway answer is also fairly easy. It is the difference between a global and interface gateway address. The unit will use the interface specific gateway to determine where to send packets outside of its subnet if the packet came in on that interface. The unit will use the global gateway to determine where to send packets outside of its subnet if the packet is being generated independently by the SecureSync.

Issues with setting the main default gateway port via the newer black/charcoal web browser

- Refer to Mantis cases 3086 and 2788
- 3086 is associated with at least v5.2.1 and 2788 associated with 5.1.3 to 5.2.0??
- Changing back to eth0 seems ok. But it doesn't like selecting eth 1, 2 or 3.
- Work-around is to use the cli command of **gw4set m x** <enter> (where m stands for "main" and where x is the desired port to use as gateway)

Note about IPv6 Default gateway address field: versions 4.8.8 and below have an issue with being able to configure this field. It was addressed in the version 4.8.9 release (March 2013).

Validation error when trying to configure the Default gateway

Email from Keith to Roots (3 Apr 2013) Thanks for reporting their observation to us.

In order to configure the IPv6 default main gateway, all of the individual IPv6 network settings need to first be properly configured. When the IPv6 default gateway address is attempted to be configured, the SecureSync performs system checks to ensure the entered gateway address is both valid and reachable, based on the interface settings (as configured in the **Network** -> **Interfaces** page of the browser, the tabs for each of the network ports).

If your customer has not yet configured each of the network ports yet and don't have the SecureSync connected to the network that the gateway is on, please have them retry entering the IPv6 after they have configured the other settings. If it then accepts the gateway address, just let me know they are all set.

However, if they still get a validation error, please have them send us screenshots of all the tabs in the **Network** -> **Interfaces** page of the browser, as well as a screenshot of the **Network** -> **General Setup** page of the browser, General tab. We will review the values they are entering to try to determine why they are seeing a validation error.

**Interface gateway addresses (IPv4/IPv6)

Note: Used for responding to received network traffic (not used for broadcast traffic)

A) IPv4 gateway addreses

Newer (black/charcoal browser) browser: **Network** -> **Interfaces** page

Each of the tabs (eth 0 always- eth1, eth2, and eth3 when Gigabit card installed) on this page of the browser are used to configure network settings of each network port for when SecureSync is responding to network traffic that it receives (Examples of this include NTP unicast mode or web browser).

Difference between the global gateway address and the interface gateway addresses

(9/27/12 Email from Dave Sohn to Sylvain) The gateway answer is also fairly easy. It is the difference between a global and interface gateway address. The unit will use the interface specific gateway to determine where to send packets outside of its subnet if the packet came in on that interface. The unit will use the global gateway to determine where to send packets outside of its subnet if the packet is being generated independently by the SecureSync.

DHCP: Enable/Disable DHCP on each port

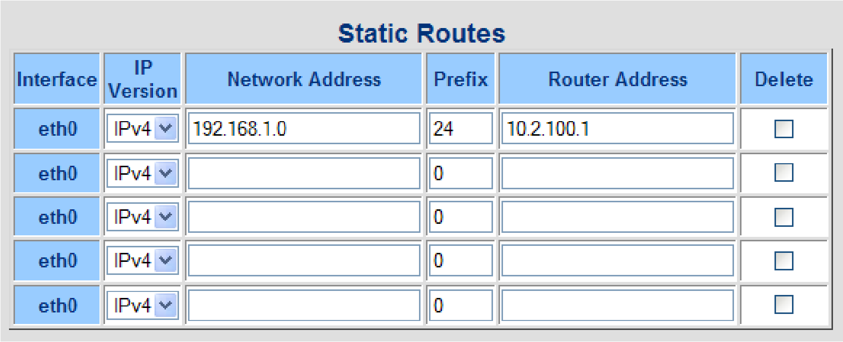
DNS Setup: Defines DNS servers on this particular port's network

Domain Setup: Not the DNS Host name (this is defined elsewhere) example: roc.spectracom.us

IP Address setup: Define the IPv4 address or IPv6 addresses for each port.

"Static Routes" table in each tab: Used to define networks on other side of routers that are attached to any or all of the Ethernet ports (but are not available through the default gateway). "Network address" will likely end in 0's (don't include the "/" and bits to define the subnet mask. These are entered with just the number in the "Prefix field". Enter the router's IP address in the "Router Address" field.

In the example screenshot below, Eth 0 has a router at 10.2.100.1 that is also attached to a 192.168.1.x network. And, it's desired for responses to network traffic to be sent to this other subnet.



Static Routes

Interface	IP Version	Network Address	Prefix	Router Address	Delete
eth0	IPv4	192.168.1.0	24	10.2.100.1	□
eth0	IPv4		0		□
eth0	IPv4		0		□
eth0	IPv4		0		□
eth0	IPv4		0		□

Desire to "reset" one particular non-DHCP network port (without having to reboot)

(10/23/12 KW) Based on feedback from Dave Sohn, reply to a customer

The SecureSync doesn't have a command/button to explicitly bring down or up the individual network interfaces (Eth0 through Eth3). Besides performing a system reboot (or power cycle), you may be able to restore the network port operation by simply enabling and then disabling DHCP for the one particular network interface.

DHCP can be toggled in the **Network** -> **Interfaces** page of the web browser. Then, select the "Eth1" tab for instance. There is an ON/OFF button to turn DHCP on and off.

If toggling DHCP for the port doesn't restore network connectivity, we would then recommend a reboot of the system (This can be performed in the **Tools** -> **Reboot/Halt** page of the browser. Press the **Reboot** button to perform the reboot. The system will be back up and running in about two minutes or so (and synced a couple of minutes thereafter).

Network switch settings for interfacing with SecureSync

Q. (from Gregory with BellAlliant) I'm wondering if the Ethernet ports need anything special parameters? The Alcatel is set force the 1 Gbps speed using the Auto negotiate limit function.

A. (reply from Dave Sohn 22 Jan 2013) I'm not aware of restrictions or configuration requirements for either the 10/100 or Gigabit ports. The pause frames wouldn't be a result of misconfiguration, but they could show an issue. I couldn't find anything definitive in the gigabit driver bug reports about flow control autonegotiation. If they are causing problems maybe we need to disable them, but I'm not sure at this point.

Q. (from Gregory with BellAlliant) I've learned that the Alcatel switch has the ports that are facing the NTP servers set to "auto-negotiate limited", which restricts some of the features that are to be negotiated.

Do you have a specification document that describes the Gigabit Ethernet (3X) module options that need to be active or disabled when the Layer 2 connection is to be made between the NTP's interface and another interface (or Alcatel switch in this case)?

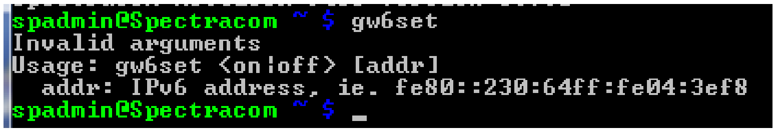
Also, can we control the layer 2 options that are active or disabled from the CLI of the NTP?

B) IPv6 gateway addresses

NOTICE: IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 netwok while configuring. Otherwise the config changes won't be accepted.

Gw6set command/Configuring IPv6 gateway address using link-local address

- Command to configure IPv6 gateway address is: **gw6set on/off xxxx:xxxx:xxxx:xxxx:xxx**



```
spadmin@Spectracom ~ $ gw6set
Invalid arguments
Usage: gw6set <on|off> [addr]
  addr: IPv6 address, ie. fe80::230:64ff:fe04:3ef8
spadmin@Spectracom ~ $ _
```

"Failed to enable or disable the IPv6 default gateway" reported

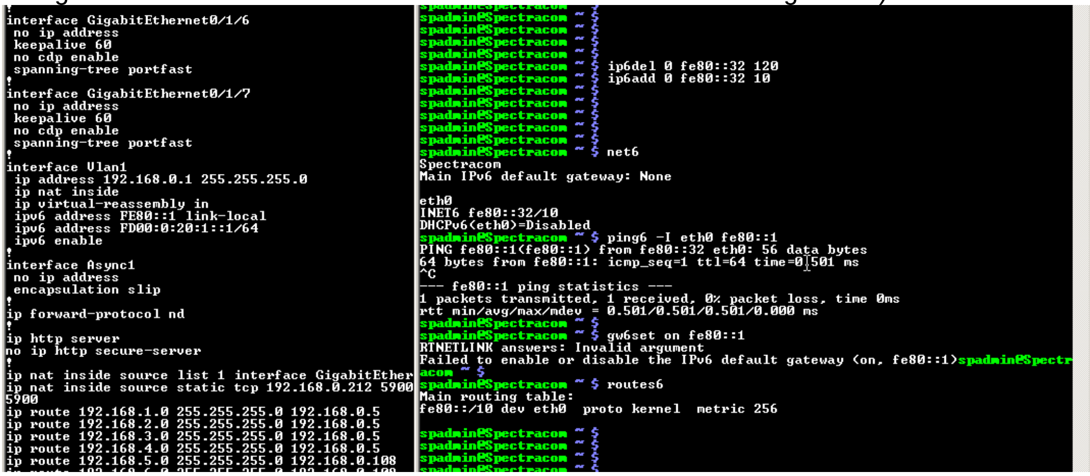
- Issue with setting IPv6 gateway address using the 'link-local' IPv6 address (works when using the Global address but not when using the link-local address)
- Refer to SF case 115892/JIRA SSS-350
- Applicable to versions 5.7.2 and below. Fixed in v5.7.3 (with 5.8.0 being the next subsequent general release)

from the v5.7.3 release notes:
Updated IPv6 networking support to more closely match IPv4 networking. Added additional routing tables per network port with individual IPv6 default gateways. Static IPv6 routes can be applied per network port.

Email from Dave Sohn (1 Aug 17) Routing is typically not done within the link-local address space, but we did find a bug in the gw6set function when used with link-local gateway addresses. It will have to be resolved in a future SW update. There is no workaround for utilizing the link-local address at this time. The only workaround is to setup IPv6 static addresses on the SecureSync and the gateway device and use that for the gateway setting.

From the original report email thread from Nori w/TOYO (1 Aug 17)

(The assigned link-local address is shown on the left-side off the below screenshot. The customer entering the gw6set command wih the link-local address is shown on the right-side).



```
!
interface GigabitEthernet0/1/6
 no ip address
 keepalive 60
 no cdp enable
 spanning-tree portfast
!
interface GigabitEthernet0/1/7
 no ip address
 keepalive 60
 no cdp enable
 spanning-tree portfast
!
interface Vlan1
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 ipv6 address FE80::1 link-local
 ipv6 address FD00:0:20:1::1/64
 ipv6 enable
!
interface Async1
 no ip address
 encapsulation slip
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
ip nat inside source list 1 interface GigabitEther
ip nat inside source static tcp 192.168.0.212 5900
5900
ip route 192.168.1.0 255.255.255.0 192.168.0.5
ip route 192.168.2.0 255.255.255.0 192.168.0.5
ip route 192.168.3.0 255.255.255.0 192.168.0.5
ip route 192.168.4.0 255.255.255.0 192.168.0.5
ip route 192.168.5.0 255.255.255.0 192.168.0.108
```

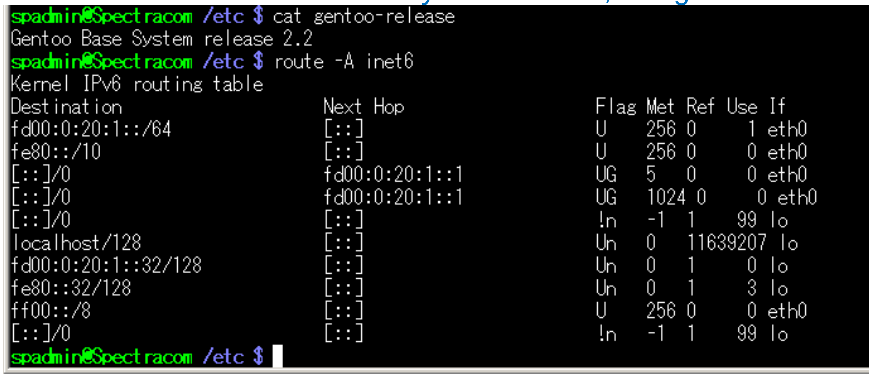
```
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $ ip6del 0 fe80::32 120
spadmin@Spectracom ~ $ ip6add 0 fe80::32 10
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $ net6
Spectracom
Main IPv6 default gateway: None

eth0
INET6 fe80::32/10
DHCPv6(eth0)=Disabled
spadmin@Spectracom ~ $ ping6 -I eth0 fe80::1
PING fe80::1(fe80::1) from fe80::32 eth0: 56 data bytes
64 bytes from fe80::1: icmp_seq=1 ttl=64 time=0.501 ms
^C
--- fe80::1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.501/0.501/0.501/0.000 ms
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $ gw6set on fe80::1
RTNETLINK answers: Invalid argument
Failed to enable or disable the IPv6 default gateway (on, fe80::1)spadmin@Spectr
acom ~ $
spadmin@Spectracom ~ $ routes6
Main routing table:
fe80::/10 dev eth0  proto kernel  metric 256

spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
```

Yes, the customer certainly had connected the SecureSync demo unit to their IPv6 gateway. (FE80::1) Actually, the customer and we could properly apply IPv6 global addresses as gateway, of course we had established physical connection between the unit and the gateway before starting the setup.

We still have an issue that we cannot use link-local addresses for the gateway settings.
Perhaps is there a limitation to use link-local addresses for IPv6 gateway in the SecureSync?

Or, as one of workaround, can we add manually new gateway settings using general linux commands as superuser?

[Current route table of our SecureSync demo unit, two global addresses have been applied as gateway]



```
spadmin@Spectracom /etc $ cat gentoo-release
Gentoo Base System release 2.2
spadmin@Spectracom /etc $ route -A inet6
Kernel IPv6 routing table
Destination                    Next Hop                   Flag Met Ref Use If
fd00:0:20:1::/64               [::]                       U    256 0     1 eth0
fe80::/10                      [::]                       U    256 0     0 eth0
[::]/0                         fd00:0:20:1::1             UG   5   0     0 eth0
[::]/0                         fd00:0:20:1::1             UG   1024 0     0 eth0
[::]/0                         [::]                       !n   -1  1    99 lo
localhost/128                  [::]                       Un   0   11639207 lo
fd00:0:20:1::32/128            [::]                       Un   0   1     0 lo
fe80::32/128                   [::]                       Un   0   1     3 lo
ff00::/8                       [::]                       U    256 0     0 eth0
[::]/0                         [::]                       !n   -1  1    99 lo
spadmin@Spectracom /etc $
```

Email from Dave Sohn (1 Aug 17) (referring to software version 5.7.0) Routing is typically not done within the link-local address space, but we did find a bug in the gw6set function when used with link-local gateway addresses. It will have to be resolved in a future SW update. There is no workaround for utilizing the link-local address at this time. The only workaround is to setup IPv6 static addresses on the SecureSync and the gateway device and use that for the gateway setting.

IPv6 Gateway will not save (observed in v5.4.1 and subsequent versions

- Observed/reported in Jun, 2016 with version 5.4.1 installed
- Refer to Mantis case 3276 and SR 5309 in SAP
- Issue with browser only. Works fine with the CLI interface.

Email from Dave Sohn (8 Jun 16) As I stated in our call, the summary is that the IPv6 default gateway configuration using the web UI is not working on SecureSync. The command line interface IPv6 default gateway configuration does work. There are two locations in the web UI to set a default IPv6 gateway and they both have issues. The IPv6 main default gateway setting under the “General Settings” in the network configuration page does not correctly set the gateway in the live configuration or the configuration file. The IPv6 default gateway setting under the per port configuration page, does a set to a routing table setup per port, but those routing tables are not used by the system, and It also does not set the configuration file correctly. However, due to how the gateway is read on the cli, when the per port default gateway is set in the incorrect table, it is read by the command line interface get (gw6get), adding to the confusion. For units that you may have already gotten into this state, this can be cleared by clearing the per port IPv6 gateway field and submitting. You should see the command line interface get (gw6get) return “None” again. Once it returns “None”, you can correctly utilize the command line gateway set (gw6set) command to correctly set the IPv6 main default gateway for the unit. Let us know how this goes tomorrow night, once you can make the attempt during the maintenance window, and we are sorry for the confusion and issues this created.

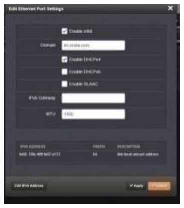
Email Dave Lorah sent to the customer

We have confirmed a problem in the web browser settings of the IPv6 parameters. A workaround for setting up an IPv6 Gateway in the Securesync.

The summary is that the IPv6 default gateway configuration using the web UI is not working on SecureSync. However, the command line interface IPv6 default gateway configuration does work.

There are two locations in the web UI to set a default IPv6 gateway and they both have issues. The IPv6 main default gateway setting under the “General Settings” in the network configuration page does not correctly set the gateway in the live configuration or the configuration file. The IPv6 default gateway setting under the per port configuration page, does a set to a routing table setup per port, but those routing tables are not used by the system, and It also does not set the configuration file correctly. However, due to how the gateway is read on the cli, when the per port default gateway is set in the incorrect table, it is read by the command line interface get (gw6get), adding to the confusion. For units that you may have already gotten into this state, this can be cleared by clearing the per port IPv6 gateway field and submitting.

For each Ethernet port, make sure the IPv6 Gateway Field is blank and SUBMIT:



Edit Ethernet Port Settings

☑ Enable v6

Domain

☑ Enable DHCPv4

□ Enable DHCPv6

□ Enable SLAAC

IPv6 Gateway

MTU 1500

After clearing the settings in the web UI you should see the command line interface get (gw6get) return “None” again. Once it returns “None”, you can correctly utilize the command line gateway set (gw6set) command to correctly set the IPv6 main default gateway for the unit.

SLAAC address for IPv6

- Refer to: http://en.wikipedia.org/wiki/IPv6_address#Stateless_address_autoconfiguration

On system startup, a node automatically creates a link-local address on each IPv6-enabled interface, even if globally routable addresses are manually configured or obtained through "configuration protocols" (see below). It does so independently and without any prior configuration by stateless address autoconfiguration (SLAAC),[29] using a component of the Neighbor Discovery Protocol. This address is selected with the prefix `fe80::/64`.

NOTICE: IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 netwok while configuring. Otherwise the config changes won't be accepted.

Software changes associated with SLAAC addresses

A) Version 5.7.3

- Corrected bug in enabling/disabling IPv6 SLAAC

B) Version 5.1.2

- Added support for IPv6 DHCP functionality and SLAAC addresses.

FAQs about SLAAC

Q. Can you check with the team and ask them for a short description on what they had to change/add to the code to allow for SLAAC to be disabled.

A. **(per Dave Sohn 29 Aug 2014)** We added code to modify our Linux kernel parameters per interface to ignore IPv6 router advertisements, which generate the SLAAC addresses when received.

Q So, the systems are responding after using the "gw6set" commands. But the underlying issues of the following are still a problem, per se:

1) missing CONFIG_ROUTES_IPV6_MAIN value. This remains blank no matter how it is set (GUI or CLI)
2) SLAAC picks up incorrect gateway, uses link-local IPv6 address
3) "General Settings" dialog to set the IPv6 gateway always comes up blank, and doesn't seem to set that value in /etc/conf.d/net. This can be confusing.

It seems the GUI is not a reliable way to set the IPv6 gateway.

A reply from Dave L (16 Jun 17) The way it was explained to me is the IPv6 routing functions are not enabled in the Securesync but there is capability to enter the Gateway address. The IPv4 routing is functional but the same routing functions for IPv6 are not. So you cannot use the same "routes" commands as IPv4.

The gw6set and gw6get are the only parameters that can be used. We are working on cleaning this up for the next firmware release. I expect it will be ready in 2 to 3 weeks.

These commands are not valid:

Rt6add
Rt6get
Rt6del
Routes6

Also, do not enter a gateway address in the web browser IPv6 gateway field. This will also cause a problem.

A reply from Dave L (16 Jun 17) Your first question was answered in my previous email. Yes, the GUI is not functional for configuring the IPv6 gateway.

The SLAAC function can be explained by this: The SecureSync automatically generates a link-local address that is based on the hardware MAC address. In general, machines using IPv6 will typically have several addresses, one of which is usually a link-local address. The SecureSync does not currently have support for permanently turning off the link-local address. It can be deleted, but will be recreated whenever the interface link is brought up or the system is rebooted. You may use your static IP address but the auto configured link-local address will be there as well.

NOTICE: IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 netwok while configuring. Otherwise the config changes won't be accepted.

Static Routes/ Default Routes /Static Routing/ Routing tables

From Wikipedia: Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing protocol to forward traffic. In many cases, static routes are usually manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case. Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured.

Info below from: http://www.cs.virginia.edu/~itlab/book/pdf/Ch3_v3.pdf

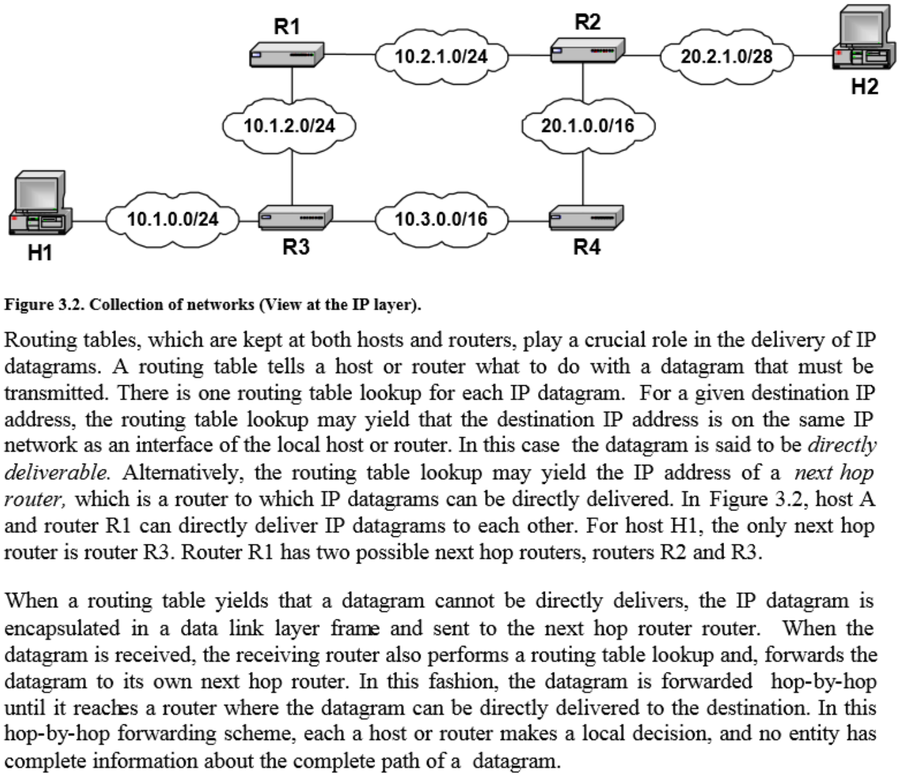

R1
R2
10.2.1.0/24
20.2.1.0/28
H2
10.1.2.0/24
20.1.0.0/16
10.1.0.0/24
10.3.0.0/16
H1
R3
R4

Figure 3.2. Collection of networks (View at the IP layer).

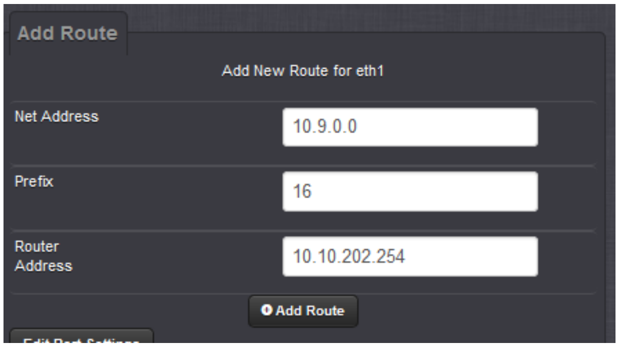
Routing tables, which are kept at both hosts and routers, play a crucial role in the delivery of IP datagrams. A routing table tells a host or router what to do with a datagram that must be transmitted. There is one routing table lookup for each IP datagram. For a given destination IP address, the routing table lookup may yield that the destination IP address is on the same IP network as an interface of the local host or router. In this case the datagram is said to be *directly deliverable*. Alternatively, the routing table lookup may yield the IP address of a *next hop router*, which is a router to which IP datagrams can be directly delivered. In Figure 3.2, host A and router R1 can directly deliver IP datagrams to each other. For host H1, the only next hop router is router R3. Router R1 has two possible next hop routers, routers R2 and R3.

When a routing table yields that a datagram cannot be directly delivers, the IP datagram is encapsulated in a data link layer frame and sent to the next hop router router. When the datagram is received, the receiving router also performs a routing table lookup and, forwards the datagram to its own next hop router. In this fashion, the datagram is forwarded hop-by-hop until it reaches a router where the datagram can be directly delivered to the destination. In this hop-by-hop forwarding scheme, each a host or router makes a local decision, and no entity has complete information about the complete path of a datagram.

- Static routes are used to route unrequested broadcast type packets (such as SNMP Traps for example) to the appropriate network, if no Static Routes are defined.
- Not required for responding to packets that originate from outside SecureSync (such as NTP packets)
- They are used to route unrequested packets (such as SNMP Traps for example) to the applicable network port on the SecureSync (if not being sent to the Default gateway address).
- Not required for packets that originate from outside SecureSync (such as NTP packets)
- If there are no Static Routes defined, unrequested packets (such as SNMP traps) will be routed to the Default Gateway address (defined towards the top of the same page of the browser)

Example for a static route to be used:

1. **Eth0** is the configured default port/gateway address (its gateway is 10.2.1.1)
2. But an internally generated packet (not respoding to an incoming packet) needs to go out **eth1** instead of **eth0** (example- the address it needs to go to is **10.9.3.4 /16**, via eth1s gateway address of **10.10.202.254**)
3. Normally, the packets would go out eth0 (the defaultgateway). So a statc route needs to be configured in eth1 that tells it to route this address/subnet (such as **10.9.0.0** va eth1's gateway address of **10.10.202.254** with a prefix of **16**

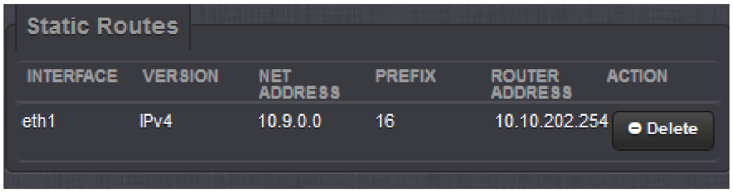


Add Route

Add New Route for eth1

Net Address	10.9.0.0
Prefix	16
Router Address	10.10.202.254

After pressing “**Add Route**”



Static Routes

INTERFACE	VERSION	NET ADDRESS	PREFIX	ROUTER ADDRESS	ACTION
eth1	IPv4	10.9.0.0	16	10.10.202.254	Delete

Notes about static routes

1. The SecureSync’s static routes are just to get packets to the correct Ethernet interface’s gateway address, if it can’t be handled by the default gateway/port (doesn’t care about routing of the packet after the default gateway sincie this is handled by the routing tables in the routers themselves).

Configuring/Viewing default static routes (IPv4 and IPv6)

A) IPv4 static routes (for eth0, eth1, eth2 or eth3)

- **Note**: info regarding **IPv6 static routes** is **futher below** in a separate section

IPV4 static routes were added in version 4.6.0

- From the update 4.6.0 Release Notes:

  “Added Static Route control for all interfaces and a main/common route section”

IPv4 Static Routes can be displayed/configured via either the web browser or via CLI commands

- refer to the SecureSync CLI section of the document for the commands associated with static route, such as **routes4**, **rt4add**, **rt4del** and **rt4get**.

IPv6 Static Routes can be displayed/configured via either the web browser or via CLI commands

NOTICE: IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 netwok while configuring. Otherwise the config changes won’t be accepted.

- refer to the SecureSync CLI section of the document for the commands associated with static route, such as **routes3**, **rt5add**, **rt6del** and **rt6get**.
- **rt6add**: Adds an IPv6 static route.
- **rt6del**: Deletes IPv6 static route.
- **rt6get**: Displays the configured IPv6 routes.
- **routes6**: Displays the current IPv6 routing table(s)

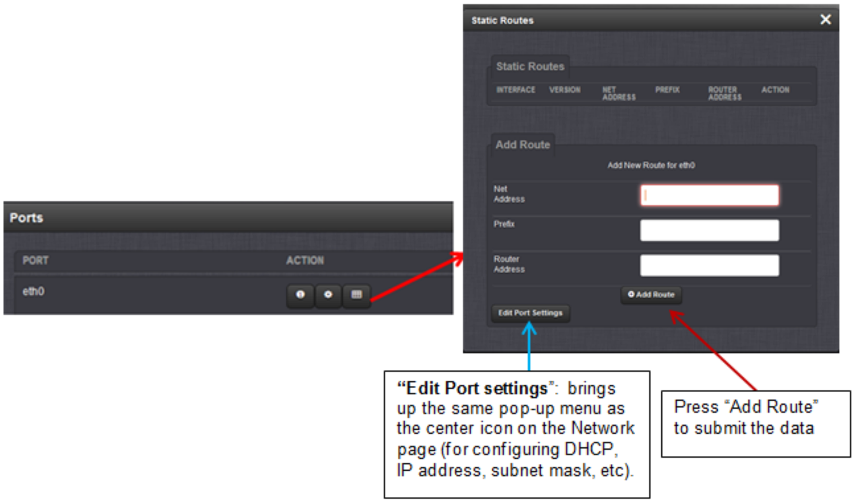
Configuring IPv4 static routes

- ➢ Static routes can be configured via ether:
  - The newer browser (refer to “**A**” below):
  - The CLI interface (refer to “**B**” below):

B) Configuring IPv4 static routes using newer web browser (software versions 5.1.2 and above):

- ➢ Navigate to the Management -> Network page of the browser
- ➢ Click on the third (“table”) icon for the applicable eth0, eth1, eth2 or eth3 interface port that it’s desired to add the route.

1. In the “Add Route” pop-up window that opens, enter the ***static route***
   - **Net Address**: This is the address/subnet to route to.
   - **Prefix**: This is the subnet mask in prefix form e.g., "24". See also Subnet Mask Values.
   - **Router Address**: This is the gateway address the packet will initially go through to get there.
2. press **“Add Route”.**

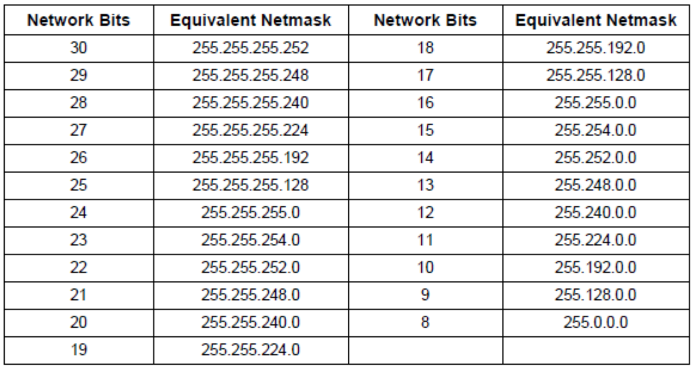


“Edit Port settings”: brings up the same pop-up menu as the center icon on the Network page (for configuring DHCP, IP address, subnet mask, etc).

Press “Add Route” to submit the data

Fields:

- **Net Address**: (“This is the address/subnet to route to”, such as **10.2.0.0** for instance). For example, enter: “**10.10.1.101**” in this field). Note that the SecureSync doesn’t care how to get to this address after its sent to its gatway address
- **Prefix**: This is the subnet mask in prefix form (a two digit number for the subnet mask. Example: for a 255.255.255.0 subnet mask, enter “**24**” in this field). Refer to the table below to determine the applicable subnet mask’s two digit number:



Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
30	255.255.255.252	18	255.255.192.0
29	255.255.255.248	17	255.255.128.0
28	255.255.255.240	16	255.255.0.0
27	255.255.255.224	15	255.254.0.0
26	255.255.255.192	14	255.252.0.0
25	255.255.255.128	13	255.248.0.0
24	255.255.255.0	12	255.240.0.0
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		

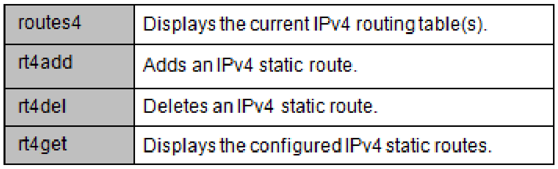
- **Router Address**: (“This is where you will go through to get there”) This is the IPv4Gateway address.

3. The entered info should now be displayed at the top of this pop-up menu.

C) Configuring IPv4 static route using CLI interface (instead of the web browser)

Note: (based on comment from Ron Dries) I believe 5.1J update added ability to both edit and view routes via CLI. Previous versions only allowed static routes to be viewed **i**n the cli.

From page 11-3 of the SecureSync Rev Q manual



routes4	Displays the current IPv4 routing table(s).
rt4add	Adds an IPv4 static route.
rt4del	Deletes an IPv4 static route.
rt4get	Displays the configured IPv4 static routes.

From table above**: Rt4get rtbl** (where **rbtl** = the following routing tables)

M=main routing table

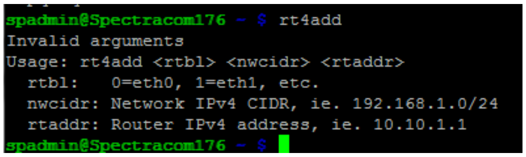
0= eth0 routing table

1= eth1 routing table

2= eth3 routing table

3= eth3 routing table

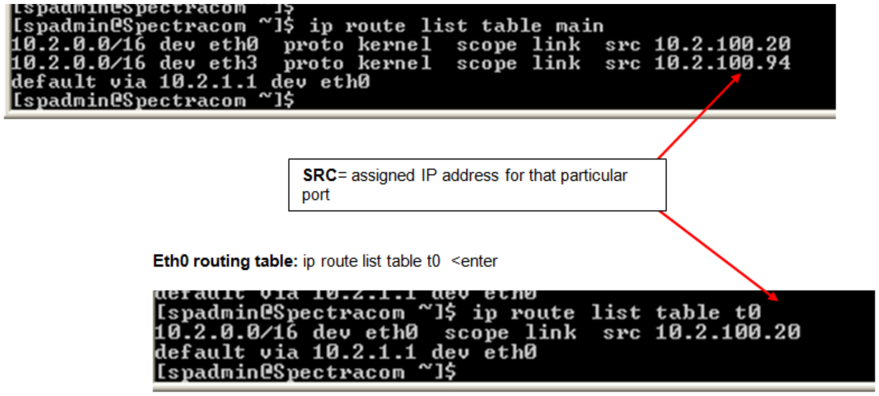
Note: The full syntax of each of these listed commands above can be obtained by typing the name of the command, followed by <enter >. For example, here is the result of typing **rt4add** <enter>, to add a new static route.



```
spadmin@Spectracom176 ~ $ rt4add
Invalid arguments
Usage: rt4add <rtbl> <nwcidr> <rtaddr>
  rtbl:   0=eth0, 1=eth1, etc.
  nwcidr: Network IPv4 CIDR, ie. 192.168.1.0/24
  rtaddr: Router IPv4 address, ie. 10.10.1.1
spadmin@Spectracom176 ~ $
```

CLI command to retrieve/view the Ipv4 routing tables

Main default routing table: **ip route list table main** <enter>



```
[spadmin@Spectracom ~]$
[spadmin@Spectracom ~]$ ip route list table main
10.2.0.0/16 dev eth0  proto kernel  scope link  src 10.2.100.20
10.2.0.0/16 dev eth3  proto kernel  scope link  src 10.2.100.94
default via 10.2.1.1 dev eth0
[spadmin@Spectracom ~]$
```

SRC= assigned IP address for that particular port

Eth0 routing table: ip route list table t0 <enter

```
default via 10.2.1.1 dev eth0
[spadmin@Spectracom ~]$ ip route list table t0
10.2.0.0/16 dev eth0  scope link  src 10.2.100.20
default via 10.2.1.1 dev eth0
[spadmin@Spectracom ~]$
```

Eth0 routing table: ip route list table t0 <enter>

Eth1 routing table: ip route list table t1 <enter>

Eth2 routing table: ip route list table t2 <enter>

Eth3 routing table: ip route list table t3 <enter>

Reasons the static route may not have been created after pressing Submit

The static route has already been created.

1) The configured "router addres" is not reachable from any Ethernet interface

Deleting static routes

- Asociated Log entry from Journal log: "requesting route for eth1 to be deleted."
- The "router address" must still be reachable in order to delete the static addresd. Otherwise, the static route won't be deleted.
    - **Example I used** - I unplugged eth1 from the network and then tried to delete a static route on Eth1. Route was not deleted. In v5.6.0, no error message was displayed.

Can't delete static routes: "Error (512) on eth0 FAILURE detected in deleting route.. (SYSAL)"

May 17 19:20:27	[WEB]	Failed to delete network access restriction (cyrustech)
May 17 19:20:27	[webui]	Error (512) on eth0 FAILURE detected in deleting route.. (SYSAL)
May 17 19:20:27	[webui]	Error (512) on eth0 FAILURE detected in deleting route.. (SYSAL)

- Refer to Salesforce case 25398
- Observed in update version 5.4.1

Issues with IPV4/IPv6 static routes

NOTICE: IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 netwok while configuring. Otherwise the config changes won't be accepted.

A) Software versions 5.4.5 and below (applicable to IPv6 static routes only)

1. IPv6 main gateway cannot be seen or set.
2. IPv6 gateway / route setup does not work for some customers so they can't setup routing.
3. If the user enters duplicate IPv6 address the first one found is valid and other ones on other units report dad failed.

Email from Paul M (1 Mar 17) from case 25398 Note some work was done on Release 5.4.5 to correct issues like this Ron commented in SSS-49 below. The issue is that there was problems with handling these addresses in earlier versions that was fixed in 5.4.5, YOU CAN USE THE COMMAND LINE TO FIX THESE issues as indicated below.

IPv6 address when duplicate cannot be deleted and IPv6 main gateway does not display or cannot set.

Since they are running 5.4.1 the text below from SSS-49 may apply.

There are general IPv6 from web ui configuration and display issues.

1. IPv6 main gateway cannot be seen or set.
2. IPv6 gateway / route setup does not work for some customers so they can't setup routing.
3. If the user enters duplicate IPv6 address the first one found is valid and other ones on other units report dad failed.

Furthermore you cannot delete these addresses fully from the Web ui. You might delete from the IPv6 stack, but an failure on delete leaves them in the /etc/conf.d/net file which restores them on reboot.

ip6del command will delete them from the file.

You can detect duplicate addresses by ip addr show eth# and look for addresses with status dadfailed

B) Software version 5.3.1

Static routes aren't being restored upon reboot

- (Mantis case 3228, Salesforce case 20224)
- Fix to be included in the version 5.4.0 update (~ Mar 2016).

C) Software version 5.3.0

Static routes broken

2. (Mantis cases 3115 and 3118) Software update version 5.3.0 broke static routing functionality. Routes are still configurable, but don't work.

- This issue was addressed in the version 5.3.1 update (~Dec 2015)

Error messages/conditions associated with static routes

1) "v6: eth1: IPv6 duplicate address 2001:4888:a03:310a:c0:fee:0:3 detected!"

- Refer to Salesforce case 23679

Email from Paul M (1 Mar 17) from case 25398 Note some work was done on Release 5.4.5 to correct issues like this Ron commented in SSS-49 below. The issue is that there was problems with handling these addresses in earlier versions that was fixed in 5.4.5, YOU CAN USE THE COMMAND LINE TO FIX THESE issues as indicated below.

IPv6 address when duplicate cannot be deleted and IPv6 main gateway does not display or cannot set.

Since they are running 5.4.1 the text below from SSS-49 may apply.

There are general IPv6 from web ui configuration and display issues.

1. IPv6 main gateway cannot be seen or set.

2. IPv6 gateway / route setup does not work for some customers so they can't setup routing.
3. If the user enters duplicate IPv6 address the first one found is valid and other ones on other units report dad failed.

Furthermore you cannot delete these addresses fully from the Web ui. You might delete from the IPv6 stack, but an failure on delete leaves them in the /etc/conf.d/net file which restores them on reboot.

ip6del command will delete them from the file.

You can detect duplicate addresses by ip addr show eth# and look for addresses with status dadfailed

IPv6 static routes

Note: info regarding IPv4 static routes is futher above in a separate section

NOTICE: IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 netwok while configuring. Otherwise the config changes won't be accepted.

Software updates associated with IPv6 static routes

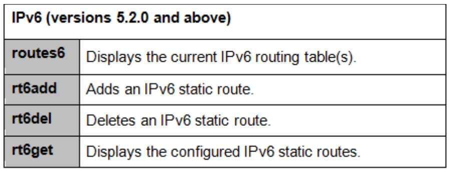
v5.7.3

- Updated IPv6 networking support to more closely match IPv4 networking. Added additional routing tables per network port with individual IPv6 default gateways. Static IPv6 routes can be applied per network port.
- Note: As of at least software update version 5.2.1, IPv6 static routes are only available for the configured main default gateway port only, (not available for the other network ports).

v5.2.0

Software update version 5.2.0 added basic **static IPv6 routing capability** by allowing manual configuration of IPv6 routes via CLI commands (not yet available via the web browser, as of at least version 5.2.1)

Note: an example of each command is below the table



IPv6 (versions 5.2.0 and above)	
routes6	Displays the current IPv6 routing table(s).
rt6add	Adds an IPv6 static route.
rt6del	Deletes an IPv6 static route.
rt6get	Displays the configured IPv6 static routes.

- **routes6:** Displays the current IPv6 routing table(s)

  Usage: rt6add <nwcidr> <rtaddr>

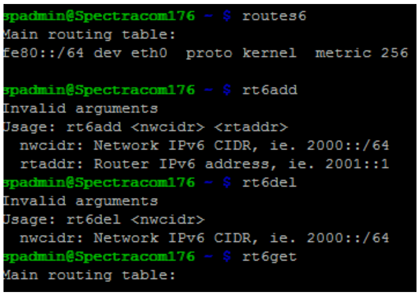
  nwcidr: Network IPv6 CIDR, ie. 2000::/64

  rtaddr: Router IPv6 address, ie. 2001::1

- **rt6get**: Displays the configured IPv6 routes.
- **rt6add**: Adds an IPv6 static route.
- **rt6del**: Deletes IPv6 static route

Where:

- **<nwcidr>** is the IPv6 address (CIDR) for the main default gateway.
- **<rtaddr>** is the IPv6 address for the router



```
spadmin@Spectracom176 ~ $ routes6
Main routing table:
fe80::/64 dev eth0  proto kernel  metric 256

spadmin@Spectracom176 ~ $ rt6add
Invalid arguments
Usage: rt6add <nwcidr> <rtaddr>
  nwcidr: Network IPv6 CIDR, ie. 2000::/64
  rtaddr: Router IPv6 address, ie. 2001::1
spadmin@Spectracom176 ~ $ rt6del
Invalid arguments
Usage: rt6del <nwcidr>
  nwcidr: Network IPv6 CIDR, ie. 2000::/64
spadmin@Spectracom176 ~ $ rt6get
Main routing table:
```

Troubleshooting customer's routes/static routes

NOTICE: IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 netwok while configuring. Otherwise the config changes won't be accepted.

- Request a topographical diagram of the customer's network.
- Software update version 5.2.0 added basic static IPv6 routing capability by allowing manual configuration of IPv6 routes via CLI commands (not yet in web browser)
- (Mantis cases 3115 and 3118) Software update version 5.3.0 broke static routing functionality. Routes are still configurable, but don't work. Fixed in version 5.3.1.

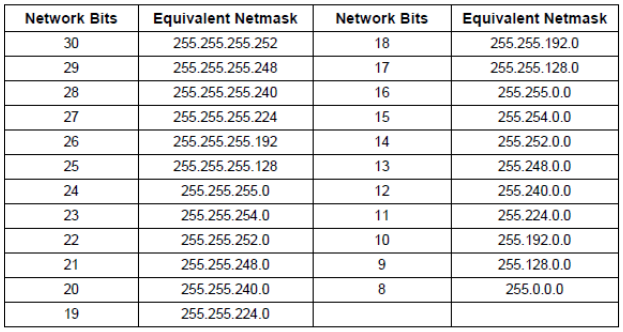
Configuration of IPv6 static routes

D) Classic Interface web browser:

Network -> **General Setup** page, **General** tab (or via CLI interface)

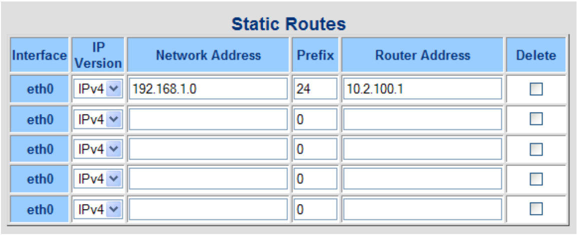
"Static Routes" table in this tab: Used to define networks on other side of routers that are attached to any or all of the Ethernet ports (but are not available through the default gateway). "Network address" will likely end in 0's (don't include the / and bits to define the subnet mask. These are entered with just the number in the "Prefix field". Enter the router's IP address in the "Router Address" field.

In the example screenshot below, Eth 0 happens to have a router at 10.2.100.1 that is also attached to a 192.168.1.x network. And, it's desired for network traffic to be broadcasted to this other subnet.



Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
30	255.255.255.252	18	255.255.192.0
29	255.255.255.248	17	255.255.128.0
28	255.255.255.240	16	255.255.0.0
27	255.255.255.224	15	255.254.0.0
26	255.255.255.192	14	255.252.0.0
25	255.255.255.128	13	255.248.0.0
24	255.255.255.0	12	255.240.0.0
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		

Table 2-2: Subnet mask values



Static Routes

Interface	IP Version	Network Address	Prefix	Router Address	Delete
eth0	IPv4	192.168.1.0	24	10.2.100.1	□
eth0	IPv4		0		□
eth0	IPv4		0		□
eth0	IPv4		0		□
eth0	IPv4		0		□

Note (as of 3/28/13) about IPv6 Static Routes: IPv4 Static Routes are supported. IPv6 Static Routes are **not** currently supported (Refer to Mantis case 1936/1937 http://cvsmantis.int.orolia.com/mantis/view.php?id=1937). The drop-downs only allow IPv4 to be selected (this is beyond just adding a new value to the drop-down.

Email from Dave Sohn regarding the intentions to add IPv6 Static Routes (28 March 2013) In my response to the issues presented by Roots I presented the resolution of some issues and feature requests. IPv6 gateway support fix was included, but IPv6 routing was not. IPv6 routing requires sone extensive development similar to getting the multiple interface IPv4 routing to work we did a few years ago. It is in our sustaining plan to add this, but is dependent on resources, which are allocated elsewhere at this time. I hope to get something into our end of Q3 or Q4 release, but that is still dependent on resource availability.

Issues/software changes associated with IPv6 static routes

- Refer also to “Issues with IPv4/IPv6 Static routes” further above in the “IPv4 static routes” section

Email from Paul M (1 Mar 17) from case 25398 Note some work was done on Release 5.4.5 to correct issues like this Ron commented in SSS-49 below. The issue is that there was problems with handling these addresses in earlier versions that was fixed in 5.4.5, YOU CAN USE THE COMMAND LINE TO FIX THESE issues as indicated below.

IPv6 address when duplicate cannot be deleted and IPv6 main gateway does not display or cannot set.

Since they are running 5.4.1 the text below from SSS-49 may apply.

There are general IPv6 from web ui configuration and display issues.

1. IPv6 main gateway cannot be seen or set.
2. IPv6 gateway / route setup does not work for some customers so they can't setup routing.
3. If the user enters duplicate IPv6 address the first one found is valid and other ones on other units report dad failed. Furthermore you cannot delete these addresses fully from the Web ui. You might delete from the IPv6 stack, but an failure on delete leaves them in the /etc/conf.d/net file which restores them on reboot.

ip6del command will delete them from the file.

You can detect duplicate addresses by ip addr show eth# and look for addresses with status dadfailed

**Network troubleshooting in SecureSync (tcpdump, ping, arp, traceroute/tracepath, etc)

- Refer to Mantis case 1583 for more details.

TCPdump (wireshark for Linux)

- TCPdump is a command line packet capture tool (these captures can be opened with wireshark)

Note: includes the ability to delete tcpdump via web browser, if desired. See additional info below.

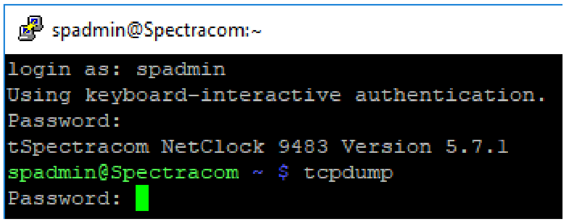
Software version changes associated with tcpdump

Location of TCPdump in the system

- tcpd (tcpdump) is in the **home/spectracom/usr/sbin** directory

Disabling TCPDump (if desired)

Note: If tcdump **responds with a password** (as shown below) tcpdump has been disabled (and cant be re-enabled without performing a full update/restore to default)



spadmin@Spectracom:~

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

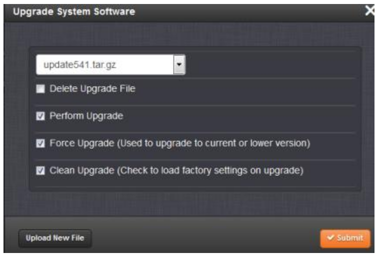
TCPdump can be disabled in the bottom-left corner of the **Management** -> **Network** pages via a slider switch (under "**Network Services**"). Once deleted, it can only be brought back with a "restore to factory defaults" update (It's not restored just by performing a "clean" or by updating the software to a newer version). See additional info below.

Re-enabling tcpdump once its been "disabled" in the system

To begin, tcpdump is available for use, by factory default, in SecureSync software versions 5.2.1 and above. Tcpdump remains available for use until its "permanently" disabled via the "tcpdump" slider switch in the **Management** -> **Network** page of the browser. Unlike other Services which can be disabled/re-enabled as desired, for security purposes, tcpdump availability is removed from the system once its been changed to disabled.   Once the tcpdump slider switch has been moved, this service is no longer available until a "Clean Upgrade" (not just a "clean" command) has been performed.

To restore tcpdump once its been disabled, perform a "**Clean Upgrade**", Note this will reset all of the unit's configurations back to the factory default settings for the version of software being applied during this process (the same version of software can be re-applied to keep it the same version, as desired).

The start of this process is similar to performing a standard software update to the latest version. But after selecting/uploading the software update bundle into the SecureSync, instead of just selecting the "**Perform Upgrade**" checkbox, both the "**Force Update**" and "**Clean Upgrade**" checkboxes also need to be selected, as well (as shown below). Then press Submit.



update541.tar.gz

□ Delete Upgrade File

☑ Perform Upgrade

☑ Force Upgrade (Used to upgrade to current or lower version)

☑ Clean Upgrade (Check to load factory settings on upgrade)

Once the "Clean Upgrade" process has been completed, the unit can then be reconfigured as desired and TCPdump will be available for use again (until the slider bar for TCPdump is changed to disabled again).

Attached for your reference is a copy of the standard software update instructions for version 5,4,1. To apply the version 5.4.1 software (either to keep it at version 5.4.1 or to upgrade it to version 5.4.1 from as earlier version, as we always recommend having the latest version of software installed), the version 5.4.1 software update bundle can be downloaded from our website. Here is the link to download the version 5.4.1 update bundle and upgrade instructions: http://spectracom.com/support/securesync-and-netclock-9400-support (scroll down to the "**Software**" section).

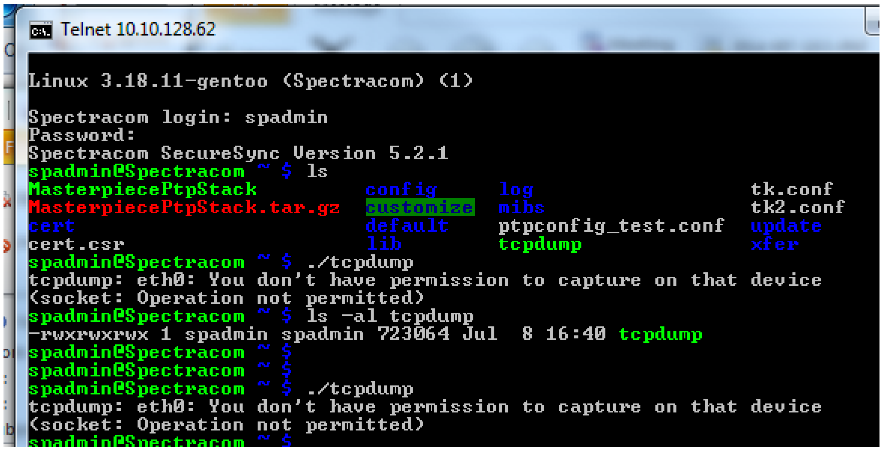
Follow the update instructions up to the point where it indicates to select "**Perform Upgrade**", but then ALSO select the other two checkboxes referenced above (both the "**Force Update**" and "**Clean Upgrade**" checkboxes). Then press Submit

Configuration of whether TCPdump has been removed from the system

- The setting of whether TCPDump has been removed is in the *remove.conf* file (located in the /config file)
  - If not yet removed, this file will be empty
  - If TCPDump has been removed, this file will contain: "usr/sbin/tcpdump"

Ability for a "user" to install tcpdump into SecureSync to be able to capture network traffic (i.e. if an admin has already removed tcpdump for security reasons)

Per Paul Myers (7 jul 15) You can't get access to underlying features using spadmin owned tcpdump (note from Keith- Paul had a co-op remove TCPDump using the slider switch and then brought it back into the system using spadmin. This shows a user can't simply install tcpdump and start using it with just admin rights (must use the default tcpdump or be logged in as a root to use a different tcpdump.



```
Linux 3.18.11-gentoo (Spectracom) (1)

Spectracom login: spadmin
Password:
Spectracom SecureSync Version 5.2.1
spadmin@Spectracom ~ $ ls
MasterpiecePtpStack          config     log                    tk.conf
MasterpiecePtpStack.tar.gz   customize  mibs                   tk2.conf
cert                         default    ptpconfig_test.conf    update
cert.csr                     lib        tcpdump                xfer
spadmin@Spectracom ~ $ ./tcpdump
tcpdump: eth0: You don't have permission to capture on that device
(socket: Operation not permitted)
spadmin@Spectracom ~ $ ls -al tcpdump
-rwxrwxrwx 1 spadmin spadmin 723064 Jul  8 16:40 tcpdump
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $
spadmin@Spectracom ~ $ ./tcpdump
tcpdump: eth0: You don't have permission to capture on that device
(socket: Operation not permitted)
spadmin@Spectracom ~ $
```

Network "Access Control" and ability to run TCPdump

- TCPdump requires access to a command prompt (Telnet or SSH) in order to run.
- If Network "Access Control" has been established (limiting access to Services by IP addresses) and a user on a PC that is not on the Access list tries to "sniff" the network, they won't be able to connect with telent or ssh in order to run tcpdump.

Email from Keith to a customer (8 July 2015) Sniffing the network traffic requires a unique tool be installed on the machine (TCPdump for Linux or a program such as wireshark for Windows). Prior to version 5.2.0 software in SecureSync, none of these type programs were available on SecureSync. But TCPdump was added to SecureSync in version 5.2.0 for customers that want to be able to view the raw SecureSync packets from within the SecureSync.

For customers that don't want TCPDump to be available (note it can only be run from the CLI command prompt and can't be run from the web browser) it can be disabled from the Management -> Network page of the browser (there is a slider switch for it on the left side). Once it's been disabled by a user, even performing a "clean" or updating the software to a newer version will enable it again (the other slider switches for each of the other Services listed on this page can be disabled and re-enabled whenever desired). The only way to re-enable tcpdump once it's been disabled is to perform a "restore to factory default settings". Once it's been disabled, it can't be run from any network port, even if the Access Control list remains empty.

In order to run this utility (as long as it hasn't been disabled yet), a user logs into Telnet or SSH to establish a command line interface with the SecureSync. In order to connect via either telnet or SSH, a user account and password has to be known. With no IP addresses in the Network Access Control list, a user can try to connect to telnet or ssh and will get a login prompt. If they know a valid username and password, they can connect and run tcpdump. But if the Access Control List is used to limit access to all Services, and someone tries to connect to the CLI from a machine that isn't allowed in this Access list, they will not even be able to get to the telnet or SSH login screen. Even if they have a valid username and password, they won't be able to connect to any of the Services (telnet, SSH, FTP, web browser, etc). Since they won't be able to reach any of the Services to even attempt to connect, they can't run tcpdump or any other utility that can be used to sniff the network packets. If the machine's address isn't in the access list to allow it, they can only sync their PC with NTP time stamps.

In summary, the Access list blocks access to the ability for all unauthorized machines to be able to open a command prompt, which is needed to run the tcpdump program that is used to sniff the network ("not authorized" IP addresses can only obtain NTP time stamps for network time synchronization - note that even this capability can be blocked if desired, because NTP has its own access control available, as well).

Using TCPdump

Need to use a mirrored port (port mirroring) on switches

- Applicable to unicast packets only (not applicable to multicast)
- Switches direct traffic to the appropriate port only, so packets not meant for other ports aren't router to that port
- Won't be able to capture packets unless on the same port or traffic is also directed to another port as well (this is port mirroring)
- Some, but not all switches support port mirroring.

Desire to use TCPdump to capture PTP traffic

- TCPdump can be used to capture PTP traffic that is on the same network as eth0, eth1, eth2 or eth3.
- TCPdump cannot be used to capture PTP traffic if the PTP Master and PTP Slaves are on their own dedicated network.

Email from Keith (9 Sept 16) As the PTP cards and the SecureSync's Ethernet ports are internally not on the same network, and as both the PTP Master and slaves need to be involved in the capture, you can't just loop a PTP connection over to any of the standard network ports to perform a capture.

The only way to use the SecureSync to perform a PTP packet capture is to connect one of its standard Ethernet interfaces (eth0 - eth3) to a mirrored port on the switch (making one of the SecureSync' Ethernet interfaces act like a PC on the same switch). Then run tcpdump in the SecureSync's CLI interface by typing: sudo tcpdump <enter>.

Refer to tcpdump info online on how to use this program: sites such as http://www.tcpdump.org/tcpdump_man.html or https://danielmiessler.com/study/tcpdump/

For example, **tcpdump –i eth1** will capture the traffic on eth1 (instead of the default port of eth0).

To capture just PTP packets on Eth0: **tcpdump port 319 and 320**
To capture just PTP packets on Eth1: **tcpdump** –i eth1 **port 319 and 320**

To capture all traffic to a File sudo tcpdump -w securesync .pcap
Note the file is created/stored in the home/spectracom directory (FTP it out from this directory).

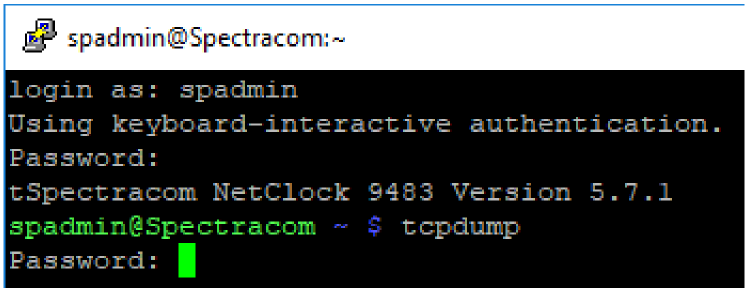
Control + c stops the capture.

Running/using tcpdump

Notes:

1) use **CTRL** + **C** to stop a capture in progress

2) If the tcdump command responds with a password (as shown below) tcpdump has been disabled in the time sever (and can't be re-enabled without performing a full upgrade/restore to factory default)



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

CLI Command:

1. Versions 5.4.5 and above:

- **tcpdump** (No need to issue sudo to run it)
- Tcpdump can only be run from a command prompt (telnet or ssh). It cannot be run from the web browser

Note: tcpdump is not in helpcli.

- Refer to normal tcpdump info on how to use this program- sites such as http://www.tcpdump.org/tcpdump_man.html or https://danielmiessler.com/study/tcpdump/

Login as spadmin and type:

tcpdump <enter>

Ethernet interface data is captured on (eth0 is the default)

Unless one or more ports are specified, the default is to listen on Eth0 only. To listen on a port other than eth0, after tcpdump type –i (lower case, like in india) followed by **eth1 eth2** or **eth3**

Examples

To capture data on specific (or all) Ethernet interfaces

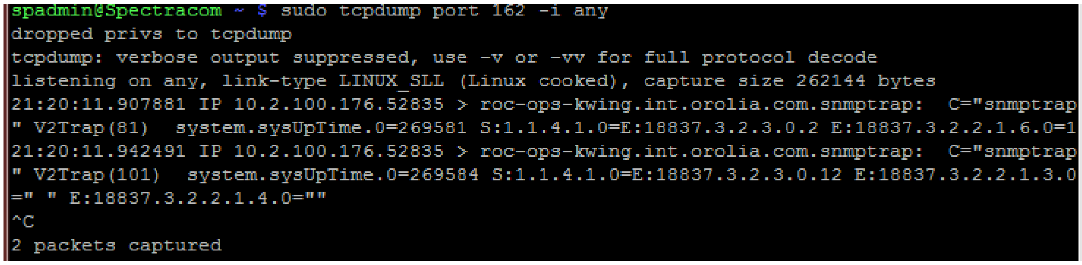
Note-omit the word "sudo" in all the below commands for software versions 5.4.5 AND ABOVE

- To capture traffic on **eth1** instead of eth0: **tcpdump –i eth1**
- To capture traffic on more than one interface (such as eth0 and eth1: **\ tcpdump –i eth0 –i eth**
- To capture traffic on all interfaces (eth0 thru eith 3): **tcpdump –i any**

To capture specific data type of packets (such as Radius packets only, snmp only)

Note-omit the word "sudo" in all the below commands for software versions 5.4.5 AND ABOVE

- **NTP** on eth0: **tcpdump port 123** (no need to define interface as eth0 is default)
- **Radius** on eth0: **tcpdump port 1812 and 1813** (no need to define interface as eth0 is default)
- **LDAP** on eth0: **tcpdump port 389 and 636** (no need to define interface as eth0 is default)
- **Syslog** on eth0: **tcpdump port 514** (no need to define interface as eth0 is default)
- **PTP** on eth0: **tcpdump ports 319 and 320** (no need to define interface as eth0 is default)
- **SNMP Traps** sent to **any** Ethernet interface: **sudo tcpdump port 162 -i any**



```
spadmin@Spectracom ~ $ sudo tcpdump port 162 -i any
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
21:20:11.907881 IP 10.2.100.176.52835 > roc-ops-kwing.int.orolia.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.orolia.com.snmptrap:  C="snmptrap
" V2Trap(101)  system.sysUpTime.0=269584 S:1.1.4.1.0=E:18837.3.2.3.0.12 E:18837.3.2.2.1.3.0
=" " E:18837.3.2.2.1.4.0=""
^C
2 packets captured
```

To stop a capture and exit tcpdump Use: **Control + C**

To highlight specific words, type: **sudo tcpdump | grep xxxxx**

To be able to scroll through packets: **sudo tcpdump | less**
Then: Press "/" followed by letter(s) to highlight the letters in all of the packets
(press **q** to exit out of the view)

Options

Note-omit the word "sudo" in all the below commands for software versions 5.4.5 AND ABOVE

1) **Basic communication** // see the basics without many options **sudo tcpdump –nS** <enter>
2) **Basic communication (very verbose)** // see a good amount of traffic, with verbosity and no name help **:** **sudo tcpdump –nnvvS** <enter>
3) **A deeper look at the traffic** // adds -X for payload but doesn't grab any more of the packet

sudo tcpdump –nnvvXS <enter>

4) **Heavy packet viewing** // the final "s" increases the snaplength, grabbing the whole packet

sudo tcpdump -nnvvXSs 1514 <enter>

There are three main types of expression: type, dir, and proto.

Note: omit the word "sudo" in all the below commands for software versions 5.4.5 AND ABOVE

Type options are **host**, **net**, and **port**. Direction is indicated by dir, and there you can have src, dst, src or dst, and src and dst. Here are a few that you should definitely be comfortable with:

- **host // look for traffic based on IP address (also works with hostname if you're not using -n)**

```
sudo tcpdump host 1.2.3.4
```

- **src, dst // find traffic from only a source or destination (eliminates one side of a host conversation)**

```
sudo tcpdump src 2.3.4.5
sudo tcpdump dst 3.4.5.6
```

- **net // capture an entire network using CIDR notation**

```
sudo tcpdump net 1.2.3.0/24
```

- **proto // (works for tcp, udp, and icmp). Note that you don't have to type proto**

```
sudo tcpdump tcp

sudo tcpdump udp

sudo tcpdump i
```

- **port // see only traffic to or from a certain port**

```
sudo tcpdump port xxx
```

(whe re is the desired port number to listen for)

  - **src, dst port** // filter based on the source or destination port

```
sudo tcpdump src port 1025 # tcpdump dst port 389
```

- **src/dst, port, protocol // combine all three**

```
sudo tcpdump src port 1025 and tcp
sudo tcpdump udp and src port 53
```

- **You also have the option to filter by a range of ports instead of declaring them individually, and to only see packets that are above or below a certain size.**

SYNOPSIS

tcpdump [**-AbdDefhHIJKlLnNOpqRStuUvxX#**] [**-B** *buffer_size*]

[**-c** *count*]

[**-C** *file_size*] [**-G** *rotate_seconds*] [**-F** *file*]

[**-i** *interface*] [**-j** *tstamp_type*] [**-m** *module*] [**-M** *secret*]

[**--number**] [**-Q** *in*|*out*|*inout*]
[**-r** *file*] [**-V** *file*] [**-s** *snaplen*] [**-T** *type*] [**-w** *file*]

[**-W** *filecount*]

[**-E** *spi@ipaddr algo:secret,...*]

[**-y** *datalinktype*] [**-z** *postrotate-command*] [**-Z** *user*]
[**--time-stamp-precision=***tstamp_precision*]
[**--immediate-mode**] [**--version**]

[*expression*]

Options
Below are a few options (with examples)

First off, I like to add a few options to the tcpdump command itself, depending on what I'm looking at. The first of these is **-n**, which requests that names are not resolved, resulting in the IPs themselves always being displayed. The second is **-X**, which displays both hex and ascii content within the packet. The final one is **-S**, which changes the display of sequence numbers to absolute rather than relative. The idea there is that you can't see weirdness in the sequence numbers if they're being hidden from you. Remember, the advantage of using tcpdump vs. another tool is getting manual interaction with the packets.

It's also important to note that tcpdump only takes the first ~~68~~ 96 bytes of data from a packet by default. If you would like to look at more, add the **-s *number*** option to the mix, where *number* is the number of bytes you want to capture. I recommend using 0 (zero) for a snaplength, which gets everything. Here's a short list of the options I use most:

- -i any : Listen on all interfaces just to see if you're seeing any traffic.
- -n : Don't resolve hostnames.
- -nn : Don't resolve hostnames *or* port names.
- -X : Show the packet's *contents* in both hex and ASCII.
- -XX : Same as -X, but also shows the ethernet header.
- -v, -vv, -vvv : Increase the amount of packet information you get back.
- -c : Only get *x* number of packets and then stop.
- -s : Define the *snaplength* (size) of the capture in bytes. Use -s0 to get everything, unless you are intentionally capturing less.
- -S : Print absolute sequence numbers.
- -e : Get the ethernet header as well.
- -q : Show less protocol information.
- -E : Decrypt IPSEC traffic by providing an encryption key.

- **Port Ranges** // see traffic to any port in a range
  tcpdump portrange 21-23
- **Packet Size Filter** // only see packets below or above a certain size (in bytes)
  tcpdump less 32
  tcpdump greater 128

[You can use the symbols for less than, greater than, and less than or equal / greater than or equal signs as well.]
// filtering for size using symbols
tcpdump > 32
tcpdump <= 128

Writing to a File

- tcpdump allows you to send what you're capturing to a file for later use using the -w option, and then to read it back using the -r option. This is an excellent way to capture raw traffic and then run it through various tools later.

The traffic captured in this way is stored in tcpdump format, which is pretty much universal in the network analysis space. This means it can be read in by all sorts of tools, including Wireshark, Snort, etc.

Capture all traffic to a File

Note-omit the word “sudo” in all the below commands for software versions 5.4.5 AND ABOVE

- The file is created/stored in the home/spectracom directory.

```
sudo tcpdump -w securesync .pcap
```

Note: securesync.pcap below is an arbitrary file name used as an example (Can name the file as desired).

Then, at some point in the future, you can then read the traffic back in like so:

Read Captured Traffic back into tcpdump

```
sudo tcpdump -r secureSync.pcap
```

Log entries associated with tcpdump

Auth.log

- No auth log entries are asserted when starting tcpdump normally.

Trying to start tcpdump using “su” instead of “sudo” (or just typing “tcpdump” by itself)

- Note the correct command to start tcpdump is “**sudo tcpdump**”

```
su[8096]: pam_unix(su:auth): authentication failure; logname=spadmin uid=1002 euid=0 tty=/dev/pts/2 ruser=spadmin rhost=
user=tcpdump
su[8096]: FAILED su for tcpdump by spadmin su[8096]: - /dev/pts/2 spadmin:tcpdump
```

System log

Two entries asserted when logging into the classic interface browser with versions 5.2.0 and above.

```
Aug  3 15:10:57 custservice176 custservice176: [spadmin] ERROR (2) - Error SEC_GetGroup (username[0,1]=quagga)  (WEB)
Aug  3 15:10:57 custservice176 custservice176: [spadmin] ERROR (2) - Error SEC_GetGroup (username[1,2]=tcpdump)  (WEB)
```

Example email Keith sent (reference Case 286924) for performing PTP packet captures on both a PTP Masdter and PTP Slave

Though I have been working on/off with Dave Sohn and our Apps team, I have formally escalated this case to our Apps engineers.   Looking back at your provided screenshots, I am circling back with them about the PTP statistics reports from the browser. They are reporting "missing packets". I'm working with them for more details on this column.

They and I both agree that the likely solution to this condition is via a PTP packet capture. Would it be possible for you to send us at least one packet capture file from the PTP Master, and another file from the PTP Slave, with the captures running simultaneously)

One method to capture the PTP packets being sent/received is by using Wireshark on a networked device between the two units (such as a Windows PC). However, likely even easier, the SecureSyncs have tcpdump installed (by factory default). Unless tcpdump has been already disabled by a user, tcpdump captures can be performed using the CLI interface (via an SSH session).

PTP packets are on ports 319 and 320. The PTP captures can be limited to just these two ports. Tcpdump packet captures default to interface eth0, unless another/other interfaces is/are specified. A tcpdump file can be created inside the SecureSync and then exported out/uploaded to us using the same fileshare site as used to send us log bundles, if desired.

The general CLI command to perform tcpdump captures after first Logging into SSH as spadmin is **tcpdump** <enter>

To capture all traffic to an internal File stored in the SecureSync, first type **tcpdump -w securesync.pcap** (This creates a file named securesync.pcap)
Note the file is created/stored in the **home/spectracom** directory (SFTP it out from this directory).

Please send us packet capture files running at about the same time/ for about the same length of time (a couple minutes) on both units, for both PTP ports 319 and 320. Make sure to select the correct ethernet interface (eth 0 or eth1) on both captures, for the port sending/receiving the packets on that unit. For eth0, no interface number needs to be defined in the tcpdump command. For eth1, eth1 can be specified as follows: **tcpdump –i eth1**

To capture all ptp messages sent/received on **eth0** for instance, type: **tcpdump ports 319 and 320**
To capture all ptp messages sent/received on **eth1** for instance, type: **tcpdump ports 319 and 320 –i eth1**

To stop a capture and exit tcpdump Use: **Control + C**

Note: tcpdump is not in helpcli.

- Refer to normal tcpdump info on how to use this program- sites such as http://www.tcpdump.org/tcpdump_man.html or https://danielmiessler.com/study/tcpdump/

Available CLI commands for troubleshooting network issues (ping, traceroute, dig, etc)

Starting in SecureSync software version 4.8.0, customers will be able to troubleshoot network issues from within SecureSync (instead of just external to the SecureSync). There are several tools being added to provide standard Linux commands for troubleshooting the network traffic. These commands are only available in the CLI port (not on the web browser) and are intended for experienced users only.

The added commands are:

Ping, ifconfig, arp, rarp, route, netstat, domainname, dig, host, nslookup, traceroute

To use these commands, login with any CLI connection (Serial port, telnet or ssh). Then, type these commands at the command prompt.

Note: Pressing **CTRL / C** can be used to end the command (for commands like ping which will keep going until CTRL and C are pressed together)

Ping

- ➢ type ping followed by IP address of the other device you wish to ping)

Function: Can ping another network device FROM the NTP server. Note that it will continue to ping until press **CTRL** / **C**.

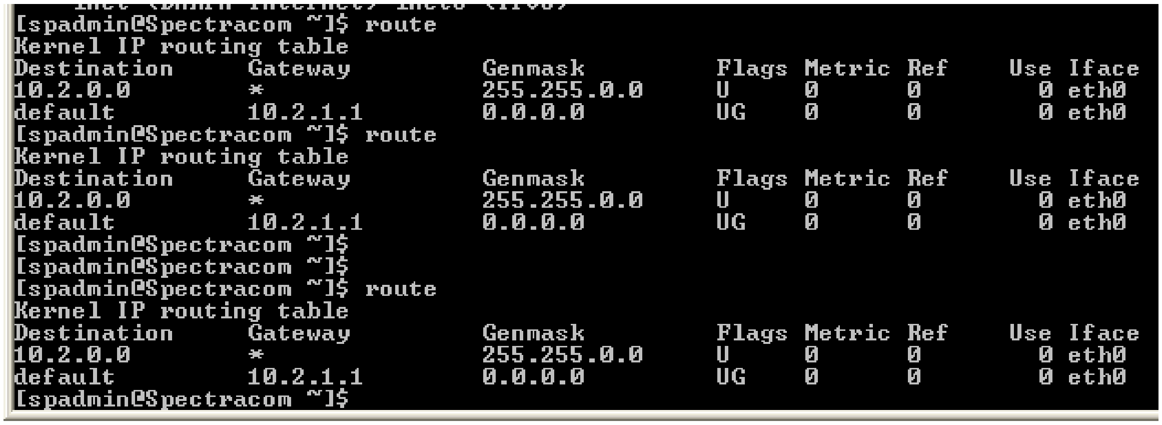
Routes/Routing tables for the network ports

Note: Software update version 5.2.0 added basic static IPv6 routing capability by allowing manual configuration of IPv6 routes via CLI commands (not yet in browser)

- Refer also to routing tables further below in the network section of this document
- Route: (just type "**route**")

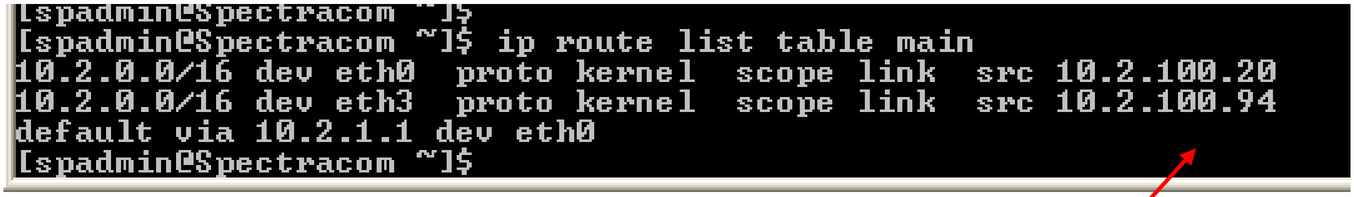
Function: manipulates the kernel's IP routing tables. Its primary use is to **set up static routes** to specific hosts or networks via an interface after it has been configured with the **ifconfig** program.

Note: Can VIEW routing tables, but not CONFIGURE via CLI



```
[spadmin@Spectracom ~]$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.2.0.0        *               255.255.0.0     U     0      0        0 eth0
default         10.2.1.1        0.0.0.0         UG    0      0        0 eth0
[spadmin@Spectracom ~]$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.2.0.0        *               255.255.0.0     U     0      0        0 eth0
default         10.2.1.1        0.0.0.0         UG    0      0        0 eth0
[spadmin@Spectracom ~]$
[spadmin@Spectracom ~]$
[spadmin@Spectracom ~]$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.2.0.0        *               255.255.0.0     U     0      0        0 eth0
default         10.2.1.1        0.0.0.0         UG    0      0        0 eth0
[spadmin@Spectracom ~]$
```

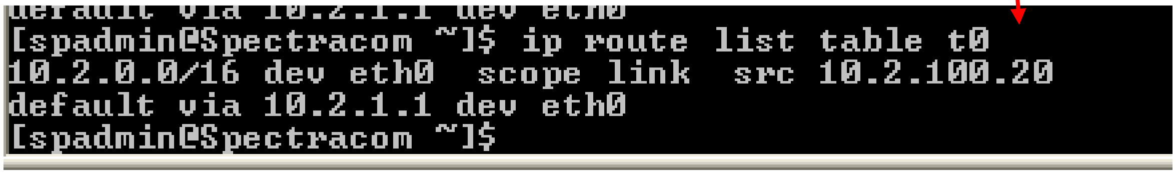
Main default routing table: **ip route list table main** <enter>



```
[spadmin@Spectracom ~]$
[spadmin@Spectracom ~]$ ip route list table main
10.2.0.0/16 dev eth0  proto kernel  scope link  src 10.2.100.20
10.2.0.0/16 dev eth3  proto kernel  scope link  src 10.2.100.94
default via 10.2.1.1 dev eth0
[spadmin@Spectracom ~]$
```

SRC= assigned IP address for that particular Ethernet interface

Eth0 routing table: **ip route list table t0** <enter>



```
default via 10.2.1.1 dev eth0
[spadmin@Spectracom ~]$ ip route list table t0
10.2.0.0/16 dev eth0  scope link  src 10.2.100.20
default via 10.2.1.1 dev eth0
[spadmin@Spectracom ~]$
```

Eth1 routing table: **ip route list table t1** <enter>

Eth2 routing table: **ip route list table t2** <enter>

Eth3 routing table: **ip route list table t3** <enter>

tracepath and traceroute commands

- The command used to be “traceroute”. Has since been changed to “tracepath” in at least v5.4.1 (traceroute is no longer a valid command. Not sure in which software update this change occurred).

Function: Shows the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes

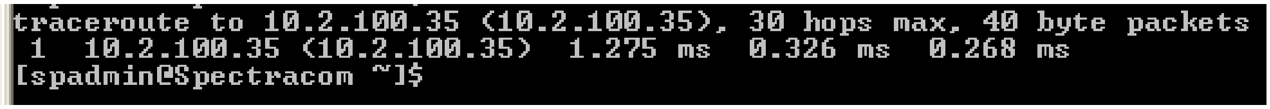
.

A) Traceroute

- **Note: it appears tracepath may no longer work in at least 5.8.2 (if not earlier, also)**

  - **IPv4** or **IPv6:** Type “**traceroute** followed by the destination address.

- This command works for both IPv4 or IPv6 (the -4 or -6 switch can be added to force one or the other, but this isn’t necessary).

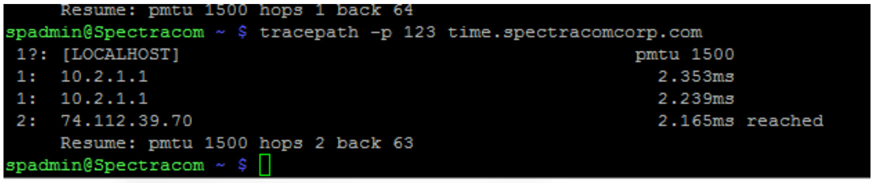


```
traceroute to 10.2.100.35 (10.2.100.35), 30 hops max, 40 byte packets
 1  10.2.100.35 (10.2.100.35)  1.275 ms  0.326 ms  0.268 ms
[spadmin@Spectracom ~]$
```

traceroute using a specified port number (such as port 123)

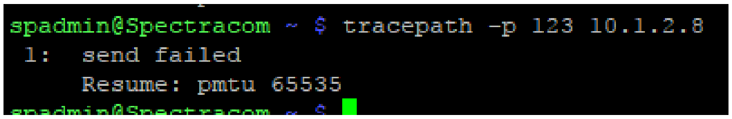
- Switch “-p” allows a desired port number to be specified

traceroute -p 123 time.spectracomcorp.com As shown below, verify the last value is **74.112.39.70** followed by “**reached**” at the end of the line:



```
     Resume: pmtu 1500 hops 1 back 64
spadmin@Spectracom ~ $ tracepath -p 123 time.spectracomcorp.com
 1?: [LOCALHOST]                                        pmtu 1500
 1:  10.2.1.1                                             2.353ms
 1:  10.2.1.1                                             2.239ms
 2:  74.112.39.70                                         2.165ms reached
     Resume: pmtu 1500 hops 2 back 63
spadmin@Spectracom ~ $
```

Example of a destination address not being available via port 123 (“send failed” to a bad address)

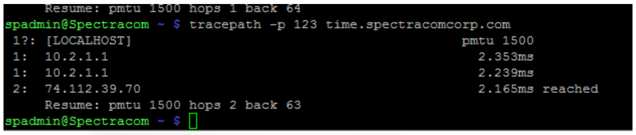


```
spadmin@Spectracom ~ $ tracepath -p 123 10.1.2.8
 1:  send failed
     Resume: pmtu 65535
spadmin@Spectracom ~ $
```

What is the “**Reach**” value for “nytime” (its row) in this ntpq -q response? Note it should be “377” if it can get receive good NTP packets from nytime (such as what is being reported in the second row of the screenshot above). If it’s a “0”, this SecureSync is not getting any NTP packets from nytime, or the NTP packets are indicating nytime is not in sync/Stratum1

The response to this command should list nytime’s IP address/DNS host name in the first column. First try pinging this value (exactly as shown in the ntpq -p response) from the command prompt to ensure there is a response from nytime to this SecureSync.

Then at its command prompt, type the following: traceroute -p 123 time.spectracomcorp.com As shown below, verify the last value is **63.138.60.57** **(note this IP address may vary)** followed by “**reached**” at the end of the line:



```
     Resume: pmtu 1500 hops 1 back 64
spadmin@Spectracom ~ $ tracepath -p 123 time.spectracomcorp.com
 1?: [LOCALHOST]                                        pmtu 1500
 1:  10.2.1.1                                             2.353ms
 1:  10.2.1.1                                             2.239ms
 2:  74.112.39.70                                         2.165ms reached
     Resume: pmtu 1500 hops 2 back 63
spadmin@Spectracom ~ $
```

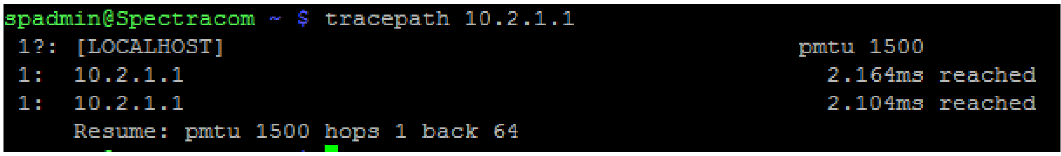
Repeat this same command above, but replace “time.spectracomcorp.com” (at the end of the command) with the exact IP/hostname for “nytime” (As reported in the ntpq -p response). The last value in this response should be the IP address of “nytime” (instead of 74.112.39.70) followed by “**reached**” at the end of the line (assuming nytime is routable from dentime and that port 123 is open all the way through).

B) Tracepath (for some versions of software prior to 5.8.1ish)

Note: can specify a particular port (such as port 123) to confirm its open all the way through (more info on this further below) Example tracepath -p 123 time.spectracomcorp.com (IP address of 63.138.60.57)

Function: From tracepath man page:“It traces path to *destination* discovering MTU along this path. It uses UDP port *port* or some random port. It is similar to **traceroute**, only does not require superuser privileges and has no fancy options.”

- **IPv4**: Type “**tracepath** followed by the destination address.
- **IPv6:** Type “**tracepath6** followed by the destination address.



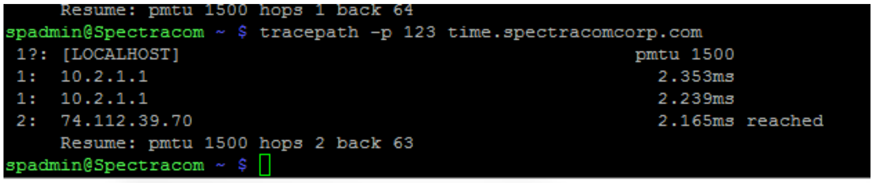
```
spadmin@Spectracom ~ $ tracepath 10.2.1.1
 1?: [LOCALHOST]                                         pmtu 1500
 1:  10.2.1.1                                              2.164ms reached
 1:  10.2.1.1                                              2.104ms reached
     Resume: pmtu 1500 hops 1 back 64
```

Note: it appears tracepath may no longer work in at least 5.8.2 (if not earlier, also)

tracepath using a specified port number (such as port 123)

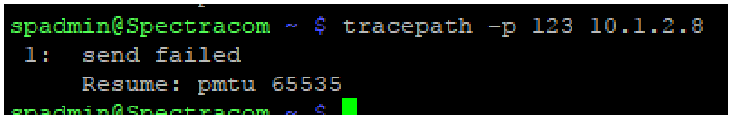
- Switch “-p” allows a desired port number to be specified

tracepath -p 123 time.spectracomcorp.com As shown below, verify the last value is **74.112.39.70** followed by “**reached**” at the end of the line:



```
     Resume: pmtu 1500 hops 1 back 64
spadmin@Spectracom ~ $ tracepath -p 123 time.spectracomcorp.com
 1?: [LOCALHOST]                                         pmtu 1500
 1:  10.2.1.1                                              2.353ms
 1:  10.2.1.1                                              2.239ms
 2:  74.112.39.70                                          2.165ms reached
     Resume: pmtu 1500 hops 2 back 63
spadmin@Spectracom ~ $ 
```

Example of a destination address not being available via port 123 (“send failed” to a bad address)

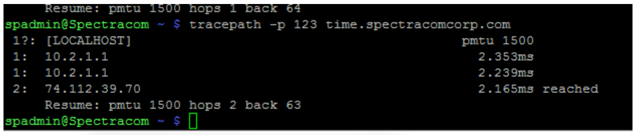


```
spadmin@Spectracom ~ $ tracepath -p 123 10.1.2.8
 1:  send failed
     Resume: pmtu 65535
spadmin@Spectracom ~ $ 
```

What is the “**Reach**” value for “nytime” (its row) in this ntpq -q response? Note it should be “377” if it can get receive good NTP packets from nytime (such as what is being reported in the second row of the screenshot above). If it’s a “0”, this SecureSync is not getting any NTP packets from nytime, or the NTP packets are indicating nytime is not in sync/Stratum1

The response to this command should list nytime’s IP address/DNS host name in the first column. First try pinging this value (exactly as shown in the ntpq -p response) from the command prompt to ensure there is a response from nytime to this SecureSync.

Then at its command prompt, type the following: tracepath -p 123 time.spectracomcorp.com As shown below, verify the last value is **63.138.60.57** **(note this IP address may vary)** followed by “**reached**” at the end of the line:



```
     Resume: pmtu 1500 hops 1 back 64
spadmin@Spectracom ~ $ tracepath -p 123 time.spectracomcorp.com
 1?: [LOCALHOST]                                         pmtu 1500
 1:  10.2.1.1                                              2.353ms
 1:  10.2.1.1                                              2.239ms
 2:  74.112.39.70                                          2.165ms reached
     Resume: pmtu 1500 hops 2 back 63
spadmin@Spectracom ~ $ 
```

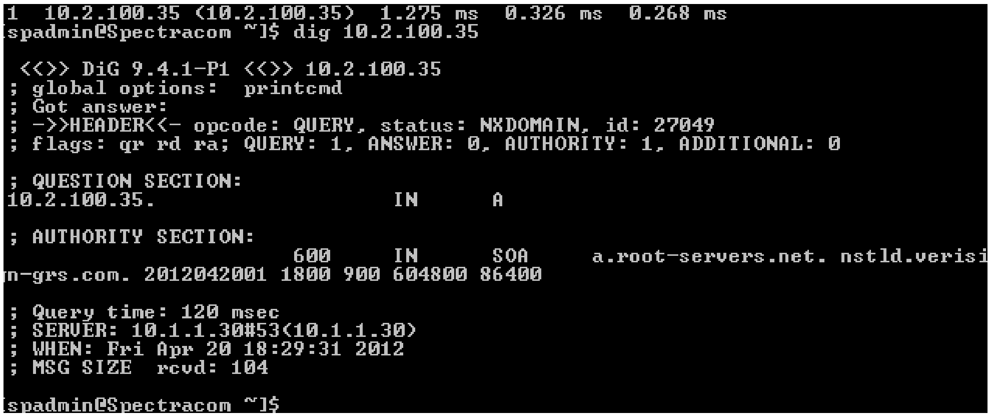
Repeat this same command above, but replace “time.spectracomcorp.com” (at the end of the command) with the exact IP/hostname for “nytime” (As reported in the ntpq -p response). The last value in this response should be the IP address of “nytime” (instead of 74.112.39.70) followed by “**reached**” at the end of the line (assuming nytime is routable from dentime and that port 123 is open all the way through).

Dig: (Domain Information Groper)

Note (24 Jan KW) Appears dig may have removed (or disabled for spadmin)

- type “**dig**” followed by address

Function: a flexible tool for interrogating **DNS name servers**. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.

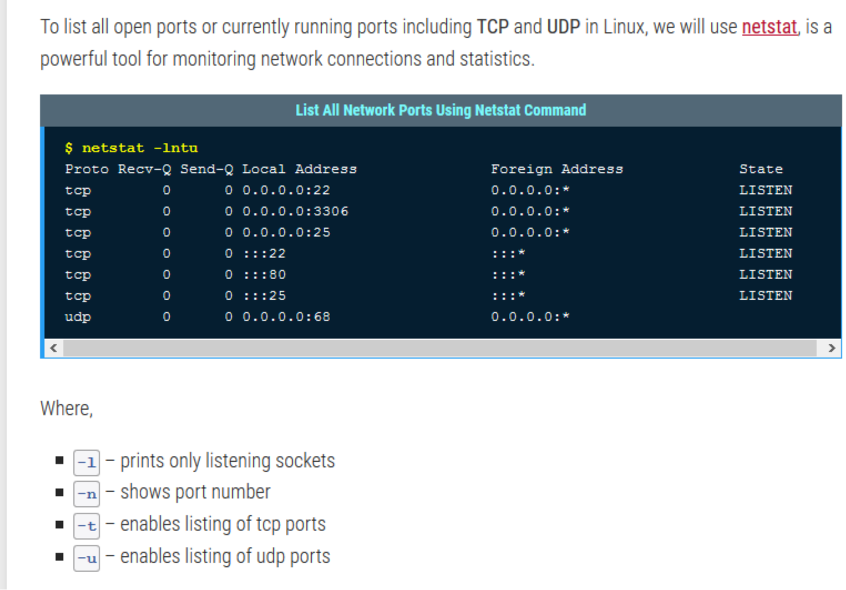


```
1  10.2.100.35 (10.2.100.35)  1.275 ms  0.326 ms  0.268 ms
[spadmin@Spectracom ~]$ dig 10.2.100.35

 <<>> DiG 9.4.1-P1 <<>> 10.2.100.35
; global options:  printcmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 27049
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

; QUESTION SECTION:
10.2.100.35.                    IN      A

; AUTHORITY SECTION:
                        600     IN      SOA     a.root-servers.net. nstld.verisi
gn-grs.com. 2012042001 1800 900 604800 86400

; Query time: 120 msec
; SERVER: 10.1.1.30#53(10.1.1.30)
; WHEN: Fri Apr 20 18:29:31 2012
; MSG SIZE  rcvd: 104

[spadmin@Spectracom ~]$
```

netstat and ss commands:

- ➢ Refer to “**netstat**” section in the Custserviceassist doc: ..\CustomerServiceAssistance.pdf
- ➢ Function: Shows network connections, routing tables, network status

https://www.tecmint.com/find-open-ports-in-linux/



To list all open ports or currently running ports including **TCP** and **UDP** in Linux, we will use netstat, is a powerful tool for monitoring network connections and statistics.

List All Network Ports Using Netstat Command

```
$ netstat -lntu
Proto Recv-Q Send-Q Local Address            Foreign Address          State
tcp        0      0 0.0.0.0:22               0.0.0.0:*                LISTEN
tcp        0      0 0.0.0.0:3306             0.0.0.0:*                LISTEN
tcp        0      0 0.0.0.0:25               0.0.0.0:*                LISTEN
tcp        0      0 :::22                    :::*                     LISTEN
tcp        0      0 :::80                    :::*                     LISTEN
tcp        0      0 :::25                    :::*                     LISTEN
udp        0      0 0.0.0.0:68               0.0.0.0:*
```

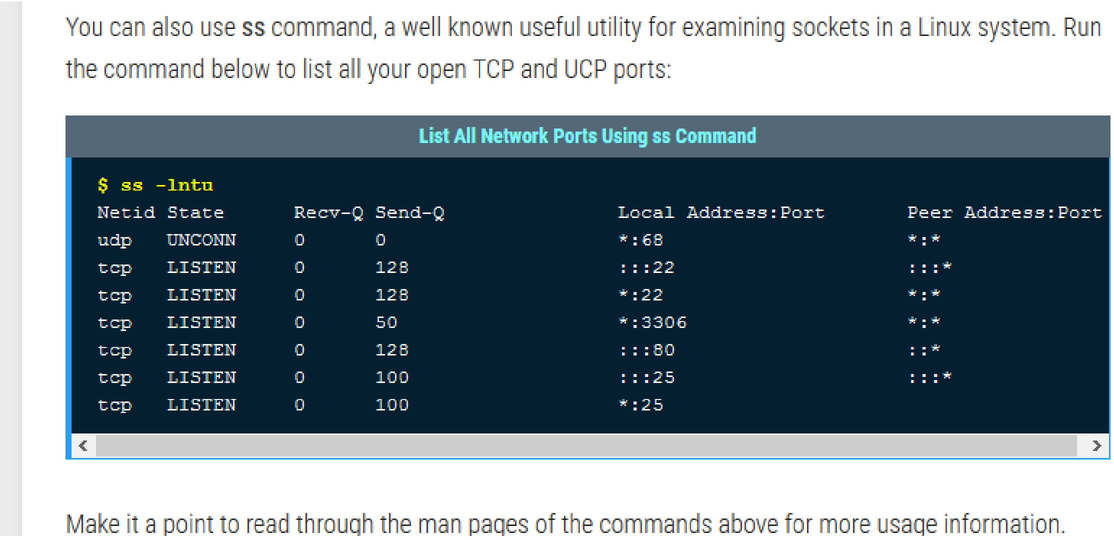
Where,

- `-l` – prints only listening sockets
- `-n` – shows port number
- `-t` – enables listing of tcp ports
- `-u` – enables listing of udp ports

- ➢ just type “**netstat**”, or can optionally add various combinations of swithches (list together)
- ➢ For more parameters and info, refer to: http://en.wikipedia.org/wiki/Netstat and https://www.tecmint.com/20-netstat-commands-for-linux-network-management/

ss -lntu command

- ➢ refer to L https://www.tecmint.com/find-open-ports-in-linux)



You can also use **ss** command, a well known useful utility for examining sockets in a Linux system. Run the command below to list all your open TCP and UCP ports:

List All Network Ports Using ss Command

```
$ ss -lntu
Netid State      Recv-Q Send-Q              Local Address:Port        Peer Address:Port
udp   UNCONN     0      0                   *:68                      *:*
tcp   LISTEN     0      128                 :::22                     :::*
tcp   LISTEN     0      128                 *:22                      *:*
tcp   LISTEN     0      50                  *:3306                    *:*
tcp   LISTEN     0      128                 :::80                     ::*
tcp   LISTEN     0      100                 :::25                     :::*
tcp   LISTEN     0      100                 *:25
```

Make it a point to read through the man pages of the commands above for more usage information.

Loopback interface/logical interface

- Refer to SR 6212 in SAP
- Refer to sites such as: http://www.cisco.com/c/en/us/td/docs/ios/12_2/interface/configuration/guide/finter_c/icflogin.html

Email from Paul Myers (8 Aug 16) They are thinking we are like a CISCO router.
http://www.cisco.com/c/en/us/td/docs/ios/12_2/interface/configuration/guide/finter_c/icflogin.html

I don't think I have an answer at this time as we did not support this. I don't know if we have an alternative interpretation of how to relate what we do to this. Are they talking about NTP interface only?

Loopback interface: a software-only, virtual interface that is always up and and allows BGP sessions to stay up, even if the outbound interface is down,.

From the link above(referring to a Cisco Router):
You can specify a software-only interface called a loopback interface to emulate an interface. Loopback interfaces are supported on all platforms. A loopback interface is a virtual interface that is always up and allows Border Gateway Protocol (BGP) and remote source-route bridging (RSRB) sessions to stay up even if the outbound interface is down.

You can use the loopback interface as the termination address for BGP sessions, for RSRB connections, or to establish a Telnet session from the device's console to its auxiliary port when all other interfaces are down. You can also use a loopback interface to configure IPX-PPP on asynchronous interfaces. To do so, you must associate an asynchronous interface with a loopback interface configured to run IPX. In applications in which other routers or access servers attempt to reach this loopback interface, you should configure a routing protocol to distribute the subnet assigned to the loopback address.

Packets routed to the loopback interface are rerouted back to the router or access server and processed locally. IP packets routed out the loopback interface but not destined to the loopback interface are dropped. This means that the loopback interface serves as the Null 0 interface also.

Samba software

Samba: "Samba is an Open Source/Free Software suite that provides seamless file and print services to SMB/CIFS clients." Samba is freely available, unlike other SMB/CIFS implementations, and allows for interoperability between Linux/Unix servers and Windows-based clients.

Q- I asked Paul M if SecureSyncs/9400s use Samba
A Reply from Paul (5/30/17) regarding SecureSyncs.9400s (as of at least v5.7.0). No the shipping product does NOT use samba. We can use it for development on the VMs, but shipping SecureSync's do NOT use this.

****user accounts and passwords (spadmin, spfactory, root, etc)

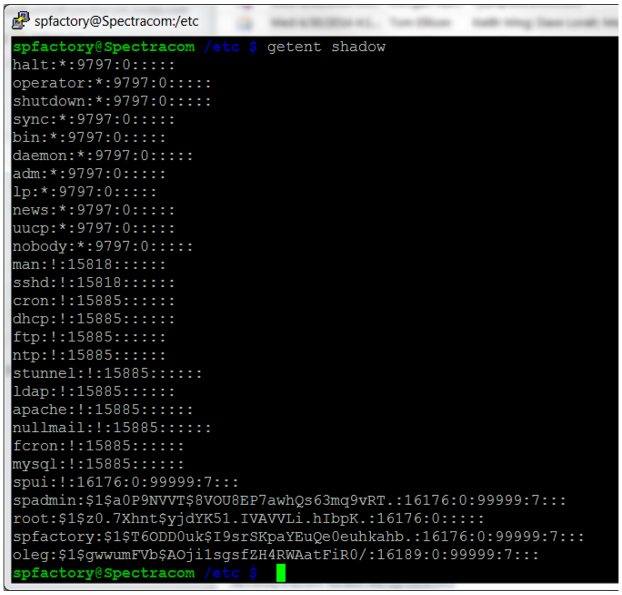
Default account passwords

******Default Username/Password**
Username: spadmin
Password: admin123

******Factory account Username/Password**
Username: spfactory
Password: (not provided for security reasons)

Viewing all accounts via the CLI interface: /etc and type: **getent shadow**. Scroll down to the bottom of the response.

> **Note**: Refer to "**Shadow**" in the "all products" section at the beginning of this document for deciphering this response.
>
> **Note**: Not sure if this command required spfactory login, or can work with admin rights. Also not sure if it works on 2400 SecureSyncs. Screenshot below is from 1200 SecureSync (not 2400)



```
spfactory@Spectracom /etc $ getent shadow
halt:*:9797:0:::::
operator:*:9797:0:::::
shutdown:*:9797:0:::::
sync:*:9797:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
nobody:*:9797:0:::::
man:!:15818::::::
sshd:!:15818::::::
cron:!:15885::::::
dhcp:!:15885::::::
ftp:!:15885::::::
ntp:!:15885::::::
stunnel:!:15885::::::
ldap:!:15885::::::
apache:!:15885::::::
nullmail:!:15885::::::
fcron:!:15885::::::
mysql:!:15885::::::
spui:!:16176:0:99999:7:::
spadmin:$1$a0P9NVVT$8VOU8EP7awhQs63mq9vRT.:16176:0:99999:7:::
root:$1$z0.7Xhnt$yjdYK51.IVAVVLi.hIbpK.:16176:0:::::
spfactory:$1$T6ODD0uk$I9srSKpaYEuQe0euhkahb.:16176:0:99999:7:::
oleg:$1$gwwumFVb$AOji1sgsfZH4RWAatFiR0/:16189:0:99999:7:::
spfactory@Spectracom /etc $
```

Accounts

cat /etc/passwd | grep -v nologin | grep /bin/bash

root:x:0:0:root:/root:/bin/bash This entry is for the root user, Linux.

spfactory:x:1000:110::/root:/bin/bash default This entry is for factory default login for Web U/I, CLI, and configuration.

spui:x:1001:0::/home/spectracom:/bin/bash? This entry is for the user of the Web U/I

spadmin:x:1002:111::/home/spectracom:/bin/bash default This entry is the factory default login for web U/I and CLI through serial or SSH terminal

Statement from Dave Sohn (Can be sent to customers) 20 Dec 2017

To Whom It May Concern;
The Spectracom Securesync provides remote access through only the spadmin and spfactory default accounts. The spfactory account password is only available to Spectracom employees for production and support use. However, the spfactory login can be disabled by the user, if desired.

All other accounts displayed in Linux such as root and spui etc are not accessible for remote access.

Summary table for Accounts (created by a customer and approved by Dave Sohn on 28 Mar 17)

Account	Roles	Login method	Account and Password owner	Can it be removed and what is the impact	Password can be reset / kept by user
spadmin	Admin account	Access via Ethernet (browser/CLI) or RS-232 (front panel Serial port)	Machine owner	It cannot be removed	Yes / Yes
Root group member					
spfactory	Factory account for factory engineer logon at factory	Access via Ethernet, RS-232	Manufacturer only	It can be removed. No impact.	No/No
spui	Web UI	No Access	Manufacturer only	It cannot be removed	No/No
root	OS super-user account	Cannot direct logon access. Must fist login as either spadmin or spfactory then “su”	Manufacturer only	It cannot be removed	No/No

Note: Details for each acount are below

A) spui account

- Also refer to info/emails in: ../../EQUIPMENT/SPECTRACOM%20EQUIPMENT/SecureSync/Accounts%20(root%20and%20spui)
- account used **internally only** for the web browser
- must be logged into **root** to access **spui** (can't log directly into spui)

Access to the spui account

MUST be logged into root to access spui (can't log directly into spui account)

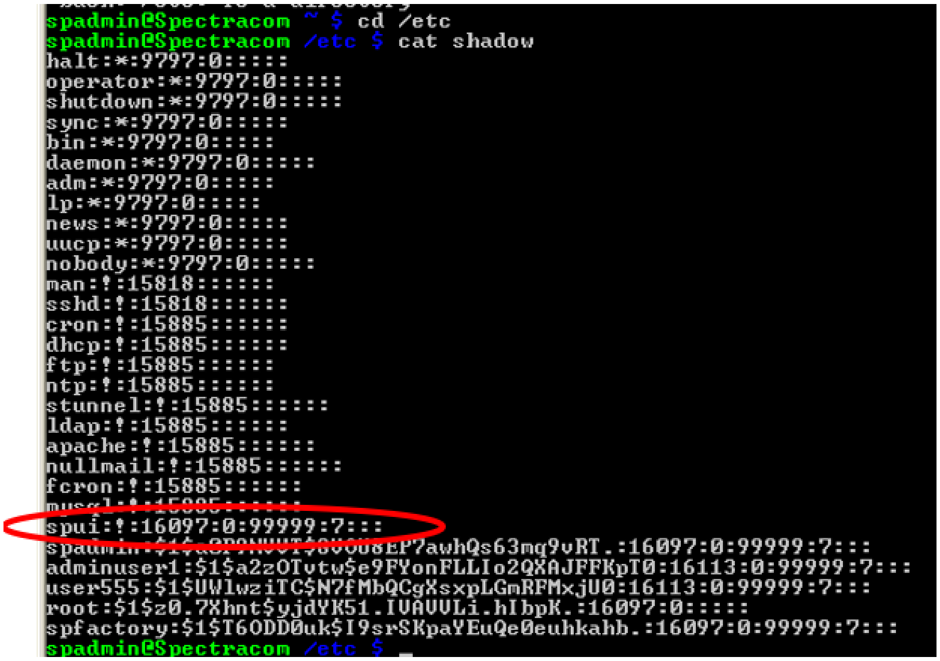
- Refer to **Root account** login info in the next section below for details on root access
- email in the link above helpS expiain how spui access is blocked for all external connections

Other info about the spui account

shadow file

- located in the **home/Spectracom/xfer/config** directory (exported in the config bundle file)
- The shadow file shows that the spui user has its password locked. Here is the spui entry in that file:

spui:!:17710:0:99999:7:::



```
-bash: /etc: is a directory
spadmin@Spectracom ~ $ cd /etc
spadmin@Spectracom /etc $ cat shadow
halt:*:9797:0:::::
operator:*:9797:0:::::
shutdown:*:9797:0:::::
sync:*:9797:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
nobody:*:9797:0:::::
man:!:15818::::::
sshd:!:15818::::::
cron:!:15885::::::
dhcp:!:15885::::::
ftp:!:15885::::::
ntp:!:15885::::::
stunnel:!:15885::::::
ldap:!:15885::::::
apache:!:15885::::::
nullmail:!:15885::::::
fcron:!:15885::::::
mysql:!:15885::::::
spui:!:16097:0:99999:7:::
spadmin:$1$[illegible]8EP7awhQs63mq9vRT.:16097:0:99999:7:::
adminuser1:$1$a2zOTvtw$e9FYonFLLIo2QXAJFFKpT0:16113:0:99999:7:::
user555:$1$UWlwziTC$N7fMbQCgXsxpLGmRFMxjU0:16113:0:99999:7:::
root:$1$z0.7Xhnt$yjdYK51.IVAVVLi.hIbpK.:16097:0:::::
spfactory:$1$T6ODD0uk$I9srSKpaYEuQe0euhkahb.:16097:0:99999:7:::
spadmin@Spectracom /etc $ _
```

Q Is there something we can verify? We don't have access to shadow.

A (per Ron Aug, 2018) If you save a configuration bundle it will be located in **the /home/Spectracom/xfer/config directory.**
The file will be called **securesync.conf.**
I tested as spadmin and you can issue the following CLI command to see the spui shadow line in the configuration bundle:

zgrep -a spui:\!: securesync.conf

B) Root account / Root password (OS super-user account)

- Also refer to info/emails in: ../../EQUIPMENT/SPECTRACOM%20EQUIPMENT/SecureSync/Accounts%20(root%20and%20spui)

Logging in as root

Remote access to the root account is not available/blocked

- **v5.8.1 and below:** direct connect to root account via serial cable only (see note belowm indicating this will be changing in 5.8.2 and above
- **v5.8.2 and above** **Note email from Ron Dries (16 Aug 2018) before 5.8.2 was released** The front panel RS-232 serial port does currently allow root login (v5.8.1 and below). However, we intend on changing this front panel functionality in the next SecureSync software update (version 5.8.2) , so that root login won't be available with a direct serial connection, either

Per Dave Sohn (20 Dec 17) "…All other accounts displayed in Linux, such as root and spui, etc, are not accessible for remote access."

Q Does the root account have interactive logon privileges?
A Keith's response: NO. Root is for factory use only and you **have to attach directly to the processor board inside the chassis to be able to login as root** (cannot connect to root via Ethernet connection).

Q If so, by what mechanism do I change the root password?
A Keith's response: You cannot delete the root account, but it is not useable unless you gain physical access to physical connections inside of the SecureSync. You cannot change its password. However, you can delete the **spfactory** user from the **Management**->**Authentication** page of the browser to meet this goal. We don't login as root, but login as spfactory and can then use sudo to do 'root things'.

You must delete/remove the spfactory account to meet this requirement.

Q Why we do not disclose the root password
A Email from Paul Myers to Wade Sober (8 July 2013) We do not give out the Root password because we do not want configuration changes made to the product, as they can destroy the software stability or installation.

Note about root account

Much earlier Email from Mike Sander: The only way to get at the "root" account is log-in as another user, then switch to root. There is no way to log on directly as "root", not through the serial port and certainly not remotely.

Once the user changes the spadmin password, there is no way for anyone to use the root password without also knowing a password created by the customer.

Our position is that root is not an account, in the sense that it does not provide access to the system.

Keith's response to customer

To begin, root is not an available login account, because there is no way to directly login to the appliance with a root account. The highest login account is the default "spadmin" account. The root account is barred from being a login account on all ports, including the Ethernet interface and the front panel interfaces (keypad and SERIAL port).

Root can only be accessed through another login account, such as the default "spadmin" account or a user account that has been created. Once a user changes the default spadmin password (as is highly recommended, since the spadmin password is a published value), there is no way to access root without knowing the new spadmin account passwords (or one of the user account passwords), even if someone was to know what the root password happens to be.

Another Email Keith sent: Though it's not possible to directly deactivate the root account directly, it is possible to remove access to it. Access to the root account is only available via either the factory default "spfactory" account or another user account (Access to root is only available after logging into a user account and then switching to root). The spfactory account can be removed, if desired, thereby removing access to the root account via the spfactory account. Once the spfactory account has been removed, and the spadmin account password has been changed from the default value (as is highly recommended, since the spadmin password is a published value), access to root is no longer available.

The “spfactory” account can be deleted as desired, thereby removing all access to the root account from that point forward (unless a restore to factory defaults is performed using the software update process- not just by performing a standard “clean” of the configurations).

To remove the default spfactory account (inhibiting access to the root account)

- Refer to the “**spfactory account**” info in the next section below.

Must be logged into the root account first, to have access to the the spui account (cannot log directly into spui)

Note: details/email exchanges below were with Ron Dries for WAPA (~July/Aug 2018)

- In the PAM config files, we use **pam_securetty.so** to ensure that the root account cannot be logged into.There is a config file in SecureSyncs called **securetty** (as in “secure tty”) which lists the terminals that root is allowed to login to.

Q As mentioned before, when we look at the output of the local “passwd” file indicates that a Shell is available to them so that makes it appear as though we can login into them. For compliance purposes, we need to be able to provide evidence. Since we cannot change the password on root and spui, we need to be able to either prove that they cannot be logged into or show vendor documentation that the passwords were generated pseudo-randomly and are thereby unique to the device.
We need your assistance to find a command or setting in a local file to prove they cannot be logged into, or some documentation asserting that the passwords are random and unique.
Reply from Keith (based on info from Ron) In the PAM config files. we use **pam_securetty.so** to ensure that the root account cannot be logged into.There is a config file in SecureSyncs called **securetty** (as in “secure tty”) which lists the terminals that root is allowed to login to.
In the next SecureSync software version upgrade (note from Keith- Shoud be in 5.8.2) , this will be updated to also not allow root login from the front panel serial port.
Here is an example of the PAM login config file, with the line that uses this config file highlighted:

```
 cat /etc/pam.d/login
auth include /etc/tacacs_pam.conf
#auth requisite pam_securetty.so
auth required pam_tally.so deny=5 unlock_time=60 per_user
auth requisite pam_nologin.so
auth required pam_env.so
auth sufficient pam_unix.so try_first_pass
auth required pam_deny.so
account required pam_securetty.so
account include /etc/tacacs_pam.conf
account required pam_tally.so
account sufficient pam_unix.so
account required pam_deny.so
session include /etc/tacacs_pam.conf
session required pam_motd.so
session required pam_limits.so
#session optional pam_lastlog.so
session required pam_unix.so
password required pam_unix.so shadow md5
```

Q What about the spui account? How do we prove that it can’t login. Does the securetty clearly show that root can’t login? What about spui? I couldn’t find in ssh_config where this is related. If we configure in the /etc/security/access.conf to deny root and spui tty access would that work or is it ignored by the system?
A (email from Ron) In the /etc/shadow file for spui there is an “!” for spui.

The “!” point means the password is locked and login with a Unix password is disabled.

The root user is the only user that is able to get access to spui.

An empty securetty file will disable root login for any console device. This will be added in the next release.

The ssh_config file has “PermitRootLogin no”.

C) spfactory account

- Per Dave Sohn (20 Dec 17) The spfactory account password is only available to Spectracom employees for production and support use. However, the spfactory login can be disabled by the user, if desired.

Function: The spfactory account provides our Engineers with the ability to able to remotely connect and have root access to the server, if it was necessary for some reason (root privilege is only available by first logging into the spfactory account).   The spfactory account can be safely removed with no detrimental effects (We just will be no longer able to remote in with root permissions).

Deleting the Spfactory account

- This account provides our Engineers with the ability to able to remotely connect and have root access
- Once this account has been deleted, it can't be re-enabled, unless the unit is restored to factory defaults (not just cleaned or updating the software to a newer version. We can no longer remote in with root permissions.
- There are no other detrimental effects of deleting the spfactory account.

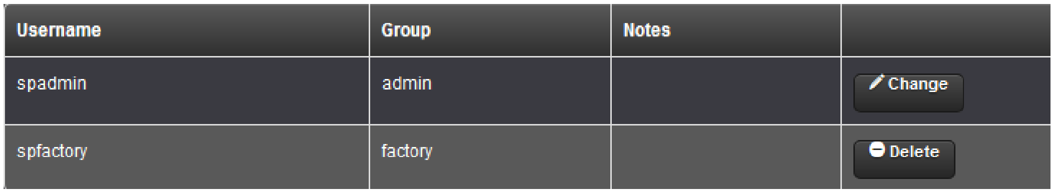
The spfactory account provides our Engineers with the ability to able to remotely connect and have root access to the server, if it was necessary for some reason (root privilege is only available by first logging into the spfactory account).   The spfactory account can be safely removed with no detrimental effects (We just will be no longer able to remote in with root permissions).

However, once the spfactory account has been deleted, it can't be re-enabled, unless the unit is "restored to factory defaults" (not just "cleaned" or the software updated to a newer version).

1. Using the web browser to delete the spfactory account

Note: Once the spfactory account has been deleted, it can't be re-enabled, unless the unit is "restored to factory defaults" (not just "cleaned" or the software updated to a newer version).

1) Login as spadmin or other custom account in the Admin group (custom accounts in the User group don't have permissions to delete the spfactory account)
2) Navigate to the **Management** -> **Authentication** page of the browser
3) Under "**Users**", press the **Delete** button next to spfactory.



Username	Group	Notes	
spadmin	admin		✎ Change
spfactory	factory		⊖ Delete

Protection/encryption of local account passwords

- Refer to (in this document): ****/etc/shadow (Linux password file)

Account Passwords

User accounts / Permissions

Creating new accounts/Editing accounts

As of at least Archive version 4.8.9:

- SecureSync's user accounts can only be managed (editing user names, changing passwords, etc) via the web browser (HTTP/HTTPS)
- User accounts cannot be created or edited via CLI commands using telnet or SSH.

viewing user accounts

- created user accounts and Passwords are stored/viewed in **"/etc/shadow**" (customers cannot view with spadmin. Must be logged in as **spfactory** to view the contents of this file

Rules for usernames (versions 5.1.2 and above, when using the newer browser)

- **Length**: Can be between 3 and 32 characters long.
- **Must start** with a lower-case letter.
- All letters must be lower-case.
- **Accepts**: all letters, numbers, underscores and dashes. It **does not** accept special characters such as the following characters **! @ # $ % ^ & * ( )**

- MAX Number of accounts that can be created: Per Ron Dries (21 Oct 2014) he is not aware of any established limit on the number of user accounts that can be created. There should be no limit.

  - **Newer browser (versions 5.1.2 and above)** Accounts and passwords are managed in the **Management** -> **Authentication** page of the browser. Click on the "+" sign in the upper-right corner to create new user accounts.
  - **Classic Interface** Accounts and passwords are managed in the **Tools** -> **Users** page of the browser

Users can be assigned to be in either the user group or the admin group. Users in the admin group can't make configurations changes. Configuration changes can only be made via the Admin account or a user account that is in the Admin group.

The **Tools** -> **Users** page allows password management (in order to edit User accounts, have to be logged in as either Admin or a user account that is configured to be in the admin).

Permissions

- Group Rights/privileges are exactly the same for both SSH and web browser login

Note: Information below is based on version 5.1.2 (future versions may change this info)

Note: Red text below indicates items that are different for the group as compared to the spadmin account

spadmin account

No limitations
Can manage passwords/user accounts

admin group

No limitations

Same as spadmin account

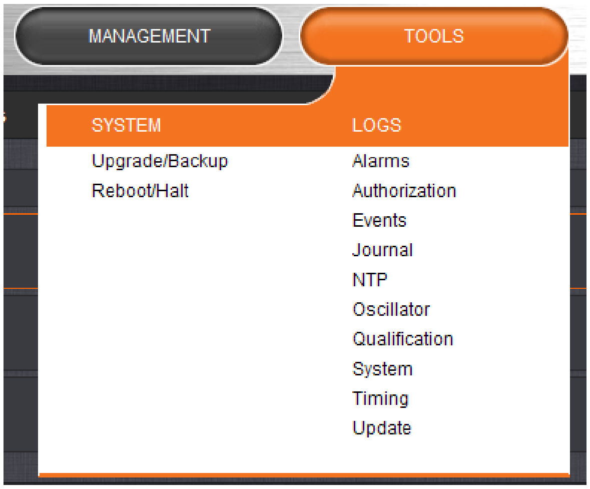
user group

I'll start by saying the privileges for user and admin groups are exactly the same whether logging in via the web browser or connecting via SSH.

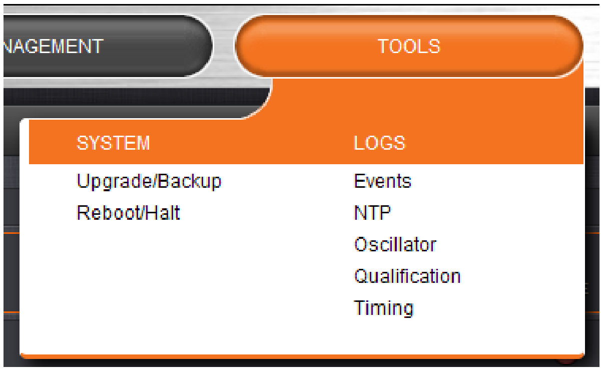
The following is the information for the new web browser with version 5.1.2 software installed. The easiest way to see the differences is to compare the web browser menus for an admin and a user side-by-side. You will then be able to notice ~~what capabilities are not available to th~~ose that login with SSH or the browser as a member of the user group.

1. Tools menu

With admin rights



with only user rights



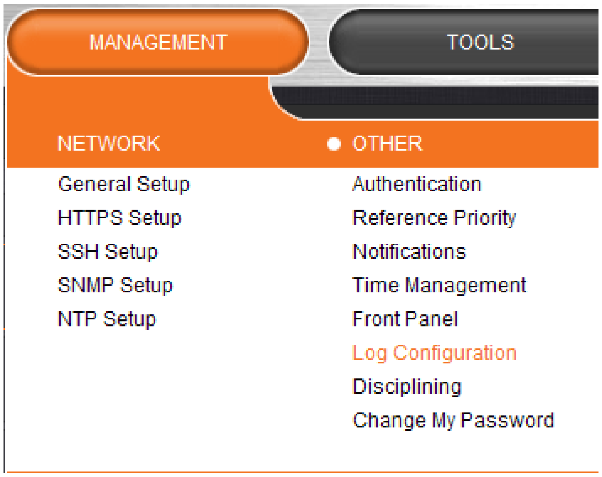
Logs: Limited logs can be viewed by user (only the listed logs can be viewed)

Upgrade/Backup: User cannot access this page (Goes to the Home page). Can't perform any updates.

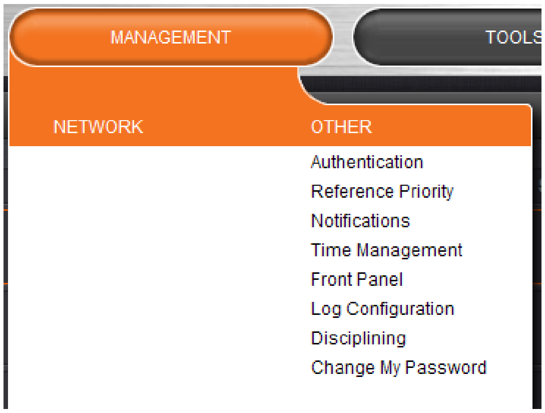
Reboot/Halt: User cannot access this page. Can't reboot/shutdown/halt.

2. Management menu

With admin rights



with only user rights

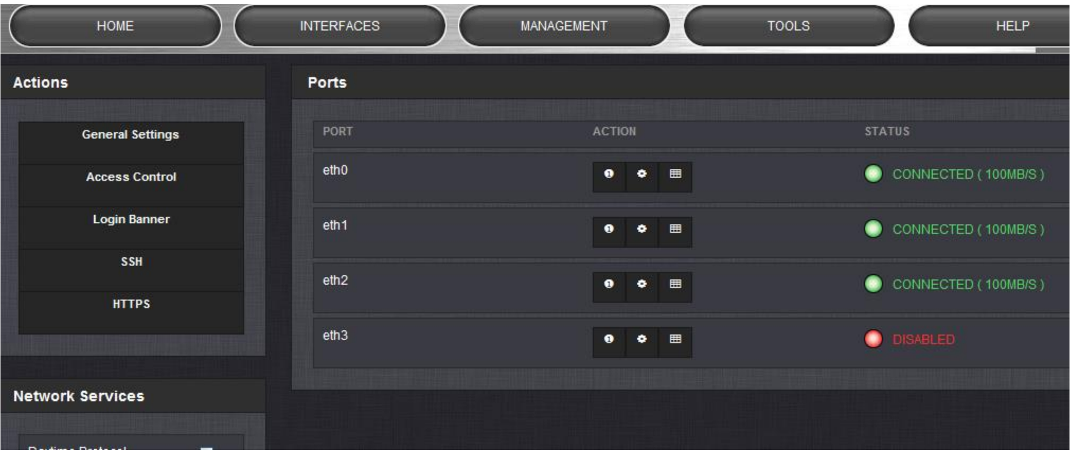


Network: Users cannot modify any of the network-related configurations (if they click on “Network”), they can only view the **Tools** -> **Network** page. But they can’t make any modifications to this page. They cannot access HTTPS, SSH, SNMP or NTP pages (cannot view or change current settings).

As shown below, when logged in as user and “Network is selected, the “Actions” buttons (for General Settings, Access Control, login banner, SSH and HTTPS) normally located on the left-side of the screen is not available. Also, when logged in as a user, the only one of the three normally available boxes for the ports is the status box (users can’t make changes to the network settings or disable Ethernet ports).

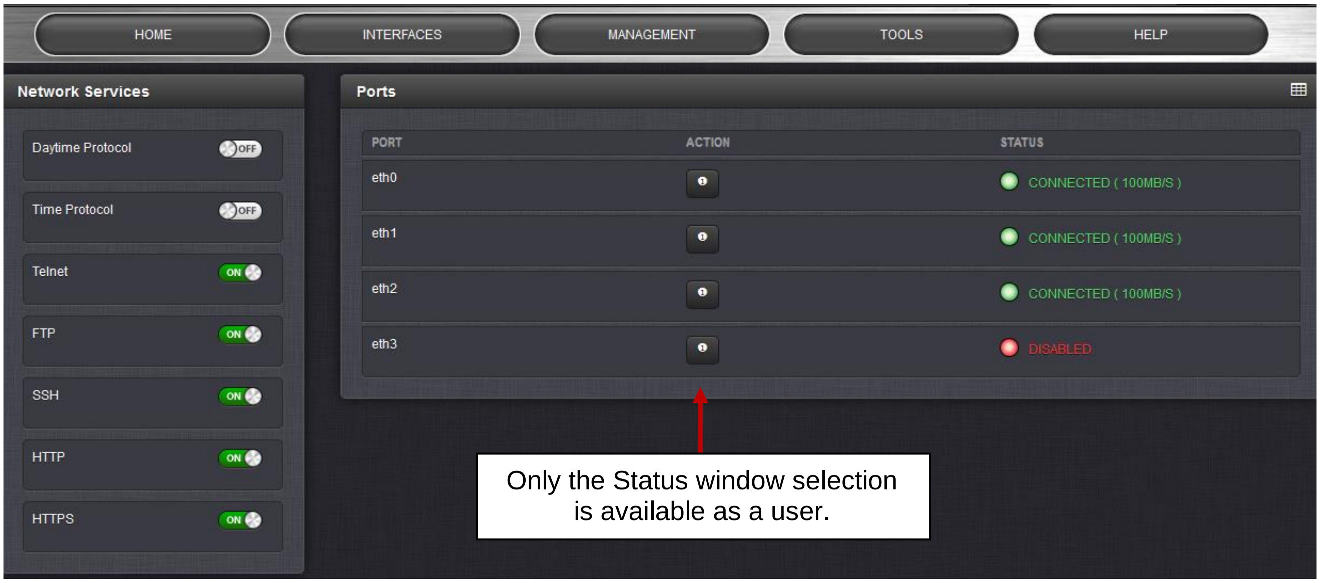
admin account:

These selections are only available as spadmin



PORT	ACTION	STATUS
eth0		CONNECTED (100MB/S)
eth1		CONNECTED (100MB/S)
eth2		CONNECTED (100MB/S)
eth3		DISABLED

User account

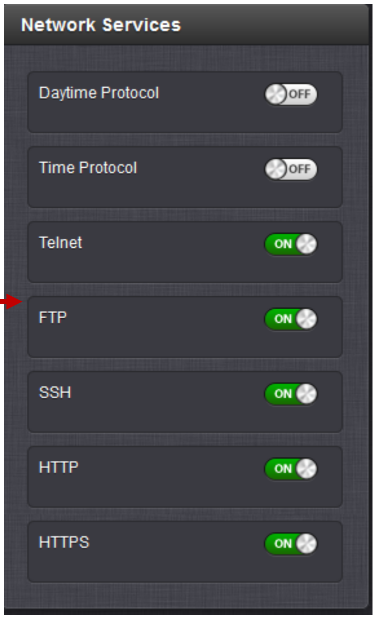


Network Services	
Daytime Protocol	OFF
Time Protocol	OFF
Telnet	ON
FTP	ON
SSH	ON
HTTP	ON
HTTPS	ON

PORT	ACTION	STATUS
eth0		CONNECTED (100MB/S)
eth1		CONNECTED (100MB/S)
eth2		CONNECTED (100MB/S)
eth3		DISABLED

Only the Status window selection is available as a user.

Network Services (such as telnet, FTP, SSH and HTTP/HTTPS): Can move the switches, but they won't do anything. So a user cannot enable or disable any Services. Browser will report "Setting FTP Failed" if a switch is moved.



Network Services

Daytime Protocol OFF

Time Protocol OFF

Telnet ON

FTP ON

SSH ON

HTTP ON

HTTPS ON

"**Network Services**" Switches do not allow a "user" to be able to enable or disable any Services (must be an admin to enable/disable)

Authentication: Users can access this page but can only change their own password. Users cannot create any new accounts and can't modify any accounts, other than changing their own password.

Reference Priority: Users can access this page and modify settings.

Notifications: Users can access this page and modify settings.

Time Management: Users can access this page and modify settings.

Front panel: Users can access this page and modify settings.

Log Configuration: Users can access this page and modify settings.

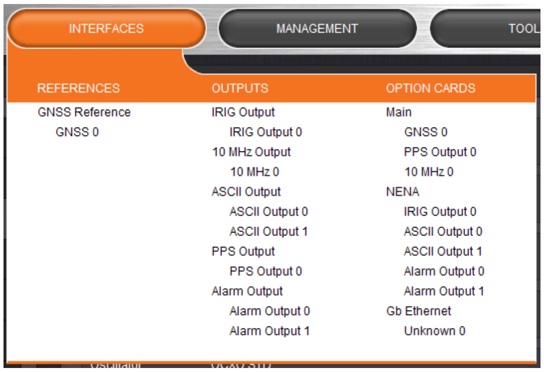
Disciplining: Users can access this page and modify settings.

Change my password: Users can access this page and change only their password.

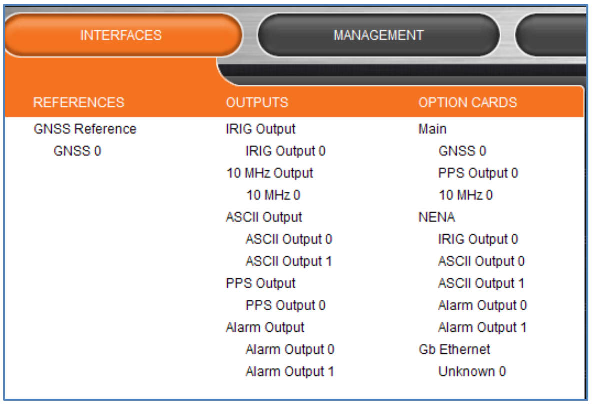
Interfaces menu

Note: No differences in privileges for this menu and all items listed. User and admin accounts can view and modify all settings in these pages (can view/edit GPS receiver, outputs and Option Cards)

admin



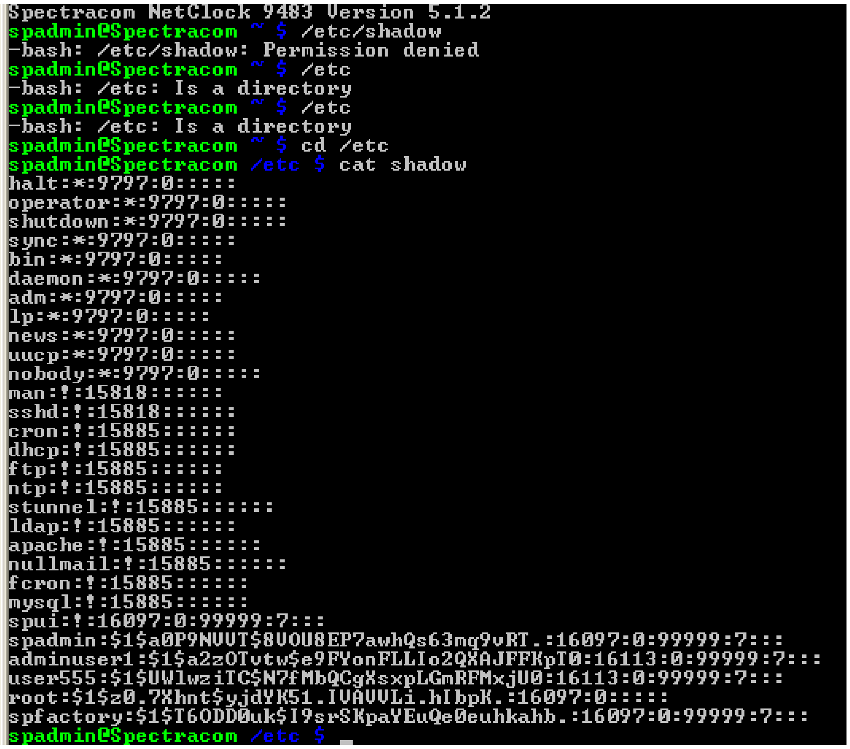
user



****/etc/shadow (Linux password file)

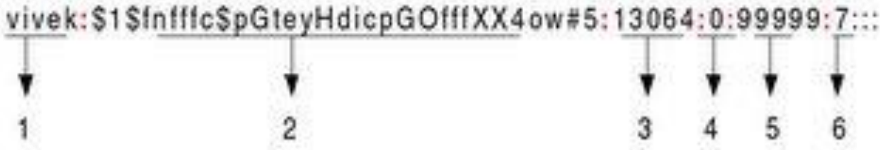
- Refer to: http://www.cyberciti.biz/faq/understanding-etcshadow-file/ http://searchsecurity.techtarget.com/definition/shadow-password-file
- Customers (spadmin) do not have permission to view/change this file
  - (“Without root access we can’t view the shadow file The ssh_config file does not have “PermitRootLogin no” in it).

/etc/shadow file stores actual password in encrypted format for user's account with additional properties related to user password i.e. it stores secure user account information. All fields are separated by a colon (:) symbol. It contains one entry per line for each user listed in /etc/passwd file Generally, shadow file entry looks as follows (click to enlarge image):



```
Spectracom NetClock 9483 Version 5.1.2
spadmin@Spectracom ~ $ /etc/shadow
-bash: /etc/shadow: Permission denied
spadmin@Spectracom ~ $ /etc
-bash: /etc: Is a directory
spadmin@Spectracom ~ $ /etc
-bash: /etc: Is a directory
spadmin@Spectracom ~ $ cd /etc
spadmin@Spectracom /etc $ cat shadow
halt:*:9797:0:::::
operator:*:9797:0:::::
shutdown:*:9797:0:::::
sync:*:9797:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
nobody:*:9797:0:::::
man:!:15818::::::
sshd:!:15818::::::
cron:!:15885::::::
dhcp:!:15885::::::
ftp:!:15885::::::
ntp:!:15885::::::
stunnel:!:15885::::::
ldap:!:15885::::::
apache:!:15885::::::
nullmail:!:15885::::::
fcron:!:15885::::::
mysql:!:15885::::::
spui:!:16097:0:99999:7:::
spadmin:$1$a0P9NVUT$8VOU8EP7awhQs63mq9vRT.:16097:0:99999:7:::
adminuser1:$1$a2zOTvtw$e9FYonFLLIo2QXAJFFKpT0:16113:0:99999:7:::
user555:$1$UWlwziTC$N7fMbQCgXsxpLGmRFMxjU0:16113:0:99999:7:::
root:$1$z0.7Xhnt$yjdYK51.IVAVVLi.hIbpK.:16097:0:::::
spfactory:$1$T6ODD0uk$I9srSKpaYEuQe0euhkahb.:16097:0:99999:7:::
spadmin@Spectracom /etc $ _
```

/etc/shadow file fields



- **User name** : It is your login name
- **Password**: It your encrypted password. The password should be minimum 6-8 characters long including special characters/digits
- **Last password change (lastchanged):** Days since Jan 1, 1970 that password was last changed
- **Minimum**: The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
- **Maximum**: The maximum number of days the password is valid (after that user is forced to change his/her password)
- **Warn**: The number of days before password is to expire that user is warned that his/her password must be changed
- **Inactive**: The number of days after password expires that account is disabled

- **Expire**: days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used:

Protection/encryption of the local account passwords/shadow file

- Encoding/protection of the password file is automatic- no user interaction is required
- we use the standard Linux /etc/shadow file/encprytion- we don't change anything
- refer to sites such as :

  https://www.slashroot.in/how-are-passwords-stored-linux-understanding-hashing-shadow-utils
  https://www.oreilly.com/library/view/practical-unix-and/0596003234/ch04s03.html
  http://web.deu.edu.tr/doc/oreily/networking/puis/ch08_06.htm

https://www.oreilly.com/library/view/practical-unix-and/0596003234/ch04s03.html

As the name implies, a shadow password file is a secondary password file that *shadows* the primary password file. On Solaris and Linux systems, the shadow password is usually stored in the file */etc/shadow* and contains the encrypted password and a password expiration date. The */etc/shadow* file is protected so that it can be read only by the superuser. Thus, an attacker cannot obtain a copy to use in verifying guesses of passwords.

http://web.deu.edu.tr/doc/oreily/networking/puis/ch08_06.htm

…UNIX avoids this problem by not keeping actual passwords anywhere on the system. Instead, UNIX stores a value that is generated by using the password to encrypt a block of zero bits with a one-way function called *crypt( )*; the result of the calculation is (usually) stored in the file */etc/passwd*. When you try to log in, the program */ bin/login* does not actually decrypt your password. Instead, */bin/login* takes the password that you typed, uses it to transform another block of zeros, and compares the newly transformed block with the block stored in the */etc/passwd* file. If the two encrypted results match, the system lets you in.

The security of this approach rests upon the strength of the encryption algorithm and the difficulty of guessing the user's password. To date, the *crypt* () algorithm has proven highly resistant to attacks

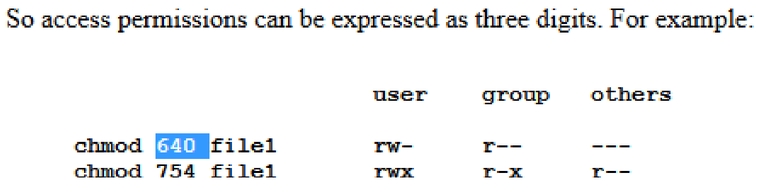
two questions from a customer:

- Are local stored credential encrypted? If yes, what type of encryption is used to encrypt local passwords? And how to enable it?
- What type of authentication mechanism used for local authentication? Are there different settings can be configured?

Answers: The answers to both questions above is dependant on software version installed (5.5.0 and above/5.4.5 and below)

A) Software Versions 5.5.0 and higher

Per Paul Myers (6 Mar 17) The /etc/shadow folder in release 5.5.0 and higher is **permissions 640** and **hides user passwords hashes**. Please upgrade to the version 5.5.1.



So access permissions can be expressed as three digits. For example:

```
                        user     group    others

chmod 640 file1         rw-      r--      ---
chmod 754 file1         rwx      r-x      r--
```

B) Software Versions 5.4.5 and below

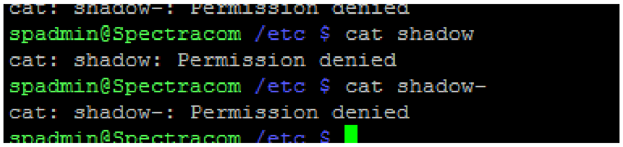
Per Ron Dries (24 Feb 16) As of at least versions 5.4.0 and below, we just use the standard Linux shadow file for storing and protecting passwords. There are some limitations to this encryption mechanism, but a user has to be logged in already in order to access/view the file.

- For more info on the protection of the shadow file, refer to websites such as: http://searchsecurity.techtarget.com/definition/shadow-password-file

  "The original password is encrypted (or encoded) by using a randomly-generated value or encryption key between

1 and 4096 and a one-way hashing function to arrive at the encoded password that is actually stored. Note that the stored result is not something that you can enter as a password itself.

- In at least versions 5.8.1 and below, there are no options/capabilities available to change the password protection.
- The shadow file for storing passwords is located: **/etc/shadow**
- The shadow file cannot be viewed by either spadmin or other user accounts (must be logged in as spfactory to view it) (the screenshot below is while logged in as spadmin)



```
cat: shadow-: Permission denied
spadmin@Spectracom /etc $ cat shadow
cat: shadow: Permission denied
spadmin@Spectracom /etc $ cat shadow-
cat: shadow-: Permission denied
spadmin@Spectracom /etc $ 
```

Desire to change the root password and/or spfactory account password

- The root password and spfactory account password cannot be changed. However, the spfactory account can be deleted, which removes all remote access to the root account.
- Refer to the Account information further above for info on removing the spfactory account to remove access to spfactory and therefore also root.

spui account protection

Q What about the spui account? How do we prove that it can’t login. Does the securetty clearly show that root can’t login? What about spui? I couldn’t find in ssh_config where this is related. If we configure in the /etc/security/access.conf to deny root and spui tty access would that work or is it ignored by the system?

A (email from Ron) In the /etc/shadow file for spui there is an “!” for spui.

The “!” point means the password is locked and login with a Unix password is disabled.

Reset the SPADMIN account password

Reset the spadmin account password back to default value

A) Via the CLI interface

- If current password is known, **resetpw** CLI command will reset the password back to admin123

B) Via the front panel menus

- As of at least versions 1.6.0 and below, there is no '***resetpw'*** menu command (unlike the 1200 SecureSyncs)
  - Refer to JIRA ticket DMND-1958 (created 15 March 2023) requesting **resetpw** command be added to 2400 front panel menu selection.
- Besides remote login via the **spfactory** account (if this account hasn't already been removed and remote login is allowed) being able to change the spadmin account password, the other option is to use the available front panel "**Restore Factory Default**" menu selection. Though less-desirable than having **resetpw** cli command available (as this menu selection restores all configs back to default settings), at least the user will be able to access the unit again.

- ~~The front panel **resetpw** command will reset the password back to admin123, even if it's been recently changed less than 10 password changes ago (it will override the "remember" of not allowing password re-use before 10 other passwords have been used.~~

~~**Note**: resetpw on front panel also disables LDAP/Radius (versions 5.2.1 and above)~~
~~Starting in version 5.2.1 (~Apr 2015) **resetpw also sets LDAP and Radius to "Disabled"** to help prevent total lockout. They need to be re-enabled thereafter, if desired. Refer to Mantis case 3026~~

~~Q help to clarify that if the RESETPW on panel LCD is used, will it erase all the machine configuration to default or just reset the spadmin password to default value?~~
~~A **Keith's response** (23 May 17) Unlike the CLEAN command, the RESETPW command will NOT erase all the configurations back to default. The RESETPW command only resets the spadmin account password back to the default value of 'admin123'.~~

~~Note that in software versions 5.2.1 and above, the RESETPW command also disables Radius and LDAP remote authentication services (if enabled for use). This command doesn't change the configurations for these two services. It just unselects the checkbox which enables/disables the functionality of these services. So after performing a RESETPW command, the enable checkbox(es) for LDAP and/or Radius need to be reselected, if using either or both of these authentication services.~~

~~**Note:** Applicable to SecureSync and Model 9483 only (not applicable to 9489)~~

- ~~When the spadmin account password is known, it can be reset back to factory default via the web browser, front panel keypad or via the front panel SERIAL port.~~
- ~~If the password is not known, it can be reset back to factory default via the front panel keypad or via the front panel SERIAL port (web browser won't be accessible without knowing the password).~~
- ~~The Serial command to reset the password via the Serial port is "resetpw"~~
- ~~Front panel keypad admin account password reset is via the **System -> Cmd** menus~~
- ~~**Versions 5.2.1 (12 May 2015) and above:** resetpw command also disables LDAP and Radius (see additional info below).~~

Retrieving/Changing user account passwords

**Retrieving unknown account password

- Passwords can be changed, but can’t be retrieved.
- Passwords are stored in “**/etc/shadow**”.
- Passwords are “hash” protected (encrypted) when they are created. They can be “viewed” but can’t tell what they really are.

Changing user account passwords

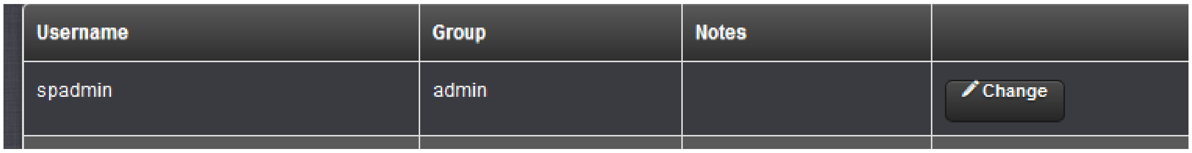
Note: Further below are the “rules” for creating/changing usernames and passwords (what’s allowed. What’s not allowed, etc)

A) Via the CLI interface

- The CLI command to change only the spadmin account password (if current password is known) is **passwd**
- Refer to the CLI section of this document for more info (such as how in at least version 5.6.0 and below, the available ‘Password Security’ rules don’t apply (are bypassed) when the spadmin account password is changed via this cli command): Available CLI calls (API calls)

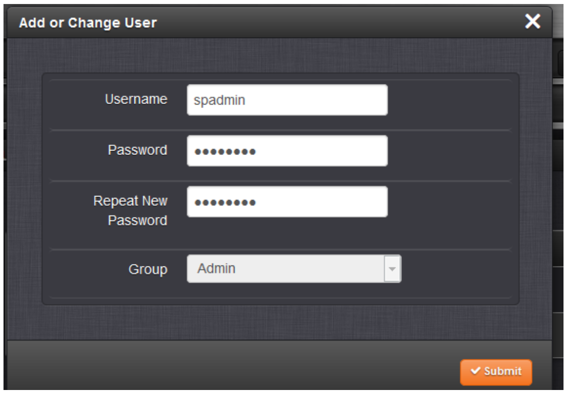
B) Using the Newer web browser (versions 5.1.2 and above)

1) Login as spadmin or other custom account in the Admin group (custom accounts in the user group don’t have permissions to change passwords)
2) Navigate to the **Management** -> **Authentication** page of the browser
3) Press the “**Change”** button next to the desired account name to change the password



Username	Group	Notes	
spadmin	admin		Change

4) This will open a pop-up window. Enter the desired new password and press Submit.



Add or Change User

Username: spadmin

Password: ••••••••

Repeat New Password: ••••••••

Group: Admin

“Password Security” (Available minimum password rules/requirements that can be enforced, if desired)

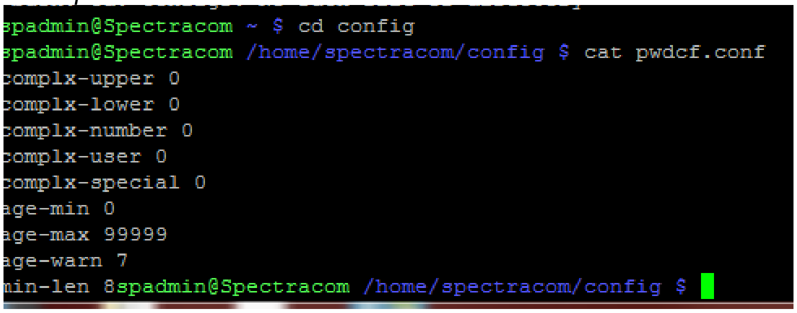
There are several other minimum password requirements which can be enabled as desired. These include rules such as minimum length of passwords, required use of either capital and/or lower-case letters, numerals, special characters, password expiration (with expiration warning), etc.

These special requirements for creating new passwords going forward or changing existing passwords in the future can be enforced via the “**Security Policy**” (**Management** -> **Authentication** page of the browser. Click on “**Security Policy**” on the left side of the page) as shown below. These minimum password requirements include the following:

1. With newer black/charcoal web browser (v5.1.2 and above)

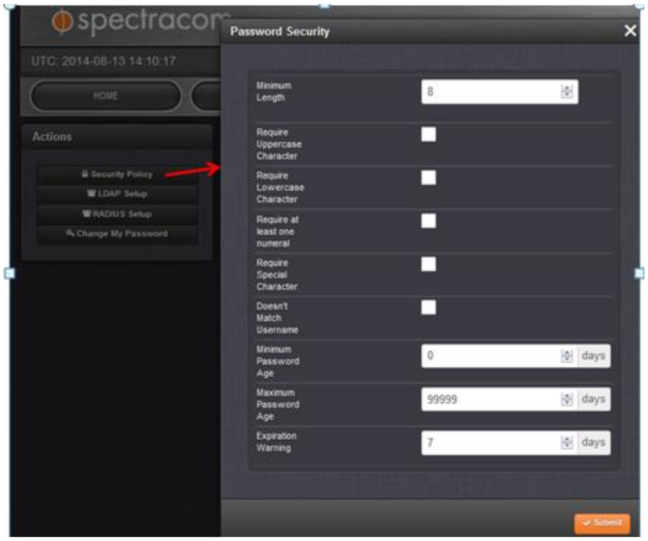
Note: Password complexity settings are stored in ***pwdcf.conf*** file (located in **home/spectracom/config directory**)

Example below



```
spadmin@Spectracom ~ $ cd config
spadmin@Spectracom /home/spectracom/config $ cat pwdcf.conf
complx-upper 0
complx-lower 0
complx-number 0
complx-user 0
complx-special 0
age-min 0
age-max 99999
age-warn 7
min-len 8spadmin@Spectracom /home/spectracom/config $
```

- ➢ Consists of: password aging, password length, complex passwords and delete the default spfactory account
  - Software Versions 5.1.2 and above**: in the **Management** -> **Authentication** page of the browser. Click on **Security policy** on the left side of the page
- ➢ There are several other minimum password requirements which can be enabled as desired, via “Security Policy” (Management -> Authentication page of the browser. Click on “Security Policy” on the left side of the page) as shown below. These minimum password requirements include the following:



Minimum Length: 8
Require Uppercase Character: □
Require Lowercase Character: □
Require at least one numeral: □
Require Special Character: □
Doesn't Match Username: □
Minimum Password Age: 0 days
Maximum Password Age: 99999 days
Expiration Warning: 7 days

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

- ➢ Refer to SF case 117138

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

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

Created By: Ron Dries (10/17/2017 2:47 PM) | Last Modified By: Ron Dries (10/17/2017 2:47 PM)
The directory '/var/db/pkg' did not exist in either software versions 5.4.1, or 5.6.0. I am not sure how the Nessus credentialed scan would have passed at 5.6.0 as it should not have been able to find '/var/db/pkg'. There is the potential that the Nessus scan updated, or changed. Further investigations needs to be performed to see if a change in SecureSync software could be causing the issue.

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

From SecureSync manual:

Require complex passwords: If enabled, every password must have at least one of each of the following character types:
- Letters (a-z or A-Z)
- Numbers (0-9)
- Special characters (~ @ # % ^ & * ( ) _ - + = { } [ ] : ; < > . |)

The following special characters are NOT allowed: single quote, double quote, dollar sign, comma, backslash, exclamation mark, and apostrophe
Additionally, the username may not be included in the password.

Complex passwords

When we dug into some of the security standards we found another feature we need - Passwords with at least one of each type: letters, numbers, and special characters.

The feature is configurable on the Security tab of the Tools->Users page.

When complex passwords are enabled, new passwords must include at least one letter, at least one number AND at least one special character (_+=&< etc.

The list of allowed special characters is: ~ @ # % ^ & * ( ) _ - + = { } [ ] : ; < > . |

The list of special characters that are not allowed is: single quote, double quote, dollar sign, comma, backslash, exclamation mark, and apostrophe.
(These characters retain their meaning on a BASH command line, even inside double quotes.)

The software will give you precise feedback if you use one of the not acceptable special characters.

Adam –We already had a feature that passwords can't contain the user name. It used to be always on, but I changed that to be configurable with the same "complex passwords" switch. So, if customers don't enable complex passwords, the password for user "mike" can be "mike1234".
Complex passwords will be disabled by default.

Hard-coded in software (not configurable)

- ➢ Limits the number of failed login attempts before needing to wait to try again (see Note below).
- ➢ (5) "retries" are allowed, before a (60 second timeout) period has to occur, before a successful login can occur. During this timeout, "Permission Denied" will be displayed on the browser window (user name and password fields are still displayed, but you can't successfully login for 6 seconds).
- ➢ The Number of retries (5) and the time-out period (60 seconds) are set in software. They are not customer-configurable values.

Note regarding the limit on the number of failed login attempts (at least v4.5.0)
With the web browser: The failed login attempt feature has an issue that will likely appear as normal operation, unless you are testing for "normal expected operation". The first time entering what appears to be five incorrect passwords, the login screen won't reappear for about 4-5 minutes. Then, as long as the unit remains powered-up, if the right password is entered no problem. But each time thereafter that a wrong password is typed, the login page goes away for several minutes

each time. It does not reset to allowing several wrong passwords again.
Mike Sander is aware and a Mantis case has been opened. To the customer, this will appear as we are not allowing a machine to constantly hit the browser with a wrong password until the correct one is possibly entered.

Prevention of ability to re-use password (can't re-use the last 10 passwords)

- To override any limitations on the number of times you can use the same password, either reset the password 10 times in a row, or perform a resetpw command from the front panel.

Email from Dave L (7 May 18) The Securesync will not allow you to use the same password again if it has been used less than ten password changes in the past. This is for security purposes.
You could keep changing the password to a different value (accept the desired password) 10 times in a row. Then an earlier password can be re-used. The counter resets after 10 password changes.

• Even better work-around If current password is known, performing resetpw command from front panel or **resetpw** CLI command will automatically reset the password back to admin123, even if it's been recently changed less than 10 password changes (will override the "remember" of not allowing password re-use before 10 other passwords have been used.

Try the resetpw command from the CLI first and see if that works best.

Report of an issue with resetting the password back to a previous value

Refer to JIRA ticket SSS-466 (May 2018)

email from Dave Lorah (7 May 18) referring to SF case 163235
Hello Ryan and Apps,
Morgan Stanley is having some trouble resetting the password on one of their v5.7.1 Securesyncs to a password that was used previously. I had them try the resetpw command and also change the password 13 times over but no success. You can see the actions in the email train below.
I believe the Securesync stores the last 10 passwords in a register and will not allow duplication if the password is in that table, is this correct?

I was experimenting on our SS 10.2.192.227 and was able to break the counter. The old passwords are now able to be entered at will.
I used an unknown combination of the Chang My Password button and resetpw command from the CLI.
I am retrieving the logs from the customer.
Please enter a JIRA case and assign engineering support to help resolve this bug.

Reply from Paul Myers (7 May 18) I created a ticket "SSS-466 Case 163236 - Resetting a password to one used previously" and assigned it to Ryan Johnson. NO ONE IS WORKING ON IT YET.
Is this really a bug? Does it do what was intended which is keep the user from using the same password according to the user password settings?

Login password has expired

The password expiration "counter" starts when the password was last changed. Technically, a short expiration period could cause it to immediately be expired (if you were to set the expiration to 10 days and the password was last changed 15 days ago, it's now automatically expired). Once expired, the web browser will no longer allow login access and will not prompt you for the old/new password (**Access Denied** is displayed). However, login with either telnet or SSH and either of these connections will prompt you for the old and new passwords. Then, you can log back into the web browser using the new password.

Or, use the **resetpw** command to reset the Spadmin password via the front panel RS-232 SERIAL port or the keypad/LCD. Then, you can login using the spadmin123 password.

Note: Starting in version ~~5.2.1 (~Apr 2015)~~ **resetpw also sets LDAP and Radius to "Disabled"** to help prevent total lockout. They need to be re-enabled thereafter, if desired. Refer to Mantis case 3026   Update- this change was inadvertently left out of the v5.2.1 release. It will need to be added in with the next release (5.3.0?)

When resetpw is performed, and if LDAP and/or Radius were intentionally enabled, they will need to be re-enabled after performing a resetpw.

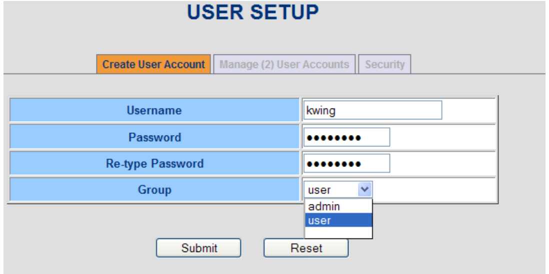
- The Serial command to reset the password via the RS-232 Serial port is "resetpw"
- Front panel keypad admin account password reset is via the System -> Cmd menus

Note: With Archive Versions 4.8.1 and below installed, a minor bug causes "**Not Supported**" to be displayed in the LCD after performing resetpw command, even though the command did reset the password.

Fields are grayed-out when logged into a User account

There are two different permission levels (referred to as "Groups") available to choose from for each User account that is created in the SecureSync- these are the "admin" and "user" groups. When "user" is selected, fields are grayed-out on several pages due to not having privilege to edit all the fields in the web browser.

Below is a screenshot for the **Tools**-> **Users** page of the browser, showing how to initially assign (or change thereafter) permissions for each User account that is created:



USER SETUP

Username	kwing
Password	••••••••
Re-type Password	••••••••
Group	user

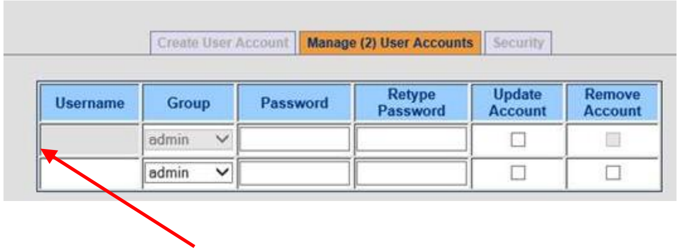
Root and spfactory accounts

Email from Dave Sohn to Morgan Stanley (7/5/12) As a point of clarification on security, the root account is disabled for all interactive logins. It can only be reached via an interactive account. We do have a default factory account with sudo privileges enabled for interactive login on the unit, but we allow the customer the ability to delete that account for security. With that account deleted, the only way to access the unit would be through a customer controlled and configured account.

User Accounts created successfully but name fields show a null

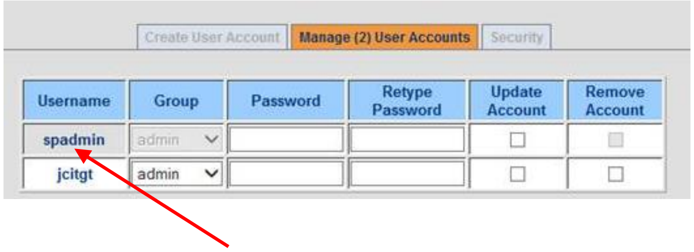
- Refer to Salesforce case 9834 (for Greg Thomas)
- Observed in Archive version 4.8.9

Viewed on Windows 8



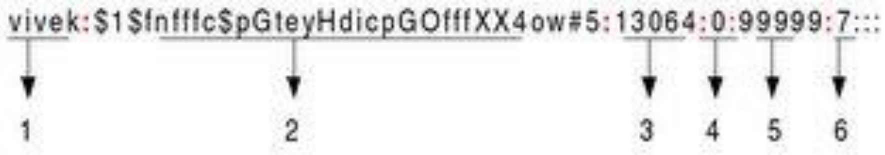
Username	Group	Password	Retype Password	Update Account	Remove Account
	admin			□	□
	admin			□	□

Viewed on Windows 7



Username	Group	Password	Retype Password	Update Account	Remove Account
spadmin	admin			□	□
jcitgt	admin			□	□

etc/shadow file fields

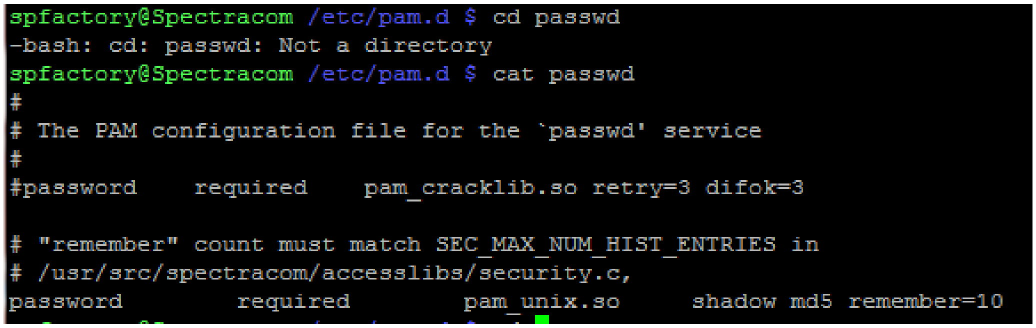


- **User name** : It is your login name
- **Password**: Its your encrypted password. The password should be minimum 6-8 characters long including special characters/digits
- **Last password change (lastchanged):** Days since Jan 1, 1970 that password was last changed
- **Minimum**: The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
- **Maximum**: The maximum number of days the password is valid (after that user is forced to change his/her password)
- **Warn**: The number of days before password is to expire that user is warned that his/her password must be changed
- **Inactive**: The number of days after password expires that account is disabled
- **Expire**: days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used:

"Rules" for creating/editing passwords/Password reuse/Password Hi

- **Max length (newer browser):** Password can be up to 50 characters long (set limitation of the web browser- not a limitation of Linux).
- **Min length (newer browser):** By factory default, password minimum length is 8 characters, but this value can be changed via the "Security Policy" settings (as discussed further below).
- **Inability to re-use an earlier password** ("**Password has already been used"** message is displayed)

  Internal reference note: The Linux OS uses the "remember" command in PAM to store earlier-used passwords. The default Value is "**13**" but we change this to "**10**"

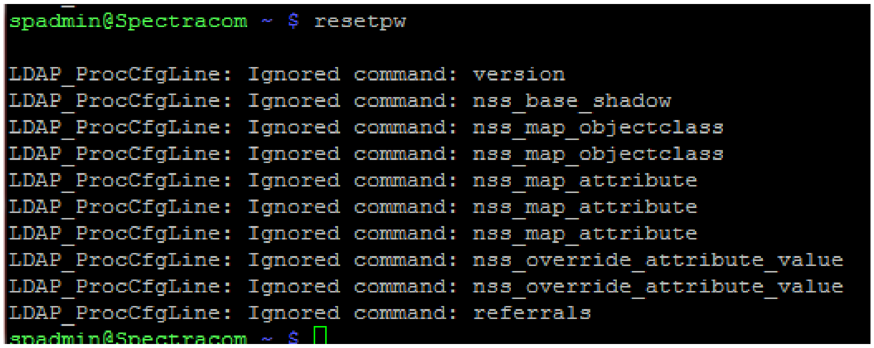


```
spfactory@Spectracom /etc/pam.d $ cd passwd
-bash: cd: passwd: Not a directory
spfactory@Spectracom /etc/pam.d $ cat passwd
#
# The PAM configuration file for the `passwd' service
#
#password    required    pam_cracklib.so retry=3 difok=3

# "remember" count must match SEC_MAX_NUM_HIST_ENTRIES in
# /usr/src/spectracom/accesslibs/security.c,
password        required        pam_unix.so     shadow md5 remember=10
```

This message is displayed if trying to re-use an earlier account password that has been used within the last 10 password changes.

To override any limitations on the number of times you can resue password either pefrorm **resetpw** (via CLI or front panel) OR use the same password, reset the password 10 times in a row, to fill the list with arbirtrary valiues - thus allowing an earlier password to be re-used.

- **Work-around:** Can apparently keep changing the password to a different value (accept the desired password) 10 times in a row. Then an earlier password can be re-used. The counter resets after 10 password changes.
- Even better work-around If current password is known, performing resetpw command from front panel or **resetpw** CLI command will automatically reset the password back to admin123, even if its been recently changed less than 10 password changes (will override the “remember” of not allowing password re-use before 10 other passwords have been used.



```
spadmin@Spectracom ~ $ resetpw

LDAP_ProcCfgLine: Ignored command: version
LDAP_ProcCfgLine: Ignored command: nss_base_shadow
LDAP_ProcCfgLine: Ignored command: nss_map_objectclass
LDAP_ProcCfgLine: Ignored command: nss_map_objectclass
LDAP_ProcCfgLine: Ignored command: nss_map_attribute
LDAP_ProcCfgLine: Ignored command: nss_map_attribute
LDAP_ProcCfgLine: Ignored command: nss_map_attribute
LDAP_ProcCfgLine: Ignored command: nss_override_attribute_value
LDAP_ProcCfgLine: Ignored command: nss_override_attribute_value
LDAP_ProcCfgLine: Ignored command: referrals
spadmin@Spectracom ~ $ 
```

Password Re-use/Password History

Info below is from 1200 SecureSyncs

Q My Customer prefers this to be 24, not 10 (as in /home/spectracom/default/etc/pam.d/passwd).
1) Is this configurable somewhere? (It wasn't obvious anywhere).

A Keith’s response: Password requirements which can be changed/edited are “**Password Security**” under **Management**->**Authentication**->**Security Policy** page of the browser to change password requirements.

‘Remember’ for password history is set to 10 and cannot currently be edited. However, I am forwarding your customer’s desire to be able to change it over to the Product Manager for consideration of possibly changing this in a future software update.

2) The text within /home/spectracom/default/etc/pam.d/passwd indicates the history is to match SEC_MAX_NUM_HIST_ENTRIES in /usr/src/spectracom/access_libs/security.c. Where is this file (if, by some chance the ...pam.d/passwd file can be updated)?

Keith's response: NO. This file can't be updated.

Password Change Attempt Logging

auth.log (/home/spectracom/log/auth.log)
Q Is this treated differently between execution by a privileged (admin) user against another account vs. self-update by a given account?
A Keith's response: NO. It's not treated differently.

Special character/symbol limitations for passwords:

A) Using the newer black background web browser to create/edit password

- All keyboard characters and symbols are now accepted. Can use all special characters, such as the following: ! @ # $ % ^ & * ( )

B) While using the classic interface web browser to create/edit password,

- Just like in software versions 4.8.9 and below, installed packages related to the web browser limit the use of special characters.

  The list of allowed special characters is: ~ @ # % ^ & * ( ) _ - + = { } [ ] : ; < > . |

  The following special characters are **NOT** allowed to be used when creating or editing password via the "classic interface" browser (or in versions 4.8.9 and below) : single quote ("), double quote (""), dollar sign ($), comma (,) , backslash (\), exclamation mark (!), and apostrophe (')

Note: This limitation of special characters was due to the PAM or Pamecea packages we used with the earlier **version of Linux. These package are not used in the newer version of linux**

Note: Can create a password using any special characters via the new browser and be able to successfully login to the classic interface with those credentials. Just can't create the credentials in the classic interface

Web browser (HTTP/HTTPS) SSL / Enhanced security / login accounts / banner

Network port numbers for the web browsers (443 for HTTP, 80 for HTTPS, and 8080)

A) Newer black/charcoal browser (v5.1.2 and above

TCP	**443**	HTTPS/SSL	Not configurable
TCP	**80**	HTTP	Not configurable

B) Classic interface web browser

- Accessible via **Port 8080**
- In addition to port 8080, the classic UI is only accessible through HTTPS (not available via HTTP).

web browser interface

***Desire to create scripts for the web browser interface

- Browser itself can't be scripted- need to use the REST API interface
- REST API interface allows scripting of everything available in the web browser interface
- Refer to the REST API section of this document: ****secure REST API interface (alternate to using the standard web browser or CLI)

**PC Browser requirements (Java to run Javascript)

Requirements to use the web browser

- The newer browser requires **Java** be installed on the PC and be working correctly in order to run Javascript in the browser
- Note the newer browser does not use/require Flash.

Javascript

- For general and Javascript version info, refer to: http://en.wikipedia.org/wiki/JavaScript
- Javascript is not a package installed in the SecureSync. It consists of library files with their own versions.

Q (from Masataka with TOYO) User manual include following description as condition of control PC.
HTTP, HTTPS Servers: For browser-based administration, configuration and monitoring using Internet Explorer 7 or higher wit JavaScript support, Mozilla Firefox 3 or higher (per RFCs 1945 and 2068), with JavaScript support. Could you please let us know which version of Javascript supported?

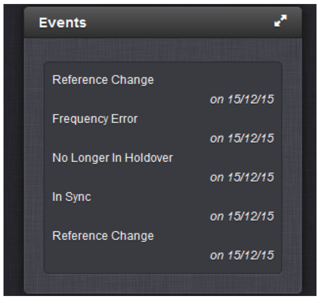
A. From Keith The answer is the Javascript version is web browser dependent. So the answer to your question isn't a version number. The answer is what browsers does SecureSync support. The SecureSync supports Chrome, Firefox and newer versions of Internet Explorer (we recommend IE versions 10 and above only).

Security features added to prevent login simultaneously from multiple locations and mitigate brute force password attacks.

Update version 1.1.0A (Feb 2020): Added Web UI security features to prevent login simultaneously from multiple locations and mitigate brute force password attacks.

***Home page of the newer browser

Events window on Home page



Events

Reference Change
on 15/12/15
Frequency Error
on 15/12/15
No Longer In Holdover
on 15/12/15
In Sync
on 15/12/15
Reference Change
on 15/12/15

- Events window displays only the most recent entries

Entries displayed are future dates and don't update (in the example above, the entries are for 2015, in 2014)
If the unit is manually set to a future date, these "future" events will become the "most recent" events, until the date/time passes those events that occurred "in the future". So the future events will continue to be displayed.

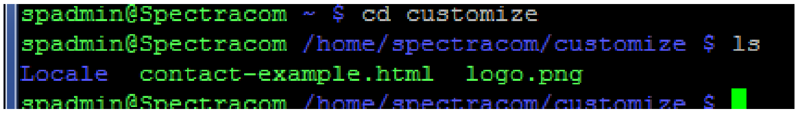
In at least version 5.1.7, deleting the logs does not restore the Events window to "real time" events being displayed. To allow the Events window to show "real time" events again, until this issue is addressed, it looks like the system needs to be cleaned. Refer to Mantis case 2948.

What should fix the "future" dates being displayed- once Mantis case 2948 is fixed: Delete all the logs (no need to perform a full system clean). Logs can be deleted in the **Management** -> **Log Configuration** page of the browser. On the left side of the page, click on "**Clear all Logs**". This will clear the logs and the Event window of all of the "future" events.

***Customization of the browser

- Newer browser can be customized with a custom logo("logo.png" file) custom language ("Locale" directory) and or custom contact info ("contact-example.html" file)
- Custom items such as a logo, locale or contact info are placed in the home/spectracom/customize folder (spadmin has access to this folder)

Default contents of this folder (shown with v5.3.1 software installed)



```
spadmin@Spectracom ~ $ cd customize
spadmin@Spectracom /home/spectracom/customize $ ls
Locale   contact-example.html   logo.png
spadmin@Spectracom /home/spectracom/customize $
```

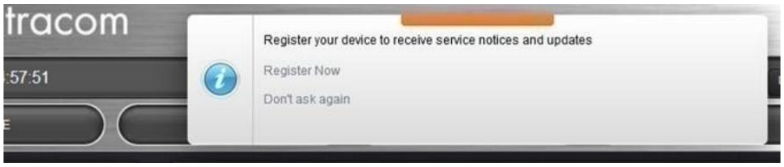
***Product Registration reminder / register your product

- **Website address to register a Spectracom product:** http://register.spectracomcorp.com/?ProductFamily=SecureSync&SN=ENG-1208

Q. (email from Mark Day) I have had an unusual customer comment, they have registered their unit however they are still getting the notifications asking them to register the unit. Is there a way to confirm the registration and to stop the notifications?

A. Reply from Keith (11 May 15) The SecureSync has no way to detect whether a customer has already registered it on our website. So they can just acknowledge that it's been manually registered. We originally discussed the SecureSyncs having the ability to "auto-register" and "auto-detect software updates being available. But these require it being open on the Internet. Many of our customers install them on closed networks isolated from the Internet. So these capabilities wouldn't work. Therefore, we decided not to spend time incorporating these specific functions.

When a customer sees the pop-up reminder in the browser to register, they can simply acknowledge the reminder, they can simply click on "Don't' ask again" in this pop-up.



Register your device to receive service notices and updates

*Cookies for web browser

- For info on enabling cookies, refer to: https://kb.iu.edu/d/ajfi
- Cookies do need to be enabled for the newer web browser.
- note is displayed if cookies are not enabled in the browser.

Cookie fields

Name

- Name= spectracom (cookie for browser)

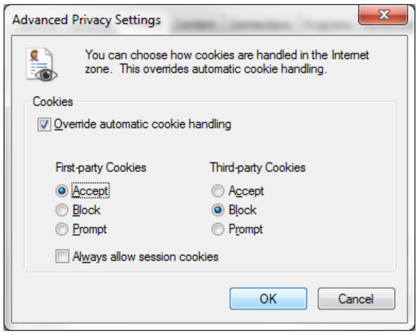
Content = Session ID

Host = IP address of time server

If cookies are blocked/disabled, the login page will report "certificate error" near the IP address and will just keep clearing the login name (won't allow access to the browser)

A) Internet Explorer:

- Enable "First party Cookies" in Tools -> Internet Options, Privacy tab, Advanced button:



Advanced Privacy Settings

You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

Cookies

☑ Override automatic cookie handling

First-party Cookies: ● Accept ○ Block ○ Prompt

Third-party Cookies: ○ Accept ● Block ○ Prompt

□ Always allow session cookies

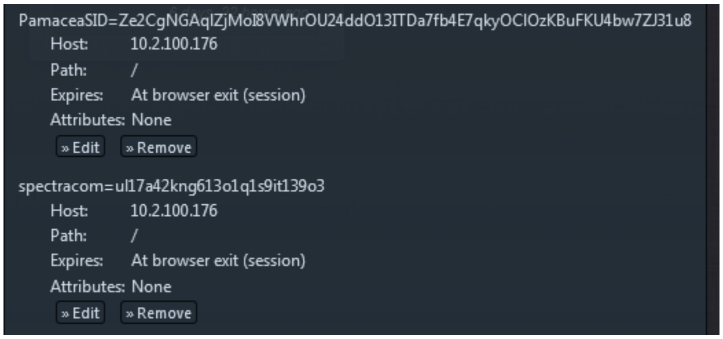
Important note: Also make sure the time server is not listed as a "Site" which is configured as "**Always bocked**" (this will block cookies for just the time server, even if cookies are enabled in the Advanced button) .

In **Tools** -> **Internet Options**, **Privacy** tab,press the **Sites** button. Can optionally add the time server to the list of Sites as "**Always Allow"** if desired (this step isn't required but doesn't hurt to do).

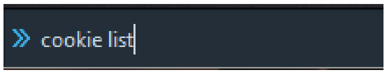
B) FireFox

Enable "First party Cookies" in **Tools** -> **Options**, **Privacy** tab, **History** drop-down
To allow sites to set cookies on your computer, select **Accept cookies from sites**. To specify which sites are always or never allowed to use cookies, click Exceptions.

To view or remove individual cookies, press **Shift** and **F2.** At the arrow that appears at the very bottom of the page, type **cookie list** <enter> (as shown below)



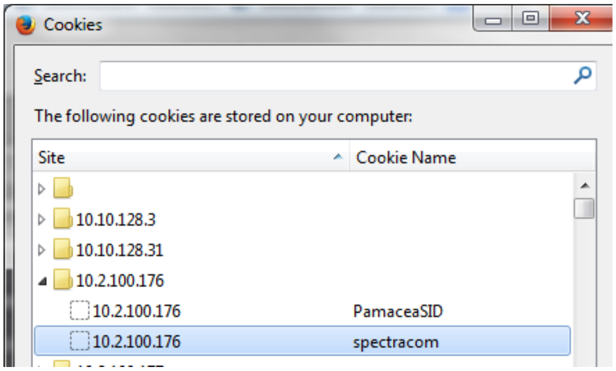
```
PamaceaSID=Ze2CgNGAqIZjMoI8VWhrOU24ddO13ITDa7fb4E7qkyOCIOzKBuFKU4bw7ZJ31u8
    Host:       10.2.100.176
    Path:       /
    Expires:    At browser exit (session)
    Attributes: None
     » Edit   » Remove

spectracom=ul17a42kng613o1q1s9it139o3
    Host:       10.2.100.176
    Path:       /
    Expires:    At browser exit (session)
    Attributes: None
     » Edit   » Remove
```



```
cookie list
```

Browse to the web browser and login.

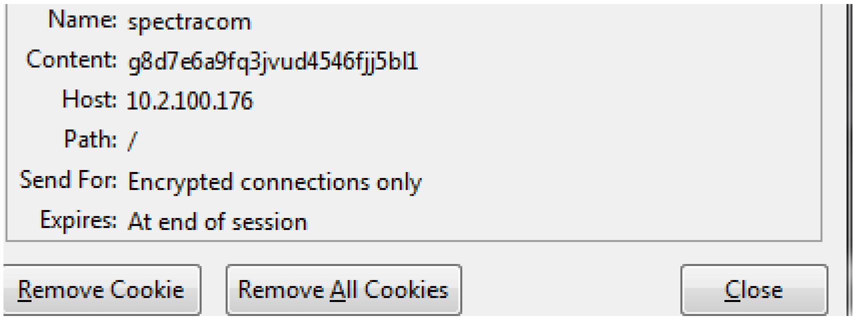
Then go to Tools -> **Options** -> **Privacy**. Change “**Remember History**” drop-down to “**Use Custom Settings for History**”. Now click on “**Show Cookies” and** select the applicable IP address of time server.
There will likely be a “cookie” for newer browser).



Search:

The following cookies are stored on your computer:

Site	Cookie Name
10.10.128.3	
10.10.128.31	
10.2.100.176	
10.2.100.176	PamaceaSID
10.2.100.176	spectracom



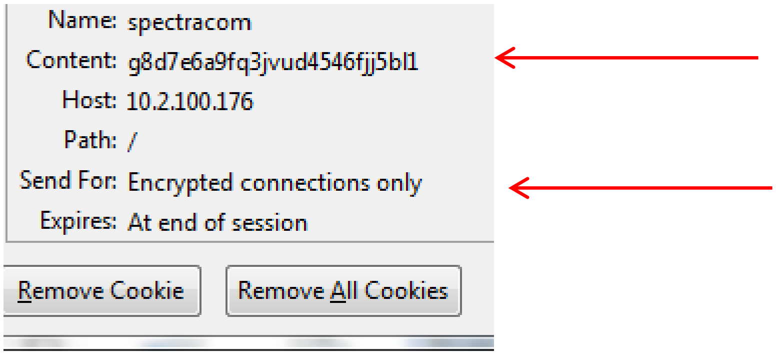
Name:	spectracom
Content:	g8d7e6a9fq3jvud4546fjj5bl1
Host:	10.2.100.176
Path:	/
Send For:	Encrypted connections only
Expires:	At end of session

- “**HttpOnly**” and “**Secure connections only**” / “**Encrypted connections only**” cookies
- Refer to Salesforce case 17412 (Justin with Wegmans)
- Refer to websites such as: https://www.owasp.org/index.php/Testing_for_cookies_attributes_%28OTG-SESS-002%29
- Newer web browser has both **HTTPonly** and **Secure connections only** Flags set in software (not user configurable).

Email from Dave Sohn (16 Mar 15): Here is the cookie from my 5.2.0 unit in house showing the HttpOnly and Secure flags both being set. Did the cookie actually have the key “spectracom=deleted”? That usually contains the session ID. If they deleted the info before they sent it that’s ok, but it is just strange. Maybe it’s an expired cookie, so the flags are cleared? Not sure about that.

Name:	spectracom
Content:	<deleted>
Domain:	10.10.16.20
Path:	/
Send for:	Secure connections only
Accessible to script:	No (HttpOnly)
Created:	Monday, March 16, 2015 at 11:04:43 AM
Expires:	When the browsing session ends

FireFox cookie (from further above)



Name: spectracom
Content: g8d7e6a9fq3jvud4546fjj5bl1
Host: 10.2.100.176
Path: /
Send For: Encrypted connections only
Expires: At end of session

*Supported/unsupported web browsers and browser versions

Supported browsers

- Chrome
- Firefox
- **Internet Explorer** (if using IE, we recommend using at least IE versions **10** and above)

IE6: not compatible at all with newer browser.

IE9: "I found all the bottoms are not visible"

Email from Dave Sohn (17 Sept 14) At least IE9 is required for some of our UI elements to function properly due to javascript and HTML5 requirements. We had previously looked at workarounds that emulated portions to allow the UI to run, but there were issues. This remains an open issue in our tracking system, but no additional progress has been made.

IE8 and below

(applicable to software versions 5.6.0 and above) Internet Explorer versions 8 and below not logging in because our default signature algorithm was upgraded to SHA256 starting in 5.6.0

- Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
- An example defcer CLI syntax (5.6.0 and above only) is **defcert -sha256**
- V5.6.0 also changed the default algoritm to **SHA256** for better security (the defauit in 5.5.1 and below was SHA1) .
- As IE8 and below do not support SHA-256, in versions 5.6.0 and above, use **defcert -sha1** to regenerate a new certitficate using SHA1 to gain access to IE8 and below

Email from Keith (20 Jul KW) One thing to keep in mind is that, depending on the current software version installed in the SecureSync, the **defcert** command will create its new default certificate using either a **SHA1** cipher or a **SHA256** cipher.

With software **versions 5.6.0 and above** installed in the SecureSync, the more secure SHA256 encryption cipher will be used to generate its new certificate (with version 5.5.1 and below, the defcert command used the SHA1 cipher).

The issue with the more secure SHA256 cipher is **Internet Explorer versions 8** and below can't use this newer cipher. With these more recent versions of software installed in the SecureSync (5.6.0 and above), and when using IE8 or below to access the SecureSync, instead of using the CLI command of **defcert** to replace the existing certificate, issue instead the following CLI command to generate a new certificate using the earlier SHA1 cipher: **defcert -sha1** <enter>. Then try accessing the web browser again.

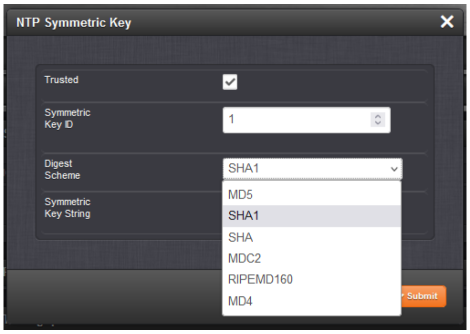
Signature Algorithms (Such as SHA1/SHA-1, SHA2/SHA-256 (and MD5)

- MD5 and SHA1 are recommended to be replaced by newer, more secure algorithms, such as SHA-256 (SHA-1 has been broken)
    - Refer to articles such as: http://www.networkworld.com/article/3173996/security/replace-sha-1-it-s-not-that-hard.html?idg_eid=218d22f55abd3e2c29f91225dde70f2c&email_SHA1_lc=064024a3b5046cfb24a2b0c69fd42455f0f40e0b&utm_source=Sailthru&utm_medium=email&utm_campaign=NWW%20Security%20Alert%202017-02-27&utm_term=networkworld_security_alert

Support of SHA-2(SHA2)/SHA-256(SHA256) in 2400 SecureSyncs

(As of at least versions 1.6.0 and below)

- **NTP symmetric Key:** NTP supports SHA2, but SHA2 is **not** listed/available in the drop-down field as a selection (refer to work-around further below)



NTP Symmetric Key

Trusted ☑

Symmetric Key ID: 1

Digest Scheme: SHA1

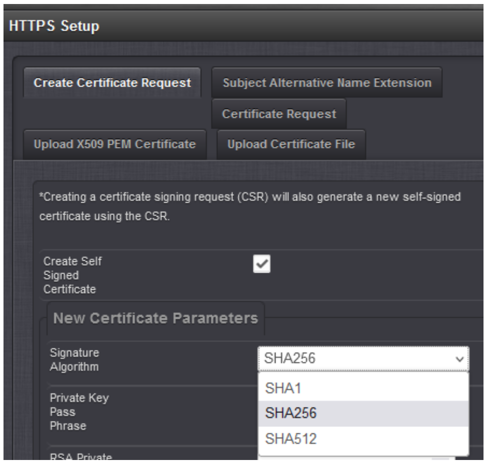
Symmetric Key String

Refer to Salesforce Case [300177]()

Per Mike Pratt (17 May 2023) Hi Keith, you're correct that the products don't support SHA2. It's mainly just a limitation of the UI. I recently wrote an App Note regarding a workaround for this for 2400. I'll send it to you.

  - **Link to referenced workaround App Note Mike Pratt created:** [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync-2400 (Diamond)\NTP\NTP Restriction and Authentication-MD5 and SHA]()

- **HTTPS Certificate:** supports SHA1, **SHA256** and **SHA512)**



HTTPS Setup

*Creating a certificate signing request (CSR) will also generate a new self-signed certificate using the CSR.

Create Self Signed Certificate ☑

New Certificate Parameters

Signature Algorithm: SHA256

Private Key Pass Phrase

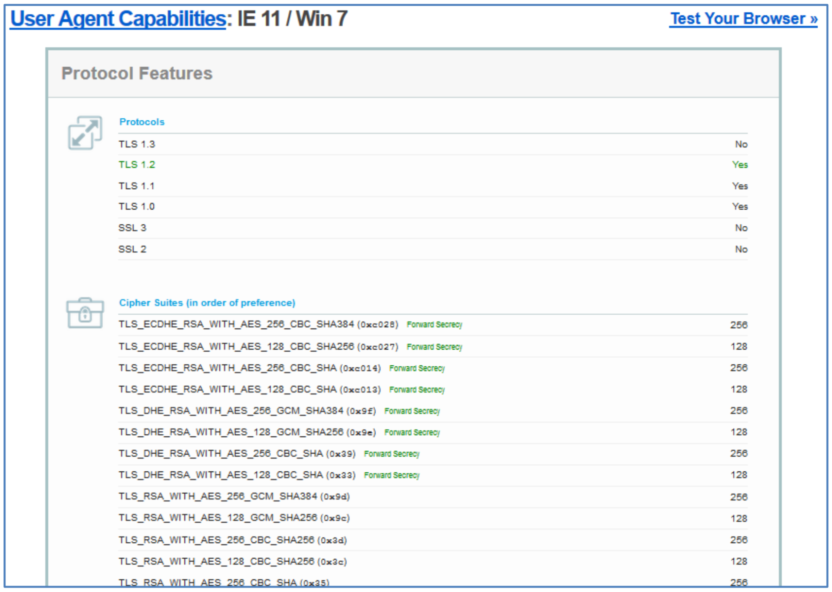
RSA Private

Create Certificate Request
Subject Alternative Name Extension
Certificate Request
Upload X509 PEM Certificate
Upload Certificate File
SHA1
SHA256
SHA512

List of supported ciphers list for various browser versions (such as Firefox, Chrome, Internet Explorer, etc):

- refer to: https://www.ssllabs.com/ssltest/clients.html

Example below is for IE11



User Agent Capabilities: IE 11 / Win 7

Protocol Features

Protocols	
TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Cipher Suites (in order of preference)	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) Forward Secrecy	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) Forward Secrecy	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) Forward Secrecy	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) Forward Secrecy	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) Forward Secrecy	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) Forward Secrecy	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) Forward Secrecy	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) Forward Secrecy	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256

Internet Explorer versions such as IE 11 not logging in, with no error messages being displayed

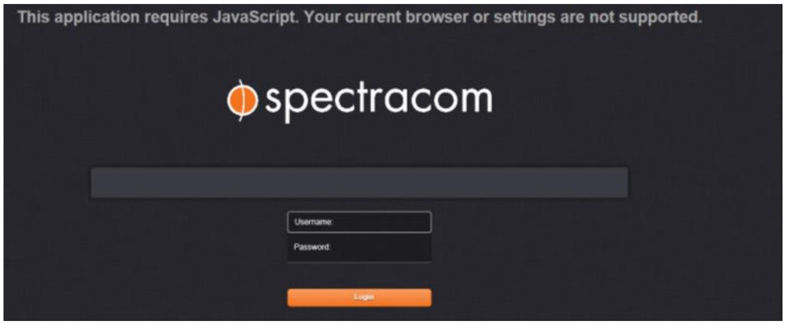
- Refer also to the "**Enable High Security**" Checkbox section
- **IMPORTANT NOTE**: Cookies also have to be enabled. In IE- **Tools** –> Internet Options -> Privacy tab. Advanced button: makes sure Cookies are set to Allow/Allow. Also in the Sites button, make sure that if the time server is listed in the Sites list, that its set to "Always Allow and not set to Always block (always block will disable cookies for this one site, and login will be denied.
- Make sure Proxy server isn't selected
  - In **IE- Tools** –> **Internet Options** -> **Connections** tab. **LAN Settings** button ("use a proxy server for your LAN" should not be selected).

Q I'm trying to use IE 11 when I try to login to the SecureSync unit with login name and password it just looks to refresh the login page and not log me in to do anything with the SecureSync unit. If I try a bad password it does give an error and I am able to SSH in and also log into the unit using Firefox and IE 10 just can't get IE 11 to let me fully login.

A Keith's response (5 Jan 17): I suspect this observation is a direct factor of a difference in the cipher list/security level setting between the two versions of IE.

I happen to have IE11 installed on my PC and I can login with no problems. In IE 11, go into **Tools**-> **Internet Options, Security tab.** If the **Security level** is not already set to **Medium-high**, change it this setting and then try logging in again.

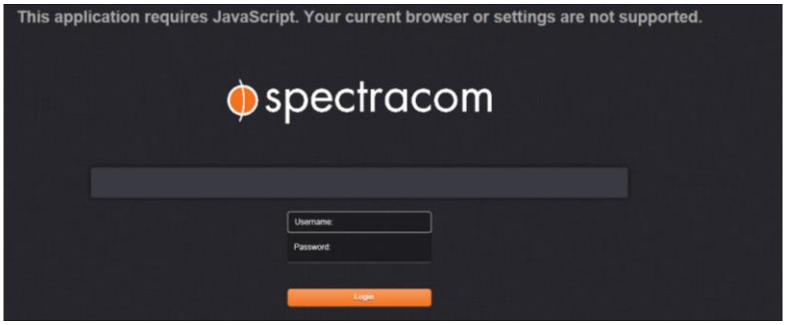
Note that when I changed my setting to high, logged-out and then tried logging back in, I can no longer login and also have an error message displayed that indicates "This application requires JavaScript. Your current browser or settings are not supported.


This application requires JavaScript. Your current browser or settings are not supported.

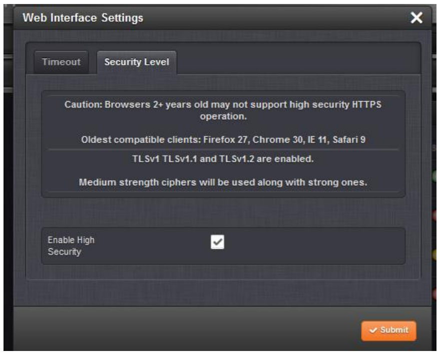
This error message is a newer one that was added in one of the more recent SecureSync software updates, specifically for this reason. I suspect your Security setting in the PC is set too high, but with an earlier software version installed, you just aren't getting the error message indicating this.

Error message: "This application requires JavaScript. Your current browser or settings are not supported"

C) No successful login occurs and the following error message is displayed at the top of the window: "This application requires JavaScript. Your current browser or settings Are not supported." (as shown below)


This application requires JavaScript. Your current browser or settings are not supported.

- ➢ If no successful login, and this error message is displayed at the top of the page, change the Security level in the PC's browser. For IE, go to Tools-> Internet Options, Security tab. If the Security level is set to High, lower it to Medium-high and then try logging in again.
- ➢ Update v5.4.5 added user selectable High and Medium level HTTPS Security settings (Management-> Network Settings page, Web Interface Settings button. Select Security Level tab in the pop-window. This window selects which list of ciphers to use for the connection with the browser.


Web Interface Settings

Caution: Browsers 2+ years old may not support high security HTTPS operation.

Oldest compatible clients: Firefox 27, Chrome 30, IE 11, Safari 9

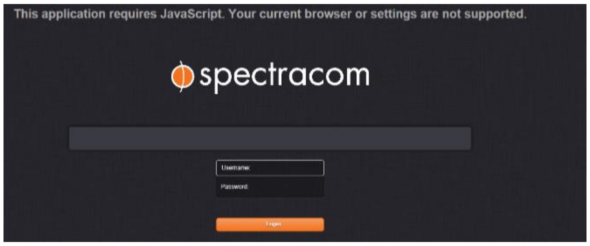
TLSv1 TLSv1.1 and TLSv1.2 are enabled.

Medium strength ciphers will be used along with strong ones.

Enable High Security ☑

I happen to have IE11 installed on my PC and I can login with no problems. In IE 11, go into **Tools**-> **Internet Options, Security tab.** If the **Security level** is not already set to **Medium-high**, change it this setting and then try logging in again.

Note that when I changed my setting to **high**, logged-out and then tried logging back in, I can no longer login and also have an error message displayed that indicates "This application requires JavaScript. Your current browser or settings are not supported."



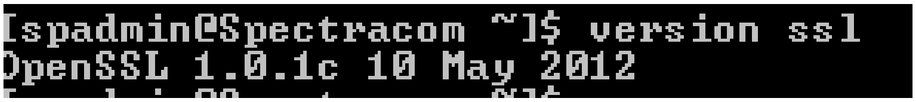
This application requires JavaScript. Your current browser or settings are not supported.

This error message is a newer one that was added in one of the more recent SecureSync software updates, specifically for this reason. I suspect your Security setting in the PC is set too high, but with an earlier software version installed, you just aren't getting the error message indicating this,

**OpenSSL version installed

- Software version 5.2.0 added display of ssl version in the Tools -> Upgrade/Backup page of the newer black browser.
- Software versions 5.1.7 and below: ssl version is not reported in the browser, but is available via cli command:
- cli command to obtain the ssl version is version ssl <enter>

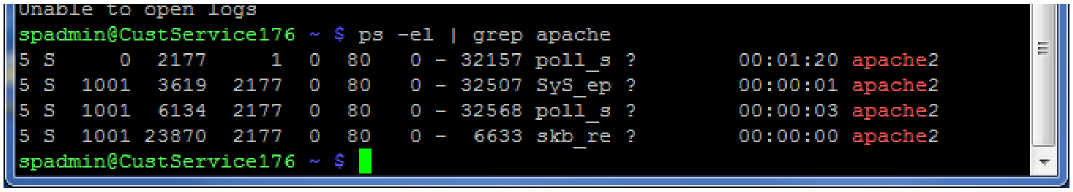
  (shown below with V4.8.8 installed)



```
[spadmin@Spectracom ~]$ version ssl
OpenSSL 1.0.1c 10 May 2012
```

Determining if Apache web browser is running

Type: **ps –el | grep apache**



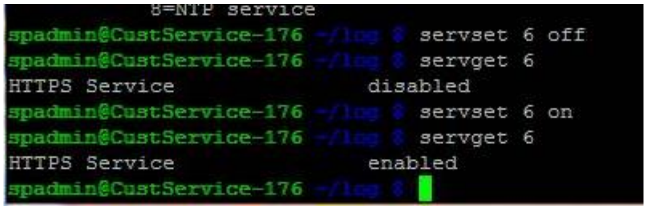
```
Unable to open logs
spadmin@CustService176 ~ $ ps -el | grep apache
5 S     0  2177     1  0  80   0 - 32157 poll_s ?        00:01:20 apache2
5 S  1001  3619  2177  0  80   0 - 32507 SyS_ep ?        00:00:01 apache2
5 S  1001  6134  2177  0  80   0 - 32568 poll_s ?        00:00:03 apache2
5 S  1001 23870  2177  0  80   0 -  6633 skb_re ?        00:00:00 apache2
spadmin@CustService176 ~ $
```

As shown above, there should be **apache2** in the list

*Restart HTTP/HTTPS instead of rebooting the unit (HTTPS reload command)

- There is an HTTPS "reload" command but it's not supported in our CLI.

Perform a **servset 6 off** <enter> command followed by **servset 6 on** <enter> (as shown below). Note the two servget commands in the screenshot are optional. This will restart just the web browser service alone.



```
           8=NTP service
spadmin@CustService-176 ~/log $ servset 6 off
spadmin@CustService-176 ~/log $ servget 6
HTTPS Service                   disabled
spadmin@CustService-176 ~/log $ servset 6 on
spadmin@CustService-176 ~/log $ servget 6
HTTPS Service                   enabled
spadmin@CustService-176 ~/log $
```

Graceful restart of Apache browser (*Graceful restart requested, doing restart*)

Note about "[error] (9)Bad file descriptor: apr_socket_accept: (client socket)"

"*Graceful restart requested, doing restart"* may also be accompanied by another error log entry of "[error] (9)Bad file descriptor: apr_socket_accept: (client socket)" This is not a reason for the Apache restart. It is a result of the restart. Apache can apparenty have trouble with a graceful restart.

Per: https://www.linuxquestions.org/questions/linux-server-73/apache-bad-file-descriptor-593925/

You might be hitting this bug:

http://issues.apache.org/bugzilla/show_bug.cgi?id=42829

I'd suggest just doing a full stop and start to get around the error until fixed. I never do graceful restarts with apache, never seems to do the job accurately.

Email from Verizon to Dave Lorah: I am attaching the logs of a second server that has been rebooted randomly this week at the same location.

Email from Dave Lorah to Engineering (18 Jan 16) regarding a Verizon SecureSync: This is a second unit in Colorado Springs that has rebooted itself. I see this message in the error log:
[Sat Jan 16 16:26:45 2016] [notice] Graceful restart requested, doing restart

Reply fron Paul Myers (18 Jan 16) Ron points out this is an Apache restart.We do them on occasion. This one occurs during the reboot.

Here is an online report of Apache not running after a graceful restart (until stopped/restarted). Could this be related to what this customer has reported: https://serverfault.com/questions/780793/apache2-not-running-after-graceful-restart

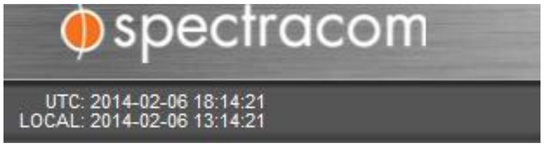
D) Problem report: Graceful restart entry with no other associated entries in the logs. Reported loss of network connection after reboot

- Refer to case 120843

Hi Ron,
Here is an online report of Apache not running after a graceful restart (until stopped/restarted). Could this be related to what this customer has reported: https://serverfault.com/questions/780793/apache2-not-running-after-graceful-restart
Today my apache instance was automatically restarted gracefully by some cron job I guess, afterwards it was not running.

Today my apache instance was automatically restarted gracefully by some cron job I guess, afterwards it was not running.

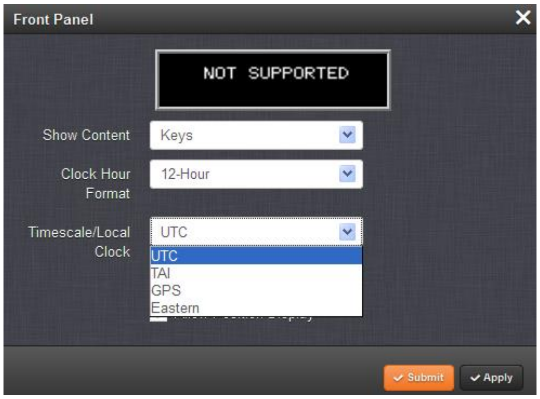
**Desire to show local time in the web browser



UTC: 2014-02-06 18:14:21
LOCAL: 2014-02-06 13:14:21

- Web browser time display is linked to the front panel configuration (doesn't have its own configuration).
- The "**local clock**" selected in front panel configuration is displayed below the UTC time.
- If "**None**" is selected, browser only shows local time. If a user-created local clock has been created and selected, this is displayed below the UTC time.

Management -> **Front Panel** page of the browser



NOT SUPPORTED

Show Content: Keys

Clock Hour Format: 12-Hour

Timescale/Local Clock: UTC

UTC
TAI
GPS
Eastern

Troubleshooting local time error in browser

Make sure the "**UTC offset**" in the Local Clock configuration is set for the correct offset for **STANDARD** Time (not the UTC Ofset for DST time).

A) Web browser is reporting the wrong time (just the minutes/seconds are incorrect- Hours is correct)

- Dwain Barcena w/Blue Cross saw a 20 minute error in the time display of the browser, as compared to the front panel and his Windows PC.
- While the browser is connected to the SecureSync, the browser periodically sends getTime calls to the SecureSync to keep the browser clock accurate (Ron saw this call sent a few times during just the couple minutes I was in his office)
- If the connection to the browser is broken but the page stays open (login times-out, the server is rebooted, etc) the browser can no longer get responses to the gettimes, so the browser clock will just free-run/drift off in time until a gettime call can be completed successfully again to correct the time

HTTP / HSTS (HTTP Strict Transport Security)

A) HTTP

- HTTP is not secure
- Disabled by factory default

B) HSTS (HTTP Strict Transport Security) for HTTP

- Refer to JIRA ticket DMND-1491 (Feb 2021) for request to add this feature to 2400 SecureSyncs

What is HSTS

Per https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

HTTP Strict Transport Security (**HSTS**) is a web security policy mechanism that helps to protect websites against protocol downgrade attacks[1] and cookie hijacking. It allows web servers to declare that web browsers (or other complying user agents) should interact with it using only HTTPS connections, which provide Transport Layer Security (TLS/SSL), unlike the insecure HTTP protocol used alone. HSTS is an IETF standards track protocol and is specified in RFC 6797.

The HSTS Policy is communicated by the server to the user agent via an HTTPS response header field named "Strict-Transport-Security".[1] HSTS Policy specifies a period of time during which the user agent should only access the server in a secure fashion.[2] Websites using HSTS often do not accept clear text HTTP, either by rejecting connections over HTTP or systematically redirecting users to HTTPS (though this is not required by the specification). The consequence of this is a user-agent not capable of doing TLS will not be able to connect to the site anymore.

- Refer to Salesforce Case 220401 (Jan 2020)
- HSTS module is in SecureSync, but as of at least v5.8.6, its not configured to work with SecureSync and is not available to/configurable by users (not enabled in the unit).

"HSTS Missing from HTTPS Server (RFC 6797)"

- Refer to Salesforce Cases such as 257254
- Refer to sites such as: https://www.ibm.com/support/pages/resolving-missing-hsts-or-missing-http-strict-transport-security-websphere

Q Report from Customer: "HSTS missing from HTTPS server. if HTTPS is in use on port 443, HSTS must be enforced. Inquire with vendor how to configure. if not possible, need vendor documentation."

A reply from Dave L (17 Jan 2020) The Securesync is equipped with HSTS but this is not user accessible or configurable. You asked about documentation about this. What do you require?
Also, HSTS is not supported in some web browsers. What browser are you using to access the Securesync?

A reply from Dave L (30 Jan 2020) I have consulted our engineering group and confirmed HSTS is not enabled and will not function in the Securesync product. It is not capable of enabling or configuring HSTS. To enable HSTS would require a product design change.

HTTP Hyper Strict Transport Security (HSTS) setup/configuration (Refer to online 2400

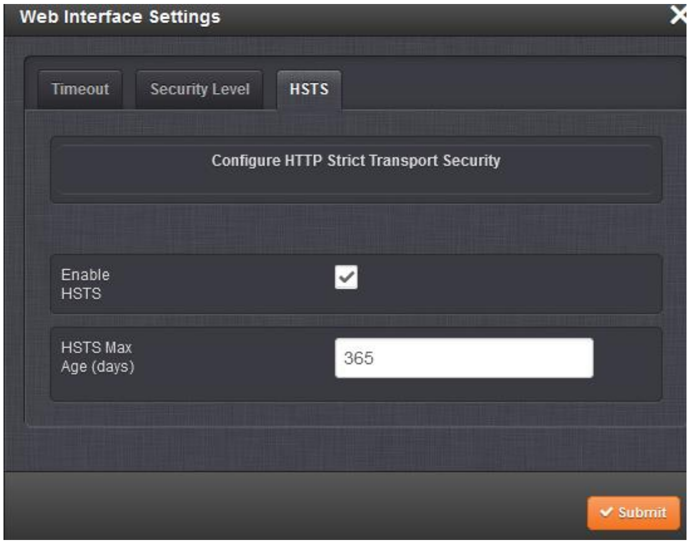
- Refer to SecureSync user guide at: ???
- Applicable to update versions 1.6.0 and above
  - Per 1.6.0 Release Notes "Added support for HSTS (HTTP Strict Transport Security)"

The HTTP Strict Transport Security header informs the browser that it should never load a site using HTTP and should automatically convert all attempts to access the site using HTTP to HTTPS requests instead.

(note all the following HSTS info was excerpted from 1200 SecureSync assist doc)

To configure HSTS

1) Navigate to ***MANAGEMENT*** > ***Network Setup***.
2) Select **Web Interface Settings** (button on left)
3) Select the **HSTS** tab to Enable/Disable HSTS, or to configure the Max Age of the functionality (default is set to 1 year).



Web Interface Settings

Enable HSTS ☑

HSTS Max Age (days) 365

For more information on HSTS requirements, refer to https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security.

Viewing the HSTS header (when HSTS is enabled)

Per: https://blog.nvisium.com/is-your-site-hsts-enabled

Testing HSTS

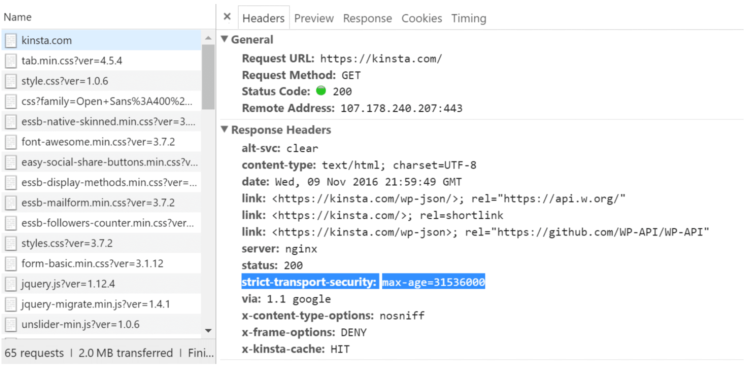
- Leverage an intercepting proxy (e.g. Burp) or browser tools (e.g. Chrome DevTools / Firefox Developer Tools) to examine server responses
- In **Chrome**, type the below to determine if a host is in your STS cache chrome://net-internals/#hsts
- In **Firefox**, you can use the Strict Transport Security Detector add-on to see if the site supports HSTS (https://addons.mozilla.org/en-US/firefox/addon/strict-transport-security-d/)

- “PinPatrol” (Firefox Add-On)

Per: https://kinsta.com/knowledgebase/hsts-strict-transport-security/

Verify HSTS Header

There are a couple easy ways to check if the HSTS is working on your WordPress site. You can **launch Google Chrome Devtools, click into the “Network” tab and look at the headers tab. As you can see below on our Kinsta website the HSTS value: “strict-transport-security: max-age=31536000” is being applied.**



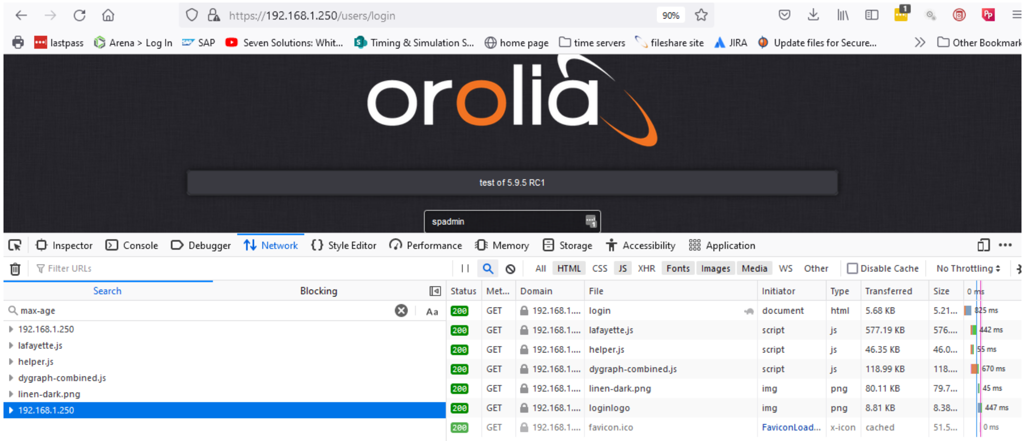
kinsta.com
tab.min.css?ver=4.5.4
style.css?ver=1.0.6
css?family=Open+Sans%3A400%2...
essb-native-skinned.min.css?ver=3....
font-awesome.min.css?ver=3.7.2
easy-social-share-buttons.min.css?v...
essb-display-methods.min.css?ver=...
essb-mailform.min.css?ver=3.7.2
essb-followers-counter.min.css?ver...
styles.css?ver=3.7.2
form-basic.min.css?ver=3.1.12
jquery.js?ver=1.12.4
jquery-migrate.min.js?ver=1.4.1
unslider-min.js?ver=1.0.6
65 requests | 2.0 MB transferred | Fini...

```
▼General
  Request URL: https://kinsta.com/
  Request Method: GET
  Status Code: ● 200
  Remote Address: 107.178.240.207:443
▼Response Headers
  alt-svc: clear
  content-type: text/html; charset=UTF-8
  date: Wed, 09 Nov 2016 21:59:49 GMT
  link: <https://kinsta.com/wp-json/>; rel="https://api.w.org/"
  link: <https://kinsta.com/>; rel=shortlink
  link: <https://kinsta.com/wp-json>; rel="https://github.com/WP-API/WP-API"
  server: nginx
  status: 200
  strict-transport-security: max-age=31536000
  via: 1.1 google
  x-content-type-options: nosniff
  x-frame-options: DENY
  x-kinsta-cache: HIT
```

Keith’s testing: In Firefox or Chrome

1. Open a browser connection to the SecureSync
2. In Google, click the “three dots” and select More Tools -> Developer Tools

   In Firefox, go to Tools -> Browser Tools -> Web Developer Tools
3. Select the “**Network**” tab
4. Click the magnifying glass and search for “**max-age**”
5. Reload the page
6. The list on the left is/are all the locations max-age (a parameter for HSTS) was found.

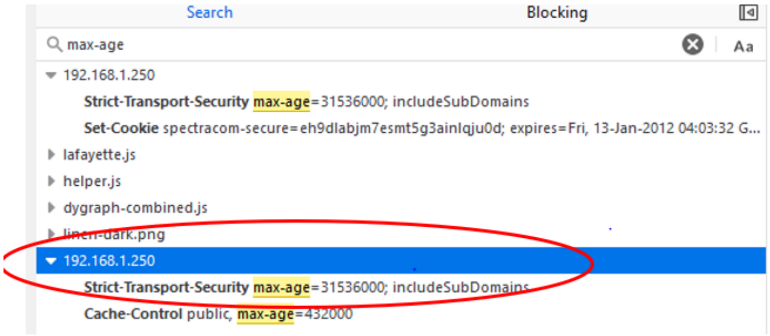


max-age

- 192.168.1.250
- lafayette.js
- helper.js
- dygraph-combined.js
- linen-dark.png
- 192.168.1.250

Status	Met...	Domain	File	Initiator	Type	Transferred	Size	0 ms
200	GET	192.168.1....	login	document	html	5.68 KB	5.21...	825 ms
200	GET	192.168.1....	lafayette.js	script	js	577.19 KB	576....	442 ms
200	GET	192.168.1....	helper.js	script	js	46.35 KB	46.0...	55 ms
200	GET	192.168.1....	dygraph-combined.js	script	js	118.99 KB	118....	670 ms
200	GET	192.168.1....	linen-dark.png	img	png	80.11 KB	79.7...	45 ms
200	GET	192.168.1....	loginlogo	img	png	8.81 KB	8.38...	447 ms
200	GET	192.168.1....	favicon.ico	FaviconLoad...	x-icon	cached	51.5...	0 ms

7. Click on the item(s) listed on the left to see the HSTS parameters (**Strict-Transport-Security max age**) drop-down below it.



```
max-age
▼ 192.168.1.250
    Strict-Transport-Security max-age=31536000; includeSubDomains
    Set-Cookie spectracom-secure=eh9dlabjm7esmt5g3ainlqju0d; expires=Fri, 13-Jan-2012 04:03:32 G...
▶ lafayette.js
▶ helper.js
▶ dygraph-combined.js
▶ linen-dark.png
▼ 192.168.1.250
    Strict-Transport-Security max-age=31536000; includeSubDomains
    Cache-Control public, max-age=432000
```

HSTS is enabled in web browser, but not being detected (v5.9.4, and apparently 5.9.5 pre-release. Fixed in 5.9.5)

- Refer to Salesforce Case 284393 (May 2022: observed with 5.9.4 installed)
- Refer to JIRA **SSS-1277**
- I seem to be duplicating this on 5.9.4, both before and after a reboot.
- Believe this was fixed in the v5.9.5 released update

The following is an excerpt from internal Engineering notes about the v5.9.5 update:
5.9.5 also contains fixes to address several issues (most customer reported, one internally identified):
- HSTS was added and can be enabled, but not working

Per Tim Hammer (excerpt from SSS-1277): June 8, 2022 at 9:53 AM

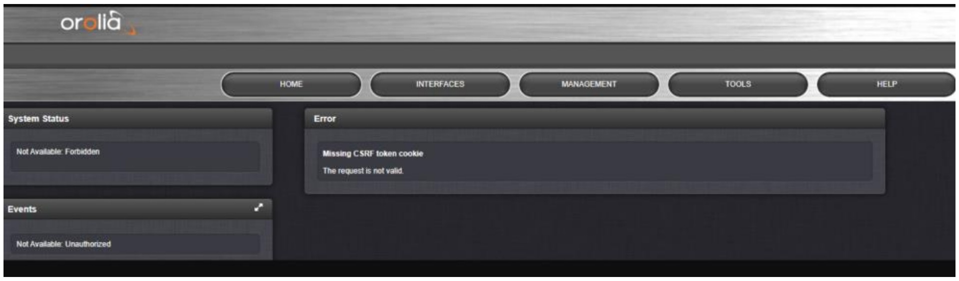
I confirmed behavior reported by customer & Keith Wing.
When updating from 5.9.1 (or earlier) to 5.9.4, the 000-httpd-default.conf file will be carried forward because it is included in the config transfer list.

However, we did not create a transfer script to handle the HSTS support added in the feature for 5.9.4.

Also in 5.9.4, we removed the Classic WUI code and supporting files. One of the changes resulted in the 000-httpd-default.conf file being removed from the transfer list (filelist.txt). Thus, when upgrading from 5.9.4 to 5.9.5 the file is not carried forward, the new file from the upgrade bundle is installed, and support for HSTS is in place.
So, there is no actual change required to "fix" this in 5.9.5.

CSRF (Cross-Site Request Forgery) / “Missing CSRF Token Cookie” message

- Refer to Salesforce Case 301537
- Example screenshot below:



Not Available: Forbidden

Missing CSRF token cookie

The request is not valid.

Not Available: Unauthorized

Per *https://support.ucraft.com/en/articles/5491128-how-to-fix-the-csrf-token-mismatch-error-message*

What's CSRF?
Cross-Site Request Forgery is an attack that forces the user to execute unwanted actions on a website during state-changing requests.

The “Invalid or missing CSRF token” message means that your browser couldn’t create a secure cookie or couldn’t access that cookie to authorize your login. This can be caused by ad- or script-blocking plugins or extensions and the browser itself if it's not allowed to set cookies.

**HTTPS/SSL Certificates (HTTPS certificates)

Good references regarding SSLx509 certificates:

- https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-authentication-54/Certificates.htm#Cert_What_is_it
- https://www.openssl.org/
- https://www.openssl.org/docs/man1.0.2/man5/x509v3_config.html

Apparently very good general reference about Certificate generation:

- https://mivilisnet.wordpress.com/2020/05/08/pem-cer-der-whats-that/#:~:text=Many%20times%2C%20those%20two%20formats,stored%20as%20the%20separated%20files.

FIPS-140 validation: https://www.openssl.org/docs/fips.html

Below is from online SecureSync user guide:
http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/HTTPS_cert_formats.htm

SecureSync supports X.509 PEM and DER Certificates, as well as PKCS#7 PEM and DER formatted Certificates.

You can create a unique X.509 self-signed Certificate, an RSA private key and X.509 certificate request using the Web UI. RSA private keys are supported because they are the most widely accepted. At this time, DSA keys are not supported.

SecureSync supports two different modes of HTTPS operation: The Standard HTTPS Level (default), and a High-Security Level. For more information, see HTTPS Security Levels.

Hashing and encryption algorithms

- Certificates define which hash to use for browser connections (such as “SHA1’ or ‘MD5’)
- Certificates do not define which encryption algorithms to select (this is determined by the **cipher lists** on the server and client)

HTTPS certificate validity/expiry

- Spectracom default certificate is valid for **10** years.
- New certificate needs to be manually created by user when it expires.

Supported Certificate Formats

- SecureSync supports X.509 PEM and DER Certificates, as well as PKCS#7 PEM and DER formatted Certificates.

CAC cards/DoD PKI certificates (for Dept of Defense)

- Refer to Salesforce Case 232854 (May 2020)
- Refer to sites such as: https://public.cyber.mil/pki-pke/

Q is the SecureSync capable of using DoD PKI Certificates for login authentication either for the GUI or SSH login? If not, is there a plan to incorporate this feature and when?

What is a DOD PKI certificate?
A **certificate** is a digital document providing the identity of a Web site or individuals. **DoD** Web sites use a **certificate** to identify themselves to their users and to enable secure connections. ... The **DoD PKI** Infrastructure is comprised of two Root **Certification** Authorities and a number of Intermediate Authorities.

Root certificate/Intermediate SSL certificates (chain certificates)

- Refer to sites such as https://kb.wisc.edu/page.php?id=18923

What is a **Root Certificate**?

- A Root SSL certificate is a certificate issued by a trusted certificate authority(CA).
- A root certificate is an unsigned or a self-signed public key certificate that identifies the root certificate authority (CA). A root certificate is part of a public key infrastructure scheme. The most common commercial variety is based on the ITU-T X.509 standard, which normally includes a digital signature from a certificate authority.
- A root certificate is the top-most certificate of the tree, the private key of which is used to "sign" other certificates.

What Is an **Intermediate Certificate**? To enhance the security of the Root certificate, we create two intermediate certificates from which SSL certificates are signed and issued.

An intermediate certificate is a subordinate certificate issued by the trusted root specifically to issue end-entity server certificates. The result is a certificate chain that begins at the trusted root CA, through the intermediate and ending with the SSL certificate issued to you. Such certificates are called chained root certificates.

Q Does the SecureSync support the inclusion of intermediate SSL certificates (chain certs)? If so, how does one install them? If not, is it on the roadmap (and what's the ETA)?

Certificate Chain

- It is also possible to upload a X.509 PEM Certificate Chain by pasting the text of the second certificate behind the regular CA Certificate.

Creating a new HTTPS Certificate Request (CR)

- Refer to the online SecureSync user manual: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/HTTPS_CertRequ.htm?Highlight=https%20certificate

SecureSync HTTPS doc: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\HTTPS certificate

- New HTTPS certificates/Certificate requests can only be created via the web browser.
- I believe the default certificate is created using sha256

A) Using the defcert CLI command to create new CR (Certificate Request)

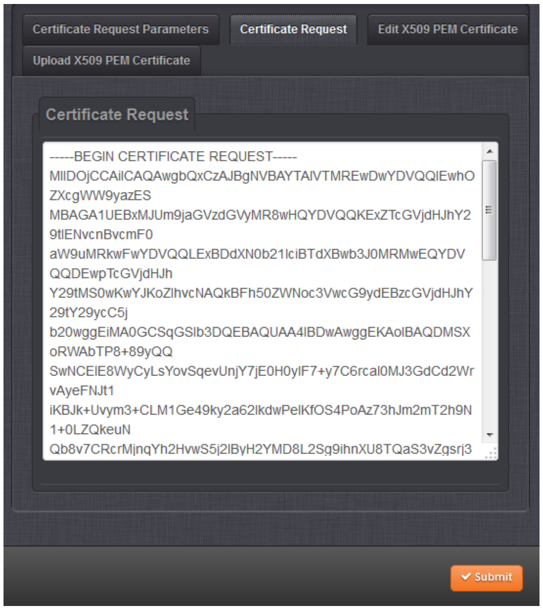
- The only CLI command associated with HTTPS certificates is the **defcert** command (to reset the certificate back to default)
  - optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
  - Example syntax is **defcert -sha256**
  - IE8 and below do not support SHA-256 (use **defcert -sha1** to regenerate a new certificate using SHA1 to gain access).

Note about keys for authentication and ciphers for encryption when generating new certificates

1) Keys for authentication are chosen via drop-downs when the certificate is created.
2) Ciphers for encryption are not defined in the certificate. A cipher is selected from a list (one in both the NTP server and the client) of ciphers supported. The most secure Cipher in both lists is typically selected.

B) Creating a new CR (Certificate Request) using the Web browser

1. Navigate to the **Management** -> **HTTPS Setup** page of the browser
2. (Optional Step to be able to confirm a new certificate has been created at the end of this process): Go to the **Certificate Request** tab to view the current certificate. Either screenshot it, as shown below or copy/paste the contents to a Word document.

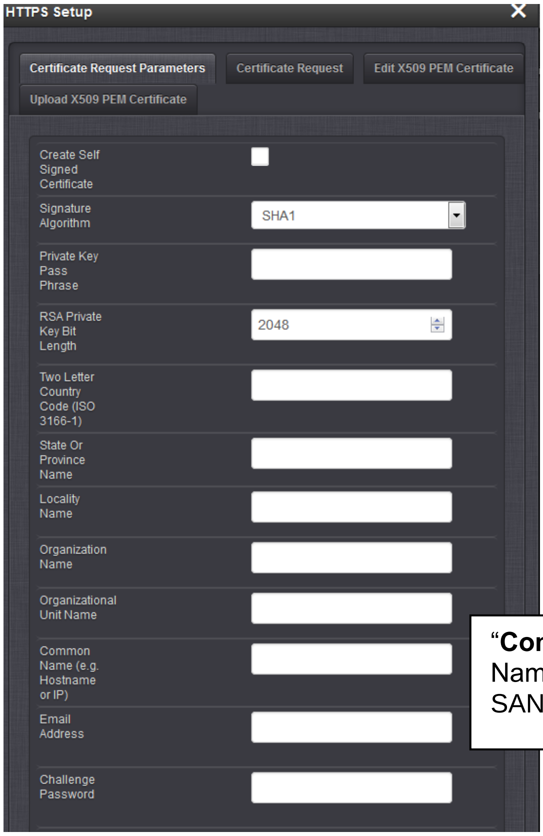


Certificate Request Parameters
Certificate Request
Edit X509 PEM Certificate
Upload X509 PEM Certificate
Submit

Certificate Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDOjCCAiICAQAwgbQxCzAJBgNVBAYTAlVTMREwDwYDVQQIEwhO
ZXcgWW9yazES
MBAGA1UEBxMJUm9jaGVzdGVyMR8wHQYDVQQKExZTcGVjdHJhY2
9tIENvcnBvcmF0
aW9uMRkwFwYDVQQLExBDdXN0b21lciBTdXBwb3J0MRMwEQYDV
QQDEwpTcGVjdHJh
Y29tMS0wKwYJKoZIhvcNAQkBFh50ZWNoc3VwcG9ydEBzcGVjdHJhY
29tY29ycC5j
b20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDMSX
oRWAbTP8+89yQQ
SwNCElE8WyCyLsYovSqevUnjY7jE0H0ylF7+y7C6rcal0MJ3GdCd2Wr
vAyeFNJt1
iKBJk+Uvym3+CLM1Ge49ky2a62lkdwPeIKfOS4PoAz73hJm2mT2h9N
1+0LZQkeuN
Qb8v7CRcrMjnqYh2HvwS5j2lByH2YMD8L2Sg9ihnXU8TQaS3vZgsrj3
```

3. Select the **“Certificate Request Parameters”** tab.

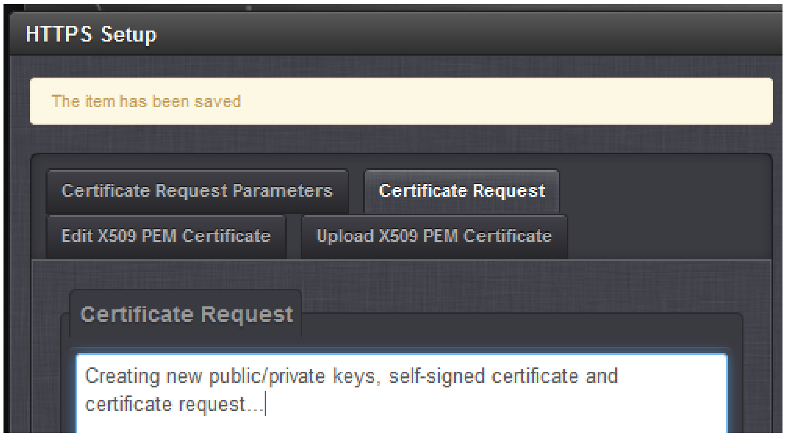


HTTPS Setup
Certificate Request Parameters
Certificate Request
Edit X509 PEM Certificate
Upload X509 PEM Certificate

Create Self Signed Certificate	□
Signature Algorithm	SHA1
Private Key Pass Phrase	
RSA Private Key Bit Length	2048
Two Letter Country Code (ISO 3166-1)	
State Or Province Name	
Locality Name	
Organization Name	
Organizational Unit Name	
Common Name (e.g. Hostname or IP)	
Email Address	
Challenge Password	

“**Common Name” field:** See additional “Common Name” info further below regarding RFC 2818 (DNS SAN) compliancy)

1. Enter data in the remaining fields
2. Press Submit
3. (Optional Step to see the new certificate is being/has been created)-Click on the “**Certificate Request**” tab after submitting the data. The Screenshot below shows the new certificate request is being generated.


HTTPS Setup
Certificate Request Parameters
Certificate Request
Edit X509 PEM Certificate
Upload X509 PEM Certificate

The item has been saved

Certificate Request

Creating new public/private keys, self-signed certificate and certificate request...

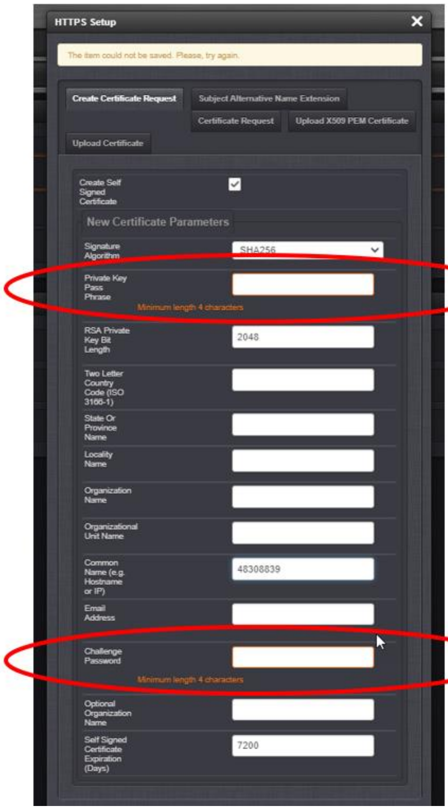
4. Once the certificate has been successfully created, the browser connection will be lost. Log back in and navigate back to the **Management** -> **HTTPS Setup** page of the browser. **Certificate Request** tab.

   Note: the larger the key size that was entered in the Certificate Request, the longer it takes for the new certificate to be created. It may take a few minutes to create the new certificate.

5. The Certificate Request field should now be different than the screenshot or copy/paste of the original certificate.

Info regarding particular fields in the CR creation

2. Private Key Pass phrase" and "Challenge Password" fields


HTTPS Setup
✕
Create Certificate Request
Subject Alternative Name Extension
Certificate Request
Upload X509 PEM Certificate
Upload Certificate

The item could not be saved. Please, try again.

Create Self Signed Certificate ☑

New Certificate Parameters

Signature Algorithm: SHA256

Private Key Pass Phrase:

Minimum length 4 characters

RSA Private Key Bit Length: 2048

Two Letter Country Code (ISO 3166-1):

State Or Province Name:

Locality Name:

Organization Name:

Organizational Unit Name:

Common Name (e.g. Hostname or IP): 48308839

Email Address:

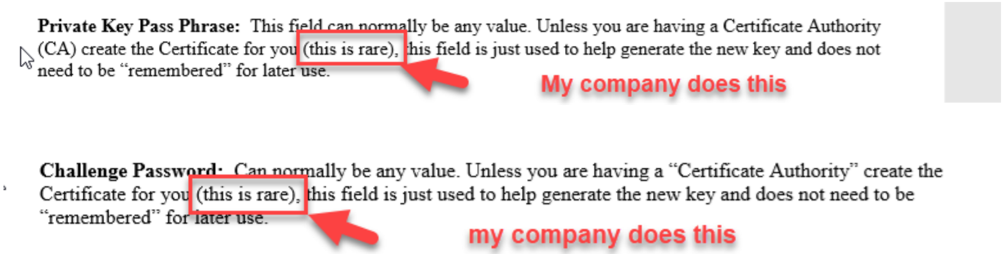
Challenge Password:

Minimum length 4 characters

Optional Organization Name:

Self Signed Certificate Expiration (Days): 7200

- Both these are mandatory fields (can't be left blank/null)
- Refer to Salesforce Cases such as 241766 for customers wanting to leave these fields blank (excerpt below)



Private Key Pass Phrase: This field can normally be any value. Unless you are having a Certificate Authority (CA) create the Certificate for you (this is rare), this field is just used to help generate the new key and does not need to be "remembered" for later use.

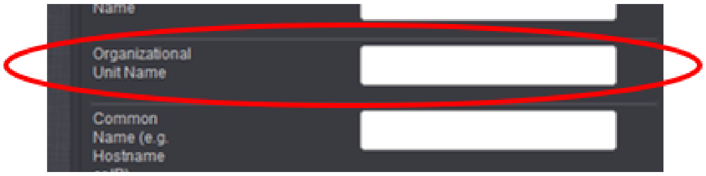
My company does this

Challenge Password: Can normally be any value. Unless you are having a "Certificate Authority" create the Certificate for you (this is rare), this field is just used to help generate the new key and does not need to be "remembered" for later use.

my company does this

So I need to leave those 2 fields blank and only enter CN info. How can I get past this?

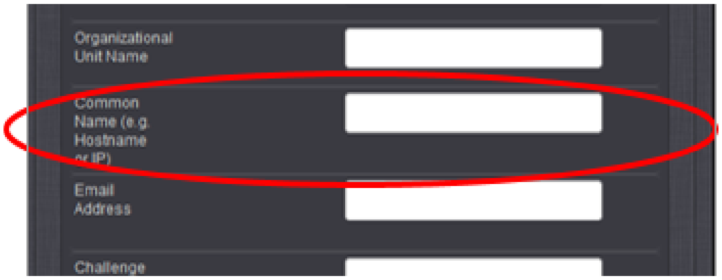
3. "Organizational Unit (OU)" field



CA requires multiple Organizational Unit (OU)

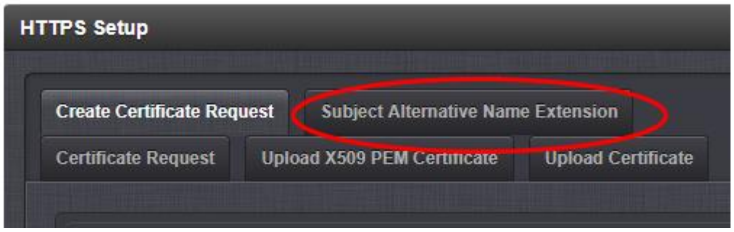
- ➢ This functionality not available in versions 5.7.1 and below (can only enter one OU value)
- ➢ Refer to SF case 119473 and JIRA ticket JIRA-SSS-380

4. "Common Name field" - Subject Alternate Name (DNS SAN) / RFC-2818 compliancy



RFC-2818 compliancy/ SAN Name (Subject Alternate Names) / UCC Certificate

- ➢ Refer to https://www.openssl.org/docs/apps/x509v3_config.html
- ➢ Refer to sites such as https://tools.ietf.org/html/rfc2818
  - o the Common name must be DNS SAN
- ➢ SAN certificates essentially allow adding more than one Common Name for the time server (standard certificate only supports one Common Name)
- ➢ Creating a SAN certificate involves configuring a second tab ("**Subject Alternative Name Extension**") in the HTTPS Setup page of the browser


HTTPS Setup
Create Certificate Request
Subject Alternative Name Extension
Certificate Request
Upload X509 PEM Certificate
Upload Certificate

Multiple Domain UCC Certificate (just another name for "SAN Certificate")

(Note: UCC stands for Unified Communication Certificate**)**

- Refer to sites such as:
  - https://www.godaddy.com/help/what-is-a-multiple-domain-ucc-ssl-certificate-3908 and https://www.ssl.com/faqs/what-is-a-ucc/

    A Unified Communications Certificate (UCC) is an SSL certificate that protects multiple domains and subdomains.

  - https://www.ssl.com/faqs/what-is-a-ucc/

    A **Unified Communication Certificate** (or **UCC**) is a digital security certificate which allows multiple hostnames to be protected by a single certificate.

    UC certificates are also known as **Subject Alternate Name** (or **SAN**) certificates, **multi-domain certificates** or **Exchange certificates**.

Q Is SecureSync RFC 2818 compliant?

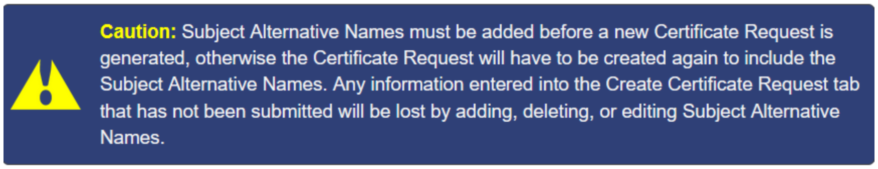
I am asking does your screens allow us to add a DNS Subject alternative Name(DNS SANS). https://www.chromestatus.com/features/4981025180483584 It is now being enforced by google chome, and eventually by all browser vendors.

Refer to https://www.openssl.org/docs/apps/x509v3_config.html

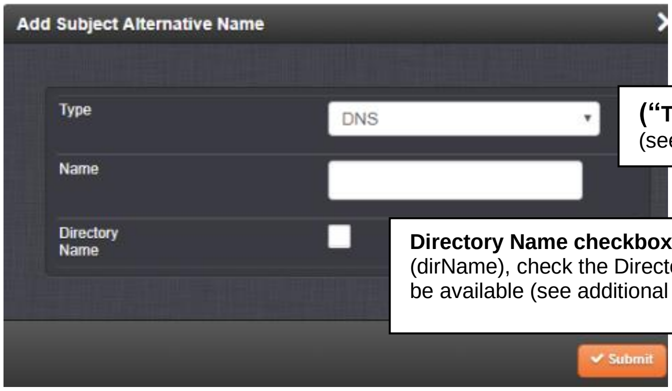
Refer to sites such as https://tools.ietf.org/html/rfc2818

the Common name must be DNS SAN

For info on creating a SAN certificate, Refer to the Model 2400 online SecureSync user guide at: https://www.orolia.com/manuals/2400/Content/NC_and_SS/Com/Topics/SETUP/HTTPSubjAltName.htm



Caution: Subject Alternative Names must be added before a new Certificate Request is generated, otherwise the Certificate Request will have to be created again to include the Subject Alternative Names. Any information entered into the Create Certificate Request tab that has not been submitted will be lost by adding, deleting, or editing Subject Alternative Names.



Add Subject Alternative Name

Type: DNS

Name:

Directory Name: □

✔ Submit

(“Type” dropdown) select: DNS, IP, email, URI, RID, or dirName (see additional info below)

Directory Name checkbox: For “Directory Subject Alternative Names” (dirName), check the Directory Name box, and additional optional fields will be available (see additional info below)

A) “Type” drop-down

Per https://www.openssl.org/docs/man1.0.2/man5/x509v3_config.html

The subject alternative name extension allows various literal values to be included in the configuration file. These include:

- **email** (an email address)
- **URI** a uniform resource indicator,
- **DNS** (a DNS domain name),
- **RID** (a registered ID: OBJECT IDENTIFIER),
- **IP** (an IP address, can be in either IPv4 or IPv6 format),
- **dirName** (a distinguished name) and otherName.

“Directory Name” (dirName) checkbox (to enable “Directory Subject Alternative Names”)

For Directory Subject Alternative Names (dirName), check the Directory Name box, and additional optional fields will be available:

- **Two Letter Country Code**: must match ISO-3166-1 value.
- **Organization name**: name of organization creating certificate.
- **Organizational Unit Name**: The applicable subdivision of the organization creating the certificate.
- **Common name**: The name of the host being authenticated. The Common Name field in the X.509 Certificate must match the host name, IP address, or URL used to reach the host via HTTPS.

B) Support for SANS/RFC-2818 was added in version 5.8.0 (May, 2018) and above:.

) Per the 5.8.0 Release Note: “Added HTTPS certificate support of SANS fields for Common Names”

A) Refer to JIRA Ticket JIRA-SSS-372 https://spectracom.atlassian.net/browse/SSS-372?jql=text%20~%20%22san%22%20order%20by%20created%20DESC

➢ Refer to earlier Mantis case 2867 (http://cvsmantis.int.orolia.com/mantis/view.php?id=2867

➢ Example associated Salesforce cases: 124543, 118702, 15127

➢ Software versions 5.7.3 and below, SAN is not supported.

➢ Refer to https://www.openssl.org/docs/apps/x509v3_config.html

Email Keith sent to Engineering I’m not aware of SecureSync currently being able to support Subject Alternate Names (SAN) SSL certificates (https://www.openssl.org/docs/apps/x509v3_config.html). But I wanted to confirm this before responding. I was wondering if it's possible to create SSL signing requests with subject alternate names? There doesn't seem to be any field for this value within the certificate generation utility provided within the web GUI.

- Refer to sites such as https://tools.ietf.org/html/rfc2818

  B) the Common name must be DNS SAN

Q Is SecureSync RFC 2818 compliant?

I am asking does your screens allow us to add a DNS Subject alternative Name(DNS SANS). https://www.chromestatus.com/features/4981025180483584 It is now being enforced by google chrome, and eventually by all browser vendors.

Note: Questions/Answer/info below are for all versions prion to v5.8.0 (before SANS support was added in 5.8.0)

A Per Keith (26 Sep 17) Apparently not (in update versions 5.7.1 and below …)

- (26 Sep 17) Per Paul M: "JIRA-SSS-372 is created and assigned to Ryan Johnson"

Note: As indicated below, this inquiry (case 118702) was due to Chrome browser:

Q Dave L to Paul (26 Sep 17) Cigna is looking to be compliant with the RFC2818 and had a comment about out Certificate Request setup in the SecureSync's web UI. They said we are missing a "Subject Alternative Name" field and this makes it difficult to generate a valid Certificate Request. This could be added in the next firmware update?

A Reply from Paul to Dave L (26 Sep 17) You are correct we will have to deprecate and remove use of COMMON NAME for SAN Subject Alternative Name.

I had believed we WERE basically compliant to RFC 2818 by accepting a single fully qualified domain name (FQDN) due to current practices of using the common name…

However, it appears I am wrong now. RFC2818 when properly read and implemented calls for dropping support of COMMON NAME for SAN (Subject Alternative Name) except NO ONE DID IT for the last 17 years.

Google Chrome 58 stable in April 2017 finally initiated this long overdue change likely because it is being exploited.

https://www.thesslstore.com/blog/security-changes-in-chrome-58/
https://productforums.google.com/forum/#!topic/chrome/-19ZxwjaCjw
https://en.wikipedia.org/wiki/Subject_Alternative_Name

The Subject Alternative name appears to be referenced/defined in RFC 5280
https://tools.ietf.org/html/rfc5280#section-4.2.1.6

Reported bug in SW V5.9.4" (new certificate request under HTTPS Setup, creates new line in "Subject Alternative Names)

"We noticed a new bug in version 5.9.4. If you create a new certificate request under HTTPS Setup, it creates a new line in "Subject Alternative Names", when the line already exists. This causes new cert requests on the CA side to fail. It should probably check if the alternative name exists and not add it if it does. Please let me know if you need more details."

- Reported July 2022
- Refer to Salesforce Case 286588/JIRA ticket SSS-1288

Creating a new Certificate from the exported Certificate Request (CR)

Certificate formats we can accept

From the SecureSync user manual

“The SecureSync’s software supports X.509 DER and PEM and P7 PKCS#7 PEM and DER formatted certificates. The user can create a customer specific X.509 self-signed certificate, an RSA private key and X.509 certificate request using the web browser user interface. RSA private keys are supported because they are the most widely accepted (at this time, DSA keys are not supported).”

Per Paul Myers (1 Nov 16)

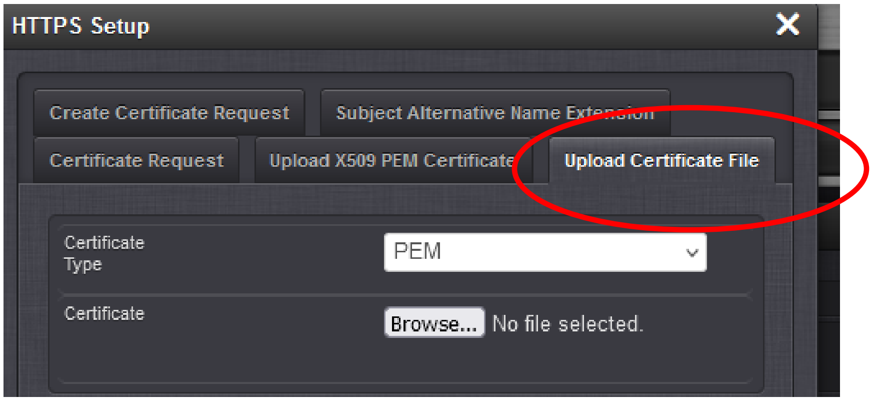
You can ONLY paste x509 PEM certificates. You must upload the other certificate types using the defined filenames in the manual to correctly install them.

Again cut and paste ONLY applies to **PEM**.

The other certificate types must be renamed, selected and uploaded to the SecureSync web ui where they are converted to PEM x509 internally and installed.

Copy/pasting or Uploading a custom-created PEM or PKCS certificate into the time server

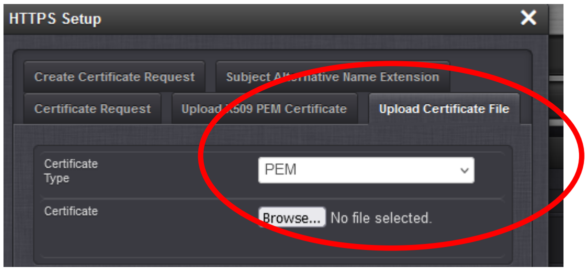
- **PEM files can be either copy/pasted into the browser or the file uploaded.**
- **PKCS7/DER files must be uploaded using the “Upload Certificate File” (they cant be copy/pasted into the browser like PEM certs)**


HTTPS Setup
Create Certificate Request
Subject Alternative Name Extension
Certificate Request
Upload X509 PEM Certificate
Upload Certificate File
Browse...

Certificate Type: PEM

Certificate: No file selected.

A) Known software issue with “Upload Certificate File” tab (fixed in update version 1.7.0)


HTTPS Setup
Create Certificate Request
Subject Alternative Name Extension
Certificate Request
Upload X509 PEM Certificate
Upload Certificate File
Browse...

Certificate Type: PEM

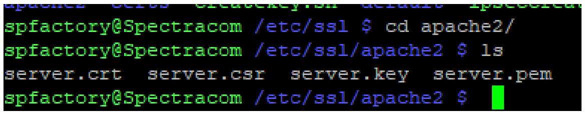
Certificate: No file selected.

- ➢ With at least 2400 version 1.6.0 (and likely previous- fixed in 1.7.0) Uploading a PEM/DER file via the “Upload Certificate File” tab doesn’t work
- ➢ Can successfully copy/paste ”.PEM” cert into the browser. But can’t upload .PEM or .DER files via the Upload
- ➢ Refer to JIRA Tickets CAR-2222 (*Problems in uploading .der https certificates*) and CAR-2378 (*Problem uploading PKCS7 .der and .pem https certificates*)
- ➢ Per the v1.7.0 Release Notes:

- ○ "Repaired PKCS7 http certificate uploads in the .der and .pem file formats"

HTTPS Certificate files in the SecureSync (server.crt, server.csr, server.key server.pem)

(internal use only) location of HTTPS certificate files: /etc/ssl/apache2

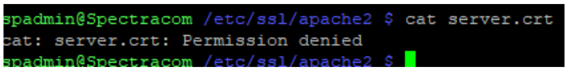


```
spfactory@Spectracom /etc/ssl $ cd apache2/
spfactory@Spectracom /etc/ssl/apache2 $ ls
server.crt  server.csr  server.key  server.pem
spfactory@Spectracom /etc/ssl/apache2 $
```

A) server.crt file (I believe this is the X509 PEM (plain text) HTTPS public key Certificate file)

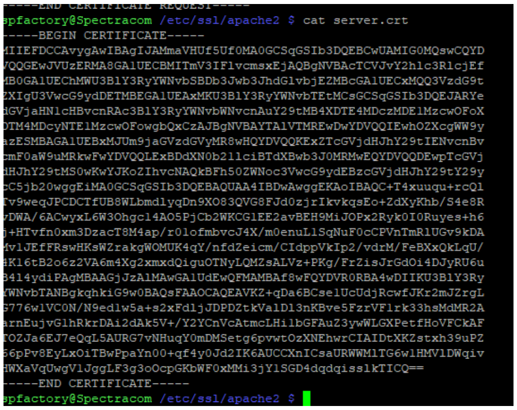
- ➢ I confirmed this file changes automatically after creating a new Certificate Request (CR) via Management **-> HTTPS Setup** page

cat server.crt ***(as spadmin) "Permission denied"***



```
spadmin@Spectracom /etc/ssl/apache2 $ cat server.crt
cat: server.crt: Permission denied
spadmin@Spectracom /etc/ssl/apache2 $
```

cat server.crt ***(as spfactory)***

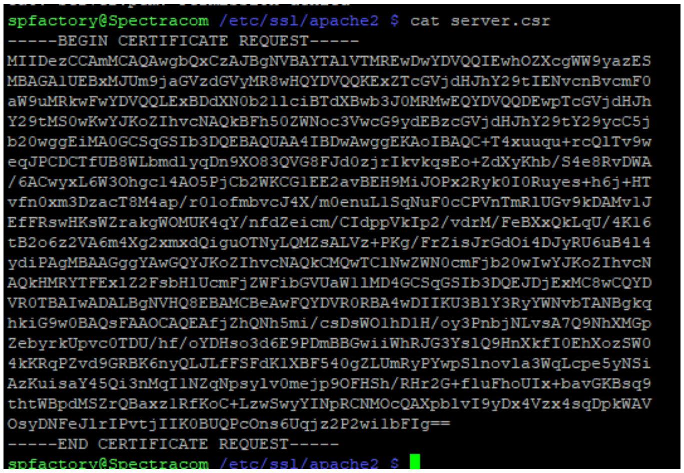


```
-----END CERTIFICATE REQUEST-----
spfactory@Spectracom /etc/ssl/apache2 $ cat server.crt
-----BEGIN CERTIFICATE-----
MIIEFDCCAvygAwIBAgIJAMmaVHUf5Uf0MA0GCSqGSIb3DQEBCwUAMIG0MQswCQYD
VQQGEwJVUzERMA8GA1UECBMITmV3IFlvcmsxEjAQBgNVBAcTCVJvY2hlc3RlcjEf
MB0GA1UEChMWU3BlY3RyYWNvbSBDb3Jwb3JhdGlvbjEZMBcGA1UECxMQQ3VzdG9t
ZXIgU3VwcG9ydDETMBEGA1UEAxMKU3BlY3RyYWNvbTEtMCsGCSqGSIb3DQEJARYe
dGVjaHNlcHBvcnRAc3BlY3RyYWNvbWNvcnAuY29tMB4XDTE4MDczMDE1MzcwOFoX
DTM4MDcyNTE1MzcwOFowgbQxCzAJBgNVBAYTAlVTMREwDwYDVQQIEwhOZXcgWW9y
azESMBAGA1UEBxMJUm9jaGVzdGVyMR8wHQYDVQQKExZTcGVjdHJhY29tIENvcnBv
cmF0aW9uMRkwFwYDVQQLExBDdXN0b21lciBTdXBwb3J0MRMwEQYDVQQDEwpTcGVj
dHJhY29tMS0wKwYJKoZIhvcNAQkBFh50ZWNoc3VwcG9ydEBzcGVjdHJhY29tY29y
cC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+T4xuuqu+rcQl
Tv9weqJPCDCTfUB8WLbmdlyqDn9XO83QVG8FJd0zjrIkvkqsEo+ZdXyKhb/S4e8R
vDWA/6ACwyxL6W3Ohgcl4AO5PjCb2WKCGlEE2avBEH9MiJOPx2Ryk0I0Ruyes+h6
j+HTvfn0xm3DzacT8M4ap/r0lofmbvcJ4X/m0enuLlSqNuF0cCPVnTmRlUGv9kDA
MvlJEfFRswHKsWZrakgWOMUK4qY/nfdZeicm/CIdppVkIp2/vdrM/FeBXxQkLqU/
4Kl6tB2o6z2VA6m4Xg2xmxdQiguOTNyLQMZsALVz+PKg/FrZisJrGdOi4DJyRU6u
B4l4ydiPAgMBAAGjJzAlMAwGA1UdEwQFMAMBAf8wFQYDVR0RBA4wDIIKU3BlY3Ry
YWNvbTANBgkqhkiG9w0BAQsFAAOCAQEAVKZ+qDa6BCselUcUdjRcwfJKr2mJZrgL
G776wlVC0N/N9edlw5a+s2xFdljJDPDZtkValDl3nKBve5FzrVFlrk33hsMdMR2A
arnEujvGlhRkrDAi2dAk5V+/Y2YCnVcAtmcLHilbGFAuZ3ywWLGXPetfHoVFCkAF
TOZJa6EJ7eQqL5AURG7vNHuqY0mDMSetg6pvwtOzXNEhwrCIAIDtXKZstxh39uPZ
66pPv8EyLxOiTBwPpaYn00+qf4y0Jd2IK6AUCCXnICsaURWWMlTG6wlHMVlDWqiv
HWXaVqUwgVlJggLF3g3oOcpGKbWF0xMMi3jYlSGD4dqdqisslkTICQ==
-----END CERTIFICATE-----
spfactory@Spectracom /etc/ssl/apache2 $
```

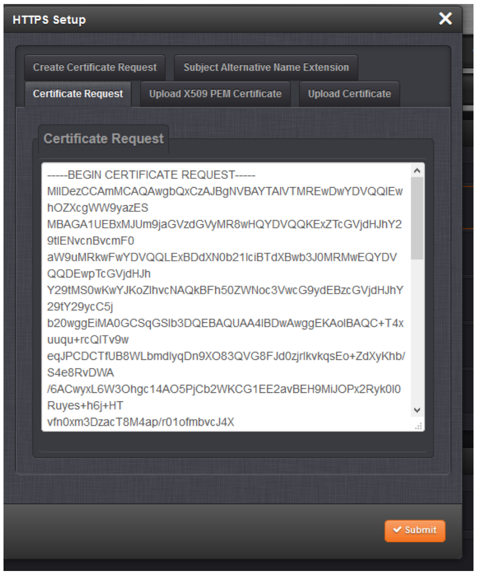
B) server.csr file (this is the Certificate Request / “CR” file)

cat server.csr ***(as either spadmin or spfactory)***

Management -> HTTPS Setup page



```
spfactory@Spectracom /etc/ssl/apache2 $ cat server.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIDezCCAmMCAQAwgbQxCzAJBgNVBAYTAlVTMREwDwYDVQQIEwhOZXcgWW9yazES
MBAGA1UEBxMJUm9jaGVzdGVyMR8wHQYDVQQKExZTcGVjdHJhY29tIENvcnBvcmF0
aW9uMRkwFwYDVQQLExBDdXN0b21lciBTdXBwb3J0MRMwEQYDVQQDEwpTcGVjdHJh
Y29tMS0wKwYJKoZIhvcNAQkBFh50ZWNoc3VwcG9ydEBzcGVjdHJhY29tY29ycC5j
b20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+T4xuuqu+rcQlTv9w
eqJPCDCTfUB8WLbmdlyqDn9XO83QVG8FJd0zjrIkvkqsEo+ZdXyKhb/S4e8RvDWA
/6ACwyxL6W3Ohgc14AO5PjCb2WKCG1EE2avBEH9MiJOPx2Ryk0I0Ruyes+h6j+HT
vfn0xm3DzacT8M4ap/r01ofmbvcJ4X/m0enuLlSqNuF0cCPVnTmRlUGv9kDAMvlJ
EfFRswHKsWZrakgWOMUK4qY/nfdZeicm/CIdppVkIp2/vdrM/FeBXxQkLqU/4Kl6
tB2o6z2VA6m4Xg2xmxdQiguOTNyLQMZsALVz+PKg/FrZisJrGdOi4DJyRU6uB4l4
ydiPAgMBAAGggYAwGQYJKoZIhvcNAQkCMQwTClNwZWN0cmFjb20wIwYJKoZIhvcN
AQkHMRYTFExlZ2FsbHlUcmFjZWFibGVUaW1lMD4GCSqGSIb3DQEJDjExMC8wCQYD
VR0TBAIwADALBgNVHQ8EBAMCBeAwFQYDVR0RBA4wDIIKU3BlY3RyYWNvbTANBgkq
hkiG9w0BAQsFAAOCAQEAfjZhQNh5mi/csDsWOlhDlH/oy3PnbjNLvsA7Q9NhXMGp
ZebyrkUpvc0TDU/hf/oYDHso3d6E9PDmBBGwiiWhRJG3YslQ9HnXkfI0EhXozSW0
4kKRqPZvd9GRBK6nyQLJLfFSFdKlXBF540gZLUmRyPYwpSlnovla3WqLcpe5yNSi
AzKuisaY45Qi3nMqIlNZqNpsylv0mejp9OFHSh/RHr2G+fluFhoUIx+bavGKBsq9
thtWBpdMSZrQBaxzlRfKoC+LzwSwyYINpRCNMOcQAXpblvI9yDx4Vzx4sqDpkWAV
OsyDNFeJlrIPvtjIIK0BUQPcOns6Uqjz2P2wilbFIg==
-----END CERTIFICATE REQUEST-----
spfactory@Spectracom /etc/ssl/apache2 $
```



HTTPS Setup

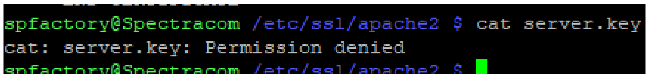
✕
Create Certificate Request
Subject Alternative Name Extension
Certificate Request
Upload X509 PEM Certificate
Upload Certificate

Certificate Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDezCCAmMCAQAwgbQxCzAJBgNVBAYTAlVTMREwDwYDVQQIEw
hOZXcgWW9yazES
MBAGA1UEBxMJUm9jaGVzdGVyMR8wHQYDVQQKExZTcGVjdHJhY2
9tIENvcnBvcmF0
aW9uMRkwFwYDVQQLExBDdXN0b21lciBTdXBwb3J0MRMwEQYDV
QQDEwpTcGVjdHJh
Y29tMS0wKwYJKoZIhvcNAQkBFh50ZWNoc3VwcG9ydEBzcGVjdHJhY
29tY29ycC5j
b20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+T4x
uuqu+rcQlTv9w
eqJPCDCTfUB8WLbmdlyqDn9XO83QVG8FJd0zjrIkvkqsEo+ZdXyKhb/
S4e8RvDWA
/6ACwyxL6W3Ohgc14AO5PjCb2WKCG1EE2avBEH9MiJOPx2Ryk0I0
Ruyes+h6j+HT
vfn0xm3DzacT8M4ap/r01ofmbvcJ4X
```

C) server.key file (this is the **private key** file which has to remain inside the SecureSync)

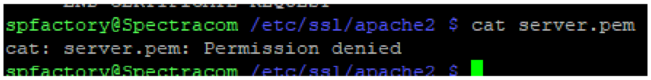
cat server.key (as either spadmin or spfactory) *“***Permission denied***”*



```
spfactory@Spectracom /etc/ssl/apache2 $ cat server.key
cat: server.key: Permission denied
spfactory@Spectracom /etc/ssl/apache2 $
```

D) server.pem file (this is the file

cat server.pem (as either spadmin or spfactory) *“*Permission denied*”*



```
spfactory@Spectracom /etc/ssl/apache2 $ cat server.pem
cat: server.pem: Permission denied
spfactory@Spectracom /etc/ssl/apache2 $
```

Issues observed after installing the CERT

A) Customers often install a “generic” CERT that was not generated from the Certificate Request (CSR) generated in/extracted from the SecureSync (or install the same Cert on more than one SecureSync)

1. This corrupts HTTPS (it stops working)
2. All PC’s display will likely show an error message, such as “This site can’t be reached”
3. Login to the CLI interface (telnet or ssH) and type: **defcert**
   - Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.

     Example syntax is **-sha256**

- V5.6.0 also changed the default algorithm to SHA256 for better security. IE8 and below do not support SHA-256 (use **defcert -sha1** to regenerate a new certificate using SHA1 to gain access).

4. Perform an **unrestrict** CLI command
5. Perform a **servset 6 off** and then a **servset 6 on**

Slightly modified Email Keith sent to help troubleshoot (15 May 2020) "This site can't be reached" is a very generic message, that the PC can't reach the SecureSync over the network. It doesn't appear this message is related to the HTTPS certificate, especially if it's the only message displayed. (no certificate error messages being displayed).

Some questions for you:

1) Was the PEM certificate generated directly from the Certificate Request (CSR) first created/extracted from the SAME SecureSync the certificate was installed in Note this is absolutely essential. Installing a "generic certificate not generated from the Certificate Request (or installing a cert in a different SecureSync than the SecureSync that the CSR was generated in) will corrupt HTTPS. The "invalid certificate needs to be deleted for HTTPS to work again.
2) What browser app (and its version) are you using on this PC to connect (such as Internet Explorer, Firefox, Chrome, etc?
3) To confirm is "This site can't be reached" the only message being displayed?
4) Is this PC on the very same subnet as the SecureSync? or, are there any routers/firewalls in between?
5) Was it verified that this same PC was able to login to the SecureSync's browser JUST before copy/pasting the new PEM certificate into the SecureSync?
6) Can you connect to the SecureSync's web browser from this same PC, using a different browser app installed on this PC (if you are currently using Internet Explorer to try to connect, can you connect to the SecureSync using Chrome or Firefox, for instances)?
7) Can you still connect to the SecureSync's web browser from any other PC on the network?
8) Can you access/login to the SecureSync's CLI interface (via an ssh session) from this same PC displaying the error.

Let us know the answers to the above questions and then we can go from there.

"Accept" the new certificate in each PC, the next time the PC is used to connect to the SecureSync

---

Emailed general info from Paul Myers (3/5/12)

- **In regards to HTTPS:**
    - Certificates are used for HTTPS sessions. We only support the following.
    - **Loading x509 PEM certificates from the Web UI – Default for APACHE web server**
    - We support the user loading Public Keys via FTP by specific filename and then selecting then enabling that certificate for use using the WebUI
    - This could be improved on with a better web UI but so far no one has complained or even used it I believe.
    - We convert the following certificates from these types identified by file name to the x509 PEM used by Apache
    - FTP a file named **cert.pem** which means **x509 PEM**
    - FTP a file named **cert.der** which means **x509 DER**
    - FTP a file named **certpem.p7c** which means **PKCS7 PEM**
    - FTP a file named which means **PKCcdS7 DER**

B) For an x509 PEM certificate (either copy/paste or upload the new certificate)

1) X509 PEM (plain text) certs can be simply copy/pasted into the web browser

- Refer to the online SecureSync user guide: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/UploadX509Cert.htm

After extracting the certificate request via copy/paste, a new certificate can be created and then be transferred into the time server.

Email from Paul Myers (1 Nov 16) I did issue a F5 refresh SOMETIMES and was forced to accept the new certificate in these case. BUT I did not have to login.

1. Using Chrome Login as spadmin (specify customer version)
   - Go to ***Management***->***HTTPS Setup***
   - Create a new HTTPS Self-Signed Certificate and Certificate Request
   - Enter Certificate Request Parameters and select the checkbox at top of page
   - Press submit
   - Select Certificate Request Tab and wait
   - You will see "Creating new public/private keys, self-signed certificate and certificate request..."
   - It takes TBD minutes depending on key length chosen to create new internal SELF-Signed certificate
   - In the meantime when the new Self-Signed certificate is created the Apache2 web server is restarted.
   - If the user closes the tab OR hits F5 to refresh and watches the Certificate Request tab eventually the Certificate Request text will appear.
   - The user does not need to login to the web ui.
   - The Certificate Request (CR) can now be provided to their CA Certificate Authority to create a Certificate they can reload it.

2) X509 PEM (plain text) certs can alternatively be uploaded using the web browser

- Refer to the online SecureSync User Manual: :http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/LoadNonX509cert.htm

C) For formats other than PEM (such as DER and PKCS) (uploading a new certificate)

- unless it is a X.509 PEM-format Certificate, once the HTTPS Certificate has been issued by your Certificate Authority, you have to upload the Certificate file to SecureSync,
  - Refer to online SecureSync User Manual: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/LoadNonX509cert.htm

Obtaining SSL Certificate details (such as expiration date) from SecureSync

- Refer to Salesforce Case 240116
- "**View**" the certificate in the web browser (Firefox, Internet Explorer, etc)

Q I am working on pulling the SSL Cert details for NTP devices. Do we have any API where we can pull SSL cert info like certname and Expiry date.

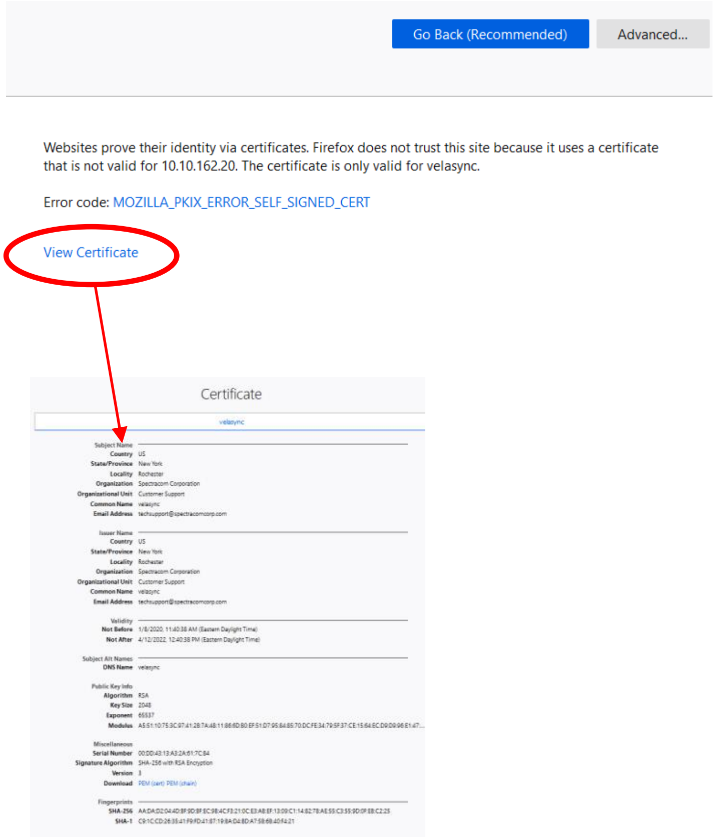
A Reply from Dave L (27 July 2020) Onboard the SecureSync we do not have a CLI command that will read the information you are looking for. Once installed the SSL Certificate expiration date and name cannot be read in the SecureSync. Openssl can be used to decode a certificate, but I am not sure the path to do this. Perhaps your web browser of choice can provide the information you need for the certificate.

Viewing certificate in Firefox:

2. **Tools -> Options -> Privacy & Security -> View Certificate**

OR

3. **Cerificate can be viewed while establishing an HTP connections**



Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 10.10.162.20. The certificate is only valid for velasync.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

Certificate

velasync

Subject Name	
Country	US
State/Province	New York
Locality	Rochester
Organization	Spectracom Corporation
Organizational Unit	Customer Support
Common Name	velasync
Email Address	techsupport@spectracomcorp.com
Issuer Name	
Country	US
State/Province	New York
Locality	Rochester
Organization	Spectracom Corporation
Organizational Unit	Customer Support
Common Name	velasync
Email Address	techsupport@spectracomcorp.com
Validity	
Not Before	1/8/2020, 11:40:38 AM (Eastern Daylight Time)
Not After	4/12/2022, 12:40:38 PM (Eastern Daylight Time)
Subject Alt Names	
DNS Name	velasync
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	A5:51:10:75:3C:97:41:28:7A:48:11:86:6D:B0:EF:51:D7:95:84:85:70:DC:FE:34:79:5F:37:CE:15:64:EC:D9:D9:96:E1:47:...
Miscellaneous	
Serial Number	00:DD:43:13:A3:2A:61:7C:84
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)
Fingerprints	
SHA-256	AA:DA:D2:04:4D:8F:9D:8F:EC:98:4C:F3:21:0C:E3:A8:EF:13:09:C1:14:82:78:AE:55:C3:55:9D:0F:EB:C2:25
SHA-1	C9:1C:CD:26:35:41:F9:FD:41:87:19:8A:D4:8D:A7:58:68:40:F4:21

Desire to export private key or public/private key pair

- Refer to case 116919, Sep 2017 (for Cerner desiring to export private key for external storage)

Per Paul Myers (26 Sep 17, as of alt least v5.7.1 and below) At this time we do not support access to the Public/Private Keys or allow their retrieval or loading on the SecureSync. The netClock 9100/9200 I believe supported this feature, but we found it to be a security risk and NOT common practice to do this.

I think we would need to add web ui and some script changes to effect loading and retrieval of public/private keys and loading certificates. We would need affect changes for software update possibly and to add this change to a new release.

If we created a hotpatch to do this and allowed user access to add files it might teach them how to modify and attack our SecureSync security.

I think we need to do the following:

1. Discuss this with David Sohn and Ryan to see if we should do this.
2. Create a use case or user story as to WHY the customer must do this.
3. Determine if this results in an unacceptable security vulnerability?
4. Determine if any competitors allow this and is it a competitive advantage or disadvantage.

Possibly this might have to be NOT done, added as an expert mode or license hidden. I don't know yet.

https://na28.salesforce.com/5001A00001Lt4DC

Backing-up of the HTTPS certificates

- As of at least versions 5.3.0 and below, public and private SSL certificates are not backed-up.

Q (from David Bradley) My question is, how to backup/save my private key. When requesting a purchased SSL certificate you generate the private key and the certificate request pair. You then send the certificate request to the certificate provider.

If the spectracom NTP server is restored to factory conditions the SSL certificate is lost. If you were able to reinstate you previously generated private key you could simply re-use your SSL certificate, but without the private key you have generate a new key and request and contact the certificate provider for a replacement.

I cannot see any way within the web interface a way to copy the private key, I wondered if this was possible via the command line, using the SPADMIN user.

A Reply from Morgan (9 Nov 15- applies to at least 5.3.0 and below) We better understand your question now. From a Spectracom perspective we have not seem this as a problem, because the provider of our certificates allow us to regenerate a new certificate as long as we have active service with them. Will you certificate provider allow you to regenerate a new certificate during your activation period? If not let us know and I will forward to engineering.

Issues with creating/installing a new SSL certificate (HTTPS certificate)

A) Issues with creating a new certificate (specific to Chrome)

- (2 Nov 16) Dave L had a customer having issues with transferring in a new certificate using Chrome

(Email from Dave L to Paul Myers) Turns out Chrome was not updating the screens properly. We had much better luck using Firefox.

B) Issues with creating a new certificate (specific to Internet Explorer- IE)

- Refer to Mantis case 1903 (noticed in version 4.8.7 Dec 2012)
- Internet Explorer 8 sometimes requires the user to press OK many times to accept the new HTTPS certificate. This ONLY observed with IE and does not always occur.

C) Error message generated when creating a new certificate in version 5.3.1

- Refer to Mantis case 3202
- Error message asserted: “the item could not be saved. Please try again”.

Email from Paul Myers (12 Jan 16) If they really need this they might be able to drop to an old release, setup certificate then update and keep using it under new firmware. They just can’t create a new one. ordan Comstock looked into it and has not found why yet.

D) Creating a HTTPS Certificate Request and Public/Private key pair fails when entering FQDN (Fully qualified Domain Name, also known as Common Name) instead of entering the IP address (~~versions 5.1.7 and below. Fixed in 5.2.0~~).

- Refer to Mantis case 2940.
- Applicable to software versions 5.2.1 and below (fixed in update version ~~5.2.0~~ ~~5.2.1~~ 5.3.0)
- Common Name field won’t accept a dot (and apparently not a hyphen either) unless it’s for an IP address. But dots are needed to enter a common name (FQDN)
- Actually fixed in version 5.3.0 update (April 2015). Not sure what happened but a customer saw this issue with 5.2.0 installed and I also duplicated with 5.2.0 (30 Apr 15). So ~~it looks like~~ it really wasn’t fixed in either 5.1.8 or 5.2.0 OR 52.1, 5.2.0 candidate was good, but the candidate was changed back, before 5.2.0 was released. Fix was also omitted from 5.2.1 update, as well.
- Note that a ‘hyphen’ now appears to be accepted in v5.3.0 (it appears in 5.3.0 and above, this field will now accept

any character).

E) Versions 4.8.5 and below have a web browser buffer size limitation

Q. I am able to create a valid CSR and self-signed certificate. Our CA accepts the CSR and issues a certificate. Uploading the certificate to the NTP server succeeds, regardless of the mechanism (HTTP or FTP). Validation of the certificate claims to succeed - but immediately afterward, the Apache web server process crashes and does not recover.

From /var/log/apache2/error_log:

```
[Fri Apr 20 03:55:34 2012] [error] Init: Unable to read server certificate from file /etc/apache/ssl.crt/server.crt

[Fri Apr 20 03:55:34 2012] [error] SSL Library Error: 218529960 error:0D0680A8:asn1 encoding
routines:ASN1_CHECK_TLEN:wrong tag

[Fri Apr 20 03:55:34 2012] [error] SSL Library Error: 218595386 error:0D07803A:asn1 encoding
routines:ASN1_ITEM_EX_D2I:nested asn1 error
```

- Refer to Salesforce Case Number 00005314 for specifics.

Likely cause is either inadvertently uploading the Certificate Request instead of the CA-generated Certificate (or not uploading a Certificate format we accept).

(5/18/12 KW) update to this issue. See comment below that the issue is due to the buffer size being limited to just 2kb. A file larger than this will be truncated. Paul Myers plans to increase buffer to 8k to likely prevent this from occurring again.

Refer to Salesforce case 5314 for details

NOTE: Versions 4.8.5 and below have a 2k web browser buffer size (should be increased to 8k in version 4.8.6). This can truncate an imported HTTPS certificate. If the certificate file is transferred with scp, this is not an issue.

Either transfer the file via SCP or update the SecureSync to a newer version of software.

Email from Ian Roussos It appears that the combination of the 4.8.5 software upgrade and SCP instead of HTTP upload has resolved my issue. I have a production certificate from the correct CA installed now.

When I used the HTTP upload process, the file size for /etc/apache/ssl.crt/server.crt did not change correctly – it was much smaller than it was supposed to be. When I used the SCP upload process the file size was exactly correct. This was true regardless of which CA I used. On 4.8.0, it did not appear to matter which transfer mechanism I used, the file did not update correctly.

Regardless, from my perspective this issue is closed. Thank you for your assistance and patience in helping me resolve it – I appreciate it.

HTTP/HTTPS automatic re-direct

- The need to enter “HTTPS://” before the IP address: “HTTPS re-direct” can only occur if HTTP is enabled in Services (The redirect is inside the Spectracom box, so it has to be able to get in through http first).

With HTTP enabled, all you need to type in the browser window is the IP address (don’t have to type anything in front of the IP address. However, if the HTTP service is disabled in the spectracom box, you have to type “HTTPS://” in the browser (in front of the IP address) in order to be able to access the browser.

Need to Reset HTTPS certificate (bad certificate was created, or certificate has expired, for examples)

defcert is the RS-232 command used to reset the HTTPS certificate (for security reasons, this command can only be performed via an RS-232 connection to the front panel SERIAL port. It’s not available with the other CLI interfaces, such as telnet and SSH).

- The only CLI command associated with certificates is the **defcert** command (to reset the certificate back to default)

- Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
- An example defcert CLI syntax (5.6.0 and above only) is **defcert -sha256**
- V5.6.0 also changed the default algorithm to **SHA256** for better security (the default in 5.5.1 and below was SHA1) .
- As IE8 and below do not support SHA-256, in versions 5.6.0 and above, use **defcert -sha1** to regenerate a new certificate using SHA1 to gain access to IE8 and below

Email from Keith (20 Jul KW) One thing to keep in mind is that, depending on the current software version installed in the SecureSync, the **defcert** command will create its new default certificate using either a **SHA1** cipher or a **SHA256** cipher.

With software **versions 5.6.0 and above** installed in the SecureSync, the more secure SHA256 encryption cipher will be used to generate its new certificate (with version 5.5.1 and below, the defcert command used the SHA1 cipher).

The issue with the more secure SHA256 cipher is **Internet Explorer versions 8** and below can't use this newer cipher. With these more recent versions of software installed in the SecureSync (5.6.0 and above), and when using IE8 or below to access the SecureSync, instead of using the CLI command of **defcert** to replace the existing certificate, issue instead the following CLI command to generate a new certificate using the earlier SHA1 cipher: **defcert -sha1** <enter>. Then try accessing the web browser again.

The RS-232 command to reset the HTTPS Certificate back to the default value is "defcert". This command is issued via the front panel RS-232 Serial port, using a PC running HyperTerminal (or other terminal emulator program). The PC's com port should be connected to the NTP server using a standard DB9M to DB9F serial cable that is pinned straight-thru (at least pin 2 to 2, pin 3 to 3 and pin 5 to 5 for the minimum configuration). If a serial com port is not available on your PC, a standard USB to Serial adapter will be needed and its driver installed.

Account Locked due to xx failures": Limit number of web browser/ssh login attempts/re-tries (entering incorrect password several times in a row)

- Refer also to the "**User Accounts and passwords**" section further below for information.
- Refer also to SalesForce cases such as 172784
- Refer to "**Number of Failed login attempts**" in online SecureSync user guide (excerpt below) http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/CONFIG/OpeningWebUI.htm?Highlight=login%20attempts

Number of available login attempts (web browser versus Telnet/ssh)

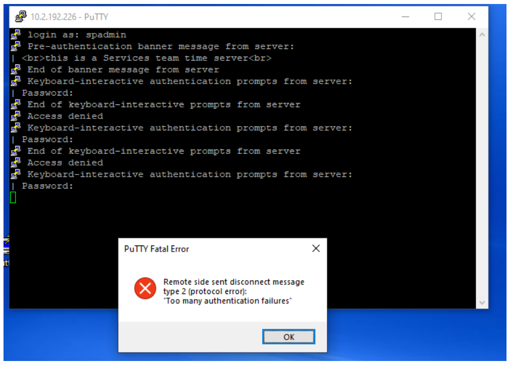
A) Web UI (HTTP/HTTPS)

- The number of failed login attempts for the Web UI (HTTP/HTTPS) is hard-set to (5) five failed login attempts, with a 60 second lock. These two values are not configurable.

  Note from Keith (7 Sept 18) The web browser doesn't show/report any indication that it's locked for 60 seconds after the 5th failed. The "lock" is only in the "background".

B) Telnet/SSH:

- The number of failed login attempts for ssh is hard-set to **(4) four**. This value is not configurable
- The number of failed login attempts for ssh is hard-set to **(3) three, with a 60 second lock thereafter**. This value is not user-configurable.



```
login as: spadmin
Pre-authentication banner message from server:
| <br>this is a Services team time server<br>
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
| Password:
```

PuTTY Fatal Error

Remote side sent disconnect message
type 2 (protocol error):
"Too many authentication failures"

- ➢ After waiting a full **60 seconds**, users are provided just **one** attempt thereafter to login successfully (instead of the normal **three** attempts) or the 60 second lock counter starts again (trying to login before 60 seconds has elapsed counts as that **one** attempt, and so user has to wait an additional 60 seconds before trying to login again).

Email from Morgan (11 Apr 16) For all services we allow 5 login attempts then force a 60 sec lockout time then allow login attempts. This is to prevent bot's from rapidly attempting logins. This is not configurable

---

associated config files

A) httpd.conf file

/etc/apache
type cat httpd.conf

B) etc/apache/sites-enabled

type cat 000-httpd-default

- ➢ **type cat 000-httpd-default** (**note**: "000" is for the new browser, while "001" is for the classic interface browser)

- ➢ Refer to Salesforce Cases such as 116912 118079 and 218266 (excerpt below from 218266)

  Q Can you provide instructions on how to regain access for a locked account?
  ssh spadmin@kj05fd1i01
  Password:
  Account locked due to 38 failed logins

- ➢ MAY be related to using LDAP/Radius/Tacacs to connect to ssh, and the message is actually from their remote auth server (not from the SecureSync).
- ➢ Case 116457: we found SecureSync had a bad CF card.
- ➢ wtmp file may be full (reboot to delete)
- ➢ is browser still accessible?

After talking with Stuart (12 Dec 2019) after **three** failed SSH login attempts (or **Five** browser login failed attempts), a 60 second lock is asserted. Once this lock has been set, and after at least a full 60 second wait, users are given just one failed attempt (instead of the normal 3 for ssh, or 5 for browser) before another 60 second lock is placed again.

If another login attempt occurs before the full 60 second lock has elapsed, that allowed attempt is automatically failed, and so the user must wait at least another 60 seconds before attempting login again. After each failed login attempt, the failed login account counter is incremented.

He said this applies to both the SSH and web browser connections. So a failed ssh login with an account requires at least 60 seconds before using the same account to try logging into the browser.

In summary, if the wrong login password is initially issued three times (ssh) or five times (browser) make sure to wait at least 60 seconds before trying to login again, to prevent additional failed logins just due to trying to login too soon.

Other example responses we've sent in the past for this message

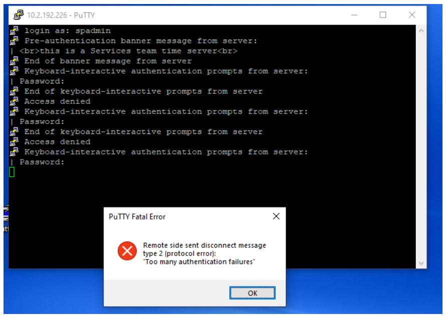
(Keith , Dec 2019 for 218266) I've seen this error message asserted for a couple different reasons.

Question: Are you trying to connect to the SecureSync using an account on a remote authentication server (LDAP, Radius or TACACS)? Or, are you trying to connect directly to the SecureSync. using an account created inside the SecureSync (such as the default spadmin account, or a user account which has been created in the SecureSync)?

This message typically indicates an account on a remote auth server (LDAP, Radius or TACACS) has been locked out due to incorrect credentials. if you haven't already, try logging into the SecureSync using the spadmin account and the associated spadmin password.

If you are not logging in using an account on a LDAP/Radius/Tacacs remote auth server (if you are instead logging in directly to an account on the SecureSync) this is not a "normal condition" to occur for ssh in the SecureSync (SecureSync normally drops the attempted connection after just three failed password attempts, and without locking the account, as shown in the screenshot below). But a remote auth server may allow more than just three failed login, and then may lock that account after "some number" of failed attempts.

So, this condition would only occur in the SecureSync with direct login, due to abnormal operation of the SecureSync. We've seen this condition previously caused once by the SecureSync needing to be rebooted (its wtmp directory was too full) and also once by the SecureSync's internal Compact Flash (CF) card starting to fail/needing to be replaced. Notice that rebooting a SecureSync having a CF card needing to be replaced can potentially prevent the SecureSync from being able to boot back-up thereafter, until its CF card has been replaced.



```
login as: spadmin
Pre-authentication banner message from server:
| <br>this is a Services team time server<br>
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
| Password:
```

PuTTY Fatal Error

Remote side sent disconnect message type 2 (protocol error): "Too many authentication failures"

Are you able to login to the web browser, using the same credentials that were being used to try connecting via SSH?

If you are trying to connect to ssh using a remote auth server, the user account will likely need to be unlocked in that remote server. But if you are logging in directly with a SecureSync account, reboot/power cycle the SecureSync and then try connecting again.

Please let us know this info helped you connect to the SecureSync! Thanks in advance!

(Dave L, Sept 2017 for 116457) This oz00pdmi11 Unit was replaced just two months ago so it is very new. There could be issues with the configuration like the DNS Server addresses were not entered or there are user accounts that need to be setup. It indicates the password you are using is incorrect. Please note the password is case sensitive.
Can you login as spadmin using the default password admin123?

(Dave L, Aug 2017 for 116457) Is the web UI accessible? This problem may be caused by a wtmp file becoming full. A reboot should fix the problem. Can you try a reboot and send the results?

(Morgan, April 2018 for 160169) Ae you trying to login in with the default account information (spadmin/admin123)? Did you give it 90 min. and try to login again? What happens if you do the "resetpw" command from the keypad? Let me know what happens.

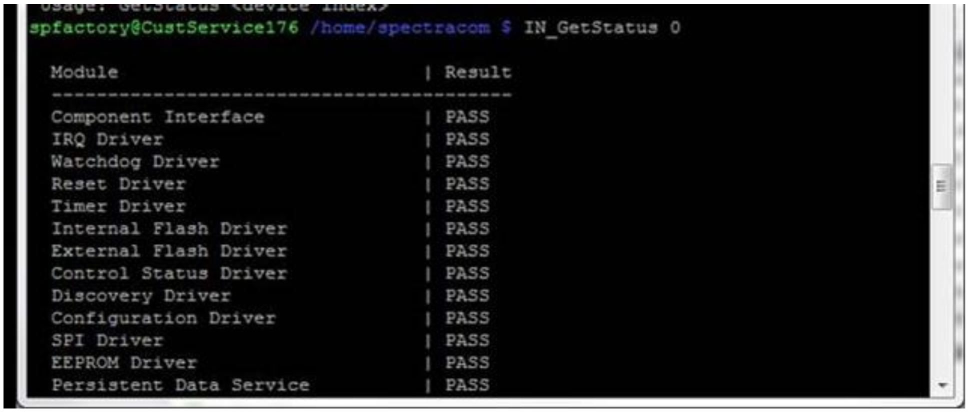
**Apache Web browser/general lock-up troubleshooting (error messages displayed/abnormal web browser operation, etc)

- Good document for troubleshooting web browser/ssh issues: https://www.linode.com/docs/troubleshooting/troubleshooting/

**Indications of KTS (Kramden Timing System) not running

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

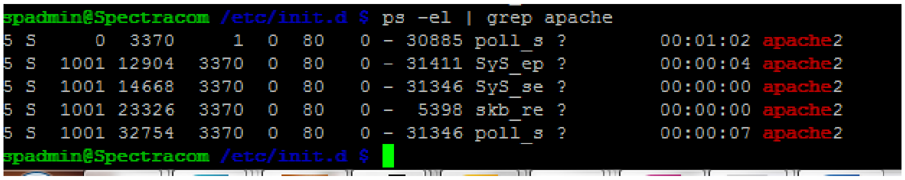
Note: Refer to the **IN_GetStatus 0** CLI command in the CLI section of this document to display a list of pass/fail state for KTS initialization (Example below). See if any items report FAIL. This command is available in the spadmin account.



```
Usage: GetStatus <device index>
spfactory@CustService176 /home/spectracom $ IN_GetStatus 0

  Module                                  | Result
  -----------------------------------------------
  Component Interface                     | PASS
  IRQ Driver                              | PASS
  Watchdog Driver                         | PASS
  Reset Driver                            | PASS
  Timer Driver                            | PASS
  Internal Flash Driver                   | PASS
  External Flash Driver                   | PASS
  Control Status Driver                   | PASS
  Discovery Driver                        | PASS
  Configuration Driver                    | PASS
  SPI Driver                              | PASS
  EEPROM Driver                           | PASS
  Persistent Data Service                 | PASS
```

Verifying if Apache web browser is actually running

To see if Apache is running, type **ps -el | grep *apache*** <enter> (where it will list everything with the name typed after “grep”):



```
spadmin@Spectracom /etc/init.d $ ps -el | grep apache
5 S     0  3370     1  0  80   0 - 30885 poll_s ?        00:01:02 apache2
5 S  1001 12904  3370  0  80   0 - 31411 SyS_ep ?        00:00:04 apache2
5 S  1001 14668  3370  0  80   0 - 31346 SyS_se ?        00:00:00 apache2
5 S  1001 23326  3370  0  80   0 -  5398 skb_re ?        00:00:00 apache2
5 S  1001 32754  3370  0  80   0 - 31346 poll_s ?        00:00:07 apache2
spadmin@Spectracom /etc/init.d $
```

Find out what web browser (and its version) they are using on the PC (such as IE11, Firefox, etc).

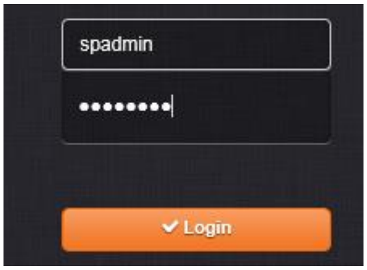
IE 11 and above require a valid HTTPS certificate (doesn’t allow you to accept an invalid certificate to proceed.

Per: https://answers.microsoft.com/en-us/windows/forum/windows_7-update/after-applying-3205394-ie11-version-is-listed-as/4a1dc892-8bcb-45f0-9390-418c81d753db?page=2

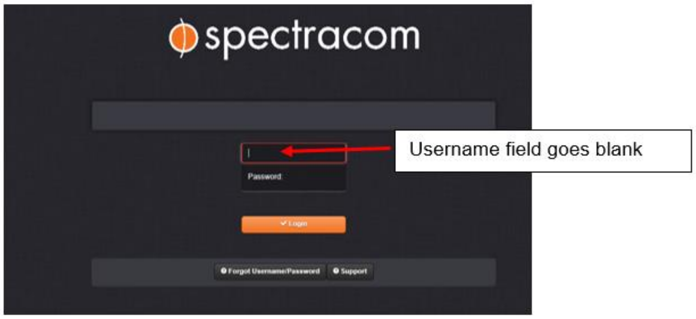
> My IE 11 lost ability to "Continue on..." when there is a certificate error. That option is usually between the "We recommend you close this page" and the "More information" line

A) **Can't login to JUST the newer black/charcoal browser (no error message displayed and username keeps disappearing with each login attempt) But if invalid credentials are entered, it indicates "invalid username or password"**

- ➢ CLI login is fine, and CAN login to the classic browser using HTTPS.



Entering valid login credentials and then after pressing login (username field goes blanks)"



Username field goes blank

1) **When logging in using "HTTPS" make sure HTTPS is enabled in Services (cli command servget 6 <enter> should respond HTTPS is enabled**

   - o If HTTPS is disabled, type: **servset 6 on** <enter>

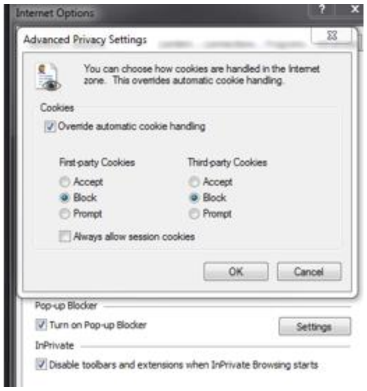
2) **This issue most likely due to "Cookies" being "blocked" or "disabled"**

- ➢ This condition will cause a certificate error to occur
- ➢ This condition is also discussed further below in this list of possible issues (CERTIFICATE ERRORS)

Haven't run across this one in a VERY long time. But its an even simpler explanation and also matches what you are observing. I just duplicated it with my IE11.

In IE, go to **Tools** -> **Internet Options.** Select the **Privacy** tab, and press **Advanced**

The **Advanced Privacy Settings** window which opens, make sure both the **First party** and **Third party** cookies are not "**blocked**". If I recall correctly, **I** think its only the first party cookies which matter (but configure them both the same,just in case). If the cookies are blocked, you won't be able to login, there won't be an error message displayed, and the username goes away each time.



Internet Options

Advanced Privacy Settings

You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

Cookies

☑ Override automatic cookie handling

First-party Cookies	Third-party Cookies
○ Accept	○ Accept
● Block	● Block
○ Prompt	○ Prompt

☐ Always allow session cookies

Pop-up Blocker

☑ Turn on Pop-up Blocker

InPrivate

☑ Disable toolbars and extensions when InPrivate Browsing starts

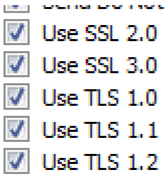
Or, if you select "**prompt**", but then don't allow the cookie requests while actually logging in, the same effect happens- there is no error message displayed and the username disappears each time.

3) **Could also potentially be due to the HTTPS certificate failing due to an incorrect "Common Name" ("Spectracom") in our default HTTPS certicate (need to change this value to the applicabe hostname or static IP Addres they use to login to the browser).**

   - IE Versions 10 and below (as well as IE 11, before v11.9600) allow a user to still accept an invalid certificate. IE 11.9600 and above (IE 11.0.49 does not exhibit this, but 11.9600 does) do not allow the ability to accept an invalid certificate (such as the default factory certificate) Refer to: https://blogs.msdn.microsoft.com/ieinternals/2013/12/12/continue-link-missing-from-certificate-error-page/.

4) **SSL/TLS selection**

- In IE, go to Tools -> Internet Options. Select the Advanced tab. Scroll down towards the bottom



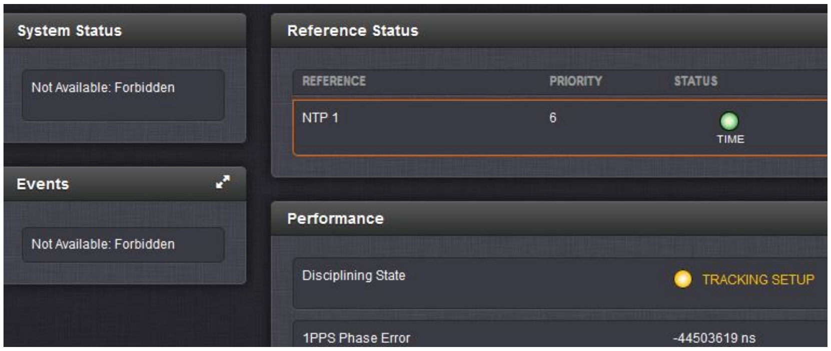
☑ Use SSL 2.0
☑ Use SSL 3.0
☑ Use TLS 1.0
☑ Use TLS 1.1
☑ Use TLS 1.2

- If HISEC (the "High Security" checkbox) is enabled in the time server, make sure "TLS 1.2" is enabled.

B) Error message of "Not Available: Forbidden" error message displayed in web browser

Symptom: "*Not Available: Forbidden*" error message is being displayed while trying to login to the newer (black/charcoal) web browser (login fails with "Not Available: Forbidden" displayed

This message indicates not currently logged into the browser (earlier login may have since timed-out)



System Status

Not Available: Forbidden

Reference Status

REFERENCE	PRIORITY	STATUS
NTP 1	6	● TIME

Events

Not Available: Forbidden

Performance

Disciplining State ● TRACKING SETUP

1PPS Phase Error -44503619 ns

Fix: refresh the browser page and login.

Note this message of “Forbidden” can indicate network access restriction has been configured. Try typing the CLI command of **unrestrict** if a reboot/power cycle does not restore access to the newer browser (with the error message no longer displayed).

C) Error code: ssl_error_no_cypher_overlap displayed when trying to connect.

- Verify the browser (IE, Firefox, Chrome) on the PC is up to date

Email from Harris (3 March 15): Brian, I loaded the 5.2.0 software and now my Firefox browser won’t connect to the webpage. My firefox version is 13.0.1. the page message is:
Secure Connection Failed
An error occurred during a connection to 10.128.13.97.
Cannot communicate securely with peer: **no common encryption algorithm(s)**.
(Error code: ssl_error_no_cypher_overlap)
The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
Please contact the website owners to inform them of this problem. Alternatively, use the command found in the help menu to report this broken site.

Keith’s finding: Firefox 13 was release in 2013. I recommended updating Firefox to a much newer version.

D) Apache Web browser no longer accessible (can’t even get to login prompt), but ping, telnet, SSH still work

5) Versions 5.0.0 and above

- Connection refused” may be displayed
- CF card may be full,
  - Perform a **df -h** CLI command to check disk usage.
  - Can’t delete logs in earlier versions such as with v5.0.2, but deleting any update files that may be present and also running the cleaner patch (uploading the cleaner file via FTP upload of the cleaner file and then using the **sysupgrade cli** command) may help.

Email Keith sent to Mark Day (1 Apr 15 for his customer JPMC. We have reviewed the SecureSync logs that you provided us with. Based on these logs entries and also due to the CLI interface operating normally, we suspect this condition you are observing with the web browser not connecting is related to either the unit’s configuration or the Apache web browser.

The logs don’t show an immediate indication of why you aren’t able to connect to the web browser. We would like to request from you a copy of the SecureSync’s configuration files, if possible, to correlate with the logs. And if it this is feasible, our engineers being able to remotely connect to the SecureSync (or being able to “remote desktop” into a PC on the same network) would also likely be very helpful. However, if this isn’t possible for security reasons, we completely understand.

Can you perform a few steps for us that will likely help with the diagnosis of this condition?

E) Invalid / undesired IP address or subnet value may have been entered in the Access Control table

- Try performing an **unrestrict** <enter> cli command

  Note: this command not available via the front panel)

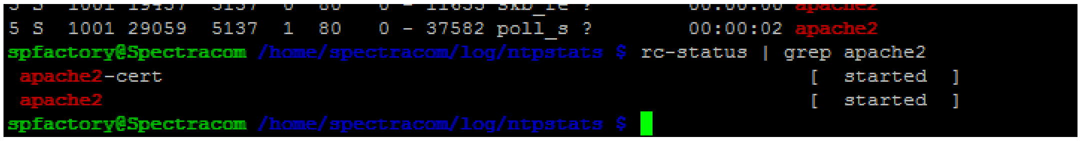
A. With an FTP connection to the SecureSync:

- The unit’s config files are located in the /home/spectracom/config directory. Can you FTP and bundle these config files into a single bundle file and then send them to us?

B. With a telnet or ssh connection to the SecureSync:

1. Type **rc-status** <enter> and send us a screenshot of the response. (**rc-status | grep apache**)

   Note: look to see if any services are unexpectedly "crashed" or stopped

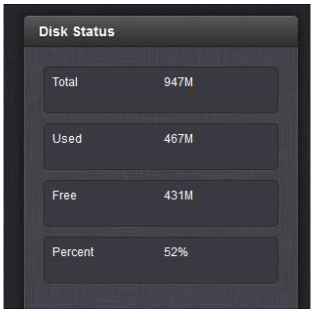


```
5 S  1001 19437  5137  0  80   0 - 11033 skb_re ?        00:00:00 apache2
5 S  1001 29059  5137  1  80   0 - 37582 poll_s ?        00:00:02 apache2
spfactory@Spectracom /home/spectracom/log/ntpstats $ rc-status | grep apache2
 apache2-cert                                                    [  started  ]
 apache2                                                         [  started  ]
spfactory@Spectracom /home/spectracom/log/ntpstats $
```

2. Type **ps -elf**<enter> and send us a screenshot of the response. (**ps –el | grep apache**)
3. Type **df -h** <enter> and send us a screenshot of the response

   Note: CF card usage is now reported in the browser (alleviating need to have to use CLI command)

   Tools -> **Upgrade/Backup** page of the browser (under "**Disk Status**")



Disk Status

Total	947M
Used	467M
Free	431M
Percent	52%

4. Type **servget 6** <enter>. Verify the response indicates **HTTPS Service** is **Enabled**
5. Type **servget 5** <enter>. See if the response indicates **HTTP Service** is Enabled or Disabled.
6. If **servget 5** (referenced in the step above) indicated **HTTP** is currently **Disabled**, type **servset 5 on** <enter> to enable HTTP.
7. Type **servset 6 off** <enter> to disable HTTPS.
8. Try connecting to the web browser with "**HTTP://**" in front of the address (instead of using "https")
9. Type **servset 6 on** <enter> to enable HTTPS.
10. Try logging into the browser with "**HTTPS://**" in front of the address.
11. Type **unrestrict** <enter> to clear the network access restriction table (may have inadvertently entered a value in this table that locked out the address of the PC, the subnet or all network IP addresses).
12. Try logging into the browser again with "HTTPS://" in front of the address.
13. Type **defcert** <enter> to reset the HTTPS certificate (note there won't be a response to this command).
    - The only CLI command assocated with certificates is the **defcert** command (to reset the certificate back to default)
14. Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
    - Example syntax is **defcert -sha256**
15. V5.6.0 also changed the default algoritm to SHA256 for better security. IE8 and below do not support SHA-256 (use **defcert -sha1** to regenerate a new certitficate using SHA1 to gain access).
16. Try logging into the browser again with "**HTTPS://**" in front of the address.

F) Neither Apache or telnet/ssh now available.

- See if can connect via RS-232 Serial port on the front of the unit.
- Try connecting to browser/telnet again after rebooting
  - If it can connect after power cycling, get both the log and config bundles to review. Check the kern log and System log. See if there are any “out of memory” entries in the System log. (Refer to the System.log for more info on this condition)

G) HTTPS certificate somehow corrupt

- Try performing a **defcert** <enter> cli command (as of at least v5.3.0, this command not available via the front panel)
  - Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
  - Example syntax is **defcert -sha256**
  - V5.6.0 also changed the default algoritm to SHA256 for better security. IE8 and below do not support SHA-256 (use **defcert -sha1** to regenerate a new certitficate using SHA1 to gain access).

H) Memory leak in software versions 4.8.9 and below

- Versions 4.8.9 and below have a memory leak occurring when the units have been up for an extended amount of time. There isn’t enough free memory available to run Apache.
- With a Telnet or SSH session, perform/capture the results of a “**free -m**” command to verify the free memory is less than about 100MB (about the minimum for Apache to be able to run).

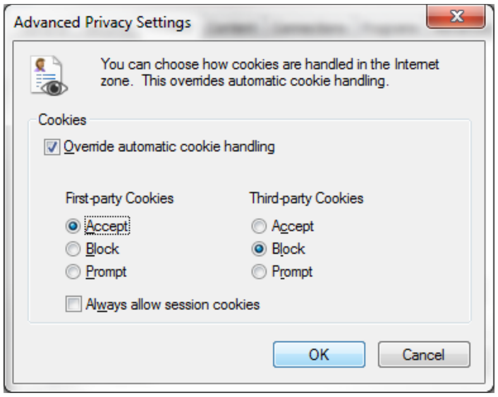
Note (status update): this issue was fixed with the version 5.0.0 (and above) updates.

I) “Certificate Error” reported. Verify “first-party Cookies” aren’t blocked

- Refer to: https://kb.iu.edu/d/ajfi

If cookies are blocked/disabled, the login page will report “**certificate error**” near the IP address and will just keep clearing the login name (won’t allow access to the browser).

1. Internet Explorer: Enable “First party Cookies” in Tools -> Internet Options, Privacy tab, Advanced button:



Advanced Privacy Settings

You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

Cookies

☑ Override automatic cookie handling

First-party Cookies	Third-party Cookies
● Accept	○ Accept
○ Block	● Block
○ Prompt	○ Prompt

□ Always allow session cookies

2. FireFox

- Enable “First party Cookies” in Tools -> Options, Privacy tab, History drop-down

- To allow sites to set cookies on your computer, select Accept cookies from sites. To specify which sites are always or never allowed to use cookies, click Exceptions.
- To view or remove individual cookies, click "remove individual cookies"

J) Web browser very sluggish/not available

Possible reasons:

1) LDAP and/or Radius Enabled, servers configured- but not accessible.
2) If one or more LDAP or Radius servers are configured but not available (such as using a direct connect for instance), the login will be delayed while the time server tries to establish comms with each one. The timeout and number of retries for each server will primarily determine how long it will take to login locally. Local login doesn't occur until all configured Radius and/or LDAP servers have been contacted and timed-out.
3) KTS stopped running- is the front panel time still incrementing?
4) Bad ETX module.
5) Memory leak in versions 4.8.9 and below (if CLI is still available, type version <enter>) More on this further below.
6) Lots of processes on the "outer processor" (ETX module) such as NTP, multiple SNMP connections, several simultaneous web browser connections, etc.

K) "ERROR: The web server encountered an unexpected error and failed to display the page you requested.

This error message may be displayed if the SecureSync isn't available yet. Also, deleting "cgi-bin/StatusConfig.cgi" after the SecureSyncs IP address/DNS name in the web browser address field (leaving just https:// and the address) may also help.

Using Chrome
(Refer to case 6452) Mark Dion reported that in Chrome, each time he selects a main menu, it keeps taking him back to the login screen. I spoke to Paul Myers and he recommended he make sure that screen/page caching is not enabled. It should be configured for refresh on each new page/screen.

Regarding the condition you reported when accessing the SecureSync using Chrome, I wanted to let you know I had a moment to discuss this condition with one of our engineers.

He mentioned that he hasn't ever seen or heard of anyone else seeing this abnormal web browser operation. He said it sounds like your browser may be currently configured to cache pages/screens. It is recommended that whichever browser is used to access the SecureSync (IE, Firefox or Chrome), that the browser be configured with no page caching. It should instead be configured with "refresh with each new page" (I'm not sure where this setting is in Chrome).

Please let me know either way, if you had screen/page caching enabled in Chrome, and if turning it off resolved this issue. OR, if you have any other questions or of you need anything else from us (now or in the future), please don't hesitate to let me know!

L) Web browser failing after login (due to memory leak in 4.8.9 and below)

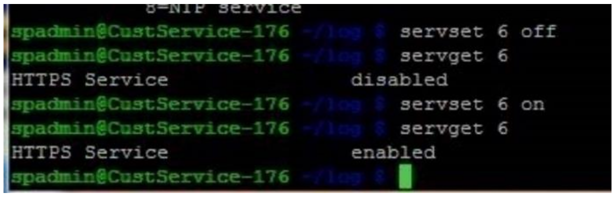
- Use **df -h** cli command to verify CF card isn't too full

If you can connect/login to the CLI interface (via ssh or telnet, or via a serial cable connected to the DB9 port on the front of the unit), there are a couple of commands to issue.

After logging in, first perform a **defcert** <enter> command (as shown below). Then try logging in again via the browser (can keep the connection to the CLI open). This command resets the HTTPS certificate.

- Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
- Example syntax is **defcert -sha256**
- V5.6.0 also changed the default algoritm to SHA256 for better security. IE8 and below do not support SHA-256 (use **defcert -sha1** to regenerate a new certitficate using SHA1 to gain access).

If defcert doesn't restore access to the browser, perform a **servset 6 off** <enter> command followed by **servset 6 on** <enter> (as shown below). Note the two servget commands in the screenshot are optional). This will restart just the web browser service alone.



```
           8=NTP Service
spadmin@CustService-176 ~/log $ servset 6 off
spadmin@CustService-176 ~/log $ servget 6
HTTPS Service                  disabled
spadmin@CustService-176 ~/log $ servset 6 on
spadmin@CustService-176 ~/log $ servget 6
HTTPS Service                  enabled
spadmin@CustService-176 ~/log $ 
```

Please let me know if either of these commands restore access to the browser!!! Thanks!

****REST API interface/Postman (alternate to using the standard web browser or CLI)

- REST API Postman collection on our website: https://www.orolia.com/document/securesync-netclock-9400-rest-api-collection-and-documentation/

- Refer also to documents (such as API guide) in: \\rocfnp02\idrive\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

Blog by Ron Dries ("The REST API: A Powerful Interface for Remote Control of PNT Devices")

- https://spectracom.com/resources/blog/ron-dries/2018/rest-api-powerful-interface-remote-control-pnt-devices

Monitoring and managing PNT devices that can be spread across the globe can be challenging. It is also necessary to ensure the devices are configured and running properly. In certain applications, there could also be the need to schedule a task or automate some functionality of a PNT device.

The built-in web GUI (Graphical User Interface) in Orolia products, such as the SecureSync and VersaSync, is designed to quickly and easily show status and provide configuration settings for users to manage their devices. It does, however, require the user to manually log in to the device and navigate to the desired web pages. This is not always practical and can be time consuming if multiple devices need to be monitored and managed at the same time.

But, by utilizing the built-in **REST (Representational State Transfer)** API, any functionality that can be done manually through the web GUI can also be scripted, allowing for machine-to-machine communication and control. The REST API utilizes JSON (JavaScript Object Notation) formatted data for sending commands and receiving status information from the devices.

One example of a task that can be simplified and automated using the REST API is downloading log and configuration bundles. The log and configuration bundles are important files to retrieve from a PNT device for troubleshooting issues or to determine how a PNT device has been running over time. Configuration bundles are also necessary to control the configuration of a PNT device, as well as to quickly configure multiple devices with the same configuration.

The REST API can simplify this task by automatically creating a script to go out to specified Orolia PNT devices and then saving the log and configuration bundles to a PC. This removes the need to manually log in to each device and download both files. Also, this process can be scheduled to download the configuration bundle periodically, which can be useful for controlling the configuration.

Monitoring applications, like Nagios, can utilize python scripts using the REST API to create custom queries to pull the exact information from the device that they are interested in monitoring. After this status information is retrieved, a quick health report of the device can be shown in the tool. The REST API makes integration into existing monitoring tools easier.

The REST API is a powerful interface that can allow for more advanced remote control of PNT devices, and it can be utilized in a variety of different applications.

REST API/Postman documentation

- Here is a link to what we have for the REST API documentation in SecureSync. https://www.orolia.com/document/securesync-netclock-9400-rest-api-collection-and-documentation/

- REST API /Postman collection on our website: REST API /Postman collection on our website: https://www.orolia.com/document/securesync-netclock-9400-rest-api-collection-and-documentation/

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 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.

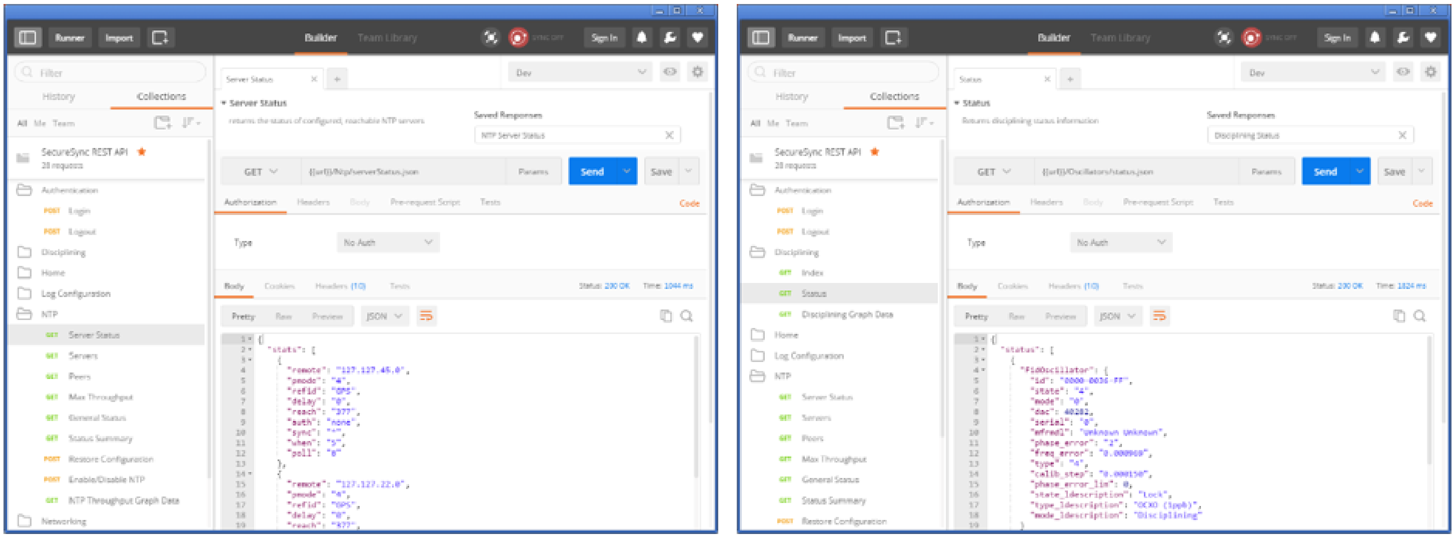
To perform these HTTP operations, it is necessary to know the data format required to retrieve and send data to SecureSync. Spectracom's Postman™1 collection is a compilation of frequently used operations which may serve as examples of how to pull and send data through the SecureSync API.

Representational state transfer (**REST**) is an architectural style consisting of a coordinated set of architectural constraints applied to components, connectors, and data elements, within a distributed hypermedia system. REST ignores the details of component implementation and protocol syntax in order to focus on the roles of components, the constraints upon their interaction with other components, and their interpretation of significant data elements.[1][2]

OROLIA PROPRIETARY – COMPETITION SENSITIVE

REST API

Documented/Delivered as Postman Collection



Server Status

returns the status of configured, reachable NTP servers

GET {{url}}/ntp/serverStatus.json

Type: No Auth

Status: 200 OK Time: 1044 ms

```
{
  "stats": [
    {
      "remote": "127.127.46.0",
      "pmode": "4",
      "refid": "GPS",
      "delay": "0",
      "reach": "377",
      "auth": "none",
      "sync": "*",
      "when": "5",
      "poll": "8"
    },
    {
      "remote": "127.127.22.0",
      "pmode": "4",
      "refid": "GPS",
      "delay": "0",
      "reach": "377",
```

Status

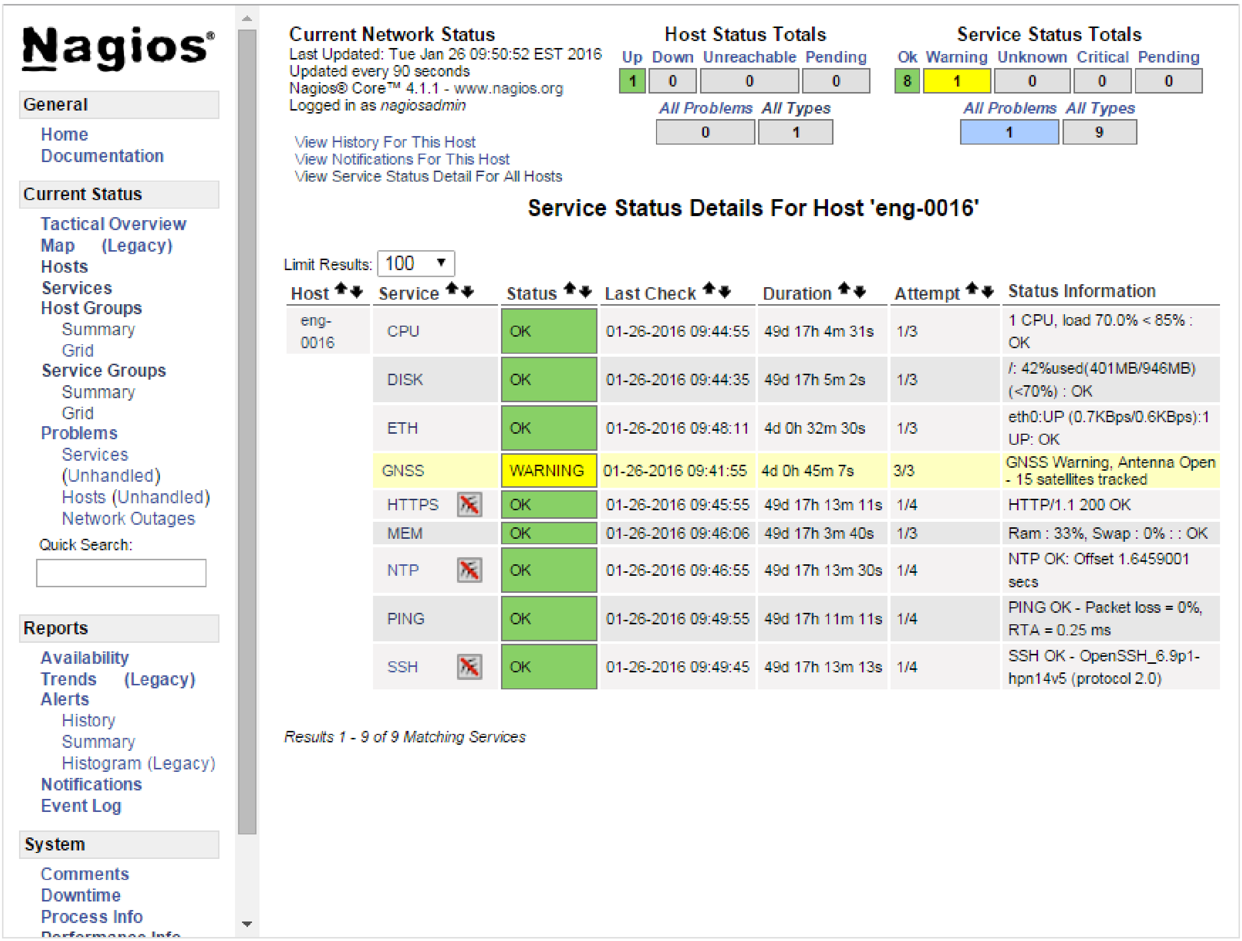
Returns disciplining status information

GET {{url}}/Oscillators/status.json

Type: No Auth

Status: 200 OK Time: 1824 ms

```
{
  "status": [
    {
      "FidOscillator": {
        "id": "0000-0036-FF",
        "state": "4",
        "mode": "0",
        "dac": 40282,
        "serial": "0",
        "mfrmdl": "Unknown Unknown",
        "phase_error": "2",
        "freq_error": "0.000969",
        "type": "4",
        "calib_step": "0.000150",
        "phase_error_lim": 0,
        "state_ldescription": "Lock",
        "type_ldescription": "OCXO (1ppb)",
        "mode_ldescription": "Disciplining"
      }
```



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*

View History For This Host
View Notifications For This Host
View Service Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

All Problems	*All Types*
0	1

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
8	1	0	0	0

All Problems	*All Types*
1	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

- All versions of 2400 SecureSync support REST API

General info about REST API

The graphical Web User Interface ("Web UI") used with Spectracom's SecureSync 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**” futher 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 tutororial: 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**)

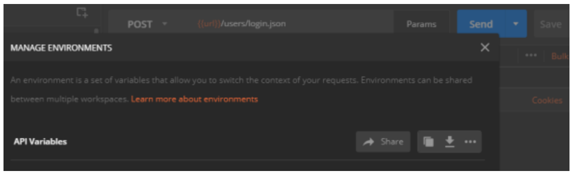
“To run the script, issue at the Windows command prompt the following command on a PC that has python installed (https://www.python.org/downloads/release/python-352/).

```
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 fiile 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 “A**PI Variables.postman_envirnmment.json**” file. “**API Variabes**” will be displayed in the middle and top-right side of the page (as shown below).

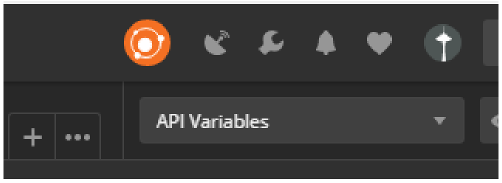


POST {{url}}/users/login.json

MANAGE ENVIRONMENTS

An environment is a set of variables that allow you to switch the context of your requests. Environments can be shared between multiple workspaces. Learn more about environments

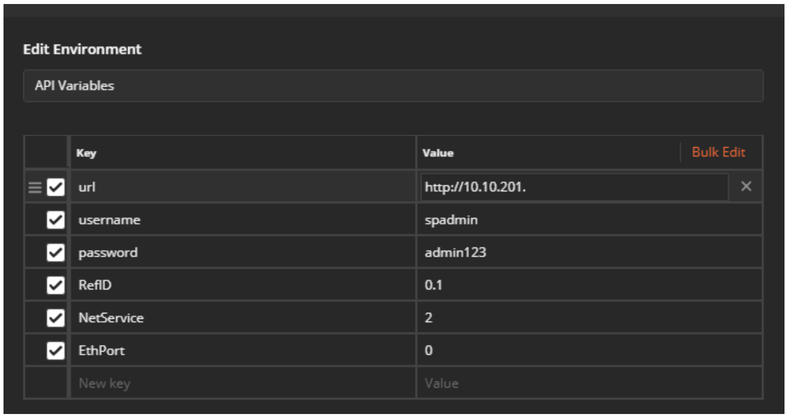
API Variables



API Variables

3. In the Environment drop-down menu (next to the EYE button), select Dev to load the environment imported above.
4. Click the **EYE** button to see which environment variables have been loaded with this environment file: One variable is called **url**, another one is **spadmin**, etc.

   Click edit to change any/all the values (such as the URL of the desired SecureSync). Then click “**Update**”.

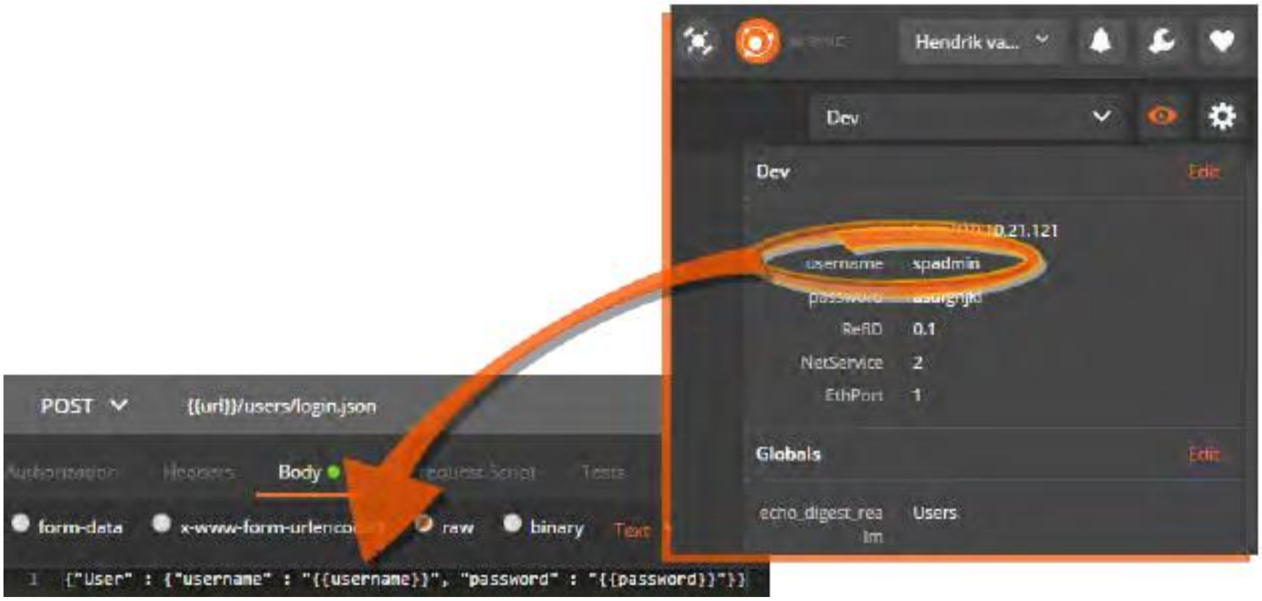


Edit Environment

API Variables

	Key	Value
☑	url	http://10.10.201.
☑	username	spadmin
☑	password	admin123
☑	RefID	0.1
☑	NetService	2
☑	EthPort	0
	New key	Value

To use a development variable, apply two curly brackets in the body code:



Dev

url	10.10.21.121
username	spadmin
password	asdfghjkl
RefID	0.1
NetService	2
EthPort	1

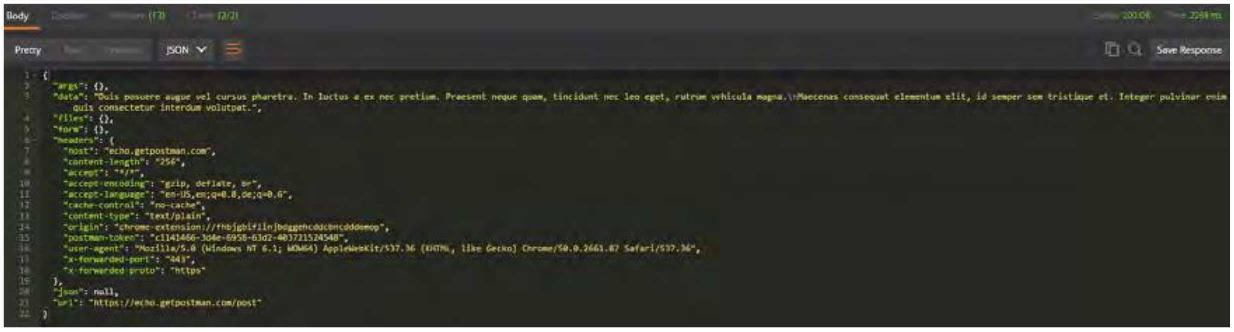
Globals

echo_digest_realm	Users

POST {{url}}/users/login.json

```
{"User" : {"username" : "{{username}}", "password" : "{{password}}"}}
```

To test, click the blue **Send** button (top-right corner of the page). The coding window will display the requested code:



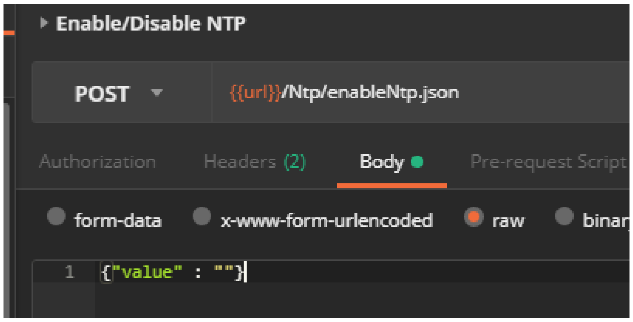
```
{
  "args": {},
  "data": "Duis posuere augue vel cursus pharetra. In luctus a ex nec pretium. Praesent neque quam, tincidunt nec leo eget, rutrum vehicula magna.\nMaecenas consequat elementum elit, id semper sem tristique et. Integer pulvinar enim
    quis consectetur interdum volutpat.",
  "files": {},
  "form": {},
  "headers": {
    "host": "echo.getpostman.com",
    "content-length": "256",
    "accept": "*/*",
    "accept-encoding": "gzip, deflate, br",
    "accept-language": "en-US,en;q=0.8,de;q=0.6",
    "cache-control": "no-cache",
    "content-type": "text/plain",
    "origin": "chrome-extension://fhbjgbiflinjbdggehcddcbncdddomop",
    "postman-token": "c1141466-3d4e-6958-63d2-403721524548",
    "user-agent": "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.87 Safari/537.36",
    "x-forwarded-port": "443",
    "x-forwarded-proto": "https"
  },
  "json": null,
  "url": "https://echo.getpostman.com/post"
}
```

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</spa**”
- 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 tehe 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).



{{url}}/Ntp/enableNtp.json

```
{"value" : ""}
```

Logout of the 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 also to**: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API and Python scripts\Python scripts

A) Input Reference Priority table

1. **Enabling/disabling References (Difference between 1200s and 2400s)**

   - Refer to Salesforce Case 284997

   Report: “We have a problem controlling the 2400 via REST API in that we cannot disable and or enable a given Reference. The same REST api python code that works with the 1200 unit fails to change anything on the 2400.”

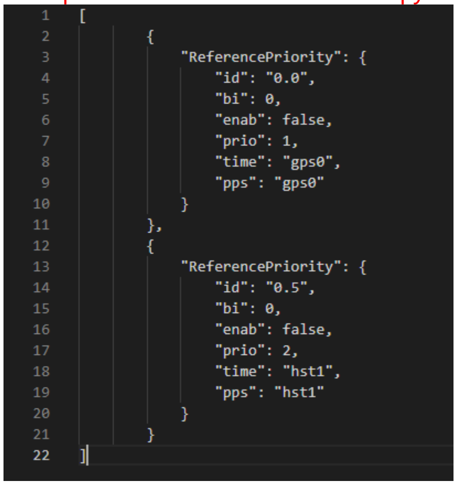
   Keiths response based on reply from Ron Dries (27 May 2022) Working with one of our Apps Engineers, he was able to duplicate your observation, as well. Directly below is the info he has provided:

   What I found was that the SecureSync 2400 needs to have the whole Reference Priority table sent back to the Configure References endpoint, even to enable disable a single reference.

   I was able to get it to work by querying the current Reference Priority table with the Get Reference Configuration request, copying the returned JSON array of the Reference Priority table, and using that exact JSON array in the Configure References request.

   The steps I took were:

   1) I issued the GET request to the {{host}}/References/edit.json, and copied the Reference Priority table returned from this call.
   2) When I copied the JSON reference priority I just copied the portion that was in “[“ brackets, removing the “data” : . for example the below is what I would copy from the return of the GET request removing any extra data:



```
[
        {
            "ReferencePriority": {
                "id": "0.0",
                "bi": 0,
                "enab": false,
                "prio": 1,
                "time": "gps0",
                "pps": "gps0"
            }
        },
        {
            "ReferencePriority": {
                "id": "0.5",
                "bi": 0,
                "enab": false,
                "prio": 2,
                "time": "hst1",
                "pps": "hst1"
            }
        }
]
```

   3) Once I had the copied Reference Priority table from the GET Request, I added this into the Body of the POST configuration request.

   4) Then to disable a reference the “enab” variable can be set to false.

B) 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.

C) 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

1. 500 web UI error

- **Fixed in Version 5.7.0** [JIRA ticket SSS-262] – "500 web UI error 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 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.

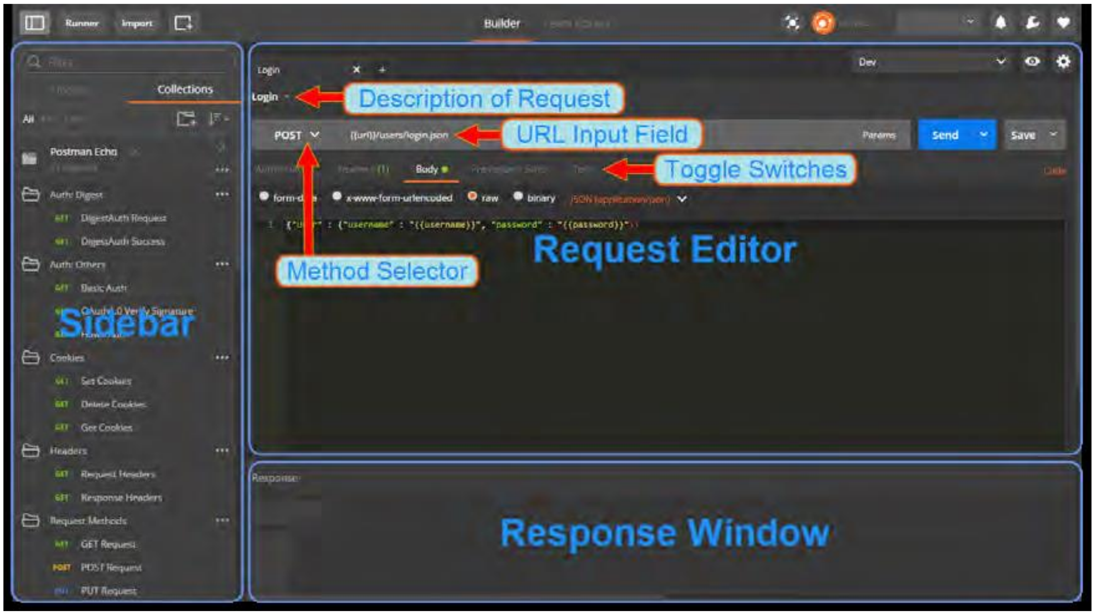
Downloading and Installing the Postman™ Chrome™ App

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 Post man.
5. Create an account by signing up. This will ensure your requests, collections, envir onments 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 sub mitted 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.

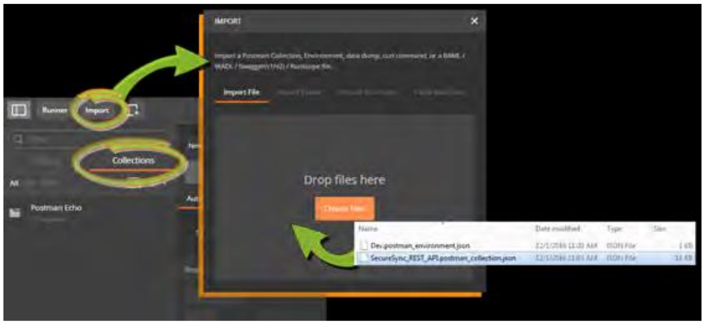
To import this collection:

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.

b. 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.

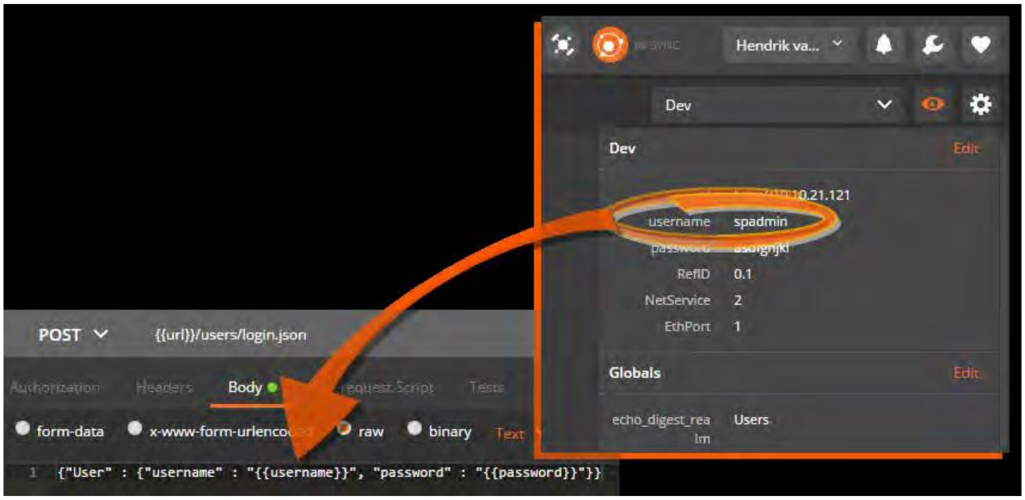
Importing the DEV Environment

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 Developer Kit files, and select the file `Dev.postman_environment.json`.
3. In the Environment drop-down menu (next to the EYE button), select Dev to load the envir onment imported above.
4. Click the EYE button to see which environment variables have been loaded with this envir onment file: One variable is called url, another one is spadmin, etc.

To use a development variable, apply two curly brackets in the body code:



Dev

POST {{url}}/users/login.json

Dev

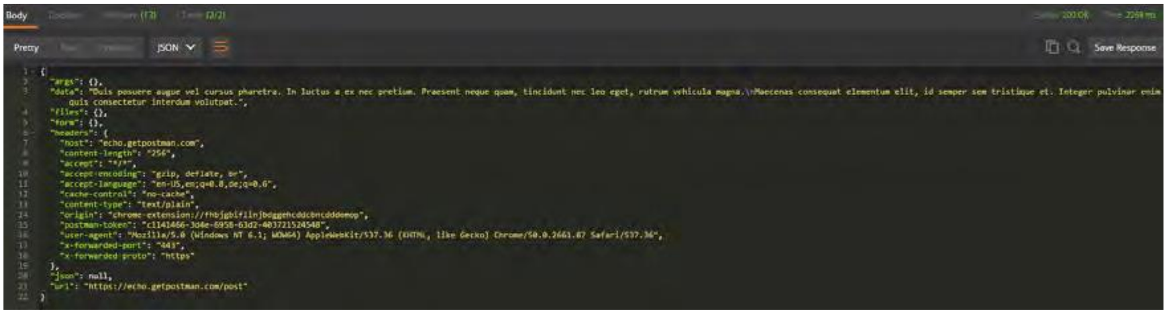
url	http://10.21.121
username	spadmin
password	asdfghjkl
RefID	0.1
NetService	2
EthPort	1

Globals

echo_digest_realm	Users

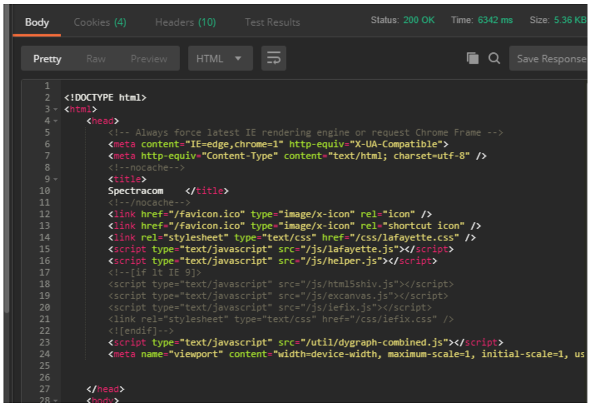
```
{"User" : {"username" : "{{username}}", "password" : "{{password}}"}}
```

To test, click the blue Send button. The coding window will display the requested code:



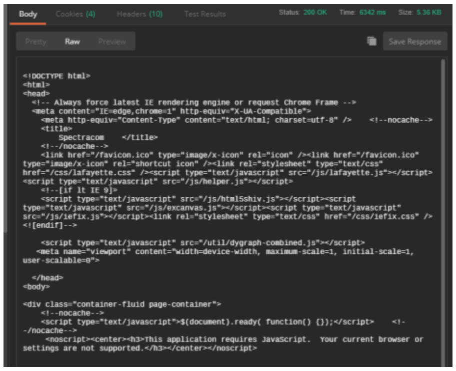
```
{
  "args": {},
  "data": "Duis posuere augue vel cursus pharetra. In luctus a ex nec pretium. Praesent neque quam, tincidunt nec leo eget, rutrum vehicula magna.\nMaecenas consequat elementum elit, id semper sem tristique et. Integer pulvinar enim
      quis consectetur interdum volutpat.",
  "files": {},
  "form": {},
  "headers": {
    "host": "echo.getpostman.com",
    "content-length": "256",
    "accept": "*/*",
    "accept-encoding": "gzip, deflate, br",
    "accept-language": "en-US,en;q=0.8,de;q=0.6",
    "cache-control": "no-cache",
    "content-type": "text/plain",
    "origin": "chrome-extension://fhbjgbiflinjbdggehcddcbncdddomop",
    "postman-token": "c1141466-3d4e-6958-63d2-403721524548",
    "user-agent": "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.87 Safari/537.36",
    "x-forwarded-port": "443",
    "x-forwarded-proto": "https"
  },
  "json": null,
  "url": "https://echo.getpostman.com/post"
}
```

Pretty tab



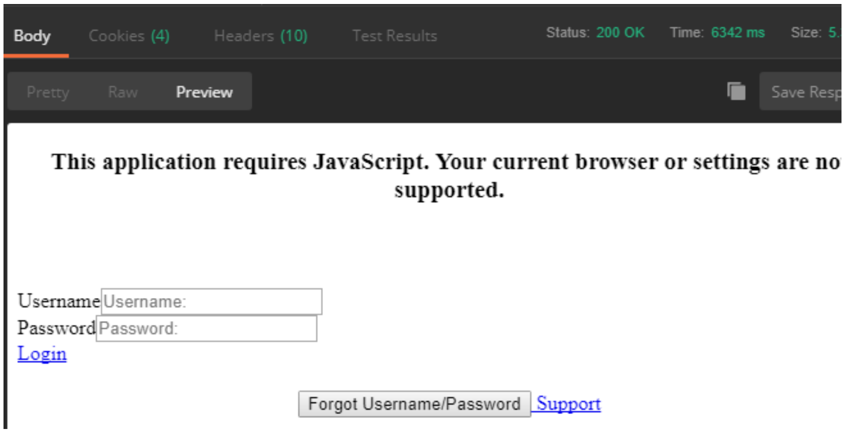
```

<!DOCTYPE html>
<html>
    <head>
        <!-- Always force latest IE rendering engine or request Chrome Frame -->
        <meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible">
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        <!--nocache-->
        <title>
        Spectracom    </title>
        <!--/nocache-->
        <link href="/favicon.ico" type="image/x-icon" rel="icon" />
        <link href="/favicon.ico" type="image/x-icon" rel="shortcut icon" />
        <link rel="stylesheet" type="text/css" href="/css/lafayette.css" />
        <script type="text/javascript" src="/js/lafayette.js"></script>
        <script type="text/javascript" src="/js/helper.js"></script>
        <!--[if lt IE 9]>
        <script type="text/javascript" src="/js/html5shiv.js"></script>
        <script type="text/javascript" src="/js/excanvas.js"></script>
        <script type="text/javascript" src="/js/iefix.js"></script>
        <link rel="stylesheet" type="text/css" href="/css/iefix.css" />
        <![endif]-->
        <script type="text/javascript" src="/util/dygraph-combined.js"></script>
        <meta name="viewport" content="width=device-width, maximum-scale=1, initial-scale=1, us


    </head>
    <body>
```

Raw tab



```
<!DOCTYPE html>
<html>
<head>
  <!-- Always force latest IE rendering engine or request Chrome Frame -->
  <meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible">
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />    <!--nocache-->
    <title>
        Spectracom    </title>
    <!--/nocache-->
    <link href="/favicon.ico" type="image/x-icon" rel="icon" /><link href="/favicon.ico"
type="image/x-icon" rel="shortcut icon" /><link rel="stylesheet" type="text/css"
href="/css/lafayette.css" /><script type="text/javascript" src="/js/lafayette.js"></script>
<script type="text/javascript" src="/js/helper.js"></script>
    <!--[if lt IE 9]>
    <script type="text/javascript" src="/js/html5shiv.js"></script><script
type="text/javascript" src="/js/excanvas.js"></script><script type="text/javascript"
src="/js/iefix.js"></script><link rel="stylesheet" type="text/css" href="/css/iefix.css" />
<![endif]-->

    <script type="text/javascript" src="/util/dygraph-combined.js"></script>
   <meta name="viewport" content="width=device-width, maximum-scale=1, initial-scale=1,
user-scalable=0">

  </head>
<body>

<div class="container-fluid page-container">
    <!--nocache-->
    <script type="text/javascript">$(document).ready( function() {});</script>    <!-
-/nocache-->
     <noscript><center><h3>This application requires JavaScript.  Your current browser or
settings are not supported.</h3></center></noscript>
```

Preview tab



This application requires JavaScript. Your current browser or settings are no supported.

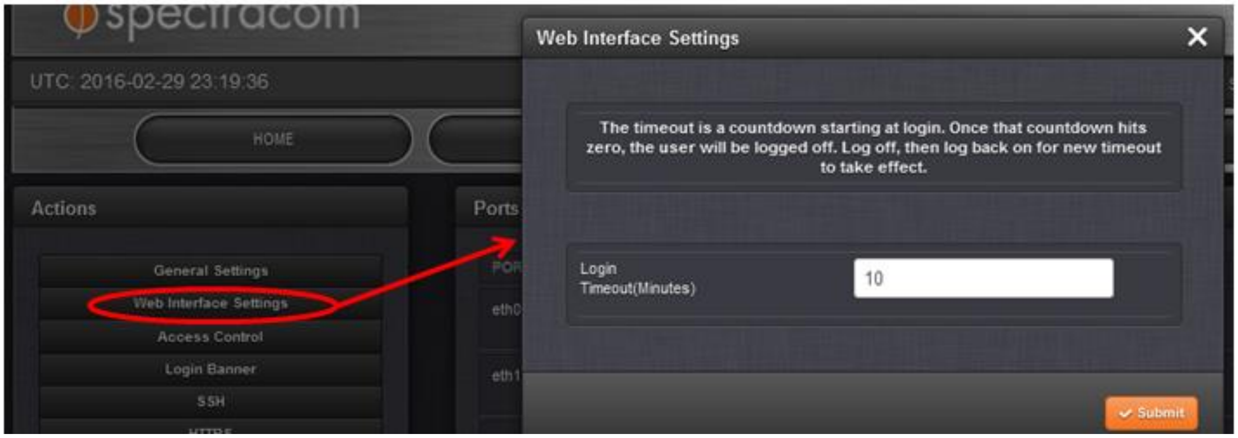
- GET: **Whenever a user accesses a page, the View component issues a GET** request to the Controller, since the user ultimately wants to retrieve (or: GET) the data that is displayed on the loadedpage.
- SET/POST: If, however, a user wants to add or configure a setting, the View component will issue 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

****web browser Idle login timeout (login time-out after no activity)

A) newer (black/charcoal) web browser

1. Versions 5.4.0 and above (newer browser)

- Update version 5.4.0 added configurable time-out (and consistent timeout of the browser)
- Click “Web interface Settings” on the left side of the Management -> Network page
- Configured in “Minutes”
- Available timeout range is from **10 minutes to 1440 minutes** (24 hours)
- A change to the time-out period doesn’t take effect until the NEXT login (not while already logged-in)



Web Interface Settings

The timeout is a countdown starting at login. Once that countdown hits zero, the user will be logged off. Log off, then log back on for new timeout to take effect.

Login Timeout(Minutes): 10

Apache Web Server in SecureSync

- SecureSync (like NetClock 9300s/9200s) also uses the Apache web server.

A) Obtaining Apache version info

1. Obtaining Apache version based on SecureSync software version installed

- Refer to the "Software Release Date" spreadsheet at : I:\Customer Service\PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates

2. Obtaining Apache version via CLI command (telnet, ssh or RS-232)

- Version can be queried via the CLI (refer to Specific available CLI commands/API calls)
- The command to get the Apache version is: version web <enter> (not "version apache").

3. Obtaining Apache version via the web browser

- Software versions 5.1.7 and below:
  - The Apache version isn't displayed in the web browser.
  - Obtain it via the CLI interface, instead.
  - web browser: The Apache version is reported in the Tools -> Upgrade/Backup page

Web Server Vendor / Version Disclosure (Customer request to "hide" the Apache version, to prevent potential security vulnerability)

Summary of the info below: A customer requested the Apache version no longer be reported. Knowing the version installed could disclose potential vulnerabilities.

Vulnerability Explanation
A typical web server response contains an HTTP Server header that reveals both the vendor and the version of the web server software. Additionally, third parties may inject headers disclosing supported software such as PHP or ASP. This information can lead an attacker to more focused attacks.

Remediation - NTP not a windows box, will need to ask spectrum
Sequris Group recommends that SRPMIC scrub the response headers before they are returned to the user. Microsoft has released a utility (URLScan) that helps modify headers before being sent to the requesting client. Please see the following URL for additional details: http://www.iis.net/downloads/microsoft/urlscan

Or

Can Spectracom edit the host file or related file on the Spectracom device to change or hide vendor information?

Email from Paul Myers (6 Mar 17) regarding SecureSyncs/9400s (at least 5.5.1 and below) In regards to hiding the Apache web server version information, we are reviewing this security recommendation internally with the Product Manager to see if we can fix this via Apache configuration in a future release.

Apache Web browser page refresh

SQLite database (Lafayette file) and DB browser program

Available SQLite database browser program

- browser program available for SQLite: "**dB browser for SQLite**" http://sqlitebrowser.org

Lafayette File (sqlite database)

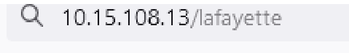
Availably of Lafayette file in the log bundles

Note: sqlite database (lfayette) is not available in log bundles in versions prior to 1.4.1

- Per version 1.4.1 update release notes "Added statistics database to log bundles"

Temporary work-around to manually Save (export) the SQLlite database (per JIRA CAR-1231) (versions prior to 1.4.1)

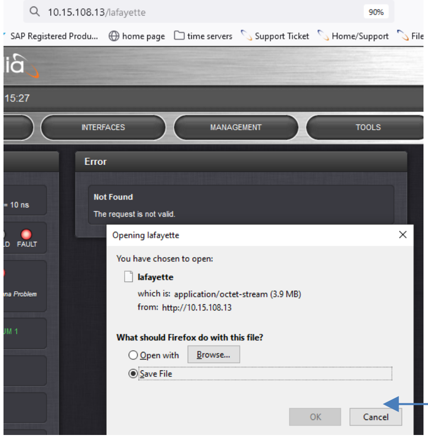
- The lafayette db file can be downloaded by navigating to **Error! Hyperlink reference not valid.** (example below)



10.15.108.13/lafayette

Chrome/Edge vs Firefox

Note this doesnt work on at least certain version of **Chrome** or **Edge** ("*I have tried Chrome and Edge and neither one of them allows you to save as a file"*). I tested it with Firefox and it worked.



Error

Not Found

The request is not valid.

Opening lafayette

You have chosen to open:

lafayette

which is: application/octet-stream (3.9 MB)

from: http://10.15.108.13

What should Firefox do with this file?

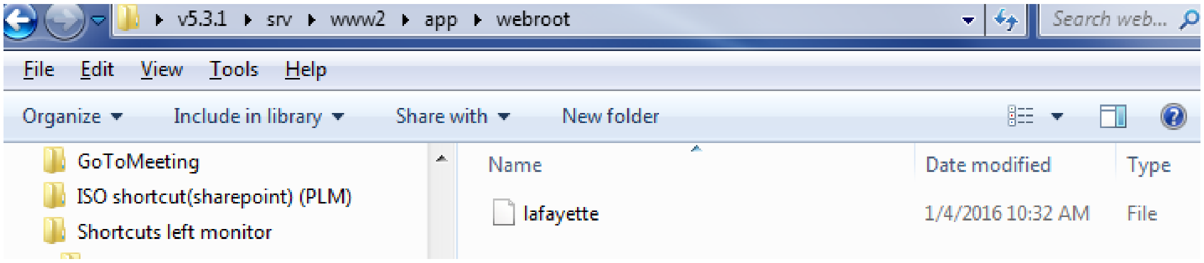
○ Open with [Browse...]

● Save File

right click or save the page as a file, which will be the database.

Per Dave Sohn (18 Nov 2021) Going to the database url, it will try to parse it as text, which is why you see all the garbage. You can right click or save the page as a file, which will be the database.

1) **Database (”lafayette”) is located in the “srv” folder (available after untarring the log bundle)**



v5.3.1 ▸ srv ▸ www2 ▸ app ▸ webroot
Search web...
File Edit View Tools Help
Organize ▾ Include in library ▾ Share with ▾ New folder
GoToMeeting
ISO shortcut(sharepoint) (PLM)
Shortcuts left monitor

Name	Date modified	Type
lafayette	1/4/2016 10:32 AM	File

2) **Rename “Lafayette” as Lafayette.db”.**

3) **Select “Open Database” in DB browser and select this file.**

To view/plot oscillator/temperature data for instance:

A) Select the “Browse Data” tab and then select “log_oscillators” in the “Table” drop-down at the top of the tab.

B) To plot oscillator data, select View-> Plot (at the top of the page). At the top-right, select the desired columns.

Note: Select either ID or RowId for the X and desired value(s) to graph in Y column. Graph updates automatically.

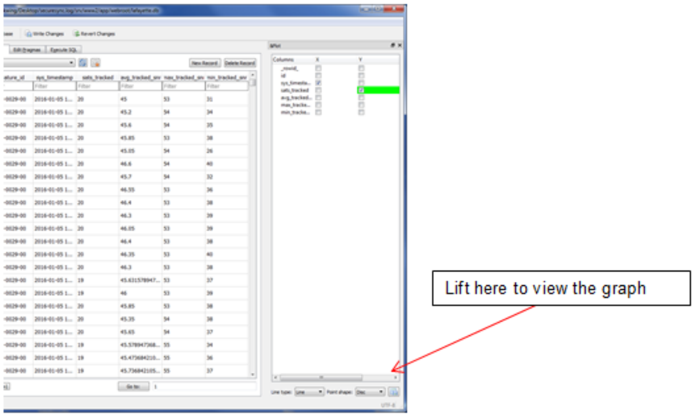
To view/plot (graph) satellite data for instance:

A) Select the “Browse Data” tab and then select “log_gps_statuses” in the “Table” drop-down at the top of the tab.

B) To plot satellite data, select **View**-> **Plot** (at the top of the page). At the top-right, select the desired columns.

Note: Select “**sys_timestamp**” for the X column and desired value(s) to graph in Y column. Graph updates automatically.

Note: if the graph can’t be found in the screen (and if **View** -> **Plot** has been selected) move the Plot table to the right side of the screen and use the mouse to pull up on the bottom bar.



ature_id	sys_timestamp	sats_tracked	avg_tracked_snr	max_tracked_snr	min_tracked_snr
	Filter	Filter	Filter	Filter	Filter
-0029-00	2016-01-05 1...	20	45	53	31
-0029-00	2016-01-05 1...	20	45.2	54	34
-0029-00	2016-01-05 1...	20	45.6	54	35
-0029-00	2016-01-05 1...	20	45.85	53	38
-0029-00	2016-01-05 1...	20	45.05	54	26
-0029-00	2016-01-05 1...	20	46.6	54	40
-0029-00	2016-01-05 1...	20	45.7	54	32
-0029-00	2016-01-05 1...	20	46.55	53	36
-0029-00	2016-01-05 1...	20	46.4	53	38
-0029-00	2016-01-05 1...	20	46.3	53	39
-0029-00	2016-01-05 1...	20	46.05	53	39
-0029-00	2016-01-05 1...	20	46.4	53	38
-0029-00	2016-01-05 1...	20	46.35	53	40
-0029-00	2016-01-05 1...	20	46.3	53	38
-0029-00	2016-01-05 1...	19	45.631578947...	53	37
-0029-00	2016-01-05 1...	19	46	53	39
-0029-00	2016-01-05 1...	20	45.85	53	38
-0029-00	2016-01-05 1...	20	45.35	54	38
-0029-00	2016-01-05 1...	20	45.65	54	37
-0029-00	2016-01-05 1...	19	45.578947368...	55	34
-0029-00	2016-01-05 1...	19	45.473684210...	55	36
-0029-00	2016-01-05 1...	19	45.736842105...	55	37

Columns	X	Y
rowid	□	□
id	□	□
sys_timesta...	☑	□
sats_tracked	□	☑
avg_tracked...	□	□
max_tracke...	□	□
min_tracke...	□	□

Lift here to view the graph

Specific available selections

Log_ntp_stats (ntp _client and ntp_server throughput stats)

Log_sys_mons: System Monitor info

- **Load01**, **load02** and **load03** : associated with CPU load – not NTP/network loading (these are memory values reported in the linux top command- I believe they are (in order left to right- VIRT, RES and SHR)
- **CPU_used**: % CPU usage
- **Sys_temp**:
- **Cpu_temp**:
- **Log_oscillators (discstats**) Sync, Holdover, selected Time/PPS references, DAC, Phase/freq errors, System/CPU temps

General info regarding MySQL/Sqlite databases

- MySQL database was replaced by SQLite database in **version 5.3.1** update.
- Oleg is the primary point of contact for MySQL questions/issues
- MySQL database is located in the **/usr/bin** directory
- MySQL is an open source database that was added in version 5.1.0 to support the new, black/charcoal background browser.
- MySQL is a configuration database for the web browser that stores configurations (standard functionality for MySQL) and also logs data for generating our graphs in the newer browser (this is custom function we created for MySQL to store the graph data).
- A problem with MySQL database typically only affects the web browser graphs.
- Configuration storage in MySQL uses one connection to MySQL and the logging of data for the graphing functions in the newer browser uses a separate connection to MySQL.
- We periodically poll the GPS receiver for SNR and Number of tracked sats and poll the oscillator to log its data. This polling is completely separate to the standard SecureSync logs that are asserted (no correlation between the polling period and log entries being asserted).
- If something adverse was to happen to the MySQL connection while updating a configuration, MySQL has its own way of recovering from this without losing any info (recovery is built-into MySQL because this is a standard function of MySQL).
- If something adverse was to happen to the logging connection to MySQL while updating the logging data, MySQL doesn't have a way of recovering from this without potentially losing that one data point

1) The logging connection can be lost at any point due to MySQL restarting to fix any of its errors.

2) The log entry of **General error: 2006 MySQL server has gone away (WEB)"** indicates the **logging** connection to MySQL was initially present but was lost while storing data. It doesn't try again to store the data.

3) Whether or not that data at that poll is lost depends on when the connection to MySQL is lost.

    - If the connection was lost at the beginning of the logging, the one data point was likely lost.
    - If the connection was lost at the end of the logging, the one data point was likely stored.

backup.sql file residing somewhere within the file system

- This is a large (~150MB) unnecessary file which just a couple of customers have found in the file system (one was in Jul, 2017 and Morgan mentioned he has seen it once and they just deleted it during a remote connection for an unlreated issue. See SF case 25682 for this earlier instance).
- This file was likeky "left behind" during an earlier process (perhaps during a software upgrade??)
- The location of this file may change (so the cleaner file can't remove it)
- If the file is in the **/tmp** directory, rebooting/power cycling the unit should delete the file.
- Otherwise, this undesirable/unnecessary file can be safely removed with the customer proving us with remote connection to the unit for us to delete the file, or by performing a 'clean' and then reconfiguring the unit (use caution restoring a backup config bundle. Depending on when the bundle was exported from the unit, this same file may be put back into the unit again).

Email from Ron D (25 Jul 17) I took a look at the cleaner tool and it doesn't look like it will remove this file.Currently the two ways to get rid of it would be remote access and delete it, or using the clean operation

Email Keith sent to customer (25 Jul 17) I just spoke with the engineer I had forwarded this info along to…

The backup.sql file isn't an "intentional" file that needed to be placed (and remain) in this directory. It was likely "left behind" at some point in the past.during a process being performed at that time.

This file can be removed using a couple of different methods. The easiest and fastest is if you can make the SecureSync remotely accessible, by either putting it on the Internet and providing us with the login credentials, or by providing us with remote control of a PC on the same network as the time server. One of our Engineers can then use the PC to remotely remove this large file for you!

If remote access/control of a PC is not possible/not allowed, the other method is to perform a 'clean' command via the SecureSync's browser, its cli interface (ssh or telnet connection), or via its front panel keypad buttons (the clean comand is listed in the cmd menu, which lets you cycle through the list via the up or down keypad buttons and the green checkmark key accepts the command). This will reset the time server back to its factory default configuration. This method is a bit more "intrusive", as it will require the desired configuratons to be restored (it would be like receiving a new unit from the factory and having to configure it as desired).

If you happen to have an earlier backup of the config files (from before this backup.sql file was created/left behind) the configs can alternately be automatically restored, once the network settings have been manually configured (thereby allowing network access to the browser to perform the restoring of the configurations).

Note a new CF card, which is pre-burned with the same version of software currently installed, could also be sent to you. But this would require the top cover be removed and the CF card swapped out. This is very simimlar to performing a clean command, which doesn't require any dissasemly of the unit to gain access to the CF card. The unit could then be updated to version 5.7.0 (as the timing system software is not stored on the CF card, we can't send the CF card with 5.7.0 pre-burned. the main software on the CF card and the timing system software sub-assy need to be upgraded together, at the same time, to ensure they can continue communicating with each other).

Please let us know if you can provide either our Engineering team in France, or our team in the US, remote access to the SecureSync and we can then delete this file for you. Or, if you prefer to perform a 'clean' via the browser/cli or front panel and then just restore the configs, before updating the software to version 5.7.0. Then we can go from there!!!

I apologize for any inconvenience this condition may have caused □!!

Oracle database (not used/applicable to SecureSyncs/9400s)

Q Basically we are concern if our spectracom is actually using any Oracle as internal database? If we are not, then i can say the issue in the link provided are pretty much not applicable to us. I would just need a confirmation from the support side regarding this.

A (Reply from Keith, 14 Nov 16, applies to at least version 5.5.0 And likely all versions beyond) I can confirm for you that the SecureSyncs do not/have not, contained an Oracle database. Instead, it uses an SQLite database (earlier versions of software used a mysql database.- neither of these are from Oracle).

Web browser time display (upper right corner of the browser)

A) browser.

- Displayed time is corrected each second while connected to the time server.

Email from Dave Sohn on 8/23/11

"(The Time) is updated whenever the page loads or is refreshed (tested on IE, FireFox, and Chrome). However, due to network delays and when the read actually takes place, the time displayed in the UI may not match exactly the time on the SecureSync front panel display. It wouldn't be strange to see it off by a second or more depending on the network."

Apache Struts and Apache Tomcat server

- neither of these add-on programs (Apache Struts or Apache Tomcat server) are used in SecureSyncs, as confirmed by Engineering, and are not likely to start being used anytime in the future
- Any potential vulnerabilities directly associated with these avaialable add-on programs do not apply

A) Apache Struts

- Refer to https://struts.apache.org/
- Refer also to CVEs associated with Strut (such as "CVE-2017-5638") in the Customerserviceassist doc.

Apache Struts is a free, open-source, MVC framework for creating elegant, modern Java web applications. It favors convention over configuration, is extensible using a plugin architecture, and ships with plugins to support REST, AJAX and JSON.

Email from Paul Myers (16 Mar 17)

https://struts.apache.org/
We don't include apache struts.
I don't see apache struts as part of Gentoo anyway.
We use apache web server.

B) Apache Tomcat server

Email from Ron Dries (16 Oct 17) Correct, SecureSync does not use Apache Tomcat.

**Web browser can't open (can't login at the login prompt or prompt not displayed) yet telnet and/or SSH is working

- Refer to the known issues for a list of reasons a user may not be able to login at the browser login prompt or may not get the prompt to login
- Good document for troubleshooting web browser/ssh issues:

https://www.linode.com/docs/troubleshooting/troubleshooting/

- ➢ Review the Apache Error and Access logs

Apache logs (Access and Error logs)

- ➢ For general info, refer to http://httpd.apache.org/docs/2.2/logs.html
- ➢ **error_log** (Apache error log) and **ssl_request.log** (Apache Access log)
- ➢ Starting in version 5.2.1, these logs are contained in the saved log bundle.
- ➢ Can also be viewed in the CLI in the **home/spectracom/log** directory.
- ➢ Refer to the “logs” section of this document for details on log entries.

Apache Access log (ssl_request.log)

“Apache uses the access log files to record information about every visitor to your site. You can see which files visitors view, how the web server responds to requests, and other information such as the web browsers visitors use.”

A. Apache Error logs (error_log)

“The error log is where Apache records information about any errors or anomalies it encounters. Many of the “errors” Apache records are typically minor, such as a visitor requesting a file that doesn't exist. Apache also uses the error logs to record warnings that can indicate a potential problem with a particular event or configuration.

Symptoms relating to possible issue with Apache

- ➢ Can connect via telnet/ssh (rules out any likely network issues).
- ➢ May be able to get to the login screen, but error occurs when trying to login.
- ➢ May not be able to get to the login screen at all (Apache IS needed to be able to see the login screen).

Summary to potentially fix issues with the Apache browser

1. Starting in version 5.2.1- Refer to the logs: **error_log** and **ssl_request.log** (both are associated with Apache) via either a saved log bundle or via the CLI in the home/spectracom/log director
2. Any error messages displayed (more on error messages further below.
3. Decrease the security settings of the customer’s browser

*__Note__: If the browser settings are set too high, no logs or indicators are generated in the time server. It just stays at the login page with no changes.

For example, Internet Explorer set to “High” security will block the browser connection, even though the SecureSync’s logs indicate a successful connection (we can’t sense the browser settings are too high, so we can’t assert any error messages if this happens

Internet Explorer: Tools -> Internet Options, Security tab -> Security level for this zone.

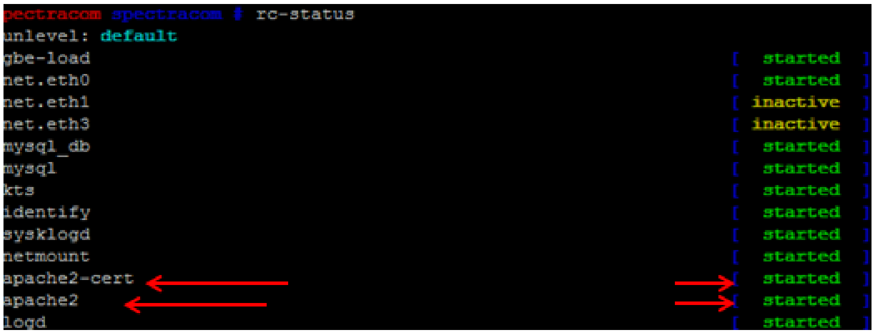
Note that:

- **Medium-high** should allow access.
- **High** will block access to the site.

1) Reboot or power cycle.

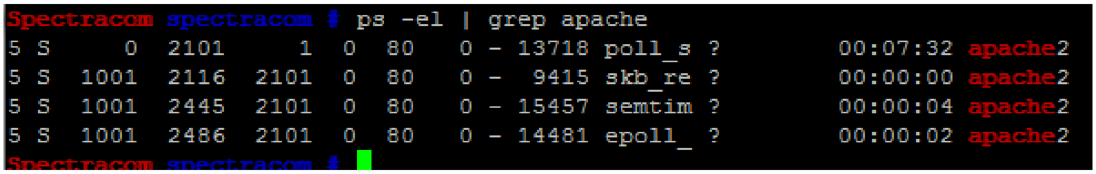
2) Perform a **servget 6** <enter>. Make sure it responds “**HTTPS Service Enabled**”.

3) Perform an **rc-status** CLI command. See if two instances of “Apache2” are listed and “started”



```
pectracom spectracom # rc-status
unlevel: default
gbe-load                                                                  [  started  ]
net.eth0                                                                  [  started  ]
net.eth1                                                                  [ inactive  ]
net.eth3                                                                  [ inactive  ]
mysql_db                                                                  [  started  ]
mysql                                                                     [  started  ]
kts                                                                       [  started  ]
identify                                                                  [  started  ]
sysklogd                                                                  [  started  ]
netmount                                                                  [  started  ]
apache2-cert                                                              [  started  ]
apache2                                                                   [  started  ]
logd                                                                      [  started  ]
```

4) Perform a **ps -el | grep apache** CLI command. Make sure Apache2 is listed



```
Spectracom spectracom # ps -el | grep apache
5 S     0  2101     1  0  80   0 - 13718 poll_s ?        00:07:32 apache2
5 S  1001  2116  2101  0  80   0 -  9415 skb_re ?        00:00:00 apache2
5 S  1001  2445  2101  0  80   0 - 15457 semtim ?        00:00:04 apache2
5 S  1001  2486  2101  0  80   0 - 14481 epoll_ ?        00:00:02 apache2
Spectracom spectracom #
```

5) Perform an **unrestrict** CLI command

6) Perform a **defcert** CLI command

- Update version 5.6.0 (once installed) adds the optional ability to select which Signature algorithm (such as sha1, sha256 or MD5) to user for the generation of the new certificate.
- Example syntax is **-sha256**
- V5.6.0 also changed the default algoritm to SHA256 for better security. IE8 and below do not support SHA-256 (use **defcert -sha1** to regenerate a new certitficate using SHA1 to gain access).

7) Perform a **servset 6 off** and then a **servset 6 on**

8) Perform a **Force/Clean upgrade** using the **sysupgrade** CLI command

From the SecureSync Software update instructions (example below- file name may need to be changed):

1) Perform cli command: **sysupgrade force updatexxx.tar.gz** (where x is the version)

2) Perform cli command: **sysupgrade clean updatexxx.tar.gz** (where x is the version)

3) Get the logs using CLI (either FTP or cat the logs and copy/paste them)

4) Use the **savelog** CLI command to generate a bundle with all the logs (**savelog** followed by a file name, such as **SecureSync**)

5) FTP out this file from the **home/spectracom/xfer/log** directory and send to us.

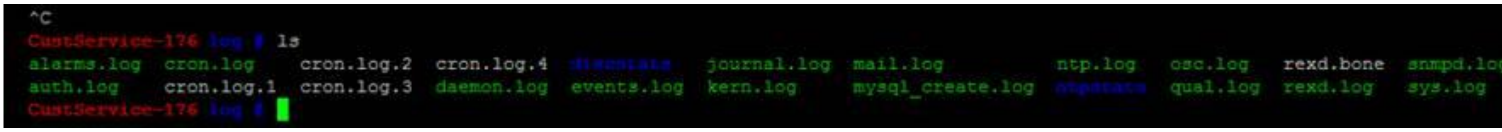
6) Are there any KTS issues indicated in the logs (such as KTS time-out issues for example).   KTS could be loading down the system, preventing the browser from being able to open.

7) **cd /var/log/apache2   cat error_log**. (**Note**: Versions 4.8.9 and below only. With Versions 5.0.0 and higher, spadmin doesn’t have permissions to apache2 folder.   Refer to Mantis case 2906).

8) **Note**: Update version 5.2.1 added this log to the saved log bundle (refer to “error_log” and “ssl_request.log”)

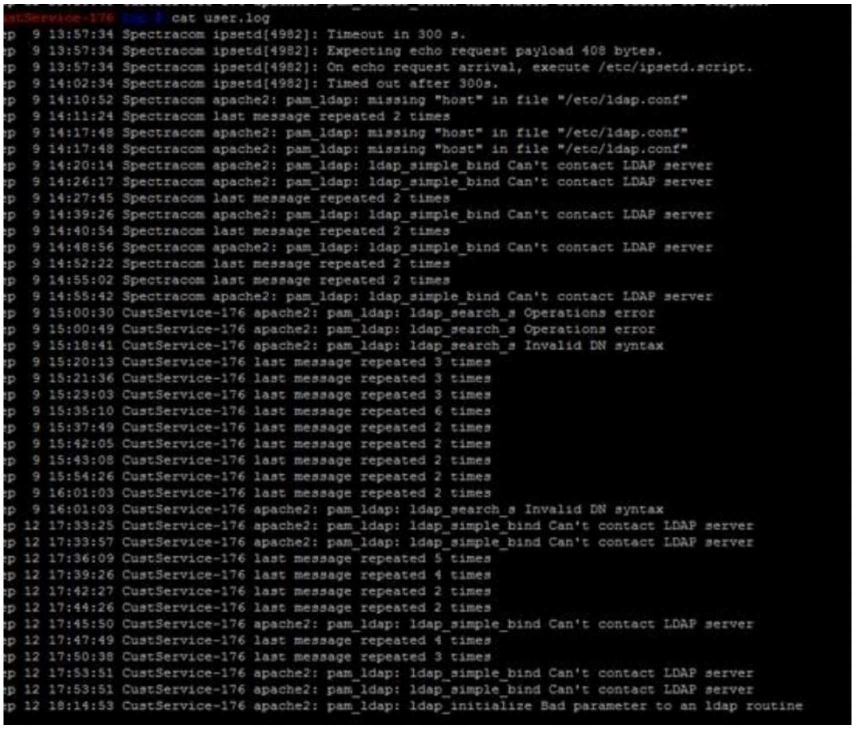
9) **/home/spectracom/log folder**:   auth.log,   daemon.log,   kern.log, user.log.

The logs we would like to initially review are the following:
In the home/spectracom/log directory:
auth.log
kern.log
user.log
daemon.log



```
^C
CustService-176 log # ls
alarms.log  cron.log    cron.log.2  cron.log.4  [illegible]   journal.log  mail.log          ntp.log   osc.log   rexd.bone  snmpd.lo
auth.log    cron.log.1  cron.log.3  daemon.log  events.log  kern.log     mysql_create.log  ntpstats  qual.log  rexd.log   sys.log
CustService-176 log #
```

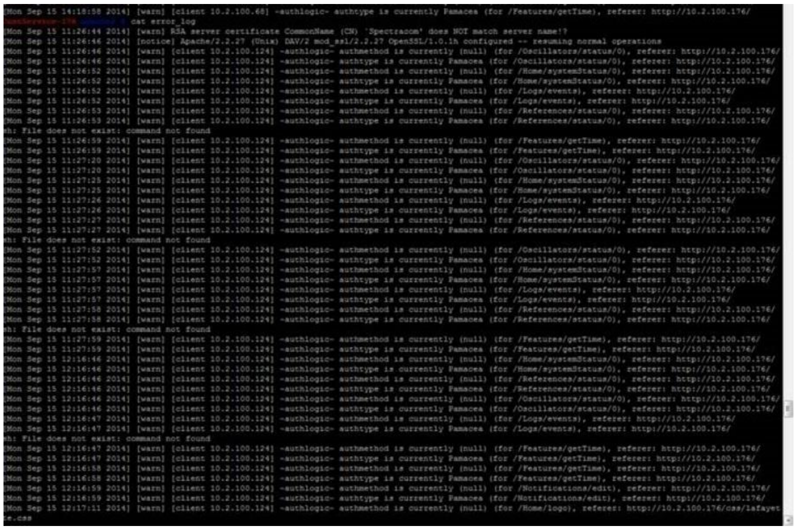
For example:



```
stService-176 log # cat user.log
ep  9 13:57:34 Spectracom ipsetd[4982]: Timeout in 300 s.
ep  9 13:57:34 Spectracom ipsetd[4982]: Expecting echo request payload 408 bytes.
ep  9 13:57:34 Spectracom ipsetd[4982]: On echo request arrival, execute /etc/ipsetd.script.
ep  9 14:02:34 Spectracom ipsetd[4982]: Timed out after 300s.
ep  9 14:10:52 Spectracom apache2: pam_ldap: missing "host" in file "/etc/ldap.conf"
ep  9 14:11:24 Spectracom last message repeated 2 times
ep  9 14:17:48 Spectracom apache2: pam_ldap: missing "host" in file "/etc/ldap.conf"
ep  9 14:17:48 Spectracom apache2: pam_ldap: missing "host" in file "/etc/ldap.conf"
ep  9 14:20:14 Spectracom apache2: pam_ldap: ldap_simple_bind Can't contact LDAP server
ep  9 14:26:17 Spectracom apache2: pam_ldap: ldap_simple_bind Can't contact LDAP server
ep  9 14:27:45 Spectracom last message repeated 2 times
ep  9 14:39:26 Spectracom apache2: pam_ldap: ldap_simple_bind Can't contact LDAP server
ep  9 14:40:54 Spectracom last message repeated 2 times
ep  9 14:48:56 Spectracom apache2: pam_ldap: ldap_simple_bind Can't contact LDAP server
ep  9 14:52:22 Spectracom last message repeated 2 times
ep  9 14:55:02 Spectracom last message repeated 2 times
ep  9 14:55:42 Spectracom apache2: pam_ldap: ldap_simple_bind Can't contact LDAP server
ep  9 15:00:30 CustService-176 apache2: pam_ldap: ldap_search_s Operations error
ep  9 15:00:49 CustService-176 apache2: pam_ldap: ldap_search_s Operations error
ep  9 15:18:41 CustService-176 apache2: pam_ldap: ldap_search_s Invalid DN syntax
ep  9 15:20:13 CustService-176 last message repeated 3 times
ep  9 15:21:36 CustService-176 last message repeated 3 times
ep  9 15:23:03 CustService-176 last message repeated 3 times
ep  9 15:35:10 CustService-176 last message repeated 6 times
ep  9 15:37:49 CustService-176 last message repeated 2 times
ep  9 15:42:05 CustService-176 last message repeated 2 times
ep  9 15:43:08 CustService-176 last message repeated 2 times
ep  9 15:54:26 CustService-176 last message repeated 2 times
ep  9 16:01:03 CustService-176 last message repeated 2 times
ep  9 16:01:03 CustService-176 apache2: pam_ldap: ldap_search_s Invalid DN syntax
ep 12 17:33:25 CustService-176 apache2: pam_ldap: ldap_simple_bind Can't contact LDAP server
ep 12 17:33:57 CustService-176 apache2: pam_ldap: ldap_simple_bind Can't contact LDAP server
ep 12 17:36:09 CustService-176 last message repeated 5 times
ep 12 17:39:26 CustService-176 last message repeated 4 times
ep 12 17:42:27 CustService-176 last message repeated 2 times
ep 12 17:44:26 CustService-176 last message repeated 2 times
ep 12 17:45:50 CustService-176 apache2: pam_ldap: ldap_simple_bind Can't contact LDAP server
ep 12 17:47:49 CustService-176 last message repeated 4 times
ep 12 17:50:38 CustService-176 last message repeated 3 times
ep 12 17:53:51 CustService-176 apache2: pam_ldap: ldap_simple_bind Can't contact LDAP server
ep 12 17:53:51 CustService-176 apache2: pam_ldap: ldap_simple_bind Can't contact LDAP server
ep 12 18:14:53 CustService-176 apache2: pam_ldap: ldap_initialize Bad parameter to an ldap routine
```

- ➢ In the /var/log/apache2 folder cat error.log (example below) (Note: versions 4.8.9 and below only. In versions 5.0.0 and above, user doesn’t have permission to access this file)

Note: Update version 5.2.1 added this log to the saved log bundle (refer to “error_log” and “ssl_request.log”)



```
[Mon Sep 15 14:18:58 2014] [warn] [client 10.2.100.68] -authlogic- authtype is currently Pamacea (for /Features/getTime), referer: http://10.2.100.176/
CustService-176 apache2 # cat error_log
[Mon Sep 15 11:26:44 2014] [warn] RSA server certificate CommonName (CN) `Spectracom' does NOT match server name!?
[Mon Sep 15 11:26:46 2014] [notice] Apache/2.2.27 (Unix) DAV/2 mod_ssl/2.2.27 OpenSSL/1.0.1h configured -- resuming normal operations
[Mon Sep 15 11:26:46 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Oscillators/status/0), referer: http://10.2.100.176/
[Mon Sep 15 11:26:46 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Oscillators/status/0), referer: http://10.2.100.176/
[Mon Sep 15 11:26:52 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Home/systemStatus/0), referer: http://10.2.100.176/
[Mon Sep 15 11:26:52 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Home/systemStatus/0), referer: http://10.2.100.176/
[Mon Sep 15 11:26:52 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Logs/events), referer: http://10.2.100.176/
[Mon Sep 15 11:26:52 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Logs/events), referer: http://10.2.100.176/
[Mon Sep 15 11:26:53 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /References/status/0), referer: http://10.2.100.176/
[Mon Sep 15 11:26:53 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /References/status/0), referer: http://10.2.100.176/
sh: File does not exist: command not found
[Mon Sep 15 11:26:59 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Features/getTime), referer: http://10.2.100.176/
[Mon Sep 15 11:26:59 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Features/getTime), referer: http://10.2.100.176/
[Mon Sep 15 11:27:20 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Oscillators/status/0), referer: http://10.2.100.176/
[Mon Sep 15 11:27:20 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Oscillators/status/0), referer: http://10.2.100.176/
[Mon Sep 15 11:27:25 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Home/systemStatus/0), referer: http://10.2.100.176/
[Mon Sep 15 11:27:25 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Home/systemStatus/0), referer: http://10.2.100.176/
[Mon Sep 15 11:27:26 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Logs/events), referer: http://10.2.100.176/
[Mon Sep 15 11:27:26 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Logs/events), referer: http://10.2.100.176/
[Mon Sep 15 11:27:27 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /References/status/0), referer: http://10.2.100.176/
[Mon Sep 15 11:27:27 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /References/status/0), referer: http://10.2.100.176/
sh: File does not exist: command not found
[Mon Sep 15 11:27:52 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Oscillators/status/0), referer: http://10.2.100.176/
[Mon Sep 15 11:27:52 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Oscillators/status/0), referer: http://10.2.100.176/
[Mon Sep 15 11:27:57 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Home/systemStatus/0), referer: http://10.2.100.176/
[Mon Sep 15 11:27:57 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Home/systemStatus/0), referer: http://10.2.100.176/
[Mon Sep 15 11:27:57 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Logs/events), referer: http://10.2.100.176/
[Mon Sep 15 11:27:57 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Logs/events), referer: http://10.2.100.176/
[Mon Sep 15 11:27:58 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /References/status/0), referer: http://10.2.100.176/
[Mon Sep 15 11:27:58 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /References/status/0), referer: http://10.2.100.176/
sh: File does not exist: command not found
[Mon Sep 15 11:27:59 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Features/getTime), referer: http://10.2.100.176/
[Mon Sep 15 11:27:59 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Features/getTime), referer: http://10.2.100.176/
[Mon Sep 15 12:16:46 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Home/systemStatus/0), referer: http://10.2.100.176/
[Mon Sep 15 12:16:46 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Home/systemStatus/0), referer: http://10.2.100.176/
[Mon Sep 15 12:16:46 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /References/status/0), referer: http://10.2.100.176/
[Mon Sep 15 12:16:46 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /References/status/0), referer: http://10.2.100.176/
[Mon Sep 15 12:16:46 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Oscillators/status/0), referer: http://10.2.100.176/
[Mon Sep 15 12:16:46 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Oscillators/status/0), referer: http://10.2.100.176/
[Mon Sep 15 12:16:47 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Logs/events), referer: http://10.2.100.176/
[Mon Sep 15 12:16:47 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Logs/events), referer: http://10.2.100.176/
sh: File does not exist: command not found
[Mon Sep 15 12:16:47 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Features/getTime), referer: http://10.2.100.176/
[Mon Sep 15 12:16:47 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Features/getTime), referer: http://10.2.100.176/
[Mon Sep 15 12:16:58 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Features/getTime), referer: http://10.2.100.176/
[Mon Sep 15 12:16:58 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Features/getTime), referer: http://10.2.100.176/
[Mon Sep 15 12:16:59 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Notifications/edit), referer: http://10.2.100.176/
[Mon Sep 15 12:16:59 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Notifications/edit), referer: http://10.2.100.176/
[Mon Sep 15 12:17:11 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Home/logo), referer: http://10.2.100.176/css/lafayet
te.css
```

Please either FTP out these log files to send them to us for review. Or “cat” the files to view them, and then copy/paste them to a Word document. Then send them to us for review.

var/log/apache2 error log entries

A) Normal entries for logging out of spadmin account

```
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Users/logout), referer:
http://10.2.100.176/
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Users/logout), referer:
http://10.2.100.176/
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /toolsb) /contact), referer:
http://10.2.100.176/
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /tools/contact), referer:
http://10.2.100.176/
```

B) Normal entries for login to spadmin account

```
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Home), referer:
http://10.2.100.176/tools/contact
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Home), referer:
http://10.2.100.176/tools/contact
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /users/login), referer:
http://10.2.100.176/tools/contact
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /users/login), referer:
http://10.2.100.176/tools/contact
[Mon Sep 15 16:37:15 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /users/login), referer:
http://10.2.100.176/users/login
[Mon Sep 15 16:37:15 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /users/login), referer:
http://10.2.100.176/users/login
```

C) Logs from a SecureSync exhibiting error 500 messages when logging in

```
enable, referer: https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Not processing line, referer:
https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Could not find the required information linedefault value then, referer:
https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Could not find the required information linedefault value then, referer:
https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Premature end of script headers: StatusConfig.cgi, referer:
https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
[Sat Sep 13 19:15:22 2014] [warn] [client 206.218.195.190] -authlogic- authmethod is currently (null) (for /spec500err.html), referer:
https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
[Sat Sep 13 19:15:22 2014] [warn] [client 206.218.195.190] -authlogic- authtype is currently Pamacea (for /spec500err.html),
referer: https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
```

D) “RSA server certificate CommonName (CN) `Spectracom' does NOT match server name!?”

- Indicates web browser Security Settings may be set too high. Try lowering the settings to the lowest value and then login again.
- May need to replace the default HTTPS certificate with a new one using values particular to the network.

****No Error messages displayed when trying to login (stays at login screen)

- Try decreasing the security settings of the customer’s browser (such as Internet Explorer, Firefox or Chrome). Or try a different bowser altogether

***Note:** If the browser settings are set too high, no logs or indicators are generated in the time server. It just stays at the login page with no changes.

For example, Internet Explorer set to “High” security will block the browser connection, even though the SecureSync’s logs indicate a successful connection (we can't sense the browser settings are too high, so we can't assert any error messages if this happens.

Internet Explorer: **Tools** -> **Internet Options**, **Security** tab -> **Security level f**or this zone.
Note that:

- **Medium-high** should allow access.
- **High** will block access to the site.

****Error messages displayed when trying to login

E) "(Hostname) didn't send any data. ERR_EMPTY_RESPONSE"

- Refer to SF case 120558

Reply from Dave L (26 Oct 17) The Securesync may be suffering from a stalled web browser service. This can usually be restored by power cycling the unit. After power cycle the web UI should work again. Then perform a firmware update.

Here are some useful notes to help you with the update:

Make sure there are no older update files listed along with the new version 5.7.1 when you select it to perform the upgrade. If there are any others, select them and Delete Update file.

Run the updateCleaner file prior to performing the update. This will help clean out any old files that are taking up a lot of memory.
Here is a link to get the updateCleaner: https://files.spectracom.com/public-downloads/updatecleaner-securesyncnetclock-9400
If the upgrade fails again, from the command line interface run the df -h command and make sure the memory used is less than 70%. It should be. IF not contact us and we can have a look as to why. This should result in a successful update. Please let me know how it goes.

F) Generic error 500 messages (can be reported as any of the below)

- "This error (HTTP 500 Internal Server Error) means that the website you are visiting had a server problem which prevented the webpage from displaying."
- "500 Internal Server Error"
- "HTTP 500 – Internal Server Error"
- "Internal Server Error"
- "HTTP 500 Internal Error"
- "500 Error"
- "HTTP Error 500″
- "An internal error has occurred. An error occurred while processing this request. No further information is available"

Potential Solutions

- Software crash/ with earlier versions such as v5.5.1

  Email from Dave L (8 Jan 18) The Internal Server Error may be caused by a crash of the web service in the 9483. This can happen on rare occasions in older firmware versions such as 5.5.1.
  Typically a power cycle will restart the web service and restore communications.

  Updating the firmware will help prevent this from happening in the future. We recommend updating to the latest version 5.7.1 which is available for free from our website. Here is a link to download the update and instructions.

  https://files.spectracom.com/public-downloads/latest-securesync-netclock-files

- IF the power cycle does not restore the web browser please let me know and we can explore a solution or RMA this 9483.
- Web browser time-out

Email from Dave L (19 Sep 17) It appears to me the web browser had timed out, causing the 500 Internal Server Error. Closing the web browser and reopening will resolve that issue.

- (v4.8.9 and below only) Use the CLI to type **version** <enter> and **free -m** <enter>. Then power cycle. If connection restored, or free is less than 100MB, likely caused by memory leak and should have software update applied.
- (v5.x.x only) Use the CLI to perform a **df –h** <enter> to see if the CF card is full or nearly full.
- Use the CLI to obtain logs (such as the Auth log)
- Refer to sites such as the following:

From: http://kb.mediatemple.net/questions/1903/Why+am+I+getting+a+500+Internal+Server+Error+message%3F
500 Internal Server Error is a generic error message, given when no more specific message is suitable. There are a number of causes for a 500 Internal Server Error to display in a web browser. Figure 1 is a sample error message.

Email Keith sent to Salesforce case 15738: To begin, “Error 500” messages are very generic messages that can be reported by the SecureSync’s web browser, if the browser can’t open. These messages are rare, but are typically related to a network issue of some sort and not likely an issue with the SecureSync itself. In this case, the SecureSync does not need to be rebooted to restore connection to the browser.

First, if you haven’t already attempted this, try connecting to the SecureSync via its CLI interface (such as by using telnet, ssh or FTP). As long as each service is enabled in the SecureSync (SSH is usually one that remains enabled), you should be able to successfully connect and login to the time server. If this connection also fails, it’s not just an issue associated with the browser. Also try just pinging the IP address of the time server, from the same PC trying to open its browser. If ping fails and the time server is on a different subnet, try pinging it from another PC on the same subnet as the time server. Does it respond to ping from both nodes?

If it doesn’t respond to ping from any PCs on the network, connect a PC directly to the SecureSync and try accessing it from this PC. If the Model 1204-06 Gb Ethernet Option Card is installed, and when connecting to Eth1, Eth2 or Eth3 on this option card, a network cross-over or straight network cable can be used (connecting to base Ethernet port Eth0 requires the use of a network cross-over cable). Temporarily configure the computer to have a static IP address on the same subnet as the time server’s address. Now try accessing the browser again. If the browser opens with this direct connection, there is a network related issue with the NetClock connected to the network that is preventing connection to the time server.

If it still doesn’t ping, try pinging a different Ethernet interface on the back panel, if the Model 1204-06 Option Card is installed. If it still doesn’t ping from another port, I recommend rebooting the server and see if then responds to pings and allows browser login. If it does, let me know and I will have you send us the logs to review, so that we can see if they indicate what might have caused this condition to occur.

Let me know what you find and then we can go from there.

G) “[Fiddler] The socket connection to 10.2.100.176 failed. ErrorCode: 10060.

H) A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond 10.2.100.176:80” (note the values in green will be the assigned IP address)

I) Time server is not accessible on the network. May have a network cable issue or it was recently rebooted.

Try connecting again in a couple of minutes. If still can’t connect, might be a network issue or network is connected to a port of a Model 1204-06 Gb Eth card (Eth1,Eth2 Eth3) that is not enabled (issue the portstate get x <enter> CLI command to verify the current port state.

J) “ERROR: The web server encountered an unexpected error and failed to display the page you requested”

1. **System memory leak occurring (versions 4.8.9 and below).**
   - Refer to: “Known issue: Apache Web browser no longer accessible, but can still ping, telnet etc still work.

- Power cycle or reboot to temporarily recover use of browser.

2. **Potential SNMP issue (fixed in 4.8.0)**
   - Refer to: Known issue with SNMP in versions 4.7.0 and below
   - Perform a clean command from Setup port to restore connectivity. Refer to Mantis case 1477 and Todd Belcher in PSalesforce. Note: An automatic reboot occurs when performing a clean command.

   Note: This issue was fixed in software version 4.8.0.

K) An error occurred: Failed to insert session

- Check the CF card's disk usage (**df -h** in the CLI) to see if card is nearly full (especially with version 5.0.2 installed). May be full of nullmailers

Draft reply from Morgan: Thank you for the information, we have a few other questions:

1) Can you access the device via the cli in interface (telnet or ssh session)?
2) What is the version of software currently installed ? (the CLI command is **version**) From your screenshot, it looks like it is version 5.0.2 or below.
3) Have you power cycled the time server?
4) If you can login via the cli, can you type the command (**df -h**) and let us know the percent used?

L) "An error occurred: @PAMSERVICE@ is not an authorized PAM service" displayed after entering username and password.

- Can be caused by memory leak issue in versions 4.8.9 and below (fixed in 5.0.0). Perform either a free or free mem command to see if the free mem is less than about 100MB (the min for Apache to run).
- Refer to Mantis case number 1339 http://cvsmantis.int.orolia.com/mantis/view.php?id=1339
- Can occur if there are issues with the HTTPS certificate in the Windows computer (try logging in with telnet/ssh.   If this login is successful, the issue is likely with the HTTPS certificate).
- Can occur if username is entered in all caps (SPADMIN).
- Can occur if there are general issues with the network, preventing connection to the time server.

Email Keith sent to Centurylink (1/28/13) Did you happen to enter the user name in upper-case letters (SPADMIN) instead of lower-case letters (spadmin)? Entering the username in upper-case letters can cause this message to be displayed. The only other known reason to see this message is if there is a network issue that is preventing the PC from being able to access the NTP server.

If you enter the username in lower-case and still see this message, try telnetting into the unit (telnet xxx.xxx.xxx.xxx <enter> where x is the IP address of the NTP server). It should prompt you for a login, if telnet hasn't been turned off by a user, yet. (if it has been disabled, it should indicate the connection was refused).

M) "Permission denied"

- Make sure the username is lower-case (spadmin) and not upper-case (SPADMIN).
- Wrong username and/or password may be being entered.

If you can access it via telnet or SSH, can you login and:

1) Type **servget 6** (for HTTPS). Make sure it responds that HTTPS is enabled.
2) Type **rc-status** while trying to login to the browser (after typing its IP address into the Web browser). "Apache2" should be listed.

1) Reset password from front panel (resetpw command) if cant login to browser or cli

I had one customer update to v5.0.2 who couldn't login to browser with either his password or the default password. He reset the password back to default and got in.

Try this only if can't login to either browser or CLI (if can connect via telnet/ssh, password is OK),

Note: Starting in version ~~5.2.1 (~Apr 2015)~~ **resetpw also sets LDAP and Radius to "Disabled"** to help prevent total lockout. They need to be re-enabled thereafter, if desired. Refer to Mantis case 3026 Update- this change was inadvertently left out of the v5.2.1 release. It will need to be added in with the next release (5.3.0?)

When resetpw is performed, and if LDAP and/or Radius were intentionally enabled, they will need to be re-enabled after performing a resetpw.

Q help to clarify that if the RESETPW on panel LCD is used, will it erase all the machine configuration to default or just reset the spadmin password to default value?

A **Keith's response** (23 May 17) Unlike the CLEAN command, the RESETPW command will NOT erase all the configurations back to default. The RESETPW command only resets the spadmin account password back to the default value of 'admin123'.

Note that in software versions 5.2.1 and above, the RESETPW command also disables Radius and LDAP remote authentication services (if enabled for use). This command doesn't change the configurations for these two services. It just unselects the checkbox which enables/disables the functionality of these services. So after performing a RESETPW command, the enable checkbox(es) for LDAP and/or Radius need to be reselected, if using either or both of these authentication services.

A. "Target machine actively refused it xxx.xxx.xxx.xxx:80"

Example:

[Fiddler] The socket connection to 10.2.100.176 failed.
ErrorCode: 10061.
No connection could be made because the target machine actively refused it 10.2.100.176:80

- "HTTP" is likely disabled in Services (*Management* -> *Network* page of new browser
- SecureSync can't be reached / in the process of booting-up or rebooting.
- Try adding **Error! Hyperlink reference not valid.** to the front of the IP address.
- Try pinging it
- Wait a couple of minutes and try again, especially if it was recently rebooted.

B. "Firefox can't establish a connection to the server at xxx.xxx.xxx.xxx" or Internet Explorer reports "Unable to connect"

- "HTTPS" is likely disabled in Services (**Management** -> **Network** page of new browser)
- Will automatically redirect to an HTTP (unsecure) connection, if HTTP is enabled in Services.

C. Full CF card is another reason besides memory leak that the web browser may not be accessible

- Refer to Salesforce cases such as 11568
- SNMP, NTP statistics (versions 4.4.0 and below) and/or NTP logs can potentially fill the CF card to 100% capacity, which will prevent the web browser from being able to open.
- In the case of the SNMP log being full, the log was full of "Subcontainer" error messages.

Note: Refer to Mantis case 2343 (http://cvsmantis.int.orolia.com/mantis/view.php?id=2343)

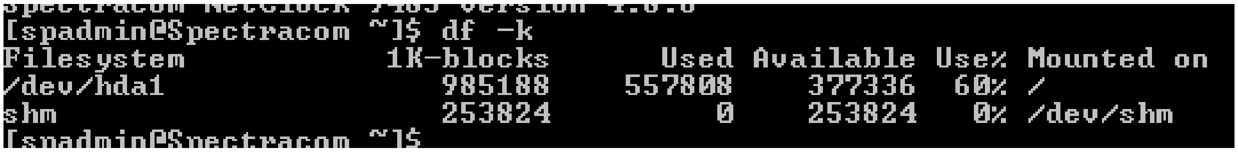
Note: Refer to the SecureSync logs section for more information about this potential condition.

- (Versions 4.4.0 and below only) In the case of the NTP Statistics being full, Paul Myers found that versions 4.4.0 and below weren't rotating out any of the NTP statistics. After several years, they can become so large that they fill the CF card.

Note: Because the clean command was not available in versions 4.4.0 and below, this command is not a temporary fix. Need to send a 4.3.2 CF card to swap in and then update to at least v4.5.0 to prevent it from happening again.

- In the case of the NTP log being full, the log was full of NTP Buffer overflow" messages.
- Use the df <enter> or **df –h** <enter> CLI commands to see if the CF card is full.

Type "**df –h**" at the command prompt (note there is a space between the "f" and the "-h")



```
Spectracom NetClock 7405 version 4.0.0
[spadmin@Spectracom ~]$ df -k
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/hda1               985188    557808    377336  60% /
shm                     253824         0    253824   0% /dev/shm
[spadmin@Spectracom ~]$
```

Example of a full CF card below (using the df command)

```
[spadmin@stjhnblab-mr-ntp-001 log]$ df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/hda1               985188    984516         0 100% /
shm                     253824         0    253824   0% /dev/shm
```

Note: Refer to the "du" command information further below if the card is nearly or completely full.

- If the SecureSync's time is manually set backwards (such as for simulation), FCron stops rotating logs until "time catches back up" to the "correct" time. This can cause the logs to become very large during that time.

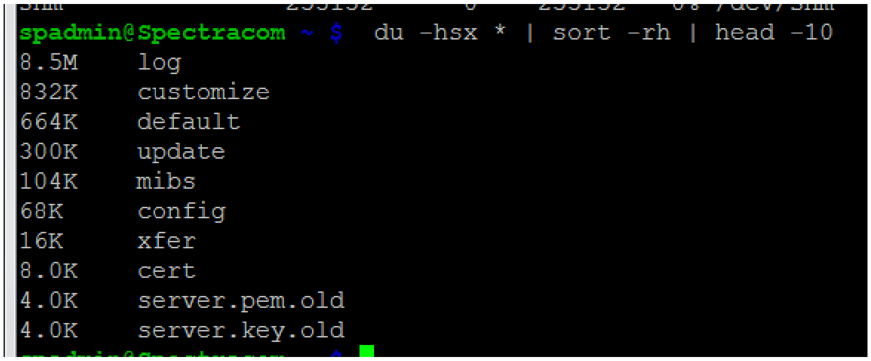
Update: this issue was reportedly fixed in the version 5.0.0 software update. Refer to Mantis case 2091 (http://cvsmantis.int.orolia.com/mantis/view.php?id=2091)

du command (use if the CF card is quite or completely full)

- Refer to http://www.cyberciti.biz/faq/how-do-i-find-the-largest-filesdirectories-on-a-linuxunixbsd-filesystem/

Note: If the card is full or nearly full, to see the top 10 largest directories (and each file, in "MB) perform the following command:

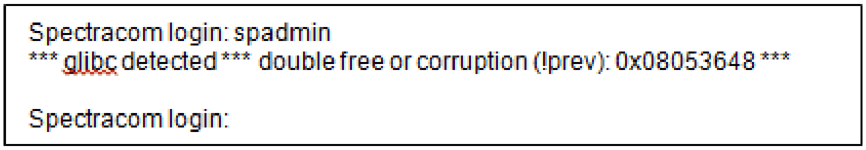
`du -hsx * | sort -rh | head -10`<enter (where the vertical line "pipe" is CTRL and the key under backspace)



```
shm                  255152         0    255152   0% /dev/shm
spadmin@Spectracom ~ $  du -hsx * | sort -rh | head -10
8.5M    log
832K    customize
664K    default
300K    update
104K    mibs
68K     config
16K     xfer
8.0K    cert
4.0K    server.pem.old
4.0K    server.key.old
spadmin@Spectracom ~ $
```

glibc detected * double free or corruption (!prev): 0x08053648**

- glibc detected *** double free or corruption (!prev): 0x08053648 displayed at login prompt (shown below)
- Reported by Robert Farrell w/Verizon (26 Feb 2014)
- Archive version 4.8.9 with 1204-06 card installed
- Appears to be the memory leak issue that was addressed in the version 5.0.0 update.
- Fix: update to versions above 4.8.9.



```
Spectracom login: spadmin
*** glibc detected *** double free or corruption (!prev): 0x08053648 ***

Spectracom login:
```

Paul Myers responded
This may be indicative of a memory problem possibly a memory leak or memory problem.

Is the Front panel updating?
Can they change the front panel screen operation?
Can the user login to the Web UI?
Can they login to the serial console?
Can they login SSH?
Can they FTP connect? (probably not)

*Internet Explorer not displaying the gear icons on the web pages

- Refer to Salesforce case 24808.
- The * setup Icons will not appear on the Home Status page or other pages.

Finding: Internet Explorer was set to use "**Trusted Sites**" and that was blocking the web UI.

Login Banner

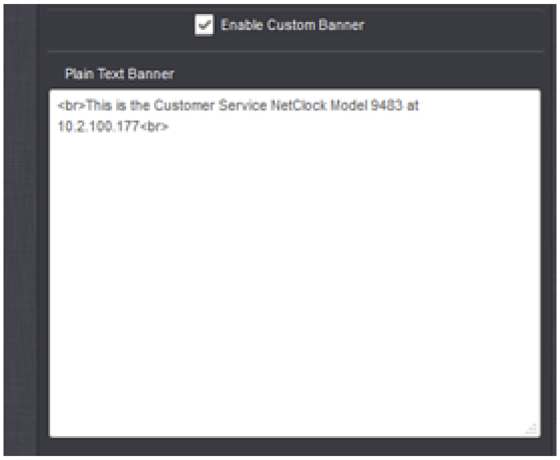
A) Newer browser:

- The Banner configuration is in the Management -> Network page of the browser,
- Click on the "Login Banner" button (left side of the page).

Note: The newer browser has two separate banners displayed/edited on this page. The top one is for telnet/ssh and the bottom one is for the web browser

Make sure the applicable "enable" button is selected if it's desired to display the banner when logging in.

Top banner (SSH login)

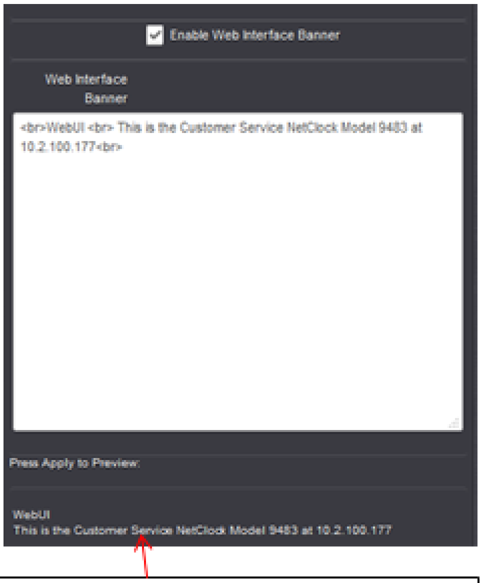


☑ Enable Custom Banner

Plain Text Banner

```
<br>This is the Customer Service NetClock Model 9483 at
10.2.100.177<br>
```

Bottom banner (web browser login)



☑ Enable Web Interface Banner

Web Interface Banner

```
<br>WebUI <br> This is the Customer Service NetClock Model 9483 at
10.2.100.177<br>
```

Press Apply to Preview:

WebUI
This is the Customer Service NetClock Model 9483 at 10.2.100.177

Sample Banner displays at bottom after pressing "Apply"

Note: "<br>" is to start a new line.

Desire for empty/white-space only lines between text lines

- Apparently, you can add hyphens to obtain blank lines.

Q. One minor issue I noticed - the Network Banner strips out empty or whitespace-only lines from what's pasted into the web form. I put in hyphens in order to get a line between paragraphs of the banner.

A. Keith's response: Thanks for mentioning this to me. I spoke with our engineer who had implemented the banner capability in the software. He mentioned that code was implemented in the banner function to have this intentionally happen. He doesn't recall the specific reasons he added it the code, but he found it was necessary while implementing this features. He believes it may have been either associated with the window size on the login page, and/or many Carriage Returns would cause the banner text display to look "abnormal" with many lines of space being present.

OpenSSL (Secure Socket Layer) /TLS-SSL for encryption (and HTTPD.conf file)/Security Level

**OpenSSL/TLS-SSL

- (Libraries for encryption)/ Ciphers for encryption

SSL protocol versions (SSL versions 2.0 and 3.0)

- “OpenSSL version (Such as version 1.01k) isn’t the same as the “SSL protocol version (Such as SSL versions 2.0 or 3.0)
- SSL was replaced by TLS 1.0 after SSL version 3.0 (so there is no SSL version 4.0),
- In at least software versions v5.2.0 and above, SSL protocol versions 2.0 and 3.0 are disabled for both the newer and classic interface web browser (Both browsers only support TLS versions 1.0 and higher. They no longer support either SSLv2 or SSLv3).
- Paul Myers and Oleg confirmed that software version 5.0.2 had both SSL version 3 and TLS version 1 enabled (not SSLv2). SSL v3 was disabled sometime after v5.0.2 and by version 5.2.0 (Oleg believes it was around HeartBleed, like possibly v5.1.4/v5.1.5).
- See below for how to determine which SSL protocols are supported.

***TLS (Transport Layer Security) such as TLS 1.0, 1.1, 1.2 etc

- TLS is a “successor to SSL” (TLS was formerly known as “SSL”)
- SSL version 3.0 was the last version of SSL before TLS 1.0.

TLS vs SSL

from *https://www.howsmyssl.com/s/about.html*)
Okay, last thing. The jargon around is a little funny, so let's be a little more explicit. The 'S' in "HTTPS" is the TLS protocol. When folks refer to the "TLS" they are referring to the most common of modern protocols of encrypting data across the internet. "SSL", when used by experts, refers to the older versions of these protocols. In general, people use "SSL" and "TLS" interchangeably, but that's changing towards everyone saying "TLS". "TLS" is what everyone will call it in the future, while "SSL" is the phrase everyone knows right now.

TLS protocol versions

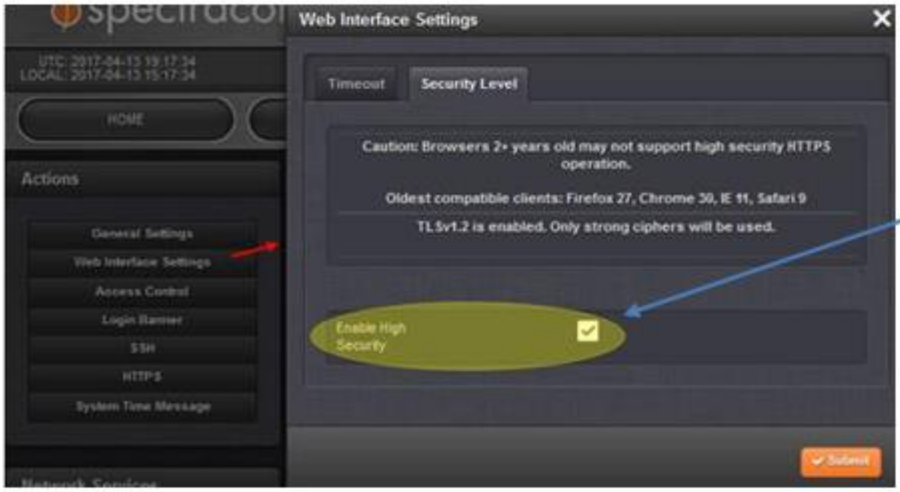
- TLS protocol version 1.0 was first release of TLS, which replaced SSL v3
- TLS versions (such as versions 1.0, 1.1, 1.2 are protocols that can be enabled via the OpenSSL packages. It’s not something that is automatically applied or automatically updated via an OpenSSL version update.
- See further below for how to determine which TLS protocols are supported.

TLS 1.0 enabled / Desire to disable TLS (Enable High Security/“Hisec”) (2400 SecureSync versions 1.1.0a and above)

(Ability to select both medium and high cipher OR just high/strong ciphers) (available in 2400 SecureSync versions 1.1.0A and above)

- 24 SecureSyncs: Ability to enable either ‘*both high and medium level ciphers*’, or ‘*high level ciphers only’* was added in software version 1.1.0a (Feb 2020)
- Selecting the “Enable High Security” checkbox limits the ciphers list on the time server to only thoses algorithms considered most secure (preventing earlier browsers such as IE11 from being able to login)
- Factory default state is the “Enable High Security” checkbox NOT selected (providing both strong and medium ciphers for earlier browsers such as IE11)

- Selection is in the Management -> Network Setup page of the browser (press the “web interface settings” button on the left). Then select the “Enable High Security” checkbox in the “Security Level” tab (as shown below):



Caution: Browsers 2+ years old may not support high security HTTPS operation.

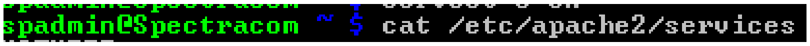
Oldest compatible clients: Firefox 27, Chrome 30, IE 11, Safari 9

TLSv1.2 is enabled. Only strong ciphers will be used.

Enable High Security ☑

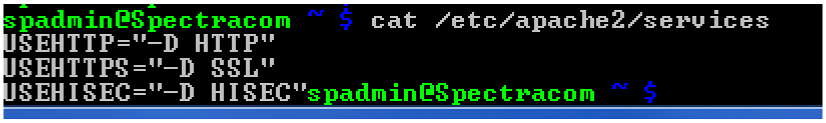
Using the CLI interface (such as if browser is not accessible) to determine if “Enable High Security” is selected

To determine via CLI if “Enable High Security” is selected, type the following command**: cat /etc/apache2/services**



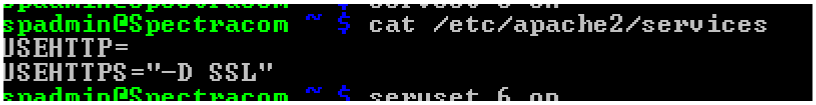
```
spadmin@Spectracom ~ $ cat /etc/apache2/services
```

- If the response lists both “**USEHTTPS=”-D SSL**” and **USEHTTPS=”-D HISEC”** (as shown below) the “Enable High Security” checkbox **IS** currently selected:



```
spadmin@Spectracom ~ $ cat /etc/apache2/services
USEHTTP="-D HTTP"
USEHTTPS="-D SSL"
USEHISEC="-D HISEC"spadmin@Spectracom ~ $
```

- But if the response does not include “**USEHTTPS=”-D HISEC**” (as shown below) the “Enable High Security” checkbox **is not** currently selected:



```
spadmin@Spectracom ~ $ cat /etc/apache2/services
USEHTTP=
USEHTTPS="-D SSL"
spadmin@Spectracom ~ $ seruset 6 on
```

Security scan reported “SSL/TLS server supports TLSv1.0 (“port 443/tcp over SSL)”

Reply from Paul Myers (20 Dec 16) TLS 1.0 is enabled for Medium level web browser security. High Security will disable TLS 1.0 at the cost of older browser support.

How to verify which SSL and TLS protocols are enabled/disabled (can be performed with spadmin account)

1) **“CD”** to the /etc/apache2/sites-enabled directory. Type (or copy/paste): **cd /etc/apache2/sites-enabled**
2) Type :**cat 000-httpd-default.conf**

3) In the conf file is an “**SSLProtocol**” line (like shown below and near the ciphers list). In this Example line, “ALL -SSLv2 -SSLv3” indicates all **TLS and SSL** protocols accept ssl 2.0 and ssl 3.0.

- **Note for TLS**: The word “**All**” includes all SSL and all **TLS** protocols. (not just “SSL”)

Example conf file entry for the web browser,
: **SSLProtocol ALL -SSLv2 -SSLv3** ("**All**" indicates all SSL and all TLS protocol versions)

Example from v5.4.1 (showing in red that all versions of TLS - minus SSLv2 and SSLv3 - are currently enabled as of this release)

```
#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on

# Security Patches
# CVE-2012-4929 CRIME attack on Gentoo BUG# 438680
SSLCompression off

#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+SSLv2:!EXP:!eNULL

SSLProtocol ALL -SSLv2 -SSLv3
SSLHonorCipherOrder On
#SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4-SHA:+HIGH:+MEDIUM
# Generated by https://mozilla.github.io/server-side-tls/ssl-config-ge
```

SSL Cipher suites (CBC Ciphers) /MAC Algorithms

- OpenSSL in the NTP servers have a supported Ciphers list. The client also has its own list of supported ciphers.
- The supported ciphers list is in order of most secure to least secure, with the considered most secure at the top of the list and the least secure at the bottom of the list
- The client and NTP server negotiate which cipher to use, typically the first common one in both lists. This allows the most secure cipher, supported by both Server and Client to be selected for encryption.

**SHA-1(SHA1) vs SHA-2 (SHA2) family (SHA-224, SHA-256, SHA-384, SHA-512)

- Refer to http://www.infoworld.com/article/2879073/security/all-you-need-to-know-about-the-move-to-sha-2-encryption.html
- "SHA-2, the set of cryptographic hash functions to succeed SHA-1"

Intro to SHA

- SHA stands for (Secure Hash Algorithm) and were created by the NSA.
- The number after "SHA" is the hash value (number of bits).

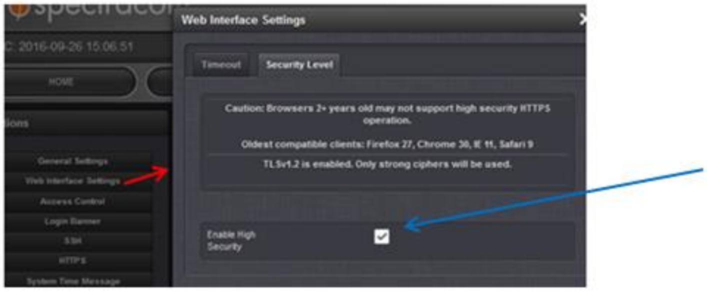
SHA-1 was designed by the NSA and published as a federal standard in 1995. Hashes are used for digitally signing content for integrity validation and are a part of any digital certificate. Without cryptographically sound hashing algorithms, digital authentication and integrity would be very hard to do, if not impossible.

In 2002, SHA-2 became the new recommended hashing standard. SHA-2 is often called the SHA-2 family of hashes because it contains many different-size hashes, including 224-, 256-, 384-, and 512-bit digests. When someone says they are using the SHA-2 hash, you don't know which bit length they are using, but the most popular one is 256 bits (by a large margin). Although SHA-2 is constantly attacked and minor weaknesses are noted, in crypto-speak, it's considered "strong." Without question, It's way better than SHA-1, which experts believe will be fallible in the near term.

**Ability to select medium and high ciphers OR just high-level ciphers

- Ability to select either high and medium level ciphers or just high level ciphers was added in software version 5.4.5.

- Seleting “Enable High Security” limits the ciphers list to only thoses algorithms considered most secure.
- Selection is in the Management -> Network Setup page of the browser (press “web interface settings” button on the left). Then select the “Enable High Security” checkbox in the “Security Level” tab *as shown below):



Caution: Browsers 2+ years old may not support high security HTTPS operation.

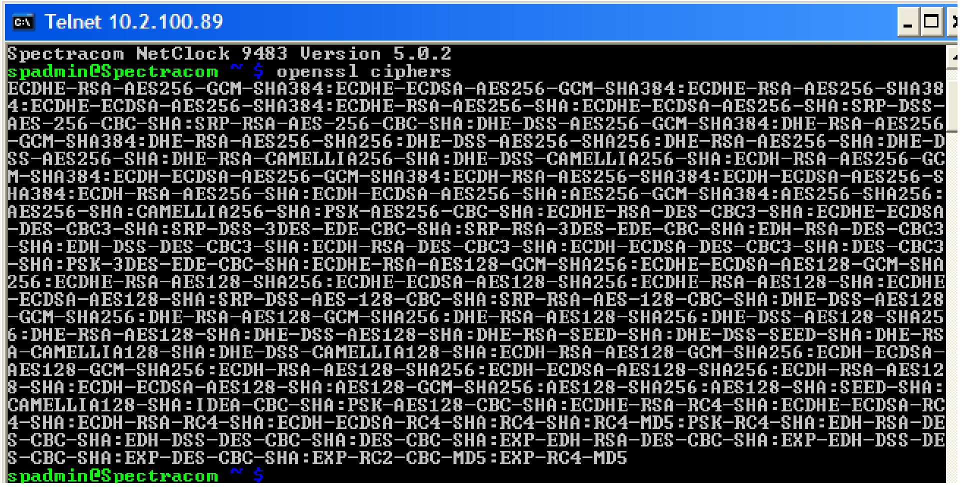
Oldest compatible clients: Firefox 27, Chrome 30, IE 11, Safari 9

TLSv1.2 is enabled. Only strong ciphers will be used.

Enable High Security ☑

A) **To see all ciphers available in OpenSSL versions installed**

B) Login as spadmin and type openssl ciphers <enter>



```
Spectracom NetClock 9483 Version 5.0.2
spadmin@Spectracom ~ $ openssl ciphers
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA38
4:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:SRP-DSS-
AES-256-CBC-SHA:SRP-RSA-AES-256-CBC-SHA:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256
-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA256:DHE-RSA-AES256-SHA:DHE-D
SS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:ECDH-RSA-AES256-GC
M-SHA384:ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-SHA384:ECDH-ECDSA-AES256-S
HA384:ECDH-RSA-AES256-SHA:ECDH-ECDSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:
AES256-SHA:CAMELLIA256-SHA:PSK-AES256-CBC-SHA:ECDHE-RSA-DES-CBC3-SHA:ECDHE-ECDSA
-DES-CBC3-SHA:SRP-DSS-3DES-EDE-CBC-SHA:SRP-RSA-3DES-EDE-CBC-SHA:EDH-RSA-DES-CBC3
-SHA:EDH-DSS-DES-CBC3-SHA:ECDH-RSA-DES-CBC3-SHA:ECDH-ECDSA-DES-CBC3-SHA:DES-CBC3
-SHA:PSK-3DES-EDE-CBC-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA
256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE
-ECDSA-AES128-SHA:SRP-DSS-AES-128-CBC-SHA:SRP-RSA-AES-128-CBC-SHA:DHE-DSS-AES128
-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-DSS-AES128-SHA25
6:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:DHE-RSA-SEED-SHA:DHE-DSS-SEED-SHA:DHE-RS
A-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA:ECDH-RSA-AES128-GCM-SHA256:ECDH-ECDSA-
AES128-GCM-SHA256:ECDH-RSA-AES128-SHA256:ECDH-ECDSA-AES128-SHA256:ECDH-RSA-AES12
8-SHA:ECDH-ECDSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:SEED-SHA:
CAMELLIA128-SHA:IDEA-CBC-SHA:PSK-AES128-CBC-SHA:ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC
4-SHA:ECDH-RSA-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:PSK-RC4-SHA:EDH-RSA-DE
S-CBC-SHA:EDH-DSS-DES-CBC-SHA:DES-CBC-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-EDH-DSS-DE
S-CBC-SHA:EXP-DES-CBC-SHA:EXP-RC2-CBC-MD5:EXP-RC4-MD5
spadmin@Spectracom ~ $
```

C) To view the ciphers list allowed for either the new browser or (can be done with spadmin account) perform either of the following:

webbrowser

Note: This process below will only display the list for either High or Medium, depending on which is configured to be used. Screenshot below shows list for v5.4.5 with high security selected (instead of medium)

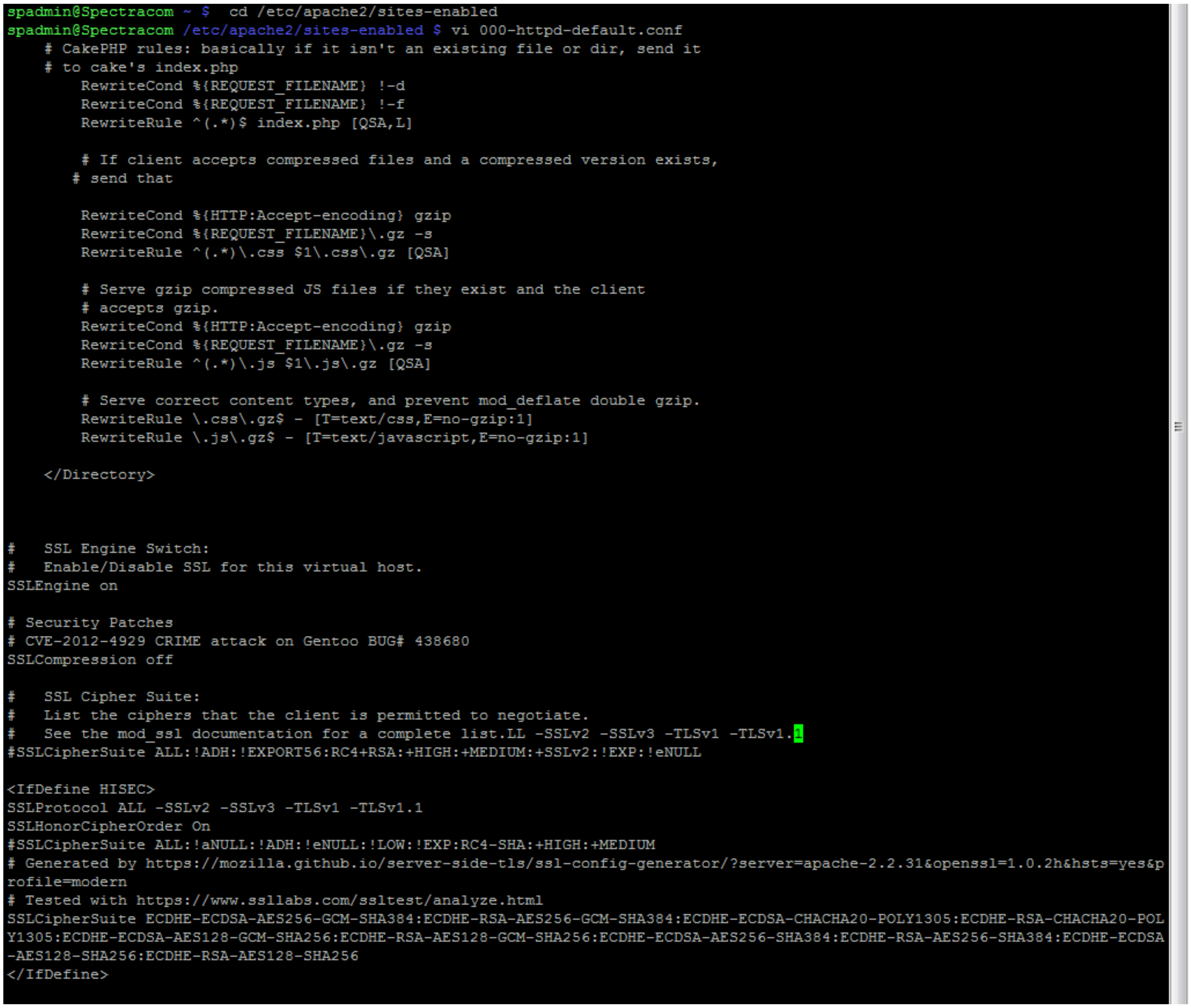
1. Type cd **/etc/apache2/sites-enabled** directory.
2. type the following: **vi 000-httpd-default.conf**

   A. Press: **/** and then type **ssl** next to it

   B. This will display the enabled and disabled SSL/TLS ciphers (Note that "ALL" includes SSLv2, SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, etc and ! before a cipher indicates not enabled).

Note: the "!" is a "not" symbol to exclude that item from being allowed

Note: to exit out of the file, press both ctrl + z



```
spadmin@Spectracom ~ $  cd /etc/apache2/sites-enabled
spadmin@Spectracom /etc/apache2/sites-enabled $ vi 000-httpd-default.conf
    # CakePHP rules: basically if it isn't an existing file or dir, send it
    # to cake's index.php
        RewriteCond %{REQUEST_FILENAME} !-d
        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]

        # If client accepts compressed files and a compressed version exists,
       # send that

        RewriteCond %{HTTP:Accept-encoding} gzip
        RewriteCond %{REQUEST_FILENAME}\.gz -s
        RewriteRule ^(.*)\.css $1\.css\.gz [QSA]

        # Serve gzip compressed JS files if they exist and the client
        # accepts gzip.
        RewriteCond %{HTTP:Accept-encoding} gzip
        RewriteCond %{REQUEST_FILENAME}\.gz -s
        RewriteRule ^(.*)\.js $1\.js\.gz [QSA]

        # Serve correct content types, and prevent mod_deflate double gzip.
        RewriteRule \.css\.gz$ - [T=text/css,E=no-gzip:1]
        RewriteRule \.js\.gz$ - [T=text/javascript,E=no-gzip:1]

    </Directory>



#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on

# Security Patches
# CVE-2012-4929 CRIME attack on Gentoo BUG# 438680
SSLCompression off

#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.LL -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+SSLv2:!EXP:!eNULL

<IfDefine HISEC>
SSLProtocol ALL -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLHonorCipherOrder On
#SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4-SHA:+HIGH:+MEDIUM
# Generated by https://mozilla.github.io/server-side-tls/ssl-config-generator/?server=apache-2.2.31&openssl=1.0.2h&hsts=yes&p
rofile=modern
# Tested with https://www.ssllabs.com/ssltest/analyze.html
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POL
Y1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA
-AES128-SHA256:ECDHE-RSA-AES128-SHA256
</IfDefine>
```

```
<IfDefine HISEC>
SSLProtocol ALL -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLHonorCipherOrder On
#SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4-SHA:+HIGH:+MEDIUM
# Generated by https://mozilla.github.io/server-side-tls/ssl-config-generator/?server=apache-2.2.31&openssl=1.0.2h&hsts=yes&profile=modern
# Tested with https://www.ssllabs.com/ssltest/analyze.html
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256
</IfDefine>
```

```
# This is essentially an else
<IfDefine !HISEC>
SSLProtocol ALL -SSLv2 -SSLv3
SSLHonorCipherOrder On
# Generated by https://mozilla.github.io/server-side-tls/ssl-config-generator/?server=apache-
2.2.31&openssl=1.0.2h&hsts=yes&profile=intermediate
# Tested with https://www.ssllabs.com/ssltest/analyze.html
SSLCipherSuite ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-
AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-
RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-
ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-
SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-
RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-
AES256-SHA:!ECDHE-ECDSA-DES-CBC3-SHA:!ECDHE-RSA-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-
SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-
SHA:!DES-CBC3-SHA:!DSS
</IfDefine>
```

**TLSv1.2 Security Level selection

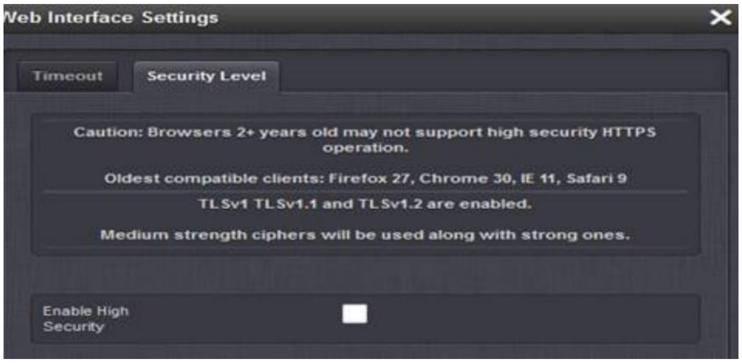
- the ability to either limit the newer black browser to use only strong security ciphers or to allow it to use both medium and strong ciphers (As determined by the requirements of the browsers desiring to connect to the SecureSync)
  - There are two different cipher lists. This checkbox determines which of the two is used).
  - TLSv1.2 is enabled when high Security is selected.

Configure SecureSync to use High-level ciphers only

- I believe default is to allow both medium and high ciphers to be used

1. Navigate to the **Management** -> **Network** page
2. On the left side of the page, click “**Web interface Settings**”
3. Select the **Security Level** tab.
4. Select the “**Enable High Security**” checkbox to disable the medium-level security ciphers and press Submit.

Medium and Strong security configured



eb Interface Settings

Caution: Browsers 2+ years old may not support high security HTTPS operation.

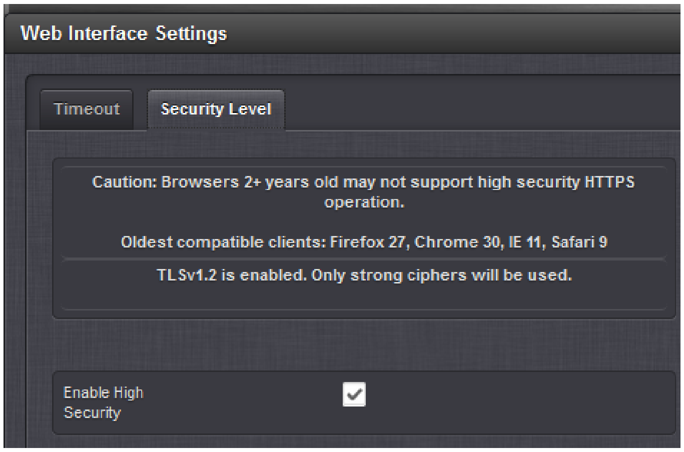
Oldest compatible clients: Firefox 27, Chrome 30, IE 11, Safari 9

TLSv1 TLSv1.1 and TLSv1.2 are enabled.

Medium strength ciphers will be used along with strong ones.

Enable High Security □

Enable High Security ciphers



Web Interface Settings

Caution: Browsers 2+ years old may not support high security HTTPS operation.

Oldest compatible clients: Firefox 27, Chrome 30, IE 11, Safari 9

TLSv1.2 is enabled. Only strong ciphers will be used.

Enable High Security ☑

How is the cipher chosen in an SSL or TLS session?

- From http://luxsci.com/blog/256-bit-aes-encryption-for-ssl-and-tls-maximal-security.html

In general, when an SSL client, such as an email program or web browser, connects to a server and wishes to use SSL or TLS, the client sends the server a list of encryption ciphers that it supports. The server then goes through the list, in order, and chooses the first match that it also supports. Usually, the client orders the list with the most secure methods first, so that the most secure method supported by both the client and server is selected. Sometimes, the client orders the list based on other criteria to make a compromise between security and speed; this can result in a sub-optimal cipher being chosen.

Most modern web and email servers that support SSL encryption, like LuxSci.com's servers, support many different strong encryption techniques all the way up to 128-bit RC4 and 256-bit AES. They provide a variety, instead of just a single really good method, so that users who have old or broken software can still take advantage of encryption, even if it is weaker than it should be. Additionally, most companies that provide security services do not permit use of techniques that deemed are "too weak" and which can be broken very easily (like the old "export grade ciphers" that used to be in prevalent use). So, if you are connecting to a reputable service provided over SSL or TLS, the type of encryption that will be used is almost certainly determined by your client program (i.e. email program or web browser).

Q. What is the maximum SSH cipher suites that the box can support?

A. As for the question on cipher suites, below is a screenshot of the SSH configuration page. This screen will likely answer many of your customer's questions about SSH configuration of the SecureSync.

As shown in the screenshot above, SecureSync supports **RSA, DSA and ECDSA** encryption (as mentioned earlier, it does not support AES). The allowable key sizes for each of these algorithms are listed below:

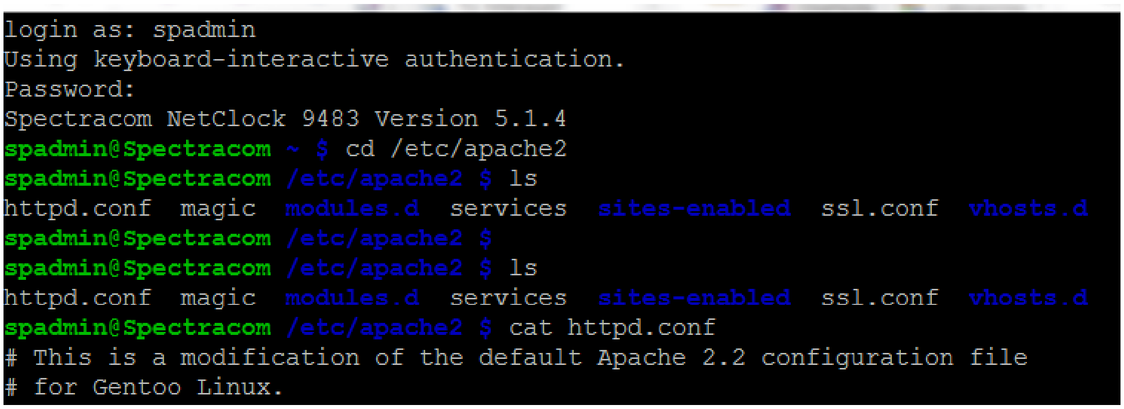
- RSA keys can be 768 to 4096 bits
- DSA keys are limited to 1024 bits
- ECDSA keys can be 256, 384 or 521 bits

The SecureSync also supports Authentication of Password only, Public Key only, or either of these (as configured in the "Authentication Type" drop-down field).

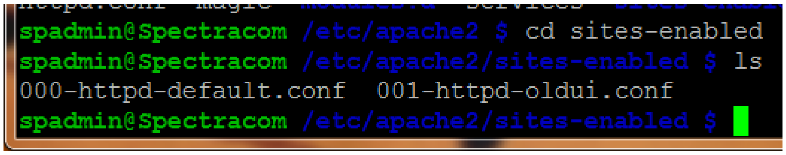
HTTPD.conf file

Q. Is there a way to look at the httpd.conf file?

A. **Per Dave Sohn (22 Apr 014)** httpd.conf is visible in the /etc/apache2 directory on the SecureSync. There are additional conf files in the /etc/apache2/sites-enabled directory



```
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom NetClock 9483 Version 5.1.4
spadmin@Spectracom ~ $ cd /etc/apache2
spadmin@Spectracom /etc/apache2 $ ls
httpd.conf  magic  modules.d  services  sites-enabled  ssl.conf  vhosts.d
spadmin@Spectracom /etc/apache2 $
spadmin@Spectracom /etc/apache2 $ ls
httpd.conf  magic  modules.d  services  sites-enabled  ssl.conf  vhosts.d
spadmin@Spectracom /etc/apache2 $ cat httpd.conf
# This is a modification of the default Apache 2.2 configuration file
# for Gentoo Linux.
```



```
spadmin@Spectracom /etc/apache2 $ cd sites-enabled
spadmin@Spectracom /etc/apache2/sites-enabled $ ls
000-httpd-default.conf  001-httpd-oldui.conf
spadmin@Spectracom /etc/apache2/sites-enabled $
```

UserDir Disabled

Q. Can you confirm the following directive command is set in httpd.conf file for the SecureSync 1200 appliance? "**UserDir Disabled**" in httpd.conf file. This directive value is a fix for CVE2001-1013

A. Per Dave Sohn (22 Apr 2014) This directive command is not in SecureSync. However, no username disclosure is available via the SecureSync via the vulnerability described. When tested, all user directory queries respond with a 404 response whether the username exists on SecureSync or

**AES (Advanced Encryption Standard)

- AES is a specification for the encryption of electronic data.

Q. What BIT (size) of AES encryption is supported?
A. Email from Paul Myers (2/2/12) “We support “AES 128, 192, and 256 bit ciphers”

**MTU (Maximum Transmission Unit)

- for info on MTU: http://en.wikipedia.org/wiki/Maximum_transmission_unit
- In versions 5.1.4 and below, MTU is hard-set to1500 (users cannot change)
- Harris requested ability to change this value to 1400. Refer to Salesforce case 13244.
- Ability to change MTU value was added in update version 5.1.4.

**Network ports/Management/Network Access restriction (Access control)

- ➢ Internal use only- for CLI, the access table entries are in /home/spectracom/config and type: cat access.conf

Note: refer also to "IPTables" (applicable to versions 5.4.0/5.4.1 and above) for customized port restriction capabilities.

Important note: entering a subnet value of "**/0**" is not valid. In versions 5.30 and below, It will cause Apache to crash and prevent access to the browser. In versions 5.3.0 and below, the browser doesn't prevent a user from inadvertently entering this value (Refer to Mantis case 3110). This potential condition was fixed in **version 5.3.1**.

Format of table entries: uses **CIDR format** (x.x.x.x/zz (where zz is the two digit subnet mask. Example: 10.10.1.1/32)

The two digit subnet mask does not have to be the same mask that the network is using. With using CIDR in this particular functionality of blocking access, the specified address and the subnet are "or" together to determine a range of allowable addresses. So an even smaller subnet of allowed addresses can be defined, than the subnet that the time server is plugged into.

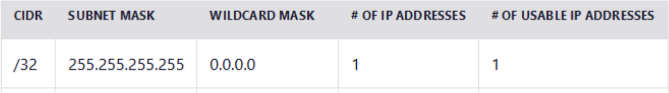
- If it's desired to define **one specific IP address** (and allow no others on that same subnet), use the two digit subnet mask of **/32**. Note that more than one address using "/32" can be added to the list to allow access to more than one specific address.
- If it's desired to allow access to any nodes that have the same last octet as the configured address, use a subnet mask of /24
- If it's desired to allow access to any nodes that have the same last two octets as the configured address, use a subnet mask of /16.

To calculate the CIDR value to use, refer to online CIDR tools such as https://www.subnet-calculator.com/cidr.php (change the CIDR Netmask to the value which allows the number of individual PC's desired, or to a value that allows the desired entire subnet)

Management -> **Network** page. Then click on "**Access Control**" (on the left side of the page)

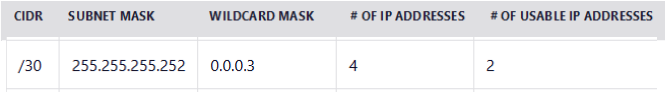
Note: IP address(es) must be entered in CIDR format ("IP address / two digit subnet mask) as described further above.

- ○ To limit access to only one PC for example: 10.10.128.2**/32**



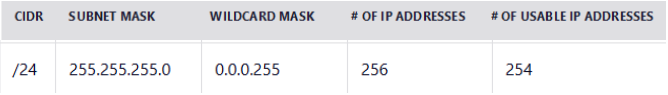
CIDR	SUBNET MASK	WILDCARD MASK	# OF IP ADDRESSES	# OF USABLE IP ADDRESSES
/32	255.255.255.255	0.0.0.0	1	1

- ○ To limit access to only two PCs for example: 10.10.128.2**/30**



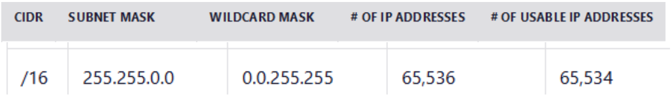
CIDR	SUBNET MASK	WILDCARD MASK	# OF IP ADDRESSES	# OF USABLE IP ADDRESSES
/30	255.255.255.252	0.0.0.3	4	2

- ○ To limit access to an entire subnet of 255.255.255.0: 10.10.128.2**/24**

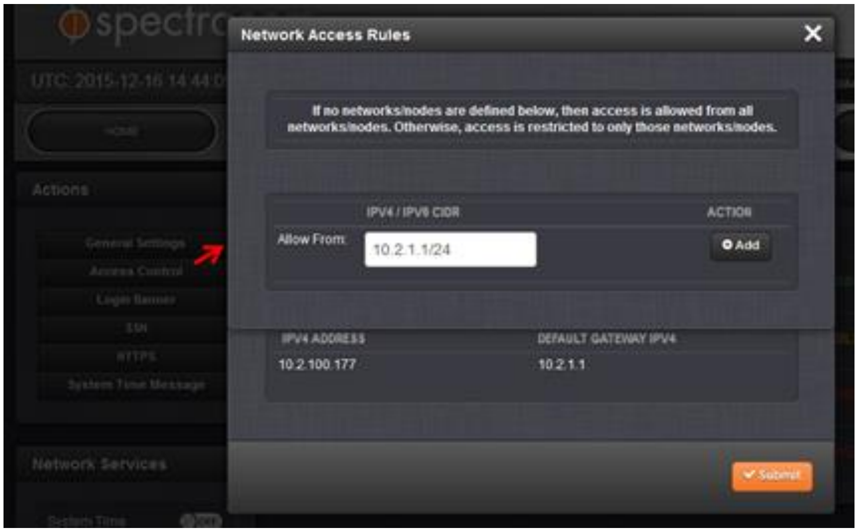


CIDR	SUBNET MASK	WILDCARD MASK	# OF IP ADDRESSES	# OF USABLE IP ADDRESSES
/24	255.255.255.0	0.0.0.255	256	254

- ○ To limit access to an entire subnet of 255.255.0.0: 10.10.128.2**/16**



CIDR	SUBNET MASK	WILDCARD MASK	# OF IP ADDRESSES	# OF USABLE IP ADDRESSES
/16	255.255.0.0	0.0.255.255	65,536	65,534



If no networks/nodes are defined below, then access is allowed from all networks/nodes. Otherwise, access is restricted to only those networks/nodes.

Allow From: 10.2.1.1/24

IPV4 ADDRESS	DEFAULT GATEWAY IPV4
10.2.100.177	10.2.1.1

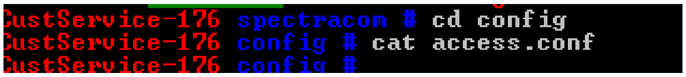
Note: IP address(es) must be entered in CIDR format ("IP address / two digit subnet mask) as described further above.

- To limit access to only one PC for example: 10.10.128.2/32
- To limit access to an entire subnet of 255.255.255.0: 10.10.128.2/24
- To limit access to an entire subnet of 255.255.0.0: 10.10.128.2/16

Command to reset the Network Access table (unrestrict)

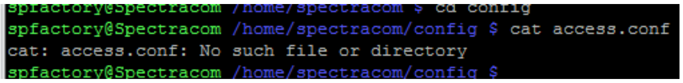
CLI command ("**unrestrict**") to clear the Access table. No need to clean all configurations. This can be performed via the CLI- It's not available via the keypad (it's not in the front panel "Cmd" menu).

Note: the configs for network access restriction are stored in the **access.conf** file (**home/spectracom/conf**irectory and then type: **cat access.conf** . If there is no response to this command, the table is empty (as shown below)



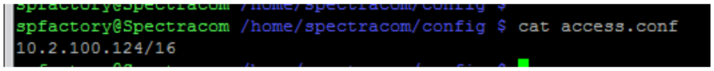
```
CustService-176 spectracom # cd config
CustService-176 config # cat access.conf
CustService-176 config #
```

Example from v5.3.1 showing no entries have been added added to the Access table



```
spfactory@Spectracom /home/spectracom $ cd config
spfactory@Spectracom /home/spectracom/config $ cat access.conf
cat: access.conf: No such file or directory
spfactory@Spectracom /home/spectracom/config $
```

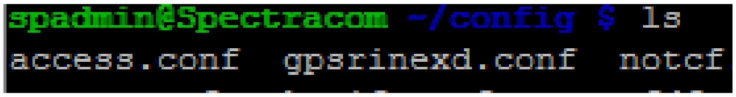
Example from v5.3.1 showing an entry HAS been added to the table (type "***unrestrict***" to clear all entries in the table)



```
spfactory@Spectracom /home/spectracom/config $
spfactory@Spectracom /home/spectracom/config $ cat access.conf
10.2.100.124/16
spfactory@Spectracom /home/spectracom/config $
```

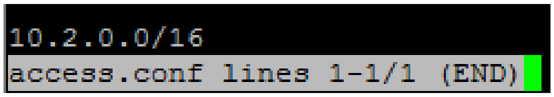
Access configuration storage (from the 1200s. not sure if the same for 2400s)

Access Restriction configuration is in the “access.conf” file (/config directory). The “access.conf” file is only present if Access Restriction configuration has been changed from the factory default settings.



```
spadmin@Spectracom ~/config $ ls
access.conf  gpsrinexd.conf  notcf
```

After adding 10.2.0.0/16 to the Access Restriction page.



```
10.2.0.0/16
access.conf lines 1-1/1 (END)
```

Important note (versions 5.3.0 and below): entering a subnet value of “**/0**” is not valid. It will cause Apache to crash and prevent access to the browser. In software versions 5.3.0 and below, the browser doesn’t prevent a user from inadvertently entering this value (Refer to Mantis case 3110). Version 5.3.1 update prevents the ability to accept this value.

Base unit has one 10/100 Management port with Option Card (Model 1204-06) providing 10/100/1000 base-T network connections).

Purpose of Management/Access: Provides capability to restrict all management functionality (such as the web browser, telnet, FTP, etc) access to desired ports, with the exception of NTP

Note: Access applies to all network ports (Eth0, Eth1, Eth2 and Eth3)

Note: CLI command (“**unrestrict**”) to clear the Access table. no need to clean all configurations. This can be performed via the CLI- it’s not available via the keypad (it’s not in the front panel “Cmd” menu).

Email from Dave Sohn (2 Apr 2013) There is an error on the datasheet. There is no current mechanism to enable/disable management by individual ports. However, network access controls can be setup by IP address range to limit unit accessibility.

All network functionality including management and NTP is available from any interface.

For your information, "Mgmt" (Management) is the ability to enable or disable all management services (such as HTTP/HTTP/telnet, FTP, etc) from one or more of the SecureSync’s Ethernet ports, thereby allowing only NTP functionality on that particular Ethernet port. It is primarily intended for those SecureSyncs with the available Gigabit multi-port Ethernet Option Cards (Model 1204-06) installed in the SecureSync. This Option Card adds an additional three network ports to the SecureSync (in addition to the standard base unit Ethernet port that is installed in every SecureSync).

The Management feature allows one or more network port/clients to be assigned SecureSync management capabilities, while all other network ports or PCs can only access the appliance via NTP. This available functionality is configured in the "Network"/"General Setup" page, "Access" tab, in the SecureSync’s web browser. This functionality is also referred to as “Access Restriction” because it provides the means to block access to PCs that are not listed in this Access table.

By factory default and as long as the table in the "Access" tab remains empty, all network ports/clients are able to access the SecureSync, using any enabled service (as configured in the "Services" tab on this same page of the web browser). If a service is enabled in the Services Tab, and the Access tab has nothing configured in it, all port/clients can access SecureSync using that particular service (if a service is disabled, it's automatically not allowed on any network port).

The Ethernet ports themselves (“Eth0”, “Eth1”, “Eth2” and “Eth3”) are not directly configured to restrict access by the port name/number. Instead, each port is indirectly restricted by its applicable IP addresses. For example, if the network connector “Eth1” is connected to a network with IP addresses of 192.168.1.x, if the 192.168.1.x network is not listed in the Access table (and if the Access table has any other values entered), the PCs that are connected to port “Eth1” will not have access to the management functions of SecureSync.

As shown in the left screenshot below, all of the “management services” are enabled (Daytime and Time protocols are not management protocols) and no clients or subnets have been configured to “allow” access via any of the management services (as shown in the right screenshot below), this indicates that any computer that can see this SecureSync can utilize any of the enabled services (assuming they know the login password, of course).

However, If its desired to prevent/block all services except NTP on a particular port or to most clients, you configure the network address(es) that you want to allow all enabled services to be able to be accessed from, in the Access table. Then, if a network address is not listed in the Access tab, that network or particular PC will not have any access to SecureSync, other than NTP (it has to be listed to be able to access the SecureSync. The Access can be configured to allow an individual PC/client access or an entire subnet to have access to SecureSync.

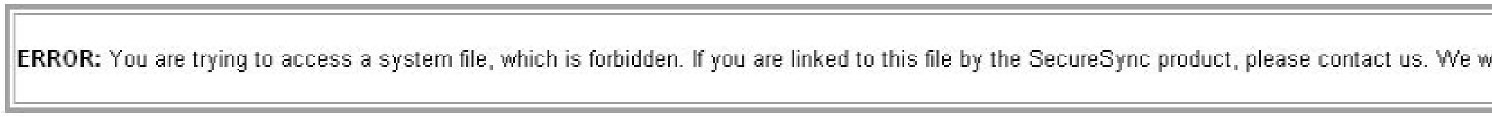
To allow only specific IP addresses to have management capability, just list each desired IP address (that you wish to have management access) in individual “Allow From” fields. If a PC is not one if the configured IP addresses, it will not have management capability.

Configuring an entire subnet to have management capability uses CIDR notation (Classless Inter-Domain Routing) in each “Allow From” field. This format consists of the first IP address in the subnet, followed by a slash (“/”). The slash is then followed by a number representing the subnet mask. For more information on CIDR notation, refer to http://en.wikipedia.org/wiki/CIDR_notation. Contact your network administrator to obtain the CIDR notation for the desired subnet, if you are not sure what this value should be.

An example of this CIDR formatting is: “192.168.0.0/24”. If this example was to be added to an “Allow From” field in the Access table, the entire 192.168.0.0 network would then have management access. If it was the only entry listed in the Access table, the only computers that could then access the SecureSync would be the computers on the 192.168.0.0 network.

Caution: Entering an incorrect value in the Access table can potentially result in all network PCs being locked out of the SecureSync’s web browser. If at least one undesired value is entered into the Access table and the configured value(s) due not correspond to the networks that are connected to SecureSync (none of the configured values in the Access table correlate to the networks that are connected to SecureSync), a PC will need to be directly connected to SecureSync (set the IP address of the stand-alone computer to a static IP address that was entered into the table. Otherwise, to regain access to the web browser, use the front panel CLI port to perform a “clean” (resets all of the SecureSync configurations back to the factory default values). **Note**: An automatic reboot is performed when performing a Clean command.

The following error message is displayed if the PC has restricted access to the SecureSync, because of the Access table configuration. (“You are trying to access a system file, which is forbidden…”



ERROR: You are trying to access a system file, which is forbidden. If you are linked to this file by the SecureSync product, please contact us. We w

**VLANs/VLAN tagging (IEEE 802.1Q)

Software support for VLANs: added in version 1.4.2

- As of at least versions 1.6.0 and below, PTP over a VLAN interface is not currently functional.
  - Per the 1.6.0 release Notes: *PTP over a VLAN interface is not currently functional (from 1.4.1)*

- Link to info on IEEE 802.1Q (regarding VLANS) https://en.wikipedia.org/wiki/IEEE_802.1Q

In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a **virtual local area network**, **virtual LAN** or **VLAN.**

Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections. Most enterprise-level networks today use the concept of virtual LANs. Without VLANs, a switch considers all interfaces on the switch to be in the same broadcast domain.

Portions of the network which are VLAN-aware (i.e., IEEE 802.1Q conformant) can include VLAN tags. When a frame enters the VLAN-aware portion of the network, a tag is added to represent the VLAN membership of the frame's port or the port/protocol combination, depending on whether port-based or port-and-protocol-based VLAN classification is being used. Each frame must be distinguishable as being within exactly one VLAN. A frame in the VLAN-aware portion of the network that does not contain a VLAN tag is assumed to be flowing on the native (or default) VLAN.

802.1Q does not encapsulate the original frame. Instead, for Ethernet frames, it adds a 32-bit field between the source MAC address and the EtherType/length fields of the original frame, leaving the minimum frame size unchanged at 64 bytes (octets) and extending the maximum frame size from 1,518 bytes to 1,522 bytes (for the payload a 42-octet minimum applies when 802.1Q is present; when absent, a 46-octet minimum applies. IEEE 802.3-2005 Clause 3.5). Two bytes are used for the tag protocol identifier (TPID), the other two bytes for tag control information (TCI). The TCI field is further divided into PCP, DEI, and VID.[3]

ACS / AAA / Secure ACS (Cisco standards) protocols / environments.

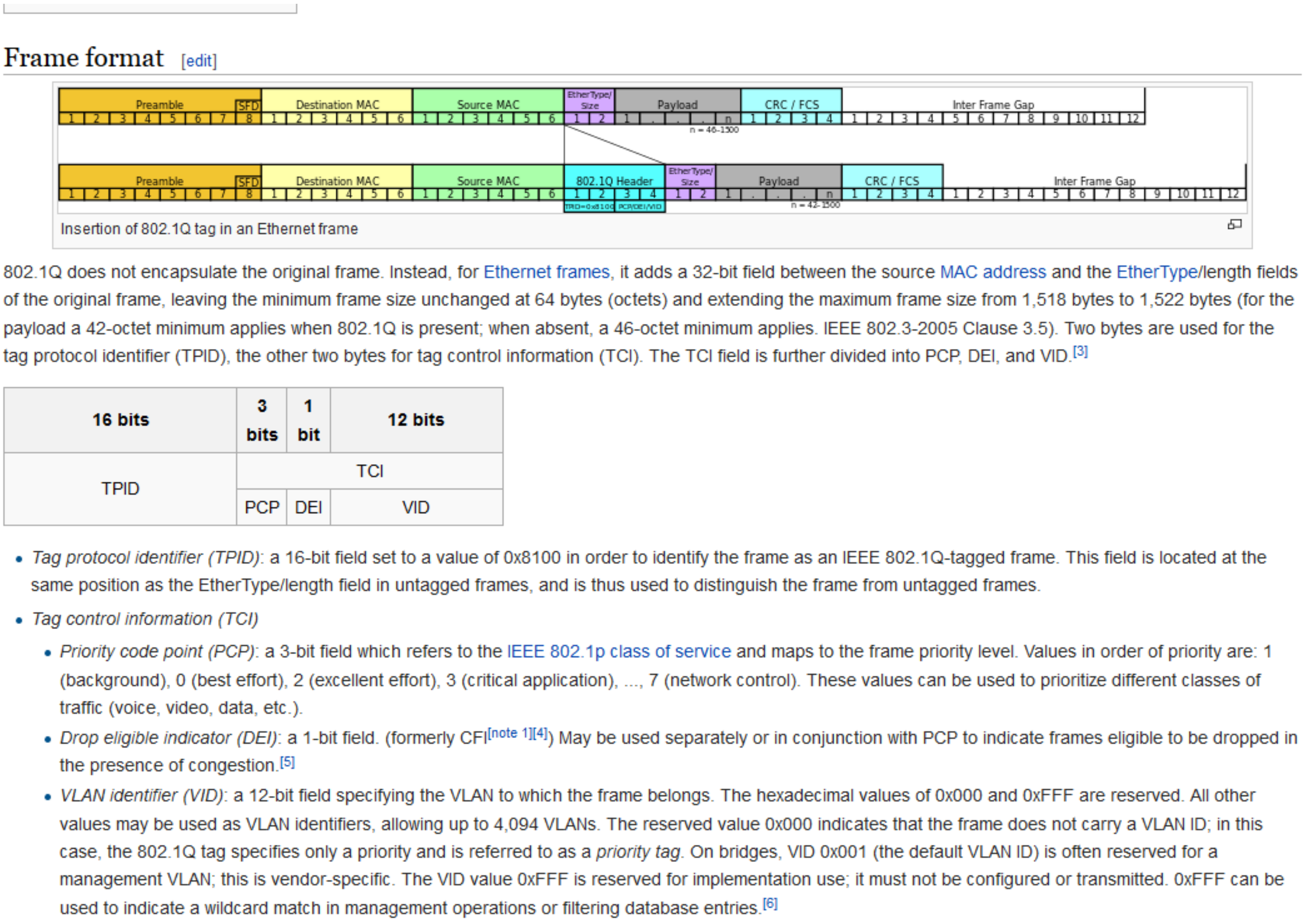
Q. **(From George Bown)** Aimil our Indian partner are asking if SecureSync NTP server can work in ACS / AAA / Secure ACS (Cisco standards) protocols / environments.
Reply from Keith (2 Feb 2015) Though the SecureSync supports its own network access restriction, I don't believe it supports Cisco AAA/ACS. It appears that special software is required to support this capability; I do know that the SecureSync has no special software installed to support it. So this is why I don't believe we support it.

I have copied in Dave Sohn to confirm this, and also just so he is aware of the request to be able to support it.

FYI- Below is information regarding the SecureSync's/9400 series access restriction…

VLANs/VLAN FRAMING/VLAN TAGGING

- ➢ Note info below is from https://en.wikipedia.org/wiki/IEEE_802.1Q



Frame format [edit]

Insertion of 802.1Q tag in an Ethernet frame

802.1Q does not encapsulate the original frame. Instead, for Ethernet frames, it adds a 32-bit field between the source MAC address and the EtherType/length fields of the original frame, leaving the minimum frame size unchanged at 64 bytes (octets) and extending the maximum frame size from 1,518 bytes to 1,522 bytes (for the payload a 42-octet minimum applies when 802.1Q is present; when absent, a 46-octet minimum applies. IEEE 802.3-2005 Clause 3.5). Two bytes are used for the tag protocol identifier (TPID), the other two bytes for tag control information (TCI). The TCI field is further divided into PCP, DEI, and VID.[3]

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID

- *Tag protocol identifier (TPID)*: a 16-bit field set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame. This field is located at the same position as the EtherType/length field in untagged frames, and is thus used to distinguish the frame from untagged frames.
- *Tag control information (TCI)*
  - *Priority code point (PCP)*: a 3-bit field which refers to the IEEE 802.1p class of service and maps to the frame priority level. Values in order of priority are: 1 (background), 0 (best effort), 2 (excellent effort), 3 (critical application), ..., 7 (network control). These values can be used to prioritize different classes of traffic (voice, video, data, etc.).
  - *Drop eligible indicator (DEI)*: a 1-bit field. (formerly CFI[note 1][4]) May be used separately or in conjunction with PCP to indicate frames eligible to be dropped in the presence of congestion.[5]
  - *VLAN identifier (VID)*: a 12-bit field specifying the VLAN to which the frame belongs. The hexadecimal values of 0x000 and 0xFFF are reserved. All other values may be used as VLAN identifiers, allowing up to 4,094 VLANs. The reserved value 0x000 indicates that the frame does not carry a VLAN ID; in this case, the 802.1Q tag specifies only a priority and is referred to as a *priority tag*. On bridges, VID 0x001 (the default VLAN ID) is often reserved for a management VLAN; this is vendor-specific. The VID value 0xFFF is reserved for implementation use; it must not be configured or transmitted. 0xFFF can be used to indicate a wildcard match in management operations or filtering database entries.[6]

VLAN tagged vs untagged

- ➢ Refer to sites such as http://h30499.www3.hp.com/t5/Switches-Hubs-Modems-Legacy-ITRC/Tagged-vs-Untagged/td-p/4004330#.VbZ0hbWnTig

Does SecureSync support VLANS (IEE 802.1Q)?

- ➢ As of at least software version 5.8.2 and below, SecureSync does nothing specific to support VLANS (it is a “non-compliant 802.1 Q device”.
- ➢ VLAN routing is handled by the switch that the SecureSync is plugged into
- ➢ The SecureSync should be connected to an “untagged” port on a VLAN switch.

From: http://www.microhowto.info/tutorials/802.1q.html#idp132208

Trunk and access ports

There are two ways in which a machine can be connected to a switch carrying 802.1Q VLAN traffic:

- via an access port, where VLAN support is handled by the switch (so the machine sees ordinary, untagged Ethernet frames); or
- a trunk port, where VLAN support is handled by the attached machine (which sees 802.1Q-tagged Ethernet frames).

It is also possible to operate a switch port in a hybrid mode, where it acts as an access port for one VLAN and a trunk port for others (so the attached Ethernet segment carries a mixture of tagged and untagged frames). This is not recommended *due to the potential for VLAN hopping (described below).*

Email from Dave Sohn about VLANs

We don't provide any configuration capability to support VLAN-tagging directly on our interfaces. Customer edge switches can still be used to add VLAN tags to traffic from our units as it enters the connected switch ports to support their network needs. Do you have any more information on the customer's application?

Email Keith sent to Ben Cosstick regarding whether SecureSync supports VLANs (27 Jul 2015)

I am by no means an expert with VLANS. But with Dave Sohn out of the office, I'll give you my input on this.

VLAN tagging consists of tags ("frames") added to standard network packets to direct the packets on trunk likes to only certain parts of the network, as handled by the switches. For example, tags (frames) can be applied to only the packets that are intended for the "Engineering Dept".

The SecureSync does not support the addition of VLAN tags/frames to its packets received or transmitted), so the switches outside of the SecureSync decide where to send the traffic on the network based on the destination address (no different than any other network). The switch port that the SecureSync connects to (an untagged port on the switch) strips the framing from all packets that are sent to the SecureSync. So the SecureSync receives a standard packet (no frames) from its switch. If it receives an NTP request from any VLAN, it simply responds to the address that sent the request to the time server. Its switch then routes the packet as necessary.

Because the SecureSync receives packets stripped of the VLAN tags, it can operate with as many VLANs that it can be routed to (the limit has nothing to do with VLANS and their tagging- the limit is based on how many VLANS it can physically get to through the network).

So in summary, as far as the SecureSync is concerned (because it only processes packets stripped of their framing), there is no difference between syncing VLANS and syncing any other network.

Q We also like the multi-port GB module which we hope would allow us to have the timing system on multiple VLANs. Is it possible to run multiple instances of the NTP server on the SecureSync such that different servers can be accessed via different VLANs and ports? We believe this could provide us great benefit within our network architecture design.

A The Gb Ethernet card allows connection to up to 4 different subnets. VLANs are not directly supported via the SecureSync, however, the edge switches the SecureSync connects to can be set up with the appropriate VLANs for your network topology.

Radius (Remote Authentication Dial-In User Service)

- Refer to sites such as https://en.wikipedia.org/wiki/RADIUS
- Refer to the SecureSync I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\LDAP and Radius

Tech notes available for Radius/LDAP

- **SecureSync LDAP / Radius tech note**: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\LDAP and Radius
- **Model 9400 LDAP / Radius tech note** EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\LDAP and Radius

RADIUS RFCs (in this document): **Port assignments and RFCs for all products

OpenRadius: http://sites.e-advies.nl/openradius/

Shortcut to SecureSync LDAP/Radius design info: S:\Projects\Lafayette

Radius

Note: For example engineering software release testing of Radius, in Arena, refer to the ECO of the release (such as ECO 1338 for v5.7.1 https://app.bom.com/changes/detail-summary?change_id=2389346979) to find the PVP Test validation in the list of "ITEMS"

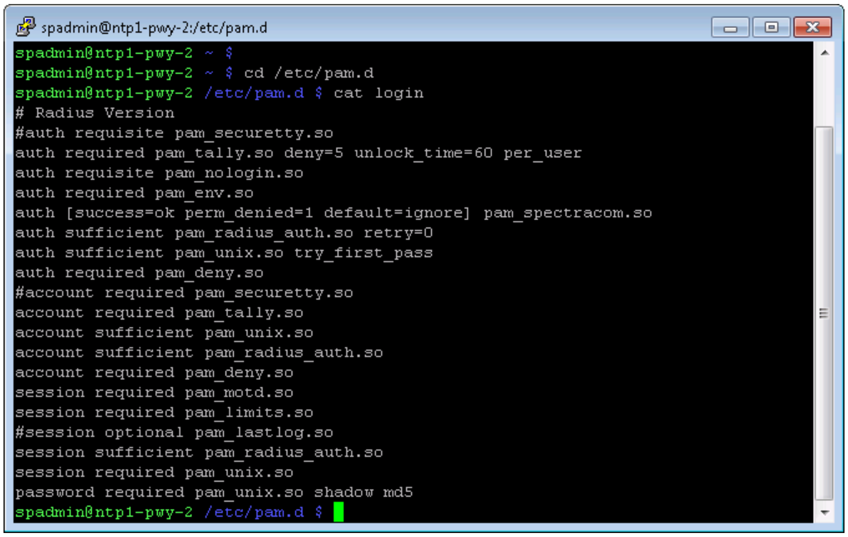
Version-related info for Radius

- 2400 SecureSync software support for Radius: Added in update version 1.1.0a (Feb 2020)

Order of precedence for both Radius and LDAP when logging in (Per Ron)

- Radius authentication is attempted
- LDAP authentication is attempted.
- Local login (accounts in the NTP server).

As indicated: (internal use only) Spectracom/etc/pam.d/radius and type: **cat login**



spadmin@ntp1-pwy-2:/etc/pam.d

```
spadmin@ntp1-pwy-2 ~ $
spadmin@ntp1-pwy-2 ~ $ cd /etc/pam.d
spadmin@ntp1-pwy-2 /etc/pam.d $ cat login
# Radius Version
#auth requisite pam_securetty.so
auth required pam_tally.so deny=5 unlock_time=60 per_user
auth requisite pam_nologin.so
auth required pam_env.so
auth [success=ok perm_denied=1 default=ignore] pam_spectracom.so
auth sufficient pam_radius_auth.so retry=0
auth sufficient pam_unix.so try_first_pass
auth required pam_deny.so
#account required pam_securetty.so
account required pam_tally.so
account sufficient pam_unix.so
account sufficient pam_radius_auth.so
account required pam_deny.so
session required pam_motd.so
session required pam_limits.so
#session optional pam_lastlog.so
session sufficient pam_radius_auth.so
session required pam_unix.so
password required pam_unix.so shadow md5
spadmin@ntp1-pwy-2 /etc/pam.d $
```

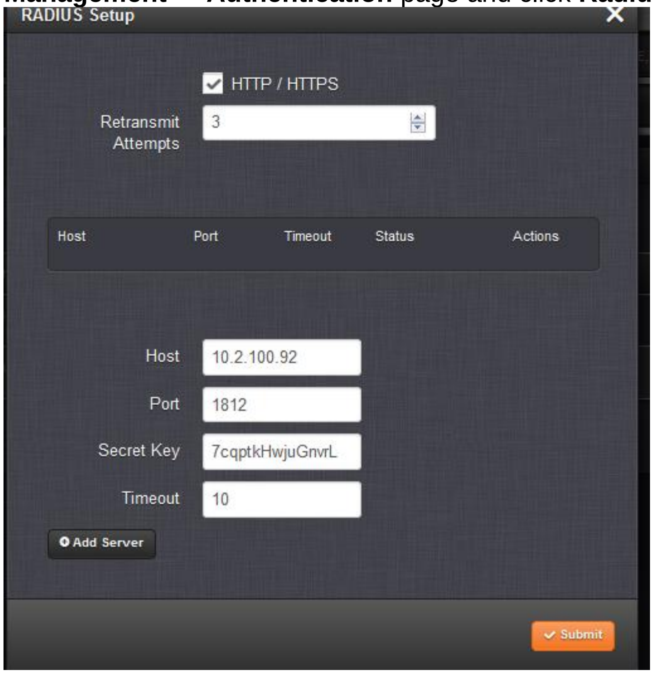
***Our Radius server in Rochester

Set up and maintained by the IT team

Note: For example engineering software release testing of Radius, in Arena, refer to the ECO of the release (such as ECO 1338 for v5.7.1 https://app.bom.com/changes/detail-summary?change_id=2389346979) to find the PVP Test validation in the list of "ITEMS"

For testing, use our server with an IP address of 10.2.100.177
Note: SecureSync has to be configured for a specific static IP address to work- **~~10.10.30.10~~ 10.2.100.177**

Management -> **Authentication** page and click **Radius**



RADIUS Setup

☑ HTTP / HTTPS

Retransmit Attempts: 3

Host	Port	Timeout	Status	Actions

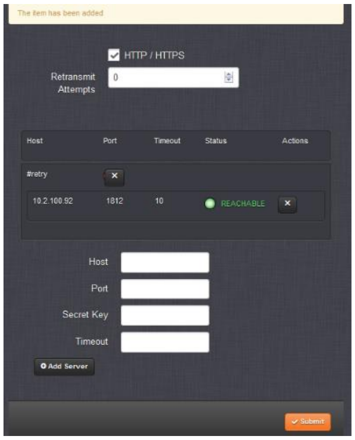
Host: 10.2.100.92

Port: 1812

Secret Key: 7cqptkHwjuGnvrL

Timeout: 10

Check “HTTP/HTTPS” box
Retransmit attempts= 3
Host= 10.2.100.31
Port= 1812
Radius Secret key: 7cqptkHwjuGnvrL
Timeout = 10
Click “Add Server”



The item has been added

☑ HTTP / HTTPS

Retransmit Attempts: 0

Host	Port	Timeout	Status	Actions
#retry	✕			
10.2.100.92	1812	10	● REACHABLE	✕

Host:
Port:
Secret Key:
Timeout:

Login info
Username: ~~keith~~ oleg
password: password (all lowercase)

General info on Radius

***Radius Authentication versus Radius accounting

- Radius authentication (RFC 2865) provides remote authentication for connections (this is what we support)
- Radius accounting (RFC 2866) is often used for billing purpose

RADIUS accounting consists of an accounting server and accounting clients (PortMasters). The radiusd daemon for accounting is a child process of the radiusd authentication daemon; it starts automatically when radiusd is executed.

Radius authentication messages

A RADIUS message consists of a RADIUS header and zero or more RADIUS attributes. Each RADIUS attribute specifies a piece of information about the connection attempt. For example, there are RADIUS attributes for the user name, the user password, the type of service requested by the user, and the IP address of the access server. RADIUS attributes are used to convey information between RADIUS clients, RADIUS proxies, and RADIUS servers

Note: For additional info on attributes, refer to: https://en.wikipedia.org/wiki/Radius_Values

- **Access-Request**
  Sent by a RADIUS client to request authentication and authorization for a connection attempt.
- **Access-Accept**
  Sent by a RADIUS server in response to an Access-Request message. This message informs the RADIUS client that the connection attempt is authenticated and authorized.
- **Access-Reject**
  Sent by a RADIUS server in response to an Access-Request message. This message informs the RADIUS client that the connection attempt is rejected. A RADIUS server sends this message if either the credentials are not authentic or the connection attempt is not authorized.

- **Access-Challenge**
  Sent by a RADIUS server in response to an Access-Request message. This message is a challenge to the RADIUS client that requires a response.

UDP Port 1813 (Radius accounting/ accounting messages)

- RADIUS accounting logs information about dial-in connections. This information is often used for billing purposes.
- With our Radius client configured to use port 1812, there are no messages sent/received on port 1813 (using tcpdump).

Radius authentication

Radius Extensions for OpenRadius (RFC 2869)

Extensible Authentication Protocol (EAP / (EAP-Message and Message-Authenticator)
Refer to RFC 2869 http://datatracker.ietf.org/doc/rfc2869/?include_text=1 (excerpt below)
The Extensible Authentication Protocol (EAP), provides a standard mechanism for support of additional authentication methods within PPP. Through the use of EAP, support for a number of authentication schemes may be added, including smart cards, Kerberos, Public Key, One Time Passwords, and others. In order to provide for support of EAP within RADIUS, two new attributes, **EAP-Message** and **Message-Authenticator**, are introduced.

FreeRadius support of EAP/ Refer to http://freeradius.org/features/eap.html
FreeRadius Message Authenticator attribute: http://freeradius.org/rfc/rfc2869.html#Message-Authenticator

Radius Attributes: RADIUS Attributes carry the specific authentication, authorization, information and configuration details for the request and reply.

Attributes defined in RFC 2869 include "User-Name", "Vendor-specific", "CHAP-Challenge", "framed", "Login", "NAS" and several others. Refer to **Section 5** at http://freeradius.org/rfc/rfc2869.html#Message-Authenticator)

**Radius with IPv6 addresses

Mantis case 1722: No current support for IPV6 Radius

- Applicable to at least versions 5.2.0 and below

Update to this case (4 Apr 2013) Per Dave Sohn: The pam_auth_radius module we use does not support IPv6. There is an IPv6 patch for it that would need to be tested. So the answer is we do not support IPv6 RADIUS at this time.

(3/23/11) Software versions 4.4.0 and earlier, LDAP and Radius authentication only work with the web browser login. Neither LDAP nor Radius worked with the other login services (SSH, telnet, etc). Unlike NetClock, no local user account needs to be created in the box to use LDAP or Radius.

With software version 4.5.0, we're adding LDAP authentication to all login services. However, Radius login is still restricted to just the web browser login. The other services (telnet, ssh, etc) will still require logging into a local account stored on the box, as we can't make Radius login available on the other login services.

Archive Version 4.8.0 removed the enabling of Radius with the CLI interfaces.

Note: SecureSync requires commas "," as separators between values. It can't accept periods "." as separators.

Email from Dave Sohn 11/21- regarding Radius w/web browser only: RADIUS is only utilized for authentication for HTTP/HTTPS because of a limitation at the time with the security package we were using for managing logins to the system. The RADIUS plugin only allowed it to be used for authentication against HTTP/HTTPS. RADIUS is probably low on the list for resolving issues, when looking at its usage and our resource utilization.

Notes about the need for User accounts and passwords being created/stored in SecureSync

A) LDAP only

Unlike earlier 9200 and 9300 series NetClocks, no User accounts have to be created in the SecureSync in order to use LDAP.

B) Radius only

Unlike earlier 9200 and 9300 series NetClocks, no User accounts have to be created in the SecureSync in order to use Radius with the web browser (HTTP/HTTPS). However, due to technical limitations, Radius user can only login via the Web browser! Other services such as telnet and SSH are not technically available via Radius.

RSA authentication (SecurID)

Unlike with the Model 9200 and 9300 series NetClocks, RSA authentication (SecurID) should be compatible with SecureSync/9400 series NetClocks. However, if a customer has any problems while using RSA authentication, please let Engineering know. See Mike Sander's comments below about this.

Email from Mike Sander

I'm doing the SecureSync Radius app-note and I found the part about:

"RSA authentication requires a different Radius login password be entered when navigating from one page of the web browser to another. Radius requires the password to be the same value when navigating between pages of the browser. Using RSA authentication in conjunction with Radius will result in messages indicating the "password has been changed" being displayed when navigating in the time servers web browser. "

This may not be a problem with SecureSync. NetClock uses the Basic Auth type of Apache web authentication where the password is sent for every web page. We switched to an authentication module called Pamacea. Pamacea uses session files to authenticate across web pages. So the web browser wouldn't be asking RSA for the password every time a page is displayed.

If enough customers ask about RSA we could try it again, maybe it works with Pamacea.

Defining the LDAP/Radius account login permissions (user or admin)

Unlike earlier NetClocks, the SecureSyncs don't need a user account created in the box. So there is no longer a place to configure whether the account has admin or user rights in the NTP server itself. For these units, this needs to be configured in the LDAP or Radius server.

A) LDAP account permissions

For **LDAP**, refer to: "**Specific LDAP Server Configuration"** in the LDAP section of the Radius/LDAP Tech note in the SecureSync folder (pasted below, as well)

Specific LDAP Server Configuration
Follow the instructions specific to your LDAP server(s) to create and modify users in the LDAP server(s).

A SecureSync LDAP user needs the following LDAP fields:

homeDirectory	/home/spectracom
loginShell	/bin/bash
uid	A user name, (not "spadmin")
uidNumber	Use a number outside the range 1000 to 1050
gidNumber	"**admin"** group is "111", "**user**" group is "112" (See the Note below)
userPassword	<password>

Note: "**gidNumber**" defines the permissions for each account, to be either **admin** account or **user** account. User account permissions for configuration capabilities are limited. Many of the web browser fields will be grayed-out when logged into the SecureSync's web browser with an account using the user group.

Active directory permissions (user or admin)

Q. The instructions to setup different permissions levels, that is shown below, doesn't make sense to me. I can not setup a "gidNumber" with my active directory. Maybe these instructions are more Linux based machines? How do I do this is active directory? I will attach a screenshot of all the attributes of a user on my active directory.

A Email from Dave Sohn (19 Mar 2013) "Below is my best effort. I can't guarantee all of this, but I believe this is all accurate."

I believe the information that is requested for the Specific LDAP Server Configuration is independent of Linux or Windows. This needs to be present on both. If the user completes authentication, but an object like the Group ID is missing, then they will default to user privileges. I don't have a Windows Server 2008 installation to look at, but on the Windows Server 2003 I can see these. They need to enable editing/display of UNIX attributes, which means the schema of their Active Directory installation needs to be extended. They should have installed "Identity Management for UNIX" role service installed. You should now see a tab labeled "UNIX Attributes" in the properties for users and groups. The group ID of the domain group used to collect users for the SecureSync management needs to be set to **111 or 112** depending on admin or user privileges. Then for each of the users, you need to setup their UNIX attributes as described and make them a member of that group within the UNIX attributes.

B) Radius account permissions

(8/24/12 KW) For **Radius**, accounts, I'm not sure at this time on how this is defined in the radius server. But since the User accounts don't have to be in the NTP server, it has to be defined somehow in the Radius server itself, similar to how it's done with LDAP.

Note: Information below is not yet confirmed to be correct (but may work). I haven't added this to the LDAP/Radius document yet- waiting on some feedback as to if this info is correct. Then, it should be added.

(8/29/12 KW email I sent to Jeremy Halterman with Harris)
As for a FreeRadius Server (a Radius server running open source FreeRadius program), I found the following at http://kb.juniper.net/InfoCenter/index?page=content&id=KB19446&actp=RSS.

It looks like the "Service-Type" (bolded and enlarged below) may define the Login permissions. Login should be defined as "Admin". Refer to this website page for the full context of this information.

RADIUS server configuration:
In this example a freeradius server is used (more info about freeradius at http://freeradius.org/). The following users are configured in the file `/etc/freeradius/users` on the freeradius server:

```
tom Cleartext-Password := "tom123"
Service-Type = Login-User,
Juniper-Local-User-Name := "readonly-users",

jerry Cleartext-Password := "jerry123"
Service-Type = Login-User,
Juniper-Local-User-Name := "super-users",
```

This may work with a FreeRadius Server. If the Radius server isn't running open source software, you may need to contact the Radius server vendor to find out how to edit user account permissions.

******Windows Active Directory / Radius Server / Group policy / Radius clients**

Refer to: http://technet.microsoft.com/en-us/library/dd759205.aspx (Info for Server 2003, Server 2008. Server 2012

Radius Client: http://technet.microsoft.com/en-us/library/cc754033.aspx

***Radius vendor-specific attributes (vendor specific attributes) (VSAs) - Vendor code/Vendor ID

- Refer to Salesforce case 12223

- Refer to https://en.wikipedia.org/wiki/RADIUS

RADIUS is extensible; many vendors of RADIUS hardware and software implement their own variants using Vendor-Specific Attributes (VSAs).

Vendor specific attributes

In addition to the RADIUS standard attributes, which are described in Request for Comments (RFC) 2865 and RFC 2866, you can configure vendor-specific attributes (VSAs) in Network Policy Server (NPS) network policy and connection request policy that are returned to RADIUS clients in RADIUS response messages.

VSAs allow RADIUS client vendors, such as the manufacturers of wireless access points, 802.1X authenticating switches, and devices that act as virtual private network (VPN) servers, to support their own proprietary RADIUS attributes that are not included in the RFCs. NPS includes VSAs from a number of vendors in its dictionary; however, the NPS dictionary does not include VSAs for all vendors.

Some network access server (NAS) manufacturers use VSAs to provide functionality that is not supported in RADIUS standard attributes. NPS enables you to create or edit VSAs to take advantage of proprietary functionality supported by some NAS vendors.

Service-Type attribute

Email from a customer

Thanks for looking into to it for us. We are using Microsoft NPS as our RADIUS. I tried configuring (service-type – Administrative) on the Microsoft side. It looks like it gets sent back to SecureSync with the accept-accept packet, though it has no effect. Not sure if you guys use any vendor specific Attribute-value pairs or not. Our next go was to look at the pam_auth_module that SecureSync uses.

Email from Dave Sohn (28 Oct 2013): I'm not sure that we have any vendor specific attributes, or a vendor ID. See more info here on VSAs. http://technet.microsoft.com/en-us/library/cc754417(v=ws.10).aspx (excerpt below):

Q. We are using Microsoft NPS as our RADIUS. I tried configuring (service-type – Administrative) on the Microsoft side. It looks like it gets sent back to SecureSync with the accept-accept packet, though it has no effect.

Not sure if you guys use any vendor specific Attribute-value pairs or not. Our next go was to look at the pam_auth_module that SecureSync uses.

From RFC 2865

Description
This Attribute indicates the type of service the user has requested, or the type of service to be provided. It MAY be used in both Access-Request and Access-Accept packets. A NAS is not required to implement all of these service types, and MUST treat unknown or unsupported Service-Types as though an Access-Reject had been received instead.

A summary of the Service-Type Attribute format is shown below. The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |             Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
          Value (cont)          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Type    6 for Service-Type.

Length    6
```

The service types are defined as follows when used in an Access- Accept. When used in an Access-Request, they MAY be considered to be a hint to the RADIUS server that the NAS has reason to believe the user would prefer the kind of service indicated, but the server is not required to honor the hint.

Login The user should be connected to a host.

Framed A Framed Protocol should be started for the User, such as PPP or SLIP.

Callback Login The user should be disconnected and called back, then connected to a host.

Callback Framed The user should be disconnected and called back, then a Framed Protocol should be started for the User, such as PPP or SLIP.

Outbound The user should be granted access to outgoing devices.

Administrative The user should be granted access to the administrative interface to the NAS from which privileged commands can be executed.

NAS Prompt The user should be provided a command prompt on the NAS from which non-privileged commands can be executed

Authenticate Only Only Authentication is requested, and no authorization information needs to be returned in the Access-Accept (typically used by proxy servers rather than the NAS itself).

Callback NAS Prompt The user should be disconnected and called back, then provided a command prompt on the NAS from which non-privileged com*m*ands can be executed.

Call Check: Used by the NAS in an Access-Request packet to indicate that a call is being received and that the RADIUS server should send back an Access-Accept to answer the call, or an Access-Reject to not accept the call. Typically based on the Called-Station-Id or Calling-Station-Id attributes.

802.1x authentication (Encapsulation of EAP – also called EAPOL)

- As of at least software versions 5.1.4 and below, SecureSync does not support 802.1x
- It's a part of freeradius, but we don't have the Supplicant application software to support it.
- Radius server handles the certificates –SecureSync is just a supplicant.
- SecureSync would need third-party application software installed to make it a Supplicant. Refer to the following link for good info on this software:

http://www.nowiressecurity.com/articles/third-party_80211x_client_supplicant.htm

From Wikipedia (http://en.wikipedia.org/wiki/IEEE_802.1X)
IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

Requires both Radius and EAP (http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol)

IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802[1][2] which is known as "EAP over LAN" or EAPOL

With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network

Q. Do we support 802.1x authentication?

A. Email from Ron Dries (8 July 2014) referring to at least version 5.1.4 software

FreeRadius does support 802.1x but the configuration for that is at the server level not the client. The Radius authentication server gets configured for 802.1x and generates the certificates.

However the SecureSync is not the authentication server, but a client. It appears in the 802.1x standard the SecureSync would be considered a supplicant, a device that requires authentication. For this it would need a supplicant application, i.e. Xsupplicant, installed and would need to be configured correctly for 802.1x.

So currently we do not support this feature, because we do not have the ability to make the SecureSync a supplicant.

I hope I was able to answer your question, if you have any further questions please let me know.

A. older Email from Mike Sander (2/2/12)

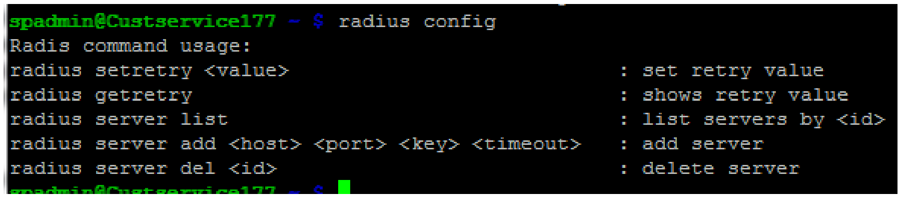
We don’t support 802.1x authentication. It can be added to RADIUS, but we don’t currently support it. It looks like a significant effort, adding packages to Linux, and supporting a new kind of certificate.

***Radius configuration

- **online SecureSync user guide**: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/RADIUS_Auth.htm

A) Configuration via CLI interface commands

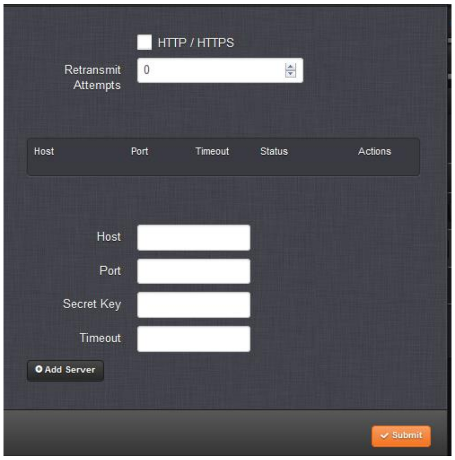
- Not sure which software version these were added in (possibly v5.1.7??)
- Type **radius** <enter> to view the list of all radius commands



```
spadmin@Custservice177 ~ $ radius config
Radis command usage:
radius setretry <value>                               : set retry value
radius getretry                                       : shows retry value
radius server list                                    : list servers by <id>
radius server add <host> <port> <key> <timeout>       : add server
radius server del <id>                                : delete server
spadmin@Custservice177 ~ $
```

B) Configuration via web browser

Management -> ***Authentication*** page of the browser. Click "**Radius Setup**" button on left side of page



□ HTTP / HTTPS

Retransmit Attempts: 0

Adding/Removing a RADIUS Server

To add a RADIUS authentication server, or remove a server from the list:

1. Navigate to MANAGEMENT > OTHER: Authentication.
2. In the Actions panel on the left, click RADIUS Setup. The RADIUS Setup window will be displayed:

- Host: The hostname or IP address of the RADIUS server
- Port: Defines the RADIUS Port to use. The default RADIUS Port is 1812, but this can be changed, as required.
- Secret Key: The secret key which is shared by SecureSync and the RADIUS server (the key is used to generate an MD5 hash).

- Timeout: [seconds] Defines the Timeout that SecureSync will wait to communicate with the RADIUS server e.g., 10 seconds.

3. Click the Add Server button. A confirmation message The item has been added will be displayed if the server could be added, nd the server will be added to the list, indicating its status (more info directly below)

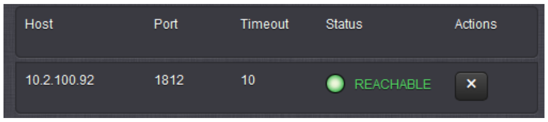
"Status" field

The "**Status**" field in the row with the configured Radius server will report whether Radius is currently enabled and if the SecureSync can successfully reach that particular Radius server, as described below:

- REACHABLE: This RADIUS server can be reached.

indicates the **HTTP/HTTPS** checkbox at the top of the Radius Setup menu is currently selected (Radius is enabled) and the SecureSync can successfully reach the Radius Server. Note that "Reachable" does not show that the Secret Key has been entered correctly.   It just shows it can see that the Radius server is on the network with the SecureSync. The Secret Key is verified by successfully logging in to the web browser using a Radius account.

Status reports REACHABLE

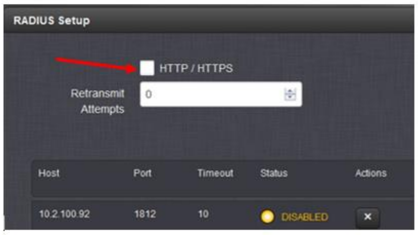


Host	Port	Timeout	Status	Actions
10.2.100.92	1812	10	● REACHABLE	×

- DISABLED: RADIUS service is disabled.

indicates the **HTTP/HTTPS** checkbox at the top of the Radius Setup menu isn't currently selected. Press the "Radius Setup" button the left side of the page and select the HTTPS/HTTPS checkbox at the top of the "Radius Setup" menu. Then press Submit.

HTTP/HTTPS checkbox not selected



RADIUS Setup

□ HTTP / HTTPS

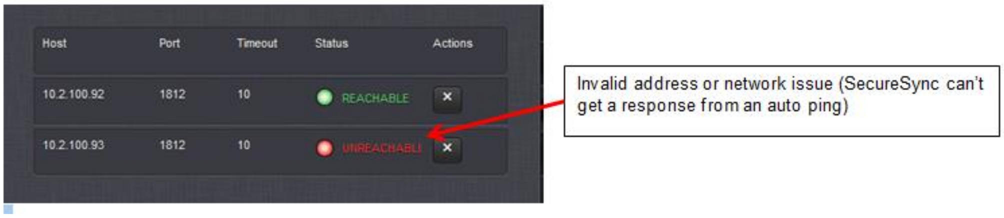
Retransmit Attempts: 0

Host	Port	Timeout	Status	Actions
10.2.100.92	1812	10	● DISABLED	×

- UNREACHABLE: This RADIUS server cannot be reached.

indicates a Radius server that the SecureSync is not able to communicate with. The Host address may not be correct or the Radius server may not be on the same network as the SecureSync.

Radius Server unreachable



Host	Port	Timeout	Status	Actions
10.2.100.92	1812	10	● REACHABLE	×
10.2.100.93	1812	10	● UNREACHABLE	×

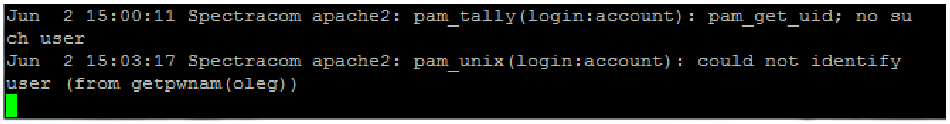
Invalid address or network issue (SecureSync can't get a response from an auto ping)

Note: See Radius troubleshooting on diagnosing this condition.

Successful Radius login:

Auth log

- ➢ Successful Radius login



```
Jun  2 15:00:11 Spectracom apache2: pam_tally(login:account): pam_get_uid; no su
ch user
Jun  2 15:03:17 Spectracom apache2: pam_unix(login:account): could not identify
user (from getpwnam(oleg))
```

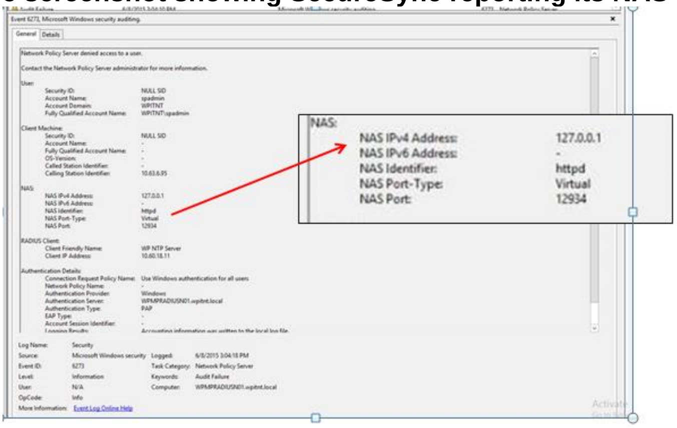
Radius known issues/troubleshooting

- ➢ Refer to LDAP/Radius doc: [..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\LDAP and Radius]()

Known issues with Radius

1) **NAS address**: Are they possibly using the NAS address as a second layer of authentication (allowing only certain devices to be able to even contact the Radius server). Microsoft found our NAS address was being outputted in v5.2.0 and below as 127.0.0.1 which was blocking the SecureSync from even trying to authenticate (instead of it being the IP address of the SecureSync). This is expected to be addressed in 5.2.1. Refer to Mantis case 3017 and Salesforce case

Example screenshot showing SecureSync reporting its NAS address as its loop back address instead:



```
Event 6273, Microsoft Windows security auditing.

General | Details

Network Policy Server denied access to a user.

Contact the Network Policy Server administrator for more information.

User:
        Security ID:                        NULL SID
        Account Name:                       spadmin
        Account Domain:                     WPITNT
        Fully Qualified Account Name:       WPITNT\spadmin

Client Machine:
        Security ID:                        NULL SID
        Account Name:                       -
        Fully Qualified Account Name:       -
        OS-Version:                         -
        Called Station Identifier:          -
        Calling Station Identifier:         10.63.6.95

NAS:
        NAS IPv4 Address:                   127.0.0.1
        NAS IPv6 Address:                   -
        NAS Identifier:                     httpd
        NAS Port-Type:                      Virtual
        NAS Port:                           12934

RADIUS Client:
        Client Friendly Name:               WP NTP Server
        Client IP Address:                  10.60.18.11

Authentication Details:
        Connection Request Policy Name:     Use Windows authentication for all users
        Network Policy Name:                -
        Authentication Provider:            Windows
        Authentication Server:              WPMPRADIUSN01.wpitnt.local
        Authentication Type:                PAP
        EAP Type:                           -
        Account Session Identifier:         -
        Logging Results:                    Accounting information was written to the local log file.

Log Name:        Security
Source:          Microsoft Windows security   Logged:         6/8/2015 3:04:18 PM
Event ID:        6273                         Task Category:  Network Policy Server
Level:           Information                  Keywords:       Audit Failure
User:            N/A                          Computer:       WPMPRADIUSN01.wpitnt.local
OpCode:          Info
More Information: Event Log Online Help
```

```
NAS:
        NAS IPv4 Address:       127.0.0.1
        NAS IPv6 Address:       -
        NAS Identifier:         httpd
        NAS Port-Type:          Virtual
        NAS Port:               12934
```

Details about the NAS address

- If the SecureSync can’t find a DNS server, its NAS address will remain its loopback address of “127.0.0.1”
- If the SecureSync finds a DNS server, the SecureSync will then change its NAS address to the IP address it receives from the DNS server (which is the IP address that has been mapped to its hostname within the DNS server).

If the NAS address is the wrong address for the SecureSync and as long as it’s not still 127.0.01 (indicating an issue with the SecureSync finding the DNS server) the DNS server needs to be checked to ensure the SecureSync’s hostname has been mapped to the correct IP address. The SecureSync just reports the NAS as the address it gets from the DNS.
Note: Valid LDAP logins do not result in any User or Auth log entries.

A) General Radius troubleshooting

Radius troubleshooting tips/summary

1. Check software version installed:
2. refer to Radius/LDAP tech note
3. get full logs/configs bundles (review especially the Auth, Journal and User logs. More info further below)

4. Review Radius config files (more info futher below)
5. Try momentarily disabling and re-enabling Radius. Then logout of the browser and try logging in again using credentials only in the Radius server.
6. get a wireshark/tcpdump capture (more info futher below)

   Use **tcpdump** to see the request and accept messages (see info further above) Make sure the packets are on the correct Ethernet interface to be able to reach the Radius server.

7. Is HTTP/HTTPS checkbox at the top of the **Management** -> **Radius Setup** config page selected?
8. Is the Radius Setup page showing the Radius server is "reachable" (responding to ping)
9. Any firewalls in between with TCP ports 1812, 1813 or 3799 closed?
10. Delete and re-enter the Radius server(s) using an intentionally wrong shared secret key and grab the logs. See if the System log contains the following entry **pam_radius_auth: packet from RADIUS server 10.82.122.16 fails verification: The shared secret is probably incorrect.** This entry indicates the SecureSync is communicating with the Radius server.
11. Re-enter the Radius server using the correct Shared secret key and try logging in.

Draft email for initial troubleshooting

In order for us to be able to better assist you with getting Radius login to the web browser working, please:

If it's not accessible, please send a copy of the response to the following CLI command: version <enter> to show the current version of software.

Send us a screenshot of the Management -> Authentication page, Radius Setup button in the browser (if it's still accessible).
A full copy of all the unit's logs for our review (via the CLI interface command and FTP/SCP, if you aren't able to access the browser any longer using the spadmin account)

Logs

- ➢ get logs/configs bundles (review especially the Auth and Uuser logs
- ○ **View Auth log Via CLI:** Spectracom/home/spectracom/log and then type **cat auth.log**

To obtain all of the logs via the web browser (if it's still accessible):
All of the SecureSync's logs (including those shown in the browser and also those in the background) can be easily bundled into one file and then exported from the SecureSync to send as an attachment.

Instead of copy/pasting all of the log entries into a Word document, starting in Archive software update version 5.1.2, the logs can be easily saved to single bundled file and exported into a networked PC. Earlier versions of software allowed the bundle to be created, but then the file still needed to be transferred out using an FTP/SCP connection. Now, a button in the web browser alleviates the need to create an FTP session to transfer this file out to a PC.

The log bundling and export to a PC is controlled in the "**Management" -> "Log Configuration"** page of the SecureSync's web browser. On the left-side of the browser, click on the "**Save and download all logs**" button. You can then select where to save the log bundle to. The default file name is "securesync.log".

To obtain all the logs via the CLI interface if the browser is not accessible

1) Login the CLI interface via telnet or ssh.
2) Type **savelog** SecureSync <enter>
3) Login to the CLI interface using an FTP or SFP utility and navigate to the following directory**: /Home/Spectracom/Xfer/Log**
4) Transfer out this log file and send it to us as an attachment. Note that you may need to zip the file due to its size.

Example user.log log entries (connection to radius server issues)

1) No Radius servers found

```
apache2: pam_radius_auth: No RADIUS server found in configuration file /etc/raddb/server
```

Cause: No Radius servers have been configured. Need at least one server to be added. Verify configuration of the **Management** -> **Authentication** page of the browser. Click “**Radius Setup**” on the left side of the page.

2) Servers failed to respond

```
apache2: pam_radius_auth: RADIUS server 10.2.100.92 failed to respond
apache2: pam_radius_auth: All RADIUS servers failed to respond
```

Cause: Invalid Radius server address(es) or network issue exists. Verify configuration of the **Management** -> **Authentication** page of the browser. Click “**Radius Setup**” on the left side of the page.

3) Shared secret key is incorrect

```
apache2: pam_radius_auth: packet from RADIUS server 10.2.100.92 fails verification: The shared secret is probably incorrect.
apache2: pam_radius_auth: All RADIUS servers failed to respond.
```

Cause: Valid server, valid port, **but wrong Secret Key** entered in Radius configuration. Verify configuration of the **Management** -> **Authentication** page of the browser. Click “**Radius Setup**” on the left side of the page.

Example auth.log log entries (authentication with radius server issues)

Note: to see the latest entry of the user log: **tail –f log/auth.log** (or change to the log directory and then type): **tail –f auth.log**)

Cause: invalid Radius server address

```
Sep 12 21:54:19 CustService-176 unix_chkpwd[6256]: password check failed for user (oleg)
Sep 12 21:54:19 CustService-176 apache2: pam_unix(httpd:auth): authentication failure; logname= uid=1001 euid=1001 tty= ruser=
rhost=10.2.100.124  user=oleg
Sep 12 21:54:19 CustService-176 apache2: pam_tally(httpd:auth): conversation failed
Sep 12 21:54:19 CustService-176 apache2: pam_tally(httpd:auth): user oleg (1052) tally 15, deny 5
```

Cause: wrong username and ambiguous password

```
Sep 12 21:47:19 CustService-176 apache2: pam_securetty(httpd:auth): cannot determine user's tty
Sep 12 21:47:19 CustService-176 apache2: pam_unix(httpd:auth): check pass; user unknown

Sep 12 21:47:19 CustService-176 apache2: pam_unix(httpd:auth): authentication failure; logname= uid=1001 euid=1001 tty= ruser=
rhost=10.2.100.124
Sep 12 21:47:19 CustService-176 apache2: pam_tally(httpd:auth): pam_get_uid; no such user
```

Cause: right username but wrong password

```
Sep 12 21:44:09 CustService-176 unix_chkpwd[30024]: password check failed for user (oleg)
CustService-176 apache2: pam_unix(httpd:auth): authentication failure; logname= uid=1001euid=1001 tty= ruser=
rhost=10.2.100.124  user=oleg
CustService-176 apache2: pam_tally(httpd:auth): conversation failed
CustService-176 apache2: pam_tally(httpd:auth): user oleg (1052) tally 11, deny 5
```

Cause: right server IP address, but wrong port number configured

```
Sep 12 21:59:00 CustService-176 unix_chkpwd[25159]: password check failed for user (oleg)
Sep 12 21:59:00 CustService-176 apache2: pam_unix(httpd:auth): authentication failure; logname= uid=1001 euid=1001 tty= ruser=
rhost=10.2.100.124  user=oleg
```

Questions that may help determine the cause of this issue:

1) Just to confirm, all three units have the same Archive version 4.8.4 software installed (as indicated on the Tools/Versions page)?
2) Are all three Model 9483s, at least temporarily, placed on the same subnet? (for instance, are you putting each one individually on the network, using the same IP address for each NTP server, or plugging all three into the same subnet at the same time by using different IP addresses)? Or, instead, are they located on different subnets or different networks altogether?
3) If they are installed in different subnets or isolated networks, have you tried swapping the one unit with either of the other two to see if the issue follow
4) Are there any firewalls between the Radius server and the NTP servers?
5) Just to confirm, all the Radius configurations in the Network/ Radius Setup page of the browser (in both the "General Settings" and "Server Configuration" tabs) are exactly the same in all three time servers?
6) Is the table located in the Network/General Setup page of the browser, "Access" tab, empty in all of the units?
7) Do the three units you received have this available Option Card installed? Or, is there only one network port on the back of each of the three units?
8) If this Option Card is installed, is the network connected to the base Ethernet port on the main chassis, or one of the three ports on the installed Option Card installed on the Option Bay?
9) With this Model 9483 connected to the network and Radius not working, have you tried to ping, telnet, FTP or SSH in (which will all indicate whether the specific port is operational). If not, I recommend first trying to ping and then telnet into the NetClock's address, via the command prompt window, or ssh or ftp in using an ssh/ftp program (such as puttySSH or CoreFTP).

Note: If you can't ping, telnet, ssh or FTP connect to the NTP sever, this indicates a network port issue exists.

10) If this Option Card is installed, have you tried connecting to one of the other three network ports (with that other port configured with a similar IP address)? If not, I recommend trying this to ensure there isn't a problem with that one particular port.
11) Are you using dynamic/DHCP IP addresses or static IP addresses?

To reset all of the configs and logs back to factory default values, perform a "clean" CLI command. A "clean" command can be performed by connecting a PC running HyperTerminal (or other terminal emulator software) to the front panel SERIAL port with a straight-thru DB8F to DB9F serial cable. The settings for HyperTerminal are 9600, N, 8 1.).

Once connected, type: **clean** <enter>. Note that this same command can also be sent with a telnet or an SSH connection (as long as these services are still enabled in the web browser). Either telnet or ssh into the NTP server and then type: clean <enter>. After issuing this command via RS-232, telnet or SSH, the logs and configurations will be reset and the web browser should be accessible again. Then just configure the SecureSync as desired.
Note: An automatic reboot is performed when performing a Clean command

.

Radius not working on a unit

I verified with our engineering team that there are no hardware issues that can cause an issue specific to only Radius connection (as I suspected). Any potential hardware issues with the Model 9483 itself that affect Radius would have to also affect network connectivity in general on that port.
So, along these lines, we want to make sure whichever network port on the Model 9483 that the network is connected to is able to successfully communicate with the network. All Model 9483s have an available base Ethernet port ("eth0"). However, the Model 9483 also has an available Option Card (Called the "Gigabit Option Card", Model 1204-06) that can be installed in a rear panel Option Bay to add three additional network ports (eth1, eth2 and eth3) to the Model 9483.

FYI- Software version 4.8.0 added standard Linux "out-bound" network tools to the Model 9483's Command Line Interface (CLI). These network tools can be helpful with troubleshooting network-related issues.

If you connect to the Model 9483 via the front panel RS-232 SERIAL port, or over network via telnet or ssh, try pinging the IP address of the Radius server. With a good network connection between the time server and the Radius server, the Radius server should continue to respond to pings, until you press CTRL/C.

***Radius ports (UDP)

UDP Port 1812 (Radius authentication messages)

- When Radius is enabled, the SecureSync is a Radius client
- UDP Port 1812 is the typical port to use for Radius
- When Radius is enabled, the SecureSync doesn't listen on port 1812. The SecureSync only transmits (and only transmits when someone is actively logging into the web browser)
- Because the SecureSync doesn't listen on UDP port 1812, it won't show up in a netstat response or other port sniffer program.
- To see UDP port 1812 listening, run **netstat** on the radius server itself, as the radius server listens for Radius clients on port 1812

B) Radius server reporting "unreachable"

1. Is ping disabled in Radius server

2. in CLI perform the following command: **traceroute -p xxx yyy.yyy.yyy** (where xxx is radius port, such as 1812 and where yyy is the address for the Radius server. Make sure response indicates the radius server was reachable.

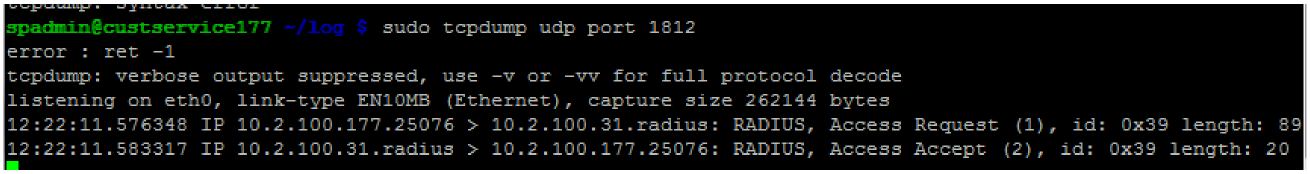
C) Cant enable Radius Service

1. make sure at least one Radius server has been listed (added via the Add Server button)
2. Refer to Salesforce cases such as 173674 (v5.8.0 installed)

Tcpdump capture of radius traffic

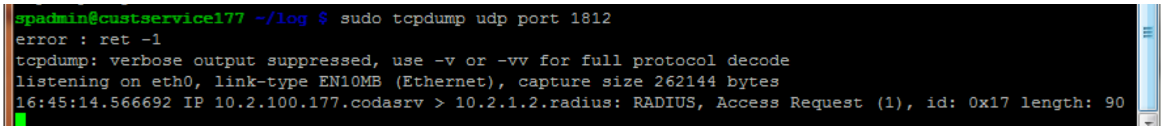
- To see the messages being sent to the Radius server, login to the CLI via telnet or ssh. Then type: **tcpdump udp port 1812**. Then with Radius configure/enabled, login to the web browser. (Note this particular command looks on eth0 only. The port will need to be specified in this command if the Radius server is on a different Ethernet interface than eth0):

  A) Example below is from a **successful Remote login to the "oleg" account** (not stored in the SecureSync). Port 1812



```
tcpdump: syntax error
spadmin@custservice177 ~/log $ sudo tcpdump udp port 1812
error : ret -1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:22:11.576348 IP 10.2.100.177.25076 > 10.2.100.31.radius: RADIUS, Access Request (1), id: 0x39 length: 89
12:22:11.583317 IP 10.2.100.31.radius > 10.2.100.177.25076: RADIUS, Access Accept (2), id: 0x39 length: 20
```

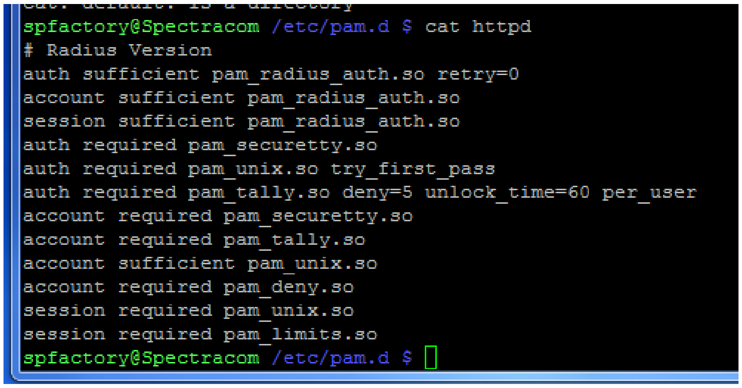
  B) Example below is from a **failed radius login attempt** (invalid configurations for the radius server- wrong address wrong key. Etc) Notice there is AN Access Request sent from the SecureSync but no Access Accept sent back from the Radius server. Port 1812.



```
spadmin@custservice177 ~/log $ sudo tcpdump udp port 1812
error : ret -1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:45:14.566692 IP 10.2.100.177.codasrv > 10.2.1.2.radius: RADIUS, Access Request (1), id: 0x17 length: 90
```

******Radius configuration file

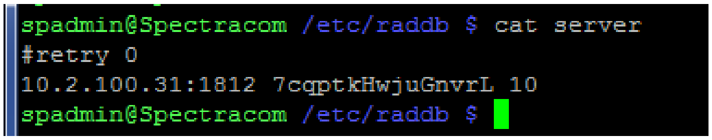
- ➢ Customers can view the Radius login config file with the spadmin account
- ➢ **/etc/pam.d** and then type: **cat login**
- ➢ Radius is controlled in **/etc pam.d**
- ➢ **Path to Radius configuration**: cd /etc/pam.d/radius   Then type either: **cat httpd** or **cat login** (example from v5.3.0 below):



```
cat: default: is a directory
spfactory@Spectracom /etc/pam.d $ cat httpd
# Radius Version
auth sufficient pam_radius_auth.so retry=0
account sufficient pam_radius_auth.so
session sufficient pam_radius_auth.so
auth required pam_securetty.so
auth required pam_unix.so try_first_pass
auth required pam_tally.so deny=5 unlock_time=60 per_user
account required pam_securetty.so
account required pam_tally.so
account sufficient pam_unix.so
account required pam_deny.so
session required pam_unix.so
session required pam_limits.so
spfactory@Spectracom /etc/pam.d $
```

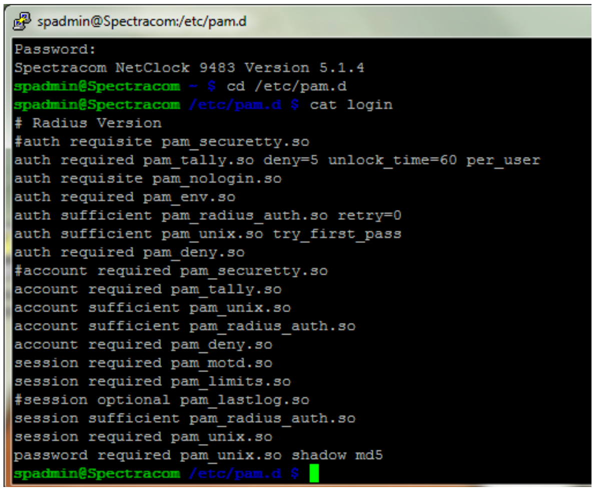
- ➢ Per Ron Dries, the radius settings are stored in **/etc/raddb** (the file is named "server" so type: **cat server**)

Example Radius config file ("server") in /etc/raddb/server (can be viewed in spadmin account)



```
spadmin@Spectracom /etc/raddb $ cat server
#retry 0
10.2.100.31:1812 7cqptkHwjuGnvrL 10
spadmin@Spectracom /etc/raddb $
```

File from our NetClock with Radius working correctly:

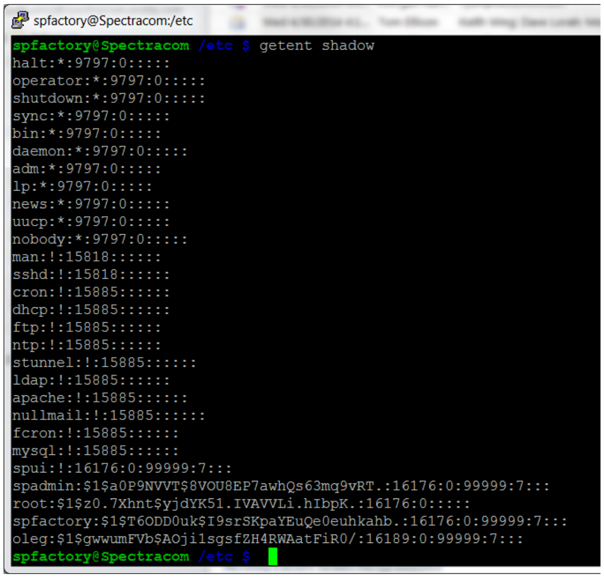


spadmin@Spectracom:/etc/pam.d

```
Password:
Spectracom NetClock 9483 Version 5.1.4
spadmin@Spectracom ~ $ cd /etc/pam.d
spadmin@Spectracom /etc/pam.d $ cat login
# Radius Version
#auth requisite pam_securetty.so
auth required pam_tally.so deny=5 unlock_time=60 per_user
auth requisite pam_nologin.so
auth required pam_env.so
auth sufficient pam_radius_auth.so retry=0
auth sufficient pam_unix.so try_first_pass
auth required pam_deny.so
#account required pam_securetty.so
account required pam_tally.so
account sufficient pam_unix.so
account sufficient pam_radius_auth.so
account required pam_deny.so
session required pam_motd.so
session required pam_limits.so
#session optional pam_lastlog.so
session sufficient pam_radius_auth.so
session required pam_unix.so
password required pam_unix.so shadow md5
spadmin@Spectracom /etc/pam.d $
```

Viewing all accounts via the CLI interface: /etc and type: **getent shadow**. Scroll down to the bottom of the response.

> **Note**: Refer to "**Shadow**" in the "all products" section at the beginning of this document for deciphering this response.
>
> **Note**: Not sure if this command required spfactory login, or can work with admin rights. Also not sure if it works on 2400 SecureSync. Screenshot below is from 1200 SecureSync (not 2400)



```
spfactory@Spectracom /etc $ getent shadow
halt:*:9797:0:::::
operator:*:9797:0:::::
shutdown:*:9797:0:::::
sync:*:9797:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
nobody:*:9797:0:::::
man:!:15818::::::
sshd:!:15818::::::
cron:!:15885::::::
dhcp:!:15885::::::
ftp:!:15885::::::
ntp:!:15885::::::
stunnel:!:15885::::::
ldap:!:15885::::::
apache:!:15885::::::
nullmail:!:15885::::::
fcron:!:15885::::::
mysql:!:15885::::::
spui:!:16176:0:99999:7:::
spadmin:$1$a0P9NVVT$8VOU8EP7awhQs63mq9vRT.:16176:0:99999:7:::
root:$1$z0.7Xhnt$yjdYK51.IVAVVLi.hIbpK.:16176:0:::::
spfactory:$1$T6ODD0uk$I9srSKpaYEuQe0euhkahb.:16176:0:99999:7:::
oleg:$1$gwwumFVb$AOji1sgsfZH4RWAatFiR0/:16189:0:99999:7:::
spfactory@Spectracom /etc $
```

***NAS (Network Access Server)

NAS-IP address

***Permissions assigned to Radius accounts

- Radius (and tacacs) to remote authenticate both the browser login and now also CLI interface, alleviating need to have an account stored on the box for CLI

Admin/User rights for Radius users

- All users who login to the SecureSync through Radius are automatically assigned Admin rights.
- Radius accounts can't be assigned user rights, unless either Radius authentication is combined with LDAP Authentication as well, or a local user account is created in the SecureSync.
- RADIUS only provides authentication. You provide it a username and a password, and it provides back whether that username and password is authenticated. It doesn't provide any permissions or other authorization information. The only alternatives to allow accounts to have user rights (instead of admin rights) are to either:
  1. Combine RADIUS with another system that provides authorization (such as LDAP),
  2. Or to make local user accounts matching those that are being authenticated.
     - If there is a local account with the same username, it will be authenticated using RADIUS, and use the permissions from the local account.

Ability to disable LDAP/Radius via the front panel to regain access to locked-out unit.

- **resetpw** (in the front panel “cmd” menu) disables LDAP/Radius (versions 5.3.0 and above)

Note: Starting in version ~~5.2.1 (~Apr 2015)~~ **resetpw also sets LDAP and Radius to “Disabled”** to help prevent total lockout. They need to be re-enabled thereafter, if desired. Refer to Mantis case 3026 Update- this change was **inadvertently left out of the v5.2.1 release. It will need to be added in version 5.3.0**

When resetpw is performed, and if LDAP and/or Radius were intentionally enabled, they will need to be re-enabled as desired, after performing a resetpw command.

Q Help to clarify that if the RESETPW on panel LCD is used, will it erase all the machine configuration to default or just reset the spadmin password to default value?

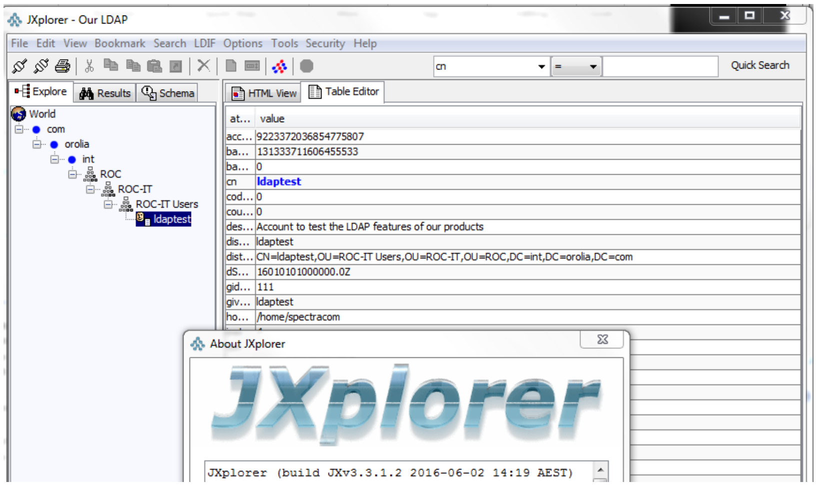
A Keith’s response (23 May 17) Unlike the CLEAN command, the RESETPW command will NOT erase all the configurations back to default. The RESETPW command only resets the spadmin account password back to the default value of ‘admin123’.

Note that in software versions 5.2.1 and above, the RESETPW command also disables Radius and LDAP remote authentication services (if enabled for use). This command doesn’t change the configurations for these two services. It just unselects the checkbox which enables/disables the functionality of these services. So after performing a RESETPW command, the enable checkbox(es) for LDAP and/or Radius need to be reselected, if using either or both of these authentication services.

LDAP

Active Directory/schema viewer to see the directory structure of the IT's AD server

- Example of a freeware/opensource viewer: JXplorer



at...	value
acc...	9223372036854775807
ba...	131333711606455533
ba...	0
cn	**ldaptest**
cod...	0
cou...	0
des...	Account to test the LDAP features of our products
dis...	ldaptest
dist...	CN=ldaptest,OU=ROC-IT Users,OU=ROC-IT,OU=ROC,DC=int,DC=orolia,DC=com
dS...	16010101000000.0Z
gid...	111
giv...	ldaptest
ho...	/home/spectracom

```
JXplorer (build JXv3.3.1.2 2016-06-02 14:19 AEST)
```

Management -> **Authentication** page and click **LDAP Setup**

Refer to:

- **SecureSync Tech Note:** EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\LDAP and Radius
- ***Model 9400 Tech Note:*** *EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\LDAP and Radius*

LDAP/RADIUS RFCs (in this document): **Port assignments and RFCs for all products

OpenLDAP: http://www.openldap.org/

Shortcut to SecureSync LDAP/Radius design info: S:\Projects\Lafayette

Version-related info for LDAP

- 2400 SecureSync software support for LDAP: Added in update version 1.1.0a (Feb 2020)

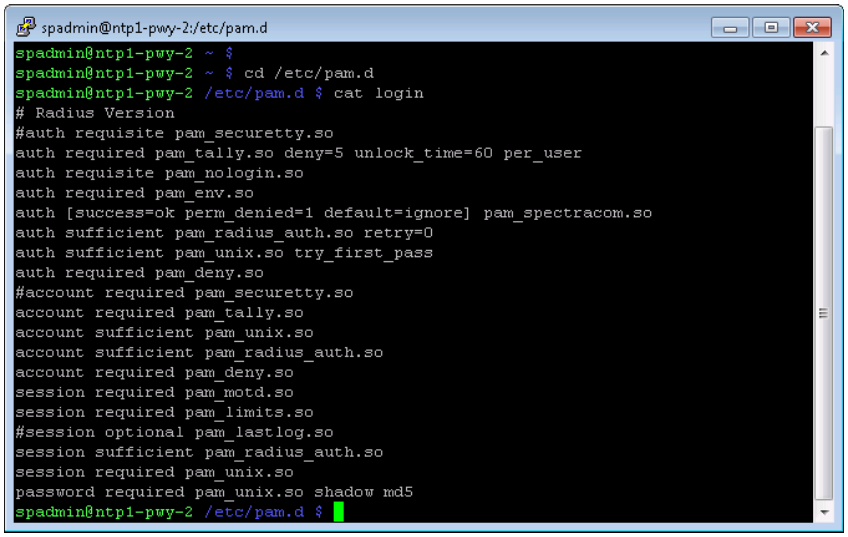
LDAP

Note: For example engineering software release testing of Radius/LDAP, in Arena, refer to the ECO of the release (such as ECO 1338 for v5.7.1 https://app.bom.com/changes/detail-summary?change_id=2389346979) to find the PVP Test validation in the list of "ITEMS"

Order of precedence for both Radius and LDAP when logging in (Per Ron)

- Radius authentication is attempted
- LDAP authentication is attempted.
- Local login (accounts in the NTP server).

As indicated: (internal use only) /etc/pam.d/radius and type: **cat login**



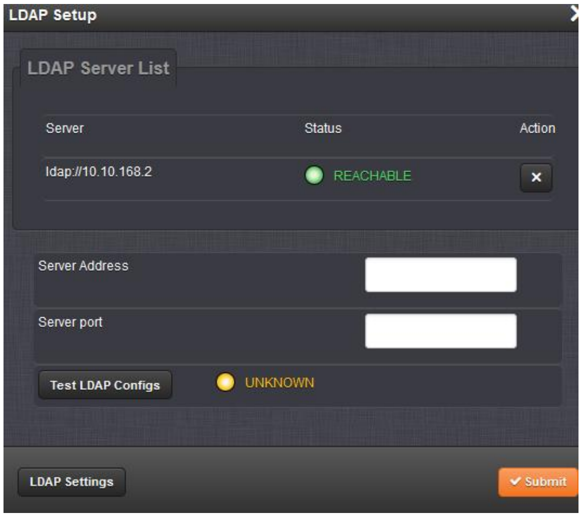
spadmin@ntp1-pwy-2:/etc/pam.d

```
spadmin@ntp1-pwy-2 ~ $
spadmin@ntp1-pwy-2 ~ $ cd /etc/pam.d
spadmin@ntp1-pwy-2 /etc/pam.d $ cat login
# Radius Version
#auth requisite pam_securetty.so
auth required pam_tally.so deny=5 unlock_time=60 per_user
auth requisite pam_nologin.so
auth required pam_env.so
auth [success=ok perm_denied=1 default=ignore] pam_spectracom.so
auth sufficient pam_radius_auth.so retry=0
auth sufficient pam_unix.so try_first_pass
auth required pam_deny.so
#account required pam_securetty.so
account required pam_tally.so
account sufficient pam_unix.so
account sufficient pam_radius_auth.so
account required pam_deny.so
session required pam_motd.so
session required pam_limits.so
#session optional pam_lastlog.so
session sufficient pam_radius_auth.so
session required pam_unix.so
password required pam_unix.so shadow md5
spadmin@ntp1-pwy-2 /etc/pam.d $
```

Our LDAP Server (on Eng lab network)

- can no longer use IT team's LDAP server (due to security concerns)
- Now using LDAP server on the Eng Lab network (at 10.10.168.2)
- SecureSync for testing LDAP needs to physically reside on the Eng Lab network, with the LDAP server to work. Can't use custservice rack units or a unit at home to test.
- Example settings below from 2400 SecureSync v1.6.0 (confirmed by Keith to be working)

(After pressing "Test LDAP Configs")



LDAP Setup

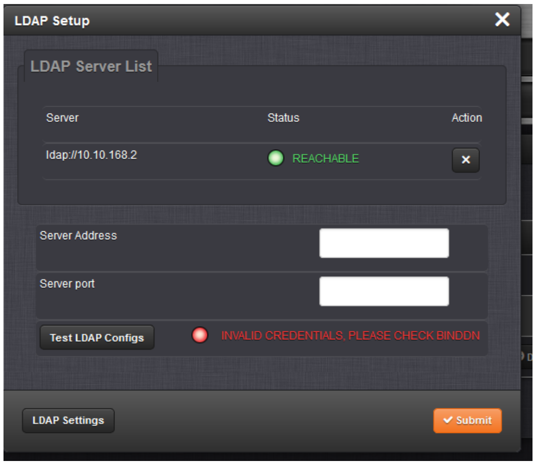
LDAP Server List

Server	Status	Action
ldap://10.10.168.2	● REACHABLE	×

Server Address

Server port

Test LDAP Configs ● UNKNOWN



LDAP Setup

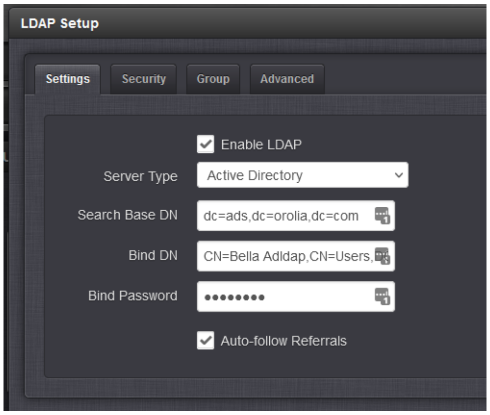
LDAP Server List

Server	Status	Action
ldap://10.10.168.2	● REACHABLE	×

Server Address

Server port

Test LDAP Configs ● INVALID CREDENTIALS, PLEASE CHECK BINDDN



☑ Enable LDAP

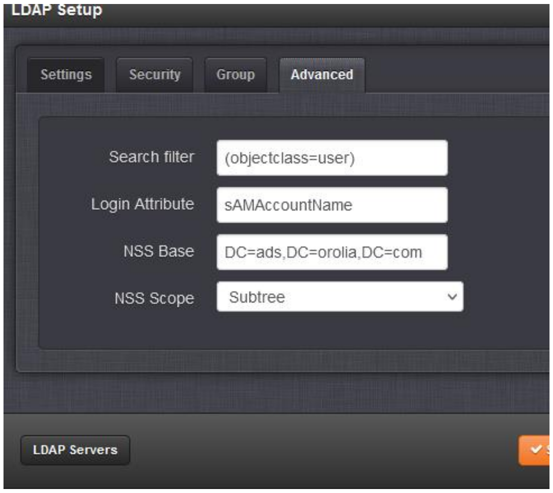
Server Type: Active Directory

Search Base DN: dc=ads,dc=orolia,dc=com

Bind DN: CN=Bella Adldap,CN=Users,

Bind Password: ••••••••

☑ Auto-follow Referrals



Search filter: (objectclass=user)

Login Attribute: sAMAccountName

NSS Base: DC=ads,DC=orolia,DC=com

NSS Scope: Subtree

Navigate to the Managment->Authentication setup page and click on the "LDAP SETUP" link. Add LDAP Server '10.10.168.2' Leave Server port field Blank
2. Click on the "Settings" Tab Check Enable LDAP. Fill in Fields:
Search Base DN: dc=ads,dc=orolia,dc=com
Bind DN: CN=BellaAdldap,CN=Users,DC=ads,DC=orolia,DC=com
Bind Password: Bell@123
3. Click on the

"**Advanced** " **Tab**. Fill in Fields:

NSS Base: DC=ads,DC=orolia,DC=com
NSS Scope: Subtree (Pull
Down) Click the
"Submit" button
4. Go back to the
"Servers" tab

1. Logout of the
UUT, then attempt
to login with the
LDAP credentials:
User : "adbella"
Password:"Bell@123

Note: For example engineering software release testing of LDAP, in Arena, refer to PVP for 2400s (https://app.bom.com/changes/detail-affected?change_id=2414359153) Select **Files** tab, and then open "PVP-000037 SecureSync 2400 Software" (direct link: https://app.bom.com/items/detail-spec?item_id=1264437951&version_id=12206310348&)

Our Eng Lab LDAP server's configuration

Tabs

Settings Tab

Check "**Enabled**"

Server type = Active Directory

Search Base DN dc=ads,dc=orolia,dc=com

Bind DN ("Distinguished name") CN=Bella Adldap,CN=Users,DC=ads,DC=orolia,DC=com

Bind Password: Bell@123 (note: may not accept certain special characters)

(**Note**: "NSS allows administrators to specify a list of sources where authentication files, host names and other information will be stored and searched for")

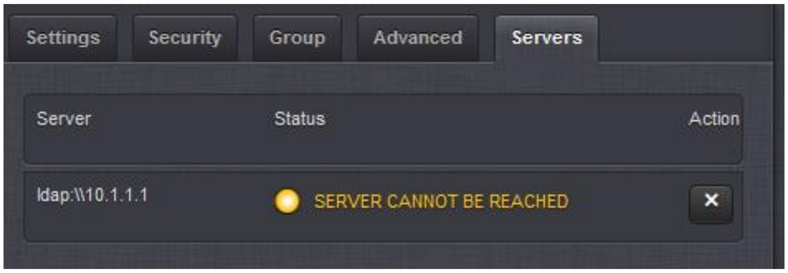
Servers Tab

Add an additional server:

Note: to use its IP address instead: ldap://10.10.168.2

Note: After entering the LDAP server address, if the "**Servers**" tab reports "**Invalid Configuration, please…"** **(**instead of "**LDAP Configuration valid")** verify the "**DNS primary**" address in Eth0 is set to "10.1.1.20. Missing or incorrect DNS sever address will cause this to occur.

Note: After entering the LDAP server address, if the "**Servers**" tab reports "**server cannot be reached" (**instead of "**LDAP Configuration valid")**



ldap:\\10.1.1.1 ● SERVER CANNOT BE REACHED

Verify:

1) Whether using the LDAP server's IP addresss or hostname, the Server line must begi with **ldap://** (and **not "ldap:\\")**

   ○ Example above shows the wack/wack going in the wrong direction (instead of \\, it should be //)

2) (if using a hostname instead of IP address) DNS is configured correctly and working (try temporarily using its IP address to see if it then connects. If it does, there is a DNS-related issue.

Group Tab
Enable group filter: not selected
All three fields empty

Advanced Tab
Search Filter: objectclass=user
Login Attribute: sAMAccountName
NSS Base DC=ads,DC=orolia,DC=com
NSS Scope: Subtree

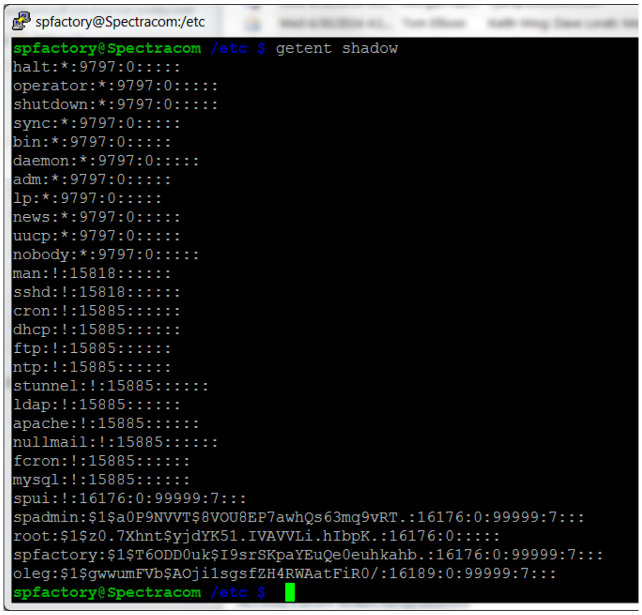
Logout of browser and Login with:

Username:
Password:

Viewing all accounts via the CLI interface: /etc and type: getent shadow <enter> Scroll down to the bottom of the response.
Getent

Note: Refer to "**Shadow**" in the "all products" section at the beginning of this document for deciphering this response.

Getent Note: appears this command requires spfactory login, Screenshot below is from 1200 SecureSync (not 2400)

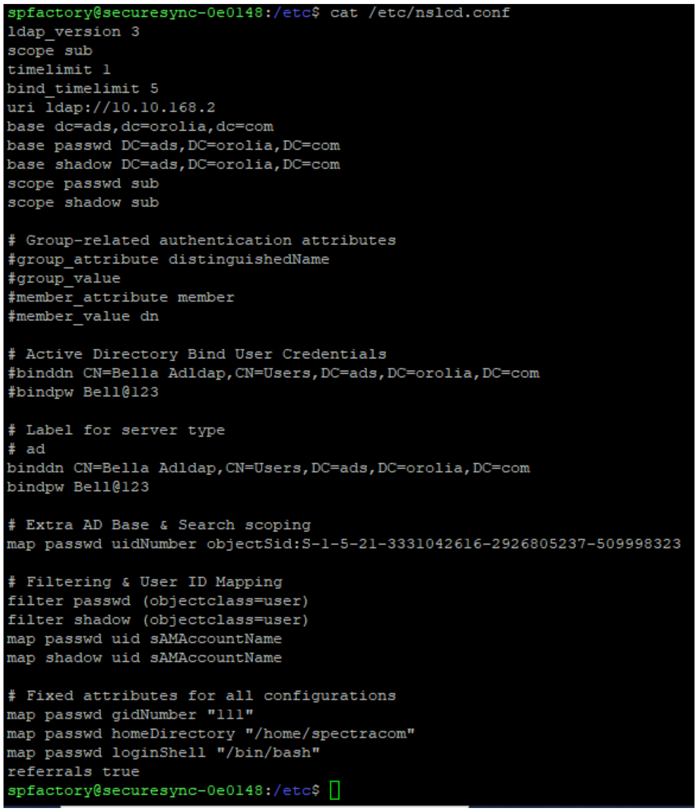


spfactory@Spectracom:/etc

```
spfactory@Spectracom /etc $ getent shadow
halt:*:9797:0:::::
operator:*:9797:0:::::
shutdown:*:9797:0:::::
sync:*:9797:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
nobody:*:9797:0:::::
man:!:15818::::::
sshd:!:15818::::::
cron:!:15885::::::
dhcp:!:15885::::::
ftp:!:15885::::::
ntp:!:15885::::::
stunnel:!:15885::::::
ldap:!:15885::::::
apache:!:15885::::::
nullmail:!:15885::::::
fcron:!:15885::::::
mysql:!:15885::::::
spui:!:16176:0:99999:7:::
spadmin:$1$a0P9NVVT$8VOU8EP7awhQs63mq9vRT.:16176:0:99999:7:::
root:$1$z0.7Xhnt$yjdYK51.IVAVVLi.hIbpK.:16176:0:::::
spfactory:$1$T6ODD0uk$I9srSKpaYEuQe0euhkahb.:16176:0:99999:7:::
oleg:$1$gwwumFVb$AOji1sgsfZH4RWAatFiR0/:16189:0:99999:7:::
spfactory@Spectracom /etc $
```

To view the LDAP config file after editing, type cat /etc/nslcd.conf ~~<enter>~~ **(ctrl x to escape)**

Note: must be logged-in as spfactory. Admin accounts will report "permission denied"



```
spfactory@securesync-0e0148:/etc$ cat /etc/nslcd.conf
ldap_version 3
scope sub
timelimit 1
bind_timelimit 5
uri ldap://10.10.168.2
base dc=ads,dc=orolia,dc=com
base passwd DC=ads,DC=orolia,DC=com
base shadow DC=ads,DC=orolia,DC=com
scope passwd sub
scope shadow sub

# Group-related authentication attributes
#group_attribute distinguishedName
#group_value
#member_attribute member
#member_value dn

# Active Directory Bind User Credentials
#binddn CN=Bella Adldap,CN=Users,DC=ads,DC=orolia,DC=com
#bindpw Bell@123

# Label for server type
# ad
binddn CN=Bella Adldap,CN=Users,DC=ads,DC=orolia,DC=com
bindpw Bell@123

# Extra AD Base & Search scoping
map passwd uidNumber objectSid:S-1-5-21-3331042616-2926805237-509998323

# Filtering & User ID Mapping
filter passwd (objectclass=user)
filter shadow (objectclass=user)
map passwd uid sAMAccountName
map shadow uid sAMAccountName

# Fixed attributes for all configurations
map passwd gidNumber "111"
map passwd homeDirectory "/home/spectracom"
map passwd loginShell "/bin/bash"
referrals true
spfactory@securesync-0e0148:/etc$
```

LDAP configuration:

- ➢ Refer to sites such as: https://technet.microsoft.com/en-us/library/cc755809(v=ws.10).aspx

What connections are controlled by LDAP (when LDAP is enabled)?

1) Web browser
2) Telnet/SSH/FTP/SCP
3) Front panel serial port

Note: all of these are automatically controlled when LDAP is enabled. There is no individual enabling for each.

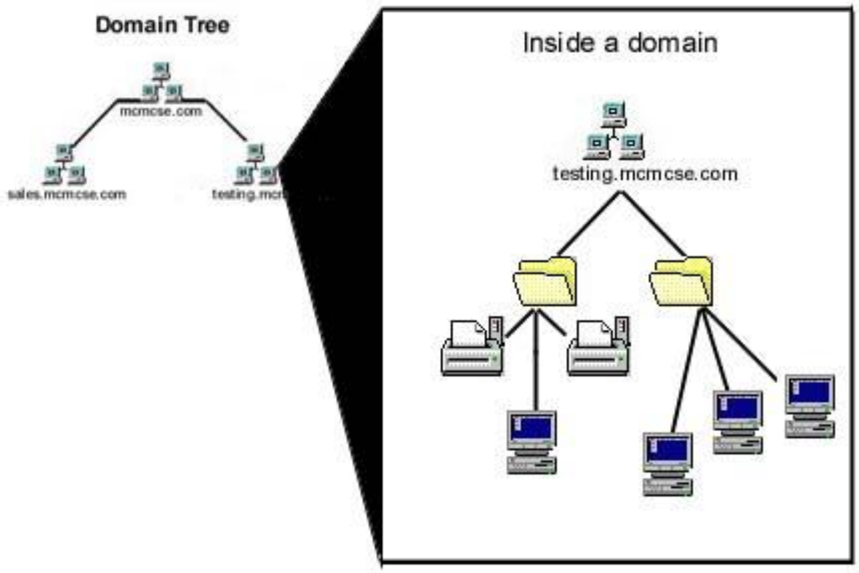
From: http://www.mcmcse.com/microsoft/guides/ad.shtml

Directory Components:
what happens inside a domain? To get started, the first concept that you will need to understand what the directory is made of. A common analogy for a directory is a phonebook. Both contain listings of various objects and information↗ and properties about them. Within the directory are several other terms that you must know to gain even an entry level understanding as to how it all works.

- **Objects** - Objects in the database can include printers, users, servers, clients, shares, services, etc. and are the most basic component of the directory.
- **Attributes** - An attribute describes an object. For example, passwords and names are attributes of user objects. Different objects will have a different set of attributes that define them, however, different objects may also share attributes. For example, a printer and Windows Vista computer may both have an IP address as an attribute.
- **Schema** - A schema defines the list of attributes that describe a given type of object. For example, let's say that all printer objects are defined by name, PDL type and speed attributes. This list of attributes comprises the schema for the object class "printers". The schema is customizable, meaning that the attributes that define an object class can be modified.
- **Containers** - A container is very similar to the folder concept in Windows. A folder contains files and other folders. In Active Directory, a container holds objects and other containers. Containers have attributes just like objects even though they do not represent a real entity like an object. The 3 types of containers are Domains, Sites and Organizational Units and are explained in more detail below.

- ➢ *Domains* - We have already discussed this concept in the preceding paragraphs.
- ➢ *Sites* - A site is a location. Specifically, sites are used to distinguish between local and remote locations. For example, company XYZ has its headquarters in San Fransisco, a branch office in Denver and an office that uses DUN to connect to the main network from Portland. These are 3 different sites.
- ➢ *Organizational Units* (OU) - Organizational units are containers into which you can place users, groups, computers, and other organizational units. An organizational unit cannot contain objects from other domains. The fact that organizational units can contain other OUs, a hierarchy of containers can be created to model your organization's structure and hierarchy within a domain. Organizational units should be used to help minimize the number of domains required for a network.

Now that we know what these concepts mean, let's take a visual look at what is going on inside a domain.



The folder symbols represent Organizational Unit (OU) containers and within each of these we find objects such as printers, servers, computers, users, etc. Instead of objects directly located inside these OUs, there could be more OU containers.

Object Names:
Active Directory uses the Lightweight Directory Access Protocol (LDAP) to supply the naming convention for objects. The 2 basic concepts that you need to know are distinguished names and common names. Distinguished names are the complete "path" through the hierarchical tree structure to a specific object. This is similar to specifying the complete path to a file from a DOS prompt. This "path" points to the location of an object in the hierarchy. Let's take a look in more detail.

Distinguished Name (DN)

- ➢ The following are the components that make up a distinguished name:
  - **OU - Organizational Unit.** This attribute is used to divide a namespace based on organizational structure as previously discussed. An OU usually is associated with an Active Directory container or folder.
  - **DC - Domain Component**. Domain components. A distinguished name that uses DC attributes will have one DC for every domain level below root. Another way of thinking of this would be that there would be a DC attribute for every item separated by a dot in the domain name.
  - **CN - Common Name**. This attribute represents the object itself within the directory service.

Note: Indented info below is from https://technet.microsoft.com/en-us/library/cc755809(v=ws.10).aspx

Distinguished Name
Every object in Active Directory has a distinguished name (also known as DN). A distinguished name uniquely identifies an object by using the name of the object, plus the names of the container objects and domains that contain the object. Therefore, **the distinguished name identifies the object as well as its location in a tree**. The distinguished name is unambiguous (that is, it identifies one object only) and unique (that is, no other object in the directory has this name). It contains enough information for an LDAP client to retrieve the object's information from the directory.

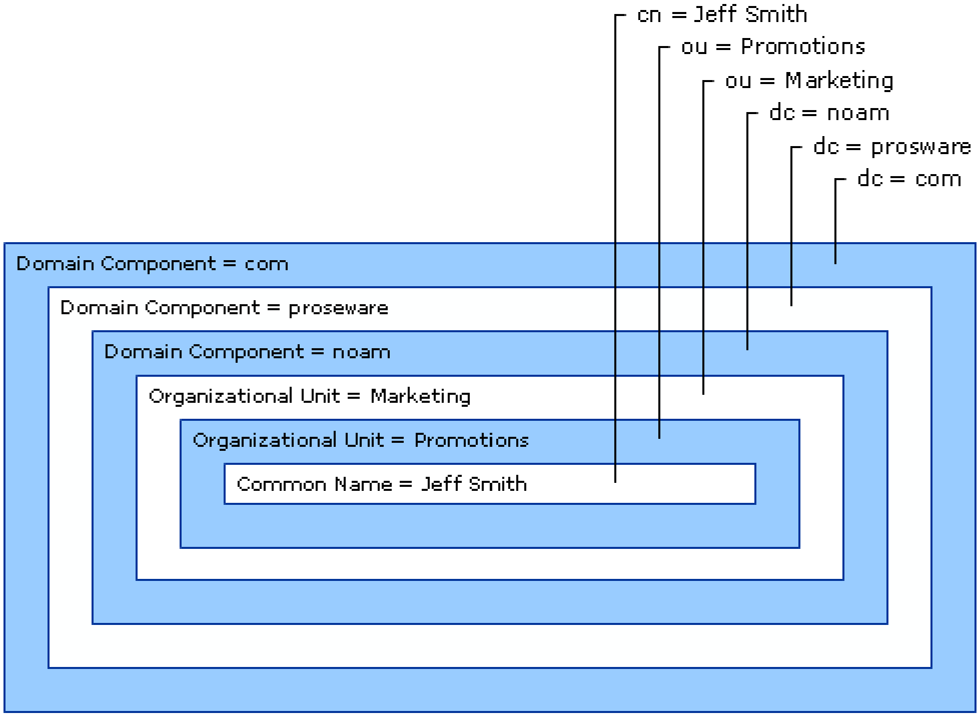
For example, a user named Jeff Smith works in the marketing department of a company as a promotions coordinator. His user account is created in an OU that stores the accounts for marketing department employees who are engaged in promotion activities. The root domain of the company is proseware.com, and the local domain is noam.proseware.com. The distinguished name for this user object is:
cn=Jeff Smith,ou=promotions,ou=marketing,dc=noam,dc=proseware,dc=com

Relative Distinguished Name
The relative distinguished name (also known as the RDN) of an object is the part of the distinguished name that is an attribute of the object itself — the part of the object name that identifies this object as unique within a container. For the

example in the previous paragraph, the relative distinguished name of the user object:
cn=Jeff Smith,ou=promotions,ou=marketing,dc=noam,dc=proseware,dc=com
is cn=Jeff Smith.

The following figure illustrates the relative distinguished names that make up the distinguished name of the user object Jeff Smith.

Relative Distinguished Names That Make Up a Distinguished Name

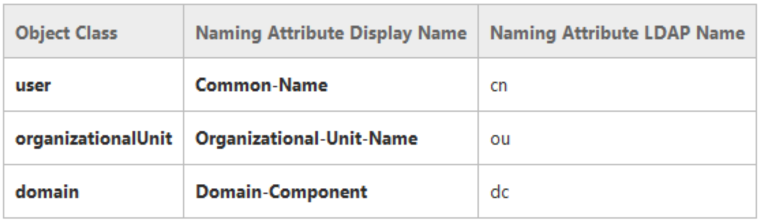


The maximum length that is allowed for a relative distinguished name is 255 characters, but attributes have specific limits that are imposed by the directory schema. For example, in the case of the common name (cn), which is the attribute type that is often used for naming the relative distinguished name, the maximum number of characters that is allowed is 64.

Active Directory relative distinguished names are unique within a container; that is, Active Directory does not permit two objects with the same relative distinguished name under the same parent container. However, two objects can have identical relative distinguished names but still be unique in the directory because, within their respective parent containers, their distinguished names are not the same. For example, the object cn=Jeff Smith,cn=users,dc=noam,dc=proseware,dc=com is recognized by LDAP as being different from cn=Jeff Smith,ou=marketing,dc=noam,dc=proseware,dc=com.

The relative distinguished name for each object is stored in the Active Directory database. Each object in the directory contains a reference to the parent of the object. An LDAP operation can construct the entire distinguished name by following these references to the root.

Default Active Directory Naming Attributes



Object Class	Naming Attribute Display Name	Naming Attribute LDAP Name
user	**Common-Name**	cn
organizationalUnit	**Organizational-Unit-Name**	ou
domain	**Domain-Component**	dc

Each portion of the distinguished name is expressed as attribute_type=value. The attribute type that is used to describe the object's relative distinguished name (in the Jeff Smith example, cn) is called the naming attribute. In Active Directory, instances of classes have a default mandatory naming attribute that is defined in the schema. For example, part of the definition of the class user is the attribute cn (Common-Name) as the naming attribute. Therefore, the relative distinguished name for user Jeff Smith is expressed as cn=Jeff Smith.
Classes that do not define a naming attribute inherit the naming attribute from their parent class. If you create a new class in the Active Directory schema (that is, if you create a new classSchemaobject), you can use the optional rDNAttID attribute to specify the naming attribute for the class.
The following table shows the naming attributes that are used in Active Directory.

Here is an example of a distinguished name:
CN=Jason Sprague,CN=Users,DC=mcmcse,DC=COM

Now let's say that I was a member of the sales.mcmcse.com domain. My new DN would be:
CN=Jason Sprague,CN=Users,DC=sales,DC=mcmcse,DC=COM

And what about my computer called WOPR? It would be:
CN=WOPR,CN=Computers,DC=mcmcse,DC=COM

Authentication

LDAP authentication consists of the following operations:

- **Bind**. Initiates a protocol session to the DSA. After a session is established, a method of authentication is negotiated between the DSA and the client. When the client is authenticated by the DSA, the DSA returns a bind response to the client.
- **Unbind**. Terminates an LDAP session between the client and the DSA.
- **Abandon**. Issued by the client to stop obtaining the results of a previously initiated operation.

A) Binding

- ➢ Bind initiates a protocol session to the DSA. After a session is established, a method of authentication is negotiated between the DSA and the client. When the client is authenticated by the DSA, the DSA returns a bind response to the client.
- ➢ Binding determines at which level a user has rights to. They will have rights for everything at that particular level and below but don't have rights above that value.

Binding consists of:

- **An LDAP request:** initiates a protocol session to the domain controller. After a session is established, a method of authentication is negotiated between the domain controller and the client. By default, Kerberos is used, but other methods can also be used. Finally, the domain controller returns a bind response to the client when the client is authenticated.
- **Followed by an LDAP bind response**: an indication from the server regarding the status of a request for authentication of the client. If the bind is successful, the result code is "success." Otherwise, an error is reported in accordance with RFC 2251.

The following is a Network Monitor example of a successful LDAP bind response:

In Active Directory Domain Services, the act of associating a programmatic object with a specific Active Directory Domain Services object is known as *binding*. When a programmatic object, such as an IADs or DirectoryEntry object, is associated with a specific directory object, the programmatic object is considered to be *bound to* the directory object.

From: http://www.faq.nuvotera.com/determine**-base-dn-bind-dn-domain-configuring-directory-sync/**

How do I determine the Base DN and Bind DN for a domain configuring Directory Sync?

Instructions/Procedure:

1. Log in to your Active Directory.
2. Browse to the location of your user accounts.
3. Pick a single user.
4. Have the distinguished name of that user provided.

The distinguished name of a user will also include the Base DN. You simply need to remove the beginning entry in the distinguished name to find the Base DN. Below is an example:
Distinguished Name:
CN=Test User,OU=Non Admin Users,OU=Users,DC=corp,DC=yourdomain,DC=com

Search Base DN:
OU=Non Admin Users,OU=Users,DC=corp,DC=yourdomain,DC=com
(The Search Base DN tells the server which part of the external directory tree to search)
The Administrator account may not be in the same location as the user accounts. Locate the distinguished name for the Administrator account to find your Bind DN. The Bind DN is the distinguished name of the Administrator account.
Distinguished Name:
CN=Administrator,OU=Admins, OU=Users,DC=corp,DC=yourdomain,DC=com

Search Bind DN:
CN=Administrator,OU=Admins, OU=Users,DC=corp,DC=yourdomain,DC=com
(The Search Bind DN is the user on the external AD server that is permitted to search the AD directory within the defined search base)

Additional Information
Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor. You can use AD Explorer to easily navigate an AD database and identify the Bind and Base DNs as necessary.

Email from Ron Dries (8 Apr 15)

I jotted down some quick notes to try and remove confusion:

Search Base DN – default base distinguished name to use for searches
Bind DN – Administrator user account on the LDAP server in distinguished name format
Bind Password – Password for the administrator account used for binding
NSS Password – distinguished name format of where on the LDAP server to search for user credentials

Email from Ron Dries (3 oct 16)

The **NSS password** is needed even for Windows active directory. This field is just specifying which directory on the Active Directory server to search for user passwords and other attributes needed. This field helps to limit the search and make it more direct. Without it the search can take a very long time, or it could not find the information at all if it hits its search limit before finding what its looking for.

LDAP allows you to use more than one account for logging in. The Bind DN and password are only used to connect to the server and search for users on it.

For example:
A base DN could be DC=test, DC=com
Bind DN could be CN=Admin, OU=Administrators, DC=test, DC=com
Bind PW could be password: testpassword

The bind user authenticates with the LDAP server, and with the correct permissions is allowed to search for the user credentials that the login was attempted with.

NSS password is a distinguished name of where to look, with a scope. For example OU=Users, OU=Test,?sub which will look in the Test/Users directory for the credentials that were used in the attempted login.

LDAP users all have admin level access. You will be able to configure a group for ldap users.

Logging in to the Time server using LDAP – When logging in the time server, the times server will try to bind to the

admin account that has been configured using the password that has been configured. If the bind is succesful, the LDAP server will search the user list for the username that was typed. If a user is found, it checks the password that was typed. If the pasword is correct the LDAP server tells the time server that access is granted for that user.
If the bind fails, the database search cant occur. Make sure that the Bind DN can be manually logged into using the configured Bind password. If login isn't possible, this issue has to be addressed in the LDAP server before proceeding,.

Internal use only- Note that here at the factory, we happen to use the same user login password as the bind pasword for our testing. This was just for simplicity as these two passwords are usually diffenent values!!!

LDAP configuration in the SecureSync

LDAP config file (ldap.conf)

- **Path to ldap.conf config file** Spectracom/etc/ and then type **cat ldap.conf**
- **Path to LDAP:** Spectracom/etc/openldap

Network ports used with LDAP:

- LDAP port is **389** (and port **636** for SSL when using an SSL certificate)

A) LDAP config via CLI

Note: must be logged in as spfactory. Admin accounts will respond “permission denied”

1. **Type nslcd (followed by the tab key) to view the list of all ldap commands**

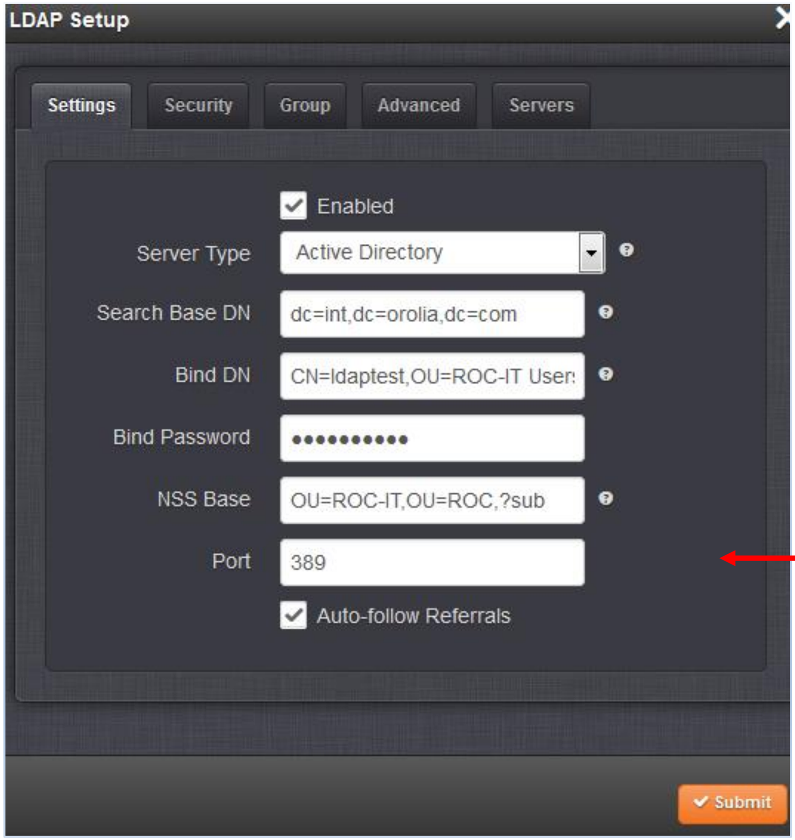
~~~~~~~~~~~

B) LDAP config via web browser

Five tabs for LDAP setup

- **Settings**: This is where you set up the general LDAP Distinguished Name and Bind settings.
- **Security**: This is where you upload and manage the CA server certificate, CA client certificate and CA client key.
- **Group**: This is where you enable/disable group-based authentication.
- **Advanced**: This is where you set up your search filter(s) and login attribute.
- **Servers**: This is where you identify the LDAP server to be used.

Management -> **Authentication** page of the browser. Click “**LDAP Setup**” on the left side of the page
~~~~~~~~~~~



☑ Enabled

Server Type: Active Directory

Search Base DN: dc=int,dc=orolia,dc=com

Bind DN: CN=ldaptest,OU=ROC-IT User:

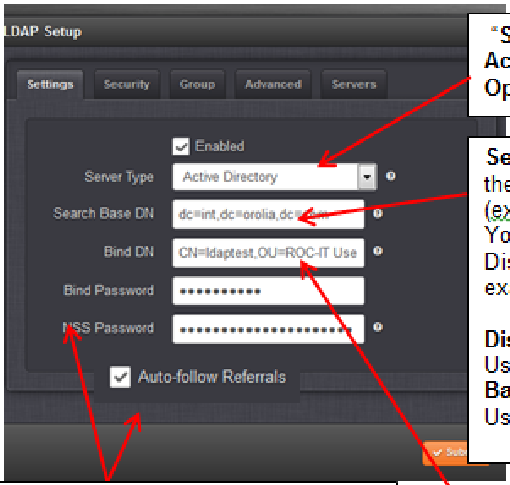
Bind Password: ●●●●●●●●●●●

NSS Base: OU=ROC-IT,OU=ROC,?sub

Port: 389

☑ Auto-follow Referrals

Port field: wasn't available in versions 5.4.1 and below. Is available in at least versions 5.5.1 and above.



☑ Enabled

Server Type: Active Directory

Search Base DN: dc=int,dc=orolia,dc

Bind DN: CN=ldaptest,OU=ROC-IT Use

Bind Password: ••••••••••

NSS Password: •••••••••••••••••••••

☑ Auto-follow Referrals

"Search Type" field
Active Directory: For Windows
Open LDAP: For Linux

Search Base DN (Domain Name): The Search Base DN tells the server which part of the external directory tree to search. (example for us ".int.orolia.com")
You simply need to remove the beginning entry in the Distinguished Name to find the Base DN. Below is an example:

Distinguished Name :CN=Test User,OU=Non Admin Users,OU=Users,DC=corp,DC=yourdomain,DC=com
Base DN:OU=Non Admin Users,OU=Users,DC=corp,DC=yourdomain,DC=com

Bind Password

Note: "Bind DN" and "Bind Password" are "paired"
The Active Directory password for the account that can search for users.
Note: The Bind password is the same password used in association with the Bind DN user account.

Bind DN

Note: "Bind DN" and Bind Password are "paired"
The Search Bind DN is the full distinguished name (DN), including common name (CN), of an Active Directory user account that has privileges to search for users.

Locate the distinguished name for the Administrator account to find your Bind DN. The Bind DN is the distinguished name of the Administrator account.
Distinguished Name:
CN=Administrator,OU=Admins,
OU=Users,DC=corp,DC=yourdomain,DC=com
Bind DN:
CN=Administrator,OU=Admins,
OU=Users,DC=corp,DC=yourdomain,DC=com

NSS Password

Note: "NSS password" field left blank - login will take a long time but will still result in a successful login.

Only displayed when the "Server Type" field (in the "Settings" tab) is set to "**Active Directory**". This field is mandatory when displayed.

Note: "NSS" allows administrators to specify a list of sources where authentication files, host names and other information will be stored and searched for in the AD server.

Note: Bind DN / Bind Password may not accept certain special characters.

Search base DN field in new browser

This field is too restrictive with rules (5.5.1 and below):

(email from, Dave L on 24 Mar 17) There is a limitation in the web browser when configuring LDAP. The Search Base DN and some other fields are too restrictive to what characters can be used. In this case we recommend using the "Classic" interface to setup LDAP. The Classic web UI does not have these restrictions. This is still an issue in version 5.5.1. We have addressed this in the new firmware release but it will be a few weeks until this is available to the general public. Please use the Classic UI for now.

NSS password field

Example of an NSS password ROC-IT,OU=ROC,?sub

This is not really a "password" (the word 'password' is associated with the unix 'password' directory, where user accounts are stored in unix). This field definds the path to the closest directory containing all of the users with unix (GID) attributes you wish to be able to login to the SecureSyncs (shortest path possible, but high enough to be able to include all desired users)

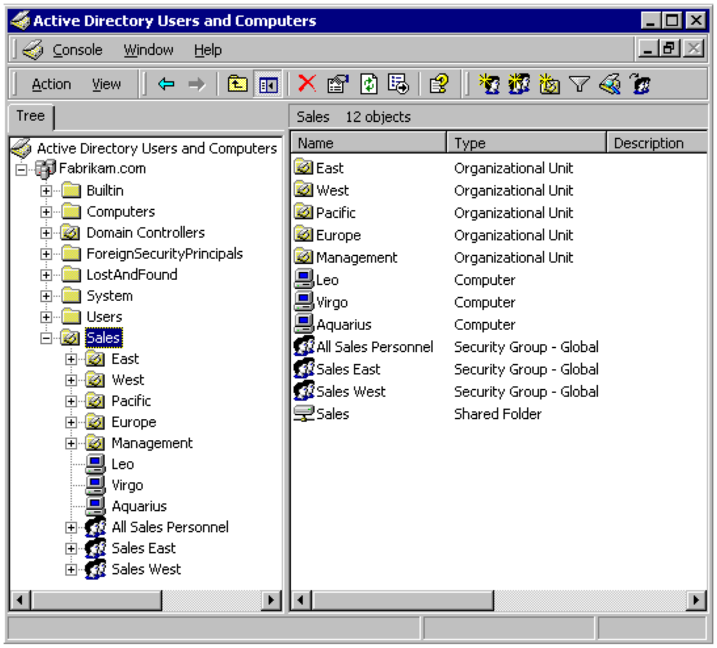
Windows Active Directory/ Group policy / LDAP

- Refer to: http://social.technet.microsoft.com/Forums/windowsserver/en-US/cff39c31-b82b-4e69-babb-9dd94caa0267/ldap-client?forum=winserverGP (Info for Server 2003, Server 2008. Server 2012

Note: For simplicity, think of "**Active Directory**" as being the "LDAP server for Windows". The two choices for LDAP configurations is either **Active Directory** (for Windows) or "**Open LDAP**" (for Linux). These are essentially treated similarly but changes the configs in the SecureSync.

Active Directory (**AD**) is a directory service that Microsoft developed for Windows domain networks and is included in most Windows Server operating systems as a set of processes and services.[1][2]
An AD domain controller authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user.[3]
Active Directory makes use of Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.

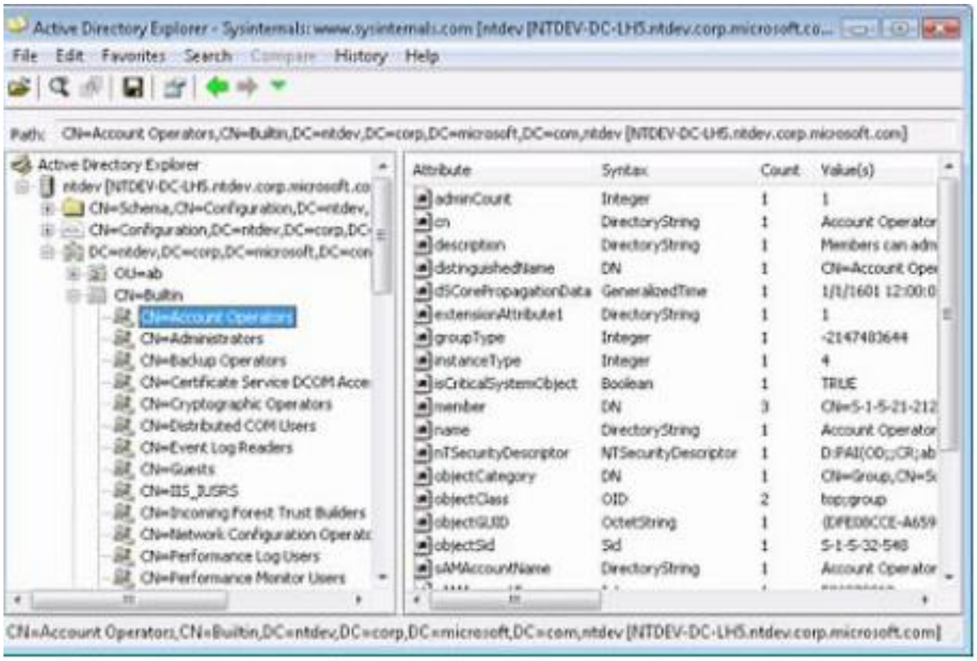
From: https://msdn.microsoft.com/en-us/library/aa746492%28v=vs.85%29.aspx
Active Directory is a special-purpose database. The directory is designed to handle a large number of read and search operations and a significantly smaller number of changes and updates. Active Directory data is hierarchical, replicated, and extensible. Because it is replicated, you do not want to store dynamic data, such as corporate stock prices or CPU performance. If your data is machine-specific, store the data in the registry. Typical examples of data stored in the directory include printer queue data, user contact data, and network/computer configuration data. The Active Directory database consists of objects and attributes. Objects and attribute definitions are stored in the Active Directory schema.
You may be wondering what objects are currently stored in Active Directory. In Windows 2000, Active Directory has three partitions. These are also known as naming contexts: domain, schema, and configuration. The domain partition contains users, groups, contacts, computers, organizational units, and many other object types. Because Active Directory is extensible, you can also add your own classes and/or attributes. The schema partition contains classes and attribute definitions. The configuration partition includes configuration data for services, partitions, and sites.
The following screen shot shows the Active Directory domain partition.



Sales 12 objects

- Active Directory Users and Computers
  - Fabrikam.com
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - LostAndFound
    - System
    - Users
    - Sales
      - East
      - West
      - Pacific
      - Europe
      - Management
      - Leo
      - Virgo
      - Aquarius
      - All Sales Personnel
      - Sales East
      - Sales West

Name	Type	Description
East	Organizational Unit	
West	Organizational Unit	
Pacific	Organizational Unit	
Europe	Organizational Unit	
Management	Organizational Unit	
Leo	Computer	
Virgo	Computer	
Aquarius	Computer	
All Sales Personnel	Security Group - Global	
Sales East	Security Group - Global	
Sales West	Security Group - Global	
Sales	Shared Folder	


Active Directory Explorer - Sysinternals: www.sysinternals.com [ntdev [NTDEV-DC-LH5.ntdev.corp.microsoft.co...
File
Edit
Favorites
Search
Compare
History
Help

Path: CN=Account Operators,CN=Builtin,DC=ntdev,DC=corp,DC=microsoft,DC=com,ntdev [NTDEV-DC-LH5.ntdev.corp.microsoft.com]

- Active Directory Explorer
  - ntdev [NTDEV-DC-LH5.ntdev.corp.microsoft.co
    - CN=Schema,CN=Configuration,DC=ntdev,
    - CN=Configuration,DC=ntdev,DC=corp,DC=
    - DC=ntdev,DC=corp,DC=microsoft,DC=con
      - OU=ab
      - CN=Builtin
        - CN=Account Operators
        - CN=Administrators
        - CN=Backup Operators
        - CN=Certificate Service DCOM Acce
        - CN=Cryptographic Operators
        - CN=Distributed COM Users
        - CN=Event Log Readers
        - CN=Guests
        - CN=IIS_IUSRS
        - CN=Incoming Forest Trust Builders
        - CN=Network Configuration Operatc
        - CN=Performance Log Users
        - CN=Performance Monitor Users

Attribute	Syntax	Count	Value(s)
adminCount	Integer	1	1
cn	DirectoryString	1	Account Operator
description	DirectoryString	1	Members can adm
distinguishedName	DN	1	CN=Account Oper
dSCorePropagationData	GeneralizedTime	1	1/1/1601 12:00:0
extensionAttribute1	DirectoryString	1	1
groupType	Integer	1	-2147483644
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
member	DN	3	CN=S-1-5-21-212
name	DirectoryString	1	Account Operator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OD;;CR;ab
objectCategory	DN	1	CN=Group,CN=S
objectClass	OID	2	top;group
objectGUID	OctetString	1	{DFED8CCE-A659
objectSid	Sid	1	S-1-5-32-548
sAMAccountName	DirectoryString	1	Account Operator

CN=Account Operators,CN=Builtin,DC=ntdev,DC=corp,DC=microsoft,DC=com,ntdev [NTDEV-DC-LH5.ntdev.corp.microsoft.com]

Below info is from: http://msdn.microsoft.com/en-us/library/ff632147.aspx

The server activities are as follows:

- Upon receiving an LDAP bind request ([RFC2251] section 4.2, Bind Operation) from the Client Application, the directory server interacts with the Microsoft Windows® Authentication Services which authenticates the Administrator using the supplied credentials ([MS-AUTHSO] section 4, Interactive Domain Logon Task).
- The directory server receives the LDAP add request, containing data about the new user object to be created. The directory server validates that the Administrator has the necessary access to perform the operation. If the Administrator does not have the necessary access to perform the operation, the directory server rejects the LDAP add request.
- The directory server verifies the constraints for add operations are satisfied as outlined in [MS-ADTS] sections 3.1.1.5.1, General, and 3.1.1.5.2, Add Operation. If the constraints are not satisfied the add request will be terminated with an appropriate error.
- Additional constraints specific to account creation are validated as outlined in [MS-SAMR] section 3.1.1.6, Attribute Constraints for Originating Updates. If the constraints are not satisfied, the add request will be terminated with an appropriate error.
- The user object is created in the directory and populated with the data supplied in the request. Additional attributes on the object are populated based on the server's processing rules as outlined in [MS-ADTS] section 3.1.1.5.2.4, Processing Specifics, and [MS-SAMR] section 3.1.1.8, Attribute Triggers for Originating Updates.
- The directory server receives password information from the KDC. The password is set to the supplied value.
- The directory server receives LDAP modify requests containing new values for the userAccountControl and pwdLastSet attributes. The attributes are updated with the supplied values.

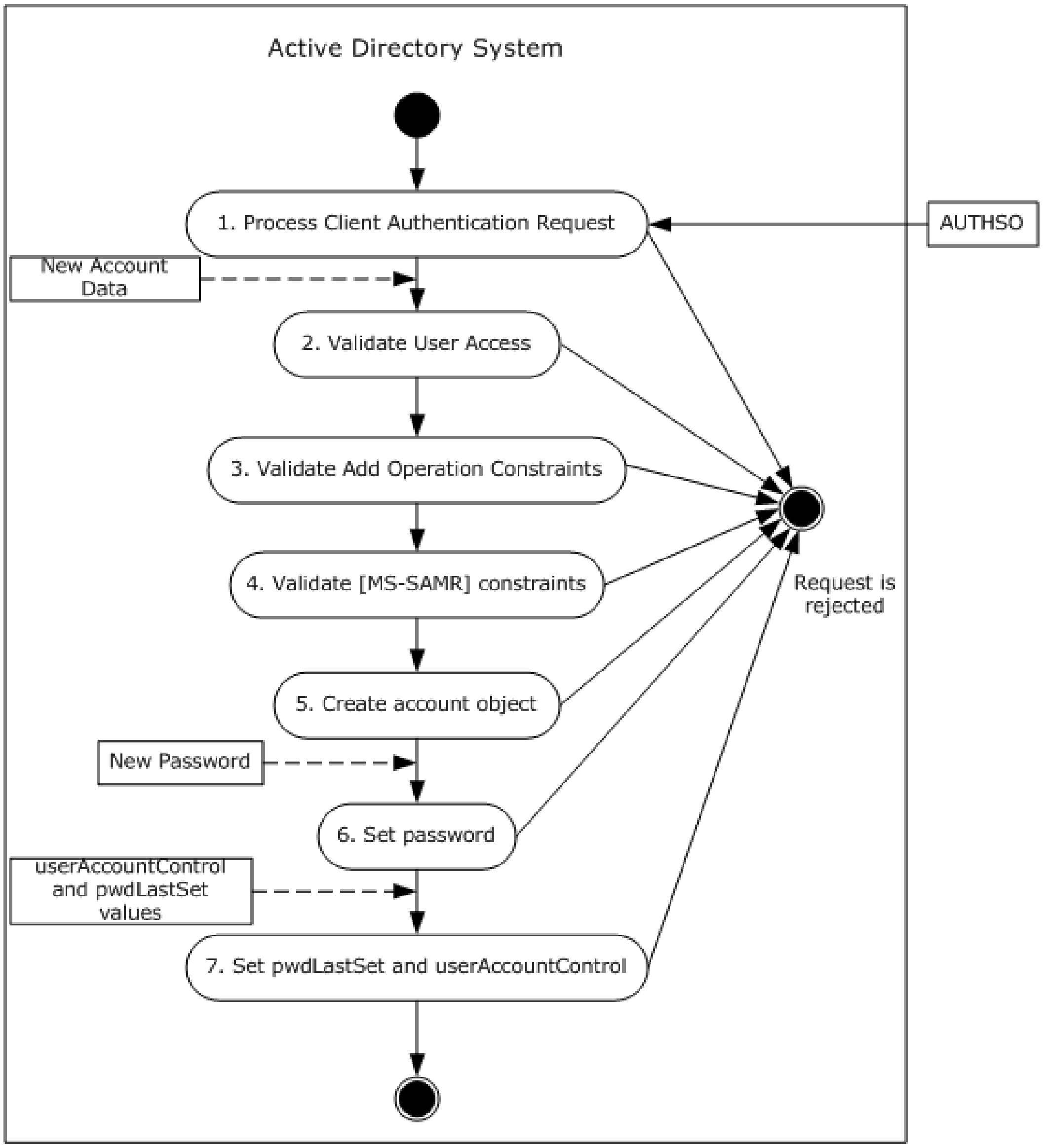
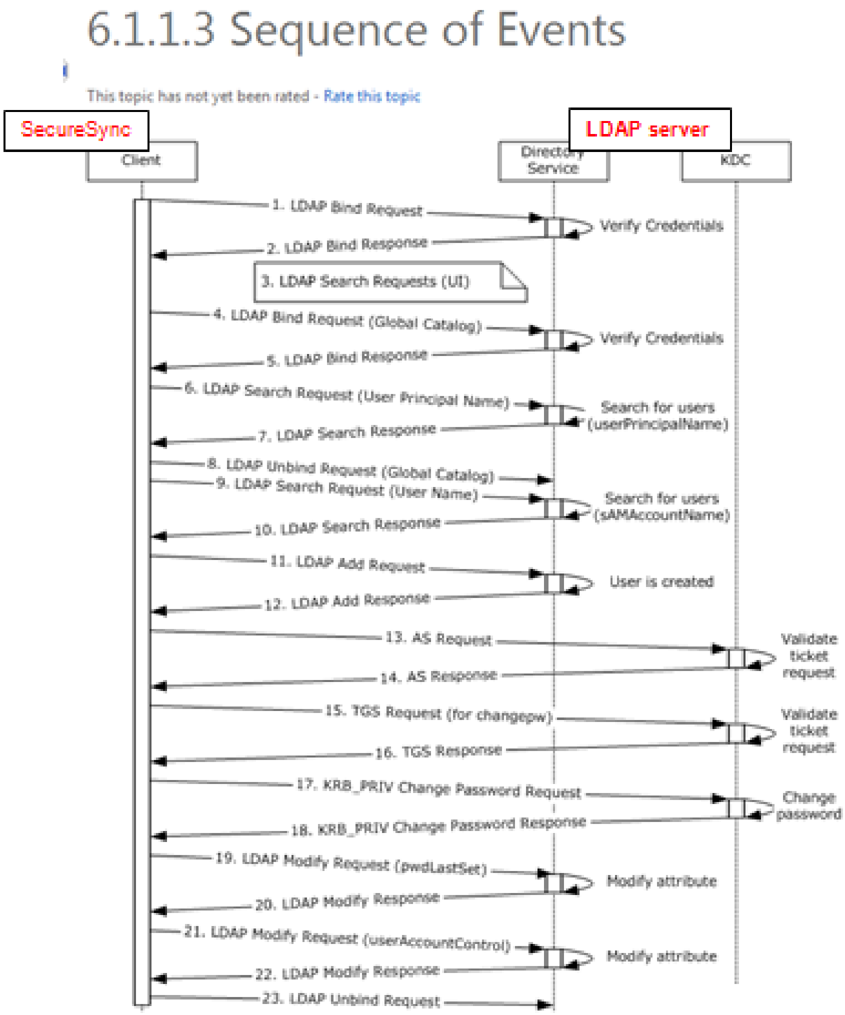

Active Directory System
1. Process Client Authentication Request
AUTHSO
New Account Data
2. Validate User Access
3. Validate Add Operation Constraints
4. Validate [MS-SAMR] constraints
Request is rejected
5. Create account object
New Password
6. Set password
userAccountControl and pwdLastSet values
7. Set pwdLastSet and userAccountControl

Figure 23: Server activity diagram for provisioning a user account using the LDAP protocol

Connection



6.1.1.3 Sequence of Events

This topic has not yet been rated - Rate this topic

Unless otherwise noted, all responses that include a return code contain a return code indicating that the operation was successfully performed.

1. The program (see section 6.1.1) establishes an LDAP connection to the directory server. An **LDAP bind request** ([RFC2251] section 4.2, Bind Operation) is sent to the directory server with the credentials of an administrator.

2. The directory server uses one of the methods defined elsewhere (see [MS-AUTHSO] section 4, Interactive Domain Logon Task) to verify the credentials. Depending on the negotiated authentication method, this may involve additional client and server interactions not directly relevant here. After that verification, the directory server sends an **LDAP bind response** ([RFC2251] section 4.2.3, Bind Response) to the client.

3. At this point the client sends **LDAP search requests** ([RFC2251] section 4.5.1, Search Request) to populate data in the tool's user interface. This step is necessary only for user-interface display purposes specific to the example shown in the figure captioned, "Message flow for provisioning a user account using the LDAP protocol".

4. An LDAP connection to a global catalog is established. **An LDAP bind request** ([RFC2251] section 4.2, Bind Operation) to the global catalog is sent with the administrator's credentials.

5. The global catalog verifies the credentials ([MS-AUTHSO] section 4, Interactive Domain Logon Task) and sends an **LDAP bind response** ([RFC2251] section 4.2.3, Bind Response).

6. An **LDAP search request** ([RFC2251] section 4.5.1, Search Request) is sent to the global catalog, querying the entire forest, starting at the root of the forest, looking for security principals that have the same user principal name as the requested user principal name of the new account, to verify that the requested user principal name of the new account is not currently in use.

7. The global catalog sends an **LDAP search response** ([RFC2251] section 4.5.2, Search Result) listing any accounts that have the user principal name specified.

8. An **LDAP unbind request** ([RFC2251] section 4.3, Unbind Operation) is sent to the global catalog. The LDAP connection to the global catalog is closed.
9. The program sends an **LDAP search request** ([RFC2251] section 4.5.1, Search Request) to the directory, querying the entire domain, starting at the root of the domain, looking for security principals that have the same name (stored in the sAMAccountName attribute) as the one requested for the new account, to ensure that the name specified by the administrator is not currently in use.
10. The server sends an **LDAP search response** ([RFC2251] section 4.5.2, Search Result) listing any accounts that have the user name specified.
For the purposes of this scenario, assume that the LDAP search responses for the user principal name and the account name do not contain any accounts, that is, there were no matches. The program has now verified that the user principal name and user name chosen are not currently in use and continues with the add operation.
11. An **LDAP add request** ([RFC2251] section 4.7, Add Operation) is sent to the server. The LDAP add operation contains the distinguishedName, sAMAccountName, userPrincipalName, displayName, and givenName of the new user, and specifies that the object class of the object to be created is user.
12. The server processes the add request ([RFC2251] section 4.7, Add Operation) and performs validation as described in [MS-ADTS] sections 3.1.1.5.1, General, and 3.1.1.5.2, Add Operation. It then sends an **LDAP add response** indicating success.
Now that the user has been created, the program starts setting additional attributes provided by the administrator. It begins by setting the password for the new account. This is done via Kerberos messages sent to the Kerberos Key Distribution Center (KDC).
13. The client begins by sending a Kerberos AS request ([RFC4120] section 3.1, The Authentication Service Exchange) to the Authentication Service (AS) requesting a Ticket-Granting Ticket (TGT) that it will use for later authentication.
14. The service validates the credentials ([MS-AUTHSO] section 4, Interactive Domain Logon Task) in the AS request and sends an AS response ([RFC4120] section 3.1, The Authentication Service Exchange) with a TGT.
15. The client sends a Kerberos TGS ([RFC4120] section 3.3, The Ticket-Granting Service (TGS) Exchange) request to the Ticket-Granting Service (TGS) using the TGT and requesting a service ticket for the kadmin/changepw service ([RFC3244]), which provides functionality to change an account's password via Kerberos.
16. The service validates the credentials in the TGS request and sends a TGS response ([RFC4120] section 3.3, The Ticket-Granting Service (TGS) Exchange) with the service ticket.
17. Using the service ticket, the client sends a KRB_PRIV change password request ([RFC4120] section 3.5, The KRB_PRIV Exchange, and [RFC3244] section 2, The Protocol) to the Kerberos password-changing service with the new password for the account.
18. The password-changing service processes the request and sends a KRB_PRIV response ([RFC4120] section 3.5, The KRB_PRIV Exchange, and [RFC3244] section 2, The Protocol) indicating success. As part of this change-password operation, the Active Directory database is modified according to the sequence of actions described in [MS-SAMR] section 3.1.1.8.5, clearTextPassword.
At this point the Kerberos operations are completed. The client now continues to set remaining attributes via LDAP.
19. If the administrator indicated that the user must change his or her password at next logon, the client sends an LDAP modify request ([RFC2251] section 4.6, Modify Operation) setting the pwdLastSet attribute to 0. This setting tells the server that the user's password has expired and must be changed the next time the new user attempts to log on.
20. The server processes the request and sends a response ([RFC2251] section 4.6, Modify Operation).
The client computes the new desired value for the userAccountControl attribute. At a minimum this includes the ADS_UF_NORMAL_ACCOUNT bit ([MS-ADTS] section 2.2.15, userAccountControl Bits) and may contain additional bits depending on administrator-provided values.
21. The client sends an LDAP modify request ([RFC2251] section 4.6, Modify Operation) with the new value for userAccountControl.
22. The server processes the request and sends a response ([RFC2251] section 4.6, Modify Operation).
The new user account (represented as a directory object of class user) has now been created. The user object has been populated with all specified attributes.
23. The client sends an LDAP unbind request ([RFC2251] section 4.3, Unbind Operation) to the server. The LDAP connection to the directory server is closed.

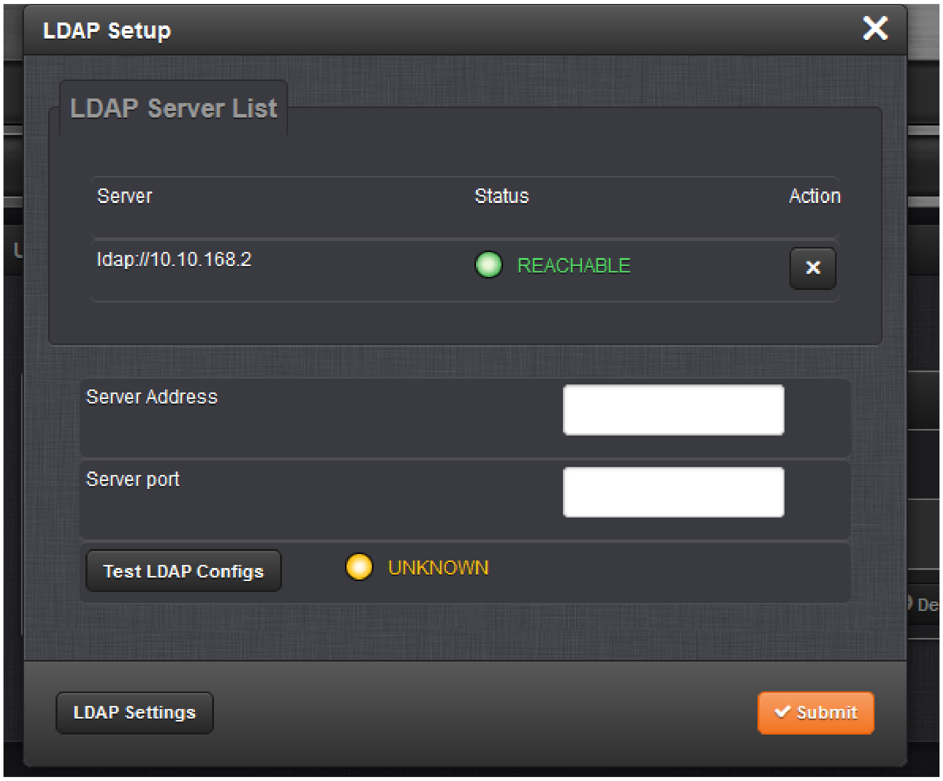
“Auto-follow Referrals” field

- Was added to the bottom of the “**Settings**” tab (I believe in version 5.2.0)
- For more info on referrals, refer to: https://technet.microsoft.com/en-us/library/cc978014.aspx and https://technet.microsoft.com/en-us/library/cc978014.aspx

An LDAP referral is a domain controller's way of indicating to a client application that it does not have a copy of a requested object (or, more precisely, that it does not hold the section of the directory tree where that object would be, if in fact it exists) and giving the client a location that is more likely to hold the object, which the client uses as the basis for a DNS **search for a domain controller.**

To make use of cross-references, clients must be enabled to follow ("chase") referrals that are returned. Windows Address Book chases referrals by default. In LDAP, you can specify **Chase Referrals** in the search options. When you are using ADSI programmatically (for example, by using Active Data Objects [ADO] to search), you must specify whether to chase referrals.

2. Servers pop-up window



LDAP Setup

LDAP Server List

Server	Status	Action
ldap://10.10.168.2	● REACHABLE	×

Server Address

Server port

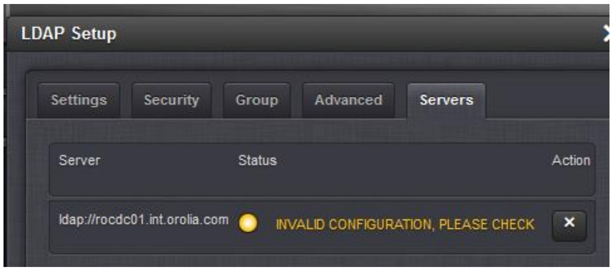
Test LDAP Configs ● UNKNOWN

Number of LDAP servers that can be listed (response below from 1200 SecureSyncs)

Email from Dave L (20 Jan 17) I am not sure exactly what the limit of the number of LDAP Servers you can enter is but it is over 10. The number of LDAP Servers you configure depends on how many you have available and where they are located. I do not think more than two is necessary.

If more than one LDAP Server is configured and is not available, the login will be delayed while the Securesync tries to establish communications with each one of the LDAP Servers. The delay depends on the timeout and number of retries
The local login will not occur until all the LDAP Servers have been contacted or timed out. So please make sure you enter LDAP Servers that will always be reachable.

“Invalid configuration, please check” displayed, after entering LDAP server’s address



ldap://rocdc01.int.orolia.com ● INVALID CONFIGURATION, PLEASE CHECK ✕

1) **Make sure the Primary DNS /Secondary DNS server addresses are correct in the Ethernet interface settings. If DNS settings are missing or incorrect, this will occur.**
2) **Must use URI format for the LDAP address (“LDAP://” in front of the address- not LDAP:\\)**

➢ Must user URI format (refer to: https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol#URI_scheme)

Important Note about URI format: whether configuring the LDAP sever using its IP address or its hostname, this value MUST use **URI** format (value must always begin with the following: **ldap:// (not ldap:\\)**

Examples: **ldap://10.1.1.1** or **ldap://Microsoft.com**

Enter the hostname or IP address of the LDAP server and then press “**Add Server**”

Version 5.2.0 Improved add/delete of LDAP severs.

LDAP Server Status

➢ Only displayed if at least one LDAP server has been added.

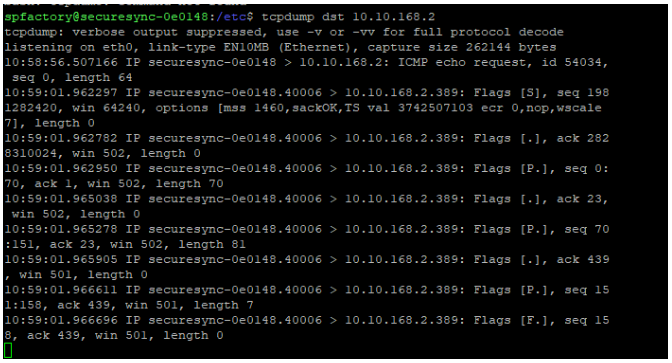
➢ SecureSync pings the configured server to see if its reachable on the network.

➢ Mantis case 2834 (software versions 5.1.4 and 5.1.5): “LDAP Servers status” reports "Configuration missing" even though LDAP is working just fine (“Servers Status” was improved in version 5.2.0)

Displays one of the following states:

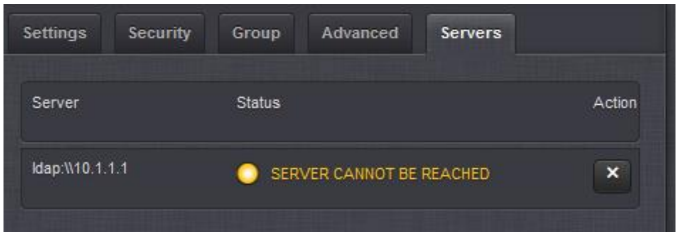
- **Reachable (green):** indicates LDAP configuration is valid, an LDAP server that has been set up is available and is able to pass data. The configured LDAP server is responding to ping (reachable on the network)

Tcpdump screenshot below shows the ICMP (Ping) packets sent to the LDAP server, as soon as LDAP is “Enabled” in the Settings tab.



```
spfactory@securesync-0e0148:/etc$ tcpdump dst 10.10.168.2
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:58:56.507166 IP securesync-0e0148 > 10.10.168.2: ICMP echo request, id 54034,
 seq 0, length 64
10:59:01.962297 IP securesync-0e0148.40006 > 10.10.168.2.389: Flags [S], seq 198
1282420, win 64240, options [mss 1460,sackOK,TS val 3742507103 ecr 0,nop,wscale
7], length 0
10:59:01.962782 IP securesync-0e0148.40006 > 10.10.168.2.389: Flags [.], ack 282
8310024, win 502, length 0
10:59:01.962950 IP securesync-0e0148.40006 > 10.10.168.2.389: Flags [P.], seq 0:
70, ack 1, win 502, length 70
10:59:01.965038 IP securesync-0e0148.40006 > 10.10.168.2.389: Flags [.], ack 23,
 win 502, length 0
10:59:01.965278 IP securesync-0e0148.40006 > 10.10.168.2.389: Flags [P.], seq 70
:151, ack 23, win 502, length 81
10:59:01.965905 IP securesync-0e0148.40006 > 10.10.168.2.389: Flags [.], ack 439
, win 501, length 0
10:59:01.966611 IP securesync-0e0148.40006 > 10.10.168.2.389: Flags [P.], seq 15
1:158, ack 439, win 501, length 7
10:59:01.966696 IP securesync-0e0148.40006 > 10.10.168.2.389: Flags [F.], seq 15
8, ack 439, win 501, length 0
```

- **Server cannot be reached (orange/yellow)**



Server	Status	Action
ldap:\\10.1.1.1	● SERVER CANNOT BE REACHED	✕

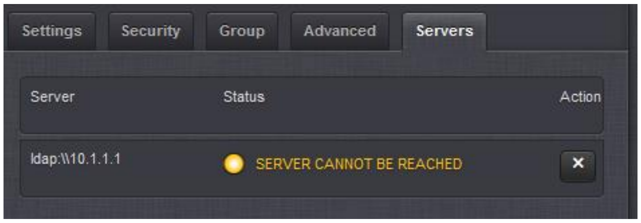
CONFIGURATION MISSING (red): No configuration files are available.

LDAP may not be configured in SecureSync or software versions 5.1.4 or 5.1.5 installed (refer to "**Mantis case 2834**" note above)

- **FAILED TO READ DATA (red):** An LDAP server is available but no data was passed.
- **FAILED NOT REACHABLE (red**): No LDAP server could be reached.
- **LDAP DISABLED**: The Enabled checkbox under the Settings tab as not been selected. (LDAP not Enabled in the Settings tab).
- **"INVALID CONFIGURATION"**: whether configuring the LDAP sever using its IP address or its hostname, this value **MUST** use **URI** format (value must always begin with the following: "**ldap://"**

Examples: **ldap://10.1.1.1** or **ldap://Microsoft.com**

Note: After entering the LDAP server address, if the "**Servers**" tab reports "**server cannot be reached"** **(**instead of "**LDAP Configuration valid")**



Server	Status	Action
ldap:\\10.1.1.1	● SERVER CANNOT BE REACHED	✕

Verify:

- (if using a hostname instead of IP address) DNS is configured correctly and working (try temporarily using its IP address to see if it then connects. If it does, there is a DNS-related issue.
- Whether using the LDAP server's IP address or its hostname, the Server line must begin with ldap:// (and not "ldap:\\").
  - Example above shows the wack/wack going in the wrong direction (instead of \\, it should be //)

LDAP allows more than one account for logging in

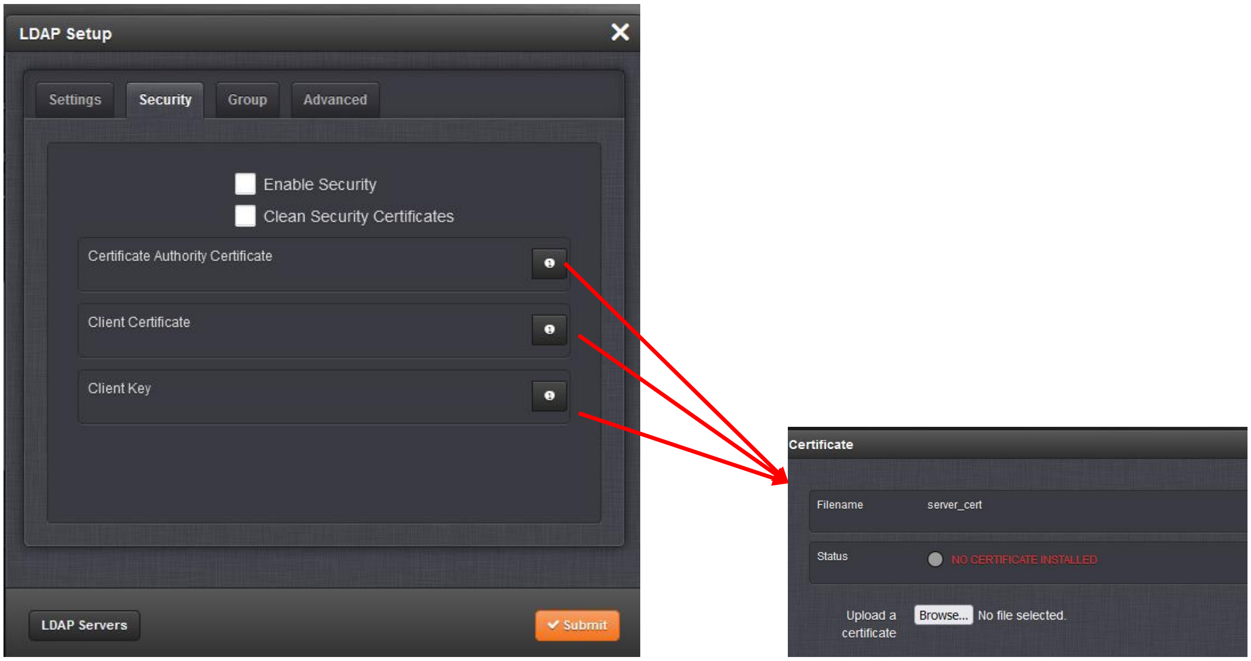
- LDAP allows you to use more than one account for logging in. The Bind DN and password are only used to connect to the server and search for users on it.

***Login access levels (permissions/rights)

- In at least software versions 5.2.0 and below, all authorized LDAP users automatically have admin rights.
    - There is no way to differentiate between admin (Read/Write- “RW”) and user rights (Read Only - “RO”)

3. Security tab (SSL certificate)

A) Version 1.6.0 screenshots



LDAP Setup

Settings | Security | Group | Advanced

□ Enable Security

□ Clean Security Certificates

Certificate Authority Certificate

Client Certificate

Client Key

LDAP Servers | ✓ Submit

Certificate

Filename: server_cert

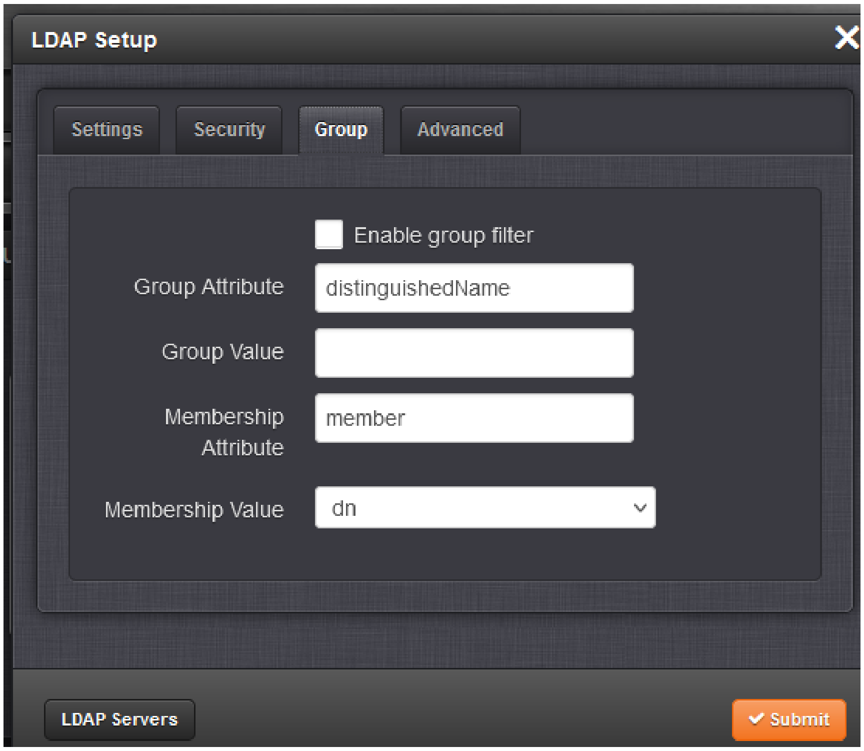
Status: ● NO CERTIFICATE INSTALLED

Upload a certificate: Browse... No file selected.

4. Group Tab (to apply an LDAP Group Filter)

Groups are a quick way of giving users common access to certain features or functionality within an LDAP directory.

Email from Ron Dries (12 Jan 2015) regarding Salesforce case 16840 So I'm not entirely sure if this will work for their setup, but it's currently how I believe group authentication with LDAP works now in the SecureSync.



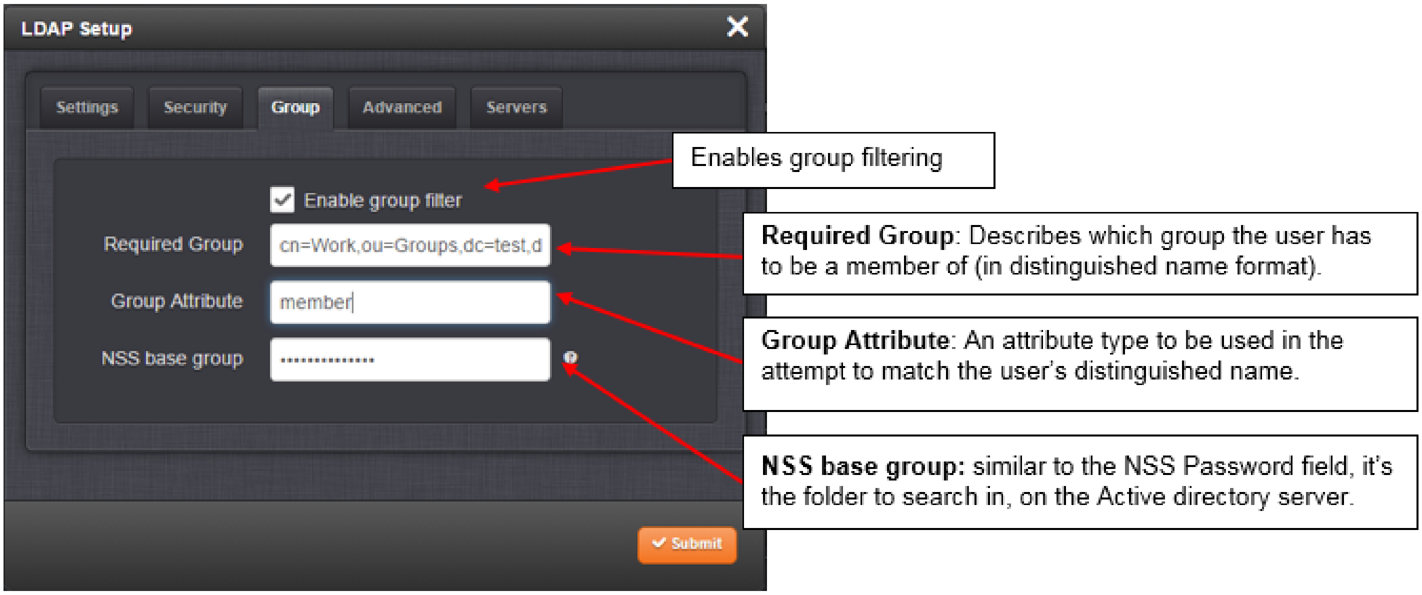
□ Enable group filter

Group Attribute: distinguishedName

Group Value:

Membership Attribute: member

Membership Value: dn



☑ Enable group filter

Required Group: cn=Work,ou=Groups,dc=test,d

Group Attribute: member

NSS base group: •••••••••••••••

Enables group filtering

Required Group: Describes which group the user has to be a member of (in distinguished name format).

Group Attribute: An attribute type to be used in the attempt to match the user's distinguished name.

NSS base group: similar to the NSS Password field, it's the folder to search in, on the Active directory server.

The above image is the group filter configuration tab for LDAP.

- The "**Enable Group filter**" checkbox enables group filtering
- The "**Required Group**" field describes which group the user has to be a member of (in distinguished name format). In the above example it's the group "Work" in the "Groups" organizational unit
- The "**Group attribute"** field is an attribute type to be used in the attempt to match the user's distinguished name.

In the above example, ldap will search the values of the member attribute of the work group looking to see if the user's "distinguished name" is listed.

- The "**NSS Base group"** field is similar to the NSS Password field. It's the folder to search in, on the Active directory server.

I believe that the Required Group and NSS base group fields they have, I'm not sure if they have an attribute on the group which can be used to determine if the user's distinguished name is a member of the group or not.

AD has to support RFC 2307???? (not yet confirmed)

Note from keith (7 Mar 17) I BELIVE the Active Directory's schema must be configured to support RFC 2307 in order to be able to define unix client attributes. Refer to info on "Winbind" with sites such as: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Windows_Integration_Guide/winbind.html#samba

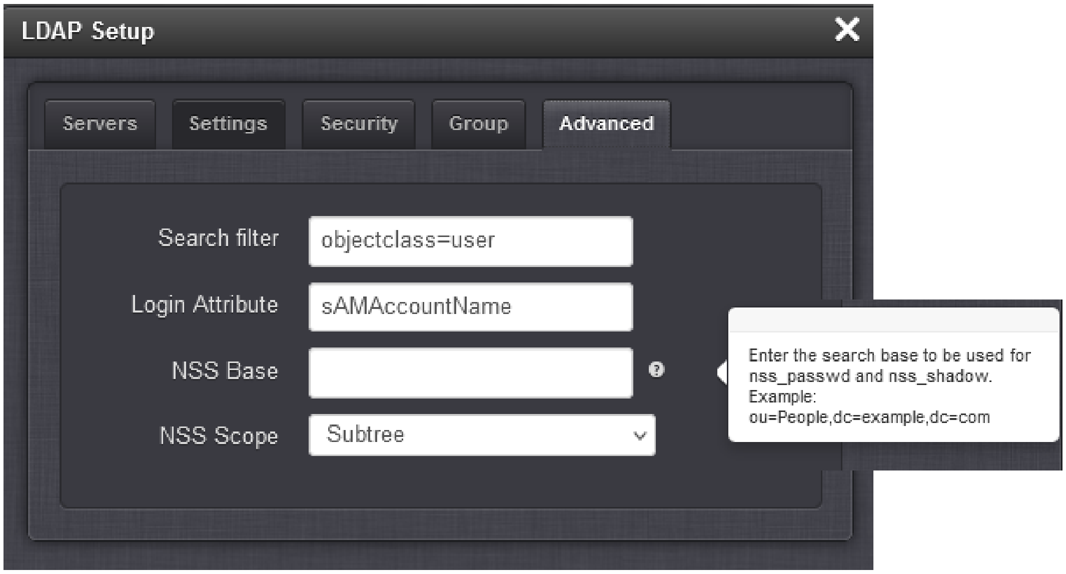
Expert mode for LDAP Group
Currently the GUI is the only method of configuring LDAP on the SecureSync; there is no expert mode for this feature.

"Group filter" being enabled can cause very long delays in logging in (like 20 minutes for instance)

Having the group filter enabled ("groups enabled") can significantly increase the time it takes to authenticate/login (one customer reported it took 20 minutes to login).Disable this checkbox and see if the time it takes to login goes way down. If it does, the SecureSync having to search all of the groups is the reason for the long delay in logging in.

5. Advanced Tab ("Search filter" and "Login Attribute")

With v1.2.1 installed



Search filter: objectclass=user

Login Attribute: sAMAccountName

NSS Base:

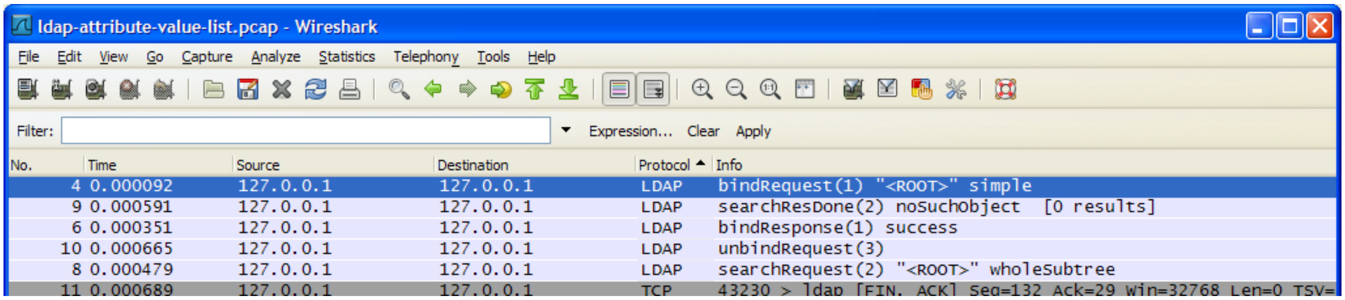
NSS Scope: Subtree

Enter the search base to be used for nss_passwd and nss_shadow. Example: ou=People,dc=example,dc=com

NSS Base

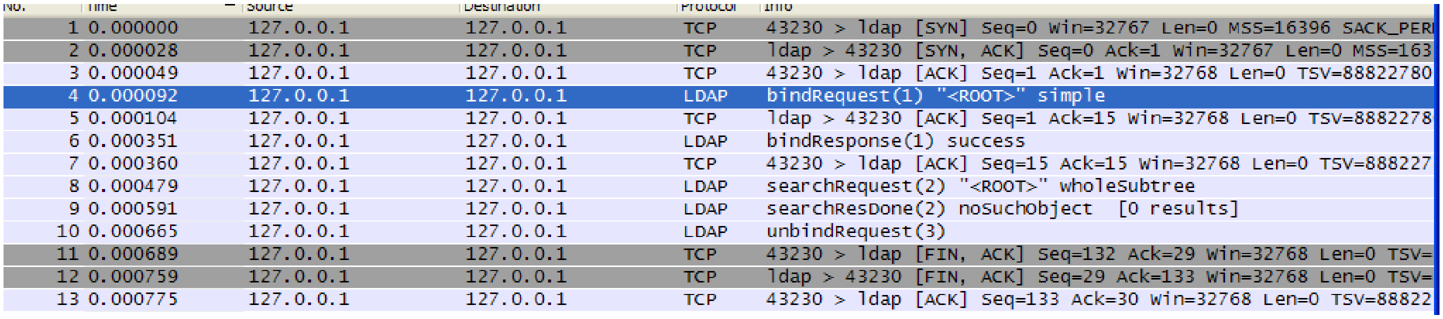
Packet capture analysis

- **Sample LDAP Packet captures:** Refer to http://wiki.wireshark.org/SampleCaptures
- **Sample LDAP packet capture** (showing only LDAP protocol messages)


ldap-attribute-value-list.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
4	0.000092	127.0.0.1	127.0.0.1	LDAP	bindRequest(1) "<ROOT>" simple
9	0.000591	127.0.0.1	127.0.0.1	LDAP	searchResDone(2) noSuchObject [0 results]
6	0.000351	127.0.0.1	127.0.0.1	LDAP	bindResponse(1) success
10	0.000665	127.0.0.1	127.0.0.1	LDAP	unbindRequest(3)
8	0.000479	127.0.0.1	127.0.0.1	LDAP	searchRequest(2) "<ROOT>" wholeSubtree
11	0.000689	127.0.0.1	127.0.0.1	TCP	43230 > ldap [FIN, ACK] Seq=132 Ack=29 Win=32768 Len=0 TSV=

(Same sample capture showing both LDAP and TCP protocol messages)



No.	Time	Source	Destination	Protocol	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	43230 > ldap [SYN] Seq=0 Win=32767 Len=0 MSS=16396 SACK_PERI
2	0.000028	127.0.0.1	127.0.0.1	TCP	ldap > 43230 [SYN, ACK] Seq=0 Ack=1 Win=32767 Len=0 MSS=163
3	0.000049	127.0.0.1	127.0.0.1	TCP	43230 > ldap [ACK] Seq=1 Ack=1 Win=32768 Len=0 TSV=88822780
4	0.000092	127.0.0.1	127.0.0.1	LDAP	bindRequest(1) "<ROOT>" simple
5	0.000104	127.0.0.1	127.0.0.1	TCP	ldap > 43230 [ACK] Seq=1 Ack=15 Win=32768 Len=0 TSV=8882278
6	0.000351	127.0.0.1	127.0.0.1	LDAP	bindResponse(1) success
7	0.000360	127.0.0.1	127.0.0.1	TCP	43230 > ldap [ACK] Seq=15 Ack=15 Win=32768 Len=0 TSV=888227
8	0.000479	127.0.0.1	127.0.0.1	LDAP	searchRequest(2) "<ROOT>" wholeSubtree
9	0.000591	127.0.0.1	127.0.0.1	LDAP	searchResDone(2) noSuchObject [0 results]
10	0.000665	127.0.0.1	127.0.0.1	LDAP	unbindRequest(3)
11	0.000689	127.0.0.1	127.0.0.1	TCP	43230 > ldap [FIN, ACK] Seq=132 Ack=29 Win=32768 Len=0 TSV=
12	0.000759	127.0.0.1	127.0.0.1	TCP	ldap > 43230 [FIN, ACK] Seq=29 Ack=133 Win=32768 Len=0 TSV=
13	0.000775	127.0.0.1	127.0.0.1	TCP	43230 > ldap [ACK] Seq=133 Ack=30 Win=32768 Len=0 TSV=88822

Understanding LDAP traffic

When you look at the Info column, you will see several different types data.

- **bindRequest()** This to be authentication request from us to the ldap server
- **bindResponse()**This is the response from the ldap server (domain controller) in response to our bindRequest().
- **SASL GSS-API Integrity: searchRequest()**This is a request to the ldap server. If you look in the middle pane of Wireshark, you will see a collapsed section called *Lightweight-Directory-Access-Protocol* | *SASL Buffer* | *GSS-API payload* | *LDAPMessage searchRequest().* Here you will see specifics of what you are requesting from the ldap server. In particular, you can drill down to *protocolOp: searchRequest().* Here you can see the *Filter* (this is the actual ldap query sent) that was used. You can also see the *attributes* that were requested. You can also see the *baseObject* here.

In terms of SQL, this is basically like the select statement.

- **Filter** = SQL where clause
- **attributes** = SQL list of columns to select
- **baseObject** = roughly translates to a SQL table, but more just specifying at what level in the ldap tree the search should take place.

SASL GSS-API Integrity: searchResEntry()

This is the response to the *searchRequest()* request from the ldap server. If you look in the middle pane of Wireshark, you will see a collapsed section (unless you already opened it :) called *Lightweight-Directory-Access-Protocol* | *SASL Buffer* | *GSS-API payload* | *LDAPMessage searchResEntry().* Each *LDAPMessage searchResEntry()* is a result from the ldap server. This is essentially a row or record. So, if the query found 7 matches, then you should have 7 *LDAPMessage searchResEntry()* here. You can expand each *LDAPMessage searchResEntry()* to see the exact objectName, and the values.

Here you will see specifics of what the response from the ldap server. In particular, you can drill down to *protocolOp: searchRequest().* Here you can see the *Filter* (this is the actual ldap query sent) that was used. You can also see the *attributes* that were requested. You can also see the *baseObject* here.

SASL GSS-API Integrity: unbindRequest()
This is the disconnect from the ldap server. The clean up. The thing that tells the ldap server that we are done with it.

***Known issues with OpenLDAP/Active Directory

Ability to disable LDAP/Radius via the front panel (carry-over from 1200s)

- resetpw (in the front panel “cmd” menu) disables LDAP/Radius??
  - Refer to Mantis case 3026

resetpw also sets LDAP and Radius to “Disabled” to help prevent total lockout. They need to be re-enabled thereafter, if desired

When resetpw command is performed, and if LDAP and/or Radius were intentionally enabled, they will need to be re-enabled after performing a resetpw.

Q help to clarify that if the RESETPW on panel LCD is used, will it erase all the machine configuration to default or just reset the spadmin password to default value?

A Keith’s response (23 May 17)   Unlike the CLEAN command, the RESETPW command will NOT erase all the configurations back to default. The RESETPW command only resets the spadmin account password back to the default value of ‘admin123’.

Note that in software versions 5.2.1 and above, the RESETPW command also disables Radius and LDAP remote authentication services (if enabled for use). This command doesn’t change the configurations for these two services. It just unselects the checkbox which enables/disables the functionality of these services. So after performing a RESETPW command, the enable checkbox(es) for LDAP and/or Radius need to be reselected, if using either or both of these authentication services.

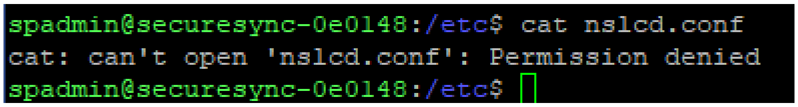
Group authentication doesn’t work/do anything (at least versions 1.2.2 and below)

- Expected to be fixed in version 1.3.0 update (~Nov 2021)

***Troubleshooting LDAP (2400s)

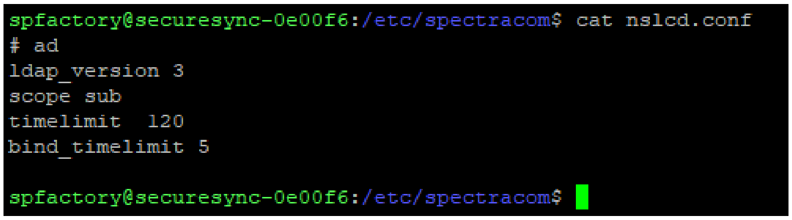
Note: The ldap conf file (“**nslcd.conf”** in 2400s) is located in **/etc/ directory**

1) cat the “**nslcd.conf**” ldap config file (/etc/) (in at least v1.6.0 and below, **spadmin** account **CANNOT** view this file. Get the unit’s configs bundle to view the file’)



```
spadmin@securesync-0e0148:/etc$ cat nslcd.conf
cat: can't open 'nslcd.conf': Permission denied
spadmin@securesync-0e0148:/etc$
```

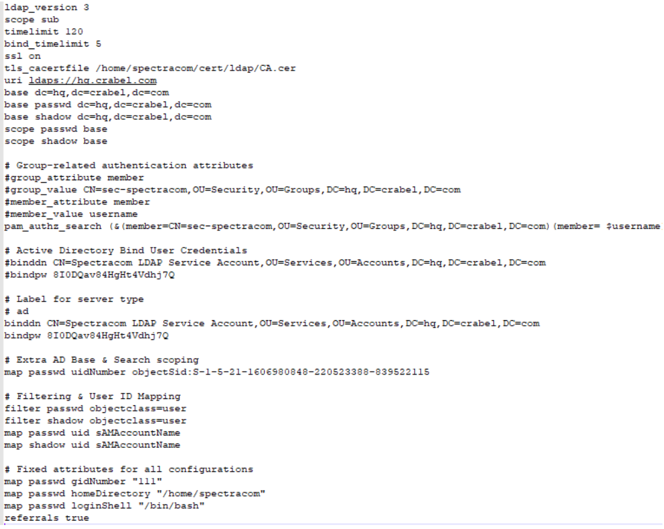
Factory default nslcd.conf file (ldap not yet configured)



```
spfactory@securesync-0e00f6:/etc/spectracom$ cat nslcd.conf
# ad
ldap_version 3
scope sub
timelimit  120
bind_timelimit 5

spfactory@securesync-0e00f6:/etc/spectracom$
```

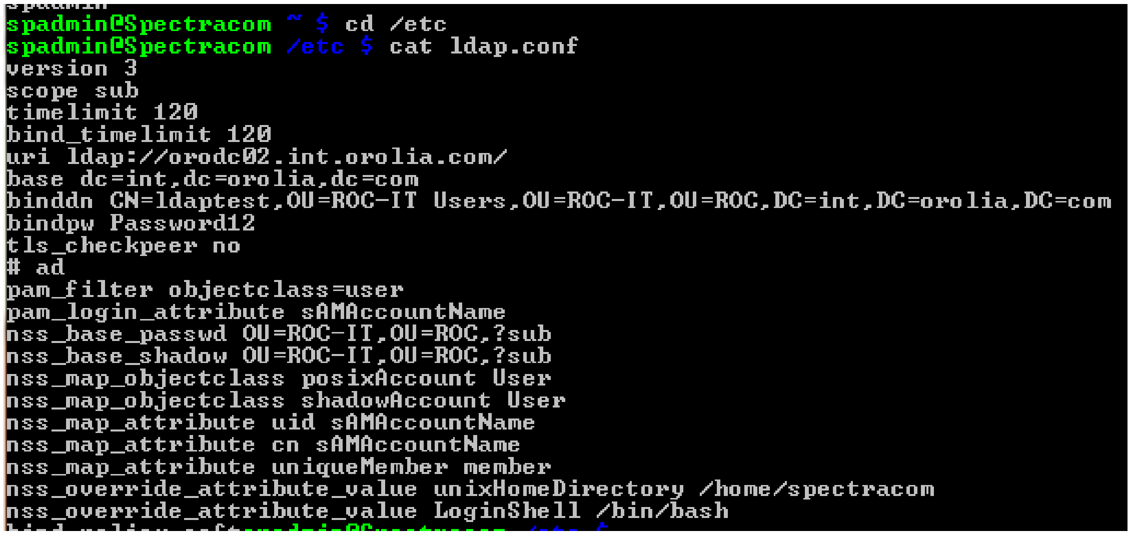
Sample nslcd.conf file after configuring our unit for IT’s LDAP server (not able to test)

From a Customer’s 2400 SecureSync (LDAP NOT working, Salesforce Case 273203)



```
ldap_version 3
scope sub
timelimit 120
bind_timelimit 5
ssl on
tls_cacertfile /home/spectracom/cert/ldap/CA.cer
uri ldaps://hq.crabel.com
base dc=hq,dc=crabel,dc=com
base passwd dc=hq,dc=crabel,dc=com
base shadow dc=hq,dc=crabel,dc=com
scope passwd base
scope shadow base

# Group-related authentication attributes
#group_attribute member
#group_value CN=sec-spectracom,OU=Security,OU=Groups,DC=hq,DC=crabel,DC=com
#member_attribute member
#member_value username
pam_authz_search (&(member=CN=sec-spectracom,OU=Security,OU=Groups,DC=hq,DC=crabel,DC=com)(member= $username

# Active Directory Bind User Credentials
#binddn CN=Spectracom LDAP Service Account,OU=Services,OU=Accounts,DC=hq,DC=crabel,DC=com
#bindpw 8I0DQav84HgHt4Vdhj7Q

# Label for server type
# ad
binddn CN=Spectracom LDAP Service Account,OU=Services,OU=Accounts,DC=hq,DC=crabel,DC=com
bindpw 8I0DQav84HgHt4Vdhj7Q

# Extra AD Base & Search scoping
map passwd uidNumber objectSid:S-1-5-21-1606980848-220523388-839522115

# Filtering & User ID Mapping
filter passwd objectclass=user
filter shadow objectclass=user
map passwd uid sAMAccountName
map shadow uid sAMAccountName

# Fixed attributes for all configurations
map passwd gidNumber "111"
map passwd homeDirectory "/home/spectracom"
map passwd loginShell "/bin/bash"
referrals true
```

1200 SecureSync ldap.conf fIle for comparison



```
spadmin@Spectracom ~ $ cd /etc
spadmin@Spectracom /etc $ cat ldap.conf
version 3
scope sub
timelimit 120
bind_timelimit 120
uri ldap://orodc02.int.orolia.com/
base dc=int,dc=orolia,dc=com
binddn CN=ldaptest,OU=ROC-IT Users,OU=ROC-IT,OU=ROC,DC=int,DC=orolia,DC=com
bindpw Password12
tls_checkpeer no
# ad
pam_filter objectclass=user
pam_login_attribute sAMAccountName
nss_base_passwd OU=ROC-IT,OU=ROC,?sub
nss_base_shadow OU=ROC-IT,OU=ROC,?sub
nss_map_objectclass posixAccount User
nss_map_objectclass shadowAccount User
nss_map_attribute uid sAMAccountName
nss_map_attribute cn sAMAccountName
nss_map_attribute uniqueMember member
nss_override_attribute_value unixHomeDirectory /home/spectracom
nss_override_attribute_value LoginShell /bin/bash
```

1) Is LDAP login to classic interface browser successful? If it is, the LDAP Server settings are valid.

2) Get at least the full **Auth log, System log, User log** and **Journal log** (or just get a full log bundle)

3) Review the **Auth, USER and System** log (especially the User logs which logs errors)

4) Make sure LDAP port 389 (and 636 for SSL) is open on firewalls between the SecureSync and Radius server:

5) Make sure the main default port/gateway is configured properly so that the SecureSync can route to the LDAP server.

   Partial email from Keith (20 Oct 16) Is the configured LDAP server on the same subnet as the SecureSync' Ethernet interface(s? If its not on the same subnet as the base Ethernet port "eth0" (or one of the three additional Ethernet interfaces, if the Model 1204-06 Gb Ethernet Option Card is installed), please ,make sure the correct main default port/gateway is configured correctly so that the SecureSync knows how to be routed to the LDAP server (as configured in the **Management** -> **Network Setup** page of the web browser. On the left side of this page, press the **General Settings** button and select the correct **Default Port** drop-down).

6) Make sure DNS is setup correctly if using hostname of the LDAP server (try temporarily using an IP address instead of the hostname. If it connects, issue is related to DNS).

   Partial email from Keith (20 Oct 16) Is the LDAP server specified in the **Management** -> **Authentication** -> **LDAP Setup** page of the browser (Servers tab) using its IP address or its DNS name? If its configured using its DNS name, try at least temporarily changing its name to its IP address and then try logging in again to the LDAP server. If it now allows the SecureSync to connect to the LDAP server, the issue is associated with DNS identifying the LDAP server.

7) **"NSS password" field left blank:** login will take a long time but will still result in a successful login.

NTPSERVER sudo: nss_ldap: failed to bind to LDAP server ldap://10.0.100.30: Invalid credentials
NTPSERVER sudo: nss_ldap: could not search LDAP server - Server is unavailable

- ➢ (Note: not sure if these entries were from the Auth log or the User log)

Appears to be associated with the LDAP Bind password for connecting with the LDAP sever (not the ldap login itself)

- Make sure the account being used has sufficient permissions to be able to “search the databbse”

- This particular customer (who saw the error message above) was initially using special characters in their Bind DN and/or Bind password. Worked fine after removing the special characters:
  - “I changed the password for the BIND and that fixed the problem. Apparently it didn't like one of the special characters. I was using a password with **&#($** in it”

Authorization log entries

- **Note:** Valid LDAP logins do not result in any Auth (or USER) log entries.
- **“Entity”** value for LDAP login log entries**:** httpd

Example entries for all LDAP configs correct. But wrong password for the LDAP login account was entered.

```
Jul 06      httpd   pam_unix(httpd:auth): authentication failure; logname= uid=1001 euid=1001 tty= ruser= rhost=10.15.252.52
11:31:26            user=adbella
Jul 06      httpd   pam_ldap(httpd:auth): Authentication failure; user=adbella
11:31:04
```

User log entries

- **Note:** Valid LDAP logins do not result in any User (or Auth) log entries.
- **Note:** to see the latest entry of the user log in CLI connection: **tail -f log/user.log**

```
apache2: pam_ldap: missing “host” in file “/etc/ldap.con
```

Cause: “**Servers**” tab of the **Management** -> **LDAP** page of the browser does not have any LDAP servers listed.

```
apache2: pam_ldap: ldap_initialize Bad parameter to an ldap routine
```

Cause: Can’t find the LDAP server on the network

Possible reasons

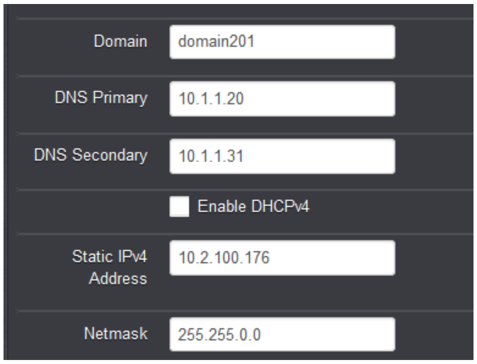
- **IP address**- when using the LDAP server’s IP address, the IP address MUST be in URI format (the configured IP address must begin with the following: **ldap:// (example: ldap://xxx.xxx.xxx.xxx)**
- **DNS hostname**: when using the LDAP server’s hostname, the hostname MUST be in URI format (the configured hostname must begin with the following: **ldap:// (example: ldap://icrosoft.com)**
- **Configured LDAP server isn’t an LDAP server** (SecureSync can reach it, but it’s not an LDAP server).

  Note: I saw this here by adding a second LDAP server using the IP address of one of our SecureSyncs (10.2.100.176). LDAP login was not successful, even though other server was fine (Deleted this second “server” and logged in successfully)
- “**Servers**” tab of the **Management** -> **LDAP** page of the browser does not have a valid or LDAP Server address configured.

- If a hostname is listed instead of an address, could be DNS is not configured correctly in the Management -> Network page of the browser, (Gear box ICON the particular network interface). Try temporarily using its IP address.
- LDAP server requires SSL connection, but the LDAP Server's certificates/keys aren't loaded.

Email from Keith (8 Sept 2014) Does your LDAP server require an encrypted SSL connection? If it does, make sure port 636 is also open on any firewalls and go to the **Management** -> **Authentication** page of the browser**, LDAP Setup** button (where the LDAP settings are). Make sure the server and client certificates and Client key for your LDAP server are properly installed (click on the "I" ICON next to each of these settings to verify whether or not they are currently installed, as may be required by your LDAP server. If it's required, and these aren't loaded or are invalid, the SecureSync won't be able to communicate with the LDAP server.

- **Main default gateway issue.**



Domain: domain201
DNS Primary: 10.1.1.20
DNS Secondary: 10.1.1.31
□ Enable DHCPv4
Static IPv4 Address: 10.2.100.176
Netmask: 255.255.0.0

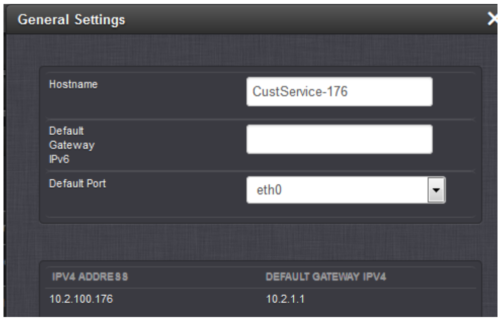
Email from Keith (8 Sept 2014) Go to the **Management** -> **Authentication** page of the browser**, LDAP Setup button** (where the LDAP settings are). Then click on the **Servers** tab at the top. As shown below, the LDAP server's IP address or hostname should be listed.

Is the Server's IP address or its hostname listed in this pop-up window? Either way, make sure this value is correct for that server. If it's the hostname one suggestion is temporarily enter a "new server" using its IP address instead of its hostname and fill in the rest of the configuration for that server. Logout and login using the correct credentials.

If login was successful, the issue is related to DNS configuration. Go to the **Management** -> **Network** page of the browser. Click on the gear box for the Ethernet port that goes to the LDAP server. Verify the domain and DNS server(s) are entered correctly for the network. Also verify the main default port/gateway address is configured correctly (**Management** -> **General Settings)** page of the browser.

apache2: pam_ldap: ldap_simple_bind Can't contact LDAP server

- Cause: can't reach the LDAP server on the network
- I saw it here when there was an error in the default gateway address for Eth0. So it wasn't able to reach the LDAP server. Management -> General Setup page of the browser a

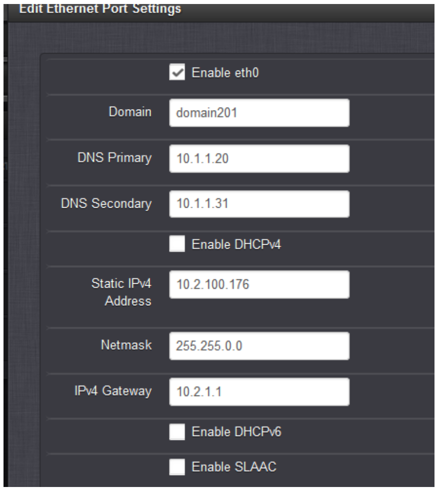


General Settings

Hostname: CustService-176
Default Gateway IPv6:
Default Port: eth0

IPV4 ADDRESS	DEFAULT GATEWAY IPV4
10.2.100.176	10.2.1.1

- DNS- Also saw it here when the DNS sever values were deleted. DNS has to be setup correctly if using the DNS hostname for the LDAP server (instead of configuring its IP address). DNS is configured in the Management -> Network page of the browser and edit the particular port that goes to the DNS server.



Edit Ethernet Port Settings

☑ Enable eth0

Domain: domain201

DNS Primary: 10.1.1.20

DNS Secondary: 10.1.1.31

□ Enable DHCPv4

Static IPv4 Address: 10.2.100.176

Netmask: 255.255.0.0

IPv4 Gateway: 10.2.1.1

□ Enable DHCPv6

□ Enable SLAAC

apache2: pam_ldap: error trying to bind as user "CN=ldaptest,OU=ROC-IT Users,OU=ROC-IT,OU=ROC,DC=int,DC=orolia,DC=com" (Invalid credentials)
Causes (**Management** -> **Authentication** -> page of the browser, **LDAP Setup** button)

- Valid account name but invalid password OR
- invalid account name

apache2: pam_ldap: ldap_search_s Referral
Cause: invalid "Search Base DN" field (**Management** -> **Authentication** -> page of the browser, **LDAP Setup** button)

apache2: pam_ldap: ldap_search_s Invalid DN syntax
Cause (Note there may be more than one reason)

- I saw it here and couldn't login when there was an error in the **NSS password**" field (I cleared this field and resolved this entry).

apache2: pam_ldap: error trying to bind (Invalid credentials)
Cause:

- invalid "**Bind DN**" field OR
- invalid "**Bind password**" field
- invalid "**NSS password**" field (note that successful LDAP login can still occur if this field is left null or possibly if it's incorrect, but this log entry is asserted if the correct value is not entered).

apache2: pam_ldap: ldap_search_s Operations error
Cause (Note there may be more than one reason)

I saw it here when there was a missing comma in the **NSS password** field (**Management** -> **Authentication** -> page of the browser, **LDAP Setup** button).

apache2: could not search LDAP server - Server is unavailable
Cause: issue with LDAP server or with its associated network

TACACS + (Remote authentication)

TACACS+ info (in online 2400 SecureSync user guide):
https://www.orolia.com/manuals/2400/Content/NC_and_SS/Com/Topics/ADMIN/TACACS.htm

What is TACACS

- Refer also to RFC 1492: https://tools.ietf.org/html/rfc1492

(From Wikipedia) **Terminal Access Controller Access-Control System** (**TACACS**) is a remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks. TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network. TACACS is defined in RFC 1492, and uses (either TCP or UDP) port 49 by default.

TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon or simply TACACSD. TACACSD uses TCP and usually runs on port 49. It would determine whether to accept or deny the authentication request and send a response back. The TIP (routing node accepting dial-up line connections, which the user would normally want to log in into) would then allow access or not, based upon the response. In this way, the process of making the decision is "opened up" and the algorithms and data used to make the decision are under the complete control of whomever is running the TACACS daemon.
A later version of TACACS introduced by Cisco in 1990 was called **Extended TACACS** (**XTACACS**). The XTACACS protocol was developed by and is proprietary to Cisco Systems.

Terminal Access Controller Access-Control System Plus (**TACACS+**) is a protocol developed by Cisco and released as an open standard beginning in 1993. Although derived from TACACS, TACACS+ is a separate protocol that handles authentication, authorization, and accounting (AAA) services. TACACS+ and other flexible AAA protocols have largely replaced their predecessors.

TACACS+ and RADIUS have generally replaced TACACS and XTACACS in more recently built or updated networks. TACACS+ is an entirely new protocol and is not compatible with TACACS or XTACACS. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP). Since TCP is connection oriented protocol, TACACS+ does not have to implement transmission control. RADIUS, however, does have to detect and correct transmission errors like packet lost, timeout etc. since it rides on UDP which is connectionless. RADIUS encrypts only the users' password as it travels from the RADIUS client to RADIUS server. All other information such as the username, authorization, accounting are transmitted in clear text. Therefore it is vulnerable to different types of attacks. TACACS+ encrypts all the information mentioned above and therefore does not have the vulnerabilities present in the RADIUS protocol.

Tacacs AAA (Authentication, Authorization, Accounting)

- TACACS can do much more (Authentication, Authorization, Accounting) than what the SecureSync supports
- SecureSync only supports Tacacs for **Authentication** (it doesn’t support **Authorization** or **Accounting**)

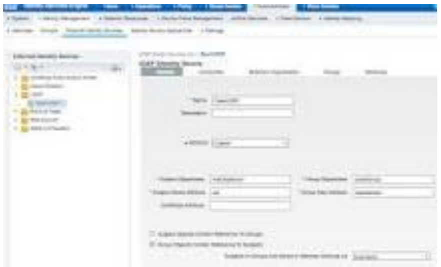
(Below Is from: https://www.networkworld.com/article/2838882/radius-versus-tacacs.html**)**

Before allowing and entity to perform certain actions, you must:

2) Ensure you know who that entity actually is (**Authentication**) (Supported in SecureSync)
3) And if the entity is authorized to perform that action (**Authorization**).
4) Additionally, you need to ensure that accurate records are maintained showing that the action has occurred, so you keep a security log of the events (**Accounting**).

Cisco ISE (Identity Services Engine)

What is ISE TACACS+ Server



Cisco ISE is **a security policy management platform that provides secure access to network resources**. Cisco ISE functions as a policy decision point and enables enterprises to ensure compliance, enhance infrastructure security, and streamline service operations.

Cisco ISE apparently not supported in 1200 SecureSyncs (and likely 2400s)

- Refer to Salesforce Cases such as **283987** (and JIRA ticket **DMND-1842**, submitted 12 Aug 2022, for Model 2400 SecureSyncs)
- Appears to be due to SecureSyncs not supporting TACACS Authorization functionality (not sure whether TACACS Accounting functionality is also required by ISE)

TACACS users can login to the browser or CLI interface

Per Ron Dries (19 May 2020, as of at least v5.8.9 and below) TACACS+ users can login via the CLI and GUI.

TACACS security

What method is the SecureSync using for TACACS auth protocol (PAP, CHAP, EAP)?

5) Tacacs+ uses TCP port 49

Q One follow up question: what method is the SecureSync using for TACACS auth protocol? PAP, CHAP, EAP?

A Reply from Pritam (16 June 2020) TACACS uses TCP protocol so it will not use any PAP, CHAP or EAP type authentication method. In fact TACACS demon will encrypt entire communication between the Server and the client/NAS hence do not require authentication method.. If more details is needed it can be found in RFC 1492.

And I do not know why our manual is asking either PAP or Global methods. One thing I can think of is – TACACS+ has compatibility for PAP method when the P2P protocols (Not Ethernet - like SDH, ATM, Frame Relay) are in use.

Packet Encryption

Info below from https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html#comp_udp_tcp

RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting, can be captured by a third party.

TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether the body is encrypted or not. For debugging purposes, it is useful to have the body of the packets unencrypted. However, during normal operation, the body of the packet is fully encrypted for more secure communications.

Configuration of the Tacacs server itself/Message types

From: *https://www.networkworld.com/article/2838882/radius-versus-tacacs.html*

TACACS+ communication between the client and server uses different message types depending on the function. In other words, different messages may be used for authentication than are used for authorization and accounting. Another very interesting point to know is that TACACS+ communication will encrypt the entire packet.

Tacacs Authentication messages (we only support Authentication messages):

1) Refer to sites such as: https://tools.ietf.org/id/draft-ietf-opsawg-tacacs-07.html
2) Refer also to **RFC 1492**: https://tools.ietf.org/html/rfc1492

A) The Authentication **START** Packet Body

B) The Authentication **REPLY** Packet Body

C) The Authentication **CONTINUE** Packet Body

Description of Authentication Process

The action, authen_type and authen_service fields (described above) combine to determine what kind of authentication is to be performed Every authentication START, REPLY and CONTINUE packet includes a data field. The use of this field is dependent upon the kind of the Authentication.

A set of standard kinds of authentication is defined in this document. Each authentication flow consists of a START packet. The server responds either with a request for more information (GETDATA, GETUSER or GETPASS) or a termination (PASS or FAIL). The actions and meanings when the server sends a RESTART, ERROR or FOLLOW are common and are described further below.

When the REPLY status equals TAC_PLUS_AUTHEN_STATUS_GETDATA, TAC_PLUS_AUTHEN_STATUS_GETUSER or TAC_PLUS_AUTHEN_STATUS_GETPASS, then authentication continues and the SHOULD provide server_msg content for the client to prompt the user for more information. The client MUST then return a CONTINUE packet containing the requested information in the user_msg field.

All three cause the same action to be performed, but the use of TAC_PLUS_AUTHEN_STATUS_GETUSER, indicates to the client that the user response will be interpreted as a username, and for TAC_PLUS_AUTHEN_STATUS_GETPASS, that the user response represents will be interpreted as a password. TAC_PLUS_AUTHEN_STATUS_GETDATA is the generic request for more information to flexibly support future requirements. If the TAC_PLUS_REPLY_FLAG_NOECHO flag is set in the REPLY, then the user response must not be echoed as it is entered. The data field is only used in the REPLY where explicitly defined below.

Configuration of TACACS + in 2400s

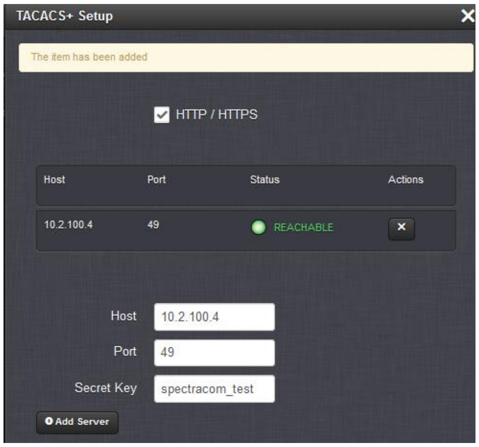
B) Our Tacacs server settings for testing Tacacs (note this info may have since changed)

Server: 10.10.241.249

Port: 49

secret key: spectracom_test (all lower-case)

after pressing "add Server"



TACACS+ Setup

The item has been added

☑ HTTP / HTTPS

Host	Port	Status	Actions
10.2.100.4	49	● REACHABLE	✕

Host: 10.2.100.4

Port: 49

Secret Key: spectracom_test

Test account to login as (this account shouldn't be added to the SecureSync)

User name: testuser

password: testpwd (all lower-case)

C) Configuration of fielded 1200 SecureSyncs

- Refer to online 2400 SecureSync user guide at: https://www.orolia.com/manuals/2400/Content/NC_and_SS/Com/Topics/ADMIN/TACACS.htm
- Refer to Cisco's "TACACS+ Configuration Guide" (https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/xe-16/sec-usr-tacacs-xe-16-book/sec-usr-tacacs-att-value-pairs.html
- (Apparently in at least 2400 v1.6.0 and below) SecureSync only uses the Tacacs account for Authentication (The SecureSync doesn't support AAA -authentication, authorization, accounting)
- Tacacs server should work with just fine with a generic TACACS config

Q (From 1200 SecureSync Case 236694) "I'd like to get additional details on setting up TACACS+ on the SecureSync. The instructions provide no details beyond how to add the TACACS+ server, **but I need to know what kind of TACACS+ response the SecureSync expects**. For example, what kind of response should I send for authorization. I tried using LDAP and RADIUS, but the LDAP requirements for having homeDirectory, loginShell, etc for the user's won't work for us. And RADIUS only supporting PAP isn't secure enough for us to use. So any guidance on TACACS+ would be greatly appreciated.

A Reply from Pritam (16 June 2020) "They would need to create a user account in their TACACS server that can be authenticated. Our SecureSync only uses the TACACS account for Authentication."

A Reply from Keith to customer (16 June 2030)
My response
In summary, the only configuration necessary to use the Tacacs Authentication functionality supported by the SecureSync, is to:

1) Configure the Tacacs server info in the SecureSync (as you alluded to, and as discussed in the online SecureSync user guide at: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/TACACS.htm

2) Have one or more accounts created on the Tacacs server, which support authentication (can be authenticated). Just make sure the account names (and any derivates of the account names) created on the Tacacs server and desired to be used with the SecureSync, are not also in the SecureSync itself (these include the default account name of "spadmin", and any other accounts which can optionally be created in the SecureSync for local login).

   There should be no "manual configuration" necessary of the response sent to the SecureSync. The Tacacs should send an authentication message when the account credentials are authenticated (the SecureSync only supports the Authentication functionality of the Tacacs protocol).

When a user tries logging into the SecureSync's browser or CLI interface using a Tacacs account (not using "spadmin' or any optional local accounts which may have been created in the SecureSync), the Tacacs server verifies the login credentials entered and then lets the SecureSync know that the user can be logged in as an admin user.

Please let me know you can successfully login to the SecureSync's browser and CLI interface as an admin user, when using valid Tacacs account credentials, after configuring the Tacacs server info in the SecureSync. Thanks in advance.

Adding/Removing a TACACS server

- Refer to online 2400 SecureSync user guide at: https://www.orolia.com/manuals/2400/Content/NC_and_SS/Com/Topics/ADMIN/TACACS.htm

Management **->** ***Authentication*** **-> "TACACS+ Setup" button**

Journal log asserted after adding a TACACS server (1200 SecureSync v5.8.2)
"Saved Tacacs Server data (spadmin)"

TACACS+ User rights/permissions/privileges/role-based authentication (admin/user)

Refer to Salesforce Cases such as 251723 (Nov 2020)

Per Chris Olin (20 Nov 2020) I was able to speak with one of our engineering directors about this today who confirmed it is a planned feature, but is not currently targeted for a future release.

Per Ron Dries (19 May 2020, as of at least v5.8.9 and below) Currently TACACS+ users always have **admin** privileges when logged into SecureSync.

Per Dave Sohn (22 May 2020, as of at least v5.8.9 and below) We do not have currently support role based authentication controls via TACACS+. The only centralized service we currently support with that capability is LDAP. Additionally, we do not have read-only user roles available within SecureSync, just admin and user levels.

Tacacs Attribute info/Attribute-Value (AV) Pairs

- Refer to sites such as: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/xe-16/sec-usr-tacacs-xe-16-book/sec-usr-tacacs-att-value-pairs.html (excerpt below):

Terminal Access Controller Access Control System Plus (TACACS+**) attribute-value (AV) pairs are used to define specific authentication, authorization, and accounting elements in a user profile that is stored on the TACACS+ daemon.**

- ➢ In part, used to assign either Admin or User rights/permissions
- ➢ Not supported (as of at least versions 1.6.0 and below. We only support Authentication- we don't support Authorization and Accounting)
  - ○ Refer to JIRA ticket **DMND-1842**, submitted 12 Aug 2022, for Model 2400 SecureSyncs)

Q I'm in the process of enabling Tacacs+ on our NTP/PTP appliances and the below question is being asked by our Clearpass engineer… If you can get any TACACS+ attribute info from the vendor (ppp:ip AV-pairs) that would be helpful.

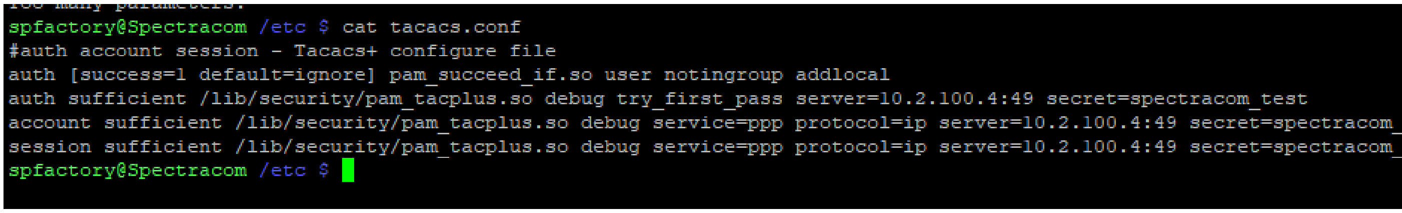
A Per Pritam (31 July 2020) It is correct we only support Authentication part of TACACS+. Authorization and Accounting piece is not supported.

A Reply from Dave L to customer (31 July 2020) We do not support the TACACS+ Attribute Value pairs feature in the Securesync or Velasync products.

(Excerpt from 1200 SecureSyncs)

A) tacacs.conf file is located in /etc folder

Example tacacs.conf file from one of our 5.8.0 units with TACACS login functional

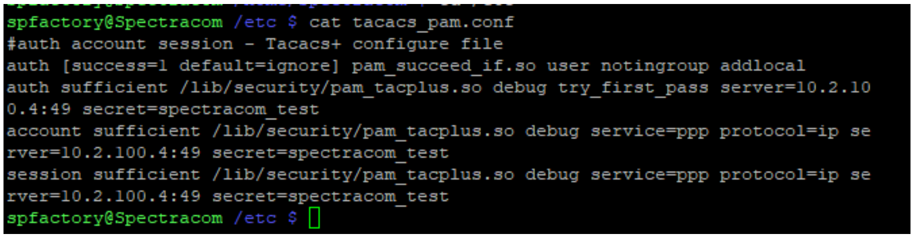


```
Too many parameters.
spfactory@Spectracom /etc $ cat tacacs.conf
#auth account session - Tacacs+ configure file
auth [success=1 default=ignore] pam_succeed_if.so user notingroup addlocal
auth sufficient /lib/security/pam_tacplus.so debug try_first_pass server=10.2.100.4:49 secret=spectracom_test
account sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip server=10.2.100.4:49 secret=spectracom_
session sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip server=10.2.100.4:49 secret=spectracom_
spfactory@Spectracom /etc $ █
```

B) tacacs_pam.conf config file)

Path to tacacs_pam.conf file ***/etc/*** and then type **cat tacacs_pam.conf**

Example tacacs_pam.conf file from one of our units with TACACS login functional



```
spfactory@Spectracom /etc $ cat tacacs_pam.conf
#auth account session - Tacacs+ configure file
auth [success=1 default=ignore] pam_succeed_if.so user notingroup addlocal
auth sufficient /lib/security/pam_tacplus.so debug try_first_pass server=10.2.10
0.4:49 secret=spectracom_test
account sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip se
rver=10.2.100.4:49 secret=spectracom_test
session sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip se
rver=10.2.100.4:49 secret=spectracom_test
spfactory@Spectracom /etc $ ▯
```

TACACS account can't also be a user account created in the unit

Caution: In order to utilize TACACS+ authentication, the account username on the TACACS+ server must NOT be used with a local user account. EXAMPLE: Can't create a username such as "username" in both the TACACS server and in the SecureSync. Create the user account on the TACACS server only (not in the SecureSync also).

- ➢ if the TACACS account name has been added as a user account in the SecureSync, trying to login with the TACACS account name will respond with "**Access Denied**". Delete the user in the **Management** ->

Authorization page of the browser

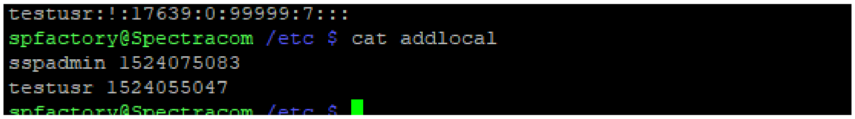
- Refer to online SecureSync guide: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/ADMIN/TACACS.htm

Notes about user account names /. addlocal temporary account

1) The user account name can only be in the TACACS server (the same username can't be in the SecureSync also)

2) The username cannot be the same as any of the account names created by factory default (such as spadmin, spfactory, spui, etc)

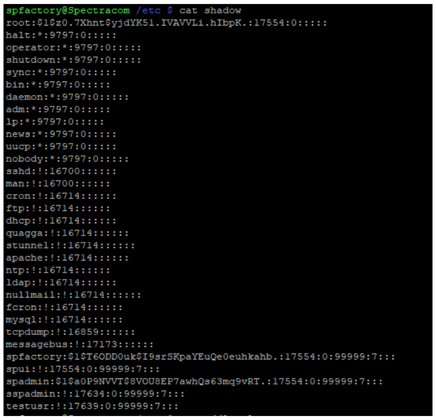
3) each time a TACACS account name is used with a successful CLI login (such as ssh – not with the browser, this account name is temporarily added/stored in a file named addlocal (located in **/etc).** Viewing the contents of "addlocal" will show the custom account names that which been used to login via the CLI interface (to view the contents in ssh, cd to **/etc**, type: **cat addlocal**)



```
testusr:!:17639:0:99999:7:::
spfactory@Spectracom /etc $ cat addlocal
sspadmin 1524075083
testusr 1524055047
spfactory@Spectracom /etc $
```

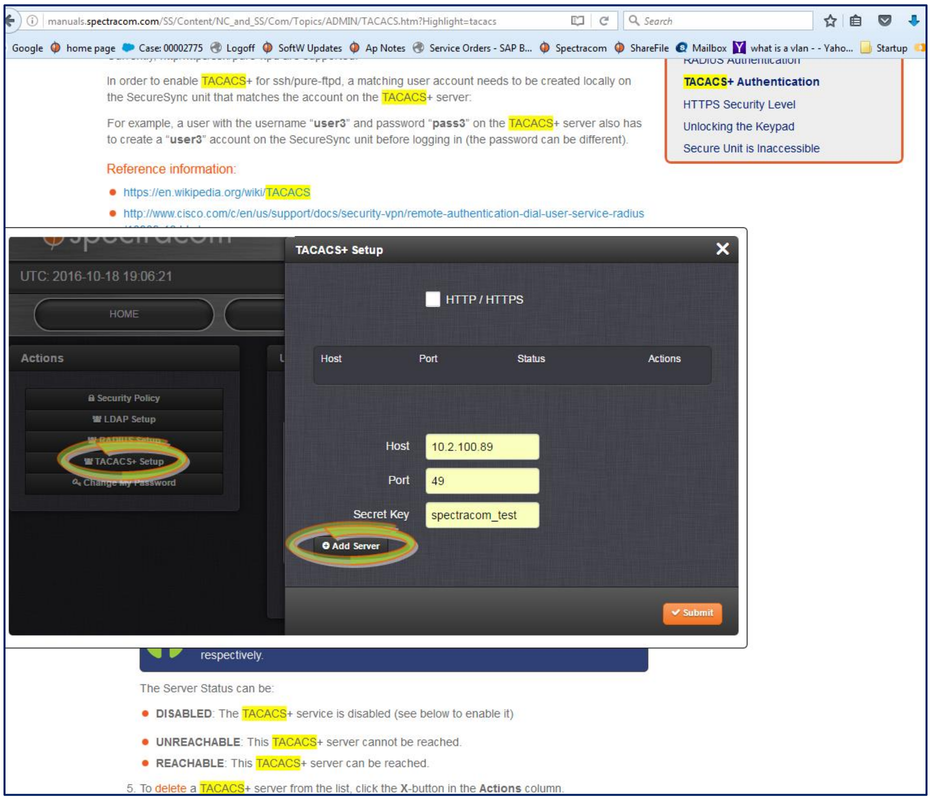
Note: the username(s) is cleared from the addlocal table upon reboot or when performing a "logout" of the cli connection (not just disconnecting out of the service using the "x" button). for instance, type "exit" at our command prompt closes the session and does remove the temp account.

4) (spfactory only- not available as spadmin): While logged into the CLI interface (not applicable to browser login), the TACACS username (same as the one in the addlocal file) will be displayed in **/etc** (to view, type **cd /etc** and type: **cat shadow**)



```
spfactory@Spectracom /etc $ cat shadow
root:$1$z0.7Xhnt$yjdYK5l.IVAVVLi.hIbpK.:17554:0:::::
halt:*:9797:0:::::
operator:*:9797:0:::::
shutdown:*:9797:0:::::
sync:*:9797:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
nobody:*:9797:0:::::
sshd:!:16700::::::
man:!:16700::::::
cron:!:16714::::::
ftp:!:16714::::::
dhcp:!:16714::::::
quagga:!:16714::::::
stunnel:!:16714::::::
apache:!:16714::::::
ntp:!:16714::::::
ldap:!:16714::::::
nullmail:!:16714::::::
fcron:!:16714::::::
mysql:!:16714::::::
tcpdump:!:16859::::::
messagebus:!:17173::::::
spfactory:$1$T6ODD0uk$I9srSKpaYEuQe0euhkahb.:17554:0:99999:7:::
spui:!:17554:0:99999:7:::
spadmin:$1$a0P9NVVT$8VOU8EP7awhQs63mq9vRT.:17554:0:99999:7:::
sspadmin:!:17634:0:99999:7:::
testusr:!:17639:0:99999:7:::
```

Note: exiting out of the cli interface (such as typing "exit" at our command prompt) removes the account name from shadow, very shortly thereafter.



In order to enable TACACS+ for ssh/pure-ftpd, a matching user account needs to be created locally on the SecureSync unit that matches the account on the TACACS+ server.

For example, a user with the username "**user3**" and password "**pass3**" on the TACACS+ server also has to create a "**user3**" account on the SecureSync unit before logging in (the password can be different).

Reference information:

- https://en.wikipedia.org/wiki/TACACS
- http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius

TACACS+ Setup

□ HTTP / HTTPS

Host	Port	Status	Actions

Host: 10.2.100.89

Port: 49

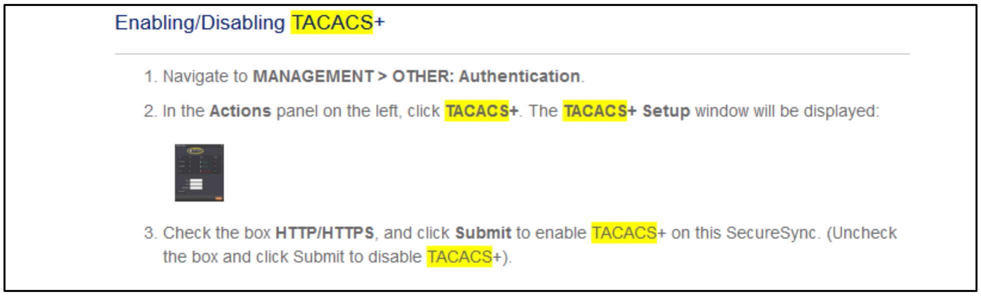
Secret Key: spectracom_test

respectively.

The Server Status can be:

- **DISABLED**: The TACACS+ service is disabled (see below to enable it)
- **UNREACHABLE**: This TACACS+ server cannot be reached.
- **REACHABLE**: This TACACS+ server can be reached.

5. To delete a TACACS+ server from the list, click the **X**-button in the **Actions** column.



Enabling/Disabling TACACS+

1. Navigate to **MANAGEMENT > OTHER: Authentication**.
2. In the **Actions** panel on the left, click **TACACS+**. The **TACACS+ Setup** window will be displayed:
3. Check the box **HTTP/HTTPS**, and click **Submit** to enable TACACS+ on this SecureSync. (Uncheck the box and click Submit to disable TACACS+).

Version-related info for TACACS+

- 2400 SecureSync software support for TACACS+: Added in update version 1.1.0a (Feb 2020)

TACACS operation

A) TACACS login password is sent out unsecure (in the clear/not encrypted)

- Refer to Salesforce cases such as 165341 and JIRA ticket Number SSS-486
- This is the case in at least versions 5.8.0 and below

Email from Mike Sutton (9 Jul KW) The engineering team has reviewed the TACACS KEY displayed in clear text. It appears this is an issue due to debug levels being left on.

I am reaching out to Ryan J. in engineering to see when we can get the fix into an upcoming release. Possibly 5.8.1, but I have to confirm with engineering.

Log entries associated with TACACS

- Auth log, Journal log (user log doesn't seem to log anything about TACACS)

A) Journal log

- Per Keith- only one entry was asserted when I successfully confgured/enabled TACACS on our unit

```
Apr 11 18:24:46 Spectracom Spectracom: [WEB] Saved Tacacs Server data (spadmin)
```

B) Auth Log

1. **"pam_sm_acct_mgmt: returned attribute `PRIV_LVL=15' from server" followed by "pam_unix(useradd:auth): auth could not identify password for [spui]"**

- refer to Salesforce Case 177475

We may've found a subtle difference relating to authentication AND authorization using TACACS (these devices just care about authentication, but we're sending back both authentication and authorization)
For the record, good vs bad logs:

- Prod (failing):

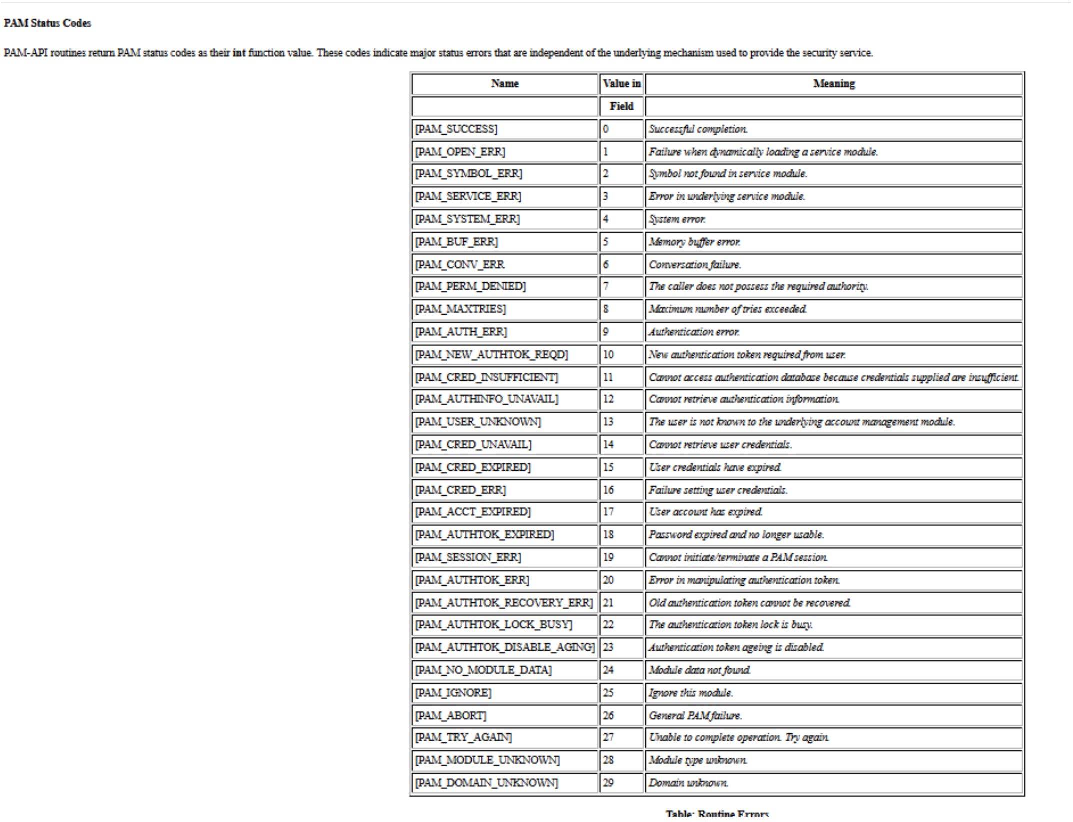
```
Nov  1 14:33:33 time512587gps01-new apache2[32096]: pam_sm_acct_mgmt: active server is [204.27.45.5:49]
Nov  1 14:33:33 time512587gps01-new apache2[32096]: pam_sm_acct_mgmt: sent authorization request
Nov  1 14:33:33 time512587gps01-new apache2[32096]: Args cnt 1
Nov  1 14:33:33 time512587gps01-new apache2[32096]: Adding buf/value pair (priv-lvl,15)
Nov  1 14:33:33 time512587gps01-new apache2[32096]: pam_sm_acct_mgmt: user [<username>] successfully authorized
Nov  1 14:33:33 time512587gps01-new apache2[32096]: pam_sm_acct_mgmt: returned attribute `PRIV_LVL=15' from server
Nov  1 14:33:33 time512587gps01-new apache2[32096]: pam_tally(httpd:account): pam_get_uid; no such user
Nov  1 14:33:33 time512587gps01-new apache2[32096]: pam_unix(httpd:account): could not identify user (from getpwnam(username))
```

- Lab (working):

```
Nov  1 14:35:56 timel097771gps01 apache2[25307]: pam_sm_acct_mgmt: active server is [204.151.176.210:49]
Nov  1 14:35:56 timel097771gps01 apache2[25307]: pam_sm_acct_mgmt: sent authorization request
Nov  1 14:35:56 timel097771gps01 apache2[25307]: Args cnt 1
Nov  1 14:35:56 timel097771gps01 apache2[25307]: Adding buf/value pair (priv-lvl,15)
Nov  1 14:35:56 timel097771gps01 apache2[25307]: pam_sm_acct_mgmt: user [username] successfully authorized
Nov  1 14:35:56 timel097771gps01 apache2[25307]: pam_sm_acct_mgmt: returned attribute `PRIV_LVL=15' from server
Nov  1 14:35:56 timel097771gps01 useradd[31989]: pam_unix(useradd:auth): auth could not identify password for [spui]
Nov  1 14:35:56 timel097771gps01 useradd[31989]: Authentication information cannot be recovered
Nov  1 14:35:56 timel097771gps01 useradd[31989]: failed adding user 'username', data deleted
Nov  1 14:35:56 timel097771gps01 useradd[32003]: pam_unix(useradd:auth): auth could not identify password for [spui]
Nov  1 14:35:56 timel097771gps01 useradd[32003]: Authentication information cannot be recovered
Nov  1 14:35:56 timel097771gps01 useradd[32003]: failed adding user 'username', data deleted
```

2. **"pam_sm_authenticate: exit with pam status: 9" (note the number at the end can vary)**

- table below excerpted from: **http://pubs.opengroup.org/onlinepubs/8329799/chap5.htm**



PAM Status Codes

PAM-API routines return PAM status codes as their **int** function value. These codes indicate major status errors that are independent of the underlying mechanism used to provide the security service.

Name	Value in	Meaning
	Field	
[PAM_SUCCESS]	0	*Successful completion.*
[PAM_OPEN_ERR]	1	*Failure when dynamically loading a service module.*
[PAM_SYMBOL_ERR]	2	*Symbol not found in service module.*
[PAM_SERVICE_ERR]	3	*Error in underlying service module.*
[PAM_SYSTEM_ERR]	4	*System error.*
[PAM_BUF_ERR]	5	*Memory buffer error.*
[PAM_CONV_ERR	6	*Conversation failure.*
[PAM_PERM_DENIED]	7	*The caller does not possess the required authority.*
[PAM_MAXTRIES]	8	*Maximum number of tries exceeded.*
[PAM_AUTH_ERR]	9	*Authentication error.*
[PAM_NEW_AUTHTOK_REQD]	10	*New authentication token required from user.*
[PAM_CRED_INSUFFICIENT]	11	*Cannot access authentication database because credentials supplied are insufficient.*
[PAM_AUTHINFO_UNAVAIL]	12	*Cannot retrieve authentication information.*
[PAM_USER_UNKNOWN]	13	*The user is not known to the underlying account management module.*
[PAM_CRED_UNAVAIL]	14	*Cannot retrieve user credentials.*
[PAM_CRED_EXPIRED]	15	*User credentials have expired.*
[PAM_CRED_ERR]	16	*Failure setting user credentials.*
[PAM_ACCT_EXPIRED]	17	*User account has expired.*
[PAM_AUTHTOK_EXPIRED]	18	*Password expired and no longer usable.*
[PAM_SESSION_ERR]	19	*Cannot initiate/terminate a PAM session.*
[PAM_AUTHTOK_ERR]	20	*Error in manipulating authentication token.*
[PAM_AUTHTOK_RECOVERY_ERR]	21	*Old authentication token cannot be recovered.*
[PAM_AUTHTOK_LOCK_BUSY]	22	*The authentication token lock is busy.*
[PAM_AUTHTOK_DISABLE_AGING]	23	*Authentication token ageing is disabled.*
[PAM_NO_MODULE_DATA]	24	*Module data not found.*
[PAM_IGNORE]	25	*Ignore this module.*
[PAM_ABORT]	26	*General PAM failure.*
[PAM_TRY_AGAIN]	27	*Unable to complete operation. Try again.*
[PAM_MODULE_UNKNOWN]	28	*Module type unknown.*
[PAM_DOMAIN_UNKNOWN]	29	*Domain unknown.*

Table: Routine Errors

3. "pam_sm_acct_mgmt entries"

Note: refer to https://linux.die.net/man/3/pam_acct_mgmt (excerpted below)
http://www.xperiencetech.com/online/tacauthentication.htm

- **PAM_ACCT_EXPIRED** User account has expired.
- **PAM_AUTH_ERR** Authentication failure.
- **PAM_NEW_AUTHTOK_REQD** The user account is valid, but their authentication token is *expired*. The correct response to this return-value is to require that the user satisfies the **pam_chauthtok()** function before obtaining service. It may not be possible for some applications to do this. In such cases, the user should be denied access until such time as they can update their password.
- **PAM_PERM_DENIED** Permission denied.
- **PAM_SUCCESS** The authentication token was successfully updated.
- **PAM_USER_UNKNOWN** User unknown to password service.

Note: refer to: http://www.xperiencetech.com/online/tacauthentication.htm

TACACS+ Specific Authentication

START packet processing

- Authentication method is selected first by authentication type field from the packet.

Authentication action is selected.

- **TAC_PLUS_AUTHEN_CHPASS** (that is "password change" request) and authentication method is not AT_ASCII, ERROR packet is returned back to TACACS+ client.

  If authentication method is AT_ASCII and:

  a) If there's no user name in the packet, TAC_PLUS_AUTHEN_STATUS_GETUSER packet is sent back with a string prompting a user to input his name.
  b) If there's user name in the packet, TAC_PLUS_AUTHEN_STATUS_GETDATA packet is sent back with prompt to a user requesting his old password.

  - **TAC_PLUS_AUTHEN_SENDPASS** (that is "send clear text password to NAS" request) and TACACS+ minor version 0 support is turned off (defined by server configuration), ERROR packet is sent back.
    If no user name is present in the packet, ERROR packet is sent back.

    ICommonAuthentication::GetUserPassword is called next. If it indicates that there is no user known to server extension with such name, TAC_PLUS_AUTHEN_STATUS_FAIL packet is sent, and user is rejected.
    If user is found, but his password is not available in clear text or *ignorePassword* parameter is set to VARIANT_TRUE, TAC_PLUS_AUTHEN_STATUS_FAIL packet is sent, and user is rejected.
    Otherwise, TAC_PLUS_AUTHEN_STATUS_PASS packet is sent back with user's password.

  - **TAC_PLUS_AUTHEN_SENDAUTH** and **authentication type is AT_ASCII, ERROR** packet is sent back. Then server calls ICommonAuthentication::GetUserPassword to get user's password. If it is not available in clear text or no user exists with such name, TAC_PLUS_AUTHEN_STATUS_FAIL response is sent back, TAC_PLUS_AUTHEN_STATUS_PASS response is sent otherwise with authentication data dependant on authentication method.

  - **TAC_PLUS_AUTHEN_LOGIN**, common authentication process is initiated.

CONTINUE packet processing

- If authentication method is not AT_ASCII, ERROR packet is sent back.

If TAC_PLUS_CONTINUE_FLAG_ABORT flag is set, authentication process **terminates**.

  - If action is **TAC_PLUS_AUTHEN_CHPASS**

    a) If server extension does not know user name, old password or new password yet, it issues appropriate response with prompt to a user.

    b) If all authentication information is collected, server calls ICommonAuthentication::SetUserPassword.

- If action is **TAC_PLUS_AUTHEN_LOGIN**

  A) If there's no user name in the packet, **TAC_PLUS_AUTHEN_STATUS_GETUSER** packet is sent back prompting auser to input his name.

  B) If there's user name in the packet, **TAC_PLUS_AUTHEN_STATUS_GETPASS** response is sent back with prompt to a user requesting his password.

  C) If server has both user name and password, common authentication process is initiate

Note: log entries for web browser (apache) versus SSH login aren’t the same

1) **Apache web browser login using TACACS (ssh login is further below)**

   - “indented log entries below are TACACS-server related entries. Other entries are internal to SecureSync (such as ssh)

notes
testuser (in blue) is our correct TACACS account name
'spectracom_test' **(in brown) is our correct TACACS secret ley**

Actual Auth log entries from our unit with a successful login to the Apache web browser

```
Aug  7 21:55:30 Spectracom apache2: pam_succeed_if(httpd:auth): requirement "user notingroup
addlocal" not met by user "testuser"                (note this is the starting entry for browser loging)
     Aug  7 21:55:30 Spectracom PAM-tacplus[7567]: 1 servers defined
     Aug  7 21:55:30 Spectracom PAM-tacplus[7567]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
     Aug  7 21:55:30 Spectracom PAM-tacplus[7567]: tac_service=''
     Aug  7 21:55:30 Spectracom PAM-tacplus[7567]: tac_protocol=''
     Aug  7 21:55:30 Spectracom PAM-tacplus[7567]: tac_prompt=''
     Aug  7 21:55:30 Spectracom PAM-tacplus[7567]: tac_login=''
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: called (pam_tacplus v1.3.8)
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: user [testuser] obtained
Aug  7 21:55:30 Spectracom apache2[7567]: tacacs_get_password: called
Aug  7 21:55:30 Spectracom apache2[7567]: tacacs_get_password: obtained password
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: password obtained
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: tty [unknown] obtained
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: rhost [10.2.100.52] obtained
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: trying srv 0
Aug  7 21:55:30 Spectracom apache2[7567]: tacacs status: TAC_PLUS_AUTHEN_STATUS_PASS
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: active srv 0
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_authenticate: exit with pam status: 0
     Aug  7 21:55:30 Spectracom PAM-tacplus[7567]: 1 servers defined
     Aug  7 21:55:30 Spectracom PAM-tacplus[7567]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
     Aug  7 21:55:30 Spectracom PAM-tacplus[7567]: tac_service='ppp'
     Aug  7 21:55:30 Spectracom PAM-tacplus[7567]: tac_protocol='ip'
     Aug  7 21:55:30 Spectracom PAM-tacplus[7567]: tac_prompt=''
     Aug  7 21:55:30 Spectracom PAM-tacplus[7567]: tac_login=''
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_acct_mgmt: called (pam_tacplusv1.3.8)
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_acct_mgmt: username obtained [testuser]
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_acct_mgmt: tty obtained [unknown]
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_acct_mgmt: rhost obtained [10.2.100.52]
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_acct_mgmt: active server is [10.2.100.4:49]
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_acct_mgmt: sent authorization request
Aug  7 21:55:30 Spectracom apache2[7567]: Args cnt 0
Aug  7 21:55:30 Spectracom apache2[7567]: pam_sm_acct_mgmt: user [testuser] successfully authorized
```

Actual Auth log entries from our unit with Unsuccessful login using TACACS (right account name/bad password)

```
     Apr 11 18:33:37 Spectracom PAM-tacplus[28240]: 1 servers defined
     Apr 11 18:33:37 Spectracom PAM-tacplus[28240]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
     Apr 11 18:33:37 Spectracom PAM-tacplus[28240]: tac_service=''
     Apr 11 18:33:37 Spectracom PAM-tacplus[28240]: tac_protocol=''
     Apr 11 18:33:37 Spectracom PAM-tacplus[28240]: tac_prompt=''
     Apr 11 18:33:37 Spectracom PAM-tacplus[28240]: tac_login=''
Apr 11 18:33:37 Spectracom apache2[28240]: pam_sm_authenticate: called (pam_tacplus v1.3.8)
Apr 11 18:33:37 Spectracom apache2[28240]: pam_sm_authenticate: user [testuser] obtained
Apr 11 18:33:37 Spectracom apache2[28240]: tacacs_get_password: called
Apr 11 18:33:37 Spectracom apache2[28240]: tacacs_get_password: obtained password
Apr 11 18:33:37 Spectracom apache2[28240]: pam_sm_authenticate: password obtained
Apr 11 18:33:37 Spectracom apache2[28240]: pam_sm_authenticate: tty [unknown] obtained
Apr 11 18:33:37 Spectracom apache2[28240]: pam_sm_authenticate: rhost [10.2.100.52] obtained
Apr 11 18:33:37 Spectracom apache2[28240]: pam_sm_authenticate: trying srv 0
Apr 11 18:33:37 Spectracom apache2[28240]: tacacs status: TAC_PLUS_AUTHEN_STATUS_FAIL
Apr 11 18:33:37 Spectracom PAM-tacplus[28240]: auth failed: 2
Apr 11 18:33:37 Spectracom apache2[28240]: pam_sm_authenticate: exit with pam status: 7
Apr 11 18:33:37 Spectracom apache2[28240]: pam_unix(httpd:auth): check pass; user unknown
Apr 11 18:33:37 Spectracom apache2[28240]: pam_unix(httpd:auth): authentication failure; logname= uid=1001 euid=1001
tty= ruser= rhost=10.2.100.52
Apr 11 18:33:37 Spectracom apache2[28240]: pam_tally(httpd:auth): pam_get_uid; no such user
```

2) SSH login using TACACS

1. Successful login to ssh on our SecureSync (valid username and password)

- “indented log entries below are TACACS-server related entries. Other entries are internal to SecureSync (such as ssh)
- shown below as two “sets” of log entries- the first “set” after typing username <enter>, and the second set after typing password <enter>

A) First set of SSH login entries, after typing just the uername <enter> (before entering a password)

```
Aug  7 21:27:51 Spectracom xinetd[2615]: START: ssh pid=22432 from=::ffff:10.2.100.52   (first entry for SSH)
Aug  7 21:27:59 Spectracom sshd[22703]: pam_succeed_if(sshd:auth): requirement "user notingroup
addlocal" not met by user "testuser"
     Aug  7 21:27:59 Spectracom PAM-tacplus[22703]: 1 servers defined
     Aug  7 21:27:59 Spectracom PAM-tacplus[22703]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
     Aug  7 21:27:59 Spectracom PAM-tacplus[22703]: tac_service="
     Aug  7 21:27:59 Spectracom PAM-tacplus[22703]: tac_protocol="
     Aug  7 21:27:59 Spectracom PAM-tacplus[22703]: tac_prompt="
     Aug  7 21:27:59 Spectracom PAM-tacplus[22703]: tac_login="
Aug  7 21:27:59 Spectracom sshd[22703]: pam_sm_authenticate: called (pam_tacplus v1.3.8)
Aug  7 21:27:59 Spectracom sshd[22703]: pam_sm_authenticate: user [testuser] obtained
Aug  7 21:27:59 Spectracom sshd[22703]: tacacs_get_password: called
```

B) Second set of SSH login entries, after typing password <enter>

```
Aug  7 21:27:51 Spectracom xinetd[2615]: START: ssh pid=22432 from=::ffff:10.2.100.52
Aug  7 21:27:59 Spectracom sshd[22703]: pam_succeed_if(sshd:auth): requirement "user notingroup addlocal" not
met by user "testuser"
     Aug  7 21:27:59 Spectracom PAM-tacplus[22703]: 1 servers defined
     Aug  7 21:27:59 Spectracom PAM-tacplus[22703]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
     Aug  7 21:27:59 Spectracom PAM-tacplus[22703]: tac_service="
     Aug  7 21:27:59 Spectracom PAM-tacplus[22703]: tac_protocol="
     Aug  7 21:27:59 Spectracom PAM-tacplus[22703]: tac_prompt="
     Aug  7 21:27:59 Spectracom PAM-tacplus[22703]: tac_login="
Aug  7 21:27:59 Spectracom sshd[22703]: pam_sm_authenticate: called (pam_tacplus v1.3.8)
Aug  7 21:27:59 Spectracom sshd[22703]: pam_sm_authenticate: user [testuser] obtained
Aug  7 21:27:59 Spectracom sshd[22703]: tacacs_get_password: called
Aug  7 21:28:16 Spectracom sshd[22703]: tacacs_get_password: obtained password
Aug  7 21:28:16 Spectracom sshd[22703]: pam_sm_authenticate: password obtained
Aug  7 21:28:16 Spectracom sshd[22703]: pam_sm_authenticate: tty [ssh] obtained
Aug  7 21:28:16 Spectracom sshd[22703]: pam_sm_authenticate: rhost [10.2.100.52] obtained
Aug  7 21:28:16 Spectracom sshd[22703]: pam_sm_authenticate: trying srv 0
Aug  7 21:28:16 Spectracom sshd[22703]: tacacs status: TAC_PLUS_AUTHEN_STATUS_PASS
Aug  7 21:28:16 Spectracom sshd[22703]: pam_sm_authenticate: active srv 0
Aug  7 21:28:16 Spectracom sshd[22703]: pam_sm_authenticate: exit with pam status: 0
```

```
    Aug  7 21:28:16 Spectracom PAM-tacplus[22703]: 1 servers defined
    Aug  7 21:28:16 Spectracom PAM-tacplus[22703]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
    Aug  7 21:28:16 Spectracom PAM-tacplus[22703]: tac_service='ppp'
    Aug  7 21:28:16 Spectracom PAM-tacplus[22703]: tac_protocol='ip'
    Aug  7 21:28:16 Spectracom PAM-tacplus[22703]: tac_prompt="
    Aug  7 21:28:16 Spectracom PAM-tacplus[22703]: tac_login="
Aug  7 21:28:16 Spectracom sshd[22703]: pam_sm_acct_mgmt: called (pam_tacplus v1.3.8)
Aug  7 21:28:16 Spectracom sshd[22703]: pam_sm_acct_mgmt: username obtained [testuser]
Aug  7 21:28:16 Spectracom sshd[22703]: pam_sm_acct_mgmt: tty obtained [ssh]
Aug  7 21:28:16 Spectracom sshd[22703]: pam_sm_acct_mgmt: rhost obtained [10.2.100.52]
Aug  7 21:28:16 Spectracom sshd[22703]: pam_sm_acct_mgmt: active server is [10.2.100.4:49]
Aug  7 21:28:16 Spectracom sshd[22703]: pam_sm_acct_mgmt: sent authorization request
Aug  7 21:28:16 Spectracom sshd[22703]: Args cnt 0
Aug  7 21:28:16 Spectracom sshd[22703]: pam_sm_acct_mgmt: user [testuser] successfully authorized
Aug  7 21:28:16 Spectracom sshd[22432]: Accepted keyboard-interactive/pam for testuser from 10.2.100.52 port 49779
ssh2
     Aug  7 21:28:16 Spectracom PAM-tacplus[22432]: 1 servers defined
     Aug  7 21:28:16 Spectracom PAM-tacplus[22432]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
     Aug  7 21:28:16 Spectracom PAM-tacplus[22432]: tac_service="
     Aug  7 21:28:16 Spectracom PAM-tacplus[22432]: tac_protocol="
     Aug  7 21:28:16 Spectracom PAM-tacplus[22432]: tac_prompt="
     Aug  7 21:28:16 Spectracom PAM-tacplus[22432]: tac_login="
Aug  7 21:28:16 Spectracom sshd[22432]: pam_sm_setcred: called (pam_tacplus v1.3.8)
Aug  7 21:28:16 Spectracom PAM-tacplus[22432]: 1 servers defined
Aug  7 21:28:16 Spectracom PAM-tacplus[22432]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
     Aug  7 21:28:16 Spectracom PAM-tacplus[22432]: tac_service='ppp'
     Aug  7 21:28:16 Spectracom PAM-tacplus[22432]: tac_protocol='ip'
     Aug  7 21:28:16 Spectracom PAM-tacplus[22432]: tac_prompt="
     Aug  7 21:28:16 Spectracom PAM-tacplus[22432]: tac_login="
Aug  7 21:28:16 Spectracom sshd[22432]: _pam_account: [start] called (pam_tacplus v1.3.8)
Aug  7 21:28:16 Spectracom sshd[22432]: _pam_account: tac_srv_no=1
Aug  7 21:28:16 Spectracom sshd[22432]: _pam_account: username [testuser] obtained
Aug  7 21:28:16 Spectracom sshd[22432]: _pam_account: tty [ssh] obtained
Aug  7 21:28:16 Spectracom sshd[22432]: _pam_account: rhost [10.2.100.52] obtained
Aug  7 21:28:16 Spectracom sshd[22432]: _pam_account: connected with fd=6 (srv 0)
Aug  7 21:28:16 Spectracom sshd[22432]: _pam_account: [start] for [testuser] sent
     Aug  7 21:28:16 Spectracom PAM-tacplus[23389]: 1 servers defined
     Aug  7 21:28:16 Spectracom PAM-tacplus[23389]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
     Aug  7 21:28:16 Spectracom PAM-tacplus[23389]: tac_service="
     Aug  7 21:28:16 Spectracom PAM-tacplus[23389]: tac_protocol="
     Aug  7 21:28:16 Spectracom PAM-tacplus[23389]: tac_prompt="
     Aug  7 21:28:16 Spectracom PAM-tacplus[23389]: tac_login="
Aug  7 21:28:16 Spectracom sshd[23389]: pam_sm_setcred: called (pam_tacplus v1.3.8)
```

2. Failed ssh login using TACACS to one of our secureSyncs (VALID account/bad password)

```
Apr 13 17:36:25 Spectracom sshd[15672]: Invalid user testuser\\ from 10.2.100.52 port 64386
        Apr 13 17:36:25 Spectracom PAM-tacplus[16150]: 1 servers defined
        Apr 13 17:36:25 Spectracom PAM-tacplus[16150]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
        Apr 13 17:36:25 Spectracom PAM-tacplus[16150]: tac_service="
        Apr 13 17:36:25 Spectracom PAM-tacplus[16150]: tac_protocol="
        Apr 13 17:36:25 Spectracom PAM-tacplus[16150]: tac_prompt="
        Apr 13 17:36:25 Spectracom PAM-tacplus[16150]: tac_login="
Apr 13 17:36:25 Spectracom sshd[16150]: pam_sm_authenticate: called (pam_tacplus  v1.3.8)
Apr 13 17:36:25 Spectracom sshd[16150]: pam_sm_authenticate: user [testuser\] obtained
Apr 13 17:36:25 Spectracom sshd[16150]: tacacs_get_password: called
Apr 13 17:36:25 Spectracom sshd[15672]: Postponed keyboard-interactive for invalid user testuser\\\\ from 10.2.100.52 port 64386
ssh2 [preauth]
Apr 13 17:36:29 Spectracom sshd[15672]: Connection closed by invalid user testuser\\\\ 10.2.100.52 port 64386 [preauth]
Apr 13 17:36:29 Spectracom xinetd[2383]: EXIT: ssh pid=15672 duration=13(sec)
Apr 13 17:36:33 Spectracom xinetd[2383]: START: ssh pid=16583 from=::ffff:10.2.100.52
Apr 13 17:36:41 Spectracom useradd[17005]: new user: name=testuser, UID=1003, GID=111, home=/home/spectracom, shell=/bin/bash
Apr 13 17:36:41 Spectracom useradd[17005]: add 'testuser' to group 'spadmin'
Apr 13 17:36:41 Spectracom useradd[17005]: add 'testuser' to group 'spuser'
Apr 13 17:36:41 Spectracom useradd[17005]: add 'testuser' to group 'addlocal'
Apr 13 17:36:41 Spectracom useradd[17005]: add 'testuser' to shadow group 'spadmin'
Apr 13 17:36:41 Spectracom useradd[17005]: add 'testuser' to shadow group 'spuser'
Apr 13 17:36:41 Spectracom useradd[17005]: add 'testuser' to shadow group 'addlo cal'
Apr 13 17:36:42 Spectracom sshd[17061]: pam_succeed_if(sshd:auth): requirement "user notingroup addlocal" not met by user "testuser"
        Apr 13 17:36:42 Spectracom PAM-tacplus[17061]: 1 servers defined
        Apr 13 17:36:42 Spectracom PAM-tacplus[17061]: server[0] { addr=10.2.100.4:49, key='spectracom_test' }
        Apr 13 17:36:42 Spectracom PAM-tacplus[17061]: tac_service="
        Apr 13 17:36:42 Spectracom PAM-tacplus[17061]: tac_protocol="
        Apr 13 17:36:42 Spectracom PAM-tacplus[17061]: tac_prompt="
        Apr 13 17:36:42 Spectracom PAM-tacplus[17061]: tac_login="
Apr 13 17:36:42 Spectracom sshd[17061]: pam_sm_authenticate: called (pam_tacplus v1.3.8)
Apr 13 17:36:42 Spectracom sshd[17061]: pam_sm_authenticate: user [testuser] obtained
Apr 13 17:36:42 Spectracom sshd[17061]: tacacs_get_password: called
Apr 13 17:36:46 Spectracom sshd[17061]: tacacs_get_password: obtained password
Apr 13 17:36:46 Spectracom sshd[17061]: pam_sm_authenticate: password obtained
Apr 13 17:36:46 Spectracom sshd[17061]: pam_sm_authenticate: tty [ssh] obtained
Apr 13 17:36:46 Spectracom sshd[17061]: pam_sm_authenticate: rhost [10.2.100.52]  obtained
Apr 13 17:36:46 Spectracom sshd[17061]: pam_sm_authenticate: trying srv 0
Apr 13 17:36:46 Spectracom sshd[17061]: tacacs status: TAC_PLUS_AUTHEN_STATUS_FAIL
        Apr 13 17:36:46 Spectracom PAM-tacplus[17061]: auth failed: 2
Apr 13 17:36:46 Spectracom sshd[17061]: pam_sm_authenticate: exit with pam status: 7
Apr 13 17:36:46 Spectracom sshd[17061]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.2.100.52  user=testuser
```

C) User Log entries for TACACS

Successful login using TACACS

- Per Keith: I saw no User log entries asserted with a successful login

Unsuccessful login using TACACS (right account name/bad password)

- Per Keith: I saw no User log entries asserted with an unsuccessful login

Troubleshooting issues with tacacs login

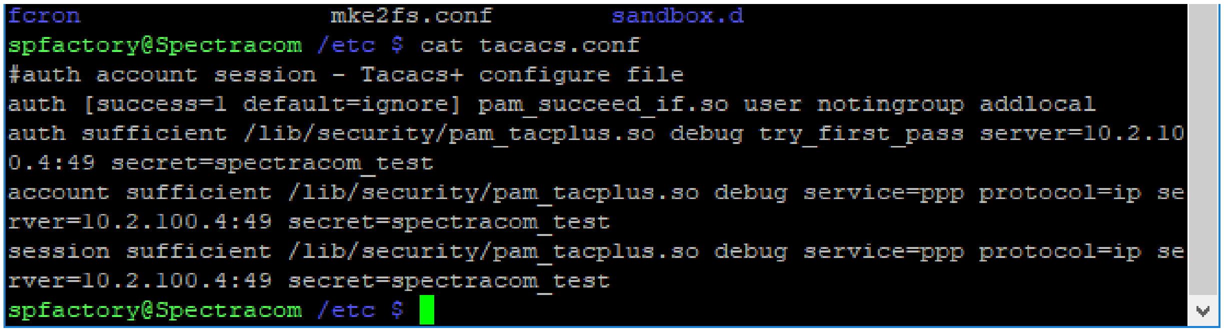
General troubleshooting

1. Check the **Journal** and **Auth** logs (in the log bundle) for entries (user log does not seem to assert any entries for TACACS)
2. Make sure to try connecting/logging into both the web browser and a CLI service (such as ssh). With TACACS, browser login where handled differently than cli/ssh login:
   - **If both the browser and the cli/ssh login are failing**: Likely issue with TACACS account/tacacs server, or with the TACACS configuration (TACACS button on left side of ***Management*** -> ***Authorization*** page of browser)
   - **if browser login is working but cli/ssh login is failing**: Connection to the TACACS Server/TACACS account info in the TACACS server is likely fine. Probally an issue with the actual login name being typed (such as including domain info) or issue related to the 'addlocal' table. See info directly below
3. if the initial connection to the TACACS server(s) is failing, ask what type of TACACS server it is and ask for any logs in the TACACS server whick may be asserted when the SecureSync tries connecting to it.
4. confirn the secret keystring is 100% correct.

TACACS config files

A) tacacs.conf file (in /etc)

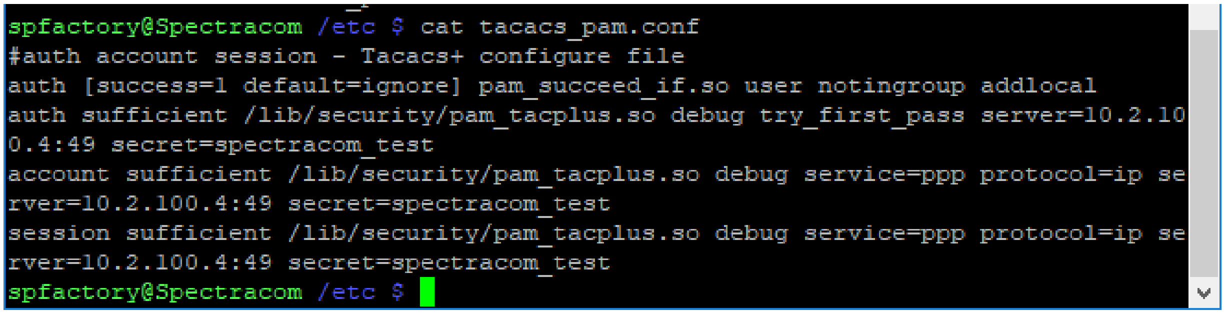
- example below from a v5.8.0 unit with succusful TACACS login working correctly



```
fcron                    mke2fs.conf          sandbox.d
spfactory@Spectracom /etc $ cat tacacs.conf
#auth account session - Tacacs+ configure file
auth [success=1 default=ignore] pam_succeed_if.so user notingroup addlocal
auth sufficient /lib/security/pam_tacplus.so debug try_first_pass server=10.2.10
0.4:49 secret=spectracom_test
account sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip se
rver=10.2.100.4:49 secret=spectracom_test
session sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip se
rver=10.2.100.4:49 secret=spectracom_test
spfactory@Spectracom /etc $
```

B) tacacs_pam.conf file (in /etc)

- example below from a v5.8.0 unit with succusful TACACS login working correctly



```
spfactory@Spectracom /etc $ cat tacacs_pam.conf
#auth account session - Tacacs+ configure file
auth [success=1 default=ignore] pam_succeed_if.so user notingroup addlocal
auth sufficient /lib/security/pam_tacplus.so debug try_first_pass server=10.2.10
0.4:49 secret=spectracom_test
account sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip se
rver=10.2.100.4:49 secret=spectracom_test
session sufficient /lib/security/pam_tacplus.so debug service=ppp protocol=ip se
rver=10.2.100.4:49 secret=spectracom_test
spfactory@Spectracom /etc $
```

TACACS Authentication (based on entries in the two conf files above)

- Refer to sites such as: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/xe-16/sec-usr-tacacs-xe-16-book/sec-cfg-tacacs.html#GUID-7642CA69-B131-4F33-B626-7C49A83CA437

- **try_first_pass** causes **pam_tacplus** to use a previously entered password, if one is available. If no password has been entered, **pam_tacplus** prompts for one as usual.
- **service=PPP** "service" defines the ACACS+ service for authorization and accounting (in this case, it's PPP)
- **protocol=IP** "protocol" defines the ACACS+ protocol for authorization and accounting (in this case, it's over the IP protocol)

Note: ARAP and CHAP: don't appear to be supported

Specific conditions:

A) Tacas password is sent in clear text (unsecure)

- Refer to "**TACACS login password is sent out unsecure**" just a litte ways up on this page .

B) SecureSync is failing to initially connect to TACACS server(s) (even before TACACS account is authenticated)

- Look at the Auth.log to see if the initial connection of SecureSync to TACACS server(s) (even before the credentials are checked) is failing. The following sequence of auth log entries will be asserted:

```
apache2[2152] : tac_authen_read: short reply header, read 0 of 12: Operation now in progress

ilrlm600ntpcentral-m01 apache2[2152]: error communicating with tacacs server

ilrlm600ntpcentral-m01 PAM-tacplus[2152]: no more servers to connect

ilrlm600ntpcentral-m01 apache2[2152]: pam_sm_authenticate: exit with pam status: 9
```

- if the initial connection to the TACACS server(s) is failing (entries below are **in the auth logs)**, ask what type of TACACS server the customer is using, and ask for any logs in the TACACS server itself, whick may be being asserted when the SecureSync tries connecting to it.

C) if SecureSync is successfully connecting to at least one TACACS sever(s), but login to a tacacs user account is not working at all (with neither the Browser or the CLI/ssh)

Note: Always make sure to try logging in with both web browser and CLI connection (ssh) to see if both or only one of the two logins is failing.

As long as the SecureSync is able to initially connect to at least one TACACS server ("***user not authenticated by TACACS+" is not present in the auth.log***), if login with a tacacs account is not working at all (with nether the Browser, nor the CLI) and all the configs are correct, (correct username, password, worked in the past, etc.), TACACS SHOULD be working.

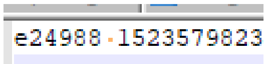
1. Reboot the unit and then try logging in again.
   - **Per Stuart (5/24/17)** If login is succesful after just a reboot, let Stuart in Engineering know this happened (there is a very small chance a reboot will be needed to "clean up" some functions "running in the background").

D) Issue is only with SSH (login to browser with tacacs is working)

- This indicates the “TACACS” account/login to the TACACS server itself is likely fine.

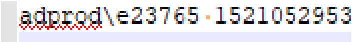
1. **This condition is likely related to the temporary username entry(entries) in the /etc/addlocal file (used tfor temporarily account name for ssh and other CLI services- this entry is not used with browser login).**
    1. Verify the installed software is versions 5.6.0 or above (prior softwareversions allow TACACS connection to the browser only (addlocal was added in v5.6.0).
    2. View the **/etc/addlocal** file in the configs bundle (or cat this file in **/etc**). It should contain only the user account name(s) (and some random numbers) of user tacacs account name(s) which have been used to connect via the cli/ssh. Examples below

       Below is an example of an expected addlocal file having only one TACACS user account

       ```
       e24988·1523579823
       ```

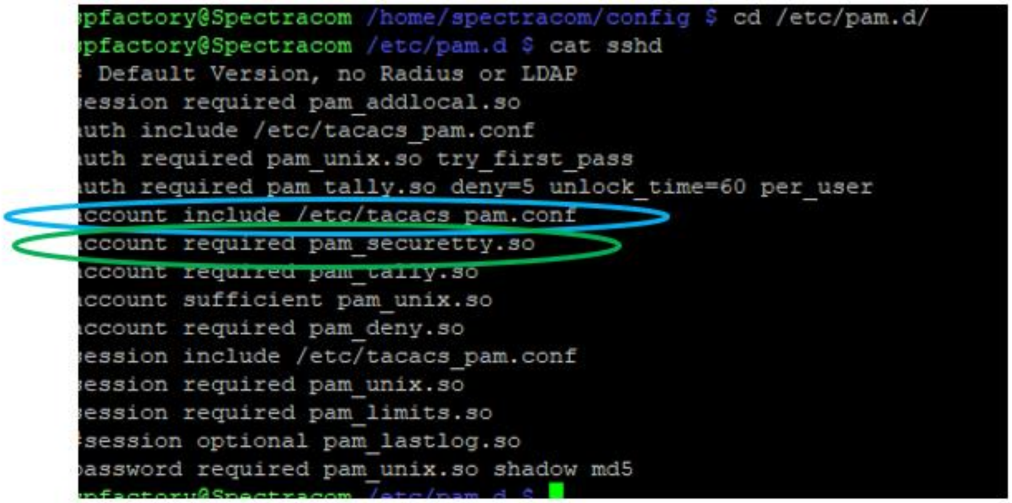
       Below is an example of an expected addlocal file having the domain name as part of the TACACS user account (preventing ssh conection)

       ```
       adprod\e23765·1521052953
       ```

    3. View the **/etc/pam.d/sshd/default** file in the config bundle ???

       Example from our worrking unit



```
pfactory@Spectracom /home/spectracom/config $ cd /etc/pam.d/
pfactory@Spectracom /etc/pam.d $ cat sshd
 Default Version, no Radius or LDAP
ession required pam_addlocal.so
uth include /etc/tacacs_pam.conf
uth required pam_unix.so try_first_pass
uth required pam_tally.so deny=5 unlock_time=60 per_user
ccount include /etc/tacacs_pam.conf
ccount required pam_securetty.so
ccount required pam_tally.so
ccount sufficient pam_unix.so
ccount required pam_deny.so
ession include /etc/tacacs_pam.conf
ession required pam_unix.so
ession required pam_limits.so
session optional pam_lastlog.so
assword required pam_unix.so shadow md5
pfactory@Spectracom /etc/pam.d $
```

After performing an upgrade to version 5.8.2 (or above) from a previous version 5.8.0 or 5.8.1

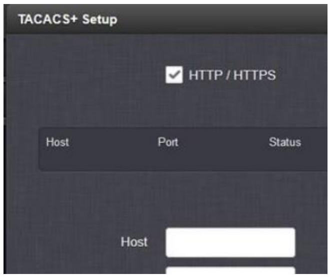
(this is about the specific sequence requirement of the config file entries)

- After updating to 5.8.2 (or above) from either versions 5.8.0 or 5.8.1 SSH with TACACS may work fine, while browser with TACACS login doesn’t work. This is due to two lines in a config file being reversed during the earlier to newer software update proces (not actually an issue in 5.8.2 or above) if a restore to defaults update is performed from versios 5.8.0 or 5.8.1
- The simple fix is to togge TACACS off and back on (ensure the Submit buttom is pressed after unchecing the “HTTP/HTTPS” checkbox and then presssubmit a second time after re-selecting the checkbox). the order of the two lines is corrected when TACACS is disabled and then re-enabled.
- As I understood from Ron D (as higlighted in the above screenshot) The entry “account include /etc/tacacs_pam.conf” has to be **BEFORE** the entry “account required pam_securetty.so”
- Toggling TACACS off and back on switches the order of the two lines, if they are currently reversed
- Per SF Case 158734, if these two lines are reversed in the file, not able access the device through CLI while

browser login works fine.

fix is to disable/re-enable TACACS (make sure to press Submit after unchecking the box,. and then press it again after selecting the box again- pressing submit a total of two times and no just once.

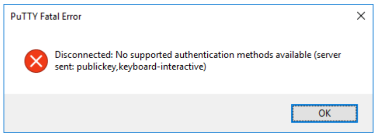
- toggle the current state of TACACS (toggle it off and then back on again, using the "HTTP/HTTPS" checkbox at the top of the pop-up window for TACACS setup (**Management** -> **Authentication** page, **TACACS Setup** button on the left side) as shown below:



TACACS+ Setup

☑ HTTP / HTTPS

2. **SSH login fails with a Fatal Error "Disconnected: No supported authentication methods available (server sent publickey, keyboard-interactive)"**



PuTTY Fatal Error

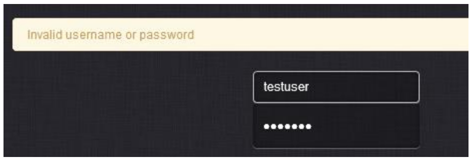
Disconnected: No supported authentication methods available (server sent: publickey,keyboard-interactive)

- The SSH "**Authentication Type**" field (***Management*** -> ***SSH Setup*** page of the browser) is likely configured as "**Only Public Key**". When using TACACS, it needs to be set to either "**Only Password**" or "**Public Key or Password"**
- **SSH protocol versions supported (as of at least v5.7.1 and below):** SecureSync supports SSH protcol version v2 only (not v1 or v3, as configured in /etc/ssh/ssh_config)

3. **SSH responds with "Access Denied" every time trying to connect with TACACS account**

    1. Verify the TACACS account name is not also listed as an account created in the SecureSync (***Management*** -> ***Authentication*** page of browser).
    2. Delete this TACACS user account if it's listed.

E) (v5.8.0 and 5.8.1) TACACS login to browser fails ("invalid username or password"), unless TACACS login to ssh is first performed, and connection remains open- then login to browser. SSH login with TACACS is fine.



Invalid username or password

testuser

•••••••

- Refer to SF cases such as 170655
- try rebooting the unit and try again

iPass

- iPass is not available as of at least update version 5.8.2 (not aware of any plans to ever implement)
  - IPass requires specialized software from the iPass organization be installed, which is not currently possible with Spectracom time servers.

Halt/Shutdown (software only) /System reboot (from 1200s- may not apply to 2400s)

Upon a Halt, Network Processor Software (NPS) is stopped / KTS Timing System software continues operating

- Refer to Salesforce case 24195
- When a Halt or Halt/Shutdown is performed, the Network Processor Software (NPS) stops running (the web browser/CLI/ front panel display, NTP etc all stop working). However, the KTS timing system continues running after a Halt command has been performed
- Because the Timing System continues to operate after a Halt, unless the SecureSync is using NTP as its input (NTP stops running on a Halt), the SecureSync can remain in sync and Option Cards can continue providing outputs.

For example, the PTP Option Cards can continue indicating they are Clock Class 6 and providing useable PTP time stamps after performing a Halt command.
Email Keith sent to NASA: Your understanding of the Halt command is correct. With the exception of using NTP as the only input reference for the unit's synchronization (when using inputs such as either GPS or IRIG), the oscillator is still being disciplined and the rest of the timing functionality is still fully operational (the PTP card is still providing accurate and useable time) after the Halt has been performed.

Differentiating between a reboot and a normal power cycle

(KW 27 Aug 2015) As of at least version 5.2.1, the only two differences I found between a power cycle and a reboot is

1. With a reboot (not a power cycle) the following two entries were asserted in the **kern.log** (they weren't asserted with a power cycle.

```
Aug 27 11:37:52 custservice177 kernel: Kernel logging (proc) stopped.
Aug 27 11:37:52 custservice177 kernel: Kernel log daemon terminating.
```

2. With a reboot (not a power cycle) the following entry was asserted in the user.log (it wasn't asserted with a power cycle.

```
Aug 27 11:37:27 custservice177 shutdown[10762]: shutting down for system reboot
```

Reboot

- Reboot can be performed via web browser, front panel keypad, CLI and SNMP (SNMP with software versions 4.8.8 and above)

A) Reboot via CLI command

- The CLI command to reboot is "**reboot**"
- "**reboot hard**"

B) Reboot from front panel

- Front panel keypad reboot is via the System -> Cmd menus

C) Reboot via SNMP

OID / Object to reboot (ssSysCtrlCommand)

OID	Name	Function	Value to "Set"
8837.3.2.2.5.1	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)

Halt/Shutdown

Halt (shutdown) can be performed via web browser,CLI commands, front panel keypad, or SNMP

A) Via web browser

- Halt is located in the ***Tools*** -> ***Reboot/Halt*** page of the newer black/charcoal browser.

B) Via CLI interface

- CLI command to halt without cleaning/resetting configs is "**halt**"
- CLI command to halt with cleaning/resetting configs is "**cleanhalt**"

C) Via front panel keypad

- Front panel keypad halt is via the **System** -> **Cmd** menus

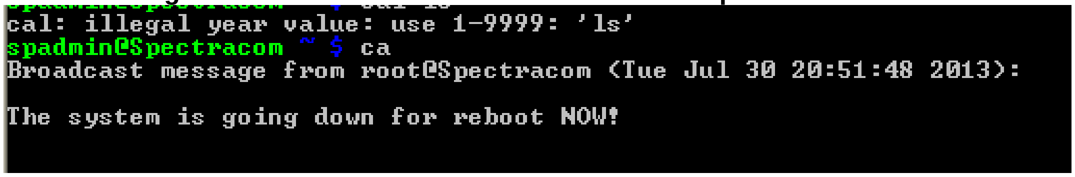
D) Via SNMP

- **Reboot** is available via SNMP
- **Halt/Shutdown** is not available via SNMP (as of at least version 5.1.5):

Upon performing HALT/Shutdown

- Once Halt has been performed, front panel LED time will stop counting up and the front panel LCD will display "**Power off SecureSync**"
- (we confirmed this here with our unit) 1PPS output and 10MHz outputs (hardware outputs) continue to be present after performing a halt.
  - halt is a software-only shutdown. It does not shutdown the hardware, hardware outputs such as 1PPS and 10 MHz continue to be outputted as long as power is applied- they are not stopped if the software is not running (even if Signature control is enabled, because Signature Control is a software function).

Broadcast message to CLI interfaces when Halt/Clean Halt is performed



```
cal: illegal year value: use 1-9999: 'ls'
spadmin@Spectracom ~ $ ca
Broadcast message from root@Spectracom (Tue Jul 30 20:51:48 2013):

The system is going down for reboot NOW!
```

This is a very good question, and I have some information for you that I hope will help alleviate any concerns that you may have about this:

Like any other computer, it is always best to stop the programs that are currently running before just pulling the power cord out of the computer. Otherwise, there is always that small chance that you could corrupt a program this was running at power down. So, computers usually internally stop all processes before they power-down, just to be safe. The HALT command is the method used to stop all processes in the SecureSync before powering power.

The Halt Command is provided to promote file system stability. It does take time to preserve data in the file system. Using halt to shutdown the SecureSync rather than just removing power ensures log data, and configuration information being written to the file system is successfully stored. Also, it avoids any issues of file system corruption.   The file system can recover from corruption and errors. However, to avoid file system corruption the use of Halt is recommended. Also if a file error was to occur, the file system will try to fix it the next time the unit is booted up. This process could cause the power-on to take longer than normal.

Q. Is there any SNMP or other API call that will shut the system off? The web interface is close but I don't like the idea of screen-scraping the web-response to determine when the system is ready for a power. Is there a simple C or java blocking call or system command we can invoke to do this, with response saying if it did shut down or pulled an error?

A In addition to the web browser interface, the SecureSync can also be shut-down (halted) via the front panel keypad or via the CLI interface (such as the front panel RS-232 SERIAL port, telnet or SSH). The CLI command to cause the shut-down is "**halt**". The halt command is discussed in Section 3.8 (starting on page 3-21) of the attached SecureSync manual. It's also listed in the available CLI commands section (Section 11).

Once the halt has been performed, all processes are stopped. Since there is no way to send an indication when all processes have been stopped, the SecureSync itself cannot indicate it has been halted. However, it can be confirmed as being shut-down by trying to contact it after about 20 seconds or so with any network method. Once halted, SNMP, ping, etc will fail. An SNMP Manager will also show it no longer responding. Once the halt has been issued, it will shut-down completely shortly thereafter.

Report of SecureSync appearing to have rebooted itself

- This may be a misconception due to a graceful restart of the Apache web browser and the associated log entry that is asserted.
- Refer to "**Graceful Restart"** in the HTTPS Section of this document (just search for this term).
- It could also be related to "preemption" being enabled in Linux (software update versions 5.3.1 and below). Preemption was disabled in version 5.4.0. See info below.

Linux preempt/preemption (potential cause of lock-ups/ system hanging??)

- Preemption (prempt) was enabled in the Linux kernel with software update versions 5.3.1 and below
- It was disabled/turned-off starting in software update version 5.4.0
- "preempt" has often been found in the kern.log along with oops, call trace and other error messages.
- Engineering found reports from others that prempt being enabled in the linux kernel can cause poblems. So it was disabled starting in 5.4.0 as a potential fix to issue that Verizon and others may be experiencing.

Lilkely fix- version 5.7.0

* [JIRA Ticket SSS-272] – “Bug in Gentoo 4.0.5 kernel: periodic call traces”

**Parallel Redundancy Protocol (PRP)

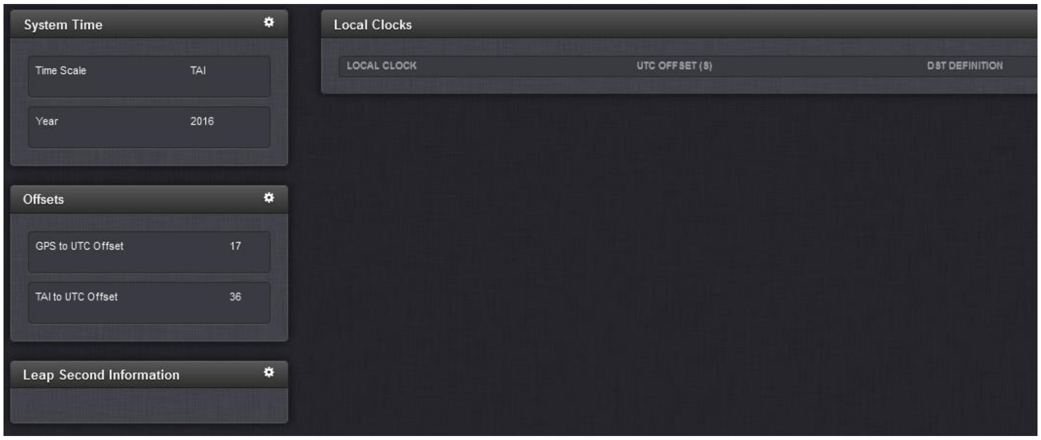
Q. **Email from Mark Day regarding question from Aimil** -Could you please advise on Sunil’s question below regarding support of the Parallel Redundancy Protocol in the SecureSync? I can find no mention of it on the datasheet or in the manual. My understanding is that identical data packets are sent out over two separate networks and assumed to be fail independent, allowing for zero-time recovery and check the redundancy continuously to detect lurking failures on the network as long as one network is operational– is that correct?

A. Reply from Dave Sohn (3 Apr 2013) We do not support parallel redundancy protocol in SecureSync.

Time Management (System Time, GPS/TAI Offsets, local clocks)

**System Time/Year and System timescale

System Time is configured in the browser: Management -> Time Management page of the browser



System Time

Time Scale TAI

Year 2016

Offsets

GPS to UTC Offset 17

TAI to UTC Offset 36

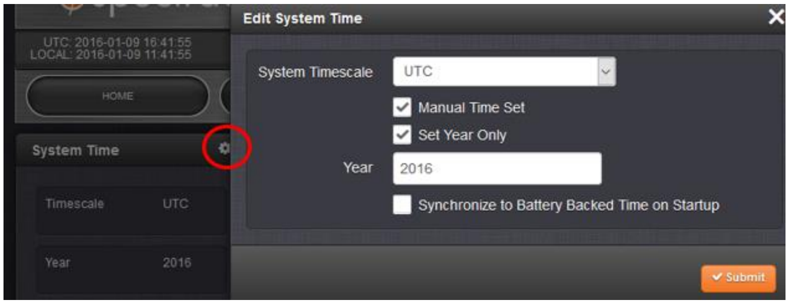
Leap Second Information

Local Clocks

LOCAL CLOCK	UTC OFFSET (S)	DST DEFINITION

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



UTC: 2016-01-09 16:41:55
LOCAL: 2016-01-09 11:41:55

System Time

Timescale UTC

Year 2016

Edit System Time

System Timescale UTC

☑ Manual Time Set

☑ Set Year Only

Year 2016

☐ Synchronize to Battery Backed Time on Startup

1. **Management** -> **Time Management** page and press the gear icon to the right of "**System Time**"
2. Select "Manual Time Set"
3. Select "**Set Year Only**"
4. Change the Year, as desired, and then press Submit (don't need to also select "synchronize to battery backed…"
5. With the system synced via IRIG input, can either perform a reboot command (via the browser, CLI or front panel) or wait at least 10 minutes after changing the year for the RTC to be updated. before power cycling.
    - If the unit doesn't run long enough (up to 10 minutes) afer setting the year before its power cycled, the year will be set to the earlier configured year once its boots-up. The RTC is only periodically set (every 10 minutes or when a reboot is commanded). RTC is set on commanded reboot, so no delay is necessary when rebooting.
    - See additional info below

Delay of up to 10 minutes is needed after changing the year to set the RTC, before power cycling.

- Refer to SF case 123677

Email Keith sent (9 Jan 18) I just worked with one of our Apps engineers to more closely duplicate your same scenario of IRIG B000 input (I performed a quick test without an IRIG input applied).

He had a SecureSync outputting IRIG B000 to another SecureSync, with both set to year “2018”. He then changed the “Set Year only” field in the Slave SecureSync to “2017”, and then **rebooted** via the web browser the Slave SecureSync. The Slave SecureSync then powered-back up with the year value still set to the value of “2017” as expected.

We want to first confirm the version of software currently installed in the IRIG Slave (as reported in the Tools -> Upgrade/Backup page of its browser). This is not likely a factor, but just want to make sure. If I recall correctly, I believe it’s the latest version of version 5.7.1,

We may end up needing the logs and configs files. But as I realize this can be very difficult, one other factor that we can also review first, as this can affect this field, is the actual test process and durations between steps.

The test we performed used a “graceful” shutdown/restart of the Slave SecureSync (as commanded with the **Tools -> Reboot/Halt** page of the browser, and selecting the “**Restart after Shutdown**” checkbox.

Note that when you manually change the year value, just submitting the change doesn’t immediately set the Real Time Clock (RTC) which is used for the initial time/date/year at startup of the system. The RTC is only set periodically, or when a Halt/reboot (graceful shutdown) has been commanded. If the system is just power cycled (instead of being commanded to reboot) too soon after changing the year, the newly set year value will not be set to the RTC, and therefore will not be used at the next boot-up (it will revert back to the year that was set before it was manually changed).

For your testing, was the SecureSync rebooted via the browser or instead power cycled? Also, how long after changing the year did the unit continue to run thereafter, before it was rebooted/power cycled? Just moments later, or several minutes later (at least 10 minutes before a power cycle was performed)?

If testing with a loss of power, the unit needs to be running long enough after setting the year, for the periodic routine which sets the year in RTC to have been performed again. As its performed every 10 minutes, if the unit is not commanded to reboot, and is instead power cycled, and unless you first check to see when the RTC has been set, you will need to wait at least 10 minutes after setting the year before power cycling, in order for the RTC to contain the new year, and to have it boot-up with the correct year value.

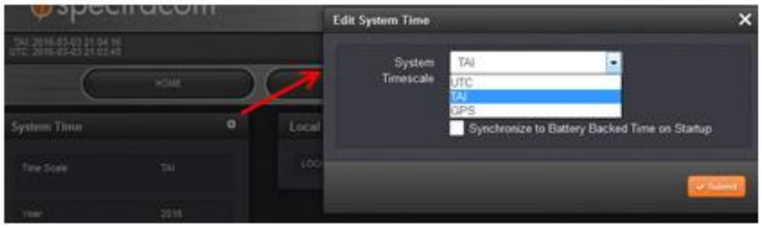
To ensure the RTC has been changed to the new year value before rebooting or power cycling, open an ssh session and perform a date <enter> cli command. Once this command starts showing the newly set year value (in place of the earlier year), the RTC has now been updated and the unit will use this new year value upon its subsequent boot-ups.

FYI- instead of just typing ‘date’, if you type watch -n1 date <enter> you can see each second when the year has been set in the RTC, indicating it can then be power cycled (this alleviates needing to keep typing date, as it will refresh the date each second).

Our testing is showing the Set Year for IRIG input is operating as expected. Let me know if you observe anything different (the operational time required after setting the year- before power cycling - explains why you were “sometimes” seeing the expected results. These times, the unit likely ran long enough after setting the year for the RTC to be set, before it was subsequently power cycled).

System Timescale

- System Time is UTC timescale by default
- Can be changed to either TAI or GPS timescale as desired (press the gear icon next to “System Time”):



TAI 2016-03-03 21:04:16
UTC 2016-03-03 21:03:40

System Time

Time Scale TAI

Year 2016

Edit System Time

System Timescale TAI
UTC
TAI
GPS

□ Synchronize to Battery Backed Time on Startup

- Changing the System Timescale value changes the “System Time”. So all references to time with the exception of PTP output (outputs such as the front panel, browser, NTP, logs, etc) use the new timescale offset.
- As of at least software version 5.4.1, NTP (and the unit’s logs) doesn’t have its own individual timescale configuration, so it will always follow the System’s timescale.

  Besides NTP, other inputs/outputs (such as ASCII and IRIG for examples) have their own individual timescale configurations available. So, for instance, the System timescale can be set to UTC, but IRIG can be outputted as either GPS or TAI.

- PTP Option Cards always read the System Time in UTC timescale, no matter what timescale is selected. It always outputs TAI (if the UTC to TAI offset is set correctly). The 1204-12 and 1204-32 cards can’t be configured to utput any other timescale except TAI.
- Timekeeper software (with the timekeeper license installed) outputs time in UTC timescale (timekeeper software doesn’t always follow the PTP standards).

Affect on NTP when the System Timescale is changed to a different value

- ntpmond should automatically stop and restart NTP due to the larger than one second correction.
- Sample log entry from version 5.4.0 (NTPv4.2.8p6) when changing TAI back to UTC: 0.0.0.0 0413 03 spike_detect -35.999985 s

Timescale configuration of certain input references can affect the System Time, even if the System timescale is set as desired.

- References such as IRIG, RS-232, RS-485, etc can provide the SecureSync with time in a difference timescale or offset than the System timescale is set to.
- When this is the case, the input reference needs to be properly configured with the timescale/offsets being supplied so that the System know how to properly convert the time its receiving to be in the correct timescale that the system is configured to operate in.
- For example, if the IRIG source is providing TAI timescale. It needs to be configured to report its receiving-providing TAI time.

**GPS Offset (Antenna Cable Delay)

- Provides a "group of all outputs" delay/advance configuration (instead of using individual output delay compensation)
- When configuring the antenna cable delay for a SecureSync, you want to use "+" (or no sign entered) . This will advance/forward the System PPS by the same amount the cable is going to inherently "retreat/retract" the 1PPS Offset.

Refer also to "**GNSS Receiver Offset"** in the online 2400 SecureSync user guide at: https://www.orolia.com/manuals/2400/Content/_Global/Topics/GNSS/GNSS_recOffset.htm?Highlight=receiver%20offset

Whether to use a positive (+) value or a negative (-) offset value (from Case 259422, discussing IRIG output OFFSET)

Email from Keith Adding delay (Offset) compensation on the input reference that the SecureSync is synced with (such as GPS or IRIG input) will inherently move the SecureSync's System 1PPS and all its outputs by the Offset value entered (a positive value to push the 1PPS ahead, or negative to pull the 1PPS back). But if its desired to only offset one particular output (such as an IRIG output), the Offset should be configured for just that particular output.

A positive Offset value will "advance/forward" the 1PPS, while a "negative" Offset value will "retreat/retract" the 1PPS Offset. So, adding a positive 27000 ns Offset in the dedicated IRIG output going over to the other SecureSync will advance the 1PPS its providing by 27 microseconds. Adding a negative "27000" ns Offset will retreat the 1PPS of the IRIG by 27 microseconds.

If the 27 microseconds of offset is due to the coax cable delay between the IRIG out of the GPS-synced SecureSync to the other SecureSync, adding a positive 27000 ns of Offset to the IRIG output (Interfaces -> IRIG out page of the web browser) will "advance" the 1PPS of the IRIG output by 27 microseconds.

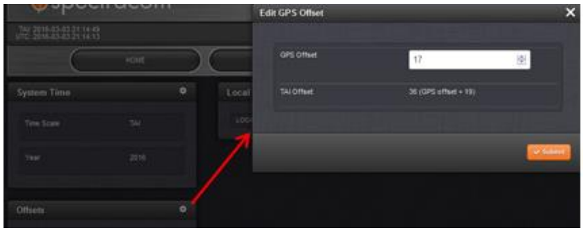
When the IRIG output signal reaches the secondary SecureSync, the advancing of the PPS (inside the GPS SecureSync) will have then been negated at the input of secondary SecureSync by the actual delay through the cable, resulting in the PPS of the IRIG output and the PPS of the IRIG input coincident with each other (as if they were directly connected to each other, instead of having a cable located between them).

Calculating Antenna Cable Delay values (Coax or Fiber)

- Refer to "1PPS / Antenna cable delay calculations" in I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf

Entering the calculated value into the SecureSync browser

- ***Management*** –> ***Time Management*** page of the browser
- Click on the "gear" icon next to "**Offsets**" (left side of the page)



GPS Offset 17

TAI Offset 36 (GPS offset + 19)

From the SecureSync user manual, cable delay can be set to a max of + /- 50 milliseconds (entered as 50,000,000 nanoseconds).

**"GPS to UTC offset" (Number of leap seconds)

Reported in:

- Newer browser: **Management** -> **Time Management** page

Automatic updating of this value

- This value is only automatically updated if GPS changes its data message to indicate it's now a different value.
- It's the change in the GPS message (a leap second occurring) that automatically updates this value in the time server.
- If the value is manually changed to an incorrect value while GPS is present, or if GPS is subsequently reconnected, GPS WON'T simply correct the value   It will need to be manually corrected or it will remain set to the incorrect value.

UT1 (GPS to UTC offset) is now stored in SecureSync for faster GPS sync

UT1 offset is now stored after the first time that the GPS receiver downloads the UT1 offset value from the 12.5 minute ephemeris data (the first time after it's been cleaned, its stored).
Special release Version 4.5.N introduced the ability for the UT1 offset to persist through power cycles.

- This new capability was officially cut-in with the version 4.7.0 software update.
- This capability reduces sync to GPS time to about 2 minutes or so after power-up.

**Leap Second insertion

- For general info on NTP handling leap seconds, refer to: Leap Seconds (in CustomerServiceAssistance.pdf)
- Refer also to the draft SecureSync email from the 2015 leap second: ..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\leap second. First part is about NTP and the second is about PTP.

General info

- The GPS receiver automatically flags leap second to occur on last second of the last day of the month (typically either last day of June and/or December)
- GPS typically announces leap second at least 30 days prior to insertion but no more than 6 months prior to insertion.

Next scheduled leap second flagged in the system

CLI command to obtain the next scheduled leap second: **CS_getLeapSec 0**

Next scheduled leap sec is displayed in the **Mangement** -> **Time Management** page of the newer browser.

Once a scheduled date is "in the past", it no longer affects the system operation

Changes in outputs to indicate the Leap second is pending:

- **NTP** changes LI bits (Leap indicator bits) 24 hours prior. (initially 00 and then change to "01")
- **PTP** changes Announce message 12 hours prior.

- **IRIG** changes data 1 hour prior

Desire to slew the time for leap second (like Google now does) instead of an “immediate” correction

- This functionality is not currently available in standard SecureSyncs (using NTPd software)
- Suspect this capability is available by purchasing/installing Timekeeper option (SS-OPT-TKL) which replaces NTPd when enabled.
  - FSM has implemented this function into their software to allow either a slew or immediate correction. So it would be available with the Timekeeper license, if its purchased and installed (our P/N SS Opt-TKL. Refer to https://na8.salesforce.com/01tC0000004KDut?srPos=13&srKp=01t for additional info on this available purchasable Option).

Leap second event for PTP (both the 12 and 32 PTP Option Cards)

A) 12 hours prior to the insertion, the Announce message indicates a leap second is pending.

B) Because PTP time stamps are in TAI time (which doesn’t observe leap seconds), the time stamps at the moment of the leap second are going to count up sequentially just like nothing happened (no two seconds are duplicated like they are in NTP). It’s up to the clients to update the UTC to TAI offset value correctly at the moment of leap second.

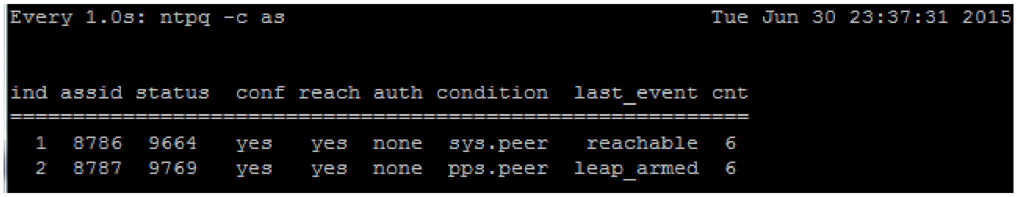
Leap second event for NTP:

E) 24 hours prior to leap second is inserted (00:00:00 UTC, the day prior)

1. LI bits are initially “00”
2. System Time notifies NTP that leap second is pending

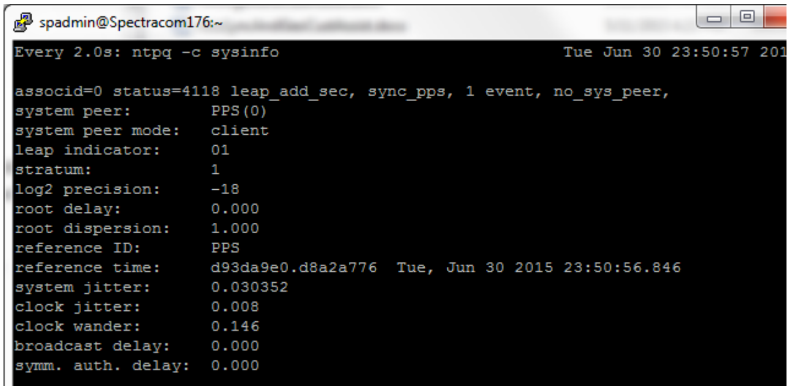
F) ntpq -c as CLI command will change the pps.peer (second row) to “leap_armed”

note: **ntpq rv** command also reports leap second info.



```
Every 1.0s: ntpq -c as                                  Tue Jun 30 23:37:31 2015


ind assid status  conf reach auth condition  last_event cnt
===========================================================
  1  8786  9664   yes   yes  none  sys.peer   reachable  6
  2  8787  9769   yes   yes  none  pps.peer  leap_armed  6
```

G) LI bits change to “01” in Management -> NTP Setup page of the browser (and in the NTP packets) to 01.



```
Every 2.0s: ntpq -c sysinfo                              Tue Jun 30 23:50:57 201

associd=0 status=4118 leap_add_sec, sync_pps, 1 event, no_sys_peer,
system peer:        PPS(0)
system peer mode:   client
leap indicator:     01
stratum:            1
log2 precision:     -18
root delay:         0.000
root dispersion:    1.000
reference ID:       PPS
reference time:     d93da9e0.d8a2a776  Tue, Jun 30 2015 23:50:56.846
system jitter:      0.030352
clock jitter:       0.008
clock wander:       0.146
broadcast delay:    0.000
symm. auth. delay:  0.000
```

H) At the leap second insertion (23:59:59 UTC on the day of the leap second being inserted)

1. NTP should go to “60”
2. The Front panel should display the seconds as “60”.

I) Just after the leap second insertion. Leap indicator bits go back to “00”

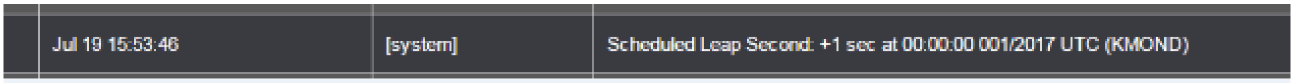
Associated Log entries for the leap second insertion

Timing log and System log

- Just the Happy New Year message was inserted for the start of the year.

1) When GPS has flagged the system months in advace that a leap second is pending at the end of June or Dec

- When the GPS receiver starts to see a pending leap second being announced in the GPS signal, this is flagged in the **System** log (the example below was from our internal house refernce)



```
Jul 19 15:53:46    [system]    Scheduled Leap Second: +1 sec at 00:00:00 001/2017 UTC (KMOND)
```

"Scheduled leap second: +1 second ."

Note: This log entry will only be observed in the System log, later than the date it was asserted, if it hasn't already been rotated out (the System log may need to go back to as much as 6 months in order for it to still be in the logs). But if the logs are being sent to a remote syslog server, it may still be present in the syslog server

Note: This next scheduled leap second is also logged in the System log after each subsequent reboot.

2) Day of the leap second insertion

Note: the Log entries below are from the 31 Dec, 2016 leap second (filtered for "leap") with v5.5.0 installed and ublox GPS being the selected reference.

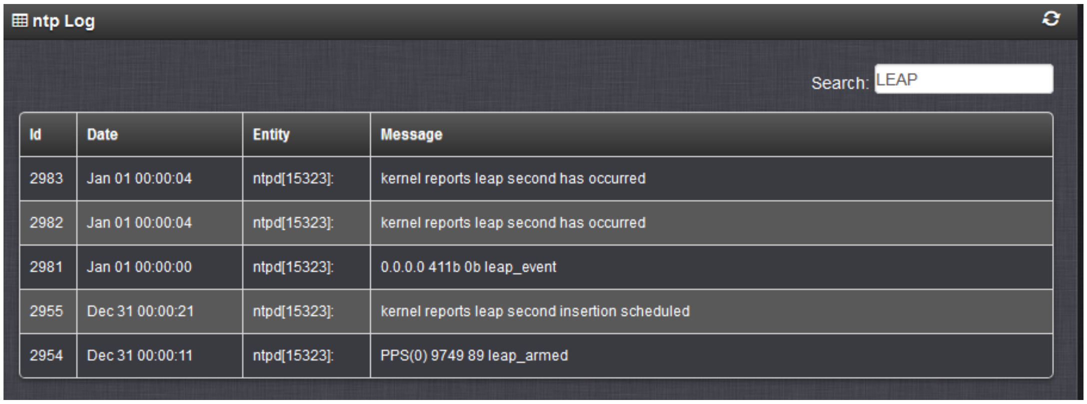
J) Kernel log

```
Dec 31 23:59:59 Spectracom kernel: Clock: inserting leap second 23:59:60 UTC
Jan 01 00:00:00 Spectracom Spectracom: [fcron] Happy New Year Sun Jan  1 00:00:00 UTC 2017
```

K) NTP log

The **Tools** -> **NTP** log page should have four new log entries associated with leap sec (below in ascending order. Screenshot is in descending order):

1. "…leap_armed" (about 24 hours prior to the leap second insertion)
2. "kernel reports leap second insertion scheduled" (about 24 hours prior to the leap second insertion)
3. "…leap_event" (at the moment of the leap occurring)
4. "kernel reports leap second has occurred" (just a few seconds after the moment of the leap occurring)



ntp Log

Search: LEAP

Id	Date	Entity	Message
2983	Jan 01 00:00:04	ntpd[15323]:	kernel reports leap second has occurred
2982	Jan 01 00:00:04	ntpd[15323]:	kernel reports leap second has occurred
2981	Jan 01 00:00:00	ntpd[15323]:	0.0.0.0 411b 0b leap_event
2955	Dec 31 00:00:21	ntpd[15323]:	kernel reports leap second insertion scheduled
2954	Dec 31 00:00:11	ntpd[15323]:	PPS(0) 9749 89 leap_armed

Note: The two “kernel reports leap second has occurred” log entries are at the exact same time and for the exact same event. Having the event logged twice is just a factor of how logging works and not a software defect.

Qual log (no direct log entries for leap second, but the first entry after the insertion should have a Q= value of 3601)

Email Keith sent: Most logs don’t have “routine” entries. They only have new entries asserted in them when a particular event happens. But there is one log that needs to account for every second in each hour that the unit is powered-up, the GNSS Qualification log.

The Qual.log reports the total number of satellites being tracked each hour. Since there are normally **3600** seconds in an hour, each qual log entry accounts for 3600 seconds, reported with a “Q=” value at the end of each entry (if the receiver is tracking at least one satellite for the hour. the Q value will normally be 3600.

But if the leap second was added as expected, there will be a total of **3601** seconds in the log entry for 1 Jan 01:00 UTC log entry (the first entry following the leap insertion).

The entry below in red has a Q value of 3601, whereas all other entries before and after have a e value of 3600.

```
an 01 00:00:00 Spectracom Spectracom: [fcron] Happy New Year Sun Jan  1 00:00:00 UTC 2017
Jan  1 00:00:01 Spectracom Spectracom: [system] GPS 0: 8 = 6 9 = 953 10 = 2212 11 = 429 Q = 3600
Jan  1 01:00:02 Spectracom Spectracom: [system] GPS 0: 7 = 12 8 = 75 9 = 1060 10 = 1956 11 = 233 12 = 265 Q = 3601
Jan  1 02:00:02 Spectracom Spectracom: [system] GPS 0: 7 = 232 8 = 1395 9 = 1762 10 = 211 Q = 3600
Jan  1 03:00:02 Spectracom Spectracom: [system] GPS 0: 7 = 32 8 = 139 9 = 1428 10 = 2001 Q = 3600
Jan  1 04:00:02 Spectracom Spectracom: [system] GPS 0: 8 = 70 9 = 1975 10 = 1555 Q = 3600
Jan  1 05:00:02 Spectracom Spectracom: [system] GPS 0: 8 = 133 9 = 3051 10 = 416 Q = 3600
Jan  1 06:00:02 Spectracom Spectracom: [system] GPS 0: 8 = 1217 9 = 174 10 = 1305 11 = 904 Q = 3600
Jan  1 07:00:02 Spectracom Spectracom: [system] GPS 0: 9 = 63 10 = 1209 11 = 2168 12 = 160 Q = 3600
```

If the leap wasn’t correctly added, its Q value wouldn’t be 3601.

New IRIG Control field added to distribute leap second info earlier than just one hour

- Refer to Mantis case 3008.
- Version 5.2.1 Added new IRIG control field format, Spectracom IEEE C37, to extend leap second notification to a month.
- Intended for SecureSyncs syncing via IRIG input and outputting NTP (SecureSync acting like a Slave to

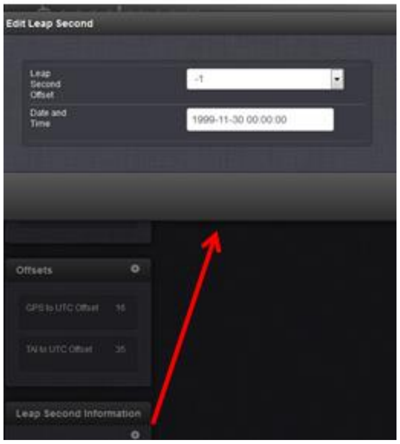
another SecureSync). Without this new control field, the leap second won’t be announced until just one minute before the leap second is inserted. This doesn’t leave enough time for NTP on those IRIG units to read the leap second and announce it in time.

- Was primarily for Verizon, but others can benefit from this new capability

Web browser interface pages associated with leap second

A) web browser

Management -> **Time Management** page (bottom-left corner)



Edit Leap Second

Leap Second Offset: -1

Date and Time: 1999-11-30 00:00:00

Offsets

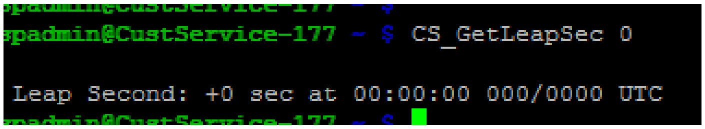
GPS to UTC Offset 16

TAI to UTC Offset 35

Leap Second Information

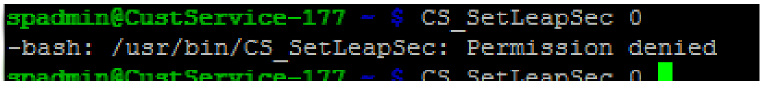
CLI command for reading the next scheduled leap second

- Command to get the next scheduled leap second: **CS_GetLeapSec 0**



```
spadmin@CustService-177 ~ $
spadmin@CustService-177 ~ $ CS_GetLeapSec 0

 Leap Second: +0 sec at 00:00:00 000/0000 UTC
spadmin@CustService-177 ~ $
```

Note: User doesn’t have permission to schedule the next leap second via the cli. It needs to be scheduled via the browser.



```
spadmin@CustService-177 ~ $ CS_SetLeapSec 0
-bash: /usr/bin/CS_SetLeapSec: Permission denied
spadmin@CustService-177 ~ $ CS_SetLeapSec 0
```

- I wanted to make sure that leap seconds events information is automatically passed down to Stratum-3 clients.

Reply from Sam Otto (2 Apr 2013)which was reviewed by Dave Sohn: Correct, The Stratum-2 does pass along the leap second bits 24 hours prior to the leap second event.

Email from Paul Myers (15 Feb 2013)

The scheduled leap second will tell the KTS clock to make a leap second adjustment.

The KTS will be read by the network processor using the NTP Reference Clock driver.

The NTP daemon will be aware of a pending leap second and will schedule one in the Linux kernel.

There will be a single leap second inserted by the KTS, received on the 60th second of the havequick input, and the NTP and linux kernel will be aware of only a single leap second.

There is not issue with 2 leap seconds, being adjusted.

The NTP step should occur at or be logged shortly after the leap second. I do agree I have seen the step logged slightly late before, but I can't remember under which circumstance of testing. If it was a unscheduled leap second or a scheduled one…

To ensure your customer is satisfied I recommend you have someone perform this test:

1. Handset the time to several hours before a leap second adjustment on 2 SecureSyncs and let them sync the linux time to NTP
2. Using a SecureSync with HaveQuick output schedule a leap second using the format without notification
3. Sync SecureSync with a havequick input card
4. Ensure NTP is synced and the time is set correctly.
5. Hand set a scheduled leap second several hours hence
6. Allow the NTP to sync
7. Verify the LI bits indicate a leap second is pending
8. Configure the Front Panel, ASCII output, etc so you can watch the leap second rollover
9. Observe the rollover

- You will observe the 58, 59, 60, 0, 1, 2
- You will observe a 1 second step in the NTP log slightly after the rollover
- This is normal behavior.
- KTS, Linux and NTP are all aware of the 60th second.
- NTP will distribute the scheduled leap second by sending leap indicator LI bits set to other NTP servers.

From: Paul Myers
Subject: Leap Second Document

\\Roc.spectracom.us\ICS\Engineering\Projects\Lafayette\301 Verification Test Results\Release 4.8.2\Leap Second Changes.docx

This is my first cut at the leap second document. I will improve it where it is not clear or additions are needed.
In general what was done was:

- Improve Clock Service to better handle leap seconds when operating in Time Scales other than UTC and provide functions to facilitate time scale conversions
- Time Manipulation library
- Output 60 for the leap second when appropriate
- Fix Time conversions so errors don't happen
- Fix NTP stratum 2 to avoid premature leap second announcers.
- Fix Leap Indictors in any Outputs that were not working
- Detect leap seconds as appropriate in any Input References that did not.
- Fix any error conditions found
- Implement and test HaveQuick Leap Seconds

The document above contains a list of all files changed since 4.8.0 to NOW (pre-4.8.3) which were changed for Leap Second related reasons.
Also, it contains at the end information for Keith to write Leap Second Application note as to what features are improved and why.

I think Keith should read it, if it is not clear enough tell me, and I can fix it, and then he can shorten it to say if you are using ASCII and you need this update. If you don't you may have this problem such as skipped Leap Second, late adjustment, no 60 values, wrong GPS-UTC offset briefly, etc.

I will likely update it with any of Mark's changes and any feedback he has.

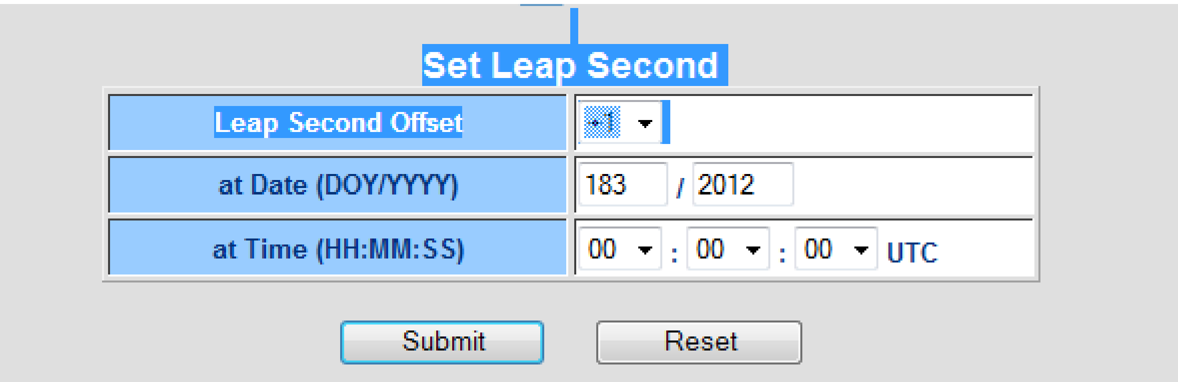
Email from Paul Myers about manually scheduling a leap second (14 Feb 2013)
I believe the manual is incorrect about scheduling leap seconds.

Mark Goodlein designed the interface to set Leap Seconds in both the SecureSync and in the KTS.

The time to 'schedule' them was 1 second after the adjustment. In theory they can be added or removed.

The constant is the time after.

I ran the GSG Leap Second test and observed what was 'scheduled' in KTS.



Set Leap Second

Leap Second Offset	+1
at Date (DOY/YYYY)	183 / 2012
at Time (HH:MM:SS)	00 : 00 : 00 UTC

Note that for a +1 adjustment at 23:59:59 on 182/2012 the above scheduled date is shown.

To similarly schedule a leap second you must do the same. SO the 23:59:59 in the manual is incorrect in my opinion.

Note: when testing Leap Second functionality, make sure no external references are connected/present. If a user manually sets a leap second with a reference connected, the reference will interfere with the test results, and may cause abnormal output time stamps!

Email from Paul Myers:

To simulate a Leap Second Rollover you CANNOT have a reference attached as it will try to correct the time if you handset a leap second that is NOT provided by a Reference.

To handset a leap second condition:

1. Remove all references.
2. Handset the clock to the desired time say 23:58:00 hours, Day 366 of a leap year or 365 of a non-leap year
3. Handset the rollover to the first second of the next day. 1/year 00:00:00
4. Watch the rollover condition

Note: Responses to questions below are from **Paul Myers**

- To confirm, if an input reference doesn't provide Leap Second pending notification (such as not using extended havequick) , a user can still manually schedule a pending leap second via the "Set Leap Second" section of the Setup- > Time Management page? Manually scheduling the leap second should result in System Time making a one second time jump at the last second of the scheduled month.

[PEM] The user can schedule a leap second when a reference is present or not.
[PEM] The leap second gets automatically updated if the reference is aware of leap seconds.
[PEM] NTP will be made aware leap seconds from the Reference clock driver or in the case of NTP Stratum 2-15 servers from NTP packets LI bits.

- ➢ If the leap second section is filled in by a user (because the input reference can't set these fields), will NTP know to apply a one second jump correction at the last second of the scheduled month? Or, as I suspect, will NTP instead slew its time by one second, once System Time makes the one second time jump at the last second of the month).

[PEM] Yes. NTP will be informed of the pending leap second because the reference clock driver communicates this information along with time to the NTP from the KTS.   NTP will make its leap second adjustment 58, 59, 60, 0, 1, by adjusting the kernel time. NTP can step the second and slew in the remainder. If NTP is NOT notified of the pending leap second it will have to step/slew to correct the offset later based upon poll rate.
NTP sets its LI bits to indicate a leap second is pending 24 hours before the leap second insertion.

- ➢ If NTP slews its time for the one second time jump that occurs in System Time, over how long of a period will NTP need to slew the time until its correct again? Does the current poll interval affect how long it takes to slew its time by one second?

[PEM] It depends up on poll rate, but scheduled leap seconds are known to the kernel and NTP to be handled. Unplanned offsets can take longer.

LI Bits (Leap indicator bits) now displayed in the Status -> NTP page of the browser

Starting in version 4.8.4, the LI bits were added to the NTP input references tables. Earlier versions of software did not display the LI bits in each row of the tables.

Leap second testing only allows leap second to occur last day of June or last day of December
Paul Myers coded the Leap Second functionality to allow Leap Second to only be able to occur on the last day of June or December. When testing for Leap second, set the leap second to occur on one of these two days only. Then with User mode enabled, manually set the date/time for a day prior to leap second, to see it occur.

SecureSync that is synced via NTP

The following is from http://www.meinberg.de/english/info/leap-second.htm#irig:

IRIG time codes are often used to synchronize time between computers and other devices via cables or fiber optic connections.

Several IRIG frame types have been specified to transport time information between two IRIG devices. Most of the commonly used IRIG frames carry the day-of-year and the current time, but they do neither contain the year number which would be required to convert the day-of-year to a calendar date unambiguously in leap years and non-leap years, nor the UTC offset of the transported time, or a leap second announcement.

The IRIG frame type **IEEE1344** contains all this information. However, by specification the leap second is announced only about 60 seconds before it actually occurs.
If such an IRIG receiver is used as a reference time source for NTP then there's a good chance the NTP daemon misses the leap second announcement at a polling interval of 64 seconds and thus is unable to handle the leap second correctly. Even if the NTP daemon received the leap second announcement, it was too late to pass the announcement on to the clients, so most of the NTP clients would probably miss the leap second.
This is the reason why in general a leap second file should be installed for NTP if an IRIG receiver is used as reference time source.

If the NTP server that SecureSync is synced to is synced via IRIG, as IRIG only changed the LI bits one minute before the leap second occurs, will require NTP to step the time about 15-20 minutes thereafter, to account for the one second time change.

Email from Keith to Rob Amos (ASX) 7/13/12

Hi Rob,

Good day to you!

We have reviewed the SecureSync logs you sent to us (thanks for sending them to us)!! I have some feedback for you that should help!

To begin, attached are individual documents for each SecureSync, with each document excerpting the log entries relating to the leap second time-frame. At the end of each document is a list of our findings, for that particular SecureSync.

In short summary of all of the logs, the SecureSyncs properly handled the leap second insertion. However, we fell "victim" to the IRIG reference not providing enough advance warning of the pending leap second. Because only one minute of advanced warning was provided to the kernel, the leap second time correction was delayed by several minutes after the leap second insertion occurred.

Now for the details:
First: two points for clarification:

- NTP adjusts the SecureSync's kernel "Time" by one second for the leap second insertion.

- The System Time's (displayed in the Time Management page of the browser) leap second flag adjusts the Timing System's time scale offsets (such as the UTC to TAI offset, as needed for PTP) by one second when the leap second insertion has occurred.

The SecureSync's System time for its outputs is derived from the kernel time, which is updated by NTP and its selected reference. NTP can select various input references to synchronize with (such as GPS or NTP, for examples). When NTP is synced to GPS (via the System Time) NTP has a direct and continuous time reference to sync with. However, when NTP is syncing to another NTP time server, the time stamps to sync NTP with are only periodically available (with the interval based on the poll rate of its selected NTP server (as determined by NTP, to be between the configured MinPoll and MaxPoll intervals).

Even though the Stratum 1 server only gave one minute of advanced notice of the pending leap second, we were fortunate that the SecureSync had been able to sync to GPS at least once since March. When the SecureSync synced to GPS, it flagged the system to the pending leap second, well in advance. If it hadn't been for this GPS selection, the only way SecureSync would have known to update its time offset corrections (such as the TAI offset) at the moment of the leap second is if NTP had been provided ample notice to the pending leap second. Since GPS had already flagged the leap second prior to the leap second, SecureSync was able to correct the offsets just after the leap second was asserted.

In addition to the System Time offset for TAI needing to be updated at the leap second, the System time (kernel time) also needed to be updated by one second, as well. NTP updates the kernel (which is the time reference for the system) for this one second correction. As long as NTP can obtain from its selected reference, sufficient notice of the pending leap second before it actually occurs, the kernel time is automatically corrected at the correct second. However, if NTP cannot obtain sufficient advanced notice from its selected reference before it's inserted, the time correction is delayed until it can receive the LI bit change from its reference.

The PTP Option Cards, when configured as a PTP Master, read the System time every second. So once both the UTC to TAI offset as well as the kernel time have been corrected by one second, the PTP Master sends out the corrected time, immediately thereafter.

Specific to the logs you sent:
The logs you sent show that the System's time correction (the kernel "step") occurred on all of the SecureSyncs between 15:29 and 19:53 (Minutes / Seconds) after the leap second had been inserted. This is because this was the

first opportunity it had to obtain the LI bit change from its selected NTP reference and to apply the leap second to the kernel time.

If the SecureSyncs had been synced to GPS prior the leap second insertion (instead of to the Stratum 1 NTP server) the SecureSync's time would have adjusted at 23:59:60 two to three seconds after the leap second was inserted, instead of 15 to 20 minutes thereafter (as a result of the poll interval for the Stratum 1 server).

For any future leap second that may occur, we initially discussed potentially having you change both the Min and Max Poll intervals for the Stratum 1 server configuration to "4 (16 seconds)" on the day of the leap second. This would ensure NTP polled the Stratum 1 server every 16 second and therefore a couple of times during the one minute period that the Stratum 1 server has the LI bits set to indicate the pending leap second. However, we tested this and found that only one minute of advanced notice from the NTP reference, even at the quickest possible NTP poll interval, does not provide enough advanced notice to the kernel to apply the time correction at the leap second. Because the kernel was not able to flagged to correct the time at the Leap second, when the selected input is another NTP server, a few polls after the leap second occurred, NTP realized a one second step was needed. So about 15 to 20 minutes later, NTP stepped the kernel time on your SecureSyncs (other SecureSyncs using input references such as GPS, did not need to step the kernel after the leap second- the time was automatically corrected at the correct second because the kernel had ample notice of the pending leap second).

In summary of the above information:

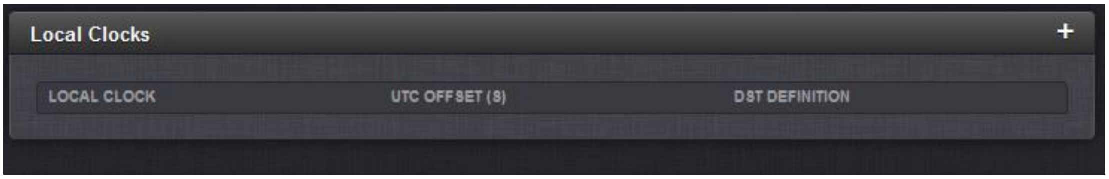
The GPS input had flagged the timing system of the pending leap second, well in advance (GPS started broadcasting this information on the leap second back in the March time-frame) this allowed the timing system to adjust the TAI offset within just a couple of seconds of the leap second. However, the IRIG signal limiting the LI bit change to only one minute did not provide the kernel with enough advanced notice.

So, our recommendation to you, if another leap second is scheduled in the future (and since it's unlikely that the IRIG reference can provide a longer advanced notice with the LI bit change occurring earlier than just one minute prior), would be to temporarily select GPS as the highest priority reference (instead of NTP) on the day of the leap second, via the Reference Priority table. This will provide both NTP and the timing system with sufficient advanced notice to prevent the need for NTP to have to step the time several minutes after the leap second has been inserted. Then, switch back to using NTP as the selected reference by making it the highest priority reference. Otherwise, using NTP as the input during the leap second will result in a delay of the one second time correction of the NTP and PTP timing outputs.

**Local System Clocks (Local Clock)

web browser

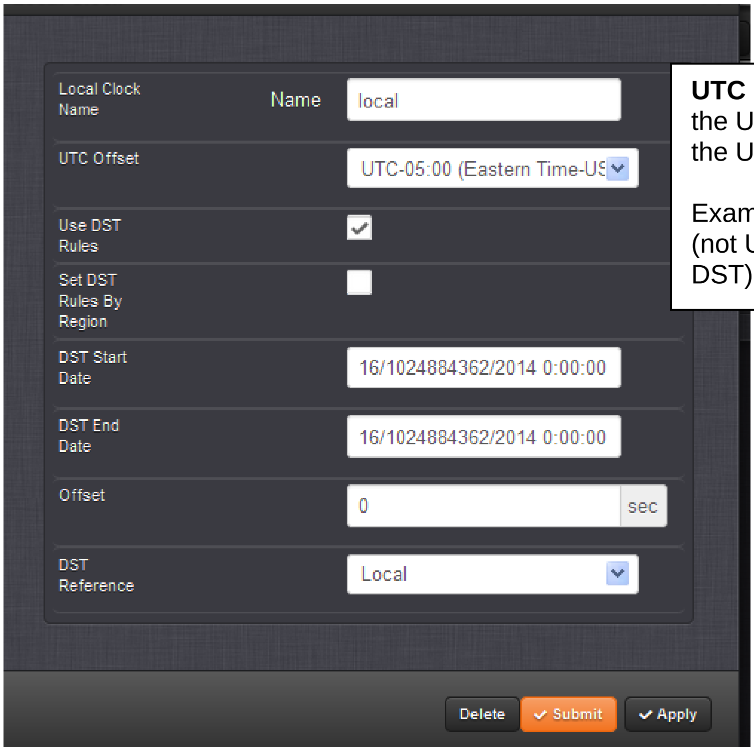
Management -> **Time Management** (click on the + to add a new local clock)



Local Clocks +

LOCAL CLOCK	UTC OFFSET (S)	DST DEFINITION

If “**Use DST rules**” is selected, bottom of page expands.



Local Clock Name — 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

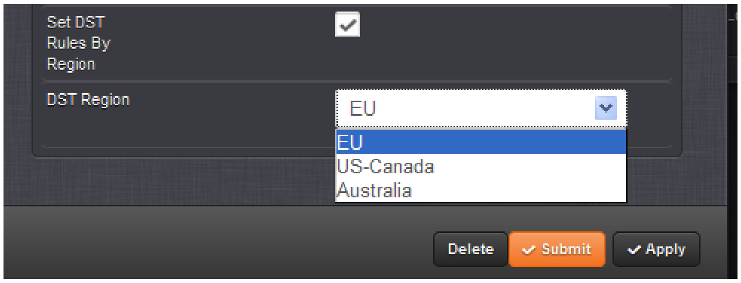
Offset: 0 sec

DST Reference: Local

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.

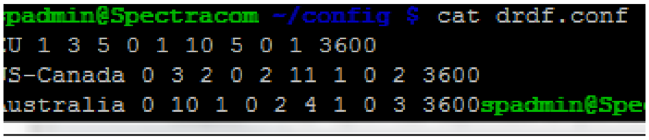


Set DST Rules By Region: ☑

DST Region: EU

DST Configuration

- Local clock configuration is stored in the “drdf.conf” file **(/config** directory) Example entry below:



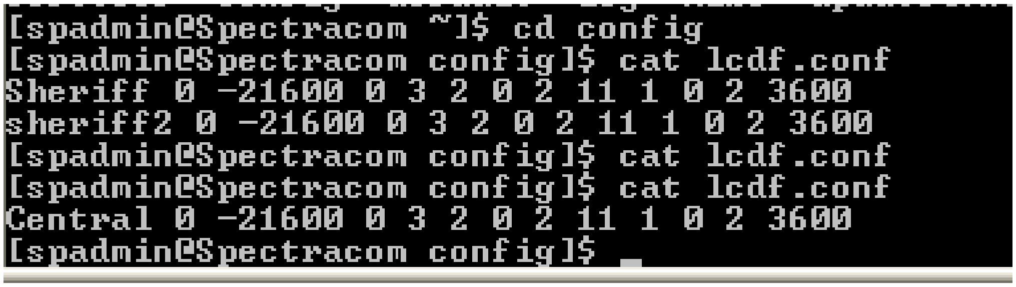
```
padmin@Spectracom ~/config $ cat drdf.conf
U 1 3 5 0 1 10 5 0 1 3600
S-Canada 0 3 2 0 2 11 1 0 2 3600
ustralia 0 10 1 0 2 4 1 0 3 3600spadmin@Spe
```

To view all created local system clocks in the SecureSync config file:

1) telnet/sh 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:

5. IRIG can send out a time code based on a local clock
6. On initial Setup, SecureSync can use the GPS position to setup a time zone offset used for a local clock
7. However, SecureSync's GPS position is only used for initial setup of the local clock. As the ship moves and the

GPS position changes, the time zone is NOT automatically updated based on position.

So if the NTP server moves to a new time zone, the offset would have to be manually changed.

Known issues with Local Clocks

A) Super-set Local Clock names (refer to Salesforce Case 5929 for NASA)

At least versions 4.8.6 and below will have issues with Local Clock names that are a super-set of another case-sensitive Local Clock name (Such as “Tom” and “Tom1”). Tom1 is selected as the Local Clock, “Tom” is actually the Local Clock selected.

Starting in v4.8.6, the pre-defined local clocks names of GPS, TAI and UTC , in the Front Panel setup were moved to the Local Clock selection (Time Scale field was removed). If a Local Clock name is created with any of these same case-sensitive letters, (such as “UTC-NONE”), and this name is selected in the drop-down, after hitting Submit, “UTC” is actually displayed/selected in the “Local Clock” field.

In summary:

- The only letters that can’t be capital letters in the Local Clock name are the ones at the beginning of the name that happen to match the default names in the “Local Clock” drop-down (UTC, TAI and GPS).
- Each Local Clock that is created shouldn’t be a super-set of another Local Clock name that has already been created (with the same case-sensitive letters). For example, if you have one named “Eastern”, you shouldn’t create another one call “Eastern-DST”. Otherwise, if you try to select “Eastern-DST”, “Eastern” will actually be selected.

Input references / Reference Priority table/ Reference Monitor/Time Sync / Holdover

*Input References (GPS-GNSS/Glonass/SAASM, PTP, IRIG, Freq in NTP, Havequick, ASCII, etc) /Reference Priority table/Time to synchronize to input reference

Input Reference designations for SecureSync (as of 6/5/12)

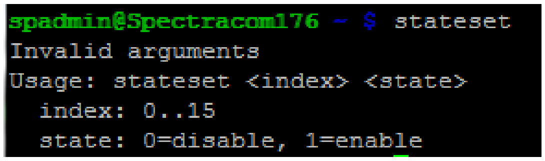
Reference Designation	CLI "Status" command displays	Input description	Refer to Hyperlink Section below
GPS/GNSS	gps	GPS / Glonass	GPS/Glonass
		(SAASM GPS)	SAASM GPS
IRIG	ir	IRIG (Inter-Range Instrumentation Group)	IRIG
HaveQuick	hvq	HaveQuick/Stanag	HaveQuick
ASCII Timecode	asc	ASCII time code reference	ASCII
Local System	self	SecureSync's built-in clock OR internal 1PPS generation	Local System
NTP	hst1	NTP (Network Time Protocol)	NTP
PTP (base)	mac	PTP input via base eth0 or 1	MAC (mac1 for instance)
PTP (1204-3B)	ptp	PTP (Precision Time Protocol)	PTP
User	User	Manually set time/Battery backed time	User/User
External 1PPS	epp	External 1PPS reference	EPP0
Frequency in (such as 1kHz to 10 MHz in)	frq	Frequency Reference	Frequency input (such as 10 MHz)
10 MHz/T1/E1	N/A	T1/E1 from an external source	T1 and E1 input

Note that some of these will be followed by a number (such as GPS 0 or IRIG 0). This number can vary, based on the number of similar inputs. GPS is currently limited to just one instance, so this one is currently always GPS 0. However, there can be multiple instances of the same inputs, such as IRIG. So this number may not always be a 0.

Input "Reference Priority" table

Note: The Reference Priority table settings are stored in the ***rmnf.conf*** file (located in the **/config** directory)

CLI commands used to configure the Reference Priority table

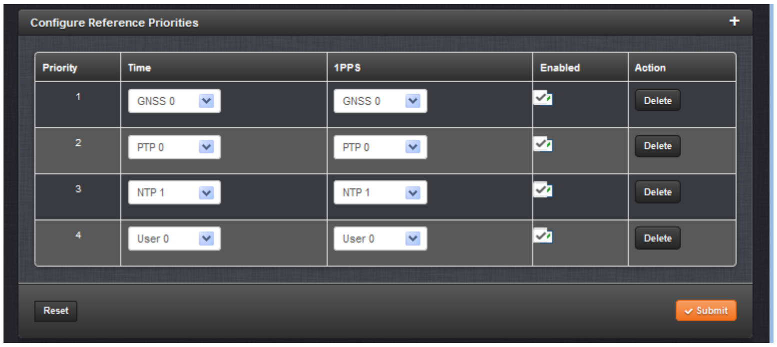


```
spadmin@Spectracom176 ~ $ stateset
Invalid arguments
Usage: stateset <index> <state>
  index: 0..15
  state: 0=disable, 1=enable
```

- To display the Reference Priority table: **reftable** <enter>
- To enable/disable entries in the Reference Priority table: **stateset** <enter>
- To set the priority of an entry in the Reference Priority table: **priorset** <enter>

A) Via browser

Management -> Reference Priority page



Configure Reference Priorities

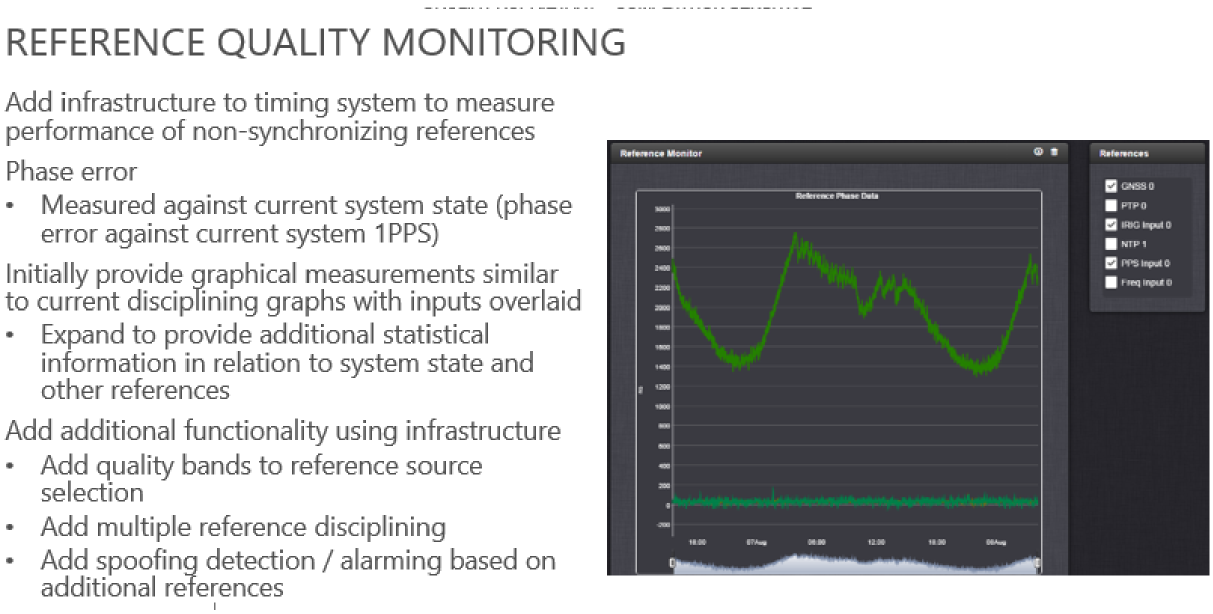
Priority	Time	1PPS	Enabled	Action
1	GNSS 0	GNSS 0	☑	Delete
2	PTP 0	PTP 0	☑	Delete
3	NTP 1	NTP 1	☑	Delete
4	User 0	User 0	☑	Delete

**Input Reference Monitoring

- ➢ Link to Reference Monitor info in 2400 SecureSync online manual:
  https://www.orolia.com/manuals/2400/Content/NC_and_SS/Com/Topics/TIME/RefMon.htm

  Note that if you click on the figures in this guide, they will expand and became much clearer!!

- ➢ Allows comparison of filtered phase offsets between input references (Individually compares each input reference against the System's on-time point)
  - ○ The phase values shown are the filtered phase differences between each input reference 1PPS, and the internal disciplined 1PPS.



☑ GNSS 0
□ PTP 0
☑ IRIG Input 0
□ NTP 1
☑ PPS Input 0
□ Freq Input 0

REFERENCE QUALITY MONITORING

Add infrastructure to timing system to measure performance of non-synchronizing references

Phase error

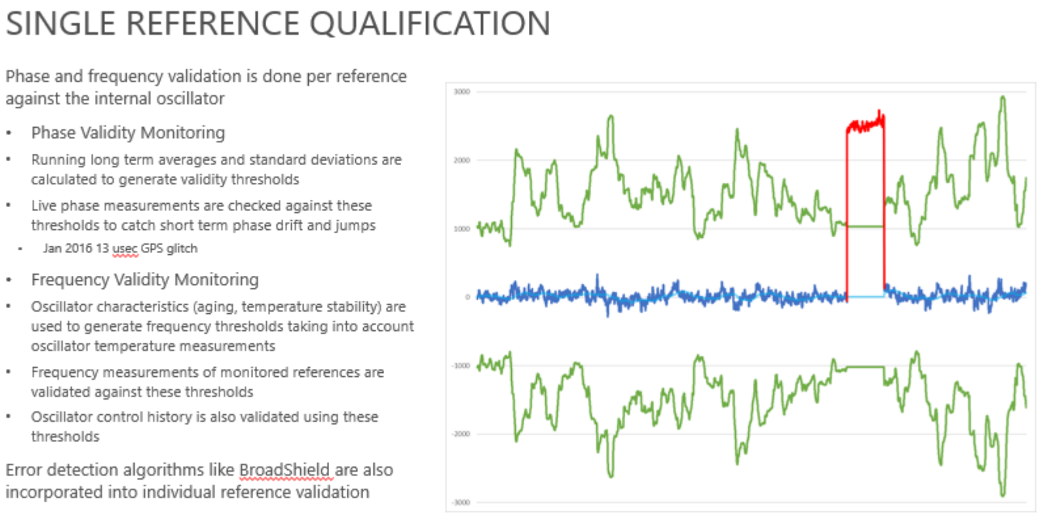
- Measured against current system state (phase error against current system 1PPS)

Initially provide graphical measurements similar to current disciplining graphs with inputs overlaid

- Expand to provide additional statistical information in relation to system state and other references

Add additional functionality using infrastructure

- Add quality bands to reference source selection
- Add multiple reference disciplining
- Add spoofing detection / alarming based on additional references



SINGLE REFERENCE QUALIFICATION

Phase and frequency validation is done per reference against the internal oscillator

- Phase Validity Monitoring
- Running long term averages and standard deviations are calculated to generate validity thresholds
- Live phase measurements are checked against these thresholds to catch short term phase drift and jumps
  - Jan 2016 13 usec GPS glitch
- Frequency Validity Monitoring
- Oscillator characteristics (aging, temperature stability) are used to generate frequency thresholds taking into account oscillator temperature measurements
- Frequency measurements of monitored references are validated against these thresholds
- Oscillator control history is also validated using these thresholds

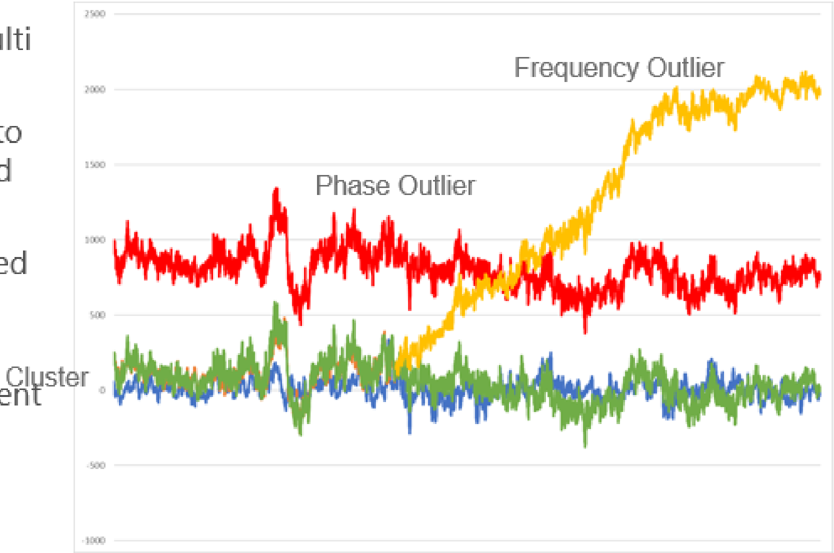
Error detection algorithms like BroadShield are also incorporated into individual reference validation

MULTI REFERENCE QUALIFICATION

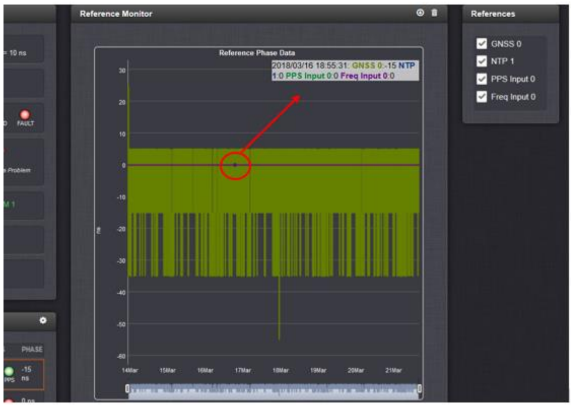
References validated by single reference checks are utilized in multi reference qualification checks

- Clustering techniques are used to group references together based on phase/frequency statistics
- Outliers can be determined based on phase biases or frequency drifts

All input references and independent monitoring sources like the fiber optic reference can be utilized in these techniques



Tools -> Reference Monitor page of the browser



Email from Keith (21 Mar 18) The table on the right of the plot lists all available 1PPS input references, allowing the ability to enable/disable the display of each one in the graph.   Mouse-hovering over the graph plot (shown with the red circle I added to the plot) opens a gray display window (upper-right corner of the plot window) displaying the details of each reference at that particular date/time (in UTC timescale) and also indicates the corresponding line color of each reference being displayed in the plot area. The 1PPS phase error on the left side of the plot area, for the actual values of the 1PPS phase error for each input reference, is in "Nanoseconds"

The phase in the Reference Status location is the difference between the Reference and the On-time point (1PPS). So all the reference compare themselves to the System's on-time point.

Reference Monitoring helps to understand and predict system behavior, and is an interference mitigation tool. It can also be used to manually re-organize reference priorities e.g., by assigning a lower reference priority to a noisy reference or a reference with a significant phase offset, or to automatically failover to a different reference if certain quality thresholds are no longer met (see Smart Reference Monitoring).

SecureSync allows Reference Monitoring by comparing the phase data of references against the System Ontime Point.
The phase values shown are the filtered phase differences between each input reference 1PPS, and the internal disciplined 1PPS.

The data is plotted in a graph in real-time. The plot also allows you to display historic data, zoom in on any data range or on a specific reference. A data set can be exported, or deleted.

To monitor the quality of references:

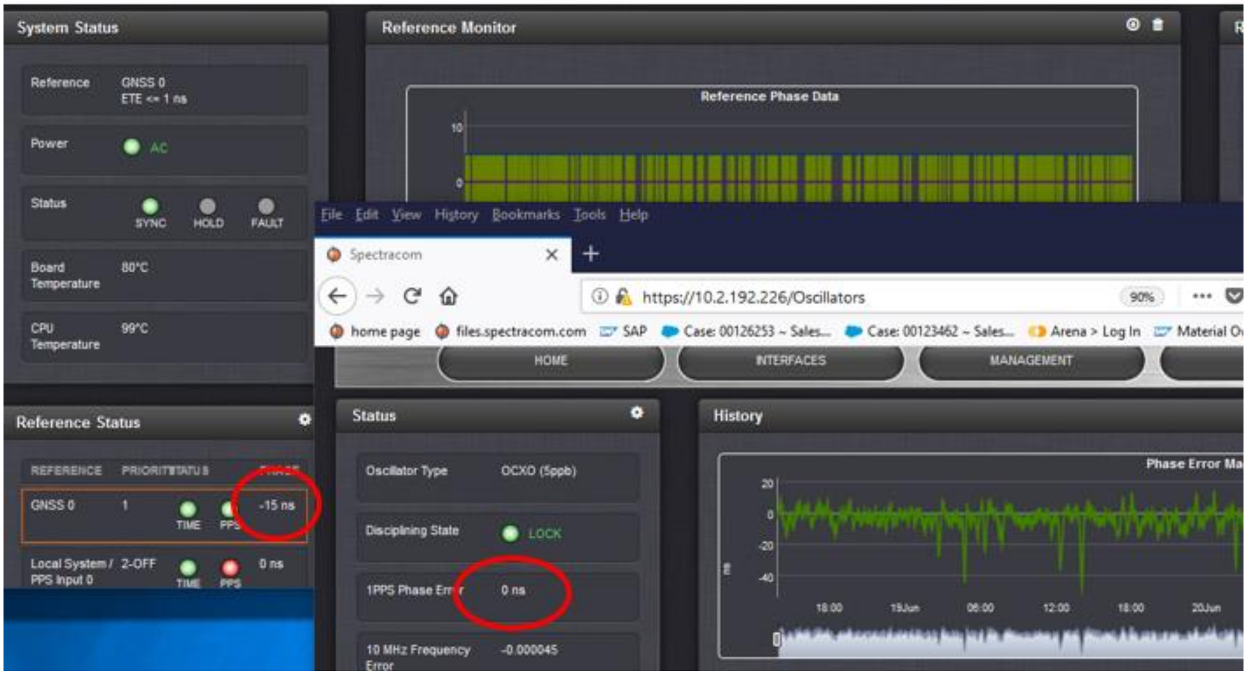
On the left side of the screen, Status information is displayed for the System and the References. Note that the Reference Status panel also displays the latest PHASE OFFSET reading (1) for active references against the System Ontime Point. The reading is updated every 30 seconds.

This Reference Phase Offset Data is plotted over time (abscissa) in the Reference Monitor panel in the center of the screen. Use the check boxes in the References panel (2) to select the reference(s) for which you want to plot the phase offset data. Use the handles (3) to zoom in on a time window.

The scale of the axis of ordinate (4) is determined by the largest amplitude of any of the references displayed in the current time window. Use the checkboxes in the References panel on the right to remove references from the graph, or add them to it

“Side-by-side” variances between “disciplining” phase error values (reported in the Management -> Disciplining and Reference Priority pages) versus the phase error values reported in the Tools -> Reference Monitor page

- Due to differences in granularity in the ***Disciplining**/ **Reference Priority*** pages, versus the ***Reference Monitor*** page. the phase error values for the same reference may be reported as two different values.
  - As shown below, the phase error is reported as **0 ns** in the Disciplining page, while the GPS phase error is being reported as **-15 ns** in the Reference Monitor page



System Status

Reference: GNSS 0, ETE <= 1 ns
Power: AC
Status: SYNC HOLD FAULT
Board Temperature: 80°C
CPU Temperature: 99°C

Reference Status

REFERENCE	PRIORITY	STATUS	PHASE
GNSS 0	1	TIME PPS	-15 ns
Local System / PPS Input 0	2-OFF	TIME PPS	0 ns

Status

Oscillator Type: OCXO (5ppb)
Disciplining State: LOCK
1PPS Phase Error: 0 ns
10 MHz Frequency Error: -0.000045

Per Dave S (19 Jun 2018) I don’t remember the direction of the offset (negative vs positive), but as far as the differences, the disciplining phase error is a filtered error, that has higher resolution. The reference monitor phase errors are raw offset values with a 20ns resolution. They should absolutely track each other in terms of trends, but due to the filtering and differences in resolution/granularity there will be differences in the reported offsets.

Reference Monitor data/data storage (errors may occur when dowmloading large amounts of data)

- Data is stored in the “**log_red_mon_statuses**” table of the SQLite database
- This data can be exported by either:
  1) Saving/exporting the logs:
     A. View the **lafayette** (sqllite) database using the “**DB browser for SQLite.exe**” freeware.
     B. In the “**Browse Data**” tab, select the “**log_red_mon_statuses**” table:

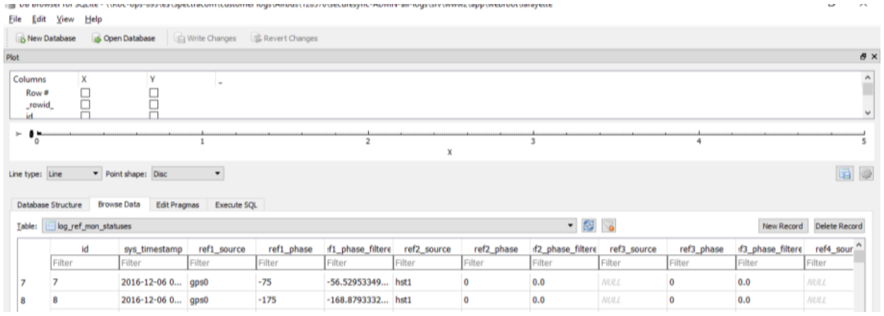
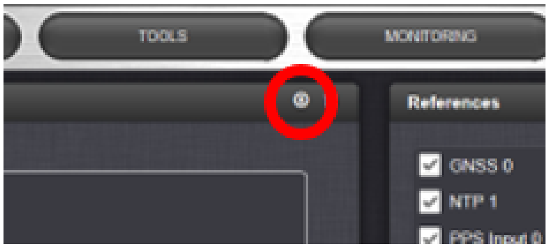


Table: log_ref_mon_statuses

	id	sys_timestamp	ref1_source	ref1_phase	f1_phase_filtere	ref2_source	ref2_phase	f2_phase_filtere	ref3_source	ref3_phase	f3_phase_filtere	ref4_sour
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
7	7	2016-12-06 0...	gps0	-75	-56.52953349...	hst1	0	0.0	NULL	0	0.0	NULL
8	8	2016-12-06 0...	gps0	-175	-168.8793332...	hst1	0	0.0	NULL	0	0.0	NULL

2) Or by clicking the “down arrow” (download) icon (next to the garbage can icon) in the ***Tools*** -> ***Reference Monitor*** page of the browser.



Note the amount of data in the Reference Monitor table may be too large to be able to use the download to csv file button

- Refer to Salesforce Case 1777373 (Oct 2018, with v5.8.2)

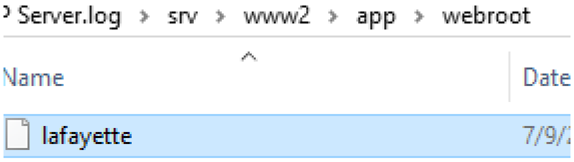
Attempted download from 'Reference Monitor':
https://<servername>/Logs/getGraphStatus/LogRefMonStatus.csv
returns HTTP ERROR 500

Response from Keith (21 Nov 2018) I just spoke with the Engineer again and believe we have the explanation for you. Shortly after initially reading your report, he (and then I, after he mentioned it) believed the only issue with the downloading of the table (using the download button in the browser) was strictly related to the amount of data being downloaded via the browser, and also being converted to a csv file. This was also helped confirmed when I initially saw similar conditions occur, until I disabled all but one of the References on the side of the table (so that the data for just one reference was to be downloaded). This resulted in a successful download of this reference's data using the download icon in the browser.

To confirm what you are seeing when downloading the table via the browser icon is a limitation of the amount of data which can be processed by the web browser, please first perform the CLI command of **clearstats**<enter>. This command will only delete the “statistics” data from the database (it doesn’t delete any logs, which uses a separate command for these items to be deleted). Very shortly thereafter, perform the download table using the icon in the web browser again, to confirm the data is downloaded/processed successfully, and as expected, into a csv file by the web browser's functionality.

Note that if you wish to download the entire table (instead of selecting various references from the table to induvially download data) when there is more extensive data present in this table, note this table is also contained in each Logs bundle file you download from the unit. So, there is a second available method to obtain all the data, besides using the browser download icon (the download icon in the browser uses a different method to download the data to your computer than the logs download function).

The logs bundle (once extracted a couple times to unbundle it) contains the sqlite database, which stores data such as the Monitor table, is housed in the main "**srv**" folder of the extracted log bundle (there are a couple sub-folders after clicking the “srv” folder, but only one file- so just keep clicking until you see the file "Lafayette", as shown below):



This database file can then be opened to view the various tables/data using the freeware program “**DB Browser for SQLite**” (http://sqlitebrowser.org/)

After opening the lafayette file with this freeware program, and to see all the data in the Reference Monitor table, first select the second tab from left Browse Data”. Then in the “Table” drop-down (just below the tabs) select **log_ref_mon_statuses**”

The tables/data shown in the viewer program should also be able to be exported to csv files. But for some reason, I get an error message on my PC when I try to export any of the tables to a file (engineers are able to export them from their PCs).

Please confirm the download icon function works when pressed shortly after performing the clearstats command.

Length of time Reference Monitor data is stored for:

- Refer to the email below from Ron (and in the SecureSync online user guide at th following link, scroll down to "**Deleting Temperature Data**") http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm
  - Excerpted below

    "*Temperature graphs (and other graphs as well) will display up to approximately 10000 readings, which are generated at a 1/min. rate, i.e. the data displayed covers about 7 days. Thereafter, the oldest data gets overwritten.*"

Email from Ron D (28 Mar 18) (Note- not edited to be directly sent to a customer- except the last paragraph)
The reference monitoring data is stored for the same amount of time as every other graph in SecureSync.

The temperature monitor graph page in the online manual states it. It should probably be added to all of the graph sections that it applies to.

**Smart Reference Quality Monitoring/Reference validation

Refer to online SecureSync User Manual:
http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/RefMon.htm#Smart

- Provides 1PPS Phase Validation/Phase Verification using Reference Monitor
- Provides automatic reference switching to the next lower priority reference/ or coasting of the oscillator for 1200 seconds (while in a force Holdover state).

Description of Smart Reference Monitoring

Spectracom's Smart Reference Monitoring uses phase error validation in combination with automatic failover:

The phase error validation **calculates long-term averages and standard deviations** of the phase offset between the monitored external reference and the internal system reference. The standard deviation is used to calculate two validity thresholds, a higher and a lower one (the latter acts as a hysteresis buffer, preventing the status flip/flopping of the actual phase error validation value varies closely around the outer threshold). The thresholds are not user-configurable.

If the higher threshold value is exceeded, the automatic failover will cause SecureSync to fall back to its next lower reference (if available).

If no other reference is found, the unit will transition into a **1200-second coasting period**. During this coasting period, the TIME and 1PPS references will continue to be considered valid, but SecureSync's oscillator will flywheel. Note that the PPS reference status light will turn yellow. After expiration of the 1200 seconds. the unit will transition into Holdover.

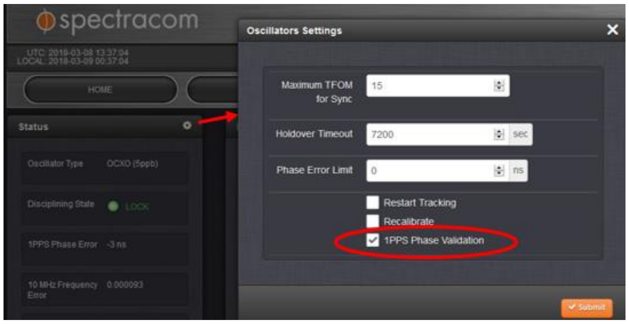
Should, however, the above-mentioned higher threshold value no longer be exceeded, the unit will remain in the 1200-second flywheel mode until either (a) the lower threshold value is no longer exceeded, or (b) the 1200-second flywheel period expires. In both cases the PPS status light will turn green again.

Email from Hughes (15 Oct 2018) pertaining to PRN27 signal change: Spectracom has reported that with the Phase Validation feature turned on, has shown that the 1 PPS jump is minimized to about 100 ns and no 10 MHz jump in holdover during the 10/7 1800 PRN27 event emulation with the GG unit.

Enable/disable state of Smart Reference Monitoring

- **Disabled** by factory default (upgraded units / units which are cleaned and newly shipped units)
- “**Enabled** in the **Management** -> **Disciplining** page.

1. Press the gear icon to the right of “STATUS” (on the left side of the page).
2. then select “**1PPS Phase Validation**” checkbox.



UTC: 2018-03-08 13:37:04
LOCAL: 2018-03-09 00:37:04

Status

Oscillator Type OCXO (5ppb)

Disciplining State ● LOCK

1PPS Phase Error -3 ns

10 MHz Frequency Error 0.000093

Oscillators Settings

Maximum TFOM for Sync: 15

Holdover Timeout: 7200 sec

Phase Error Limit: 0 ns

□ Restart Tracking

□ Recalibrate

☑ 1PPS Phase Validation

- **Once this function has been enabled**: “Phase measurements and thresholds are dynamically calculated based on the input references statistics”

Example Log entries associated with Smart Reference Monitoring enabled

osc.log

```
Mar 12 12:16:15 HOU-GPS-01 HOU-GPS-01: [system] 2018 071 12:16:15 000 XO: Phase Reference Valid.
```

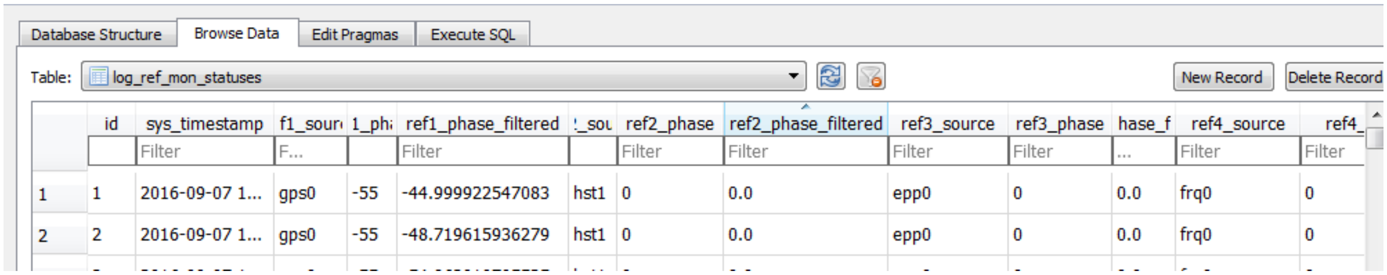
Timing.log

```
Jan  3 19:06:41 FR2-PQT-M512-309-GM2 FR2-PQT-M512-309-GM2: [system] 2018 003 19:06:41 000 PHASE INVALID
Reference gps0 Restart=0 PPS Valid
```

Reference Monitor log data/graphs

- Phase error values for all input references are stored in the “Lafayette” database.

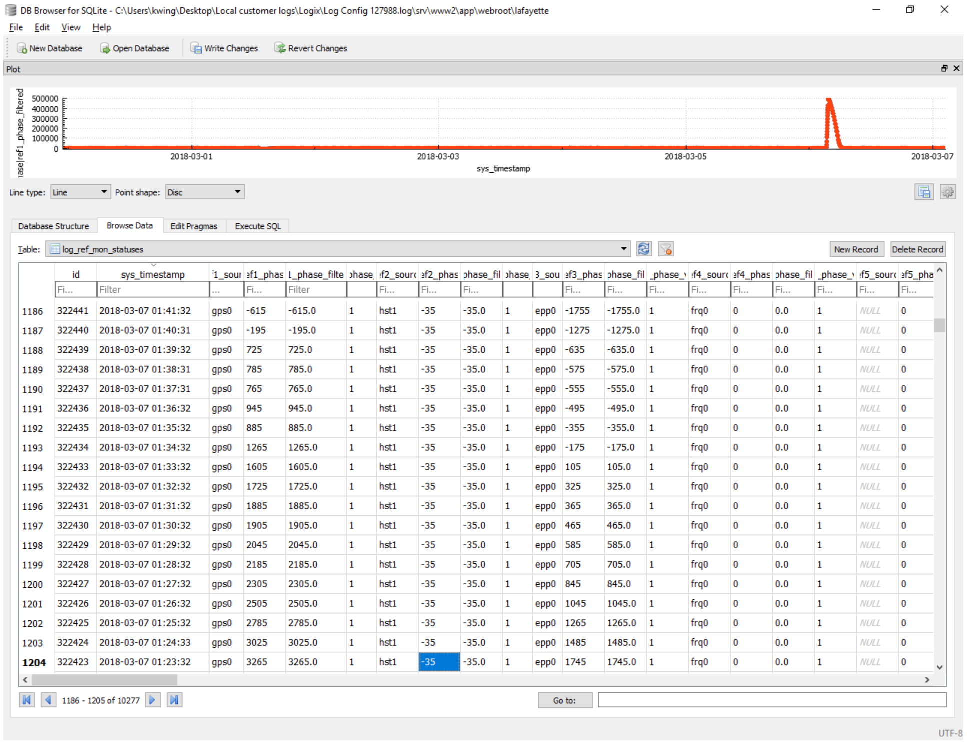
The Reference Monitor log data is stored in the SQL database that is in the log bundle (select “**log_ref_mon_statuses**” in the Table dropdown), or it can be extracted using the “arrow” icon in the upper-right corner of the graph display in the **Management** -> **Disciplining** page of the browser.



	id	sys_timestamp	f1_sour	1_phi	ref1_phase_filtered	!_sou	ref2_phase	ref2_phase_filtered	ref3_source	ref3_phase	hase_f	ref4_source	ref4_
		Filter	F...		Filter		Filter	Filter	Filter	Filter	...	Filter	Filter
1	1	2016-09-07 1...	gps0	-55	-44.999922547083	hst1	0	0.0	epp0	0	0.0	frq0	0
2	2	2016-09-07 1...	gps0	-55	-48.719615936279	hst1	0	0.0	epp0	0	0.0	frq0	0

Three associated fields for each timestamp

- **Refx_source:** name/number for each input reference
- **Ref phase**: coarse phase error measurement from FPGA (don’t use this value)
- **Ref phase_filter:** accurate phase error measurement (use this value)



	id	sys_timestamp	'1_sour	ef1_phas	l_phase_filte	phase_	f2_sour	ef2_phas	phase_fil	phase_	3_sou	ef3_phas	phase_fil	_phase_	f4_sour	ef4_phas	phase_fil	_phase_	f5_sour	ef5_pha
	Fi...	Filter	...	Fi...	Filter		Fi...	Fi...	Fi...			Fi...	Fi...	Fi...	Fi...	Fi...	Fi...	Fi...	Fi...	Fi...
1186	322441	2018-03-07 01:41:32	gps0	-615	-615.0	1	hst1	-35	-35.0	1	epp0	-1755	-1755.0	1	frq0	0	0.0	1	NULL	0
1187	322440	2018-03-07 01:40:31	gps0	-195	-195.0	1	hst1	-35	-35.0	1	epp0	-1275	-1275.0	1	frq0	0	0.0	1	NULL	0
1188	322439	2018-03-07 01:39:32	gps0	725	725.0	1	hst1	-35	-35.0	1	epp0	-635	-635.0	1	frq0	0	0.0	1	NULL	0
1189	322438	2018-03-07 01:38:31	gps0	785	785.0	1	hst1	-35	-35.0	1	epp0	-575	-575.0	1	frq0	0	0.0	1	NULL	0
1190	322437	2018-03-07 01:37:31	gps0	765	765.0	1	hst1	-35	-35.0	1	epp0	-555	-555.0	1	frq0	0	0.0	1	NULL	0
1191	322436	2018-03-07 01:36:32	gps0	945	945.0	1	hst1	-35	-35.0	1	epp0	-495	-495.0	1	frq0	0	0.0	1	NULL	0
1192	322435	2018-03-07 01:35:32	gps0	885	885.0	1	hst1	-35	-35.0	1	epp0	-355	-355.0	1	frq0	0	0.0	1	NULL	0
1193	322434	2018-03-07 01:34:32	gps0	1265	1265.0	1	hst1	-35	-35.0	1	epp0	-175	-175.0	1	frq0	0	0.0	1	NULL	0
1194	322433	2018-03-07 01:33:32	gps0	1605	1605.0	1	hst1	-35	-35.0	1	epp0	105	105.0	1	frq0	0	0.0	1	NULL	0
1195	322432	2018-03-07 01:32:32	gps0	1725	1725.0	1	hst1	-35	-35.0	1	epp0	325	325.0	1	frq0	0	0.0	1	NULL	0
1196	322431	2018-03-07 01:31:32	gps0	1885	1885.0	1	hst1	-35	-35.0	1	epp0	365	365.0	1	frq0	0	0.0	1	NULL	0
1197	322430	2018-03-07 01:30:32	gps0	1905	1905.0	1	hst1	-35	-35.0	1	epp0	465	465.0	1	frq0	0	0.0	1	NULL	0
1198	322429	2018-03-07 01:29:32	gps0	2045	2045.0	1	hst1	-35	-35.0	1	epp0	585	585.0	1	frq0	0	0.0	1	NULL	0
1199	322428	2018-03-07 01:28:32	gps0	2185	2185.0	1	hst1	-35	-35.0	1	epp0	705	705.0	1	frq0	0	0.0	1	NULL	0
1200	322427	2018-03-07 01:27:32	gps0	2305	2305.0	1	hst1	-35	-35.0	1	epp0	845	845.0	1	frq0	0	0.0	1	NULL	0
1201	322426	2018-03-07 01:26:32	gps0	2505	2505.0	1	hst1	-35	-35.0	1	epp0	1045	1045.0	1	frq0	0	0.0	1	NULL	0
1202	322425	2018-03-07 01:25:32	gps0	2785	2785.0	1	hst1	-35	-35.0	1	epp0	1265	1265.0	1	frq0	0	0.0	1	NULL	0
1203	322424	2018-03-07 01:24:33	gps0	3025	3025.0	1	hst1	-35	-35.0	1	epp0	1485	1485.0	1	frq0	0	0.0	1	NULL	0
1204	322423	2018-03-07 01:23:32	gps0	3265	3265.0	1	hst1	-35	-35.0	1	epp0	1745	1745.0	1	frq0	0	0.0	1	NULL	0

Length of time the Reference Monitor data is stored for:

- refer to (in the SecureSync online user guide, then scroll down to "**Deleting Temperature Data**") http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm

Email from Ron D (28 Mar 18) The temperature monitor graph page in the online manual states it. It should probably be added to all of the graph sections that it applies to.

"Temperature graphs (and other graphs as well) will display up to approximately 10000 readings, which are generated at a 1/min. rate, i.e. the data displayed covers about 7 days. Thereafter, the oldest data gets overwritten."

http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/TempMon.htm

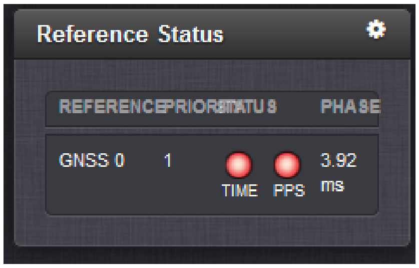
**Input “Reference Status” table

- The SecureSync’s Input “Reference Status” table shows the sync status of all possible input references that SecureSync can sync with.
- Each reference’s phase error is also individually reported in the “**Reference Status**” table (reported in both ***Home*** and the ***Management*** -> ***Reference Priority*** pages of the browser)

A) Web browser

Left-side of the Management -> Reference Priority page

- current 1PPS phase error (to the right of each listed reference)



Reference Status

REFERENCE	PRIORITY	STATUS	PHASE
GNSS 0	1	● TIME ● PPS	3.92 ms

Switching from one input reference to another

SecureSync can be "synced" to more than one reference at a time, with only the highest priority input selected at any given moment. Theoretically, if the highest priority input goes away or becomes not valid, SecureSync will seamlessly transition to the next highest priority without going into Holdover alarm (an entry is created indicating SecureSync switched references). However, Engineering has seen it glitch when switching from one input to another, where the Holdover alarm is generated for one second, and then it's back in sync by the next second. You can let the customer know that the switchover from one reference to another will take no more than one second, as long as more than one valid input is present.

Time to synchronize System Time once an input reference is present and valid

(Questions below were answered by Dave Sohn on 10/11/11)

Q. Does the above time depend on the type (IRIG, ASCII time, NTP) of a reference signal as well?

A. The time for references to become valid from connection of input varies between references, and the state of the input reference. Once a reference is valid and synchronizing the system, the system time will sync within three seconds. The 1PPS may take longer to synchronize depending on the difference between the system and the reference, and is not dependent on which reference is used.

Q. Under the following conditions, how long [s] does the synchronization take?
Difference between SecureSync's time and reference signal's is 1 second:
Difference between SecureSync's time and reference signal's is 1 minute:

A. There is no difference in how long to synchronize the time of the timing system based on the time difference. The time reported by NTP may take additional time depending on the time difference. I don’t have estimates for the time to resolve that.

NTP Input

- Refer to the **NTP SecureSync Peering** document for more info :I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP peering

** "Time Reset" when NTP first starts-up

- Time Steps/Time slews/panic threshold (1000 seconds)
- Refer to **"Time Reset" when NTP starts up** (..\CustomerServiceAssistance.pdf) for more details on how NTP initially corrects the time.

**(HST1) Host disciplining of the oscillator when using NTP as the PPS input reference

1. Applicable to TCXO and OCXO only
2. Refer to (in this doc:(HST1) Host disciplining of oscillator when NTP or "User set time"

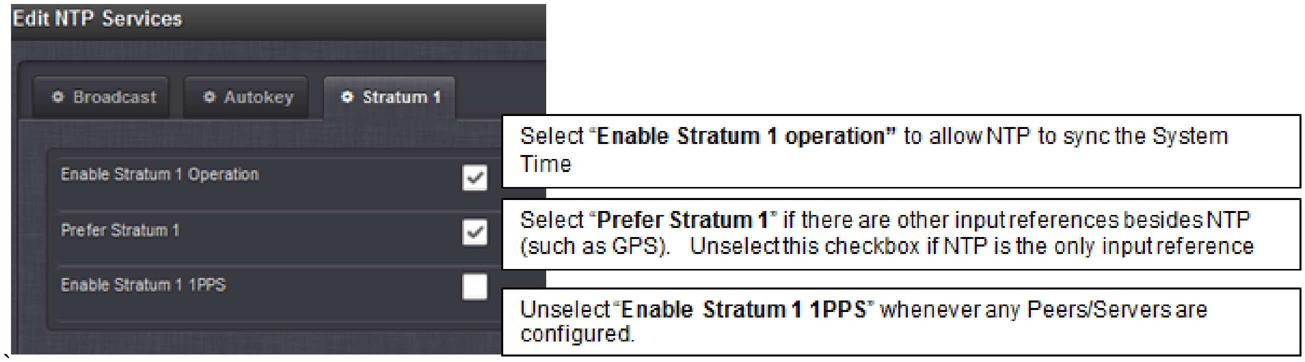
NTP/External PPS input

- The System 1PPS is controlled by NTP – not by the oscillator (bypasses the oscillator). However, NTP input can be combined with epp0 (external 1PPS input).
- This mode requires a 1PPS input Option Card be installed and changes made to NTP via the Expert Mode). Refer to: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert mode- 1PPS input

Important Notice: Using NTP and external PPS input as the selected references requires **NTP Expert mode be enabled** so the ntp.conf file can be manually edited. Failure to edit the ntp.conf file in Expert mode degrades the performance of the SecureSyncs outputs (including PTP) and the system does not take advantage of the external PPS accuracies.

1PPS synchronization with NTP input - configuration notes

Management -> **NTP Setup** page, click on the "Gear" ICON (next to "NTP Services") and Select the "**Stratum 1**" tab



Edit NTP Services

Enable Stratum 1 Operation ☑

Prefer Stratum 1 ☑

Enable Stratum 1 1PPS □

Select "**Enable Stratum 1 operation"** to allow NTP to sync the System Time

Select "**Prefer Stratum 1**" if there are other input references besides NTP (such as GPS). Unselect this checkbox if NTP is the only input reference

Unselect "**Enable Stratum 1 1PPS**" whenever any Peers/Servers are configured.

`

Syncing NTP with a SecureSync that is synced via NTP/ External PPS input

- Morgan Stanley is one example of a customer using this mode.
- Make sure SecureSync indicates in sync with NTP/External PPS.
- When syncing NTP via external 1PPS input, NTP Expert mode is required. Must manually change the Atom

clock driver (127.127.22.0) value in the ntp.conf file from Stratum 0 to Stratum 1.

Change the **“fudge 127.127.22.0 stratum 0**” line to **“fudge 127.127.22.0 stratum 1**” (no other changes need to be applied.

Note: leave Expert Mode enabled or this ntp.conf file will go back to the default vaues.

- Refer to the User Case examples in the NTP Peering document: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP peering

Or the Tech note at:
EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert mode- 1PPS input\NTP PPS Configuration V4.docx

Note: We recommend adding at least two Stratum 1 servers, to avoid a potential condition which might cause NTP to periodically switch between the Stratum 2 server, the System PPS and the System Time (System Time may periodically go into the Holdover mode, making the System Time a valid input to NTP). Listing more than one Stratum 1 server gives the Stratum 1 servers more “weight” so that NTP can always select one of the Stratum 1 servers.

The logs will show **periodic Holdover alarms** occurring, and NTP log will show periodically switching between TSync 0 (System Time), PPS 0 (System PPS) and one or more Stratum 1 servers.

- Note that in at least software versions 5.3.1 and below, Holdover is an Event (entry in the Events log) instead of being an Alarm (entry in the Alarms log)

NTP input/1PPS synchronization operation

When SecureSync is synced with NTP input, the oscillator’s 10 MHz output frequency is not disciplined (the oscillator is in a free-run mode). Starting once NTP goes into sync and changes from Stratum 16 to a lower stratum (changes to Stratum 2 for example) and then every 60 seconds thereafter, the System 1PPS/1PPS output (1PPS phase error) is stepped about every two seconds into alignment with NTP’s 1PPS to keep it in alignment with NTP.

The oscillator’s 10 MHz output frequency will continue to drift off because the oscillator isn’t being disciplined to an input. TFOM will remain at 15 while synced with NTP input.

With a scope, and after the 1PPS output of the Stratum 2 server finished stepping. I was seeing about 750us to 800us of offset between the Stratum 1 and Stratum 2 server’s 1PPS output. Over time, I was seeing about 20us or so of average periodic jitter on the S2 server’s 1PPS output. On occasion, it went to about 3 to 4ms, but could potentially jump higher.

1. The Oscillator Frequency is not disciplined with NTP input (oscillator’s output frequency remains in free-run mode).
2. TFOM will start at the value it was at, just prior to NTP sync. Then it will increase as the oscillator continues to drift while synced to NTP.
3. So if it was synced to GPS at Stratum 3 when switching to NTP sync, TFOM will start at 3 and then slowly ramp up.
4. If it hasn’t previously synced to another reference before syncing to NTP, TFOM will be and remain “15” unless it switches to another external reference (such as GPS) sometime thereafter. (“Accuracy Not determined” will be indicated),

TFOM is reported in the browser/CLI:

Management -> **Disciplining** page

- CLI command for **TFOM**: **SS_GetTfom 0** <enter>

○ CLI command for reading the **MaxTFOM** value **SS_GetMaxTfom 0** <enter>

1. "1PPS Phase Error" will continue to report "1 Sec" (linked to TFOM not being measured) if SecureSync hasn't previously synced to another external reference, such as GPS. Then it will increment from there.
2. With NTP input being a lower priority input reference, a 1PPS jump will occur about a minute after losing a higher priority reference (holdover for about a minute and then NTP kicks in, causing the 1PPS to jump.
3. As typical, NTP output accuracy is like 1-10ms, 1PPS output/System Time/on-time point will have more jitter than with GPS input.
4. Due to NTP Stratum 2 offset between the S2 server and its selected S1 server, the 1PPS/on-time point will be delayed from the on-time point of its reference by about a 1ms processing delay PLUS the NTP offset value (if NTP offset is 50ms because of lots of hops, the offset between the on-time points will be about 51ms).
5. NTP input does not become a "valid" reference, until the Linux kernel has been corrected (second round of NTP sync has to have occurred- so it doesn't go valid until the second time it goes into sync). KTS timing engine does not use it for a reference until this second sync.
6. User and NTP references only go "valid" when they become the "selected reference". They do not remain valid if they aren't selected (they remain not valid when they aren't selected. with NTP, it's the selected reference, when NTP selects another Time Server to be its selected reference (as displayed on the NTP-> Status page or in the NTP log).

The reason it does not remain valid is because NTP can be an input or an output, but not both at the same time. So, NTP switches to output mode and is then toggled back to input mode again (so it's not a constant input reference.

Note: NTP may periodically and temporarily select an NTP server (before switching back to the System Time reference, for example). In this scenario, NTP will go momentarily valid and then back to not valid again, because NTP is no longer synced to another NTP server.

Even though it's normally displayed as "not valid", NTP inputs from other NTP servers are checked for validity each second, allowing NTP to become the selected reference within one second of losing all higher priority references (it doesn't have to wait to be re-qualified, when all other higher priority references are lost. Instead, it can switch over to NTP "right away".

Questions from Masataka - answers from Keith (8 Jan 15 based on 5.1.7 software)

Q And customer measure phase change of 1PPS from SecureSync by comparing phase difference between 1PPS of SecureSync and 1PPS of sample itself. But as soon as SecureSync sync to strtum1 NTP server(ntp.nict.jp),
this phase difference start to expand .

[Question]
1.Could you please let us know possible cause of this symptom?
Keith's response: In summary of the below information, the observed phase change of the 1PPS output is a direct result of the 1PPS output being aligned with the NTP reference.

When SecureSync is synced via NTP input, the oscillator's 10 MHz output is not disciplined. The oscillator remains in a free-run state, and the TFOM value starts at the value it was at, when synchronization occurs (with no other input references syncing it first, the TFOM will remain at 15). In this configuration, once NTP has fully synced and is no longer at Stratum 16 (and continuing every 60 seconds thereafter) its 1PPS output (System PPS) is step-adjusted to the internal 1PPS being generated by the NTP input. This is to maintain alignment of the System PPS to the NTP reference.

The phase change of the 1PPS output from the SecureSync when compared to the sample after NTP went into sync is the system adjusting the SecureSync's 1PPS to be in alignment with the NTP 1PPS (in small steps about once every two seconds). This alignment/ adjustment can't start to occur until after NTP within the SecureSync has gone into sync and its NTP is no longer Stratum 16 (When it's syncing to a Stratum 1 server, this alignment process starts when SecureSync's NTP goes to Stratum 2 for instance).

2.Could you please let us know how 1PPS output from SecureSync is affected by syncing to strtum1 NTP server?
Keith's response: Once NTP goes to stratum 2 in the SecureSync, the SecureSync's 1PPS output will be stepped as necessary to bring it into alignment with the NTP's 1PPS reference. This continues to occur every 60 seconds as long as the SecureSync continues to remain synced via NTP input in order to maintain the alignment of the System PPS with the NTP reference.

Note that as the NTP reference's 1PPS inherently has much more jitter than the 1PPS from GPS input, this will translate into more System 1PPS jitter than when the SecureSync is synced via GPS instead of via NTP.

3.Could you please let us know how 10MHz output from SecureSync is affected by syncing to strtum1 NTP server?   (I do not know what Sampler is using 10MHz output from SecureSync for. But please let us know behavior of 10MHz from SecuerSync when syncing to strtum1 NTP server.)

Keith's response: The oscillator's 10 MHz output is not disciplined while the SecureSync synced to NTP. The oscillator remains in a free-run mode with i's 10 MHz output frequency drifting off at the typical drift rate of the oscillator. The better the type of oscillator installed, the less frequency drift that will occur. Because the oscillator is not being disciplined with NTP input, its frequency is not being corrected back to an accurate 10 MHz to account for drift, as it normally does when the input reference is GPS, for instance.

DSCP values for NTP

Q I was analyzing network traffic and noticed that our clock is sending NTP responses to client requests at a QoS DSCP value of 46. This puts in our priority voice queue. I've looked through the GUI for a way to modify this setting but haven't been successful. Can you tell me how I can change this QoS value in the GUI or CLI? Thanks. As an alternative, we will configure the Cisco switch port inbound policy for the change in DSCP.
A reply from Dave L (26 Sept 16) DSCP values for NTP can be adjusted in NTP expert mode. By default, NTP 4.2.8 uses a DSCP value of 0x2e (46) for expedited forwarding. The DSCP value can be adjusted by adding the below line in the config file in expert mode.

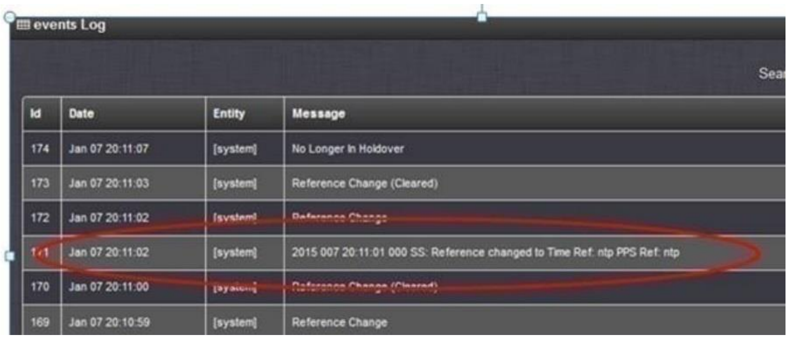
```
dscp <value>
```

For instance, to change the DSCP value to 0x30 (48) CS6 add the below line

```
dscp 48
```

Log entry for reporting the selected NTP server it's synced with

Q. Is there any logs that show where it has synced its time from the other NetClock. I have looked through all the different logs, but can't find it if there is one.
A Reply from Keith (6 JAN 15) Regarding the unit's logs indicating that its synced with the Model 9383, the only available entry for indication that it's in sync with another NTP server is in the "Events" log which will report "**Reference Changed to Time Ref: ntp PPS Ref: ntp**" (as shown below). But it doesn't log the specific IP address of the time server it's synced with.



Id	Date	Entity	Message
174	Jan 07 20:11:07	[system]	No Longer In Holdover
173	Jan 07 20:11:03	[system]	Reference Change (Cleared)
172	Jan 07 20:11:02	[system]	Reference Change
171	Jan 07 20:11:02	[system]	2015 007 20:11:01 000 SS: Reference changed to Time Ref: ntp PPS Ref: ntp
170	Jan 07 20:11:00	[system]	Reference Change (Cleared)
169	Jan 07 20:10:59	[system]	Reference Change

Issues with NTP Stratum synchronization

A) Periodic large 1PPS jumps (like ~300ms) in 1PPS phase error/NTP periodically goes to Stratum 16

- Make sure the "**Prefer Stratum 1**" checkbox is NOT selected if NTP is the only input reference available (no GPS input for instance).

Email from Keith (9 Jan 15) Besides periodically losing NTP time stamps (which doesn't sound like is occurring in this case), the only other thing I can think of is to unselect the "Prefer Stratum 1" checkbox.

Navigate to the **Management** -> **NTP Setup** page of the browser, click on the "**Gear**" ICON (next to **"NTP Services**") and Select the "**Stratum 1**" tab. Unselect the "Prefer Stratum 1" checkbox (leaving just the "Enable Stratum 1 Operation" checkbox selected in this tab).

This checkbox puts more weight on external references such as GPS for NTP's sync. With NTP being the only input reference, NTP may periodically switch to another free-running clock as its reference (temporarily making NTP go to Stratum 16) and then switching back to the 9383 again (allowing NTP to go back to Stratum 2 again). Note that after pressing Submit, NTP will automatically restart and resyncs just a couple minutes later (there is no need to manually stop/restart NTP for this checkbox change to become effective).

B) Nearly one second (0.99xxx) potential System Time (1PPS output jumps when syncing via NTP input

- Refer to Salesforce case 14648 (https://na8.salesforce.com/500C000000ZhjGW) for Open Access
- Potential "edge" issue starting with new version of NTP (v4.2.6) in versions 5.0.0 through 5.1.4 (should be fixed in version 5.1.5 and above updates)
- Can result in periodic one second time jumps and time corrections back sometime later
- Temporary fix is patch update version 5.1E
- Fix expected to be included in the next software update (anticipated as version v5.1.5) (UPDATE: 9 Jan 5 KW – I confirmed with Dave Sohn this fix was added to the software as of at least 5.1.7 if not earlier).

PTP Input (eth0/eth1)

PTP input from the Base/Chassis network interfaces (eth0/eth1)

- Refer to online 2400 SecureSync user guide: http://manuals.spectracom.com/2400/Content/VS/Topics/INTRO/VS_PTP.htm
- Requires software versions 1.3.0 or above be installed?

"mac1" input reference

26 Oct 2021 Per Ron Dries The reference **mac1** is the new reference created for PTP.

Software changes associated with PTP on base eth0/eth1 (refer also to Release Notes)

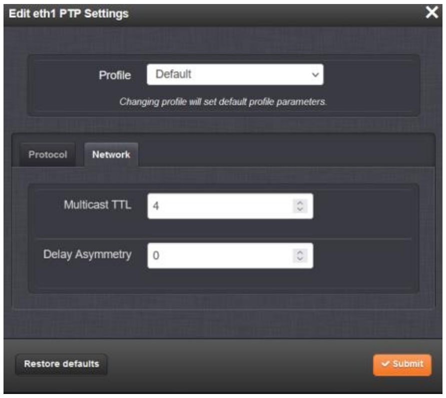
PTP software module installed

A) Version 1.4.1 and above: ptp4L

B) Versions prior to version 1.4.1: Orolia '*Masterpiece'* software

1) Version 1.6.0 update (~Nov 2022)

- Added "**Delay Asymmetry**" field (nanoseconds)



Edit eth1 PTP Settings

Profile: Default

Changing profile will set default profile parameters.

Multicast TTL: 4

Delay Asymmetry: 0

2) Update version 1.4.1 (April 2022)

- **Fixed the Known Issue**: When configured as a slave, the on-unit PTP will sometimes incorrectly remain in a Sync state when the Master has gone out of sync (found in 1.3.0).

3) Update version 1.2.2

The following defects were corrected:

- Fixed a one second offset found in PTP synchronization between the master and slave.
- Corrected an issue with PTP slaves incorrectly reporting as in-sync despite no longer receiving messages from the master.
- Corrected an issue with PTP slaves incorrectly reporting as in-sync despite the designated master no longer being in sync

Known Issues/limitations/software changes associated with PTP input

- In at least versions 1.2.2 and below, the 2400 cannot be configured to operate as both a PTP slave and NTP client.
- When switching PTP configuration between master and slave, occasionally the change will not take effect unless manually disabling/reenabling PTP on that interface.

PTP4L (also named "PTP for Linux")

- Open source PTP package replaced our PTP masterpiece software starting in v1.4.1 (I believe)

Good online Reference info on ptp4l:

(Config file): https://manpages.debian.org/unstable/linuxptp/ptp4l.8.en.html

"PTP4L – Man Page": https://www.mankier.com/8/ptp4l

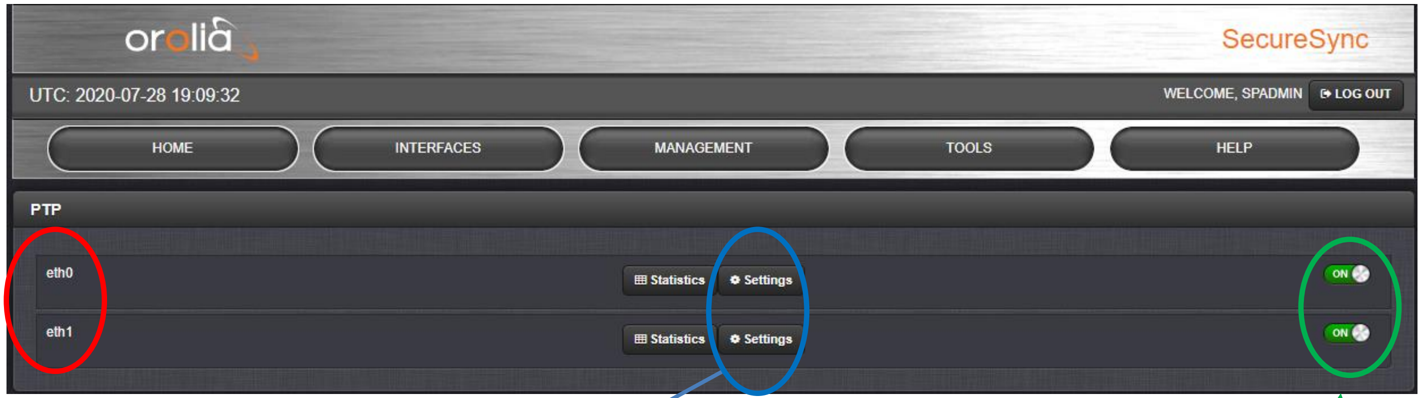
(Configuration, install, operation, logging, PTP Management Client, syncing/verifying client sync etc)

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/ch-configuring_ptp_using_ptp4l

(Servo States: "Clock Matrix": examples Servo_Locked Servo_unlocked, Servo_locked_unstable)
https://www.renesas.com/us/en/document/apn/clockmatrix-channel-control-ptp-time-day-counter?language=en

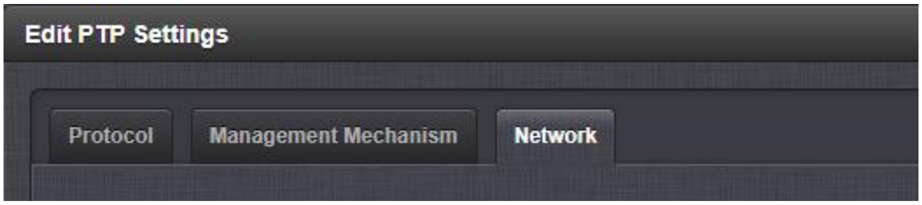
PTP Input Configuration/browser pages for PTP input

Management -> ***PTP Setup*** page



Settings button (Displays three Tabs for each interface)

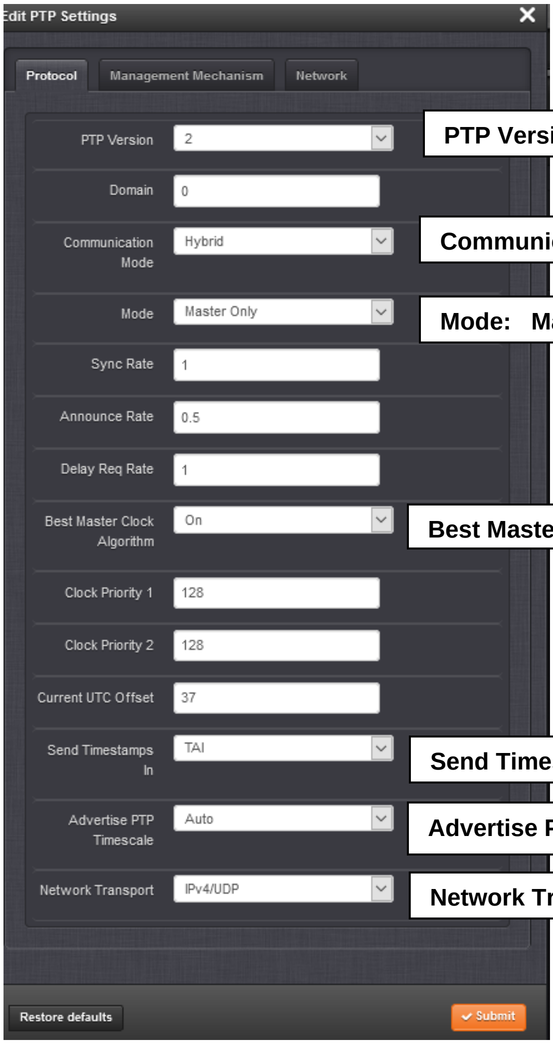
PTP Enable/Disable slider switches:



Network settings (IP Address, NetMask, port speeds etc)

- Not configured in the ***Management*** -> ***PTP Setup*** pages
  - Refer instead to ***Management*** -> ***Network Setup*** page of the browser

Protocol Tab (PTP version, mode, BMC, Timescale, Priorities, Message rates, etc)



PTP Version: 2
Domain: 0
Communication Mode: Hybrid
Mode: Master Only
Sync Rate: 1
Announce Rate: 0.5
Delay Req Rate: 1
Best Master Clock Algorithm: On
Clock Priority 1: 128
Clock Priority 2: 128
Current UTC Offset: 37
Send Timestamps In: TAI
Advertise PTP Timescale: Auto
Network Transport: IPv4/UDP

PTP Version: V1 or **V2**

Communication Mode: Multicast Hybrid Unicast

Mode: Master Only or **Slave only**

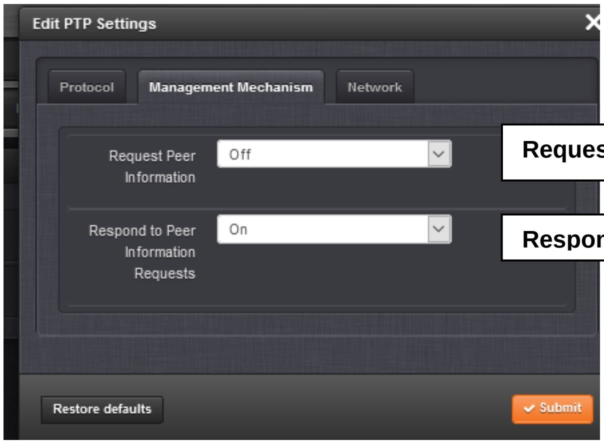
Best Master Clock algorithm: On or **Off**

Send Timestamps in: TAI or **UTC**

Advertise PTP timescale Network Transport: Auto or **Yes** or **No**

Network Transport: Ethernet or **IPv4/UDP** or **IPv6/UDP**

Management Mechanisms Tab (Peer Info requests)

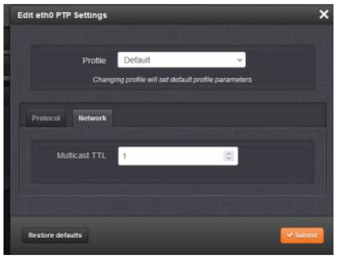


Request Peer Information: Off
Respond to Peer Information Requests: On

Request Peer Info: On/Off

Respond to Peer Info requests (Slave Only) On/Off

Management Mechanisms Tab (Multicast TTL values)



Profile Default

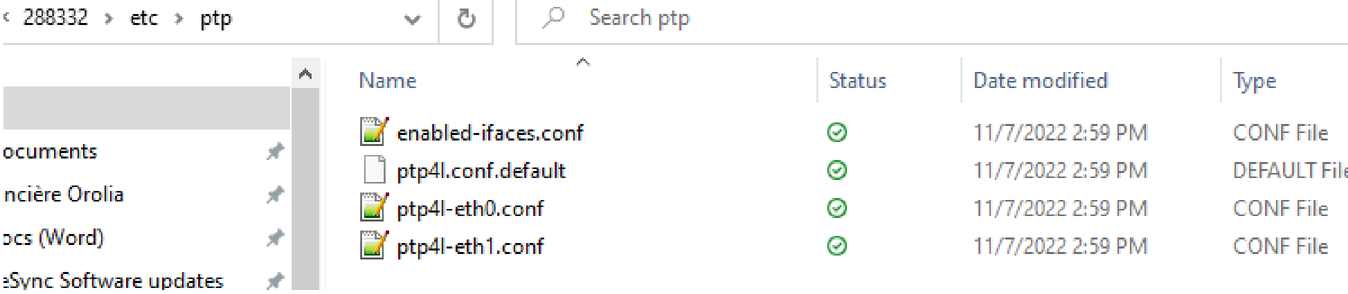
Changing profile will set default profile parameters

Multicast TTL 1

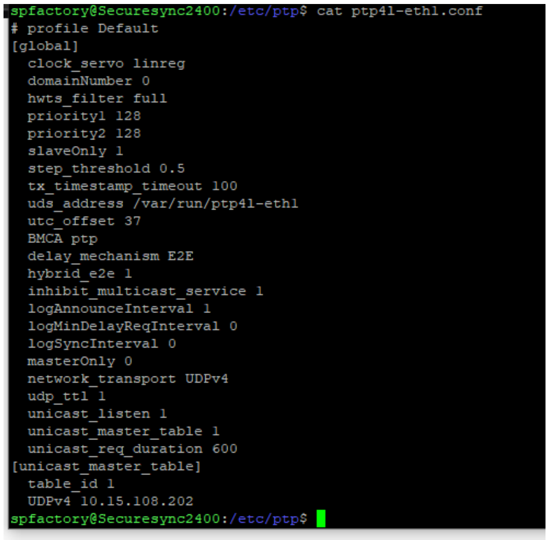
**Storage/Description of PTP configuration settings (ptp4L in versions 1.4.1 and above)

- PTP configs for eth0/eth1 of the base unit are stored in the **/etc/ptp** directory

- There are two separate config files for eth0 and eth1 (***ptp4p-eth0.conf*** and ***ptp4p-eth1.conf)***



Name	Status	Date modified	Type
enabled-ifaces.conf	✓	11/7/2022 2:59 PM	CONF File
ptp4l.conf.default	✓	11/7/2022 2:59 PM	DEFAULT File
ptp4l-eth0.conf	✓	11/7/2022 2:59 PM	CONF File
ptp4l-eth1.conf	✓	11/7/2022 2:59 PM	CONF File



```
spfactory@Securesync2400:/etc/ptp$ cat ptp4l-eth1.conf
# profile Default
[global]
  clock_servo linreg
  domainNumber 0
  hwts_filter full
  priority1 128
  priority2 128
  slaveOnly 1
  step_threshold 0.5
  tx_timestamp_timeout 100
  uds_address /var/run/ptp4l-eth1
  utc_offset 37
  BMCA ptp
  delay_mechanism E2E
  hybrid_e2e 1
  inhibit_multicast_service 1
  logAnnounceInterval 1
  logMinDelayReqInterval 0
  logSyncInterval 0
  masterOnly 0
  network_transport UDPv4
  udp_ttl 1
  unicast_listen 1
  unicast_master_table 1
  unicast_req_duration 600
[unicast_master_table]
  table_id 1
  UDPv4 10.15.108.202
spfactory@Securesync2400:/etc/ptp$
```

Good description of each PTP4l configuration value:

Refer to https://manpages.ubuntu.com/manpages/impish/man8/ptp4l.8.html

PTP Master versus PTP Slave modes / Multicast vs Unicast vs Hybrid (Troubleshooting PTP input)

A) PTP Master mode

B) PTP Slave mode

Diagnostics/troubleshooting for 2400 PTP Slave mode

1. 2400 Slave not syncing to a PTP Master

A) PTP reference periodically/continuously being declared not valid, even though all PTP packets are being exchanged

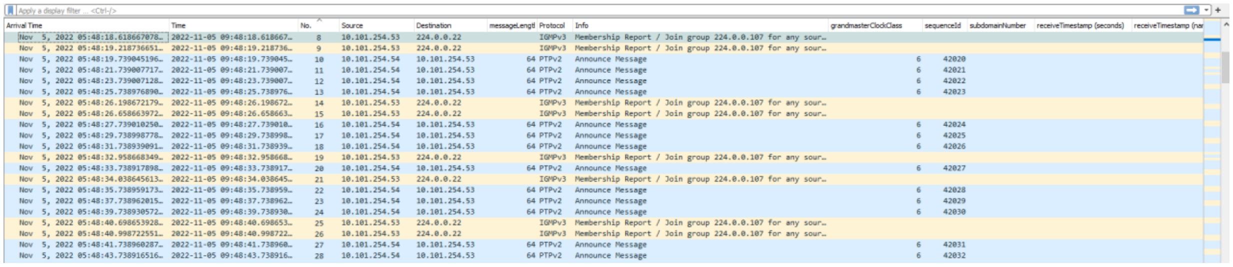
- Can verify PTP packets received/transmitted via the Statistics Panel.
- Versions 1.4.1 and 1.4.3 can disqualify PTP reference due to a quality check of Mean Path Delay. 1.6.0 update (~Nov 2022) adding ability to change qualification threshold.
- Refer to Salesforce Case 286924 / JIRA tickets DMND-1838 and DMND-1793

B) PTP Master and Slave operating in Uncast or Hybrid Mode. Slave not syncing at all.

- Make sure configured Unicast Master is fully reachable/routable on the network from the SecureSync (perform a CLI **traceroute** command from SecureSync to the PTP Master to make sure Master is reachable.

  If the Unicast/hybrid Master is not reachable, Signalling TLV messages for Unicast cant be sent/exchanged.

- Refer to Salesforce cases such as `288332.` This was a customer with a SecureSync on a VLAN, and the Unicast Master couldn't be found. Resulted in the 2400 Slave sending out no Signalling TLV messages, and instead sending "IGMPv3 Membership Report Joing Group" requests. ARPs and other Multicast packets to try and find the PTP Master on the network. Duplicated this here by entering an invalid address for the unicast Master:



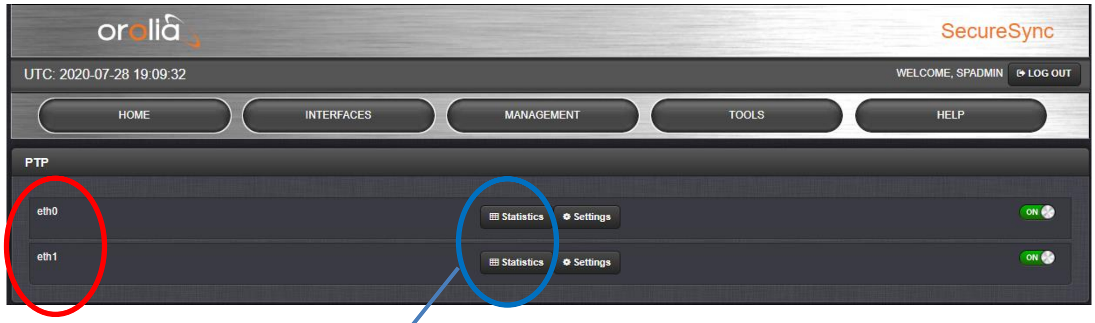
Arrival Time	Time	No.	Source	Destination	messageLengtl	Protocol	Info	grandmasterClockClass	sequenceId	subdomainNumber	receiveTimestamp (seconds)	receiveTimestamp (nar
Nov 5, 2022 05:48:18.618667078…	2022-11-05 09:48:18.618667…	8	10.101.254.53	224.0.0.22		IGMPv3	Membership Report / Join group 224.0.0.107 for any sour…					
Nov 5, 2022 05:48:19.218736651…	2022-11-05 09:48:19.218736…	9	10.101.254.53	224.0.0.22		IGMPv3	Membership Report / Join group 224.0.0.107 for any sour…					
Nov 5, 2022 05:48:19.739045196…	2022-11-05 09:48:19.739045…	10	10.101.254.54	10.101.254.53	64	PTPv2	Announce Message	6	42020			
Nov 5, 2022 05:48:21.739007717…	2022-11-05 09:48:21.739007…	11	10.101.254.54	10.101.254.53	64	PTPv2	Announce Message	6	42021			
Nov 5, 2022 05:48:23.739007128…	2022-11-05 09:48:23.739007…	12	10.101.254.54	10.101.254.53	64	PTPv2	Announce Message	6	42022			
Nov 5, 2022 05:48:25.738976890…	2022-11-05 09:48:25.738976…	13	10.101.254.54	10.101.254.53	64	PTPv2	Announce Message	6	42023			
Nov 5, 2022 05:48:26.198672179…	2022-11-05 09:48:26.198672…	14	10.101.254.53	224.0.0.22		IGMPv3	Membership Report / Join group 224.0.0.107 for any sour…					
Nov 5, 2022 05:48:26.658663972…	2022-11-05 09:48:26.658663…	15	10.101.254.53	224.0.0.22		IGMPv3	Membership Report / Join group 224.0.0.107 for any sour…					
Nov 5, 2022 05:48:27.739010250…	2022-11-05 09:48:27.739010…	16	10.101.254.54	10.101.254.53	64	PTPv2	Announce Message	6	42024			
Nov 5, 2022 05:48:29.738998778…	2022-11-05 09:48:29.738998…	17	10.101.254.54	10.101.254.53	64	PTPv2	Announce Message	6	42025			
Nov 5, 2022 05:48:31.738939091…	2022-11-05 09:48:31.738939…	18	10.101.254.54	10.101.254.53	64	PTPv2	Announce Message	6	42026			
Nov 5, 2022 05:48:32.958668349…	2022-11-05 09:48:32.958668…	19	10.101.254.53	224.0.0.22		IGMPv3	Membership Report / Join group 224.0.0.107 for any sour…					
Nov 5, 2022 05:48:33.738917898…	2022-11-05 09:48:33.738917…	20	10.101.254.54	10.101.254.53	64	PTPv2	Announce Message	6	42027			
Nov 5, 2022 05:48:34.038645613…	2022-11-05 09:48:34.038645…	21	10.101.254.53	224.0.0.22		IGMPv3	Membership Report / Join group 224.0.0.107 for any sour…					
Nov 5, 2022 05:48:35.738959173…	2022-11-05 09:48:35.738959…	22	10.101.254.54	10.101.254.53	64	PTPv2	Announce Message	6	42028			
Nov 5, 2022 05:48:37.738962015…	2022-11-05 09:48:37.738962…	23	10.101.254.54	10.101.254.53	64	PTPv2	Announce Message	6	42029			
Nov 5, 2022 05:48:39.738930572…	2022-11-05 09:48:39.738930…	24	10.101.254.54	10.101.254.53	64	PTPv2	Announce Message	6	42030			
Nov 5, 2022 05:48:40.698653928…	2022-11-05 09:48:40.698653…	25	10.101.254.53	224.0.0.22		IGMPv3	Membership Report / Join group 224.0.0.107 for any sour…					
Nov 5, 2022 05:48:40.998722551…	2022-11-05 09:48:40.998722…	26	10.101.254.53	224.0.0.22		IGMPv3	Membership Report / Join group 224.0.0.107 for any sour…					
Nov 5, 2022 05:48:41.738960287…	2022-11-05 09:48:41.738960…	27	10.101.254.54	10.101.254.53	64	PTPv2	Announce Message	6	42031			
Nov 5, 2022 05:48:43.738916516…	2022-11-05 09:48:43.738916…	28	10.101.254.54	10.101.254.53	64	PTPv2	Announce Message	6	42032			

~~~~~~~~~~~~~~~

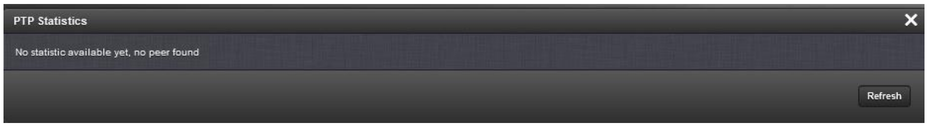
2. PTP Statistics Panel (versions 1.4.1 and above only?)

- Refer to "**The PTP Statistics Panel" in** 2400 SecureSync online user guide at: https://orolia.com/manuals/2400/Content/VS/Topics/INTRO/VS_PTP.htm
- This panel provides statistics for each Ethernet interface (0 and 1). If the PTP is set to OFF for a specific port, this screen will not display any information.
- All statistics shown are based on the traffic that is detectable by SecureSync, i.e. in a Unicast environment, SecureSync may only detect traffic that is addressed to it, based on switch configuration.

Management -> ***PTP Setup*** page



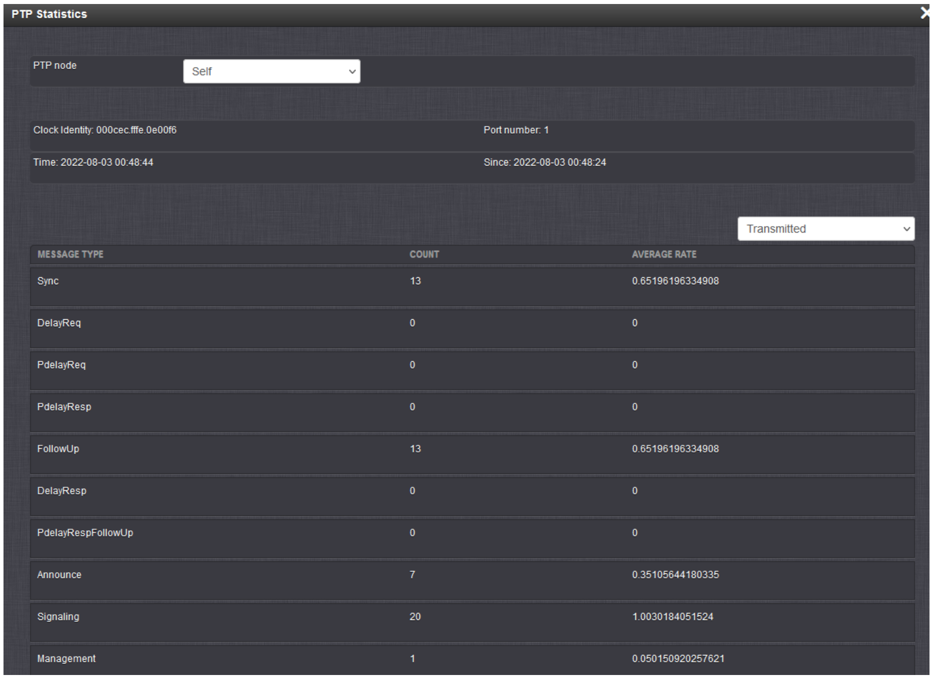
Statistics button



No statistic available yet, no peer found

OR

A) Outgoing PTP packets ("Transmitted" Selected)



PTP node: Self

Clock Identity: 000cec.fffe.0e00f6

Port number: 1

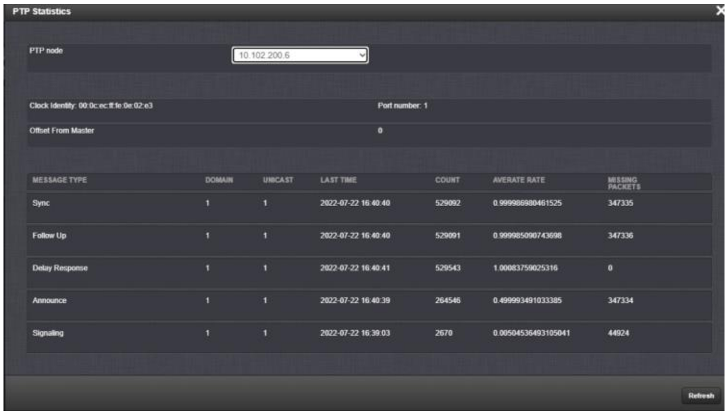
Time: 2022-08-03 00:48:44

Since: 2022-08-03 00:48:24

Transmitted

MESSAGE TYPE	COUNT	AVERAGE RATE
Sync	13	0.65196196334908
DelayReq	0	0
PdelayReq	0	0
PdelayResp	0	0
FollowUp	13	0.65196196334908
DelayResp	0	0
PdelayRespFollowUp	0	0
Announce	7	0.35105644180335
Signaling	20	1.0030184051524
Management	1	0.050150920257621
~~~~~~~~~~~~~~~

B) Incoming PTP packets (“Received” Selected)



PTP Statistics

PTP node: 10.102.200.6

Clock Identity: 00:0c:ec:ff:fe:0e:02:e3 Port number: 1

Offset From Master 0

MESSAGE TYPE	DOMAIN	UNICAST	LAST TIME	COUNT	AVERATE RATE	MISSING PACKETS
Sync	1	1	2022-07-22 16:40:40	529092	0.999986980461525	347335
Follow Up	1	1	2022-07-22 16:40:40	529091	0.999985090743698	347336
Delay Response	1	1	2022-07-22 16:40:41	529543	1.00083759025316	0
Announce	1	1	2022-07-22 16:40:39	264546	0.499993491033385	347334
Signaling	1	1	2022-07-22 16:39:03	2670	0.00504536493105041	44924

- **PTP Node:** IP address of PTP node.
- **Clock Identity**: [e.g., "a0:36:9f:ff:fe:37:b9:5d"]
- **Offset from Master:**
- **Domain**: Domain number of the selected PTP node.
- **Unicast**: [0,1] OFF or ON (1)
- **Last Time**: [e.g., "2016-08-12 18:19:15"] The last time a packet was received.
- **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: (*example:* *refer to Salesforce Case* ***286924***)

PTP interfaces showing "time invalid" error (after configuring PTP)

- Refer to Salesforce case 288112
- This message is displayed in the ***Interfaces*** -> References PTP page of the browser when PTP packets aren’t available (such as PTP for both eth0 and eth1 is configured for PTP Master mode).

IRIG input

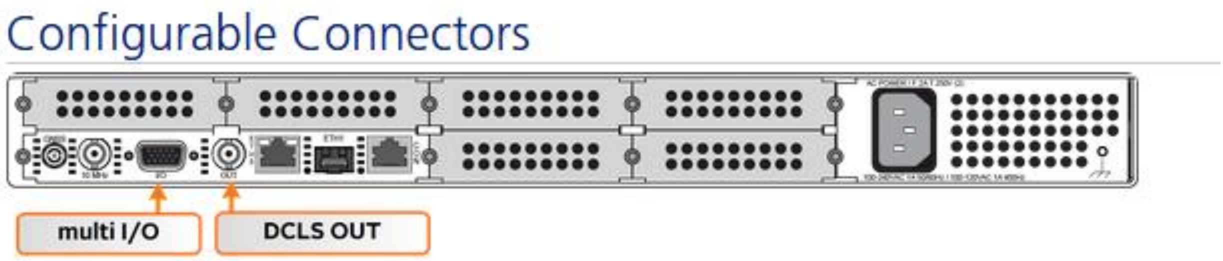
- Does not Require IRIG Input/Output Option card be installed in the SecureSync (but IRIG Cards can be optionally installed)
  - IRIG DCLS input is available via Multi I/O connector on rear panel

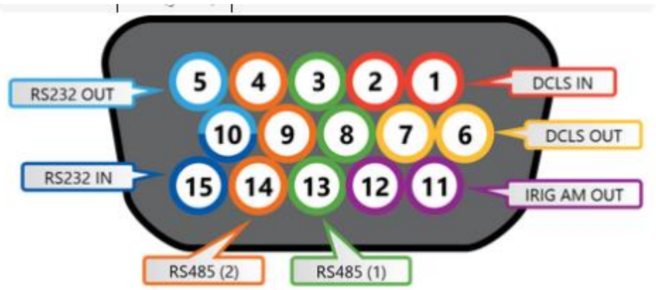
A) IRIG input via IRIG Input Option Cards

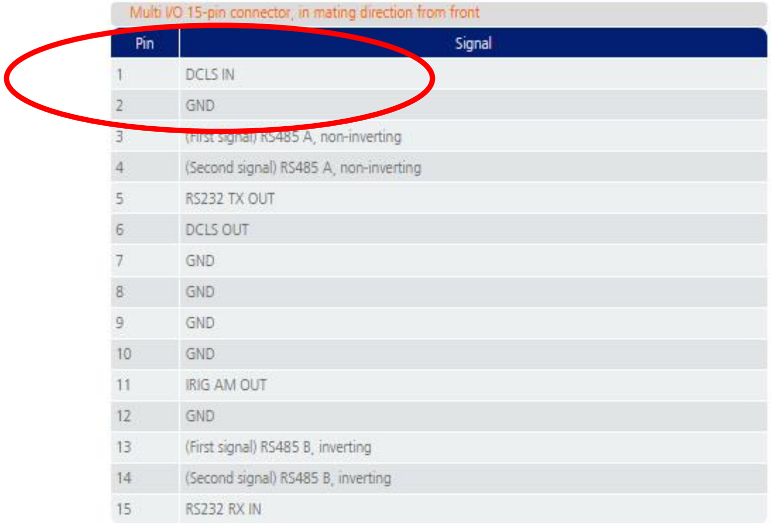
- Refer to SecureSync Option Card information document for more information I:\Customer Service\1- Cust Assist documents\SecureSync Option Card information.pdf

B) IRIG DCLS input via rear panel Multi I/O connector (DB15)

- Refer to online 2400 SecureSync user guide at: http://manuals.spectracom.com/2400/Content/NC_and_SS/2400/INSTALL/Conf_15pin_BNC.htm







Multi I/O 15-pin connector, in mating direction from front

Pin	Signal
1	DCLS IN
2	GND
3	(First signal) RS485 A, non-inverting
4	(Second signal) RS485 A, non-inverting
5	RS232 TX OUT
6	DCLS OUT
7	GND
8	GND
9	GND
10	GND
11	IRIG AM OUT
12	GND
13	(First signal) RS485 B, inverting
14	(Second signal) RS485 B, inverting
15	RS232 RX IN

**Time Synchronization for Secure Networks using fiber

- Refer to: http://www.spectracomcorp.com/Desktopmodules/Bring2Mind/DMX/Download.aspx?EntryId=1606&PortalId=0

Using a DAGR as an input reference to Sync SecureSync

1) For more information on using a DAGR with Model 1200 or 2400 series SecureSyncs, refer to the "DAGFR" section of the SecureSync Option Card information document for more information I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Option Cards\SecureSync Option Card information.pdf

HaveQuick/Stanag input

- Requires Havequick/Stanag Input/Output Option card be installed in the SecureSync
- For more information on Stanag/Havequick, refer to the SecureSync Option Card information document for more information I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Option Cards\SecureSync Option Card information.pdf

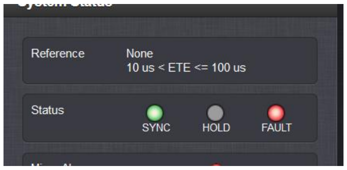
ASCII Input

- Requires ASCII RS-232 (1204-02) or RS-485 (1204-04) Input/Output Option card be installed in the SecureSync
- For more information, refer to the 1204-02 or 1204-04 sections of Option Card information document I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Option Cards\SecureSync Option Card information.pdf

Manually setting the System Time (User/User "self" mode)

- The "User" reference can be combined with another reference, if desired (such as user/External PPS for instance). But manual intervention is still required to make it a valid reference. For no manual intervention need to use the "Local System" reference instead of "User" reference.

Minor software issue with reporting of selected reference when User/User ref is selected (browser reports "None" instead of "User" selected)



Reference None
10 us < ETE <= 100 us

- Observed in at least v1.4.3 and below
- Refer to Salesforce Case 281257 and JIRA ticket DMND-1771

NOTE: **USER/USER** mode MUST be enabled in the ***Management*** -> ***Reference Priority*** table to be able to manually change the date/time via the web browser, CLI interface (such as dateset or doyset) or front panel. If USER/USER is not enabled, the time/date will not be changed.

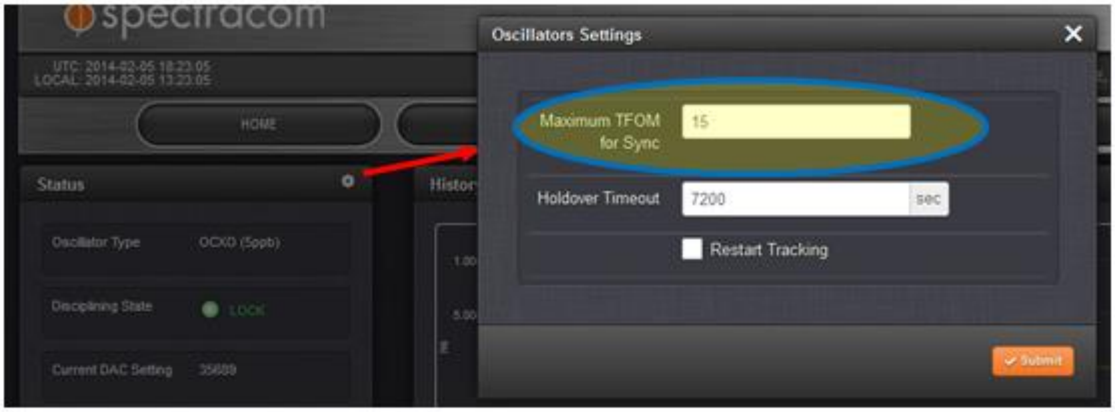
(Host mode): “One time use only” input reference to allow a user to set the time. If unit power cycles or if it selects a higher priority input and then loses all higher priority inputs, the time has to be manually set by the user in order for this reference to be valid again.

“Per Dave Sohn (14 JAN 15) “USER” can be combined with other input references (such as GNSS 0 /USER or USER /GNSS 0 as two examples). This is similar to “Local System” reference, but USER requires manual input for validity.

Note: (applicable to TCXO/OCXO with versions 5.3.0 and below installed, and RB oscillators) While in Host mode (time manually set and no higher 1PPS inputs with a higher priority), there is no external reference to use for monitoring the oscillator frequency. Therefore, the Freq Error (Frequency Error alarm) will remain asserted, and the Fault LED will remain solid red. It can only be cleared by applying an external 1PPS reference (it remains asserted until an external 1PPS input reference becomes available).

- TFOM with User set time will be 15. If MaxTFOM is set to less than 15, User/User mode will not allow SecureSync to go into Sync.

- Configured in the ***Management*** -> ***Disciplining*** page and then clicking on the “gear” next to “Status”
- Make sure Max TFOM is set to 15



UTC: 2014-02-05 18:23:05
LOCAL: 2014-02-05 13:23:05

Oscillator Type OCXO (5ppb)
Disciplining State ● LOCK
Current DAC Setting 35689

Maximum TFOM for Sync 15
Holdover Timeout 7200 sec
□ Restart Tracking

Note: If Max TFOM is lower than 15, User/User will be “OK” but Sync Status will not go to “OK”

1. Hit Submit on Setup -> Time Management page.
2. Synchronization should go to “OK”
3. TFOM value will remain at 15 (reported on Status -> Time and Frequency page).
4. The Oscillator is not disciplined with NTP input (oscillator remains in free-run mode).

Linux Kernel time

- Refer to Mantis case 0001704 for more info.
- The battery-backed Real Time Clock (RTC) is read upon each boot-up in order to set the Linux kernel time.
- The kernel time then sets the KTS time.

- The kernel time is adjusted by NTP during synchronization to other references.
- Fcron (scheduler program) runs every 10 minutes to write the linux time to the RTC.
- Upon a Reboot or halt being performed, the kernel time is set into the RTC.

Holdover Mode while in User mode

- DAC value (reported in discstats) should remain constant when in user set time

After sync has occurred when using the User mode, the time server does not go into Holdover mode thereafter. It remains in full sync mode. So the Holdover timeout value doesn't apply to this mode. The Holdover timeout only applies if a higher priority reference becomes valid sometime after the User reference has gone valid, and then the higher priority reference(s) is lost. The unit will then go into Holdover mode.

System PPS while in User mode

- System PPS starts at the arbitrary spot it's at when the time is hand-set by a user (it can be off by +/- 500ms)
- With the oscillator being in free-run, System PPS will then start to drift.
- If an higher priority external reference then becomes present/valid, the System PPS will jump to the reference (not slew like it normally does when switching references that aren't aligned with each other)
  - Because the other device(s) already synced when the time was first hand-set, devices syncing to the SecureSync will see a large shift in their input reference from the SecureSync. This may adversely affect their operation, resulting in logs/alarms being asserted (with Spectracom devices, such as the Frequency Error alarm for instance).

Email Keith sent to Sylvain (5 Feb 2013): You can certainly manually sync the SecureSync to itself, allowing the NTP stratum to go to Stratum 1. This is known as the "Self" input reference. Once the Self/Self reference has been enabled in the **Setup**-> **Reference Priority** page of the browser (it is disabled by factory default), a user is then allowed to manually set the System Time and Date, as desired (as configured in the **Setup** -> **Time Management** page of the browser.

Once the time has been manually set, SecureSync will go into Sync and NTP will go to Stratum 1 within just a couple of minutes thereafter. As long as the SecureSync isn't power cycled, and as long as no higher priority references become present/valid, SecureSync will remain synced to itself, allowing NTP to continue to report it's at Stratum1.

To alleviate the need for a user to manually set the time after each boot-up, the "Battery Backed Time on Start-up "feature can be enabled (in the **Setup** -> **Reference Priority** page of the browser. With this checkbox selected, SecureSync will automatically go back to Stratum 1 shortly after each boot-up (no user interaction is required). The time/date that is used for synchronization is the time from the Real Time Clock, which "maintains" an approximation of the correct time/date while the system is powered-down.

The ability to manually set the time/date of the SecureSync ("Self" mode) and the "Battery Backed Time at Start-up" feature is discussed in the "Reference Priority Use Case Examples" in the SecureSync manual. Refer to "Example 4", starting on page 3-53 of this manual.

Email from Keith to a customer (26 Apr 2013) If it's desired to manually set the time of the SecureSync, instead of syncing it to an external time reference such as GPS, this can be performed via the Setup -> Time Management page of the web browser. It can also be performed using a telnet/ssh session or by using the front panel keypad/LCD window ("Clock" menu).

Notes about manually setting the time:

1) The “State” field User/User entry (row) of the Reference Priority table needs to be enabled (by default, its set to disabled). This table is configured in the **Setup** -> **Reference Priority** page of the browser (this table can also be configured using SNMP Sets).

2) If there are any higher priority input references that are present and valid, they will override and correct the user set time/date. Any other reference that may be present can be disabled in the Reference Priority table, if desired to keep it from overriding the manually set time/date. This configuration change alleviates the need to have to physically disconnect an input from the NTP server.

3) Unless the “**Synchronize to Battery Backed Time**” checkbox underneath the Reference Priority page of the browser is selected, the time needs to be manually set after each boot-up, in order for the SecureSync to go back into sync. When this box is selected, the SecureSync will go back into sync automatically after each power-up, without requiring a user to have to manually set the time to achieve sync status again.

Manually setting the System time backwards into the past

- When System Time is advanced into the future, RTC is updated every 10 minutes.
- When System Time is set back into the past, RTC isn’t updated the first time for about 3 to 4 hours. Then its updated every 10 minutes again.

The system is not intended to be a simulator. It especially does not like being set backwards to an earlier time. This causes Cron to completely stop running, until time has caught up to the correct time.

If the time is set backwards and then power cycled without a several minute delay, it will not power-up with the time that it was manually set to. It takes several minutes for NTP to change the kernel time, once it’s been manually set. Then cron, which is used to periodically set the RTC stops running until time catches up to the kernel time. If the time is set backwards, a delay of several minutes (like 20 to 30 minutes) should occur between setting the time and power cycling the unit.

Email Keith sent to Masataka (18 Feb 15) Thanks for your email. Our Applications Engineering team has reviewed the information you provided us with regards to the SecureSync’s RTC being saved. I am happy to pass along to you their findings.

To begin, when manually setting the time of the SecureSync, there is a one particular scenario that will allow the RTC to be automatically saved within 10 minutes of setting the time. There is another scenario which prevents the System Time from being able to be automatically saved to the RTC for a few hours, unless a reboot or halt of the SecureSync is commanded.

If the System Time/date is manually set by a user to a time/date ahead of the current System Time, the SecureSync continues to be able to automatically set the time into the RTC every 10 minutes (on a 10 minute schedule). However, if a user manually sets the date/time to an earlier date/time than the System Time was set to, the System Time can’t be automatically set into the RTC for about 3 to 4 hours, unless a *reboot* or *halt* command is performmed.

If the date/time is set by a user to a date/time in the past and its desired to save this “new” date/time into the RTC without waiting the 3 to 4 hours for it to be automatically saved, the SecureSync should be commanded to be either rebooted or halted (not just power cycled) after setting the date/time backwards. Note the RTC is not updated upon a power cycle of the SecureSync. However, the RTC is updated with the System Time upon either a reboot or a halt command being issued. The SecureSync can be either rebooted or halted via the front panel menus, the web browser, the CLI command line interface or via SNMP.

Please be aware that the RTC taking a few hours to be set when a user sets the date/time into the past is not a software bug and Spectracom has no intentions at this time of changing how this operates. If it’s desired to manually set the time of the SecureSync backwards to a previous date/time for some reason, the SecureSync should be either rebooted or halted (via its user interfaces) in order to alleviate the need to wait the 3 to 4 hours that is needed for the RTC to be updated with this earlier System Time. Note that the RTC is updated with each reboot or halt command, whether the date/time was set forward or backwards from the starting

System Time.   The reboot/halt command alleviates any need to wait for the RTC to be updated, as the RTC update occurs before the SecureSync is brought down with either command being performed.

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

Configuration

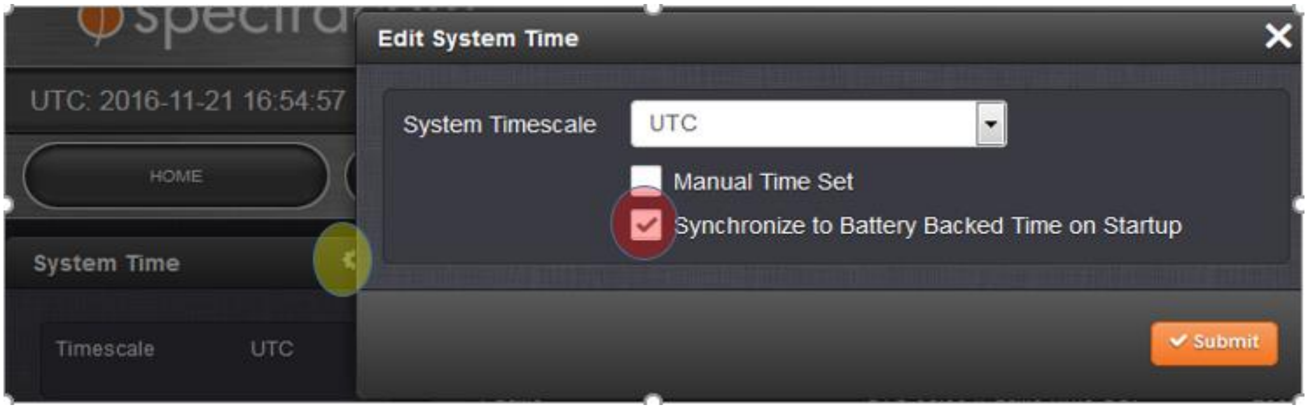
- The button selection is stored in the “rmsf.conf” file (/config directory)

rmsf.conf	Enable battery-backed time button	**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)



UTC: 2016-11-21 16:54:57

System Time

Timescale UTC

Edit System Time

System Timescale: UTC

□ Manual Time Set

☑ Synchronize to Battery Backed Time on Startup

A log entry is created in the System log that the unit synced to itself and is not traceable.

Important Notes:

1) The Input reference priority table needs to have an enabled row that has “User” defined as a “Time” reference, in order to use this capability.

2) If a higher priority reference becomes available anytime after initial time sync has occurred (such as GPS, for instance), the input reference will may cause a time jump to occur while SecureSync is already in sync (if the RTC is not correct when it boots-up). The amount of time change will be dependent on how long the unit was powered down for and if it was in sync, before it was last powered down.

Q. What would the daily drift rate be with an undisciplined OCXO?

A. (from Dave Sohn on 11/29/11): The daily frequency aging of the standard OCXO is 5.00E-10. The daily frequency aging of the high-performance OCXO is 2.00E-10.

The daily drift will be a combination of the initial frequency error, which is unknown for an undisciplined system, and the increasing effects of the frequency aging. The actual offset will also include the initial phase offset of the 1PPS, which is also unknown for an undisciplined system.

Local System reference (Self Reference)

- Local System is the “Self” reference as referred to in the Tsync boards
- Local System can be used as EITHER the Time OR the PPS reference, but NEVER as both references.
  - **Local System/Local System**: Not a valid combination. Local System has to be combined with a different time reference or 1PPS reference in order to be a valid (internal) reference.

TSync-PCIe can be "synced" to more than one reference at a time, with only the highest priority input selected at any given moment. Theoretically, if the highest priority input goes away or becomes not valid, SecureSync will seamlessly transition to the next highest priority without going into Holdover alarm (an entry is created indicating SecureSync switched references). However, Engineering has seen it glitch when switching from one input to another, where the Holdover alarm is generated for one second, and then it's back in sync by the next second. You can let the customer know that the switchover from one reference to another will take no more than one second, as long as more than one valid input is present.

NTP operation while in User/User mode

Note: Per Ron Dries, NTPMOND “wakes-up” every 16 seconds to check if NTP is running. It will restart NTP as necessary and then go back to sleep. Depending on when NTP dies in relation to ntpmond going to sleep, it can take up to 16 seconds for NTP to be restarted by ntpmond. Then it will take a couple of minutes for NTP to resyncs and be useable again.

- Manually changing the System Time by 1 second or greater will cause NTPMOND to automatically stop and restart NTP to account for the time change of the NTP input
- NTPMOND stopping and restarting NTP is logged in the system.log (not the ntp.log)

```
[system] ntp monitor stopping ntpd, found 3590 second difference (NTPMOND)
```

followed by:

```
[system] ntp monitor restarting ntpd (NTPMOND)
```

NTP.log entries also asserted:

```
ntpd [xxxx] ntpd exiting on signal 15
   followed by
ntpd [xxxx] “127.127.1.0 interface 127.0.0.1 -> (none)
```

Issue with NTPMOND trying to stop NTP when error >1 second

Version 5.3.0 update (~Sept 2015) fixed issue caused by NTP monitor Daemon NTPMOND, trying to stop NTP when the Timing System and Linux kernel time differ by more than 1 sec

NTP step threshold (NTP’s Reference time change limits)/ ntpmond restarting NTPD

- Refer to http://doc.ntp.org/4.1.2/debug.htm
- Default step threshold is **128 milliseconds or less**
- Default stepout threshold (how long the error has to exceed the step threshold before NTP steps - after NTP is already running) is 900 seconds.
- The step threshold can be changed by the tinker step command (refer to “tinker” at http://doc.ntp.org/4.1.2/miscopt.htm)

NTP Step threshold (128 milliseconds)

A) Initial NTP startup

- If the initial time error is greater than 128ms - NTP is allowed to step (correct) the time right away.

B) After NTP is already running

- If a time error is greater than 128ms, normally NTP would have to wait 900 seconds (15 minutes) with this large of an error before NTP steps (due to the default stepout threshold).
- But our NTPmond daemon checks NTP every 16 seconds and restarts NTP if the error is greater than 1 second. So NTP can step the error much sooner than usual (it doesn't have to wait 900 seconds before correcting the time).

NTPmond restarting NTP if time offset greater than 1 second

- NTPMOND "wakes-up" and check NTP every 16 seconds to check if NTP is running and if it's within 1 second of the System Time (while synced to System Time).
- NTPMOND will restart NTP if NTP is in sync and the time error from KTS is 1 second or greater, or if NTP exceeded sanity limit of 1000 seconds (16min 40 sec) which can cause it to stop running

Note: Per Ron Dries, NTPMOND "wakes-up" every 16 seconds to check if NTP is running. It will restart NTP as necessary and then go back to sleep. Depending on when NTP dies in relation to ntpmond going to sleep, it can take up to 16 seconds for NTP to be restarted by ntpmond. Then it will take a couple of minutes for NTP to resyncs and be useable again.

NTP also has its own Reference time change limits, as well (NTP step threshold of 128ms)

- If NTP's selected input changes by **128 milliseconds or less** NTP **slews** to the reference. (maximum rate of 500 microseconds per second-which is about 4 minutes to slew 128ms)

  Fastest time to slew
  500us = 1 second
  1ms = 2 seconds
  64ms = 128 seconds (2.1 minutes)
  28ms = 256 seconds (4.2 minutes)

- If NTP's selected input changes by **more than 128 millisecond,** NTP **steps** to the reference.

Use the ntpq -p CLI command to report the current time offset between NTP and the System Time (KTS)

- Perform an ntpq -p (or ntpq -pn) in CLI and look at the Offset value of "PCI_TSYNC(0)" (or "10.2.100.45.0")
- The initial time offset will vary after every reboot/power cycle (can be up to 1 second off).
- The offset can be less than or greater than 128ms after each boot-up.
- If the "offset" of "tsyncpci(0)" is less than 128ms, it can take NTP a few minutes to slew to the correct time (fastest possible slew rate is 500 microseconds per second- about 4 minutes to slew 128ms).

STL *(Satelles) “Resilient PNT” input Option Card (Option Card 1204-3D)

- For all details, refer to SecureSync Option Card Model 1204-3D in the SecureSync Option Card info document: ..\SecureSync Option Card information.pdf
- For general info on STL, refer also to STL tech note: I:\Customer Service\1- Cust Assist documents\Satelles resilient PNT.pdf
- STL info on our website: https://spectracom.com/resources/essential-education/what-is-stl

GPS antenna alarm asserted

- This alarm is only associated with the GPS receiver
- If GPS antenna is not also connected, mask this alarm in the Management -> Notifications pagee

Log info associated with STL (Timing log and Journal log)

- Refer to “1204-3D” in the SecureSync Option Card document: ..\SecureSync Option Card information.pdf

Summary of log info

- **Timing log** contains entries for burst info:

Example entries

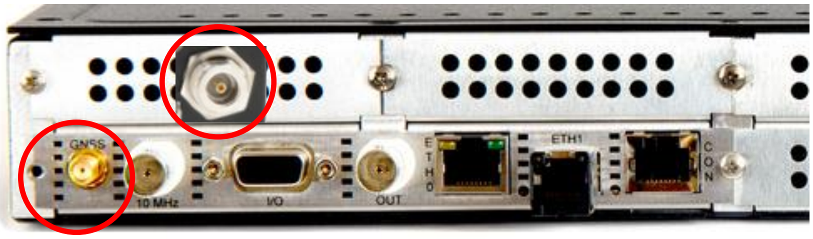
```
Oct  4 07:32:27 Spectracom Spectracom: [system] 2017 277 07:32:36 000 STL Status: Total Burst:1 Strong Burst:0

Dec  1 12:02:16 Spectracom Spectracom: [system] 2017 335 12:02:16 000 AR stl0 has lost communication.
Dec  1 12:02:24 Spectracom Spectracom: [system] 2017 335 12:02:24 000 AR stl0 has established communication.
```

- **Journal log** contains user config changes to the STL configs

Example entry

```
Nov 27 20:35:20 Spectracom Spectracom: [webui] Changed STL Configuration for ASCII Reference 0 in slot 3 from   STR
(0) Configuration:   Serial Number: EVK2-066   Latitude: 40.584330   Longitude: -74.243270   Altitude: 100.000000   EE
axis: 100.000000   NN axis: 100.000000   UU axis: 50.000000   Geolocation mode: 1   Sensitivity level: 40  to    STR (0)
Conf: EVK2-066 0.708330 -1.295790 100.000000 100.000000 100.000000 50.000000 1 40
```

GNSS (GPS) input



GNSS: SMA Connector on 2400s

SMA connector on rear panel / Type N to SMA cable / Strain relief

- Unlike 1200 SecureSyncs having N type connector, 2400s have a rear panel SMA connector

* **Desire for strain relief of the SMA pigtail**

- Refer to Salesforce Case **290183** and JIRA ticket **DMND-1926** (requesting consideration for us to offer a blank cover plate having a Type N connector in it.
- Having no Option Card installed above the GNSS SMA will alleviate the need for the cover plate.

GPS/GNSS receiver and antenna (such as Model 8230) is "receive-only" (it doesn't transmit)

- For documentation indicating the GPS/GNSS receiver is receive only, refer to:
  - "***GPS antennas are Receive-only***" in I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf
  - The "Model-specific" document: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\GPS-GNSS\GPS is receive-only

GPS/Glonass/QZSS SAASM GPS input reference- GPS Receiver operation /Mobile (Dynamic) mode operation/SAASM

Storage of receiver configurations, Backup/restore receiver configs

Home/spectracom/config directory

Config file name	Configurations for:	Notes
gpscf.conf	GPS Receiver	**Interfaces** -> **GNSS 0** page Rcvr mode, constellations, offset

Circular Error Probability (CEP) for SecureSyncs

(Note: this info is from 1200 SecureSyncs)

- Refer to SF case 124480

Description: CEP refers to the radius of a circle in which 50% of the values occur, i.e. if a CEP of 5 meters is quoted then 50% of horizontal point positions should be within 5 meters of the true position. The radius of the 95% is often quoted and the term R95 used. R95 is CEP with the radius of the 95% probability circle.

Email from Dave L (4 Jan 18) I did recognize the term CEP after reminding myself via Google.

Circular Error Probability (CEP)
CEP refers to the radius of a circle in which 50% of the values occur, i.e. if a CEP of 5
meters is quoted then 50% of horizontal point positions should be within 5 meters of the
true position

The Spectracom Securesync uses the uBlox M*T GNSS Receiver. From the receiver data sheet:

Horizontal Position Accuracy with GPS is 2.5m.
CEP, 50%, 24 hours static, -130dBm, > 6 SVs

https://www.u-blox.com/sites/default/files/NEO-LEA-M8T-FW3_DataSheet_%28UBX-15025193%29.pdf

Associated CLI commands for GPS

- Refer to (in the GPS info (“GR_” commands)

GPS reception issues/GPS Jamming

- For GPS reception issues, refer to the SecureSync or NetClock GPS reception tech note: I:\Customer Service\GPS\GPS reception Ap Notes
- For information/suggestions on eliminating GPS jamming, refer to Jamming” in the custserviceassistance doc

Time it takes for NTP to sync after power-up:

Refer to “Time after initial boot-up for NTP to sync as Stratum 1” (such as in a mobile environment)

GPS 1024 Week roll-over issue due to number of bits in the message (GPS Epoch every 20 years)

- For more info, refer to sites such as: http://www.colorado.edu/geography/gcraft/notes/gps/gpseow.htm

Note: the next 1024 week rollover occurs on **7 April, 2019**

- **On our website: https://spectracom.com/resources/blog/lisa-perdue/2017/gps-2019-week-rollover-what-you-need-know**

Email from Dave L (12 Feb 18) The Receiver Year Rollover will occur in April 2019. None of the receivers used in the SecureSync product are affected by the year 2019 GPS week rollover issue.

Here is some more information from our website:
https://spectracom.com/resources/blog/lisa-perdue/2017/gps-2019-week-rollover-what-you-need-know

Q I have been made aware of an issue with another manufacturer of GPS Clocks and although not one we use it prompts me to ask the same question to all our clock suppliers.

Apparently, there are several scenarios when a GPS clock can roll over due to “a limited number of bits in the satellite message". A roll over in a Gorky unit is believed to have failed the in the past and there will be a major roll over in 2019.

Could you confirm that a limited number of bits in the satellite message will not cause the Spectracom 9383 units we have in service to fail in any way?

A Email from Paul Myers (22 Jul 16) "This is an end of epoch issue a 20 year period of GPS weeks which rolls over in a counter which can't go beyond the number 1024."

Testing/certification of our GPS receivers for week rollover

GPS/GNSS Receiver Models

Determining which Model receiver is installed and its current firmware version

Note:2400 SecureSyncs started with ublox receivers (have never used Trimble Res-T/Res-SMT-GG or Res-360 receivers)

Email from Keith The Model of the GNSS receiver and its installed version is reported about half way down, in the **Tools** -> **Upgrade/Backup** page of the browser (under System Configuration), as shown below

Commercial GNSS receivers

A) Ublox M8T

Resurvey/Need to manually delete position in Stationary Mode in Res-SMT-GG and uBlox receivers (not applicable to Res-T receivers)

GNSS Receiver	Receiver firmware version	Resurvey requirements
uBlox M8T	All uBlox firmware versions	**All SecureSync versions** (unlike earlier software versions of 1200 SecureSyncs, 2400 SecureSync **software causes uBlox receiver to automatically re-survey upon each unit power-up.**
Trimble Res-SMT-GG	**N/A (never used in 2400 SecureSyncs)**	**N/A (never used in 2400 SecureSyncs)**
Trimble Res-T	**N/A (never used in 2400 SecureSyncs)**	**N/A (never used in 2400 SecureSyncs)**

uBlox log entries in Timing log

- Refer to the "ublox receiver" section in the custassist doc: I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf

SAASM GPS receivers (Rockwell Collins GB-Gram /Trimble Force-22)

Note: this info is from 1200 SecureSyncs

Available SAASM receivers:

A) Model 1204-1A (Rockwell Collins GB-Gram Model MPE-S receiver)

- Refer also to the SS Option Card document for more details: I:\Customer Service\1- Cust Assist documents\SecureSync Option Card information.pdf

Rockwell Collins P/N for the GB-Gram MPE-S receiver: 987-9705-X01

Min GPS signal level at input

Email from Paul Myers: "Dennis H at Rockwell Collins said he would recommend no more than 8dB loss between Antenna and MPE-S receiver."

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

- 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)

- **Important Note (per Paul Myers 28 Nov, 2017)** do not mention or discuss this issue,or the fix, with any customers without first talking with either Paul or Dave Sohn first!

B) Model 1204-07 (Trimble Force 22e recevier)

- Refer also to the SS Option Card document for more details: I:\Customer Service\1- Cust Assist documents\SecureSync Option Card information.pdf

Battery disconnect switch

- Like the Model 1204-1A Option Card, the 1204-07 also has a battery disconnect switch
- (~9 Dec 16) Per Dave West, apparently two SecureSyncs were recently shipped with a metal plate that does not have a hole in the metal to be able to access the shut-off switch.

GPSD (a GPS service daemon)

- Standard feature in 2400 SecureSyncs
- Refer to online **2400 SecureSync** user guide: http://manuals.spectracom.com/2400/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:

- Connect to the unit over a network via TCP at the specified port using any GPSD-compatable software
- Receive position and timing information from the GNSS receiver in a consistent format, and
- 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
  - **gpsd software update Fix (gpsd to v3.23) for 2400 SecureSyncs** expected to be in v1.3.0 (around end of October 2021)
  - **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
  - “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.”

2400 SecureSync/VersaSync/VersaPNT Requirements

1. I BELIEVE (not confirmed) Versa device MUST have commercially available uBlox receiver installed (not compatible with SAASM receiver)

   Refer to Salesforce Cases 185435/185456 (Feb 2019)

2. Installed VersaSync/VersaPNT software version needs to be **version 1.3.1 or above**

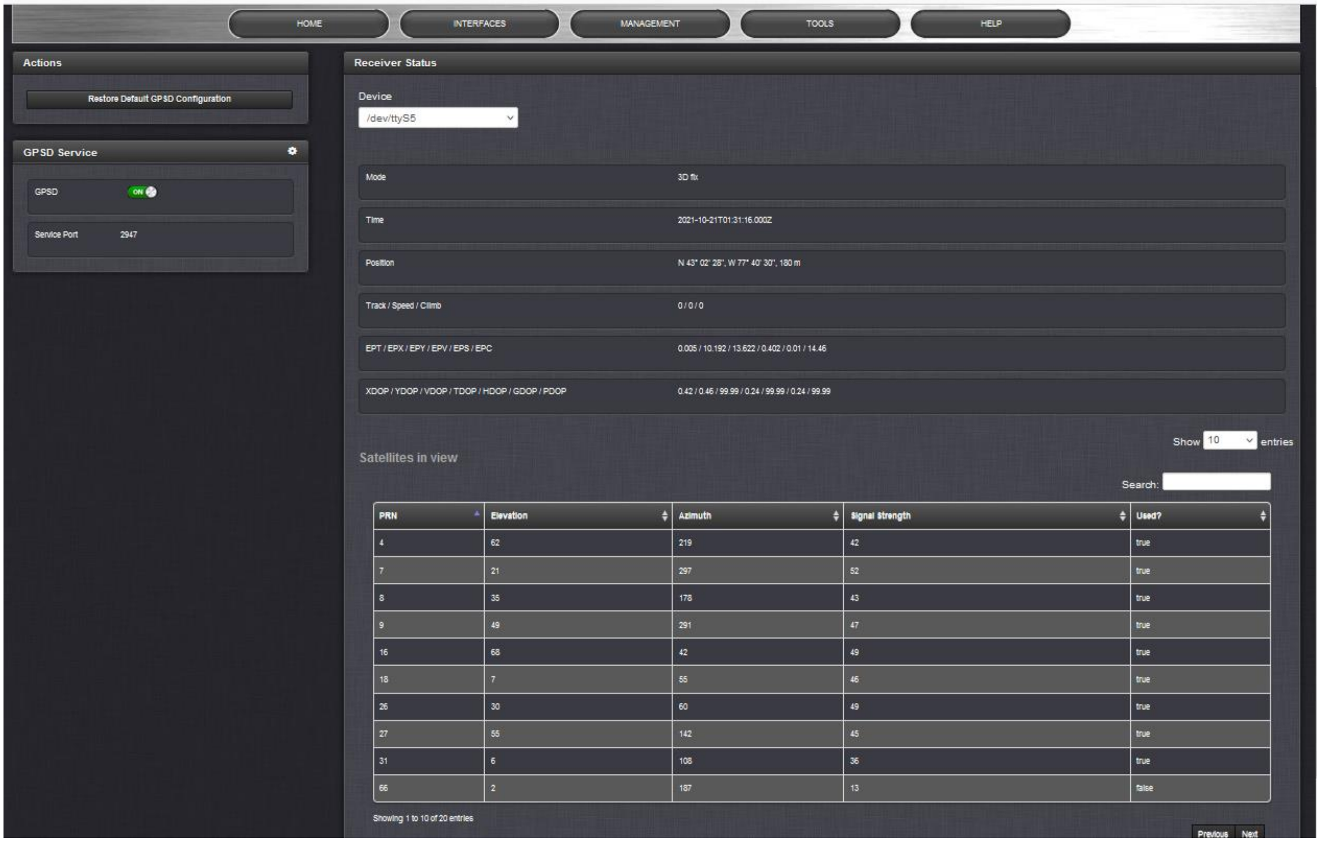
   Per the version 1.3.1 update Release Notes: *"Added GPSD support and GSPD configuration and display via VersaSync/VersaPNT CLI and WebUI. GPSD displays the status of the ublox receiver."*

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*** > > ***GPSD Setup*** to access the **GSPD Setup Screen**



Actions

GPSD Service

GPSD ON

Service Port 2947

Receiver Status

Device /dev/ttyS5

Mode	3D fix
Time	2021-10-21T01:31:16.000Z
Position	N 43° 02' 28", W 77° 40' 30", 180 m
Track / Speed / Climb	0 / 0 / 0
EPT / EPX / EPY / EPV / EPS / EPC	0.005 / 10.192 / 13.622 / 0.402 / 0.01 / 14.46
XDOP / YDOP / VDOP / TDOP / HDOP / GDOP / PDOP	0.42 / 0.46 / 99.99 / 0.24 / 99.99 / 0.24 / 99.99

Satellites in view

Show 10 entries

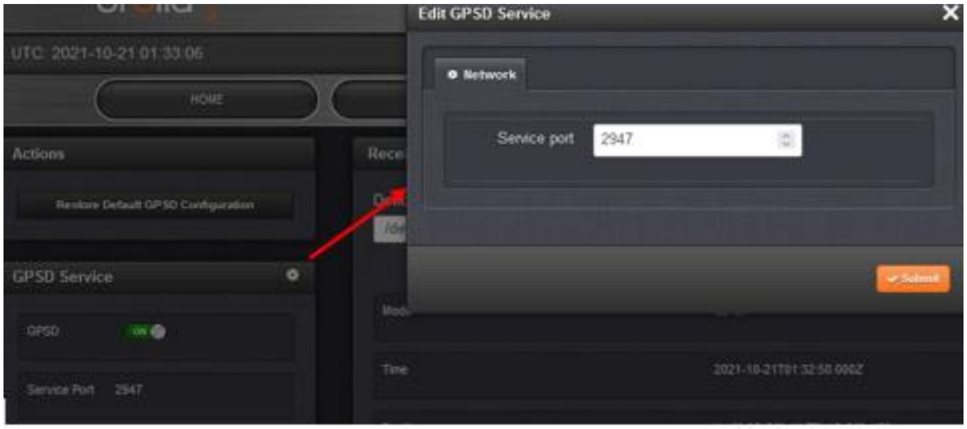
Search:

PRN	Elevation	Azimuth	Signal Strength	Used?
4	62	219	42	true
7	21	297	52	true
8	35	178	43	true
9	49	291	47	true
16	68	42	49	true
18	7	55	46	true
26	30	60	49	true
27	55	142	45	true
31	6	108	36	true
66	2	187	13	false

Showing 1 to 10 of 20 entries

The GPSD Setup Screen is divided into three panels:

3. **The GPSD Service panel:**
   - allows you to toggle the service ON or OFF
   - lists the Service Port (default is port 2947 but is user configurable)


UTC: 2021-10-21 01:33:06

Actions

Restore Default GPSD Configuration

GPSD Service

GPSD ON

Service Port 2947

Time 2021-10-21T01:32:50.000Z

Edit GPSD Service

Service port 2947

- 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 2400 SecureSync, this is where you can reset the service port.

4. The Actions panel

- provides an option to restore the default configuration.

5. The Receiver Status panel

- lists the information required by the GPSD service:
  - Device name
  - Mode, Time, Position, Track/Speed/Climb, Error Statistics, and Precision Statistics
  - 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 2400 SecureSync 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.

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

M-Code (M Code) receiver/capabilities

Note: this info is from 1200 SecureSyncs

Question from Keith: Hi Dave (Tony, Mike, Wade and Steve),
Just got a call from Jerome ? with NGC inquiring if SAASM SecureSyncs are currently M-Code compliant.

Wasn't really sure what we could say on this topic (such as for future plans). Told him not currently and gave him Tony's number for additional info on this topic. For tech support, what general type of info/future plans/timeframes, etc can we provide on this?

A Reply from Tony Diflorio (10 Jan 17) My story to our customers (and I am sticking to it☺) is that we have it in our roadmap to add M-Code capability to our SecureSync when the M-Code receivers are available to integrators such as Spectracom. At this time, M-Code production receivers are not available. David can correct me if I am wrong…

SBAS

- As of at least version 5.7.1 (Oct, 2017), SBAS is NOT supported in SecureSync/9400s
- I have not heard of any intentions for SBAS support to be added.

Obtaining/Loading SAASM keys

- Refer to "SecureSync SAASM manual addendum" (1200-0000-0053): U:\Engineering\SAASM-FOUO\CustomerService\SecureSync

  Note: Upload to customer using ARMDEC website: https://safe.amrdec.army.mil/safe/ (Select "**non CAC users**").

  An automatic email will be sent to you to verify the sender. The requested password to use for the verification will be included towards the bottom of this auto-email (example: "The Password is: Q$#2975!99?62J*2*3!J")

ICD-GPS-153c messages (Ground speed, heading)

- Per Paul Myers (23 jan 17) "Force 22E ICD-GPS-153C messages provide ground speed and heading values"
- ICD-GPS-153 is apparently documentation for the:
- Refer to (ICD-GPS): I:\Engineering\Specs and Standards\GPS
- Refer also to SecureSync Option Card doc: I:\Customer Service\1- Cust Assist documents\SecureSync Option Card information.pdf
- ASCII Output NMEA messages RMC, GGA, ZDA were designed for stationary applications because we don't populate all fields. The SecureSync otherwise is good for mobile applications.
- NRE needed to get needed values and transform/store and then add to ASCII Output message RMC
- Force 22E ICD-GPS-153C messages provide ground speed and heading values
- We would need to verify these values are correct and can be converted to values needed in RMCmessage which lacks them. And are in correct coordinate systems for RMC use.
- Message 5040 which we receive provides Ground speed
- Message 4 which we receive provides Attitude True Heading
- Check other GGA, RMC, ZDA for other issues.

Opt-SEM (Option SAASM Modulation) / Time Mark Data Message (ID 3)

Note: this info is from 1200 SecureSyncs

- See Paul Myers or Scott Hildebrandt for details
- Applicable to SAASM receiver units only.
- Was initially a special for a customer (3DLLR/ Raytheon C-Band Radar project)
- Per Paul Myers “OPT-SEM provides ICD-GPS-153C messaging on the 1204-02 ASCII Output for the Time Mark Data Message (ID 3). Allows the SecureSync to emulate the message coming directly from the installed SAASM receiver
- Verify with Scott Hildebrandt
- Provides data from the ICD-GPS-153 interface, specifically the Time Mark Data Message (ID 3).
    - Time Mark Data Message is apparently an on-time marker from a SAASM receiver.

Per Paul Myers (23 Jan 17) Opt-SEM was validated on the MPE-S Type II GB-GRAM, but should work for Force 22E.

u-blox Model M8T receivers

Note: this info is from 1200 SecureSyncs

- This is a 72 channel GNSS receiver
- Refer to additional info on the M8T receiver in ..\CustomerServiceAssistance.pdf (search it for “M8T”)

GPS-only is still the standard configuration.

“SS-Opt-GNS” (https://na28.salesforce.com/01tC0000003lGr1?srPos=0&srKp=01t) also adds **Glonass**, **BeiDou** and **QZSS**

- **Galileo constellation**: the ublox M8T receiver is hardware compatible with the Galileo constellation, but a receiver firmware update (beyond versions 2.01) for the Receiver/ and software update for SecureSync will be needed- expected around ~~Q4-2016~~)

Per Paul M (9/7/2016)

U-Blox Resurvey on Reboot

1. Resurvey’s on reboot by default
2. User can select NO resurvey option by adjusting Dynamic value
3. Standard Land (Resurvey)
4. If the user selects this mode, every reboot the U-Blox receiver ONLY re-survey’s.
5. This is default product behavior.
6. Standard Stationary (No Resurvey)
7. If user selects dynamic value of stationary, then NO resurvey is performed on reboot.
8. This is to avoid dissatisfying customers who don’t want this.

Email from Dave Sohn to Derek (3 Jun 16)
Here was a statement I put together for service on this:

One of the characteristics of the new u-blox receiver is that it does not automatically "resurvey" its position in standard (stationary) mode if the unit is relocated. Stationary mode provides some improved timing stability, operation down to a single satellite, and is able to employ a T-RAIM algorithm that can exclude satellite signal measurements that fall outside expected values. Normally, this behavior is not problematic, however when pre-staging deployments or redeploying systems, the system will survey at the staged location and won’t resurvey again at the deployed location, which will prevent the system from synchronizing. The system may show tracked satellites, but will not synchronize to the constellation.

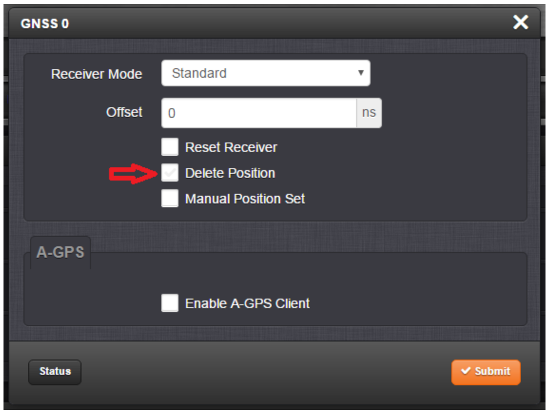
The Spectracom factory has always cleared location (and history) on all SecureSyncs before shipping them to any of our customers, so delivered units will always perform a survey on location.

There are two options to minimize any noticeable impact on systems due to staging prior to a move to final install site

1) Change the staging process to perform a "Delete Position" as part of the system power down (details below).
2) As part of the configuration done during staging, enable mobile mode, which does not perform the survey process. This will not have any appreciable effect on 1PPS (or 10MHz) accuracy. We only saw a difference of 3 ns between the 1 sigma 1PPS synchronization accuracy over 24 hours between the two modes.

To clear position:

1. Launch a web browser and load the web user interface of the unit
2. Navigate to the GNSS status page (Interfaces -> REFERENCES -> GNSS Reference -> GNSS 0)
3. On the “Main” tab, click the “Edit” button
4. Check the “Delete Position” selection and click the “Submit” button
5. The survey will automatically restart
6. Shut down the unit prior to survey completion (~33 minutes)



GNSS 0

Receiver Mode: Standard

Offset: 0 ns

□ Reset Receiver

☑ Delete Position

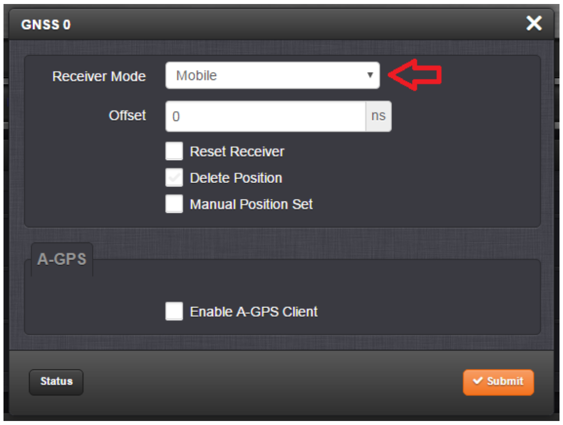
□ Manual Position Set

A-GPS

□ Enable A-GPS Client

To enable mobile mode:

1. Launch a web browser and load the web user interface of the unit
2. Navigate to the GNSS status page (Interfaces -> REFERENCES -> GNSS Reference -> GNSS 0)
3. On the “Main” tab, click the “Edit” button
4. Change the “Receiver Mode” selection to “Mobile” and click the “Submit” button



GNSS 0

Receiver Mode: Mobile

Offset: 0 ns

□ Reset Receiver

☑ Delete Position

□ Manual Position Set

A-GPS

□ Enable A-GPS Client

Desire to add a GPS receiver to the SecureSync in the field (after initial purchase)

- Requires hardware modification, and spfactory login to reconfigure the Options.
- Time server does have to be returned to factory for this hardware/software/ reconfiguration/ retrofit (even if the request is from one of our dealers).

GPS-Glonass-QZSS-Galileo satellite constellation / number of satellites being tracked

Using a Model 8228 window-mount antenna with a GNSS receiver having multi-constellation support

- The Model 8228 antenna is a GPS consteallation-only antenna.
- Can still be used to track GPS satellites, but won't allow the recieever to track any other consteallation besides GPS

Q Does 8228 indoor antenna support SS-OPT-GNS?

A Keith's response (5 Oct 17): The Model 8228 window-mount antenna is a GPS consteallation-only antenna. Since it can only receive GPS signals (it can't receive Glonass, Galileo, etc) a GNSS receiver in the SecureSync which is connected to this antenna will only be able to track GPS satellites. So it can't be used with a SecureSync, if it's desired for the SecureSync to be able to track satellites beyond just GPS satellites.

A) Galileo

B) QZSS option (reception only available if SecureSync is located in Japan/its neighbors or Australia)

Note: QZSS is also referred to as "**MICHIBIKI**"

email from Josh (19 Jun KW) MICHIBIKI is simply the nickname given to the QZSS system that is referred to in our manual. So the answer to your question about MICHIBIKI is yes. MICHIBIKI also supported officially.

- QZSS capability was added in software update version 5.3.0 (Sept 2015)
- (Versions 5.6.0 and below) QZSS capability requires the Glonass license file to purchased/installed (QZSS is included with Glonass)
- QZSS option not available with Trimble Res-T receiver or with software versions 5.2.1 and below.
- QZSS is only displayed if the Glonass/QZSS license file is installed (license file not required in v5.7.0 and above)

Email from Josh (15 Sept 15) The QZSS constellation moves in a figure of 8 , the top half covers Japan as well as her neighboring countries while the bottom half covers Australia.

The last I checked a couple of months ago, the folks Down Under are not considering QZSS as yet but that is not to say that they will not in the future.

Summary of QZSS support

Receiver	QZSS available?	Requirements
uBlox M8T	**Yes**	**A) just uBlox receiver (license file not needed)**

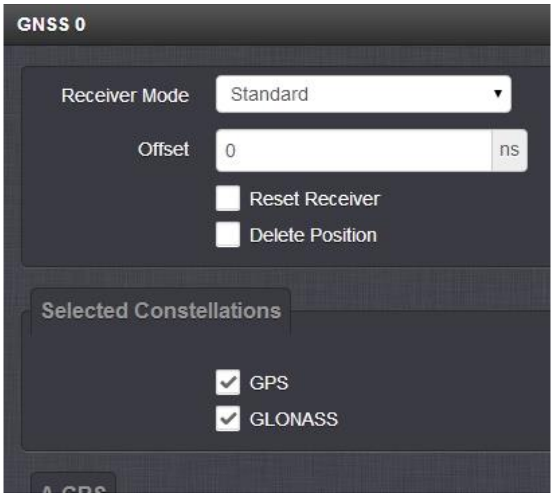
Enable or Disable Glonass/QZSS/GPS (if SS-Opt-GNS license file is installed and versions 5.6.0 and

below)

Note: update version 5.7.0 (Jun 2017) alleviates the need to purchase the multi-GNSS license if its desired to add additional constellations beyond just GPS. Once a unit has been updated to 5.7.0 or above, the unit has the ability to enable GPS and other satellite constellations (units with just GPS before updating will just have GPS enabled after updating. But they can then go in and enable other constellations if desires.
GPS and Glonass/QZSS (if these license files are installed) are enabled/disabled in the **Interfaces** -> **GNSS Reference** page of the browser. Then click on the "Gear" box between "GNSS 0" and the indication of how many satellites are being tracked (below the photo)

Note: if neither GPS nor Glonass is enabled, it defaults to **GPS** being active.

(Versions 5.2.1 and below- GPS and Glonass)



GNSS 0

Receiver Mode: Standard

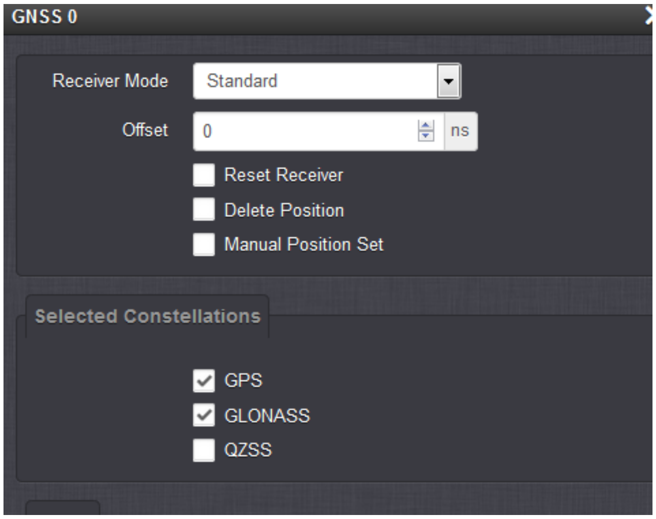
Offset: 0 ns

□ Reset Receiver
□ Delete Position

Selected Constellations

☑ GPS
☑ GLONASS

(Versions 5.3.0 and above- GPS, Glonass and QZSS)



GNSS 0

Receiver Mode: Standard

Offset: 0 ns

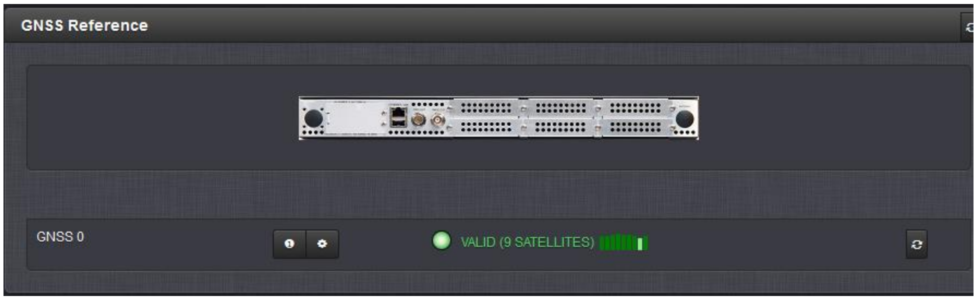
□ Reset Receiver
□ Delete Position
□ Manual Position Set

Selected Constellations

☑ GPS
☑ GLONASS
□ QZSS

Number of tracked GPS/Glonass satellites

To determine the number of satellites currently being tracked, log in to the SecureSync's Web UI. The **Interfaces** -> **GNSS** page of the browser reports the number of satellites being tracked.

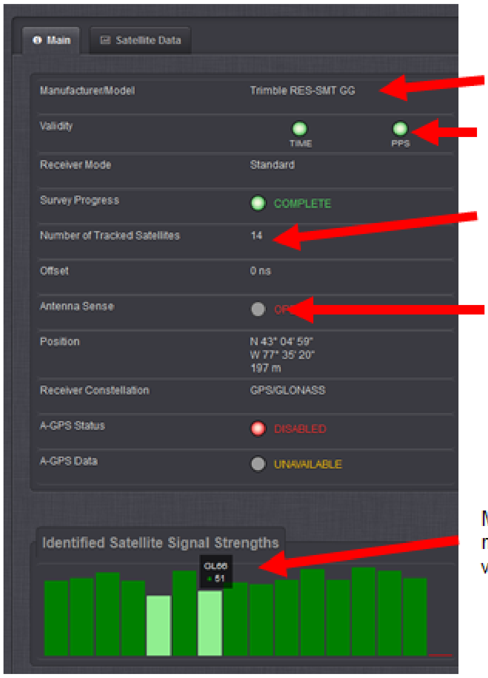


GNSS Reference

GNSS 0 ● VALID (9 SATELLITES)

GNSS Signal Status view

For a detailed view, from this page, click on the “circled i” ICON in the bottom row, under the photo.   Or from the main menu, click on “**Interfaces**” at the top of the page and in the drop-down, select “**GNSS 0**”. The “**Main**” tab should be automatically selected (as shown below):



Manufacturer/Model	Trimble RES-SMT GG
Validity	● TIME ● PPS
Receiver Mode	Standard
Survey Progress	● COMPLETE
Number of Tracked Satellites	14
Offset	0 ns
Antenna Sense	● OP
Position	N 43° 04' 59" W 77° 35' 20" 197 m
Receiver Constellation	GPS/GLONASS
A-GPS Status	● DISABLED
A-GPS Data	● UNAVAILABLE

GPS or GNSS receiver Model installed.

This line indicates the validity of the GNSS receivers Time and PPS inputs.

This line indicates the number of combined GPS and/or Glonass satellites currently being used for time/position fix information.

This line indicates whether an open or short is being detected in the antenna cable (“OK” indicates no cable issues are being detected at this moment). In this example, an open in the cable is being detected.

Mouse-hover over each of the bar graphs to indicate the satellite ID numbers being used in the fix and their relative signal strengths (SNR values) for those particular satellites.

GNSS Signal Status view (Trimble Res-T or Res-SMT-GG)

- **Red bars:** (really bad) less than??
- **Yellow bars**: SNR values of less than 35?
- **Light green bars:** SNR values from 35 to 39??
- **Darker green bars:** SNR values of 40 or greater?

The “GNSS 0 Input Status” page will indicate the current number of GPS and/or Glonass satellites being used in the positional fix (based on the number of vertical bars being displayed). If this field indicates no bars, it is currently not tracking any satellites. If this field indicates a low number of bars, such as only “1”, “2” or “3”, the unit is tracking a few satellites, but it’s not tracking the minimum number of satellites required for initial sync.

(ID field) Distinguishing between GPS satellites and Glonass satellites, when the Glonass/QZSS Option is enabled

9. To determine if each bar represents a GPS or a Glonass satellite, Mouse-hover each bar to see a report of three values (two letters, the Satellite ID number and the signal strength value for that satellite).

- **GPS** satellites are indicated with “**G**” (v5.3.0 and above) or the two letters of “**GP**” (v5.2.1 and below) and have a Satellite ID Number of 0 to 59.

Addititional constellations only available if the SS Opt-GNS License is installed

- **Glonass** (Russia) satellites are indicated with an “**R**” (v5.3.0 and above) or the two letters of “**GP**” (v5.2.1 and below) the two letters of “**GL**” and have a Satellite ID Number of 60 and above.
- **QZSS** (Japan) satellite(s) are indicated with a “**J**”. Note these satellites are only available insoftware

versions v5.3.0 and above and if the Glonass option is enabled.

Note: QZSS is also referred to as “**MICHIBIKI”**

email from Josh (19 Jun KW) MICHIBIKI is simply the nickname given to the QZSS system that is referred to in our manual. So the answer to your question about MICHIBIKI is yes. MICHIBIKI also supported officially.

- **Beideu:** satellite(s) are indicated with a “   ” Note these satellites are only available in softwave versions 5.4.0 or above, with a u-blox Model M8T receiver installed and Opt-GNS license enabled (Started shipping this receiver ~17 March 2016 with approximate Serial Numbers 11718 and above).

**GR_GetSatData 0 0 CLI command (undocumented command)

Breakdown of the Satellite Data table:

ch: Receiver channel Number

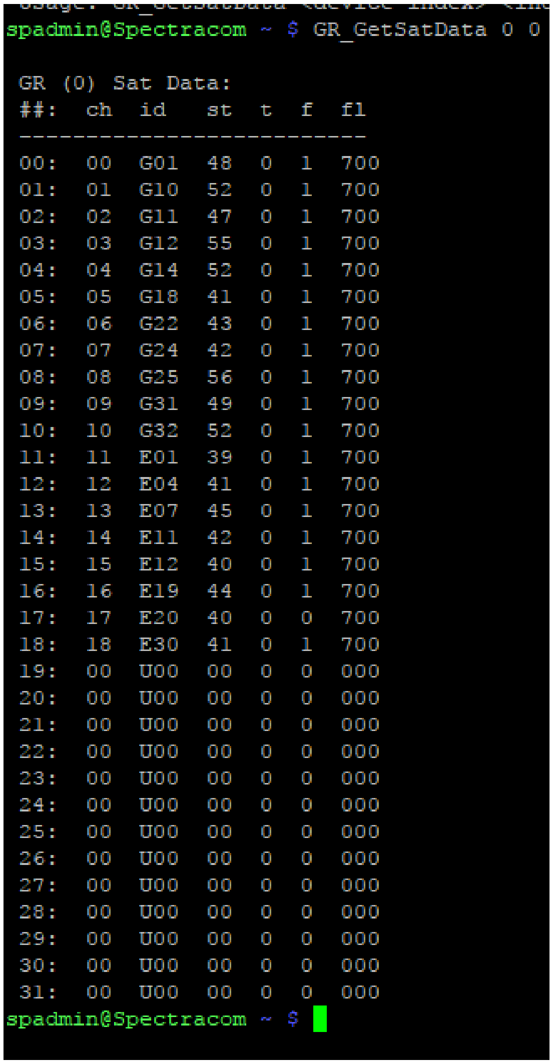
Id: (SVN) Space Vehicle Number/ID Number of the satellite being tracked

st: signal strength of the satellite being tracked

t: TRAIM (aka "**bTraim**") Is satellite accepted by the TRAIM algorithm? ("0" if no, "1" if yes)

f: fix status (aka "**bInfix**") Is satellite being used in the fix? ("0" if not in fix, "1" if satellite is being used in fix)

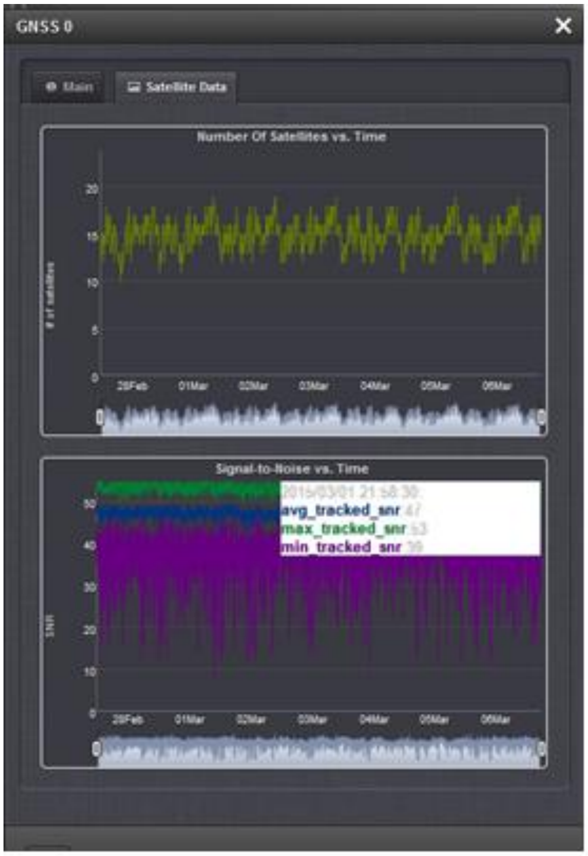
fl: flags reported by the receiver (always "00" with Res-T, REs-SMT and RES-SMT-GG receivers. Used only with SAASM receivers)



```
 Usage: GR_GetSatData <device index> <ind
spadmin@Spectracom ~ $ GR_GetSatData 0 0

 GR (0) Sat Data:
 ##:  ch  id   st  t  f  fl
 --------------------------
 00:  00  G01  48  0  1  700
 01:  01  G10  52  0  1  700
 02:  02  G11  47  0  1  700
 03:  03  G12  55  0  1  700
 04:  04  G14  52  0  1  700
 05:  05  G18  41  0  1  700
 06:  06  G22  43  0  1  700
 07:  07  G24  42  0  1  700
 08:  08  G25  56  0  1  700
 09:  09  G31  49  0  1  700
 10:  10  G32  52  0  1  700
 11:  11  E01  39  0  1  700
 12:  12  E04  41  0  1  700
 13:  13  E07  45  0  1  700
 14:  14  E11  42  0  1  700
 15:  15  E12  40  0  1  700
 16:  16  E19  44  0  1  700
 17:  17  E20  40  0  0  700
 18:  18  E30  41  0  1  700
 19:  00  U00  00  0  0  000
 20:  00  U00  00  0  0  000
 21:  00  U00  00  0  0  000
 22:  00  U00  00  0  0  000
 23:  00  U00  00  0  0  000
 24:  00  U00  00  0  0  000
 25:  00  U00  00  0  0  000
 26:  00  U00  00  0  0  000
 27:  00  U00  00  0  0  000
 28:  00  U00  00  0  0  000
 29:  00  U00  00  0  0  000
 30:  00  U00  00  0  0  000
 31:  00  U00  00  0  0  000
spadmin@Spectracom ~ $
```

****GPS Satellite/Signal Strength (Signal to Noise) graphs

- Graphs are in the newer black/charcoal browser only (software versions 5.1.2 and above only)
- Graphs are displayed in the **Interfaces** -> **GNSS 0** page of the browser, **Satellite Data** tab



Yellow line: Total number of tracked satellites
(mouse-hover to see exact numbers or use bottom sliders to zero-in)

Green line: Maximum SNRvalues
Blue line: Average SNR values
Purple line: Minimum SNRvalues
(mouse-hover to see exact numbers or use bottom sliders to zero-in)

- GPS graphs not available in classic interface web browser (new browser in version 5.1.0 and above only)
- Hover over graphs to see specific values at a particular moment (a small dot will show in the top line to indicate a specific point where the mouse hover is reading the data from).
- Graphs show up to one week of data.
- GPS graph data is stored in the mysql database, or the SQLite database starting in v5.3.1 (not in the "log" directory). Refer to info below on exporting this data as either a **.csv** or **.json** file.
- If Satellite Data graphs aren't displayed (as shown below), switch back to the "**Main**" tab and then switch back to the "**Satellite Data**" tab again to refresh this

Issue with Min SNR/Max SNR values being displayed backwards (v5.7.1 and below)

- Applies to v5.7.1 and below (expected to be corrected in update v5.7.3, ~ Feb/March 2018)

Issue with graphs potentially not always being displayed in the browser

With at least 5.3.0 and below, graph data may not always be displayed after switching from **Main** to **Satellite** tab. Switch back to Main and then switch back to the Satellite tab again to see the data. This is a very minor issue with the refreshing that should occur when selecting the other tab.

Storage, Exporting and Clearing of the raw satellite data used to generate the graphs

- The raw data for the generation of the graphs is stored in the MySQL database (versions 5.3.0 and below) or in the SQLite database which is exported as part of the savelogs bundle (versions 5.3.1 and above)
- Versions 5.3.1 and above download the satellite data as part of the save and download logs bundle (**Management** -> **Log Configuration** page), Data is included with the SQLite data placed in the /srv folder
- The raw data for the generation of the graphs can be exported (via browser or CLI) as either a ".csv" (can open in Excel) or ".json" file (for graphing) using the web browser

Summary of downloading/exporting Satellite data

There are two main ways to download the satellite data for graphing. One method allows a freeware program to both display and graph the raw data after downloading a saved log bundle from the time server. The other method allows the raw data to just be downloaded as either a .csv or .json file.

Note the method to display and graph the data with a freeware program requires software version 5.3.1 (the latest available version) be installed in the time server. Downloading the raw data as either a .csv or .json file just requires the use of the new (black/charcoal) web browser which was implemented in version 5.1.2.

1. View the raw data and graph in the freeware "Sqlite DB browser" program

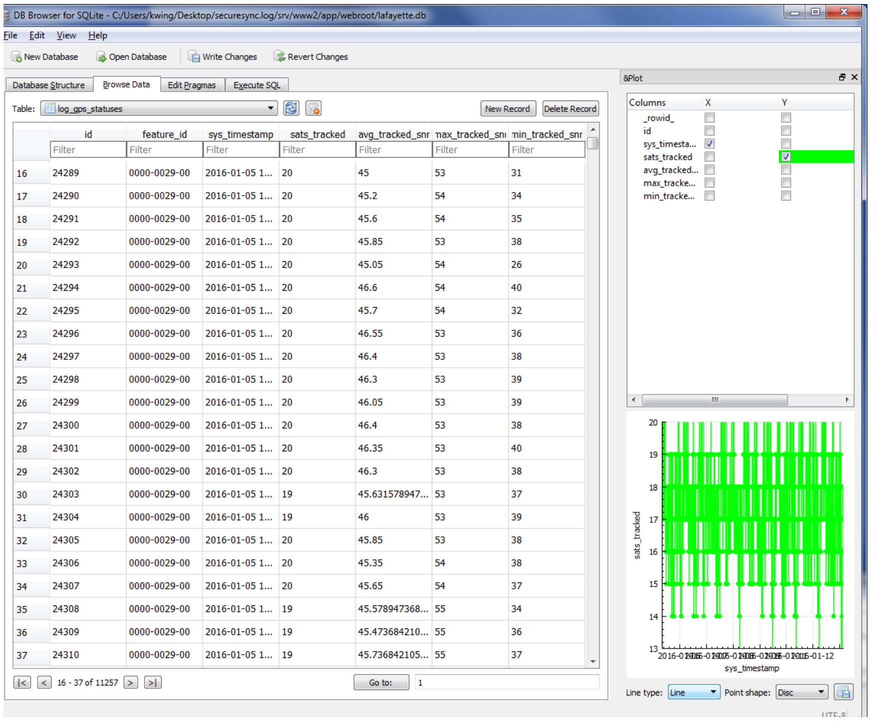


Table: log_gps_statuses

	id	feature_id	sys_timestamp	sats_tracked	avg_tracked_snr	nax_tracked_sni	min_tracked_snr
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
16	24289	0000-0029-00	2016-01-05 1...	20	45	53	31
17	24290	0000-0029-00	2016-01-05 1...	20	45.2	54	34
18	24291	0000-0029-00	2016-01-05 1...	20	45.6	54	35
19	24292	0000-0029-00	2016-01-05 1...	20	45.85	53	38
20	24293	0000-0029-00	2016-01-05 1...	20	45.05	54	26
21	24294	0000-0029-00	2016-01-05 1...	20	46.6	54	40
22	24295	0000-0029-00	2016-01-05 1...	20	45.7	54	32
23	24296	0000-0029-00	2016-01-05 1...	20	46.55	53	36
24	24297	0000-0029-00	2016-01-05 1...	20	46.4	53	38
25	24298	0000-0029-00	2016-01-05 1...	20	46.3	53	39
26	24299	0000-0029-00	2016-01-05 1...	20	46.05	53	39
27	24300	0000-0029-00	2016-01-05 1...	20	46.4	53	38
28	24301	0000-0029-00	2016-01-05 1...	20	46.35	53	40
29	24302	0000-0029-00	2016-01-05 1...	20	46.3	53	38
30	24303	0000-0029-00	2016-01-05 1...	19	45.631578947...	53	37
31	24304	0000-0029-00	2016-01-05 1...	19	46	53	39
32	24305	0000-0029-00	2016-01-05 1...	20	45.85	53	38
33	24306	0000-0029-00	2016-01-05 1...	20	45.35	54	38
34	24307	0000-0029-00	2016-01-05 1...	20	45.65	54	37
35	24308	0000-0029-00	2016-01-05 1...	19	45.578947368...	55	34
36	24309	0000-0029-00	2016-01-05 1...	19	45.473684210...	55	36
37	24310	0000-0029-00	2016-01-05 1...	19	45.736842105...	55	37

|< < 16 - 37 of 11257 > >|

Go to: 1

Columns	X	Y
rowid	☐	☐
id	☐	☐
sys_timesta...	☑	☐
sats_tracked	☐	☑
avg_tracked...	☐	☐
max_tracke...	☐	☐
min_tracke...	☐	☐

Line type: Line Point shape: Disc

Pre-requisite: Download/install the freeware program "**dB browser for SQLite**": http://sqlitebrowser.org

A) If the current software version is 5.3.0 or below, upgrade the software to versions 5.3.1 or above to change the MySQL database to SQLlite database.

B) With software versions 5.3.1 or above installed, "Save and download logs" (**Management** -> **Log Configuration** page of the browser)

C) Use the Sqlite DB Browser program to view the database (database file is named “lafayette” and is located in the **/srv/www2/app/webroot** directory of the saved log file. Rename this file as “**lafayette.db**”)

D) In the DB browser, open the database and then select the “**Browse Data**” tab. **I**n the “Table” drop-down, select “**log_gps_statuses**” in the Plot table, select desired fields to be graphed.

E) Data can be saved (as .png, .jpg, PDF or .bmp file) by pressing te “Save” ICON in the upper-right corner.

2. Output the raw satellite data as either a .csv or json file Output of raw satellite data as a “csv” file (can be opened in excel)

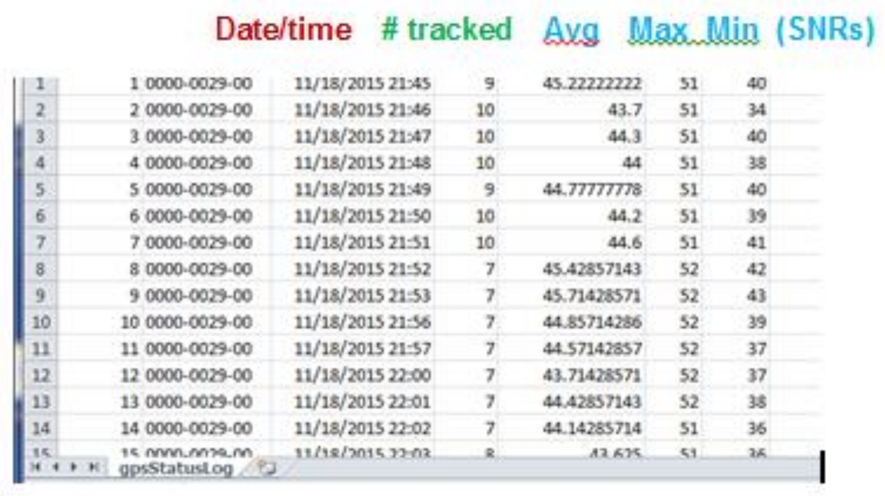
Note: This method works with MYSQL Database (versions 5.3.0 and below) or with SQLite (versions 5.3.1 and above)

Email from Ron Dries (18 Nov 15) If you manually enter **/Logs/gpsStatusLog.csv after the URL** of the SecureSync in the web browser it will download a csv file that can be opened in Excel with the GPS status log data.

Example: http://10.10.128.1/Logs/gpsStatusLog.csv (change address as applicable) (link is cap-letter sensitive)

I have tried this in Chrome and it worked. I haven’t tried it in any other browser.

Example file download below



Date/time # tracked Avg Max Min (SNRs)

1	1	0000-0029-00	11/18/2015 21:45	9	45.22222222	51	40
2	2	0000-0029-00	11/18/2015 21:46	10	43.7	51	34
3	3	0000-0029-00	11/18/2015 21:47	10	44.3	51	40
4	4	0000-0029-00	11/18/2015 21:48	10	44	51	38
5	5	0000-0029-00	11/18/2015 21:49	9	44.77777778	51	40
6	6	0000-0029-00	11/18/2015 21:50	10	44.2	51	39
7	7	0000-0029-00	11/18/2015 21:51	10	44.6	51	41
8	8	0000-0029-00	11/18/2015 21:52	7	45.42857143	52	42
9	9	0000-0029-00	11/18/2015 21:53	7	45.71428571	52	43
10	10	0000-0029-00	11/18/2015 21:56	7	44.85714286	52	39
11	11	0000-0029-00	11/18/2015 21:57	7	44.57142857	52	37
12	12	0000-0029-00	11/18/2015 22:00	7	43.71428571	52	37
13	13	0000-0029-00	11/18/2015 22:01	7	44.42857143	52	38
14	14	0000-0029-00	11/18/2015 22:02	7	44.14285714	51	36
15	15	0000-0029-00	11/18/2015 22:03	8	43.625	51	36

Automating the generation of the .csv file (being provided via CLI interface)

- Dave Sohn created a python script file that automates a **.csv** file being generated via **CLI** interface. Refer to: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\GPS\python script for gps info

Output of graphable data (as a “.json” file for graphing)

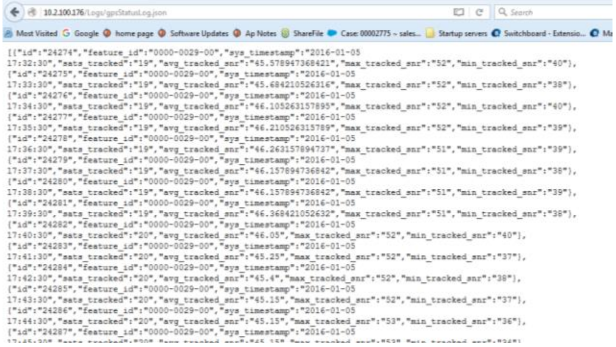
Note: This method works with MYSQL Database (versions 5.3.0 and below) or with SQLite (versions 5.3.1 and above)

- Same process as downloading.csv file, but replace “.csv” with “.json” instead.

If you manually enter **/Logs/gpsStatusLog.json** after the URL of the SecureSync in the web browser it will download a csv file that can be opened in Excel with the GPS status log data.

Example: http://10.10.128.1/Logs/gpsStatusLog.json   (change address as applicable) (link is cap-letter sensitive)

Example file download below


10.2.100.176/Logs/gpsStatusLog.json
Search
Most Visited
Google
home page
Software Updates
Ap Notes
ShareFile
Case: 00002775 ~ sales...
Startup servers
Switchboard - Extensio...
Ma

```
[{"id":"24274","feature_id":"0000-0029-00","sys_timestamp":"2016-01-05
17:32:30","sats_tracked":"19","avg_tracked_snr":"45.578947368421","max_tracked_snr":"52","min_tracked_snr":"40"},
{"id":"24275","feature_id":"0000-0029-00","sys_timestamp":"2016-01-05
17:33:30","sats_tracked":"19","avg_tracked_snr":"45.684210526316","max_tracked_snr":"52","min_tracked_snr":"38"},
{"id":"24276","feature_id":"0000-0029-00","sys_timestamp":"2016-01-05
17:34:30","sats_tracked":"19","avg_tracked_snr":"46.105263157895","max_tracked_snr":"52","min_tracked_snr":"40"},
{"id":"24277","feature_id":"0000-0029-00","sys_timestamp":"2016-01-05
17:35:30","sats_tracked":"19","avg_tracked_snr":"46.210526315789","max_tracked_snr":"52","min_tracked_snr":"39"},
{"id":"24278","feature_id":"0000-0029-00","sys_timestamp":"2016-01-05
17:36:30","sats_tracked":"19","avg_tracked_snr":"46.263157894737","max_tracked_snr":"51","min_tracked_snr":"39"},
{"id":"24279","feature_id":"0000-0029-00","sys_timestamp":"2016-01-05
17:37:30","sats_tracked":"19","avg_tracked_snr":"46.157894736842","max_tracked_snr":"51","min_tracked_snr":"38"},
{"id":"24280","feature_id":"0000-0029-00","sys_timestamp":"2016-01-05
17:38:30","sats_tracked":"19","avg_tracked_snr":"46.157894736842","max_tracked_snr":"51","min_tracked_snr":"39"},
{"id":"24281","feature_id":"0000-0029-00","sys_timestamp":"2016-01-05
17:39:30","sats_tracked":"19","avg_tracked_snr":"46.368421052632","max_tracked_snr":"51","min_tracked_snr":"38"},
{"id":"24282","feature_id":"0000-0029-00","sys_timestamp":"2016-01-05
17:40:30","sats_tracked":"20","avg_tracked_snr":"46.05","max_tracked_snr":"52","min_tracked_snr":"40"},
{"id":"24283","feature_id":"0000-0029-00","sys_timestamp":"2016-01-05
17:41:30","sats_tracked":"20","avg_tracked_snr":"45.25","max_tracked_snr":"52","min_tracked_snr":"37"},
{"id":"24284","feature_id":"0000-0029-00","sys_timestamp":"2016-01-05
17:42:30","sats_tracked":"20","avg_tracked_snr":"45.4","max_tracked_snr":"52","min_tracked_snr":"38"},
{"id":"24285","feature_id":"0000-0029-00","sys_timestamp":"2016-01-05
17:43:30","sats_tracked":"20","avg_tracked_snr":"45.15","max_tracked_snr":"52","min_tracked_snr":"37"},
{"id":"24286","feature_id":"0000-0029-00","sys_timestamp":"2016-01-05
17:44:30","sats_tracked":"20","avg_tracked_snr":"45.15","max_tracked_snr":"53","min_tracked_snr":"36"},
{"id":"24287","feature_id":"0000-0029-00","sys_timestamp":"2016-01-05
17:45:30","sats_tracked":"20","avg_tracked_snr":"45.15","max_tracked_snr":"53","min_tracked_snr":"34"}
```

Alignment of 1PPS output from receiver to system, based on the Satellite constellation selected (not applicable to Trimble Res-T GPS receiver)

- Refer to Mantis case 2938 for details
- **Summary**: SecureSync 1PPS output can be offset (by up to 300ns) depending on which GNSS constellations are selected. Different timescales have different definitions of their 1PPS Signal.

Bent center plate on rear panel Type N GPS input connector

- Search for “**Bent center plate**” in the Custserviceassistance document

Note: this condition of one of the four plates being spread out too far has resulted in at least one instance where the GPS RF signal was still getting in (receiver was tracking satellites) but the antenna problem alarm was still asserted.

**GPS Antenna Problem alarm

Antenna Sense = “unknown”

It sounds like the internal GPS receiver may have suffered a power surge or lightning strike. The “unknown” state is indicating that the GPS receiver’s antenna sense circuit (which measure the current draw of the 5vdc used to power the GPS antenna) is detecting some type of problem with the GPS antenna connection, but can’t tell what the problem is. This is an abnormal indication for the GPS receiver to be reporting. It would not be caused by any normal failure of either the antenna connection or with the GPS antenna itself. If the GPS receiver suffered a surge, the antenna may or may not have also been affected.

For troubleshooting this condition- treat it as if there is an open or short in the antenna cable.

- **GPS preamp or splitter installed-** these devices can block the detection of an open/short in the cable on the antenna side of the device (the device draws current, so the receiver thinks there is a good connection to the antenna, even though the antenna is not getting any voltage.

- **One or more of the four center plates of the rear panel GPS input connector may be spread out too far**

  Note: this condition of one of the four plates being spread out too far has resulted in at least one instance where the GPS RF signal was still getting in (receiver was tracking satellites) but the antenna problem alarm was still asserted.

  Refer to “**Bent center plate**…”section further above and also in the Customerserviceassistance doc.

Desire to clear Antenna Problem alarm when GPS antenna is not connected

Note: Archive Version 4.8.7 (Sept 2012) is adding the ability to disable the Antenna Problem alarm indications via the **Setup**-> **Notifications** page of the browser. Log entries for cable issues will still be asserted, if the alarm is disabled.

As a matter of fact, there certainly is a way to prevent the Fault LED from blinking. This is an indication that the Antenna Problem alarm is asserted, because the GPS sense circuit is detecting an open in the GPS port.

To clear this alarm, you just need to simulate a GPS antenna being connected. The output voltage of the rear panel antenna jack (used to power the antenna) is a nominal +5vdc. To simulate a GPS antenna being connected to this jack, simply put a 60 to 200 ohm resistor from the center of the antenna jack to the outer- tiller hreaded portion of the same jack. This resistive load will simulate a GPS antenna being connected, therefore clearing the Antenna Problem alarm (the LED will no longer blink).

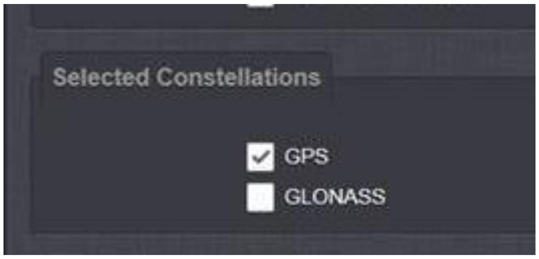
The specific resistor value doesn't really need to be a specific value. The sense circuit is pretty wide open in order to support GPS antennas with varying impedance values. We have used antennas with 67 ohm impendence as well as around 200 ohm impedance. Any value in this general range will simulate the GPS antenna being connected.

**GPS Reception troubleshooting/issues with GPS reception

- Refer to: GPS\GPS reception Ap Notes\SecureSync

Sporadic losses of GPS reception (one or a couple of seconds) with Res-SMT-GG receiver and Glonass being enabled (requires Glonass License be installed) (noticed ~ June 2015)

- Res-SMT-GG receiver can drop to 0 satellites for one or just a couple of seconds and then go back to great reception again (more predominant when Glonass license is installed and Glonass is enabled).
- Likely due to receiver firmware versions 1.0.7 (1.7) or 1.0.6 (1.6) being installed in the Res-SMT-GG receiver. Receiver should be updated to version 1.08 (1.8). Refer to known issues with the Res-SMT-GG receiver
- Version 1.0.8 (1.8) update is included in the version 5.3.0 release - Sept 2015). Temp work-around: Either disable Glonass or return receiver to the factory for update to firmware version 1.08 update.
- Glonass can be disabled in the **Interfaces** -> **GNSS 0** page of the newer browser (as shown below):



Selected Constellations

☑ GPS

□ GLONASS

Mobile (Continuous) mode and Single Satellite mode

**Operational Speed and Altitude limitations

**Speed and Altitude limitations when using a commercial GPS receiver

As far as speed (and altitude) limitations for the Res-T receiver (these are common limitations across all commercial GPS receivers due to export controls).

- **Altitude** 18,000 m
- **Velocity** 515 m/s

Note: Either limit may be exceeded, but not both!

GPS Receiver update rate /refresh rate

Q. What is the update rate of the GPS position information, assuming access through the CLI on SNMP?
A. The receiver updates position at a 1 Hz rate.

Ground speed/track angle

Q Is there any way to access the ground speed or track angle information through either the CLI or SNMP?
A **Reply from Dave Lora (SR 6575)** The Front Panel, command line interface “gpsloc” command and the SNMP MIB variables for Latitude, Longitude and Altitude can be read. We do NOT recommend walking the MIB to read the data, however, reading these values at no faster than 1Hz is possible.

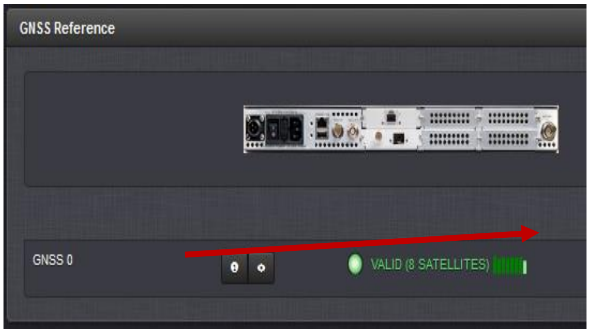
Q Would the unit moving at moderate speeds (25 knots / 39 mph / 46kph) have any effect on the timing accuracy? If the user places the SecureSync in Mobile mode it can be used in mobile operation. The use of timing receivers in low speed, low dynamic (meaning slow turns) motion will be the lowest risk in degrading Time/1PPS signal performance depending on GNSS/GPS Receiver type installed.
A **Reply from Dave Lorah (SR 6575)** The Trimble receivers will experience degraded 1PPS performance 3x worse than our stated specification in the best case. The recommended receiver type to use is the U-Blox M8T which should suffer little to no performance loss under these conditions. It is recommended the customer use Release 5.4.1 firmware until Release 5.4.5 is available. Release 5.4.5 will display Land/Sea/Air Dynamics selection for Mobile Mode users.

Degradation of timing/positional accuracies while in mobile mode (Continuous mode)

- The mount of degradation varies depending on whether the SecureSync has the earlier Model Res-T GPS receiver installed or a newer Res-SMT-GG GNSS receiver installed.
- Refer to either the “Trimble Res-T” or “Trimble Res-SMT-GG” receiver section in the Customerserviceassistance document for details.

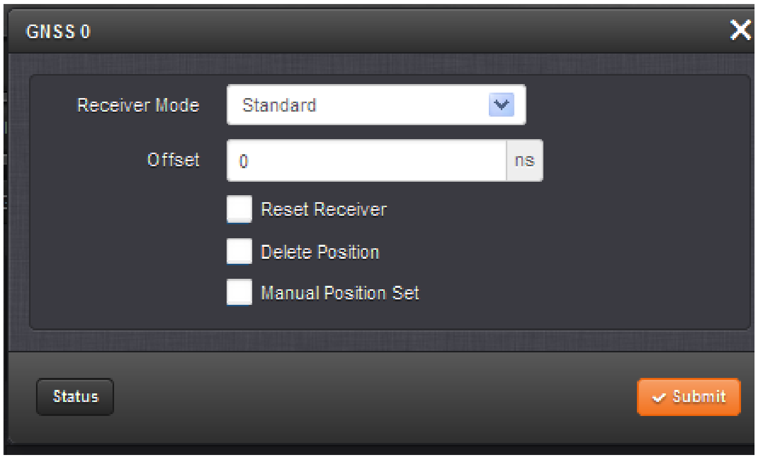
Change the GNSS Receiver Mode (Standard, Mobile or Single Satellite)

1) Go to **Interfaces** -> **GNSS 0**
2) Click the “**gear**” near “**GNSS 0**”



GNSS Reference

GNSS 0 — VALID (8 SATELLITES)



GNSS 0

Receiver Mode: Standard

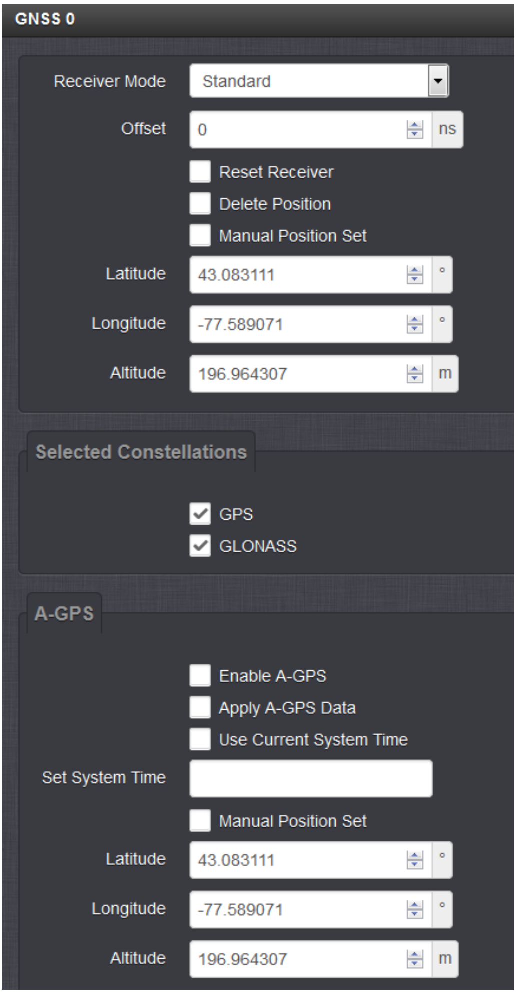
Offset: 0 ns

□ Reset Receiver

□ Delete Position

□ Manual Position Set

Interfaces -> GNSS 0, Edit (Glonass Option enabled) **Interfaces -> GNSS 0, Edit (Glonass Option not enabled)**



GNSS 0

Receiver Mode: Standard

Offset: 0 ns

□ Reset Receiver

□ Delete Position

□ Manual Position Set

Latitude: 43.083111 °

Longitude: -77.589071 °

Altitude: 196.964307 m

Selected Constellations

☑ GPS

☑ GLONASS

A-GPS

□ Enable A-GPS

□ Apply A-GPS Data

□ Use Current System Time

Set System Time:

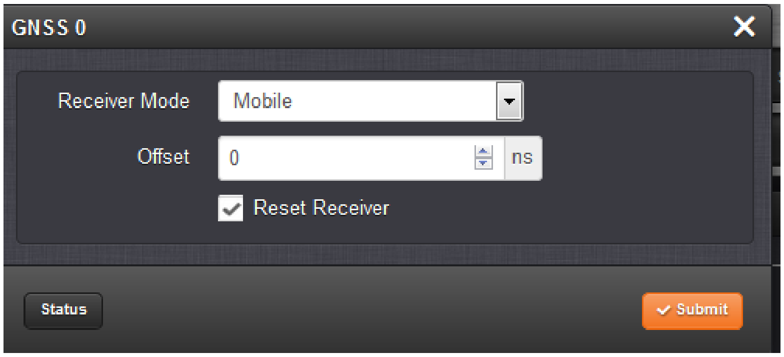
□ Manual Position Set

Latitude: 43.083111 °

Longitude: -77.589071 °

Altitude: 196.964307 m

`



GNSS 0

Receiver Mode: Mobile

Offset: 0 ns

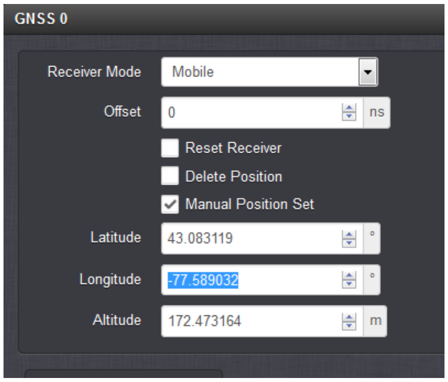
☑ Reset Receiver

Desire to manually set the positon

1) Disconnect the GPS antenna
2) Delete the position (select “**Delete Position**” and Submit)

3) Select “**Manual Position Set**” checkbox

4) Must enter latitude, longitude and an altitude value for the manual position to be accepted.



GNSS 0

Receiver Mode: Mobile

Offset: 0 ns

□ Reset Receiver

□ Delete Position

☑ Manual Position Set

Latitude: 43.083119 °

Longitude: -77.589032 °

Altitude: 172.473164 m

To manually enter the latitude

- ○ As “**N**”: don’t add any sign at the beginning (N is +).
- ○ As “**S**”: add a minus (-) sign at the beginning (S is -).

  Example entry for “North 43 12 34 56: 43.123456

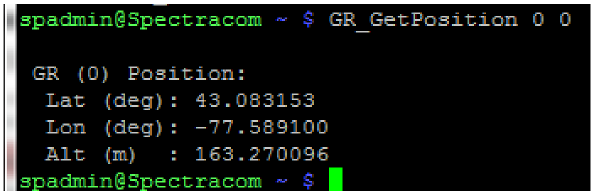
To manually enter the longitude

- ○ As “**E**”: don’t add any sign at the beginning (E is +).
- ○ As “**W**”: add a minus (-) sign at the beginning (S is -).

  Example entry for “West 077 12 34 56**: -077.123456**

Notes about manually setting the position via CLI interface

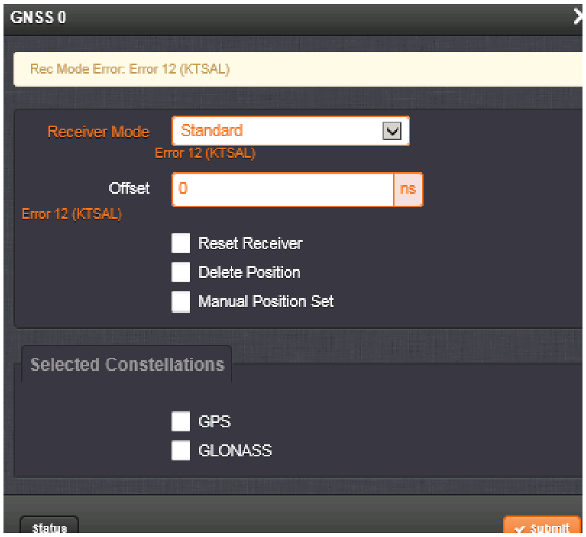
1. The KTS call for setting position is **GR_SetPosition 0 0**, but the admin and user accounts don’t have permission to use this call to manually set the position. However, these accounts do have permission to get/display the current position using the **GR_GetPosition 0 0** call.



```
spadmin@Spectracom ~ $ GR_GetPosition 0 0

 GR (0) Position:
  Lat (deg): 43.083153
  Lon (deg): -77.589100
  Alt (m)   : 163.270096
spadmin@Spectracom ~ $
```

“Rec Mode Error: Error 12 (KTSAL)

- ○ Refer to SR4597 in SAP (see screenshot further below)
- ○ Reported by Wells Fargo in two SecureSyncs with v5.2.0 software installed
- ○ They reported the GNSS receiver changed on its own from Standard to Single Satellite mode.
- ○ They have Glonass Option enabled.
- ○ They weren’t making any changes to the GNSS receiver configs when this condition was observed.
- ○ Fixed with reboot.



Rec Mode Error: Error 12 (KTSAL)

Receiver Mode: Standard
Error 12 (KTSAL)

Offset: 0 ns
Error 12 (KTSAL)

□ Reset Receiver
□ Delete Position
□ Manual Position Set

Selected Constellations

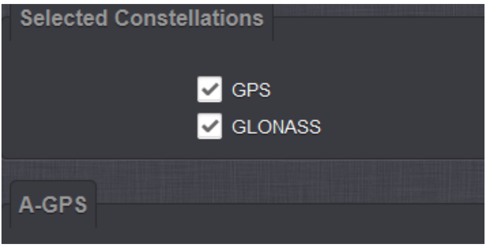
□ GPS
□ GLONASS

“Constellation Error: Error 12 (KTSAL)”: Error message displayed and “[webui] ERROR (7) - ERROR in KTSAL_Set:
GR_SetConstSel 0 0 0 (KTSAL)” in the System log when changing GNSS receiver configuration “**Note about Offset field**: Error 12 is also associated with changing the antenna cable offset value and pressing Submit, for the same reasons mentioned below. As discussed below, this is just an error message issue in 5.1.7 and below with RES-SMT-GG receiver installed. The offset value is still accepted though the message is displayed.

This error message is a known minor software issue (in at least versions 5.1.7 and below) associated with changing the receiver configuration with a Res-SMT-GG receiver installed and the Glonass option not enabled. Should be fixed in the Jan 2015 V5.2.0 update.

- Refer to Mantis case 2900
- Applicable to versions 5.1.7 and below, with a RES-SMT-GG receiver, and Glonass Option not enabled
- This error message doesn’t adversely affect the system in any way.
- Can occur when a user is changing GNSS receiver configuration (**Interfaces** -> **GNSS 0** page, Edit button)

For internal FYI info only: When the Glonass option isn’t enabled and a Res-SMT-GG receiver is installed in software versions 5.1.7 and below, the GPS and/or Glonass selection (shown in the screenshot below) isn’t displayed on the web page- So neither constellation can be selected by a user. The “default setting” results in an “invalid” combination, so this error message is displayed. But the user config changes that were being made when the error was displayed are still applied, even though this condition occurred. So it’s just an error message display issue.



Selected Constellations

☑ GPS
☑ GLONASS

`

10. Fix for this issue is planned for the release sometime near the beginning of 2015

Front panel indicates receiver is tracking >4 satellites, but Status -> Inputs -> GPS page reports tracking only 1 satellite.

- The **Status -> Inputs -> GPS** page of the browser will report its tracking only "1" satellite when the GPS receiver is configured for **Single Satellite mode**.
- The SNR table on this same page of the browser and the front panel (when configured to display satellites being tracked) will report the number of sats actually being tracked.
- Refer to the section below for more info on the receiver modes.

"Receiver modes" (Stationary, mobile and single satellite modes)

A) Standard Receiver mode (factory default) and GPS Survey

- With a few earlier versions of software, the GPS receiver required four satellites at all times, even after GPS survey has been completed. The minimum requirement with most newer versions of software drops to requiring just one satellite after the GPS survey has been completed (just like the Model 9200 and 9300 series).

GPS Survey (stationary/Standard mode only)

- GPS Survey takes 2000 seconds (33.5 minutes) to complete, once GPS receiver is tracking at least four satellites.
- GPS survey is not performed while the GPS receiver is in mobile mode.
- GPS survey only performed first time in new location, while in stationary mode. If the equipment is relocated, the survey is performed again, at the new location.
- While the GPS receiver is in stationary mode, the Status-> Inputs -> on board reference GPS page will first boot-up showing:

Mode: Standard (Stationary)
Dynamics Code: Land

- The "Survey Prog" field (Status-> Inputs -> on board reference GPS page) displays percent complete.
- Once the GPS Survey has been successfully completed, the Dynamics code changes to: "**Stationary**" and the **Survey Prog**" field changes to "**Complete**".

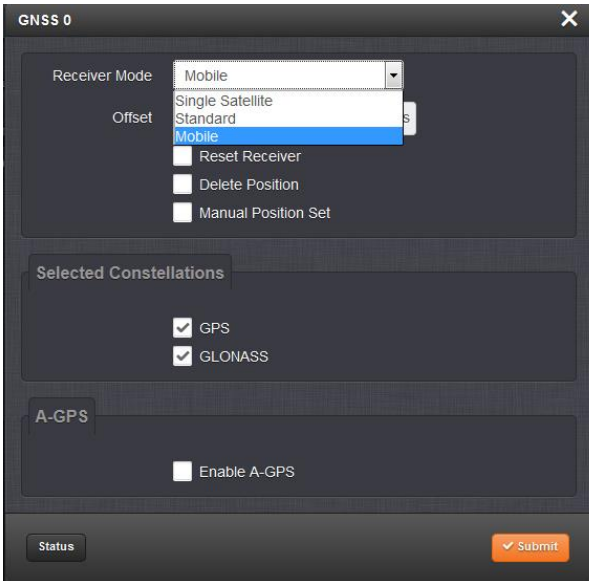
B) GPS Mobile mode

- Mobile mode requires four satellites at all times to maintain full sync status (to prevent going into Holdover mode)

Receiver dynamics codes

Receiver dynamics codes for mobile mode (such as land, sea, etc.) were removed in software **version 5.0.0.**

➢ Mobile mode is enabled/disabled in the Interfaces -> GNSS 0 page of the browser. Then click on the "Edit" box. Select Mobile and then Submit:


GNSS 0

Receiver Mode: Mobile

Offset

□ Reset Receiver

□ Delete Position

□ Manual Position Set

Selected Constellations

☑ GPS

☑ GLONASS

A-GPS

□ Enable A-GPS

- ○ Once in mobile mode, the minimum requirement to maintain sync is for the GPS receiver to track at least four satellites at all times. Dropping below 4 will put unit into Holdover mode.
- ○ PDOP/TDOP info- If PDOP or TDOP exceed a certain level, a log entry is added to the GPS Qualification log. High PDOP/TDOP results in less accuracy of the receiver. The lower the values, the better the timing. The rough estimate for timing accuracy is 1 meter of position error = 3.3 ns of timing error. A PDOP above 12 will stop the GPS survey from continuing if it was in a survey.
- ○ Accuracy of the receiver while in mobile mode (and the GPS receiver is not in motion) is no better than 3 times worse than while in stationary mode. While in motion, accuracy may get even works, depending on the PDOP/TDOP valued which may be affected by the movement, such as aircraft banking.

Signal Satellite mode:

- ➢ Requires at least one QUALIFED satellite and valid position information (either by completing a GPS survey or manually entering the correct position)
- ➢ (versions 5.0.2 and below) The Status -> Inputs -> GPS page of the browser will report its tracking only "1" satellite when the GPS receiver is configured for Single Satellite mode.
- ➢ The SNR table on this same page of the browser and the front panel (when configured to display satellites being tracked) will report the number of sats actually being tracked.

Desire ability to remotely disable GPS as an input reference

- ➢ The GPS input reference can be remotely disabled, if desired, without needing to physically disconnect the GPS antenna.
- ➢ Remotely change the "State" field for GPS to "Disabled"
- ➢ Once GPS "State" has been disabled, SecureSync will sync to the next highest priority reference (if one is present/valid) or it will immediately go into Holdover mode.
- ➢ The GPS receiver continues to track GPS satellites when "State" field is disabled.
- ➢ Switch the GPS "State" field back to "Enabled" to re-enable GPS input. GPS will become valid immediately and will be selected (if it's the highest priority reference).

GPS can be remotely disabled via:

Web browser

In the **Setup** -> **Reference Priority** table, change the **State** field for **GPS 0** / **GPS 0** to “**Disabled**”.

CLI interface (telnet or ssh)

Use the “**stateset”** command to remotely change the **State** field of any input of the Reference Priority.

SNMP

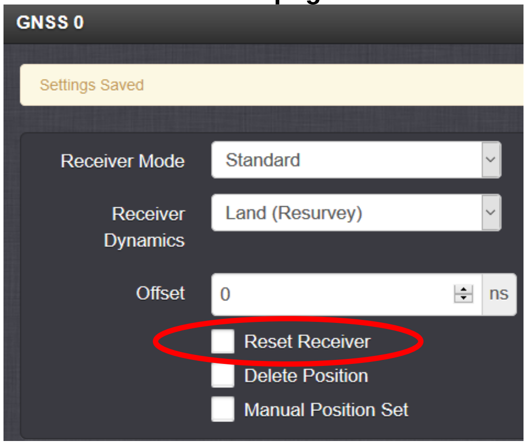
Refer to “**ssReferenceMgmtObjs”** in the **SPECTRACOM-SECURE-SYNC-MIB.mib** file for the items used to configure the Reference Priority table (specifically, see “**ssRefMgmtState**”, which is used to enable or disable input references).

Receiver reset/reset GNSS receiver

- Refer to online SecureSync user guide: http://manuals.spectracom.com/SS/Content/_Global/Topics/GNSS/GNSS_recReset.htm

The Reset Receiver command causes the GNSS receiver to execute a cold start: All data will be erased from the volatile receiver memory. Only non-volatile memory is preserved.

Interfaces **->** ***GNSS 0*** **page**



GNSS 0

Settings Saved

Receiver Mode: Standard

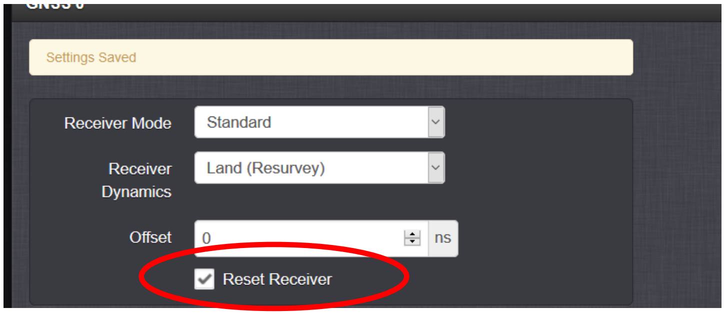
Receiver Dynamics: Land (Resurvey)

Offset: 0 ns

□ Reset Receiver

□ Delete Position

□ Manual Position Set



Settings Saved

Receiver Mode: Standard

Receiver Dynamics: Land (Resurvey)

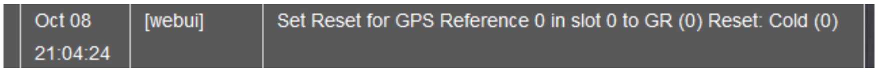
Offset: 0 ns

☑ Reset Receiver

Note: "Delete Position" and "**Manual Postion Set**" checkboxes disappear right after selecting the "Reset Receiver" checkbox (before pressing Submit)

Journal log entry asserted after resetting receiver

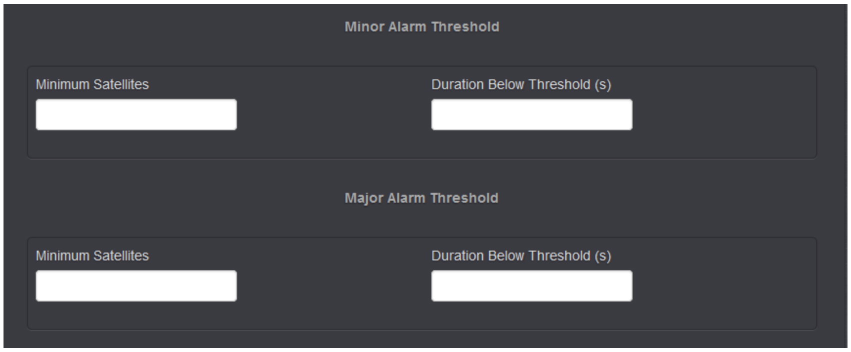
"Set Reset for GPS Reference 0 in slot 0 to GR (0) Reset: Cold (0)"



```
Oct 08     [webui]   Set Reset for GPS Reference 0 in slot 0 to GR (0) Reset: Cold (0)
21:04:24
```

User-defined Minimum Satellites alarms/traps

A) web browser User defined alarms are configured in the *Management* -> *Notifications* page (bottom of the GPS tab)



- **User defined alarm can be Masked, if desired, in the Management -> Notifications page, GPS tab**

T1 and E1 input

Note (16 Jun 2016): T1 (DS1) and E1 input are **NOT** currently available as input references (There are currently no T1 or E1 input Option Cards available. All T1/E1 Option Cards are currently output only cards).

According to Dave Sohn, there are no plans at this time to incorporate T1/E1 inputs.

**MSF/WWVB/DCF77

Email from Dave Sohn (7/24/12)

There are no plans for radio time signals like MSF, WWVB, and DCF77 in the SecureSync products at this time. Our alternatives for GPS signal failure are to provide holdover during the failure period with our OCXO and Rubidium oscillator options, if they do not have supported alternative time signal sources available.

SAASM GPS Receiver operation

- **Links to documents about SAASM:**

(2/3/12) **Important Note**: do not email information on SAASM, because our servers are hosted in Europe.

Other reference documents

- I:\Company Wide\Project Folders\Rainier(938x)\400 Customer Service Plan\Tech Notes
- The U:\Engineering\SAASM-FOUO\Docs & Tools\Crypto Key Ordering folder contains a document for ordering crypto
- The U:\Engineering\SAASM-FOUO\Docs & Tools\Crypto Key Ordering folder also contains a document for the Model 9300 SAASM operation

B) For SecureSyncs

- SecureSync SAASM receiver Manual Addendum (1200-5000-0053) Note: NOT in Arena as it's a FOUO document: **U:\Documentation\Released\Manuals\1200-xxxx-xxxx**

- (SecureSync only) The U:\Engineering\SAASM-FOUO\Released\Manuals folder contains the Spectracom doc regarding SAASM keyloading (loading keys, key status, and warning messages)

Troubleshooting a GPS reception issue

If the GPS receiver has been keyed and is having any difficulty tracking satellites (not tracking any satellites or is tracking a low number of satellites)

1) Zeroize the receiver.
2) See if it starts tracking a normal number of satellites (>4)
3) Re-key the receiver after at least an hour.
4) Verify it continues to track while being keyed.

Known potential issue with GB-Gram (MPE-S) SAASM receiver going into Holdover for 1 second

A) MPE-S sometimes enters holdover at 12:01-12:02 UTC

- Refer to MANTIS Case 2641

SAASM GPS Option Cards

- **GB-GRAM** (GBGRAM/GB Gram): SAASM GPS receiver (stands for Ground-Based GPS Receiver Application Module). Designed as a low cost SAASM GPS receiver for ground-based (ARMY) applications.

Type of SAASM Receiver installed

- **To determine type of SAASM receiver installed, refer to:** U:\Engineering\SAASM-FOUO\CustomerService\SAASM Receivers

GB-Gram SAASM receiver installed

- Two types of GB-GRAM receivers (Type 1 and Type II)
- Refer to: U:\Engineering\SAASM-FOUO\CustomerService\SAASM Receivers\GB-Gram receivers

---

- Replacement SAASM components

3. Front panel Keyfill connector / zeroize switch wiring harness (wiring, connector and switch): CA08R-MT00-0001

- Refer to PD: 1200-0017-0600 for picture of this assembly.

SAASM Key operation

- **Link to documents about SAASM:** U:\Engineering\SAASM-FOUO

CONTACT: Rolf Speziale
Zeli Systems
33 Pagosa Ct
El Paso TX 79904
(915) 751-3222
gps@zeli.com
KLIF account is ZELI001 (ID of the SAASM Facility)

Simple Key Loader (SKL)

Refer to: U:\Engineering\SAASM-FOUO\CustomerService\SKL (Simple Key loader)

Standard Positioning Service (SPS) mode

This is the unkeyed mode of SAASM receiver operation. To verify operation in SPS mode:

1. Simply attach the antenna and verify the NetClock is in Sync.
2. Look at the GPS Signal Status page for L1 Only satellites. (SPS)
3. See Security SAASM page and verify unkeyed.

Number of Keys remaining

- Refer to: U:\Engineering\SAASM-FOUO\CustomerService\Key expiration

Low battery power indicator

Email from Paul Myers

In preparation for the update to the SAASM addendum, here is what a low battery SAASM GPS condition looks like.

You will see this message in the Operational Log.
Mar 13 17:04:06 Spectracom spectracom: [system] GPS Warning (11): Low memory battery
Mar 13 17:09:06 Spectracom spectracom: [system] GPS Warning (11): Low memory battery
The Force 22E (and MPE-S GB-GRAM) will post a similar message in the SecureSync Timing log.

Desire to convert a commercial GPS input to a SAASM GPS receiver

Email from Dave Sohn on 11/17/11 (for a customer of Florise with Les Ulis):
There is a lot involved with converting a unit from standard Res-T to SAASM, and that is before the controlled item issues.

4. The physical assembly steps are involved to convert from Res-T to SAASM
5. The front panel needs to be changed and the key fill / zeroize cable needs to be attached. This involves first removing the AC/DC converter and front panel PCB.

6. The battery holder and battery needs to be installed.
7. The Res-T and antenna cable needs to be removed.
8. The SAASM option card and SAASM unit need to be installed and cabled, including the new antenna cable.
9. The serial number label needs to be replaced showing the new model and serial number with the required SAASM prefix.
10. The unit also needs to be updated with the new model number and a patch to tell the SW about the removal of the Res-T.
11. We would not be able to test functionality of the option card, SAASM, and cabling together, which is a risk.

Dave Lorah also mentioned the Factory password would need to be provided in order to make the necessary configuration changes in the web browser.

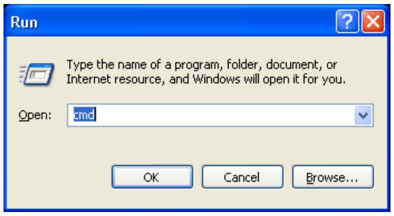
SecureSync thinks a GPS receiver is installed but really isn't (such as a SecureSync 011)

A "Remove GPS Patch" (SSO4-1200) is FTP'd into the SecureSync during Manufacturing to mask the GPS functionality. If the unit reports GPS alarms (such as Antenna Problem alarm) with no GPS receiver installed, this software patch must have been inadvertently not installed. The patch file can be installed remotely if FTP port is open, by logging into FTP using the spfactory account password (do not provide this password to ANUY customers)!

The patch file is located at: I:\New Released\Firmware_Software\1200-xxxx-xxxx\1200-SS04-1000.

The instructions to apply this patch (from the SecureSync factory test procedure) are listed below (This procedure is explaining how to FTP transfer the patch into SecureSync).

1. Copy F/W from controlled drive to local C:\TEMP.
2. From Start Menu on PC, select Run and type cmd <ENTER>.

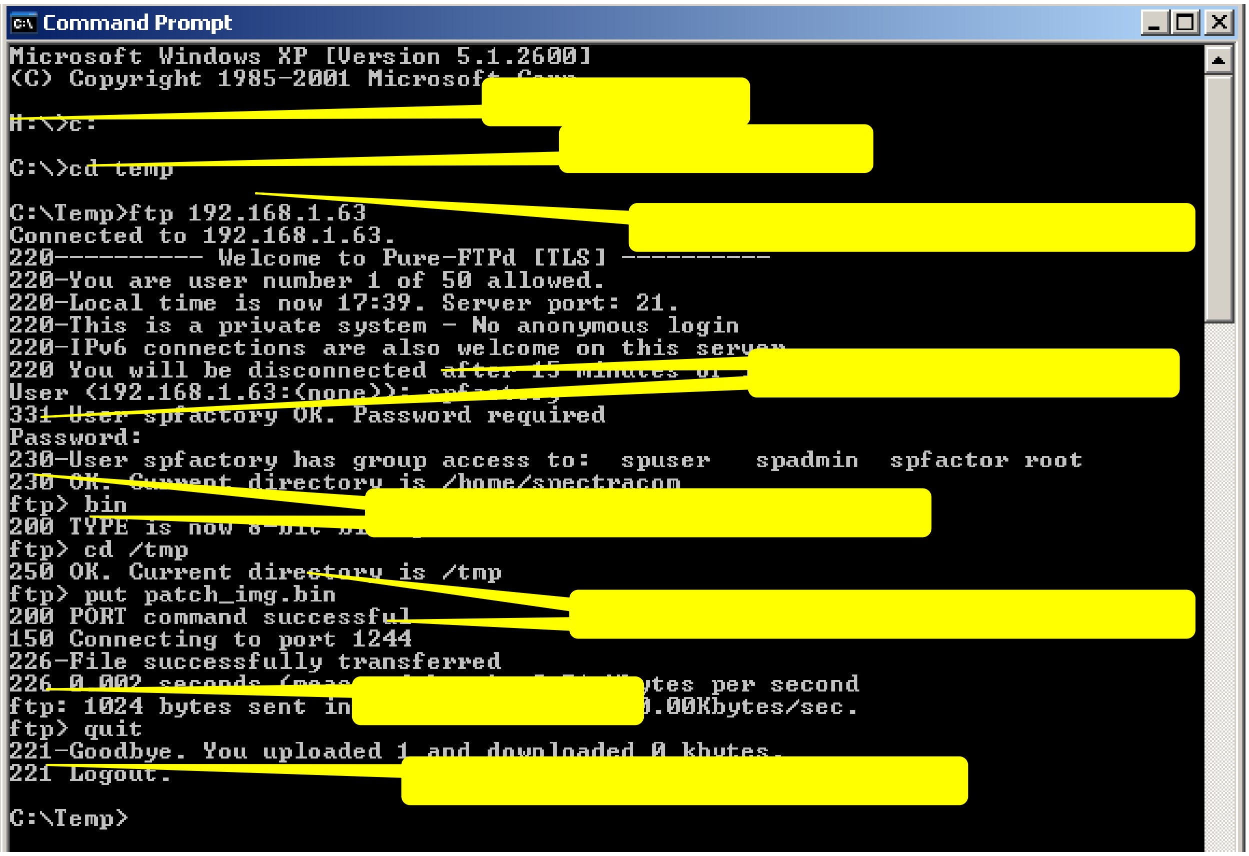


Run

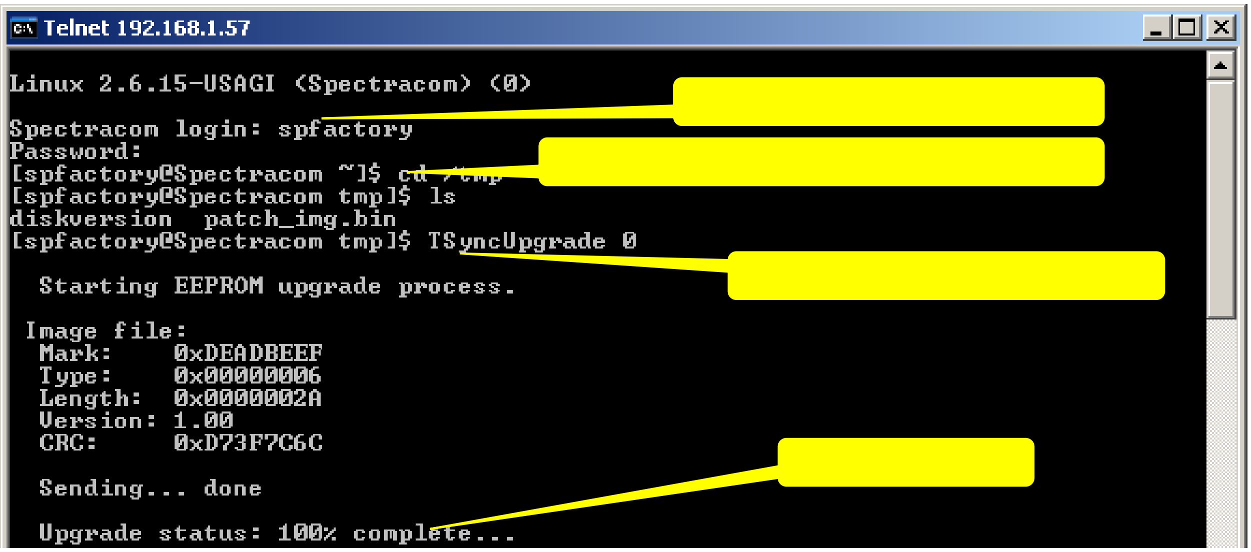
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

CAUTION: All patch files have same name. Ensure correct file is selected for installation or UUT will not function properly for customer. In some cases, the wrong file will not display any errors until sufficient data has been logged.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

H:\>c:

C:\>cd temp

C:\Temp>ftp 192.168.1.63
Connected to 192.168.1.63.
220---------- Welcome to Pure-FTPd [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 17:39. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server
220 You will be disconnected after 15 minutes of
User (192.168.1.63:(none)): spfactory
331 User spfactory OK. Password required
Password:
230-User spfactory has group access to:  spuser   spadmin  spfactor root
230 OK. Current directory is /home/spectracom
ftp> bin
200 TYPE is now 8-bit bi
ftp> cd /tmp
250 OK. Current directory is /tmp
ftp> put patch_img.bin
200 PORT command successful
150 Connecting to port 1244
226-File successfully transferred
226 0.002 seconds (meas                   ytes per second
ftp: 1024 bytes sent in                   .00Kbytes/sec.
ftp> quit
221-Goodbye. You uploaded 1 and downloaded 0 kbytes.
221 Logout.

C:\Temp>
```



```
Linux 2.6.15-USAGI (Spectracom) (0)

Spectracom login: spfactory
Password:
[spfactory@Spectracom ~]$ cd /tmp
[spfactory@Spectracom tmp]$ ls
diskversion  patch_img.bin
[spfactory@Spectracom tmp]$ TSyncUpgrade 0

  Starting EEPROM upgrade process.

 Image file:
  Mark:     0xDEADBEEF
  Type:     0x00000006
  Length:   0x0000002A
  Version:  1.00
  CRC:      0xD73F7C6C

  Sending... done

  Upgrade status: 100% complete...
```

3. Repeat Step 12 for any additional patch installs needed.
4. Reboot UUT by typing "**reboot;exit**" and allow UUT to reboot.
5. Using PROCOMM, select metakey **FACTORY** and **PASSWORD**.
6. Type **HALT** to power down UUT and disconnect all connections.

GPS receiver FAQs

Q. Does the SecureSync support manual entry of location/coordinates and altitude? (manual appears to indicate this is the case) If so, what format(s) can the coordinates be entered in (lat/lon, MGRS, etc.)?

A Yes. Info is entered as lat/lon/alt in degrees,minutes,seconds and meters.

Q We are considering use of the RS-232 NMEA output module. Assuming it outputs data reflective of the source currently used by the SecureSync. For example, if manual coordinates were entered rather than using GPS coordinates automatically, would the NMEA sentences include the manually entered coordinates in lieu of what would normally come from GPS?

A NMEA outputs are reflective of the current system information including position. Assuming the position information was set manually and accepted by the GPS reference/receiver, they would be used for the NMEA data. Refer to the SecureSync manual for the specific NMEA message formats provided.

**T1/E1 and AFNOR input time references

- refer to: ..\SecureSync Option Card information.pdf

**External 1PPS input (epp0)

- There is no 1PPS input on the base SecureSync (Option Card is required)
  - refer to ..\SecureSync Option Card information.pdf

- In summary: External 1PPS input requires the use of one or more installed 1PPS input Option cards, such as the following (Refer to: Specific Option Cards)
  - **Model 1204-01**: Single ended input
  - **Model 1204-02**: Balanced differential input
  - **Model 1204-28:** TTL single ended input
  - **Model 1204-1D**: non-isolated 1PPS input on a BNC connector
  - **Model 1204-2A**: Fiber Optic (1) 1PPS in and (2) 1PPS outputs
  - **Model 1204-2B**: Fiber Option (4) 1PPS outputs

1PPS Input impedance: 50 ohms

NTP/External 1PPS input requires a unique change to ntp.conf file via NTP Expert mode

- refer to refer to (in this doc): NTP/External PPS input

NTP/ External 1PPS input references

Important Notice: Using NTP and external PPS input as the selected references requires **NTP Expert mode be enabled** so the ntp.conf file can be manually edited. Failure to edit the ntp.conf file in Expert mode degrades the performance of the SecureSyncs outputs (including PTP) and the system does not take advantage of the external PPS accuracies.

for more info, refer to (in this doc): NTP/External PPS input

“Frequency 0” (Freq 0) external input frequency (such as 10 MHz input)

- Refer to ..\SecureSync Option Card information.pdf
- Frequencies of 1kHz to 10 MHz can be inputted into SecureSync via Option Cards
- Refer to Models 1204-01 and 1204-03 Option Cards in the SecureSync Option Card document
  - 1204-01: TTL in (single-ended input)
  - 1204-03: RS-485 n (Balanced input)

With Frequency input cards (such as 1204-01 or 1204-03), a 1 kHz to 10 MHz (sine or square wave) frequency can be inputted in order for SecureSync to generate a 1PPS from this signal.

**Reference Status table

Reference Status is viewable via browser:

A) web browser

User reference: Only "OK" (valid) after the time is set and it only remains valid if it becomes the selected reference.

NTP Reference: Only "Valid" right after NTP is qualified. It will only remain "Valid" if becomes the selected reference. Otherwise goes to "Not Valid" normally displayed.

Refer to Article
https://na8.salesforce.com/knowledge/publishing/articlePreview.apexp?id=kA0C00000008X5K&popup=true&pubstatus=d&preview=true

Note (22 Jul 13 KW) : Per Dave Sohn, the NTP Ready LED will blink green for one second every 60 seconds, when NTP is not the selected reference, at the moment NTP input is valid.

Note: NTP may periodically and temporarily select an NTP server (before switching back to the System Time reference, for example). In this scenario, NTP will go momentarily valid and then back to not valid again, because NTP is no longer synced to another NTP server.

- ➢ User and NTP references only go "valid" when they become the selected reference. They do not remain valid if they aren't selected (they remain not valid when they aren't selected. with NTP, it's the selected reference, when NTP selects another Time Server to be its selected reference (as displayed on the NTP-> Status page or in the NTP log).

NTP (and User" mode) are two unique input references that are only "valid" when they are selected as the input reference. When other references are the selected refer (Email Keith sent to customer 8/8/12)
ence (instead of NTP), "NTP" (and User) will remain "not valid" in the "Reference Status" table. The other configured higher Stratum NTP servers are verified each second as being available for selection, but their validity isn't "confirmed" until NTP needs to be selected as the input reference (either NTP is configured as the highest reference in the Reference Priority table, or all higher priority references have since been lost and NTP is the next highest available reference). Once NTP is selected, the Reference Status table will then show NTP as being valid.

As shown in this screenshot above, NTP is currently yellow and indicating "Not Valid". There is a reason that NTP remains yellow, instead of turning green like other references in this table do (such as GPS). Unlike many other input references, NTP (and User set time) only turn green when they are the selected input reference.

To see NTP go to "OK", and with GPS the only other input reference applied, you can easily and temporarily disable GPS input, to allow NTP to become the selected reference. Navigate to the Setup->
Reference Priority page of the browser. In the row that lists "GPS 0" in both columns, temporarily change the "State" field to "Disabled" and hit "Submit". This will disable GPS input, causing the next highest priority reference to be selected, until GPS input is enabled again. With NTP input being the next highest priority value, NTP will now be selected as the input reference. The Reference Status table should now show NTP as "OK" (in green).

Now go back to the Reference Priority table and re-enable the GPS row. Because GPS is a higher priority reference than NTP, it will automatically switch back to GPS being the selected reference. The Status table for NTP will go back to reporting its "Not Valid", unless GPS input is lost/declared not valid again.

PTP Reference: "PTP 0" will indicate "**Not Valid**" for one of two reasons.

1) When the PTP Module is configured as a PTP Master, this entry will always indicate "Not Valid".

   When the PTP module is configured as a PTP Slave, it will indicate "Not Valid" until the SecureSync has been synced to a PTP Master, which is connected to the Ethernet port of the PTP module (whether connected directly with a network cross-over cable or through network hubs and switches. Once connect to a PTP master, the PTP Module should achieve sync within about a minute of connecting the Ethernet cables.

2) With PTP 0 being enabled in the Input Reference Priority Table (Setup/ Reference Priority page of the web browser) and with it being the highest valid priority reference, SecureSync will declare its in sync using PTP as its selected reference.

**Time Sync / Holdover mode

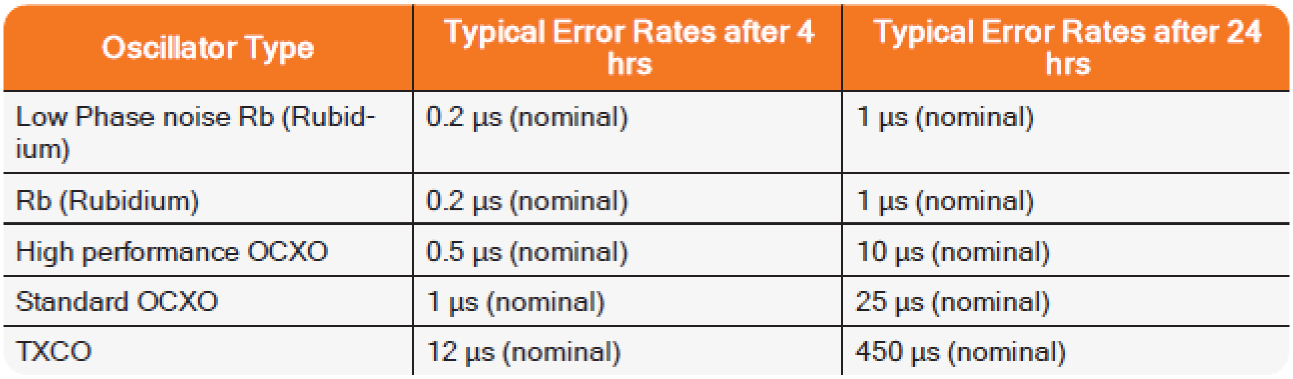
Holdover

- The SecureSync user guide has a good description of Holdover mode (search for “Holdover mode”)
- Holdover value is stored in the ktsif.conf file
- ktsif.conf file is located in home/spectracom/config directory

Delay to go into Holdover mode once satellite reception is lost

- Due to a past observed issue w/SAASM receivers dropping to 0 sats for like 1 second, since then there is an intentional delay of a few seconds after receiver reports tracking 0 sats before time server actually goes into Holdover mode. It no longer transitions into Holdover the moment the receiver reports tracking 0 sats.

Typical oscillator holdover rates (from the SecureSync manual)



Oscillator Type	Typical Error Rates after 4 hrs	Typical Error Rates after 24 hrs
Low Phase noise Rb (Rubidium)	0.2 µs (nominal)	1 µs (nominal)
Rb (Rubidium)	0.2 µs (nominal)	1 µs (nominal)
High performance OCXO	0.5 µs (nominal)	10 µs (nominal)
Standard OCXO	1 µs (nominal)	25 µs (nominal)
TXCO	12 µs (nominal)	450 µs (nominal)

Table 3-3: Estimated oscillator error rates during Holdover

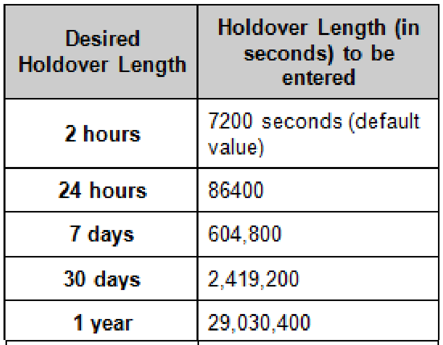
Configuring the length of Holdover Timeout

- The timeout value is configured in seconds with a valid range of 1 second up to 5 years. The default holdover period is 2 hours (7200 seconds).

From the SecureSync user guide:
Holdover Timeout is a user-configurable allowable time period in which SecureSync remains in Holdover mode before it declares loss of synchronization. Holdover Timeout can be adjusted according to personal requirements and preferences. The factory default Holdover period is 2 hours..

Note: Changes made to the Holdover Timeout always take effect immediately. If SecureSync is in holdover and the Holdover Timeout is changed to a value that is less than the current time period that SecureSync has been Holdover Mode, the unit will immediately transition to out of sync.

Holdover timeout is configured in “seconds”



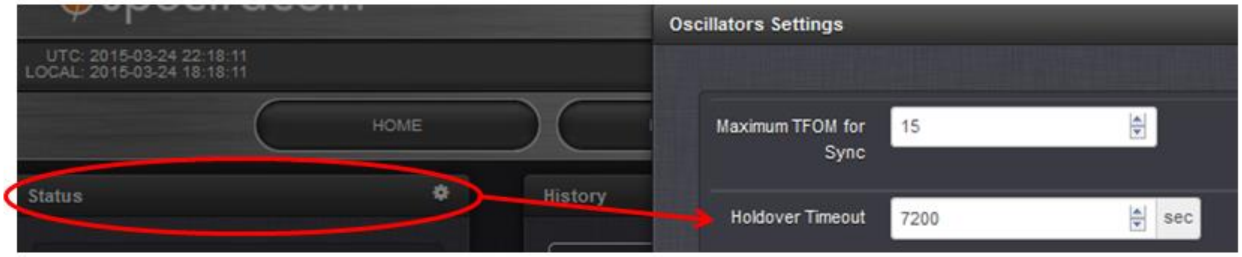
Desired Holdover Length	Holdover Length (in seconds) to be entered
2 hours	7200 seconds (default value)
24 hours	86400
7 days	604,800
30 days	2,419,200
1 year	29,030,400
5 years	10.450,944,010

A) Configure via the CLI

- ➢ Read current Holdover value: **SS_GetHoldoverTo 0** <enter> (in seconds)
- ➢ Change Holdover value**: SS_SetHoldoverTo 0 xxxx** <enter> (in seconds)

B) Configure via the web browser

The length of Holdover is configured in the ***Management*** -> ***Disciplining*** page and then clicking on the “gear” next to **“Status**” (in seconds)



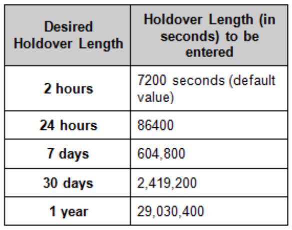
UTC: 2015-03-24 22:18:11
LOCAL: 2015-03-24 18:18:11

Maximum TFOM for Sync: 15

Holdover Timeout: 7200 sec

The value is configured in seconds with a valid range of 1 second up to 5 years. The default holdover period is 2 hours (7200 seconds).

When a valid input is connected, the SecureSync is in sync, and not in the holdover mode.   Once the input is lost, for a certain duration, the SecureSync will go into the holdover mode of operation. During this interval (default Holdover is 2 hours), the time is being derived from the SecureSync’s oscillator and so it also remains in the sync mode in addition to the holdover mode being active. If the external reference is restored before the holdover period expires, the SecureSync remains in sync, but holdover is turned off. If two hours elapses with the reference not returning, both sync and holdover are then removed.



Desired Holdover Length	Holdover Length (in seconds) to be entered
2 hours	7200 seconds (default value)
24 hours	86400
7 days	604,800
30 days	2,419,200
1 year	29,030,400

Nice detailed Holdover mode draft

Excellent point about the desire to appear as "synchronized" even upon loss of either unit's input reference(s). There is a built-in mode of operation just for this reason. This available mode of automatic operation is called the Holdover mode. Holdover mode starts when all its input references (as configured in the Reference Priority table) are lost or become not valid. Holdover mode ends when one of the following events occurs:
At least one input reference becomes present and valid again
The Holdover period times-out before at least one input reference becomes valid again
The unit power cycles (it doesn't boot back-up into Holdover mode, without first going back into Sync mode).
While it's in Holdover mode, the System Time (and therefore also NTP) is maintained by a 1PPS signal generated by the internal 10 MHz oscillator. In Holdover mode, the unit is treated as if it's still in full sync mode. The outputs are still fully useable while it's in Holdover mode.

The length of holdover is configured in the **Setup -> Disciplining** page of the web browser. The value is configured in seconds with a valid range of 1 second up to 5 years. The default holdover period is 2 hours (7200 seconds).

When a valid input is connected, the SecureSync is in sync, and not in the Holdover mode. Once all inputs are lost/ declared not valid (GPS tracking 0 satellites for instance, or the Slave no longer able to talk to the Master), the SecureSync will go into the Holdover mode of operation. During this interval (the default allotted Holdover period is 2 hours), the time is being derived from the SecureSync's internal oscillator and so it also remains in the sync mode in addition to the Holdover mode being active. If the external reference(s) is restored before the holdover period expires, the SecureSync remains in sync, but Holdover is turned off. If the Holdover period elapses with no reference(s) returning by then, both sync and Holdover modes are then removed.

The table below, from the SecureSync user manual, provides the conversion of commonly desired Holdover periods into seconds.

Desired Holdover Length	Holdover Length (in seconds) to be entered
2 hours	7200 seconds (default value)
24 hours	86400
7 days	604,800
30 days	2,419,200
1 year	29,030,400

The better the stability of the 10 MHz oscillator type installed, the more accurately maintained the System Time will be while in the Holdover mode. For examples, the typical time drift during Holdover of a TCXO oscillator is about 5 seconds/month, for the OCXO oscillator is about 52 milliseconds/month or for the Rubidium oscillator is about 130 microseconds/month. Using these typical values, and based upon your typical time accuracy requirements, they can then be used to calculate how much of a Holdover mode period can be tolerated, before loss of sync occurs to prevent the outputs from being useable.

"Time Sync" is true when:

- ➢ The SecureSync is in full sync with one of its input references (In this state, "Holdover" is false).
- ➢ The SecureSync is in Holdover mode (all input references are lost, but the Holdover period has not yet expired). (In this state, "Holdover" is also true).

Time Sync is false when:

1) All input references are no longer present/valid and the Holdover mode has since expired. (In this state, "Holdover" is also false).
2) The unit first boots-up and has not yet synced to any input reference. (In this state, "Holdover" is also false).

"**Time Sync" is true when:**

- The SecureSync is in full sync with one of its input references (In this state, “Holdover” is false).
- The SecureSync is in Holdover mode (all input references are lost, but the Holdover period has not yet expired). (In this state, “Holdover” is also true).

Time Sync is false when:

1) All input references are no longer present/valid and the Holdover mode has since expired. (In this state, “Holdover” is also false).
2) The unit first boots-up and has not yet synced to any input reference. (In this state, “Holdover” is also false).

Holdover mode

Important note: Drift is non-linear!

Email from Dave Sohn (17 Oct 2013) Drift in holdover is not linear as implied here. The phase drift will be exponential as the frequency drifts. So, no oscillator will provide <1ms per day indefinitely. For example, the TSync OCXO will provide less than 1ms per day for around 6-7 days, but more than that afterwards. Also, all our models are based on good starting values starting out from GPS synchronization, which won’t be available here.

Email from Tony DiFlorio to a potential customer looking for 1ms/day accuracies A couple of other ideas to help you: You could use a portable (battery operated) GPS synchronization device to provide re-synchronization to the TSync-PCIe-Opt-OCXO card, such as our model GPS-12/12R (see attached). This re-synchronization would have to be done every few days though to maintain the TSync-PCIe-OCXO to <1ms per day of drift. Or, you might be able to use our popular “SecureSync”, rack mounted GPS Synchronization system (see attached) with a Rubidium internal oscillator. This depends on whether you must have specific features that only a Bus-Level card can provide. Using our SecureSync with a Rubidium internal oscillator will provide the holdover accuracy you are looking for, over a much longer period of time (almost indefinitely).

The holdover mode begins when all input references are considered invalid and ends when either at least one input is considered valid or until the holdover period expires.

Holdover FAQs

Q Why is the default holdover value 2 hours

A As for 7200 seconds of default holdover- this equates to 2 hours of holdover, which just happened to be the same value as the "worst-case" NetClock (With TCXO oscillator installed). Because the default Holdover value is not linked to the type of on-board oscillator, Engineering went with the default of the NetClock with TCXO being 2 hours of holdover. This value is customer configurable for up to 5 years.

Q Are there any holdover performance specifications for the high-stability Rubidium internal clock option? We have a specific requirement of no more than 1 microsecond of drift per day when operating on internal clock for timing.

A Holdover specs are provided in the datasheet. The standard Rubidium holdover spec for 1 day is 2us.

Known potential issue with GB-Gram (MPE-S) SAASM receiver going into Holdover for 1 second

1. **MPE-S sometimes enters holdover at 12:01-12:02 UTC**
   - Refer to MANTIS Case 2641

**Local interference, GPS jamming and GPS Spoofing

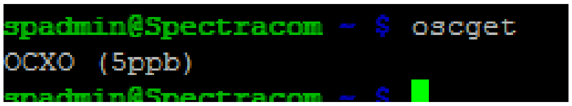
- Refer to: “GPS Spoofing and GPS jamming” in the “Custserviceassistance” PDF document

Oscillators/ disciplining to 1PPS input reference/TFOM/1PPS phase error

**Types of available Oscillators/installed oscillator type

Which type oscillator is installed?

A) CLI command to determine type of oscillator installed: oscget <enter> or XO_GetOscType 0



```
spadmin@Spectracom ~ $ oscget
OCXO (5ppb)
spadmin@Spectracom ~ $
```

B) Web browser report of oscillator installed

The installed oscillator type is reported in the "**Oscillator Type**" field located in the top-left corner of the ***Management*** -> ***Disciplining*** page.

Types of Oscillators that can be installed

1) Low Phase Noise Rubidium" or "Low Phase Noise Rb" (Y100R-0002-RC04) (SecureSync–x5x, such as SecureSync-051 or SecureSync-057 for examples)

- Displayed in browser as: "**LPN Rubidium (.1ppb**)"
- Consists of the Low phase noise OCXO oscillator combined with the SpectraTime SRO-100 Rubidium oscillator

~~(9/28/12 design in progress) Will~~ provides the low phase noise specs of an OCXO combined with the greater stability of installed Rb oscillator. The Rb oscillator will lock to GPS and output a very stable 1PPS to discipline the OCXO oscillator.

Our P/N for the two oscillators combined: Y100R-0002-RC04

- "**Y100R-0002-RC04**" consists of two combined internal oscillators:

1. SpectraTime SRO-100 Rb oscillator

- **Refer to**: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\10 MHz Oscillators\Rb oscillator
- **Our PN**: **Y100R-0002-RC03** (see additional info further below)

2. Morion MV197 low phase noise OCXO

- see info further below for "**LPN OCXO"**
- **Our P/N**: **Y100R-0002-PH10**

2) Standard Rubidium oscillator (SpectraTime SRO-100) (also the RB osc for Harris) (SecureSync– x3y, such as SecureSync-031, SecureSync-033 or SecureSync-037 for examples)

- Displayed in browser as (I believe): "**Rbxo (.5ppb)"**
- "**Option 4**" in Models 9483 and 9489
- Uses SRO-100 Rb oscillator from SpectraTime (\\Rocfnp01\idrivedata\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\10 MHz Oscillators\Rb oscillator)
  - **Our P/N:** Y100R-0002-RC03
  - **MFG: SpectraTime**

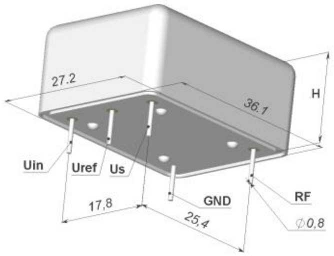
- MFG. P/N and description: **SRO-100/10M/12V/NO60/F/S/E**
  - **In Arena at**: https://app.bom.com/items/detail-spec?item_id=1202848069&version_id=10268167148

- link to SRO-100 manual: http://www.spectratime.com/documents/iSync_SRO-100%20SynClock%20Manual_140522.pdf
- Link to SRO-100 data sheet: http://www.spectratime.com/products/isync/gps-disciplined/SRO-100/
- Also refer to: "SRO-100 Rubidium oscillators" in the Customerserviceassistance document

3) HP (high Performance) Low phase noise OCXO oscillator (LPN OCXO) (P/N: SecureSync– x2y, such as SecureSync-021, SecureSync-023 or SecureSync-027 for examples)

Note: Low phase noise oscillator is not available with the Models 9483 and 9489

- Displayed in browser as: "**OCXO (1PPB)**"
- Used by itself or combined with Rb osc for the low phase noise Rb configuration
- MFG info for low phase noise OCXO
  - **Our P/N:** Y100R-0002-PH10
  - **MFG**: Morion Inc (in Saint-Petersburg, Russia) http://www.morion.com.ru/
  - **Model** XO01273M (made-to-specs for Spectracom. Per Arena, appears it's a mod of the MV-197 OCXO but its not labelled as MV-197)



  - **Description:** OCXO,TH,10MHz,12V,1PPB,EURO,-20C,90C, Low Aging
- Data sheet also in Arena:
  - **In Arena at:** https://app.bom.com/items/detail-sourcing?item_id=1202848068&version_id=10228404878&orb_msg_single_search_p=1&redirect_seqno=7252161677

Note from Dave Sohn: The low phase noise MV197 is marked **XO01273M**.

- Using this LPN oscillator with a 5MHz (1204-08) or 1MHz (1204-26) output card
- Note this LPN oscillator provides low phase noise 10 MHz outputs (as specified in the SecureSync data sheet) for the base output and 1204-1C 10MHz Option Cards. But these same 10MHz specs DO NOT apply to the 5 MHZ or 1MHz outputs. Because of the way these other signals are derived, their phase noise is inherently higher.

4) Standard OCXO oscillator for SecureSyncs only (not NetClocks) (PN: SecureSync– x1y such as SecureSync-011 or SecureSync-013 for examples)

- Displayed in browser as: “**OCXO (5ppb)”**
- **Our P/N**: Y100R-0002-PH05
- **MFG**: Morion Inc (in Saint-Petersburg, Russia) http://www.morion.com.ru/
- **MFG P/N** X000980M Rev 2 (it’s apparently a MV-197 made-to-specs for Spectracom)
- **Description:** VCOCXO,TH,10MHz,12V,5PPB,EUROPK,-20C,90C
- **Part is labeled as “MV-197”**
- **in Arena at**: https://app.bom.com/items/detail-spec?item_id=1202848066&version_id=10228404838

5) TCXO oscillator (P/N SecureSync– x0y such as SecureSync-001, SecureSync-003 or SecureSync-011 for examples)

- Available with SecureSync as well as the Models 9483 and 9489
- Displayed in browser as: “??

Our P/N for this external oscillator: Y100R-0002-TS01

Mfg. P/N: refer to Arena link further below

Description: VCTCXO, SM, 10.000MHz, 3.3V, 1PPM -40C- 85C, 5x7mm

- **Our Spec sheet:** https://files.bom.com/download/tbvAbexlHEgxf4dhx2u5EEJfjz9mWz1z/xrpajljoubsimkfwogqxfhygszqrbfub/Y100R-0002-PH09%20SCD%20Rev%20C.pdf
- In **Arena at:** https://app.bom.com/items/detail-spec?item_id=1202848067&version_id=10228404868&orb_msg_single_search_p=1&redirect_seqno=7251889364

6) Raytheon AMDR specialL 1200 LPN, Wenzel g-Compensated Oscillator SecureSync (SecureSync-R563)

- For more info on Raytheon AMDR SecureSync special, refer to: I:\Customer Service\Customers\Raytheon AMDR project
- See Tim Tetreault for any specifics regarding this special SecureSync master oscillator.

A) "-2 Config" (2nd generation)

- SecureSync R563,15,06,15,3B,15,00
- **SecureSync P/N purchased: 1200-9013-0601** (in Arena): **https://app.bom.com/items/detail-spec?item_id=1228737122&version_id=10956131348&**

B) "-4 Config" (2nd generation)

- Fiber PTP, Single mode fiber (SecureSync R563,15,06,15,3B,15,00)
- **SecureSync P/N purchased: 1200-9029-0601** (in Arena): https://app.bom.com/items/detail-spec?item_id=1238722969&version_id=10956131378&

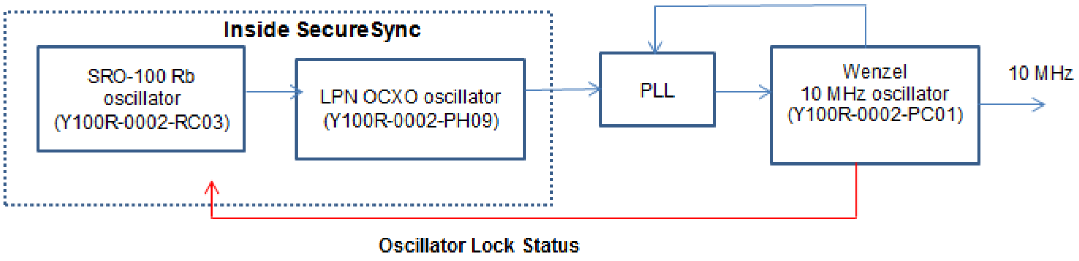
C) "Original configuration"

- **SecureSync P/N purchased:** 1200-R007-0601 (in Arena) https://app.bom.com/items/detail-spec?item_id=1204952326&version_id=10291838828

Has three (3) 10 MHz Oscillators: Low phase noise 10 MHz in a high G environment on ships

- One (1) internal SpectraTime SRO-100 Rubidium oscillator
- One (1) internal Morian 10 MHz OCXO oscillator
- One (1) External osc from Wenzel that is specialized for High Gs (details for this oscillator below):

- **Our P/N for this external 10 MHz oscillator from Wenzel:** Y100R-0002-PC01
- **In Arena at:** https://app.bom.com/items/detail-attach?item_id=1204722998&version_id=10245567288&orb_msg_single_search_p=1&redirect_seqno=7327495950
  - VCOCXO,CM,10MHz,12V,5x10-10,5x6x2.75",20C to 35C
  - **MFG. P/N** 28056d

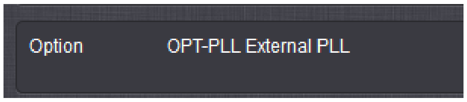

Inside SecureSync
SRO-100 Rb oscillator (Y100R-0002-RC03)
LPN OCXO oscillator (Y100R-0002-PH09)
PLL
Wenzel 10 MHz oscillator (Y100R-0002-PC01)
10 MHz
Oscillator Lock Status

A. **Wenzel Low-G 10 MHz-SC Citrine Crystal Oscillator (Hughes SecureSync, for example)**

- ➢ P/N: Y100R-0002-PC02 (in PLM) https://app.bom.com/items/detail-spec?item_id=1211979123&version_id=10370425508&orb_msg_single_search_p=1&redirect_seqno=7539269985
- ➢ Very low phase noise / low vibration (low G) oscillator for Hughes special SecureSync (refer to “Specials” section in this document for more info on this Hughes SecureSync
- ➢ Internal oscillator (inside the SecureSync chassis)

Lock Status for Raytheon AMDR special SecureSync (our Rb oscillator locking a Wenzel OCXO Oscillator very low phase noise OCXO)

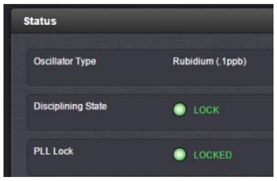
- ➢ Referred to as “Opt-PLL External PLL”
- ➢ Enabled with license file



Option OPT-PLL External PLL

- ➢ Available starting in version 5.2.1
- ➢ Only viewable in the Raytheon AMDR special SecureSyncs (Management -> Disciplining, under “Status”

Email from Tim Tetreault (~13 July 2015) PLL status is available visibly within the web UI on the MANAGEMENT -> Disciplining page under the “Status” section like below.

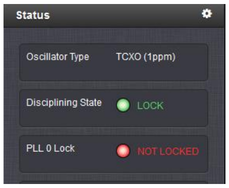


Status

Oscillator Type Rubidium (.1ppb)

Disciplining State ● LOCK

PLL Lock ● LOCKED



Status

Oscillator Type TCXO (1ppm)

Disciplining State ● LOCK

PLL 0 Lock ● NOT LOCKED

The PLL status is also rolled up into our frequency error condition, which triggers notifications through our standard mechanisms (UI, logs, SNMP, email, etc.)

Another email from Tim Tetreault (9/21/2018) Did we get any background info on this unit from Raytheon? Was it working and then stopped or never worked?
Did they give you any logs that we can look at that show the “Lock” status? I think that info was in the System logs.

The “Lock” detect is very straight forward. A Licenses installed in the unit enables it. If the Licenses was not installed, it would not report any information about the lock.

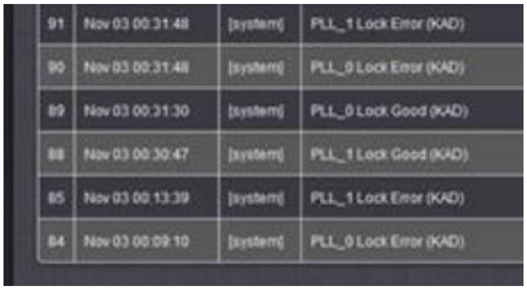
If we don’t see anything in the logs, they might need to send us the units back to fix. Before making that decision, have them answer the questions above.

Log entries for Wenzel PLL lock status (in osc.log)

- Refer to the CGU manual addendum for Hughes (1200-5000-C050) in Arena at: https://app.bom.com/items/detail-spec?item_id=1217182411&version_id=10446313248&orb_msg_single_search_p=1

  PLL_0 Lock Error (KAD)
  PLL_0 Lock Good (KAD)
  PLL_1 Lock Error (KAD)
  PLL_1 Lock Good (KAD)

Example entries in osc.log



```
91   Nov 03 00:31:48   [system]   PLL_1 Lock Error (KAD)
90   Nov 03 00:31:48   [system]   PLL_0 Lock Error (KAD)
89   Nov 03 00:31:30   [system]   PLL_0 Lock Good (KAD)
88   Nov 03 00:30:47   [system]   PLL_1 Lock Good (KAD)
85   Nov 03 00:13:39   [system]   PLL_1 Lock Error (KAD)
84   Nov 03 00:09:10   [system]   PLL_0 Lock Error (KAD)
```

Issue: glitches in 10 MHz oscillator (typically associated with OCXO) output causes LED time to stop counting up. LCD display is fine.

- Refer to Mantis case 2916 (except below)

Some SecureSyncs/ in field are locking up/freezing/losing comms until rebooted.

This was reproduced here with an RMA SecureSync on Burn-in/ Engineering found 10 10 MHz output from the OCXO was missing until unit was rebooted. Apparently, even a momentary glitch in the 10 MHz oscillator output sent to the FPGA can adversely affect the operation of the unit until its rebooted (time on front panel display freezes, sluggish operation, etc).

All but one unit has an OCXO. The other one has a TCXO.

- If 10 MHz into FPGA glitches, KTS can't recover without a reboot
- Initial intentions were to add a log entry when it happens and then eventually add a second source of 10MHz into KTS in case the main 10 MHz is temporarily lost.
- As of version 5.2.1, two System log entries are associated with this issue (more info on this below). No fix has been implemented yet to restore operation if it happens (10 MHz input is restored). So if this issue happens, it still won't recover on its own. Power cycle (or possibly reboot) required to restore ops.

Associated Alarm log entries for loss of 10 MHz

major alarm ="Timing System Hardware Error".

Associated Kern log entries for loss of 10 MHz (versions 5.2.0 and above)

- Disabling lock debugging due to kernel taint
- pps pps0: tsyncpci PPS source unregistered
- Spectracom TSync Timing Board removed

Associated System log entries for loss of 10 MHz (versions 5.2.0 and above)

- Starting in version 5.2.0. System Log entries will be asserted if the10 MHz input to the FPGA is lost.
- Look for the following entries in the System Log

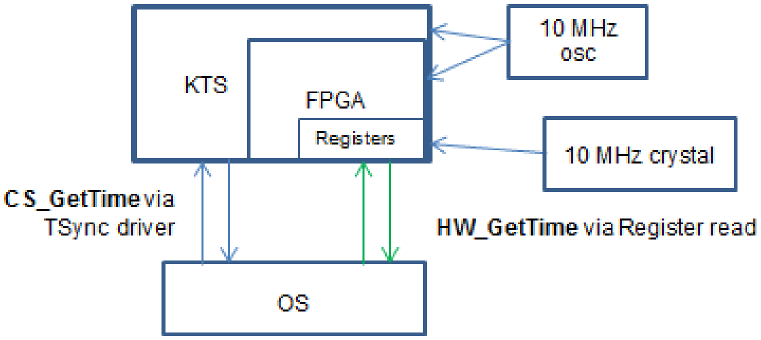
- Timing System Hardware error
- Failed CS_GetTime (KAD)

Then look for either:

- Passed HW_GetTime (possible oscillator error) (KAD) OR

- Failed HW_GetTime (probably FPGA failure)

Details



1. If there are at least five (5) "Failed to read alarm info from KTS (KAD)…" entries in the System log, a "**CS_GetTime"** call is sent to KTS to see if KTS is still communicating via the TSync driver.

    - If there are less than 5 entries, nothing happens and the counter is reset
    - If there are at least 5 entries, the Tsync driver **will** be unloaded (reboot will be necessary to restore operation)

    Associated kern.log entries for driver unloading:

    - pps pps0: tsyncpci PPS source unregistered
    - Spectracom TSync Timing Board removed

2. When a "**HW_GetTime" call** is sent to the FPGA registers to see if the FPGA is communicating.
    - If this call passes, the registers are still able to respond (if KTS isn't running, the same data may remain in the registers). This confirms the TSync driver is still running normally.
    - If this call fails, the registers are not able to provide any data whatsoever. This means either bad FPGA or Tsync driver not running.
3. If both time calls fails, the issue could be with the TSync driver, so it's unloaded (and remains unloaded) to allow the Network Processor to continue working. Reloading the Tsync driver requires the unit be rebooted.
4. If both calls fail, the oscillator likely glitched, causing both FPGA and KTS to stop responding.
5. If **CS_GetTime** fails but **HW_GetTime** passes, FPGA is still working.

**Rubidium oscillator-associated alarms

- ➢ Also refer to: "SRO-100 Rubidium oscillators" in the Customerserviceassistance document

Alarms associated with likely hardware failure of Rb oscillator

- ➢ Are there "**Rb lamp error**", "**Rb peak voltage error**" or "**Rb fault detected**" messages in the Timing Log? This will indicate a failed Rubidium oscillator module.

1) Rb Peak voltage error

Note: Archive software versions 5.0.0 and below reported all alarms associated with the Rubidium oscillator as "**Rb peak voltage error**" alarms. This was noticed just prior to the version 5.0.1 release, so version 5.0.1 now differentiates each Rb oscillator alarm to indicate what the real issue with the Rb oscillator.

Q. (log entry from Morgan Stanley Rb-based SecureSync) **Rb peak voltage error** (val=6, min=51, max=255)
A (1/25/12) Mark Goodlein emailed SpectraTime with: We have a customer with one of our SecureSync products, in which we use an SRO-100 Rubidium oscillator module. Recently, this customer saw some behavior that was questionable and

would like to know if they should be concerned about it.

Our software that communicates with the SRO requests the internal parameters using the ‘M’ command once a second. It then compares the values returned with boundary values to detect if something is out of the ordinary, in which case we log the condition. This customers unit had been running for over 150 days then the following log messages were recorded for 5 seconds then went away and no more have been logged since then.

```
2011 357 21:26:54 000 Rb peak voltage error (val=6, min=51, max=255)
2011 357 21:26:55 000 Rb peak voltage error (val=7, min=51, max=255)
2011 357 21:26:56 000 Rb peak voltage error (val=7, min=51, max=255)
2011 357 21:26:57 000 Rb peak voltage error (val=9, min=51, max=255)
2011 357 21:26:58 000 Rb peak voltage error (val=35, min=51, max=255)
```

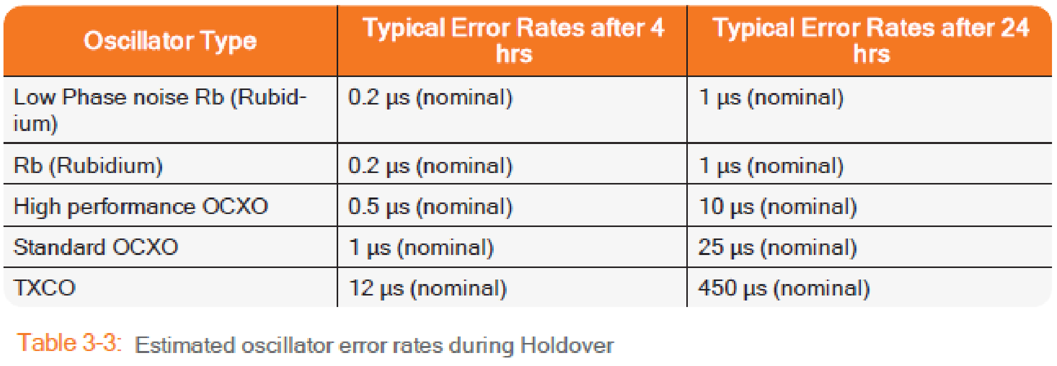
The manual for the SRO indicates that this signal stabilizes to between 1 and 5 volts after warm-up, so these are the boundary conditions that our software checks for. In this case, the voltage dipped below 1V (almost reaching 0V) for 5 seconds. This is the first case of an event like this that has ever been reported to us from a customer.

Is this event something to be concerned about? Does it indicate a condition that may result in failure?

**Oscillator free-run/Holdover specs

- Refer to SecureSync data sheet for most recent oscillator specs ("SecureSync 3 page"):

From the 1200 SecureSync user manual



Oscillator Type	Typical Error Rates after 4 hrs	Typical Error Rates after 24 hrs
Low Phase noise Rb (Rubidium)	0.2 µs (nominal)	1 µs (nominal)
Rb (Rubidium)	0.2 µs (nominal)	1 µs (nominal)
High performance OCXO	0.5 µs (nominal)	10 µs (nominal)
Standard OCXO	1 µs (nominal)	25 µs (nominal)
TXCO	12 µs (nominal)	450 µs (nominal)

Table 3-3: Estimated oscillator error rates during Holdover

From the 1200 SecureSync data sheet

Holdover (constant temp after 2 weeks of GPS lock)

	TCXO (nominal)	OCXO (nominal)	Low Phase Noise OCXO (nominal)	Rubidium (nominal)	Low Phase Noise Rubidium (nominal)
After 4 hours	12 microseconds	1 microsecond	0.5 microseconds	0.2 microseconds	0.2 microseconds
After 24 hours	450 microseconds	25 microseconds	10 microseconds	1 microsecond	1 microsecond
after 7 days	3150 microseconds (3.1milliseconds)	175 microseconds	70 microseconds	7 microseconds	7 microseconds
after 30 days (nominal)	13,950 microseconds	775 microseconds	310 microseconds	31 microseconds	31 microseconds

Important Note: The 1PPS drift is not linear. It ramps up, as the oscillator ages. You can't just multiply the numbers above by the desired amount of lapsed time to determine how far off it will be. Dave Sohn has a Model they use to calculate time drift over a given amount of time.

Link to Engineering's simulated OCXO/TCXO oscillator drift graphs over an extended periods of time: I:\Engineering\1PPS drift simulations for various Spectracom oscillators

A) Low phase noise OCXO Oscillators

(From Dave Sohn) Estimate for low phase noise OCXO holdover at constant temperature (after 2 weeks with GPS lock)

Days	Drift
1	10 us
2	40 us
3	80 us
7	430 us

B) Rubidium Oscillators

1PPS holdover estimates for Rubidium oscillators at constant temperature after 2 weeks of GPS lock

Days	**1PPS Phase Error**
1	2us
7	11us
14	30us
30	95us

Here are results if you had a temperature change of 10 degrees C at a rate of 1 degree per hour over the same holdover time periods.

Days	**1PPS Phase Error**
1	3us
7	25us
14	55us

Sonet/Telecom Stratum hierarchy levels for 1544/2048 kHz, T1/DS1 and E1 outputs

- Such as Stratum 1 and Stratum 3E
- Refer to “Stratum timing for 1544/2048 kHz, T1/DS1 and E1 outputs” in the T1/E1 section of the SecureSync Option Card info document for more info.

OCXO comparison chart

- The following is a link to a chart which shows accuracy when locked and free run mode:

  I:\Engineering\Products\ProductPerformanceSpecs5.xls

Holdover for Simulcast specs (time to drift 5 microseconds)

- Per Ed, certain Simulcast systems can tolerate up to **5 microseconds** of 1PPS drift before issues start to happen
  - Customers may ask how long can “Holdver timeout be set to. while maintaining less than 5 microseconds of drift (refer to Salesforce Case 177534)
  - Ed’s recommendations are to set Holdover to 5 **days for a Rubidiu**m oscillator or **5 hours with an OCXO**

**Oscillator Calibration/Recalibrate checkbox

Two types of “H/S’ cal data logs are asserted into the Oscillator logs:

- “New Cal Value”: only happens at factory or if a patch is applied to reset it. This entry can be eventually overwritten.

- "Saved Cal Value": the previous calculated value stored in the EEPROM.

A) TCXO/OXCXO oscillator calibration

- TCXO/OXCXO oscillators are calibrated first time they are powered-up/synced. This cal data is then stored in a file.

TCXO/OCXO oscillator recalibrate in the field (BAD/questionable oscillator calibration/Recalibrate checkbox)

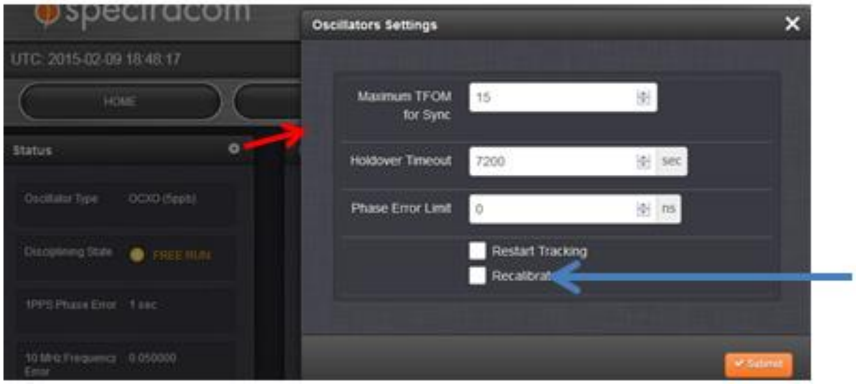
- Refer to the Word document in the folder: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\10 MHz Oscillators\Recalibrate a TCXO or OCXO osc

A) Versions 5.1.7 and below (the "Recalibrate: checkbox is not available)

- For TCXO/OCXO oscillators only
- Requires remote access to the spfactory account.
- If a bad occurs requires an EEPROM patch update file (patch_img.bin) be uploaded by a customer, Then we need to remote ssh in to issue a command that applies the patch. Then the unit can be rebooted.
  - With Software versions 5.1.7 and below, the cal value needs to be deleted while logged in as root or spfactory. Then, the cal process is performed again, once the system boots again (might be able to remotely access the unit here for our Engineering team to reset the value for them)

B) "Recalibrate" checkbox

- For TCXO/OCXO oscillators only
- This checkbox (**Management** -> **Disciplining** page of the browser) allows the oscillator to be recalibrated by a customer without the need to run a patch or login as spfactory mode.
  - **Note**: This checkbox sends the following newer CLI command: **XO_SetMode 0 3** to recal the oscillator.



Oscillators Settings

UTC: 2015-02-09 18:48:17

Status

Oscillator Type OCXO (5ppb)

Disciplining State FREE RUN

1PPS Phase Error 1 sec

10 MHz Frequency Error 0.050000

Maximum TFOM for Sync: 15

Holdover Timeout: 7200 sec

Phase Error Limit: 0 ns

□ Restart Tracking

□ Recalibrate

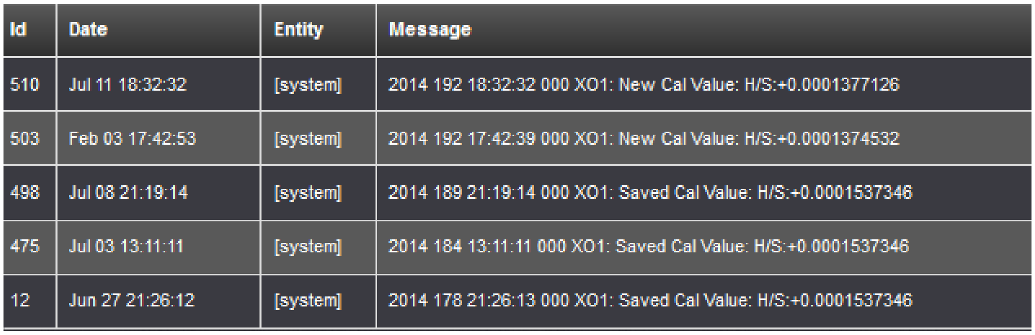
- If a bad oscillator calibration happens to occurs, it won't run the cal again:
- With Software versions 5.2.0 and above, can perform a "Recalibrate"
- Make sure SecureSync is in full sync (not Holdover) with a good 1PPS referene (such as GPS or IRIG from a very stable generator).

"Recalibrate" button with a Rubidium or Low phase noise Rubidium oscillator

- Recalibrate button shouldn't have any effect on a standard rubidium unit

- Low Phase Noise Rubidium consists of an OCXO that locks to a standard Rubidium after each boot-up. This button shouldn't affect the Rb oscillator lock, but will affect the OCXO lock to the Rubidium oscillator, until the SecureSync is rebooted again. If the recalibrate button is pressed, reboot the SecureSync to restore OCXO lock to the standard Rb oscillator.

Typical "H/S" cal values (from a standad OCXO oscillator) as obtained by searching an Oscillator log for "H/S" entries



Id	Date	Entity	Message
510	Jul 11 18:32:32	[system]	2014 192 18:32:32 000 XO1: New Cal Value: H/S:+0.0001377126
503	Feb 03 17:42:53	[system]	2014 192 17:42:39 000 XO1: New Cal Value: H/S:+0.0001374532
498	Jul 08 21:19:14	[system]	2014 189 21:19:14 000 XO1: Saved Cal Value: H/S:+0.0001537346
475	Jul 03 13:11:11	[system]	2014 184 13:11:11 000 XO1: Saved Cal Value: H/S:+0.0001537346
12	Jun 27 21:26:12	[system]	2014 178 21:26:13 000 XO1: Saved Cal Value: H/S:+0.0001537346

Oscillator Calibration log entries (Tools -> Logs page of the browser, Oscillator tab)

Starting in version 4.8.6 (June 2012) Oscillator calibration value (which is stored in EEPROM during manufacturing) are reported in the Oscillator log after every power-up.

Example log entries below:

Valid / expected log entries

```
Jun 29 16:07:02 Spectracom spectracom: [system] 2012 181 16:07:02 000 Saved Cal Value: H/S:+0.000150
Jun 29 16:07:02 Spectracom spectracom: [system] 2012 181 16:07:02 000 Initial DAC Setting: 0x8639
Jun 29 16:04:29 Spectracom spectracom: [system] 2012 181 16:04:29 000 New DAC Setting: 0x863D
Jun 29 16:03:39 Spectracom spectracom: [system] 2012 181 16:03:39 000 New DAC Setting: 0x8630
Jun 29 16:02:49 Spectracom spectracom: [system] 2012 181 16:02:49 000 New DAC Setting: 0x8635
```

Bad / invalid log entries

```
Jun 27 21:41:07 Spectracom spectracom: [system] 2012 179 21:41:06 000 New DAC Setting: 0xFFFF
Jun 27 21:39:08 Spectracom spectracom: [system] 2012 179 21:39:07 000 Saved Cal Value: H/S:+0.000000
Jun 27 21:39:08 Spectracom spectracom: [system] 2012 179 21:39:07 000 Initial DAC Setting: 0xA670
Jun 27 21:18:39 Spectracom spectracom: [system] 2012 179 21:18:39 000 Frequency error recalculated: 05.112250
```

Note: H/S value should not be displayed as all 0's. This indicates a bad calibration occurred. Oscillator Alarm will likely be asserted in the Alarms log. Cal needs to be set to all 0.s which will cause the calibration to be re-performed.

Resolution for this known potential issue with 4.8.9 having bad cal data out of the box

- Refer to Michael Cribbs, Salesforce case 11202
- Symptoms are not syncing to GPS (even with good reception) much higher TFOM than usual, and oscillator log containing entry of "XO1: New Cal Value: H/S:+0.0000000000.
- Flag record as out of box failure.
- Fixes are to

Version 5.2.0- Perform a "**Recalibrate**" (**Management** - > **Disciplining** page).

Versions 5.1.7 and below:

1) Update to 5.2.0 and then perform a "**Recalibrate**"(**Management** - > **Disciplining** page).
2) Return it to us
3) An engineer to remote login as root,
4) Or best method for field fix – either upgrade to v5.0.0 or higher (Not downgrade to 4.8.8 and clean and then upgrade back to 4.8.9 anytime thereafter). If they update to 5.0.0 or higher, it will cal the oscillator after getting valid GPS input.

Note that it's much easier to upgrade to v5.x.x than to downgrade to 4.8.8, because you don't have to clean, and alleviates the need to upgrade back to 4.8.9 anytime thereafter.

H/S being all 0's with units that shipped with 4.8.9 is a potential issue that can occur. It will cause higher than expected TFOM (such as 10) and trouble syncing, even with good GPS.

Per the draft email for this condition (also below in red), besides an engineer logging remotely into root,or needing for it to be sent back to us for re-cal, the best fix in the field is to downgrade from 4.8.9 to 4.8.8, perform a clean configs (which erases the cal value from the file) let it sync back up for a couple of hours. Then it can be upgraded back to v4.8.9 anytime thereafter (the cal value persists through normal upgrades, but is reset on a clean.

FYI- during the Manufacturing process, a one-time self-calibration of the oscillator is performed to determine its individual Hertz Range for disciplining purposes. Due to a step that was performed in manufacturing, the cal data was inadvertently lost just prior to shipment. So the unit currently has a Hertz Range of 0, which is adversely affecting the oscillator disciplining and its ability to lock/declare sync to GPS (as you are observing).

We can assign an RMA Number for the NetClock to be returned for this self-cal to be performed again, if you prefer. However, with just a software downgrade and then a software upgrade, this process can also be performed in the field, without the need to return it to us. Downgrading it from version 4.8.9 to 4.8.8 and letting it run for a couple of hours will allow the oscillator to be re-calibrated. Anytime thereafter, it can be upgraded back to 4.8.9 again, with this issue resolved.

If you prefer to send it back to us, let me know and I will assign an RMA Number for it to be returned to us for the recal. But in case you would rather not have to return it and want to perform the software "upgrade" process, I have attached the version 4.8.8 upgrade instructions and here is a link to download the version 4.8.8 upgrade file: https://www.dropbox.com/s/hm87jjogciba0ij/update488.tar.gz.

Downgrading to version 4.8.8 is the same as upgrading to any newer version, with the exception that you just need to check the "Force Upgrade" button during the update, in addition to the "Update Firmware" checkbox. The Force update just overrides the version check that normally occurs during upgrades. Once the NetClock has been Force "upgraded" to version 4.8.8, it should be "cleaned" back to the factory default settings (via the Tools-> Upgrade/Backup page of the browser). If you like, the settings can be backed-up off the box and then restored, once it's been updated back to version 4.8.9. Let me know if you would like to do this, instead of reprogramming it.

After downgrading to version 4.8.8, let it sync up to GPS again and then just let it run for at least a couple of hours for the oscillator to settle out and automatically perform its cal.

You will notice the reported TFOM value (as indicated in the **Status** -> **Time and Frequency** page of the web browser) will go to a much lower value. Go to the Tools -> Logs page and select the Oscillator log. You should see an entry similar (but not likely exactly the same) as the one below. The highlighted/enlarged portion indicates a good oscillator cal has been performed.

Jun 29 16:07:02 Spectracom spectracom: [system] 2012 181 16:07:02 000 **Saved Cal Value**: ***H/S:+0.000150***

Then, it can be upgraded back to version 4.8.9, using the same update process (upgrades don't need the "Force" box checked, but it doesn't hurt anything if it is checked) and using a version 4.8.9 upgrade file, instead. The version 4.8.9 upgrade file is on our website and can be downloaded at:

http://www.spectracomcorp.com/Support/HowCanWeHelpYou/Software/9400NetClockSoftware/tabid/1511/Default.aspx

Please let me know how you would like to proceed or if you have any questions pertaining to this info!

**Oscillator warm-up/stabilization (time to warm up to operating temperature)

A) Rb oscillator

- At least three days recommended for full warm-up and for the oscillator to stabilize.

B) OCXO oscillator

C) TCXO oscillator

- Not applicable: TCXO oscillator is not an ovenized oscillator.

**Oscillator Disciplining

Software changes related to oscillator disciplining

A) LPN Rubidium oscillator disciplining

B) Standard Rubidium oscillator disciplining

C) TCXO/OCXO disciplining

(HST1) 2400 Host disciplining of oscillator when NTP or “User set time” is the selected reference

Host disciplining (using NTP input to discipline TCXO/OCXO oscillators)

Note: not applicable to Rb oscillators- TCXO and OCXO only (see additional info further below)

- NTP with then be able to discipline the 10 MHz oscillator (potentially clearing the Frequency Error alarm)
- Dave Lorah was seeing TFOMs of 5 and 6 with our time servers (OCXO)
- In at least v1.4.3 and below, host disciplining associated configurations are not present in the Management -> NTP Setup pop-up window.

Issues associated with Host disciplining

1. **Some v1.4.3 dedicated Stratum 2 SecureSyncs have oscillator lock, while others don’t (osc freerun and KTS not in sync)**
    - Refer to Salesforce Case 289610

API calls associated with Host Reference

- Refer to Tim Tetreault’s “cheat sheet” at: ..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\Timing boards\TSync family\Tsync driver calls cheat sheet
- These API calls are primarily for internal use, but the associated “**get**” calls are available via the CLI interface (“sets” are not available to either spadmin or user accounts)
- These are examples - additional calls may have since been added

Host Reference Commands
HR_GetLocal
HR_GetNumInst
HR_GetRefId
HR_GetTimeScale
HR_GetValidity
HR_SetLocal
HR_SetTime
HR_SetTimeScale
HR_SetValidity

Use of Host disciplining (NTP input) with Simulcast applications

Important note: Due to the System PPS being moved/adjusted when synced to other NTP servers, it is NOT recommended for Simulcast customers to use NTP to sync SecureSyncs**.**

NTP input with a Rubidium oscillator installed

Email from Dave Lorah The only way to discipline the oscillator on these Stratum 2 units is to use a 1PPS Input or another stable high quality reference. The NTP simply is not stable enough to discipline the Rubidium.

Another email from Dave Lorah (20 Dec 16) I have verified with Engineering support that the Rubidium Oscillator will not discipline if the Securesync is using an NTP Input. This is the same whether you use Timekeeper or not.
I am sorry for the confusion.

The only way to discipline the oscillator on these Stratum 2 units is to use a 1PPS Input or another stable high quality reference. The NTP simply is not stable enough to discipline the Rubidium.

Customer reported TFOMs of around 6 and 7 when syncing via NTP

Reply from Dave Lorah (22 Sept 15) This may be the best performance you can hope for using an Internet based NTP Server. The path delays and jitter of the NTP messages depend on the network path and how busy the timer server is. The path delays and jitter are likely just too large with the Internet server to get any better TFOM.
If you had a neighboring SecureSync NTP Server located on the same network it would have better performance.

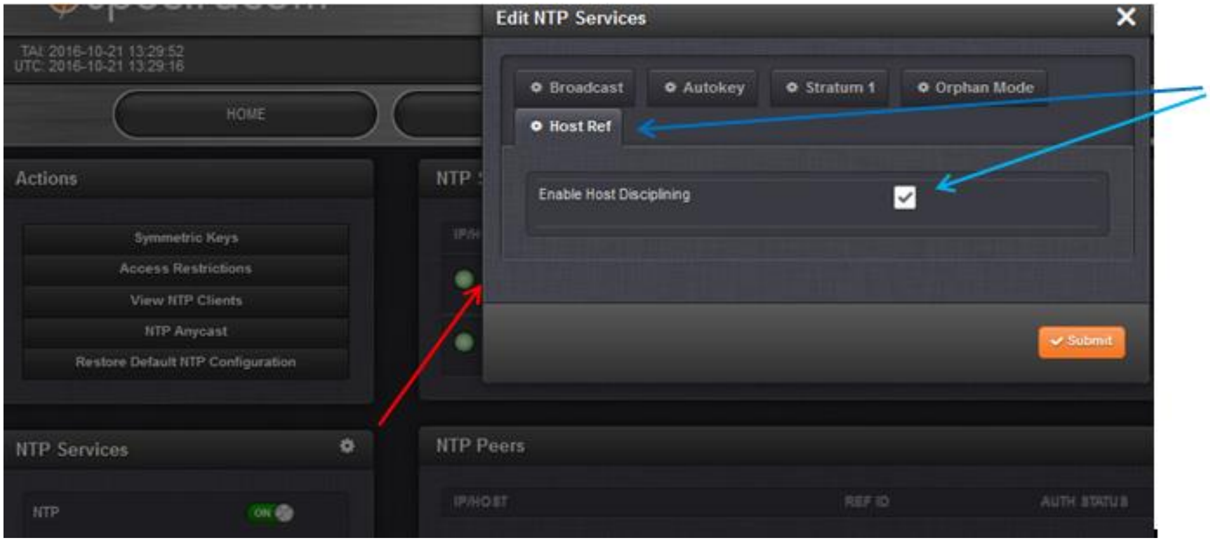
I have setup an SecureSync OCXO system disciplined to an in house close by NTP Server and I am getting TFOM of 6. If you are using an internet time server a TFOM of 7 is not unusual.

Interesting to note: I have also been monitoring a system here that is syncing to 66.219.116.140 in Carson City Michigan and it is performing pretty well. It has been running for two hours and TFOM is 5.

The disciplining should settle in after an hour or two.

D) Versions 5.4.5 and above (ability to Enable/Disable Host disciplining).

- Software update version 5.4.5 now defaults Host disciplining to OFF by factory default. But a user can enable it in the Management -> NTP Setup page of the newer browser. Press the gear icon to the right of “NTP Services” and in the pop-up window that opens, select the “Host Ref” tab. Then select the “Enable Host Disciplining” checkbox.
  - **Note**: likely need to also mask the Antenna Problem alarm for the Fault LED to clear.



Enable Host Disciplining ☑

(email from Keith, 21 Oct 16) FYI: Due to some customers preferring the oscillator not be steered by NTP input, update version 5.4.5 added a new checkbox to be able to either enable this function, or to leave it disabled so that NTP doesn't discipline the oscillator.

The factory default setting is this checkbox being disabled (not selected), so that the oscillator is not disciplined by NTP. Since this is a brand new configuration in the software, this checkbox goes to the factory default state after the first update which added it to the software (once selected, updating it again to a newer version of software will return it to the state it was in before updating it). So after updating to version 5.4.5, this checkbox needs to be selected once, if its desired to discipline the oscillator to NTP (thereby clearing the Frequency Error alarm, instead of having to mask this alarm).
The checkbox to enable (or disable it thereafter) NTP host disciplining of the oscillator is in the **Management** -> **NTP Setup** page of the browser. On the left side of this page, select the gear icon that is just to the right of "**NTP Services**". As shown below, select the new "**Host Ref**" tab, select the "**Enable Host Disciplining"** checkbox and then press **Submit**. NTP input will now start disciplining the oscillator again, just like it was before updating the software to version 5.4.5.

E) Versions 5.2.1 and below

Note: info below with software versions 5.2.1 and below (version 5.3.0 update added host disciplining for NTP disciplining)

- The oscillator is not disciplined with NTP/NTP or User/User modes, when selected as the input reference. In these two modes, the oscillator will remain in free-run mode.
- The System 1PPS is "stepped" as necessary.

When NTP or user set time is the selected reference, the oscillator is not disciplined. It is in free-run mode and the DAC value is not being changed to maintain exactly 10 MHz output. The 1PPS is periodically stepped to align it as necessary. But we are not doing any oscillator disciplining when running with NTP as the synchronizing source.

The Frequency alarm will remain asserted because the oscillator is not being disciplined. But this alarm can be masked in the **Management** -> **Notifications** page of the web browser

An external 1 PPS reference (other than NTP) should be applied, if it's desired to sync the System Time to NTP and provide accurate 10 MHz output.

Q. From Masataka ("And customer measure phase change of 1PPS from SecureSync by comparing phase difference between 1PPS of SecureSync and 1PPS of sample itself. But as soon as SecureSync sync to stratum1 NTP server (ntp.nict.jp,this phase difference start to expand").
A Reply from Keith Wing (6 Jan 15) Thanks for including the system diagram showing a Stratum 1 server sending NTP time stamps to the SecureSync, as this is important to your customer's observation Your diagram doesn't indicate if the Stratum 1 server is also a SecureSync. But your customer's observations indicate the unit they are likely referring to is the one labeled "SecureSync" and is getting NTP time from the Stratum 1 server.

To begin, if the SecureSync is syncing to a Stratum 1 NTP time server on the network, NTP in the SecureSync will become Stratum 2 (not Stratum 1). Unless the SecureSync has another higher priority input available (such as GPS or IRIG for examples, or unless it's synced to itself) NTP won't go to Stratum 1 in the SecureSync.

Secondly, the SecureSync's oscillator operation when syncing to NTP is quite different than it is when the SecureSync syncs via other external references such as GPS. When the SecureSync is synced via NTP, the oscillator is not disciplined by the NTP input, as it is when the SecureSync is synced via GPS. Instead, its periodically adjusted, starting after NTP has synced. When the SecureSync syncs via GPS, there is no correlation between the oscillator operation and NTP operation, though shortly after each power-up, both operations are going through process changes at around the same time. Shortly after power-up with GPS available, NTP will be syncing and going to Stratum 1, at around the same time the oscillator is being coarsely adjusted and starting its disciplining. Any observed correlation between NTP going to Stratum 1 and changes to the 10MHz oscillator are strictly coincidental with GPS input, just because of state changes occurring to both operations after every power-up and the SecureSync syncing to GPS.

However, when the SecureSync is being synced via NTP input only (instead of to GPS), the NTP input is influencing the operation of the oscillator, and therefore, also affecting its 10 MHz output. With NTP input synchronization, starting when NTP has synced (gone to one less Stratum than its selected NTP reference- if the reference is Stratum 1, it will go to

Stratum 2), the oscillator starts being phase-stepped to bring it into alignment with its NTP input. As long as the SecureSync continues to be synced via NTP, this phase-stepping of the oscillator periodically continues to occur in order to re-align it with its NTP input (because the oscillator is not being continuously disciplined with its 1PPS input). So phase shifts will periodically be observed when syncing via NTP instead of with GPS.

Log entries associated with host disciplining

Note- KHTD is our KTS Host Time Daemon. It is responsible for NTP time sets to KTS when operating in Stratum 2, and for setting kernel time when NTP is not running

```
[system] 2015 289 16:31:24 001 HR: Enabling Host Disciplining Mode
```

- **This entry is asserted each time KHTD is restarted (as indicated in the System log):** KTS Host Time Daemon has restarted (KHTD)
  - Note his entry indicates NTP shutdown for halt/reboot by a user (other daemons will also be terminated, as well).

Rubidium oscillator disciplining

Note: For more info, refer also to the Rubidium oscillator information in the "**SpectraTime SRO-100 Rubidium oscillators**" section in the Customerserviceassistance document.

Note: Refer to the Oscillator Disciplining documents in the following link for more info
S:\Engineering\Projects\Kramden\KTS_Project Development\200 Engineering Documents\System Architecture

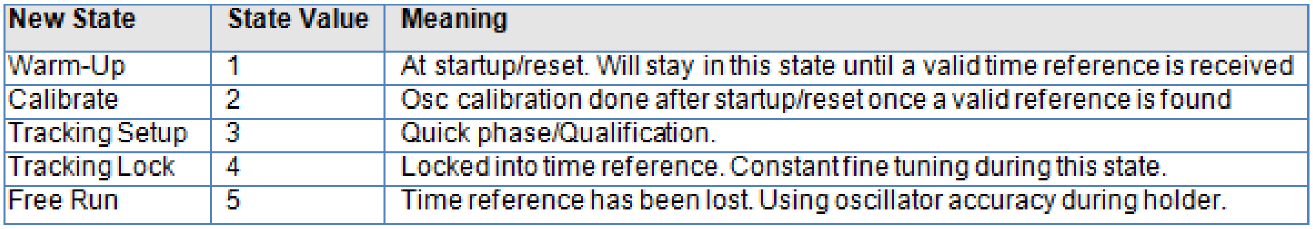
TCXO/OCXO disciplining (Disciplining states, D/A DAC values)

HST disciplining (disciplining with NTP input

Note: With software versions 5.2.1 and below, the oscillator is not disciplined with NTP/NTP or User/User modes, when selected as the input reference. In these two modes, the oscillator will remain in free-run mode (starting in version 5.3.0, NTP now disciplines the oscillator).

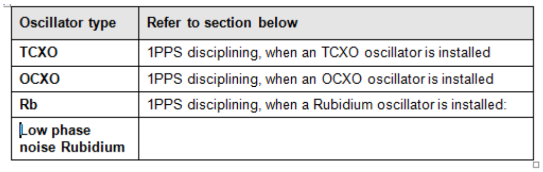
TCXO AND OCXO oscillator disciplining states

- CLI command to read Oscillator Disciplining State : **XO_GetState 0** <enter>



New State	State Value	Meaning
Warm-Up	1	At startup/reset. Will stay in this state until a valid time reference is received
Calibrate	2	Osc calibration done after startup/reset once a valid reference is found
Tracking Setup	3	Quick phase/Qualification.
Tracking Lock	4	Locked into time reference. Constant fine tuning during this state.
Free Run	5	Time reference has been lost. Using oscillator accuracy during holder.

Note: There was a State value 6 ("NoRef") in earlier versions of software. But it was removed in an earlier software update



Oscillator type	Refer to section below
TCXO	1PPS disciplining, when an TCXO oscillator is installed
OCXO	1PPS disciplining, when an OCXO oscillator is installed
Rb	1PPS disciplining, when a Rubidium oscillator is installed:
Low phase noise Rubidium	

If you have a valid time reference connector to the board, the state should go from “1” to “4”, “4” indicating it has locked in to the reference. If you were to remove the time reference, the state would go to “5” indicating that the unit was now in holdover mode.

When the unit is in state “4” and you were to run the command “XO_SetMode 0 2”, you should see the state change to “3” indicating that the unit is in the quick phase state and that the tracking has restarted.

Can you verify this on your setup? This will tell us for sure if the “reset tracking” is working in your setup.

TCXO AND OCXO DAC VALUES (D/A VALUES)

Note the **DAC** values in the Oscillator log entries are reported as hex values (“0x”). Convert the hex value to decimal value, via an Internet converter, such as: https://www.rapidtables.com/convert/number/hex-to-decimal.html?x=D555

A) 1PPS disciplining, when a TCXO oscillator is installed

DAC values:

- **Min D/A**: **0x0000** (00000 in decimal)
- **Max D/A**: **0xFFFF** (**65535** in decimal)

TCXO D/A Vdc steering range: **0-3 vdc**

Valid D/A range is: **0x2AAA** (**10922** in decimal) to **0xD555** (**54613** in decimal)

“Oscillator Alarm” is asserted when D/A **+/- 10% (0.2vdc)** of the valid D/A range

HR (Hertz range) is calculated once at the factory and then stored in EEPROM (not erased with a Clean)

Software update version 4.8.6 (June 2012) puts the calibration values in the Oscillator log after every reboot. Refer to the Oscillator log entries in this section for more info.

B) 1PPS disciplining, when an OCXO oscillator is installed

DAC values:

- **Min D/A:** 0x0000
- **Max D/A**: 0xFFFF (**65535** in decimal)

Valid D/A range is:

OCXO D/A Vdc steering range: 0-5vdc

HR (Hertz range) is calculated once at the factory and then stored in EEPROM (not erased with a Clean)

Software update version 4.8.6 (June 2012) puts the calibration values in the Oscillator log after every reboot. Refer to the Oscillator log entries in this section for more info.

"Oscillator Alarm" is asserted when D/A +/- 10% (0.2vdc) of the valid D/A range ???

Typical Oscillator log entries (DAC values) with an OCXO installed and being disciplined

```
Aug 28 19:20:32 Spectracom spectracom: [system] 2012 241 19:20:32 000 New DAC Setting: 0x7F3A  (32570 in decimal)
Aug 28 19:18:52 Spectracom spectracom: [system] 2012 241 19:18:52 000 New DAC Setting: 0x7F3E  (32574 in decimal)
Aug 28 19:18:52 Spectracom spectracom: [system] 2012 241 19:18:52 000 Frequency error recalculated: 00.000050 (5.00^-12)
```

Note the **DAC** values in the Oscillator log entries are reported as hex values ("0x"). Convert the hex value to decimal value, via an Internet converter, such as: https://www.rapidtables.com/convert/number/hex-to-decimal.html?x=D555

D/A value not valid

DAC values such as **oxEEEE (61166 decimal)** or **0xD555 (54613 decimal)** indicate a bad OCXO oscillator that needs to be replaced.

Note: If the oscillator is failing, the TFOM value may start off, or be drifting, higher than expected (such as TFOM 6 or 7, for example).

If the D/A value appears to have been thrown off, causing problems with oscillator disciplining, (which can affect outputs such as NTP, 10MHz, 1PPS, etc) , there is a **patch.img** file available that can reset the oscillator calibration value back to 0. This causes the board to re-perform the oscillator calibration procedure, with a new cal value calculated and the D/A value being placed at a reasonable value.

Time it takes for OCXO oscillator to lock

- TFOM exceeding MaxTFOM is **10 times faster slew** rate than if MaxTFOM is not exceeded.
- It only stays at the increased slew rate while MaxTFOM is exceeded. As the System PPS is pulled in, TFOM will continue to decrease. It may eventually fall below MaxTFOM, at which point is slows down to the slower slew rate until its back into alignment.

- Also keep in mind that oscillator disciplining is dependent upon a very stable input PPS. If there is excessive jitter in the reference PPS, oscillator disciplining will be trying to keep up with the jitter. This will inherently help dampen out the input jitter so the System PPS is not as jittery as the reference. But the TFOM may not be able to ever decrease, because it can never actually be able to become aligned with the Reference PPS.

Email after talking to Mark Goodlein

After a cold-start, The OCXO oscillators take about 4 minutes to warm-up. A quick-phase oscillator adjustment then occurs as soon as the 1PPS reference has been detected and is considered valid. This quick phase-align adjustment takes about a minute to complete. Then, it takes around 2 minutes for the oscillator to be disciplined "right on".

Total oscillator alignment process time, after a cold start (assuming the input reference is connected at power-up) is about 6 to 7 minutes from power-up.

For the TSync with an OCXO oscillator, the 1PPS is always slewed during re-alignment.
The rate at which it is slewed depends upon how the "Maximum TFOM" setting has been configured. This setting allows the user to define how accurate the 1PPS must be in order for the box to report that it is "In Sync".

If the current TFOM value is less than or equal to the Max TFOM setting, then the frequency of the oscillator is offset by a maximum of 0.4 Hz (40 ns/s) until the 1PPS is realigned.

If the current TFOM value is more than the Max TFOM setting, then the frequency of the oscillator is offset by a maximum of 4 Hz (400 ns/s) until the 1PPS is realigned.
As you can see by these slew rates, it may take a long time to re-align the 1PPS if it is very far off. However, there are always 10 million cycles between each 1PPS (except during power-up).

Keep in mind that it only stays at the increased slew rate while MaxTFOM is exceeded. As the System PPS is pulled in, TFOM will continue to decrease. It may eventually fall below MaxTFOM, at which point is slows down to the slower slew rate until its back into alignment.

80 microseconds of phase error is 80,000 nanoseconds. So if TFOM is not exceeding MaxTFOM, at 40ns/second of slew rate, it will take 2000 seconds (about 30 minutes) for the System PPS to be aligned. However, if TFOM exceeds MAXTFOM, it will speed up to 400ns/second (until TFOM no longer exceeds MaxTFOM, which causes it to slow back down to 40ns/second). Assuming TFOM exceeds MaxTFOM the entire time until it was back into alignment, at 400ns/second, it will take 200 seconds for it to be realigned.

Also keep in mind that oscillator disciplining is dependent upon a very stable input PPS. If there is excessive jitter in the reference PPS, oscillator disciplining will be trying to keep up with the jitter. This will inherently help dampen out the input jitter so the System PPS is not as jittery as the reference. But the TFOM may not be able to ever decrease, because it can never actually be able to become aligned with the Reference PPS. So the TFOM will remain a much higher number than usual.

Time it takes for OCXO oscillator to lock

- TFOM exceeding MaxTFOM is 10 times faster slew rate than if MaxTFOM is not exceeded.
- it only stays at the increased slew rate while MaxTFOM is exceeded. As the System PPS is pulled in, TFOM will continue to decrease. It may eventually fall below MaxTFOM, at which point is slows down to the slower slew rate until its back into alignment.
- Also keep in mind that oscillator disciplining is dependent upon a very stable input PPS. If there is excessive jitter in the reference PPS, oscillator disciplining will be trying to keep up with the jitter. This will inherently help dampen out the input jitter so the System PPS is not as jittery as the reference. But the TFOM may not be able to ever decrease, because it can never actually be able to become aligned with the Reference PPS.

Email after talking to Mark Goodlein

After a cold-start, The OCXO oscillators take about 4 minutes to warm-up. A quick-phase oscillator adjustment then occurs as soon as the 1PPS reference has been detected and is considered valid. This quick phase-align adjustment takes about a minute to complete. Then, it takes around 2 minutes for the oscillator to be disciplined “right on”.

Total oscillator alignment process time, after a cold start (assuming the input reference is connected at power-up) is about 6 to 7 minutes from power-up.

For the TSync with an OCXO oscillator, the 1PPS is always slewed during re-alignment.

The rate at which it is slewed depends upon how the “Maximum TFOM” setting has been configured.

- If the current TFOM value is less than or equal to the Max TFOM setting, then the frequency of the oscillator is offset by a maximum of 0.4 Hz (40 ns/s) until the 1PPS is realigned.
- If the current TFOM value is more than the Max TFOM setting, then the frequency of the oscillator is offset by a maximum of 4 Hz (400 ns/s) until the 1PPS is realigned.

As you can see by these slew rates, it may take a long time to re-align the 1PPS if it is very far off. However, there are always 10 million cycles between each 1PPS (except during power-up).

Keep in mind that it only stays at the increased slew rate while MaxTFOM is exceeded. As the System PPS is pulled in, TFOM will continue to decrease. It may eventually fall below MaxTFOM, at which point is slows down to the slower slew rate until its back into alignment.

80 microseconds of phase error is 80,000 nanoseconds. So if TFOM is not exceeding MaxTFOM, at 40ns/second of slew rate, it will take 2000 seconds (about 30 minutes) for the System PPS to be aligned. However, if TFOM exceeds MAXTFOM, it will speed up to 400ns/second (until TFOM no longer exceeds MaxTFOM, which causes it to slow back down to 40ns/second). Assuming TFOM exceeds MaxTFOM the entire time until it was back into alignment, at 400ns/second, it will take 200 seconds for it to be realigned.

Also keep in mind that oscillator disciplining is dependent upon a very stable input PPS. If there is excessive jitter in the reference PPS, oscillator disciplining will be trying to keep up with the jitter. This will inherently help dampen out the input jitter so the System PPS is not as jittery as the reference. But the TFOM may not be able to ever decrease, because it can never actually be able to become aligned with the Reference PPS. So the TFOM will remain a much higher number than usual.

Email after talking to Mark Goodlein

After a cold-start, The OCXO oscillators take about 4 minutes to warm-up. A quick-phase oscillator adjustment then occurs as soon as the 1PPS reference has been detected and is considered valid. This quick phase-align adjustment takes about a minute to complete. Then, it takes around 2 minutes for the oscillator to be disciplined “right on”.

Total oscillator alignment process time, after a cold start (assuming the input reference is connected at power-up) is about 6 to 7 minutes from power-up.

For the SecureSync with an OCXO oscillator, the 1PPS is always slewed during re-alignment.
The rate at which it is slewed depends upon how the “Maximum TFOM” setting has been configured. This setting allows the user to define how accurate the 1PPS must be in order for the box to report that it is “In Sync”.

If the current TFOM value is less than or equal to the Max TFOM setting, then the frequency of the oscillator is offset by a maximum of 0.4 Hz (40 ns/s) until the 1PPS is realigned.
If the current TFOM value is more than the Max TFOM setting, then the frequency of the oscillator is offset by a maximum of 4 Hz (400 ns/s) until the 1PPS is realigned.

As you can see by these slew rates, it may take a long time to re-align the 1PPS if it is very far off. However, there are always 10 million cycles between each 1PPS (except during power-up).

Using MAX TFOM to go into Holdover Mode/ cause oscillator coarse adjust to occur again

Besides resetting just the timing board itself in order for the oscillator coarse adjustment to automatically occur again (if the TFOM is excessively high), you can also take advantage of the "Max TFOM" value, if you want. If the estimated TFOM value ever exceeds the configured "Max TFOM" value, the coarse adjustment will occur again, until the TFOM value no longer exceeds Max TFOM.

The default Max TFOM is a value of "15". With Max TFOM still set to the highest possible value of "15", TFOM is never exceeded. However, you can lower the Max TFOM, so that if estimated timing errors exceed the desired values, the oscillator adjustment will occur much faster, instead of it being slewed very slowly. As the 1PPS is brought it, the TFOM value will decrease., Then, when its much closer, the TFOM will be within its set limits, and it will then switch from coarse adjust to software fine-tune slewing mode.

The Max TFOM value is set using **SS_setMaxTfom**.

Example: The Max TFOM is changed to "5". If the estimated TFOM is 6 or greater, the TSync will go into Holdover mode and a coarse adjustment occurs, until TFOM becomes 5. Then, it switches back to slewing mode, until TFOM becomes the lower possible value.

C) 1PPS disciplining, when a Rubidium oscillator is installed:

Note: For more info, refer also to "Rubidium oscillators" in the "Oscillators/10MHz outputs (for all products)" section in the Custserviceassistance document.

1PPS alignment (both initial alignment and re-alignment after reference is lost/then restored)

We tell the SRO-100 to use Track mode and then Sync Mode (Track State 1 and then Track State 2) for initial alignment and for re-alignment after a reference is restored.

The SRO-100 first snaps to within 133 ns. Then, it will start to very slowly slew in to the1PPS input reference. This slewing can takes hundreds of seconds to complete.

Email from Mark Goodlein (11/2/10):

For the SecureSync with an Rb oscillator, we use a self-disciplining Rb (SpectraTime SRO-100). When the 1PPS reference is restored, our software simply tells the SRO to track it then synchronize to it. The actual behavior is according to the SRO. This is the same behavior as would be found in the Rb NetClock 93XX which uses the same RB oscillator module.

The SecureSync uses the same disciplining algorithm for OCXO as the TSync, which is different from all other products. It has a different way of re-aligning the 1PPS.

Rb oscillator stability after power-up

- A long initial GPS disciplining interval is required to accurately setup the Rubidium Oscillator disciplining.

Email from Dick Fox (6/10/12) to TOYO

"Our design team is telling me the rubidium needs 2 weeks of GPS disciplining to settle"

Email from Dick Fox to a customer (6/10/12)

To obtain predictable drift rates for Rubidium Oscillators you need to:
Keep the units powered. Temperature stability is a major factor in determining the accuracy, so once powered you need to keep them powered.

A long initial GPS disciplining interval is required to accurately setup the Rubidium Oscillator disciplining.

SecureSync sets a DAC value that controls the frequency of the Rubidium Oscillator

SecureSync must be synchronized to GPS for a minimum 24 hours before the DAC value is set.

SecureSync will not make any changes to this DAC value unless SS is synchronized to GPS for 24 hours or more.

This means that short GPS syncs will NOT reset the Rubidium frequency and its drift. But short GPS syncs will correct the time offsets.

Based on this Spectracom can commit to a drift rate of 5 x10-12 per month provided

A. The unit is initially synchronized to GPS for a minimum of 2 weeks
B. The unit isn't powered off after it was synchronized.

Oscillator 10 MHz Accuracy (Oscillator accuracy when locked to a reference)

- Oscillator accuracy is based on being locked to an external reference that we can discipline with (such as GPS, IRIG, etc.)
- Our Oscillator accuracy specs (manual and data sheet) are based on GPS being the selected reference

What if the selected reference is another reference other than GPS (such as IRIG input)?

- Oscillator accuracy will depend on the quality of the external input being provided
- IRIG input
- IRIG DCLS input is better than IRIG AM input
- A SecureSync feeding IRIG DCLS to another SecureSync can achieve synchronization close to that of a 1PPS connection because of how stable the IRIG output of the SecureSync is.

Email from Dave Sohn (19 Nov 14) The statement from the manual is a generic statement that we've been looking at revising. The real answer is that the stability and accuracy will depend on the quality of the IRIG provided to the SecureSync. For instance, a SecureSync feeding IRIG DCLS to another SecureSync can achieve synchronization close to that of a 1PPS connection because of how stable the IRIG output of the SecureSync is.

Email from Dave Sohn (19 Nov 14) Stability during holdover isn't based at all on the synchronizing reference prior to entry into holdover. It is entirely based on the oscillator and the effects due to aging, temperature, etc. The accuracy will be affected by the input reference. Similar to my email on SecureSync IRIG input, the accuracy of the system will depend on the quality of the IRIG reference.

Effects of NTP peering on the oscillator/System PPS/1PPS outputs

- NTP peering is not recommended for use with Simulcast applications
- No matter what type oscillator is installed (TCXO, OCXO or RB), when NTP peering is used (such as loss of GPS reception for instance), the System 1PPS (and therefore 1PPS outputs also) is dithered to initially align it with the1PPS obtained from NTP. I believe it's then periodically dithered to keep it aligned to the NTP 1PPS (in at least versions 5.2.1 and below, which don't discipline the oscillator when NTP is the selected reference. Host disciplining is included in update version 5.3.0 - Sept, 2015).
- The moving of the System PPS when peering is active adversely affects simulcast systems that are relying on a stable 1PPS output/
- The only input reference recommended for simulcast is GPS!

**Fractional Frequency Error (FFE) for 10 MHz

- Note: Fractional Frequency errors are reported in "Hertz" (Hz)

- Refer to: http://www.nist.gov/pml/div688/generalpubs.cfm
- Good conversion website: http://www.convertworld.com/en/frequency/Millihertz.html

Notes for using a scientific calculator:

- Use the "+/- " and the "Exp" buttons on the calculator to enter values in scientific notation
- The "F-E" button converts the value to scientific notation.

FFE= **Frequency error** (which is the measured freq – nominal desired frequency of $1x10^{+7}$)

$1x10^{+7}$ (Nominal desired frequency of "10MHz")

Therefore

FFE for 10MHz = **Frequency Error (**which is the measured freq – $1x10^{+7}$)

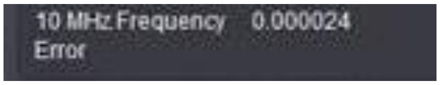
$1x10^{+7}$

Examples

Email from Tom Richardson (26 Jan 15) Fractional Frequency error of 1e-11 at 10 MHz is .0001 Hz. Take the error (1e-11) and multiply by the frequency (1e+7) to get the error (1e-4) in Hertz.
The error on the screen below is the reverse, take the error in frequency, 0.000024 Hz or 2.4e-5, and divide by the frequency, 10 MHz or 1e7, to get the fractional frequency error, 2.4 e-12.

Given the measured frequency error. Calculate FFE

First Example: Measured frequency error in this example is 0.000024 Hz ($2.4e^{-5}$)



10 MHz Frequency Error 0.000024

(From **Management** -> **Disciplining** page of browser)

FFE= **Frequency Error** (measured frequency - $1x10^{+7}$)

$1x10^{+7}$ (10 MHz)

0.000024 Hz (or $2.4e^{-5}$)

FFE=

= 0.9999999999976 which is $2.4e^{-12}$ (negative because <1)

$1x10^{+7}$

-

Second Example: actual measured output frequency is exactly 1 Hz high (10,000,001 Hz)

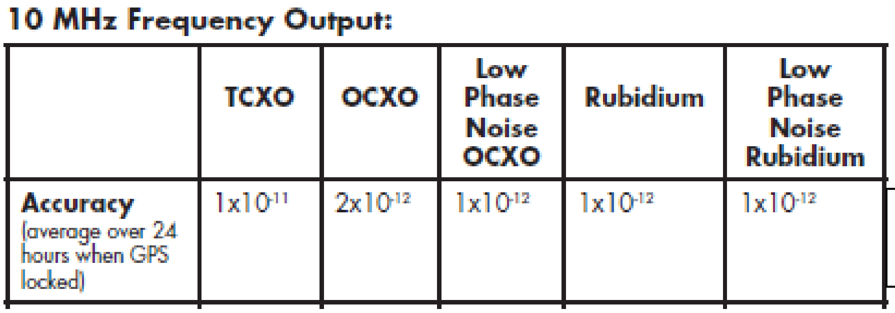
1 Hz

FFE=

$1x10^{+7}$ (10MHz) So, **FFE** = .0000001 Hz, which is also 1 $x10^{-7}$ Hz (negative because <1)

Given the FFE. Calculate the measured frequency (Hz)

Note: use this to calculate expected frequency errors (+/-) based on specs in SecureSync data sheet:



10 MHz Frequency Output:

	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium
Accuracy (average over 24 hours when GPS locked)	$1\text{x}10^{-11}$	$2\text{x}10^{-12}$	$1\text{x}10^{-12}$	$1\text{x}10^{-12}$	$1\text{x}10^{-12}$

Fractional Frequency Error (FFE) values

Example 1 for TCXO: The TCXO spec for "FFE" from the data sheet is **$1\text{x}10^{-11}$** typical

So the known **FFE value** in this case is $1e^{-11}$

FFE ($1e^{-11}$) = **Frequency error** **(**which is the measured frequency – $1\text{x}10^{+7}$)

$1\text{x}10^{+7}$ (10 MHz)

Measured frequency = multiply ($1e^{-11}$) by $1\text{x}10^{+7}$ = measured frequency of **0.0001 Hz** (**1x 10^{-4})**

To calculate the typical Frequency range = add to and subtract from 10,000,000 the frequency above.

Example 2 for OCXO: The TCXO spec for "FFE" from the data sheet is **$2\text{x}10^{-12}$** typical

So the known **FFE value** in this case is $2e^{-12}$

FFE ($2e^{-12}$) = **Frequency error** **(**which is the measured frequency – $1\text{x}10^{+7}$)

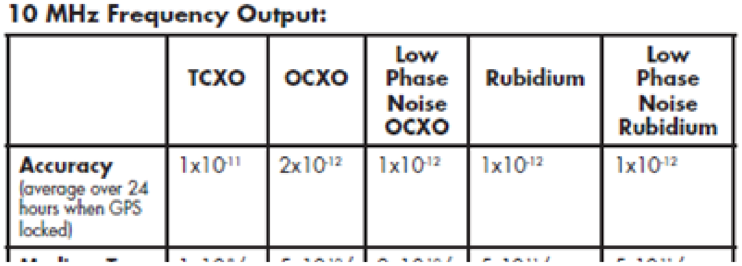
$1\text{x}10^{+7}$ (10 MHz)

Measured frequency = multiply ($2e^{-12}$) by $1\text{x}10^{+7}$ = measured frequency of **0.00002** Hz ($2\text{x}10^{-5}$)

To calculate the typical Frequency range = add to and subtract from 10,000,000 the frequency above.

*Oscillator 10 MHz accuracy (Frequency Error)

Frequency Error



10 MHz Frequency Output:

	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium
Accuracy (average over 24 hours when GPS locked)	$1x10^{-11}$	$2x10^{-12}$	$1x10^{-12}$	$1x10^{-12}$	$1x10^{-12}$

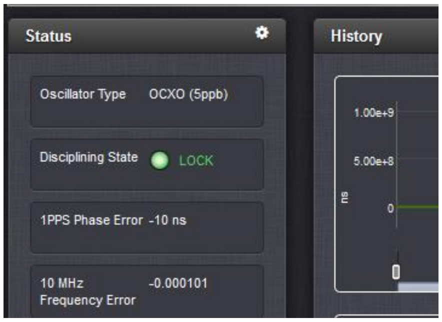
Fractional Frequency Error (FFE)

Frequency error measurements internal to the SecureSync

“Raw” Frequency error measurements are reported

A) web browser

Management -> **Disciplining** page



Status

Oscillator Type	OCXO (5ppb)
Disciplining State	● LOCK
1PPS Phase Error	-10 ns
10 MHz Frequency Error	-0.000101

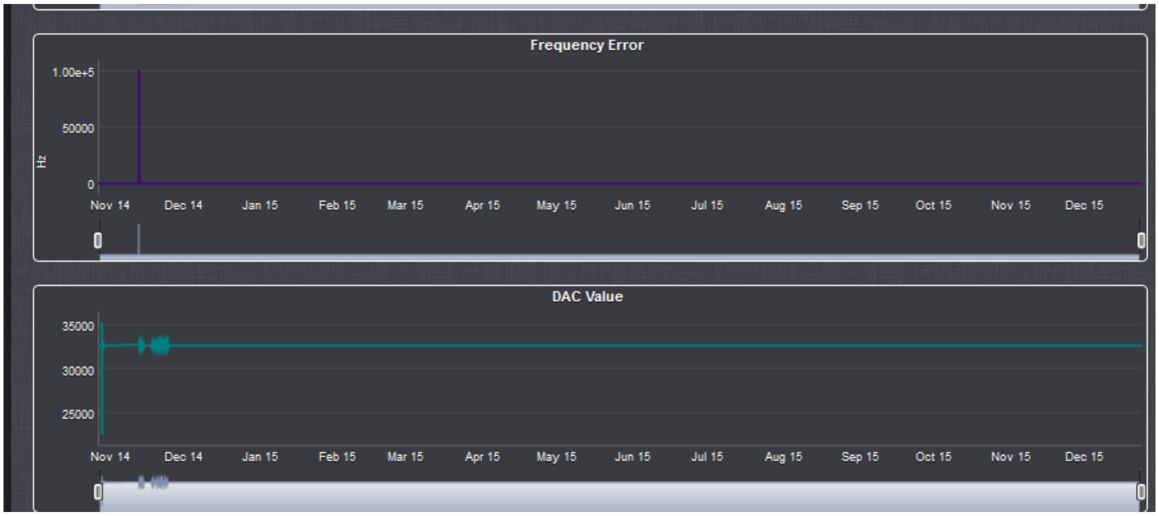
Note: Typical values for the “raw” frequency errors are like “.000076”

B) The 10MHz Frequency error can also be read using the XO_GetFreqError 0 cli command.

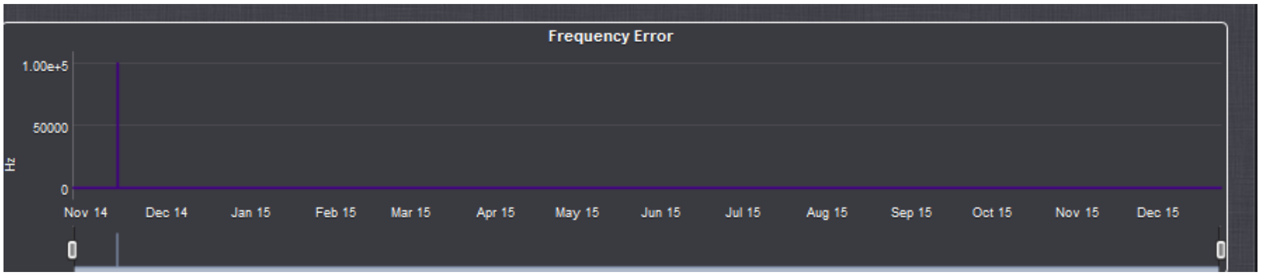
Monitoring the 10 MHz output (Frequency error and DAC values)

10 MHz Frequency Error / DAC Value Graphs

A) web browserManagement -> Disciplining page of the browser:



1. Frequency Error Graph



Vertical scale (Hertz)

- Vertical scale is dynamic
- Vertical scale is the “RAW Frequency error” value in Hertz) (its not a Fractional Frequency Error value, like values reported in the Oscillator log)
- Typical values for the “raw” frequency error are like 1 x 10 $^{+/- 4}$, or 1 x 10 $^{+/- 5}$, (not like the fractional frequency error values such x10 $^{-11}$, or x10 $^{-12}$ like we are used to seeing in the Osc log)

While the oscillator is in free-run

While the oscillator is in Free Run (SecureSync’s in Holdover mode), the Frequency Error will stop being measured and will remain the same value it was last calculated to be, while an external 1PPS reference was still available. The graph will continue to show a straight horizontal line at the same value, until an external 1PPS reference becomes present and valid again.

Vertical scale

The vertical scale varies depending upon the actual error values so pay close attention to the labeling. Above a certain value, a decimal notation is used (such as 0.01 seconds). Once the error value decreases, the values change to scientific notation (such as 2e-06).

The scientific breakdown is as follows:

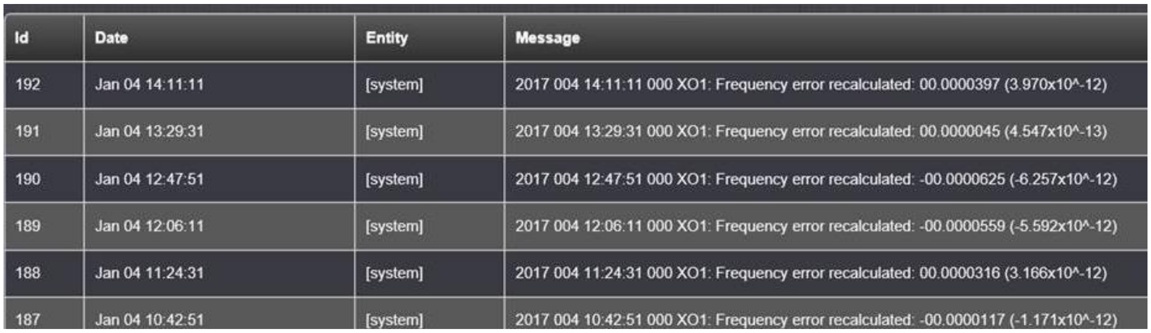
1e-12 = **1 pico Hz**	(or 0.000,000,000,001 Hz)
1e-11 = **100 nano Hz**	(or 0.000,000,000,010 Hz)
1e-10 = **10 nano Hz**	(or 0.000,000,000,100 Hz)
1e-09 = **1 nano Hz**	(or 0.000,000,001,000 Hz)
1e-08= 10 micro Hz	(or 0.000,000,01 Hz)
1e-07= 0.1 micro Hz	(or 0.0000001 Hz)
1e-06= 1 micro Hz	(or 0.000001 Hz)
1e-05= 10 micro Hz	(or 0.00001 Hz)
1e-04= **100 micro Hz**	(or 0.0001 Hz)
1e-03= 1 milli Hz	(or 0.001 Hz)
1e-02= 10 milli Hz	(or 0.01 Hz)
1e-01= **100 milli Hz**	(or 0.1 Hz)
1e+00=**1 Hz**	(or 1.0 Hz)
1e+01= **10 Hz**	(or 10.000000000 Hz)
1e+02= **100 Hz**	(or 0100.000000000 Hz)
1e+03= **1000 Hz**	(or 1000.000000000 Hz)
1e+07= 10 MHz	(or 10,000,000 Hz)

Note: If the first digit isn't a "1", multiply the first digit by the "time" value in the table above

Examples:

- **2e-05**= 20 micro Hz or 0.000020000 ("2" times "10 microseconds" is 20 microseconds)
- **5e-06**= 5 micro Hz or 0.000050000 ("5" times "1 microseconds" is 5 microseconds)

"Frequency Error recalculated" messages in the Oscillator log



Id	Date	Entity	Message
192	Jan 04 14:11:11	[system]	2017 004 14:11:11 000 XO1: Frequency error recalculated: 00.0000397 (3.970x10^-12)
191	Jan 04 13:29:31	[system]	2017 004 13:29:31 000 XO1: Frequency error recalculated: 00.0000045 (4.547x10^-13)
190	Jan 04 12:47:51	[system]	2017 004 12:47:51 000 XO1: Frequency error recalculated: -00.0000625 (-6.257x10^-12)
189	Jan 04 12:06:11	[system]	2017 004 12:06:11 000 XO1: Frequency error recalculated: -00.0000559 (-5.592x10^-12)
188	Jan 04 11:24:31	[system]	2017 004 11:24:31 000 XO1: Frequency error recalculated: 00.0000316 (3.166x10^-12)
187	Jan 04 10:42:51	[system]	2017 004 10:42:51 000 XO1: Frequency error recalculated: -00.0000117 (-1.171x10^-12)

- If customer is concerned this is an alarm/potential issue, refer customer to the FAQ on our website: http://support.spectracom.com/articles/FAQ/Why-are-there-so-many-errors-in-the-oscillator-log?q=frequency%20error&

Q, it also seems to be recalculating frequency error every 40 minutes.
A Reply from Dave L (5 Jan 17) The osc Log reports the Frequency Error every 40 minutes. This is not an error but the *difference* between the oscillator frequency and the GPS Reference frequency. We get questions all the time on this and probably should have used a different word than error in this log. There is nothing wrong. This is normal operation.

When the frequency error measurement exceeds a certain threshold, the Frequency Error Alarm is asserted. The alarm remains until the frequency error drops below the alarm threshold again. This can be caused by a loss of GPS reception, a change in the synchronization reference or even a sudden thermal change.

I can see the unit went into Holdover 1 week four days ago which means it lost GPS for a short time. The internal oscillator would have taken over to provide backup timing until the GPS signal was restored. It appears to be working properly. A loss of GPS from time to time can happen due to heavy weather or mobile GPS jammers.

I do not think this unit is malfunctioning. I do recommend updating the firmware though. Version 5.1.5 is a few years old. We currently have version 5.5.1 on our website. Please consider updating at your convenience.

Here is a link to the firmware on our website: https://spectracom.citrixdata.com/share?#/view/sb15ef818d73417e9

Typical values for a good OCXO, when locked to GPS: no worse than around " 5.994x10^-11"

Email from Dave Sohn (28 Jan 2015) With a typical reference, I believe that the minimum non-zero value we can report is +/- 6.25e-13.

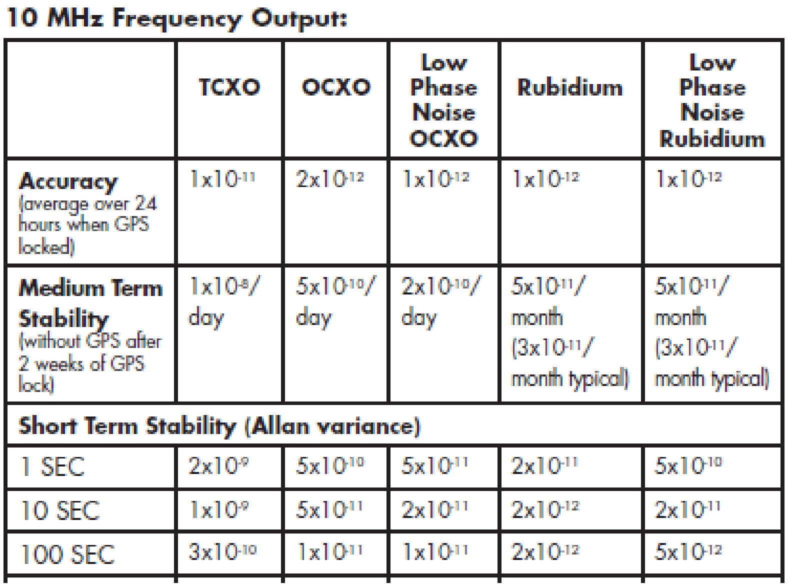
Spectracom SecureSyncs contain one of five types of internal 10 MHz oscillators. The internal oscillator is used to output 10 MHz and to generate an internal 1PPS signal.

The "Oscillator" log provides an indication of the frequency counts of the oscillator's 10 MHz output, as measured using the selected 1PPS Input Reference (Such as a GPS receiver's 1PPS output signal) as a reference.

The "frequency error recalculated" messages in this log indicate the accuracy of the oscillator output, in comparison to a perfect 10 MHz signal (known as the "fractional frequency error"). The 10 MHz oscillator output is measured against the 1PPS generated by the selected 1PPS input reference.

Important Note- The "FREQUENCY ERROR RECALCULATED" phrases displayed on this web page DO NOT mean a problem exists with either the internal oscillator or with the NTP server. "FREQUENCY ERROR RECALCULATED" refers to the Fractional Frequency Error which is a comparison of the actual output frequency versus the desired frequency (The desired frequency is 10.0000000 MHz), reported in scientific notation. This phrase will ALWAYS be present on this page to show the measured 10 MHz frequency. If a problem DOES happen to exist with the oscillator frequency measurements, a Frequency alarm will be entered in the "Alarms" log.

The lower the "Frequency error recalculated" value is, the closer the oscillator is to outputting an exact 10 MHz signal. Below is a table of the 10MHZ specifications. The "Frequency error calculated" values should typically be less than the values in the "Short term Stability" section of this table, for the specific type of oscillator installed, as long as SecureSync is synced to an external reference (other than other NTP severs).



10 MHz Frequency Output:

	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium
Accuracy (average over 24 hours when GPS locked)	1x10^{-11}	2x10^{-12}	1x10^{-12}	1x10^{-12}	1x10^{-12}
Medium Term Stability (without GPS after 2 weeks of GPS lock)	1x10^{-8}/ day	5x10^{-10}/ day	2x10^{-10}/ day	5x10^{-11}/ month (3x10^{-11}/ month typical)	5x10^{-11}/ month (3x10^{-11}/ month typical)
Short Term Stability (Allan variance)					
1 SEC	2x10^{-9}	5x10^{-10}	5x10^{-11}	2x10^{-11}	5x10^{-10}
10 SEC	1x10^{-9}	5x10^{-11}	2x10^{-11}	2x10^{-12}	2x10^{-11}
100 SEC	3x10^{-10}	1x10^{-11}	1x10^{-11}	2x10^{-12}	5x10^{-12}

“Frequency error recalculated: 00.0000000 (0.000x10^-16)” (0.000e-16 or 0.000x10-16)

Note: This oscillator.log entry can be asserted for one of two reasons:

A) The actual frequency error is less than we can measure

Email from Dave Sohn (27 Jan 15) after I alluded to the software issue below It is still possible to receive a frequency error of 0 if it is below our measurement capability. We fixed where negative frequency errors were reported as 0.

Edited Email Keith sent to Masataka (27 Jan 15)
Thanks for forwarding along your customer’s inquiry about the oscillator log entries.
The oscillator log entry of “**Frequency error recalculated: 00.000000 (0.000x10^-16)”** is not a symptom of any problems occurring with the SecureSync. These log entries just mean that the magnitude of the frequency error at that time was less than the threshold that the system can even measure. In this case, the Frequency Error is reported as “0.000x10^-16” (the lowest value possible for the system to report). So instead of these log entries being a symptom of a problem, they instead indicate the oscillator is as close to being at the desired frequency as the system is capable of measuring.

Email from Dave Sohn (28 Jan 2015) With a typical reference, I believe that the minimum non-zero value we can report is +/-6.25e-13.

B) A minor software issue in software versions 5.10 through 5.1.4 (fixed in 5.1.5)

- Software issue with reporting the frequency error in the Oscillator log
- Negative values were being incorrectly being reported as “0” (“So any negative frequency error measurements will show as 0.000x10-16.")
- Refer to Mantis case 2862 http://cvsmantis.int.orolia.com/mantis/view.php?id=2862
- This issue first started in version 5.1.0.
- Fixed in version 5.1.5 software update

Email from Dave Lorah to Masataka (24 June 2014) The minimum measurable values are based on the error range of the reference, the adjustable measurement window, and the oscillator type, but it should be in the range 10x-13.

I was incorrect saying the 0.000x10-16 was reporting a 0 value, actually the 10x-16 is no measurable error. I found out there is a bug in the current logging that reports negative values as10x-16. They are displayed correctly in the disciplining pages in the UI, but the log entries will have the issues. So any negative frequency error measurements will show as 0.000x10-16.

As far as changes between 5.0.2 and 5.1.4, we improved our measurement window adjustments, improved our initial sync time performance, and added adjustable filtering based on input reference error. There would be a difference in the oscillator log measurements due to these changes. The oscillator measurement range should be in the x10-11 to x10-13 range. The oscillator log you sent us shows typical performance.

Software version 5.1.4 improvements to oscillator disciplining
Email from Dave Lorah to Masataka (24 June 2014) As far as changes between 5.0.2 and 5.1.4, we improved our measurement window adjustments, improved our initial sync time performance, and added adjustable filtering based on input reference error. There would be a difference in the oscillator log measurements due to these changes. The oscillator measurement range should be in the x10-11 to x10-13 range. The oscillator log you sent us shows typical performance.

“Rb Reference unstable” / “Rb synchronized” / “Rb track off -- free run”

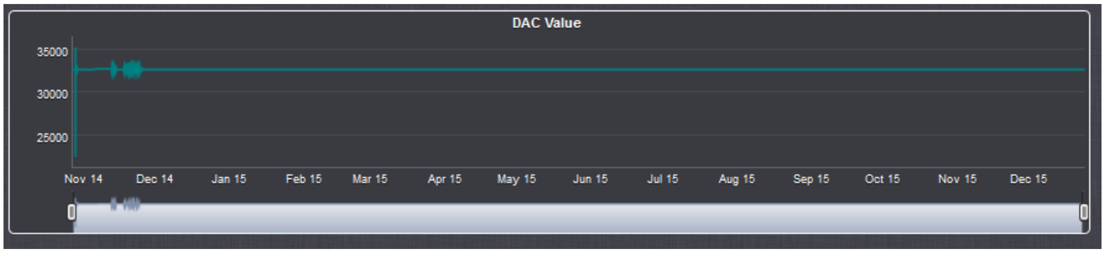
- Could indicate a bad Rb oscillator
- Can also be caused by issues with the selected 1PPS reference (such as issues with a Res-SMT-GG receiver)
    - The “Rb Reference unstable” alarm was seen correlated with the following entry in the Timing log

      ```
      “[system] 2014 291 13:01:08 002 Error: CS_Set(CS_SA_LEAP_SEC) call from GR.”
      ```

    - The “Rb Reference unstable” alarm was seen correlated with the following entries in the oscillator log

      ```
      [system] 2016 048 17:02:00 000 XOS: Rb Reference unstable
      [system] 2016 048 17:02:01 000 XOS: Rb tracking
      system] 2016 048 17:02:32 000 XOS: Rb synchronized
      [system] 2016 048 17:03:08 000 XO1: Phase Err: -31170.0
      [system] 2016 048 17:03:08 000 XO1: Freq Err: +0.132500
      ```

DAC Value Graph



Frequency Error measurements, while the oscillator is in free-run

While the oscillator is in Free Run (SecureSync’s in Holdover mode), the Frequency Error **will stop being able to be calculated**. So the DAC value will remain at its last calculated value, while the oscillator remains in free-run (no changes are made to the DAC value while in Holdover mode).

To download the raw oscillator data

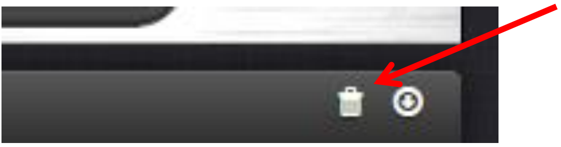
- A “.csv” or “.json” file with the oscillator values (and system temperatures) can be downloaded as desired.

Download of raw oscillator data as a “.csv” file (can be opened in excel)

A “.csv” file can be downloaded using either of two different methods:

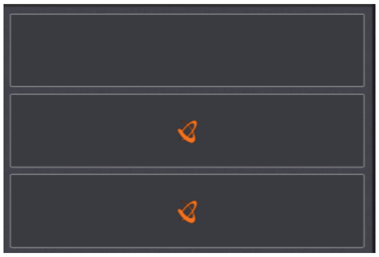
1. A .CSV file download button is available in the Management -> Disciplining page of the browser

From the **Management** -> **Disciplining** page of the browser (click on the “down arrow” ICON on the right side of the page to download the .csv file. Press the garbage can icon to delete all of the oscillator and temperature data used to display the graphs)



Note: The “garbage can” ICON on the upper-right corner clears/deletes all of the graph data.

Note: Deleting the log data will refresh the graphs.

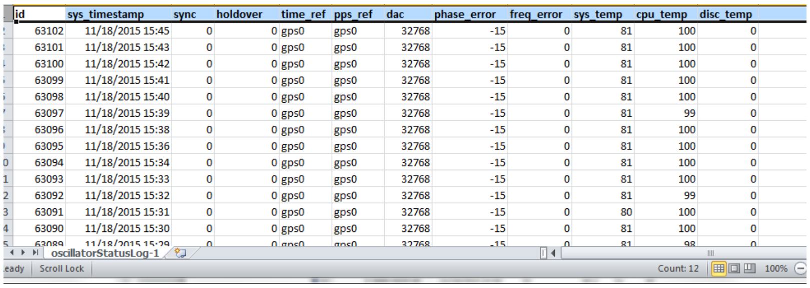


2. Manually enter the link to the OscillatorStatuslog

If you manually enter **/logs/OscillatorStatusLog.csv** after the URL of the SecureSync in the web browser it will download a csv file that can be opened in Excel with the GPS status log data.

Example: http://10.10.128.1/logs/OscillatorStatusLog.csv (change address as applicable)

Example .csv file output below ("Sys temp" and "**CPU temp**" fields were added in software version 5.3.0**)**



id	sys_timestamp	sync	holdover	time_ref	pps_ref	dac	phase_error	freq_error	sys_temp	cpu_temp	disc_temp
63102	11/18/2015 15:45	0	0	gps0	gps0	32768	-15	0	81	100	0
63101	11/18/2015 15:43	0	0	gps0	gps0	32768	-15	0	81	100	0
63100	11/18/2015 15:42	0	0	gps0	gps0	32768	-15	0	81	100	0
63099	11/18/2015 15:41	0	0	gps0	gps0	32768	-15	0	81	100	0
63098	11/18/2015 15:40	0	0	gps0	gps0	32768	-15	0	81	100	0
63097	11/18/2015 15:39	0	0	gps0	gps0	32768	-15	0	81	99	0
63096	11/18/2015 15:38	0	0	gps0	gps0	32768	-15	0	81	100	0
63095	11/18/2015 15:36	0	0	gps0	gps0	32768	-15	0	81	100	0
63094	11/18/2015 15:34	0	0	gps0	gps0	32768	-15	0	81	100	0
63093	11/18/2015 15:33	0	0	gps0	gps0	32768	-15	0	81	100	0
63092	11/18/2015 15:32	0	0	gps0	gps0	32768	-15	0	81	99	0
63091	11/18/2015 15:31	0	0	gps0	gps0	32768	-15	0	80	100	0
63090	11/18/2015 15:30	0	0	gps0	gps0	32768	-15	0	81	100	0
63089	11/18/2015 15:29	0	0	gps0	gps0	32768	-15	0	81	98	0

Definition of fields

Sync and **Holdover**: 1 is true, 0 is false

Time ref and **PPS ref:** Selected input reference at that time

DAC: Oscillator's DAC value

Phase Error: 1PPS Phase Error

Freq Error: Oscillator's Frequency Error

Temps: Board, CPU and **Oscillator**

Notes:

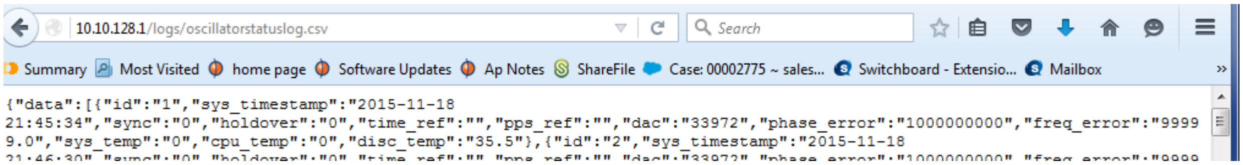
1. **Oscillator** temp is only available if the temperature sensor (U60) is installed on the main PCB (very close to the oscillator). Refer to ECN 2807 (5 Dec,2011)
2. **Board** and **CPU** temps were added in software version 5.3.0

A. Output of graphable oscillator and temperature data as a .json file for graphing

Same process as downloading.csv file with direct link, but replace ".csv" with "**.json"** instead.

If you manually enter **/logs/OscillatorStatusLog.json** after the URL of the SecureSync in the web browser it will download a json file.

Example: http://10.10.128.1/logs/OscillatorStatusLog.json (change address as applicable)


10.10.128.1/logs/oscillatorstatuslog.csv
Search
Summary
Most Visited
home page
Software Updates
Ap Notes
ShareFile
Case: 00002775 ~ sales...
Switchboard - Extensio...
Mailbox

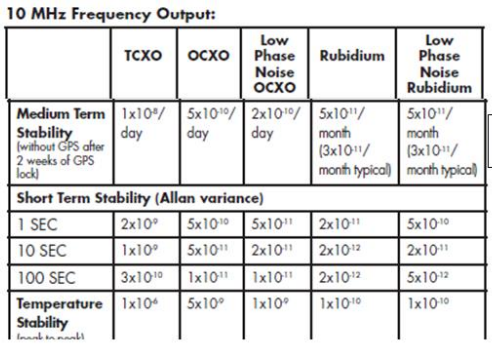
```
{"data":[{"id":"1","sys_timestamp":"2015-11-18
21:45:34","sync":"0","holdover":"0","time_ref":"","pps_ref":"","dac":"33972","phase_error":"1000000000","freq_error":"9999
9.0","sys_temp":"0","cpu_temp":"0","disc_temp":"35.5"},{"id":"2","sys_timestamp":"2015-11-18
21:46:30","sync":"0","holdover":"0","time_ref":"","pps_ref":"","dac":"33972","phase_error":"1000000000","freq_error":"9999
```

Frequency Error measurements while in oscillator Free-Run mode (SecureSync in Holdover mode)

- While the oscillator is in in Free Run, the Frequency error stops being calculated and remains at the last calculated value. To determine if the frequency error is the current or the last calculated value, user needs to determine if the oscillator is locked or currently in free run.
- Because the frequency error measurements stop being calculated while the oscillator is in free run mode, an external frequency counter (such as the Spectracom frequency counters, Models CNT-90 or CNT-91) should be used to measure the Frequency Error while SecureSync is in Holdover mode (oscillator free run).

Typical/expected Frequency Error calculations when not locked

Below are the typical expected measurements of the 10MHz output. Note these are not specs, but averages over a period of 24 hours.



10 MHz Frequency Output:

	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium
Medium Term Stability (without GPS after 2 weeks of GPS lock)	1x10^{8}/ day	5x10^{-10}/ day	2x10^{-10}/ day	5x10^{11}/ month (3x10^{-11}/ month typical)	5x10^{11}/ month (3x10^{-11}/ month typical)
Short Term Stability (Allan variance)					
1 SEC	2x10^{9}	5x10^{-10}	5x10^{11}	2x10^{11}	5x10^{-10}
10 SEC	1x10^{9}	5x10^{11}	2x10^{11}	2x10^{-12}	2x10^{11}
100 SEC	3x10^{-10}	1x10^{11}	1x10^{11}	2x10^{-12}	5x10^{-12}
Temperature Stability (peak to peak)	1x10^{6}	5x10^{9}	1x10^{9}	1x10^{-10}	1x10^{-10}

Fractional Frequency Error (FFE)

TCXO/OCXO frequency error

- Measurements with a TCXO/OCXO can be either positive or negative numbers.

Rubidium oscillator frequency errors

- Frequency Error observed on our House reference (10.10.10.2 with Low phase noise rb): -000026ns
- Measurements with a Rb oscillator will always be reported as a positive number, even if it’s a negative value

Per Dave Sohn (15 May 2014) Keith, I also believe the Rb error calculation is always provided as a magnitude value error, which means that regardless of whether it is actually positive or negative it is returned as a positive value.

Q. About phase error/frequency error. We would like to know physical meaning of these numbers so we can properly interpret and try to use them in our measurement analysis

A. Frequency and phase error for the Rubidium are both provided as unsigned magnitude values. Frequency error is determined by the phase error accumulated during a period of time equal to the tracking loop constant as determined by the Rubidium disciplining. The tracking loop constant starts at 1000s, but can grow and shrink depending on quality of the reference and other conditions. The phase error is determined from the current phase error comparator value plus the measured error fluctuation of the reference.

Q. Is temperature stability data available for SecureSync? The only data we have is p-p frequency error across operating temperature range from specification. We have found that the phase error anomaly is very likely rack temperature related and it would be helpful to know tolerance limits and optimal working temperature.

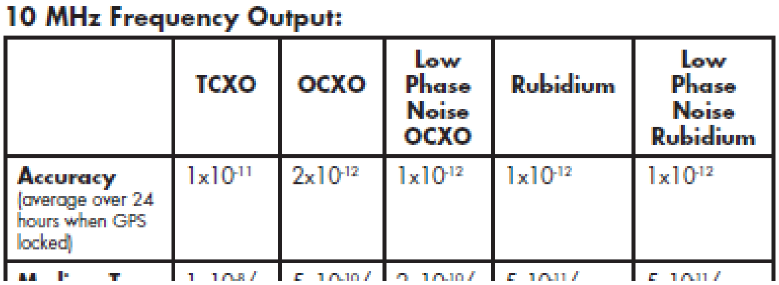
A Per Dave Sohn (22 May 2014) We specify the temperature stability across the entire range as provided from our oscillator vendor. We do not have information on optimal or more problematic temperature ranges.

Freq error of 0.00e+00

Per Dave Sohn (15 May 2014) Seeing a zero value for the frequency error is not an indicator of any issues. It just means that the error is less than what we can measure for that period.

Oscillator Accuracies (From the SecureSync Data Sheet):

Important Note: these average accuracy specs below are average over 24 hours when locked to GPS.



10 MHz Frequency Output:

	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium
Accuracy (average over 24 hours when GPS locked)	$1x10^{-11}$	$2x10^{-12}$	$1x10^{-12}$	$1x10^{-12}$	$1x10^{-12}$
[illegible]	$1x10^{-8}$/	$5x10^{-10}$/	$2x10^{-10}$/	$5x10^{-11}$/	$5x10^{-11}$/

TCXO: $1x10^{-11}$ Hz/day=
$1x10^{-11}$ Hz/day = 0.00000000001 Hz/ day = 0.01 nano Hz/day

OCXO $2x10^{-12}$ Hz/day=
$2x10^{-12}$ Hz/day = 0.000000000002 Hz /day = 0.002 nano Hz /day

Low Phase Noise OCXO $1x10^{-12}$
$1x10^{-12}$ Hz/day= 0.000000000001Hz/day = 0.001 nano Hz /day

Low Phase Noise Rb $1x10^{-12}$
$1x10^{-12}$ Hz/day= Hz/day= 0.000000000001 Hz/day = 0.001 nano Hz /day

Holdover mode/ Oscillator 10 MHz free-run (Oscillator Stability)

Oscillator stability

Several factors affect oscillator stability

- Aging rate
- Temperature variations
- Oscillator’s input Power fluctuations
- Humidity variations
- And others

Oscillator drift is essentially the oscillator aging rate, plus temperature drift, plus the effects of other variables.

Factors that don’t affect stability:

- The Selected reference before oscillator goes into Free run mode (such as IRIG input instead of GPS)

Email from Dave Sohn (19 Nov 14) The statement from the manual is a generic statement that we've been looking at revising. The real answer is that the stability and accuracy will depend on the quality of the IRIG provided to the SecureSync. For instance, a SecureSync feeding IRIG DCLS to another SecureSync can achieve synchronization close to that of a 1PPS connection because of how stable the IRIG output of the SecureSync is.

Email from Dave Sohn (19 Nov 14) Stability during holdover isn't based at all on the synchronizing reference prior to entry into holdover. It is entirely based on the oscillator and the effects due to aging, temperature, etc. The accuracy will be affected by the input reference. Similar to my email on SecureSync IRIG input, the accuracy of the system will depend on the quality of the IRIG reference.

Important note: Drift is non-linear

Email from Dave Sohn (17 Oct 2013) Drift in holdover is not linear as implied here. The phase drift will be exponential as the frequency drifts. So, no oscillator will provide <1ms per day indefinitely. For example, the TSync OCXO will provide less than 1ms per day for around 6-7 days, but more than that afterwards. Also, all of our models are based on good starting values starting out from GPS synchronization, which won't be available here.

Email from Tony Diflorio to a potential customer looking for 1ms/day accuracies A couple of other ideas to help you: You could use a portable (battery operated) GPS synchronization device to provide re-synchronization to the TSync-PCIe-Opt-OCXO card, such as our model GPS-12/12R (see attached). This re-synchronization would have to be done every few days though to maintain the TSync-PCIe-OCXO to <1ms per day of drift. Or, you might be able to use our popular "SecureSync", rack mounted GPS Synchronization system (see attached) with a Rubidium internal oscillator. This depends on whether you must have specific features that only a Bus-Level card can provide. Using our SecureSync with a Rubidium internal oscillator will provide the holdover accuracy you are looking for, over a much longer period of time (almost indefinitely).

Oscillator stability with reference removed (in freeeun)

1PPS output holdover specs with OCXO oscillator

Email from Dave Sohn (10/3/11) regarding low phase noise drift (no GPS) after at least two weeks of lock:
Estimate for holdover at constant temperature after 2 weeks of GPS lock

Days	Drift
1	10 us
2	40 us
3	80 us
7	430 us

Email from Tim Tetreault to Will Hickey:

Will,
The Holdover spec's for the TCXO is the same between the TSync and SecureSync:

Standard TCXO:
450usec/24hr (constant temp after 2 weeks of GPS lock)

The Holdover spec's for the OCXO is not the same because they use different OCXO's. The spec for the TSync is:

Optional OCXO:
90usec/24hr (constant temp after 2 weeks of GPS lock)

So if the customer wanted to calculate the drift per seconds:
The TCXO would be:
45E-5/(60sec x 60min x 24 hours) = 5.2 ppb

The error for the OCXO would be:
9E-5/(60sec x 60min x 24 hours) = 1.0 ppb

- **Disciplined to Timecode**: 2 x 10–7

- **Undisciplined Freewheel Drift**: 1 x 10–6

Oscillator stability when the board is in holdover mode:

- TCXO our oscillator stability is 1E-6 (1 ppm),
- OCXO our oscillator stability is 5E-8 (50 ppb).

There are two main error factors for oscillator stability – Initial startup and aging over time. The initial startup and lifetime aging specs are as follows:

Oscillator	Initial startup	Lifetime aging
OCXO oscillator	0.2 PPM	2.0 PPM
TCXO oscillator	1.0 PPM	5.0 PPM

With an external input reference (such as GPS and IRIG), we can account for these errors.

C) To calculate the estimated amount of Freewheel drift with a TCXO:

Convert the time to seconds and multiply by 1.5E-6.

Examples (where 1 hr = 3600sec):
Amount of drift per hour = 3600 * 1.5E-6 = 0.0054 seconds per hour (or **5.4 milliseconds**) of estimated drift

Amount of drift per second= 0.0054sec / 3600 (seconds) = .0000001 seconds per second (or **0.1 microseconds)** of estimated drift

Amount of drift per day= 0.0054sec x 24 (hours) = .0123 seconds per day (or **12 milliseconds**) of estimated drift

D) To calculate the estimated amount of Freewheel drift with an OCXO:

Convert the time to seconds and multiply by 5E-8.

Examples (where 1 hr = 3600sec):

Amount of drift per hour = 3600 * 5E-8= 0.00018 seconds per hour (or **0.18 milliseconds**) of estimated drift

Amount of drift per second= 0.00018sec / 3600 (seconds) = 0.00000005 seconds per second (**or 0.05 microseconds)** of estimated drift

Amount of drift per day= 0.00018 sec x 24 (hours) = 0.00432 seconds per day (or **4.32 milliseconds**) of estimated drift

Selected reference (GPS, IRIG, etc) before Holdover/oscillator free run begins

Q What type of input reference (GPS, IRIG, external PPS, etc) that was selected before the oscillator goes into Freerun mode has no effects on free-run operation.

A Dave Sohn (19 Nov 2014) Stability during holdover isn't based at all on the synchronizing reference prior to entry into holdover. It is entirely based on the oscillator and the effects due to aging, temperature, etc. The accuracy will be affected by the input reference. Similar to my email on SecureSync IRIG input, the accuracy of the system will depend on the quality of the IRIG reference.

Oscillator aging rates

- Refer to: I:\Engineering\Oscillators
- Aging rates are based on 30 days of continuous operation
- Rates are much higher with less than 30 days of operation (it's a huge curve)

Examples:

SRO-100 Rb oscillator: Aging rate is < 5E-11/month (after 30 days of continuous operation)

Our Specs

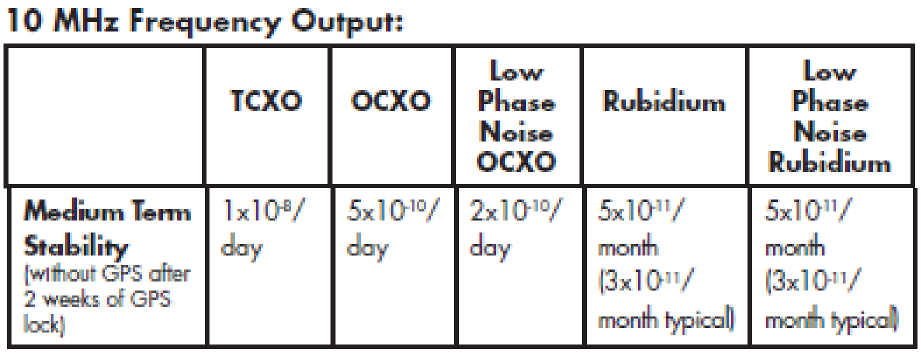
- Medium term Stability is over a longer period of time (such as either after 24 hours or after 1 month, as specified)
- Short term Stability is over short "windows" of time (such as in just 1 second, over 10 seconds, or over 100 seconds).
- Our specs (discussed below) are TYPICAL or average values – not Absolute values!

Oscillator Medium Term stability in free run: From SecureSync Data Sheet (with some modification for presentation)

- "Holdover" values over one day or one month (as specified)

Important Note: this medium term stability specs below are average values upon loss of input reference that has been present for at least two weeks (system running the whole time). Shortening this period can severely degrade these values.

.



10 MHz Frequency Output:

	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium
Medium Term Stability (without GPS after 2 weeks of GPS lock)	$1x10^{-8}$/ day	$5x10^{-10}$/ day	$2x10^{-10}$/ day	$5x10^{-11}$/ month ($3x10^{-11}$/ month typical)	$5x10^{-11}$/ month ($3x10^{-11}$/ month typical)

TCXO: $1x10^{-8}$ per day

- **$1x10^{-8}$ Hz/day** = 0.00000001 Hz/ day = 10 nano Hz/day

OCXO $5x10^{-10}$ per day

- **$5x10^{-10}$ Hz/day** =0.0000000005 Hz /day = 0.5 nano /day

Low Phase Noise OCXO 2x10^{-10} per day

- ○ **2x10^{-10} Hz/day**= 0.0000000002 Hz/day = 0.2 nano Hz /day

Rubidium 5x10^{-11} per month

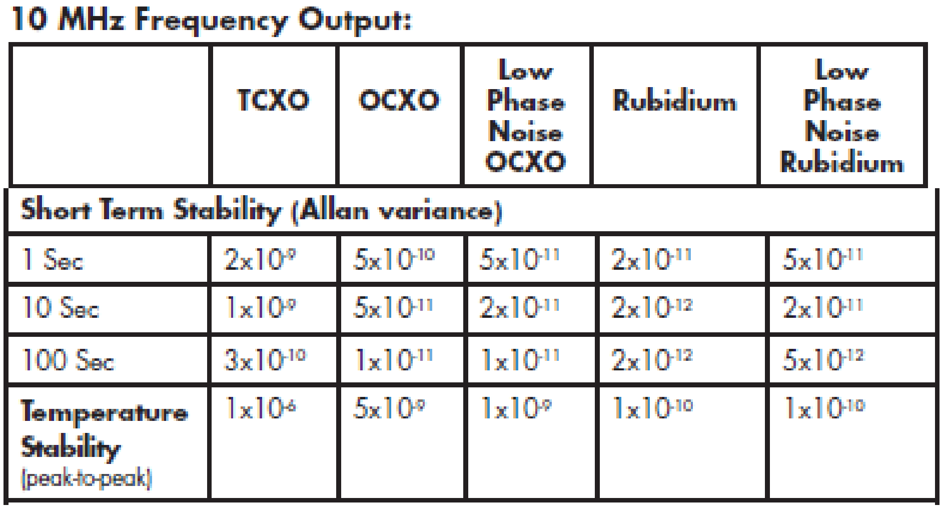
- ○ **5x10-11 Hz/month**= 0.00000000005 Hz/month = 0.05 nano Hz /month
- ○ **3x10-11 Hz/month typical**= 0.00000000003 Hz/month = 0.03 nano Hz /month

Low Phase Noise Rb 5x10^{-11} per month

- ○ **5x10^{-11} Hz/month**= 0.00000000005 Hz/month = 0.05 nano Hz /month
- ○ **3x10^{-11} Hz/month typical**= 0.00000000003 Hz/month = 0.03 nano Hz /month

Oscillator Short Term stability in free run: From SecureSync Data Sheet (with some modification for presentation)

- ➢ “Holdover” values over very short “windows of time (such as 1 second to the next, over just 10 seconds, or over just 100 seconds)



10 MHz Frequency Output:

	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium
Short Term Stability (Allan variance)					
1 Sec	2x10^{-9}	5x10^{-10}	5x10^{-11}	2x10^{-11}	5x10^{-11}
10 Sec	1x10^{-9}	5x10^{-11}	2x10^{-11}	2x10^{-12}	2x10^{-11}
100 Sec	3x10^{-10}	1x10^{-11}	1x10^{-11}	2x10^{-12}	5x10^{-12}
Temperature Stability (peak-to-peak)	1x10^{-6}	5x10^{-9}	1x10^{-9}	1x10^{-10}	1x10^{-10}

Oscillator D/A value while in Holdover/reboot (TCXO/OCXO)

The following info is for TCXO and OCXO oscillators. If they have a Rb oscillator, let me know and I will check with our Engineering team to see if it’s similar to these other two oscillators.

When the SecureSync goes into Holdover mode (loses all input references), the D/A remains the same value it was before the reference(s) was lost. Because disciplining stops when there are no references, this D/A will remain constant thereafter, until at least one input reference is restored and declared valid

The D/A value is stored, so after a reboot/power cycle, the D/A value is restored to the same value it was before the reboot.

Low phase noise (HP) oscillator free run

Email from David Sohn to Dick Fox.

The holdover for one day would be around 10 microseconds, but the drift is not linear, it's exponential. Based on our model, the drift after 14 days would be around 1.7 milliseconds.

Email from Dick to TOYO (based on input from Dave Sohn)

To obtain predictable drift rates for Rubidium Oscillators you need to:

- keep the units powered. Temperature stability is a major factor in determining the accuracy so once powered you need to keep them powered
- A long initial GPS disciplining interval is required to accurately setup the Rubidium Oscillator disciplining.
- Secure Sync sets a DAC value that controls the frequency of the Rubidium Oscillator
- Secure Sync must be synchronized to GPS for a minimum 24 hours before the DAC value is set.
- Secure Sync will not make any changes to this DAC value unless SS is synchronized to GPS for 24 hours or more
- This mean that short GPS syncs will NOT reset the Rubidium frequency and its drift
- But short GPS syncs will correct the time offsets

Based on this, Spectracom can commit to a drift rate of 5 X10-12 per month provided

- The units is initially synchronized to GPS for a minimum of 2 weeks
- The unit isn't powered off after it was synchronized

If this is acceptable?

Here is what the drift rate table looks like

- The 2 hours of GPS lock – initializes Secure Sync's 1 PPS to track UTC within +or-25 nanosecond standard deviation
- No adjustment to the oscillator frequency is made
- The 4 hours of GPS lock – initializes Secure Sync's 1 PPS to track UTC within +or-25 nanosecond standard deviation
- No adjustment to the oscillator frequency is made
- The 24 hours of GPS lock – initializes Secure Sync's 1 PPS to track UTC within +or-25 nanosecond standard deviation
- The DAC value that controls the Rubidium oscillator frequency can be adjusted

There is little incremental value is syncing to GPS for 4 hours versus 2 hours. It doesn't adjust the Rubidium oscillator frequency just correct the time.

Only GPS lock for 24 hours or more adjusts the oscillator frequency.

Here is the table

GPS lock time	2 hours	4 hours	24 hours
> After 4 hours of holdover	.20 usec	0.20 usec	0.2 usec
> After 24 hours of holdover	2 usec	2 usec	2usec
> After 2 weeks of holdover	28 usec	28 usec	28 usec

Again this is based on initial power up and synced to GPS for 2 weeks
Then as long as you continue to keep the unit powered
We are well below the 100 usec specifications but it requires an initial 2 week GPS sync and then you have to keep it powered

Short GPS lock time will correct the time due to drift, but won’t affect the oscillator drift rate

---

**“Rb(Sync)" displayed on the front panel LCD

Q. (Email from Masataka) When TFOM is more than MAX TFOM but it is not exceeded in Holdover time,
"OSC" field in display of front panel indicated "Rb(Sync)" state.
Is following understand correct?
-Our understanding
This field indicate "Rb(Sync)" when following situation is existing.
・TFOM is less than MAX TFOM.
・TFOM is more than MAX TFOM but it is not exceed in Holdover time.

A. Email from David Sohn (9 Nov 2012) The “Rb (Sync)” indicator is not related to the TFOM and MAX TFOM checks. There is a difference between the disciplining sync state displayed there, and the overall system sync state. The overall system sync will go into holdover when TFOM exceeds MAX TFOM. Once the holdover timeout expires, the system will then transition to out of sync. However, if the input reference table entry is still valid, the disciplining system will still be attempting to synchronize and align the system to the 1PPS reference to reduce the TFOM value. During this period, the “Rb (Sync)” indicator is asserted.

Oscillator lock State name changed (changed from “Sync” to “Trk/Lock” or “Track/Lock”)

(**Mantis Case 1880)** Version 4.8.8 update changed the reported state name, to also account for the newest Low Phase Noise Rb oscillator, also.

Note in this Mantis case from Dave Sohn: The new disciplining states associated with the low phase noise rubidium changed the lock state to track/lock to cover all oscillator cases. The procedure should be updated to reflect that.

**1PPS Phase Error / TFOM / MaxTFOM

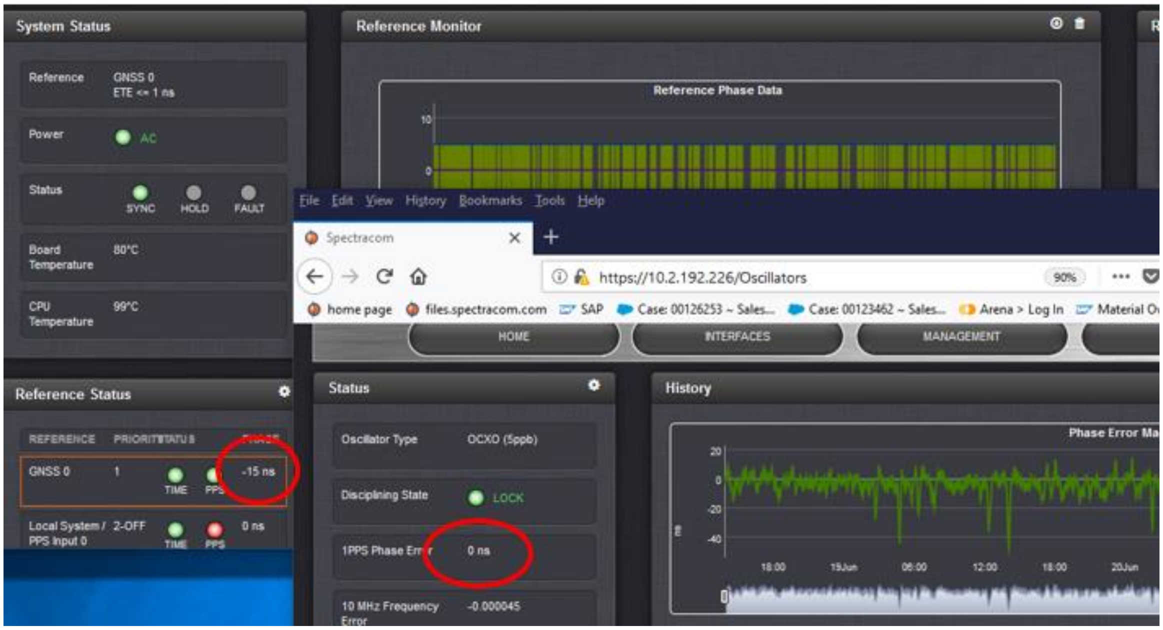
Disciplining 1PPS phase error

- Estimation of 1PPS error as compared with the Reference 1PPS input.
- 1PPS Phase Error can be a positive or negative number (negative phase error)

Notes about 1PPS Phase Error

1) "Side-by-side" variances between "disciplining" phase error values (reported in the Management -> Disciplining and Reference Priority pages) versus the phase error values reported in the Tools -> Reference Monitor page

- Due to differences in granularity in the ***Disciplining***/ ***Reference Priority*** pages, versus the ***Reference Monitor*** page. the phase error values for the same reference may be reported as two different values.
- s shown below, the phase error is reported as **0 ns** in the Disciplining page, while the GPS phase error is being reported as **-15 ns** in the ***Reference Monitor*** page



System Status

Reference: GNSS 0 ETE <= 1 ns

Power: AC

Status: SYNC HOLD FAULT

Board Temperature: 80°C

CPU Temperature: 99°C

Reference Status

REFERENCE	PRIORITY	STATUS	PHASE
GNSS 0	1	TIME PPS	-15 ns
Local System / PPS Input 0	2-OFF	TIME PPS	0 ns

https://10.2.192.226/Oscillators

Status

Oscillator Type: OCXO (5ppb)

Disciplining State: LOCK

1PPS Phase Error: 0 ns

10 MHz Frequency Error: -0.000045

Per Dave S (19 Jun 2018) I don't remember the direction of the offset (negative vs positive), but as far as the differences, the disciplining phase error is a filtered error, that has higher resolution. The reference monitor phase errors are raw offset values with a 20ns resolution. They should absolutely track each other in terms of trends, but due to the filtering and differences in resolution/granularity there will be differences in the reported offsets.

2) Effects on 1PPS Phase Error graphs if a GPS Offset (Cable delay) has been configured in the browser

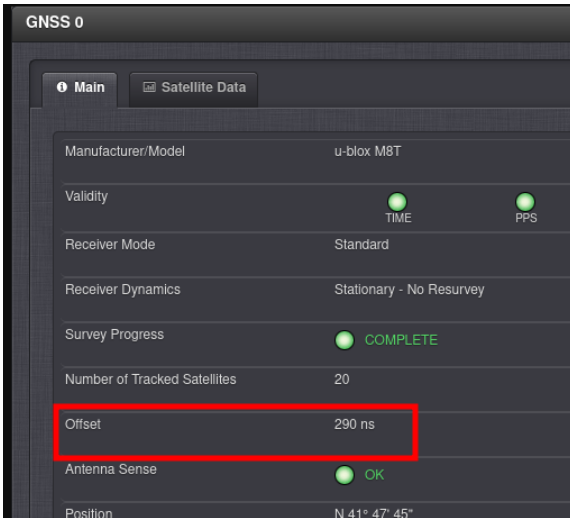
- Refer to Salesforce cases such as 289423 and *255365*

Unlike the Phase Error data reported in "**log_ref_mon_statuses**", the Phase Error data in **"log_oscillators"** is based on raw (no offset applied) GPS.

If any "**GPS Offset**" has been applied to the GPS configuration in the browser, Phase Error data reported in "**Ref Monitor**" will be offset by the value in the GPS Offset configuration (such as 800ns for instance). The Phase Error data in **Log_oscillators** is based on raw (no offset applied) GPS.

Example from Case 289423

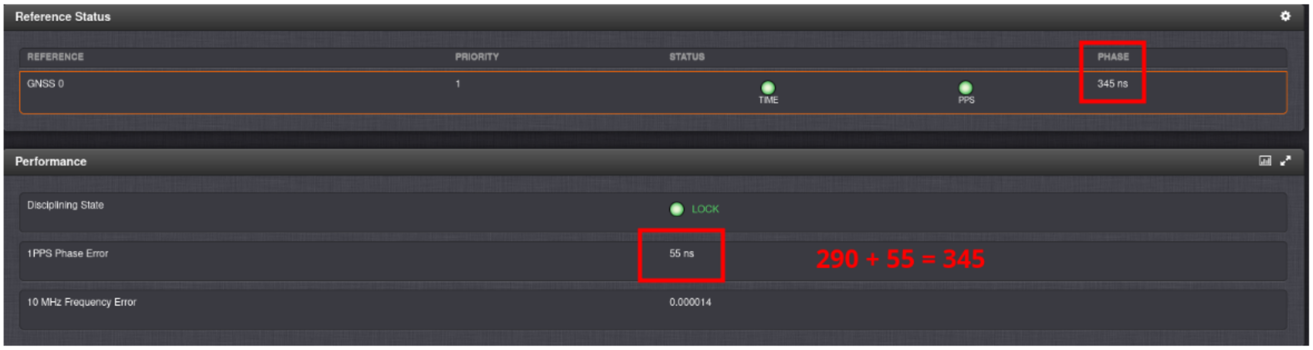
- Customer configured a **290ns** GPS cable delay/offset



GNSS 0

Manufacturer/Model	u-blox M8T
Validity	● TIME ● PPS
Receiver Mode	Standard
Receiver Dynamics	Stationary - No Resurvey
Survey Progress	● COMPLETE
Number of Tracked Satellites	20
Offset	290 ns
Antenna Sense	● OK
Position	N 41° 47' 45"

Also, just to make sure I 100% understand what you're saying. You're referring to this:



Reference Status

REFERENCE	PRIORITY	STATUS		PHASE
GNSS 0	1	● TIME	● PPS	345 ns

Performance

Disciplining State	● LOCK
1PPS Phase Error	55 ns
10 MHz Frequency Error	0.000014

290 + 55 = 345

Is that right? In essence, the antenna delay offset is a fixed offset and not accounted for with displaying the GNSS 0 phase of 345 ns. So the sum of the fixed offset and the actual 1PPS phase error of 55 is what we're seeing for the reference phase of 345 ns.

Another earlier Example below (both graphs from same SecureSync) per Salesforce Case 255365

Email from Ron Dries (12 Jan 2021) I looked at the logs and the sqlite data.

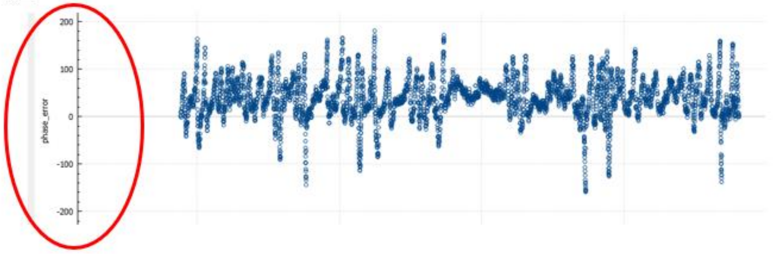
The difference between the phase error in log_oscillators and the phase measured in the log_ref_mon_statuses is due to having an offset configured for the GPS reference.

In journal.log.1 there are entries where they set the GPS offset from 600 to 897:

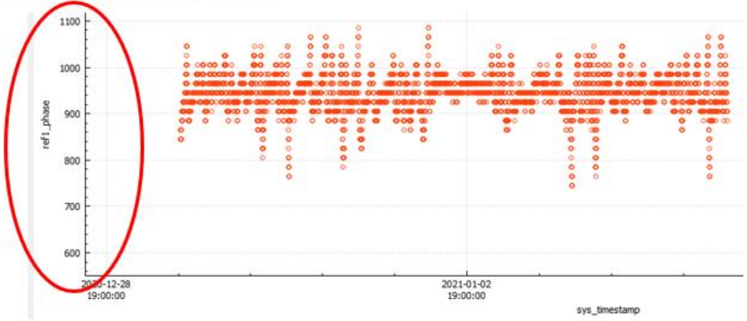
Feb 9 03:15:13 [webui] Changed Offset for GPS Reference 0 in slot 0 from GR (0)Offset: 600 to **GR (0) Offset: 897**

The reference monitor is a measurement taken before that offset gets applied

A) log_oscillators Phase Errors

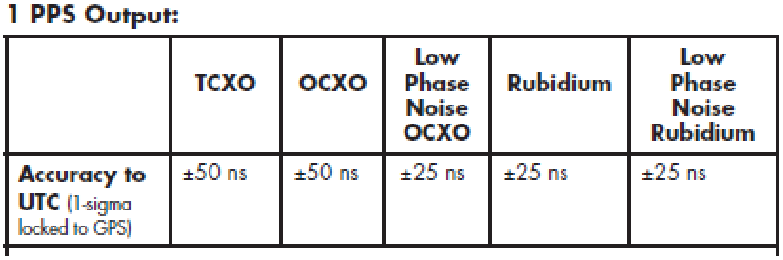


B) log_oscillators Phase Errors



3) Typical phase error values

- Below are the typical expected measurements of the System PPS to UTC time. Note these are not specs, but measurement "averages" over a period of time.



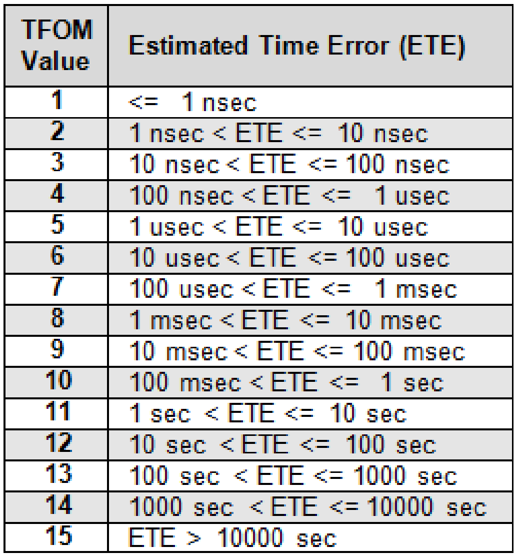
1 PPS Output:

	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium
Accuracy to UTC (1-sigma locked to GPS)	±50 ns	±50 ns	±25 ns	±25 ns	±25 ns

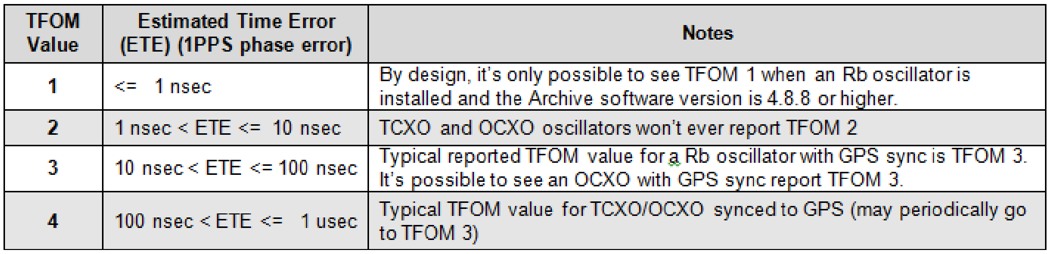
Per Dave Sohn "These are phase error estimates carried out in SW we provide to the customer to provide general status of the performance. They are in their nature a bit conservative and so should be taken in that regard"

Typical discipling1PPS phase error

- **TCXO/OCXO (synced to GPS): 10ns to 1us (TFOM 3 or 4)**
- **Rb (synced to GPS): 1ns to 1us (TFOM 4)**



TFOM Value	Estimated Time Error (ETE)
1	<= 1 nsec
2	1 nsec < ETE <= 10 nsec
3	10 nsec < ETE <= 100 nsec
4	100 nsec < ETE <= 1 usec
5	1 usec < ETE <= 10 usec
6	10 usec < ETE <= 100 usec
7	100 usec < ETE <= 1 msec
8	1 msec < ETE <= 10 msec
9	10 msec < ETE <= 100 msec
10	100 msec < ETE <= 1 sec
11	1 sec < ETE <= 10 sec
12	10 sec < ETE <= 100 sec
13	100 sec < ETE <= 1000 sec
14	1000 sec < ETE <= 10000 sec
15	ETE > 10000 sec



TFOM Value	Estimated Time Error (ETE) (1PPS phase error)	Notes
1	<= 1 nsec	By design, it's only possible to see TFOM 1 when an Rb oscillator is installed and the Archive software version is 4.8.8 or higher.
2	1 nsec < ETE <= 10 nsec	TCXO and OCXO oscillators won't ever report TFOM 2
3	10 nsec < ETE <= 100 nsec	Typical reported TFOM value for a Rb oscillator with GPS sync is TFOM 3. It's possible to see an OCXO with GPS sync report TFOM 3.
4	100 nsec < ETE <= 1 usec	Typical TFOM value for TCXO/OCXO synced to GPS (may periodically go to TFOM 3)

TCXO/OCXO 1PPS phase error

- With TCXO or either type of OCXO oscillator installed, it takes about 20 minutes to calculate this phase error.
- Phase Errors with a TCXO/OCXO can be either positive or negative numbers.
- Like with TFOM, while the oscillator is in in Free Run, the phase error continues to increase as an estimate, based on the general characteristics of the installed oscillator (it continues to ramp up).

Rubidium oscillator 1PPS Phase Error

- With a Rubidium oscillator installed, the oscillator reports this phase error every second.
- Phase Errors with a Rubidium oscillator will always be reported as a positive number, even if it's a negative value.
- Like with TFOM, while the oscillator is in in Free Run, the phase error continues to increase as an estimate, based on the general characteristics of the installed oscillator (it continues to ramp up).

Typical 1PPS Phase Error values to expect:

1) 1PPS Phase Errors with a TCXO/OCXO can be either positive or negative numbers.
2) With our House reference SecureSync, low phase noise Rb synced to GPS, the 1PPS Phase Error range for 24 hours was **23** to **159**.
3) With the Sales demo SecureSync, OCXO, the 1PPS Phase Error range for 24 hours was **-55** to **122**
4) 1PPS Phase Errors with a Rb oscillator will always be reported as a positive number, even if it's a negative value**,**

Per Dave Sohn (15 May 2014) Keith, I also believe the Rb error calculation is always provided as a magnitude value error, which means that regardless of whether it is actually positive or negative it is returned as a positive value.

1PPS Phase Error calculations while the oscillator is in Free-Run mode

While the oscillator is in Free Run (SecureSync's in Holdover mode), the Phase Error will continue to increase (ramp up) as an estimate based on the general characteristics of the type of oscillator installed.

- Like with TFOM, while the oscillator is in in Free Run, the phase error continues to increase as an estimate, based on the general characteristics of the installed oscillator (it continues to ramp up).

Report of current Phase error value

Current 1PPS phase error value is reported in:

- CLI command: **XO_GetPhaseError 0** <enter>
- Newer black/charcoal web browser: **Management** -> **Disciplining** page
- Phase: positive or negative number.

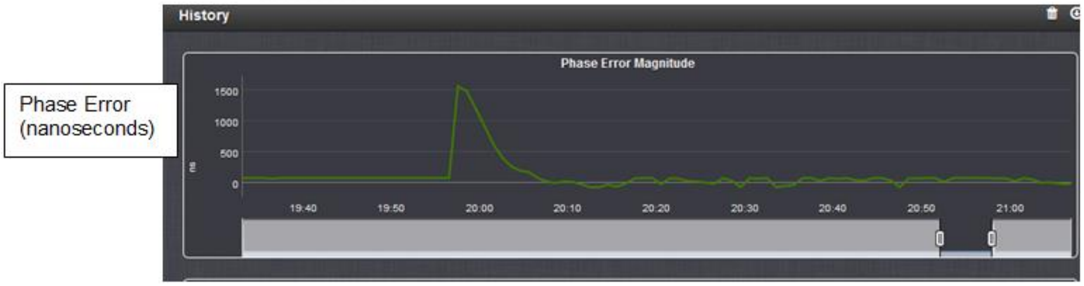
1. Logging phase error

- 1PPS phase error is periodically logged in the daily Discstats.log (refer to Discstats)
- Example (phase error is value in bold) 16438,6082,1,0,gps0,gps0,**32612**,42,-1.28e-10
- 1PPS Phase error can also be read via the CLI using the XO_GetPhaseError 0 command to see if on-time point is getting close to the input reference (should continue to decrease as it gets closer).
- Phase error can be a positive or negative number (positive phase error or negative phase error)

2. 1PPS phase error graph

web browser

Management -> Disciplining page (top graph)



- Vertical scale is dynamic
- Vertical scale (nanoseconds) is in either decimal dot or scientific notation depending on the amount of error.

The vertical scales vary depending upon the actual error values so pay close attention to the labeling. Above a certain value, a decimal notation is used (such as 0.01 seconds). Once the error value decreases, the values change to scientific notation (such as 2e-06).

The scientific breakdown is as follows:

1e-09 = 1 ns or 0000.000000001

1e-08= 10 ns
1e-07= 100ns
1e-06= 1 microsecond or 0000.000001000
1e-05= 10 microseconds 0000.000010000
1e-04= 100 microseconds or 0000.000100000
1e-03= 1 milliseconds or 0000.001000000
1e-02= 10 milliseconds or 0000.01000000
1e-01= 100 milliseconds or 0000.100000000
1e+00=1 second or 0001.000000000
1e+01= 10 Seconds or 0010.000000000
1e+02= 100 Seconds or 0100.000000000
1e+03= 1000 Seconds 1000.000000000

Note: If the first digit isn't a "1", multiply the first digit by the "time" value in the table above

Examples

2e-05= 20 microseconds or 0000.000020000 ("2" times "10 microseconds" is 20 microseconds)

5e-06= 5 microseconds or 0000.000050000 ("5" times "1 microseconds" is 5 microseconds)

A) web browser

To download the raw oscillator data

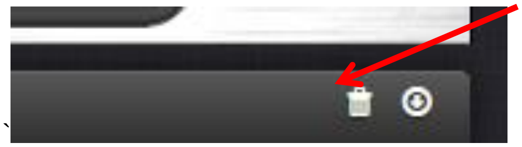
- Either a ".csv" or ".json" file with the oscillator values (and system temperatures) can be downloaded as desired.

1) Download of raw oscillator data as a ".csv" file (can be opened in excel)

- A ".csv" file can be downloaded using either of two different method (either via a download button in the Disciplining page or via a direct URL/

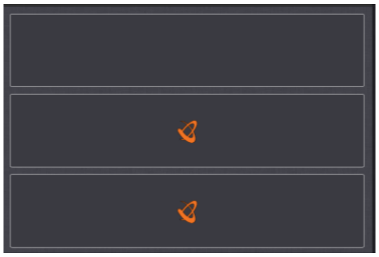
CSV file download button is available in the Management -> Disciplining page of the browser

From the **Management** -> **Disciplining** page of the browser (click on the "down arrow" ICON on the right side of the page to download the .csv file. Press the garbage can icon to delete all of the oscillator and temperature data used to display the graphs)

`

Note: The "garbage can" ICON on the upper-right corner clears/deletes all of the graph data.

Note: Deleting the log data will refresh the graphs.

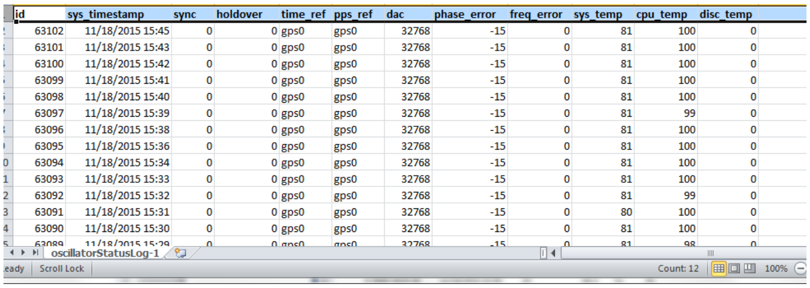


Manually enter the link to the OscillatorStatuslog

If you manually enter **/logs/OscillatorStatusLog.csv** after the URL of the SecureSync in the web browser it will download a csv file that can be opened in Excel with the GPS status log data.

Example: http://10.10.128.1/logs/OscillatorStatusLog.csv (change address as applicable)

Example .csv file output below (“Sys temp” and “**CPU temp**” fields were added in software version 5.3.0**)**



id	sys_timestamp	sync	holdover	time_ref	pps_ref	dac	phase_error	freq_error	sys_temp	cpu_temp	disc_temp
63102	11/18/2015 15:45	0	0	gps0	gps0	32768	-15	0	81	100	0
63101	11/18/2015 15:43	0	0	gps0	gps0	32768	-15	0	81	100	0
63100	11/18/2015 15:42	0	0	gps0	gps0	32768	-15	0	81	100	0
63099	11/18/2015 15:41	0	0	gps0	gps0	32768	-15	0	81	100	0
63098	11/18/2015 15:40	0	0	gps0	gps0	32768	-15	0	81	100	0
63097	11/18/2015 15:39	0	0	gps0	gps0	32768	-15	0	81	99	0
63096	11/18/2015 15:38	0	0	gps0	gps0	32768	-15	0	81	100	0
63095	11/18/2015 15:36	0	0	gps0	gps0	32768	-15	0	81	100	0
63094	11/18/2015 15:34	0	0	gps0	gps0	32768	-15	0	81	100	0
63093	11/18/2015 15:33	0	0	gps0	gps0	32768	-15	0	81	100	0
63092	11/18/2015 15:32	0	0	gps0	gps0	32768	-15	0	81	99	0
63091	11/18/2015 15:31	0	0	gps0	gps0	32768	-15	0	80	100	0
63090	11/18/2015 15:30	0	0	gps0	gps0	32768	-15	0	81	100	0
63089	11/18/2015 15:29	0	0	gps0	gps0	32768	-15	0	81	98	0

Definition of fields

Sync and **Holdover**: 1 is true, 0 is false

Time ref and **PPS ref:** Selected input reference at that time

DAC: Oscillator’s DAC value

Phase Error: 1PPS Phase Error

Freq Error: Oscillator’s Frequency Error

Temps: Board, CPU and **Oscillator**

Notes:

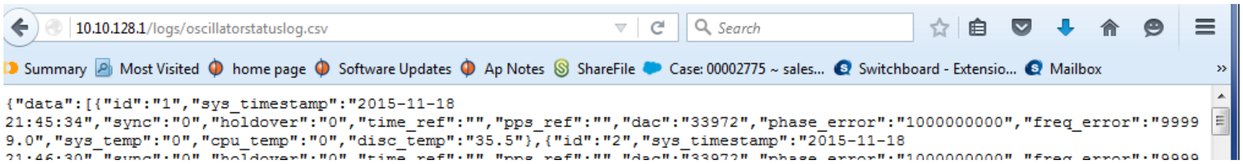
1. **Oscillator** temp is only available if sensor is installed on the main PCB
2. **Board** and **CPU** temps were added in software version 5.3.0

B. Output of graphable oscillator and temperature data as a .json file for graphing

Same process as downloading.csv file with direct link, but replace “.csv” with “**.json”** instead.

If you manually enter **/logs/OscillatorStatusLog.json** after the URL of the SecureSync in the web browser it will download a json file.

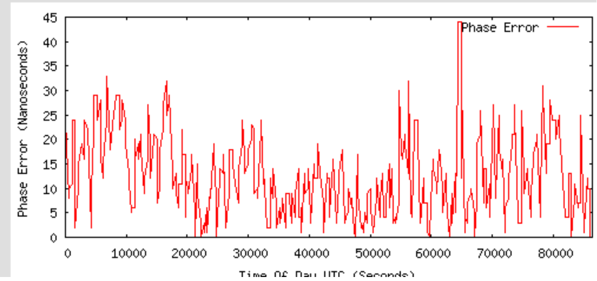
Example: http://10.10.128.1/logs/OscillatorStatusLog.json (change address as applicable)



10.10.128.1/logs/oscillatorstatuslog.csv
Search
Summary
Most Visited
home page
Software Updates
Ap Notes
ShareFile
Case: 00002775 ~ sales...
Switchboard - Extensio...
Mailbox

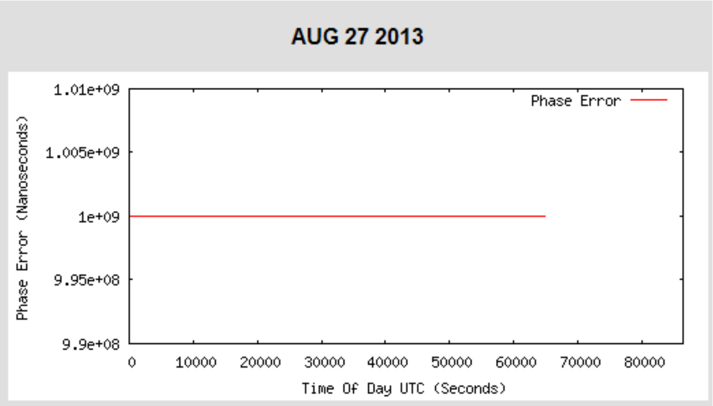
```
{"data":[{"id":"1","sys_timestamp":"2015-11-18
21:45:34","sync":"0","holdover":"0","time_ref":"","pps_ref":"","dac":"33972","phase_error":"1000000000","freq_error":"9999
9.0","sys_temp":"0","cpu_temp":"0","disc_temp":"35.5"},{"id":"2","sys_timestamp":"2015-11-18
21:46:30","sync":"0","holdover":"0","time_ref":"","pps_ref":"","dac":"33972","phase_error":"1000000000","freq_error":"9999
```

Email from Dave Sohn (12/12/12) Version 4.8.8 added phase and frequency error graphing on the unit. We generate files that include the phase and frequency errors as they are updated. Those could be pulled from the unit. We only keep the last 5 days on the box. As far as the actual logs go, we record the frequency error in the oscillator log as well.



Analyzing phase error graph (either browser)

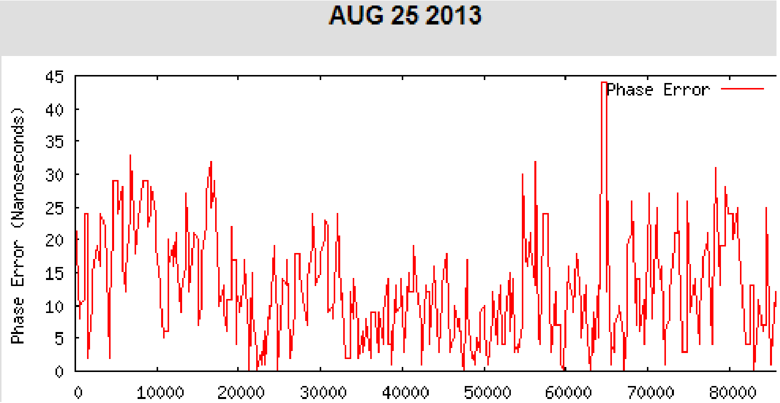
2) 10 MHz Phase Error graph showing straight line



Can be due to:

- SecureSync synced via USER/USER mode.
- SecureSync synced via NTP.
- SecureSync not synced to any reference (oscillator in free Run mode).

B. Phase Error graph showing large intermittent spikes



Can be due to:

- Ambient temperature changes
- Mechanical shock/vibration
- Intermittent GPS reception issues

**Restart tracking / Phase Error limit field

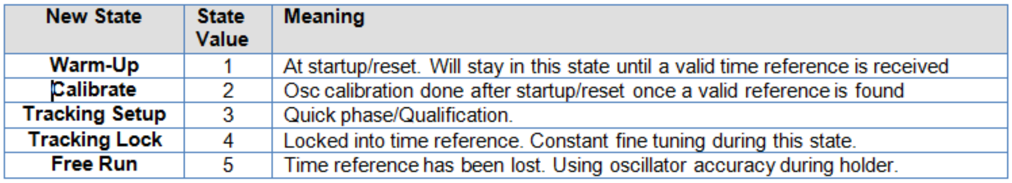
1PPS disciplining when all input references are lost for a period of time and then restored:

- **Rubidium oscillator installed**: The Rb oscillator's disciplining will cause the 1PPS (on-time point) from the oscillator to jump to align with the selected input reference 1PPS (not slewed over a period of time).
- **OCXO/TCXO oscillator installed**: Our Oscillator disciplining will slew the 1PPS (on-time point) from the oscillator to slew very slowly to the input reference 1PPS (not jumped to the reference).

Restart Tracking

- Restart tracking checkbox was added in software version 4.8.6
- ***Management*** -> ***Disciplining*** page of the newer black web browser
- Uses the **XO_SetMode 0 2** call.

Version 4.8.6 (June 2012) added a "Restart Tracking" capability to the **Management** -> **Disciplining** page of the web browser. When enabled, the oscillator goes back to the quickphase mode (hardware coarse adjust) one time to quickly re-align the oscillator to the PPS reference. Then, this field goes back to disabled. This needs to be performed each time it's desired to snap the PPS to the reference.



New State	State Value	Meaning
Warm-Up	1	At startup/reset. Will stay in this state until a valid time reference is received
Calibrate	2	Osc calibration done after startup/reset once a valid reference is found
Tracking Setup	3	Quick phase/Qualification.
Tracking Lock	4	Locked into time reference. Constant fine tuning during this state.
Free Run	5	Time reference has been lost. Using oscillator accuracy during holder.

Note: There was a Disciplining State value 6 at one time. But it was removed in an earlier version of software.

When performing a Restart Tracking

If you have a valid time reference connector to the board, the state should go from "1" to "4", "4" indicating it has locked in to the reference. If you were to remove the time reference, the state would go to "5" indicating that the unit was now in holdover mode.

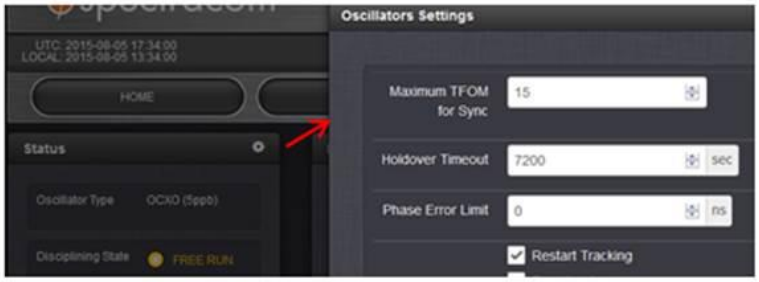
When the unit is in state "4", you should see the state change to "3" indicating that the unit is in the quick phase state and that the tracking has restarted.

Email from Keith (27 Jul 2015) Thanks for reporting what you are observing (or possibly were observing but no longer, by now) after connecting a new antenna. This is initially expected operation after connecting an antenna. The time it takes to clear the alarm thereafter, unless the unit is power cycled is dependent on how long it's been without an antenna

Once the SecureSync syncs to GPS after each power-up, it starts to adjust the oscillator. if power cycled/rebooted, it first snaps it in close with a hardware adjustment. Then it switches to very slow slewing via software. If it's not power cycled, It continues to slowly slew the oscillator until its re-aligned to GPS. During this whole time, the Frequency Error Alarm is asserted. Typically around 15 to 30 minutes after the SecureSync goes into sync to GPS, the oscillator's frequency is aligned very closely to 10 MHz (based on the GPS receiver's 1PPS signal), which causes the Frequency Error alarm (and associated Fault LED) to clear. But if it's been running a while without GPS, it can take a few hours for the Frequency Alarm to clear,

In lieu of power cycling the unit, you can also manually perform a "restart tracking" which speeds up this alignment (it is similar to a reboot as far as the oscillator is concerned with the oscillator once-again coarse adjusted to the 1PPS reference even though no reboot was actually performed).

To perform a restart tracking, navigate to the **Management** -> **Disciplining** page of the browser. On the left-side of the page, click on the "gear" icon to the right of "Status". In the pop-up window, select "**Restart Tracking**" and then press Submit.



UTC: 2015-08-05 17:34:00
LOCAL: 2015-08-05 13:34:00

Oscillator Type OCXO (5ppb)

Disciplining State ● FREE RUN

Oscillators Settings

Maximum TFOM for Sync: 15

Holdover Timeout: 7200 sec

Phase Error Limit: 0 ns

☑ Restart Tracking

The oscillator will now be realigned much faster to the GPS signal. The Frequency Error alarm should typically clear within about 15 to 30 minutes after performing this step.

Note this coarse adjust process without a reboot is a “one-time” event. The Restart Tracking checkbox doesn’t remain selected and a Restart Tracking will not be performed again, unless a user manually performs the same process again.

Associated Log entries for restart tracking

A) Timing log entry

Example entry below

Aug 6 13:57:33 Spectracom Spectracom: [system] 2013 218 13:57:33 000 Oscillator control: Reset.

B) Journal log entry for restart tracking

Example entry below

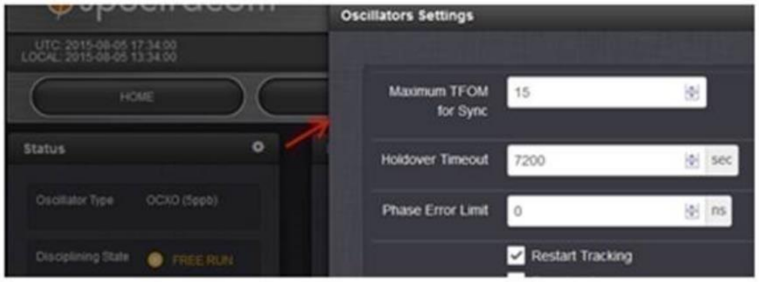
Aug 6 11:46:22 Spectracom Spectracom: [webui] Changed Mode for Oscillator in slot 0 from   XO Mode: 0 to   XO Mode: 2

Restart tracking not working (no DAC change or shift in 1PPS after issuing command)

1) Make sure an external input reference is present and valid.
2) With NTP input, software version needs to be version 5.3.0, which implanted host disciplining/

Phase Error limit field

- For TCXO and OCXO oscillators only (not Rb oscillators) ??



UTC: 2015-08-05 17:34:00
LOCAL: 2015-08-05 13:34:00

Oscillator Type OCXO (5ppb)

Disciplining State ● FREE RUN

Oscillators Settings

Maximum TFOM for Sync: 15

Holdover Timeout: 7200 sec

Phase Error Limit: 0 ns

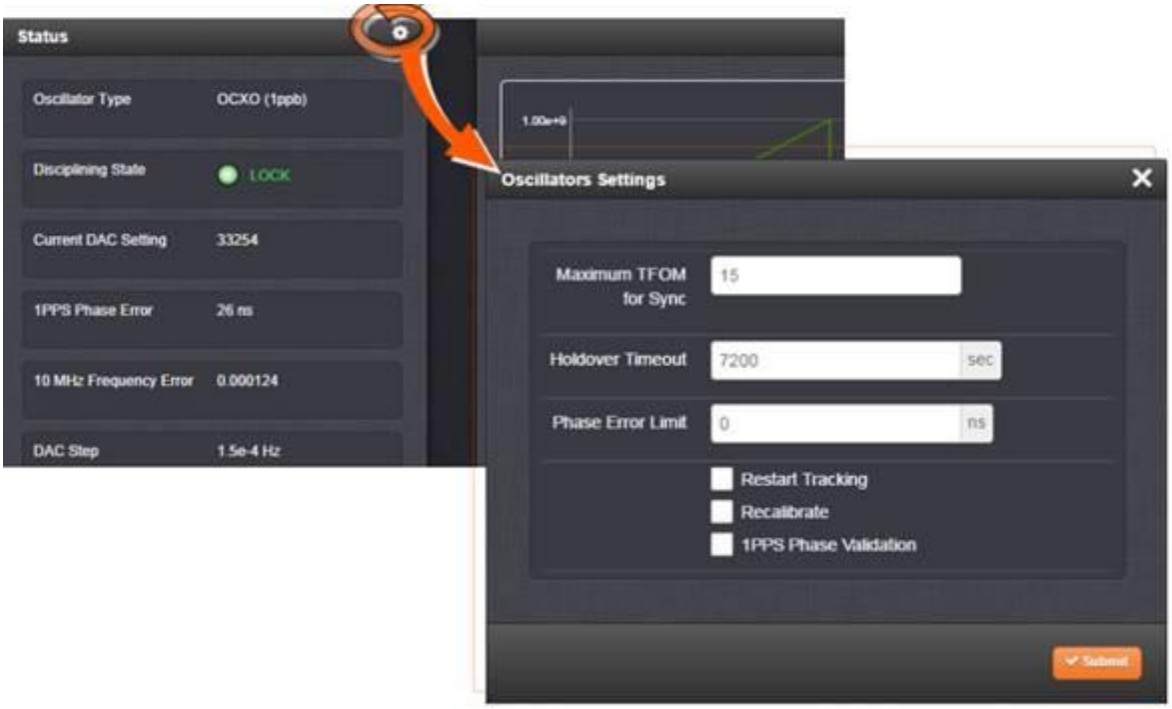
☑ Restart Tracking

A **phase error limit field** Edit window of the Disciplining page allowing for an automatic disciplining tracking restart, once the phase error limit is exceeded, thus avoiding manual intervention.

Email Keith sent (5 Aug 15) covering info on both “Restart Tracking” and “Phase Error Limit”

For more info on Restart tracking and./or Phase Error Limit, please refer to the online SecureSync user guide at: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/OscConfiguring.htm?Highlight=restart%20track

To either manually or automatically expedite the oscillator lock/relock, navigate to the **Management** -> **Disciplining** page of the browser. On the left side of the page, click on the Gear icon to the right of "Status". This will open a pop-up window (as shown below). Selecting the "Restart Tracking" checkbox at the bottom will start a "one-time" oscillator relocking (the same process as occurs the first time after each reboot that an external reference is applied). This process is only performrmed when a user selects this checkbox (it can be applied multiple times/whenever desired as long as there is an external reference available for it to lock to).



Oscillator Type	OCXO (1ppb)
Disciplining State	● LOCK
Current DAC Setting	33254
1PPS Phase Error	26 ns
10 MHz Frequency Error	0.000124
DAC Step	1.5e-4 Hz

Oscillators Settings

Maximum TFOM for Sync: 15

Holdover Timeout: 7200 sec

Phase Error Limit: 0 ns

□ Restart Tracking
□ Recalibrate
□ 1PPS Phase Validation

To alleviate manual intervention, the "Phase Error Limit field" in this same window is used to perform an "automatic Restart Tracking" whenever the 1PPS phase error (the offset between the internal 1PPS and the external input's 1PPS) exceeds a user-specified value. For instance, if the Phase Error limit is set to 1000ns, if the internal 1PPS is more than 1000ns different than the external 1PPS input, a "restart tracking" is performed at that time. Instead of slowly slewing 1000ns, the oscillator is hardware re-aligned to the reference, just like when a user manual initiates a "Restart Tracking".

TFOM (Time Figure Of Merit)

Report of current TFOM value

1. Reported on left side of the Management -> Disciplining page
2. Reported with the **SS_GetTfom 0** command
3. Reported at the end of the **status** CLI command (in conjuction with the configured MaxTfom value

Q. How does the SecureSync calculate the TFOM Value?

A. modified **reply from Keith (26 Jun 14)** The SecureSync uses the calculated phase error value as the input for the TFOM Calculation. This data is collected in a variable size window and the result compared to a table of set values to select the TFOM value.

The variable min and max measurement window gets complex. It is set depending on the accuracy of the reference source, the stability of the data and the type of oscillator used.

The TFOM is an estimate of the timing error of the board and meant to be used as an indicator of the general performance of the timing;

The Time Figure of Merit (TFOM) enumeration is defined to provide a dimensionless quality measure of the overall time/1PPS synchronization based on an Estimated Time Error (ETE). This measure is used for overall sync status of our clock to the internal 1PPS. Our synchronization definition is derived from our use of time and 1PPS to achieve both synchronization of time and synchronization of frequency.

Here's some information about TFOM for you:
In summary, a TFOM change from 3 to a 4 does not necessarily indicate any problems. You just want to make sure the front panel Sync LED is still green. If it's not solid green, the TFOM will slowly increase until the NetClock is back in sync again. It may have likely been at the top end of the range for a TFOM of 3, changed slightly and therefore became a TFOM of 4 (refer to the table further below). This is normal operation.

The TFOM value is really a factor of the type of oscillator installed and the stability/accuracy of the selected input reference that the SecureSync is synced to (With GPS typically being the best external reference for synchronization). TFOM values of 3 and 4 are expected values to see, when a TCXO or OCXO oscillator is installed and when it's synced to GPS. TFOMs are usually lower with a Rubidium oscillator installed, as long as the SecureSync is in sync.
The Time Figure of Merit (TFOM) enumeration is defined to provide a dimensionless quality measure of the overall time/1PPS synchronization based on an Estimated Time Error (ETE). This measure is used for overall sync status of internal 1PPS to the input reference 1PPS. Our synchronization definition is derived from the use of time and 1PPS to achieve both synchronization of time as well as synchronization of frequency.

Email from Dave Sohn (11/9/12) TFOM / ETE is a logarithmic scale of phase error to provide a high level view of the phase error magnitude. The phase error calculated is translated directly to a TFOM value using the table below, where the phase error falls in the ETE column (Table 4-1 in the user manual). The system determines phase differences and frequency differences between the input 1PPS reference and our system 1PPS based on our accurate system oscillator.

The TFOM (Time Figure of Merit) value is a very accurate comparison (Estimate- not a measurement) of the input reference 1PPS versus the 1PPS output from the oscillator disciplining circuit (which uses the input 1PPS as its reference). As the SecureSync is able to discipline itself to a very stable and accurate 1PPS, the TFOM values will decrease. However, if the input reference 1PPS is jittery or does not have a "crisp" rising edge that it can definitively define as the trigger point, each time the TFOM is calculated, the value is going to be higher than expected.

The current **TFOM value** can be viewed in the **Status** -> **Time and Frequency** page.

Note: As of at least version 5.1.7, TFOM values are not logged.

Phase Accuracy error can be viewed to see if on-time point is getting close to the input reference (should continue to decrease as it gets closer). The current 1PPS **Phase Error** can be viewed in the **Status->Time and Frequency** page.

TFOM Table for SecureSyncs

TFOM Value	Estimated Time Error (ETE) (1PPS phase error)	Notes
1	<= 1 nsec	Starting in **upgrade version 5.1.3** (improved disciplining), it's now possible for all oscillator types, any input reference, to report TFOM 1 and 2 Prior to version 5.1.3, it's only possible to see TFOM 1 when an Rb oscillator is installed and the Archive software version is 4.8.8 or higher.
2	1 nsec < ETE <= 10 nsec	Starting in upgrade **version 5.1.3** (improved disciplining), it's now possible for all oscillator types, any input reference, to report TFOMs 1 and 2. Prior to version 5.1.3, TCXO and OCXO oscillators won't ever report TFOM 2
3	10 nsec < ETE <= 100 nsec	Typical reported TFOM value for a Rb oscillator with GPS sync is TFOM 3.

		It’s possible to see an OCXO with GPS sync report TFOM 3.
4	100 nsec < ETE <= 1 usec	Typical TFOM value for TCXO/OCXO synced to GPS (may periodically go to TFOM 3)
5	1 usec < ETE <= 10 usec	
6	10 usec < ETE <= 100 usec	
7	100 usec < ETE <= 1 msec	
8	1 msec < ETE <= 10 msec	
9	10 msec < ETE <= 100 msec	
10	100 msec < ETE <= 1 sec	
11	1 sec < ETE <= 10 sec	
12	10 sec < ETE <= 100 sec	
13	100 sec < ETE <= 1000 sec	
14	1000 sec < ETE <= 10000 sec	
15	ETE > 10000 sec	Max TFOM 15 is the factory default setting. With MaxTFOM set to 15, MaxTFOM is never exceeded.

Notes about TFOM

1. TFOM value is updated:
   - About once-per-second with a Rubidium oscillator
   - About every 10 seconds with a TCXO or either type of OCXO oscillator installed. This is the amount of time it takes for the TFOM value to be calculated.
2. The TFOM is a calculated phase error between the reference 1PPS vs the disciplined 1PPS. With an RB, the oscillator reports this phase error every second. With an OCXO it takes about 10 minutes to calculate this phase error.
3. The calculated TFOM also adds on any correction applied in order to phase align the disciplined 1PPS to the 10 MHz from the oscillator. As corrections are made for this continuous alignment the amount of error correction are applied to the TFOM.
4. TFOM is a worst-case error measurement. It may be better than the measured error, but it won’t be any worse the measured error.
5. TFOM with an OCXO oscillator installed will be no less than 3 (never 1 or 2) because of values intentionally added to the measurements if they are “too good” for what is expected to be measured with an OCXO. This is to make sure the TFOM will be no less than 3 with the OCXO oscillator (Since we sample for very short periods of time, the values read may be VERY good during that time frame, but too good to be expected, so we throw in a correction factor so that the calculated TFOM isn’t BETTER than what the realistic values are.
6. TFOM with an Rb oscillator, synced to GPS should have a TFOM value of 3. It may on occasion go to a value of 2 for short periods of time, but for the most part, it should be a value of 3.

Known issues with TFOM:

TFOM 1 with no input reference

1. (Refer to Mantis case 1933)
2. Version 4.8.8 allows TFOM to be a “1” with a Rb oscillator installed, even without SecureSync being synced to a reference.

Time stamp for the last time the TFOM value changed to another number

Starting in Archive version 4.8.7, the **Status** -> **Disciplining** page of the browser also indicates the time stamp of the last time TFOM value changed to a different value (it doesn't display what TFOM it changed to- just that it changed at the specified date/time).

If the date/time stamp was three days ago, it's been the current TFOM value (as reported in the Status -> Time and Frequency page of the web browser) for the last three days straight (hasn't gone up or down, since the timestamp shown).

Desire to remotely monitor TFOM values:

(15 Nov 2012 KW) The TFOM values are not currently logged, but they can be monitored remotely, if desired.

3. Via the web browser.
4. Via the CLI interface using the tfomget command
5. Via an SNMP Get (from an SNMP Manager on the network). The SPECTRACOM-SECURESYNC-MIB file defines this (Refer to "ssSysStaTfom" in this MIB file)
6. Set MaxTFOM to a value other than 15. Them, send an email and/or SNMP trap when the TFOM exceeds the MAXtfom value. The "1PPS Not in Specification" alarm is asserted when this condition occurs. There is an available trap and/or email associated with this alarm. When TFOM is no longer exceeded, the "1PPS restored to Specification" log entry, and associated email/trap can indicate this.
7. Desire to remotely monitor (and record) TFOM values:
8. The TFOM value can also be polled via the tfomget CLI command. This command can be issued via telnet/SSH or via direct connect to the front panel DB9 SERIAL port. Using HyperTerminal, Procomm or Terraterm, (9600 baud, 8 bit, 1 Stop bit, No parity) issuing this command will return the TFOM. Refer to the attached HyperTerminal Application Note for info on this connection. I know with at least HyperTerminal, you can create a simple .txt file with nothing but this command in it. Then, in HyperTerminal, perform a Transfer -> Send Text File. HyperTerminal will continue to send the command until it has gone through the entire list (to make the list of this command huge, copy all and paste. This doubles the entries in the file, each time. Refer to the attached txt document.

HyperTerminal can also log all of the responses to this command (**Transfer** -> **Capture Text).**

Notes about remote monitoring of SNMP

1) Refer to the SNMP Application Note for more info on using SNMP to monitor TFOM.
2) Starting in Archive version 4.8.7, the **Status** -> **Disciplining** page of the browser also indicates the time stamp of the last time TFOM value changed to a different value (it doesn't display what TFOM it changed to- just that it changed at the specified date/time).

If the date/time stamp was three days ago, it's been the current TFOM value (as reported in the **Status** -> **Time and Frequency** page of the web browser) for the last three days straight (hasn't gone up or down, since the timestamp shown).

Notes about TFOM

1) The TFOM is a calculated phase error between the reference 1PPS vs the disciplined 1PPS.
2) With a Rubidium oscillator installed, the oscillator reports this TFOM error every second.

3) The TFOM value is recalculated/updated about every 20 seconds or so.

4) The calculated TFOM also adds on any correction applied in order to phase align the disciplined 1PPS to the 10 MHz from the oscillator. As corrections are made for this continuous alignment, the amount of error correction is applied to the TFOM.

5) TFOM is a worst-case error measurement. It may be better than the measured error, but it won't be any worse than the measured error.

6) **TFOM with an OCXO oscillator** installed will be no less than 3 (never 1 or 2) because of values intentionally added to the measurements if they are "too good" for what is expected to be measured with an OCXO. This is to make sure the TFOM will be no less than 3 with the OCXO oscillator (Since we sample for very short periods of time, the values read may be VERY good during that time frame, but too good to be expected, so we throw in a correction factor so that the calculated TFOM isn't BETTER than what the realistic values are.

7) **TFOM with an Rb oscillator** installed and with SecureSync synced to GPS, should have a TFOM value of 3. It may on occasion go to a value of 2 for short periods of time, but for the most part, it should be a value of 3.

8) **Note: (Per Dave Sohn)** Rubidium may take some time to settle into a low TFOM as it runs through disciplining.

9) **Note**: Starting in Application v4.8.8, TFOM can now be a "1" when a Rubidium oscillator is installed.

10) TFOM with no input reference after power-up will remain at 15, until an external reference becomes available.

11) The TFOM after all valid input references have been removed or declared no longer valid (Sync status was true) will initially stay at the TFOM value it was when the input references were no longer valid and will start to increment from there, based on the typical drift rates for the type of oscillator installed (If it was a 3, it will increment to a 4, etc).

12) The table above is the breakdown of the TFOM values to the corresponding Estimated Time Errors, based on the reported TFOM value:

13) High TFOM when using EPP0 (External 1PPS input)

14) The most common issue we see when customers use an external 1PPS input ("EPP0") as the 1PPS input reference is due to ringing of the signal because of improper termination. The input impendence of the 1PPS signal is high impedance. However, the 1PPS source may desire a 50 ohm termination into the TSync-PCIe-PCIe board (instead of high impedance). If the source desires a 50 ohm load termination, the input 1PPS may likely "ring" inside of the TSync-PCIe board. The ringing of the 1PPS signal prevents a "crisp" point at which the TSync-PCIe board can trigger on. With ringing of the signal present, the detected trigger point may coincidentally be at the right point, but it could also trigger too early or too late. So, with each 1PPS input when the signal is ringing, it may trigger at a different point on the signal each time. This prevents the disciplining circuit from being able to receive a stable 1PPS that is can accurately discipline to, and so the TFOM values will also be much higher than expected.

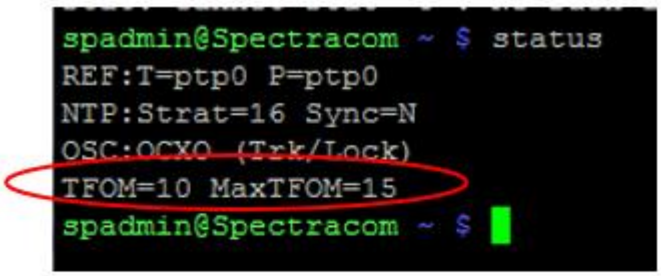
15) We have seen a few other similar cases where an external 1PPS input was causing a jittery 1PPS input because of improper termination of the signal at the input of the board. These were all resolved with a 50 ohm input being applied. To see this affect, if you have access to an oscilloscope, input the 1PPS signal from the source with a high input impedance setting on the scope. Look at the rising edge. You will likely see a ringing of the signal with no defined rising edge. Then, switch the scope to 50 ohm termination and you will likely notice the signal a become a crisp 1PPS with a very defined rising edge. This is what the board is also likely receiving and seeing, as well. To prevent the ringing of the 1PPS input from occurring and affecting the TSync-PCIe-PCIe board, terminate the 1PPS input from the source with a 50 ohm load resistor. This will often "clean up the signal" so that it can be a better reference into the board.

16) Let me know if adding the 50 ohm resistor from the input to ground allows the TFOM values to significantly decrease (TFOM values of 3 or 4 would be expected). For your information, the TFOM value is recalculated/updated about every 20 seconds or so.

MaxTFOM (Max TFOM/"Maximum TFOM for Sync")

A) Cli commands

- MaxTFOM cannot be set via the CLI (must be configured via the browser)
- Configured MaxTFOM value can be reported via CLI using either the **SS_GetMaxTfom 0** command or with the **status** command (which reports both the MaxTfom value as well as the current TFom value, as shown below):



```
spadmin@Spectracom ~ $ status
REF:T=ptp0 P=ptp0
NTP:Strat=16 Sync=N
OSC:OCXO (Trk/Lock)
TFOM=10 MaxTFOM=15
spadmin@Spectracom ~ $ 
```

(email from Keith 14 Sep 17) A short note for you regarding the SecureSync's "1PPS not in Specification" alarm being asserted (due to the TFOM value exceeding the MaxTFOM value). You may find this additional info below helpful in the future.

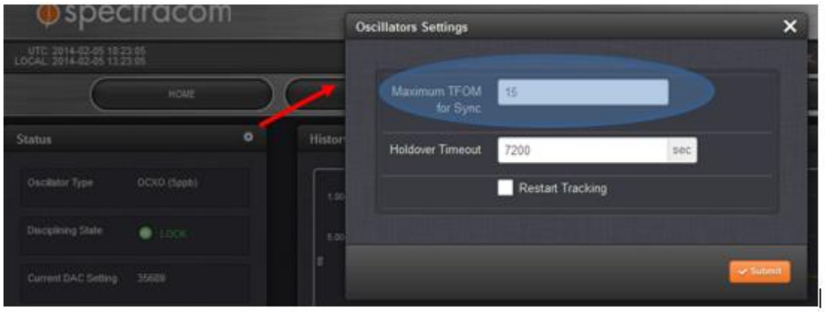
FYI- instead of needing to check the current TFOM and the MaxTFOM values via the browser, there is a convenient CLI command which will simultaneously report both the current TFOM value and the configured MaxTFOM value (there is a separate command available for each of these two values but this one command reports both at the same time).

Typing the CLI command of **status** <enter> will respond with both the current TFOM value, and the currently configured MaxTFOM value (as shown below). If the current MaxTFOM value is set to "3", while the TFOM value is a "4". the unit's MaxTFOM value just needs to be changed to a "4" instead. The MaxTFOM value can be changed via the **Management** > **Disciplining** page of the browser.

B) Web browser

- The MaxTFOM is configured in the Management -> Disciplining page and then clicking on the "gear" next to "Status"

Note the "MaxTFOM" field is configured in the **Management** -> **Disciplining** page of the newer (black/charcoal) web browser. As shown below, click on the gear icon to the right of "status" (on the left side of the page). The MaxTFOM field can be configured in the pop-up window that opens. Press Submit after changing this value.



UTC: 2014-02-05 18:23:05
LOCAL: 2014-02-05 13:23:05

Status

Oscillator Type OCXO (5ppb)

Disciplining State LOCK

Current DAC Setting 35689

Oscillators Settings

Maximum TFOM for Sync: 15

Holdover Timeout: 7200 sec

□ Restart Tracking

.

- When current TFOM value exceeds Max TFOM, SecureSync will go into "Holdover" mode, until TFOM falls below Max TFOM.

Important note: The input reference is still used to discipline the oscillator while TFOM is exceeding MaxTFOM. So, it's not truly in "Holdover" mode. It's just reported as being in "Holdover", until MaxTFOM is no longer exceeded.

- When TFOM exceeds MaxTFOM, "1PPS not in Specification" alarm is asserted. See note further below.

- When MaxTFOM is no longer exceeded, "1PPS Restored to Specification" is asserted. See note further below.
- (not applicable to the Rb oscillator) When current TFOM exceeds Max TFOM, OCXO/TCXO oscillator disciplining occurs faster.

Note: The two rates below do not apply to the Rb oscillator disciplining. There is no difference in the maximum rate of phase alignment based on TFOM during Rubidium disciplining.

- If the current TFOM value is less than or equal to the Max TFOM setting, the frequency of the oscillator is offset by a maximum of 0.4 Hz (40 ns/s) until the 1PPS is realigned.
- If the current TFOM value is more than the Max TFOM setting, the frequency of the oscillator is offset by a maximum of 4 Hz (400 ns/s) until the 1PPS is realigned.
- MaxTFOM is configured / viewed in the Setup->Disciplining page.
- MaxTFOM can be viewed in the Status->Time and Frequency page.
- Default MaxTFOM is 15 (TFOM never exceeds Max TFOM).
- If MaxTFOM is set to less than 15, User/User mode will not allow SecureSync to go into Sync.

The "**Maximum TFOM**" (Time Figure of Merit) field defines the largest TFOM value (TFOM is SecureSync's estimation of how accurately it is synchronized with its time and 1PPS reference inputs, based on several factors - known as the estimated time error or "ETE") that is allowed before disciplining is no longer performed on the oscillator. The larger the TFOM value, the less accurate SecureSync believes it is aligned with its 1PPS input that is used to perform disciplining. If this estimated error is too large, it could adversely affect the performance of oscillator disciplining. The available Max TFOM range is 1 through 15.

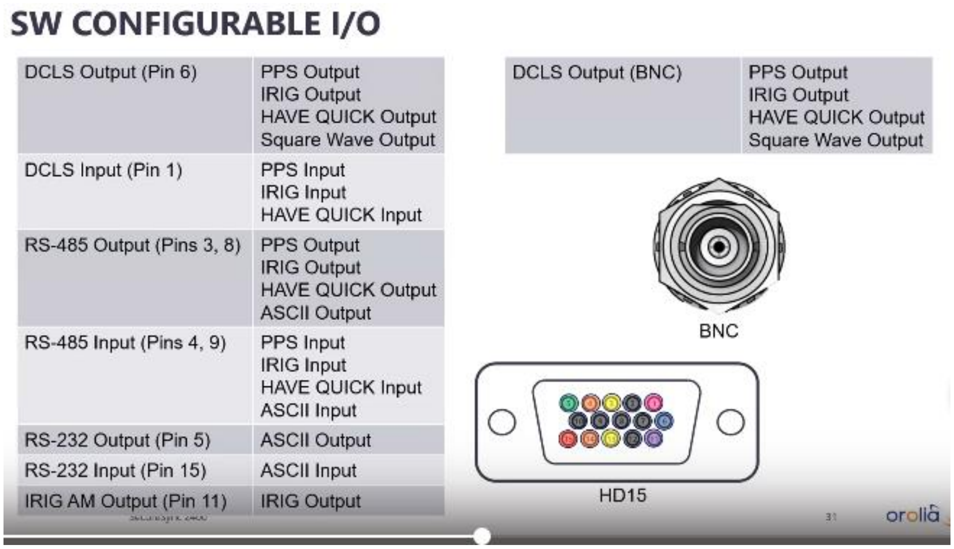
"1PPS not in Specification"/"1PPS Restored to Specification" entries in logs

These are events that occur and alarm entries that are asserted. "1PPS not in Specification" occurs if the current TFOM values exceed the user-configurable max TFOM value. When the TFOM falls below Max TFOM, the Restored to Specification event/alarm entry is asserted.

Regarding the "1PPS Not in Specification" alarm, this alarm only occurs if the current TFOM exceeds the user-configurable max TFOM value. The SecureSync going into Holdover mode will not initially and automatically cause the TFOM to increase and exceed the max TFOM value. However, if the unit continues to operate for an extended period of time without any valid input references, the oscillator will begin to drift. As long as the max TFOM is not set to 15, eventually, the max TFOM will be exceeded and the alarm is asserted. The type of oscillator (OCXO or Rubidium) and the setting of max TFOM will determine the typical amount of time in holdover required to exceed the max TFOM.

Inputs/Outputs

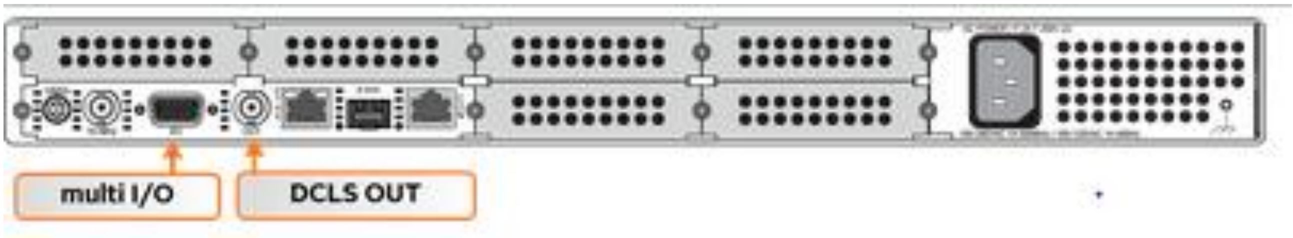
DCLS out and Multi I/O connector/ Breakout cable



SW CONFIGURABLE I/O

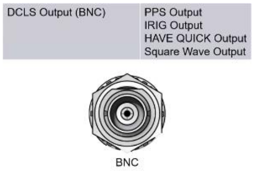
DCLS Output (Pin 6)	PPS Output IRIG Output HAVE QUICK Output Square Wave Output
DCLS Input (Pin 1)	PPS Input IRIG Input HAVE QUICK Input
RS-485 Output (Pins 3, 8)	PPS Output IRIG Output HAVE QUICK Output ASCII Output
RS-485 Input (Pins 4, 9)	PPS Input IRIG Input HAVE QUICK Input ASCII Input
RS-232 Output (Pin 5)	ASCII Output
RS-232 Input (Pin 15)	ASCII Input
IRIG AM Output (Pin 11)	IRIG Output

DCLS Output (BNC)	PPS Output IRIG Output HAVE QUICK Output Square Wave Output

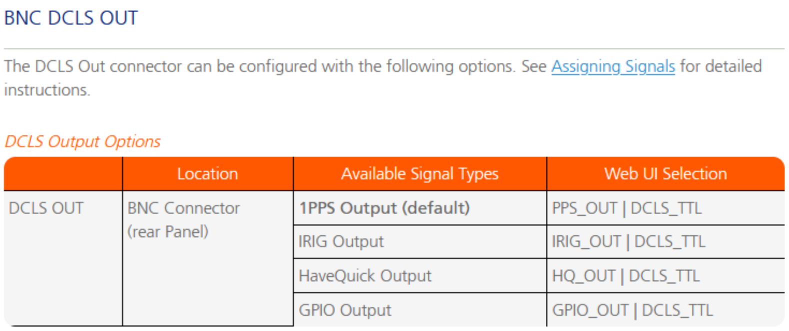


A) Rear panel configurable DCLS output (BNC)

- Refer to online 2400 SecureSync user guide at: http://manuals.spectracom.com/2400/Content/NC_and_SS/2400/INSTALL/Conf_15pin_BNC.htm



DCLS Output (BNC)	PPS Output IRIG Output HAVE QUICK Output Square Wave Output



BNC DCLS OUT

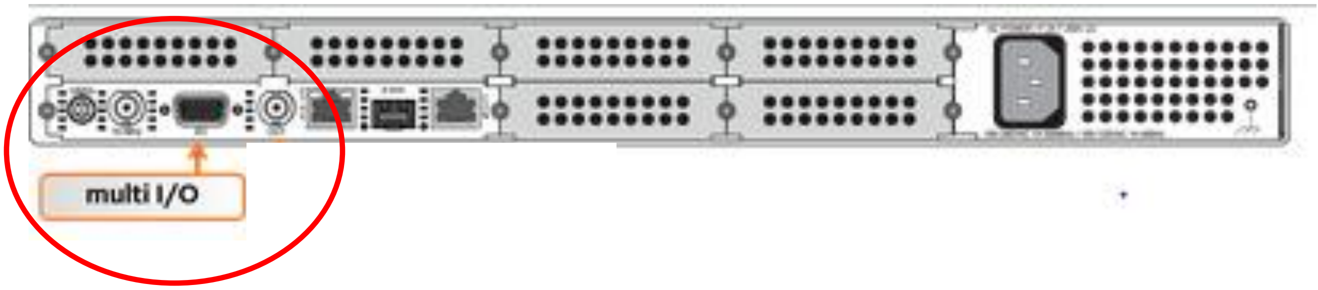
The DCLS Out connector can be configured with the following options. See Assigning Signals for detailed instructions.

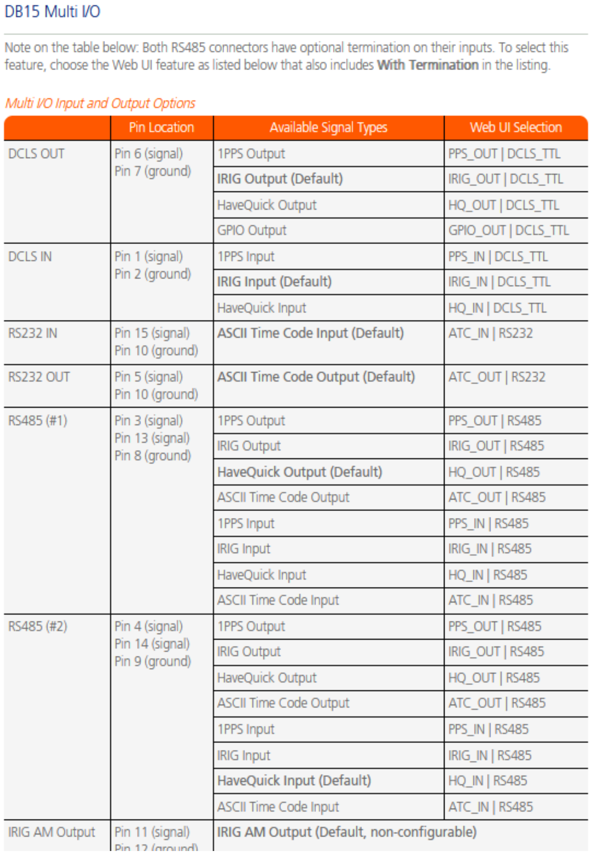
DCLS Output Options

	Location	Available Signal Types	Web UI Selection
DCLS OUT	BNC Connector (rear Panel)	**1PPS Output (default)**	PPS_OUT | DCLS_TTL
		IRIG Output	IRIG_OUT | DCLS_TTL
		HaveQuick Output	HQ_OUT | DCLS_TTL
		GPIO Output	GPIO_OUT | DCLS_TTL

Rear panel Multi I/O connector (HD15-pin) and breakout cable

- Provides Software configurable Inputs/Outputs
- Refer to online 2400 SecureSync user guide at: http://manuals.spectracom.com/2400/Content/NC_and_SS/2400/INSTALL/Conf_15pin_BNC.htm
- Refer also to GPIO pins in the TSync-PCIe Timing board assist doc.
- Refer also to available/optional Breakout cable (in the next section)



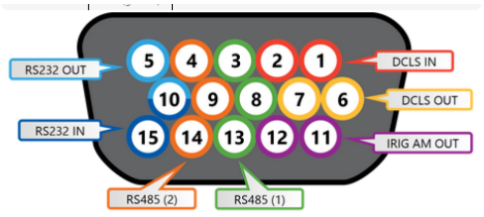


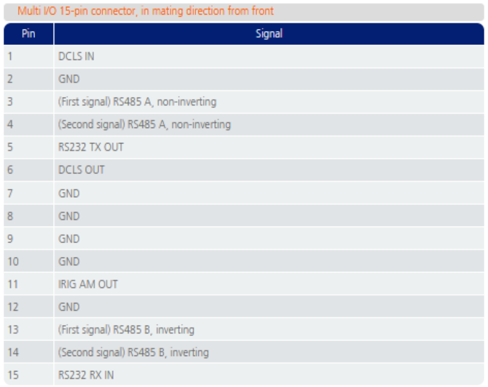
DB15 Multi I/O

Note on the table below: Both RS485 connectors have optional termination on their inputs. To select this feature, choose the Web UI feature as listed below that also includes **With Termination** in the listing.

Multi I/O Input and Output Options

	Pin Location	Available Signal Types	Web UI Selection
DCLS OUT	Pin 6 (signal) Pin 7 (ground)	1PPS Output	PPS_OUT | DCLS_TTL
		IRIG Output (Default)	IRIG_OUT | DCLS_TTL
		HaveQuick Output	HQ_OUT | DCLS_TTL
		GPIO Output	GPIO_OUT | DCLS_TTL
DCLS IN	Pin 1 (signal) Pin 2 (ground)	1PPS Input	PPS_IN | DCLS_TTL
		IRIG Input (Default)	IRIG_IN | DCLS_TTL
		HaveQuick Input	HQ_IN | DCLS_TTL
RS232 IN	Pin 15 (signal) Pin 10 (ground)	**ASCII Time Code Input (Default)**	ATC_IN | RS232
RS232 OUT	Pin 5 (signal) Pin 10 (ground)	**ASCII Time Code Output (Default)**	ATC_OUT | RS232
RS485 (#1)	Pin 3 (signal) Pin 13 (signal) Pin 8 (ground)	1PPS Output	PPS_OUT | RS485
		IRIG Output	IRIG_OUT | RS485
		HaveQuick Output (Default)	HQ_OUT | RS485
		ASCII Time Code Output	ATC_OUT | RS485
		1PPS Input	PPS_IN | RS485
		IRIG Input	IRIG_IN | RS485
		HaveQuick Input	HQ_IN | RS485
		ASCII Time Code Input	ATC_IN | RS485
RS485 (#2)	Pin 4 (signal) Pin 14 (signal) Pin 9 (ground)	1PPS Output	PPS_OUT | RS485
		IRIG Output	IRIG_OUT | RS485
		HaveQuick Output	HQ_OUT | RS485
		ASCII Time Code Output	ATC_OUT | RS485
		1PPS Input	PPS_IN | RS485
		IRIG Input	IRIG_IN | RS485
		HaveQuick Input (Default)	HQ_IN | RS485
		ASCII Time Code Input	ATC_IN | RS485
IRIG AM Output	Pin 11 (signal) Pin 12 (ground)	**IRIG AM Output (Default, non-configurable)**	





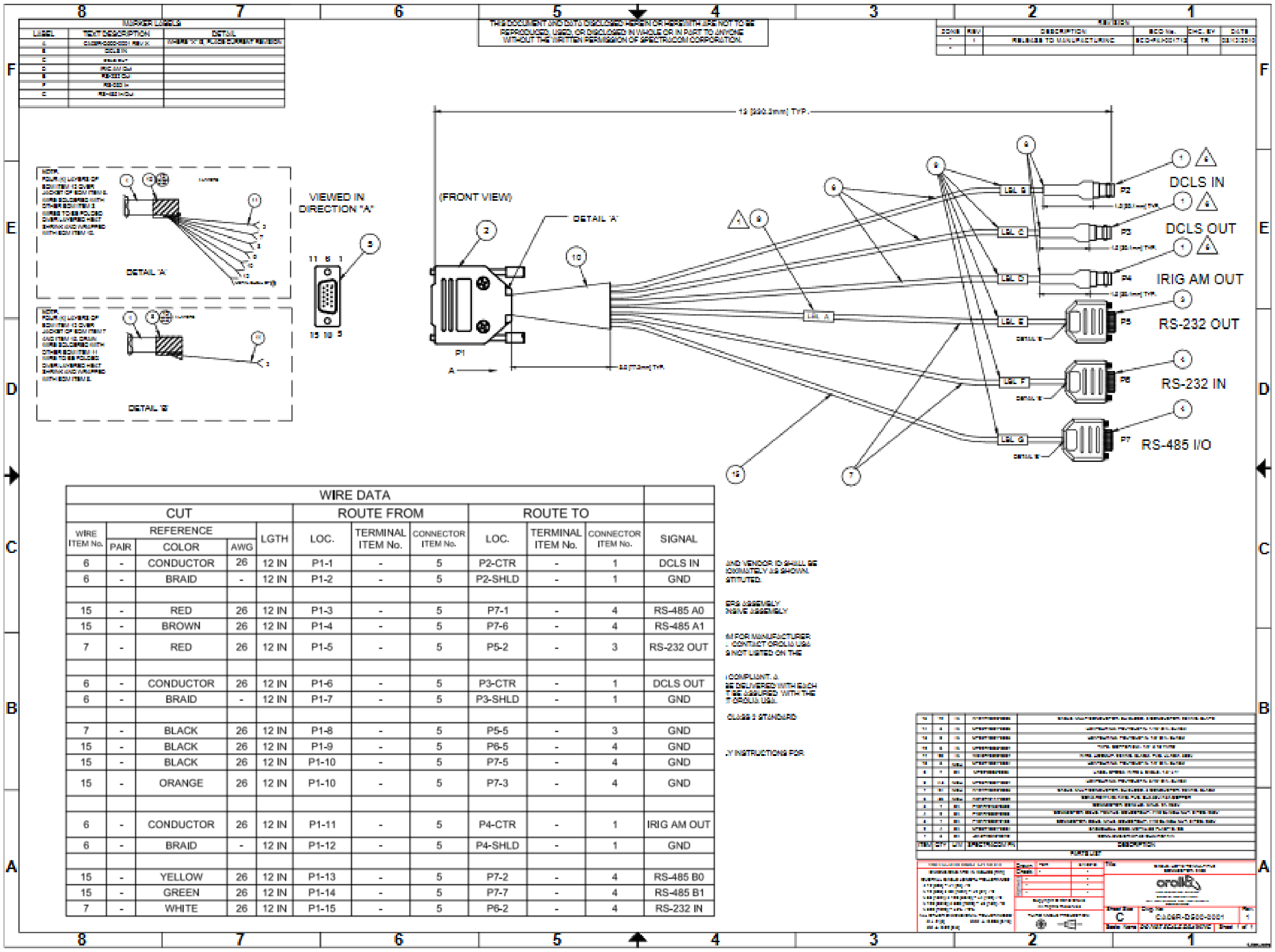
Multi I/O 15-pin connector, in mating direction from front

Pin	Signal
1	DCLS IN
2	GND
3	(First signal) RS485 A, non-inverting
4	(Second signal) RS485 A, non-inverting
5	RS232 TX OUT
6	DCLS OUT
7	GND
8	GND
9	GND
10	GND
11	IRIG AM OUT
12	GND
13	(First signal) RS485 B, inverting
14	(Second signal) RS485 B, inverting
15	RS232 RX IN

SecureSync 2400 Breakout Cable (P/N CA08R-D500-0001) for Multi I/O DB15 Connector

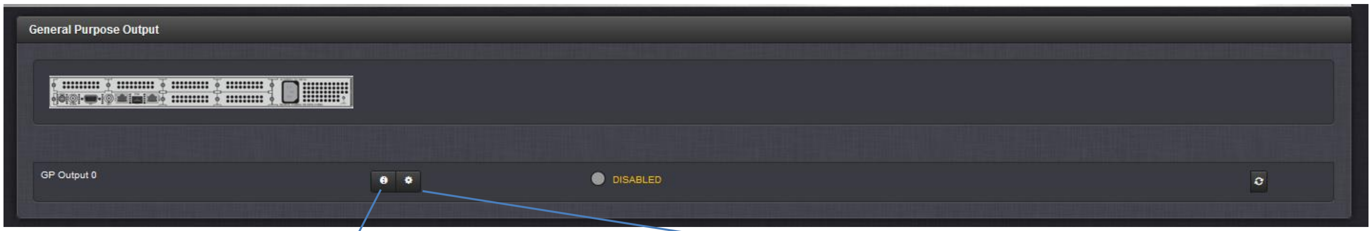
- ➢ Release of this new breakout - Refer to ECO-FAI-1713 (in Arena): https://app.bom.com/changes/detail-summary?change_id=2393758764
- ➢ Part Description: “CABLE, HD-15 TO MULTIPLE CONNECTOR, 2400”

Drawing P/N: **CA08R-D500-0001r1 (in Arena):** https://app.bom.com/items/detail-spec?item_id=1252913251&version_id=11092791388&



WIRE DATA												
CUT					ROUTE FROM			ROUTE TO				
WIRE ITEM No.	REFERENCE			LGTH	LOC.	TERMINAL ITEM No.	CONNECTOR ITEM No.	LOC.	TERMINAL ITEM No.	CONNECTOR ITEM No.	SIGNAL	
	PAIR	COLOR	AWG									
6	-	CONDUCTOR	26	12 IN	P1-1	-	5	P2-CTR	-	1	DCLS IN	
6	-	BRAID	-	12 IN	P1-2	-	5	P2-SHLD	-	1	GND	
15	-	RED	26	12 IN	P1-3	-	5	P7-1	-	4	RS-485 A0	
15	-	BROWN	26	12 IN	P1-4	-	5	P7-6	-	4	RS-485 A1	
7	-	RED	26	12 IN	P1-5	-	5	P5-2	-	3	RS-232 OUT	
6	-	CONDUCTOR	26	12 IN	P1-6	-	5	P3-CTR	-	1	DCLS OUT	
6	-	BRAID	-	12 IN	P1-7	-	5	P3-SHLD	-	1	GND	
7	-	BLACK	26	12 IN	P1-8	-	5	P5-5	-	3	GND	
15	-	BLACK	26	12 IN	P1-9	-	5	P6-5	-	4	GND	
15	-	BLACK	26	12 IN	P1-10	-	5	P7-5	-	4	GND	
15	-	ORANGE	26	12 IN	P1-10	-	5	P7-3	-	4	GND	
6	-	CONDUCTOR	26	12 IN	P1-11	-	5	P4-CTR	-	1	IRIG AM OUT	
6	-	BRAID	-	12 IN	P1-12	-	5	P4-SHLD	-	1	GND	
15	-	YELLOW	26	12 IN	P1-13	-	5	P7-2	-	4	RS-485 B0	
15	-	GREEN	26	12 IN	P1-14	-	5	P7-7	-	4	RS-485 B1	
7	-	WHITE	26	12 IN	P1-15	-	5	P6-2	-	4	RS-232 IN	

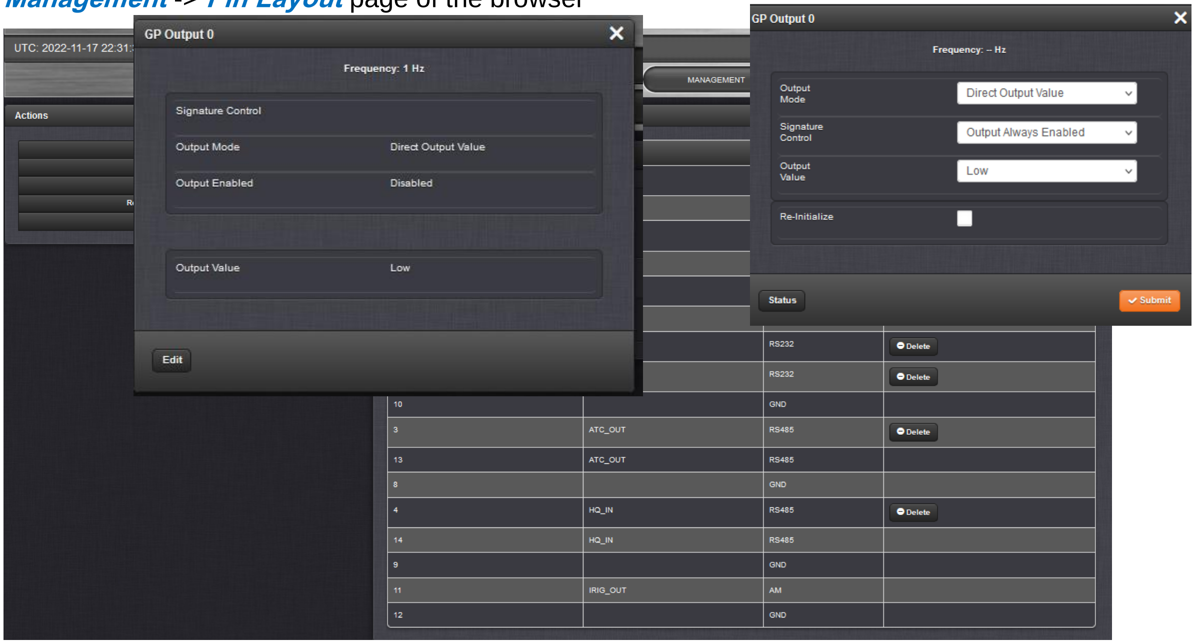
Interfaces -> ***General Purpose Output*** (**GP output 0**) page of the browser



General Purpose Output

GP Output 0 ● DISABLED

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



UTC: 2022-11-17 22:31:

GP Output 0

Frequency: 1 Hz

Signature Control

Output Mode	Direct Output Value
Output Enabled	Disabled
Output Value	Low

GP Output 0

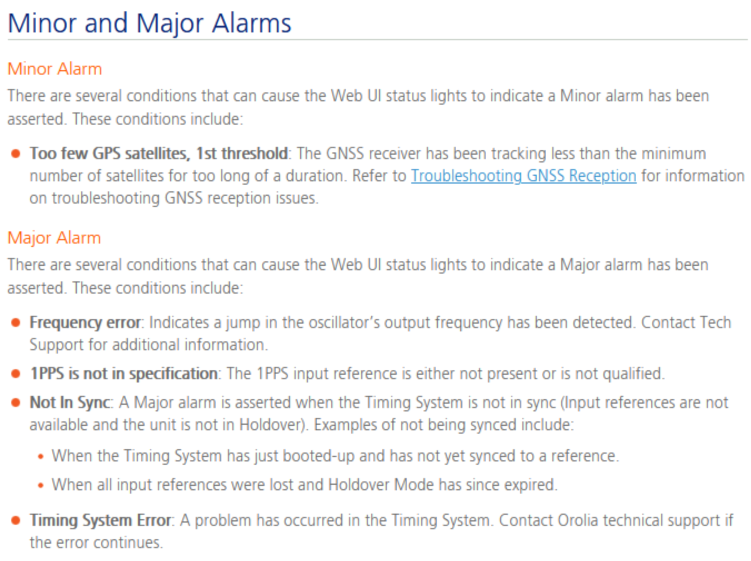
Frequency: -- Hz

Output Mode	Direct Output Value
Signature Control	Output Always Enabled
Output Value	Low
Re-Initialize	□

		RS232	Delete
		RS232	Delete
10		GND	
3	ATC_OUT	RS485	Delete
13	ATC_OUT	RS485	
8		GND	
4	HQ_IN	RS485	Delete
14	HQ_IN	RS485	
9		GND	
11	IRIG_OUT	AM	
12		GND	

Alarms (Major and Minor alarms)

- Refer to the online 2400 SecureSync user guide for Minor and Major alarms http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/TROUBLE/MinMajAlarm.htm?Highlight=alarms



Minor and Major Alarms

Minor Alarm

There are several conditions that can cause the Web UI status lights to indicate a Minor alarm has been asserted. These conditions include:

- **Too few GPS satellites, 1st threshold**: The GNSS receiver has been tracking less than the minimum number of satellites for too long of a duration. Refer to Troubleshooting GNSS Reception for information on troubleshooting GNSS reception issues.

Major Alarm

There are several conditions that can cause the Web UI status lights to indicate a Major alarm has been asserted. These conditions include:

- **Frequency error**: Indicates a jump in the oscillator's output frequency has been detected. Contact Tech Support for additional information.
- **1PPS is not in specification**: The 1PPS input reference is either not present or is not qualified.
- **Not In Sync**: A Major alarm is asserted when the Timing System is not in sync (Input references are not available and the unit is not in Holdover). Examples of not being synced include:
  - When the Timing System has just booted-up and has not yet synced to a reference.
  - When all input references were lost and Holdover Mode has since expired.
- **Timing System Error**: A problem has occurred in the Timing System. Contact Orolia technical support if the error continues.

A) Alarms classified as Major alarms

1. 1PPS is not in specification

- The 1PPS input reference is either not present or is not qualified. TFOM exceeds Maximum TFOM (MaxTFOM)

2. (User-defined Major alarm) (GPS receiver)

This alarm indicates a user has configured the NTP time server to assert a Major alarm upon the GPS receiver falling below a specified number of satellites, for a user-specified length of time. For example, a user can configure this alarm to be asserted if the unit was tracking at least five satellites, but sometime thereafter, it starts tracking only three satellites, by setting the threshold at 4 satellites. Since this alarm threshold is not directly related to the minimum number of satellites required by the system, the presence of this alarm does not automatically indicate a problem with GPS reception.

The number of satellites for the alarm threshold and whether the receiver dropping below this user-specified number of satellites is classified as a Major alarm or as a Minor alarm is configured in the System/Alarm page of the web browser.

3. GPS receiver fault

- indicates a problem with the internal GPS receiver.

4. Time Sync alarm

- Indicates the NTP server has lost synchronization to its external reference (GPS, IRIG etc) and has also timed-out of the Holdover mode (as configured in the System/Holdover page of the browser) OR The unit was rebooted (it will be in a Time Sync alarm until it is resynced to its external reference after every reboot/power cycle).

Note: this alarm is asserted after every boot-up

Rubidium Monitor alarm:

- ➢ Indicates a potential issue with the Rubidium oscillator has occurred.

  Note: This alarm can be caused by a low voltage input to the NTP time server. Time servers with Option 4 installed require 24vdc input power instead of 12vdc input. If the time server has 12vdc applied, the time server may appear to be operating normally with this alarm present.

During the Time Sync Alarm, all of the outputs, including NTP, will indicate that the NTP server is not in sync. In most cases, PCs and other systems connected to the NTP server will ignore it while the Time Sync alarm is present. They will likely fall back to using their own internal time base to derive the time. The primary external reference will need to be restored for devices to be able to use the NTP server as a time reference (or it may need several minutes to resync to the primary reference if it was recently rebooted/power cycled).

5. Frequency error alarm (Freq Error alarm):

Note: this alarm is asserted after every boot-up

- ➢ Frequency Error alarm is NOT due to the size of the frequency error. It means the DAC is within 10% of its max range

Per Dave Sohn (2 Dec 2020) The frequency alarm is related to the DAC as a frequency control alarm that is set if we get within 10% of our DAC control range limits. It is unrelated to our calculated phase or frequency values

To trigger an alarm if the phase error exceeds a certain threshold, the user could set a “Max TFOM for Sync” value which will automatically switch the SecureSync to Holdover mode if a certain phase error values is exceeded. The Holdover event will trigger alarms from the SecureSync.

Here is the section of the User Manual with more information:

http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/OscConfiguring.htm?

Email Dave L sent (8 Dec 2020) The jump in the oscillator frequency may not trigger a Frequency Alarm.

In the Securesync, the frequency alarm is generated when the DAC which controls the oscillator frequency gets within 10% of our DAC control range limits. It is unrelated to our calculated phase or frequency values shown in the oscillator log.

To trigger an alarm if the phase error exceeds a certain threshold, the user could set a “Max TFOM for Sync” value which will automatically switch the Securesync to Holdover mode if a certain phase error values is exceeded. The Holdover event will trigger alarms from the Securesync.

Here is the section of the User Manual with more information:
http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/OscConfiguring.htm?

The Frequency Error Alarm is asserted when 10 MHz Frequency Error measurement exceeds a set threshold (oscillator dependent)

- ○ **TCXO oscillator**: 1x10-7 in v5.3.0 and below (changed to 1x10-6 starting in v5.3.1 to address. See note below about Mantis case 3168)
- ○ **OCXO oscillator**” 1x10-8
- ○ **Rubidium** (and **low phase noise Rubidium-LPN Rb):** 1x10-9

  Note: (Applicable only to the Hughes special CGU SecureSync) the Frequency Error Alarm can also be asserted due to PLL Lock issues associated with the Wentzel oscillator. Refer to the Specials section of this doc for more info on this special.

Mantis case 3168: Issue with TCXO oscillator asserting Freq Error Alarms when exiting Sync

- Issue with software versions 5.3.0 and below (fixed in version 5.3.1, Dec 2015)
- Refer to Mantis case 3168 (Freq error threshold needed to be changed to 1x10-6 instead of 1x10-7)

Determine type of oscillator installed:

- **Via newer Web browser**: ***Management*** -> ***Disciplining*** page
- **Via CLI command**: **XO_GetOsctype** <enter>

Possible causes of the Freq Error alarm (Frequency Error alarm) being asserted

Per Dave Sohn: The Frequency Error Alarm should only ever be asserted if a disciplining reference (such as GPS) is present/valid (and also at boot-up). However, there have been a couple of software issues causing it to be asserted when it shouldn't be.

1. **Measured Frequency error exceeds:**
    - **Rubidium** (**and low phase noise Rubidium-LPN Rb**): Measured frequency error exceeds $1x10^{-9}$
    - **OCXO oscillator**: Measured frequency error exceeds $1x10^{-8}$
    - **TCXO oscillator**: Measured frequency error exceeds:
    - **$1x10^{-7}$** in v5.3.0 and below
    - **$1x10^{-6}$** starting in v5.3.1 to address.

Mantis cases associated with Frequency Error Alarms

- **Mantis Case 3168 (TCXOs)**

2. **Other reasons the Freq Error alarm may be asserted**
    - A Wenzel oscillator is installed in / connected to the SecureSync (such as with the "CGU SecureSync" special for Hughes) and there is an issue with either of the two (2) PLL circuits in the Wenzel oscillator
    - Note: Associated lock status messages are asserted in the oscillator log (refer to osc.log or CGU for Hughes in this document for details
    - This alarm is asserted after each boot-up for a period of time (it should clear within a few minutes later- its asserted until the oscillator has been coarse adjusted.)
    - Jitter on the input reference (such as PTP IRIG or external 1PPS input, for example).
    - Switching from one reference to another.
    - Enabling at least one reference in the Reference Priority table (with all references previously disabled)
    - Performing a restart tracking of the oscillator.
    - Faulty oscillator
    - TCXO oscillator with versions
    - Syncing via NTP input with either:

- Rb oscillator installed OR
- Software versions 5.3.0 and below with TCXO/OCXO installed (host disciplining for TCXO/OCXO was added in v5.3.1)

Note: Freq Error alarm can be asserted when the Freq error is reported AT the threshold (not exceeded) due to "rounding"

- There is rounding that goes on in the oscillator frequency errors in the logs. So if the log indicates a frequency count AT the specified threshold, the Frequency Error alarm can still be asserted, because the measured values in decimal values still exceeded the threshold (for example with a Rb oscillator- if the actual frequency error is 3.0000001, the osc.log entry may show it as 3.000 but the actual value still exceeds the threshold. So the Freq alarm was asserted.

Clearing of the Freq Error (Frequency Error alarm)

- The Frequency Error Alarm clears when 10 MHz Frequency Error measurement is less than the set threshold

B) Alarms classified as Minor alarms

1. In Holdover alarm ("In Holdover" mode event)

- Mantis case 3249: Note that in at least software versions 5.4.1 and below, Holdover is an Event (entry asserted in the Events log) instead of being an Alarm (entry in the Alarms log)

Indicates the NTP server lost synchronization to its external reference input and it's using the internal reference oscillator to derive the time outputs. This alarm is classified as a Minor alarm condition. The Holdover mode will continue until the reference is restored, it times out as configured in the System/Holdover page, or the unit NTP server is rebooted/power cycled. If Holdover mode times out, at that time a Time Sync alarm will be asserted.

During the Holdover mode, all outputs remain available to synchronize other devices. This mode is just an alert that the primary input is not available and so the oscillator is being used to provide time outputs. There is no other effect on the operation of the system while in the mode.

"In Holdover" and "Not in Holdover" event entries are always masked in versions prior to version 5.4.4

- Prior to version 5.4.5, both of these events were listed in the Notifications page but the checkbox to mask/unmask them were not visible. And in the background, they were always selected (it was this way since we added the ability to mask alarms.
- Version 5.4.5 (~Aug 2016) is adding visible Holdover/Not in Holdover MASK checkboxes to the Management -> Reference Priority page (previously these were listed with no checkboxes available. The factory default settings are for these two checkboxes to be selected (Holdover alarms masked). But starting with Version 5.4.5, customers can now unmask these alarms so that they are asserted, as desired.

2. User-defined Minor alarm (Min Sats):

This alarm indicates a user has configured the NTP time server to assert a Minor alarm upon the GPS receiver falling below a specified number of satellites, for a user-specified length of time. For example, a user can configure this alarm to be asserted if the unit was tracking at least five satellites, but sometime thereafter, it starts tracking only three satellites, by setting the threshold at 4 satellites. Since this alarm threshold is not directly related to the minimum number of satellites required by the system, the presence of this alarm does not automatically indicate a problem with GPS reception.

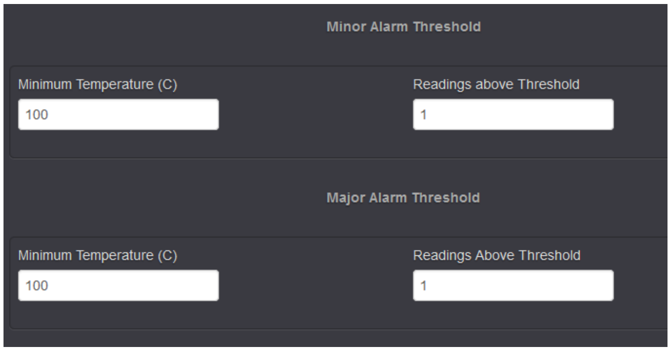
The number of satellites for the alarm threshold and whether the receiver dropping below this user-specified number of satellites is classified as a Major alarm or as a Minor alarm is configured in the:

- **Newer browser:** ***Management*** -> ***Notifications*** page of the browser, GPS tab

3. User-defined Minor Alarm (Temperature alerts)

This alarm indicates a user has configured the NTP time server to assert a Minor alarm when the internal temperature has exceeded the min or max custom-configurable threshold (***Management*** -> ***Notifications*** page of the browser, **System** tab):

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



Minor Alarm Threshold

Minimum Temperature (C): 100

Readings above Threshold: 1

Major Alarm Threshold

Minimum Temperature (C): 100

Readings Above Threshold: 1

4. Antenna Problem alarm:

This alarm log entry indicates an open or short has been detected by the GPS receiver in the antenna cable (Located somewhere between the NTP time server and the GPS antenna). This alarm is classified as a Minor alarm condition. If this alarm is present, refer to the "GPS Troubleshooting guide (http://www.spectracomcorp.com/Desktopmodules/Bring2Mind/DMX/Download.aspx?EntryId=396&PortalId=0) for troubleshooting assistance.

5. Oscillator Adjust:

Indicates a potential issue with the internal oscillator calibration.

6. The unit has rebooted:

SecureSync was either rebooted or intentionally/inadvertently power cycled.

Desire to mask or unmask alarms/events

- Refer also to the SecureSync SNMP tech note: ..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\SNMP- Notifications-email alerts\SNMP

In some SecureSync configurations, there may be one or more alarm conditions that will remain always asserted, so the associated alarm(s) may need to remain active. This results in the front panel "Fault" LED remaining lit. undesired "Spectracom-specific" alarms can be "masked" (squelched) to prevent undesired alarms from being continuously asserted.

Log entries are still inserted for masked alarm conditions, but traps and emails aren't sent for masked alarm conditions. And masking undesired alarm conditions can allow the front panel "Fault" LED to clear when all other "non-masked" alarm conditions have cleared.

Masking is configured in the **Management**-> **Notifications** page of the newer (black) web browser. There are various tabs for all the available alarms/events which can be masked, as desired. (These events/alarms are listed and described in the SNMP Tech Note at the link further above).

Factory default settings: Most, but not all, alarms/events are not masked by default. Exceptions are the "**In Holdover**" and "Not in Holdover" events which are masked by factory default.

**Obtaining Time/Date reads (desire to read/obtain time remotely/automatically)

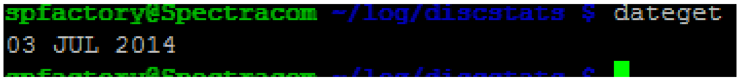
1) Can view the **Setup** -> **Time Management** page of the browser

2) Can use the Models 1204-02 (RS-232) or 1204-04 (RS-485) Option Cards to automatically output ASCII time stamps (broadcast or interrogation modes).

3) Can read the time/date via CLI interfaces (front panel SERIAL port, telnet or ssh) using the following commands:

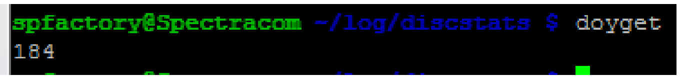
Note: CLI interfaces, including the front panel DB9 connector, are all username/password protected. Login is required to use CLI interfaces to obtain date/time stamps)

- **dateget (**displays current date)



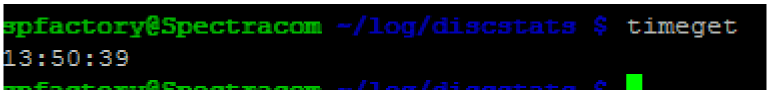
```
spfactory@Spectracom ~/log/discstats $ dateget
03 JUL 2014
```

- **doyget** (displays current day of year)



```
spfactory@Spectracom ~/log/discstats $ doyget
184
```

- **timeget** (Displays the current System Time – the time scale of this reported time is based on the System Time scale which is configured in the **Setup** -> **Time Management** page of the browser)



```
spfactory@Spectracom ~/log/discstats $ timeget
13:50:39
```

4) Can use either the Time protocol (Binary time stamp) or Daytime protocol (ASCII time stamp) over Ethernet (similar to NTP). No password is required for these time stamps, unlike what is required for the CLI interfaces. Refer to "**Daytime and Time protocols (for all poducts**)" section in the CustAssist doc for more info: ..\CustomerServiceAssistance.pdf

Note: These two Services are disabled by factory default. Must be enabled to use them
Time protocol = port **37** .
Daytime protocol = port **13**

when enabled

- The associated service for Time/Daytime is **xinetd**, although this will launch Time/Daytime upon connection

xinetd (per https://en.wikipedia.org/wiki/Xinetd)
xinetd listens for incoming requests over a network and launches the appropriate service for that request.[5] Requests are made using port numbers as identifiers and xinetd usually launches another daemon to handle the request. It can be used to start services with both privileged and non-privileged port numbers.

5) With Archive software versions 4.8.2 or higher, can also use **SNMP** to obtain the time (**ssSysStaDateTime**). Refer to the SNMP Application Note: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\SNMP

**IBM Model 9037 Sysplex timer (sysplex1) time stamps

- Not available from base SecureSync
- Refer to the SecureSync Option Card document for info on Model 1204-02 RS-232 Input/Output Option Card.

***PTP Output (1204-32 card or eth0/eth1)

A) For 1204-32 Gb PTP Option Card (if installed)

- Refer to I:\Customer Service\1- Cust Assist documents\SecureSync Option Card information.pdf
- Refer to online 2400 SecureSync userguide: https://orolia.com/manuals/2400/Content/NC_and_SS/Com/Topics/OPTCARDS/OC_List/PTP_Grandm.htm

B) PTP output from the Base/Chassis network interfaces (eth0/eth1)

- Refer to online 2400 SecureSync user guide: http://manuals.spectracom.com/2400/Content/VS/Topics/INTRO/VS_PTP.htm

Support of PTP over VLAN

- Refer to 2400 SecureSync user guide at:

Software version limitations on VLAN support of PTP

As of at least versions 1.6.0 and below, PTP over a VLAN interface is not currently functional.

- Per the 1.6.0 release Notes: *PTP over a VLAN interface is not currently functional (from 1.4.1)*

- Refer to Salesforce Cases such as 292339 (for VersaSync, but also applies to 2400s

Note from Keith (excerpted from the case Software version limitations on VLAN support of PTP

Confirm with Engineering (Will Comly), 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 it's referred to as "VLAN-unaware")

Software changes/software version changes associated with onboard PTP

Software changes associated with PTP on base eth0/eth1 (refer also to Release Notes)

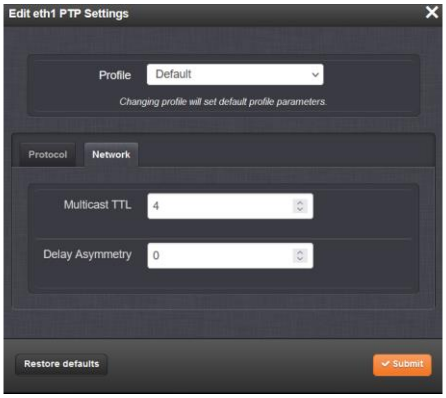
PTP module installed

A) Version 1.4.1A and above: ptp4L

B) Versions prior to version 1.4.1: Orolia '*Masterpiece'* software

1. Version 1.6.0 update (~Sept 2022)

Added "**Delay Asymmetry**" field (nanoseconds)



Edit eth1 PTP Settings

Profile: Default

Changing profile will set default profile parameters.

Multicast TTL: 4

Delay Asymmetry: 0

2. Version 1.4.1 update (April 2022)

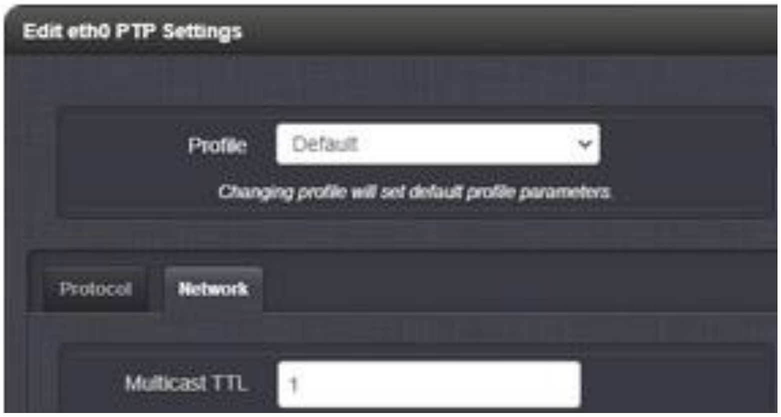
Note: Version 1.4.1A apparently made a large change to onboard PTP (switching from Orolia ‘*Masterpiece’* software to ptp4l)

Feature: Added support for **Linux PTP profiles IEEE C37.238-2017** (power systems profile) and IEC 61850-9-3:2016 (power utility profile).

Onboard PTP profiles supported

- Refer to online 2400 SecureSync user guide (under “**PTP Specifications**”): http://manuals.spectracom.com/2400/Content/VS/Topics/INTRO/VS_PTP.htm

The desired PTP profile to use is selected at the top of the PTP Settings Panel (above the *Protocol* and *Network* tabs)



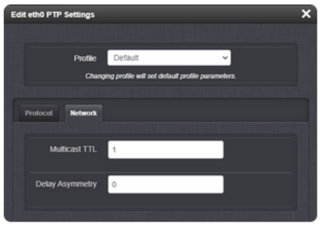
Edit eth0 PTP Settings

Profile: Default

Changing profile will set default profile parameters.

Multicast TTL: 1

Default PTP settings for each available Profile selection (excerpted from user guide)



Profile: Default

Changing profile will set default profile parameters.

Multicast TTL: 1

Delay Asymmetry: 0

Edit PTP Settings panel

▼ Profile

PTP profile selection beyond Default will result in new fields and parameters, and default values. See the Protocol tab section below for default values for the Default profile.

- **Default** Standard presets and defaults for PTP functionality.
- **Telecom G.8265.1**: [Full Timing Support] Defaults: Unicast is required, Domain is set to 4.
- **Power Utility 61850-9-3**: Defaults: Peer Delay Mechanism, with an announce rate of 1 message per second, Ethernet Network Transport, and available Peer MAC Address field.
- **Power System C37.238**: Defaults: Peer Delay Mechanism, with an announce rate of 1 message per second, Ethernet Network Transport, available Peer MAC Address and Alt Timescale Display Name fields.Domain is set to 254.

➢ **PTP Profiles supported:** Default, Telecom G.8265.1, Power Utility 61850-9-3, Power System C37.238

Note that software update v1.4.1 replaced our “masterpiece” with PTP4L software.

- **Telecom G.8265.1 (Telecom Profile):** Added in software update **version 1.4.1** (April 2022)
- **IEEE C37.238-2017 (Power Systems Profile):** Added in software update **version 1.4.1** (April 2022)
- **IEC 61850-9-3:2016 (Power Utility profile):** Added in software update **version 1.4.1** (April 2022)

Details of the various PTP Profile support

A) Telecom Profiles (G.8265.1 and G8275.1)

Note the Telecom Profiles consist of the following:

G.8265.1 (Telecom Profile for Frequency) (the simpler of the variants)

G8275.1: (Telecom Profile for Time and Phase) (full timing support for new-build networks)

G8275.2: (Telecom Profile for Time and Phase) (partial timing support over existing networks)

➢ Update Version 1.4.1 (with the switch from ‘masterpiece’ to PTP4L) implemented support of Telecom Profile **G.8265.1 for Frequency)** (the simpler of the two Telecom Profiles)

➢ As of at least version 1.7.0 and below, the more complex (Telecom Profile for Time and Phase - **G8275.1**) is not supported by PTP4L, and therefore also not supported by the 2400 SecureSyncs.

- The Precision Time Protocol (PTP) **G. 8275.2** enhanced profile **supports telecom applications that require accurate phase and time synchronization for phase alignment and time of day synchronization over a wide area network**.

➢ **Issue with 2400 operating in PTP Slave mode:** Software versions 1.6.0 and below (fixed with a hotpatch for 1.6.0, with this patch being implemented in 1.7.0 update) have a software issue preventing 2400 SecureSyncs from being able to sync to a PTP Master operating in Telecom Profile. This is because of the default ClockClasses are different from the Telecom ClockClasses.

- **Issue with 2400 operating as a Telecom Profile PTP Master:** Software versions of at least 1.7.0 and below cannot operate as a Telecom PTP Master. This is expected "someday" but not known when it will be added/implemented.

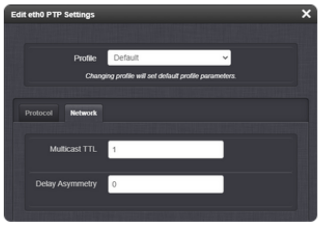
- Refer to Salesforce Case 294465 (excerpted below)

(Message Keith Sent to Alex Payne, 14 March 2023)

Thanks for inquiring about the base Model 2400 PTP support of the Telecom profile.

I was thinking the support of this profile was from "Day 1" of the 2400 SecureSync and was it completely "straight forward" with a "Yep! It's supported". But I first spoke to Will Comly with the Engineering team to confirm, before responding to you. And I'm glad I did :)!!

Initial support for the Telecom profile was added to the 2400s when we switched to "PTP4L" in the 2400 Software version 1.4.1 update.   Previous to this release, it was not supported at all. However, PTP4L software (and therefore also the base PTP functionality of the 2400) currently only supports one of the Telecom Profiles. Per the 2400 User Guide (https://www.orolia.com/manuals/2400/Content/VS/Topics/INTRO/VS_PTP.htm as excerpted below) it only supports Telecom Profile **G.8265.1.** There is another more complex Telecom Profile, but its not currently supported by the 2400 SecureSyncs..


Edit eth0 PTP Settings

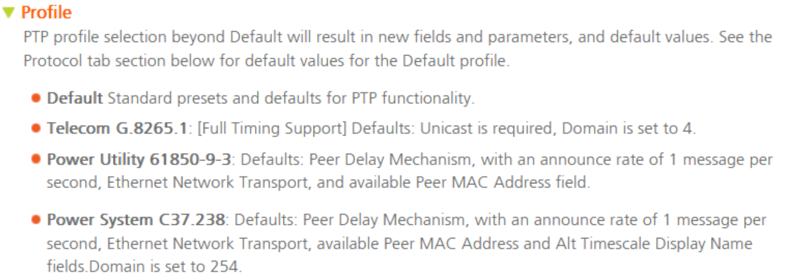
Profile: Default

Changing profile will set default profile parameters.

Multicast TTL: 1

Delay Asymmetry: 0

Edit PTP Settings panel


▼ Profile

PTP profile selection beyond Default will result in new fields and parameters, and default values. See the Protocol tab section below for default values for the Default profile.

- **Default** Standard presets and defaults for PTP functionality.
- **Telecom G.8265.1**: [Full Timing Support] Defaults: Unicast is required, Domain is set to 4.
- **Power Utility 61850-9-3**: Defaults: Peer Delay Mechanism, with an announce rate of 1 message per second, Ethernet Network Transport, and available Peer MAC Address field.
- **Power System C37.238**: Defaults: Peer Delay Mechanism, with an announce rate of 1 message per second, Ethernet Network Transport, available Peer MAC Address and Alt Timescale Display Name fields.Domain is set to 254.

According to Will, there are two limitations on the Model 2400 support of this Telecom Profile (G.8265.1). In software version 1.6.0 (the very latest release for the 2400, but being addressed in version 1.7.0, which is expected to be made available in the next couple/few weeks) the 2400 SecureSync has an issue with being a Telecom PTP Slave (it won't sync to a Telecom PTP Master). This is directly related to the ClockClass values in the Telecom Profile not being the same as the default ClockClass values.

The other limitation is that the 2400 SecureSync can't currently be configured to be a Telecom PTP Master (to sync PTP Slaves). This is expected "one day in the future", but it's not known when this functionality will be added.

Will said the two big questions to ask a potential Model 2400 PTP Telecom Profile customer is which Telecom Profile they want to use (is it G.8265.1) and do they want the Model 2400 SecureSync to operate as a PTP Master with the Telecom Profile, or for it to operate as a PTP Slave, which syncs to one or more PTP Masters operating in the Telecom Profile.

PTP over VLAN

- Not currently supported (as of at least versions 1.6.0 and below)
    - Excerpt from the version 1.4.1 update release notes “PTP over a VLAN interface is not currently functional.”

1. Onboard PTP Configuration

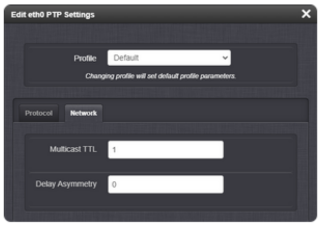
Known Issues / limitations

- In update versions 1.6.0, the 2400 SecureSyncs **can't sync to a PTP Master operating in PTP Telecom Profile** (this was addressed in a patch for 1.6.0, and the patch being implemented in 1.7.0. This change addresses the differences between the default ClockClass values and the Telecom ClockClass values.
  - Software versions of at least 1.7.0 and below cannot operate as a PTP Master operating in Telecom profile configuration.
- In at least versions 1.2.2 and below, the 2400 cannot be configured to operate as both a PTP slave and NTP client.
- When switching PTP configuration between master and slave, occasionally the change will not take effect unless manually disabling/reenabling PTP on that interface.

Management -> ***PTP Setup*** page

PTP Profiles (Telecom, Power)

- Refer to details on the various Profiles, further above.
- The desired PTP profile to use is selected at the top of the PTP Settings Panel (above the ***Protocol*** and ***Network*** tabs)



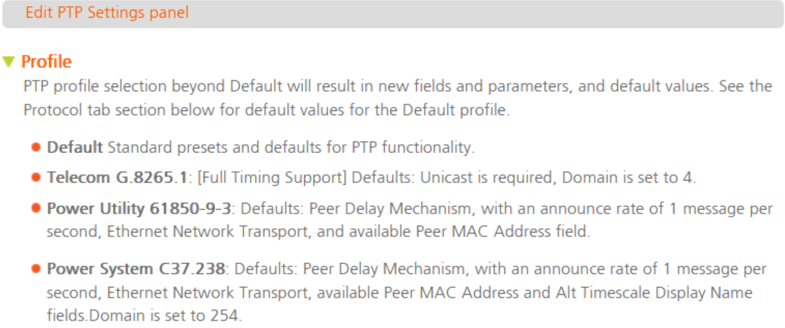
Edit eth0 PTP Settings

Profile: Default

Changing profile will set default profile parameters.

Multicast TTL: 1

Delay Asymmetry: 0

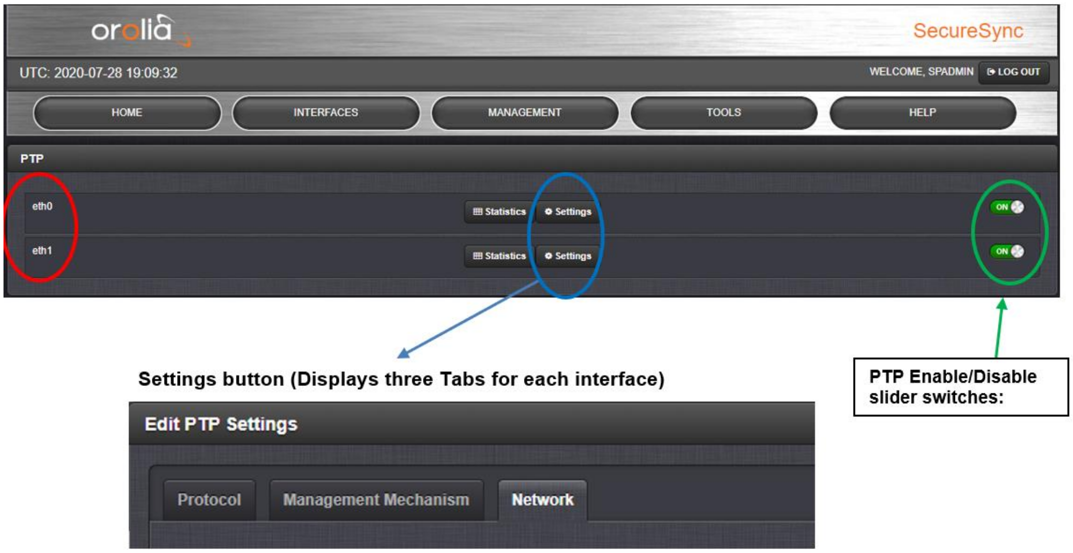


Edit PTP Settings panel

Profile

PTP profile selection beyond Default will result in new fields and parameters, and default values. See the Protocol tab section below for default values for the Default profile.

- **Default** Standard presets and defaults for PTP functionality.
- **Telecom G.8265.1**: [Full Timing Support] Defaults: Unicast is required, Domain is set to 4.
- **Power Utility 61850-9-3**: Defaults: Peer Delay Mechanism, with an announce rate of 1 message per second, Ethernet Network Transport, and available Peer MAC Address field.
- **Power System C37.238**: Defaults: Peer Delay Mechanism, with an announce rate of 1 message per second, Ethernet Network Transport, available Peer MAC Address and Alt Timescale Display Name fields.Domain is set to 254.



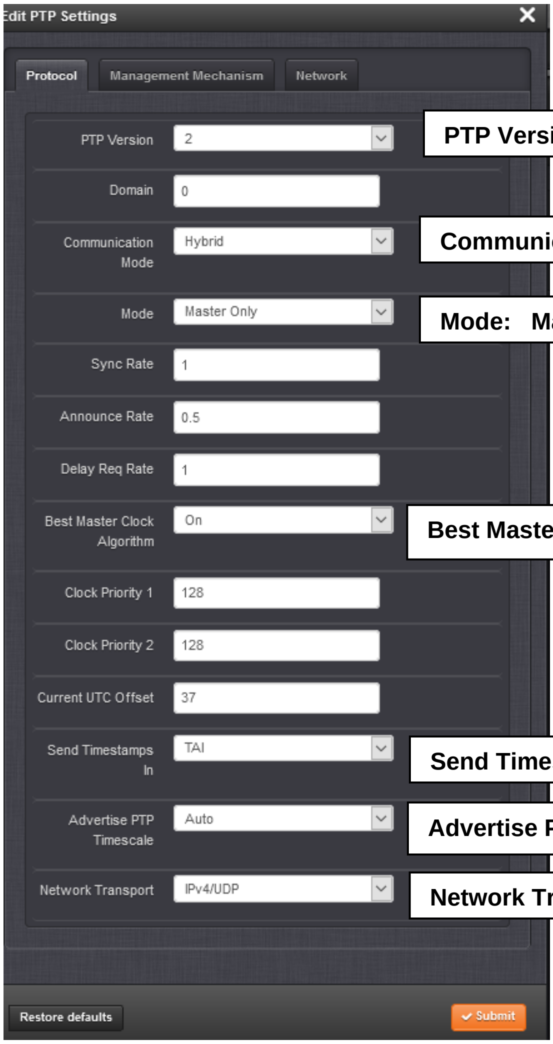
Settings button (Displays three Tabs for each interface)

PTP Enable/Disable slider switches:

Network settings (IP Address, Netmask, port speeds, etc)

- Not configured in the ***Management*** -> ***PTP Setup*** pages
  - Refer to ***Management*** -> ***Network Setup*** page of the browser

Protocol Tab (PTP version, mode, BMC, Timescale, Priorities, Message rates, etc)



PTP Version: 2

Domain: 0

Communication Mode: Hybrid

Mode: Master Only

Sync Rate: 1

Announce Rate: 0.5

Delay Req Rate: 1

Best Master Clock Algorithm: On

Clock Priority 1: 128

Clock Priority 2: 128

Current UTC Offset: 37

Send Timestamps In: TAI

Advertise PTP Timescale: Auto

Network Transport: IPv4/UDP

PTP Version: V1 or **V2**

Communication Mode: Multicast Hybrid Unicast

Mode: Master Only or **Slave only**

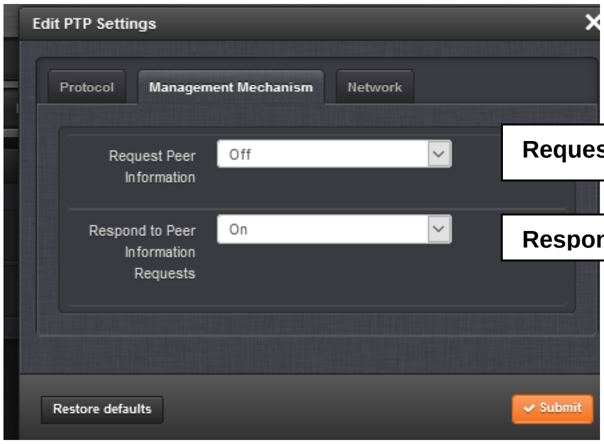
Best Master Clock algorithm: On or **Off**

Send Timestamps in: TAI or **UTC**

Advertise PTP timescale: Auto Yes or **No**

Network Transport: Ethernet or **IPv4/UDP** or **IPv6/UDP**

Management Mechanisms Tab (Peer Info requests)



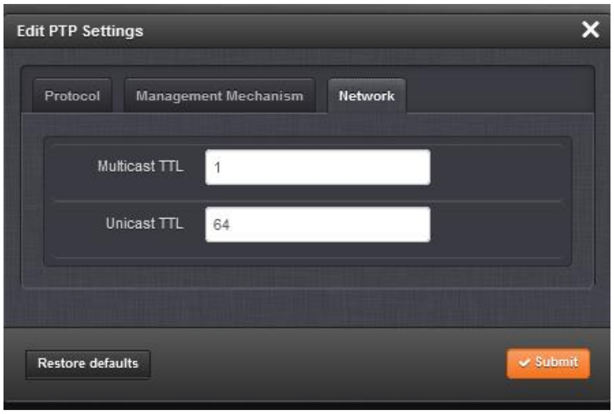
Request Peer Information: Off

Respond to Peer Information Requests: On

Request Peer Info: On/Off

Respond to Peer Info requests (Slave Only) On/Off

Management Mechanisms Tab (TTL values)



Multicast TTL: 1

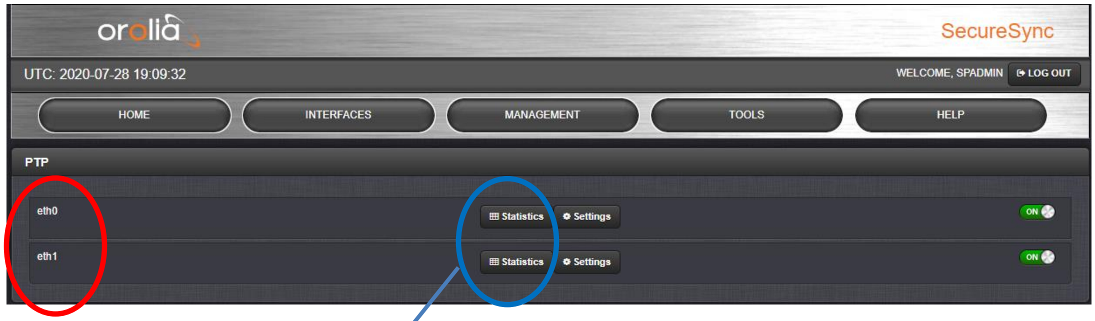
Unicast TTL: 64

~~~~~~~~~~~~~~~~~~~~~~

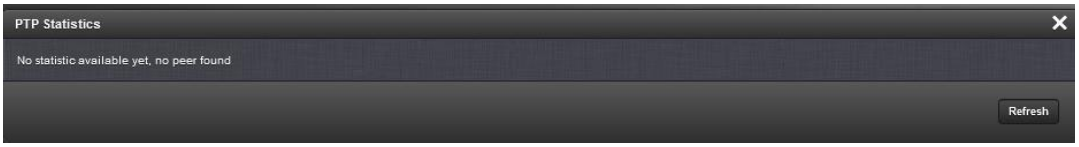
2. PTP Statistics Panel (not applicable to 1204-32 card, if installed)

- ➢ Refer to “**The PTP Statistics Panel” in** 2400 SecureSync online user guide at: http://manuals.spectracom.com/2400/Content/VS/Topics/INTRO/VS_PTP.htm?Highlight=%20Statistics
- ➢ This panel provides statistics for each Ethernet port. If the PTP is set to OFF for a specific port, this screen will not display any information.
- ➢ All statistics shown are based on the traffic that is detectable by SecureSync, i.e. in a Unicast environment, SecureSync may only detect traffic that is addressed to it, based on switch configuration.

Management -> ***PTP Setup*** page

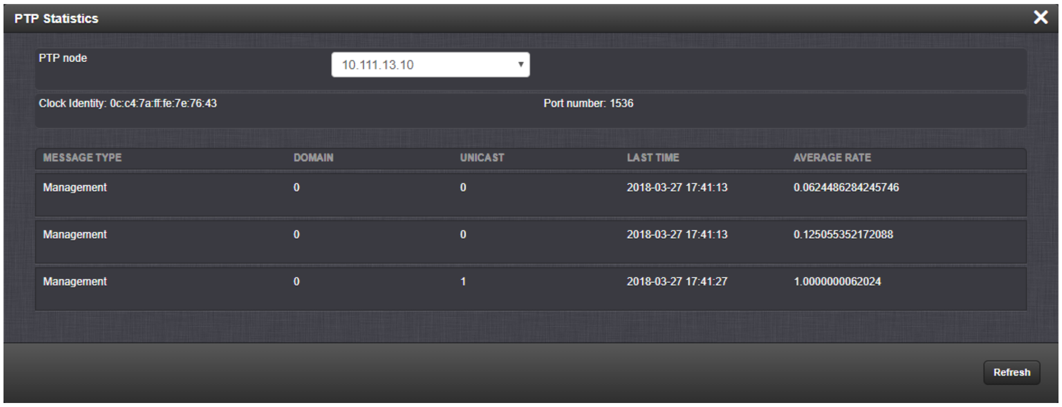


Statistics button



No statistic available yet, no peer found

OR



PTP node: 10.111.13.10

Clock Identity: 0c:c4:7a:ff:fe:7e:76:43

Port number: 1536

MESSAGE TYPE	DOMAIN	UNICAST	LAST TIME	AVERAGE RATE
Management	0	0	2018-03-27 17:41:13	0.0624486284245746
Management	0	0	2018-03-27 17:41:13	0.125055352172088
Management	0	1	2018-03-27 17:41:27	1.0000000062024

- ○ **PTP Node:** IP address of PTP node.
- ○ **Clock Identity**: [e.g., "a0:36:9f:ff:fe:37:b9:5d"]
- ○ **Domain**: Domain number of the selected PTP node.
- ○ **Unicast**: [0,1] OFF or ON (1)
- ○ **Last Time**: [e.g., "2016-08-12 18:19:15"] The last time a packet was received.
- ○ **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).
~~~~~~~~~~~~~~~~~~~~~~

Various Software changes associated with PTP on base eth0/eth1 (refer also to the Release Notes)

A) Update 1.7.0

- Fixed issue with 2400 SecureSync operating as a PTP Telecom Slave (wasn't previously syncing to a PTP Telecom Master, due to differences in ClockClass values)

B) Update 1.4.1 (switched from masterpiece to PTP4L.

- Added support for telecom and power profiles via PTP4L)

C) Update version 1.2.2

The following defects were corrected:

- Fixed a one second offset found in PTP synchronization between the master and slave.
- Corrected an issue with PTP slaves incorrectly reporting as in-sync despite no longer receiving messages from the master.
- Corrected an issue with PTP slaves incorrectly reporting as in-sync despite the designated master no longer being in sync

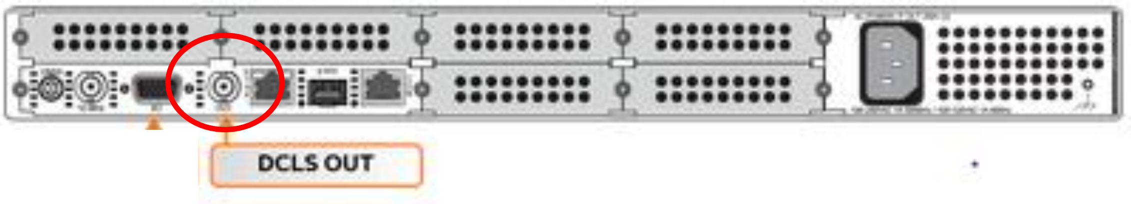
IRIG output

- IRIG output is available a couple different ways

A) IRIG output via installed IRIG Option Card

- Refer to the SecureSync Option card info document

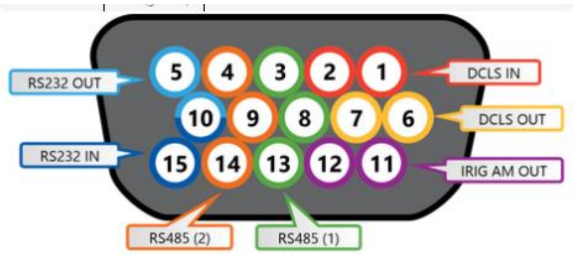
B) IRIG DCLS output via dedicated rear panel BNC connector



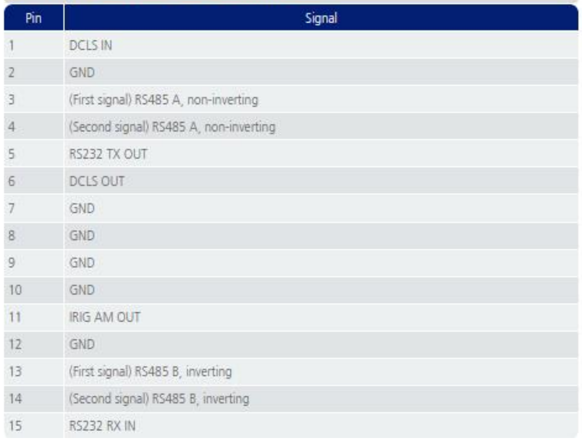
- Refer to the online 2400 SecureSync user guide at: http://manuals.spectracom.com/2400/Content/NC_and_SS/2400/INSTALL/Conf_15pin_BNC.htm

C) IRIG output via rear panel Multi I/O connector

- Refer to the online 2400 SecureSync user guide at: http://manuals.spectracom.com/2400/Content/NC_and_SS/2400/INSTALL/Conf_15pin_BNC.htm



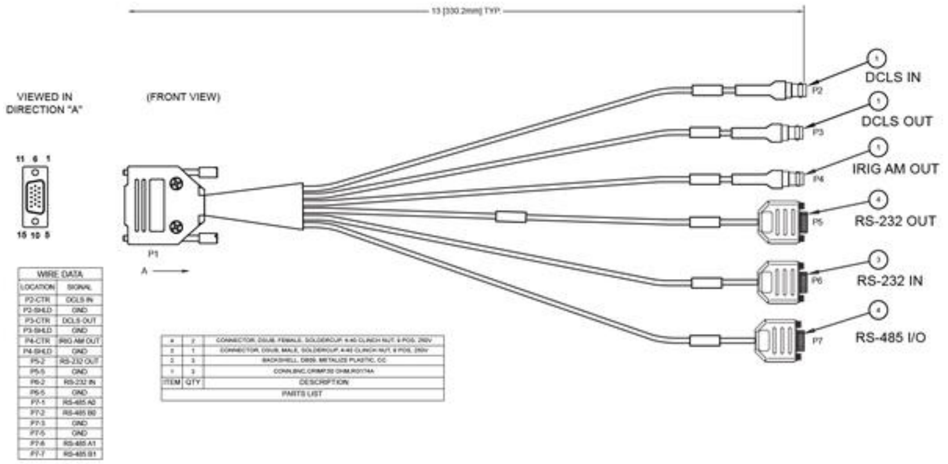
Multi I/O 15-pin connector, in mating direction from front



Pin	Signal
1	DCLS IN
2	GND
3	(First signal) RS485 A, non-inverting
4	(Second signal) RS485 A, non-inverting
5	RS232 TX OUT
6	DCLS OUT
7	GND
8	GND
9	GND
10	GND
11	IRIG AM OUT
12	GND
13	(First signal) RS485 B, inverting
14	(Second signal) RS485 B, inverting
15	RS232 RX IN

CA08R-D500-0001: Optional/Available Breakout cable

This cable option is available for purchase for the multi-I/O (15-pin) connector on the front panel.

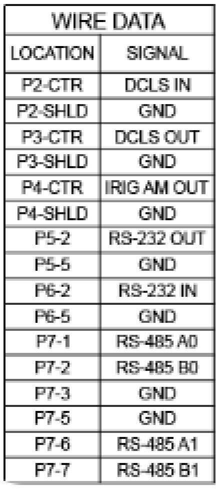


ITEM	QTY	DESCRIPTION
4	2	CONNECTOR, DSUB, FEMALE, SOLDERCUP, 4-40 CLINCH NUT, 9 POS, 250V
3	1	CONNECTOR, DSUB, MALE, SOLDERCUP, 4-40 CLINCH NUT, 9 POS, 250V
2	1	BACKSHELL, DB09, METALIZE PLASTIC, CC
1	3	CONN,BNC,CRIMP,50 OHM,RG174A

PARTS LIST

WIRE DATA

LOCATION	SIGNAL
P2-CTR	DCLS IN
P2-SHLD	GND
P3-CTR	DCLS OUT
P3-SHLD	GND
P4-CTR	IRIG AM OUT
P4-SHLD	GND
P5-2	RS-232 OUT
P5-5	GND
P6-2	RS-232 IN
P6-5	GND
P7-1	RS-485 A0
P7-2	RS-485 B0
P7-3	GND
P7-5	GND
P7-6	RS-485 A1
P7-7	RS-485 B1



WIRE DATA

LOCATION	SIGNAL
P2-CTR	DCLS IN
P2-SHLD	GND
P3-CTR	DCLS OUT
P3-SHLD	GND
P4-CTR	IRIG AM OUT
P4-SHLD	GND
P5-2	RS-232 OUT
P5-5	GND
P6-2	RS-232 IN
P6-5	GND
P7-1	RS-485 A0
P7-2	RS-485 B0
P7-3	GND
P7-5	GND
P7-6	RS-485 A1
P7-7	RS-485 B1

ASCII RS-485 and RS-232 output (ATC = ASCII time code)

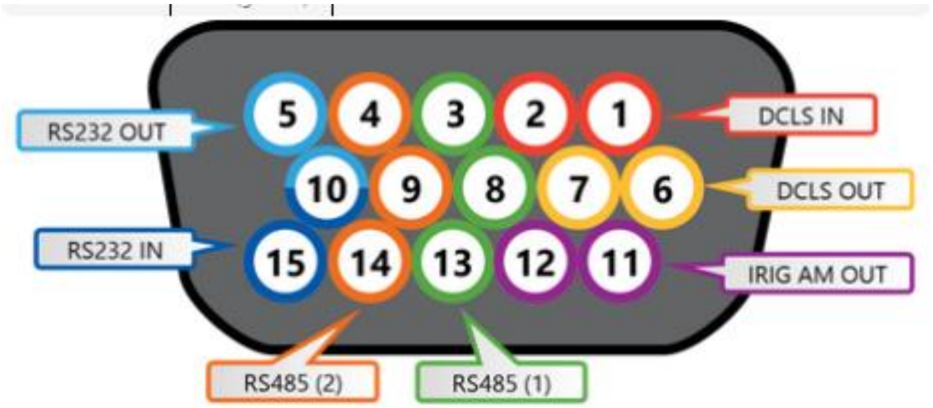
- ASCII output is available a couple different ways:

A) ASCII output via installed ASCII Option Card

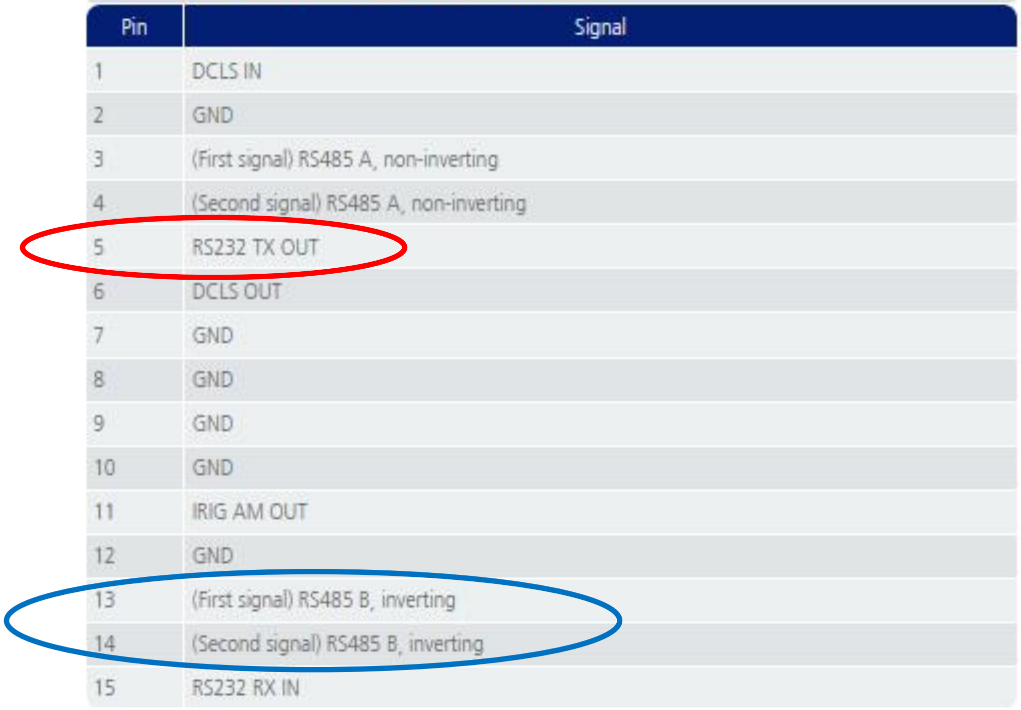
- Refer to 1204-02 and 1204-04 Cards in the SecureSync Option card info document

B) ASCII output via rear panel Multi I/O connector

- Refer to the online 2400 SecureSync user guide at: http://manuals.spectracom.com/2400/Content/NC_and_SS/2400/INSTALL/Conf_15pin_BNC.htm



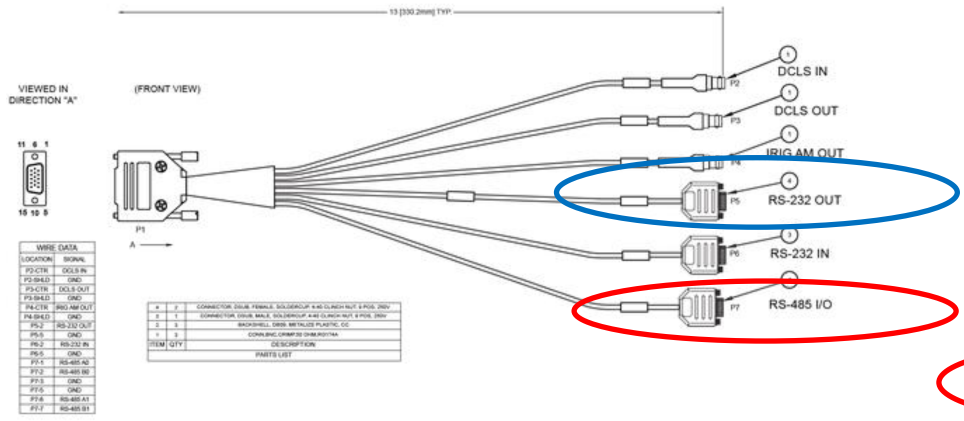
Multi I/O 15-pin connector, in mating direction from front



Pin	Signal
1	DCLS IN
2	GND
3	(First signal) RS485 A, non-inverting
4	(Second signal) RS485 A, non-inverting
5	RS232 TX OUT
6	DCLS OUT
7	GND
8	GND
9	GND
10	GND
11	IRIG AM OUT
12	GND
13	(First signal) RS485 B, inverting
14	(Second signal) RS485 B, inverting
15	RS232 RX IN

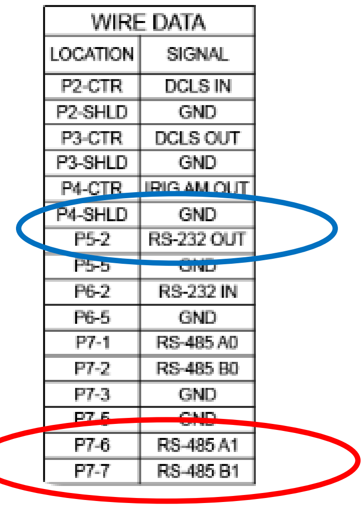
CA08R-D500-0001: Optional/Available Breakout cable

This cable option is available for purchase for the multi-I/O (15-pin) connector on the front panel.



WIRE DATA	
LOCATION	SIGNAL
P2-CTR	DCLS IN
P2-SHLD	GND
P3-CTR	DCLS OUT
P3-SHLD	GND
P4-CTR	IRIG AM OUT
P4-SHLD	GND
P5-2	RS-232 OUT
P5-5	GND
P6-2	RS-232 IN
P6-5	GND
P7-1	RS-485 A0
P7-2	RS-485 B0
P7-3	GND
P7-5	GND
P7-6	RS-485 A1
P7-7	RS-485 B1

4	2	CONNECTOR, DSUB, FEMALE, SOLDERCUP, 4-40 CLINCH NUT, 9 POS, 250V
3	1	CONNECTOR, DSUB, MALE, SOLDERCUP, 4-40 CLINCH NUT, 9 POS, 250V
2	3	BACKSHELL, DB09, METALIZE PLASTIC, CC
1	3	CONN,BNC,CRIMP,50 OHM,RG174A
ITEM	QTY	DESCRIPTION
PARTS LIST		



WIRE DATA	
LOCATION	SIGNAL
P2-CTR	DCLS IN
P2-SHLD	GND
P3-CTR	DCLS OUT
P3-SHLD	GND
P4-CTR	IRIG AM OUT
P4-SHLD	GND
P5-2	RS-232 OUT
P5-5	GND
P6-2	RS-232 IN
P6-5	GND
P7-1	RS-485 A0
P7-2	RS-485 B0
P7-3	GND
P7-5	GND
P7-6	RS-485 A1
P7-7	RS-485 B1

Syncing a TimeView display clock (such as Models TV210 TV230 and TV400) via a 2400 SecureSync

- Spectracom TimeView Model display clocks sync via **ASCII RS-485 input** from the rear panel Multi I/O connector
- Refer also to the TimeView display clock install/troubleshooting guide I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\Spectracom Display clocks
- The optional **CA08R-D500-0001** Breakout cable is not required (only included with 2400 if separately purchased)

Note: TimeView display clocks won't sync until wiring has been connected and until after the 2400 SecureSync has been configured by a user to output Spectracom group, Formats 0 or 1.

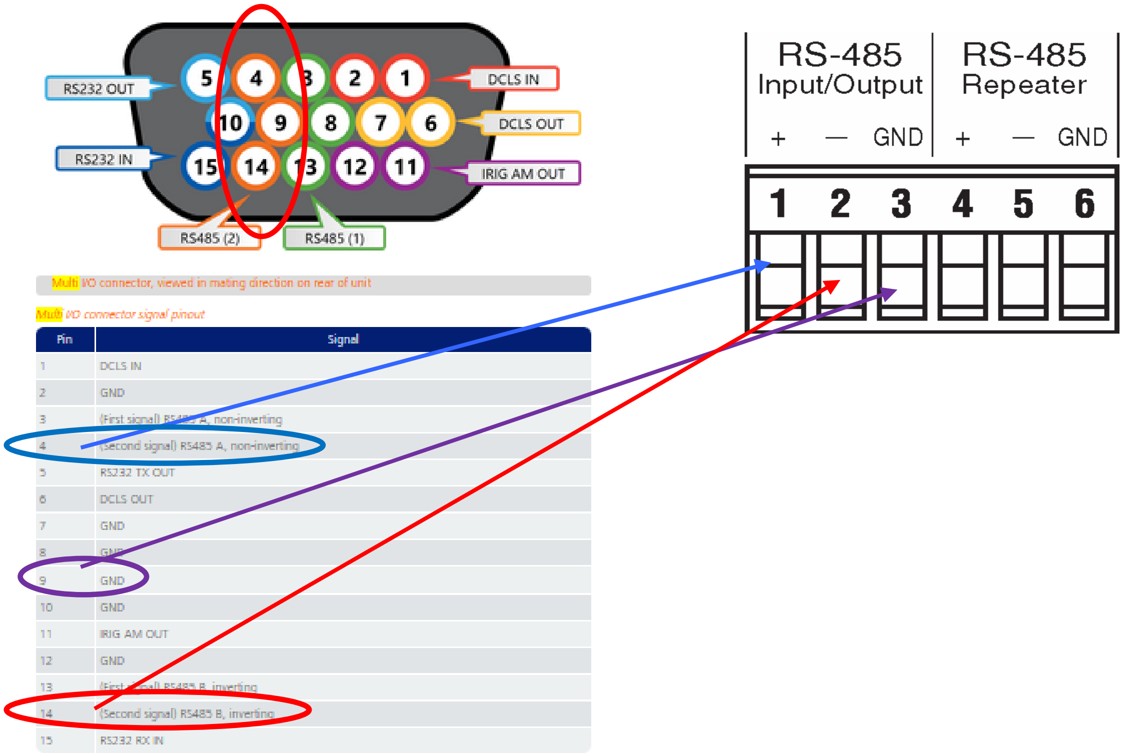
A) Physical Wiring between the 2400 SecureSync and TimeView clock

1) Connecting directly to rear panel Multi I/O (not using optional breakout cable)

- Refer to the online 2400 user guide at: https://safran-navigation-timing.com/manuals/2400/Content/NC_and_SS/2400/INTRO/Specs_Multi_IO.htm

Back of 2400 SecureSync (pins 13 and 14)

Back of TimeView Clock



Multi I/O connector, viewed in mating direction on rear of unit

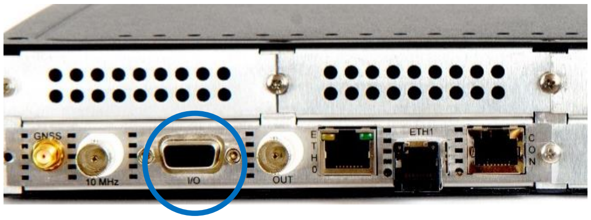
Multi I/O connector signal pinout

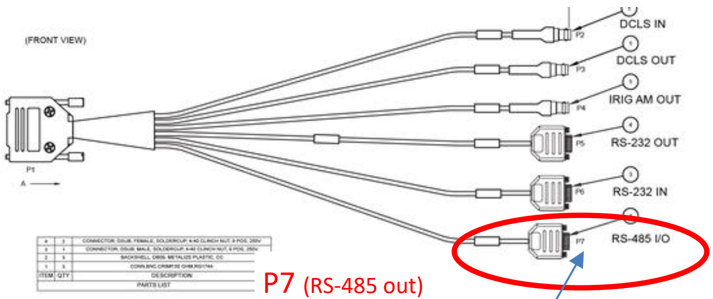
Pin	Signal
1	DCLS IN
2	GND
3	(First signal) RS485 A, non-inverting
4	(Second signal) RS485 A, non-inverting
5	RS232 TX OUT
6	DCLS OUT
7	GND
8	GND
9	GND
10	GND
11	IRIG AM OUT
12	GND
13	(First signal) RS485 B, inverting
14	(Second signal) RS485 B, inverting
15	RS232 RX IN

2) Connecting to rear panel Multi I/O (using optional CA08R-D500-0001: breakout cable)

- ➢ Refer to the online 2400 user guide at: https://safran-navigation-timing.com/manuals/2400/Content/NC_and_SS/2400/INTRO/Specs_Cables.htm

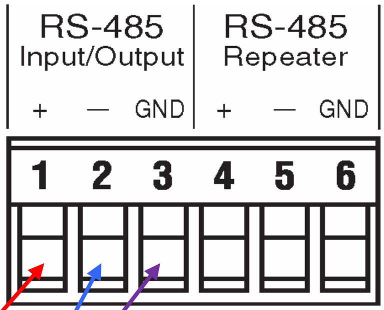
Back of 2400 SecureSync



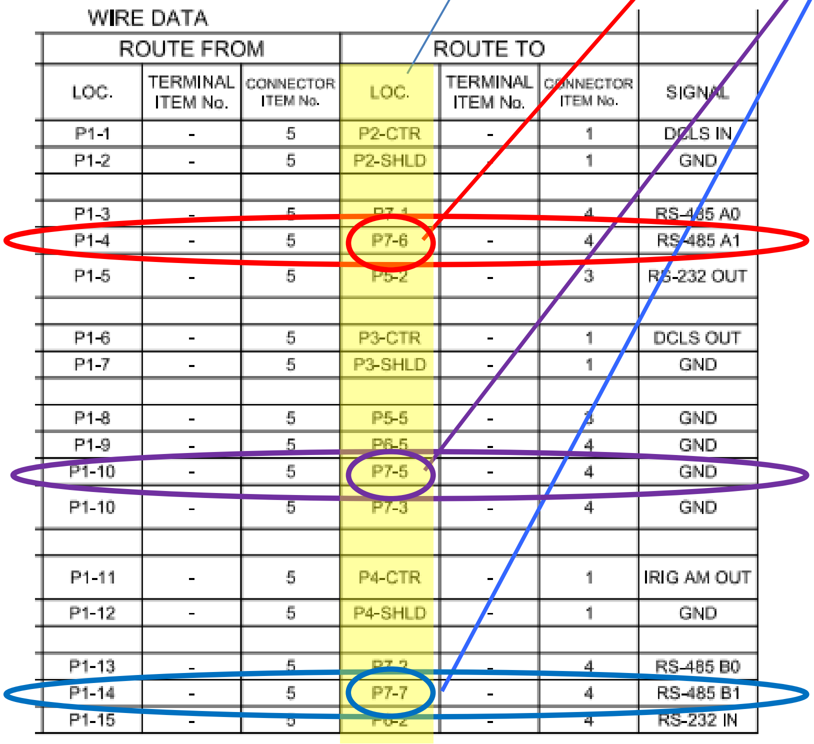


P7 (RS-485 out)

Back of TimeView Clock



CA08R-D500-0001: Optional/Available Breakout cable (Connector P7)



WIRE DATA

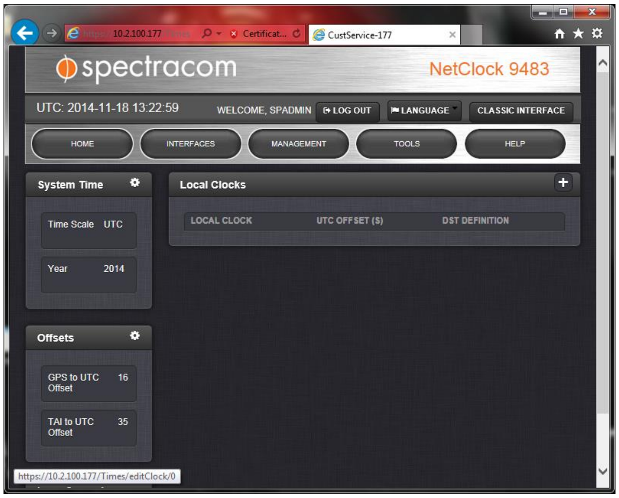
ROUTE FROM			ROUTE TO			
LOC.	TERMINAL ITEM No.	CONNECTOR ITEM No.	LOC.	TERMINAL ITEM No.	CONNECTOR ITEM No.	SIGNAL
P1-1	-	5	P2-CTR	-	1	DCLS IN
P1-2	-	5	P2-SHLD	-	1	GND
P1-3	-	5	P7-1	-	4	RS-485 A0
P1-4	-	5	P7-6	-	4	RS-485 A1
P1-5	-	5	P5-2	-	3	RS-232 OUT
P1-6	-	5	P3-CTR	-	1	DCLS OUT
P1-7	-	5	P3-SHLD	-	1	GND
P1-8	-	5	P5-5	-	3	GND
P1-9	-	5	P6-5	-	4	GND
P1-10	-	5	P7-5	-	4	GND
P1-10	-	5	P7-3	-	4	GND
P1-11	-	5	P4-CTR	-	1	IRIG AM OUT
P1-12	-	5	P4-SHLD	-	1	GND
P1-13	-	5	P7-2	-	4	RS-485 B0
P1-14	-	5	P7-7	-	4	RS-485 B1
P1-15	-	5	P6-2	-	4	RS-232 IN

Note about the specified ground pin for "ATC_out | RS485" (As of at least v1.7.0 and below) The specified pins for the RS485 data (pins 4 and 14) are on connector **P7**. But the specified ground pin (pin 9) actually correlates to a pin on connector **P6**. **Pin 5** of connector J7 is also ground, allowing all three wires to be attached to the same connector (J7). JIRA Ticket **CAR-2469** (May 2023) was created to request changing the specified ground pin to use

Setting up the 2400 SecureSync and the TV400W requires a two-step process, configuring the Multi I/O RS-485 output (ASCII Output 1) to send the correct time code and setting up a “Local Clock” in the SecureSync to adjust the time code for your local time zone and Daylight Savings Time rules.

Step 1:
Setup the Local Clock

a. In the web UI go to Management/Time Management and select the **+** symbol in the Local Clocks section to add a new local clock setting.



UTC: 2014-11-18 13:22:59

System Time

Time Scale	UTC
Year	2014

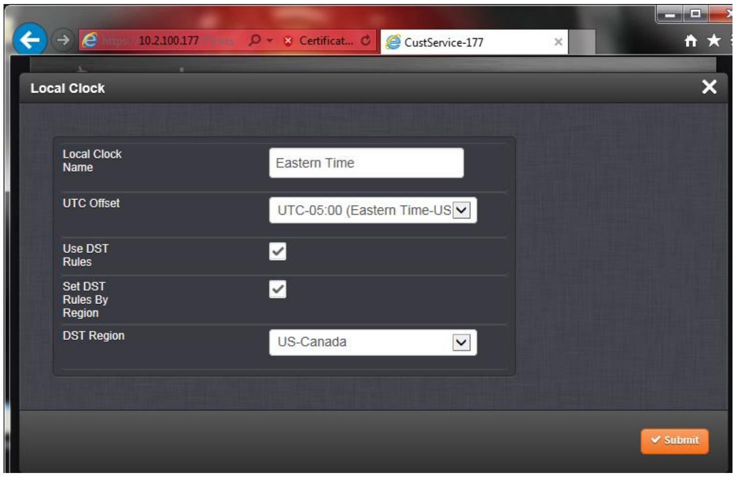
Offsets

GPS to UTC Offset	16
TAI to UTC Offset	35

Local Clocks +

LOCAL CLOCK	UTC OFFSET (S)	DST DEFINITION

b. Configure the Local Clock settings per your Time Zone and Daylight Savings Time regions. In this case a local clock named *Eastern Time* was created for the US Eastern Time Zone. Select SUBMIT to save the settings.



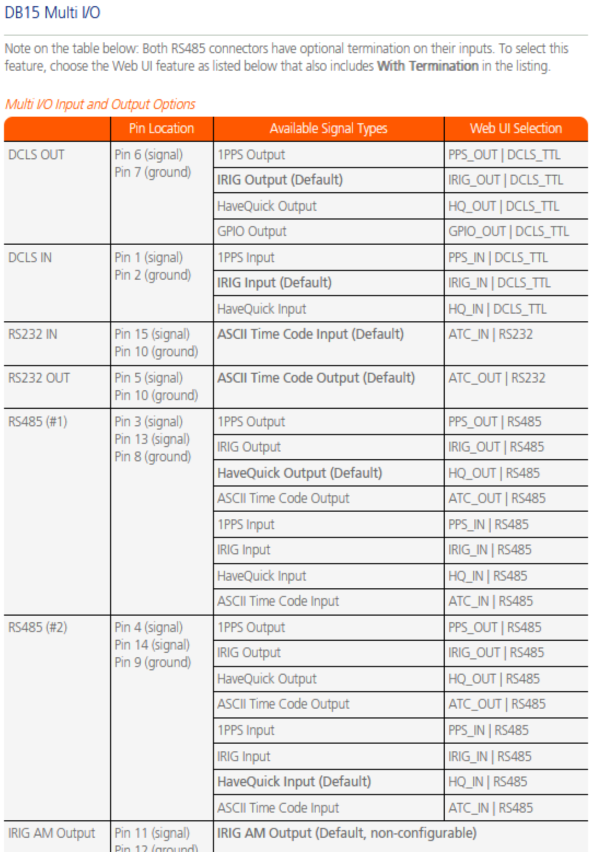
Local Clock

Local Clock Name	Eastern Time
UTC Offset	UTC-05:00 (Eastern Time-US
Use DST Rules	☑
Set DST Rules By Region	☑
DST Region	US-Canada

Step 2: Edit the software-configurable Pins via the **Management** -> **Pin Layout** page of the browser

Note: Refer also to “Configure an ASCII Output” in the online 2400 SecureSync user guide at: https://safran-navigation-timing.com/manuals/2400/Content/NC_and_SS/2400/INSTALL/Conf_15pin_BNC.htm

- (As of at least v1.7.0 and below) Unlike ASCII RS232, there are no factory default ASCII RS485 output pins for the Multi I/O connector
- Applicable “**RS485**” Output pins need to be reconfigured by a user for “**ATC_Out | RS485**” (the factory default “Pin Layout” does not configure this)
- JIRA Ticket **CAR-2469** (May 2023) was created to request RS485 become a factory default pin configuration.



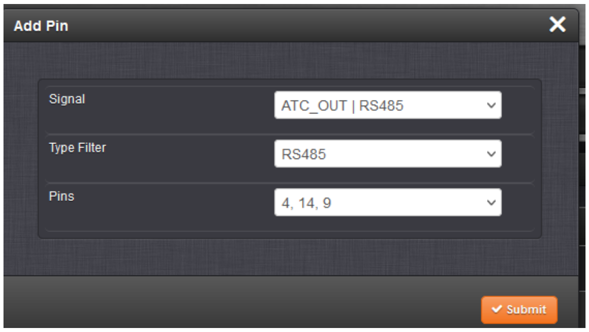
DB15 Multi I/O

Note on the table below: Both RS485 connectors have optional termination on their inputs. To select this feature, choose the Web UI feature as listed below that also includes **With Termination** in the listing.

Multi I/O Input and Output Options

	Pin Location	Available Signal Types	Web UI Selection
DCLS OUT	Pin 6 (signal) Pin 7 (ground)	1PPS Output	PPS_OUT | DCLS_TTL
		IRIG Output (Default)	IRIG_OUT | DCLS_TTL
		HaveQuick Output	HQ_OUT | DCLS_TTL
		GPIO Output	GPIO_OUT | DCLS_TTL
DCLS IN	Pin 1 (signal) Pin 2 (ground)	1PPS Input	PPS_IN | DCLS_TTL
		IRIG Input (Default)	IRIG_IN | DCLS_TTL
		HaveQuick Input	HQ_IN | DCLS_TTL
RS232 IN	Pin 15 (signal) Pin 10 (ground)	**ASCII Time Code Input (Default)**	ATC_IN | RS232
RS232 OUT	Pin 5 (signal) Pin 10 (ground)	**ASCII Time Code Output (Default)**	ATC_OUT | RS232
RS485 (#1)	Pin 3 (signal) Pin 13 (signal) Pin 8 (ground)	1PPS Output	PPS_OUT | RS485
		IRIG Output	IRIG_OUT | RS485
		HaveQuick Output (Default)	HQ_OUT | RS485
		ASCII Time Code Output	ATC_OUT | RS485
		1PPS Input	PPS_IN | RS485
		IRIG Input	IRIG_IN | RS485
		HaveQuick Input	HQ_IN | RS485
		ASCII Time Code Input	ATC_IN | RS485
RS485 (#2)	Pin 4 (signal) Pin 14 (signal) Pin 9 (ground)	1PPS Output	PPS_OUT | RS485
		IRIG Output	IRIG_OUT | RS485
		HaveQuick Output	HQ_OUT | RS485
		ASCII Time Code Output	ATC_OUT | RS485
		1PPS Input	PPS_IN | RS485
		IRIG Input	IRIG_IN | RS485
		HaveQuick Input (Default)	HQ_IN | RS485
		ASCII Time Code Input	ATC_IN | RS485
IRIG AM Output	Pin 11 (signal) Pin 12 (ground)	**IRIG AM Output (Default, non-configurable)**	

In the “**Pin layout**,” page, first press the “**+**” in the upper-right corner. The “**Add Pin**” pop-up menu will display. Configure this menu as shown below, and press Submit:



Add Pin

Signal: ATC_OUT | RS485

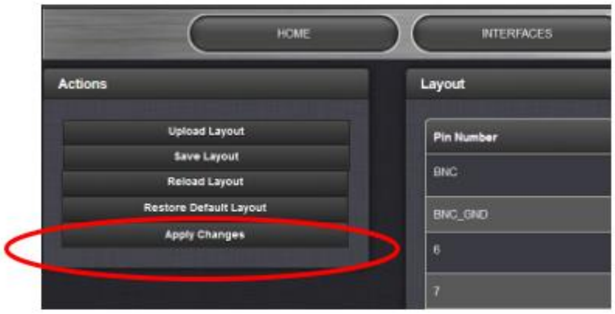
Type Filter: RS485

Pins: 4, 14, 9

IMPORTANT NOTE: for the new settings to be applied the **Apply Changes**” button, needs to be pressed after pressing **Submit**

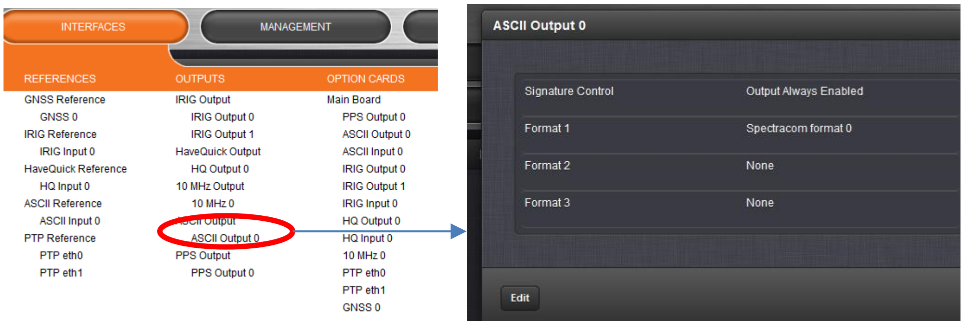
Press **Submit**

"In the Actions panel, click **Apply Changes** after all your configuration is done. This button will finalize your changes and force a server reboot (some timing sources may be affected by this change)."



The Multi-I/O connector on the rear panel will now use pins 4, 14 and 9 for ASCII RS-485 output

a. Go to INTERFACES menu and select the ASCII Output 0 and the EDIT button on the window that opens.

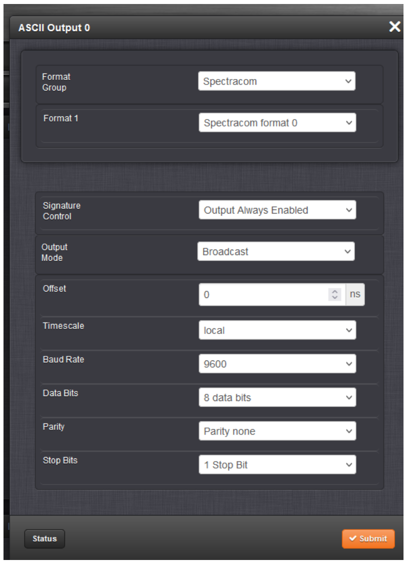


ASCII Output 0

Signature Control	Output Always Enabled
Format 1	Spectracom format 0
Format 2	None
Format 3	None

b. Select the **Format Group = Spectracom, Format 1 = Spectracom Format 0**, and select the **Local Clock** you created from the Timescale dropdown (in this case Eastern Time). Select SUBMIT to save the settings. The RS-485 output has now been setup to supply the correct time and format for the TV400W Display

- Refer also to "Configure an ASCII Output" in the online 2400 SecureSync user guide at: https://safran-navigation-timing.com/manuals/2400/Content/NC_and_SS/2400/INSTALL/Edit_Output_Sets.htm



ASCII Output 0

Format Group: Spectracom

Format 1: Spectracom format 0

Signature Control: Output Always Enabled

Output Mode: Broadcast

Offset: 0 ns

Timescale: local

Baud Rate: 9600

Data Bits: 8 data bits

Parity: Parity none

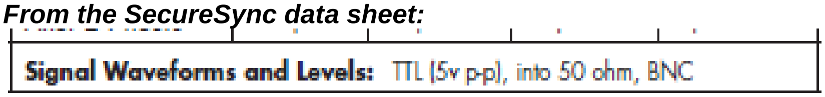
Stop Bits: 1 Stop Bit

**1PPS output (on-time point /System 1PPS) / 1PPS generation

- Every base unit has one 1PPS output (“PPS 0”) on a BNC connector (this is a standard feature on all units).

1PPS TTL output voltage level/specs

From the SecureSync data sheet:



Signal Waveforms and Levels: TTL (5v p-p), into 50 ohm, BNC

Q While looking through the user manual, I had some questions about the characteristics of the 1PPS signal that is provided on the SecureSync 1200. The manual talks about 4.3V, base to peak, but this does not tell me what is the minimum and maximum voltage?
Is the 1PPS signal synced to GPS time? So is the signal always sent out when GPS time ticks to a new second, or does it get sent out every second starting at some arbitrary time (i.e. at whatever time the system is started up)?

A Reply from Dave Lorah (21 Sept 15) The 1PPS signal is a TTL level signal. The base to peak difference is approximately 4.8 Vp-p into 50 ohms, the spec is 4.3 Vp-p minimum. The base being approximately 0 V.

The SecureSync will synchronize the 1PPS output to the GPS 1PPS Reference signal after the signal locks. When locked to the GPS signal the 1PPS output will be +/- 50 nS of the GPS 1PPS.

When the SecureSync first powers up the 1PPS will be arbitrary until it locks to the GPS (or any other) reference source.

Desire for a 3.3v 1PPS output level

- Neither the base 1PPS and or any of the available 1PPS output Option Cards can provide a 3.3v 1PPS output signal.
- Recommend getting a fixed attenuator from Min-Circuits (http://www.minicircuits.com/homepage/homepage.html) to be used external to the SecureSync.

Q According to SecureSync Instruction Manual, the minimum output Signal level is 4.3V minimum.
I got 5.2V output when tested with the Oscilloscope, and I am wondering if this voltage is programmable to output around 3.3V?

A (from Keith 29 Feb 16) The SecureSync’s 1PPS output is not adjustable in amplitude. There isn’t an availability to provide a low voltage (3.3v) 1PPS signal directly from the SecureSync (via either the standard 1PPS connector on the chassis or via an installed Option Card providing a 1PPS output).

If a lower voltage signal is required, I recommend contacting Mini-circuits (http://www.minicircuits.com/homepage/homepage.html) to obtain a fixed attenuator to be applied external to the SecureSync itself to reduce the amplitude of the output signal as necessary for your particular application.

1PPS output configuration

- Can configure the 1PPS output for: Signature Control, Offset, active edge (Rising or Falling) and pulse width

To configure the 1PPS output

1. Navigate to the **Interfaces** -> **PPS Output** page of the browser (PPS output 0 for the base output)
2. Press **Edit**

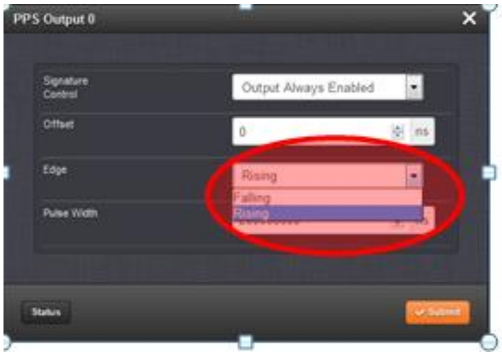
Desire to trigger on trailing/falling edge of the 1PPS output instead of rising edge

- The 1PPS signal can be inverted so that the ontime point (first/active edge) is Falling instead of Rising

- ➢ The data sheet’s 1PPS output accuracy specs are the same whether the active edge is rising or falling.

To configure the active (ontime) edge to be either the “Rising” edge (factory default) or “Falling” edge

1) Navigate to the **Interfaces** -> **PPS Output** page of the browser (PPS output 0 for the base output)
2) Press **Edit**
3) In the “**Edge**” field, select the desired edge (such as “Falling”)



PPS Output 0

Signature Control: Output Always Enabled

Offset: 0 ns

Edge: Rising

Pulse Width

4) Press Submit

1PPS output termination

- ➢ Should be terminated into 50 ohms
- ➢ High impedance termination can cause ringing of the signal
- ➢ Refer to the oscope photos for the difference between high z and 50 ohm termination: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\1PPS Photos

Internal/System delays of 1PPS (System Time)

Q Is there any data about internal delays for 1PPS output? Manual says it's a negligible, but is there any numerical value or estimate available?

A **Per Dave Sohn (22 May 2014)** We have tried to mitigate offset internal generations to minimize internal delays and propagation delays for the 1PPS. I don’t have a specific value for it. Our algorithm tracks the input reference, but is not directly tied to it.

Effects of NTP peering on the oscillator/System PPS/1PPS outputs

- ➢ NTP peering is not recommended for use with Simulcast applications
- ➢ No matter what type oscillator is installed (TCXO, OCXO or RB), when NTP peering is used (such as loss of GPS reception for instance), the System 1PPS (and therefore 1PPS outputs also) is dithered to initially align it with the1PPS obtained from NTP. I believe it’s then periodically dithered to keep it aligned to the NTP 1PPS (in at least versions 5.2.1 and below, which don’t discipline the oscillator when NTP is the selected reference. Host disciplining is in update version 5.3.0- Sept, 2015).
- ➢ The moving of the System PPS when peering is active adversely affects simulcast systems that are relying on a stable 1PPS output.
- ➢ The only input reference recommended for simulcast is GPS!

**System Time message (marker for the time to next 1PPS)

- ➢ New feature added in software version 5.2.0

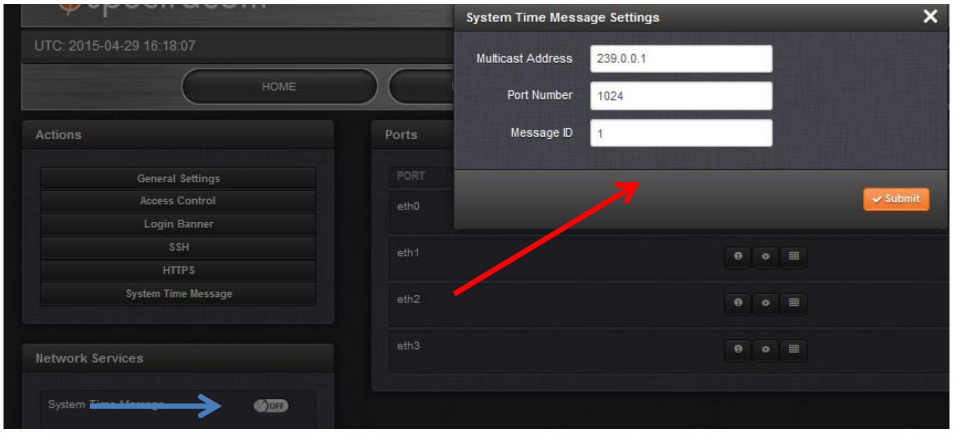
  Per Dave Sohn (29 Apr 15) This existed in 5.2.0 as well. It was done for a specific customer, but could be used by anyone.

- ➢ Once-per-second message which reports which second the 1PPS is in (which second since Jan 1, 1970) and how far into the current second it is (such as 10ns for example) allowing how long to the next 1PPS easy to calculate.

I suspect this message may be used to help determine the accuracy of the 1PPS of an external device synced to the SecureSync. It helps verify if the external device is within the correct second (whether it's behind or ahead of the actual System PPS) and how closely aligned it is to the System PPS (in nanoseconds)

Management -> **Network** page of the browser

- ○ Enable/Disable this service using the slider switch in the bottom left corner under "**Network services**")
- ○ Configure this service by selecting the "**System Time Message**" button in the upper-left corner.



UTC: 2015-04-29 16:18:07

System Time Message Settings

Multicast Address: 239.0.0.1

Port Number: 1024

Message ID: 1

System Time Message

- ➢ This message contains the time when the next 1 PPS discrete will occur. It is sent once per second prior to the 1 PPS discrete.

System Time Message Format

Word	Byte 3	Byte 2	Byte 1	Byte 0
1	Msg ID			
2	Msg Size			
3	Seconds			
4	nSec			
5	EOM			

System Time Message Field Descriptions

Data Name	Data Description	Range	Resolution	Units
Message ID	UID of the message – desire this to be programmable	Unsigned 32 bit integer	1	n/a
Message Size	Total message size in bytes	Unsigned 32 bit integer	1	Bytes
Seconds	Seconds since epoch (00:00:00 Jan 1, 1970 UTC)	Unsigned 32 bit integer	1	Seconds
NSec	NSec within the current second	Unsigned 32 bit integer	1	nsec
EOM	End-of-message	-1	1	N/A

Message ID: An arbitrary number a user can select to send with the data message.

Message Size: I suspect this is the checksum so it can be determined if the entire message was received.

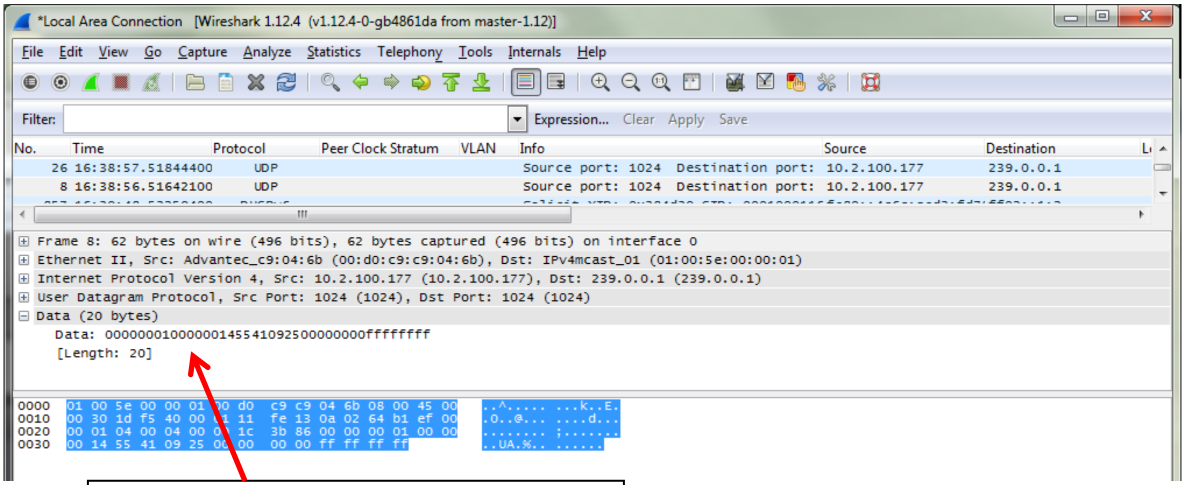
Seconds' field: I suspect this field may be used to help determine the accuracy of the 1PPS of an external device synced to the SecureSync.

Nsec field: is how far into the current second that the 1PPS is aligned to (in nanoseconds), which allows the ability to tell how closely aligned an external system syncing to the SecureSync is to the System PPS. It also allows easy calculation for when to expect the next system PPS to occur (if the field reports 10ns into the second, this indicates there is 990 ns till the next 1PPS on-time point.

EOM field- indicates the end of the message has been received.

Example messages:

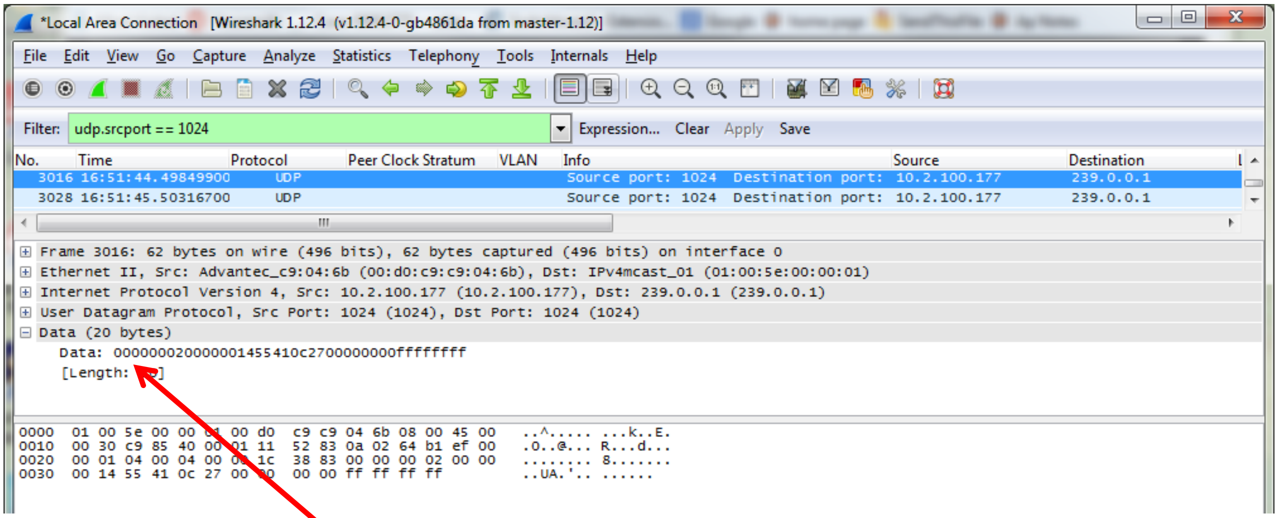
Message ID 1


*Local Area Connection [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time               Protocol  Peer Clock Stratum  VLAN  Info                                                 Source         Destination
  26 16:38:57.51844400  UDP                                 Source port: 1024  Destination port: 10.2.100.177  239.0.0.1
   8 16:38:56.51642100  UDP                                 Source port: 1024  Destination port: 10.2.100.177  239.0.0.1

⊞ Frame 8: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
⊞ Ethernet II, Src: Advantec_c9:04:6b (00:d0:c9:c9:04:6b), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
⊞ Internet Protocol Version 4, Src: 10.2.100.177 (10.2.100.177), Dst: 239.0.0.1 (239.0.0.1)
⊞ User Datagram Protocol, Src Port: 1024 (1024), Dst Port: 1024 (1024)
⊟ Data (20 bytes)
    Data: 00000001000000145541092500000000ffffffff
    [Length: 20]

0000  01 00 5e 00 00 01 00 d0  c9 c9 04 6b 08 00 45 00   ..^..... ...k..E.
0010  00 30 1d f5 40 00 01 11  fe 13 0a 02 64 b1 ef 00   .0..@... ....d...
0020  00 01 04 00 04 00 00 1c  3b 86 00 00 00 01 00 00   ........ ;.......
0030  00 14 55 41 09 25 00 00  00 00 ff ff ff ff         ..UA.%.. ......
```

Configured "Message ID" number ("1")

Message ID 2

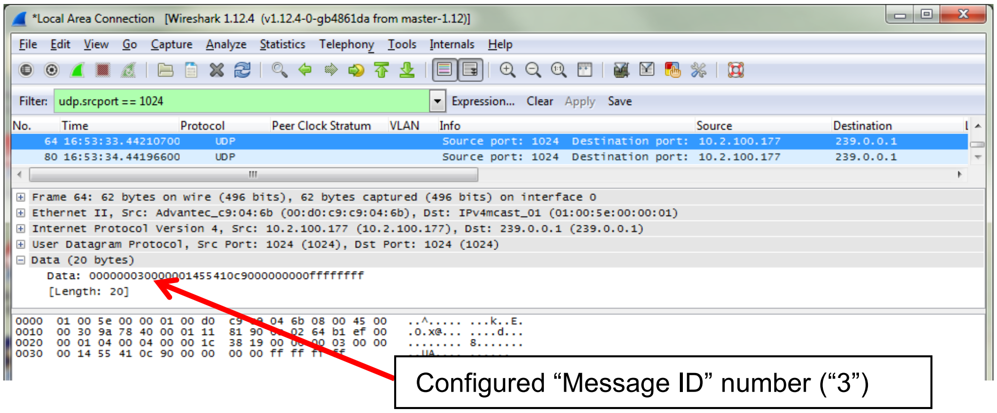

*Local Area Connection [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: udp.srcport == 1024

```
No.  Time                 Protocol  Peer Clock Stratum  VLAN  Info                                                 Source         Destination
3016 16:51:44.49849900    UDP                                 Source port: 1024  Destination port: 10.2.100.177  239.0.0.1
3028 16:51:45.50316700    UDP                                 Source port: 1024  Destination port: 10.2.100.177  239.0.0.1

⊞ Frame 3016: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
⊞ Ethernet II, Src: Advantec_c9:04:6b (00:d0:c9:c9:04:6b), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
⊞ Internet Protocol Version 4, Src: 10.2.100.177 (10.2.100.177), Dst: 239.0.0.1 (239.0.0.1)
⊞ User Datagram Protocol, Src Port: 1024 (1024), Dst Port: 1024 (1024)
⊟ Data (20 bytes)
    Data: 0000000200000001455410c2700000000ffffffff
    [Length: 20]

0000  01 00 5e 00 00 01 00 d0  c9 c9 04 6b 08 00 45 00   ..^..... ...k..E.
0010  00 30 c9 85 40 00 01 11  52 83 0a 02 64 b1 ef 00   .0..@... R...d...
0020  00 01 04 00 04 00 00 1c  38 83 00 00 00 02 00 00   ........ 8.......
0030  00 14 55 41 0c 27 00 00  00 00 ff ff ff ff         ..UA.'.. ......
```

Configured "Message ID" number ("2")

Message ID 3



```
*Local Area Connection   [Wireshark 1.12.4  (v1.12.4-0-gb4861da from master-1.12)]
Filter: udp.srcport == 1024

No.    Time                 Protocol   Peer Clock Stratum   VLAN   Info                                         Source          Destination
   64 16:53:33.44210700     UDP                                    Source port: 1024  Destination port:  10.2.100.177    239.0.0.1
   80 16:53:34.44196600     UDP                                    Source port: 1024  Destination port:  10.2.100.177    239.0.0.1

⊞ Frame 64: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
⊞ Ethernet II, Src: Advantec_c9:04:6b (00:d0:c9:c9:04:6b), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
⊞ Internet Protocol Version 4, Src: 10.2.100.177 (10.2.100.177), Dst: 239.0.0.1 (239.0.0.1)
⊞ User Datagram Protocol, Src Port: 1024 (1024), Dst Port: 1024 (1024)
⊟ Data (20 bytes)
    Data: 00000003000000145541 0c900000000ffffffff
    [Length: 20]

0000  01 00 5e 00 00 01 00 d0  c9 c9 04 6b 08 00 45 00   ..^..... ...k..E.
0010  00 30 9a 78 40 00 01 11  81 90 0a 02 64 b1 ef 00   .0.x@... ....d...
0020  00 01 04 00 04 00 00 1c  38 19 00 00 00 03 00 00   ........ 8.......
0030  00 14 55 41 0c 90 00 00  00 00 ff ff ff ff         ..UA.... ......
```

Configured “Message ID” number (“3”)

Base 1PPS output Enable / Disable control using CLI “ppsctrl” command

- Version 4.8.7 (~Sept 2012) added ppsctrl command to enable or disable the 1PPS output on the rear panel

Q from BAE systems- Our requirement is to be able to Enable\Disable the 1PPS outputs programmatically. To do so, I use the CLI command ppsctrl. The question is, can the resultant output level of a disabled 1PPS control be programmatically set? Most times, when disabled it is 0V which is what we need. Sometimes though, it is 10V which is bad for us. It seems the level depends on where in the 1PPS pulse the output transitions to disabled.

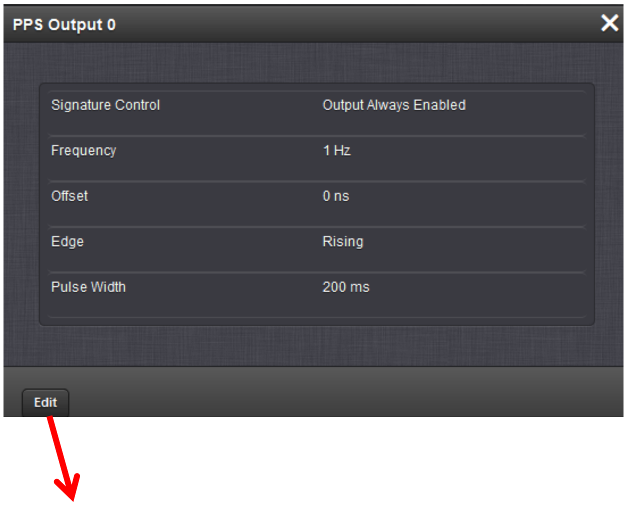
A Per Dave Sohn 19 Mar 15: “We currently freeze the output at the current level, I believe, and is played out according to your report. There isn’t a way to do what you want programmatically. However, depending on the responsiveness for your disable, you could perform the disable half way through the second, which would ensure that the 1PPS is already in its inactive state.

1PPS output configuration

- 1PPS out configuration consist of: Signature Control, Offset, Edge and Pulse Width

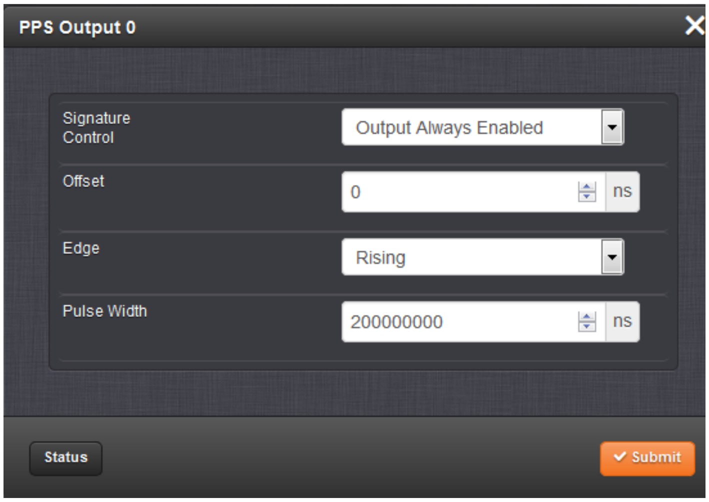
A) Newer web browser

Interfaces -> **Outputs** -> **PPS Output 0** page of the browser (see “Signature Control” below)



PPS Output 0

Signature Control	Output Always Enabled
Frequency	1 Hz
Offset	0 ns
Edge	Rising
Pulse Width	200 ms


PPS Output 0

Signature Control: Output Always Enabled

Offset: 0 ns

Edge: Rising

Pulse Width: 200000000 ns

1PPS output Signature Control

Signature Control cannot take effect during power-up, until the software is operational. During initial power-up, the 1PPS output will be present. Once the software is running, the 1PPS output will then be suppressed, if Signature Control is enabled. There is no hardware Signature Control available to suppress the output upon initial power-up.

1PPS Pulse Width

- Default Pulse Width is 200 milliseconds wide.
- 1PPS output Pulse Width range (based on the web browser and info in the Option Card section of the manual): 20ns to 900ms.
- Configurable in the ***Setup*** -> ***Outputs*** -> ***1PPS Frequency*** page of the browser.

Q. Can SecureSync send 3.3v TTL by change of configuration parameter (Base PPS or Option Card)

A. **Reply from Dave Lorah (19 Apr 13)** The 1PPS TTL is based on a 5V signal level. This is true for the main chassis 1PPS signal and any option card 1PPS TTL outputs. There is one exception of the 1204-19 1PPS card, which is 10V level.

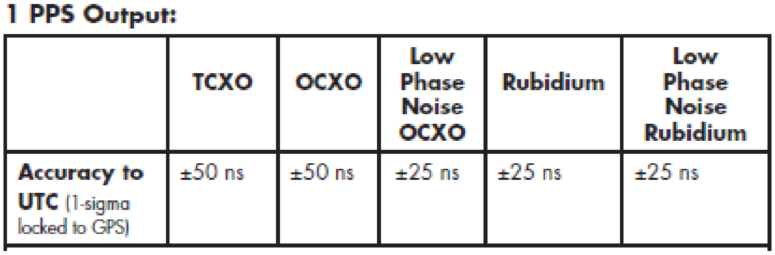
None of these has a 3.3V TTL signal. The 1PPS TTL levels are not adjustable and will always be 5V.

1PPS generation/1PPS alignment to 10 MHz

- Refer to the 10MHz output section for info regarding 10MHz and 1PPS phase alignment: 10 MHz phase alignment to 1PPS input reference

1PPS output accuracy

- Specs from the data sheet (oscillator dependent, when locked to GPS)



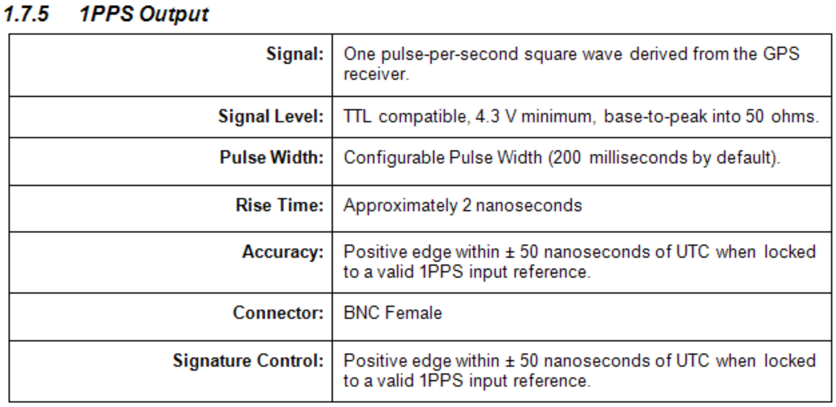
1 PPS Output:

	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium
Accuracy to UTC (1-sigma locked to GPS)	±50 ns	±50 ns	±25 ns	±25 ns	±25 ns

---

1PPS output Holdover (System Time drift with no input references available)

- Refer to: Oscillator Holdover specs
- 1PPS output connector specs from manual:



1.7.5 1PPS Output

Signal:	One pulse-per-second square wave derived from the GPS receiver.
Signal Level:	TTL compatible, 4.3 V minimum, base-to-peak into 50 ohms.
Pulse Width:	Configurable Pulse Width (200 milliseconds by default).
Rise Time:	Approximately 2 nanoseconds
Accuracy:	Positive edge within ± 50 nanoseconds of UTC when locked to a valid 1PPS input reference.
Connector:	BNC Female
Signature Control:	Positive edge within ± 50 nanoseconds of UTC when locked to a valid 1PPS input reference.

Pulse rise time <4 ns
The 1PPS output from the main unit is ~2ns.
The 1PPS output from the 1204-01 option card is ~16ns.

Jitter <50 ps
The PLLs used in our FPGAs to generate the 1PPS outputs can have as much as ±2ns jitter (The following are the clocks used internally and the maximum PLL jitter: 10MHz = ±2ns, 50MHz = ±500ps, 200MHz = ±125ps)

Stability <20 ps / K between 20 ° C and 30 ° C ambient temperature
We don't have data on this, but the oscillators have the following specs over the entire operating range of the unit of the following (MP OCXO = 5ppb, HP OCXO = 1ppb, RbXO = 0.5ppb)

Pulse transit time difference between the outputs (output to output skew) <100ps
The 1PPS output from the main unit and 1204-01 option card are ~35ns apart, although that could be resolved to within 5ns.

Optional is a **configurable output frequency** of this reference pulse output by the user benefit. We are not sure what this means. The frequency of the 1PPS output is not configurable. However, the pulse width and active edge of the 1PPS can be configured.

1PPS output impedance

Email from Mark McGregor about the SecureSync 1PPS output (11/22/10): You are correct that the source/output impedance of the SecureSync 1PPS output is about 8 to 10 ohms. Our product data sheet does not state that the source impedance of the 1PPS output is 50 ohms. For 1PPS output it states "Signal Waveforms and levels: TTL (5Vp-p) into 50 ohm, BNC". See the bottom of page two on the attached product data sheet. This statement says that the SecureSync 1PPS output can drive a 50 ohm load. It does not say that the SecureSync 1PPS output is a 50 ohm source/output impedance. It should be corrected to say 4.3Vp-p, rather than 5Vp-p. The instruction manual has the 1PPS output voltage levels correct in section 1.7.5. I attach it here as well for your reference.

You can use the SecureSync source impedance of the 1PPS output in the voltage divider you outlined several emails down, but it is around 8 to 10 ohms. The 1PPS output is 4 each, 5V powered, ACT logic gates with a 4.75 ohm resistor in series with each gate output, connected in parallel at the 4.75 ohm resistor outputs to be able to source the current needed to drive 50 ohms. The 4.75 ohm resistors are all tied together to form the 1PPS output. You will have to adjust the “Rseries” up to account for the lower “Resource” to get the voltage divider you show several emails down to work the way you want it to.

Also, the 1PPS output is a fast rise time signal, ~2 nanoseconds into 50 ohm load, so in order to avoid large amounts of reflections/ringing the 1PPS output must be terminated with 50 ohms at the destination. If the 1PPS output is connected to a digital input that is a high impedance load there will be severe reflections/ringing. The scheme you showed should do that, more or less.

1PPS cable lengths

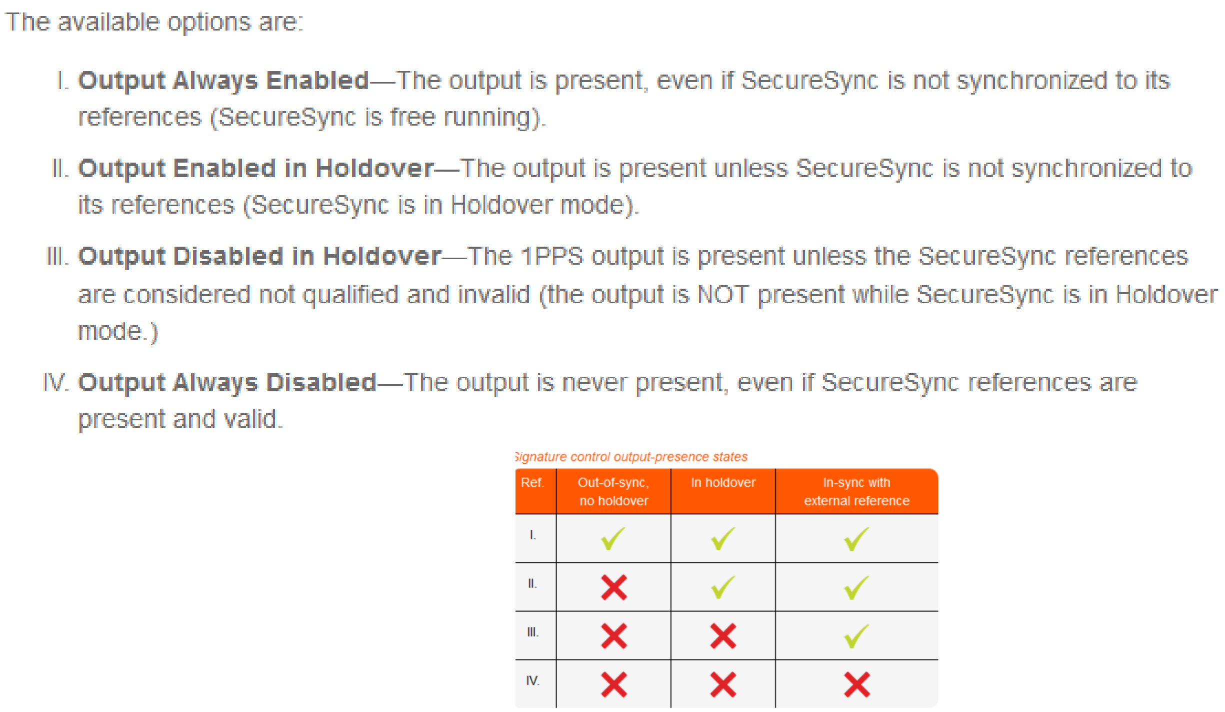
Q. How long can the RG-58 cable for the SecureSync’s 1PPS output be to an SASe.
A. Reply from Dave Lorah on 9/16/11, based on engineering feedback:
We verified overnight running a 1PPS through a SAS synchronizing a SecureSync through around 800 feet of RG58 cabling. The maximum cable length is not determined. Hopefully 800 feet is longer than you need. Of course running through that much cable, you will have to compensate for the propagation delay of the cable and the effects of the slower rise time. The propagation delay of RG-58/U cable is about 1.51 ns/ft.

Signature Control for various outputs (such as IRIG, 1PPS, 10 MHz, etc)

- Refer to (in online 2400 SecureSync online manual): http://manuals.spectracom.com/2400/Content/_Global/Topics/SETUP_Sha/Signature_Control.htm?

Function of Signature Control

Signature Control is a user-set parameter that controls under which output states an output will be present. This feature allows you to determine how closely you want to link an output to the status of the active input reference e.g., by deactivating it after holdover expiration. It is also offers the capability to indirectly send an input-reference-lost-alarm to a downstream recipient via the presence of the signal.



The available options are:

I. **Output Always Enabled**—The output is present, even if SecureSync is not synchronized to its references (SecureSync is free running).

II. **Output Enabled in Holdover**—The output is present unless SecureSync is not synchronized to its references (SecureSync is in Holdover mode).

III. **Output Disabled in Holdover**—The 1PPS output is present unless the SecureSync references are considered not qualified and invalid (the output is NOT present while SecureSync is in Holdover mode.)

IV. **Output Always Disabled**—The output is never present, even if SecureSync references are present and valid.

ignature control output-presence states

Ref.	Out-of-sync, no holdover	In holdover	In-sync with external reference
I.	✓	✓	✓
II.	✗	✓	✓
III.	✗	✗	✓
IV.	✗	✗	✗

**10 MHz output

Number of 10 MHz outputs

- **Base unit has one 10MHz out.**

Available add-in Option Card for 3 additional 10 MHz outputs (on each Card)

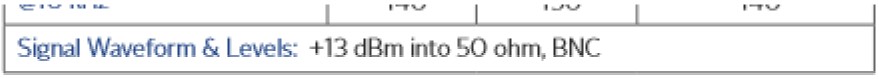
- Model 1204-1C

Output signal levels/amplitude (base unit and 1204-1C option card)

- Refer to 2400 SecureSync online user guide: http://manuals.spectracom.com/2400/Content/NC_and_SS/2400/INTRO/Specs_10MHzOut.htm?Highlight=10%20mhz

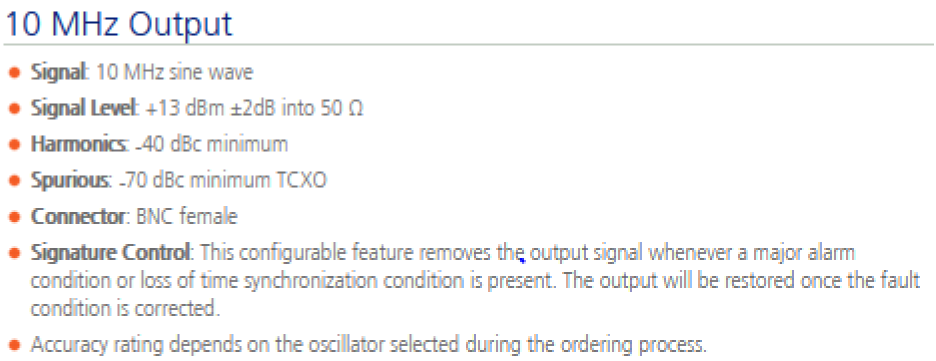
Output signal: Sinewave

- From 2400 datasheet:



Signal Waveform & Levels: +13 dBm into 50 ohm, BNC

- From 2400 online user guide:



10 MHz Output

- **Signal**: 10 MHz sine wave
- **Signal Level**: +13 dBm ±2dB into 50 Ω
- **Harmonics**: -40 dBc minimum
- **Spurious**: -70 dBc minimum TCXO
- **Connector**: BNC female
- **Signature Control**: This configurable feature removes the output signal whenever a major alarm condition or loss of time synchronization condition is present. The output will be restored once the fault condition is corrected.
- Accuracy rating depends on the oscillator selected during the ordering process.

- Output level/gain is not adjustable inside the SecureSync.
- Use external line attenuators if amplitude into 50 ohm input impedance is too high.

Output impedance: 50 ohms

Issue: LOW 10 MHz output (base and 1204-1C card) amplitude observed at about 2dBM instead of about 13dBm (as expected)

- Refer to Salesforce Case 269551

Per Jose Rodriguez (15 July 2021 This is interesting. We experienced a similar problem on 2 of the units in production. Can they check the ribbon cables inside the unit are seated correctly and that they are not misaligned?

Simulcast radio system terminations

- Also refer to the “Simulcast radio systems 10 MHZ inputs” section of the the Custserviceassistance doc

Q. How many base stations can the 10mhz output port successfully drive?
A. Reply from Ed O’Connor (8 Dec 16) In general for some bases (such as Moto GTR8000, Harris Mastr 3, Kenwood NXR700/800) our output should drives just one base since 10MHz input on those bases have a 50 ohm termination. We can probably successfully drive 2 bases, it is up to the customer to verify, and I discourage any more than 2 bases

10MHz input on Tait bases has a high-z impedance. I have heard of customers driving 7-8 base stations off a single 10MHz output

10 MHZ frequency Offset

(As of at least Nov 2012, Archive version 4.8.7 and below) Unlike the Model 8195 series Master Oscillators had the ability to offset the 10 MHz output by a specific value (using the 1FO command).This capability was not carried over to the SecureSync and 9400 series.

Ed O'Connor said today he may consider seeing it added with the “cleanup” oscillator, but it’s not currently available.

****10 MHz phase alignment to 1PPS input reference

1PPS generation

- Except after boot-up, there are always 10,000,000 frequency counts between each 1PPS.

Note: (2 Jan 2014) Curtis Somers reported they observed an extra count, especially when going into Holdover mode. (Refer to Salesforce case 12863)

Questions from a customer (refer to SF case 95886)

1. Is it possible to get the 1PPS rising edge 10-20 ns before the 10MHz rising edge with the secureSync?
2. Is there a relationship between Phase Error and the 1PPS/10MHz skew?

The relationship between the rising edge of 1PPS and the rising edge of 10MHz is unclear to me based on the SecureSync User Reference Guide Rev 23.

Scope measurement shows the 1PPS and 10MHz rising edges are not aligned. Also the Phase Error relationship to this 1PPS/10MHz skew is unclear.

We coded some VHDL assuming the 1PPS comes after the 10MHz (not before) so we may need to change some VHDL for the FPGA based on your response.

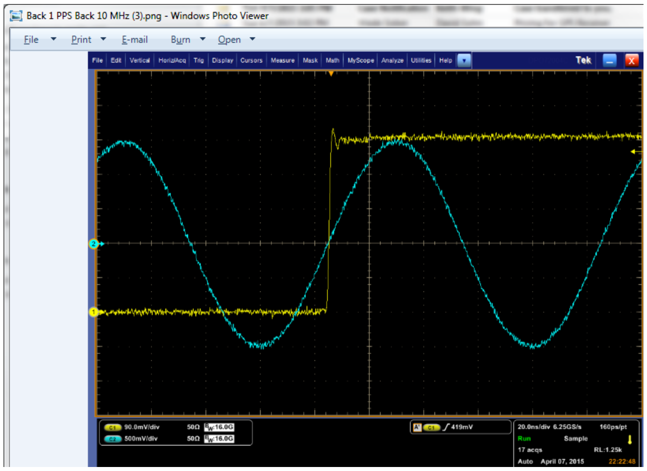
A REPLY FROM Jodi, after woking with Tom Richardson (18 Jul 17) I consulted with an Engineer yesterday about your questions. A SecureSync unit in the lab was tested, and the 1PPS rising edge was coincident with the 10 MHz rising edge with 1PPS offset set to 0. You should be able to use the offset setting in the 1PPS setup page to delay the 1PPS by 20 nSec. We have set the offset to 20 nSec on this device and the 1PPS moved 20 nSec earlier than the 10 MHz rising edge.

Also, are you using matched length cables? Cable delay is about a nanosecond per foot of coaxial cable. Another way to get a 20 nSec delay in the 1PPS is to add about 20 feet of coaxial cable to the output of the 1PPS. The resolution of the adjustment of the 1PPS offset should be approximately 5 nanoseconds so you could fine adjust by changing the length of a coaxial cable acting as a delay line.
There should always be 10 million cycles of the 10 MHz between the 1PPS output. The phase error relationship between the 1PPS and the 10 MHz should always be a fixed amount. In other words they move together when the 10 MHz is adjusted.

1PPS / 10 MHz alignment at the base 10 MHz output port versus all of the 1204-1C Option Card outputs

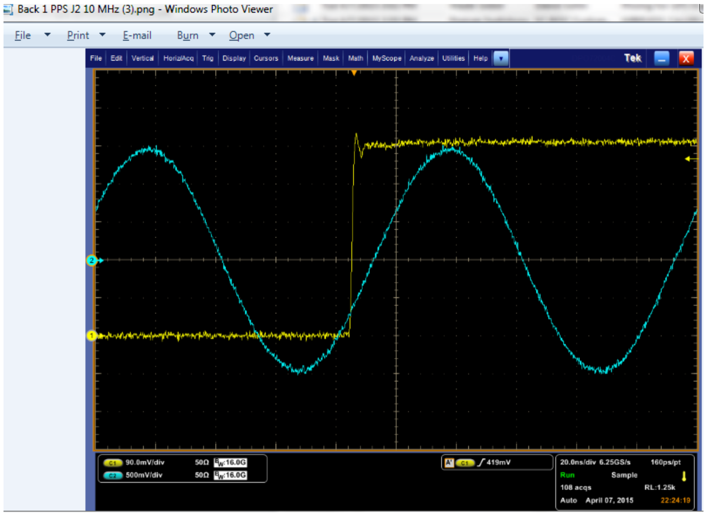
- ➢ Refer to Salesforce case 17618.
- ➢ 1PPS /10 MHz alignment at the base 10 MHz output port is slightly different on the 1204-1C 10MHz output Option Cards
- ➢ 1PPS /10 MHz alignment at the base 10 MHz output port is the same as the outputs of the earlier 1204-0C 10 MHZ Option Cards.
- ➢ This is due to the 10 MHz distribution for the base output port being different than the 1204-1C Cards.

1PPS/10MHz alignment for base output (and 1204-0C 10 MHz Option Cards)


Back 1 PPS Back 10 MHz (3).png - Windows Photo Viewer
File
Print
E-mail
Burn
Open
File Edit Vertical Horiz/Acq Trig Display Cursors Measure Mask Math MyScope Analyze Utilities Help
Tek

C1 90.0mV/div 50Ω BW:16.0G
C2 500mV/div 50Ω BW:16.0G
A' C1 ∫ 419mV
20.0ns/div 6.25GS/s 160ps/pt
Run Sample
17 acqs RL:1.25k
Auto April 07, 2015 22:22:48

1PPS/10MHz alignment for all 1204-1C option Card outputs


Back 1 PPS J2 10 MHz (3).png - Windows Photo Viewer
File
Print
E-mail
Burn
Open
File Edit Vertical Horiz/Acq Trig Display Cursors Measure Mask Math MyScope Analyze Utilities Help
Tek

C1 90.0mV/div 50Ω BW:16.0G
C2 500mV/div 50Ω BW:16.0G
A' C1 ∫ 419mV
20.0ns/div 6.25GS/s 160ps/pt
Run Sample
108 acqs RL:1.25k
Auto April 07, 2015 22:24:19

Per Dave Sohn (7 Apr 2015) This is what I would expect from the system. There is no HW issue. The phase relationship on a 10MHz output is fixed with the 1PPS, but there is a difference between the outputs on the option card versus the main unit. If they need multiple outputs that have the same phase relationship, then they can just use the 1C option card outputs.

Dave Sohn responded with: This specification is held once HW adjustments are disabled after first sync (or if restart tracking is sent). At this point, the 1PPS is generated directly from the 200HZ clock, which is generated through a PLL from the 10MHz. However, when going into holdover, the 10MHz frequency will change from the current correction frequency to our best estimate of the correct frequency without any corrections for phase errors. It's possible that with that change, the 1PPS may appeared to have one extra cycle if an edge transitioned later because of the frequency change and how their counter is tracking it and the 1PPS.

Phase alignment of 10 MHz outputs from multiple TSync-PCIe boards or SecureSyncs

Because KTS disciplining performs phase alignment of the 10 MHz output, unlike earlier NetClocks which only perform Frequency adjustments, if more than one TSync or SecureSync are synced to the same IRIG or GPS signal, the 10 MHZ outputs will be in phase with each other (not just corrected for frequency).

Frequency Accuracy Error can be viewed to see if the 10 MHz oscillator is adjusting to the input reference (should continue to decreas on as it gets closer). The current **Frequency Accuracy Error** can be viewed in the **Status ->Time and Frequency** page.

Email from Dave Sohn (12/13/11):

"Synchronization works in SecureSync by trying to adjust the oscillator frequency to match the system's 1PPS in phase and frequency to the reference source. By matching the system 1PPS phase, which is aligned to the 10MHz on-board, we also get some phase alignment of the 10MHz signal itself. In order to match phase and frequency, each unit will be making adjustments to the frequency of the internal 10MHz oscillator. There is a maximum adjustment that can be made each second, and a maximum adjustment that can be made overall to limit the frequency error generated by the disciplining itself. There is also a limit as to the minimum adjustment our disciplining system to help reduce adjustments for very accurate references to minimize issues.possible to the oscillator frequency. That is a factor of the oscillator's control voltage range, pullability, and the precision of our DAC. Typically, for a HP (High

Performance) OCXO the minimum adjustment we can do is 0.000015 Hz, which when multiplied up to their 3GHz frequency is 0.0046 Hz.

We are already working on improvements to our disciplining system to help reduce adjustments for very accurate references to minimize issues.

Desire to phase align the 10 MHz of more than one SecureSync when using IRIG input for synchronization of the SecureSyncs.

- We recommend using IRIG DCLS input (not IRIG AM) for optimum phase alignment (DCLS has a faster rise-time than AM, so it has a “crisper” on-time point).
- We don’t recommend using IRIG A input, for optimum phase alignment.
- As long as all SecureSyncs are synced to the same IRIG source, their 10 MHz outputs should be farily closely phase-aligned with each other

Email from Sam Otto to Leisa Butler after taking to Denis Reilly (26 Mar 2013)

Once the 1PPS signal from the IRIG **DCLS** signal is locked by the oscillator (OCXO or Rb) the 10MHz will be in Sync and in phase with it.

We do not recommend IRIG-A.

The same IRIG DCLS Signal will suffice as long as both SecureSyncs oscillators are in sync with the same IRIG DCLS signal their respective 10MHZ outputs will be in phase

Q. How closely are the 10MHZ and the 1PPS slaved together?
A. Except during power-up, there are always 10 million cycles of 10MHz between each 1PPS.

Additional response from Denis Reilly (8 Oct 201) “Further info (probably more than the customer needs at the moment):”

Except during power-up, there are always 10 million cycles of 10MHz between each 1PPS. After a reboot or power cycle, when the SecureSync syncs to a reference for the first time, the 1PPS and 10MHz are not guaranteed to be locked together during tracking setup.

When the Disciplining State transitions to “Locked”, we lock the 1PPS and 10MHz together, and guarantee that there will be 10 million clock cycles between PPS’s as long as the Disciplining State remains “Locked”. (We can keep both the 10 MHz and 1PPS synchronized to the reference in this state without slipping the signals relative to each other.)

If a unit loses all of its references, and the holdover timeout expires, and the unit enters the Freerun state for a long time, there is a chance that upon acquiring a reference again the relationship between the 10MHz and 1PPS may drift again. But once the disciplining state becomes “Locked” again, the 10 MHZ and 1PPS will be locked together again, and there will be exactly 10 million 10MHz cycles in between PPS’s.

Email from Dave Lorah (18 Nov 2013) The SecureSync 1PPS is derived from the 10 MHz, so it should not be wandering at all. I think your scope may be set at the wrong horizontal time base and aliasing the 10 MHz signal. I could reproduce this on my scope too if using a millisecond per division range.
Switch to a 20nS/div scale and the 10 MHz should be locked on.

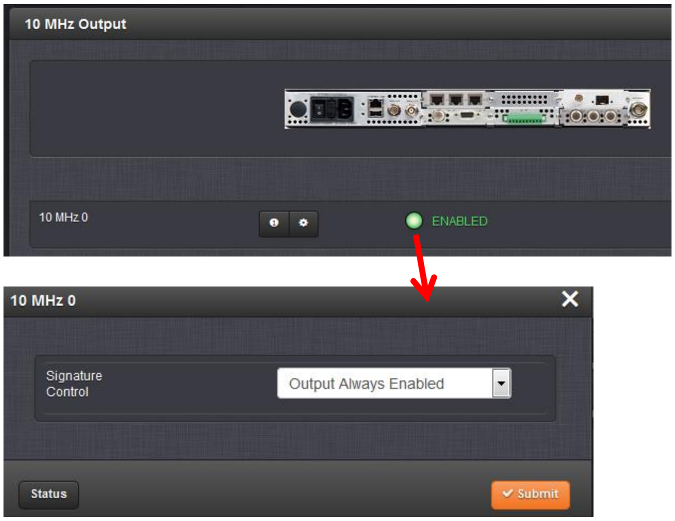
Please let me know if you see anything different.

10 MHz output configuration

9. 10 MHz out configuration is limited to just Signature Control

A) Newer web browser

Interfaces -> **Outputs** -> **10 MHz Output** page of the browser (see “Signature Control” below)



Signature Control: Output Always Enabled

****10 MHz output Signature Control

The SecureSync has a feature that can be enabled, which squelches the 10 MHz output when either the SecureSync’s Sync state is not “true” OR when the SecureSync has no valid input references present (depending on how this mode is configured). This mode is called “**Signature Control**”.

Signature Control can be enabled in SecureSync (it is disabled by default) using the web browser. Navigate to the **Setup-> Outputs -> “1PPS 10MHz”** page of the browser. Configure the “**Signature Control**” field as desired. The available selections are defined below:

- “**Output Always Enabled**”: 10 MHz output is always present (no matter the Sync status or whether input references are present and valid)
- “**Output enabled in Holdover**”: 10 MHz output is only present when the SecureSync is either in the Sync or Holdover modes.
- “**Output Disabled in Holdover**”: 10 MHz output is only outputted when the TSync board has a valid input reference present.
- “**Output Always Enabled**”: 10 MHz output is never present.

Signature Control during SecureSync power-up

Signature Control cannot take effect during power-up, until the software is operational. During intial power-up, the 10MHz output will be present. Once the software is running, the 10MHz output will then be suppressed, if Signature Control is enabled. There is no hardware Signature Control available to suppress the output upon initial power-up.

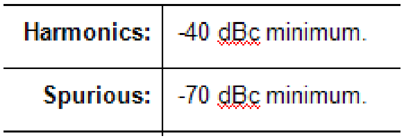
***10 MHZ output Phase noise / Harmonics/ spurs

Refer to datasheet for phase noise and harmonics measurements/specs: I:\Marketing_Product Data Sheets (archive)\Time & Frequency References

Phase noise measurements: Refer to SecureSync data sheet. Per Mark McGregor, phase noise specs are for all 10 MHz outputs (the base 10 MHz as well as 10MHz outputs from installed 10MHz output Option Cards).

Mark also said this doesn't apply to or other output Option Cards, because of the dividers used to generate the smaller frequencies cause a great amount of phase noise.

Harmonics (From the SecureSync manual)



Harmonics:	-40 dBc minimum.
Spurious:	-70 dBc minimum.

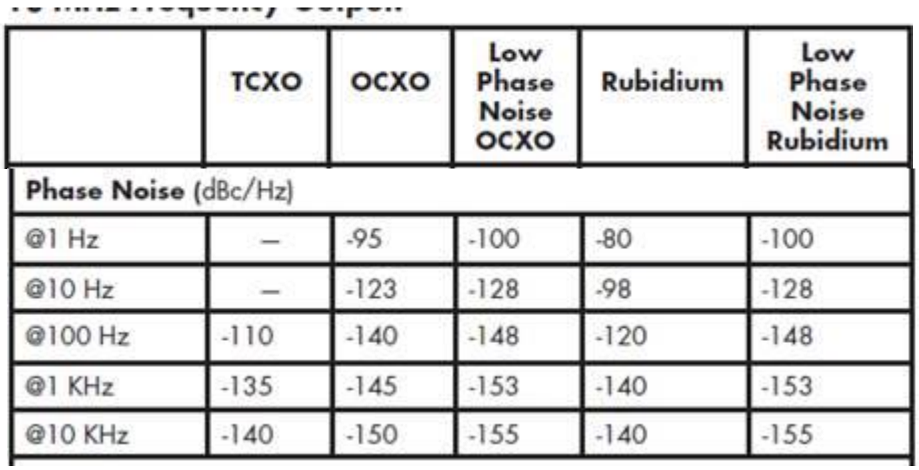
For plots of the 10 MHz harmonics and spurs with an OCXO installed, refer to the email from Tom Richardson (8/2/12) in the following folder: EQUIPMENT\SPECTRACOM EQUIPMENT\Timing boards\TSYNC-PCIe\10MHz output

Phase noise specs at 100 KHz ("@100 KHz")

- SecureSync data sheet doesn't provide phase noise specs for @100 KHz (10 KHz is highest)
- Per Tom Richardson, the phase noise at 100 KHz is very similar to, or just slightly better, than the phase noise at 10 KHz.

Q. from Danny Loke Can you help me to find out the specs of phase noise of LN OCXO and Rb @ offset 100kHz?
A The phase noise specs for all of the various SecureSync oscillator configurations are in a table on page 2 of the SecureSync data sheet (attached).

On the left side, scroll down to "**Phase Noise**" as excerpted below:

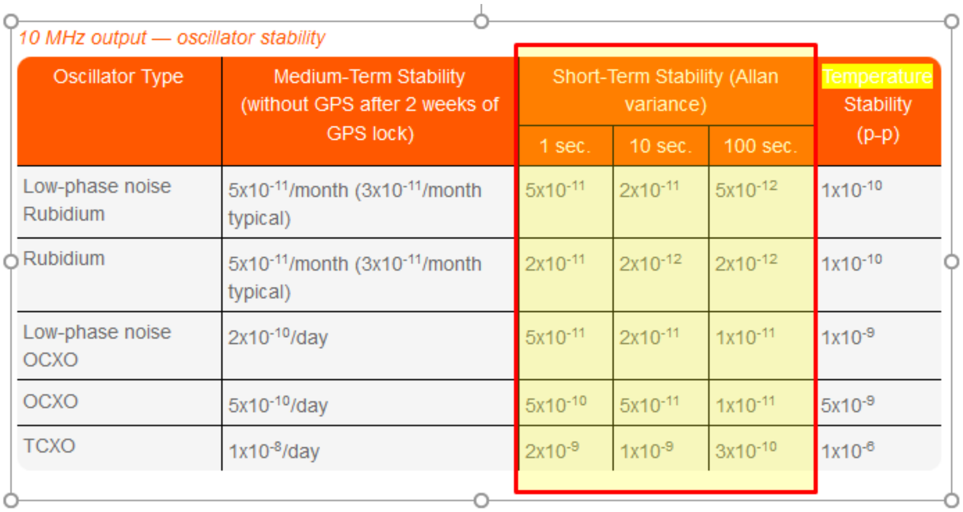


	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium
Phase Noise (dBc/Hz)					
@1 Hz	—	-95	-100	-80	-100
@10 Hz	—	-123	-128	-98	-128
@100 Hz	-110	-140	-148	-120	-148
@1 KHz	-135	-145	-153	-140	-153
@10 KHz	-140	-150	-155	-140	-155

Though we don't spec the phase noise at 100 KHz, I spoke to one of our engineers that normally performs the phase noise testing. He said the phase noise at 100 KHz is very similar to, or just slightly better, than the phase noise at 10 KHz.

Allan Deviation/Allan Variance (oscilator’s output)

- Refer to the following link for the plots referenced below: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\10 MHz Oscillators\Allen Deviation plots
- Refer to the SecureSync data sheet for specs (also in online S/S manual at: http://manuals.spectracom.com/SS/Content/NC_and_SS/SS/Topics/INTRO/Specs_10MHzOut.htm?Highlight=allan%20variance)



10 MHz output — oscillator stability

Oscillator Type	Medium-Term Stability (without GPS after 2 weeks of GPS lock)	Short-Term Stability (Allan variance)			Temperature Stability (p-p)
		1 sec.	10 sec.	100 sec.	
Low-phase noise Rubidium	$5x10^{-11}$/month ($3x10^{-11}$/month typical)	$5x10^{-11}$	$2x10^{-11}$	$5x10^{-12}$	$1x10^{-10}$
Rubidium	$5x10^{-11}$/month ($3x10^{-11}$/month typical)	$2x10^{-11}$	$2x10^{-12}$	$2x10^{-12}$	$1x10^{-10}$
Low-phase noise OCXO	$2x10^{-10}$/day	$5x10^{-11}$	$2x10^{-11}$	$1x10^{-11}$	$1x10^{-9}$
OCXO	$5x10^{-10}$/day	$5x10^{-10}$	$5x10^{-11}$	$1x10^{-11}$	$5x10^{-9}$
TCXO	$1x10^{-8}$/day	$2x10^{-9}$	$1x10^{-9}$	$3x10^{-10}$	$1x10^{-6}$

Per Wikipedia: https://en.wikipedia.org/wiki/Allan_variance

The **Allan variance** (**AVAR**), also known as **two-sample variance**, is a measure of frequency stability in clocks, The *Allan variance* is intended to estimate stability due to noise processes and not that of systematic errors or imperfections such as frequency drift or temperature effects. The Allan variance and Allan deviation describe frequency stability. See also the section entitled "Interpretation of value" below.

Email from Dave Lorah to Mark Goldage with GE (14 Feb 2013)

I had to consult engineering for this data. I think this is what you are looking for.

Here is an Allan deviation plot and a histogram of 5 days of a 9483 TCXO unit with GPS reference. This is 495634 seconds of data taken once per second.

The histogram shows a standard deviation of 8.5e-8, so 3 stds would be 2.55e-7, so uncertainty would be 10 MHz +/- 2.55Hz.
The Allan deviation plot is a measure of the stability over observation time. This shows that for an observation time of 6.55e4 (18 hours) the stability is about 2 parts in 10 -12.

Report of Allan Variance/Allan Deviation failing customer testing

- Refer to Salesforce case 171261 (9 Aug 2018)

Email from Tom Richardson (9 aug 18) Get the test methodology and equipment used if possible. Also what rev the software was at. These specs are by design and we do not 100% test our product for these specifications. If they want it I think there is an additional charge.

My reply to the customer (9 Aug 18) about the specific report, before just assigning an RMA for the two SecureSyncs to be returned to Spectracom. We have some questions/requests for you, based on the specific failure report.

There are some “variables” which can affect Allan Variance test results. Environmental/temperatures during the testing is one (were the units allowed to warm-up/stabilize before any testing was started? Did the ambient temperature remain consistent through the test?, etc). Another “variable” is the version of software installed in the SecureSync, when the testing was performed.   What is the version of software installed in the two SecureSyncs?

If you aren’t sure what version of software is currently installed, there are a few different ways to obtain the version:
Note the software version of the **SecureSync** will be a 5.x.x number:

A. Via the front panel keypad/LCD display (**System** -> **Vers** menus)

B. With a CLI connection (telnet, ssh or front panel RS-232 cable) type: **version** <enter>. The version command will respond with the current version of software installed.

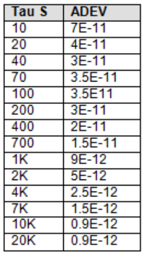
C. With the web browser. the System version is reported in the **Tools** -> **Upgrade/Backup** page.

If addition to letting us know the installed version of software, can you also send us the test methodology/environmental conditions during the testing, what test equipment was used to perform the Allan deviation testing, test reports, etc. If possible, we would like to take a look at as much info you can provide us with about the actual testing, before just having the units returned to us.

Thanks very much in advance (if its not too much inconvenience) for providing us with as much of the above info you can. Then we can go from there 😊!

1PPS output phase noise

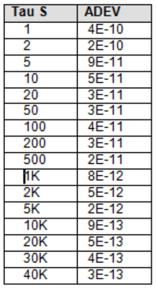
Email from John Westwood to Tom Richardson, (based on his testing)
Here is the measured 1ppS data, measured on an OCXO SS with GPS control.



Tau S	ADEV
10	7E-11
20	4E-11
40	3E-11
70	3.5E-11
100	3.5E11
200	3E-11
400	2E-11
700	1.5E-11
1K	9E-12
2K	5E-12
4K	2.5E-12
7K	1.5E-12
10K	0.9E-12
20K	0.9E-12

I will set this up for an extended run (this was 65 hours).

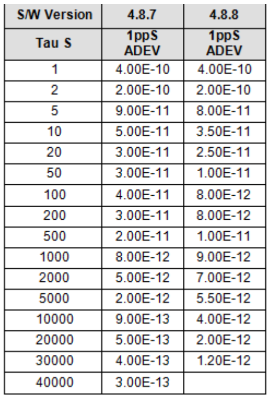
Second email from John Westwood 11 Feb 2013 Here are the ADEV measurements over 7 days, this time with our Cesium as a reference – previous data was with the internal Rb reference (no GPS on this STA-61).



Tau S	ADEV
1	4E-10
2	2E-10
5	9E-11
10	5E-11
20	3E-11
50	3E-11
100	4E-11
200	3E-11
500	2E-11
1K	8E-12
2K	5E-12
5K	2E-12
10K	9E-13
20K	5E-13
30K	4E-13
40K	3E-13

Very similar results up to 10K.

Another email from John Westwood (18 Feb 2013): Here are the results for both 4.8.7 and 4.8.8 software versions SecureSync 1200-013 with continuous GPS control Running for >7 days before start of collection 1ppS Adev measured on STA-61 with Cesium reference 1 second sample rate - run time 7 days



S/W Version	4.8.7	4.8.8
Tau S	1ppS ADEV	1ppS ADEV
1	4.00E-10	4.00E-10
2	2.00E-10	2.00E-10
5	9.00E-11	8.00E-11
10	5.00E-11	3.50E-11
20	3.00E-11	2.50E-11
50	3.00E-11	1.00E-11
100	4.00E-11	8.00E-12
200	3.00E-11	8.00E-12
500	2.00E-11	1.00E-11
1000	8.00E-12	9.00E-12
2000	5.00E-12	7.00E-12
5000	2.00E-12	5.50E-12
10000	9.00E-13	4.00E-12
20000	5.00E-13	2.00E-12
30000	4.00E-13	1.20E-12
40000	3.00E-13	

The 4.8.8 version has improved between 50 and 1000 seconds but is worse greater than 1000 seconds.

FYI: After changing to 4.8.8, the oscillator log does not show any DAC values, only frequency calculations.

****Oscillator warm-up time

- **OCXO oscillators fort TSync**: Warm-up time is about one (1) minute
- OCXO oscillators for SecureSync: Warm-up time is (3) minutes
- **Rb oscillator**: Warm-up time is about ten (10) minutes.

Note: The outputs will be stable after the warm-up time but will not be locked.

****Frequency Accuracy error measurements

Calculated Frequency error (versus desired 10.00000MHz) is displayed on the **Status** ->**Time and Frequency** page of the web browser.

Operation:
Shortly after the **first** time the NTP server powers up, the 10MHz oscillator goes through an auto-calibration procedure. During this time-frame, the oscillator is directed to each of its steerable limits for about 5 seconds each with a couple of seconds of delay so the oscillator can stabilize (The whole oscillator calibration process takes about 20 seconds or so to complete). The Hertz range is stored in memory, so it doesn't need to auto-cal after subsequent reboots.

This allows the oscillator's Hertz Range and step sizes to be calculate and calibrated. Once the calibration process has been completed, the estimated D/A for a 10MHZ output is set and the oscillator is steered to this value. Thereafter, the frequency counts oscillator disciplining can begin (assuming the external reference- IRIG in this case- is present).

As for the amount of time it will take for the oscillator to settle out after power-up, the type of oscillator will have a significant factor in how long it takes to clear the alarm. The operation of the oscillator monitoring circuit for performing the frequency counts of the oscillator's output varies depending on the type of oscillator. With a TCXO oscillator, the frequency measurements and adjustments of the D/A occur every 1000 seconds (about every 18 minutes). After each frequency count, the D/A is adjusted and the frequency count is logged in the Oscillator log (Status and Logs/Oscillator log page of the web browser). In order for the Frequency alarm to clear, the Fractional Frequency Error (labeled in this log as "Freq Error") has to be better than 1x10-7. Each frequency count should decrease the Freq Error value, bringing it closer to this value. By looking at these measurements in the Oscillator log, you can determine how close it currently is and be able to obtain a pretty good idea of about how long it will take to reach this minimum criteria threshold.

Typical time after each power-up for OCXO to be within our specs: about 10 minutes total

Note: Per our test data sheet, the acceptable range on the 10 MHZ output amplitude is 2.2 to 3.6vpp.

OCXO oscillator free-run (holdover)

Email from Dave Sohn (10/3/11): The 10MHz drift is entirely based on the aging rate of 2E-10/day.

****10 MHz stability after power-up

10. A long initial GPS disciplining interval is required to accurately setup the Rubidium Oscillator disciplining.

Email from Dick Fox to a customer (6/10/12) To obtain predictable drift rates for Rubidium Oscillators you need to:

11. Keep the units powered. Temperature stability is a major factor in determining the accuracy so once powered you need to keep them powered
12. A long initial GPS disciplining interval is required to accurately setup the Rubidium Oscillator disciplining.

A. Secure Sync sets a DAC value that controls the frequency of the Rubidium Oscillator
B. SecureSync must be synchronized to GPS for a minimum 24 hours before the DAC value is set.

13. Secure Sync will not make any changes to this DAC value unless SS is synchronized to GPS for 24 hours or more.

14. This mean that short GPS syncs will NOT reset the Rubidium frequency and its drift. But short GPS syncs will correct the time offsets.

15. Based on this Spectracom can commit to a drift rate of 5 X10-12 per month provided
    A. The unit is initially synchronized to GPS for a minimum of 2 weeks
    B. The unit isn't powered off after it was synchronized.

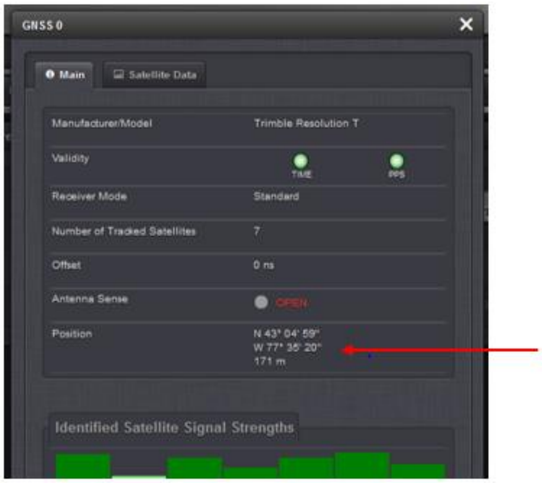
Email from Dick Fox (6/10/12) to TOYO "Our design team is telling me the rubidium needs 2 weeks of GPS disciplining to settle"

**Output GPS position information (Latitude, Longitude, altitude)

Q. Can you get GPS position information off of a SecureSync over the Ethernet port?
A. Yes! There are several ways to output position information:

1) Position is reported in the:

New web browser: Interfaces -> GNSS 0, Main tab

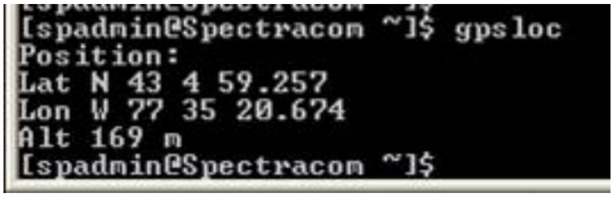


Manufacturer/Model	Trimble Resolution T	
Validity	● TIME	● PPS
Receiver Mode	Standard	
Number of Tracked Satellites	7	
Offset	0 ns	
Antenna Sense	● OPEN	
Position	N 43° 04' 59" W 77° 35' 20" 171 m	

Identified Satellite Signal Strengths

2) Via either a Telnet or SSH session

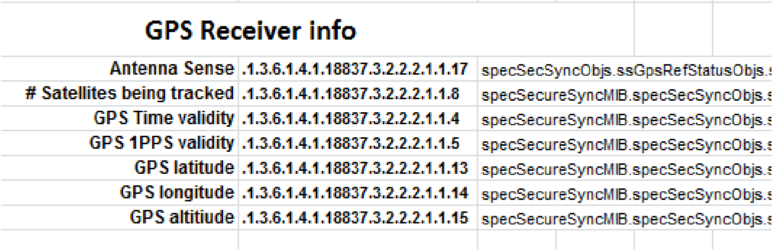
16. Position info is also available via telnet or SSH connection (over Ethernet) using the gpsloc command (as shown below):



```
[spadmin@Spectracom ~]$ gpsloc
Position:
Lat N 43 4 59.257
Lon W 77 35 20.674
Alt 169 m
[spadmin@Spectracom ~]$
```

3) Via SNMP gets (v1/v2c or v3)

- ➢ Refer also to the SNMP documentation for SecureSync: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\SNMP- Notifications-email alerts\SNMP (such as the "SNMPGets-Sets" tab of the excel spreadsheert)
- ➢ Position info is also available via SNMP (over Ethernet) using particular OID numbers, as shown below:

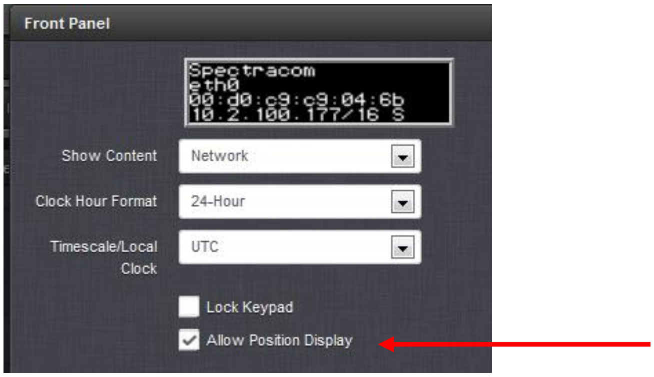


GPS Receiver info		
Antenna Sense	.1.3.6.1.4.1.18837.3.2.2.2.1.1.17	specSecSyncObjs.ssGpsRefStatusObjs.s
# Satellites being tracked	.1.3.6.1.4.1.18837.3.2.2.2.1.1.8	specSecureSyncMIB.specSecSyncObjs.s
GPS Time validity	.1.3.6.1.4.1.18837.3.2.2.2.1.1.4	specSecureSyncMIB.specSecSyncObjs.s
GPS 1PPS validity	.1.3.6.1.4.1.18837.3.2.2.2.1.1.5	specSecureSyncMIB.specSecSyncObjs.s
GPS latitude	.1.3.6.1.4.1.18837.3.2.2.2.1.1.13	specSecureSyncMIB.specSecSyncObjs.s
GPS longitude	.1.3.6.1.4.1.18837.3.2.2.2.1.1.14	specSecureSyncMIB.specSecSyncObjs.s
GPS altitiude	.1.3.6.1.4.1.18837.3.2.2.2.1.1.15	specSecureSyncMIB.specSecSyncObjs.s

4) Via the Front panel LCD

- ➢ Though it’s not “over Ethernet”, it can also be displayed on the front panel LCD (unless it’s been disabled in the web browser- for security concerns, the position display can be disabled via the web browser so that it can’t be selected to be displayed using the front panel keypad)

New web browser: **Management** -> **Front panel** page



Front Panel

```
Spectracom
eth0
00:d0:c9:c9:04:6b
10.2.100.177/16 S
```

Show Content: Network

Clock Hour Format: 24-Hour

Timescale/Local Clock: UTC

□ Lock Keypad

☑ Allow Position Display

5) Via ASCII RS-232 or RS-485 (requires a 1204-02 or 1204-04 ASCII output Option card be installed)

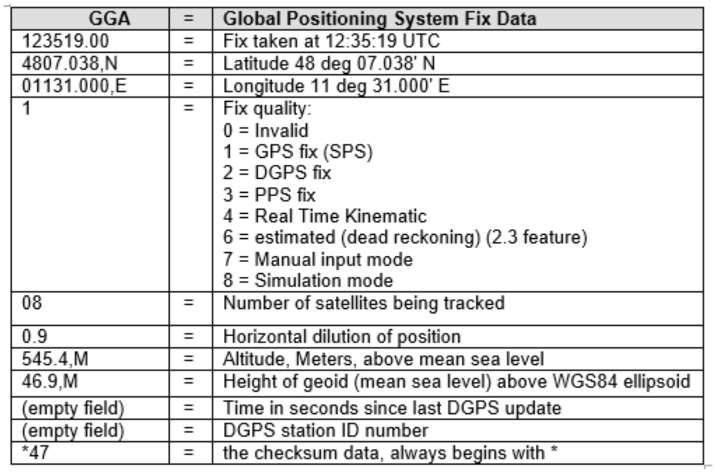
- **Model 1204-02** for RS-232 output
- **Model 1204-04** for RS-485 output

17. Though it’s not “over Ethernet”, Positon information can also be outputted via ASCII RS-485 and/or RS-232 data using NMEA data streams (GGA and RMC –NOT AVAILABLE with ZDA).

- **Note**: This method requires one or more Model 1204-02 or 1204 ASCII Option Cards be installed.

Example GGA message

$GPGGA,123519.00,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,*47



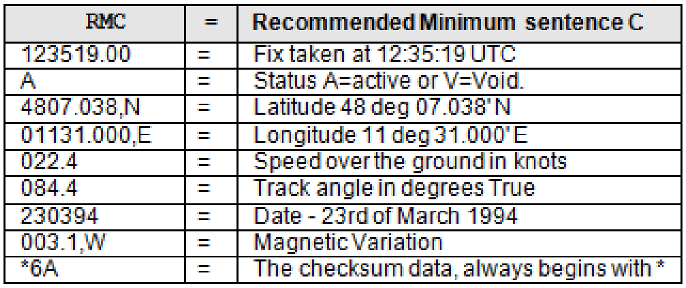
GGA	=	Global Positioning System Fix Data
123519.00	=	Fix taken at 12:35:19 UTC
4807.038,N	=	Latitude 48 deg 07.038' N
01131.000,E	=	Longitude 11 deg 31.000' E
1	=	Fix quality: 0 = Invalid 1 = GPS fix (SPS) 2 = DGPS fix 3 = PPS fix 4 = Real Time Kinematic 6 = estimated (dead reckoning) (2.3 feature) 7 = Manual input mode 8 = Simulation mode
08	=	Number of satellites being tracked
0.9	=	Horizontal dilution of position
545.4,M	=	Altitude, Meters, above mean sea level
46.9,M	=	Height of geoid (mean sea level) above WGS84 ellipsoid
(empty field)	=	Time in seconds since last DGPS update
(empty field)	=	DGPS station ID number
*47	=	the checksum data, always begins with *

“Fix Quality” value reported when SAASM reeiver is keyed vs when its unkeyed

- ➢ Refer to SF case 163026

Example RMC message:

$GPRMC,123519.00,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A



RMC	=	Recommended Minimum sentence C
123519.00	=	Fix taken at 12:35:19 UTC
A	=	Status A=active or V=Void.
4807.038,N	=	Latitude 48 deg 07.038' N
01131.000,E	=	Longitude 11 deg 31.000' E
022.4	=	Speed over the ground in knots
084.4	=	Track angle in degrees True
230394	=	Date - 23rd of March 1994
003.1,W	=	Magnetic Variation
*6A	=	The checksum data, always begins with *

GPRMC and BBB-05 data steams: speed over ground and track angle info is not outputted (in at least software versions 5.5.0 and below)

- Refer to Salesforce case 23871 for details https://na28.salesforce.com/5001A00001D7db5
- The Speed over ground and track angle fields are blank (this info is omitted from the data streams)

Email from Paul Myers (9 Dec 16) Hi Keith,
The reason why is that when the product was made with this feature it was stationary.
Since we have become mobile this is the first time someone has asked for this.
Can you make this a feature request to David Sohn.

Email Keith sent to customer (13 Dec 16) I checked with our software engineers with regards to these particular NEMA formats and their ability to provide mobile information. When they were initially incorporated into the SecureSync, they only needed to provide stationary information only (there was no Engineering requirement for them to be used in a mobile application). In order for them to be able to output speed and track data, information from each received data stream needs to be stored and processed, to output the mobile data, thereafter. This functionality has not yet been incorporated in the time servers, and is the reason the speed and track data is omitted in the data streams.

The SecureSync time servers are primarily used to provide very accurate timing. They aren’t typically used for mobile data reporting, such as speed and track info.

I am forwarding your request, to have this additional information provided in the data streams, over to our Product Manager for his consideration of having our Engineering team add this capability via a future SecureSync software update. I am flagging your record in our service database to let you know if he decides to incorporate this capability and if so, when it has been implemented!

Please let me know if you have any other questions or need anything else from us in the mean-time!!!

**Show clock page (System date/time display in the browser)

18. Provides ability to display date, time and sync status
19. Version 5.2.1: Updated Show Clock page to improve clock and system status info displays. V5.2.1 also

added a "Home" button to get back to the Home page of the browser.

**SMPTE Time code (LTC and VITC)

20. We don't support SMPTE with any of our products, as of at least July 2015.

Question from Danny Loke: … "the NTP servers will require an additional LTC or VITC input card module"

Reply from Keith (23 July 15) I don't recall ever hearing the terms of LTC or VITC, so a quick Google search to see what these terms mean in the CCTV/video realm provided me with a term I have run across a couple of times (very rarely). This word is "SMPTE". SMPTE stands for Society of Motion Picture And Television Engineers. What these two terms are referring to is also referred to as "SMPTE time code". This is a very unique time code for synchronization of a very specific application.

LTC is "Longitudal time code" and VITC is "Vertical Time Code". For more info on what these are and the differences between them, refer to http://www.filmunderground.com/34/kb/NWFS/ltc-vs.-vitc.htm.

We don't currently provide any support for SMPTE time code. It's a very seldom requested capability, so it hasn't been beneficial to us to add support to our products for it. But this is not to say we wouldn't do it for the appropriate size order that would justify all the costs associated with the development. I highly doubt we could justify it with the purchase of a SecureSync. But if there is significant potential with your customer, Josh can with our Senior Product Manager to see what it would take for us to add it, whether it's based on the quantity of units they would be ordering , or perhaps through NRE fees. But if they are looking at just one or two units for example and require this capability, unfortunately we won't likely be able to help them, (they will need to "look elsewhere" to meet their requirements).

If you feel there is significant potential with this customer, if the SecureSync was able to provide SMPTE time code, work with Josh for more details on what would be required for us to consider it!!

Logs/Syslog

- Refer to: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Alarms and logs
- And in the SecureSync online manual: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/OPRTN/Logs_Remote%20Servers.htm?Highlight=syslog
- Supports Syslog capability (sending logs to a remote Syslog server on the network).
- All SecureSync Logs are stored in the home/spectracom/log directory.

A) Syslog (Remote logs/remote logging)

- Example freeware Syslog server software:
  - "**Event Log Analyzer**" https://www.manageengine.com/products/eventlog/download-free.html
  - "**Syslog server 1.2.3**" (http://www.softpedia.com/get/System/System-Miscellaneous/Syslog-Server.shtml)

Free Syslog software for Windows:

More recently (Jan 2018) I downloaded/installed "Event Log Analyzer")

- **I downloaded/installed "Syslog Server 1.2.3" .**
  - Refer to I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Syslog

rsyslog (or syslog-ng)

- These are alternate syslog packages, we are not using either of these, in at least vesions 1.2.1 and below
- ~~we may need to switch to one of these for enhanced capabilities~~
  - ~~Refer [JIRA] (SSS-478) Raytheon is requesting syslog messages (log entries) to have milliseconds precision (per Salesforce case 162730)~~

Though its not mentioned in the v1.4.1 and below Release Note,. I believe we may now be using rsyslog (instead of syslog) in more recent 2400 SecureShnc versions. Not sure at which version this change was made, but believe it was either at, or sometime before at least, version 1.4.1.

Syslog Protocol

~~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~~

- ~~Cisco site with great info on the Syslog Protocol: http://www.ciscopress.com/articles/article.asp?p=426638~~
- ~~contains info on Facility and Severity codes, Timestamp and message formats, etc~~

Syslog header (RFC 5424) vs syslog-ng header (RFC 5424)

Refer to: https://success.alienvault.com/s/article/difference-between-Syslog-and-Syslog-NG

1. Example Syslog packet

Oct 11 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8

Example syslog-ng packet:

1 2003-10-11T22:14:15.003Z mymachine.example.com evntslog - ID47 [exampleSDID@32473 iut="3" eventSource= "Application" eventID="1011"] BOMAn application event log entry

Time/date/year info in syslog messages

Note: We use syslog format (not syslog-ng/rsyslog which uses a different header than syslog)

- UTC time only (never local)
- No year info

Example Syslog packet

Oct 11 22:14:15 *mymachine su: 'su root' failed for lonvick on*

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:
  - "**Local Logging**": You can individually configure which log files get saved in the box (**Management** -> **Logs** page, in each log tab).
  - "**Remote Logging**": You can individually configure which log files get sent to Syslog (**Management** -> **Logs** page, in each log tab)

SecureSync sends Syslog messages as UDP on port 514

UDP/Port Number

- Uses UDP port 514

Q Can syslog send logs via TCP instead of UDP

A Syslog sends logs via UDP port 514. Syslog in the SecureSync isn't able to send logs via TCP.
FYI Syslog in the SecureSync follows RFCs 3164 and 5424. The following statement is from RFC 3164 (https://www.ietf.org/rfc/rfc3164.txt)

Syslog uses the user datagram protocol (UDP) as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514."

"In the event that a syslog server does not support listening on the standard syslog port, you may redirect the syslog port to the desired port by utilizing built-in port forwarding capability in network switches (search online for port forwarding or port mapping)."

Identifying in a syslog server which SecureSync sent a log entry

- Each log entries contain the DNS Hostname of the SecureSync.

Note (Oct 31, 2012): versions 4.8.7 and below were found to be sending a hard-coded "Spectracom" as the Hostname, even if the hostname is no longer this default value. So even if the hostname has been changed, the hostname will still be reported as "Spectracom". This is supposed to be fixed in the next software release.

  - **Email from Dave Sohn (11/1/12)** How the syslog server application resolves the messages it receives to inform the user of the host's information is separate. The program I used is trying to resolve the IP address of the unit it received the message from based on several factors. If it fails to resolve to something better, it simply reports the IP address. Their syslog server may do it differently, or they want it in the message itself.

Configuration of syslog

IPv6 for Syslog

- Refer to Mantis case 1897

Mantis cases 1849/1897: Syslog not working with IPv6 addresses.
Status update per Dave Sohn (8 Mar 2013): "Our current syslog package does not support IPv6. Either a new package/version or patch are required. (This is recorded in Mantis case 1897)

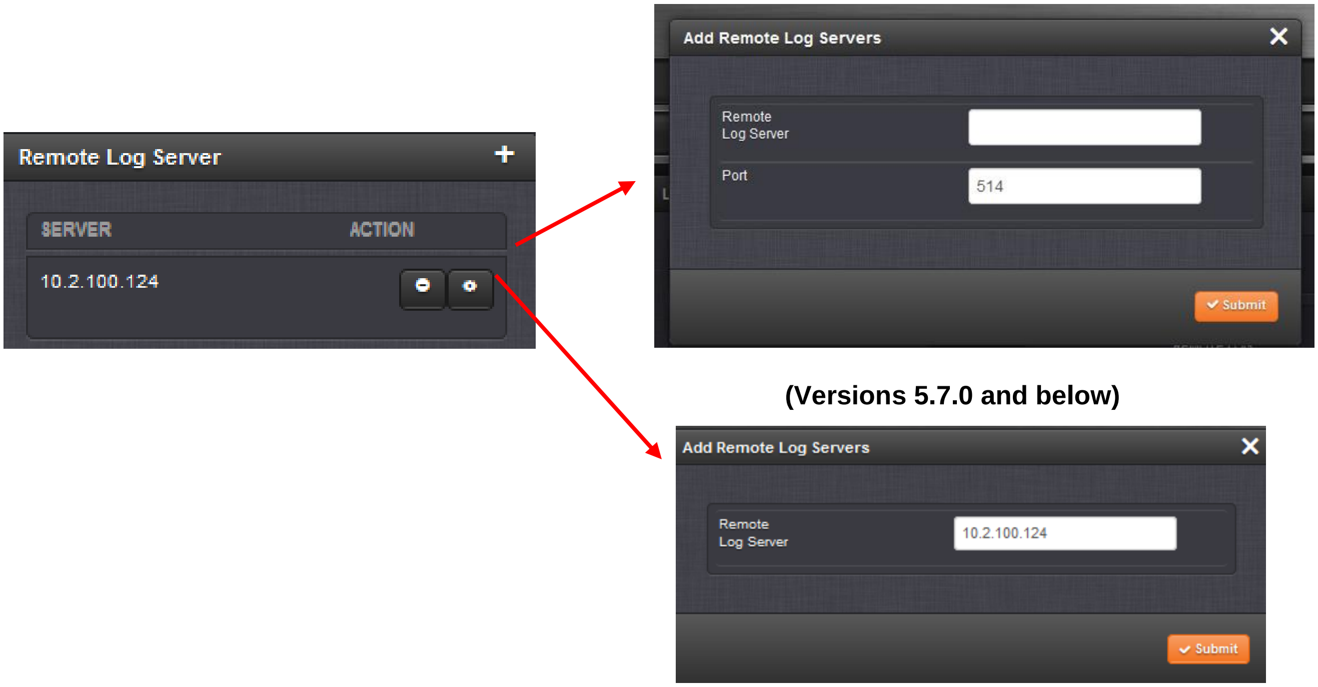
- Refer to syslog tech notes for SecureSync and 9400s
  - **SecureSync** : I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Syslog
  - **9400 series:** I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\Syslog

A) web browser:

- Configured in each log of the ***Management*** -> ***Log Configuration*** page of the browser

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)



Remote Log Server

SERVER: 10.2.100.124

Add Remote Log Servers

Remote Log Server:

Port: 514

(Versions 5.7.0 and below)

Add Remote Log Servers

Remote Log Server: 10.2.100.124

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

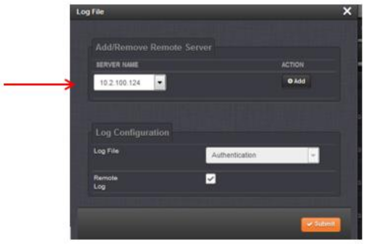
NOTE: due to ability to individually configure each log type to be able to be sent to different log servers, the user MUST individually "add" the syslog server for each log type.

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)



Log File

Add/Remove Remote Server

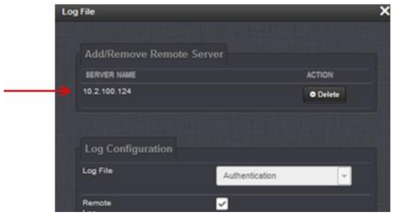
SERVER NAME: 10.2.100.124

Log Configuration

Log File: Authentication

Remote Log: ☑

B)   After pressing "add"



Log File

Add/Remove Remote Server

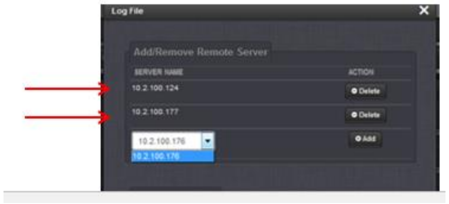
SERVER NAME	ACTION
10.2.100.124	Delete

Log Configuration

Log File: Authentication

Remote ☑

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)**



Log File

Add/Remove Remote Server

SERVER NAME	ACTION
10.2.100.124	Delete
10.2.100.177	Delete
10.2.100.176	Add

Syslog server(s) are configured for each log in the browser

2400 Local logs

Q per Hughes 2400 demo) Enable/Disable “Authentication” logging option is missing in Log Configuration screen, it is available in older units.

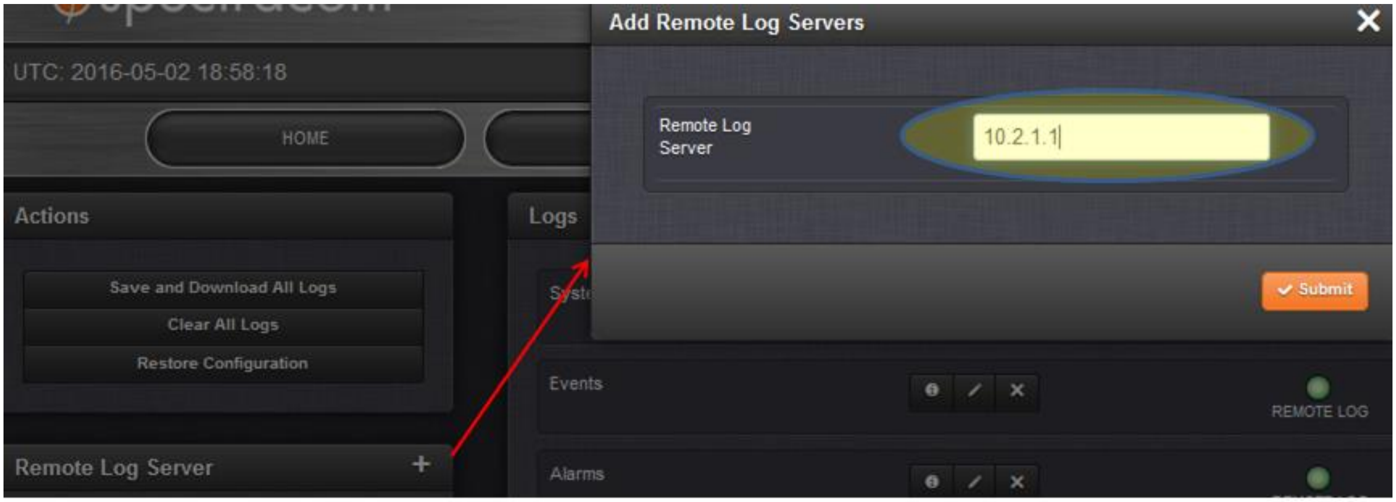
A (per Dave Sohn ~May 2021) The log configuration changed between 1200 and 2400. The local logging configuration now only includes Orolia custom logs, not the standard Linux logs, which are always enabled.
This is different than the 1200 but is it acceptable to Hughes?

Email from Keith on how to configure syslog

All of the logs that can be viewed in the web browser can also be sent to a syslog server. Below is info on how to configure the logs to be sent to a syslog server.

First, add the desired syslog server(s) to the list of available syslog servers that each log type can be individually configured to be sent to (overall, multiple syslog servers can be listed, with each log file type being able to be sent to any one of the servers in this list).

On the left side of the **Management** -> **Log Configuration** page of the browser, press the “**+**” sign to the right of “**Remote log Server**”. In the pop-up window, enter the IP address of the syslog server and Submit. Repeat as desired to enter additional



Remote Log Server: 10.2.1.1

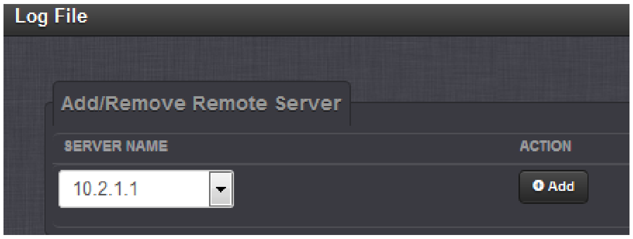
Because the log files can be individually configured as to which remote server it's entries are sent to, each log file type (such as the System Log for example) has to be individually configured to be sent to the desired remote server, before its logs will be sent to any remote server. You need to add (select) a Remote server from the list of previously added to "Remote Log servers" (on the left side of Log Configuration page).

To configure a remote sever to each log type (this can't be done as a single global setting for all of the log files), after adding one or more remote server addresses to the list (on the left side of the page) press the same middle icon (**Management** -> **Log configuration** page of the browser) for each log type you wish to send to a remote server, you need to add (select) one or more Remote servers, as previously added to the list of "Remote Log servers" on the left side of this page.

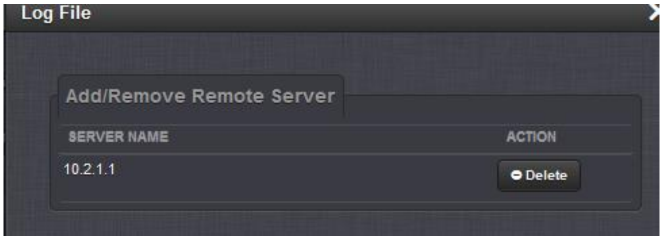
Each log of the SecureSync has its own remote logging enable checkbox that also needs to be selected, if you desire for that file's log entries to be sent to a specified syslog server.

The remote logging enable for each log file/type (such as the "Qualification" log for instance) is in the **Management** -> **Log configuration** page of the browser. For each log file you wish for its logs to be sent to remote servers, click the middle of the three ICONS (the pencil ICON) for that log file. In the **server name**" drop-down of the pop-up window, select the particular syslog server you wish to send this log file to and then press the Add button.

The "Add" button and the "Server name" drop-down field will vanish after pressing the Add button

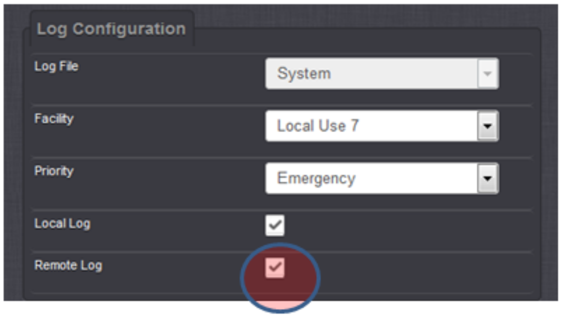


SERVER NAME	ACTION
10.2.1.1	Add



SERVER NAME	ACTION
10.2.1.1	Delete

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.



Log Configuration

Log File: System

Facility: Local Use 7

Priority: Emergency

Local Log ☑

Remote Log ☑

“**Local log**: When selected, causes log entries for this log file to be stored inside the time server. If its unselected, logs for this file will not be stored within the time server

Important Note: Please be aware that the specific combination of the **Facility** and **Severity** codes for each log file (as also configured in the same pop-up window mentioned above) define where the Log entries are actually sent to in the SecureSync/syslog server. Changing any of these two values will result in the particular log entries that are supposed to be sent to one Log file actually being sent to another Log file. So log files can become inter-mixed inside the SecureSync, making it nearly impossible to review them in the browser, the CLI or if the logs are downloaded from the unit. For this reason, we do not recommend any of the facility and Severity codes be changed from the default settings.

Troubleshooting suggestions:

- Make sure each individual log file has been configured with a syslog server address (***Management*** -> L***og Configuration*** page of the black/charcoal browser)
- Login to the CLI interface (telnet or ssh connection) and verify if you can ping the Syslog server.
    - Check the main default port/gateway in the configured correctly (***Management*** -> ***General Setup*** page of the black/charcoal browser)
    - Perform a wireshark or tcpdump capture on the SecureSync’s switch to see if syslog packets are being sent.
    - Verify the syslog server is listening on syslog port 514 and there are no firewalls in between that may be blocking this port.

Storage of Syslog configs/remote server IPv4 addresses : desire to script the adding of remote servers.

(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: Interval Server Error”
- If updated to version 5.3.1, previously entered syslog server addresses are carried forward and not an issue. This issue just affects new units shipped at 5.3.1 or units that happened to be cleaned with v5.3.1 installed.
- Planned to be addressed in v5.4.0 update, ~end of Jan 2016.

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."

Verification that Syslog is working / Troubleshooting Syslog not working

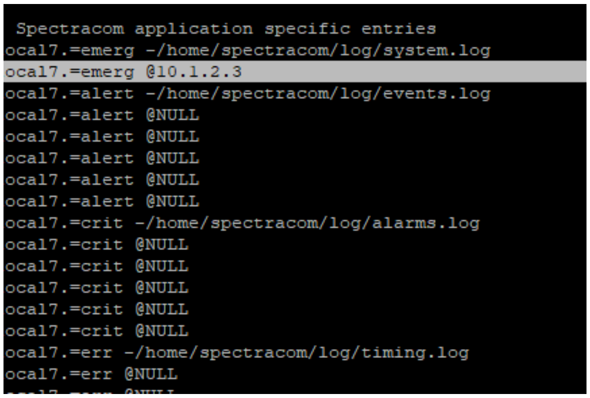
- Verify port
- Use Syslog software to verify log entries are being received.
  - Use tcpdump in the SecureSync to verify “syslog” packets are being sent
  - Use Wireshark to capture “syslog” packets are present.
  - Review the ***/etc/syslog.conf*** file (using cli interface or via config bundle)

example cat of the etc/syslog.conf below is from version 5.7B software

Note: In this example below, the System log is the only Log ile thus far to have a Syslog server added to it, from the list of available Syslog servers (as shown with the entry of “@10.1.2.3”

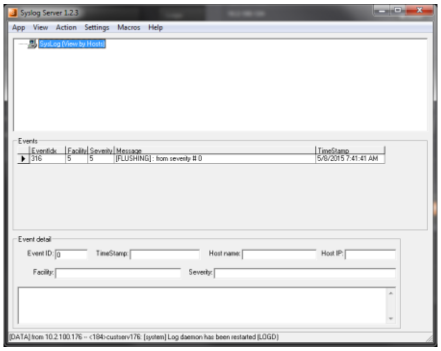
```
spadmin@Spectracom /etc $ cat syslog.conf
auth,authpriv.* -/home/spectracom/log/auth.log
*.*;local1,local2,local3,local4,local5,local6,local7,auth,authpriv,daemon,kern,mail,user,cron.none -/home/spectracom/log/sys.log
daemon.notice -/home/spectracom/log/daemon.log
kern.* -/home/spectracom/log/kern.log
mail.* -/home/spectracom/log/mail.log
user.* -/home/spectracom/log/user.log
cron.* -/home/spectracom/log/cron.log
local6.* -/home/spectracom/log/ntp.log

# Spectracom application specific entries
local7.=emerg -/home/spectracom/log/system.log
local7.=emerg @10.1.2.3
local7.=alert -/home/spectracom/log/events.log
local7.=alert @NULL
local7.=alert @NULL
local7.=alert @NULL
local7.=alert @NULL
local7.=alert @NULL
local7.=crit -/home/spectracom/log/alarms.log
local7.=crit @NULL
local7.=crit @NULL
local7.=crit @NULL
local7.=crit @NULL
local7.=crit @NULL
```

```
local7.=err -/home/spectracom/log/timing.log
local7.=err @NULL
local7.=err @NULL
local7.=err @NULL
local7.=err @NULL
local7.=err @NULL
local7.=warn -/home/spectracom/log/qual.log
local7.=warn @NULL
local7.=warn @NULL
local7.=warn @NULL
local7.=warn @NULL
local7.=warn @NULL
local7.=debug -/home/spectracom/log/osc.log
local7.=debug @NULL
local7.=debug @NULL
local7.=debug @NULL
local7.=debug @NULL
local7.=debug @NULL
local7.=notice -/home/spectracom/log/journal.log
local7.=notice @NULL
local7.=notice @NULL
local7.=notice @NULL
local7.=notice @NULL
local7.=notice @NULL
local7.=info -/home/spectracom/log/update.log
local7.=info @NULL
local7.=info @NULL
local7.=info @NULL
local7.=info @NULL
local7.=info @NULL
```



```
 Spectracom application specific entries
ocal7.=emerg -/home/spectracom/log/system.log
ocal7.=emerg @10.1.2.3
ocal7.=alert -/home/spectracom/log/events.log
ocal7.=alert @NULL
ocal7.=alert @NULL
ocal7.=alert @NULL
ocal7.=alert @NULL
ocal7.=alert @NULL
ocal7.=crit -/home/spectracom/log/alarms.log
ocal7.=crit @NULL
ocal7.=crit @NULL
ocal7.=crit @NULL
ocal7.=crit @NULL
ocal7.=crit @NULL
ocal7.=err -/home/spectracom/log/timing.log
ocal7.=err @NULL
```

Free Syslog software for Windows: I downloaded/installed “Syslog Server 1.2.3” . Refer to I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Syslog



EventIdx	Facility	Severity	Message	TimeStamp
316	5	5	[FLUSHING] : from severity # 0	5/8/2015 7:41:41 AM

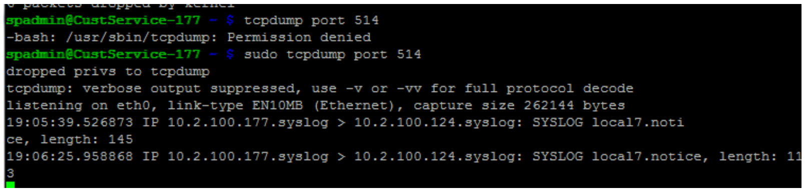
Event ID: 0 TimeStamp: Host name: Host IP:

Facility: Severity:

[DATA] from 10.2.100.176 -- <184>custserv176: [system] Log daemon has been restarted (LOGD)

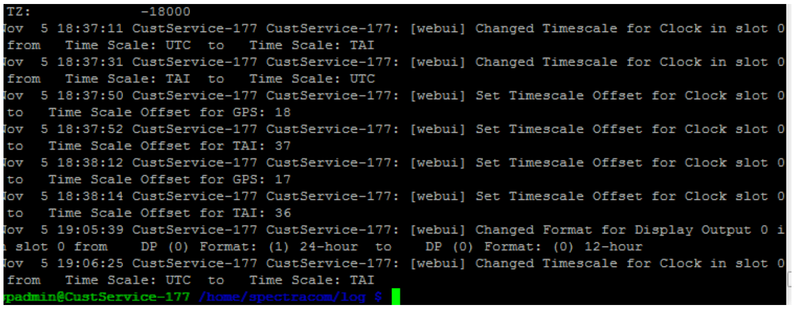
TCPdump capture of syslog messages being sent

Note: the screenshot below shows tcpdump listening on port 514 of all Ethernet interfaces (filtering for port 514 will only capture syslog messages being sent). This screenshot from v5.3.0 software shows the two separate journal log entries I caused to be sent by changing web browser configs.



```
0 packets dropped by kernel
spadmin@CustService-177 ~ $ tcpdump port 514
-bash: /usr/sbin/tcpdump: Permission denied
spadmin@CustService-177 ~ $ sudo tcpdump port 514
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
19:05:39.526873 IP 10.2.100.177.syslog > 10.2.100.124.syslog: SYSLOG local7.noti
ce, length: 145
19:06:25.958868 IP 10.2.100.177.syslog > 10.2.100.124.syslog: SYSLOG local7.notice, length: 11
3
```

Associated Journal log entries that were asserted during this test.

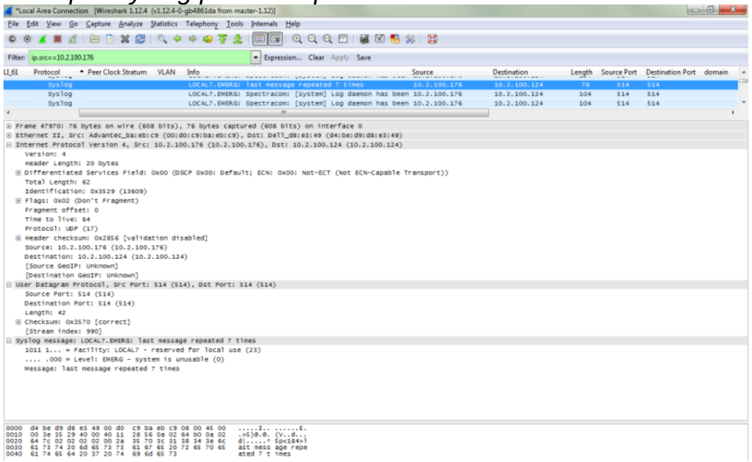


```
TZ:              -18000
Nov  5 18:37:11 CustService-177 CustService-177: [webui] Changed Timescale for Clock in slot 0
 from   Time Scale: UTC  to   Time Scale: TAI
Nov  5 18:37:31 CustService-177 CustService-177: [webui] Changed Timescale for Clock in slot 0
 from   Time Scale: TAI  to   Time Scale: UTC
Nov  5 18:37:50 CustService-177 CustService-177: [webui] Set Timescale Offset for Clock slot 0
 to   Time Scale Offset for GPS: 18
Nov  5 18:37:52 CustService-177 CustService-177: [webui] Set Timescale Offset for Clock slot 0
 to   Time Scale Offset for TAI: 37
Nov  5 18:38:12 CustService-177 CustService-177: [webui] Set Timescale Offset for Clock slot 0
 to   Time Scale Offset for GPS: 17
Nov  5 18:38:14 CustService-177 CustService-177: [webui] Set Timescale Offset for Clock slot 0
 to   Time Scale Offset for TAI: 36
Nov  5 19:05:39 CustService-177 CustService-177: [webui] Changed Format for Display Output 0 i
n slot 0 from    DP (0) Format: (1) 24-hour  to    DP (0) Format: (0) 12-hour
Nov  5 19:06:25 CustService-177 CustService-177: [webui] Changed Timescale for Clock in slot 0
 from   Time Scale: UTC  to   Time Scale: TAI
spadmin@CustService-177 /home/spectracom/log $
```

Wireshark capture of syslog entries

Example filter can use: ip.src==10.2.100.176 and udp.port==514

Example Syslog packet capture

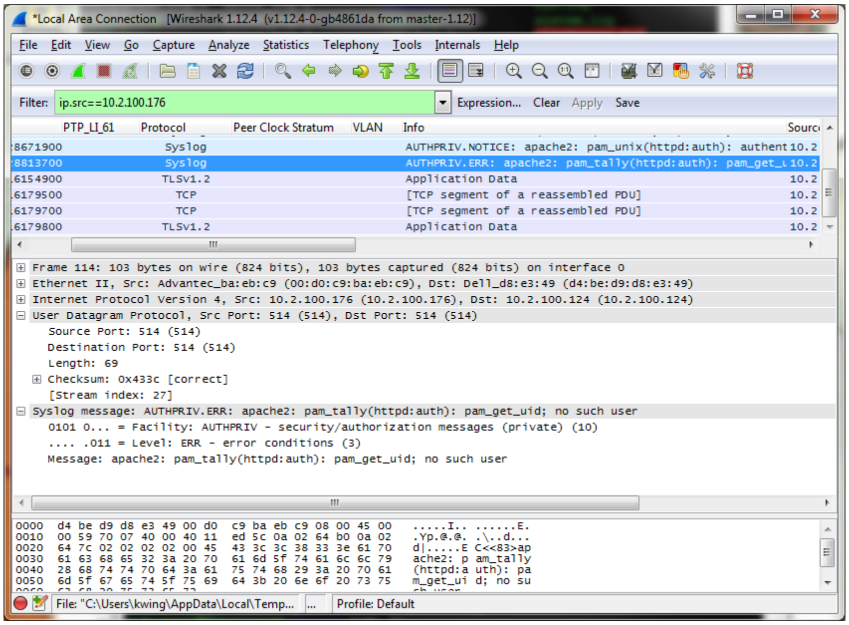

*Local Area Connection [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: ip.src==10.2.100.176

```
LI_61  Protocol  Peer Clock Stratum  VLAN  Info                                                Source         Destination    Length  Source Port  Destination Port  domain
       Syslog                              LOCAL7.EMERG: last message repeated 7 times          10.2.100.176   10.2.100.124   76      514          514
       Syslog                              LOCAL7.EMERG: Spectracom: [system] Log daemon has been 10.2.100.176 10.2.100.124   104     514          514
       Syslog                              LOCAL7.EMERG: Spectracom: [system] Log daemon has been 10.2.100.176 10.2.100.124   104     514          514
```

```
⊞ Frame 47970: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
⊞ Ethernet II, Src: Advantec_ba:eb:c9 (00:d0:c9:ba:eb:c9), Dst: Dell_d8:e3:49 (d4:be:d9:d8:e3:49)
⊟ 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: 0x3529 (13609)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
  ⊞ Header checksum: 0x2856 [validation disabled]
    Source: 10.2.100.176 (10.2.100.176)
    Destination: 10.2.100.124 (10.2.100.124)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ User Datagram Protocol, Src Port: 514 (514), Dst Port: 514 (514)
    Source Port: 514 (514)
    Destination Port: 514 (514)
    Length: 42
  ⊞ Checksum: 0x3570 [correct]
    [Stream index: 990]
⊟ Syslog message: LOCAL7.EMERG: last message repeated 7 times
    1011 1... = Facility: LOCAL7 - reserved for local use (23)
    .... .000 = Level: EMERG - system is unusable (0)
    Message: last message repeated 7 times

0000  d4 be d9 d8 e3 49 00 d0  c9 ba eb c9 08 00 45 00   .....I.. ......E.
0010  00 3e 35 29 40 00 40 11  28 56 0a 02 64 b0 0a 02   .>5)@.@. (V..d...
0020  64 7c 02 02 02 02 00 2a  35 70 3c 31 38 34 3e 6c   d|.....* 5p<184>l
0030  61 73 74 20 6d 65 73 73  61 67 65 20 72 65 70 65   ast mess age repe
0040  61 74 65 64 20 37 20 74  69 6d 65 73               ated 7 t imes
```

Example capture of an Auth log entry being sent to syslog due to trying to login with invalid credentials


*Local Area Connection [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ip.src==10.2.100.176
Expression... Clear Apply Save
File: "C:\Users\kwing\AppData\Local\Temp... ... Profile: Default

```
PTP_LI_61   Protocol   Peer Clock Stratum   VLAN   Info                                                  Sourc
:8671900    Syslog                                 AUTHPRIV.NOTICE: apache2: pam_unix(httpd:auth): authent 10.2
:8813700    Syslog                                 AUTHPRIV.ERR: apache2: pam_tally(httpd:auth): pam_get_  10.2
.6154900    TLSv1.2                                Application Data                                        10.2
.6179500    TCP                                    [TCP segment of a reassembled PDU]                      10.2
.6179700    TCP                                    [TCP segment of a reassembled PDU]                      10.2
.6179800    TLSv1.2                                Application Data                                        10.2
```

```
⊞ Frame 114: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface 0
⊞ Ethernet II, Src: Advantec_ba:eb:c9 (00:d0:c9:ba:eb:c9), Dst: Dell_d8:e3:49 (d4:be:d9:d8:e3:49)
⊞ Internet Protocol Version 4, Src: 10.2.100.176 (10.2.100.176), Dst: 10.2.100.124 (10.2.100.124)
⊟ User Datagram Protocol, Src Port: 514 (514), Dst Port: 514 (514)
    Source Port: 514 (514)
    Destination Port: 514 (514)
    Length: 69
  ⊞ Checksum: 0x433c [correct]
    [Stream index: 27]
⊟ Syslog message: AUTHPRIV.ERR: apache2: pam_tally(httpd:auth): pam_get_uid; no such user
    0101 0... = Facility: AUTHPRIV - security/authorization messages (private) (10)
    .... .011 = Level: ERR - error conditions (3)
    Message: apache2: pam_tally(httpd:auth): pam_get_uid; no such user
```

```
0000  d4 be d9 d8 e3 49 00 d0  c9 ba eb c9 08 00 45 00   .....I.. ......E.
0010  00 59 70 07 40 00 40 11  ed 5c 0a 02 64 b0 0a 02   .Yp.@.@. .\..d...
0020  64 7c 02 02 02 02 00 45  43 3c 3c 38 33 3e 61 70   d|.....E C<<83>ap
0030  61 63 68 65 32 3a 20 70  61 6d 5f 74 61 6c 6c 79   ache2: p am_tally
0040  28 68 74 74 70 64 3a 61  75 74 68 29 3a 20 70 61   (httpd:a uth): pa
0050  6d 5f 67 65 74 5f 75 69  64 3b 20 6e 6f 20 73 75   m_get_ui d; no su
```

Syslog log in the unit (sys.log)

- ➢ There is no syslog log available in the web browser.
  - o Sys.log can only be viewed via the CLI. It's in the **home/spectracom/logs** directory
- ➢ Contains entries for syslog stopping and starting

A) Logs not present in the syslog server

- o Verify the syslog configs are correct (**Management** -> **Log Configuration** page of the newer browser)
- o Check main default port/gateway is correct (**Management** -> **General Setup** page of the newer browser
- o Login to cli interface and try pinging out to the syslog server (could be a network issue)

Logs

FAQS about SecureSync Logs

Q. If I delete all the log files, does the SecureSync **automatically** generate new ones from scratch?
A. Keith's response: Absolutely. New log files will automatically start to be created, after they have been deleted.

Q. How often does the system update the log entries of the file when an "event" happens?
A. Log entries are asserted into the logs each time an event occurs and each time the event clears. No log entries are added in between the event occurring and the events clearing.

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 Seach 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. Instread, 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 ull 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.

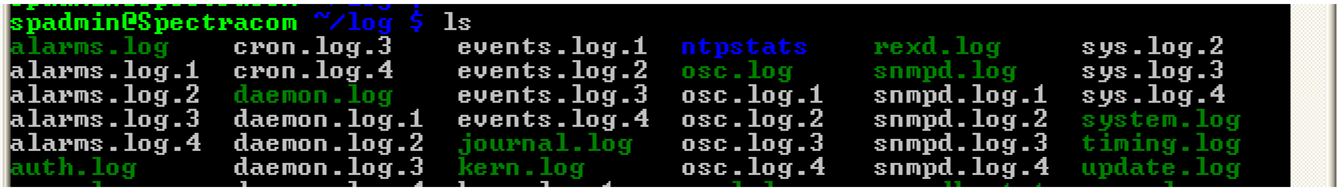
Q. Also in the logs section can you define that the log stamp use a local time stamp as opposed to just taking the time based on the UTC time input to the SecureSync?

A. (based on an email from Dave Sohn 8/24/12) The logs are always in the UTC time scale. There is no way to configure the time stamps to be in Local time scale.   We use syslog for our logging mechanism. The timestamps are provided by it and use the kernel time, which is in UTC time scale.

**Ability to view the logs (log entries) with CLI interface

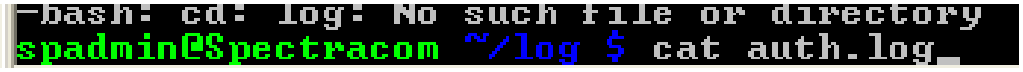
1. Login with either telnet or ssh.
2. Type **cd log** <enter> to change to the log directory

3. Type **ls** <enter> to list all logs.



```
spadmin@Spectracom ~/log $ ls
alarms.log      cron.log.3     events.log.1   ntpstats      rexd.log      sys.log.2
alarms.log.1    cron.log.4     events.log.2   osc.log       snmpd.log     sys.log.3
alarms.log.2    daemon.log     events.log.3   osc.log.1     snmpd.log.1   sys.log.4
alarms.log.3    daemon.log.1   events.log.4   osc.log.2     snmpd.log.2   system.log
alarms.log.4    daemon.log.2   journal.log    osc.log.3     snmpd.log.3   timing.log
auth.log        daemon.log.3   kern.log       osc.log.4     snmpd.log.4   update.log
```

4. To view the log entries, type **cat** <enter> followed by the name of the log (Example: type **cat auth.log** <enter>) to view the Authentication log entries.



```
-bash: cd: log: No such file or directory
spadmin@Spectracom ~/log $ cat auth.log_
```

**Ability to delete the logs

A) Ability to delete the logs via CLI

Note: The **clearlogs** command only clears the logs that are displayed in the browser (such as Qual, NTP, etc). This function does not clear the "system" logs in the background only (such as sys.log, daemon.log, kern.log, mail.log, rexd.log, cron.log, mysql_create.log and system.log)

- Can't delete the NTP logs via CLI before version 5.1.5???
- I believe version 5.1.5 introduced the **clearlogs** CLI command to clear logs.

B) Ability to delete the logs via the newer web browser

- Two different locations to delete the logs:

5. Delete just the logs that are displayed in the web browser (Alarms, Events, NTP, etc) (not the logs in the background, such as kern.log, sys.log, etc)

Management -> **Log Configuration page,** click the "**Clear All Logs**" button in the upper-left corner).

6. Delete all of the logs (the ones in the background and the ones in the browser)

Via the bottom-left corner of the **Tools** -> **Upgrade**/**Backup** page (click the "**Clear All Logs**" button).

Note: The **clearlogs** command only clears the logs that are displayed in the browser (such as Qual, NTP, etc). This function does not clear the "system" logs in the background only (such as sys.log, daemon.log, kern.log, mail.log, rexd.log, cron.log, mysql_create.log and system.log)??

Update to Note above: Update versions 5.4.5 and above now deletes the Auth and NTP logs.

Software issue associated with deleting logs and NTP stats via the browser

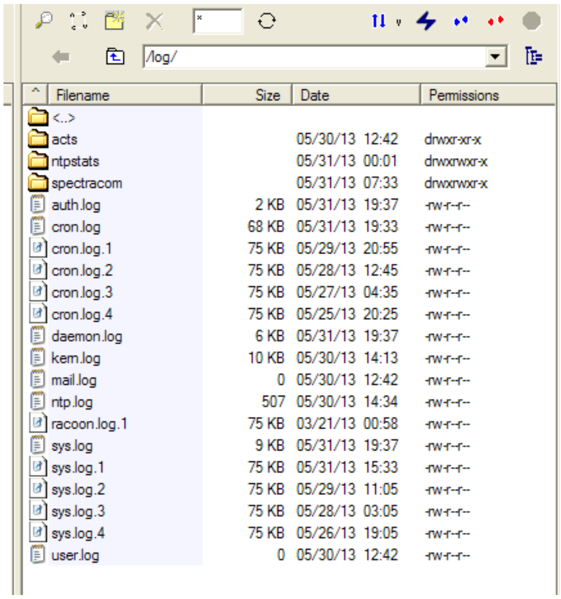
- With at least software version 5.2.1, the "Clear All logs" button.
- Note the associated CLI command work fine in both Models.
- Refer to Mantis case 3049. http://cvsmantis.int.orolia.com/mantis/view.php?id=3049
- Fixed in version 5.3.0 (Sept 2015)

Log file sizes/Log rotation

- ➢ View all of the logs via telnet/ssh
  1. Log in with telnet/ssh
  2. Issue an **ls –al /home/spectracom/log** command to view log sizes. (Note: This command doesn't report log sizes).
  3. Go to the **log** directory.

Current size of all log files can be viewed

1. Log in with FTP/SCP
2. Issue a **ls –al /home/spectracom/log** command to view log sizes. (Note: This command also works with telnet to list the logs. But it doesn't report log sizes).
3. go to the **log** directory.



/log/

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--
kem.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--

SNMP and NTP log rotate issues

1) SNMP log became too large / "error on subcontainer 'ia_addr' insert (-1")" entries

- ➢ Refer to Mantis case 1871 and 2343.
- ➢ Per 1871 - SNMP log is apparently not rotated, but instead deleted upon boot-up??
- ➢ Per 2343

Note: This was observed a couple of different times, with a weird entry of **"error on subcontainer 'ia_addr' insert (-1")** being asserted and filling up the SNMP logs.

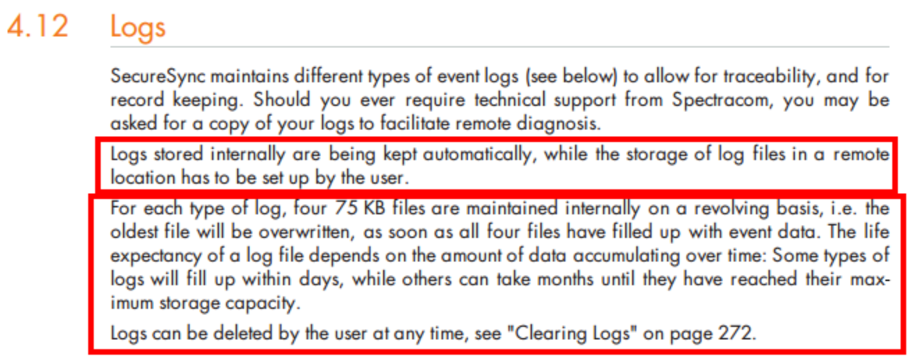
Email from Paul Myers about "subontainer entries" I found 3 possible reasons for this:

1) Snmpd.conf file which should be in /home/Spectracom/config/snmpd.conf was NOT present or found in any search path supported by snmpd.
2) Snmpd.conf is invalid and needs to be regenerated.

Httpd service loads processor and snmpd complains. (longshot)
Please see if /home/Spectracom/config has an snmpd.conf file.
Have them send that to you.
Can they reconfigure snmpd AFTER getting us the configuration file and stop/start SNMPD?
Also are they on a heavily loaded network?
Do they have multiple Ethernet ports?
Did they change IP addresses after setting up SNMPD?
Maybe we should have them setup networking THEN setup SNMP and shutdown/restart either the SecureSync OR shutdown and restart SNMP service.
Maybe it’s a snmpd config file thing or an IP address issue with the daemon having trouble with ip addresses changing?

FAQs regarding log rotations

Some info from the SecureSync’s manual regarding log rotation and deletion



4.12 Logs

SecureSync maintains different types of event logs (see below) to allow for traceability, and for record keeping. Should you ever require technical support from Spectracom, you may be asked for a copy of your logs to facilitate remote diagnosis.

Logs stored internally are being kept automatically, while the storage of log files in a remote location has to be set up by the user.

For each type of log, four 75 KB files are maintained internally on a revolving basis, i.e. the oldest file will be overwritten, as soon as all four files have filled up with event data. The life expectancy of a log file depends on the amount of data accumulating over time: Some types of logs will fill up within days, while others can take months until they have reached their maximum storage capacity.

Logs can be deleted by the user at any time, see "Clearing Logs" on page 272.

Logs/entries associated with log rotation occurring

chron.log

```
fcron[4054]: Job /usr/sbin/logrotate /etc/logrotate.conf complete
```

Other FAQs about log rotation/log rollovers

Logrotate.conf configuration file

Q Configurable, or are we restricted to what is in /etc/logrotate.conf? /etc/logrotate.d appears to be locked down)
A Keith’s response (based on input fro,m Paul M, 11 Apr 17) : No, this configuration is restricted and fixed to ensure drive space preservation.

Q What is the limited size of the log files?
A. Keith’s response: There is no set “size limit” to the log files. The log files are automatically checked every 10 minutes to see if they are at least 75kb in size. If they are, the log entries start to be rotated. If there are many log entries being made to any particular log file, they could be significantly larger than 75kb within the 10 minute interval between the log size checks. If they are any value about 75kb when checked, a new “log file” is created. Typically, the logs are between 75kb and 77kb, when they are checked at a 10 minute interval.

Q When the log files reach its limit, How is the new file created? I saw there are multiple files with .1, .2, .3,…etc, e.g.

alarm.log, alarm.log.1, alarm.log.2, alarm.log.3. It seems that the file with the bigger number is the oldest file and the .1 file is the next most recent file and the .log file (with no number) is always the current file. Is that the way the SecureSync write log files?

A Keith's response: Yes! If a log is found to be over 75 kb when its checked at the scheduled 10 minute interval, the earlier log entries start to first rotate into a .1 log. Then, when the .1 log is found to be exceeding 75 kb, the oldest logs start to be rotated into the .2 log. This continues to occur until the .4 log is found to exceed 75 kb, at which time, the .4 file is deleted (leaving the log with no number – which has the most recent entries -as well as the .1, .2 .3 logs).

When viewing the logs in the web browser, all of the same log files (the ones with no number, as well as .1, .2, .3 and .4 –if they exist- will all be displayed together as one continuous log).

Q. On the GUI, after how many logs or after what time-period are the logs cleared?

A. **Reply from Keith** Each type of log (such as Event, Alarms, etc) are stored in separate "bundles". When a log is initially detected to be 75kb or larger, those log entries are rotated as a bundle with the name of the log incremented to 1. Then, when that type of log hits 75kb again, it rotates again, the name of the "original" logs that had rotated to "1" increments to "2". When the number is 4 and the logs rotate again, that particular bundle of logs is deleted.

The web browser displays all of the entries from all bundles of that log type that have not been deleted yet. So how many logs that can be retained and for how long they can be retained is completely dependent upon how many log entries of that log type are being asserted. The more log entries of particular log type that are being asserted, the sooner those bundles will reach "75kb" and the sooner they will be rotated out.

If it's desired to periodically archive logs to prevent them from being deleted/lost, there is a way for a user to generate a single file which contains all of the log bundles. Then, it can be pulled from the NTP server using FTP. Below is information about generating and exporting this log file.

Instead of copy/pasting all of the logs to a Word document, you can also bundle the logs into a single log file. Then export this bundle file from the SecureSync using an FTP or SCP session.

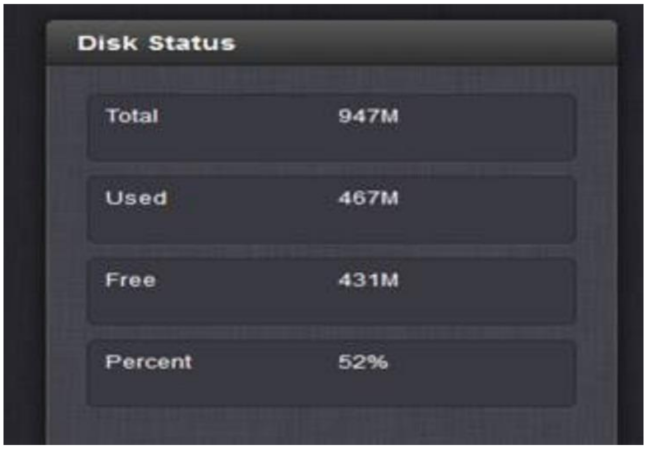
The log bundling is controlled in the "**Tools"/ "Upgrade/Backup"** page of the SecureSync's web browser. Click on the "Configuration" tab. Then, to bundle the logs, change "Save Log Files" to "Enabled" and then hit Submit. This generates a single file bundle of the logs. This file ("SecureSync.log") is placed in the "**home/spectracom/xfer/log/**" directory. Once it has been created, you can FTP/SCP it off the box (just make sure "FTP Service" is enabled in the Network/General page of the browser, "Services" tab).

If you need a free FTP client, we often use CoreFTP (http://www.coreftp.com/).

Q Is there any configuration in the system which generates an alert if the memory reaches a configured threshold value?

A We periodically here this question, as well. Note this is written for your benefit and shouldn't be just copy/pasted to a customer- Because the logs do automatically rotate, there is little risk of the logs taking up too much space in the CF card, unless there happened to be a flood of logs asserted at the same time (since the logs are reviewed every 10 minutes to find out how large they are, a flood of log entries within the same 10 minute period, could potentially fill a log file before it had a chance to see if it needed to be rotated.

There is no automatic alert if the logs start to take up too much space on the CF card. However, a customer can always view how much space on the CF card is currently being used by the system/free space still available, via the df -h CLI command, or via the "Disk Status" section on the **Tools** -> **Upgrade/Backup** page of the browser (starting in software version 5.2.1 as shown below):



Disk Status

Total	947M
Used	467M
Free	431M
Percent	52%

Q Is there any mechanism which indicates us if the logs are deleted or overwritten?

A As log rotation and deletion is automatic, there is no “indication” for this operation occurring, other than either viewing the names of the files present in the /home/spectracom/log directory, or viewing the daemon log in this directory (which indicates logs were looked at to see if any logs needed to be rotated). As a number is added to the end of each log file in this directory once its rotated, having files with a number at the end “such as **alarms.log.1” for instance**) indicates that particular log file has been rotated. A log file that has a “**.4**” at the end of its name (such as “**alarms.log.4”**) that particular set of log entries will be automatically deleted once that log files rotates again (the same file with numbers of .1, .2. and .3 will still be in the unit.

Alerts associated with Log sizes

- ➢ Refer to Mantis case 2068

Q. Is there a setting in the system that will notify a remote logging server when the log file reaches a certain size (like 75%)?

A. As of at least version 5.3.0 there are no alerts associated with the size of the log files. The logs just rotate when they reach or exceed 75kb.

Log Configuration/Mapping (Facility and Severity codes)

Software issues/changes associated with log configuration

A) Update Version 1.4.1

- Fixed the Known Issue: Any changes to the Logging Configuration (for instance, turning on Local Logging) will not take effect without restarting the unit (found in 1.3.0)
- The **Authentication logging option was** added to the Local Logging panel of the Web UI to allow user configuration

Logs are configured in the:

A) web browser

Management -> ***Log Configuration*** page, Center “**Gear**” ICON for each log type.

Note info below carry-over from 1200 SecureSync. Need to confirm if applies to 2400s

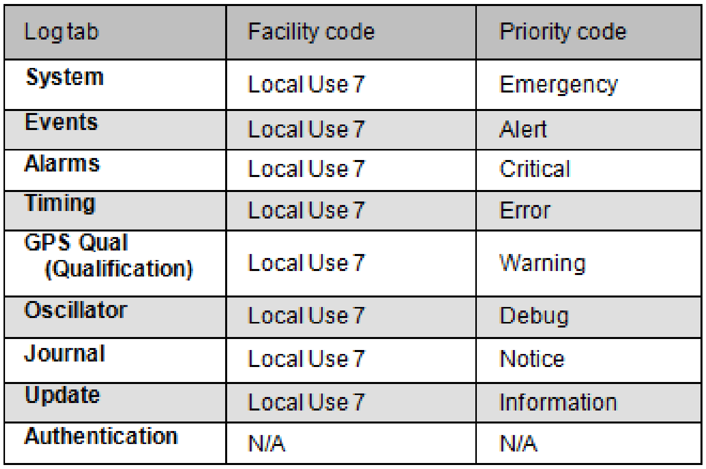
Email from Dave Sohn (3/16/12)
Facility and level are the syslog routing parameters to our log files. Our mapping is located in **config/speclog.conf**. By default the update log is local7.info

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



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/Log bundles

A) Save logs via web browser

1. Using web browser

All theSecureSync's logs (including those shown in the browser and also those in the background) can be easily bundled into one file and then exported from the SecureSync to send as an attachment.

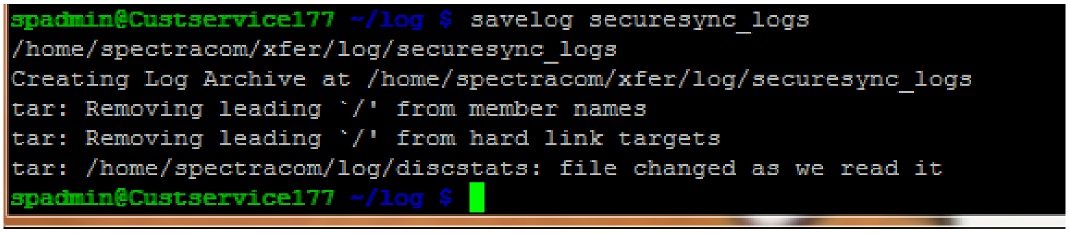
The logs can be easily saved to single bundled file and exported into a networked PC. Earlier versions of software allowed the bundle to be created, but then the file still needed to be transferred out using an FTP/SCP connection. Now, a button in the web browser alleviates the need to create an FTP session to transfer this file out to a PC.

The log bundling and export to a PC is controlled in the "**Management" -> "Log Configuration"** page of the SecureSync's web browser. On the left-side of the browser, click on the "**Save and download all logs**" button. You can then select where to save the log bundle to. The default file name is "securesync.log".

B) Save logs via CLI interface only (not using the web browser)

1. Logs can be placed into a single log file and then exported out using FTP/SCP:

CLI command to save the logs to a single file: savelog xxx<enter> (where xxx is the desired file name)

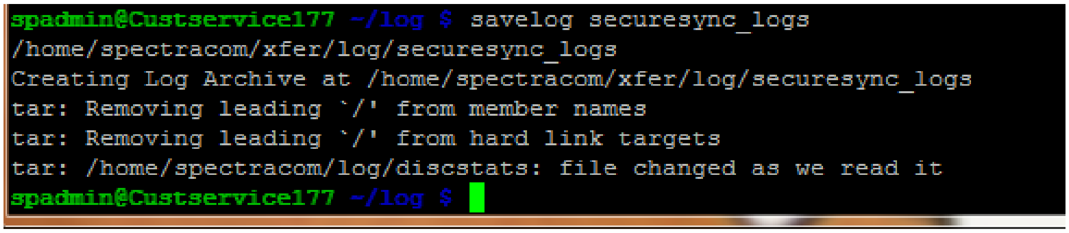


```
spadmin@Custservice177 ~/log $ savelog securesync_logs
/home/spectracom/xfer/log/securesync_logs
Creating Log Archive at /home/spectracom/xfer/log/securesync_logs
tar: Removing leading `/' from member names
tar: Removing leading `/' from hard link targets
tar: /home/spectracom/log/discstats: file changed as we read it
spadmin@Custservice177 ~/log $ 
```

Desire to manually FTP out the logs (not using the browser to bundle them first)

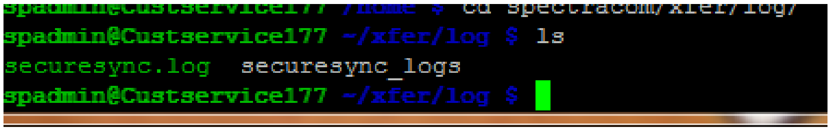
Note: All SecureSync Logs are stored in the **home/spectracom/log** directory.

1. Perform a **savelog xxx** <enter> command



```
spadmin@Custservice177 ~/log $ savelog securesync_logs
/home/spectracom/xfer/log/securesync_logs
Creating Log Archive at /home/spectracom/xfer/log/securesync_logs
tar: Removing leading `/' from member names
tar: Removing leading `/' from hard link targets
tar: /home/spectracom/log/discstats: file changed as we read it
spadmin@Custservice177 ~/log $ 
```

2. This file will be created and stored in the **home/spectracom/xfer/log** directory



```
spadmin@Custservice177 /home $ cd spectracom/xfer/log/
spadmin@Custservice177 ~/xfer/log $ ls
securesync.log   securesync_logs
spadmin@Custservice177 ~/xfer/log $ 
```

3. Use an FTP program (such as CoreFTP lite freeware) or SCP out the files.

Important Note: Transfer out this file using **Binary** mode

- an attachment.

Below is information on how to bundle the logs:
In order to capture the log files, simply copy/paste all of the log entries (from all of the log tabs) in the SecureSync's **Tools** -> **Logs** page of its web browser (such as all of the log entries in the "Event" tab, "Alarms" tab, "Oscillator" tab, etc). Paste all of the log entries into a single Microsoft Word document and then send us this document for our review.

Instead of copy/pasting all of the logs to a Word document, you can also bundle the logs into a single log file. Then export this bundle file from the SecureSync using an FTP or SCP session. Then, simply attach this extracted file to a reply email. Below is additional information on how to bundle and extract all of the unit's logs.

The log bundling is controlled in the "**Tools"/ "Upgrade/Backup"** page of the SecureSync's web browser. Click on the "Configuration" tab. Then, to bundle the logs, change "Save Log Files" to "Enabled" and then hit Submit. This generates a single file bundle of the logs. This file ("SecureSync.log") is placed in the "**home/spectracom/xfer/log/**" directory. Once it has been created, you can FTP/SCP it off the box (just make sure "FTP Service" is enabled in the Network/General page of the browser, "Services" tab).

If you need a free FTP client, we often use CoreFTP Lite (http://www.coreftp.com/).

After sending us the logs, we will review them and let you know what we find. Please let me know if you have any questions on the reception troubleshooting document. Then, we can go from there!

****Deleting/Clearing log files

A) Via the 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, mysqlls.log and system.log)

C) Via the clearlogs command

All Logs (and configs) can be deleted via the front panel/CLI “**clearlogs**” 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 reprogrammed and any other config changes that have been made will need to be reconfigured as desired.

D) Via the clean command

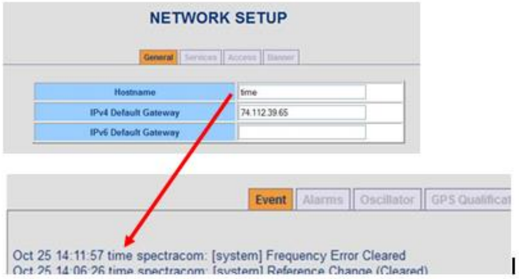
All Logs (and configs) can be deleted via the front panel/CLI “**clearlogs**”). The keypad has a “**Cmd**” menu (in the main “**System**” menu). After selecting this “Cmd” menu, press the up or down buttons until “**Clean**” is displayed. Then press the green checkbox. Once cleaned, if the network settings are statically set, they will need to reprogrammed and any other config changes that have been made will need to be reconfigured as desired.

Identifying which SecureSync sent the raw log entries to the Syslog server

- Each log entries contain the DNS Hostname of the SecureSync.

A (reply from Keith) Syslog does not use IP addresses to identify the network device that sent the log entries. For DHCP networks, this would likely be very confusing, because IP addresses can and do change, as directed by the DHCP server.

So instead of sending the IP address with the log entries, syslog uses the DNS hostname to indicate the source of the raw log data. Each of the SecureSync (and NetClock) log entries includes the unit’s hostname. This is how to identify which SecureSync sent the logs. By factory default, the hostname for the time servers is “Spectracom”. Customers can change this value as they wish. For SecureSync, the hostname is configured in the **Network** -> **General Setup** page of the browser, **General** tab.



NETWORK SETUP

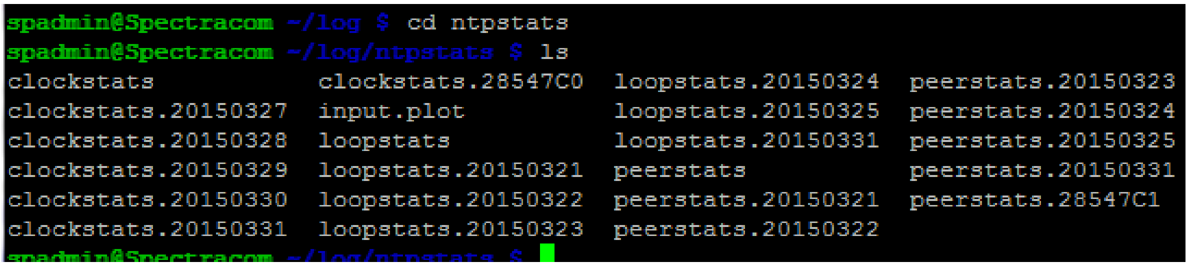
Hostname	time
IPv4 Default Gateway	74.112.39.65
IPv6 Default Gateway	

```
Oct 25 14:11:57 time spectracom: [system] Frequency Error Cleared
Oct 25 14:06:26 time spectracom: [system] Reference Change (Cleared)
```

**NTPStats (loopstats, peerstats, clockstats and sysstats)

For technical info on these available NTP Logs, refer to the following (in the custserviceassist doc) "NTP Statistics (NTP ClockStats, NTP loopstats and NTP Peerstats)"

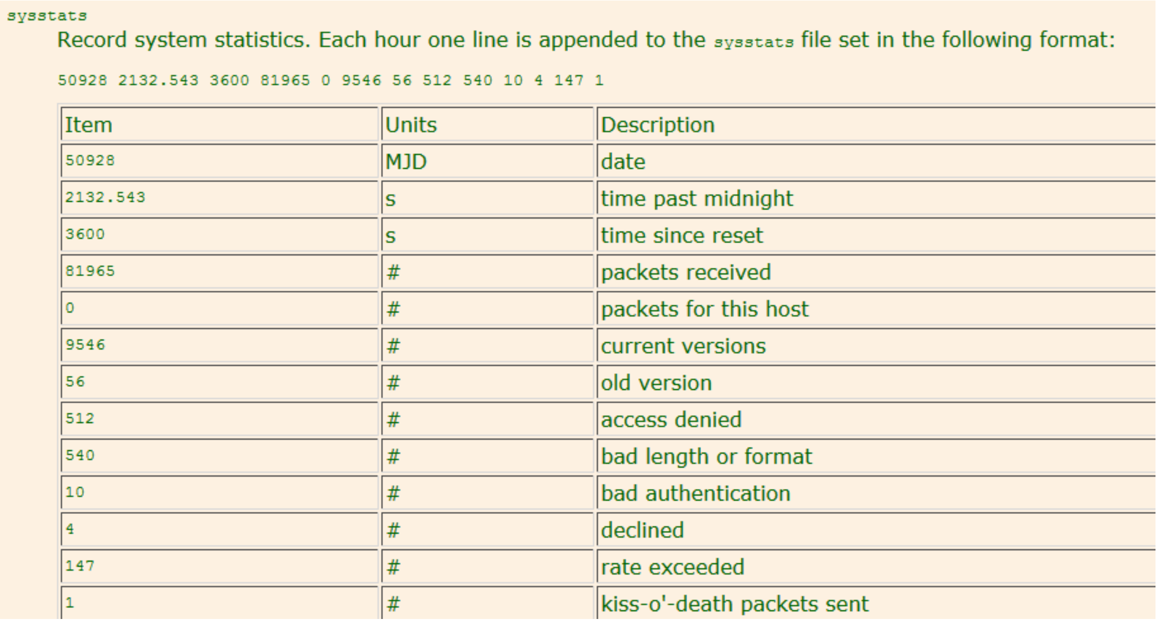
- These NTP-specific logs are stored in the /home/spectracom/log folder
- These logs can be FTP/SCP transferred out or viewed using telnet/ssh as desired.
- Systats was added in version 5.2.1 (Not available in versions 5.2.0 and below)
- NTP's loopstats, peerstats, clockstats(and sysstats starting in v5.2.1) are stored in the ntpstats folder in this directory (as shown in the screenshot below):



```
spadmin@Spectracom ~/log $ cd ntpstats
spadmin@Spectracom ~/log/ntpstats $ ls
clockstats           clockstats.28547C0  loopstats.20150324  peerstats.20150323
clockstats.20150327  input.plot          loopstats.20150325  peerstats.20150324
clockstats.20150328  loopstats           loopstats.20150331  peerstats.20150325
clockstats.20150329  loopstats.20150321  peerstats           peerstats.20150331
clockstats.20150330  loopstats.20150322  peerstats.20150321  peerstats.28547C1
clockstats.20150331  loopstats.20150323  peerstats.20150322
spadmin@Spectracom ~/log/ntpstats $
```

Systats (versions 5.2.1 and higher) packet counts/status/version info

- From: https://www.eecis.udel.edu/~mills/ntp/html/monopt.html



sysstats

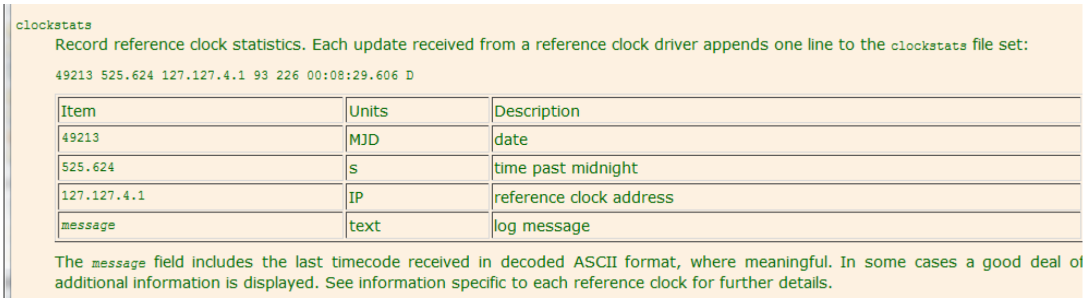
Record system statistics. Each hour one line is appended to the sysstats file set in the following format:

```
50928 2132.543 3600 81965 0 9546 56 512 540 10 4 147 1
```

Item	Units	Description
50928	MJD	date
2132.543	s	time past midnight
3600	s	time since reset
81965	#	packets received
0	#	packets for this host
9546	#	current versions
56	#	old version
512	#	access denied
540	#	bad length or format
10	#	bad authentication
4	#	declined
147	#	rate exceeded
1	#	kiss-o'-death packets sent

Clockstats (Reference Clock drivers, such as System Time input to NTP)

- From: https://www.eecis.udel.edu/~mills/ntp/html/monopt.html



`clockstats`

Record reference clock statistics. Each update received from a reference clock driver appends one line to the `clockstats` file set:

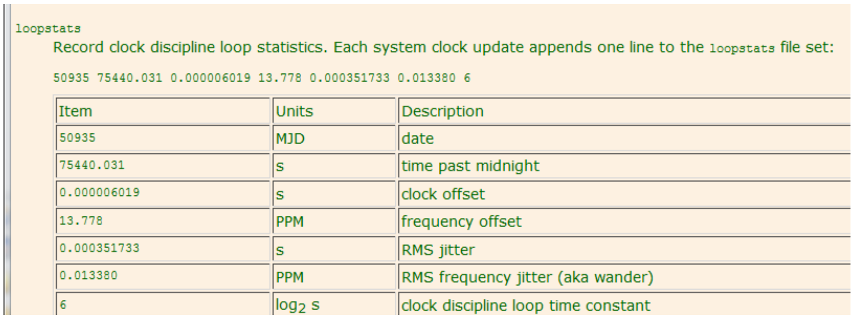
```
49213 525.624 127.127.4.1 93 226 00:08:29.606 D
```

Item	Units	Description
`49213`	MJD	date
`525.624`	s	time past midnight
`127.127.4.1`	IP	reference clock address
`message`	text	log message

The *`message`* field includes the last timecode received in decoded ASCII format, where meaningful. In some cases a good deal of additional information is displayed. See information specific to each reference clock for further details.

Loopstats (NTP's internal clock)

- From: https://www.eecis.udel.edu/~mills/ntp/html/monopt.html



`loopstats`

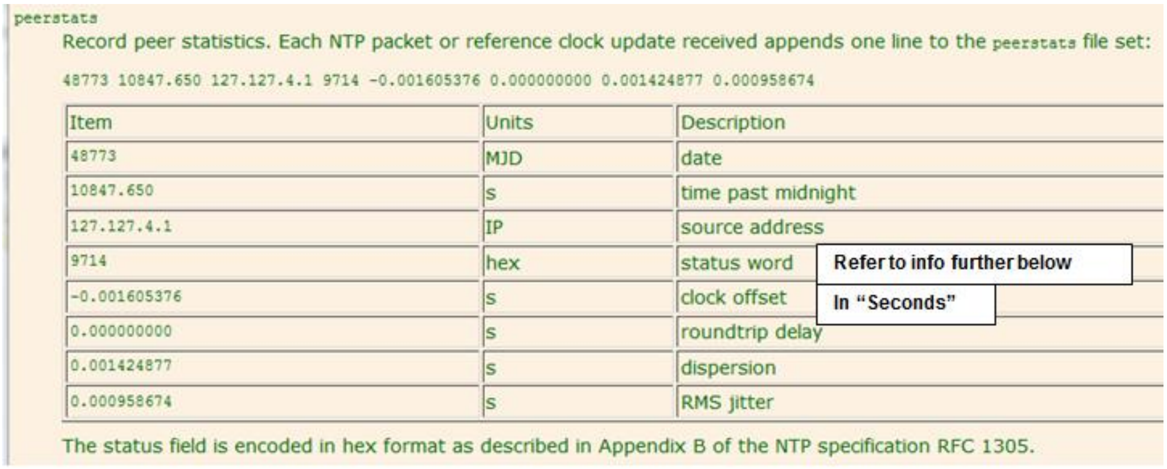
Record clock discipline loop statistics. Each system clock update appends one line to the `loopstats` file set:

```
50935 75440.031 0.000006019 13.778 0.000351733 0.013380 6
```

Item	Units	Description
`50935`	MJD	date
`75440.031`	s	time past midnight
`0.000006019`	s	clock offset
`13.778`	PPM	frequency offset
`0.000351733`	s	RMS jitter
`0.013380`	PPM	RMS frequency jitter (aka wander)
`6`	$\log_2$ s	clock discipline loop time constant

Peerstats **(other NTP servers listed in Peers/Servers tables)**

- From: https://www.eecis.udel.edu/~mills/ntp/html/monopt.html



peerstats

Record peer statistics. Each NTP packet or reference clock update received appends one line to the `peerstats` file set:

```
48773 10847.650 127.127.4.1 9714 -0.001605376 0.000000000 0.001424877 0.000958674
```

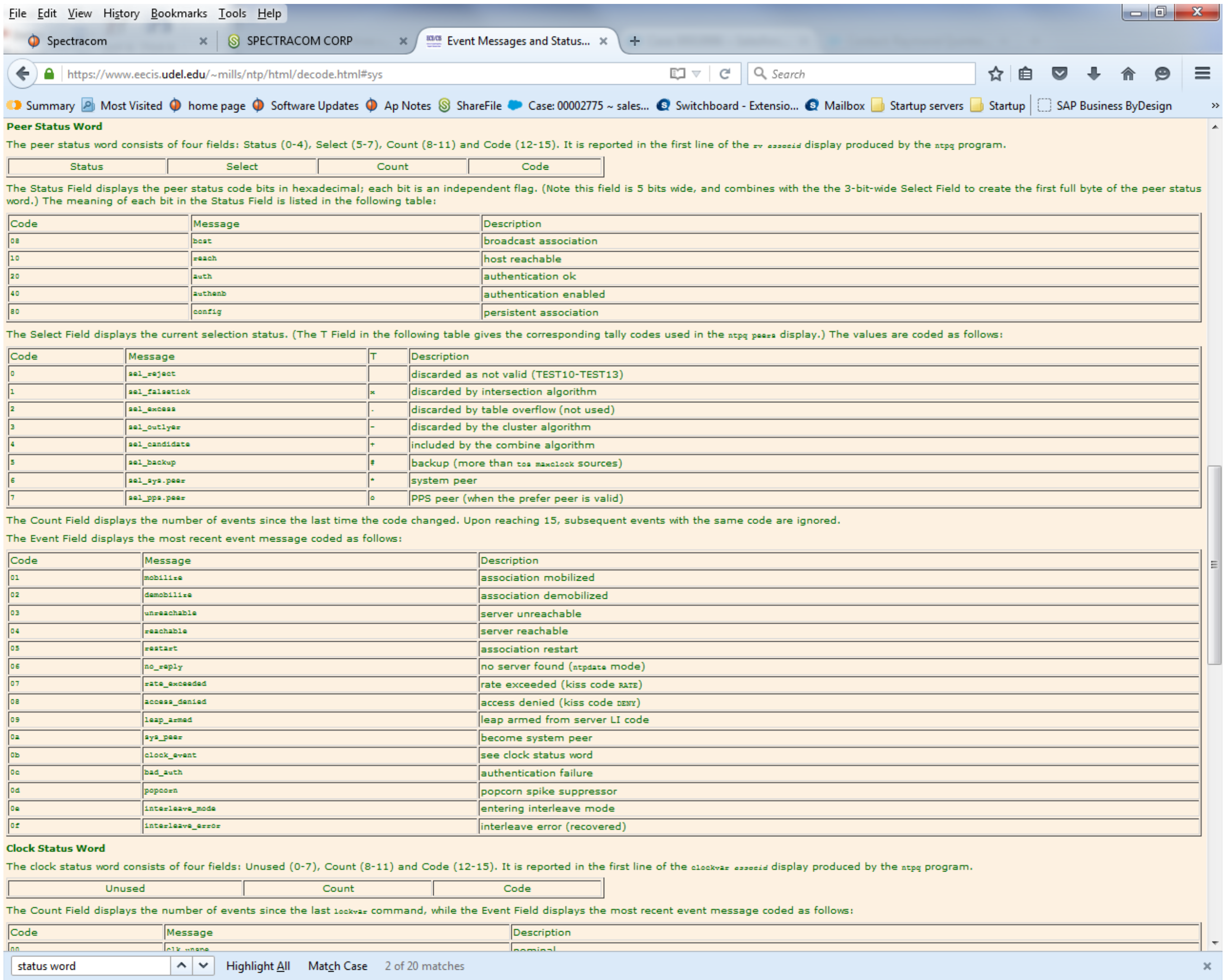
Item	Units	Description
48773	MJD	date
10847.650	s	time past midnight
127.127.4.1	IP	source address
9714	hex	status word
-0.001605376	s	clock offset
0.000000000	s	roundtrip delay
0.001424877	s	dispersion
0.000958674	s	RMS jitter

Refer to info further below

In "Seconds"

The status field is encoded in hex format as described in Appendix B of the NTP specification RFC 1305.

Peer status word (refer to: https://www.eecis.udel.edu/~mills/ntp/html/decode.html#sys)


File Edit View History Bookmarks Tools Help
Spectracom
SPECTRACOM CORP
Event Messages and Status...
https://www.eecis.udel.edu/~mills/ntp/html/decode.html#sys
Search
Summary
Most Visited
home page
Software Updates
Ap Notes
ShareFile
Case: 00002775 ~ sales...
Switchboard - Extensio...
Mailbox
Startup servers
Startup
SAP Business ByDesign

Peer Status Word

The peer status word consists of four fields: Status (0-4), Select (5-7), Count (8-11) and Code (12-15). It is reported in the first line of the `rv associd` display produced by the `ntpq` program.

Status	Select	Count	Code

The Status Field displays the peer status code bits in hexadecimal; each bit is an independent flag. (Note this field is 5 bits wide, and combines with the the 3-bit-wide Select Field to create the first full byte of the peer status word.) The meaning of each bit in the Status Field is listed in the following table:

Code	Message	Description
08	bcst	broadcast association
10	reach	host reachable
20	auth	authentication ok
40	authenb	authentication enabled
80	config	persistent association

The Select Field displays the current selection status. (The T Field in the following table gives the corresponding tally codes used in the `ntpq peers` display.) The values are coded as follows:

Code	Message	T	Description
0	sel_reject		discarded as not valid (TEST10-TEST13)
1	sel_falsetick	x	discarded by intersection algorithm
2	sel_excess	.	discarded by table overflow (not used)
3	sel_outlyer	-	discarded by the cluster algorithm
4	sel_candidate	+	included by the combine algorithm
5	sel_backup	#	backup (more than `tos maxclock` sources)
6	sel_sys.peer	*	system peer
7	sel_pps.peer	o	PPS peer (when the prefer peer is valid)

The Count Field displays the number of events since the last time the code changed. Upon reaching 15, subsequent events with the same code are ignored.

The Event Field displays the most recent event message coded as follows:

Code	Message	Description
01	mobilize	association mobilized
02	demobilize	association demobilized
03	unreachable	server unreachable
04	reachable	server reachable
05	restart	association restart
06	no_reply	no server found (`ntpdate` mode)
07	rate_exceeded	rate exceeded (kiss code `RATE`)
08	access_denied	access denied (kiss code `DENY`)
09	leap_armed	leap armed from server LI code
0a	sys_peer	become system peer
0b	clock_event	see clock status word
0c	bad_auth	authentication failure
0d	popcorn	popcorn spike suppressor
0e	interleave_mode	entering interleave mode
0f	interleave_error	interleave error (recovered)

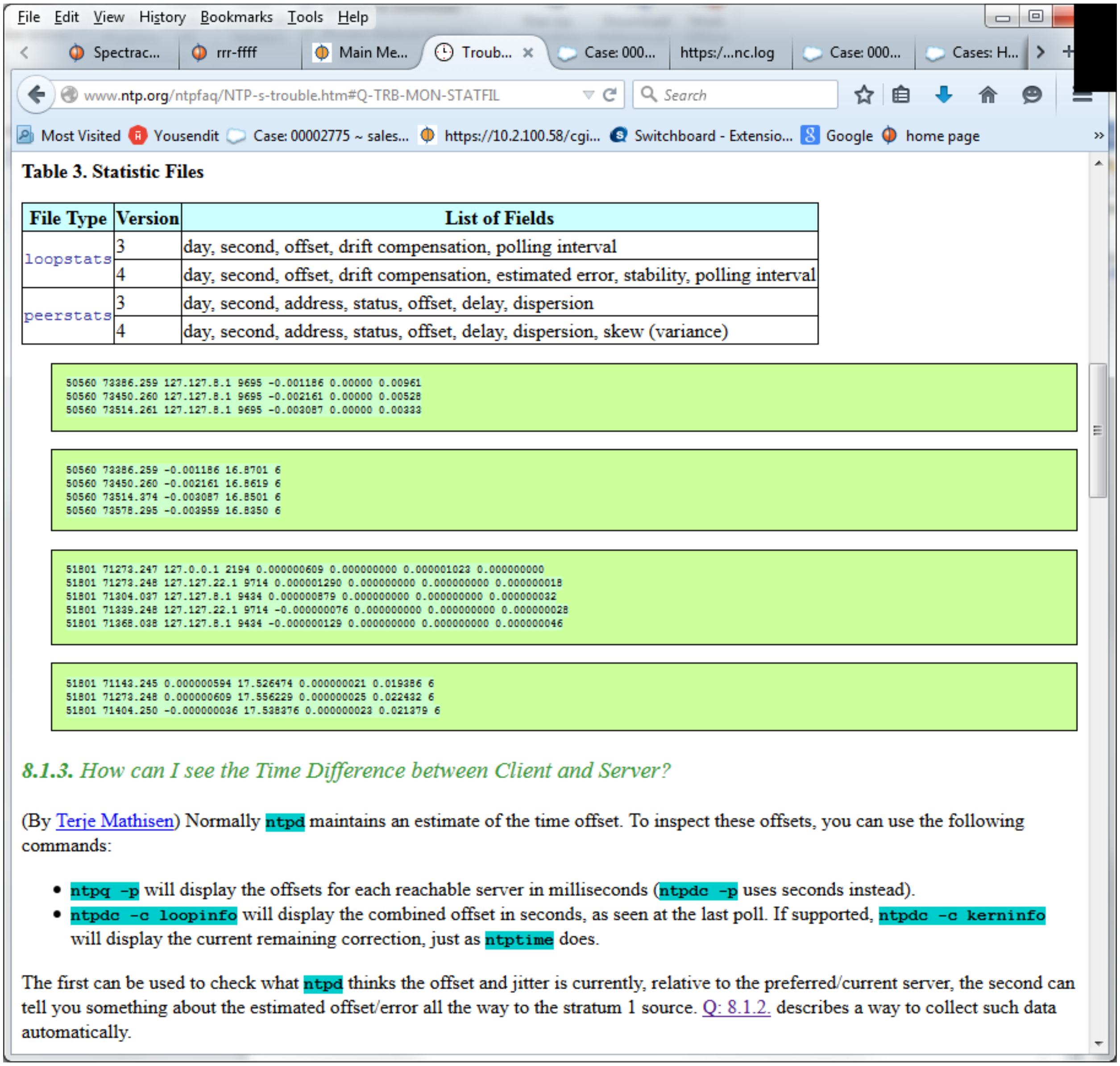
Clock Status Word

The clock status word consists of four fields: Unused (0-7), Count (8-11) and Code (12-15). It is reported in the first line of the `clockvar associd` display produced by the `ntpq` program.

Unused	Count	Code

The Count Field displays the number of events since the last `lockvar` command, while the Event Field displays the most recent event message coded as follows:

Code	Message	Description
00	clk_unspe	nominal


File Edit View History Bookmarks Tools Help
Spectrac...
rrr-ffff
Main Me...
Troub...
Case: 000...
https:/...nc.log
Case: 000...
Cases: H...
www.ntp.org/ntpfaq/NTP-s-trouble.htm#Q-TRB-MON-STATFIL
Search
Most Visited
Yousendit
Case: 00002775 ~ sales...
https://10.2.100.58/cgi...
Switchboard - Extensio...
Google
home page

[redacted]

Table 3. Statistic Files

File Type	Version	List of Fields
`loopstats`	3	day, second, offset, drift compensation, polling interval
	4	day, second, offset, drift compensation, estimated error, stability, polling interval
`peerstats`	3	day, second, address, status, offset, delay, dispersion
	4	day, second, address, status, offset, delay, dispersion, skew (variance)

```
50560 73386.259 127.127.8.1 9695 -0.001186 0.00000 0.00961
50560 73450.260 127.127.8.1 9695 -0.002161 0.00000 0.00528
50560 73514.261 127.127.8.1 9695 -0.003087 0.00000 0.00333
```

```
50560 73386.259 -0.001186 16.8701 6
50560 73450.260 -0.002161 16.8619 6
50560 73514.374 -0.003087 16.8501 6
50560 73578.295 -0.003959 16.8350 6
```

```
51801 71273.247 127.0.0.1 2194 0.000000609 0.000000000 0.000001023 0.000000000
51801 71273.248 127.127.22.1 9714 0.000001290 0.000000000 0.000000000 0.00000018
51801 71304.037 127.127.8.1 9434 0.000000879 0.000000000 0.000000000 0.00000032
51801 71339.248 127.127.22.1 9714 -0.000000076 0.000000000 0.000000000 0.00000028
51801 71368.038 127.127.8.1 9434 -0.000000129 0.000000000 0.000000000 0.00000046
```

```
51801 71143.245 0.000000594 17.526474 0.000000021 0.019386 6
51801 71273.248 0.000000609 17.556229 0.000000025 0.022432 6
51801 71404.250 -0.000000036 17.538376 0.000000023 0.021379 6
```

8.1.3. How can I see the Time Difference between Client and Server?

(By Terje Mathisen) Normally `ntpd` maintains an estimate of the time offset. To inspect these offsets, you can use the following commands:

- `ntpq -p` will display the offsets for each reachable server in milliseconds (`ntpdc -p` uses seconds instead).
- `ntpdc -c loopinfo` will display the combined offset in seconds, as seen at the last poll. If supported, `ntpdc -c kerninfo` will display the current remaining correction, just as `ntptime` does.

The first can be used to check what `ntpd` thinks the offset and jitter is currently, relative to the preferred/current server, the second can tell you something about the estimated offset/error all the way to the stratum 1 source. Q: 8.1.2. describes a way to collect such data automatically.

Loopstats/peerstats from http://www.ntp.org/ntpfaq/NTP-s-trouble.htm#Q-TRB-MON-STATFIL

Table 3. Statistic Files

File Type	Version	List of Fields
`loopstats`	3	day, second, offset, drift compensation, polling interval
	4	day, second, offset, drift compensation, estimated error, stability, polling interval
`peerstats`	3	day, second, address, status, offset, delay, dispersion
	4	day, second, address, status, offset, delay, dispersion, skew (variance)

Deleting the NTPStats (ntpstats)

A) Ability to delete both the discstats and NTP stats (loopstats, peerstats, clockstats) via CLI

- Can’t delete the NTPstats via CLI before version 5.1.5.

- Version 5.1.5 introduced the **clearstats** CLI command.

B) Ability to delete the NTP stats (loopstats, peerstats, clockstats and sysstats) via newer web browser

Bottom-left corner of the **Tools** -> **Upgrade**/**Backup** page ("**Clear All Stats"** button).

Software issue associated with deleting logs and NTP stats via the web browser

- With at least software versions 5.2.1 and below, these two browser buttons don't work.
- Note the associated CLI commands (clearlogs and clearstats) work fine in both Models (believe these were both added in version 5.1.5).
- Refer to Mantis case 3049.
- fixed in the version 5.3.0 update (Sept 2015)

**"Awk" and "Sed" filters for logs

- Refer to http://en.wikipedia.org/wiki/Sed
- We don't have any log filters

Q. Do you have some handy "awk" or "sed" filters appropriate for log file analysis? Or any other tools?
A. Reply from Dave Sohn (21 Jan 2014) I don't have any filters in general for the logs.
A. Reply from Paul Myers (21 Jan 2014) We make them as we need them.

**Specific log file entries

Log	Refer to Section below
Alarms.log	Alarms log
Auth.log (Authentication)	Auth log (Authentication log)
Cron.log (Cron)	cron.log (Cron log entries)
Daemon.log	daemon.log
Discstats	Discstats
Error.log (“ssl_request_log” (apache access log)	Error log
Events.log	Events log
Qual.log (Qualification)	Qual log
Journal.log	Journal log
Kern.log (Kernel log)	Kernel Log
Mail.log	Mail.log
Manifest.log	manifest.log/manifest.config file
Mysql_create.log	Mysql_create.log
NTP.log	NTP log
Oscillator.log (osc.log)	Oscillator log
Raccoon.log	
Rexd.bone	rexd.bone
rexd.log	rexd.log
Qual.log	qual.log
SNMPd.log	SNMPd.log
Rc.log (raccoon)	rc.log (raccoon)
Sys.log (syslog)	sys.log
System.log	System log
Timekeeper.log	Timekeeper.log
Timing.log	Timing log
Transfer.log	Transfer.log
Update.log	Update log
User.log	User log
Wtmp.log	wtmp.log file

Alarms.log (Alarms log)

In Holdover:

- Caused by loss of all input references.

Note: Time server is still in sync while in Holdover mode.

Not in Sync:

Caused by:

- Holdover mode expiring with no references being restored.
- Reboot/power cycle, until; resyncs to a reference.

Host disciplining (NTP disciplining the TCXO/OCXO oscillator) (applicable to versions 5.3.0 and above)
[system] 2015 289 16:31:24 001 HR: Enabling Host Disciplining Mode

21. **This entry is asserted each time KHTD is restarted (as indicated in the System log):** KTS Host Time Daemon has restarted (KHTD)

Frequency error alarm**-** Indicates the internal reference oscillator has experienced a large frequency correction.

The Frequency Error Alarm is asserted when 10 MHz Frequency Error measurement exceeds a set threshold (oscillator dependent)

- **TCXO oscillator**: **1x10-7** in v5.3.0 and below (changed to **1x10-6** starting in v5.3.1 to address. See note below about Mantis case 3168)
- **OCXO oscillator"** 1x10-8
- **Rubidium (and low phase noise Rubidium-LPN Rb):** 1x10-9

- Frequency Error Alarm clears once the measured frequency error no longer exceeds te applicable threshold.
- Frequency Error Alarm is only ever asserted if a disciplining reference (such as GPS) is present/valid (it's not asserted when there is no reference available).

This alarm occurs when:

- Power-up (clears shortly after TFOM gets down to TFOM 3 or below - phase error less than 100ns)
- loss of all input references
- Synced to NTP or Self
- 10 MHz Frequency Error measurement exceeds 1 x10^{-8}

Timing System Software Error: This entry can indicate an issue with the 10 MHz oscillator or GPS receiver (such as the oscillator being affected by the RES-SMT-GG GPS receiver, with v1.06 firmware)

Note: In earlier software versions (such as v5.1.4 or 5.1.5 for examples), this alarm can potentially be asserted in the logs as a "minor, spurious reporting-issue only"

email from Dave L (26 Jun 18) Also, I found some information on the "Timing System Software Error" message.
I confirmed that the specific Timing System Error entry you observed being asserted in the logs is a minor, spurious reporting-issue only. There is a condition that can potentially cause this entry to be asserted with older software versions such as v5.1.5 installed. This entry is limited to just a logging condition and does not indicate the operation of the time server was affected.
This minor logging issue was resolved with a subsequent software update.

Have seen it correlated with both of the following two log entries also being asserted at the same time:

- "Error:CS_Set(CS_SA_LEAP_SEC) call from GR" (in the Timing log)
- "Rb Reference unstable" (in the Oscillator log)
- Can be caused by the following error condition being asserted: CS_Set(CS_SA_LEAP_SEC) call from GR". This failure is caused by software issues with the Res-SMT-GG receiver (v1.06 firmware).
- Have also seen it asserted in conjunction with Holdover/Frequency Error alarms and Reference unstable" (in the Oscillator log). Examples below:

Example entries

```
Sep 16 05:04:35 Spectracom Spectracom: [system] No Longer In Holdover
Sep 16 05:04:35 Spectracom Spectracom: [system] Timing System Software Error
Sep 16 05:04:36 Spectracom Spectracom: [system] Reference Change (Cleared)
Sep 16 05:04:36 Spectracom Spectracom: [system] Timing System Software Error (Cleared)

Oct 17 06:48:39 Spectracom Spectracom: [system] Timing System Software Error
Oct 17 06:48:40 Spectracom Spectracom: [system] Timing System Software Error (Cleared)
```

Timing System Hardware error: This entry can indicate an issue with the 10 MHz oscillator.

- Seen it asserted in conjunction with Holdover/Frequency Error alarms.

Diagnosing the Timing System Hardware Error entry:

1) Review the **Timing** log for entries that indicate a problem with the Rb osc, such as the following examples"

```
[system] 2014 232 19:46:01 000 Rb varactor error (val=0, min=102, max=153)
[system] 2014 232 19:46:01 000 Rb peak voltage error (val=0, min=51, max=255)
[system] 2014 232 19:46:01 000 Rb fault detected (state=9)
```

5) Review the **Oscillator** logs for entries that indicate a potentially bad Rb oscillator, such as the following examples:

```
[system] 2014 204 12:49:19 000 XOS: Rb synchronized
[system] 2014 204 12:48:47 000 XOS: Rb tracking
[system] 2014 204 12:44:34 000 XOS: Rb track off -- free run
```

Note: Review the GPS Qual log to verify if "Rb track off -- free run" entries are due to a reception issue.

Review the Alarms log to see if there are any "1PPS Not in specification" entries

"GPS Antenna Problem": Open or short has been detected in the antenna cable.

"1PPS not in Specification" / "1PPS Restored to Specification" log entries

Note: these entries will likely be coupled with Holdover alarms (and Qual logs that may look great)

These are events that occur and alarm entries that are asserted. "1PPS not in Specification" occurs if the current TFOM values exceed the user-configurable max TFOM value. When the TFOM falls below Max TFOM, the Restored to Specification event/alarm entry is asserted.
Regarding the "1PPS Not in Specification" alarm, this alarm only occurs if the current TFOM exceeds the user-configurable max TFOM value. The SecureSync going into Holdover mode will not initially and automatically cause the TFOM to increase and exceed the max TFOM value. However, if the unit continues to operate for an extended period of time without any valid input references, the oscillator will begin to drift. As long as the max TFOM is not set

to 15, eventually, the max TFOM will be exceeded and the alarm is asserted. The type of oscillator (OCXO or Rubidium) and the setting of max TFOM will determine the typical amount of time in holdover required to exceed the max TFOM.

These alarms can be asserted with great GPS Reception in Qual logs

Auth.log (auth log/Authentication log)

- Generated from PAM (pluggable Authentication Module) - not from apache) (https://www.netbsd.org/docs/guide/en/chap-pam.html)
- Located in /home/spectracom/log auth.log

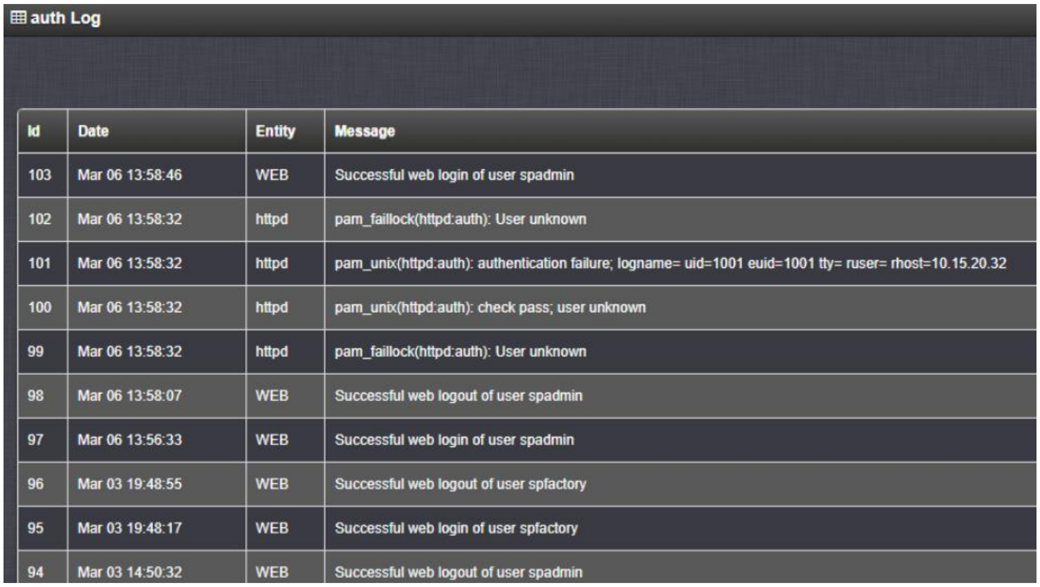
/home/spectracom/log auth.log – Contains system authorization information, including user logins and authentication machinsm that were used.

Authorization Log (from https://help.ubuntu.com/community/LinuxLogFiles)
The Authorization Log tracks usage of authorization systems, the mechanisms for authorizing users which prompt for user passwords, such as the Pluggable Authentication Module (PAM) system, the sudo command, remote logins to sshd and so on. The Authorization Log file may be accessed at /var/log/auth.log. This log is useful for learning about user logins and usage of the sudo command.

Use grep to cut down on the volume. For example, to see only information in the Authorization Log pertaining to sshd logins, use this: `grep sshd /var/log/auth.log | less`
Auth log / Ability to send Auth log entries to Syslog

Successful logins (web browser and CLI interfaces)

Status update: starting in 2400 SecureSynv update Version 1.7.0 (*per JIRA* ***CAR-1963***) is now to log SUCCESSFUL browser logins (it used to only be able to capture failed browser logins. Now it captures both Successful and unsuccessful browser logins). See example screenshot below:



auth Log

Id	Date	Entity	Message
103	Mar 06 13:58:46	WEB	Successful web login of user spadmin
102	Mar 06 13:58:32	httpd	pam_faillock(httpd:auth): User unknown
101	Mar 06 13:58:32	httpd	pam_unix(httpd:auth): authentication failure; logname= uid=1001 euid=1001 tty= ruser= rhost=10.15.20.32
100	Mar 06 13:58:32	httpd	pam_unix(httpd:auth): check pass; user unknown
99	Mar 06 13:58:32	httpd	pam_faillock(httpd:auth): User unknown
98	Mar 06 13:58:07	WEB	Successful web logout of user spadmin
97	Mar 06 13:56:33	WEB	Successful web login of user spadmin
96	Mar 03 19:48:55	WEB	Successful web logout of user spfactory
95	Mar 03 19:48:17	WEB	Successful web login of user spfactory
94	Mar 03 14:50:32	WEB	Successful web logout of user spadmin

(Versions 1.6.0 and below. Now changed in versions 1.7.0 and above).

Q Can the Authorization log be set to record successful logins and logouts?
A The Auth (Authorization) log is a log generated and maintained exclusively by the PAM module (Pluggable Access Module) PAM is the software module we use for login (The Auth log is not a "Spectracom" log). The Auth log has entries asserted for failed web browser and CLI (telnet, ssh, etc) logins. It also has entries asserted for successful CLI Logins. However, the PAM module does not assert any log entries for successful web browser login.

If a successful login occurs and the user makes any changes while logged in, these changes (including the user account name, date and time is recorded in the Journal log (displayed in the **Tools** -> **Journal** page of the browser).

Notes (as included in Auth log messages):

Word after host name (such as "Spectracom)

- **sshd**- entry is associated with SSH login
- **fcron**- entry is associated with cron scheduler (such as log rotate)
- **xinetd** Xinetd provides access control for all services based on the address of the remote host and/or on time of access and can prevent denial-of-access attacks. Xinetd provides extensive logging, has no limit on the number of server arguments, and lets you bind specific services to specific IP addresses on your host machine. Each service has its own specific configuration file for Xinetd; the files a relocated in the /etc/xinetd.d directory.
- **(pam_unix)** This is the standard Unix authentication module. It uses standard calls from the system's libraries to retrieve and set account information as well as authentication. Usually this is obtained from the /etc/passwd and the /etc/shadow file as well, if shadow is enabled.
- **(pam_ldap)** The pam_ldap module is a Pluggable Authentication Module (PAM) which provides for authentication, authorization and password changing against LDAP servers
- **(pam_tally)** This module maintains a count of attempted accesses, can reset count on success, can deny access if too many attempts fail.

Note **"/dev/tty**" is referring to the **CLI interface**

Password Change Attempt Logging
a) Is this treated differently between execution by a privileged (admin) user against another account vs. given account?

Keith's response: NO. It's not treated differently.

b) Is it logged at all (success and/or failure)?
Keith's response: Successful change is logged, Errors are not logged.

Entries associated with tcpdump

A) No auth log entries are asserted when starting tcpdump normally.

B) Trying to start tcpdump using "su" instead of "sudo" (or just typing "tcpdump" by itself)

Note-omit the word "sudo" in all the below commands for software versions 5.4.5 AND ABOVE

- Note the correct command to start tcpdump is either "**tcpdump"** (v5.4.5 and above), or "**sudo tcpdump**" (v5.4.1 and below)

```
su[8096]: pam_unix(su:auth): authentication failure; logname=spadmin uid=1002 euid=0 tty=/dev/pts/2 ruser=spadmin rhost=
user=tcpdump
su[8096]: FAILED su for tcpdump by spadmin
su[8096]: - /dev/pts/2 spadmin:tcpdump
```

Successful/unsuccessful login entries in the auth.log file

A) HTTP/HTTPS (web browser login)

- **Successful HTTP/HTTPS authentication:** No log entry sent from radius server
- **Unsuccessful HTTP/HTTPS authentication**: Log entry sent from radius severs and then local login is attempted.

B) HTTP/HTTPS (web browser login using LDAP and Radius login)

- **Successful LDAP/Radius authentication**: No log entry sent from a LDAP/Radius and no log entry in auth.log.
- **Unsuccessful LDAP/Radius authentication:** Log entry sent from radius severs LDAP/Radius and log entry asserted in auth.log.

C) CLI interface (telnet/ssh/ftp login)

- **Successful CLI interface authentication:** Log entry asserted in auth.log
- **Unsuccessful CLI interface authentication:** Log entry asserted in auth.log.

Q I am unable to find any log in/log out logs for audit. There seems to be only fail login present.

A Keith's response: This is a correct understanding for the web browser login. However, there are log entries for successful CLI logins (such as SSH connections).

The Auth (Authorization) log is a log generated and maintained exclusively by the PAM module (Pluggable Access Module) PAM is the software module we use for login (The Auth log is not a "Spectracom" log). The Auth log has entries asserted for failed web browser and CLI (telnet, ssh, etc) logins. It also has entries asserted for successful CLI Logins. However, the PAM module does not assert any log entries for successful web browser login.

If a successful login occurs and the user makes any changes while logged in, these changes (including the user account name, date and time is recorded in the Journal log (displayed in the **Tools** -> **Journal** page of the browser).

Below is an example Auth log entry indicating a **successful** ssh login:

```
SSH: Server;Ltype: Kex;Remote: 10.2.100.124-49468;Enc: aes256-ctr;MAC: hmac-sha2-256;Comp: none
```

**Authentication Log File Format

The first five fields in every authentication log entry are required by Steel-Belted Radius Carrier:

- Date—The date when the event occurred
- Time—The time when the event occurred
- RAS-Client—The name or IP address of the RADIUS client sending the authentication request
- Full-Name—The fully distinguished name of the user, based on the authentication performed by the RADIUS server
- ACC/REJ—The result of the authentication request (ACCEPT or REJECT)

The following example shows the heading line and an authentication log file entry consisting of the required attributes.

```
"Date","Time","RAS-Client","Full-Name","ACC/REJ"
"7/3/2003","12:11:55","RRAS","EdisonCarter","ACCEPT",
```

“(from getpwnam()   This is an entry at the very end of an auth log message
http://pubs.opengroup.org/onlinepubs/009604599/functions/getpwnam.html
The *getpwnam*() function shall search the user database for an entry with a matching *name*.

Example from a customer log:

Oct 21 21:33:10 ntp1-clf-6 httpd(pam_unix)[17266]: could not identify user (from getpwnam(smuthu)) –
(Where “**smuthu**” in parenthesis is the username that was entered)

Errrors

[EIO]
An I/O error has occurred.
[EINTR]
A signal was caught during *getpwnam*().
[EMFILE]
{OPEN_MAX} file descriptors are currently open in the calling process.
[ENFILE]
The maximum allowable number of files is currently open in the system.
The *getpwnam_r*() function may fail if:
[ERANGE]
[TSF] ⌦Insufficient storage was supplied via *buffer* and *bufsize* to contain the data to be referenced by the resulting **passwd** structure. ⌫

Example Auth log entries

ttyS0: input overrun

Email from Dave Lorah to Verizon- The Authorization Log entry ttyS0: input overrun message indicates there is a buffer overflow condition. This could be caused by short bursts of traffic that overrun the input. I will check with engineering to see if there is anything more I can tell you.

“**Conversation failed**” and “**tally undeflowed for user spadmin**” entries)

- Refer to salesforce case 24514
- Refer also to wtmp file: wtmp.log

This particular customer had three units (mix of versions of 5.4.1 and 5.4.5) with these two entries present. He reported trouble logging into the browser due to being “locked out of the spadmin account”. His report below”

> Recently I noticed some of SecureSync in MRT couldn't be accessed through Web UI. I was able to open login page but when I enter user and password it stated wrongly user and password. I have login through telnet and below is the appeared message: Account locked due to 39347 failed logins, Account locked due to 32010 failed logins, and Account locked due to 2362 failed logins.
> So I have reboot the unit and now can access the Web UI. Please advise is due from what?

Sample of the Auth log entries below:

```
2:31 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:auth): conversation failed
Feb 21 07:52:31 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:auth): user spadmin (1002) tally 39348, deny 5
Feb 21 07:52:34 SURS-CLK-SUBMC-00008 apache2: pam_unix(httpd:auth): authentication failure; logname= uid=1001
euid=1001 tty= ruser= rhost=10.12.21.49  user=spadmin
Feb 21 07:52:34 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:auth): conversation failed
Feb 21 07:52:34 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:auth): user spadmin (1002) tally 39349, deny 5
Feb 21 07:52:44 SURS-CLK-SUBMC-00008 login[1828]: pam_unix(login:auth): authentication failure; logname= uid=0
euid=0 tty=/dev/pts/1 ruser= rhost=10.12.122.4  user=spadmin
Feb 21 07:52:45 SURS-CLK-SUBMC-00008 apache2: pam_unix(httpd:auth): authentication failure; logname= uid=1001
euid=1001 tty= ruser= rhost=10.12.11.49  user=spadmin
Feb 21 07:52:46 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:auth): conversation failed
Feb 21 07:52:46 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:auth): user spadmin (1002) tally 39350, deny 5
Feb 21 07:52:47 SURS-CLK-SUBMC-00008 login[1828]: FAILED LOGIN (1) on '/dev/pts/1' from '10.12.122.4' FOR 'spadmin', Authentication failure
Feb 21 07:52:58 SURS-CLK-SUBMC-00008 login[1828]: pam_unix(login:session): session opened for user mrt1 by (uid=0)
Feb 21 10:56:36 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:account): Tally underflowed for user spadmin
Feb 21 11:14:05 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:account): Tally underflowed for user spadmin
Feb 21 11:18:15 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:account): Tally underflowed for user spadmin
Feb 21 11:25:45 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:account): Tally underflowed for user spadmin
Feb 21 12:11:33 SURS-CLK-SUBMC-00008 apache2: pam_tally(httpd:account): Tally underflowed for user spadmin
```

Results of this case: We suspect the wtmp file (records the logins and logouts was completely full due to potential authenticated security scans,   Refer to wtmp.log in this doc for more info.

---

fcron associated Auth log example entries

```
Spectracom fcron(pam_unix)[16819]: account root has password changed in future:
```

The System Time has been set back in time/date (likely due to a user manually setting the time/date back to a previous date). This log entry will continue to be asserted, until the System Time has been brought back to the expected date/time.

Status update: this issue was reportedly fixed in the version 5.0.0 software update. Refer to Mantis case 2091 (http://cvsmantis.int.orolia.com/mantis/view.php?id=2091)

HTTPS/web browser login associated auth log example entries

Successful "spadmin" account login (not user accounts – user account login further below)

Username of "spadmin" /correct password (valid login)

```
Oct 23 15:33:13 Spectracom pam_tally[7490]: pam_tally: unknown option; reset
```

Failed "root" account login, using an arbitrary password

Username of "root" / arbitrary password

```
16:18:58 Spectracom apache2: pam_unix(httpd:auth): authentication failure; logname= uid=1001 euid=1001 tty= ruser= rhost= user=root
16:18:58 Spectracom unix_chkpwd[30840]: password check failed for user (root)
```

Unsuccessful login using valid username but invalid password

Username of "spadmin" /wrong password (invalid login)

```
Spectracom httpd(pam_unix)[11894]: authentication failure; logname= uid=1111 euid=1111 tty= ruser= rhost= user=spadmin
```

Cause- this one entry generated when I tried logging in with web browser, using the correct "spadmin" account name but the wrong password.

Unsuccessful login using invalid username and arbitrary password

Invalid username of "admin1111" /erroneous password (invalid login)

```
14:22:34 Spectracom pam_tally[11581]: pam_tally: pam_get_uid; no such user
14:22:34 Spectracom httpd(pam_unix)[11581]: authentication failure; logname= uid=1111 euid=1111 tty= ruser= rhost=
14:22:34 Spectracom httpd(pam_unix)[11581]: check pass; user unknown
```

Cause- these three entries were generated when I tried logging in with web browser, using the incorrect “spadmin” account name of “admin11111” and just an arbitrary password.

Hitting the logout button while logged in as spadmin

Result – No Auth log entries asserted

Custom user account login

Just after creating new user account name of ‘kwing”

```
Oct 23 15:42:03 Spectracom pam_tally[32593]: pam_tally: unknown option; reset
Oct 23 15:41:20 Spectracom passwd(pam_unix)[31574]: password changed for kwing
Oct 23 15:41:20 Spectracom chage[31570]: changed password expiry for kwing
Oct 23 15:41:19 Spectracom useradd[31569]: add `kwing' to shadow group `spuser'
Oct 23 15:41:19 Spectracom useradd[31569]: add `kwing' to shadow group `spadmin'
Oct 23 15:41:19 Spectracom useradd[31569]: add `kwing' to group `spuser'
Oct 23 15:41:19 Spectracom useradd[31569]: add `kwing' to group `spadmin'
Oct 23 15:41:19 Spectracom useradd[31569]: new user: name=kwing, UID=1113, GID=111, home=/home/spectracom, shell=/bin/bash
```

Username of “kwing” /correct password (valid login)

```
Spectracom pam_tally[9494]: pam_tally: unknown option; reset (same as logging in as spadmin)
```

Username of “kwing” /wrong password (invalid login)

```
Spectracom httpd(pam_unix)[13910]: authentication failure; logname= uid=1111 euid=1111 tty= ruser= rhost= user=kwing
```

Cause: Account “kwing” does exist, but password not correct.

Invalid username “admin1111” /erroneous password (invalid login)

```
Oct 23 15:49:57 Spectracom pam_tally[16126]: pam_tally: pam_get_uid; no such user
```

Cause: there is no user account with this name.

SSH login associated example entries

```
Spectracom sshd[19393]: SSH: Server;Ltype: Authname;Remote: 10.253.96.80-32089;Name: ikkhan [preauth]
Spectracom sshd[19393]: Invalid user ikkhan from 10.253.96.80
Spectracom sshd[19393]: input_userauth_request: invalid user ikkhan [preauth]
```

```
Spectracom sshd[4195]: Accepted password for gvantrie from 10.21.32.66 port 1589 ssh2
Spectracom sshd[4195]: pam_unix(sshd:session): session opened for user gvantrie by (uid=0)
```

```
Spectracom sshd[16833]: User root from 10.252.152.134 not allowed because none of user's groups are listed in AllowGroups
Spectracom sshd[16833]: input_userauth_request: invalid user root [preauth]
Spectracom sshd[16833]: Connection closed by 10.252.152.134 [preauth]
Spectracom xinetd[824]: EXIT: ssh pid=16833 duration=1(sec)
```

Custom username of “kwing” / correct password (valid login)

```
Spectracom sshd[32499]: error: open /dev/tty failed - could not set controlling tty: Permission denied
Spectracom sshd(pam_unix)[32278]: session opened for user kwing by (uid=0)
```

Username of “spadmin” /wrong password (invalid login)

```
Spectracom sshd[12306]: error: PAM: Authentication failure for spadmin from pm-wing2.int.orolia.com
Spectracom sshd(pam_unix)[12512]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=pm-wing2.int.orolia.com
user=spadmin
```

Cause- Both entries generated when I tried logging in with SSH, using the correct “spadmin” account name but the wrong password

---

Invalid username “/correct spadmin password (invalid login)

```
Spectracom sshd[27122]: Postponed keyboard-interactive for invalid user admin from 10.2.100.29 port 1280 ssh2 [preauth]
Spectracom sshd[27122]: Failed keyboard-interactive/pam for invalid user admin from 10.2.100.29 port 1280 ssh2
Spectracom sshd[27122]: error: PAM: User not known to the underlying authentication module for illegal user admin from pm-
wing2.int.orolia.com
```

Cause- All three entries generated when I tried logging in with SSH, using the incorrect “spadmin” account name of “admin” , and the correct password of “admin123:

Exited out of a valid Putty session (just closed putty)

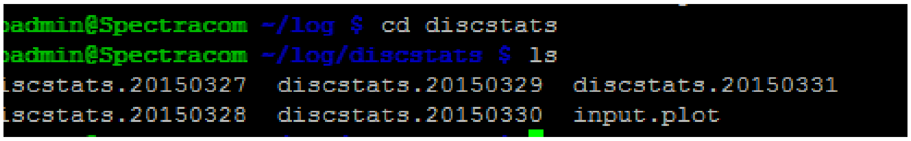
```
Spectracom xinetd[782]: EXIT: ssh pid=26141 duration=156(sec)
Spectracom sshd(pam_unix)[26141]: session closed for user kwing
```

Clockstats (ntpstats)

- The NTP clockstats are located in the ntpstats folder
- Search the log bundle for “clockstats” / “127.127.45.0” OR rename the entries in the log folder as .xls to view the data.
- 127.127.45.0 (Spectracom Reference Clock Driver) Entries indicate each time that NTP got a time input to System Time.
- Should be 16 seconds between each entry (based on the poll interval of our reference clock driver)
- Refer to clockstats in the NTP for all products section of this document for more info.

discstats

- These oscillator-specific logs are stored in /home/spectracom/log directory
- These logs can be FTP/SCP transferred out or viewed using telnet/ssh, as desired
- Discstats are stored in the discstats folder in this directory (as shown in the screenshot below).
- Discstats are also included in the log bundle.



```
admin@Spectracom ~/log $ cd discstats
admin@Spectracom ~/log/discstats $ ls
iscstats.20150327  discstats.20150329  discstats.20150331
iscstats.20150328  discstats.20150330  input.plot
```

- Selected Time/PPS reference, DAC value, Phase Error, Frequency Error, internal Temperature (starting in version 5.2.0, if a temperature sensor is installed)
- Records 5 days of data for the oscillator disciplining plots (Management -> Disciplining page of new browser)
- 5 daily Logs are located in the discstats folder of the log bundle
- Search the log bundle for "discstats" or rename the 5 entries in the log folder as .xls (or even better, .csv to seperate the columns as described below) to view the data

Recommendation to better review these files: Rename the files with the extension of "**.csv**" . The files will still open with Excel, but the comma delimited values will be in separate columns, instead of all values being in the same column when just opening as a standard excel file.

Data reported

- Data reported includes (left to right) Days since 1 Jan 1970, UTC Time Of Day (Seconds since midnight), Sync and Holdover status, selected Time/PPS reference , DAC value, Phase and Frequency Errors and Temperature (in versions 5.2.0 and above if a temp sensor is installed)

A) Software versions 5.2.0 and above (added internal temperature if thermostat is installed)

Days	TOD(S)	Sync Holdover	REF	DAC	Phase Error(ns)	Freq Error	Temp (c)
16591,	205,	1, 0	,ird0,ird0,	33384,	16,	8.94e-14	58.996452

B) Software versions prior to version 5.2.0

Days	TOD(S)	Sync Holdover	REF	DAC	Phase Error(ns)	Freq Error
16203	2789	1, 0	gps0,gps0,	-3	33164	-4.77e-11

Days = Number of Days since UNIX Epoch (1 Jan 1970)

Available converter (enter start date of **01/01/1970**)
http://www.timeanddate.com/date/durationresult.html?m1=01&d1=01&y1=1970&m2=05&d2=13&y2=2014

TOD(S) = Number of seconds since midnight on that day

Total Range is 0 to 86400

Partial hours (add this value to the previous whole hour value)

- **Seconds to xx**:**15**=900
- **Seconds to xx:30**=1800
- **Seconds to xx:45**=2700

Time Seconds	Time Seconds
00:00 = 0000	12:00 = 43200
01:00 = 3600	13:00 = 46800
02:00 = 7200	14:00 = 50400
03:00 = 10800	15:00 = 54000
04:00 = 14400	16:00 = 57600
05:00 = 18000	17:00 = 61200
06:00 = 21600	18:00 = 64800
07:00 = 25200	19:00 = 68400
08:00 = 28800	20:00 = 72000
09:00 = 32400	21:00 = 75600
10:00 = 36000	22:00 = 79200
11:00 = 39600	23:00 = 82800

- **Sync and Holdover:** 1 is true, 0 is False
- **DAC:** Believe this is the scaled DAC value for graph (not the actual DAC value)???
- **Phase error:** (in nanoseconds) Refer to the TFOM table to determine TFOM based on phase error

Reported Frequency Error values

- Reported Frequency Error measurements are "raw" frequency error – not fractional frequency errors.
- These "raw" frequency error values are like 0.00076, 1 x 10 +/- 4, or 1 x 10 +/- 5, (not like the fractional frequency error values such x10 $^{-11}$**,** 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.
11,52.023643
16649,77900,1,0,gps0,gps0,34190,-22,-1.44e-11,51.348320
16649,77902,1,0,gps0,gps0,34190,-22,-1.44e-11,51.922173
16649,78191,0,0,,,32768,1000000000,1.00e-02,49.073082
16649,78194,0,0,,,32768,1000000000,1.00e-02,49.147850
16649,78196,0,0,,,32768,1000000000,1.00e-02,49.164482
16649,78199,0,0,,,32768,1000000000,1.00e-02,49.222649
16649,78201,1,0,gps0,gps0,32768,1000000000,1.00e-02,49.297508
16649,78203,1,0,gps0,gps0,32768,1000000000,1.00e-02,49.322472
16649,78206,1,0,gps0,gps0,32768,1000000000,1.00e-02,49.230980
16649,78207,1,0,gps0,gps0,32768,1000000000,1.00e-02,49.380699
```

cron.log (Cron log entries)

```
fcrontab[2441]: installing file /tmp/fcr-9TuBXK for user root
```

- Per Paul Myers, this entry appears to be related to cron initially starting-up as part of system boot-up (it was asserted after a unit was rebooted, in addition to other log entries associated with normal system boot-up.

Cron log reports "[RESTART] Restarting initiated for snmpsad" followed by "[SUCCESS] Successfully restarted snmpsad"

- These two log entries are an indication that only the SNMPSAD subagent was restarted – not the SNMPd agent being restarted because our "watchdog" detected snmpsad wasn't running.
- If snmpsad crashes and needs to be reset, non-spectracom mibs will still be fine, but the spectracom mibs won't be able to respond until snmpsad has successfully restarted.
- snmpsad is being updated in software version 5.2.0 to allow SNMP to be updated to a newer version. If these two entries are periodically being asserted, it's recommended to update to at least version 5.2.0.

daemon.log (daemon log entries)

- log entries for daemons (such as NTP, SNMP, XINETd, etc)
- this is a linux OS log – not a Spectracom log
- This log may not be wiped with a "clean logs"

A) Example daemon.log entries for xinetd

- Refer to: http://linux.die.net/man/5/xinetd.log

1. xinetd[3637]: warning: can't get client address: Connection reset by peer

http://forum.sp.parallels.com/threads/xinetd-16263-warning-cant-get-client-address-connection-reset-by-peer.71361/
"It is normal warning that the address of remote server could not be known"

Suggestions if this entry is often being intermittently asserted:

1) Review the kern.log to see if eth0 is set to 10MB/half duplex (because it can't negotiate with a switch that is hard-set) as shown in the example entry below. This connection issue can "silent lockup" of the ETX module, (until unit is rebooted) especially in periods of heavier than usual network traffic

```
8139too 0000:00:06.0 eth0: link up, 10Mbps, half-duplex, lpa 0x0000
```

B) Example daemon.log entries for SNMP (associated with SNMPd or SNMPSAD)

- Refer to the "SNMP" section of this document for more info on these error messages.
- Recommended to update software to v5.2.0 or higher to upgrade NET-SNMP to newer version

Note: daemon log records only "WARNING" or error messages about SNMP. Refer to the Journal log for entries showing SNMPd being stopped and started (normal operation).

Wrong netlink

netlink - communication between kernel and user space (AF_NETLINK)

Netlink is used to transfer information between kernel and user-space processes. It consists of a standard sockets-based interface for user space processes and an internal kernel API for kernel modules. The internal kernel interface is not documented in this manual page. There is also an obsolete netlink interface via netlink character devices; this interface is not documented here and is provided only for backward compatibility.

```
snmpd[2065]: Wrong netlink message type 3
```

- Refer to SR 4958/SR 5490 in SAP (customer was running v5.3.0)

SNMP Build Errors

"Error building ASN.1 representation, SNMP Build Unknown Failure, RFC1213-MIB Messages" **or**

"send response: Error building ASN.1 representation (wrong type in snmp_realloc_rbuild_var_op: 199)"

- This is a known condition in RFC-1213
- Doesn't affect operation of SNMP
- Refer to http://www.teragauge.com/index.php/support/knowledge-base/19-kb-troubleshooting/53-kb-tg-snmp-syslog-error-msg

SNMP already started (trying to enable SNMP while it's already running)

/etc/init.d/snmpd[22014]: WARNING: snmpd has already been started

- Asserted when trying to start SNMP when its already enabled (using the servset 7 on command to enable SNMP, not realizing the browser shows its already running)

SNMP already stopped (trying to disable SNMP while it's already stopped)

```
/etc/init.d/snmpd[8047]: WARNING: snmpd is already stopped
```

- Asserted when trying to stop SNMP when its already disabled (using the servset 7 off command to enable SNMP, not realizing the browser shows its already disabled)

/etc/init.d/snmpsad[29156]: WARNING: snmpsad is already stopped

- Asserted when trying to stop SNMP when its already disabled (using the servset 7 off command to enable SNMP, not realizing the browser shows its already disabled)

Superuser entry

/etc/init.d/snmpd[14810]: snmpd: superuser access required

- Oleg believes this entry was likely asserted in a customer's log when a user tried to manually start/stop SNMP in "/etc/init.d" (instead of using either the browser or CLI). Note that it's unlikely there will be an associated log entry asserted in the journal log for this attempted situation.
- Since a user won't have root access, they can't issue any linux commands to stop or restart Services such as SNMP.

??

```
Spectracom-CLK2 /etc/init.d/snmpd[22442]: start-stop-daemon: no matching processes found
Spectracom-CLK2 /etc/init.d/snmpd[21939]: start-stop-daemon: no matching processes found
```

C) Example daemon.log entries for NTP

```
Spectracom-CLK2 /etc/init.d/ntp[3108]: start-stop-daemon: no matching processes found
NTP stopping: Spectracom-CLK2 /etc/init.d/ntp[14530]: status: stopping  (NTP was  stopped)
```

ntp: unknown function `kill' (followed by) status: starting   (indicates NTP was automatically restarted)

error_log (Apache HTTP Error log entries)

- These are error log entries from Apache2 (**/var/log/apache2/error.log**)

- For **general info** on this log, refer to: http://httpd.apache.org/docs/2.2/logs.html
- **For status codes** (*such as “200-OK”) refer to: https://www.rackspace.com/knowledge_center/article/interpreting-common-status-codes-in-web-logs
- This is the place where Apache httpd will send diagnostic information and record any errors that it encounters in processing requests. It is the first place to look when a problem occurs with starting the server or with the operation of the server, since it will often contain details of what went wrong and how to fix it.
- Added to the log bundle in software version 5.2.1 (I believe)
- Starts with “.log.1” as the file extension instead of just “.log” like the other log files
- Can’t view them in the browser. View this log via CLI or from a log capture file

Log entry format

- Example log entry [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/home/live/ap/htdocs/test

Error log components

1. **The first part of the log entry** is the date and time (server time) when the event occurred. Apart from just being informative, that time can be useful for looking for entries in other logs at the same time. In this case, check the access log to see the full URL that the web client tried to visit. If it was an error that indicated a module had trouble talking to a database, then look in the database server's logs at the same time to see what prevented the connection from happening.
2. **The next part**, "[error]", describes the level of the alert. This will often be "error", but sometimes other levels will indicate that the message logged is just a warning, or it may represent a critical error that caused the web server to shut down or fail to start.
3. **The next part**, "[client 80.154.42.54]", shows the source of the error. In this case the source is a web client, so the visitor's IP address was logged.
4. **The last part of the log entry is the error itself:**

   A) Normal error_log entries for logging out of spadmin account

```
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Users/logout), referer: http://10.2.100.176/
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Users/logout), referer: http://10.2.100.176/
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /toolsb) /contact), referer: http://10.2.100.176/
[Mon Sep 15 16:33:52 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /tools/contact), referer: http://10.2.100.176/
```

   B) Normal error_log entries for login to spadmin account

```
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /Home), referer: http://10.2.100.176/tools/contact
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /Home), referer: http://10.2.100.176/tools/contact
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /users/login), referer: http://10.2.100.176/tools/contact
[Mon Sep 15 16:37:06 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /users/login), referer: http://10.2.100.176/tools/contact
[Mon Sep 15 16:37:15 2014] [warn] [client 10.2.100.124] -authlogic- authmethod is currently (null) (for /users/login), referer: http://10.2.100.176/users/login
[Mon Sep 15 16:37:15 2014] [warn] [client 10.2.100.124] -authlogic- authtype is currently Pamacea (for /users/login), referer: http://10.2.100.176/users/login
```

C) Error_log entries from a SecureSync exhibiting error 500 messages when logging in

```
enable, referer: https://10.82.133.149/auth/login.html?target=/cgi-
bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Not processing line, referer:
https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Could not find the required information linedefault value then,
referer: https://10.82.133.149/auth/login.html?target=/cgi-
bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Could not find the required information linedefault value then,
referer: https://10.82.133.149/auth/login.html?target=/cgi-
bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
[Sat Sep 13 19:15:22 2014] [error] [client 206.218.195.190] Premature end of script headers: StatusConfig.cgi, referer:
https://10.82.133.149/auth/login.html?target=/cgi-bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
[Sat Sep 13 19:15:22 2014] [warn] [client 206.218.195.190] -authlogic- authmethod is currently (null) (for
/spec500err.html), referer: https://10.82.133.149/auth/login.html?target=/cgi-
bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
[Sat Sep 13 19:15:22 2014] [warn] [client 206.218.195.190] -authlogic- authtype is currently Pamacea (for
/spec500err.html), referer: https://10.82.133.149/auth/login.html?target=/cgi-
bin/StatusConfig.cgi%3fPage=index&pamservice=httpd&userfile=
```

D) “RSA server certificate CommonName (CN) `Spectracom' does NOT match server name!?”

- Indicates web browser Security Settings may be set too high. Try lowering the settings to the lowest value and then login again.
- May need to replace the default HTTPS certificate with a new one using values particular to the network.

events.log (Events log entries)

All Power Inputs Detected: The SecureSync can be configured for AC and/or DC input power. This entry indicates that applicable power has been detected on all available inputs.

"1PPS not in Specification" / "1PPS Restored to Specification"
These are events that occur and alarm entries that are asserted. "1PPS not in Specification" occurs if the current TFOM values exceed the user-configurable max TFOM value. When the TFOM falls below Max TFOM, the Restored to Specification event/alarm entry is asserted.

Regarding the "1PPS Not in Specification" alarm, this alarm only occurs if the current TFOM exceeds the user-configurable max TFOM value. The SecureSync going into Holdover mode will not initially and automatically cause the TFOM to increase and exceed the max TFOM value. However, if the unit continues to operate for an extended period of time without any valid input references, the oscillator will begin to drift. As long as the max TFOM is not set to 15, eventually, the max TFOM will be exceeded and the alarm is asserted. The type of oscillator (OCXO or Rubidium) and the setting of max TFOM will determine the typical amount of time in holdover required to exceed the max TFOM.

Frequency Error: "Frequency Error Detected" indicates either the unit had recently been rebooted, a large oscillator frequency offset was detected (such as changing from one selected input reference to another). It is also asserted when the SecureSync is synced to either NTP or USER and therefore, the oscillator cannot be disciplined to the selected reference.

The frequency error threshold for this alarm to be asserted is oscillator type dependant

Frequency Error Cleared indicates the oscillator has relocked after a recent power cycle or has been steered to compensate for a large frequency error. Fractional frequency error is less than $1\text{x}10^{-8}$

Reference Change / Reference Changed to / Reference Change Cleared: The highest present and valid priority reference that was available was lost, so the next highest present ad valid priority was selected.

> **Note:** The Reference Change entry is also asserted when the SecureSync goes into Holdover mode (no references currently available).
>
> **Note:** (Starting in software versions 5.0.1 and above), a second entry is also asserted to indicate what references were just selected (example*:* SS: Reference changed to Time Ref: gps0 PPS Ref: gps0). When the SecureSync goes into Holdover mode, the entry will indicate "none" as the selected reference (example: SS: Reference changed to Time Ref: none PPS Ref: none)

Q. What does "**Reference Change**" and "**Reference Change (Cleared)"** refer to?
A. When the preferred reference is not valid or a preferred valid reference is detected in the priority reference table the system sets a Reference Change bit in a register that tells the system that it needs to change references. After the system changes references that bit is cleared. When these events occur, their respective notifications are displayed in the logs.

Q And their relation to Holdover state?
A If NO References are available such as GPS or NTP your reference will change to Holdover state until either the holdover time that you have set has expired or until the system detects a valid reference.

Reference Change (Cleared): System entry just to reset the "Reference Change" state. This entry can be disregarded.

In Holdover / No longer in Holdover (Holdover event)

- Note that in at least software versions 5.3.1 and below, Holdover is an Event (entry in the Events log) instead of being an Alarm (entry in the Alarms log).

Indicates the NTP server lost synchronization to its external reference input and it's using the internal reference oscillator to derive the time outputs. This alarm is classified as a Minor alarm condition. The Holdover mode will continue until the reference is restored, it times out as configured in the System/Holdover page, or the unit NTP server is rebooted/power cycled. If Holdover mode times out, at that time a Time Sync alarm will be asserted.

During the Holdover mode, all outputs remain available to synchronize other devices. This mode is just an alert that the primary input is not available and so the oscillator is being used to provide time outputs. There is no other effect on the operation of the system while in the mode.

"In Holdover" indicates no input references are currently present and valid. The oscillator is in free-run mode. Time is being maintained by the oscillator and is still valid for synchronization. "No longer In Holdover" indicates at least one input reference has been restored, or no input references have been restored and the Holdover period has expired. Time is no longer valid for synchronization.

In Sync / Not In Sync: "In Sync" indicates SecureSync has at least one present and valid reference to sync with. Time is valid for synchronization. "Not In Sync" indicates SecureSync has no present and valid references to sync with and the Holdover period has elapsed. Time is no longer valid for synchronization.

GPS Antenna Problem / GPS Antenna OK: Based on measured current draw, **"**GPS Antenna Problem" indicates the GPS receiver detected the antenna is not connected or there is an open/short in the antenna cable.   "GPS Antenna OK" indicates the GPS receiver has detected an expected amount of current draw. So the antenna appears to be connected to the GPS receiver with a good cable connection

The Unit Has Rebooted: This entry indicates the SecureSync was either power cycled or rebooted via a CLI interface (such as the web browser).

Error entry periodically being asserted "[system] ERROR - KW_HR_SetTime returned [rc = 3]"

- Refer to Salesforce cases 14919 (Dongjin) and 12869 (Open Access, Australia)
- Apparently asserted when NTP input tries to set the KTS time but is not able to.
- Verify the proper configuration of the NTP Peers and NTP Servers tabs.
- Dongjin had the Enable Stratum 0 PPS reference (127.127.22.0 in Expert mode) enabled with a peer configured

Failed to report event to NOTD followed by
Failed to report event to NOTD (GPSD)

- Refer to Salesforce case 20365 (Kaiser)
- Kern log also contained "hda" error messages such as :

```
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=87817,
sector=87817
Jan 12 18:23:10 cdcntp202 kernel: hda: possibly failed opcode: 0xc8
Jan 12 18:23:10 cdcntp202 kernel: end_request: I/O error, dev hda, sector 87817
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=88049,
sector=88049
Jan 12 18:23:10 cdcntp202 kernel: hda: possibly failed opcode: 0xc8
Jan 12 18:23:10 cdcntp202 kernel: end_request: I/O error, dev hda, sector 88049
Jan 12 18:24:37 cdcntp202 kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
Jan 12 18:24:37 cdcntp202 kernel: hda: dma_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=88049,
sector=88049
```

Email fron Paul Myers (13 Jan 2016) I may have commented on this before keith, but this unit looks like 2 issues. Possibly the mysql database is not working write for some errors, but the 2nd errors you point out give me concern the CompactFlash is corrupted or worst case the interface to the CF in hardware is causing errors.

You could reboot and clean and see what happens. OR you could do a clean update. If the errors exist below then you might have a bad CF or ATA CF interface in hardware is bad. Most likely CF though.

```
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
```

Failed to report event to NOTD (KAD) followed by
Failed to read oscillator frequency error from KTS (KAD)

- Refer to Salesforce case 18880 (RMA found SecureSync had a bad OCXO osc)

The Unit Has Rebooted: This entry indicates the SecureSync was either power cycled or rebooted via a CLI interface (such as the web browser

SAASM rcevier-related log entries in the Events log (even though a SAASM receiver is not installed)

specific examples of log entries that were observed:

- "The SAASM Key will not Expire Soon"
- "The SAASM Key is Valid"

- This condition should not be observed in at least version 5.4.5 or above.
- This was a software issue that was addressed sometime before version 5.4.5 release (not sure which earlier version actually fixed it, but it was fixed before v5.4.5 was released)

Email from Paul Myers (26 Oct 16) There was a bug which caused SAASM event entries to be logged because they were not inhibited. This was corrected in some release since then. Updating to 5.4.5 or better yet 5.5.0 would fix that.

(journal.log) Journal log entries

In general:

- **[WEB]** Changes made via the spadmin account
- **[clie]** Changes made via the CLI (ssh, front panel menu buttons etc)
- **[httpd]** automatic actions by Apache daemon

Specific example entries

A) Entries associated with network settings

set DHCP for eth0 to enabled.
set DHCP for eth0 to disabled.

requests DHCP lease for eth0 to be released: (in at least versions 5.3.0 and above), only asserted when DHCP is enabled, and user performs a release (not asserted when DHCP is disabled)

requests DHCP lease for eth0 to be renewed (in at least versions 5.3.0 and above), only asserted when DHCP is enabled and user performs a renew (not asserted when DHCP is disabled)

B) Entries associated with manually setting the time

[frontpanel] Set Time for User Reference 0 in slot 0 to HR (0) Time: 2012 38 3:29:40 {500000000}: Indicated a user had manually changed the System Time to the value at the end of this log entry. The very beginning of the entry also indicates if the System Time was changed by a user via the web browser or by the front panel keypad.

"[spadmin] Changed Contellation Selection for GPS Reference 0 in slot 0 from GR (0) ConstellationSelection: (3) : ^IGPS ^IGLONASS to GR (0) ConstellationSelection: (1) : ^IGPS:" **:**

Reboots and Halts

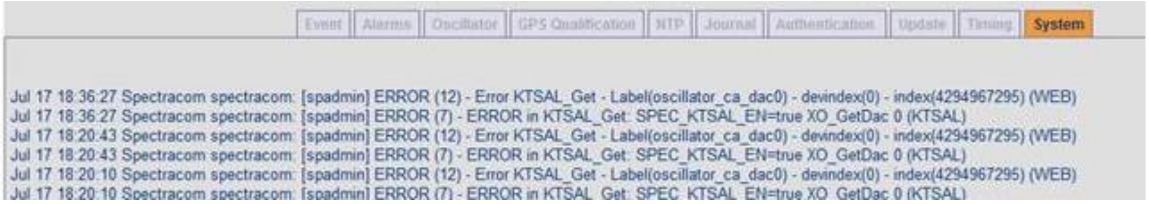
- Update version 5.4.5 added journal entries for reboots and halt commands issued in CLI interface.

GNSS receiver constellation selection was changed by a user.

Jun 20 12:44:10 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)

Jun 20 12:41:59 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB)

Jun 20 12:41:59 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)



```
Jul 17 18:36:27 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB)
Jul 17 18:36:27 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)
Jul 17 18:20:43 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB)
Jul 17 18:20:43 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)
Jul 17 18:20:10 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB)
Jul 17 18:20:10 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)
```

Email from Dave Sohn (6/20/12)

There isn't any issue with the unit. This is just a reporting bug. The system is in the background querying the DAC value for some reporting, but that isn't a valid call for a Rubidium unit, so there is an error. There is no effect on operation, and that error doesn't mean there is any problem with the unit. You can enter a Mantis case for it, and we will discuss it in SW CCB.

(8/31/12 KW) Update – the fix for this issue should be in the version 4.8.7 release

Journal log entries related to SNMP

Reset SNMP configs via button in newer black browser

[WEB] Performed SNMP restore configuration function (admin): user pressed the button to reset just the SNMP configs

Starting (Enabling) SNMP

A) web browser

Stopping (Disabling) SNMP Service

A) Via newer black interface web browser

(Note: only the one entry below is asserted each time)
[WEB] Stopped SNMP services (spadmin): user disabled SNMP via the new browser

Kern.log (Kernel Log entries)

Kernel Entries and other indicating potential software/hardware issues happening (such as a potential ETX failing. SNMP crashing or an issue with the CF card)

- Consists of log entries associated with the Linux OS (not “Spectracom” log entries)
- “Linux kernel map” added in software update version 5.2.0 for improved diagnostics
  - Maps memory locations
  - Example related kernel entries

```
“Inspecting /boot/System.map-3.8.13-gentoo”
“Cannot find map file.”
```

“kernel: net_ratelimit: callbacks suppressed” entries (log entries to syslog server being suppressed)

- Indicates log entries to be sent to syslog serve are being suppressed to prevent overloading the syslog server
  - This was observed with SF case 126253 where there were many of these kerm.log entries generated over a short period of time, with many entries also in the snmp.log

```
Feb 6 20:44:03 w0001-ntp-1200a kernel: net_ratelimit: 21 callbacks suppressed
Feb 6 20:44:13 w0001-ntp-1200a kernel: net_ratelimit: 19 callbacks suppressed
Feb 6 20:44:18 w0001-ntp-1200a kernel: net_ratelimit: 187 callbacks suppressed
Feb 6 20:44:23 w0001-ntp-1200a kernel: net_ratelimit: 216 callbacks suppressed
Feb 6 20:44:28 w0001-ntp-1200a kernel: net_ratelimit: 75 callbacks suppressed
Feb 6 20:44:33 w0001-ntp-1200a kernel: net_ratelimit: 1 callbacks suppressed
Feb 6 20:44:46 w0001-ntp-1200a kernel: net_ratelimit: 1 callbacks suppressed
Feb 6 20:44:52 w0001-ntp-1200a kernel: net_ratelimit: 23 callbacks suppressed
```

I found the note below at https://serverfault.com/questions/277009/what-does-net-ratelimit-44-callbacks-suppressed-mean-on-a-linux

> *“this "callbacks suppressed" message implies it suppressed a bulk of 44 syslog messages.* ***This is an attempt to avoid loading your syslog logging path.”***

TCPDump/packet sniffer related entries

promiscuous mode

```
Device eth0 entered promiscuous mode
kernel: device eth0 left promiscuous mode
```

From http://www.linuxquestions.org/questions/linux-security-4/kernel-device-eth0-entered-promiscuous-mode-756884/

“Promiscuous mode means a packet sniffer instructed your ethernet device to listen to all traffic. This can be a benign or a malicious act, but usually you will know if you run an application that provides you with traffic statistics (say ntop or vnstat) or an IDS (say Snort, Prelude, tcpdump or wireshark) or Something Else (say a DHCP
nt which isn't promiscuous mode but could be identified as one).

Kernel log entries associated wth the KTS driver unloading (likely due to loss of 10 MHz to KTS).

- pps pps0: tsyncpci PPS source unregistered
- Spectracom TSync Timing Board removed

Note: Refer to (**system.log entries (and MySQL database) in this document for more info on how the loss of 10 MHz from the oscillator can assert these entries due to its adverse affect on KTS.

PREEMPT (likely included in conjunction with “Call Trace” “oops”, “tainted”, “bug” entries)

- Refer also to “Preempt” in this document for more info.
- Preempt is a function that can optionally be enabled in a linux kernel. Our Engineers found references that this function being enabled can cause issues with the OS.
- Software update Version 5.4.0 disabled/turned-off preempt in the linux kernel as a potential fix to these various lockup/hanging issues/kernel log error messages.

Oops

- Example log below (This log was from a SecureSync that kept locking up- Robert Jelinek/Chris Johnston with PDT partners)

```
spadmin@setimex1 ~ $ dmesg|tail -40
[252021.702178] BUG: unable to handle kernel NULL pointer dereference at   (null)
[252021.702499] IP: [<c115d0d5>] __rb_insert_augmented+0x25/0x150
[252021.702748] *pde = 00000000
[252021.702839] Oops: 0000 [#1] PREEMPT
[252021.702971] Modules linked in: e1000e(O) e100 tsyncpci(O) pps_core 8139too
[252021.703024] Pid: 2753, comm: khtd Tainted: GO 3.8.13-gentoo #1    /AMD-GX3
```

Front panel Serial “Console” port is not responding.

SNMPD related entries

Example Kernel logs showing SNMPd crashed

- (refer to the SNMP section of this document for more info.   Note the exact info in the segfault entries may vary.

```
kernel: snmpd[3710]: segfault at 17 ip b76ad597 sp bfc49a30 error 4 in libnetsnmpagent.so.25.0.1[b768e000+67000]
kernel snmpd[1841]: segfault at 17 ip b7701597 sp bfd8d740 error 4 in libnetsnmpagent.so.25.0.1[b76e2000+67000]:
```

Review the kernel log (kern.log) in the log bundle for the following type entries that point to likely issues occurring with Eth0 (all of these entries were asserted on the same day at the same second). Dave Sohn agreed these indicate likely ETX issue.

```
Sep 30 21:38:21 ntp16 kernel: WARNING: at net/sched/sch_generic.c:254 dev_watchdog+0x204/0x210()
kernel: Hardware name:
kernel: NETDEV WATCHDOG: eth0 (e100): transmit queue 0 timed out
kernel: Modules linked in: e1000e(O) 8139too tsyncpci(O) e100 pps_core
kernel: Pid: 17577, comm: sudo Tainted: G           O 3.8.13-gentoo #1
kernel: Call Trace:
kernel:  [<c1029c1d>] warn_slowpath_common+0x6d/0xa0
kernel:  [<c1282914>] ? dev_watchdog+0x204/0x210
kernel:  [<c1282914>] ? dev_watchdog+0x204/0x210
kernel:  [<c1029cce>] warn_slowpath_fmt+0x2e/0x30
kernel:  [<c1282914>] dev_watchdog+0x204/0x210
kernel:  [<c1282710>] ? pfifo_fast_dequeue+0xe0/0xe0
kernel:  [<c10352bd>] call_timer_fn.isra.44+0x1d/0x80
kernel:  [<c10afd73>] ? __d_free+0x33/0x50
kernel:  [<c109ef83>] ? file_free_rcu+0x23/0x30
kernel:  [<c10354c6>] run_timer_softirq+0x1a6/0x1d0
kernel:  [<c1282710>] ? pfifo_fast_dequeue+0xe0/0xe0
kernel:  [<c103051f>] __do_softirq+0x7f/0x120
kernel:  [<c10304a0>] ? __tasklet_schedule+0x50/0x50
kernel:  <IRQ>  [<c10306d5>] ? irq_exit+0x65/0x70
kernel:  [<c1003ff3>] ? do_IRQ+0x43/0xb0
kernel:  [<c1072788>] ? find_get_page+0x58/0xb0
```

```
kernel:  [<c133242c>] ? common_interrupt+0x2c/0x31
kernel:  [<c132ec14>] ? __slab_alloc.isra.80.constprop.84+0x45f/0x47b
kernel:  [<c1089560>] ? __do_fault+0x270/0x410
kernel:  [<c1092747>] ? anon_vma_clone+0x47/0x140
kernel:  [<c10748f0>] ? __lock_page_or_retry+0xb0/0xb0
kernel:  [<c108b24f>] ? handle_pte_fault+0x6f/0x9a0
kernel:  [<c10998c1>] ? kmem_cache_alloc+0xb1/0xc0
kernel:  [<c1092747>] ? anon_vma_clone+0x47/0x140
kernel:  [<c1092747>] ? anon_vma_clone+0x47/0x140
kernel:  [<c108e411>] ? __split_vma.isra.36+0x71/0x130
kernel:  [<c108f2c5>] ? do_munmap+0x255/0x2c0
kernel:  [<c108f367>] ? vm_munmap+0x37/0x50
kernel:  [<c108feee>] ? sys_munmap+0xe/0x10
kernel:  [<c1331f7e>] ? sysenter_do_call+0x12/0x26
kernel: ---[ end trace 630f7c0201179bf3 ]---
kernel: e100 0000:00:06.0 eth0: NIC Link is Up 100 Mbps Full Duplex
```

"LM90" Register read failed log entries (temperature sensor)

- Associated with software versions 5.3.0 and above
- Fixed in update version 5.7.0 (June 2017). Changed the speed of a "SMBUS" monitoring bus on the ETX module.

```
Jun  1 23:21:30 s15u1clk kernel: i2c i2c-0: not master in state address (addr=0x99, len=1, status=0x41)
Jun  1 23:21:30 s15u1clk kernel: lm90 0-004c: Register 0x19 read failed (-5)
Jun  2 13:06:32 s15u1clk kernel: i2c i2c-0: not master in state address (addr=0x99, len=1, status=0x41)
Jun  2 13:06:32 s15u1clk kernel: lm90 0-004c: Register 0x5 read failed (-5)
Jun  6 11:06:33 s15u1clk kernel: i2c i2c-0: not master in state address (addr=0x99, len=1, status=0x41)
Jun  6 11:06:33 s15u1clk kernel: lm90 0-004c: Register 0x5 read failed (-5)
Jun  8 10:08:27 s15u1clk kernel: i2c i2c-0: not master in state address (addr=0x99, len=1, status=0x41)
Jun  8 10:08:27 s15u1clk kernel: lm90 0-004c: Register 0x5 read failed (-5)
Jun  8 10:37:27 s15u1clk kernel: i2c i2c-0: not master in state address (addr=0x99, len=1, status=0x40)
Jun  8 10:37:27 s15u1clk kernel: lm90 0-004c: Register 0x5 read failed (-5)
```

Per Paul Myers (20 Jun 16) **The LM90 I2C device is a I2C device driver temp sensor read. This is not uncommon failure in servers for reading I2C temp devices. I am assuming it is intermittent failure to read a temp sensor.**

Per Ron Dries (24 Sept 15) The lm90 logs have been seen before, I believe its related to reading the temperature from the ETX and CPU.

Kernel logging error "i2c i2c-0: not master in state address (addr=0x99, len=1, status=0x41)"

Example entry: Jun 2 13:06:32 s15u1clk kernel: i2c i2c-0: not master in state address (addr=0x99, len=1, status=0x41)

- Fixed in update version 5.7.0 (June 2017). Changed the speed of a "SMBUS" monitoring bus on the ETX module.

Potential Pipe software command issue (unofficially referred to as the "Verizon issue")

- Observed by Verizon Wireless and several others (Verizon Salesforce cases 17095 and 16898)
- Review the kernel log (kern.log) in the log bundle for the following type entries (especially "invoked oom-killer:" "segfault" "call trace" "bug", "inode","oops" and "tainted"   entries). Note: all of these entries below were asserted on the same day at the same second.
- Update version 5.2.1 (Apr 2015) updated the linux kernel from versions 3.17.7 to 3.18.11 as a potential fix to this kernel software issue.
- This likely software issue is causing browser and SSH to stop working and other functions to stop after kernel crashes occur (sometimes, other functions such as cron and oscillator logs don't

```
perfmond.sh invoked oom-killer: gfp_mask=0x201da, order=0, oom_score_adj=0
```

Note: “invoked oom-killer’ will indicate what was daemon invoked this linux function that is used to try to stop things to free up some memory, due to low memory being available. For example:

```
        kalarmd invoked oom-killer: gfp_mask=0x201da, order=0, oom_score_adj=0
        Apr  9 03:46:41 MEY-MNC02 kernel: CPU: 0 PID: 6149 Comm: kalarmd Tainted: G    B D    O   3.17.7-gentoo #1

        oom_kill_process+0x1be/0x320
        out_of_memory+0x256/0x290
```

This issue SHOULD be fixed in the version 5.2.1 update. (still being observed in 5.2.1)

Symptoms that may be observed when this condition occurs

Reboot commands may not work due to processes being hung up.
Web browser not accessible functioning
SNMP stops responding.
Serial console port not responding.
Ntpdate command and ntp synchronization of clients failing.
Front panel LCD/keypad not responsive.

Note: These words above are potential indications of the pipe software issues with at least v5.1.7 and below (5.1J is a beta for potential fix, with the same changes being added to v5.2.0 (Feb, 2015) as a potential fix.

```
        kernel: BUG: unable to handle kernel NULL pointer dereference at 00000028
        kernel: IP: [<00000028>] 0x27
        kernel: *pde = 00000000
        kernel: Oops: 0000 [#1] PREEMPT
        kernel: Modules linked in: e1000e(O) 8139too e100 tsyncpci(O) pps_core
        kernel: Pid: 8535, comm: sh Tainted: G           O 3.8.13-gentoo #1    /AMD-GX3
        kernel: EIP: 0060:[<00000028>] EFLAGS: 00010202 CPU: 0
        kernel: EIP is at 0x28
        kernel: EAX: d4d684d0 EBX: dbfaffb4 ECX: ded98820 EDX: 58deea96
        kernel: ESI: b752f9e0 EDI: c1021e50 EBP: dbfaffa4 ESP: dbfaff34
        kernel:  DS: 007b ES: 007b FS: 0000 GS: 0033 SS: 0068
        kernel: CR0: 8005003b CR2: 00000028 CR3: 1be71000 CR4: 00000090
        kernel: DR0: 00000000 DR1: 00000000 DR2: 00000000 DR3: 00000000
        kernel: DR6: ffff0ff0 DR7: 00000400
        kernel: Process sh (pid: 8535, ti=dbfae000 task=deea96c0 task.ti=dbfae000)
        kernel: Stack:
        kernel:  00000010 dbfaff48 deea96c0 ded98858 dbfaffb4 ded98820 00000028 00000004
        kernel:  dbfaff80 c109f0b6 00000001 00000000 00000000 d4c3f908 dec0d8d0 de8e8800
        kernel:  deea9960 deea96c0 00000000 dbfaff88 c109f228 dbfaff9c c10404a6 00000002
        kernel: Call Trace:
        kernel:  [<c109f0b6>] ? __fput+0x126/0x1f0
        kernel:  [<c109f228>] ? ____fput+0x8/0x10
        kernel:  [<c10404a6>] ? task_work_run+0x66/0xa0
        kernel:  [<c1021e50>] ? vmalloc_sync_all+0x150/0x150
        kernel:  [<c1021e58>] do_page_fault+0x8/0x10
        kernel:  [<c1331cdc>] error_code+0x58/0x60
        kernel:  [<c1021e50>] ? vmalloc_sync_all+0x150/0x150
        kernel: Code:  Bad EIP value.
        kernel: EIP: [<00000028>] 0x28 SS:ESP 0068:dbfaff34
        kernel: CR2: 0000000000000028
        kernel: ---[ end trace 36560a0db060e9c7 ]---
```

inode entries

Example entry “RC-GPSNTP01 kernel: ext3_orphan_cleanup: deleting unreferenced inode 9967”

Example from a unit that may have a bad ETX:

Note: all of these entries were asserted on the same day at the same second.

```
kernel: ext3_orphan_cleanup: deleting unreferenced inode 99679
kernel: ext3_orphan_cleanup: deleting unreferenced inode 99678
kernel: ext3_orphan_cleanup: deleting unreferenced inode 99677
kernel: ext3_orphan_cleanup: deleting unreferenced inode 99676
kernel: ext3_orphan_cleanup: deleting unreferenced inode 99675
kernel: EXT3-fs (hda1): 5 orphan inodes deleted
```

Segfaults in Kernel log / SNMPd crash

- Segfaults are BAD
- Segfault errors asserted in kernel log-kern.log when SNMPd crashes.
- Refer to the SNMP troubleshooting section in this document.
- Refer to Mantis case 2995.
- Oleg applied a patch to SNMP in update version 5.2.1 to resolve this intermittent crashing.

Examples of segfaults related to SNMPS and SNMPSAD

```
kernel: snmpsad[3407]: segfault at 37613038 ip b7575cb8 sp bff470f0 error 4 in libnetsnmp.so.25.0.1[b750e000+ae000]
kernel: snmpd[1892]: segfault at 2774388b ip b74c4032 sp bfb4cd60 error 4 in libnetsnmp.so.25.0.1[b7488000+ae000]
```

Note: these particular SNMP segfaults were observed in software version prior to 5.2.0. If this type of entry is observed in the kernel log, update to v5.2.1 or higher. 5.2.1and above applied a patch update to Net-SNMP that is likely to prevent SNMPd from crashing when walking the mibs.

mail.log (Mail log entries)

- This system log is not accessible from the browser. But it's in the Save Logs bundle.
- This log is not wiped when performing a "clear all logs" in the browser
- This log is not viewable from the web browser (can FTP it out as a single log, bundle it with all of the logs or view it with telnet/ssh)

manifest.log file /manifest.config file

Note the manifest log is not listed in the **Tools** drop-down, like other Spectracom logs.
Description (from Engineering Release Notes) Added a SecureSync/Netclock 94XX Manifest file in /home/spectracom/config/manifest.conf and a Manifest Log in /home/spectracom/log/manifest.log. The config file contains the current software/fpga/firmware versions, option cards and licenses installed. The Log shows these as they change at each reboot.

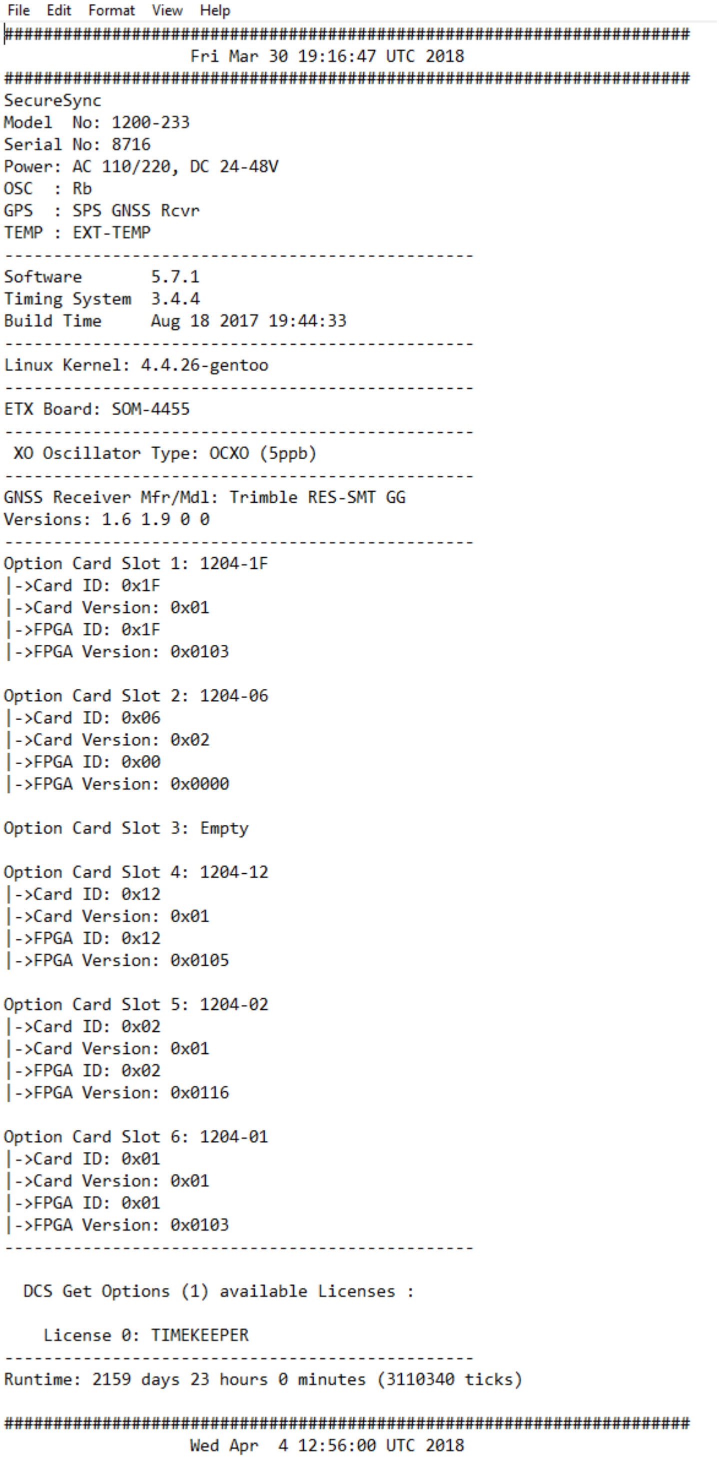
File storate locations:

- **manifest.conf** file is located in the **/home/spectracom/config/** directory
- **manifest.log** file is located in the **/home/spectracom/log/** directory

command to display the entire manifest.log in cli interface (v5.7.1 and above only)

5. Type: **manifest** <enter>

Example manifest log entry:



```
######################################################################
                   Fri Mar 30 19:16:47 UTC 2018
######################################################################
SecureSync
Model  No: 1200-233
Serial No: 8716
Power: AC 110/220, DC 24-48V
OSC   : Rb
GPS   : SPS GNSS Rcvr
TEMP : EXT-TEMP
------------------------------------------------
Software       5.7.1
Timing System  3.4.4
Build Time     Aug 18 2017 19:44:33
------------------------------------------------
Linux Kernel: 4.4.26-gentoo
------------------------------------------------
ETX Board: SOM-4455
------------------------------------------------
 XO Oscillator Type: OCXO (5ppb)
------------------------------------------------
GNSS Receiver Mfr/Mdl: Trimble RES-SMT GG
Versions: 1.6 1.9 0 0
------------------------------------------------
Option Card Slot 1: 1204-1F
|->Card ID: 0x1F
|->Card Version: 0x01
|->FPGA ID: 0x1F
|->FPGA Version: 0x0103

Option Card Slot 2: 1204-06
|->Card ID: 0x06
|->Card Version: 0x02
|->FPGA ID: 0x00
|->FPGA Version: 0x0000

Option Card Slot 3: Empty

Option Card Slot 4: 1204-12
|->Card ID: 0x12
|->Card Version: 0x01
|->FPGA ID: 0x12
|->FPGA Version: 0x0105

Option Card Slot 5: 1204-02
|->Card ID: 0x02
|->Card Version: 0x01
|->FPGA ID: 0x02
|->FPGA Version: 0x0116

Option Card Slot 6: 1204-01
|->Card ID: 0x01
|->Card Version: 0x01
|->FPGA ID: 0x01
|->FPGA Version: 0x0103
------------------------------------------------

  DCS Get Options (1) available Licenses :

    License 0: TIMEKEEPER
------------------------------------------------
Runtime: 2159 days 23 hours 0 minutes (3110340 ticks)

######################################################################
                   Wed Apr  4 12:56:00 UTC 2018
```

mysql_create.log (MySQL log entries)

- This is a MySQL log included in the log bundle (not displayed in the browser)
- This log is not accessible from the browser. But it’s in the Save Logs bundle.
- This log is not wiped when performing a “clear all logs” in the browser
- This log is not viewable from the web browser (can FTP it out as a single log, bundle it with all of the logs or view it with telnet/ssh).

“cake” (cakePHP): associated with MySQL entries (CakePHP is used to build web applications)

```
Clear MySQL history
fixing permissions
start mysql-safe in no-write mode so we can administer it no matter what the password is
150210 20:38:23 mysqld_safe Logging to '/var/log/mysql/mysqld.err'.
150210 20:38:24 mysqld_safe Starting mysqld daemon with databases from /srv/mysql
checking if lafayette database exists
result = "lafayette" if its lafayette create db and tables
Shutting down mysql_safe
150210 20:38:25 mysqld_safe mysqld from pid file /var/run/mysqld/mysqld.pid ended
restarting mysql-safe in writing mode
150210 20:38:37 mysqld_safe Logging to '/var/log/mysql/mysqld.err'.
150210 20:38:37 mysqld_safe Starting mysqld daemon with databases from /srv/mysql
Some tables exist
checking if there is mysqlstrings file
Running schema update

Welcome to CakePHP v2.3.0 Console
---------------------------------------------------------------
App : app
Path: /srv/www2/app/
---------------------------------------------------------------
Cake Schema Shell
---------------------------------------------------------------
Comparing Database to Schema...

The following statements will run.
ALTER TABLE `lafayette`.`feature_configs`
        CHANGE `feature_id` `feature_id` varchar(12) NOT NULL,
        CHANGE `local_clock_id` `local_clock_id` int(4) NOT NULL;
ALTER TABLE `lafayette`.`log_sys_mons`
        CHANGE `load01` `load01` float DEFAULT 0 NOT NULL,
        CHANGE `load02` `load02` float DEFAULT 0 NOT NULL,
        CHANGE `load03` `load03` float DEFAULT 0 NOT NULL,
        CHANGE `mem_total` `mem_total` int(11) DEFAULT 0 NOT NULL,
        CHANGE `mem_free` `mem_free` int(11) DEFAULT 0 NOT NULL,
        CHANGE `disk_used` `disk_used` int(11) DEFAULT 0 NOT NULL;
ALTER TABLE `lafayette`.`log_gps_statuses`
        CHANGE `avg_tracked_snr` `avg_tracked_snr` int(11) DEFAULT 0 NOT NULL,
        CHANGE `max_tracked_snr` `max_tracked_snr` int(11) DEFAULT 0 NOT NULL,
        CHANGE `min_tracked_snr` `min_tracked_snr` int(11) DEFAULT 0 NOT NULL;
ALTER TABLE `lafayette`.`notification_emails`
        CHANGE `address` `address` varchar(254) NOT NULL;
ALTER TABLE `lafayette`.`ethernet_logs`
        CHANGE `rx_bytes` `rx_bytes` int(11) DEFAULT 0 NOT NULL,
        CHANGE `tx_bytes` `tx_bytes` int(11) DEFAULT 0 NOT NULL,
        CHANGE `rx_bytes_per_second` `rx_bytes_per_second` int(11) DEFAULT 0 NOT NULL,
        CHANGE `tx_bytes_per_second` `tx_bytes_per_second` int(11) DEFAULT 0 NOT NULL;
ALTER TABLE `lafayette`.`remote_servers`
        CHANGE `host` `host` varchar(255) NOT NULL;
ALTER TABLE `lafayette`.`preferences`
        CHANGE `type` `type` int(4) DEFAULT 0 NOT NULL,
        CHANGE `local_time` `local_time` tinyint(1) DEFAULT '1',
    CHANGE `registration_reminder` `registration_reminder` tinyint(1) DEFAULT '1';
Are you sure you want to alter the tables? (y/n)
[n] >
Updating Database...
feature_configs updated.
log_sys_mons updated.
log_gps_statuses updated.
notification_emails updated.
ethernet_logs updated.
remote_servers updated.
preferences updated.
End update.
Shutdown mysql_safe
150210 20:38:42 mysqld_safe mysqld from pid file /var/run/mysqld/mysqld.pid ended
```

NTP.log entries (NTP Log entries)

- NTP logs are stored in the NTP System Log.   Refer to: http://www.eecis.udel.edu/~mills/ntp/html/msyslog.html for a description of several log entries that may be asserted in this log

Version 4.2.8 logs (software version 5.2.1 and above)

A) NTP startup

```
Sep  4 17:07:03 Spectracom ntpd[16050]: ntpd 4.2.8p3@1.3265-o Tue Aug 11 16:01:10 UTC 2015 (1): Starting
Sep  4 17:07:03 Spectracom ntpd[16050]: Command line: /usr/sbin/ntpd -p /var/run/ntpd.pid -g -c /etc/ntp/ntp.conf
Sep  4 17:07:03 Spectracom ntpd[16052]: proto: precision = 3.108 usec (-18)
Sep  4 17:07:03 Spectracom ntpd[16052]: Listen and drop on 0 v6wildcard [::]:123
Sep  4 17:07:03 Spectracom ntpd[16052]: Listen and drop on 1 v4wildcard 0.0.0.0:123
Sep  4 17:07:03 Spectracom ntpd[16052]: Listen normally on 2 lo 127.0.0.1:123
Sep  4 17:07:03 Spectracom ntpd[16052]: Listen normally on 3 eth0 10.2.100.176:123
Sep  4 17:07:03 Spectracom ntpd[16052]: Listen normally on 4 eth1 10.2.100.27:123
Sep  4 17:07:03 Spectracom ntpd[16052]: Listen normally on 5 lo [::1]:123
Sep  4 17:07:03 Spectracom ntpd[16052]: Listen normally on 6 eth0 [fe80::2d0:c9ff:feba:ebc9%5]:123
Sep  4 17:07:03 Spectracom ntpd[16052]: Listen normally on 7 eth1 [fe80::20c:ecff:fe05:44e%6]:123
Sep  4 17:07:03 Spectracom ntpd[16052]: Listening on routing socket on fd #24 for interface updates
Sep  4 17:07:03 Spectracom ntpd[16052]: PCI_TSYNC(0) 8011 81 mobilize assoc 24673
Sep  4 17:07:03 Spectracom ntpd[16052]: PPS(0) 8011 81 mobilize assoc 24674
Sep  4 17:07:03 Spectracom ntpd[16052]: 10.2.100.177 8011 81 mobilize assoc 24675
Sep  4 17:07:03 Spectracom ntpd[16052]: 0.0.0.0 c01d 0d kern kernel time sync enabled
Sep  4 17:07:03 Spectracom ntpd[16052]: 0.0.0.0 c012 02 freq_set kernel -79.685 PPM
Sep  4 17:07:03 Spectracom ntpd[16052]: 0.0.0.0 c016 06 restart
Sep  4 17:07:04 Spectracom ntpd[16052]: PCI_TSYNC(0) 8024 84 reachable
Sep  4 17:07:04 Spectracom ntpd[16052]: PCI_TSYNC(0) 903a 8a sys_peer
Sep  4 17:07:04 Spectracom ntpd[16052]: 0.0.0.0 c415 05 clock_sync
Sep  4 17:07:05 Spectracom ntpd[16052]: PPS(0) 8024 84 reachable
Sep  4 17:07:05 Spectracom ntpd[16052]: PPS(0) 903a 8a sys_peer
Sep  4 17:07:06 Spectracom ntpd[16052]: 10.2.100.177 8024 84 reachable
Sep  4 17:07:03 Spectracom ntpd[16050]: ntpd 4.2.8p3@1.3265-o Tue Aug 11 16:01:10 UTC 2015 (1): Starting
Sep  4 17:07:03 Spectracom ntpd[16050]: Command line: /usr/sbin/ntpd -p /var/rSep  4 17:07:30 Spectracom ntpd[16052]: ::1
config: fudge 127.127.22.0 refid GPS
```

B) NTP statistics logging (Client and server NTP packets per second)

- Added this new NTP loading feature in software update version 5.2.1 (Apr 2015) as part of NTP v4.2.8 upgrade
- Provides NTP throughput / NTP loading
- Entries are asserted into the NTP.log (NTP Log)
  - **Example log entry (with no clients): NTP statistics: Clients = 0.000 pkt/s, Servers/Peers = 0.000 pkt/s**
  - **Example log entry (with just a couple clients) NTP statistics: Clients = 0.037 pkt/s, Servers/Peers = 0.000 pkt/s**

Note: pkt/s is reported in Mbps (Megabits/sec). So 0.140 pkt/s is 1400 packets per second ???

Where:

- **Clients**: NTP requests from NTP clients on the network
- **Servers/Peers:** NTP requests from Servers or Peers configured to get time from this SecureSync

1. To convert pkt/s (values in the graphs/logs) to the actual number of packets in the hour

Multiply the number of pkt/s (value in the graphs/logs) times 60 and then round-up to nearest whole number

Examples:

0.017 pkt/s = 1 packet in one hour

0.083 pkt/s = 5 packets in one hour

0.167 pkt/s = 10 packets in one hour

1.667 pkt/s = 100 packets in one hour

166.667 pkt/s = **10,000** packets in one hour

3000 pkt/s = 180,000 packets in one hour

2. To convert actual number of packets per hour to pkt/s (values in the graphs/logs)

Divide the number of ntp packets in the hour by 60 (there are 60 minutes in the report period)

Examples:

1 packet in one hour = **0.017 pkt/s**

5 packets in one hour = **0.083 pkt/s**

10 packets in one hour = **0.167 pkt/s**

100 packets in one hour = **1.667 pkt/s**

10,000 packets in one hour = **166.667 pkt/s**

180,000 packets in one hour = **3000 pkt/s**

C) NTP on-the-fly config changes

```
::1 config: fudge 127.127.22.0 refid GPS
 ::1 config: fudge 127.127.22.0 refid PPS
```

- These entries are only present if the PPS Atom Clock driver is enabled
- Indicate the Atom clock driver is fudging the value of what it’s synced with (its synced to GPS, PPS, etc)

```
10.2.100.177 local addr 10.2.100.176 ->

10.2.100.58 local addr 10.2.100.176 ->
```

- These entries indicate peers have been added to the ntp.conf file.

D) NTP state change

```
ntpd 4.2.8p2@1.3265-o Tue Apr 21 15:01:53 UTC 2015 (1): Starting
ntpd exiting on signal 15 (Terminated)
Listen and drop on 1 v4wildcard 0.0.0.0:123
```

E) KoD (Kiss of Death) packet

- refer to (in this document): Kiss of Death packets (KOD) for SecureSync/9400s

```
example KoD packet from a customer log bundle (v5.7.1)
  Jul  9 07:53:45 amrcl1101 ntpd[23494]: receive: Drop 0 origin timestamp from sym_active@10.115.218.53 xmt
```

```
0xdeed930c.842f2072
Jul  9 07:54:12 amrcl1101 ntpd[23494]: receive: KoD packet from 10.115.218.53 has a zero org or rec timestamp.  Ignoring.
```

F) A Peer/Server unreachable or is toggling back-forth between reachable and unreachable

```
example of toggling between reachable and unreachable
Jul  9 06:32:55 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
Jul  9 06:33:02 amrcl1101 ntpd[23494]: 10.210.96.25 8314 84 reachable
Jul  9 06:33:59 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
Jul  9 06:34:05 amrcl1101 ntpd[23494]: 10.210.96.25 8314 84 reachable
Jul  9 06:35:03 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
Jul  9 06:35:09 amrcl1101 ntpd[23494]: 10.210.96.25 8314 84 reachable
Jul  9 06:36:07 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
Jul  9 06:36:15 amrcl1101 ntpd[23494]: 10.210.96.25 8314 84 reachable
Jul  9 06:37:12 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
Jul  9 06:37:18 amrcl1101 ntpd[23494]: 10.210.96.25 8014 84 reachable
Jul  9 06:38:16 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
Jul  9 06:38:21 amrcl1101 ntpd[23494]: 10.210.96.25 8314 84 reachable
Jul  9 06:39:20 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
Jul  9 06:39:24 amrcl1101 ntpd[23494]: 10.210.96.25 8314 84 reachable
Jul  9 06:40:24 amrcl1101 ntpd[23494]: 10.210.96.25 8313 83 unreachable
```

potential solutions/tests to perform

1. make sure all switch ports that SecureSync is connected to are set to auto-negotiate (v5.7.1 and below) or match the hard-coded settings in the SecureSync (5.8.0 and above only).
2. Periodically perform the following CLI commmad via telnet/ssh connection: **tracepath -p 123 xxx.xxx.xxx** (where x is the IP address or hostname of the peer/server which is unreachable. See if the SecureSync is always able to reach the peer or server.

G) Other ntp.log entries

(STATUSD errors) (such as extended status polling)

General response email from Keith (20 Nov 17) for statusd "extended status polling" error messages in the NTP log

For your information and better understanding, "statusd" is a process used to continually obtain NTP status information via NTP's NTPQ query tool. Examples of this current status info includes NTP's current NTP Stratum value, offset values, info on its NTP peers, etc. This information obtained from NTP via the NTPQ query is then provided via various SecureSync outputs- such as via SNMP, the SecureSync's web browser, its front panel LCD (if its configured to display NTP status, etc).

The log entries you observed just indicate that NTPQ was busy when it was queried, so it wasn't able to respond with NTP's status at that particular moment. The statusd program continued asking NTPQ for this status data (as it always does, to have the most recent status info available from NTP) and once NTPQ was available again to provide the status data to the rest of the system, it provided it and the log entries indicating that it was previously too busy to respond, stopped being asserted.

In summary: seeing these NTP log entries periodically asserted is not an indication of a problem with the SecureSync or its NTP functionality! They just indicate NTPQ (not NTP) was just too busy at a particular moment to be able to provide NTP status info

1) "NTP extended status polling…" combined with "Type mismatch"

- Refer to Salesforce cases 117236 and 121454

```
[system] ERROR! ERROR!!!! NTP extended status polling: Type mismatch. Expected: 3, Actual: 0
/usr/src/spectracom/easycpp/src/EasyCpp/Settings/Variant.cpp, 110, void
Easy::Settings::Variant::CheckThatTypeIs(Easy::Settings::Variant::enuType) const (STATUSD)
```

Likely causes:

1) NTPQ was just momentarily busy and couldn’t respond

Email from Paul Myers (20 Nov 19) I believe we cannot momentarily communicate with NTP successfully. It is an intermittent error condition. It can or errors like it can occur when NTP is restarting. The NTP extended status polling is the error source. I dig down into the actual 3 versus 0 value enum.

```
4 Nov 07 13:22:19 [system] ERROR! ERROR!!!! NTP extended status polling: Type mismatch. Expected: 3, Actual:
0 /usr/src/spectracom/easycpp/src/EasyCpp/Settings/Variant.cpp, 110, void
Easy::Settings::Variant::CheckThatTypeIs(Easy::Settings::Variant::enuType) const (STATUSD)
```

2) Kernel lock-up issues: with at least case 117236, these NTP entries were also accompanied by kernel errors of bug/oops/call trace type entries (with version 5.7.1 sotware installed)

2) “extended status polling: Ntpq error” combined with entry [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)

- Refer to Salesforce cases such as 117690

```
[system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
```

(6 Sept 17 KW) Paul M responded w/info and my response to customer below:
Regarding your inquiry pertaining to the two SecureSync log entries, I found out these logs entries are tied to each other and are associated with the process used to obtain status information from NTP (via the “ntpq” query tool). This status info includes items such as NTP’s sync status and current stratum value, info about its NTP peers, etc.

These two log entries are messages asserted when ntpq can’t temporarily communicate with NTP to obtain its most current status data. These entries are likely to be seen when NTP had just been just restarted (or NTP hasn’t yet started-up after a reboot/power cycle of the SecureSync (NTP isn’t fully running yet when ntpq requests the status data).

These two linked entries are not something to be alarmed about. The ntpq query will once again start obtaining the NTP status data that its requesting from NTP once NTP is again able to communicate with ntpq.

1. Popcorn spike **ntpd[4639]: 74.123.28.4 942d 8d popcorn 0.000040 s**

- Apparently can just be just a logging bug (https://tools.cisco.com/quickview/bug/CSCug48022)
- “Popcorn” is part of the Clock Filter algorithm
  - from http://tools.ietf.org/html/draft-ietf-ntp-ntpv4-algorithms-01

    “A 'popcorn spike' is a transient outlier, usually only a single sample, that is typical of congested Internet paths. The popcorn spike suppressor is designed to detect and remove them. Let theta_prime be the peer offset determined by the previous message and psi the current peer jitter. If |theta - theta_prime| > (K_s * psi), where K_s is a tuning parameter that defaults to 3, the sample is a popcorn spike and is discarded.”

2. sys_peer

140.142.16.34 941a 8a sys_peer (where the numbers at the beginning are an IP address)

Refer to sites such as: http://osdir.com/ml/comp.protocols.time.ntp/2011-05/msg00022.html

- Appears this is an abbreviated entry (starting in NTP v4.2.6 and above) to indicate a new peer has been selected for sync. The stratum value of the peer is no longer reported (like it was in earlier versions of NTP). In the log entry above, NTP is now synced with 140.142.16.34.

3. no_sys_peer

- Appears this is an abbreviated entry (started in 4.2.6 and above) to indicate a peer has been lost. Stratum value of the peer is no longer reported. In the log entry below, NTP is no longer synced to any peer

```
ntpd[5186]: 0.0.0.0 c618 08 no_sys_peer
0.0.0.0 c614 04 freq_mo
```

4. Frequency error xxx.xxx.xxx.xxx PPM exceeds tolerance 500 PPM

The max tolerance is set in <ntp-source-tree>/include/ntp_proto.h by
#define NTP_MAXFREQ 500e-6c (Note: customers don't have permissions to edit the limit of 500 PPM)

5. Ipv6 error entries present, even though IPv6 isn't configured

```
20 Jun 15:53:17 ntpd[2016]: bind(22) AF_INET6 fe80::2d0:c9ff:feed:5262%5#123 flags 0x11 failed: Cannot assign requested address
20 Jun 15:53:17 ntpd[2016]: unable to create socket on eth0 (9) for fe80::2d0:c9ff:feed:5262%5#123
20 Jun 15:53:17 ntpd[2016]: failed to init interface for address fe80::2d0:c9ff:feed:5262%5
20 Jun 15:58:17 ntpd[2016]: bind(22) AF_INET6 fe80::2d0:c9ff:feed:5262%5#123 flags 0x11 failed: Cannot assign requested address
20 Jun 15:58:17 ntpd[2016]: unable to create socket on eth0 (10) for fe80::2d0:c9ff:feed:5262%5#123
20 Jun 15:58:17 ntpd[2016]: failed to init interface for address fe80::2d0:c9ff:feed:5262%5
20 Jun 16:03:17 ntpd[2016]: bind(22) AF_INET6 fe80::2d0:c9ff:feed:5262%5#123 flags 0x11 failed: Cannot assign requested address
20 Jun 16:03:17 ntpd[2016]: unable to create socket on eth0 (11) for fe80::2d0:c9ff:feed:5262%5#123
20 Jun 16:03:17 ntpd[2016]: failed to init interface for address fe80::2d0:c9ff:feed:5262%5
20 Jun 16:08:17 ntpd[2016]: bind(22) AF_INET6 fe80::2d0:c9ff:feed:5262%5#123 flags 0x11 failed: Cannot assign requested address
20 Jun 16:08:17 ntpd[2016]: unable to create socket on eth0 (12) for fe80::2d0:c9ff:feed:5262%5#123
20 Jun 16:08:17 ntpd[2016]: failed to init interface for address fe80::2d0:c9ff:feed:5262%5
20 Jun 16:13:17 ntpd[2016]: bind(22) AF_INET6 fe80::2d0:c9ff:feed:5262%5#123 flags 0x11 failed: Cannot assign requested address
20 Jun 16:13:17 ntpd[2016]: unable to create socket on eth0 (13) for fe80::2d0:c9ff:feed:5262%5#123
20 Jun 16:13:17 ntpd[2016]: failed to init interface for address fe80::2d0:c9ff:feed:5262%5
```

- Appears to be associated with the Ethernet port (eth0) supporting both IPv4 and IPv6, and NTP is not being forced to using only IPv4.
- Refer to sites such as http://www.linuxquestions.org/questions/linux-server-73/getting-ipv6-errors-in-ntp-4175525840/ and Https://bugs.launchpad.net/ubuntu/+source/ntp/+bug/700492

6. Unexpected origin timestamp xxxxx.xxxxx does not match aorg 00000.00000 from xx

Example entries

```
Jul 12 15:04:28 ndcntp201 ntpd[2035]: receive: Unexpected origin timestamp 0xdb2a06ab.321416e8 from 172.18.33.227 xmt 0xdb2f857c.349efd85
Jul 12 15:22:34 ndcntp201 ntpd[2035]: receive: Unexpected origin timestamp 0xdb2a06ab.321416e8 from 172.18.33.227 xmt 0xdb2f89ba.349ec968
Jul 12 15:40:11 ndcntp201 ntpd[2035]: receive: Unexpected origin timestamp 0xdb2a06ab.321416e8 from 172.18.33.227 xmt 0xdb2f8ddb.34a0dfa1
```

- This is a bug in NTP- Reportedly fixed in NTP v4.2.8p7 (SecureSync versions 5.4.4 and below are susceptible. We are expecting to update to 4.2.8p7 in v5.4.5) For more info on this NTP bug, refer to http://bugs.ntp.org/show_bug.cgi?id=2952.
- Appears to cause intermittent loss of communications (NTP timestamps between peers), intermittent loss of time stamps from a peer and so the Peer(s) Reach value goes to 0.
- Refer to sites such as: https://www.suse.com/support/kb/doc?id=7017645 (info pasted below)

Situation

Having peer servers configured as part of the NTP configuration, the following messages are logged in "/var/log/ntp":

ntpd[xxxx] receive: Unexpected origin timestamp xxxxx.xxxxx does not match aorg 00000.00000 from xx (Where xx at the end of the message is the IP address of the configured peer server). Eventually this results in communication failure between the configured servers.

Resolution

Update NTP to version 4.2.8p7 or above (SecureSync versions 5.4.4 and below are susceptible. We are expecting to update to 4.2.8p8 in v5.4.5)

Cause

This was caused by changes made to bogus packet detection of NTP. Although the messages are still logged with the current latest NTP version, communication is not lost anymore and the messages can be ignored.

NTP Version 4.2.6 and 4.2.0 logs (software versions 5.2.0 and below)

clock PCI_TSYNC(0) event 'clk_fault' (0x03):

- NTP is no longer synced to the System Time (GPS, IRIG, Stanag, NTP, etc).

Deleting interface #3 eth0, 10.2.100.89#123, interface stats: received=0, sent=7, dropped=0, active_time=103 secs

- This log entry indicates a recent power cycle is resetting/restarting the Ethernet ports (note the values after “Deleting interface” will inherently vary)

127.127.1.0 interface 127.0.0.1 -> (none)

- This entry is applicable to versions 5.0.0 and above (not applicable in versions 4.8.9 and below)
- This entry is associated with the Local clock reference no longer being used to go to Stratum 16 (like it previously was in versions 4.8.9 and below).
- When we went to NTP version 4.2.6 in 5.0.0 and above, we changed how we force NTP to go to Stratum 16. Now, the local clock reference is not used.

Synchronized to PPS(0), stratum=0:

- The Atom clock (PPS) driver provides NTP with a 1pps input that it can discipline with, after NTP has synced to a time reference (such as GPS, for instance). Several minutes after NTP has synced, this NTP log entry will be asserted.

frequency error xxx PPM exceeds tolerance (the xxx value will vary):

- a very large time jump of NTP’s selected input reference has occurred. The System Time may have been manually changed, while NTP was syncing to it, for example.

kernel time sync disabled 0041:

- From link above: “The kernel reports an error.”
- ntpd doesn't sync kernel time anymore.

kernel time sync enabled 0001:

- ntpd is back to syncing kernel time.

no servers reachable**:**

- Local Clock reference has been **DISABLED** (in the ***Network*** -> ***NTP Setup*** page of the browser, **NTP Servers** tab) and NTP has NO input references to select for its sync. NTP will **NOT** be able to go to Stratum 16, even with no inputs present. NTP clients won’t ignore the NTP time stamps (time stamps won’t report Stratum 0).

ntpd exiting on signal 15:

- NTP was disabled in the web browser by a user.
- NTP was automatically restarted after configuration change made to NTP (software versions 5.0.0 and above).
- NTP was restarted by the watchdog (ntpmond) because of a large time change.
- Also appears this entry is asserted upon a reboot of the time server.

[system] KTS Host Time Daemon has restarted
Indicates KHTD was restarted

- **Note**: KHTD is our KTS Host Time Daemon. It is responsible for NTP time sets to KTS when operating in Stratum 2, and for setting kernel time when NTP is not running

pps sync disabled**:**

- The Atom clock driver’s 1PPS input has died (no longer present in NTP).

peers refreshed:

synchronized to PCI_TSYNC(0), stratum=0:

- NTP synced to the System Time (GPS, IRIG, Stanag, NTP, etc). NTP is reporting its Stratum 1.

Note: If this NTP log entry is never being asserted, System Time may never be synced. Also, make sure the “**Timing System Reference** ” field is “Enabled” in the ***Network***-> ***NTP setup*** page, “**NTP Servers”** tab, when system Time is an input to NTP (typically, it should only be “Disabled” if NTP is only syncing to other NTP servers and there is no desire to allow NTP to have any holdover capability). If this field is disabled, NTP won’t have System Time listed in the Status-> NTP page as an available reference that it can sync with.

Indicates NTP in the SecureSync synced to “System Time” (which is synced to manually set time, GPS, IRIG input , have quick input etc – but not NTP). This entry indicates NTP in the SecureSync is now Stratum 1. This entry indicates NTP is not currently synced to another NTP time server. It also indicates NTP clients getting NTP time from the SecureSync won’t reject the timestamps (as NTP clients often do, when SecureSync is at Stratum 16.

synchronized to LOCAL(0), stratum=15:

- NTP has selected the local clock reference, either because no other input is available, or NTP has decided the local reference is better than a single other input reference. NTP is Stratum 16 (NTP time stamps report

Stratum 0)

Note: This entry is applicable only to software versions 4.8.9 and below (NTPv4.2.0)

Indicates NTP in the SecureSync is no longer synced to "System Time" (manually set time, GPS, IRIG input, have quick input etc) and is not synced to any other NTP servers either. This entry means SecureSync is reporting to NTP clients that NTP is now "Stratum 16", resulting in NTP clients rejecting the NTP time stamps they are receiving from this SecureSync.

Notes about this "Local(0)" log entry:

1) If there are alternating NTP log entries of **"synchronized to Local(0) …"** and **"synchronized to PCI_TSync(0)…"** Make sure the "**Preferred**" checkbox is enabled in the **Network**-> **NTP setup** page, "**NTP Servers"** tab, when System Time (GPS, user set time, Stanag, etc) is an available input to NTP (typically, it should only be unchecked if NTP is only syncing to other NTP servers and there is no desire to allow NTP to have any holdover capability). This is rare.

2) If there are **"synchronized to Local(0)…"** log entries with no **"synchronized to PCI_TSync(0)…"** log entries, make sure the "**Timing System Reference** " field is "Enabled" in the **Network**-> **NTP setup** page, "**NTP Servers"** tab, when system Time is an input to NTP (typically, it should only be "Disabled" if NTP is only syncing to other NTP servers and there is no desire to allow NTP to have any holdover capability). This is rare.

time correction of 304925641 seconds exceeds sanity limit (1000); set clock manually to the correct UTC time: (note the number of seconds in the entry will vary):

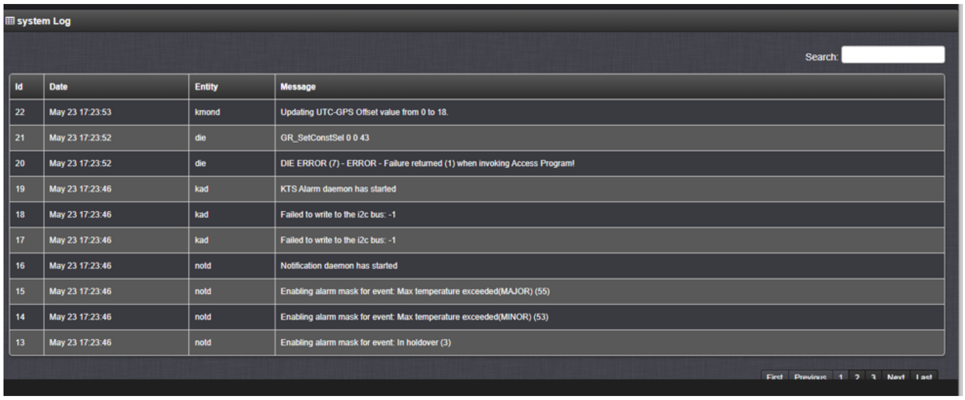
- The System Time's date/time was changed by this amount of seconds, while NTP was selected to sync to the System Time. This log entry is likely due to a user manually changing the year, date or time while NTP is syncing to System Time.

Note: Review the Journal log to see if there are any corresponding "**Set Time for User Reference 0 in slot 0**" entries, which indicate a user had manually changed System Time (this journal entry also indicates if System Time was changed via the browser or by the front panel keypad).

system.log entries

“failed to write to the i2c bus:-1” and “**DIE Error (7) - ERROR - Failure returned (1) when invoking Access Program”**

- Refer to Salesforce Case 300361 and JIRA ticket CAR-2467 (May 2023)
- Both these System log entries were first observed/reported in 2400 SecureSync v1.6.0 (see provided screenshot below)
  - Both appear to have been asserted shortly after initial power-up



Id	Date	Entity	Message
22	May 23 17:23:53	kmond	Updating UTC-GPS Offset value from 0 to 18.
21	May 23 17:23:52	die	GR_SetConstSel 0 0 43
20	May 23 17:23:52	die	DIE ERROR (7) - ERROR - Failure returned (1) when invoking Access Program!
19	May 23 17:23:46	kad	KTS Alarm daemon has started
18	May 23 17:23:46	kad	Failed to write to the i2c bus: -1
17	May 23 17:23:46	kad	Failed to write to the i2c bus: -1
16	May 23 17:23:46	notd	Notification daemon has started
15	May 23 17:23:46	notd	Enabling alarm mask for event: Max temperature exceeded(MAJOR) (55)
14	May 23 17:23:46	notd	Enabling alarm mask for event: Max temperature exceeded(MINOR) (53)
13	May 23 17:23:46	notd	Enabling alarm mask for event: In holdover (3)

**Troubleshooting “Out of memory / Killed process” entries in System Log (carry over from 1200 doc)

```
kernel: Out of memory: Kill process 5311 (mysqld) score 149 or sacrifice child
Aug 17 19:43:40 CSSknMUSalphb01 kernel: Killed process 5311 (mysqld) total-vm:105060kB, anon-rss:72416kB, file-rss:2900kB

Aug 9 23:31:58 CSSknEUKlinhb02 kernel: Out of memory: Kill process 3309 (mysqld) score 148 or sacrifice child
Aug 9 23:31:58 CSSknEUKlinhb02 kernel: Killed process 3309 (mysqld) total-vm:104840kB, anon-rss:72076kB, file-rss:2996kB
```

Notes:

- Per Oleg- This issue is not likely to cause the browser/ssh to stop responding- just loss of NTP status info.
- Typically associated with lots of open NTPQ requests in versions 5.2.1 and below.
- The specific text in the log entries will vary, depending on specific conditions of this event. Two different sets below)
- The condition associated with these entries can cause loss of web browser and ssh until power cycle, as the ones below resulted in (refer to Salesforce case 18972 for details).
- Upgrade version 5.3.0 (Sept 2015) is expected to fix this condition (this note is prior to 5.3.0 being fielded, so “time will tell” if this condition is prevented in this new version).
- The new daemon added in version 5.3.0 that is controlling the NTPQ requests was initially called masterd but was renamed shortly thereafter as statusd

Steps to diagnose/fix

1) Recommend software update to at least version 5.3.0
2) If still occurs in 5.3.0 (or above): Per Ron Dries earlier recommendations, get both the unit’s logs and config files. Review the System log to find out what the Out Of Memory Manager was trying to kill when the log entry was asserted.

Management -> Notifications page of the browser associated System log entries

- In at least version 5.4.1, submitting any changes in the Management -> Notifications page of the browser will result in the following group of log entries being asserted in the System log (daemons are restarted when changes are submitted)

```
Apr  4 21:43:22 CustService176 CustService176: [system] Notification daemon has restarted (NOTD)
Apr  4 21:43:22 CustService176 CustService176: [system] Enabling alarm mask for event: 53 (NOTD)
Apr  4 21:43:22 CustService176 CustService176: [system] Enabling alarm mask for event: 2 (NOTD)
Apr  4 21:43:22 CustService176 CustService176: [system] Enabling alarm mask for event: 55 (NOTD)
Apr  4 21:43:22 CustService176 CustService176: [system] GPS Monitor daemon has restarted (GPSD)
Apr  4 21:43:22 CustService176 CustService176: [system] Received reset request  (STATUSD)
Apr  4 21:43:22 CustService176 CustService176: [system] NTP generic status polling (pid=3333, tid=b5cffb40): thread started (STATUSD)
Apr  4 21:43:22 CustService176 CustService176: [system] NTP extended status polling (pid=3333, tid=b7012b40): thread started  (STATUSD)
Apr  4 21:43:22 CustService176 CustService176: [system] Temperature Monitoring (pid=3333, tid=b66ffb40): thread started (STATUSD)
```

NTPQ/statusd (Status daemon) associated System log entries

- I believe statusd daemon was originally implemented by Oleg. But Timofey modified it for at least version 5.4.1 (I believe Ron Dries said Timofey also modified it for version 5.3.1 but not positive on this).
- statusd obtains NTP status info via NTPQ data and stores it in a temporary location for various threads to access this info.

System command error fpaneld:DT_DrawStat (FPD)

Example entry: [system] System command error fpaneld:DT_DrawStat (FPD)

H) Versions 5.4.1 and above

Modified email from Paul Myers (22 Aug 16) regarding a unit wuith many of these entries These entries indicate front panel is locked up. They are likely running in a degraded state. Could the TSYNC Driver be unloaded? Is the FPGA failure being reported in the system log?

I) Version 5.3.0 and below

This status information reported on the front panel (if the SecureSync has been configured to display Status information instead of the network settings, as many customers choose to display) includes the NTP Stratum and NTP Sync status. Software update version 5.3.0 incorporated changes in how info from NTP is obtained for items such as the web browser, SNMP, the CLI interface and the front panel to report (v5.3.0 added statusd daemon to have one location for threads to get NT status info)

Note from Keith: I've seen this error entry in version 5.3.0, as well. Suspect it's due to an OCXO oscillator glitching/starting to fail.

- Per Oleg- This issue is not likely to cause the browser/ssh to stop responding- just loss of NTP status info.
- This daemon was initially called 'masterd;

Temperature Monitoring

Two related error messages: Error 4 and Error 5 (both associated with Temperature Monitoring)

- Both of these messages are due to a Minor Issue found in v5.7.0? and fixed in 5.7.1
  - Refer to JIRA case **SSS-293** for both entries

Note: SF case 171143 reported it was already at 5.7.1 when this entry was asserted (it was supposed to be fixed in 5.7.1). He is going to update to 5.8.1 and see if it occurs again.

A) "Error 4" message

```
[system] ERROR! ERROR!!!! Temperature Monitoring: Failed to read CPU temperature. Error: 4
/usr/src/spectracom/daemons/statusd/core/HwCpu.cpp, 20, static double Hw::Cpu::Temperature() (STATUSD)
```

- Refer to SF case 118395

Email from Ryan (28 Sept 17) This error isn't a concern. There was a bug where sometimes we'd attempt to read the temperature at the same time when it was being updated, resulting in a conflict and the error. The next time it would try and likely succeed so it would be just an occasional conflict.

This is fixed in 5.7.1: https://spectracom.atlassian.net/browse/SSS-293?dest-url=/plugins/servlet/mobile

B) "Error 5" message

```
Aug 10 15:07:53 <local7.emerg> pptp201 pptp201: [system] ERROR! ERROR!!!! Temperature Monitoring: Failed to read
CPU temperature. Error: 5 /usr/src/spectracom/daemons/statusd/core/HwCpu.cpp, 20, static double
Hw::Cpu::Temperature()  (STATUSD)
```

- Refer to SF cases 171143, 116678

Customer Report: I've powered-up and reconfigured the repaired Securesync server, including sending all the logging to my syslog server. It's been sending some messages that are concerning:

```
Aug 10 15:07:53 <local7.emerg> pptp201 pptp201: [system] ERROR! ERROR!!!! Temperature
Monitoring: Failed to read CPU temperature. Error: 5
/usr/src/spectracom/daemons/statusd/core/HwCpu.cpp, 20, static double
Hw::Cpu::Temperature()  (STATUSD)
Aug 10 15:07:53 <local7.emerg> pptp201 pptp201: [system] ERROR! ERROR!!!! Temperature
Monitoring: Failed to read CPU temperature. Error: 5
/usr/src/spectracom/daemons/statusd/core/HwCpu.cpp, 20, static double
Hw::Cpu::Temperature()  (STATUSD)
```

By this time the unit had been running for a few hours.

A **Reply from Dave L (14 Aug 17)** There messages are from the System log and I think they indicate the CPU Temperature data is not being logged correctly. I am verifying with engineering. When was this repaired? Do you have a RMA number or serial number we can record?

A **email from Ryan (14 Jul 17)** This is addressed in 5.7.1 (SSS-293 in Jira) and I'll update the SF ticket. The problem itself in innocuous and is a symptom of occasionally being unable to read the temperature. These are Stuarts comments:

I have verified that there are periods of time that the kernel takes down the temperature input file that is being

> read (/sys/class/hwmon/hwmon0/temp_input2).
>
> Very rarely, statusd will attemp to read this file at the exact same time the kernel takes it down - so the easiest way to prevent this is (as paul suggested) implement a retry capability so it will try a few times after a small delay.

A Second reply from Dave L (14 Aug 17) The problem is a symptom of occasionally being unable to read the temperature. We have a ticket in to create the resolution. Thank you and your customer for your patience while we resolve this issue.

NTP/statusd associated System log entries

"System command error: NTPQ_" / "NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS) (STATUSD)"

- ➢ Refer to SF case 119824 / JIRA ticket JIRA-SSS-202
  - ○ JIRA ticket was written for version 5.5.0, but is still unresolved in at least version 5.7.1

```
Sep 30 11:13:27 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Sep 30 11:13:27 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
Sep 30 11:14:09 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Sep 30 11:14:09 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
Oct 7 12:03:57 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Oct 7 12:03:57 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
Oct 7 12:05:21 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Oct 7 12:05:21 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
Oct 13 08:26:26 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Oct 13 08:26:26 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
Oct 13 08:28:00 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Oct 13 08:28:00 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
Oct 13 08:29:34 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Oct 13 08:29:34 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
Oct 13 08:31:07 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Oct 13 08:31:07 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS)
(STATUSD)
Oct 13 08:31:49 igm-apr-gps2 igm-apr-gps2: [system] System command error: NTPQ_GetAsscVariable_Actual (NTPAL)
Oct 13 08:31:49 igm-apr-gps2 igm-apr-gps2: [system] ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d /usr/s
```

Per Paul Myers (13 Oct 17) JIRA-SSS-202 records this issue in Release 5.5.0 and is assigned to Ryan for disposition.
This issue appears to be an intermittent polling failure to communicate between StatusD and NTPD using ntpq.
We have not directly addressed or investigated it.
I believe it is just a failure of status to communicate with NTPD.
However, 5.7.1 has made improvement to NTPD (new version) and has corrected issues with StatusD operation and restart.

Based on Security vulnerabilities and these improvements it is recommended to update.

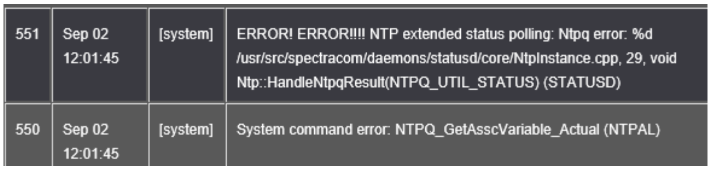
3) Statusd keeps resetting (isn't able to start) because the Min CPU temperature threshold values have been reconfigured by a user to be greater than "100" (100 is the max value)

- In at least version 5.4.1, the web browser doesn't restrict/alert to setting the thresholds to above 100 (the max value that the system allows these values to be).
- The following log entry ("statusd has started") is continuously asserted because statusd keeps resetting.
- NTP Status (Stratum, Sync state, etc) is reported as "??" because the data obtained with NTPQ keeps being deleted.

```
Apr  4 22:02:23 CustService176 CustService176: [system] statusd has started  (STATUSD)
Apr  4 22:02:23 CustService176 CustService176: [system] NTP generic status polling (pid=14524, tid=b6fa7b40): thread started (STATUSD)
Apr  4 22:02:23 CustService176 CustService176: [system] NTP extended status polling (pid=14524, tid=b65ffb40): thread started (STATUSD)
Apr  4 22:03:30 CustService176 CustService176: [system] statusd has started  (STATUSD)
Apr  4 22:03:30 CustService176 CustService176: [system] NTP generic status polling (pid=16331, tid=b6f37b40): thread started (STATUSD)
Apr  4 22:03:30 CustService176 CustService176: [system] NTP extended status polling (pid=16331, tid=b65ffb40): thread started (STATUSD)
Apr  4 22:04:38 CustService176 CustService176: [system] statusd has started  (STATUSD)
Apr  4 22:04:38 CustService176 CustService176: [system] NTP generic status polling (pid=18199, tid=b6f45b40): thread started (STATUSD)
Apr  4 22:04:38 CustService176 CustService176: [system] NTP extended status polling (pid=18199, tid=b65ffb40): thread started (STATUSD)
Apr  4 22:02:23 CustService176 CustService176: [system] statusd has started  (STATUSD)
Apr  4 22:02:23 CustService176 CustService176: [system] NTP generic status polling (pid=14524, tid=b6fa7b40): thread started (STATUSD)
Apr  4 22:02:23 CustService176 CustService176: [system] NTP extended status polling (pid=14524, tid=b65ffb40): thread started (STATUSD)
Apr  4 22:03:30 CustService176 CustService176: [system] statusd has started  (STATUSD)
Apr  4 22:03:30 CustService176 CustService176: [system] NTP generic status polling (pid=16331, tid=b6f37b40): thread started (STATUSD)
Apr  4 22:03:30 CustService176 CustService176: [system] NTP extended status polling (pid=16331, tid=b65ffb40): thread started (STATUSD)
Apr  4 22:04:38 CustService176 CustService176: [system] statusd has started  (STATUSD)
```

- Refer to the "statusd" section of this document for more info:Statusd daemon for obaining status info from NTP (v5.3.0 and above) (scroll down to "Issues associated with statusd")
  - Setting the "**Minimum CPU temperature**" thresholds above "**100**" in at least versions 5.4.0/5.4.1 will cause statusd to continuously reset (this entry will continue to be asserted). Lower the two "Minimum CPU temperaure" values (**Management** -> **Notifictions** page, **System** tab) to "100" or less to keep statusd from resetting and therefore to keep this alarm entry from being consistently asserted.

4) System command error" NTPQ_util_status (Statusd)



551	Sep 02 12:01:45	[system]	ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d /usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS) (STATUSD)
550	Sep 02 12:01:45	[system]	System command error: NTPQ_GetAsscVariable_Actual (NTPAL)

"System command error: NTPQ_GetAsscVariable_Actual (NTPAL)"   In combination with the following log entry:

```
ERROR! ERROR!!!! NTP extended status polling: Ntpq error: %d
/usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, vERROR! ERROR!!!! NTP extended status polling: Ntpq
error: %d /usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 29, void
Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS) (STATUSD)oid Ntp::HandleNtpqResult(NTPQ_UTIL_STATUS) (STATUSD)
```

Email fron Paul Myers (5 Sept 17) These are the "StatusD" status daemon monitoring NTP. These are errors thrown when it cannot communicate with NTP briefly typically using ntpq to monitor it's status.

It is often occurring if NTPD is restarted or not yet running. It most often can occur on startup if NTPD steps the system time.This is not something to be alarmed about if it occurs.It might only occur frequently if NTP were NOT responding.

---

5) 403 error message in system log

- Refer to Mantis case 3264

```
[system] ERROR! ERROR!!!! NTP generic status polling:
AccessError /usr/src/spectracom/daemons/statusd/core/NtpInstance.cpp, 38, static Ntp::GenericStatus
Ntp::Instance::ReadGenericStatus() (STATUSD)
84 Mar 23 18:36:21 [system] ntp monitor restarting ntpd (NTPMOND)
```

Note from Paul Myers: NTPD shuts down and restarts when stepping time. The statusd daemon should detect this and reestablish communication - not throw a low level error.

---

6) Cannot open /tmp/ntpq.data in NTPQ_ReadStatus (NTPAL)

- Refer to Salesforce case 20824

Email from Ole (2 Feb 16 KW): "I believe the statusd fails because of the error:
Jan 22 14:53:14 chl-securesync01 chl-securesync01: [webui] Error (7) on eth0 FAILURE detected in opening temp   lease file.. (SYSAL)". It cannot get data from NTP if ethernet port is not working.

---

7) "Ntp monitor restarting ntpd (ntpmond)"

```
[system] ntp monitor restarting ntpd (NTPMOND)":
[system] ntp monitor stopping ntpd, found 3578 second difference
```
followed by
```
[system] ntp monitor restarting ntpd (NTPMOND)
```

- NTPMOND "wakes-up" and check NTP every 16 seconds to check if NTP is running and if it's within 1 second of the System Time (while synced to System Time).
- NTPMOND will restart NTP if NTP is in sync and the time error from KTS is 1 second or greater, or if NTP exceeded sanity limit of 1000 seconds (16min 40 sec) which can cause it to stop running

Note: Per Ron Dries, NTPMOND "wakes-up" every 16 seconds to check if NTP is running. It will restart NTP as necessary and then go back to sleep. Depending on when NTP dies in relation to ntpmond going to sleep, it can take up to 16 seconds for NTP to be restarted by ntpmond. Then it will take a couple of minutes for NTP to resync and be useable again.

Note: NTP also has its own Reference time change limits, as well (**NTP step threshold of 128ms**)

- ○ If NTP's selected input changes by **128 millisecond or less**, NTP **slews** to the reference (maximum rate of 500 microseconds per second)

Fastest time to slew

500us = 1 second

1ms = 2 seconds

64ms = 128 seconds (2.1 minutes)

128ms = 256 seconds (4.2 minutes)

- If NTP’s selected input changes by **more than 128 milliseconds.** NTP **steps** to the reference

8) Network DNS issues affect NTPQ’s ability to run

```
Jun 10 20:12:40 Spectracom Spectracom: [system] Failed to read NTP system statistics (NTPMOND)
Jun 10 20:12:46 Spectracom Spectracom: [system] System command error: NTPQ_GetAsscVariable (NTPAL)
Jun 10 20:12:46 Spectracom Spectracom: [system] NTPQ_GetAsscVariable(ASSC_VAR_OFFSET) returned [rc = 1] (KHTD)
Jun 10 20:13:19 Spectracom Spectracom: [system] System command error: NTPQ_RetrievePeersData (NTPAL)
Jun 10 20:13:26 Spectracom Spectracom: [system] System command error: NTPQ_ReadSysstats (NTPAL)
Jun 10 20:13:26 Spectracom Spectracom: [system] Failed to read NTP system statistics (NTPMOND)
Jun 10 20:13:49 Spectracom Spectracom: [system] System command error: NTPQ_RetrieveAsscData (NTPAL)
Jun 10 20:14:13 Spectracom Spectracom: [system] System command error: NTPQ_ReadSysstats (NTPAL)
Jun 10 20:14:13 Spectracom Spectracom: [system] Failed to read NTP system statistics (NTPMOND)
Jun 10 20:14:19 Spectracom Spectracom: [system] System command error: NTPQ_GetAsscVariable (NTPAL)
Jun 10 20:14:19 Spectracom Spectracom: [system] NTPQ_GetAsscVariable(ASSC_VAR_LEAP) returned [rc = 1] (KHTD)
Jun 10 20:14:49 Spectracom Spectracom: [system] System command error khtd:DT_FindNonLocalCandidate (KHTD)
Jun 10 20:14:59 Spectracom Spectracom: [system] System command error: NTPQ_ReadSysstats (NTPAL)
Jun 10 20:14:59 Spectracom Spectracom: [system] Failed to read NTP system statistics (NTPMOND)
Jun 10 20:15:19 Spectracom Spectracom: [system] System command error: NTPQ_GetAsscVariable (NTPAL)
Jun 10 20:15:19 Spectracom Spectracom: [system] NTPQ_GetAsscVariable(ASSC_VAR_OFFSET) returned [rc = 1] (KHTD)
Jun 10 20:15:46 Spectracom Spectracom: [system] System command error: NTPQ_ReadSysstats (NTPAL) when the Timing
System and Linux kernel time differ by more than 1 sec
```

- Update software to at least version 5.3.0 to add “statusd” daemon (adds a central location for threads to be able to get NTP Status info from one location without having to run NTPQ)
- Refer to Salesforce case 18447
- Issues with DNS can prevent NTPQ from being able to run. It needs to establish a network socket connection with either the assigned IP address when run from external to the SecureSync or with the local host address when run from within the time server. This address is set by DNS, unless DNS times-out. This DNS timeout can take longer than the NTPD time-out. So NTPQ can’t provide the requested data.
    - Per Oleg: this issue not likely to cause browser/ssh to stop responding.

Time correction associated System logs

time reset +300784145.312704 (note the numeric value of seconds at the end will vary):
From link above: “The time error exceeds the step threshold and has been reset to the correct time.

NTP resets its time by this number of seconds with a “time step”, because the time error was greater than the step threshold of 128 milliseconds. If the time error had been less than 128 milliseconds, the time error would have instead been corrected by slew.

This entry is likely due to the System Time being manually set to an incorrect date/time, so the time was too far off when NTP synced to a valid reference. (Review the Journal log to see if there are any corresponding “**Set Time for User Reference 0 in slot 0**” entries, which indicate a user had manually changed System Time).

Note: Refer to **“Time Reset” when NTP starts up** (..\CustomerServiceAssistance.pdf) for more details on how NTP initially corrects the time.

time slew ? s

The time error exceeds the step threshold and is being slewed to the correct time. You may have to wait a very long time.

Note: Refer to “Time Reset” when NTP starts up (in NTP for all products) for more details on how NTP initially corrects the time and info how to change it via NTP Expert mode.

MYSql/SQLite (“database”) associated entries

[system] Failed to write event to the database (NOTD)

- Refer to Salesforce case 21129
- Cause of this entry not yet known.
- Note from this customer: “This error occurred after a power-cycle reboot that I had to do, due to the unit not responding to SSH or HTTP (but it was still responding to PING)”

Web browser associated entries

[webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetMfrMdl 0 (KTSAL)

- Refer to Salesforce case 23448.

Email from Paul Myers: The (4) indicates a process was killed because it received a signal. This can happen if the Web server kills process you are shutting down or rebooting. It could happen in theory because a command took longer than 30 sec and was killed by a timeout in the parent.

(internal use, 31 oct 16) Paul indicatd the error (4) entries used to be masked in earlier versions. He unmasked them to see how often they are really asserted and they are not sure exactly why these infrequeny alarms occur “out of the blue” He and Ron indicated this entry may be related to a call being placed when the web browser is being closed/timing-out,preventing it from being able to complete,

[system] Error: sendto call failed (STMD) / ERROR in KTSAL_Get: SPEC_KTSAL_EN=true

- Refer to Salesforce case **20728**

```
[system] Error:  sendto call failed (STMD)
Dec 23 16:19:41 Spectracom last message repeated 31 times
Dec 23 16:20:42 Spectracom last message repeated 61 times
Dec 23 16:21:43 Spectracom last message repeated 61 times
Dec 23 16:22:08 Spectracom last message repeated 11 times
Dec 23 19:28:39 Spectracom Spectracom: [webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true
SS_GetTimeStamp 0 3 0  (KTSAL)
Dec 31 11:58:40 Spectracom Spectracom: [webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true
XO_GetFreqError 0   (KTSAL)
Dec 31 11:58:40 Spectracom Spectracom: [webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true
SS_GetTimeStamp 0 2 0  (KTSAL)
Dec 31 12:18:40 Spectracom Spectracom: [webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true
SS_GetUptime 0   (KTSAL)
Dec 31 12:28:41 Spectracom Spectracom: [webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true
SS_GetTfom 0   (KTSAL)
Dec 31 13:08:40 Spectracom Spectracom: [webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true
XO_GetOscType 0   (KTSAL)
Dec 31 13:08:40 Spectracom Spectracom: [webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true
SS_GetTimeStamp 0 1 0  (KTSAL)
```

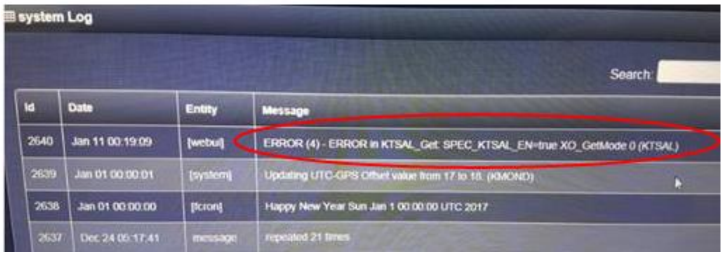
```
Dec 31 13:58:40 Spectracom Spectracom: [webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true
XO_GetPhaseError 0   (KTSAL)
Dec 31 14:18:42 Spectracom Spectracom: [webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true
XO_GetOscType 0   (KTSAL)
Dec 31 14:58:41 Spectracom Spectracom: [webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true
SS_GetFreeRun 0   (KTSAL)
Dec 31 15:18:41 Spectracom Spectracom: [webui] ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true
XO_GetFreqError 0   (KTSAL)
```

Comments from Paul Myers (9 Mar 16) These are caused by Signals being received by processes issuing commands. I believe they are caused by web UI pages terminating, or unexpected signals. I do not believe they are a cause for alarm yet…

Other System log entries

ERROR (4) ‐ ERROR in KTSAL_ Get: SPEC_KTSAL_EN=true XO_GetMode 0 (KTSAL)

Q I have a question about system log of SecureSync.



Id	Date	Entity	Message
2640	Jan 11 00:19:09	[webui]	ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetMode 0 (KTSAL)
2639	Jan 01 00:00:01	[system]	Updating UTC-GPS Offset value from 17 to 18. (KMOND)
2638	Jan 01 00:00:00	[fcron]	Happy New Year Sun Jan 1 00:00:00 UTC 2017
2637	Dec 24 05:17:41	message	repeated 21 times

A Reply from Dave L (13 Jan 17) These types of error messages can appear in the System Log from time to time. This particular error has been reported because a process to read the oscillator mode was interrupted for some reason.

We believe they are caused by web UI pages terminating, or unexpected signals. There is no cause for alarm. Similar messages may appear in all Securesyncs.

[WEB] Log Feature Failed to read OFDF or RMNF (WEB)

- Refer to Salesforce case 20365 (Kaiser)
- Observed with SecureSync that was running version 5.2.0 software
- Kern log also contained “hda” error messages such as :

```
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=87817,
sector=87817
Jan 12 18:23:10 cdcntp202 kernel: hda: possibly failed opcode: 0xc8
Jan 12 18:23:10 cdcntp202 kernel: end_request: I/O error, dev hda, sector 87817
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=88049,
sector=88049
Jan 12 18:23:10 cdcntp202 kernel: hda: possibly failed opcode: 0xc8
Jan 12 18:23:10 cdcntp202 kernel: end_request: I/O error, dev hda, sector 88049
Jan 12 18:24:37 cdcntp202 kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
Jan 12 18:24:37 cdcntp202 kernel: hda: dma_intr: error=0x44 { DriveStatusError UncorrectableError }, LBAsect=88049,
sector=88049
```

Email fron Paul Myers (13 Jan 2016) I may have commented on this before keith, but this unit looks like 2 issues.

Possibly the mysql database is not working write for some errors, but the 2nd errors you point out give me concern the CompactFlash is corrupted or worst case the interface to the CF in hardware is causing errors.

You could reboot and clean and see what happens.

OR you could do a clean update.

If the errors exist below then you might have a bad CF or ATA CF interface in hardware is bad. Most likely CF though.

```
Jan 12 18:23:10 cdcntp202 kernel: hda: dma_intr: status=0x51 { DriveReady SeekComplete Error }
```

Osc.log (Oscillator log/oscillator.log)

Minor Issue with oscillator log (decimal point one place off)

- Refer to Salesforce case 19963 / Mantis case 3177
- At least 5.3.0 and 5.3.1 have the decimal place in the numeric frequency error one place too far to the right
  - Instead of "0.0", it's being displayed in the log entry as "00.0" (need to move it one place to the left to be correcr).
  - Scientific notation value is correct. Just displaying decimal point in the wrong location.

Harris software only (such as version 5.4A)

- Refer to salesforce case 25697

```
Jun 18 01:52:58 S12u2clk S12u2clk: [system] 2017 169 01:52:58 000 XO: Ref Changed: old=gps0 new=gps0
Jun 18 01:52:59 S12u2clk S12u2clk: [system] 2017 169 01:52:58 000 XO: Phase Reference Invalid.
Jun 18 01:53:00 S12u2clk S12u2clk: [system] 2017 169 01:52:59 000 XOS: Rb track off -- free run
Jun 18 01:53:16 S12u2clk S12u2clk: [system] 2017 169 01:53:16 000 XO: Ref Changed: old=gps0 new=gps0
Jun 18 01:53:16 S12u2clk S12u2clk: [system] 2017 169 01:53:16 000 XO: Phase Reference Valid.
Jun 18 01:54:51 S12u2clk S12u2clk: [system] 2017 169 01:54:50 000 XOS: Rb synchronized
```

Oscillator Calibration log entries- Refer to: Oscillator Calibration log entries

Note: Software version 5.1.7 added **several** improvements to TCXO/OCXO disciplining.

"New Cal Value": Only happens at factory or if a patch is applied to reset it. This entry can be eventually overwritten.

"Saved Cal Value": The previously calculated value stored in the EEPROM.

"phase start" and "phase end" entries in the Oscillator log

```
Sep 17 00:02:15 clock.ld4.eexchange.com clock.ld4: [system] 2015 260 00:02:15 000 XO1: Freq error: phase start: +20.4 ns, phase end: +45.0 ns
```

- I believe these entries started being added to Oscillator log in upgrade version 5.2.1 (they are in v5.2.1, but may have been added earlier).
- Periodically logs the 1PPS phase error measurement.

Email Keith sent (17 Sept 15) Instead of SecureSync just reporting in the web browser the 1PPS phase error (which is the measured offset between the 1PPS input reference and the unit's internal System 1PPS) newer software versions now also periodically log this value in the Oscillator log. These are reported as "phase start" and "phase end". The lower the 1PPS phase error, the more accurate the SecureSync is to its external reference (with a Rubidium oscillator installed, these values will typically be less than around 100ns).

Err Mean / Standard deviation

- Group of entries for TXCO/OCXO oscillators asserted after every time Disciplining qualifies/locks the oscillator

Examples from our Customer Service.176 at version 5.1.7. OCXO (5ppb) oscillator

```
13:44:28 Custservice Custservice.176: [system] 2014 308 13:44:28 000 XO1: Initial DAC Setting: 0x8C54
Nov  4 13:44:28 Custservice Custservice.176: [system] 2014 308 13:44:28 000 XO1: Saved Cal Value: H/S:+0.0001377126
Nov  4 13:46:09 Custservice Custservice.176: [system] 2014 308 13:46:09 000 XO1: DAC Setting: 0x8C42
Nov  4 13:46:09 Custservice Custservice.176: [system] 2014 308 13:46:09 000 XO1: Phase Err: +25.0
Nov  4 13:46:09 Custservice Custservice.176: [system] 2014 308 13:46:09 000 XO1: Freq Err: +0.004166
Nov  4 13:46:09 Custservice Custservice.176: [system] 2014 308 13:46:09 000 XO1: Err Chg Mean: +0.3
Nov  4 13:46:09 Custservice Custservice.176: [system] 2014 308 13:46:09 000 XO1: Err Chg Std Dev: +5.6
```

Several examples from our Customer Service.176 at version 5.1.6 or lower. OCXO (5ppb) oscillator

```
Oct 13 11:15:35 Custservice Custservice.176: [system] 2014 286 11:15:35 000 XO1: Initial DAC Setting: 0x8CAD
Oct 13 11:15:35 Custservice Custservice.176: [system] 2014 286 11:15:35 000 XO1: Saved Cal Value: H/S:+0.0001377126

Oct 17 16:36:32 Custservice Custservice.176: [system] 2014 290 16:36:32 000 XO1: Initial DAC Setting: 0x8BC2
Oct 17 16:36:32 Custservice Custservice.176: [system] 2014 290 16:36:32 000 XO1: Saved Cal Value: H/S:+0.0001377126

Oct 17 16:45:31 Custservice Custservice.176: [system] 2014 290 16:45:31 000 XO1: Initial DAC Setting: 0x8BC2
Oct 17 16:45:31 Custservice Custservice.176: [system] 2014 290 16:45:31 000 XO1: Saved Cal Value: H/S:+0.0001377126

Oct 20 12:02:05 Custservice Custservice.176: [system] 2014 293 12:02:05 000 XO1: Initial DAC Setting: 0x8BC2
Oct 20 12:02:05 Custservice Custservice.176: [system] 2014 293 12:02:05 000 XO1: Saved Cal Value: H/S:+0.0001377126

Oct 24 21:35:24 Custservice Custservice.176: [system] 2014 297 21:35:25 000 XO1: Initial DAC Setting: 0x8BC2
Oct 24 21:35:25 Custservice Custservice.176: [system] 2014 297 21:35:25 000 XO1: Saved Cal Value: H/S:+0.0001377126

Oct 28 15:56:14 Custservice Custservice.176: [system] 2014 301 15:56:13 000 XO1: Initial DAC Setting: 0x8BC2
Oct 28 15:56:14 Custservice Custservice.176: [system] 2014 301 15:56:13 000 XO1: Saved Cal Value: H/S:+0.0001377126
Oct 28 16:33:44 Custservice Custservice.176: [system] 2014 301 16:33:59 000 XO1: Err Mean: -1.5
Oct 28 16:33:44 Custservice Custservice.176: [system] 2014 301 16:33:59 000 XO1: Err Std Dev: +5.9
```

Hi / Lo / Referr entries

- This group of entries are asserted each time system switches from Holdover back to a Reference

Per Dave Sohn (30 Jan 2014) : These are logged results from the reference qualification coming back from holdover".

(Refer to entries below in red)

```
Dec 28 15:49:49 COLW-SecureSync COLW-SecureSync: [system] 2013 362 15:49:49 000 XO1: Frequency error recalculated: 00.0000030 (3.043x10^-13)
Dec 28 16:06:59 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:06:59 000 XO1: Frequency error recalculated: 00.0001917 (1.917x10^-11)
Dec 28 16:24:52 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:24:52 000 XO1: hi= +195.0
Dec 28 16:24:52 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:24:52 000 XO1: lo= -135.0
Dec 28 16:24:52 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:24:52 000 XO1: RefErr= +165.0
Dec 28 16:27:04 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:27:04 000 XO1: hi= +40.0
Dec 28 16:27:04 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:27:04 000 XO1: lo= -40.0
Dec 28 16:27:04 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:27:04 000 XO1: RefErr= +40.0
Dec 28 16:31:36 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:31:36 000 XO1: Frequency error recalculated: 00.0004376 (4.376x10^-11)
Dec 28 16:53:18 COLW-SecureSync COLW-SecureSync: [system] 2013 362 16:53:18 000 XO1: Frequency error recalculated: 00.0000071 (7.177x10^-13)
```

"Frequency Error recalculated" messages

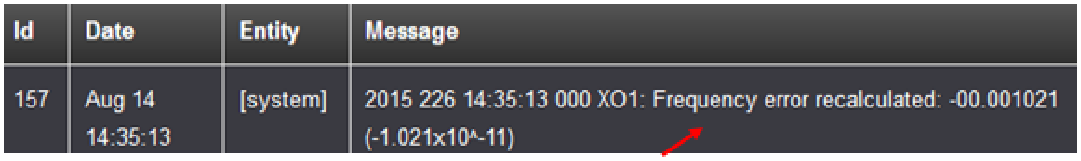
- Entries only asserted if an external reference that can discipline the oscillator is present
- Typical values for good OCXO, when locked to GPS: no worse than around " 5.994x10^-11"

Spectracom SecureSyncs contain one of five types of internal 10 MHz oscillators. The internal oscillator is used to output 10 MHz and to generate an internal 1PPS signal.

The "Oscillator" log provides an indication of the frequency counts of the oscillator's 10 MHz output, as measured using the selected 1PPS Input Reference (Such as a GPS receiver's 1PPS output signal) as a reference.

The "frequency error recalculated" messages in this log indicate the accuracy of the oscillator output, in comparison to a perfect 10 MHz signal (known as the "fractional frequency error"). The 10 MHz oscillator output is measured against the 1PPS generated by the selected 1PPS input reference.

A) Newer browser

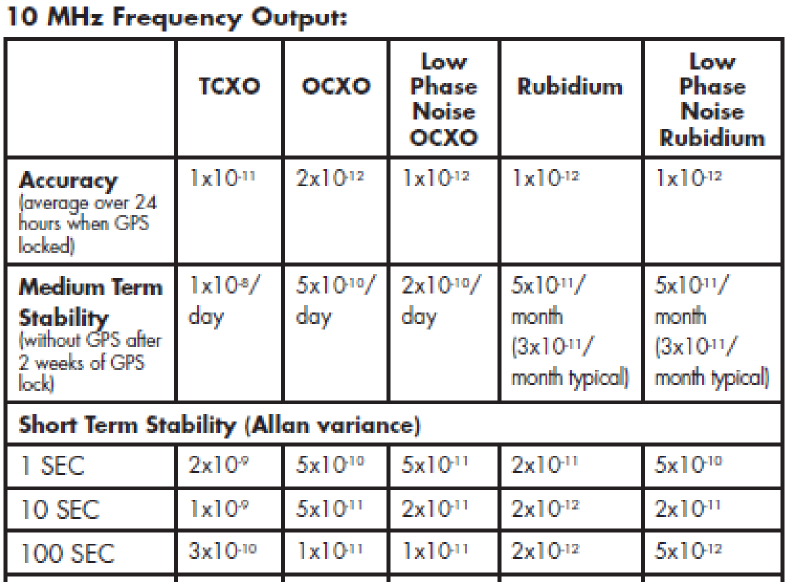


Id	Date	Entity	Message
157	Aug 14 14:35:13	[system]	2015 226 14:35:13 000 XO1: Frequency error recalculated: -00.001021 (-1.021x10^-11)

The phrase "FREQUENCY ERROR RECALCULATED" designates the value to follow is reporting how close the oscillator's actual 10 MHz output signal is to the desired frequency of 10.0000000 MHz (reported in scientific notation). This phrase is not an indication that there is a problem with the oscillator.

Important Note- The "FREQUENCY ERROR RECALCULATED" phrases displayed on this web page DO NOT mean a problem exists with either the internal oscillator or with the NTP server. "FREQUENCY ERROR RECALCULATED" refers to the Fractional Frequency Error which is a comparison of the actual output frequency versus the desired frequency (The desired frequency is 10.0000000 MHz), reported in scientific notation. This phrase will ALWAYS be present on this page to show the measured 10 MHz frequency. If a problem DOES happen to exist with the oscillator frequency measurements, a Frequency alarm will be entered in the "Alarms" log.

The lower the "Frequency error recalculated" value is, the closer the oscillator is to outputting an exact 10 MHz signal. Below is a table of the 10MHZ specifications. The "Frequency error calculated" values should typically be less than the values in the "Short term Stability" section of this table, for the specific type of oscillator installed, as long as SecureSync is synced to an external reference (other than other NTP severs).



10 MHz Frequency Output:

	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium
Accuracy (average over 24 hours when GPS locked)	1x10^{-11}	2x10^{-12}	1x10^{-12}	1x10^{-12}	1x10^{-12}
Medium Term Stability (without GPS after 2 weeks of GPS lock)	1x10^{-8}/ day	5x10^{-10}/ day	2x10^{-10}/ day	5x10^{11}/ month (3x10^{11}/ month typical)	5x10^{11}/ month (3x10^{11}/ month typical)
Short Term Stability (Allan variance)					
1 SEC	2x10^{9}	5x10^{-10}	5x10^{11}	2x10^{-11}	5x10^{-10}
10 SEC	1x10^{9}	5x10^{11}	2x10^{11}	2x10^{-12}	2x10^{11}
100 SEC	3x10^{-10}	1x10^{11}	1x10^{11}	2x10^{-12}	5x10^{-12}

“Frequency error recalculated: 00.0000000 (0.000x10^-16)”   (0.000e-16 or 0.000x10-16)

Note: This oscillator.log entry can be asserted for one of two reasons:

A) The actual frequency error is less than we can measure

Email from Dave Sohn (27 Jan 15) after I alluded to the software issue below It is still possible to receive a frequency error of 0 if it is below our measurement capability. We fixed where negative frequency errors were reported as 0.

Edited Email Keith sent to Masataka (27 Jan 15)

Thanks for forwarding along your customer’s inquiry about the oscillator log entries.

The oscillator log entry of “**Frequency error recalculated: 00.000000 (0.000x10^-16)”** is not a symptom of any problems occurring with the SecureSync. These log entries just mean that the magnitude of the frequency error at that time was less than the threshold that the system can even measure. In this case, the Frequency Error is reported as “0.000x10^-16” (the lowest value possible for the system to report). So instead of these log entries being a symptom of a problem, they instead indicate the oscillator is as close to being at the desired frequency as the system is capable of measuring.

B) A minor software issue in software versions 5.10 through 5.1.4 (fixed in 5.1.5)

- Software issue with reporting the frequency error in the Oscillator log
- Negative values were being incorrectly being reported as “0” (“So any negative frequency error measurements will show as 0.000x10-16.")
- Refer to Mantis case 2862 http://cvsmantis.int.orolia.com/mantis/view.php?id=2862
- This issue first started in version 5.1.0.
- Fixed in version 5.1.5 software update

Software version 5.1.4 improvements to oscillator disciplining

Email from Dave Lorah to Masataka (24 June 2014) As far as changes between 5.0.2 and 5.1.4, we improved our measurement window adjustments, improved our initial sync time performance, and added adjustable filtering based on input reference error. There would be a difference in the oscillator log measurements due to these changes. The oscillator measurement range should be in the x10-11 to x10-13 range. The oscillator log you sent us shows typical performance.

Rb Reference unstable

Per Dave Sohn, this entry indicates the Rb oscillator was forced into free-run due to issues with the selected 1PPS reference (system itself doesn’t go into Holdover mode. But the oscillator is in free-run.   Anther entry is asserted “Rb synchronized” once the oscillator is relocked with the 1PPS reference.

- This entry could potentially indicate a bad Rb oscillator , but is more likely caused by issues with the selected 1PPS reference (such as issues with a Res-SMT-GG receiver, including earlier firmware versions, such as 1.6 and 1.7)

Diagnosing this entry

1. Also review the **discstats** entries (in addition to the other system logs) for additional info on operation of the oscillator when this entry is asserted. In **discstats**, look for likely large increases in the frequency error measurements (such as normally around 1x10 -13, but then they change to a larger value such as 1x10-10 (which was observed in Salesforce case 20249 also mentioned below).
2. The “**Rb Reference unstable**” alarm has been seen in one case where no other log entries were asserted in other logs- Alarms, Timing, Events, etc. and reception was fine.   Refer to Salesforce case 20249.
3. The “**Rb Reference unstable**” alarm has been seen correlated with the following entry in the Timing log (Res-SMT-GG firmware issue)

“[system] 2014 291 13:01:08 002 Error: CS_Set(CS_SA_LEAP_SEC) call from GR.”

Rb peak voltage error alarms

- Also refer to: “SRO-100 Rubidium oscillators” in the Customerserviceassistance document

Note: Archive software versions 5.0.0 and below reported all alarms associated with the Rubidium oscillator as “**Rb peak voltage error**” alarms. This was noticed just prior to the version 5.0.1 release, so version 5.0.1 now differentiates each Rb oscillator alarm to indicate what the real issue with the Rb oscillator.

Q. (log entry from Morgan Stanley Rb-based SecureSync) **Rb peak voltage error** (val=6, min=51, max=255)
A (1/25/12) Mark Goodlein emailed SpectraTime with: We have a customer with one of our SecureSync products, in which we use an SRO-100 Rubidium oscillator module. Recently, this customer saw some behavior that was questionable and would like to know if they should be concerned about it.

Our software that communicates with the SRO requests the internal parameters using the ‘M’ command once a second. It then compares the values returned with boundary values to detect if something is out of the ordinary, in which case we log the condition. This customers unit had been running for over 150 days then the following log messages were recorded for 5 seconds then went away and no more have been logged since then.

```
2011 357 21:26:54 000 Rb peak voltage error (val=6, min=51, max=255)
2011 357 21:26:55 000 Rb peak voltage error (val=7, min=51, max=255)
2011 357 21:26:56 000 Rb peak voltage error (val=7, min=51, max=255)
2011 357 21:26:57 000 Rb peak voltage error (val=9, min=51, max=255)
2011 357 21:26:58 000 Rb peak voltage error (val=35, min=51, max=255)
```

The manual for the SRO indicates that this signal stabilizes to between 1 and 5 volts after warm-up, so these are the boundary conditions that our software checks for. In this case, the voltage dipped below 1V (almost reaching 0V) for 5 seconds. This is the first case of an event like this that has ever been reported to us from a customer.

Is this event something to be concerned about? Does it indicate a condition that may result in failure?

Oscillator Log entries associated with Wenzel oscillator’s PLL lock status

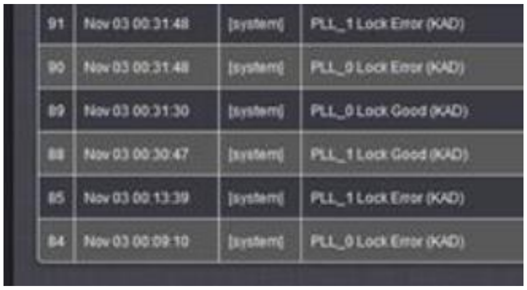
- Refer to the CGU manual addendum for Hughes (1200-5000-C050) in Arena at: https://app.bom.com/items/detail-spec?item_id=1217182411&version_id=10446313248&orb_msg_single_search_p=1

- Also refer to [Options/Specials]() in this doc (scroll down to the Hughes CGU)

Example entries in the osc.log

```
[system] PLL_0 Lock Error (KAD)
[system] PLL_0 Lock Good (KAD)
[system] PLL_1 Lock Error (KAD)
[system] PLL_1 Lock Good (KAD)
```

Example entries in osc.log



```
91  Nov 03 00:31:48  [system]  PLL_1 Lock Error (KAD)
90  Nov 03 00:31:48  [system]  PLL_0 Lock Error (KAD)
89  Nov 03 00:31:30  [system]  PLL_0 Lock Good (KAD)
88  Nov 03 00:30:47  [system]  PLL_1 Lock Good (KAD)
85  Nov 03 00:13:39  [system]  PLL_1 Lock Error (KAD)
84  Nov 03 00:09:10  [system]  PLL_0 Lock Error (KAD)
```

Raccon.log (rc log)

22. I believe this may be a Radius log, but not postive

Qual.log entries (Qual log)

23. GPS reception - Refer to: I:\Customer Service\GPS\GPS reception Ap Notes\SecureSync for a description of this log.

Reboot/power cycle of the unit erases the Qual log data before the reboot occurred (since the top of the current hour)

24. Qual log data is only written to the log 2 seconds after the end of each hour
25. If a reboot/power cycle occurs after the beginning of the hour, the data between the beginnings of the hour until the reboot occurred is lost. So the Qual log will only report the data from the power-up until the end of that hour (Q will not include any data in the current hour before the power cycle occurred).

Issue with GNSS receiver dropping to 0 sats

26. Applicable in at least version 5.1.4 software.
27. Refer to Deviation (ECN) 3481

Email from Dave West (20 May 2014) The GNSS Receiver has an error with the following:
If GPS tracks randomly 0 Satellites for 1 to 5 seconds, this is a known bug.
It is acceptable for the units that display this to ship.
This Deviation is in place until the next release later than 5.1.4

Test Procedure 1200-XXXX-0600-TP was updated to include this deviation and is now at revision 19

Havequick input (no GPS input)

28. Loss/regain of GPS reception causes “QR hvq0” log entries to be asserted.

```
Sep 20 15:10:14 Timeserver2 Timeserver2: [system] 2013 263 15:10:14 000 QR hvq0 has lost communication.
Sep 20 15:10:15 Timeserver2 Timeserver2: [system] 2013 263 15:10:15 000 QR hvq0 has established communication.
```

Email from Dave Sohn (21 Jan 2014) If the signal is disconnected or lost, these messages will appear and return. This is not a system alarm.

29. Used in conjunction with the rexd.log
30. This system log is not accessible from the browser. But it’s in the Save Logs bundle.
31. This log is not wiped when performing a “clear all logs” in the browser
32. Rexd.log was added in software version 5.0.2
33. This log is not viewable from the web browser (can FTP it out as a single log, bundle it with all of the logs or view it with telnet/ssh)

rexd.log and rexd.bone log

A) rexd.bone log

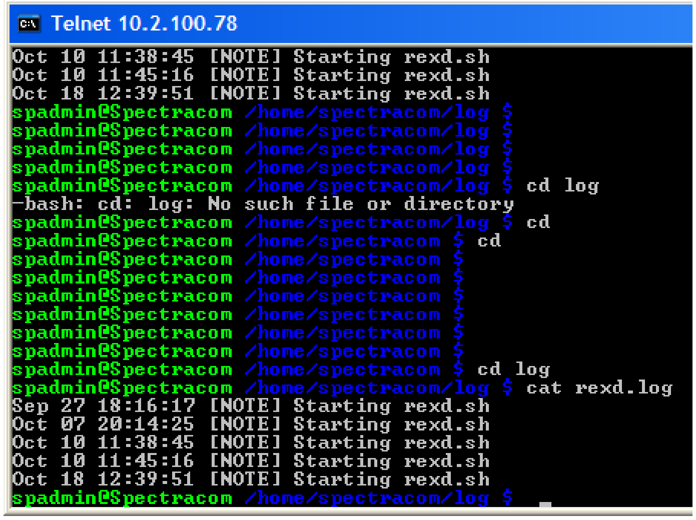
34. This system-level log is not accessible from the browser. But it’s in the Save Logs bundle.
35. Contains just a timestamp for when rexd last ran (for Nullmailer for example)

    Example entry: 12-May-2015 15:30:00

36. This time/date stamp is updated each time rexd runs (to clean up nulllmailer for instance)
37. If it’s not being updated daily, this is an indirect indication that the “system” isn’t running properly.

B) rexd.log (daemon log)

38. This system-level log is not accessible from the browser. But it's in the Save Logs bundle.
39. This log is not wiped when performing a "clear all logs" in the browser
40. Rexd.log was added in software version 5.0.2
41. This log is not viewable from the web browser (can FTP it out as a single log, bundle it This log keeps track of daemons that are restarted because they are no longer responding.
42. Daemons are checked every 5 minutes to see if they are still running.



```
Oct 10 11:38:45 [NOTE] Starting rexd.sh
Oct 10 11:45:16 [NOTE] Starting rexd.sh
Oct 18 12:39:51 [NOTE] Starting rexd.sh
spadmin@Spectracom /home/spectracom/log $
spadmin@Spectracom /home/spectracom/log $
spadmin@Spectracom /home/spectracom/log $
spadmin@Spectracom /home/spectracom/log $
spadmin@Spectracom /home/spectracom/log $ cd log
-bash: cd: log: No such file or directory
spadmin@Spectracom /home/spectracom/log $ cd
spadmin@Spectracom /home/spectracom $ cd
spadmin@Spectracom /home/spectracom $
spadmin@Spectracom /home/spectracom $
spadmin@Spectracom /home/spectracom $
spadmin@Spectracom /home/spectracom $
spadmin@Spectracom /home/spectracom $
spadmin@Spectracom /home/spectracom $
spadmin@Spectracom /home/spectracom $ cd log
spadmin@Spectracom /home/spectracom/log $ cat rexd.log
Sep 27 18:16:17 [NOTE] Starting rexd.sh
Oct 07 20:14:25 [NOTE] Starting rexd.sh
Oct 10 11:38:45 [NOTE] Starting rexd.sh
Oct 10 11:45:16 [NOTE] Starting rexd.sh
Oct 18 12:39:51 [NOTE] Starting rexd.sh
spadmin@Spectracom /home/spectracom/log $ _
```

Lots of [HANDLER] nullmailer clean up successful entries asserted

```
Jun 14 02:47:13 [HANDLER] nullmailer clean up sucessful
Jun 14 15:06:50 [HANDLER] nullmailer clean up sucessful
Jun 15 03:27:02 [HANDLER] nullmailer clean up sucessful
Jun 15 15:46:42 [HANDLER] nullmailer clean up sucessful
Jun 16 04:06:29 [HANDLER] nullmailer clean up sucessful
```

Example of normal series of entries to see at each start-up

```
Jun 12 14:35:49 [NOTE] Starting rexd.sh
Jun 12 14:35:49 [NOTE] Failed to find scast card
Jun 12 14:35:49 [NOTE] Found front panel
Jun 12 14:35:49 [NOTE] Found gps receiver
Jun 12 14:35:50 [NOTE] rexd.sh has started
Jun 12 14:39:07 [NOTE] Starting rexd.sh
Jun 12 14:39:07 [NOTE] Failed to find scast card
Jun 12 14:39:07 [NOTE] Found front panel
Jun 12 14:39:07 [NOTE] Found gps receiver
Jun 12 14:39:07 [NOTE] rexd.sh has started
Jun 13 02:55:01 [HANDLER] nullmailer clean up successful
```

-
- These entries are normal and expected,
- Linux OS messages get queued (in nullmailer package) to be sent out for every log entry. The recipient email address is not filled out and the queue folder is growing since it cannot send messages out.
- there is a script to empty the folder every 5 hours. These entries indicate it was successfully cleaned up.

“xinetd” log entries in rexd.log

Xinetd: (*extended Internet daemon*) is an open-source super-server daemon which runs on many Unix-like systems and manages Internet-based connectivity.

xinetd listens for incoming requests over a network and launches the appropriate service for that request.[4] Requests are made using port numbers as identifiers and xinetd usually launches another daemon to handle the request. It can be used to start services with both privileged and non-privileged port numbers.

errno (such as “errno = 22” for example)

- Refer to the following website for a list of errno numbers and what they mean: http://www-numi.fnal.gov/offline_software/srt_public_context/WebDocs/Errors/unix_system_errors.html

```
For example:"(errno = 22)" means "Invalid argument"
```

xinetd[21807]: socket bind: Invalid argument (errno = 22) : Appears to be a known issue with earlier versions of xinetd. Updating SecureSync to a newer version is likely to prevent these entries.

xinetd[7302]: Failed to contact identity server at ::ffff:10.14.104.11: system error

(Identity Integration server / MIIS) synchronize identity information from many different directories and services into a single, organization-wide solution. This can help protect your network's security and simplify management.

“telnetd” (telnet) log entries in rexd.log

telnetd[24923]: ttloop: peer died: EOF

- Due to an abrupt loss of telnet connection
- Can be caused by not exiting the connection before closing out, for example.

Below is from a Google search

But guessing that you see it in a telnetd log it could be something innocent like somebody connected using telnet and instead of logging out they just clicked the x in the top corner of the app to shut it down. Or the telnet app crashed or their computer crashed or lost network connectivity. All the telnetd app knows is that it was talking to someone and then that connection was lost. It could be that someone is scanning your computer to see if you are running telnet on any ports so that they can try to hack you. I am a little surprised that you are running telnet since everyone I know has banned it from their network and uses ssh instead.

GPS monitor logs in rexd.log

Oct 18 14:18:08 [RESTART] Restarting initiated for gpsmond

- GPS monitor likely reset due to a software issue with version 5.0.2, when no GPS receiver is installed. (There will be several of these entries in this log).

SNMP log entries in rexd.log

SNMP automatically restarting (snmpsad)

```
[RESTART] Restarting initiated for snmpsad
[RESTART] Restarting initiated for snmpsad
 [SUCCESS] Successfully restarted snmpsad
```

- SNMPSAD being restarted automatically if it crashed was added in version 5.1.3.
- SNMP likely restarted by rexd because of walking the MIBs with the timeout value being set too low for the NTP

associated objects. Timeout should be set to a minimum of about 9 to 10 seconds.

Nullmailer log entries in rexd.log

```
Lots of [HANDLER] nullmailer clean up successful entries asserted
Jun 14 02:47:13 [HANDLER] nullmailer clean up sucessful
Jun 14 15:06:50 [HANDLER] nullmailer clean up sucessful
Jun 15 03:27:02 [HANDLER] nullmailer clean up sucessful
Jun 15 15:46:42 [HANDLER] nullmailer clean up sucessful
Jun 16 04:06:29 [HANDLER] nullmailer clean up sucessful
```

- These entries are normal and expected (as a fix to the nullmaiiler issue)
- Refer to Mantis case 2390 (~Oct 2013)
- Email messages get queued (in nullmailer package) to be sent out for every log entry. The recipient email address is not filled out and the queue folder is growing since it cannot send messages out.
- Per the Mantis case, there is now a script to empty the folder every 5 hours. These entries indicate it was successfully cleaned up.

qual.log (Qual log entries)

- Refer to the GPS Reception Tech Note: I:\Customer Service\GPS\GPS reception Ap Notes\SecureSync

rc.log (raccoon)

- Linux start-up and shut-down log????

snmpd.log

Error log (ssl_request_log: Apache web browser's Access log)

- These log entries are from /var/log/apache2/error.log
- Refer to http://httpd.apache.org/docs/2.2/logs.html for more info
- Logs from Apache's Access log (reported pages that were accessed)
- Starts with ".log.1" as the file extension instead of just ".log" like the other log files
- View this log via CLI or from a log capture file

Format of Access log entries

The format of the access log is highly configurable. The format is specified using a format string that looks much like a C-style printf(1) format string. Some examples are presented in the next sections. For a complete list of the possible contents of the format string, see the mod_log_config format strings.

Common Log Format

A typical configuration for the access log might look as follows.

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common
CustomLog logs/access_log common
```

This defines the *nickname* common and associates it with a particular log format string. The format string consists of percent directives, each of which tell the server to log a particular piece of information. Literal characters may also be placed in the format string and will be copied directly into the log output. The quote character (") must be escaped by placing a backslash before it to prevent it from being interpreted as the end of the format string. The format string may also contain the special control characters "\n" for new-line and "\t" for tab.

The above configuration will write log entries in a format known as the Common Log Format (CLF). This standard format can be produced by many different web servers and read by many log analysis programs. The log file entries produced in CLF will look something like this:

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
```

Each part of this log entry is described below.

1. **127.0.0.1 (%h)**

   This is the IP address of the client (remote host) which made the request to the server. If `HostnameLookups` is set to `On`, then the server will try to determine the hostname and log it in place of the IP address. However, this configuration is not recommended since it can significantly slow the server. Instead, it is best to use a log post-processor such as `logresolve` to determine the hostnames. The IP address reported here is not necessarily the address of the machine at which the user is sitting. If a proxy server exists between the user and the server, this address will be the address of the proxy, rather than the originating machine.

2. **(`%l`)**

   The "hyphen" in the output indicates that the requested piece of information is not available. In this case, the information that is not available is the RFC 1413 identity of the client determined by `identd` on the clients machine. This information is highly unreliable and should almost never be used except on tightly controlled internal networks. Apache httpd will not even attempt to determine this information unless `IdentityCheck` is set to `On`.

3. **frank (%u)**

   This is the userid of the person requesting the document as determined by HTTP authentication. The same value is typically provided to CGI scripts in the `REMOTE_USER` environment variable. If the status code for the request (see below) is 401, then this value should not be trusted because the user is not yet authenticated. If the document is not password protected, this part will be "`-`" just like the previous one.

4. **[10/Oct/2000:13:55:36 -0700] (%t)**

   The time that the request was received. The format is:

   [**day/month/year:hour:minute:second zone**]
   day = 2*digit
   month = 3*letter
   year = 4*digit
   hour = 2*digit
   minute = 2*digit
   second = 2*digit
   zone = (`+' | `-') 4*digit

   It is possible to have the time displayed in another format by specifying `%{format}t` in the log format string, where `format` is as in `strftime(3)` from the C standard library.

5. **"GET /apache_pb.gif HTTP/1.0" (\"%r\")**

   The request line from the client is given in double quotes. The request line contains a great deal of useful information. First, the method used by the client is `GET`. Second, the client requested the resource `/apache_pb.gif`, and third, the client used the protocol `HTTP/1.0`. It is also possible to log one or more parts of the request line independently. For example, the format string "`%m %U%q %H`" will log the method, path, query-string, and protocol, resulting in exactly the same output as "`%r`".

4. 200 (%>s)

   This is the status code that the server sends back to the client. This information is very valuable, because it reveals whether the request resulted in a successful response (codes beginning in 2), a redirection (codes beginning in 3), an error caused by the client (codes beginning in 4), or an error in the server (codes beginning in 5). The full list of possible status codes can be found in the HTTP specification (RFC2616 section 10).

6. **2326 (%b)**

   The last part indicates the size of the object returned to the client, not including the response headers. If no content was returned to the client, this value will be "-". To log "`0`" for no content, use `%B` instead.

Example “normal” entries (from one of our NetClocks)

```
[23/Jul/2015:11:48:58 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Features/getTime HTTP/1.1" 288
[23/Jul/2015:11:49:05 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/serverStatus HTTP/1.1" 2053
[23/Jul/2015:11:49:09 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/peerStatus HTTP/1.1" 1365
[23/Jul/2015:11:49:15 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/status HTTP/1.1" 105885
[23/Jul/2015:11:49:25 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/serverStatus HTTP/1.1" 2053
[23/Jul/2015:11:49:28 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/peerStatus HTTP/1.1" 1365
[23/Jul/2015:11:49:42 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/serverStatus HTTP/1.1" 2053
[23/Jul/2015:11:49:46 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/peerStatus HTTP/1.1" 1370
[23/Jul/2015:11:49:54 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/status HTTP/1.1" 105961
[23/Jul/2015:11:49:58 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Features/getTime HTTP/1.1" 288
[23/Jul/2015:11:49:59 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/serverStatus HTTP/1.1" 2055
[23/Jul/2015:11:50:04 +0000] 10.2.100.124 TLSv1.2 DHE-RSA-AES256-SHA "GET /Ntp/peerStatus HTTP/1.1" 1365
```

**sys.log entries (Syslog log)

- This log is not wiped when performing a “clear all logs” in the browser.
- No syslog log available for viewin in the browser.
  - sys.log can only be viewed via the CLI interface (It’s in the **home/spectracom/logs** directory)
- Contains entries for syslog stopping and starting

Example “normal” entries

“Spectracom syslogd 1.5.0: restart.”: Indicates unit was rebooted.

```
Jan 21 20:06:02 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] New connection from 172.18.189.19
Jan 21 20:06:03 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] Logout.
Jan 21 20:06:20 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] New connection from 172.18.189.19
Jan 21 20:06:20 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] Logout.
Jan 21 20:11:21 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] New connection from 172.18.189.19
Jan 21 20:11:22 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] Logout.
Jan 21 20:16:22 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] New connection from 172.18.189.19
Jan 21 20:16:23 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] Logout.
Jan 21 20:21:24 Spectracom pure-ftpd: (?@172.18.189.19) [INFO] New connection from 172.18.189.19
```

**system.log entries (and MySQL database)

A) Version info reported in System log for log reviewing

- Version 5.2.1 update (Apr 2015) added Model and Serial Number to the System Log at each start-up.
- Update Version 5.2.0 added the System /Timing System version info to the system.log after each power-up (for knowing the version when reviewing logs).

B) Fan control/temperature monitoring associated log entries (starting in version 5.3.1)

1. (Starting in v5.3.1 and if the EEPROM has been reprogrammed): On boot, the Fan Control feature detection is logged in the system log.
2. Log entry asserted after each boot-up (starting in v5.3.1) Temperature Monitor daemon has started (TEMPD)

C) log entries associated with glitch in or loss of 10MHZ into the FPGA (Version 5.2.0 and above)

Event log (just some possible examples)

```
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true GR_GetMfrMdl 0 0 (KTSAL)
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetState 0 (KTSAL)
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetOscType 0 (KTSAL)
ERROR (4) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetSerialNo 0 (KTSAL)
```

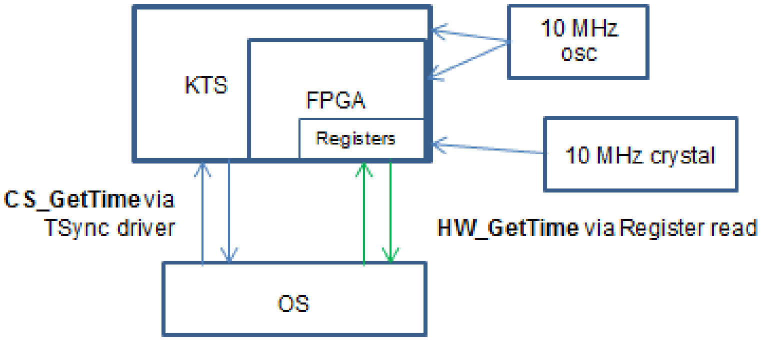
System log

- Timing System Hardware error
- Failed CS_GetTime (KAD)

Then either:

- Passed HW_GetTime (possible oscillator error) (KAD) Or
- Failed HW_GetTime (probably FPGA failure) (KAD)

Details



1. If there are at least five (5) “Failed to read alarm info from KTS (KAD)…” entries in the **System** log, first a “**CS_GetTime”** call is sent to KTS to see if KTS is still communicating via the TSync driver.
    - If there are less than 5 entries, nothing happens and the counter is reset
    - If there are at least 5 entries, the Tsync driver **will** be unloaded (reboot will be necessary to restore operation)
2. Then a “**HW_GetTime” call** is sent to the FPGA registers to see if the FPGA is communicating.

  - If this call passes, the registers are still able to respond (if KTS isn't running, the same data may remain in the registers). This confirms the TSync driver is still running normally.
  - If this call fails, the registers are not able to provide any data whatsoever. This means either bad FPGA or Tsync driver not running.

3. If both time calls fails, the issue could be with the TSync driver, so it's unloaded (and remains unloaded) to allow the Network Processor to continue working. Reloading the Tsync driver requires the unit be rebooted.
4. If both calls fail, the oscillator likely glitched, causing both FPGA and KTS to stop responding.
5. If **CS_GetTime** fails but **HW_GetTime** passes, FPGA is still working.

"ERROR (2) - Error SEC_GetGroup (username[0,1]=quagga) (WEB)"

- Refer to Mantis case 2979.
- This is a new log entry starting in update version 5.2.0.
- Note: "Quagga" is a new user account added for "NTP over Anycast" mode
- This message just indicates someone opened the "classic interface" web browser (even if no changes were made in this browser). This message is not asserted when the newer browser is accessed and doesn't indicate any problems with the time server. This entry is just because the quagga user account doesn't exist in the "classic interface browser".

D) System logs associated with KTS (KHTD) (Kramden Host Timing Daemon for input to NTP)

- KHTD is our KTS Host Time Daemon. It is responsible for NTP time sets to KTS when operating in Stratum 2, and for setting kernel time when NTP is not running.

KTS Host Time Daemon has restarted (KHTD):

- This entry indicates NTP was restarted (automatically due to an NTP config change or manually by a user)

KTS Host Time Daemon has terminated (KHTD):

- This entry indicates NTP shutdown for halt/reboot by a user (other daemons will also be terminated, as well).

E) System logs associated with NTP

1. NTPMOND monitor restarting NTP

- NTPMOND wakes-up" and check NTP every 16 seconds to check if NTP is running and if it's within 1 second of the System Time (while synced to System Time)
- NTPMOND will restart NTP, if NTP is in sync and the time error from KTS is 1 second or greater, or if NTP exceeded sanity limit of 1000 seconds (16min 40 sec) which can cause it to stop running.

Note: Per Ron Dries, NTPMOND "wakes-up" every 16 seconds to check if NTP is running. It will restart NTP as necessary and then go back to sleep. Depending on when NTP dies in relation to ntpmond going to sleep, it can take up to 16 seconds for NTP to be restarted by ntpmond. Then it will take a couple of minutes for NTP to resync and be useable again.

[system] ntp monitor stopping ntpd, found 1 second difference (NTPMOND) **followed by:**
[system] ntp monitor restarting ntpd (NTPMOND)"
NTP sanity check failed due to <1000 second (16 Min 40 sec) time correction. NTP monitor daemon restarted NTP to apply this correction. System Time was likely manually changed while NTP was still running (input

reference may have changed, for instance).

2. NTP step threshold of 128 ms

NTP also has its own Reference time change limits, as well (NTP step threshold- 128ms)

- If NTP's selected input changes by **128 milliseconds or less**, NTP **slews** to the reference
- If NTP's selected input changes by **more than 128 milliseconds** (and this error persists for more than the stepout threshold which has a default value of 900 seconds), NTP **steps** it's time to the reference.

3. SNMP related System log entries

[spadmin] SNMP agent failed to startup (SNMPAL)

- ➢ SNMPSAL tried to restart SNMPAD but was not able to do so. Software should be updated to at least version 5.2.1. Refer to the SNMP troubleshooting section in this doc.

4. System logs associated with Front panel

[system] Front Panel daemon did not detect or initialize the Keypad LCD panel (FPD)
Note: This entry is only expected if this is a Model 9489 (which has no front panel)

[webui] ERROR (7) - ERROR in KTSAL_Set: GR_SetConstSel 0 0 0 (KTSAL)

- ➢ Error condition that can occur in versions 5.1.7 and below when changing the configurations of a Res-SMT-GG receiver that doesn't have the Glonass option enabled. This condition is described in more detail in the "GNSS input" section (just search for "ERROR in KTSAL_Set: GR_SetConstSel" to easily find it).

[web] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'phase_error' cannot be null (WEB) (followed by a series of ktsal failures)

- Observed with version 5.1.7 after changing the System Time while synced with GPS.

Per Oleg, KTS is restarted if a large unexpected time change occurs. The KTS failures were likely due to KTS not being available while KTS was being restarted.

5. Issues related to Trimble RES-SMT-GG GNSS receivers (~Oct 2014)

Note: These System log entries may also be accompanied by related Timing.log entries such as the following:

[system] 2014 224 02:33:38 002 Error: CS_Set(CS_SA_LEAP_SEC) call from GR. (this entry indicates the receiver was trying to erroneously change the leap second offset to some arbitrary value. But a mask we put in place prevented it from being able to be changed)

6. Issue with erratic log entries "no newlines" (no new lines)

"ERROR (7) - ERROR no newlines in response in KTSAL_Get (KTSAL)"

- ➢ Applicable in at least version 5.1.4 software.
- ➢ Refer to Deviation (ECN) 3481
- ➢ Refer to Mantis case 2796 http://cvsmantis.int.orolia.com/mantis/view.php?id=2796
- ➢ Apparently related to software issues with the Trimble Res-SMT-GG receivers

Email from Dave West (20 May 2014) There are 2 errors that occur in logs regarding the GNSS receivers and the 5.1.4 Release. In the test Procedure, there should be no errors in the system log. With Release 5.1.4, a bug was found randomly sending out the following errors

```
[webui] ERROR (7) - SPEC_KTSAL_EN=true XO_GetSerialNo 0 (KTSAL)
[webui] ERROR (7) - ERROR no newlines in response in KTSAL_Get (KTSAL)

[webui] ERROR (7) - SPEC_KTSAL_EN=true XO_GetPhaseError 0 (KTSAL)
[webui] ERROR (7) - ERROR no newlines in response in KTSAL_Get (KTSAL)
```

These errors are acceptable for shipment per this Deviation:

A) Leap second incorrectly scheduled:[system] Scheduled Leap Second: +1 sec at 00:00:00 148/2017 UTC (KMOND)

B) **UTC offset value changes on its own** [system] Updating UTC-GPS Offset value from 16 to 3. (KMOND) (Note the second value can vary).

- A work-around to prevent this event causing a temporary time error / time jump was added in software version 5.1.5.

7. "ERROR in KTSAL" associated entries

- Repeated groupings of several "Failed to read" AND "Failed to get" Error entries asserted in System.log

Example entries that may be asserted:

```
Failed to read GPS fix data from KTS (GPSD)
ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset.
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read oscillator frequency error from KTS (KAD)
[WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)
```

- Likely due to ETX, or the parts associated with KTS: Micro (U1) 10MHz oscillator FPGA (U40) or EEPROM (U2). FPGA may need to be reloaded at factory.

Per Dave Sohn, KTS crashing not likely due to the memory consumption issue.

Entries indicate KTS crash/ KTS not talking to network processor software. Logs just below are from Salesforce case 15055 (Andy Felde with Drew Wireless. Found it needed a new oscillator)

Similar logs in Salesforce Cases:
15055 (found it needed new oscillator)
11832 (Also reported no SSH. Found bad ETX),
14375 (bad FPGA),
14744 (v5.1.4 software) needed the KTS firmware re-programmed
15326 (Open Access with v4.7A software). John also reported the front panel time display was frozen/locked up and no SSH. Happened more than once a couple weeks apart.

```
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset.

(KMOND)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset.
(KMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
```

```
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read oscillator frequency error from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to get current synchronizing references (NTPMOND)
[WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to get current sync state (DISCMOND)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 12:55:43 Spectracom Spectracom: [system] Failed to read oscillator frequency error from KTS (KAD)
Jun 23 12:55:47 Spectracom Spectracom: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
Jun 23 12:55:49 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
```

```
[system] Failed to get current synchronizing references (NTPMOND)
[system] ntp monitor stopping ntpd, found 1376668877 second difference (NTPMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] KTS Host Time Daemon has restarted  (KHTD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read oscillator frequency error from KTS (KAD)
[system] Failed to get current sync state (DISCMOND)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read oscillator frequency error from KTS (KAD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read GPS fix data from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync' cannot be null (WEB)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
[system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get variable Timescale Offset. (KMOND)
```

```
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to get current synchronizing references (NTPMOND)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read alarm info from KTS (KAD)
[system] Failed to read GPS fix data from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
Jun 23 12:59:12 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get
variable Timescale Offset. (KMOND)
Jun 23 12:59:17 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 12:59:19 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
Jun 23 12:59:21 Spectracom Spectracom: [system] Failed to get current sync state (DISCMOND)
Jun 23 12:59:28 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 12:59:30 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetLeapSec 0   (KTSAL)
Jun 23 12:59:32 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get Leap
Second. (KMOND)
Jun 23 12:59:36 Spectracom Spectracom: [system] Failed to get current synchronizing references (NTPMOND)
Jun 23 12:59:38 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 12:59:41 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
Jun 23 12:59:45 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get
variable Timescale Offset. (KMOND)
Jun 23 12:59:48 Spectracom Spectracom: [system] Failed to read oscillator frequency error from KTS (KAD)
Jun 23 12:59:50 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 12:59:52 Spectracom Spectracom: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync'
cannot be null (WEB)
[system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
[system] Failed to read GPS antenna status from KTS (GPSD)
[system] Failed to read alarm info from KTS (KAD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
Jun 23 13:00:02 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get
variable Timescale Offset. (KMOND)
Jun 23 13:00:05 Spectracom Spectracom: [system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
Jun 23 13:00:08 Spectracom Spectracom: [system] Failed to get current synchronizing references (NTPMOND)
Jun 23 13:00:12 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 13:00:14 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:00:18 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
Jun 23 13:00:21 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get
variable Timescale Offset. (KMOND)
Jun 23 13:00:23 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:00:27 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 13:00:29 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:00:35 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
Jun 23 13:00:37 Spectracom Spectracom: [system] Failed to get current synchronizing references (NTPMOND)
Jun 23 13:00:39 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
Jun 23 13:00:43 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get
variable Timescale Offset. (KMOND)
Jun 23 13:00:46 Spectracom Spectracom: [system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
Jun 23 13:00:48 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 13:00:50 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:00:52 Spectracom Spectracom: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync'
cannot be null (WEB)
Jun 23 13:00:57 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
Jun 23 13:00:59 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
Jun 23 13:01:01 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get
variable Timescale Offset. (KMOND)
Jun 23 13:01:06 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 13:01:08 Spectracom Spectracom: [system] Failed to get current synchronizing references (NTPMOND)
Jun 23 13:01:11 Spectracom Spectracom: [system] Failed to read oscillator frequency error from KTS (KAD)
Jun 23 13:01:13 Spectracom Spectracom: [system] ntp monitor stopping ntpd, found 1376669162 second difference
```

```
(NTPMOND)
Jun 23 13:01:15 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
Jun 23 13:01:18 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get
variable Timescale Offset. (KMOND)
Jun 23 13:01:21 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 13:01:23 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:01:25 Spectracom Spectracom: [system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
Jun 23 13:01:25 Spectracom Spectracom: [system] KTS Host Time Daemon has restarted  (KHTD)
Jun 23 13:01:27 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
Jun 23 13:01:30 Spectracom Spectracom: [system] ntp monitor restarting ntpd (NTPMOND)
Jun 23 13:01:31 Spectracom Spectracom: [system] Failed to get current sync state (DISCMOND)
Jun 23 13:01:33 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
Jun 23 13:01:35 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get
variable Timescale Offset. (KMOND)
Jun 23 13:01:38 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 13:01:46 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:01:48 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
Jun 23 13:01:51 Spectracom Spectracom: [system] Failed to get current synchronizing references (NTPMOND)
Jun 23 13:01:53 Spectracom Spectracom: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync'
cannot be null (WEB)
[kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true CS_GetTimeScaleOff 0 2  (KTSAL)
Jun 23 13:01:57 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get
variable Timescale Offset. (KMOND)
Jun 23 13:01:59 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:02:01 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 13:02:06 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:02:09 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
Jun 23 13:02:12 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:02:14 Spectracom Spectracom: [kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true
CS_GetTimeScaleOff 0 2  (KTSAL)
Jun 23 13:02:14 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get
variable Timescale Offset. (KMOND)
Jun 23 13:02:16 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 13:02:18 Spectracom Spectracom: [system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
Jun 23 13:02:22 Spectracom Spectracom: [system] Failed to get current synchronizing references (NTPMOND)
Jun 23 13:02:24 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:02:26 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
Jun 23 13:02:28 Spectracom Spectracom: [system] ERROR - KW_HR_SetValidity returned [rc = 3] (KHTD)
Jun 23 13:02:33 Spectracom Spectracom: [kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true
CS_GetTimeScaleOff 0 2  (KTSAL)
Jun 23 13:02:33 Spectracom Spectracom: [system] Error (12) - Failed calling KTSAL_Get to invoke Clock function to get
variable Timescale Offset. (KMOND)
Jun 23 13:02:35 Spectracom Spectracom: [system] Failed to read oscillator frequency error from KTS (KAD)
Jun 23 13:02:37 Spectracom Spectracom: [system] Failed to read GPS fix data from KTS (GPSD)
Jun 23 13:02:44 Spectracom Spectracom: [system] Failed to read GPS antenna status from KTS (GPSD)
Jun 23 13:02:46 Spectracom Spectracom: [WEB] Log SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'sync'
cannot be null (WEB)
Jun 23 13:02:48 Spectracom Spectracom: [system] Failed to read alarm info from KTS (KAD)
Jun 23 13:02:53 Spectracom Spectracom: [kmond] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true
CS_GetTimeScaleOff 0 2  (KTSAL)
```

“STR_” error messages in System log (Versions 5.8.0 and above only)

"ERROR in KTSAL_Get:SPEC_KTSAL_EN=true STR_GetSubscription 0.0 (KTSAL)"

- Refer to SF case 171405
- Caused by “**STL INFO**” menu being displayed on front panel (or rotate menus selected) with no 1204-3D/1204-

3E STL card installed in the syste,

- Version 5.8.0 added the STL Info menu in all units, even if 1204-3D/3E is installed, If the unit is downograded to below 5.8.0. this STL menu is no longer exists, so the issue no longer occurs
- if STL card isnt installed, the request by the front panel to display STL data causes this entry to be asserted

email from Keith (1 Nov 18) This “GetSubscription” entry is associated with a purchasable feature we now offer for SecureSyncs, called “STL”. In case you aren’t familiar with it, it’s a satellite signal, similar to GPS, but since these satellites are closer to the earth than the GPS constellation, their signals are stronger. There are other benefits to it, as well.

STL is available with an STL receiver Option Card and a subscription to the service. The version 5.8.0 software update added a new front panel LCD display menu which shows the signal strength of this STL signal. The error message just means that someone was scrolling through the various menu screens, which include the STL menu. But without the STL receiver/option being installed, there was no communications available to report the expected value.

This “errant” entry is expected to be no longer reported if the STL menu is selected, or scrolled thru, via a future software update. There should be no operational concerns if this entry is observed! Thanks again for asking about it, just to be sure it didn’t indicate a problem!!

8. [webui] ERROR (13) - ERROR in call to KTSAL_GetProgs in KTSAL_Get (KTSAL)

- This entry is just a logging issue
- It's not an indication of a problem with the equipment
- Fixed in the version 5.1C patch and post 5.1.3 update (5.1.4?) which incorporates this patch (PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates)

9. Rinex Server entry each hour “CAGPS ERROR (1): Failed to retrieve data from Rinex server (CAGPSD)”

- Applicable to version 5.1.3 software only
- Due to A-GPS still running, even though its disabled. Seen only on units on a closed network with no Internet access.
- Refer to knowledge base article 1275 (https://na8.salesforce.com/ka3C0000000TT7D).
- Fix is to install version 5.1C patch (PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates
- Logging issue only. Does not adversely affect operation of SecureSync.

10. GPS Monitor daemon starting and terminating from time of power-up

- Refer to Mantis case 2391and NC7252 for this issue
- Started in version 5.0.0 (in at least versions 5.0.0, 5.0.1 and 5.0.2)

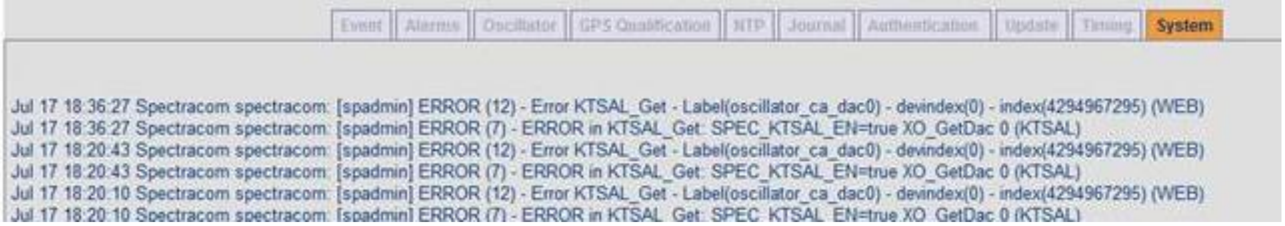
- This is just a logging issue.
- Fix already done for inclusion in the next planned release (version 5.1.0).

11. Issue with erratic log entries in units with Rb oscillator installed

- Refer to Mantis Case 1729.
- Applicable in at least version 4.8.6 software.
- Was fixed in the v4.8.7 update.

Q. I'm getting an error message in the System Log of a 1200-033 Rb. unit I just updated to 4.8.6. This occurs after I select the STATUS/TIME AND FREQUENCY (It is not happening on an OCXO unit)

```
Jun 20 12:45:19 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB)
Jun 20 12:45:19 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)
Jun 20 12:44:10 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB)
Jun 20 12:44:10 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)
Jun 20 12:41:59 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB)
Jun 20 12:41:59 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)
```



```
Jul 17 18:36:27 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB)
Jul 17 18:36:27 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)
Jul 17 18:20:43 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB)
Jul 17 18:20:43 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)
Jul 17 18:20:10 Spectracom spectracom: [spadmin] ERROR (12) - Error KTSAL_Get - Label(oscillator_ca_dac0) - devindex(0) - index(4294967295) (WEB)
Jul 17 18:20:10 Spectracom spectracom: [spadmin] ERROR (7) - ERROR in KTSAL_Get: SPEC_KTSAL_EN=true XO_GetDac 0 (KTSAL)
```

A **Email from Dave Sohn (6/20/12)** There isn't any issue with the unit. This is just a reporting bug. The system is in the background querying the DAC value for some reporting, but that isn't a valid call for a Rubidium unit, so there is an error. There is no effect on operation, and that error doesn't mean there is any problem with the unit. You can enter a Mantis case for it, and we will discuss it in SW CCB.

(8/31/12 KW) Update – the fix for this issue should be in the version 4.8.7 release

12. Error entry periodically being asserted "[system] ERROR - KW_HR_SetTime returned [rc = 3]"

- Refer to Salesforce cases 14919 (Dongjin) and 12869 (Open Access, Australia)
- Apparently asserted when NTP input tries to set the KTS time but is not able to
- Verify the proper configuration of the NTP Peers and NTP Servers tabs.
- Dongjin had the Enable Stratum 0 PPS reference enabled with a peer configured.

24 June 2014 KW- Per Oleg, this entry indicates KTHD tried to sync NTP from System Time (using the Spectracom driver) but for some reason, KTHD (not NTP) rejected the time. KHTD tries to sync NTP every 16 seconds. This entry indicates that for this one particular instance, KHTD was not able to sync NTP.

Since it couldn't sync NTP on this particular instance (for whatever reason), there was no detrimental effect in any way to the timing performance of the SecureSync at that time.

Internal info only- One thought is our driver may be trying to set the NTP time twice in the same second and only one of the two can be successful???

Patch 4.8S/v5.1.2 and above work-around to Gb dropped packets issue

- Refer to the "1204-06" section of the SecureSync Option Card document for additional info

Patch version 4.8S, as well as 5.x.x updates contain a patch to reset the network processor if it stops responding. It checks each of the processors every 10 seconds and resets any of them that stops responding to packets.
Per Dave Sohn- "The port appears to recover within a second or two". The total time that a port may not respond to packets is the 10 seconds between checks of the processor plus just a couple of seconds for the port to be restarted.
Example entries in the System log when the network processor is restarted:
Note this entry indicates which Ethernet port was restarted ("eth1" in this example)

```
Aug  6 12:34:41 Spectracom Spectracom: [system] GbE port eth1 event: RNBC=51 (KMOND)
Aug  6 13:31:33 Spectracom Spectracom: [system] GbE port eth1 event: RNBC=102 (KMOND)
```

Timekeeper.log entries

- Timekeeper log added to the log bundles starting in update version 5.2.0
- Placed in the /var/log directory
- Refer to the "**Logs tab**" Section of VelaSyncAndGeoCustAssist.pdf for details on analyzing logs

Timing log entries

IRIG input troubleshooting

A) SecureSync not syncing to an IRIG source

How to verify IRIG input signal issues

- Example timing.log entries if IRIG input is intermittent

```
Jun 22 15:01:40 Spectracom Spectracom: [system] 2015 173 15:01:39 021 IR irg0 Comm Lost.
Jun 22 15:01:44 Spectracom Spectracom: [system] 2015 173 15:01:44 000 IR irg0 Comm OK.
Jul 2 00:12:43 Spectracom Spectracom: [system] 2000 001 00:00:05 000 IR irg0 Comm OK.
Jul 8 16:53:02 Spectracom Spectracom: [system] 2015 189 16:53:02 021 IR irg0 Comm Lost.
Jul 8 17:06:52 Spectracom Spectracom: [system] 2015 189 17:06:52 000 IR irg0 Comm OK.
Jul 8 17:08:30 Spectracom Spectracom: [system] 2015 189 17:08:30 021 IR irg0 Comm Lost.
Jul 8 17:08:59 Spectracom Spectracom: [system] 2015 189 17:08:59 000 IR irg0 Comm OK.
Jul 8 17:09:23 Spectracom Spectracom: [system] 2015 189 17:09:23 021 IR irg0 Comm Lost.
Jul 8 17:10:28 Spectracom Spectracom: [system] 2015 189 17:10:28 000 IR irg0 Comm OK.
Jul 8 17:20:14 Spectracom Spectracom: [system] 2015 189 17:20:14 021 IR irg0 Comm Lost.
Jul 8 17:20:31 Spectracom Spectracom: [system] 2015 189 17:20:31 000 IR irg0 Comm OK.
Jul 8 17:21:31 Spectracom Spectracom: [system] 2015 189 17:21:31 021 IR irg0 Comm Lost.
```

Timing log entries associated with a uBlox M8T receiver installed

**Toggling between “GNSS FIX CHANGE: (5) to NONE (0)” / “GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)”

- Appears to be related to the uBlox receiver either dropping to less than 4 sats, or falling to 0 sats.
- Suggustion to fix- try deleting the receiver position for it to perform a new GPS survey.

```
l 30 01:45:28 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:28 000 PPS SYNC=0 Mode=1 tAcc=19 tAccClk=46 indoor=0 GPS Fix: NONE (0)
Jul 30 01:45:38 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:38 000 GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)
Jul 30 01:45:38 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:38 000 PPS SYNC=1 Mode=1 tAcc=109 tAccClk=56 indoor=0 GPS Fix: TIMEONLY (5)
Jul 30 01:45:39 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:39 000 GNSS FIX CHANGE: TIMEONLY (5) to NONE (0)
Jul 30 01:45:39 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:39 000 PPS SYNC=0 Mode=1 tAcc=67 tAccClk=109 indoor=0 GPS Fix: NONE (0)
Jul 30 01:45:41 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:41 000 GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)
Jul 30 01:45:41 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:41 000 PPS SYNC=1 Mode=1 tAcc=150 tAccClk=75 indoor=0 GPS Fix: TIMEONLY (5)
Jul 30 01:45:47 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:47 000 GNSS FIX CHANGE: TIMEONLY (5) to NONE (0)
Jul 30 01:45:47 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:47 000 PPS SYNC=0 Mode=1 tAcc=47 tAccClk=75 indoor=0 GPS Fix: NONE (0)
Jul 30 01:45:50 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:50 000 GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)
Jul 30 01:45:50 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:50 000 PPS SYNC=1 Mode=1 tAcc=85 tAccClk=52 indoor=0 GPS Fix: TIMEONLY (5)
Jul 30 01:45:54 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:54 000 GNSS FIX CHANGE: TIMEONLY (5) to NONE (0)
Jul 30 01:45:54 cx01pdix04 cx01pdix04: [system] 2017 211 01:45:54 000 PPS SYNC=0 Mode=1 tAcc=43 tAccClk=111 indoor=0 GPS Fix: NONE (0)
Jul 30 01:46:05 cx01pdix04 cx01pdix04: [system] 2017 211 01:46:05 000 GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)
Jul 30 01:46:05 cx01pdix04 cx01pdix04: [system] 2017 211 01:46:05 000 PPS SYNC=1 Mode=1 tAcc=186 tAccClk=128 indoor=0 GPS Fix: TIMEONLY (5)
Jul 30 01:54:13 cx01pdix04 cx01pdix04: [system] 2017 211 01:54:13 000 GNSS FIX CHANGE: TIMEONLY (5) to NONE (0)
Jul 30 01:54:13 cx01pdix04 cx01pdix04: [system] 2017 211 01:54:13 000 PPS SYNC=0 Mode=1 tAcc=10 tAccClk=49 indoor=0 GPS Fix: NONE (0)
Jul 30 01:54:14 cx01pdix04 cx01pdix04: [system] 2017 211 01:54:14 000 GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)
Jul 30 01:54:14 cx01pdix04 cx01pdix04: [system] 2017 211 01:54:14 000 PPS SYNC=1 Mode=1 tAcc=36 tAccClk=10 indoor=0 GPS Fix: TIMEONLY (5)
```

Timing log entries associated with a STL receiver Option Card installed

- The Timing log now contains burst information. Example log entries below

```
Oct  4 07:32:27 Spectracom Spectracom: [system] 2017 277 07:32:36 000 STL Status: Total Burst:1 Strong Burst:0
Oct  4 07:32:32 Spectracom Spectracom: [system] 2017 277 07:32:41 000 STL Status: Total Burst:2 Strong Burst:0
Oct  4 07:33:17 Spectracom Spectracom: [system] 2017 277 07:33:26 000 STL Status: Total Burst:3 Strong Burst:0
Oct  4 07:33:27 Spectracom Spectracom: [system] 2017 277 07:33:36 000 STL Status: Total Burst:2 Strong Burst:0
Oct  4 07:33:32 Spectracom Spectracom: [system] 2017 277 07:33:41 000 STL Status: Total Burst:1 Strong Burst:0
```

Note: Ryan indicated these entries show marginal reception

SAASM receiver-related entries (not applicable to commercial receivers)

Note: all SAASM log entries below are from tne same SecureSync which had low GPS signal strength/nearby jamming (examples of log entries- its not a complete log snippet)

```
Error 11
```

- Applicable to SAASM receiver only (Sent directly from the SAASM receiver and not one of our logs)
- Indicates the receiver’s BIOS battery is starting to fail, has failed or is not in the circuit (I believe, but not certain, this entry can indicate the on/off switch on the metal plate is off –the factory default position for this switch).

GPS Warning (63): Jamming detected single frequency

- Applicable to SAASM receiver only (Sent directly from the SAASM receiver and not one of our logs)
- Indicates either L1 or L2 is being jammed or has low signal strengths

```
2016 146 00:00:03 000 Current Status (SAASM): Days with keys=39
2016 146 00:00:08 000 SAAS Status Word 1 Changed: 0x80A7
2016 146 00:00:08 000 Days CVd's Available: 39
```

```
May  9 11:38:33 Spectracom Spectracom: [system] 2016 130 11:38:33 000 GPS Warning (62): Can't Acq/Track possible masking
May  9 11:47:00 Spectracom Spectracom: [system] 2016 130 11:47:00 000 Exit Sync: NumSats=3 NavConv=1 FOM=1 TFOM=3
HERR<=8 m VERR<=10 m mode=2 user=2
May  9 12:46:33 Spectracom Spectracom: [system] 2016 130 12:46:33 000 >=4 Measures
May  9 12:46:33 Spectracom Spectracom: [system] 2016 130 12:46:33 000 Tracking >=4 SV in State 5
May  9 12:46:34 Spectracom Spectracom: [system] 2016 130 12:46:33 000 Enter Sync: NumSats=4 NavConv=1 FOM=1 TFOM=3
HERR<=8 m VERR<=10 m mode=2 user=2
May  9 12:47:04 Spectracom Spectracom: [system] 2016 130 12:47:04 000 State 3 Operation (1)
May  9 12:47:08 Spectracom Spectracom: [system] 2016 130 12:47:08 000 Exit Sync: NumSats=3 NavConv=1 FOM=1 TFOM=3
HERR<=8 m VERR<=10 m mode=2 user=2
May  9 12:47:10 Spectracom Spectracom: [system] 2016 130 12:47:10 000 State 3 Operation (0)
May  9 12:47:10 Spectracom Spectracom: [system] 2016 130 12:47:10 000 Enter Sync: NumSats=4 NavConv=1 FOM=1 TFOM=3
HERR<=8 m VERR<=10 m mode=2 user=2
May  9 12:47:21 Spectracom Spectracom: [system] 2016 130 12:47:21 000 <4 Measures
May  9 12:47:24 Spectracom Spectracom: [system] 2016 130 12:47:24 000 Exit Sync: NumSats=3 NavConv=1 FOM=1 TFOM=3
HERR<=8 m VERR<=10 m mode=2 user=2
May  9 16:07:34 Spectracom Spectracom: [system] 2016 130 16:07:34 000 Tracking >=4 SV in State 5
May  9 16:17:57 Spectracom Spectracom: [system] 2016 130 16:17:57 000 GPS Warning (51): RAIM exclusion failed
May  9 16:18:27 Spectracom Spectracom: [system] 2016 130 16:18:27 000 GPS Warning (51): RAIM exclusion failed
May  9 16:18:57 Spectracom Spectracom: [system] 2016 130 16:18:57 000 GPS Warning (51): RAIM exclusion
May  9 17:59:21 Spectracom Spectracom: [system] 2016 130 17:59:20 000 GPS Warning (51): RAIM exclusion failed
May  9 18:00:04 Spectracom Spectracom: [system] 2016 130 18:00:03 000 Exit Sync: NumSats=7 NavConv=1 FOM=1 TFOM=4
HERR<=8 m VERR<=9 m mode=2 user=2
May  9 18:00:21 Spectracom Spectracom: [system] 2016 130 18:00:20 000 Enter Sync: NumSats=7 NavConv=1 FOM=1 TFOM=3
HERR<=8 m VERR<=9 m mode=2 user=2
May  9 18:07:28 Spectracom Spectracom: [system] 2016 130 18:07:27 000 GPS Warning (51): RAIM exclusion failed
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:01 000 GR entered failure state.
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:10 000 GSSIP: Communication OK.
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:11 000 GR exited failure state.
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:14 000 RCVR passed self-test
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:15 000 Current Status (SAASM): Days with keys=27
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:15 000 Current Status (SAASM) Changed: 0x0002
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:15 000 Current Status (SAASM): Contains today's key
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:16 000 SAASM EVENT: KEYS_VALID=TRUE The SAASM Key Is
Valid
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:16 005 GR entered failure state.
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:16 000 GR exited failure state.
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:16 000 GR antenna ok.
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:18 000 >=4 Measures
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:18 000 Tracking >=4 SV in State 5
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:20 000 NAV Data Valid
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:21 000 Enter Sync: NumSats=8 NavConv=1 FOM=1 TFOM=3
HERR<=13 m VERR<=19 m mode=0 user=0
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 SAAS Status Word 1 Changed: 0x809B
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 Days CVd's Available: 27
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 RCVR is keyed
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 SAAS Status Word 2 Changed: 0x04A0
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 KDP IP Zeroize Not Attempted
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 KDP CV Zeroize Not Attempted
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 KDP Status: Operational
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 SAASM Lock Status: RCVR Locked
May  9 18:55:36 Spectracom Spectracom: [system] 2000 001 00:00:22 000 SAASM Memory Status: Not Zeroized
May  9 18:55:36 Spectracom Spectracom: [system] 2016 130 18:54:45 000 GPS Warning (63): Jamming detected single frequency
May  9 18:55:36 Spectracom Spectracom: [system] 2016 130 18:55:35 000 GPS Mode changed from Continuous [0] to Averaging [2].
May  9 18:55:39 Spectracom Spectracom: [system] 2016 130 18:55:39 001 HR: Enabling Host Disciplining Mode.
May  9 19:05:10 Spectracom Spectracom: [system] 2016 130 19:05:10 000 GPS Warning (63): Jamming detected single frequency
May  9 19:14:28 Spectracom Spectracom: [system] 2016 130 19:14:28 000 Current Status (SAASM): Days with keys=55
May  9 19:14:29 Spectracom Spectracom: [system] 2016 130 19:14:29 000 SAAS Status Word 1 Changed: 0x80B7
May  9 19:14:29 Spectracom Spectracom: [system] 2016 130 19:14:29 000 Days CVd's Available: 55
May  9 19:15:18 Spectracom Spectracom: [system] 2016 130 19:15:18 000 GPS Warning (63): Jamming detected single frequency
```

Harris software only (such as version 5.4A)

Phase Chg(1): Fph=108.3551 LAvg=95.2027 Thr=200.0000

- ➢ This entry is at least currently limited to just Harris update version 5.4a only

Per Paul Myers (20 Jun 16) This is a log entry for the new Harris feature to detect 1PPS Jumps from the receiver. It detected a phase change.

GR: Enter Holdover due to Phase Invalid Timeout.

- ➢ Refer to Salesforce case 25697

“Error: CS_Set(CS_SA_LEAP_SEC) call from GR”

- ➢ This condition is caused by firmware issues with the Trimble RES-SMT-GG receiver (firmware version 1.07 which was made available starting in software update version 5.1.7)

  Per Dave Sohn (21 Oct 2014) We're not sure yet whether 1.07 fixes this specific issue. We received conflicting info from Trimble. However, this error does not cause any bad side effects so can be ignored by the customer and will be resolved in an upcoming SW release.

“GR antenna fault” / “GR antenna ok”

- ➢ These entries indicate opens/shorts being detected in the antenna cable and then clearing.

“GPS Startup/Reset detected”

- ➢ There are three (3) primary reasons for this alarm and condition to occur:

  1) System reboot

  2) Receiver configuration changes that require receive to reset (such as changing the receiver mode from Standard to mobile mode). Detailed in “A)” further below

  3) Marginal/poor reception. Detailed in “B)” further below.

Note: Paul Myers believes the receiver reset due to marginal reception is likely associated with factors such as multipath reception causing the receiver to perform another GPS survey to recalculate its position. This will affect its 1PPS output.

“2000 001 00:00:01” after [system] (default boot-up year and time)

[system] 2000 001 00:00:01 000 GPS Startup/Reset detected

- ➢ SecureSync was rebooted or power cycled

- ➢ Default startup date and time: Year 2000 and time of 00:00:00 (Date and time is then updated by RTC to the estimated correct date/time).

2014 134 01:28:54 000 GPS Startup/Reset detected (Correct year/date after [system]”)

```
`[system] 2014 328 15:50:58 000 GPS Startup/Reset detected
```

- **Likely causes are either:**
  - User made config changes to the receiver that required the receiver to need to restart

    Note: Look in the Journal log to see if there are any corresponding log entries for GPS/GNSS receiver config changes being made. Example change that will reset the receiver include changing the receiver mode – such as standard to mobile mode for instance).

  - RES-T GPS receiver reset itself in an attempt to improve marginal reception.
- The fix to prevent this from occurring is to: either improve GPS reception or upgrade to Glonass Option.

Modified Email Keith sent to Logix (2 June 2014)

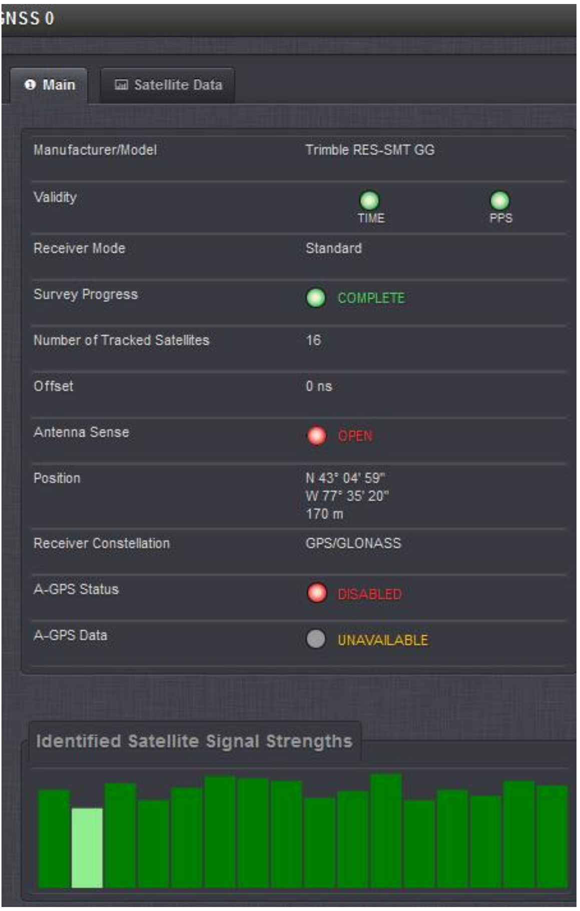
Regarding the "GPS receiver resets" and associated SecureSync alarms, the GPS receiver may internally reset itself when operating in a marginal reception environment (such as tracking only 2 or 3 satellites, for example). This is an attempt to improve its reception. The other condition that causes the GPS receiver to reset is when the unit first boots-up. The way to differentiate between the two conditions is in the associated log entry for each, the year will be "2000" when its due to a reboot, or the year will be the current year when the receiver resets due to marginal GPS reception. Below are examples of each type of receiver reset.

```
Feb 21 19:31:06 Spectracom Spectracom: [system] 2000 001 00:00:01 000 GPS Startup/Reset detected
Feb 21 19:31:06 Spectracom Spectracom: [system] 2000 001 00:00:01 000 GPS Startup/Reset detected
Feb 21 19:31:06 Spectracom Spectracom: [system] 2000 001 00:00:03 000 GPS Startup/Reset detected
Feb 21 19:31:07 Spectracom Spectracom: [system] 2000 001 00:00:03 000 GR antenna ok.
Mar  7 05:48:01 HOU-GPS-02 HOU-GPS-02: [system] 2014 066 05:48:00 000 GPS Startup/Reset detected
Apr  9 22:38:12 HOU-GPS-02 HOU-GPS-02: [system] 2000 001 00:00:01 000 GPS Startup/Reset detected
Apr  9 22:38:12 HOU-GPS-02 HOU-GPS-02: [system] 2000 001 00:00:02 000 GPS Startup/Reset detected
Apr  9 22:38:12 HOU-GPS-02 HOU-GPS-02: [system] 2000 001 00:00:03 000 GPS Startup/Reset detected
May 13 01:32:36 HOU-GPS-02 HOU-GPS-02: [system] 2014 133 01:32:36 000 GPS Startup/Reset detected
```

When the GPS receiver resets because of marginal or poor GPS reception, its 1PPS output will likely be restored out of phase with where it was at before it was reset. While the receiver is resetting, it will track 0 satellites for a few seconds as the logs you sent were indicating). Also, the Frequency alarm will be asserted because of the loss of 1PPS input (or if GPS goes not valid for a period of time). Once the internal oscillator has been re-disciplined, the Frequency alarm will clear. The Restart Tracking you had performed is a way to expedite clearing of this alarm.

To prevent the receiver from being reset due to marginal reception, the receiver needs to be able to track more satellites on a regular basis. There are essentially two ways to increase the number of satellites it can track (one may be more feasible than the other). The first it to relocate the GPS antenna to an area with more view of the sky (such as on top of the parking garage, instead of on the side of the building). However, if this isn't possible, the other method is to use the Model 8230 GNSS antenna (instead of the earlier Model 8226 GPS antenna) and a GNSS receiver inside the SecureSync, with the Glonass satellite Option enabled. This will allow the newer Model receiver to track both GPS and Glonass satellites simultaneously. Instead of tracking just 2 GPS satellites, it's likely to also track a few Glonass satellites also. So to the receiver, it's now tracking 5 satellites instead of 2 satellites, for example. It goes from poor reception to good reception with no need for it to try to improve the reception it has. This is the primary advantage of the Glonass satellite capability recently becoming available for SecureSync.

With Model 8230 GNSS antennas already installed, instead of the earlier Model 8225 antenna), in order to enable the Glonass capability, the two SecureSyncs would just need to be returned for a receiver replacement/Glonass enabling (unless they already have the newer GNSS receiver installed –then the option can be enabled in the field). If the top of the **Interfaces** -> **GNSS 0** page of the browser reports the receiver Model is a Resolution T receiver, this is a GPS only receiver and needs to be replaced for Glonass capability. The newer GPS/Glonass receiver is a Model RES-SMT receiver (as shown below):



Manufacturer/Model	Trimble RES-SMT GG
Validity	● TIME ● PPS
Receiver Mode	Standard
Survey Progress	● COMPLETE
Number of Tracked Satellites	16
Offset	0 ns
Antenna Sense	● OPEN
Position	N 43° 04' 59" W 77° 35' 20" 170 m
Receiver Constellation	GPS/GLONASS
A-GPS Status	● DISABLED
A-GPS Data	● UNAVAILABLE

As a quick summary of the Glonass satellite capability, this particular RES-SMT receiver is tracking satellites, seven of which are Glonass satellites.

Please let us know if you would like additional information on upgrading the SecureSyncs to Glonass capability to improve the number of satellites each of the SecureSyncs can track.

“Rb peak voltage error(val=0, min=51, max=255)” entries.

- The oscillator is reporting to the SecureSync that it isn’t operating normally. This value inside the oscillator is reading “0” when it should be between 51 and 255.

Email from Mark McGregor (20 Aug 2014) When that signal is low there is no atomic lock and the 10 MHZ will be off frequency. I would suggest the customer measure the 10 MHz. When the Rb peak signal is too low it will either be stuck 100 to 200HZ low or will move below and above 10 MHZ trying to find the Rb peak signal. If the 10 MHZ looks OK, then the failure is intermittent. The SecureSync does a great job of monitoring the Rb health. It reads health information every second, so if the atomic clock is lost even for a moment, it will report it right away in the logs. There are many case of this intermittent failure in other RMA and factory production test.

Transfer.log (transfer log entries)

- Entries related to software updates, for the save and restore of the configs.
- This log is not viewable via the browser (its included in the saved log bundle)
- This log is not wiped when performing a “clear all logs” in the browser

Update.log (update log entries)

- Normal Log entries from our SecureSync 10.2.100.176 after successful update of 5.1.5 to 5.1.6 (ascending order)

```
Oct 20 11:48:43 Custservice Custservice.176: [sw-upgrade] Using installed update tool from current version (SWUAL)
Oct 20 11:52:25 Custservice Custservice.176: [sw-upgrade] Using update tool supplied by upgrade (SWUAL)
Oct 20 11:53:41 Custservice Custservice.176: [spupdate] Application 5.1.5 5.1.6 Upgrade Needed (SWUE)
Oct 20 11:53:41 Custservice Custservice.176: [spupdate] Licensing  - No Upgrade Available (SWUE)
Oct 20 11:53:41 Custservice Custservice.176: [spupdate] Licensing  - No Upgrade Available (SWUE)
Oct 20 11:53:41 Custservice Custservice.176: [spupdate] Timing FW 3.17 3.17 No Upgrade Needed (SWUE)
Oct 20 11:53:41 Custservice Custservice.176: [spupdate] Timing FPGA 3.17 3.17 No Upgrade Needed (SWUE)
Oct 20 11:53:42 Custservice Custservice.176: [spupdate] GNSS 1.6 - No Upgrade Available (SWUE)
Oct 20 11:53:42 Custservice Custservice.176: [spupdate] Timing EEPROM 1.00  No Upgrade Available (SWUE)
Oct 20 11:53:42 Custservice Custservice.176: [spupdate] OC 1  ID 1F 0101 1.01 No Upgrade Needed (SWUE)
Oct 20 11:53:42 Custservice Custservice.176: [spupdate] OC 2  ID 06 0000 - No Upgrade Available (SWUE)
Oct 20 11:53:43 Custservice Custservice.176: [spupdate] OC 3  ID FF 0000 - No Upgrade Available (SWUE)
Oct 20 11:53:43 Custservice Custservice.176: [spupdate] OC 4  ID FF 0000 - No Upgrade Available (SWUE)
Oct 20 11:53:43 Custservice Custservice.176: [spupdate] OC 5  ID 01 0103 1.03 No Upgrade Needed (SWUE)
Oct 20 11:53:44 Custservice Custservice.176: [spupdate] OC 6  ID 32 0121 1.21 No Upgrade Needed (SWUE)
Oct 20 11:53:44 Custservice Custservice.176: [spupdate] Preparing Application Software for Upgrade  (SWUE)
Oct 20 11:53:54 Custservice Custservice.176: [sw-upgrade] Upgrade Initiated, Reboot Required: /home/spectracom/update516.tar.gz (SWUAL)
Oct 20  11:59:33  TRANSFER_ENGINE: [SUCCESS] Update successful
```

Update log entries when an issue occurred with an update

B) Update log contains only the first entry "Using installed update tool from current version (SWUAL)"

- Indicates the CF card was likely too full to unpack bunde. Be sure to delete any previous version bundles. Perfrom a **df -h** command to chech disk usage.

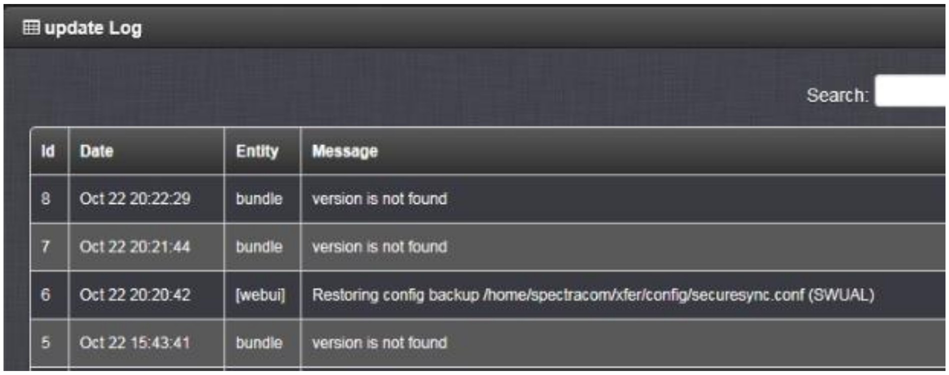
C) Update log entry indicates "[sw-upgrade] Upgrade Initiated, Reboot Required: home/spectracom/update517.tar.gz (SWUA)"

- Observed with 5.1.4 to 5.1.7 update
- Should be fixed with 5.1.J beta/ Version 5.2.0 software update (Feb 2015).
- Refer to Salesforce cases such as 16749 (Jump Trading)
- Unit doesn't complete the upgrade because it can't reboot.
- Reboot commands via browser/CLI don't work.
- Requires a hard power cycle of the unit to finish the update.
- Dave Sohn noted this has been observed with Verizon likely due to the potential pipe software command issue in 5.1.7 and below. "This sounds similar to the Verizon issue as well. I believe when we had an issue with one of the units, the hung process prevented the reboot. In that case, it took a hard power cycle to recover it."

"Upgrading GNSS Firmware (SWUE)" followed by "Problem writing GPS FW image (SWUE)"

- Starting software version (before update process was started) was versions 5.1.4 or below. The RES-SMT-GG receiver's firmware wasn't able to be updated because the starting version needs to be version 5.1.5 or higher to be able to update the receiver.
- Run the same software update process again to successfully update the GNSS receiver's firmware.

Version is not found” entry following “Restoring Config backup” entry when performing a “config restore”



update Log

Search:

Id	Date	Entity	Message
8	Oct 22 20:22:29	bundle	version is not found
7	Oct 22 20:21:44	bundle	version is not found
6	Oct 22 20:20:42	[webui]	Restoring config backup /home/spectracom/xfer/config/securesync.conf (SWUAL)
5	Oct 22 15:43:41	bundle	version is not found

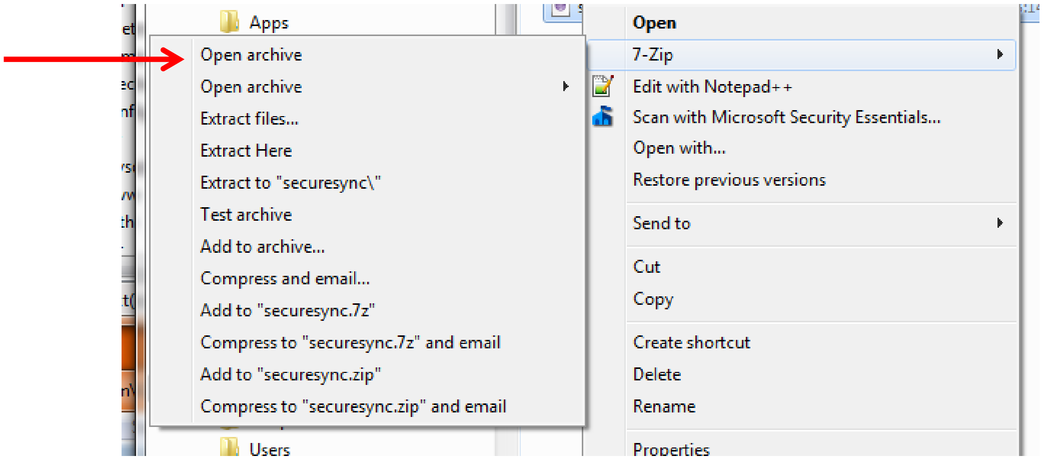
- ➢ Has been observed with a corrupt config backup file.

Note: Trying to apply a saved config file saved from a newer version than the target unit may result in a “**Version is not found**” entry in the Update log.

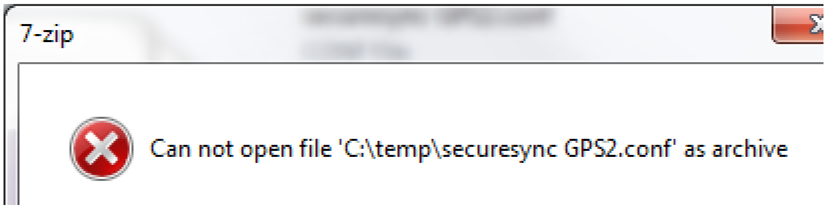
Important Note: When manually transferring the config file using FTP/SFTP, make sure to **BINARY** mode (not ASCII) ASCII mode will corrupt the file.

There is only one way to confirm if the config backup file has been corrupted.

1) Save config backup to “temp” directory for instance
2) Right click and select a program to extract the file (such as 7-Zip)
3) Select “Open Archive”



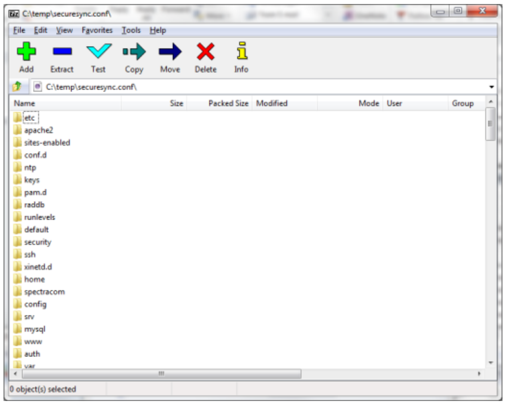
4) Below is an example report of a **corrupt file.**



7-zip

Can not open file 'C:\temp\securesync GPS2.conf' as archive

Example of a valid config backup file (Open Archive)



```
C:\temp\securesync.conf\

Name            Size   Packed Size   Modified   Mode   User   Group
etc
apache2
sites-enabled
conf.d
ntp
keys
pam.d
raddb
runlevels
default
security
ssh
xinetd.d
home
spectracom
config
srv
mysql
www
auth
var

0 object(s) selected
```

- This may happen when trying to apply to a target unit (with 5.0.0 or higher software) a backup file that was taken from a later version of software, which was also 5.0.0 or above (5.1.5 backup was trying to be restored to a version 5.1.4 SecureSync. But a newer version can't be installed on an earlier version, even if both are 5.0.0 and above with an MOTD file). But this isn't confirmed.

- This may also occur when trying to restore configs from a v4.8.9 or below unit to one running 5.0.2 or above. But this isn't confirmed.

user.log entries

- This log is not accessible from the browser. Is in the Saved Logs bundle.
- This log is not wiped when performing a "clear all logs" in the browser
- Refer to the LDAP/Radius section of this document for more info on the User log entries.

System Reboot or halt (not power cycle)

```
"shutting down for system reboot"

pam_radius_auth: RADIUS server 10.82.122.16 failed to respond
pam_radius_auth: All RADIUS servers failed to respond.
```

- Indicates likely network issue between SecureSync and Radius servers

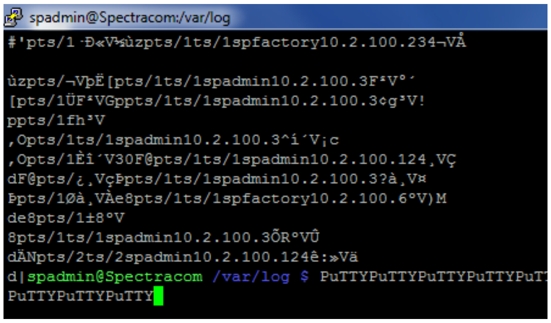
wtmp.log

- File located in home/spectracom/log directory
- Records reboots and succesful logins/logouts,
- 0.0.0.0 indicates a local/internal connection. An IP address indicates external connection (ssh, browser, serial)
- File clears on each reboot/power cycl

What is the wtmp file (refer to: http://linux.die.net/man/5/wtmp**)**"

The *wtmp* file records all logins and logouts. Its format is exactly like *utmp* except that a null username indicates a logout on the associated terminal"

Example from our server



```
#'pts/1 ·Ð«V½ùzpts/1ts/1spfactory10.2.100.234¬VÅ

ùzpts/¬VþË[pts/1ts/1spadmin10.2.100.3F²V°´
[pts/1ÜF²VGppts/1ts/1spadmin10.2.100.3¢g³V!
ppts/1fh³V
,Opts/1ts/1spadmin10.2.100.3^í´V¡c
,Opts/1Èí´V30F@pts/1ts/1spadmin10.2.100.124¸VÇ
dF@pts/¿¸VçÞpts/1ts/1spadmin10.2.100.3?à¸V¤
Þpts/1Øà¸VÀe8pts/1ts/1spfactory10.2.100.6°V)M
de8pts/1±8°V
8pts/1ts/1spadmin10.2.100.3ÕR°VÛ
dÄNpts/2ts/2spadmin10.2.100.124ê:»Vä
d|spadmin@Spectracom /var/log $ PuTTYPuTTYPuTTYPuTTYPuT
PuTTYPuTTYPuTTY
```

Slightly modified Email (I added the word “successful” to “logins”) from Paul Myers (28 Feb 17)

This wtmp file records the reboots starts/stops, successful logins and logouts.
Every time a person logs in succesfully it is recorded.
If this file is large maybe they are automating a test login or they have provided a user account to an authenticated security scan to probe the unit or they are doing some type of automatic login and web scraping??

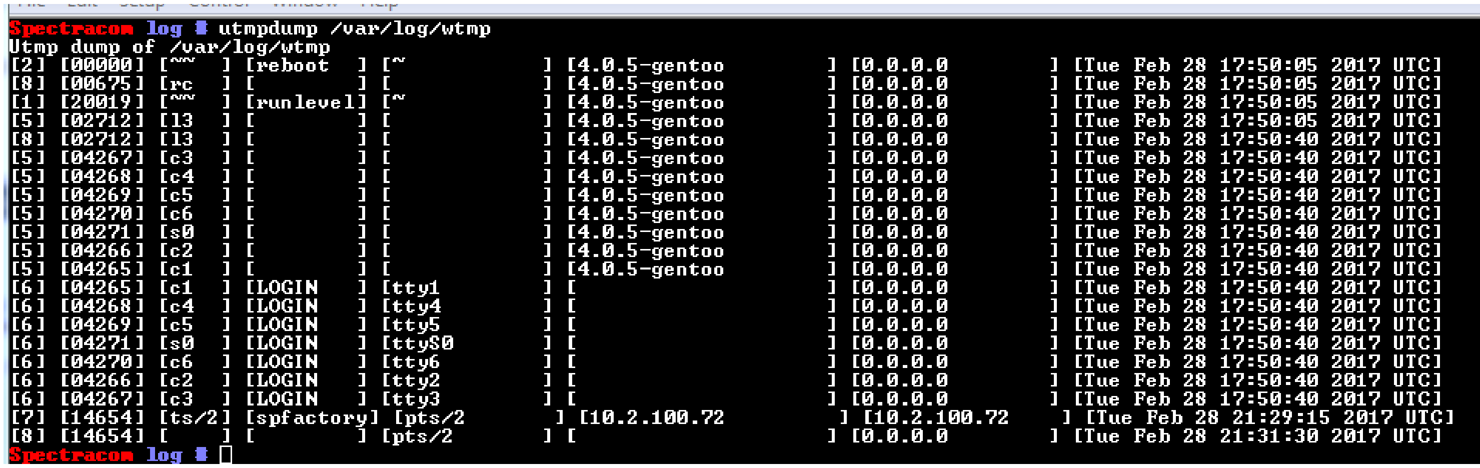
http://www.linuxquestions.org/questions/linux-security-4/var-log-wtmp-72976/ https://linux.die.net/man/5/wtmp

(**Note**: Running the following tool converts the raw wtmp file to a readable binary file)

utmpdump /var/log/wtmp | less <enter> to review recent succesful logins. If the login is from a remote location, it will be associated with a specific IP address outside your network. Examples below:

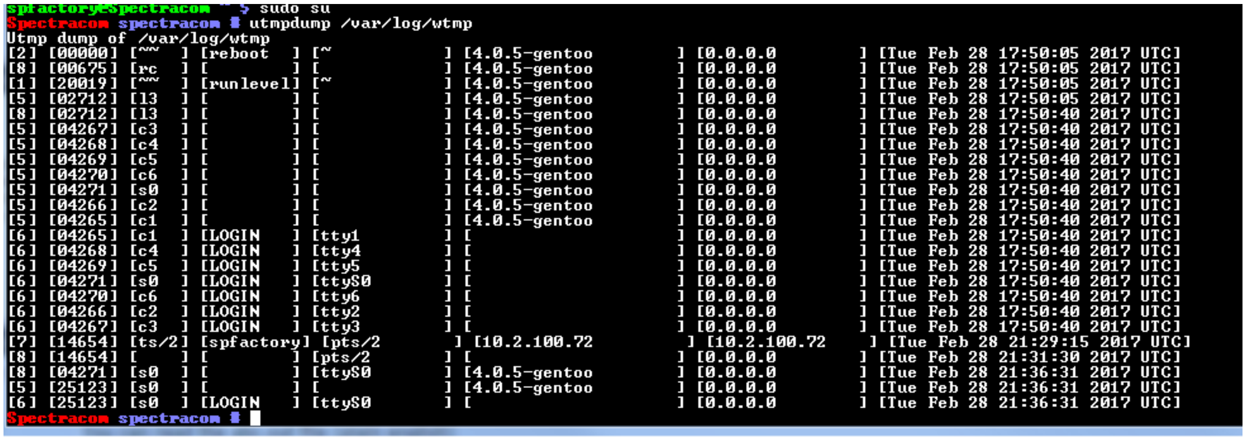
additional notes

- Space to scroll
- Shift and q to quite



```
Spectracom log # utmpdump /var/log/wtmp
Utmp dump of /var/log/wtmp
[2] [00000] [~~  ] [reboot  ] [~           ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:05 2017 UTC]
[8] [00675] [rc  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:05 2017 UTC]
[1] [20019] [~~  ] [runlevel] [~           ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:05 2017 UTC]
[5] [02712] [l3  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:05 2017 UTC]
[8] [02712] [l3  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04267] [c3  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04268] [c4  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04269] [c5  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04270] [c6  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04271] [s0  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04266] [c2  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04265] [c1  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04265] [c1  ] [LOGIN   ] [tty1        ] [                    ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04268] [c4  ] [LOGIN   ] [tty4        ] [                    ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04269] [c5  ] [LOGIN   ] [tty5        ] [                    ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04271] [s0  ] [LOGIN   ] [ttyS0       ] [                    ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04270] [c6  ] [LOGIN   ] [tty6        ] [                    ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04266] [c2  ] [LOGIN   ] [tty2        ] [                    ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04267] [c3  ] [LOGIN   ] [tty3        ] [                    ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[7] [14654] [ts/2] [spfactory] [pts/2        ] [10.2.100.72          ] [10.2.100.72     ] [Tue Feb 28 21:29:15 2017 UTC]
[8] [14654] [    ] [        ] [pts/2       ] [                    ] [0.0.0.0         ] [Tue Feb 28 21:31:30 2017 UTC]
Spectracom log #
```

Continued from Paul’s Email above See the last 2 entries above?
I logged into the unit using ssh and logged out.
Logging into a serial port and staying logged in is shown below:

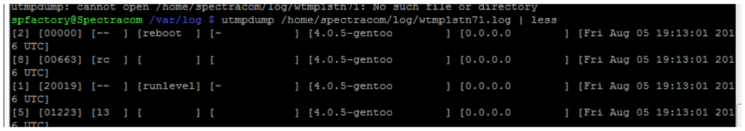


```
spfactory@Spectracom ~ $ sudo su
Spectracom spectracom # utmpdump /var/log/wtmp
Utmp dump of /var/log/wtmp
[2] [00000] [~~  ] [reboot  ] [~           ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:05 2017 UTC]
[8] [00675] [rc  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:05 2017 UTC]
[1] [20019] [~~  ] [runlevel] [~           ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:05 2017 UTC]
[5] [02712] [l3  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:05 2017 UTC]
[8] [02712] [l3  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04267] [c3  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04268] [c4  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04269] [c5  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04270] [c6  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04271] [s0  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04266] [c2  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[5] [04265] [c1  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04265] [c1  ] [LOGIN   ] [tty1        ] [                    ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04268] [c4  ] [LOGIN   ] [tty4        ] [                    ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04269] [c5  ] [LOGIN   ] [tty5        ] [                    ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04271] [s0  ] [LOGIN   ] [ttyS0       ] [                    ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04270] [c6  ] [LOGIN   ] [tty6        ] [                    ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04266] [c2  ] [LOGIN   ] [tty2        ] [                    ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[6] [04267] [c3  ] [LOGIN   ] [tty3        ] [                    ] [0.0.0.0         ] [Tue Feb 28 17:50:40 2017 UTC]
[7] [14654] [ts/2] [spfactory] [pts/2        ] [10.2.100.72          ] [10.2.100.72     ] [Tue Feb 28 21:29:15 2017 UTC]
[8] [14654] [    ] [        ] [pts/2       ] [                    ] [0.0.0.0         ] [Tue Feb 28 21:31:30 2017 UTC]
[8] [04271] [s0  ] [        ] [ttyS0       ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 21:36:31 2017 UTC]
[5] [25123] [s0  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Tue Feb 28 21:36:31 2017 UTC]
[6] [25123] [s0  ] [LOGIN   ] [ttyS0       ] [                    ] [0.0.0.0         ] [Tue Feb 28 21:36:31 2017 UTC]
Spectracom spectracom #
```

To convert a wtmp file to a readable file

1. If it’s a customer’s wtmp file from a log bundle, FTP/SCP (using spfactory account and using “default” transfer mode) the wtmp file, into the **home/spectracom/log** directory of one of our units
2. Running the following tool converts the raw wtmp file to a readable binary file):

   utmpdump /home/spectracom/log wtmp.log | less <enter> (where **wtmp.log** is the name of the wtmp log file desire to look at) to review recent logins. If the login is from a remote location, it will be associated with a specific IP address outside your network.



```
utmpdump: cannot open /home/spectracom/log/wtmp1stn71: No such file or directory
spfactory@Spectracom /var/log $ utmpdump /home/spectracom/log/wtmp1stn71.log | less
[2] [00000] [~~  ] [reboot  ] [~           ] [4.0.5-gentoo        ] [0.0.0.0         ] [Fri Aug 05 19:13:01 201
6 UTC]
[8] [00663] [rc  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Fri Aug 05 19:13:01 201
6 UTC]
[1] [20019] [~~  ] [runlevel] [~           ] [4.0.5-gentoo        ] [0.0.0.0         ] [Fri Aug 05 19:13:01 201
6 UTC]
[5] [01223] [l3  ] [        ] [            ] [4.0.5-gentoo        ] [0.0.0.0         ] [Fri Aug 05 19:13:01 201
6 UTC]
```

Notes

- Space to scroll
- Shift and q to quite

NTP operation

- Good doc for definition of terms associated with NTP: http://support.ntp.org/bin/view/Support/NTPRelatedDefinitions

NTP and Chrony in 2400 SecureSybcs

- **Note**: in at least versions 1.4.1 and below, the base 2400 SecureSync (interfaces eth0 and eth1) still runs ntpd, while the available add-on network Option Cards (dual and quad, for examples) are running chrony.
- As of ~ July 2022, Product Management and Engineering have started investigating what needs to be done to switch the Base SecureSync interfaces (eths 0 and 1) from ntpd over to chrony.

NTP Versions in the base software

Refer also to: I:\Customer Service\PSB, PSP software updates\948x and SecureSync\948x and SecureSync Software updates\Software release dates.xlsx

Quick summary below (in descending order):

System Version	NTP version	Note
V1.4.1	**v4.2.8p15**	

Chrony/chronyd

- Refer to "chrony/chronyd" in the Customerserviceassist doc: I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf
- Appears to replace NTP for linux systems. "chrony is a pair of programs for maintaining the accuracy of computer clocks. chronyd is a background daemon program that can be started at boot time.
- Link to "refclock_tsyncpci.c" file referenced in the email further below: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\Timing boards\TSync family\chrony-chronyd (replacing NTP)

Comparison of chrony, ntp and openntpd: refer to https://chrony.tuxfamily.org/comparison.html

Chronyd is a daemon which runs in background on the system. It obtains measurements (e.g. via the network) of the system's offset relative to other systems, and adjusts the system time accordingly. For isolated systems, the user can periodically enter the correct time by hand (using *chronyc*). In either case, **chronyd** determines the rate at which the computer gains or loses time, and compensates for this."

From https://chrony.tuxfamily.org/
Chrony is a versatile implementation of the Network Time Protocol (NTP). It can synchronize the system clock with NTP servers, reference clocks (e.g. GPS receiver), and manual input using wristwatch and keyboard. It can also operate as an NTPv4 (RFC 5905) server and peer to provide a time service to other computers in the network.

Compatibility of a Chrony client with a standard NTP time server (such as SecureSync)

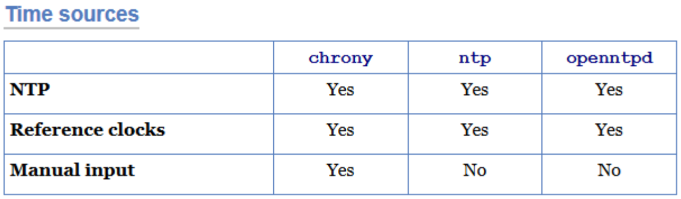
Refer also to Salesforce case 24565

Email from Paul Myers (27 Feb 17) The SecureSync runs the NTP daemon standard implementation with the current release being 4.2.8p9 in Release 5.5.1

We do NOT run chrony on the SecureSync, however, a chrony client should be compatible. See the section 1.1 overview of manual which indicates it can support NTPv4 (RFC 5905)

https://chrony.tuxfamily.org/comparison.html

https://chrony.tuxfamily.org/manual.html



Time sources

	chrony	ntp	openntpd
NTP	Yes	Yes	Yes
Reference clocks	Yes	Yes	Yes
Manual input	Yes	No	No

Another example indicating how a Chrony client can sync to an NTP server is via Section 2: Installation of Chrony of the Chrony manual at" https://chrony.tuxfamily.org/manual.html#Installation

Now that the software is successfully installed, the next step is to set up a configuration file. The default location of the file is '/etc/chrony.conf'. Several examples of configuration with comments are included in the examples directory. Suppose you want to use public NTP servers from the pool.ntp.org project as your time reference. A minimal useful configuration file could be

```
pool pool.ntp.org iburst
makestep 1.0 3
rtcsync
```

NTP Best practices document (Writen by Denis Reilly)

- Here is a link to the "IETF Best Practices draft for NTP": https://datatracker.ietf.org/doc/draft-ietf-ntp-bcp/

RFC 8915: Network Time Security (NTS) for the Network Time Protocol (NTS)

- RFC for NTS officially Released ~Oct 2020
  - Refer to https://tools.ietf.org/html/rfc8915

    "This memo specifies Network Time Security (NTS), a mechanism for using Transport Layer Security (TLS) and Authenticated Encryption with Associated Data (AEAD) to provide cryptographic security for the client-server mode of the Network Time Protocol (NTP).
    NTS is structured as a suite of two loosely coupled sub-protocols. The first (NTS Key Establishment (NTS-KE)) handles initial authentication and key establishment over TLS. The second (NTS Extension Fields for NTPv4) handles encryption and authentication during NTP time synchronization via extension fields in the NTP packets, and holds all required state only on the client via opaque cookies.

Additional info

- Refer to sites such as: https://blog.apnic.net/2019/11/08/network-time-security-new-ntp-authentication-mechanism/

  https://datatracker.ietf.org/doc/rfc8915/?include_text=1

Current Status (as of Nov 2020)

- Refer to Salesforce Case 252350

Q Email from Keith (13 Nov 2020) to Emmanuel/Apps I just received a call from Preston Cleary with Franchise Tax Board (California), inquiring about the new **RFC 8915: Network Time Security for the Network Time Protocol (NTS**) as it pertains to their SecureSyncs (1200s in his case).
I see the specs are now "official" (as of October), but couldn't find any info on when its expected to be available in NTP. Once its available, will this just be integrated into SecureSyncs (1200 and 2400s) via a standard software upgrade to the NTP package?   Will it be available for all 1200/2400 customers, as a "feature update", or will it be limited to just the 2400s/purchased update? Etc. I told Preston I would "ask around" to see about getting additional info to share with him.

A Reply from Emmanuel (16 Nov 2020) We're working on it, as this has been identified as a key security consideration.
Our current plan is to introduce NTS on 2400 (it requires to migrate the NTP implementation from NTPd to Chrony) as part of the 1.5 release (expected Q3 2021).
Then we'll do our best to port this implementation also on 1200 (this should be facilitated by the 1200/2400 platform convergence), and we will target to have it implemented on 1200 by end of next year.

NTP's timescale

- NTP output follows the System timescale (if the System Timescale is UTC, NTP output time will also be UTC)
- Unlike the 9300/9200 series (which can be independently configured to output UTC or GPS timescale) in at least versions 5.4.0 and below, NTP
- Changing the System Timescale to a different value (such as UTC to TAI) will cause ntpmond to force NTP to stop/restart because of the greater than one second error that will occur once the change is complete. A log entry should be aserted in the NTP log.

Statusd daemon for obaining status info from NTP (v5.3.0 and above)

statusd (NTP status deamon)

Software update version 5.3.0 incorporated changes in how info from NTP is obtained for items such as the web browser, SNMP, the CLI interface and the front panel to report.

- Refer to mantis cases 3140 and especially 3067.
- The new statusd daemon was added in software version 5.3.0
  - Previously, several different threads were all calling NTPQ to get similar NTP status (NTP sync state, Stratum level, etc). Sometimes there could be too many calls to NTPQ. statusd limits the number of calls to only one thread which grab all of the status data and stores it in /tmp - giving all the other threads a centralized location to get the ntp data without having to use ntpq.
- statusd was initially called masterd but was renamed shortly thereafter to statusd (Mantis case 3094)
- Version 5.4.0 redesigned-improved statusd for lower CPU cycles.

Issue with too many threads calling NTPQ

Example System.log entries associated with an issue where NTPQ stops talking to NTP to get NTP status

```
Feb 23 15:37:12 ny4-apr-gps2 ny4-apr-gps2: [system] System command error: NTPQ_ReadSysstats (NTPAL)
Feb 23 15:37:12 ny4-apr-gps2 ny4-apr-gps2: [system] Failed to read NTP system statistics (NTPMOND

Feb 23 15:39:34 ny4-apr-gps2 ny4-apr-gps2: [system] System command error: NTPQ_GetAsscVariable (NTPAL)
Feb 23 15:39:34 ny4-apr-gps2 ny4-apr-gps2: [system] NTPQ_GetAsscVariable(ASSC_VAR_LEAP) returned [rc = 1] (KHTD)
```

`[system] System command error fpaneld:DT_DrawStat (FPD)` (only asserted if the front panel has been reconfigured to display

NTP status info instead of network settings).

- Refer to Salesforce cases such as 19242, 19468 and 21098
- Symptons of this issue with NTPQ include the above log entries,
  - “ntp status” CLI command no longer responding
  - Web Browser and SNMP not reporting NTP status
  - Front panel not able to display NTP status (if it’s been reconfigured to display NTP status).
- This issue was seen in software version 5.2.1 (reported in 5.3.0 as well, but likely due to a different reason)

This status information reported on the front panel (if the SecureSync has been configured to display Status information instead of the network settings, as many customers choose to display) includes the NTP Stratum and NTP Sync status.

Email Keith sent (12 Feb 16) Both the NTP Status CLI command stopping to respond and the “System command error fpaneld:DT_DrawStat (FPD)” log entry are related to the SecureSync having earlier software version 5.2.1 installed, instead of the latest version of version 5.3.1 being installed.

Software versions 5.2.1 and below has several software threads running the NTPQ query tool to obtain similar status information from NTP (such as NTP sync status and Stratum level). Functions that all need to obtain this similar status info from NTP include the web browser, SNMP, CLI interface as well as the front panel LCD (when the front panel has been configured by a user to display NTP status info instead of the factory default setting of displaying network settings).

With all these functions calling NTPQ to get the NTP status, NTPQ could become overwhelmed with requests and therefore stop responding with this NTP status info (all other calls not needing NTP status info can continue to respond just fine while NTPQ is in this state).). The “…fpaneld:DT_DrawStat (FPD)” error message observed in the log is due to the front panel also trying to display NTP status info (just like the CLI command) but it’s not able to obtain the data from NTP.

Version 5.3.0 update added a new daemon called statusd, which centralized the request for NTP status info to a single thread, minimizing the number of instances of NTPQ needing to be run at the same time.

I recommend you consider updating the software to version 5.3.1 (or to version 5.4.0 when its released in a few weeks) to prevent this potential NTP status reporting condition from occurring. Note that in general, we recommend the SecureSync always have the latest version of software installed, as issues such as this are fixed with periodic updates we make available (we seldom remove functionalities with our software updates. The SecureSync updates add new capabilities and address potential software conditions that may be present. Customers with optional PSP packages or who have registered their contact info on our website are provided a notice when software updates become available☺!

Changes incorporated to statusd daemon

- **Version 5.3.0 update:** Created/added statusd to improve software CPU cycle usage.
- **V5.4.0 update:** Redesign of statusd and other daemons to improve software CPU cycle usage.
- **Version 5.4.5 update:** Modification of statusd to support NTPQ commands being issued in a single thread at a time.
- **Note**: As indicated in SR 7112 and the associated logs, too many instances of NTPQ runnin in versions prior to v5.4.5 can apparently cause oops,.bug.taint, call trace errors in kern log and eventually the out of memory manager killing apache to try to free up some addional memory.

Issues associated with statusd

A) Versions prior to 5.4.5 may potentially run too many simultaneous instances of NTPD, resulting in oops.taint. call trace and eventual out of memory manager killing apache.

B) Commanded shutdown resulted in system.log show statusd continuously restarting

- refer to Salesforce case 175134
- below is example from system.log

```
Oct  1 19:50:35 ntp01sldcmo ntp01sldcmo: [system] NTP generic status polling (pid=23922, tid=b6fedb40): thread started  (STATUSD)
Oct  1 19:50:35 ntp01sldcmo ntp01sldcmo: [system] NTP extended status polling (pid=23922, tid=b65ffb40): thread started  (STATUSD)
Oct  1 19:51:42 ntp01sldcmo ntp01sldcmo: [system] statusd has started  (STATUSD)
Oct  1 19:51:42 ntp01sldcmo ntp01sldcmo: [system] NTP generic status polling (pid=26580, tid=b6f57b40): thread started  (STATUSD)
Oct  1 19:51:42 ntp01sldcmo ntp01sldcmo: [system] NTP extended status polling (pid=26580, tid=b65ffb40): thread started  (STATUSD)
Oct  1 19:52:50 ntp01sldcmo ntp01sldcmo: [system] statusd has started  (STATUSD)
Oct  1 19:52:50 ntp01sldcmo ntp01sldcmo: [system] NTP generic status polling (pid=29271, tid=b6f95b40): thread started  (STATUSD)
Oct  1 19:52:50 ntp01sldcmo ntp01sldcmo: [system] NTP extended status polling (pid=29271, tid=b65ffb40): thread started  (STATUSD)
Oct  1 19:53:58 ntp01sldcmo ntp01sldcmo: [system] statusd has started  (STATUSD)
Oct  1 19:53:58 ntp01sldcmo ntp01sldcmo: [system] NTP generic status polling (pid=31988, tid=b6f09b40): thread started  (STATUSD)
Oct  1 19:53:58 ntp01sldcmo ntp01sldcmo: [system] NTP extended status polling (pid=31988, tid=b65ffb40): thread started  (STATUSD)
Oct  1 19:55:06 ntp01sldcmo ntp01sldcmo: [system] statusd has started  (STATUSD)
Oct  1 19:55:06 ntp01sldcmo ntp01sldcmo: [system] NTP generic status polling (pid=2132, tid=b6f05b40): thread started  (STATUSD)
Oct  1 19:55:06 ntp01sldcmo ntp01sldcmo: [system] NTP extended status polling (pid=2132, tid=b65ffb40): thread started  (STATUSD)
Oct  1 19:56:14 ntp01sldcmo ntp01sldcmo: [system] statusd has started  (STATUSD)
Oct  1 19:56:14 ntp01sldcmo ntp01sldcmo: [system] NTP generic status polling (pid=4744, tid=b6fa7b40): thread started  (STATUSD)
Oct  1 19:56:14 ntp01sldcmo ntp01sldcmo: [system] NTP extended status polling (pid=4744, tid=b65ffb40): thread started  (STATUSD)
```

C) Setting the “Minimum CPU temperature” thresholds to above “100” causes statusd to continuously reset. Statusd continuously resetting prevents it from being able to provide NTP status info from NTPQ where necessary. NTP runs fine. But NTP status is reported as “??” because statusd keeps clearing out the values obtained from NTPQ.

- "TemperatureThreshold" settings (one for for Major alarmand one for Minior alarm) are in located in the \config\temperature.conf file

Email Keith sent to a customer (4 Apr 16): Please just make sure that the neither of the two “**Minimum CPU temperature**” thresholds (toward the bottom of the **Management** -> **Notifications** page of the browser, **System** tab) are sent to a value above “**100**”.

As of just this morning, we found the browser will allow you to set a value above the highest available setting of “100” (no error message is asserted when either or both is set to above “100”). But having either or both of these values set to above “100” will cause statusd (the status daemon for reporting status information such as from NTP) to keep restarting.

If either or both of these values is set to a value greater than 100, please set it back to the default value of “100” and press submit to keep the status daemon from resetting.

Spectracom Reference Clock Driver (127.127.45.0)- “TSync(0)”

- Allows NTP to sync to System Time

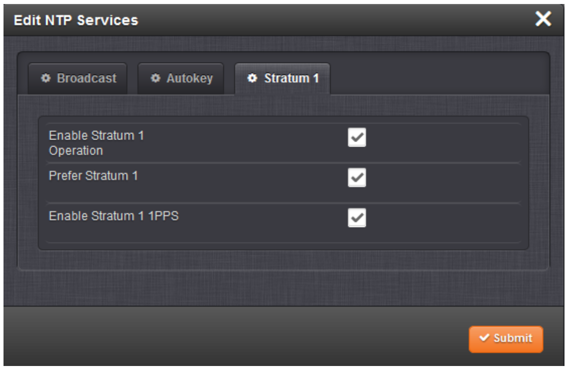
- Enabled when the “timing System Reference (***Management*** -> ***NTP Setup*** page, “**NTP Servers”** tab) is Enabled.
- When enabled, adds a “System Time” row to the Status -> NTP page (as shown below).
- Reference ID (Ref ID) for the Spectracom driver reference is “.GPS”

127.127.45.0 is the **Spectracom Reference Clock driver** which allows NTP to obtain time from System Time.

In SecureSync series

A) web browser

Management -> **NTP Setup** page of the browser (click the gear icon to the right of “**NTP Services**” and select the **Stratum 1** tab)



Edit NTP Services

Enable Stratum 1 Operation ☑

Prefer Stratum 1 ☑

Enable Stratum 1 1PPS ☑

In SecureSync series “NTP expert mode

```
server 127.127.45.0 prefer minpoll 4
```

(**Note**: “prefer” being present indicates the “preferred” checkbox is enabled)

In NTP log (when synced to System Time): `ntpd[826]: synchronized to PCI_TSYNC(0), stratum=0`

Note: The Reference Clock driver (127.127.45.0) is valid for NTP input when input references such as GPS, IRIG, Havequick, etc, are valid or if in Self mode. However, it’s not valid when syncing SecureSync to other NTP servers.

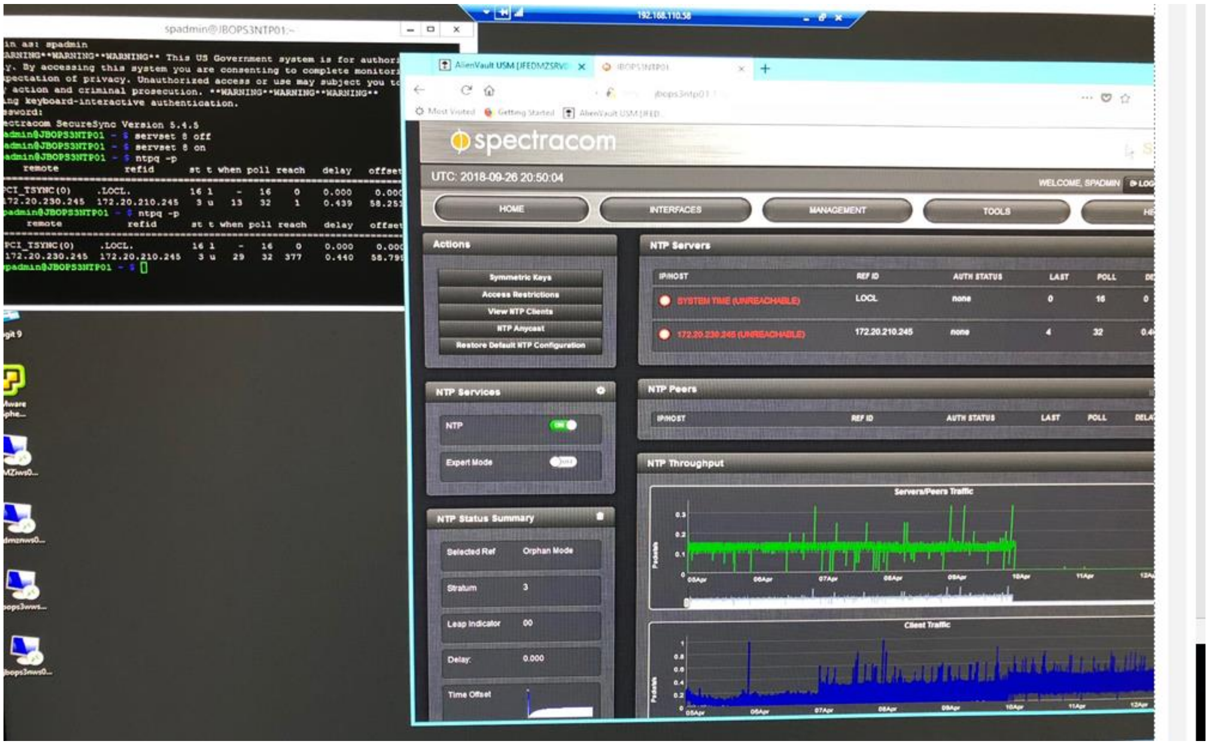
NTP Orphan mode/orphanwait / Undisciplined Local Clock Reference (127.127.1.0)

Orphan Mode (versions 5.2.1 and above)

- In software versions 5.2.0 and below, the NTP local clock reference was used to force NTP to go to Stratum 16.
- Orphan mode was added in NTP version v4.2.2 to replace the undisciplined Local Clock reference. So when we updated NTP to version 4.2.8p2 in software version 5.2.1, we had to start using NTP Orphan mode in its place.
- Orphan Mode allows a group of ntpd processes to autonomously select a leader in the event that all real time sources become unreachable (i.e. are inaccessible).
- Info about NTP Orphan mode, refer to:http://www.eecis.udel.edu/~mills/ntp/html/orphan.html and http://support.ntp.org/bin/view/Support/OrphanMode
- If there are no input references available for NTP to sync with, it will go into Orphan mode.

Indications of a time server being in Orphan mode are in the ntpq -p (peers command).

- The refid will be **127.0.0.1**
- its Reach value will **remain at "0".**



```
spadmin@JBOPS3NTP01:~
in as: spadmin
ARNING**WARNING**WARNING** This US Government system is for author
y. By accessing this system you are consenting to complete monitor
pectation of privacy. Unauthorized access or use may subject you to
 action and criminal prosecution. **WARNING**WARNING**WARNING**
ng keyboard-interactive authentication.
ssword:
ectracom SecureSync Version 5.4.5
admin@JBOPS3NTP01 ~ $ servset 8 off
admin@JBOPS3NTP01 ~ $ servset 8 on
admin@JBOPS3NTP01 ~ $ ntpq -p
   remote           refid      st t when poll reach   delay   offset
==============================================================================
PCI_TSYNC(0)    .LOCL.          16 l    -   16    0    0.000    0.000
172.20.230.245  172.20.210.245   3 u   13   32    1    0.439   58.251
padmin@JBOPS3NTP01 ~ $ ntpq -p
   remote           refid      st t when poll reach   delay   offset
==============================================================================
PCI_TSYNC(0)    .LOCL.          16 l    -   16    0    0.000    0.000
172.20.230.245  172.20.210.245   3 u   29   32  377    0.440   58.795
padmin@JBOPS3NTP01 ~ $ 
```

UTC: 2018-09-26 20:50:04

NTP Servers

IP/HOST	REF ID	AUTH STATUS	LAST	POLL
SYSTEM TIME (UNREACHABLE)	LOCL	none	0	16
172.20.230.245 (UNREACHABLE)	172.20.210.245	none	4	32

NTP Status Summary

Selected Ref	Orphan Mode
Stratum	3
Leap Indicator	00
Delay:	0.000
Time Offset	

Orphan Mode is enabled by adding the line "tos orphan N" anywhere in ntp.conf. The N specifies the stratum at which this ntpd will switch to Orphan Mode. For example, an ntpd using tos orphan 6 will not switch to Orphan Mode as long as a time source of strata 1 through 5 is reachable. The recommended value for N is 2 less than the worst-case externally-reachable source of time.

In addition to the tos orphan line all members of the Orphan Mode group must be configured in a *mesh* (i.e. they must all be clients / peers of each other). Any NTP association mode may be used to set up this mesh.

Email from Dave Sohn regarding a customer desiring SecureSync to be Stratum 4 when not in sync (30 Nov 15) What SW version are they using? In more recent versions, there should be two additional lines in the ntp configuration file:

```
tos orphanwait 1
tos orphan 15
```

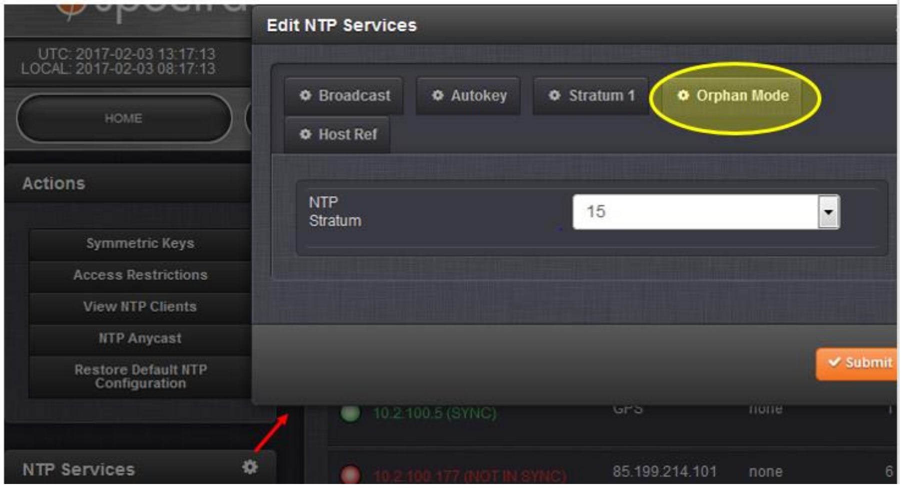
The second line "tos orphan 15" controls the out of sync stratum level. If they changed this to "tos orphan 4", the stratum level reported during the slewing, and when out of sync, will be 4. The functionality of NTP is such that even though it is slewing to the reference, it won't report the selection of the peer until it is closer in.

orphanwait 1 (our factory default setting is "1") tells NTP to wait 1 second after losing all references before going into Orphan mode.

"Orphan Mode" configuration in the newer (black/charcoal) browser (can change what stratum NTP goes to when not in sync)

- Factory default value is "**15**" (NTP clients won't sync to this NTP server when NTP is not synced to a reference)

Management -> ***NTP Setup*** page of the newer browser. Press the gear ICON to the right of "**NTP Services**" and then select the "**Orphan Mode**" tab (as shown below):



NTP Stratum: 15

Our Factory default settings for orphanmode and orphanwait settings

(Regarding SF case 164267)
Per Dave Sohn (4 Jun 18) Orphanmode in 5.8.0 is still default of 15. The orphanwait setting is 1.

"Local Clock Reference (127.127.1.0)" enable/disable field

- Field is located in ***Network*** -> ***NTP Setup*** page of the browser, NTP Servers tab
- When enabled (default setting), NTP is allowed go to stratum 16 when input reference is either jittery or no input references are present.
- When disabled (not normally recommended) NTP will never go to Stratum 16. Its time stamps will never output as Stratum 0, so NTP clients won't ever ignore te time stamps as being questionable.
- When disabled, and if no other NTP inputs are present or not valid, NTP.log will insert an entry of "no servers reachable."

Starting in Archive software version 4.8.6, a new enable/disable field has been added, in order to disable NTP's local clock reference (if needed or desired). Disabling this checkbox may help improve NTP operation when NTP's input reference(s) are not very stable or are periodically being lost.
The "Local Clock *Reference*" enable option determines whether or not NTP uses its Local Clock Reference as its selected reference, in the event all other references are lost or not selected due to stability, reliability or jitter. The Local Clock Reference degrades the NTP stratum to 15 by default when selected, so an NTP server without references cannot synchronize a timing chain of NTP servers.

When NTP selects the Local Clock Reference over any other external reference(s), NTP will go to Stratum 16 (by default). If NTP's inputs are not very stable (jittery) or are periodically not present, NTP may switch back and forth between Stratum 1 (or Stratum 2) and Stratum 16. While at Stratum 16, NTP will be ignored by the network clients. When it switches back to Stratum 1 or 2 again, it is considered a valid reference. An example where NTP may switch between an external reference and the Local Clock Reference is syncing SecureSync to an IRIG generator that is not externally synced to GPS, for instance. The IRIG input will not be jittery, resulting in NTP periodically selecting the Local Clock Reference over the IRIG generator, because the internal clock is more stable than the IRIG generator.

The Local Clock Reference can be disabled if the user does not desire this feature or to avoid switching between a reference and the Local Clock driver when the reference is intermittently reachable or less stable than the Local Clock. The Local Clock stratum can be adjusted to values other than 15 by using NTP Expert Mode.

Effects on NTP when the System Time is manually changed to something else

I just ran a test to confirm what I expected to have happen, when the time is manually set while NTP is already running.

The time can't be manually set with any higher priority references being present and valid. So, for this test, I was initially synced to IRIG. I then disabled IRIG input and all references other than USER/USER. I then set the System Time ahead by about 6 minutes (this was at 10:04:07 Eastern).

At about 10:05:23 Eastern, NTP noticed System Time had jumped, because its offset value became a very high number. This caused NTP to momentarily go to Stratum 16, with no time jump occurring on the NTP outputs (still outputting the incrementing time, based on the time it was before the time was manually advanced). Time clients would still be syncing to it, still using the old time being incremented.

AT about 10:08:53 Eastern, NTP went back to Stratum 1 with no time jump occurring on the NTP outputs (still outputting the incrementing time, based on the time it was before the time was manually advanced). Time clients would still be syncing to it, still using the old time being incremented.
This same operation continued (NTP still outputting the old time just incrementing) until about 10:22 Eastern, when NTP stepped it's time to much closer to the manually set time. The NTP Offset significantly decreased at this point, but was not nearly 0. Jitter went up, as expected because of the large time change. This was about 17 minutes after I manually set the time.

Just after the step (about 10:23 Eastern), NTP temporarily went back to Stratum 16 again, but made a 6 minute time jump and the NTP packets advanced by about 6 minutes (still remaining at Stratum 16- NTP clients would ignore it right now).

At about 10:24:17 Eastern, NTP went back to Stratum 1 and the NTP packets were still 6 minutes ahead of the actual time, because the time had been manually set. NTP did adjust for the 6 minute time advance that I made happen by manually setting the time (though NTP doesn't like to do this). The Total elapsed time for when NTP Clients would see the time advance and be able to use the advanced time, was about 20 minutes after the manual set.

As I had mentioned, NTP takes quite a while to perform an unexpected time jump. In this case, it saw a 6 minute time difference than it expected to get from System Time. NTP said that its drift calculations must be WAY off, so it had to go through a process of recalculating the "error" in its calculations, in order for it to bring its time in alignment with the "new: System Time reference.

This is the expected operation for NTP when switching between references that are not closely aligned with each other.

Note: If the NTP input time changes while NTP is running, the poll interval will affect how long it takes for NTP to notice and adjust for an input time changes (the longer then poll Interval, the longer it will likely take).

*RFC 2783 (PPS clock driver, 127.127.22.0)

- Pulse-Per-Second API to discipline the Linux kernel.
- For more info, refer to http://tools.ietf.org/html/rfc2783
- PPS clock driver is 127.127.22.0

Email from Dave Sohn (6 Feb 2013) Starting in 5.0.2, we use an rfc 2783 interface for our timing system interface to source a 1PPS to NTP to discipline it.

Q. Is the SecureSync model we have compliant with RFC 2783 (attached)? If yes, is there any documentation we can show that proves it is?
A (Reply From Keith) Regarding your question about RFC 2783, the answer to this is: As of Archive software version 5.0.2, SecureSync does now use an RFC 2783 interface for our timing system to source a 1PPS signal to NTP, to discipline the Linux kernel.

Signal 15 (“NTP Exiting on Signal 15”) or other signals

- Refer to http://stackoverflow.com/questions/16723626/what-is-signal-15-received
- This indicates the linux has delivered a `SIGTERM` to your process. This is usually at the request of some other process. This signal requests an orderly shutdown of your process (ntpd).

Web browser NTP / Chrony configurations

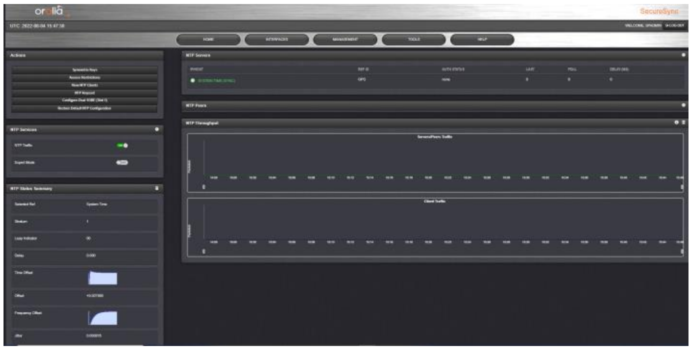
In at least versions 1.4.3 and below:

- eth0 and eth1 of the Base 2400 SecureSyncs run **NTP**
- ethernet interfaces of the 1204-49 Dual ethernet and 1204-50 quad GB ethernet Option Cards run **chrony**

Management -> NTP Setup page (used to configure both NTP and Chrony)

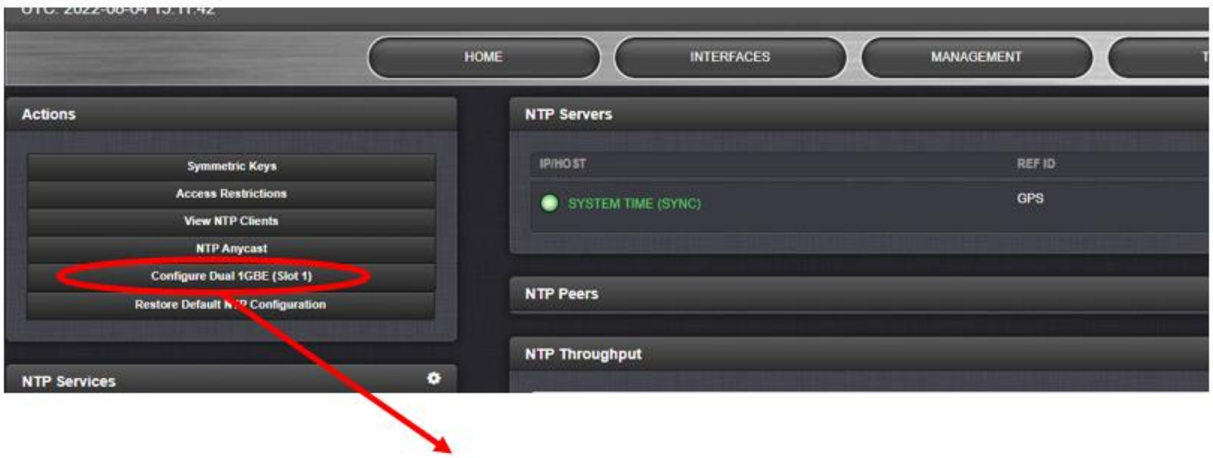
A) NTP Setup (base 2400 SecureSyncs, Eth0 and eth1)

Management -> ***NTP Setup*** page (similar to 1200 SecureSync)

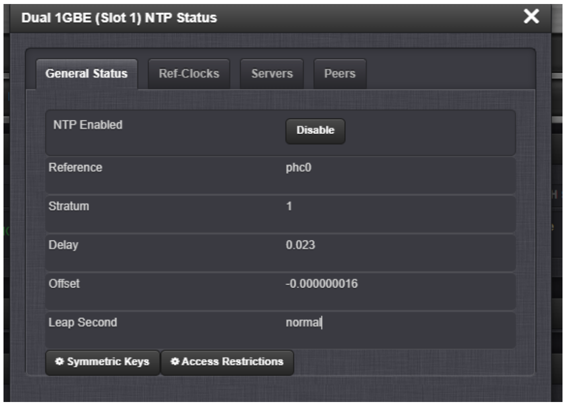


B) Chrony Setup (1204-49/1204-4A Dual/Qual ethernet cards, Eth0 and eth1)

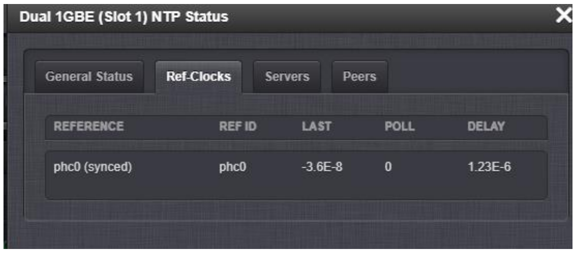
Management -> ***NTP Setup*** page (then click on either “**Configure Dual 1GBE**” or “**Configure Quad 1GBE**” button on the left side of the page)



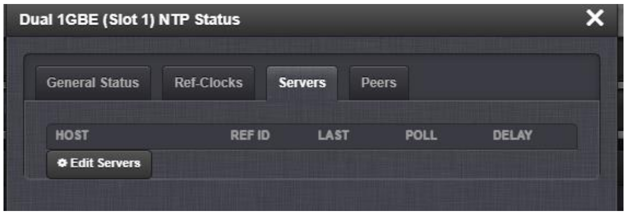
IP/HOST	REF ID
SYSTEM TIME (SYNC)	GPS



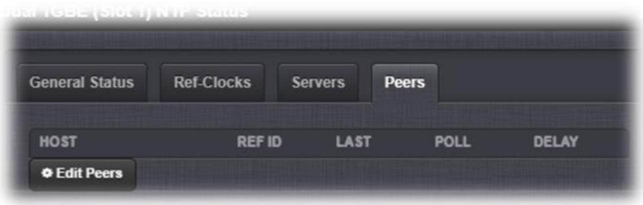
NTP Enabled	Disable
Reference	phc0
Stratum	1
Delay	0.023
Offset	-0.000000016
Leap Second	normal



REFERENCE	REF ID	LAST	POLL	DELAY
phc0 (synced)	phc0	-3.6E-8	0	1.23E-6



HOST	REF ID	LAST	POLL	DELAY



HOST	REF ID	LAST	POLL	DELAY

NTP drift file

- View NTP drift file in CLI: after going to /etc/ntp directory, type cat ntp.drift <enter>

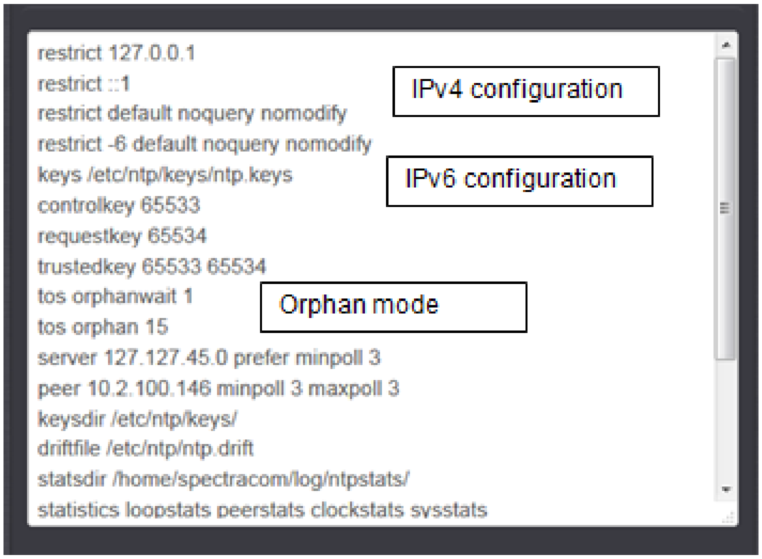
ntp.conf file

- Path to ntp.conf file: spectracom/etc/ntp
- View ntp.c**onf file in log bundle:** spectracom/etc/ntp

Default ntp.conf file settings and their purposes

A) Example default ntp.conf file from version 5.2.1 (ntp v4.2.8p2)

- Includes configs for NTP Orphan mode, starting in version 5.2.1 (replaced NTP Local clock ref)



```
restrict 127.0.0.1
restrict ::1
restrict default noquery nomodify
restrict -6 default noquery nomodify
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
tos orphanwait 1
tos orphan 15
server 127.127.45.0 prefer minpoll 3
peer 10.2.100.146 minpoll 3 maxpoll 3
keysdir /etc/ntp/keys/
driftfile /etc/ntp/ntp.drift
statsdir /home/spectracom/log/ntpstats/
statistics loopstats peerstats clockstats sysstats
```

tos ophanwait 1 and tos orphan 15: configurations for NTP Orphan mode (replaced NTP local clock in version 5.2.1)

- **orphanwait 1** tells NTP to wait 1 second after losing all references before going into Orphan mode.
- **tos orphan 15** tells ntp to go to Stratum 15 when in Orphan mode

restrict 127.0.0.1 and restrict ::1 You may need to add the following line to allow

unrestricted access from the localhost (so that you may monitor ntpd and perform on-the-fly configuration changes with ntpdc):

noquery: Ignore all NTP mode 6 and 7 packets (i.e., information queries and configuration requests) from the source.

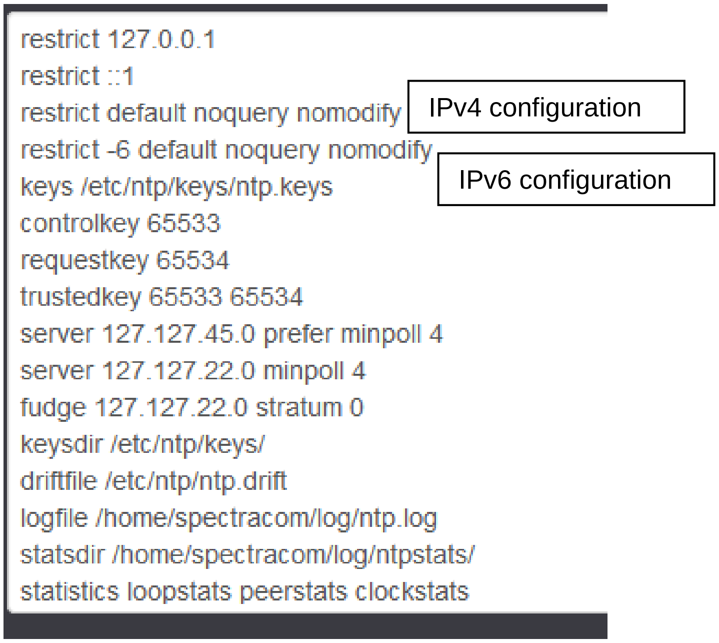
nomodify Ignore all NTP mode 6 and 7 packets which attempt to modify the state of the server (i.e., run time reconfiguration). Queries which return information are permitted.

Keys: path to the NTP keys file.

server: References NTP can sync with (such as System Time, NTP’s local ref or other time servers)

fudge: forces NTP to Stratum 1 when NTP is synced.

A. Example default ntp.conf file from version 5.1.6 (ntp V4.2.6)



```
restrict 127.0.0.1
restrict ::1
restrict default noquery nomodify
restrict -6 default noquery nomodify
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
server 127.127.45.0 prefer minpoll 4
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
keysdir /etc/ntp/keys/
driftfile /etc/ntp/ntp.drift
logfile /home/spectracom/log/ntp.log
statsdir /home/spectracom/log/ntpstats/
statistics loopstats peerstats clockstats
```

IPv4 configuration

IPv6 configuration

restrict 127.0.0.1 and **restrict ::1** You may need to add the following line to allow unrestricted access from the localhost (so that you may monitor ntpd and perform on-the-fly configuration changes with ntpdc):

noquery: Ignore all NTP mode 6 and 7 packets (i.e., information queries and configuration requests) from the source.

nomodify Ignore all NTP mode 6 and 7 packets which attempt to modify the state of the server (i.e., run time reconfiguration). Queries which return information are permitted.

Keys: path to the NTP keys file.

server: References NTP can sync with (such as System Time, NTP's local ref or other time servers)

fudge: forces NTP to Stratum 1 when NTP is synced.

Kiss of Death packets (KOD) for SecureSync/9400s

- Refer to the “KOD” section of Customerserviceassistance doc for general info on KOD
- Enabling” “KOD in SecureSync requires editing the ntp.conf file in expert mode

Q (from Sylvain) I have received the following question about our NTP server capability (SecureSync) “**NTP server implementations should include the ability to return a KOD (Kiss-of-Death Packet) Packet”**

Email from Dave Sohn (7 Oct 15) Being able to send the KOD packet is an advanced configuration on SecureSync that can be enabled on a restrict line of the NTP configuration file while in expert mode.

Reply from Sylvain to Dave S- So I understand in your message that the function is possible.
The customer will have to use the Expert mode and enter some additional extended configuration command line.

Shall I understand that: the customer will have to know the text to enter? I mean: we don’t provide the details of the text to enter – this is up to the customer to know what is the good text to enter depending on his system ?
I need this advice in order to anticipate the next question that the customer could ask to us…

Reply from Dave Sohn The kod flag is added on a restrict keyword line where kiss of death operation is desired. This is done in expert mode.

NTP verification/NTP troubleshooting

NTP is not reporting its not in sync/Stratum 15, when it really should be reporting its in sync/Stratum 1

- Such as what occurred with Salesforce case 128576
- **Descrition of this abnormal condition:** System is in sync with NTP enabled, but NTP is not reporting its not in sync, Stratum 15. NTP is likey able to sync NTP clients in this state, since its likely just an issue related to systemd/ntpq not being able to report the ntp status to the browser

General troubleshooting recommendatiins for this abnormal condtion:

1. try performing an **ntpq -p** (peers command) to see ifs able to report the status of ntp.
2. Try **restoring just the NTP configs** (via the button in the ***Managenent*** -> ***NTP Setup*** page of the browser) and see if NTP strarts reporting its status correctly d within a few minutes of NTP being restarted (refer to SF Case 128576 in the specific examples directly below)
3. optional- Try performing a clean command to restore all configs

Specific examples of this abnormal condition occurring

A) System log full of ERROR reading StatusNTP.curLI empty string (KHTD)

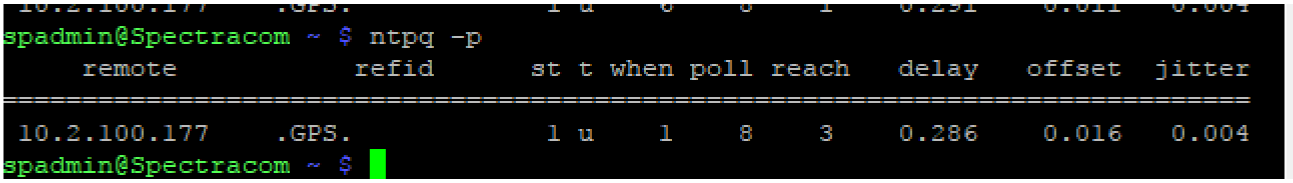
- Refer to SF case 128576

```
Mar 16 10:46:55 ADMN-SecureSync last message repeated 40 times
Mar 16 10:46:56 ADMN-SecureSync ADMN-SecureSync: [system] ERROR reading StatusNTP.curLI empty string (KHTD)
Mar 16 10:47:27 ADMN-SecureSync last message repeated 31 times
Mar 16 10:48:28 ADMN-SecureSync last message repeated 61 times
Mar 16 10:49:29 ADMN-SecureSync last message repeated 61 times
Mar 16 10:50:30 ADMN-SecureSync last message repeated 61 times
Mar 16 10:51:31 ADMN-SecureSync last message repeated 61 times
Mar 16 10:52:32 ADMN-SecureSync last message repeated 61 times
Mar 16 10:53:33 ADMN-SecureSync last message repeated 61 times
```

Finding/fix for this issue: Ron Dries saved a copy of the ntp.conf file and compated the saved conf file to the “default” ntp.conf file. He found a missing “restrict” line and some lines from an earlier version of NTP. Just performing a reset of the ntp configs fixed it the missing restrict line was preventing systemd from having permission to perform ntpq commands

Using the NTPQ -P command

- Refer to “NTPQ” in custassist doc for nore info on this query tool: ..\CustomerServiceAssistance.pdf
- Open CLI and type **ntpq -p** <enter>



```
 10.2.100.177    .GPS.            1 u    6    8    1    0.291    0.011    0.004
spadmin@Spectracom ~ $ ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 10.2.100.177    .GPS.            1 u    1    8    3    0.286    0.016    0.004
spadmin@Spectracom ~ $
```

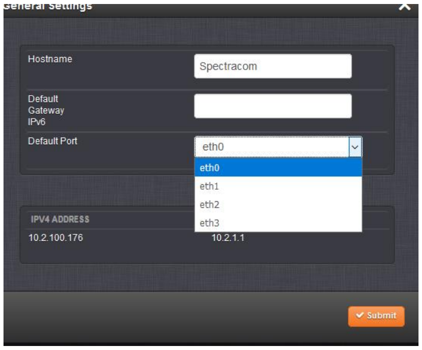
Reach value of “0”

Potential causes

- Port 123 closed on firewall in between
- Peeers/servers configured with DNS names (instead of IP addresses) and there is an issue with DNS settings/operation (in the time sever or on the network – verify DNS is configured correctly in the SecureSync)
- Configured NTP Peers/Server is a SecureSync and its NTP is not usable (stratum 16)
- (if 1204-06 Gb eth card is installed) SecureSync's main default port/default gateway is not configured correctly for thenetwork interface that has access to the configured NTP server/peer (such as to the Internet for an nternet time server)

Steps/Suggustuons to troubleshoot "Reach 0"

1. (if 1204-06 Gb eth card is installed) verify SecureSync's main default port/default gateway is not configured correctly (**Management** -> **Network Setup** page,. **General Setting** button)



General Settings

Hostname: Spectracom

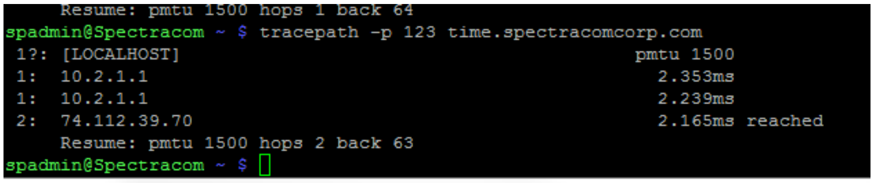
Default Gateway IPv6:

Default Port: eth0

2. In the CLI, perform a ~~**tracepatch**~~ **tracepatch** command (refer to info/example further below)
   - Refer to [tracepath and traceroute commands](#) (in this doc) for more info on this command.
   - Refer to: https://linux.die.net/man/8/tracepath for avaiable swithces

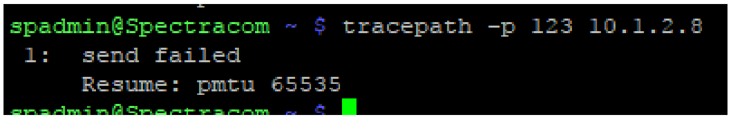
Type: **traceroute -p 123 xxxx** (where -p 123 defines NTP port and xxxx is the IP/hostname of the peer/server),   should respond with list of responses all the way to the peer/server

traceroute -p 123 time.spectracomcorp.com As shown below, verify the last value is **74.112.39.70** followed by "**reached**" at the end of the line:



```
     Resume: pmtu 1500 hops 1 back 64
spadmin@Spectracom ~ $ tracepath -p 123 time.spectracomcorp.com
 1?: [LOCALHOST]                                          pmtu 1500
 1:  10.2.1.1                                               2.353ms
 1:  10.2.1.1                                               2.239ms
 2:  74.112.39.70                                           2.165ms reached
     Resume: pmtu 1500 hops 2 back 63
spadmin@Spectracom ~ $ 
```

Example of a destination address not being available via port 123 ("send failed" to a bad address)

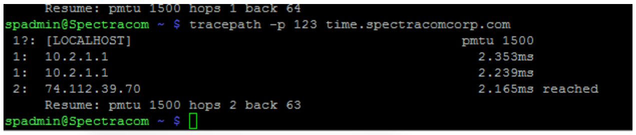


```
spadmin@Spectracom ~ $ tracepath -p 123 10.1.2.8
 1:  send failed
     Resume: pmtu 65535
spadmin@Spectracom ~ $ 
```

What is the "**Reach**" value for "nytime" (its row) in this ntpq -q response? Note it should be "377" if it can get receive good NTP packets from nytime (such as what is being reported in the second row of the screenshot above). If it's a "0", this SecureSync is not getting any NTP packets from nytime, or the NTP packets are indicating nytime is not in sync/Stratum1

The response to this command should list nytime's IP address/DNS host name in the first column. First try pinging this value (exactly as shown in the ntpq -p response) from the command prompt to ensure there is a response from nytime to this SecureSync.

Then at its command prompt, type the following: tracepath -p 123 time.spectracomcorp.com As shown below, verify the last value is **63.138.60.57** **(note this IP address may vary)** followed by "**reached**" at the end of the line:



```
    Resume: pmtu 1500 hops 1 back 64
spadmin@Spectracom ~ $ tracepath -p 123 time.spectracomcorp.com
 1?: [LOCALHOST]                                        pmtu 1500
 1:  10.2.1.1                                             2.353ms
 1:  10.2.1.1                                             2.239ms
 2:  74.112.39.70                                         2.165ms reached
     Resume: pmtu 1500 hops 2 back 63
spadmin@Spectracom ~ $ 
```

Repeat this same command above, but replace "time.spectracomcorp.com" (at the end of the command) with the exact IP/hostname for "nytime" (As reported in the ntpq -p response). The last value in this response should be the IP address of "nytime" (instead of 74.112.39.70) followed by "**reached**" at the end of the line (assuming nytime

3. Use **tcpdump** (via CLI) to confirm NTP requests are going out and if they are being returned (and if they are going out the correct port).

   The following command (v5.4.5 and above. If v5.4.1 or below, add ":sudo" to the beginning) should show all NTP packets being sent.and/or received on any of the network interfaces (eth0 and/or eth1/eth2/eth23 if 1204-06 card is installed): **tcpdump -i any port 123** (ctrl + c to stop the capture)

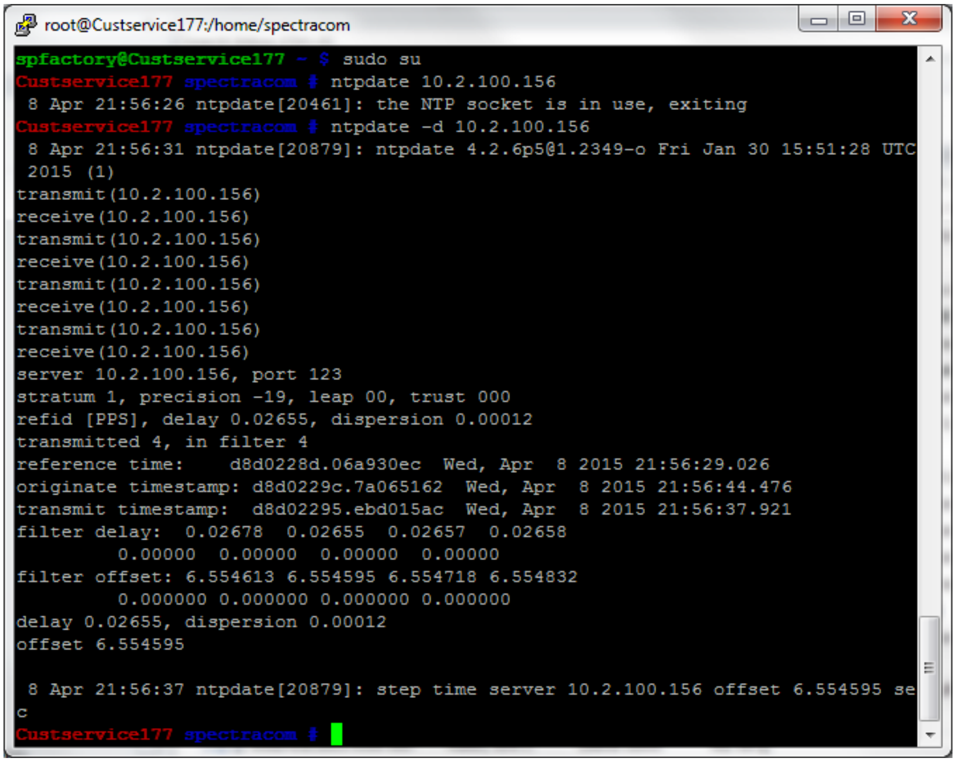
   Note: if tcdump responds with a password, tcpdump has disabled (and cant be re-enabled without performing a full update/restore to defaults

Using the ntpdate command

- " cannot be performed by spadmin, but "ntpdate -d" can be performed by spadmin
- Refer to sites such as http://www-01.ibm.com/support/knowledgecenter/ssw_aix_61/com.ibm.aix.cmds4/ntpdate.htm
- On a linux box, use the ntpdate command in debug mode (ntpdate -d xxx.xxx.xxx.xxx) to verify info in NTP packet.
- Reports info such as Stratum, delay, offset, refid, etc.

ntpdate

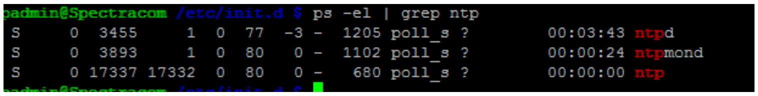
Internal use only: When using one of our SecureSyncs to perform this command, have to be logged in as root (not spadmin or spfactory) to perform "ntpdate". But don't need to be logged in as root to perform "ntpdate –d".



```
spfactory@Custservice177 ~ $ sudo su
Custservice177 spectracom # ntpdate 10.2.100.156
 8 Apr 21:56:26 ntpdate[20461]: the NTP socket is in use, exiting
Custservice177 spectracom # ntpdate -d 10.2.100.156
 8 Apr 21:56:31 ntpdate[20879]: ntpdate 4.2.6p5@1.2349-o Fri Jan 30 15:51:28 UTC
 2015 (1)
transmit(10.2.100.156)
receive(10.2.100.156)
transmit(10.2.100.156)
receive(10.2.100.156)
transmit(10.2.100.156)
receive(10.2.100.156)
transmit(10.2.100.156)
receive(10.2.100.156)
server 10.2.100.156, port 123
stratum 1, precision -19, leap 00, trust 000
refid [PPS], delay 0.02655, dispersion 0.00012
transmitted 4, in filter 4
reference time:    d8d0228d.06a930ec  Wed, Apr  8 2015 21:56:29.026
originate timestamp: d8d0229c.7a065162  Wed, Apr  8 2015 21:56:44.476
transmit timestamp:  d8d02295.ebd015ac  Wed, Apr  8 2015 21:56:37.921
filter delay:  0.02678  0.02655  0.02657  0.02658
         0.00000  0.00000  0.00000  0.00000
filter offset: 6.554613 6.554595 6.554718 6.554832
         0.000000 0.000000 0.000000 0.000000
delay 0.02655, dispersion 0.00012
offset 6.554595

 8 Apr 21:56:37 ntpdate[20879]: step time server 10.2.100.156 offset 6.554595 se
c
Custservice177 spectracom #
```

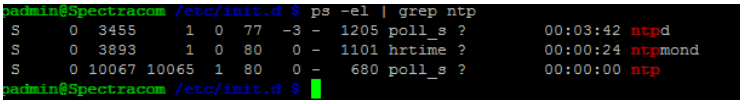
Verifying if NTP is actually running

To see if NTP is running, type **ps -el | grep ntp** <enter> (where it will list everything with the name typed after “grep):



```
padmin@Spectracom /etc/init.d $ ps -el | grep ntp
 S      0  3455      1  0  77  -3 -  1205 poll_s ?        00:03:43 ntpd
 S      0  3893      1  0  80   0 -  1102 poll_s ?        00:00:24 ntpmond
 S      0 17337 17332  0  80   0 -   680 poll_s ?        00:00:00 ntp
padmin@Spectracom /etc/init.d $
```

Note: Not all of the “NTP” services will be running all the time. NTPQ will only periodically be listed.



```
padmin@Spectracom /etc/init.d $ ps -el | grep ntp
 S      0  3455      1  0  77  -3 -  1205 poll_s ?        00:03:42 ntpd
 S      0  3893      1  0  80   0 -  1101 hrtime ?        00:00:24 ntpmond
 S      0 10067 10065  1  80   0 -   680 poll_s ?        00:00:00 ntp
padmin@Spectracom /etc/init.d $
```

Note: when the NTP enable/disable switch is off, NTP should be stopped (not listed)

**Logs for NTP

- Refer also to: NTP.log entries (NTP Log entries)

B) Tools -> NTP log (displayed in browser and part of log bundle)

Refer to **ntp.log** in the “**Logs”** section of this document (NTP log) for examples and additional info

A. Daemon.log (not displayed in browser but part of the log bundle)

- Get a full log bundle
- Logs state changes for the NTP daemon
- Refer to daemon.log in the “Logs” section of this document for examples and additional info

NTP Setup page doesn't show any fields (like a black page)

- NTP Expert mode is likely enabled (If not using Expert mode, disable it to see the fields again)

**Home page intermittently not showing NTP Stratum

- Left side of the Home page of the browser should always display NTP stratum value (if NTP is running)
- In at least versions 5.1.5 and below:
  - If there are any alarms asserted, the Stratum value will be reported on this page.
  - If there are NO alarms asserted, the Stratum value will not be reported on this page.

*Dedicated NTP input- periodic Holdover alarms being asserted

- Refer to Salesforce case 18014 for Kaiser Permanente
- Dedicated Stratum 2 SecureSync was periodically going into Holdover for a very short period of time (like a second or two). Then was fine again.

Cause: "It appears that the network switch port for this unit was incorrectly configured and the eth0 interface was only operating at 10/half. It is now auto-negotiated to 100/Full and the problem seems to have gone away."

**NTP Peering

****the newer browser doesn't provide the ability to edit/delete any NTP Peers or Servers

Solution: May need to first disable NTP (**Management** -> **NTP setup** page of the browser). After deleting/editing the NTP peers or servers, re-enable NTP again.

Email from Dave L (19 Jan 17)I worked with Rick this morning and was able to delete the Servers and Peers from the unit. All I had to do was turn off NTP using the switch on the NTP Setup page and turn it back on again. The NTPQ -p did not show them anymore.

****NTP peering of SecureSyncs in Simulcast applications

- Due to what NTP peering will do the 1PPS and other associated outputs, NTP Peering of SecureSync Master Oscillators in Simulcast applications is NOT recommended! The only viable input reference should be GPS.

If GPS is lost and the unit is peered with any other server, no matter what type oscillator is installed (Rubidium, OCXO or TCXO) the System PPS (and therefore all outputs based on the System PPS ontime point) is dithered (not slowly slewed) from where it is to where NTP's 1PPS is. This jumping of the System PPS to align with NTP and will adversely affect simulcast radios that are synced by the SecureSyncs 1PPS and other outputs.

****NTP Peers and NTP Servers status/Limited Reach/unreachable server

Issue in 2400 SecureSyncs (at least v1.2.2): Configuring NTP Peers via DNS hostnames instead of static IP addresses prevents browser from displaying peer information (though peering itself is working fine)

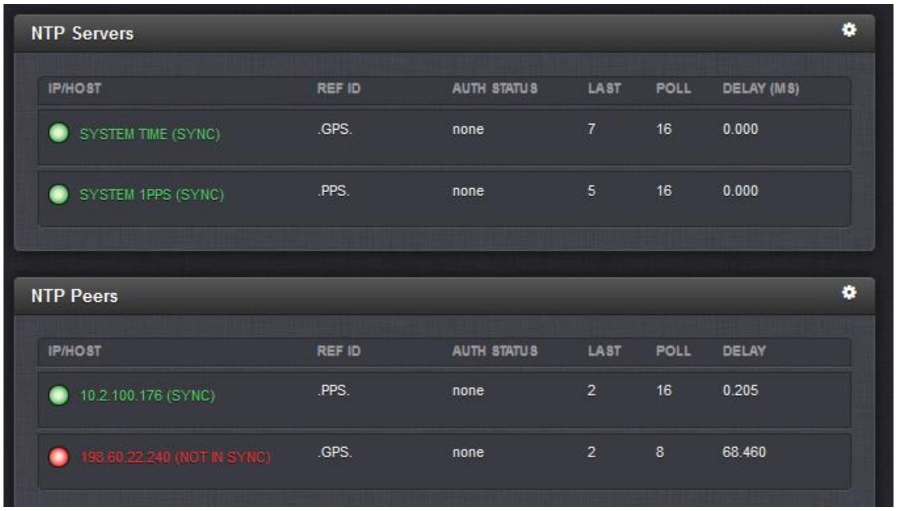
- Refer to Salesforce Case 279753 and JIRA DMND-1743
- Browser continues to report “”peers will appear shortly” though ntpq -p command shows peering still working in the background.

Email from Dave Lorah to Engineering (2 Feb 2022) This appears to be a bug in the 2400 Web UI. Adding NTP Peers using the DNS name results in a "peers will appear shortly" message in the Peers section of the NTP Setup screen. I verified the peers were active and reachable by the ntpq -p report but they never show up.

I had the customer try using the IP addresses instead and the peers showed immediately. Changing one back to the DNS name resulted in the one "peer will appear shortly" message again.
It looks like the web UI cannot handle the DNS name for some reason. We will put up a JIRA for resolution in a future firmware update.

A) web browser

Management **->** ***NTP Setup*** **page of the browser**

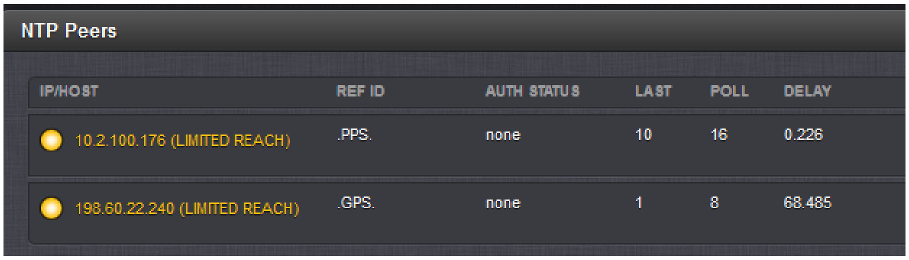


NTP Servers

IP/HOST	REF ID	AUTH STATUS	LAST	POLL	DELAY (MS)
● SYSTEM TIME (SYNC)	.GPS.	none	7	16	0.000
● SYSTEM 1PPS (SYNC)	.PPS.	none	5	16	0.000

NTP Peers

IP/HOST	REF ID	AUTH STATUS	LAST	POLL	DELAY
● 10.2.100.176 (SYNC)	.PPS.	none	2	16	0.205
● 198.60.22.240 (NOT IN SYNC)	.GPS.	none	2	8	68.460



NTP Peers

IP/HOST	REF ID	AUTH STATUS	LAST	POLL	DELAY
● 10.2.100.176 (LIMITED REACH)	.PPS.	none	10	16	0.226
● 198.60.22.240 (LIMITED REACH)	.GPS.	none	1	8	68.485

Number of listed peers/servers displayed in the Servers/Peers tables doesn’t match the response to ntpq -p commands

- **ntpq -p** and **ntpq -pn** CLI commands report a list of **all configured** NTP Servers and NTP Peers
- **NTP Setup page:** to help simplify the NTP Setup page of the browser, it only lists/displays the configred servers/peers having a reach value **greater than “0”.** Unreachable peers/servers (reach of “0”, or reach is

"377" but the other time server isn't in sync) are not displayed in the browser. even though ntpq command does list them

Servers/peers being reported as un Unreachable

- Occurs when:

1. Peers/servers have a Reach of "**0**" (no time stamps being received back from this other time server)   OR
2. Reach is **not "0**" (such as "377 for instance"), but this other NTP time server isn't in sync (its NTP may be in "Orphan mode" because it has no refernces it can sync with. So its still providing Timstamps, but its Stratum valus is being reported as Stratum 0 (not useable)

Color coding/labeling of each listed peer and server

Notes:

1) Per Ron Dries: Color coding of each reference is based on the NTP Tally code and Reach value for each.
2) The tally code is determined by NTP's "**Clock Select**" Algorithm (refer to https://www.eecis.udel.edu/~mills/ntp/html/select.html). This algorithm performs sanity checks on each reference to decide which are "sane" candidates and which are "insane".

By factory default, only a total of four NTP Peers/Servers will be listed in green

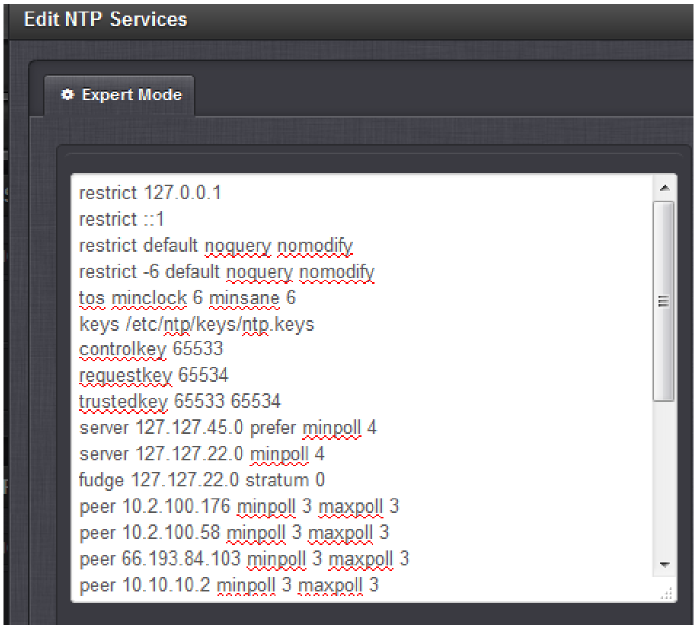
- The Clock Select algorithm (by NTP default settings) will select up to (3) three sane servers and (1) one candidate. All others are then marked as "non-candidates". So up to four total Peers/Servers will be in green by default. The rest will be red.
- See additional info further below on how to make more than four peers be in green.

While trying to peer two SecureSyncs NTP disqualifying TSync (GPS) reference as well as the NTP peer due to large time difference between the two (NTP put an "x" in front of both references so neither could be selected.

- Customer had two SecureSyncs in two different countries. There was about an 800ms offset between NTP and the TSync driver.   NTP wouldn't choose either one (it was rejecting both references because the error was so large and it only had two references). If the Peer was turned off, both synced to GPS just fine.
- Paul recommended changing the NTP peer's minpoll to 6 and its maxpoll to 10, to provide NTP with a little extra time to select TSync while it was still qualifying the peer (its Reach was still low when it selected NTP in our test case (we peered with a unit it Texas to generate a 200ms difference between TSync and NTP

Ability to increase the number of peers that can turn green (all others being "falsetickers")

- Refer to https://www.eecis.udel.edu/~mills/ntp/html/select.html
- Can alter the number of lines that can be green (candidates) instead of red (falsetickers) via NTP Expert mode (to be more than four total, the default number)
- Add the following line to the ntp.conf file (as shown below) after enabling NTP Expert mode: tos minclock 6 minsane 6 (where 6 and 6 will allow up to 12 total references that can turn green).



```
restrict 127.0.0.1
restrict ::1
restrict default noquery nomodify
restrict -6 default noquery nomodify
tos minclock 6 minsane 6
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
server 127.127.45.0 prefer minpoll 4
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
peer 10.2.100.176 minpoll 3 maxpoll 3
peer 10.2.100.58 minpoll 3 maxpoll 3
peer 66.193.84.103 minpoll 3 maxpoll 3
peer 10.10.10.2 minpoll 3 maxpoll 3
```

As for “falseticker” (and the desire to point each SecureSync to multiple other time servers) I have some additional information for you…

In general and as an FYI- we do not recommend configuring a SecureSync that is normally synced with GPS (Stratum 1) to more than 4 or 5 at most, other NTP servers for NTP peering. Though GPS is a “preferred” reference for NTP, having too many NTP servers listed as peers can cause them to “out-weigh” the GPS input into NTP. So instead of NTP syncing with the GPS time (System Time) it may instead select an NTP peer over GPS as its reference just because of the number of NTP servers it also has available. If it selects an NTP server over GPS, the SecureSync will switch from Stratum 1 to Stratum 2 and its NTP accuracy capability will also inherently decrease because NTP input is not nearly as accurate as GPS input. Limiting the number of configured peers to approximately 3 or 4 will help prevent NTP from syncing to another NTP server over the GPS synced System Time while GPS reception is present.

For a dedicated Stratum 2 server (no GPS input) there’s no reason not to list several NTP servers as peers, so that NTP always has several to choose from. But with a Stratum 1 server, its recommended (though not required) to limit the number of listed peers to three or four other NTP servers for redundancy.

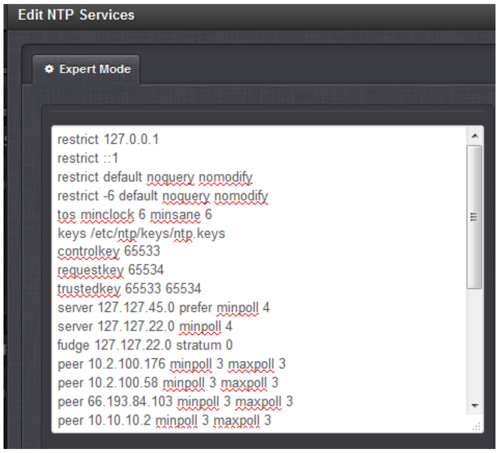
As for falseticker, this is associated with the NTP algorithms used to select which reference it syncs with and which other references are still available as candidates for selection in case NTP decides that a candidate becomes a better reference than its currently selected reference. NTP can choose to switch to another reference, as it feels best, based on many parameters (Stratum level, jitter and offset, etc).

NTP is always qualifying all of its listed/available reference for selection of one reference to sync with. It does this by selecting four of the best ones and declaring the others as “falsetickers” (or “outliers”). It selects one of the four remaining as its reference and the other three remaining are considered candidates. An outlier isn’t selected at that time for its sync. But as NTP continues to qualify all of its references, it may change a falseticker to a candidate or may select it as its reference, at any time. So even though a peer is currently a falseticker doesn’t mean it is bad or can’t be selected at a different time.

This means that up to four total references can be displayed as green in the web browser. But a red reference can turn green and a green one can turn red, as NTP sees best.

This is based on the default configuration of NTP. It can be changed, if desired with the use of NTP Expert mode (note that in Expert mode, most of the GUI settings for NTP will no longer be available and if Expert Mode is ever disabled), the NTP configuration will be restored back to the factory configuration). Adding a line to the ntp.conf file will allow all peers NTP feels are candidates for selection to be green, instead of just up to four. Though the default configuration still allows any peer to be selected at one time, this change allows more peers to be considered candidates at any one given time (more of them can be green).

As shown below, enabling expert mode and then adding the following line to the ntp.conf file will allow up to 12 total peers to be green at any given time, as long as NTP considers them good: tos minclock 6 minsane 6. Note the SecureSync user manual discusses how to enable NTP Expert mode.



```
restrict 127.0.0.1
restrict ::1
restrict default noquery nomodify
restrict -6 default noquery nomodify
tos minclock 6 minsane 6
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
server 127.127.45.0 prefer minpoll 4
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
peer 10.2.100.176 minpoll 3 maxpoll 3
peer 10.2.100.58 minpoll 3 maxpoll 3
peer 66.193.84.103 minpoll 3 maxpoll 3
peer 10.10.10.2 minpoll 3 maxpoll 3
```

Tally code	Green = (Sync)
	Red = (Not in Sync) (if the Reach is not 0)
		Truechimer (good) or falseticker (bad) (as determined by the Clock Select Algorithm)

*	The Selected Time reference	Truechimer
o	The Selected PPS reference	Truechimer
+	A **high quality candidate** for NTP reference input that can be selected by NTP as its time reference (Good reference, but not selected)	Truechimer
x	**"Falseticker"** Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference).	falseticker
-	**"Outlyer"** Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference).	falseticker
(blank)	Source **discarded**: Failed Sanity check	falseticker

Green: (SYNC): NTP is in sync with this Peer/Server. NTP has either selected it as its reference or it's available for selection.

- Tally code is one of the following: * or o or +
- Reach value is above 0

Red (NOT IN SYNC): This Peer/server is a falseticker. NTP hasn't selected it as its reference and it's NOT available for selection. The peer/server's time may be unreasonable, or it may not be in sync.

- Tally code is one of the following: x or **-** or blank
- Reach is above 0

Orange (LIMITED REACH): The Reach value of this Peer is not "177" but isn't "0" either. Either NTP was just restarted or not all Polls of that peer/server are resulting in a successful response. Packets may be getting lost in between, or that peer/server may not always be in sync and a useable reference (see below for additional troubleshooting info).

- Reach is above 0 but less than 177.
- See addition info directly below

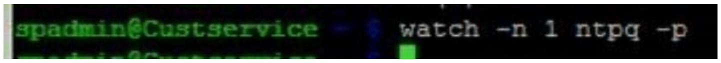
"Limited Reach" reported, though NTP wasn't just restarted in the last couple of minutes

- Indicates not all Polls of a peer/server are resulting in a successful time response
- Displayed when the peer's/server's "Reach" value is greater than "0" but less than "177".

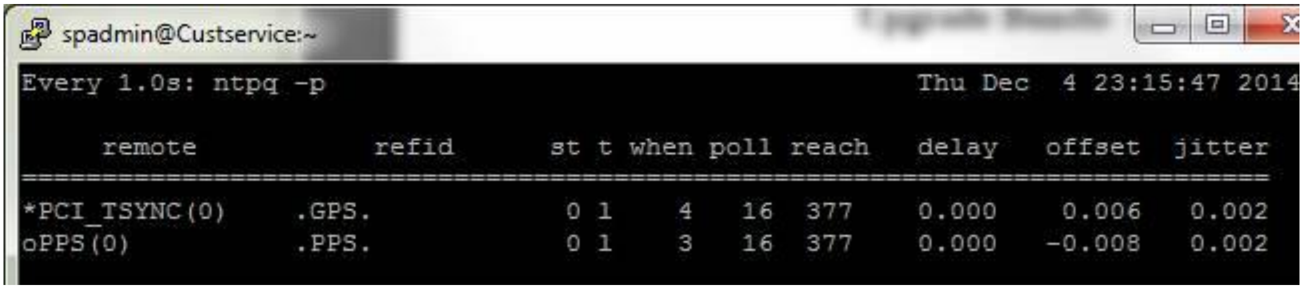
Email Keith sent (4 Dec 2014) Per our conversation, it looks like the Model 9489 may periodically be sending time requests to its two peers (the Model 9389s) but not always able to receive a response back from those time servers.

Limited Reach indicates that at least some, but not all, responses are being received. With a telnet or SSH connection, you can watch the Reach value counter to see when time responses aren't being received.

After logging in to the CLI interface, type the following command, which will automatically update every 2 seconds: watch –n 1 ntpq –p <enter>.



```
spadmin@Custservice ~ $ watch -n 1 ntpq -p
```



```
Every 1.0s: ntpq -p                                   Thu Dec  4 23:15:47 2014

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*PCI_TSYNC(0)    .GPS.            0 l    4   16   377    0.000    0.006   0.002
oPPS(0)          .PPS.            0 l    3   16   377    0.000   -0.008   0.002
```

This command will display and update the NTP statistics for each of NTP's references. The Poll value (in seconds) indicates how often NTP is currently sending NTP requests to that particular reference (at the beginning of the same row). The reach value will start at 0 when NTP first starts up and then increments at each Poll until it gets to "377". If it gets a response at each Poll of that reference, Reach will remain "377". But if one or more of the last 8 Polls doesn't result in NTP receiving a response from that peer, the Reach value decrements after the Poll occurred.

By the way, the "when" value is the number of seconds since it last sent a Poll to that time server. The Poll is sent when the "when" and "Poll" values are equal, with "when" becoming a vertical line instead of a number.

Issue with one or more NTP peers disappearing (disappears from the list of configured peers)

- Sounds like this is an NTP bug in NTP v4.2.8p6 (software v5.4.1- expected fix to be in the v5.4.5 update)
- Refer to SR 5679 in SAP.

Q. (from Eric Bizimana) Everything seems to be working after the reboot but the peering to one of the other peers that disappeared again.
A reply from Dave Lorah (11 Jul 16) You will possibly see a NTP Peer disappear again. This is a bug in NTP software and can happen over and over. We are working on incorporating a fix by adding the new version NTP in the next Securesync firmware release.

**KHTD (KTS Host Time Daemon for Stratum 2 operation)

Email from Dave Sohn (24 Apr 2014) KHTD is our KTS Host Time Daemon. It is responsible for NTP time sets to KTS when operating in Stratum 2, and for setting kernel time when NTP is not running.

****Dedicated NTP input- periodic Holdover alarms being asserted

- If NTP or KHTD are restarted for any reason while the unit remains up and running, SecureSync will go into Holdover mode (whether or not the Host clock driver, 127.127.45.0 is enabled). Holdover exits less than a minute or so later, once NTP/KHTD is back up and running.

Log entry for KHTD being restarted

[system] KTS Host Time Daemon has restarted (KHTD)

Log entries for NTPD being started/restarted

ntpd[31004]: ntpd 4.2.6p5@1.2349-o Fri Jan 30 15:51:28 UTC 2015 (1)

Note: this entry was with v5.2.0 installed (ntp 4.2.6). The NTP version is software version dependent (**n**tpd[31004]: ntpd 4.2 ….)

Examples why either NTP or KHTD will be restarted include:

- NTP being restarted by a user
- NTP config change being made by a user (config changes automatically restart NTP)
- ntpmond restating ntp due to a time error greater than one second

Specific examples of Holdover alarms in a Stratum 2 server

Kaiser Permanente

- Dedicated Stratum 2 SecureSync was periodically going into Holdover for less than a minute because NTP and KHTD were both restarting.

Refer to Salesforce case 18014 for Kaiser Permanente

- Dedicated Stratum 2 SecureSync was periodically going into Holdover for a very short period of time (like a second or two). Then was fine again.
- Cause: "It appears that the network switch port for this unit was incorrectly configured and the eth0 interface was only operating at 10/half. It is now auto-negotiated to 100/Full and the problem seems to have gone away."

KHTD restarting/Shutting down

- KHTD is restarted each time NTPD restarts

Email from Paul Myers (24 Aug 2015) If NTP is stopped and restarted KHTD will also be restarted. The NTP stop script 'reloads' KHTD to keep both at the same state.

"KTS Host Time Daemon has terminated (KHTD)"

- This entry indicates NTP shutdown for halt/reboot by a user (other daemons will also be terminated, as well).

ntpmond: statistics logging (Client and server NTP packets per second- "pkt/s")

- Added this new NTP loading feature in software update version 5.2.1 (Apr 2015) as part of NTP v4.2.8 upgrade
- Entries are asserted into the NTP.log (NTP Log) each hour (27 minutes after each hour).
- Reports NTP loading
  - **Example log entry (with no clients):** NTP statistics: Clients = 0.000 pkt/s, Servers/Peers = 0.000 pkt/s
  - **Example log entry (with just a couple clients) NTP statistics**: Clients = 0.037 pkt/s, Servers/Peers = 0.000 pkt/s

Where:

- **Clients**: NTP requests from NTP clients on the network
- **Servers/Peers**: NTP requests from Servers or Peers configured to get time from this SecureSync

B) To convert pkt/s (values in the graphs/logs) to the actual number of packets in the hour

Multiply the number of pkt/s (value in the graphs/logs) times 60 and then round-up to nearest whole number

Examples:

0.017 pkt/s = 1 packet in one hour

0.083 pkt/s = 5 packets in one hour

0.167 pkt/s = 10 packets in one hour

1.667 pkt/s = 100 packets in one hour

166.667 pkt/s = **10,000** packets in one hour

3000 pkt/s = 180,000 packets in one hour

C) To convert actual number of packets per hour to pkt/s (values in the graphs/logs)

Divide the number of ntp packets in the hour by 60 (there are 60 minutes in the report period)

Examples:

1 packet in one hour = **0.017 pkt/s**

5 packets in one hour = **0.083 pkt/s**

10 packets in one hour = **0.167 pkt/s**

100 packets in one hour = **1.667 pkt/s**

10,000 packets in one hour = **166.667 pkt/s**

180,000 packets in one hour = **3000 pkt/s**

NTP Throughput/NTP Statistics- Number of NTP requests per second/NTP Stress test

- Refer to: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP stress testing
- Refer **to NTP throughput documents on our website- links further below**
  - **SecureSync User Manual, generic note about throughput on page 10:** http://spectracom.com/sites/default/files/document-files/SecureSync_UserRefGuide_1200-5000-0050_R21.pdf
  - **Throughput (Q&A knowledge base article):** http://support.spectracom.com/articles/FAQ/NTP-Throughput?&category=SecureSync&
  - **Test protocol (tech note):** http://spectracom.com/sites/default/files/document-files/NTP_Server_Capacity_Testing_TN19-101_B.pdf (note this link is also available within the knowledge base article mentioned above)
- **Refer to the** ntp.log for info on NTP statistics (pkt/s)

D) NTP statistics logging (Client and server NTP packets per second)

- Added this new NTP loading feature in software update version 5.2.1 (Apr 2015) as part of NTP v4.2.8 upgrade

- Provides NTP throughput / NTP loading

- Entries are asserted into the NTP.log (NTP Log)
  - **Example log entry (with no clients): NTP statistics: Clients = 0.000 pkt/s, Servers/Peers = 0.000 pkt/s**
  - **Example log entry (with just a couple clients) NTP statistics: Clients = 0.037 pkt/s, Servers/Peers = 0.000 pkt/s**

Note: pkt/s is reported in Mbps (Megabits/sec). So 0.140 pkt/s is 1400 packets per second ???

Where:

- **Clients**: NTP requests from NTP clients on the network
- **Servers/Peers:** NTP requests from Servers or Peers configured to get time from this SecureSync

NTP throughput graphs added to web browser (versions 5.3.1 and above)

- **Refer to:** NTP graphs

NTP loading

(17 Jun 16) Summary of the info further below - per Ron Dries (based on testing with v5.4.1 I understand)

- **Eth0 by itself (ETX module):** ~7500 requests/sec
- **Eth1, Eth2 or Eth3 by itself**: ~8000-9000 requests/sec

Published Spec used to be about 9309 packets/Sec.

- Due to the ETX module changing from Intel to Realtec IC (and the associated change to a different drier) some time ago, the new spec is about 7500 requests/second on eth0. For eth1, eth2 and eth3, due to the faster port speed and different driver its around 8000 requests/second for these three ports

  Note: Per Tom Richardson/Ron Dries, the SecureSyncs have never shipped with an ETX having an intel IC. The change to Realtec apparently occurred before we started shipping SecureSyncs and before we stopped shipping NetClock 9300s???

The info below in red (from email Keith sent on 15 Jun, 16 after talking with Engineering/Hendrik) is regarding the newer ETX mdodules which have a Realtec (instead of Intel) component andt therefore also a different driver for slightly lower numbers of responses/second. According to Tom R, this change to the ETX happened before we started shipping SecureSyncs???

Q. What is the max number of NTP requests per second?
A. From Section 1.7.4 in the SecureSync manual, "Loading: ~7,000 NTP requests per second, typical"

Q1. In the Manual version 20, this value is 9000, is it the correct value also for the latest unit? If no, please tell us the correct value.

A Keith's response: due to a hardware change, the NTP packets per second (NTP throughput) that the SecureSyncs can provide is now slightly lower than what was indicated in earlier versions of the SecureSync manual. Eth0 (the base 10/100 port installed on all SecureSyncs) can now provide about 7500 ntp requests/second.

As NTP intentionally staggers when each client polls its configured NTP servers, and as NTP doesn't request the time every second, these factors allows the SecureSync to be able to service WELL over 7500 NTP clients on its network.

The latest NTP throughput capability is indicated on page 10 of the latest version of the SecureSync manual, which can be downloaded at: http://spectracom.com/sites/default/files/document-files/SecureSync_UserRefGuide_1200-5000-0050_R21.pdf (the info is excerpted below for your convenience)

"NTP throughput: 7000 – 9000 NTP requests per second, depending on used Ethernet port/hardware configuration"

Note there is an available knowledge base article on website that also discusses throughput. It's available at): http://support.spectracom.com/articles/FAQ/NTP-Throughput?&category=SecureSync&

There is also a Tech Note/Test report referenced in the knowledge article mentioned above. here is the link to it: http://spectracom.com/sites/default/files/document-files/NTP_Server_Capacity_Testing_TN19-101_B.pdf (excerpt below):

> The Spectracom NTP service implemented on SecureSync and NetClock 9400 was tested to determine its NTP requests per second threshold value without authentication. Specific software components can affect throughput. An earlier configuration was capable of up to 9,909 NTP requests per second. An updated configuration was able to serve approximately 7,500 NTP requests per second.

Q2. If we use 1204-06 option module, does this value change?

A Keith's response: if one of the Ethernet interfaces on the Model 1204-06 Gb Ethernet Option Card (eth1, eth2 or eth3) is used instead of using eth0, the NTP loading capability for that one particular interface does increase slightly - due to the faster network speed of the interface and due to the Gb Ethernet interfaces using a different driver than eth0 uses. However, using more than one Ethernet interface on the SecureSync (eth0 through eth3) does not increase the overall number of NTP requests that the SecureSync can provide, as all of the Ethernet interfaces share the same instance of NTP.

So the number of NTP requests/second that NTP in the SecureSync can respond to is split amongst all Ethernet ports on the SecureSync which are receiving NTP requests (for example, if eth0 and eth1 are the only two Ethernet interfaces receiving NTP requests, eth 1 can bew responding to 3500 request/sec while Eth0 is also responding to about 4000 requests- for a total of about 7500 NTP requests per second total being supplied by the SecureSync).

NTP Stress Test tool (created by Spectracom Engineering)

- **Refer to:** EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP stress testing

Per Dave Sohn (6 Nov 15) customers do not need an NDA in place with us to receive this program. However, they need to be made aware of the following info

Email from Dave Sohn We don't need an NDA in place, but they need to understand that this is an engineering tool we developed internally, so it is not a formally developed product with full support. It is provided as-is without any warranty.

Note: Don't send the entire contents of the "NTPStresTool" folder at the link above. Send the NtpStress.exe program, the "sample command.txt" document and this info (example I sent to a customer) I donlt believe they need the "source" folder or the "StressTestTool.txt" file.

As this is an .exe that would most likely be "unattached" from this email (even if you actually received this email), I have uploaded it as a .zip file to the Sharefile website (a service we purchase for providing files). Both of you should have received a link to a folder containing this program. If you didn't get the link, please let me know!

Please be aware that this program is an engineering tool that our Engineers developed internally. So it is not a formally developed product with full support available. It is provided as-is without any warranties.

Accept

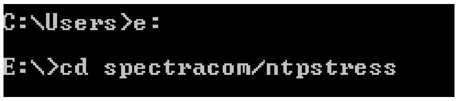
After pressing the above "Accept" button to agree to the terms mentioned ☺ , please feel free to use this program and Windows computers to generate MANY NTP time stamps!!

DOS commands to run the tool

- Refer to the NTPStress sample command.txt document
- Tool can be run with the "COD" window left open or closed when the tool is run.

Running the program

1) Open a command prompt window and change to the directory where ntpstress.exe is located.



```
C:\Users>e:

E:\>cd spectracom/ntpstress
```

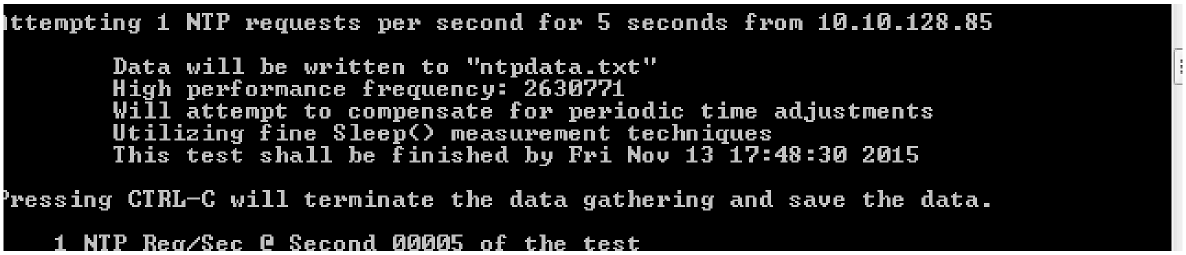
2) Run the desired command (below):

Syntax for single instance of the tool to run

NtpStress.exe -t 10.10.128.85 10000 3600 where the IP address is the address of the NTP server, "10000" is the desired number of packets/sec for the tool to send (note the actual number being sent may vary, such as far less based on capabilities of the PC) and "3600" is the number of seconds for the test to run.

Syntax to automatically open/run more than one instance of the tool at the same time

for /l %x in (1,1,10) do start cmd /k NtpStress.exe -t 10.10.128.85 10000 3600 (where the "10" -in red- is the number of instances to run at the same time. Also: where the IP address is the address of the NTP server, 10000 is the desired number of packets/sec for the tool to send (actual number may vary) and 3600 is the number of seconds for the test to run.

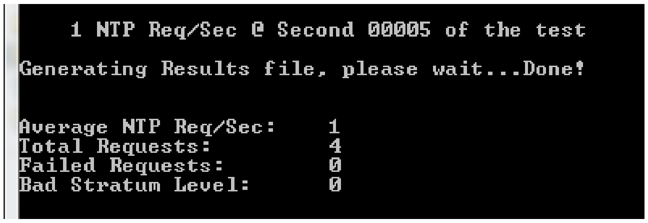


```
ttempting 1 NTP requests per second for 5 seconds from 10.10.128.85

       Data will be written to "ntpdata.txt"
       High performance frequency: 2630771
       Will attempt to compensate for periodic time adjustments
       Utilizing fine Sleep() measurement techniques
       This test shall be finished by Fri Nov 13 17:48:30 2015

ressing CTRL-C will terminate the data gathering and save the data.

   1 NTP Req/Sec @ Second 00005 of the test
```

Note: the test can be ended at any time by pressing CTRL & C. Results below will be displayed.

Results displayed when the test finishes

- How long it take the test to complete is based on the number of seconds specified in the last value of the command-such as "3600" seconds in the examples above)



```
    1 NTP Req/Sec @ Second 00005 of the test

Generating Results file, please wait...Done!


Average NTP Req/Sec:    1
Total Requests:         4
Failed Requests:        0
Bad Stratum Level:      0
```

Average NTP Req/Sec: Average number of requests sent to the time server every second
Total requests: Total number of requests sent during the test duration.
Failed requests: Number of requests sent without a response from the NTP server.
Bad Stratum level: NTP Server was at stratum 16 when it responded (??)

**Desire to output NTP in Local Time (instead of NTP)

- Refer to Salesforce case 15042
- Requires all external input references be removed/disabled in the Reference Priority table
- System Time is set to “local time” instead of UTC
- No automatic DST correction (System Time needs to be manually changed every 6 months)

Email from Dave Lorah (20 Jun 14) I did some research and experimentation and have the following instructions to setup your SecureSync unit to transmit local time zone from NTP. This involves setting up a Reference Priority Table entry and then manually setting the SecureSync time to your local time.

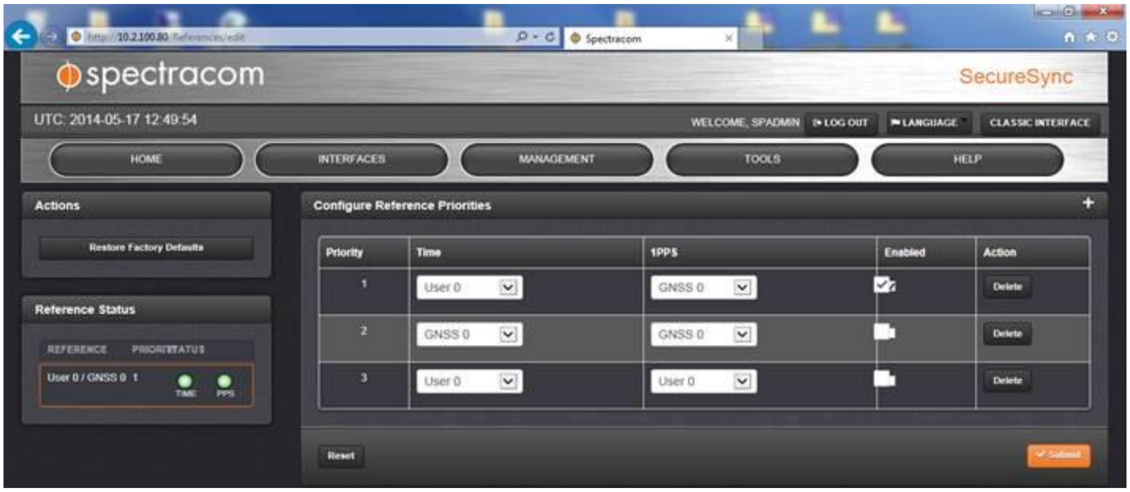
There is no way possible to introduce a Daylight Savings Time offset schedule however. So you will need to go into the unit and manually set the time twice a year to correct the DST offset.

You should update to current version 5.1.4 to eliminate the NTP 1000mS correction limitation. Here is a link to the download:

http://www.spectracomcorp.com/Support/HowCanWeHelpYou/SoftwareUpdates/SecureSyncSoftware/tabid/1352/Default.aspx

Setup Procedure:

1) Create a Reference Priority Table entry for **User0** / **GNSS 0.**



UTC: 2014-05-17 12:49:54

Configure Reference Priorities

Priority	Time	1PPS	Enabled	Action
1	User 0	GNSS 0	☑	Delete
2	GNSS 0	GNSS 0	□	Delete
3	User 0	User 0	□	Delete

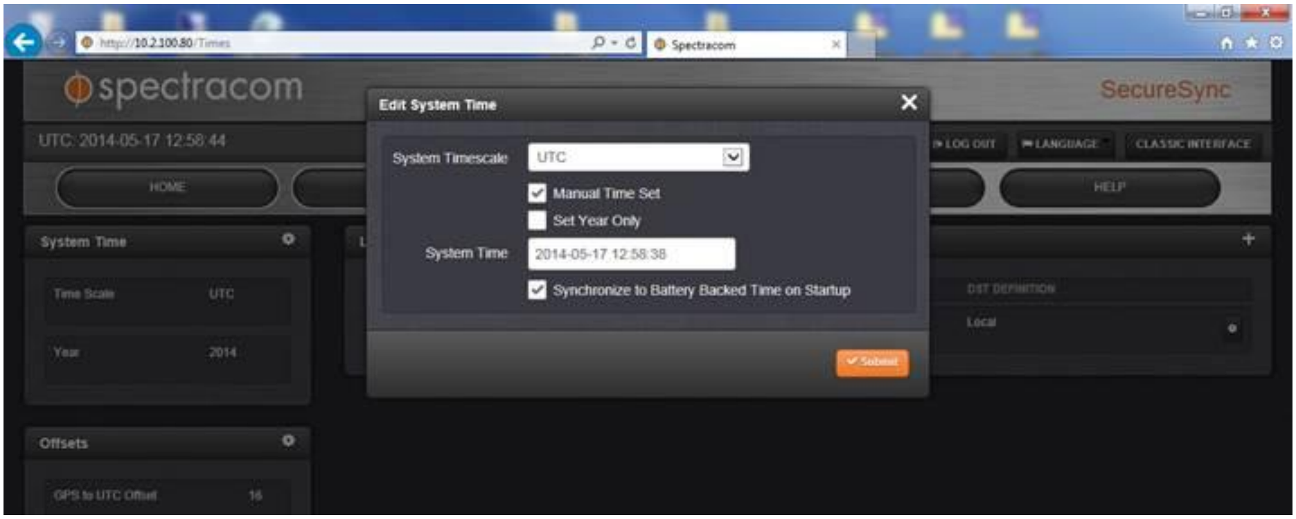
Reference Status

REFERENCE	PRIORITY	STATUS
User 0 / GNSS 0	1	● TIME ● PPS

2) Next, go to the **Management** -> **Time Management** section and select the System Time config. Select the “**Synchronize to Battery Backed Time on Startup”** checkbox. Also select the “**Manual Time Set”** checkbox.

3) Enter your local time in the System Time field. When you hit SUBMIT it will manually set the system time and start running from there. When DST goes into effect you will have to go back to this same page and change the time manually as needed.

4) The SecureSync will start running from this manually set time and keep precisely running using the GPS 1PPS as a reference.



System Timescale: UTC

☑ Manual Time Set

□ Set Year Only

System Time: 2014-05-17 12:58:38

☑ Synchronize to Battery Backed Time on Startup

Desire to prevent NTP from responding to earlier versions NTP requests (NTPv1, NTPv2 and NTPv3. Responding to NTPv4 requests only)

- Refer to “version” in the following link http://www.manpagez.com/man/5/ntp.conf/ (under “Access Control Support”)
- Refer to the NTP Expert Tech Note: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert mode- restrict earlier versions

Q. ST Electronics (Info-Security) wants to know if SS can be disabled for NTPv1 and v2.They want to restrict the unit to serve only NTPv3 and v4 requests. They currently have 3 RB SS at the staging area but will need an official response from Spectracom.

A This was a great question. We don’t recall anyone EVER asking for this capability before.
NTP doesn’t appear to support exactly what they want to do, but it can come VERY close. The SecureSyncs don’t directly support this function of NTP with browser fields, but it can be implemented with the NTP Expert mode.

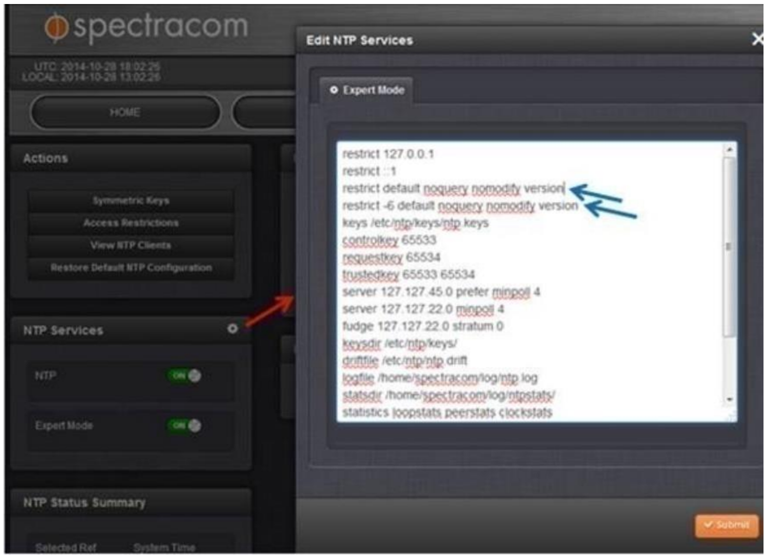
NTP has an access restriction flag available that will block all NTP requests that are not from clients at the same version of NTP it is running. So the only difference with what your customer desires and what NTP can do is it will block V1, v2 and v3 requests, allowing only v4 requests to be responded to. It doesn’t allow you to specify which versions are allowed and which versions aren’t allowed. As this is the only customer ever to ask for this capability, I suspect it won’t be added to directly to a field in the browser in any future release (it will be limited to just the Expert Mode).

If your customer would like to allow only v4 requests be responded to, here is how to configure this using the Expert Mode. Note that Expert Mode needs to remain always enabled once it’s manually changed. Disabling Expert mode will cause any changes to be lost as the ntp.conf file is reset back to the factory default state. While enabled, the majority of the NTP configurations fields will no longer be visible. But NTP can be enabled or disabled if desired, without needing to disable Expert Mode.

2) Go to the Management -> NTP Setup page

3) On the left side of the page, change Expert Mode to ON

4) Click on the Gear ICON just above the NTP switch and next to the right of “NTP Services”, This will open the “Expert Mode” Window, as shown below:



```
restrict 127.0.0.1
restrict ::1
restrict default noquery nomodify version
restrict -6 default noquery nomodify version
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
server 127.127.45.0 prefer minpoll 4
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
keysdir /etc/ntp/keys/
driftfile /etc/ntp/ntp.drift
logfile /home/spectracom/log/ntp.log
statsdir /home/spectracom/log/ntpstats/
statistics loopstats peerstats clockstats
```

5) With the window open, add the word “version” to the end of the third and fourth lines in this window (after the word “nomodify”, as shown above). This will restrict NTP responses to only version 4 clients, via either IPv4 or IPv6 addresses!

NTP IPv4/IPv6 Access Restriction / NTPQ and NTPDC (Mode 7)

- Refer to the Knowledge base article on our website:
- For more info, refer to: http://support.ntp.org/bin/view/Support/AccessRestrictions

NTP access restriction configuration (via Expert mode web browser)

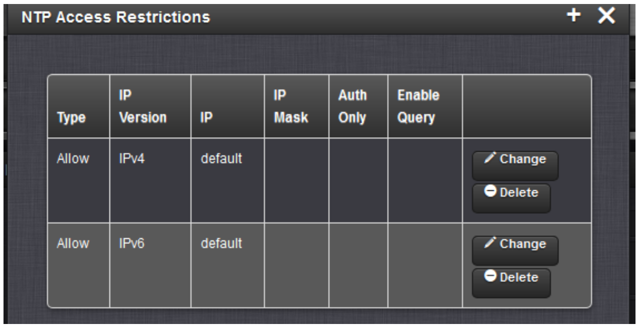
NTP Expert mode enabled

- Refer to Section 6.5.1 of the following link for info on how to edit the ntp.conf file directly for NTP access restrictions: http://support.ntp.org/bin/view/Support/AccessRestrictions
- Note when NTP Expert mode is enabled, the change/delete buttons in the NTP Access Restrictions table are not disabled, to prevent editing the settings via the web browser instead of editing the ntp.conf file.

A) Newer (black/charcoal) browser:

- NTP Access Restriction and Mode 7 (NTPQ and NTPDC) are both configured in the **Management** -> **NTP Setup** page of the browser. Click on the Access Restrictions button on the left side of the page.

Factory default settings



NTP Access Restrictions

Type	IP Version	IP	IP Mask	Auth Only	Enable Query	
Allow	IPv4	default				Change Delete
Allow	IPv6	default				Change Delete

Summary: To allow only one or only some NTP clients to get time from the SecureSync

In order to “allow” just one or more NTP clients to have access, you first have to “Deny” all clients. Then, if you want to:

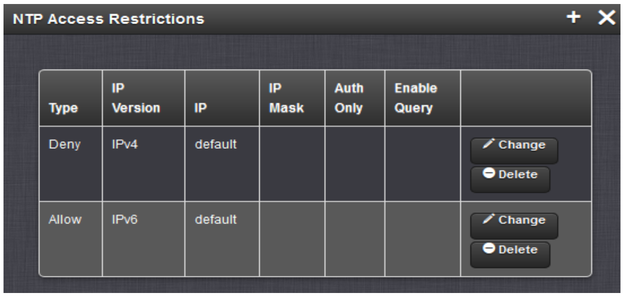
1) Allow individual clients (not an entire subnet), you add individual rows in the table that define the IP address – with no subnet mask defined.
2) Add additional rows of IP address only for each additional client you wish to Allow (no subnet mask).
3) Allow an entire subnet (not just one particular client) define the IP address of one client on that subnet and also enter the subnet mask for the network you wish to allow.

A) Specific steps to configure one or more NTP clients to be able to access the time server:

1. First “Deny” access to every client on the IPv4 network:

A) In the first row of the Access table (IPv4) just press “Change” and then switch “Allow” to “Deny”.

B) Press Submit.



NTP Access Restrictions

Type	IP Version	IP	IP Mask	Auth Only	Enable Query	
Deny	IPv4	default				Change Delete
Allow	IPv6	default				Change Delete

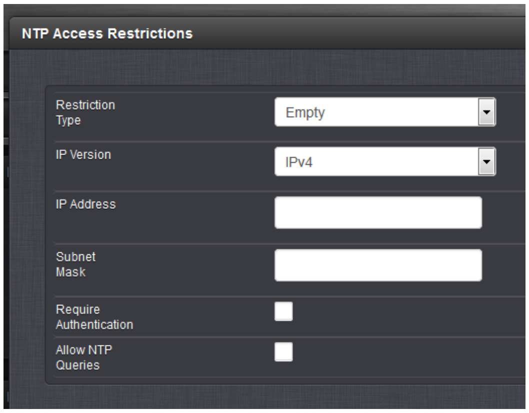
2. Then add an “Allow” for each client that you want to be able to access NTP from this time server:

A) Enter just the IP address and no subnet mask to allow just an individual client. Continue entering new “Allow” IP address lines to allow additional clients.

B) Enter an IP address and subnet mask (such as 10.2.1.2 255.255.0.0) to allow that entire subnet to have access. In this example, all clients on the 10.2.x.x network can get time from the server.

Note: can’t enter just enter a subnet with no associated IP address.

B) Press the “+” to add a client or subnet to allow

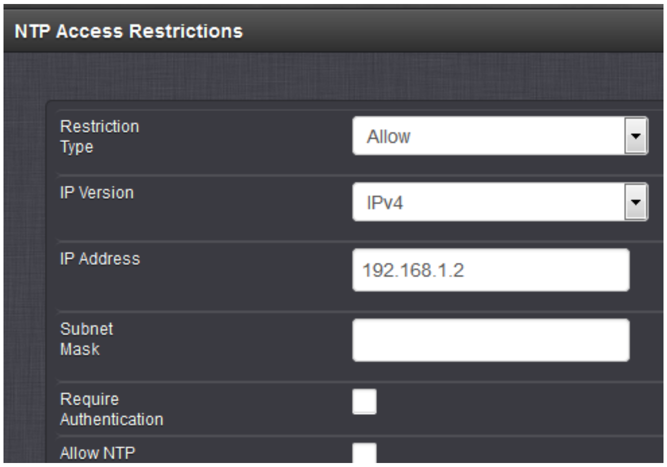


NTP Access Restrictions

Restriction Type	Empty
IP Version	IPv4
IP Address	
Subnet Mask	
Require Authentication	□
Allow NTP Queries	□

C) Restriction Type: Select “Allow”

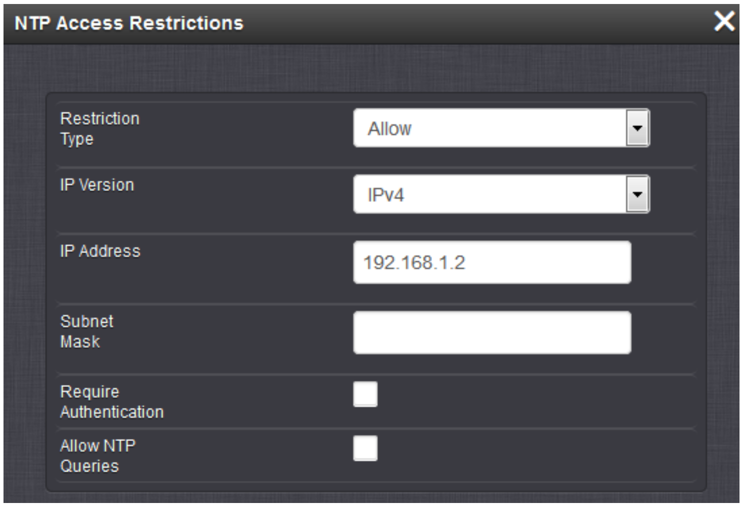
D) IP Address: enter a desired client to Allow, or any client on the subnet that is desired to be allowed.



NTP Access Restrictions

Restriction Type	Allow
IP Version	IPv4
IP Address	192.168.1.2
Subnet Mask	
Require Authentication	□
Allow NTP	□

E) Subnet mask: enter ONLY if it’s desired to Allow that entire subnet.



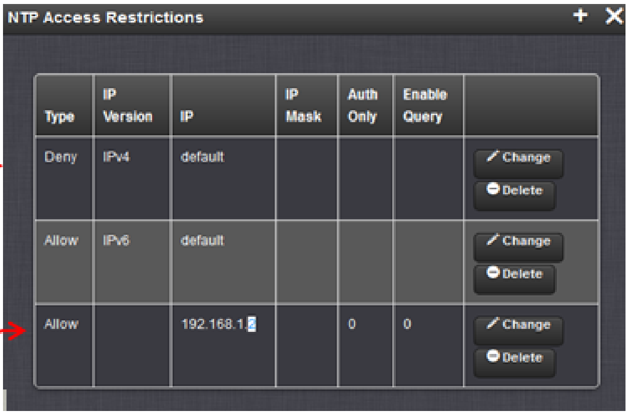
NTP Access Restrictions

Restriction Type	Allow
IP Version	IPv4
IP Address	192.168.1.2
Subnet Mask	
Require Authentication	□
Allow NTP Queries	□

F) Press Submit.

First, all NTP clients are Denied

Then, only one NTP client is allowed (additional lines can be added to allow other NTP clients)



NTP Access Restrictions

Type	IP Version	IP	IP Mask	Auth Only	Enable Query	
Deny	IPv4	default				Change Delete
Allow	IPv6	default				Change Delete
Allow		192.168.1.2		0	0	Change Delete

Now ONLY **192.168.1.2** can now access the server. All other clients are denied.

G) Repeat Step “C” for each additional client you wish to allow access to the time server

NTPv6 Access Restriction

- Refer to Mantis case 2910

Email Keith sent (23 Sept 14) Per your inquiry “system configured with access restriction to allow queries from 2607:b400:0000:: with mask of ffff:ffff:ff00:: ntpdc -c reslist returns line with incorrect mask and system cannot be queried from a matching remote system. reslist returns:
2607:b400:: ffff:ffff:ffff: 0 none”, I have some information for you that I hope will help.

This IPv6 configuration of the SecureSync currently requires the use of the available NTP Expert Mode functionality. Once NTP has been reconfigured in the web browser for Expert mode, the raw ntp.conf file can be edited with a “-6” being added to this file. Once this value has been enabled. NTP Expert Mode will need to remain enabled for the change to persist.

NTP access restrictions are discussed in the following document:
http://support.ntp.org/bin/view/Support/AccessRestrictions

I am also passing this information over to our Product Management and Engineering teams for consideration of adding this capability in a future update to alleviate needing to use the Expert mode to configure it for IPv6.

Configuring NTP Expert mode:

With other desired configuration changes to the default NTP pages of the browser already set as desired, enable the Expert mode (note the browser fields aren’t accessible once NTP expert mode is enabled). And if Expert mode is subsequently disabled, this file will return to its default state. So Expert Mode needs to remain enabled to keep the settings.

To enable Expert mode with software versions 5.1.2 and higher installed via the newer web browser, go to the **Management** -> **NTP Setup** page of the browser. On the left side of this page, slide the ”Expert Mode” slider bar over to the ON. This will open a pop-up menu displaying the raw ntp.conf file. The document referenced above will discuss how to edit this configuration file for your IPv6 requirements.

Follow-up email Keith sent to this customer.
There are two changes we recommend you incorporate in the ntp.conf file edits you are adding:

1) restrict ::1 should be changed to: restrict -6 ::1

2) you should remove: restrict -4 default ignore   (It's not needed)

So the new code with these two changes incorporated should now look like the following:

```
restrict 127.0.0.1
restrict -6 ::1
restrict -6 default nomodify noquery
```

NTPQ (Mode 6) and NTPDC (Mode 7)

NTPQ (Mode 6)

- The ntpq utility program is used to monitor NTP daemon ntpd operations and determine performance.
- Refer to: http://www.eecis.udel.edu/~mills/ntp/html/ntpq.html And http://ftp.netbsd.org/pub/NetBSD/NetBSD-current/src/external/bsd/ntp/dist/ntpq/ntpq.html#System-Variables (ntpq user's manual)

Confirming mode 6 queries are still disabled

- Refer to Salesforce Case 178716

Your question

We have a Spectracom SecureSync, Model 1200-213 (serial 13871). We have an open audit ticket to restrict Mode 6 queries. Could you please let me know where in the configuration I should modify to keep the until from responding to such queries?

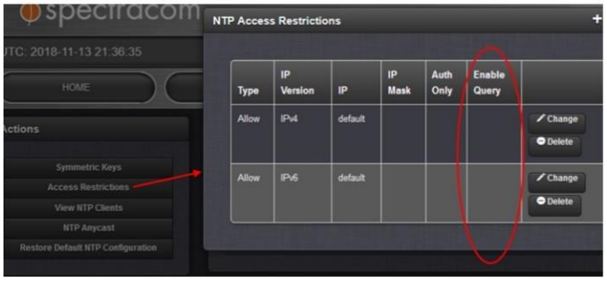
My response

In summary of the info below, Mode 6 queries are disabled by factory default. Unless a user has since enabled the NTP queries, Mode 6 queries are already being blocked.

In case you weren't already aware, there in a great (very easy searchable) online SecureSync user guide,. This document contains the most current info about the SecureSync.

For verifying Mode 6 queries is still disabled, refer to "**allow NTP queries**" at the very bottom of the following page: http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/NTP_AccsRestrict.htm?Highlight=ntp%20queries

And, press the "**Access Restrictions**" button on left side of the **Management** -> **NTP Setup** page of the browser. This will open a pop-up window. as shown below, Mode 6 queries are still disabled if the "**Enable Query**" boxes (for IPv4 and IPv6) are both empty:



NTP Access Restrictions

Type	IP Version	IP	IP Mask	Auth Only	Enable Query	
Allow	IPv4	default				Change Delete
Allow	IPv6	default				Change Delete

NTPDC (Mode 7)

- Refer to: http://www.eecis.udel.edu/~mills/ntp/html/ntpdc.html
    - The **ntpdc** is used to **query the ntpd daemon about its current state** and to request changes in that state.
    - NTPDC no longer available
    - NTPDC is being removed with the NTP version 4.2.8 update (Software version 5.2.1, ~May 8th). It was removed from NTP in this newer version of NTP. NTPQ is still available in NTP 4.2.8.

Desire to use Mode 7 queries

- If it’s desired to enable Mode 7 queries from anywhere on the network, select the “Allow queries from NTPDC or NTPQ over IPv4” and/or the “Allow queries from NTPDC or NTPQ over IPv6” checkboxes (as applicable) at the top of the “NTP Access” tab.
- If there are custom entries added in the Access table (below the list of checkboxes) and its desired to enable NTPQ/NTPDC, uncheck the Allow queries from NTPDC or NTPQ over IPv4” and “Allow queries from NTPDC or NTPQ over IPv6” checkboxes at the top of this NTP Access tab, and select the individual “Enable Query” checkboxes in the last column of the NTP Access table. These individual checkboxes override the two “Allow queries…” checkboxes at the top of this tab.

NTPQ (Mode 6) /NTDC (Mode 7)

Desire to use Mode 6/ Mode 7 queries

- Mode 7 queries no longer available starting with NTP version 4.2.8p2 (software versions 5.2.1 and above).
- If it’s desired to enable Mode 6 and 7 queries from anywhere on the network, select the “Allow queries from NTPDC or NTPQ over IPv4” and/or the “Allow queries from NTPDC or NTPQ over IPv6” checkboxes (as applicable) at the top of the “NTP Access” tab.
- If there are custom entries added in the Access table (below the list of checkboxes) and its desired to enable NTPQ/NTPDC, uncheck the Allow queries from NTPDC or NTPQ over IPv4” and “Allow queries from NTPDC or NTPQ over IPv6” checkboxes at the top of this NTP Access tab, and select the individual “Enable Query” checkboxes in the last column of the NTP Access table. These individual checkboxes override the two “Allow queries…” checkboxes at the top of this tab.

Reported Issue: ShadowServer is reporting NTP is responding to Mode 6 requests, even though “NTP Queries” is disabled in NTP Setup page

- Refer to Salesforce case 25589 (9 Jun 17)
- Refer also to
- With v5.5.1 installed, Nessus scanner reported NetClock is responding to Mode 6 queries even though qeries are not enabled (Paul M and I confirned noqueries was in the ntp.conf file.
- Though we couldnlt find any NTP bug reports for this issue, recommeneded they update to v5.7.0 (updating NTP from 4.2.8p9 to 4.2.8p10) and then rescan it.

ShadowServer foundation/scanner

Per https://ntpscan.shadowserver.org/

Established in 2004, The Shadowserver Foundation gathers intelligence on the darker side of the internet. We are comprised of volunteer security professionals from around the world. Our mission is to understand and help put a stop to high stakes cybercrime in the information age.

The Shadowserver Foundation is currently undertaking a project to search for publicly accessible devices that have NTP running and answering Mode 6 queries. The goal of this project is to identify openly accessible NTP services and report them back to the network owners for remediation.

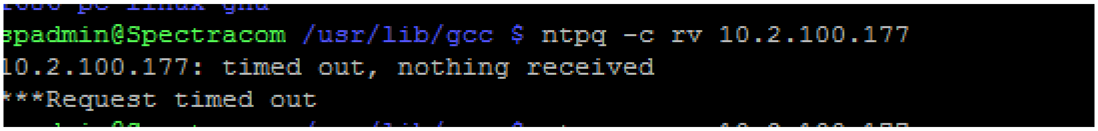
Methodology

We are querying all computers with routable IPv4 addresses that are not firewalled from the internet on port 123/udp with an NTPv2 request for **READVAR** control message. We are capturing the response from the NTP service and parsing the result. We intend no harm, but if we are causing problems, please contact us at gro [tod] revreswodahs [ta] nacssnd

If you would like to test your own device to see if it supports Mode 6 queries, try the command: "**ntpq -c rv [IP]**". If the command is successful, you will see a string of information from the IP that you queried that usually starts off with something like this: 'associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync, version="ntpd 4.2.6p2@1.2194-o Sun Oct 17 13:35:13 UTC 2010 (1)", processor="x86_64", system="Linux/3.2.0-0.bpo.4-amd64", leap=00'.

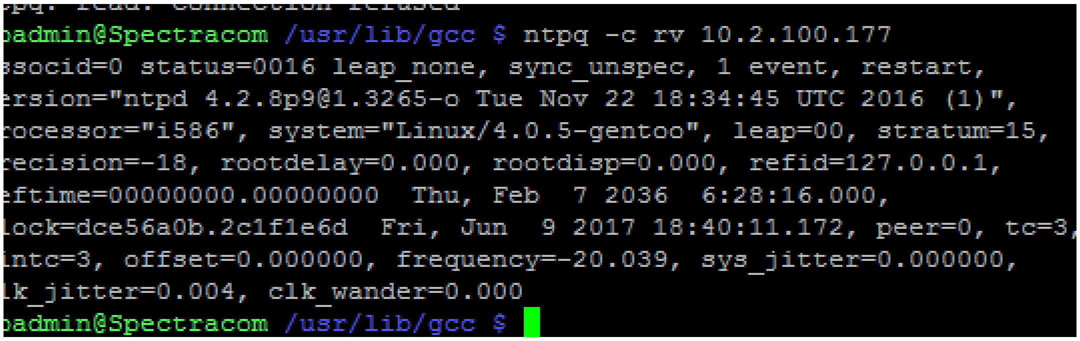
My testing with our SecureSyncs using the ntpq -c rv command (10.2.100.177 is running v5.5.1)

A) With NTP Queries disabled on 10.2.100.177 (using CLI of 10.2.100.176)



```
i686-pc-linux-gnu
spadmin@Spectracom /usr/lib/gcc $ ntpq -c rv 10.2.100.177
10.2.100.177: timed out, nothing received
***Request timed out
```

B) With NTP Queries enabled on 10.2.100.177 (using CLI of 10.2.100.176)



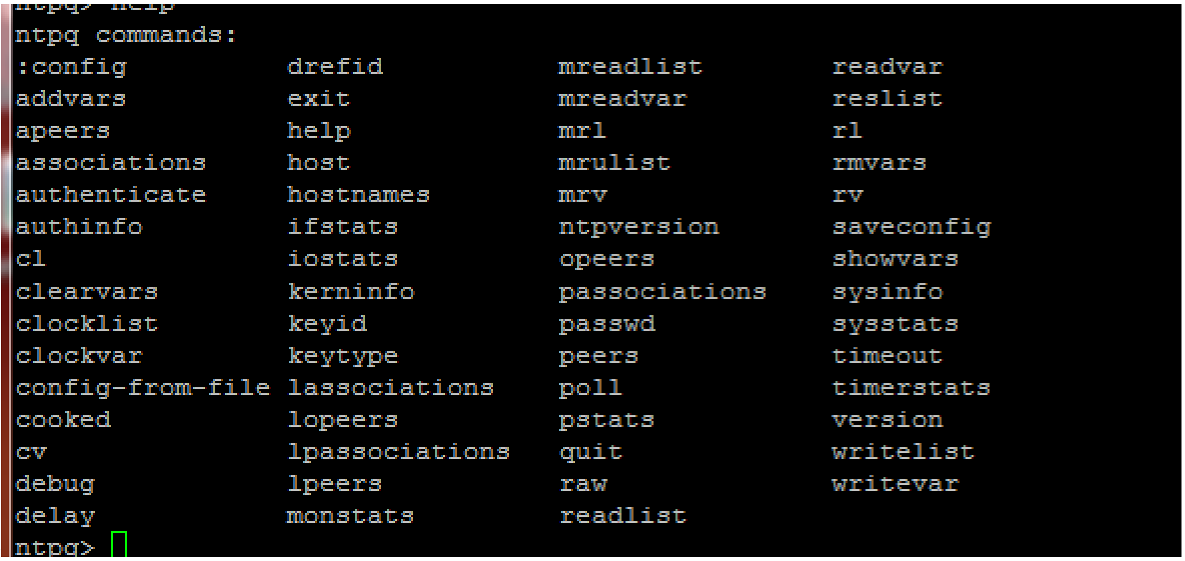
```
pq: read: Connection refused
padmin@Spectracom /usr/lib/gcc $ ntpq -c rv 10.2.100.177
ssocid=0 status=0016 leap_none, sync_unspec, 1 event, restart,
ersion="ntpd 4.2.8p9@1.3265-o Tue Nov 22 18:34:45 UTC 2016 (1)",
rocessor="i586", system="Linux/4.0.5-gentoo", leap=00, stratum=15,
recision=-18, rootdelay=0.000, rootdisp=0.000, refid=127.0.0.1,
eftime=00000000.00000000  Thu, Feb  7 2036  6:28:16.000,
lock=dce56a0b.2c1f1e6d  Fri, Jun  9 2017 18:40:11.172, peer=0, tc=3,
intc=3, offset=0.000000, frequency=-20.039, sys_jitter=0.000000,
lk_jitter=0.004, clk_wander=0.000
padmin@Spectracom /usr/lib/gcc $
```

Stuart (co-op) even went as far as using tcpdump to cofirm what is being sent out with noquery, as compared to queries enabled.

This appears to be an issue in NTP itself, associated with at least one NTPQ command responding even with queries disabled (nessus is sending a command which gets through).

(**With queries disabled)**
Commands such as the peers (pe) command seems to be being blocked correctly by queries disabled. But commands such as version still respond with queries disabled.

for a descripotion of each command, refer to:
https://www.ibm.com/support/knowledgecenter/en/ssw_aix_61/com.ibm.aix.cmds4/ntpq.htm



```
ntpq> help
ntpq commands:
:config          drefid           mreadlist        readvar
addvars          exit             mreadvar         reslist
apeers           help             mrl              rl
associations     host             mrulist          rmvars
authenticate     hostnames        mrv              rv
authinfo         ifstats          ntpversion       saveconfig
cl               iostats          opeers           showvars
clearvars        kerninfo         passociations    sysinfo
clocklist        keyid            passwd           sysstats
clockvar         keytype          peers            timeout
config-from-file lassociations    poll             timerstats
cooked           lopeers          pstats           version
cv               lpassociations   quit             writelist
debug            lpeers           raw              writevar
delay            monstats         readlist
ntpq>
```

e

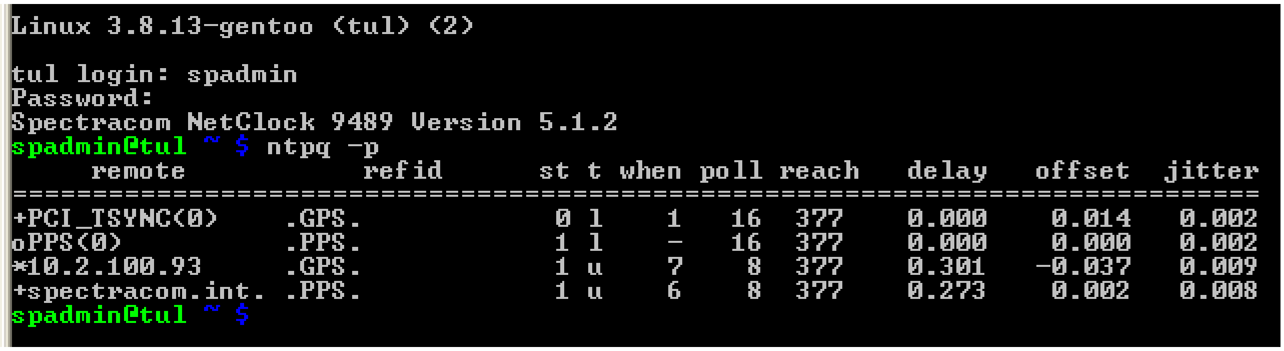
NTP peers command (ntpq –p or ntpq –pn)

- Refer to: http://doc.ntp.org/4.1.0/debug.htm
- Lists all configured NTP inputs and reports statistics of each
- Type ntpq –pn at the command prompt (the “n” changes “names” to IP addresses to alleviate confusion)
- If already in “ntpq>”, just type **pe** <enter> to repeat the command (As shown in second screenshot below):

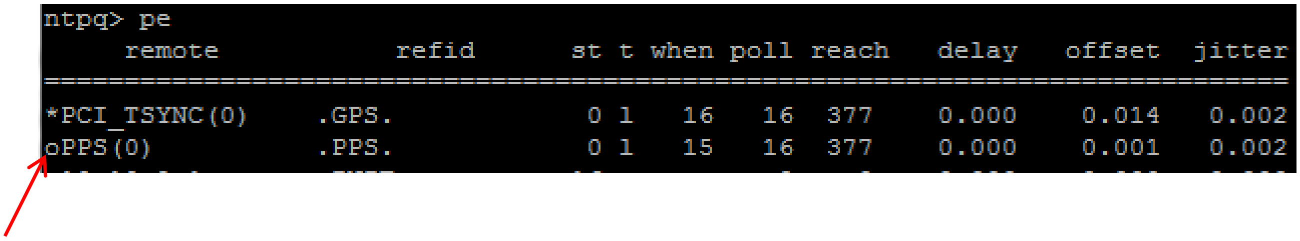
Format of response: [tally] remote refid st t when pool reach delay offset jitter (see examples)

“t” value

u: unicast or manycast client
b: broadcast or multicast client
l: local (reference clock)
s: symmetric (peer)
A: manycast server
B: broadcast server
M: multicast server.



```
Linux 3.8.13-gentoo (tul) (2)

tul login: spadmin
Password:
Spectracom NetClock 9489 Version 5.1.2
spadmin@tul ~ $ ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+PCI_TSYNC(0)    .GPS.            0 l    1   16  377    0.000    0.014   0.002
oPPS(0)          .PPS.            1 l    -   16  377    0.000    0.000   0.002
*10.2.100.93     .GPS.            1 u    7    8  377    0.301   -0.037   0.009
+spectracom.int. .PPS.            1 u    6    8  377    0.273    0.002   0.008
spadmin@tul ~ $
```



```
ntpq> pe
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*PCI_TSYNC(0)    .GPS.            0 1   16   16  377    0.000    0.014   0.002
oPPS(0)          .PPS.            0 1   15   16  377    0.000    0.001   0.002
```

“Tally Code”:

Sync (“Tally Code”): a symbol that indicates if the listed reference is available for selection as a reference. The following table indicates the symbols and their meanings.

Tally code	Green = (Sync)
	Red = (Not in Sync) (if the Reach is not 0)
		Truechimer (good) or falseticker (bad)
		(as determined by the Clock Select Algorithm)

*	The Selected **Time** reference	Truechimer
o	The Selected **PPS** reference	Truechimer
+	A **high quality candidate** for NTP reference input that can be selected by NTP as its time reference (Good reference, but not selected)	Truechimer
x	“**Falseticker**” Listed NTP Peer was discarded from selection (NTP won’t select this peer as its reference).	falseticker
-	“**Outlyer**” Listed NTP Peer was discarded from selection (NTP won’t select this peer as its reference).	falseticker
(blank)	Source **discarded**: Failed Sanity check	falseticker

Fields of the ntpq -p / ntpq -pn response

refid column shows the current source of synchronization, while
st column reveals the stratum,
t the type (u = unicast, m = multicast, l = local, - = don't know),
poll the poll interval in seconds.
when column shows the time since the peer was last heard in seconds.
reach column shows the status of the reachability register (in octal).

an 8-bit left-rotating register. Any 1 bit means that a "time packet" was received. The right most bit indicates the status of the last connection with the NTP server. It is Octal number. Use calculator in programmer interface to translate from OCT to BIN: For example, 377 translates to 11111111. Each 1 means a successful connection to the NTP server. If you just start a NTP service, and it connects successfully with its server, this number will change as follows (assuming connectivity is good):

00000001 = 001
00000011 = 003
00000111 = 007
00001111 = 017
00011111 = 037
00111111 = 077
01111111 = 177
11111111 = 377

(Delay, offset and jitter in milliseconds).

- **delay** the time delay (in milliseconds) to communicate with the remote.
- **offset** the offset (in milliseconds) between our time and that of the remote.
- **jitter** the observed jitter (in milliseconds) of time with the remote.

NTPQ Associations (as)

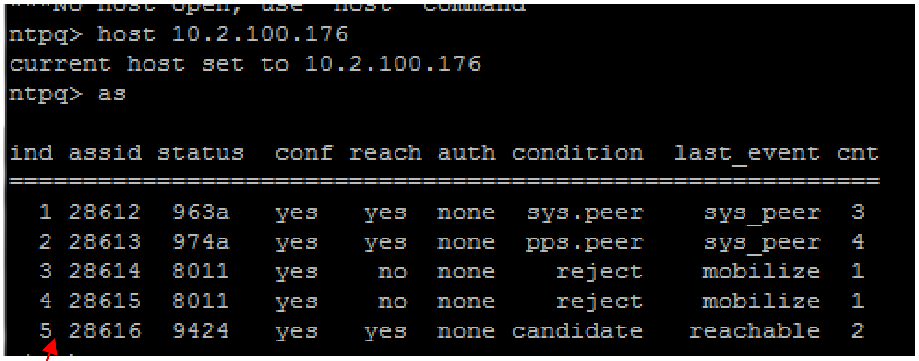
- ➢ Refer to: http://doc.ntp.org/4.1.0/debug.htm
- ➢ Provides detailed info for each peer/server
- ➢ Requires “enable queries” (for NTPQ/NTPDC) to be Enabled (disabled by default).

To enable NTPQ/NTPDC queries:

In the newer black browser: **Management** -> **NTP Setup** page and click **Access Restrictions** on the left side of the page. Press Change and enable Queries.

1. Need to first define the “host” as this particular time server.
   - ○ Use the command of host xxx.xxx.xxx.xxx <enter> (where x is the IP address of the time server).

2. Type **as** <enter>



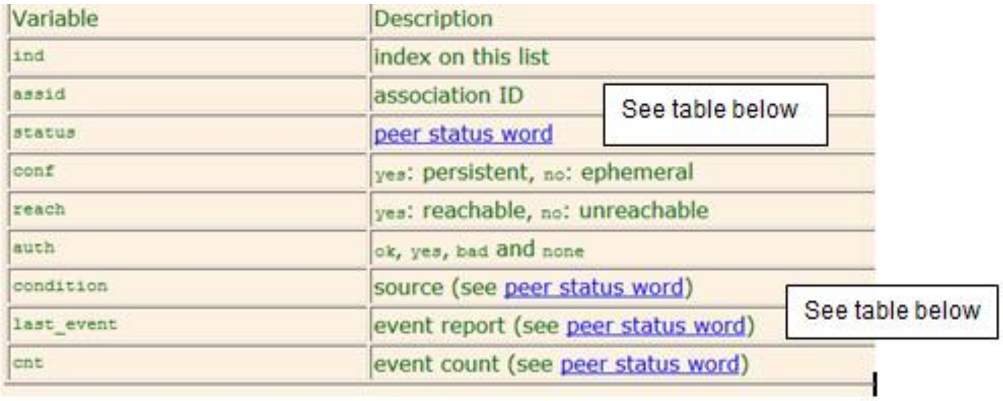
```
***No host open, use `host' command
ntpq> host 10.2.100.176
current host set to 10.2.100.176
ntpq> as

ind assid status  conf reach auth condition  last_event cnt
===========================================================
  1 28612  963a   yes   yes  none  sys.peer    sys_peer  3
  2 28613  974a   yes   yes  none  pps.peer    sys_peer  4
  3 28614  8011   yes    no  none    reject    mobilize  1
  4 28615  8011   yes    no  none    reject    mobilize  1
  5 28616  9424   yes   yes  none candidate  reachable  2
```

Condition column: Displays current NTP selection
sys.peer: System peer (current selected reference)
pps.peer: PPS peer (current selected PPS reference)
candidate: included by the combime algorithm (OK)
falseticker: currently discarded by the intersection algorithm
outlier: currently discarded by the cluser algorithm (big offset)
reject: currently discarded as not valid (not currently selectable)

Last_event column: Most recent event message received
sys_peer: become system peer (if not already)
mobilize: association mobilized (was previously rejected)
demobilize: association demobilized (reject it now)
reachable: server reachable
unreachable: server unreachable
no reply: no server found
Access denied: Access denied by Peer’s NTP configuration
Leap_armed: leap second to be applied

Assid (AS command): Correlates to the list of each peer shown in the **NTPQ -p** command. For example, **PCI_Tsync<0>** equates to “28612” (first one in response)

The below Associations (AS) table is from: http://doc.ntp.org/4.2.6/ntpq.html#clock

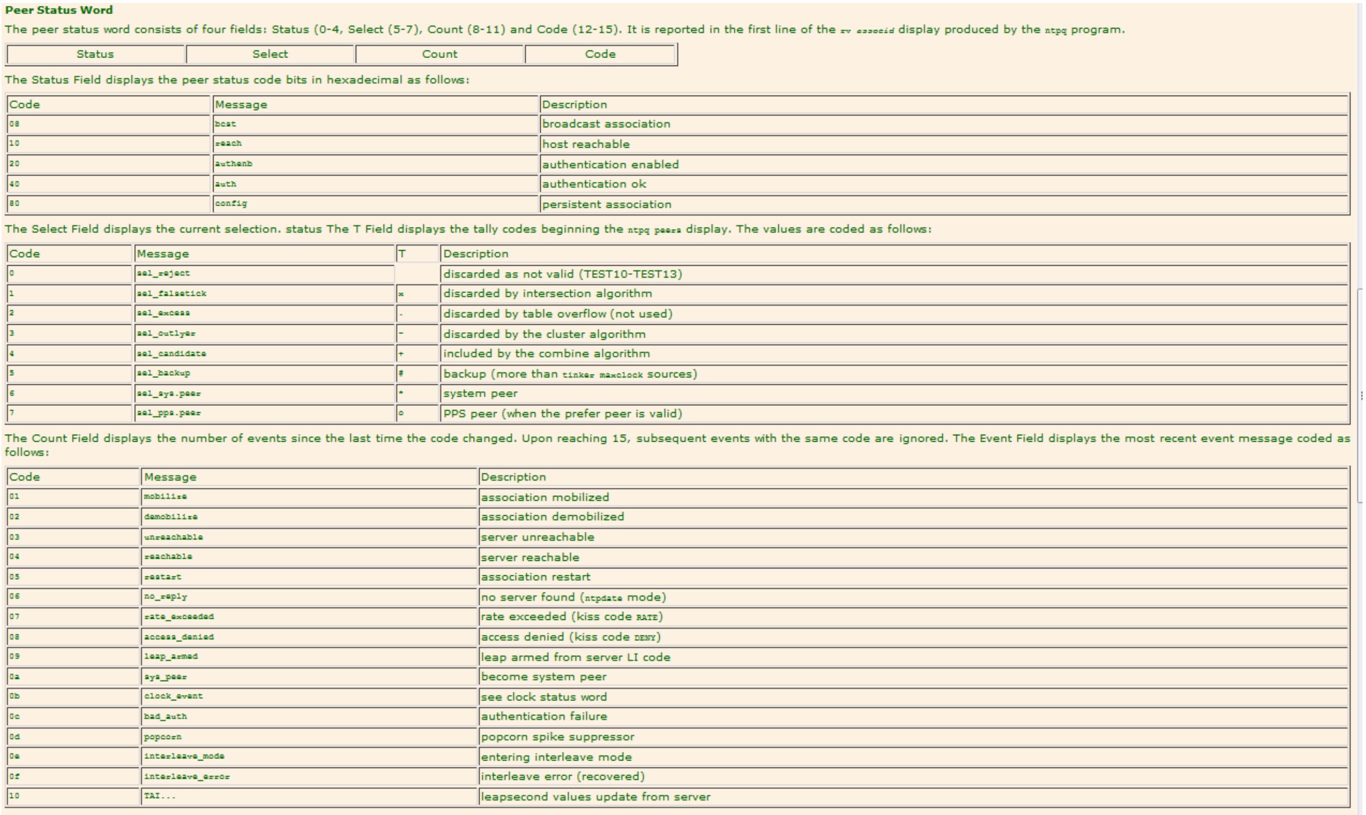


Variable	Description
ind	index on this list
assid	association ID
status	peer status word
conf	yes: persistent, no: ephemeral
reach	yes: reachable, no: unreachable
auth	ok, yes, bad and none
condition	source (see peer status word)
last_event	event report (see peer status word)
cnt	event count (see peer status word)

See table below

See table below

The below table is at: http://doc.ntp.org/4.2.6/decode.html#sys



Peer Status Word

The peer status word consists of four fields: Status (0-4, Select (5-7), Count (8-11) and Code (12-15). It is reported in the first line of the rv associd display produced by the ntpq program.

Status	Select	Count	Code

The Status Field displays the peer status code bits in hexadecimal as follows:

Code	Message	Description
08	bcst	broadcast association
10	reach	host reachable
20	authenb	authentication enabled
40	auth	authentication ok
80	config	persistent association

The Select Field displays the current selection. status The T Field displays the tally codes beginning the ntpq peers display. The values are coded as follows:

Code	Message	T	Description
0	sel_reject		discarded as not valid (TEST10-TEST13)
1	sel_falsetick	x	discarded by intersection algorithm
2	sel_excess	.	discarded by table overflow (not used)
3	sel_outlyer	-	discarded by the cluster algorithm
4	sel_candidate	+	included by the combine algorithm
5	sel_backup	#	backup (more than tinker maxclock sources)
6	sel_sys.peer	*	system peer
7	sel_pps.peer	o	PPS peer (when the prefer peer is valid)

The Count Field displays the number of events since the last time the code changed. Upon reaching 15, subsequent events with the same code are ignored. The Event Field displays the most recent event message coded as follows:

Code	Message	Description
01	mobilize	association mobilized
02	demobilize	association demobilized
03	unreachable	server unreachable
04	reachable	server reachable
05	restart	association restart
06	no_reply	no server found (ntpdate mode)
07	rate_exceeded	rate exceeded (kiss code RATE)
08	access_denied	access denied (kiss code DENY)
09	leap_armed	leap armed from server LI code
0a	sys_peer	become system peer
0b	clock_event	see clock status word
0c	bad_auth	authentication failure
0d	popcorn	popcorn spike suppressor
0e	interleave_mode	entering interleave mode
0f	interleave_error	interleave error (recovered)
10	TAI...	leapsecond values update from server

Detailed synposis (rv) for this server, or all servers on the network.

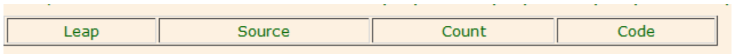
- Refer to: http://doc.ntp.org/3-5.93e/debug.html and http://doc.ntp.org/4.1.0/debug.htm
- Provides detailed info for each peer/servers
- Requires “enable queries” (for NTPQ/NTPDC) to be Enabled to see all NTP servers on the network0 beyond just the one the command is being performed on. (disabled by default).

Next, use the **rv** command and the respective `assID` identifier to display a detailed synopsis for the selected peer, such as “28612”).

From http://doc.ntp.org/4.2.6/ntpq.html

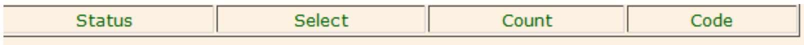
> **RV**: Display the specified variables. If *assocID* is zero, the variables are from the system variables name space, otherwise they are from the peer variables name space. The *assocID* is required, as the same name can occur in both spaces. If no *name* is included, all operative variables in the name space are displayed. In this case only, if the *assocID* is omitted, it is assumed zero. Multiple names are specified with comma separators and without whitespace. Note that time values are represented in milliseconds and frequency values in parts-per-million (PPM). Some NTP timestamps are represented in the format YYYYMMDDTTTT, where YYYY is the year, MM the month of year, DD the day of month and TTTT the time of day.

- There is one ***system status word*** and a ***peer status word*** for each association.
- **System status word** is the first line of the rv response



Leap	Source	Count	Code

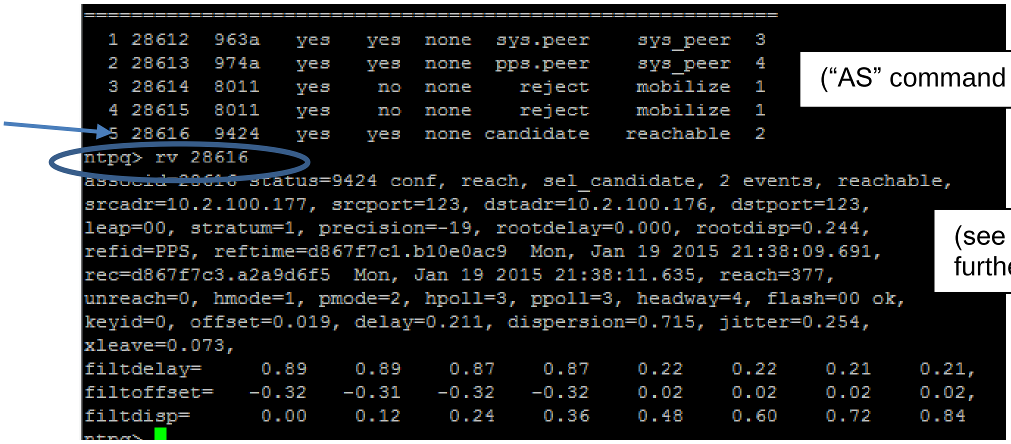
- **Peer status word** is the first line of the rv response



Status	Select	Count	Code

- There is a ***clock status word*** for each association that supports a **reference clock** (our tsync driver)

1. **Type rv yyyyy** <enter> (where yyyy is a particular **assid** number from the **as** response above (such as 28612 for example):



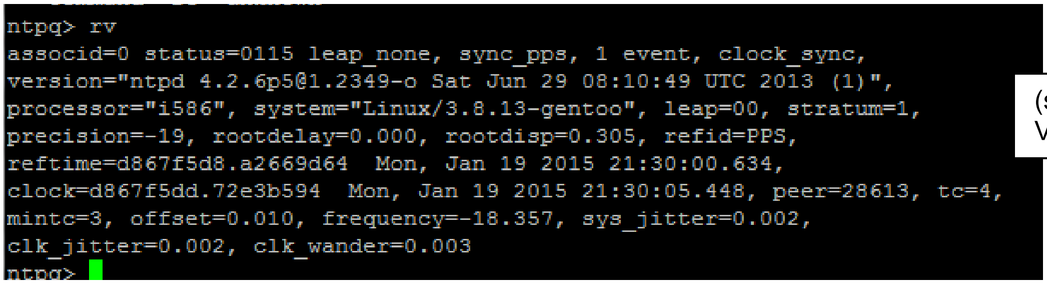
```
==========================================================================
  1 28612  963a   yes   yes  none  sys.peer    sys_peer  3
  2 28613  974a   yes   yes  none  pps.peer    sys_peer  4
  3 28614  8011   yes    no  none    reject    mobilize  1
  4 28615  8011   yes    no  none    reject    mobilize  1
  5 28616  9424   yes   yes  none candidate   reachable  2
ntpq> rv 28616
associd=28616 status=9424 conf, reach, sel_candidate, 2 events, reachable,
srcadr=10.2.100.177, srcport=123, dstadr=10.2.100.176, dstport=123,
leap=00, stratum=1, precision=-19, rootdelay=0.000, rootdisp=0.244,
refid=PPS, reftime=d867f7c1.b10e0ac9  Mon, Jan 19 2015 21:38:09.691,
rec=d867f7c3.a2a9d6f5  Mon, Jan 19 2015 21:38:11.635, reach=377,
unreach=0, hmode=1, pmode=2, hpoll=3, ppoll=3, headway=4, flash=00 ok,
keyid=0, offset=0.019, delay=0.211, dispersion=0.715, jitter=0.254,
xleave=0.073,
filtdelay=     0.89    0.89    0.87    0.87    0.22    0.22    0.21    0.21,
filtoffset=   -0.32   -0.31   -0.32   -0.32    0.02    0.02    0.02    0.02,
filtdisp=      0.00    0.12    0.24    0.36    0.48    0.60    0.72    0.84
ntpq>
```

(“AS” command response)

(see “System Variables”table further below)

Note: “filtdelay”, “filtoffset” and “filtdisp” (shown at the bottom of the “rv 28616” response screenshot above)

2. Can also type just **rv** without an assid number (as shown below):

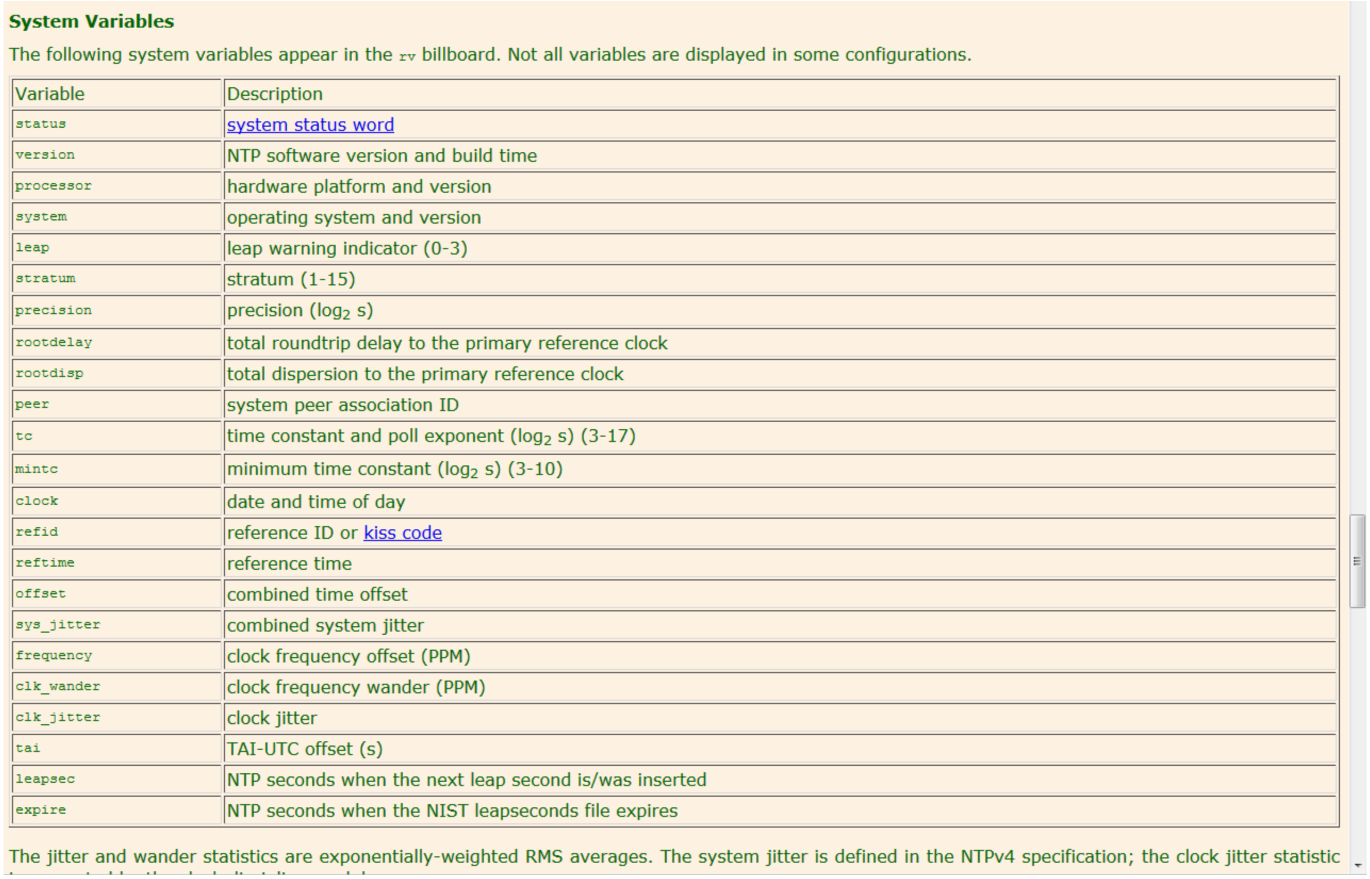


```
ntpq> rv
associd=0 status=0115 leap_none, sync_pps, 1 event, clock_sync,
version="ntpd 4.2.6p5@1.2349-o Sat Jun 29 08:10:49 UTC 2013 (1)",
processor="i586", system="Linux/3.8.13-gentoo", leap=00, stratum=1,
precision=-19, rootdelay=0.000, rootdisp=0.305, refid=PPS,
reftime=d867f5d8.a2669d64  Mon, Jan 19 2015 21:30:00.634,
clock=d867f5dd.72e3b594  Mon, Jan 19 2015 21:30:05.448, peer=28613, tc=4,
mintc=3, offset=0.010, frequency=-18.357, sys_jitter=0.002,
clk_jitter=0.002, clk_wander=0.003
ntpq> 
```

(see “System Variables” table below)

Note: “filtdelay”, “filtoffset” and “filtdisp” (shown at the bottom of the “rv 28616” response screenshot further above) are not reported when “rv” is performed with adding an association number (as show in the screenshot directly above).

Below is from: http://doc.ntp.org/4.2.6/ntpq.html#clock



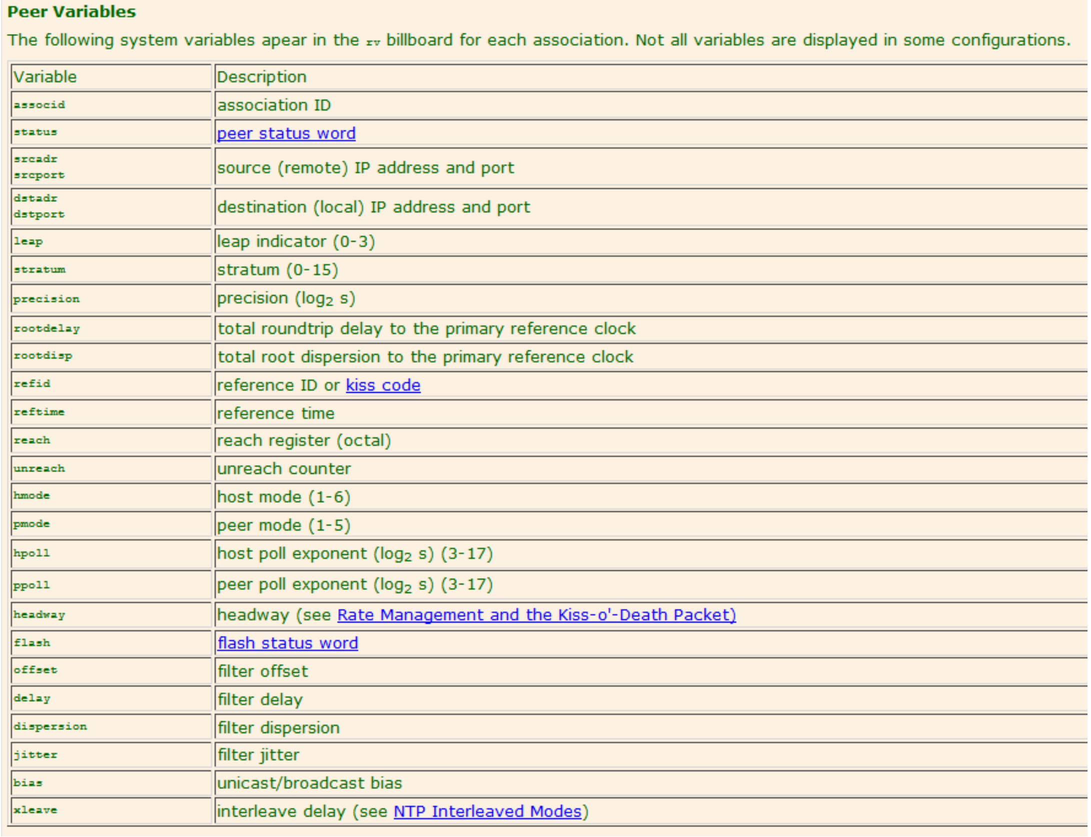
System Variables

The following system variables appear in the rv billboard. Not all variables are displayed in some configurations.

Variable	Description
status	system status word
version	NTP software version and build time
processor	hardware platform and version
system	operating system and version
leap	leap warning indicator (0-3)
stratum	stratum (1-15)
precision	precision (log$_2$ s)
rootdelay	total roundtrip delay to the primary reference clock
rootdisp	total dispersion to the primary reference clock
peer	system peer association ID
tc	time constant and poll exponent (log$_2$ s) (3-17)
mintc	minimum time constant (log$_2$ s) (3-10)
clock	date and time of day
refid	reference ID or kiss code
reftime	reference time
offset	combined time offset
sys_jitter	combined system jitter
frequency	clock frequency offset (PPM)
clk_wander	clock frequency wander (PPM)
clk_jitter	clock jitter
tai	TAI-UTC offset (s)
leapsec	NTP seconds when the next leap second is/was inserted
expire	NTP seconds when the NIST leapseconds file expires

The jitter and wander statistics are exponentially-weighted RMS averages. The system jitter is defined in the NTPv4 specification; the clock jitter statistic

Peer variables table (http://doc.ntp.org/4.2.6/ntpq.html)



Peer Variables

The following system variables apear in the `rv` billboard for each association. Not all variables are displayed in some configurations.

Variable	Description
`associd`	association ID
`status`	peer status word
`srcadr` `srcport`	source (remote) IP address and port
`dstadr` `dstport`	destination (local) IP address and port
`leap`	leap indicator (0-3)
`stratum`	stratum (0-15)
`precision`	precision ($\log_2$ s)
`rootdelay`	total roundtrip delay to the primary reference clock
`rootdisp`	total root dispersion to the primary reference clock
`refid`	reference ID or kiss code
`reftime`	reference time
`reach`	reach register (octal)
`unreach`	unreach counter
`hmode`	host mode (1-6)
`pmode`	peer mode (1-5)
`hpoll`	host poll exponent ($\log_2$ s) (3-17)
`ppoll`	peer poll exponent ($\log_2$ s) (3-17)
`headway`	headway (see Rate Management and the Kiss-o'-Death Packet)
`flash`	flash status word
`offset`	filter offset
`delay`	filter delay
`dispersion`	filter dispersion
`jitter`	filter jitter
`bias`	unicast/broadcast bias
`xleave`	interleave delay (see NTP Interleaved Modes)

NTP Status/Statistics graphs (NTP Throughput, NTP Performance, Time Offset)

- ➢ Refer to online 2400 SecureSync user guide at: http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/OPRTN/StatMon_NTP
- ➢ NTP Status Graphs are in the ***Management*** -> ***NTP Setup*** page of the the newer browser.

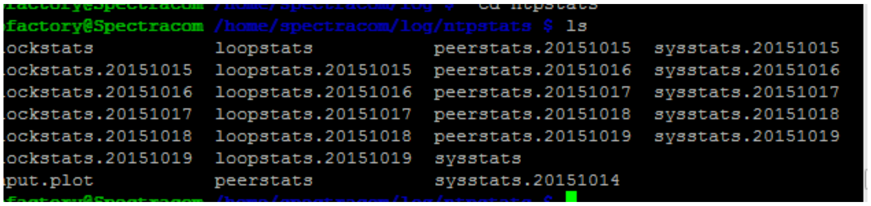
NTP Throughput/NTP Statistics: Number of NTP requests per second/NTP Stress test

- ➢ Refer to Salesforce cases such as 272108 (Sept 2021)
- ➢ Refer to: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync-2400 (Diamond)\NTP\NTP stress testing
- ➢ Refer to NTP throughput documents on our website- links further below ???
- **Test protocol (tech note):** http://spectracom.com/sites/default/files/document-files/NTP_Server_Capacity_Testing_TN19-101_B.pdf (note this link is also available within the knowledge base article mentioned above)
- ➢ **Refer to the** ntp.log for info on NTP statistics (pkt/s) ??

NTP Performance Graphs

NTP data for the NTP performance graphs (Time Offset, Freq Offset and Jitter) located on the left side of the NTP Setup page

- ➢ The graphs are generated using the NTP data (clockstats, peerstats and sysstats) stored in the NTPStats folder (/home/spectracom/logs/ntpstats)
- ➢ The graph data is included in the log bundle.



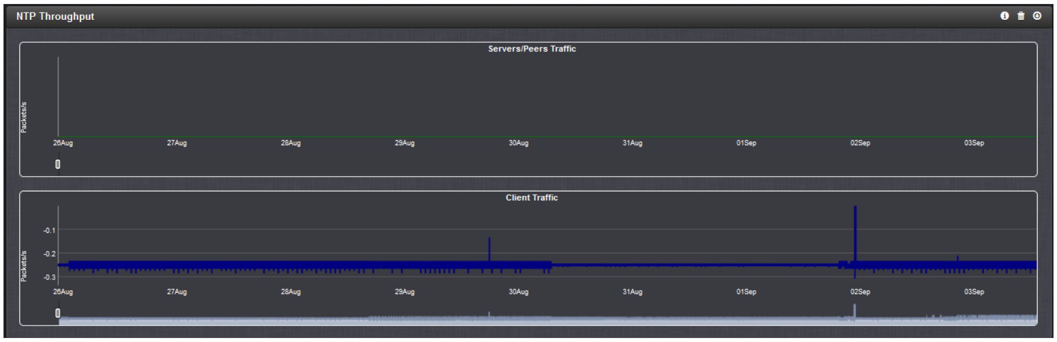
```
factory@Spectracom /home/spectracom/log $  cd ntpstats
factory@Spectracom /home/spectracom/log/ntpstats $ ls
ockstats           loopstats           peerstats.20151015  sysstats.20151015
ockstats.20151015  loopstats.20151015  peerstats.20151016  sysstats.20151016
ockstats.20151016  loopstats.20151016  peerstats.20151017  sysstats.20151017
ockstats.20151017  loopstats.20151017  peerstats.20151018  sysstats.20151018
ockstats.20151018  loopstats.20151018  peerstats.20151019  sysstats.20151019
ockstats.20151019  loopstats.20151019  sysstats
put.plot           peerstats           sysstats.20151014
factory@Spectracom /home/spectracom/log/ntpstats $
```

- ➢ For more information on the breakdown of this NTP data, refer to the following page of the ntp website: https://www.eecis.udel.edu/~mills/ntp/html/monopt.html

Recommendation to be able to better review these files: Rename the files with the extension of "**.csv**" . The file will still open with Excel, but the comma delimited values will be in separate columns, instead of all values being in the same column when just opening as a standard excel file.

NTP throughput graphs/throughput logs

The NTP Throughput graph



NTP Throughput shows two graphs depicting the rate of NTP traffic from Clients and Server/Peers.

- The INFO icon opens a window showing the maximum per second traffic rate from each.
- The graphs may be saved and downloaded (> ARROW icon), or deleted (> TRASH CAN icon).

- In addition to the existing NTP Status graphs (discussed below), NTP throughput graphs/NTP Traffic graphs (The “Servers/Peers Traffic” and “Client traffic” graphs) to the Management -> NTP Setup page of the browser.
- Reports packets being exchanged each second.

Where:

○ **Clients**: NTP requests from NTP clients on the network

○ **Servers/Peers**: NTP requests from Servers or Peers configured to get time from this SecureSync

A) To convert pkt/s (values in the graphs/logs) to the actual number of packets in the hour

Multiply the number of pkt/s (value in the graphs/logs) times 60 and then round-up to nearest whole number

Examples:

0.017 pkt/s = 1 packet in one hour

0.083 pkt/s = 5 packets in one hour

0.167 pkt/s = 10 packets in one hour

1.667 pkt/s = 100 packets in one hour

166.667 pkt/s = **10,000** packets in one hour

3000 pkt/s = 180,000 packets in one hour

B) To convert actual number of packets per hour to pkt/s (values in the graphs/logs)

Divide the number of ntp packets in the hour by 60 (there are 60 minutes in the report period)

Examples:

1 packet in one hour = **0.017 pkt/s**

5 packets in one hour = **0.083 pkt/s**

10 packets in one hour = **0.167 pkt/s**

100 packets in one hour = **1.667 pkt/s**

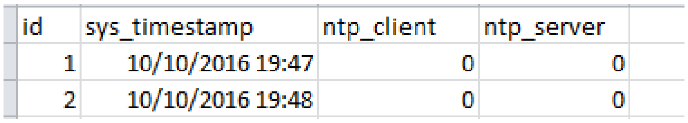
10,000 packets in one hour = **166.667 pkt/s**

180,000 packets in one hour = **3000 pkt/s**

Downloading the NTP throughput graph data

Download graph data as a .csv file

NTP Graph Data can be downloaded (using down arrow icon) or deleted (using the garbage can icon). The file is named "**LogNTPStat.csv**".



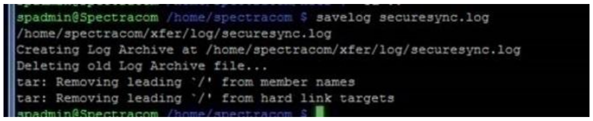
id	sys_timestamp	ntp_client	ntp_server
1	10/10/2016 19:47	0	0
2	10/10/2016 19:48	0	0

Download graph data using the CLI interface (instead of downloading a .csv file via the browser, as with heavy loading/earlier versions of software like v5.3.1 "hanging" when trying to download the data)

The NTP throughput data is stored in the mysql database, which is contained in the log bundle. Via CLI - The log bundle file can be generated (**savelog securesync.log** command) and the exported from the **home/spectracom/xfer/log directory** using FTP/SCP.

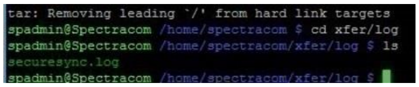
Email Keith sent (12 Oct 16) The data for the NTP throughput graphs displayed on the bottom of the **Management -> NTP Setup** page of the browser can be exported out of the time server as either a .csv file, or inside a log bundle. The log bundle is a single file containing all of the unit's log entries and other data. This log bundle file can be exported using either the browser or the CLI interface (telnet/ssh to generate the file and FTP/SCP to download the file to a computer).

This log bundle file can be generated and automatically downloaded to a PC using the "**Save and Download All Logs**" button on the left-side of the **Management -> Log Configuration** page of the browser. To download the file using the CLI interface (instead of using the web browser) first establish a telnet/ssh session and then type the following command: savelog securesync.log (where securesync.log is an arbitrary name for this file) as shown below:



```
spadmin@Spectracom /home/spectracom $ savelog securesync.log
/home/spectracom/xfer/log/securesync.log
Creating Log Archive at /home/spectracom/xfer/log/securesync.log
Deleting old Log Archive file...
tar: Removing leading `/' from member names
tar: Removing leading `/' from hard link targets
spadmin@Spectracom /home/spectracom $
```

This bundle file is generated and saved in the **home/spectracom/xfer/log** directory (as shown below). This file can then be transferred out of the unit via an FTP or SCP connection to this directory.



```
tar: Removing leading `/' from hard link targets
spadmin@Spectracom /home/spectracom $ cd xfer/log
spadmin@Spectracom /home/spectracom/xfer/log $ ls
securesync.log
spadmin@Spectracom /home/spectracom/xfer/log $
```

This log bundle file is tarred twice to decrease its size as much as possible for being able to email it to us for review. Once the file has been downloaded via either the web browser or the CLI interface, first untar this file and then untar again the file that is generated from the first untarring. The file will probally be around 30 MB or so once its been fully untarred.

With versions 5.3.1 and higher, there will be three separate folders in the untarred file. They are the **home**, **srv** and **var** files. Open the srv file and click through each of the folders that appear (**www2**, **app** and then **webroot**). This will lead you to the lafayette file. Rename this file as **lafayette.db.**

This **database** file can be opened using the freeware MySQL viewer program called "DB Browser for SQLite" (http://sqlitebrowser.org). After opening the DB browser program, click on **File** -> **Open Database** and navigate to the **lafayette.db** file. With the database now open in the DB Browser program, select the "**Browse Data**" tab at the top of the page. In the "**Table**" drop-down (just below the four tabs), select "**log_ntp_stats**". The data for the NTP throughput graphs will now be displayed (and can be copy/pasted out as desired).

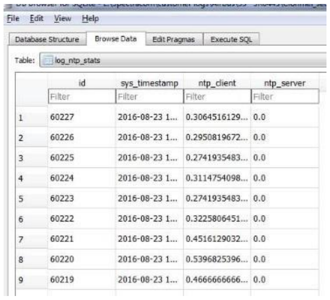


Table: log_ntp_stats

	id	sys_timestamp	ntp_client	ntp_server
	Filter	Filter	Filter	Filter
1	60227	2016-08-23 1...	0.3064516129...	0.0
2	60226	2016-08-23 1...	0.2950819672...	0.0
3	60225	2016-08-23 1...	0.2741935483...	0.0
4	60224	2016-08-23 1...	0.3114754098...	0.0
5	60223	2016-08-23 1...	0.2741935483...	0.0
6	60222	2016-08-23 1...	0.3225806451...	0.0
7	60221	2016-08-23 1...	0.4516129032...	0.0
8	60220	2016-08-23 1...	0.5396825396...	0.0
9	60219	2016-08-23 1...	0.4666666666...	0.0

FYI- All the units logs that are displayed in the **Tools** drop-down of the browser, and a couple of other logs stored in the background, are located in the **home/spectracom/log** directory of the downloaded log bundle.

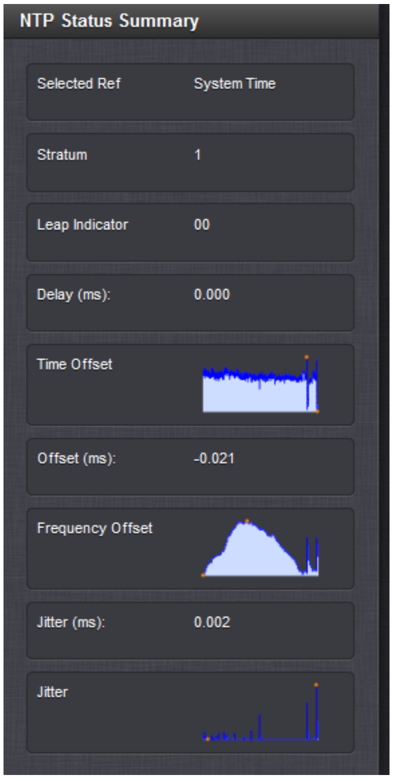
NTP throughput also provided hourly in ntp logs

- Refer to (in this document):

Management -> **NTP Setup** page of the browser (there is a separate tab for each graph) the graph is in the lower-left corner.

Note that it takes about 6 seconds for the information to be displayed once the page has been opened (delay is due to the time it takes for NTPQ to obtain the info from NTP)

Clicking on the Time Offset, Frequency Offset or Jitter graphs opens an expanded view of that graph.



NTP Status Summary

Selected Ref	System Time
Stratum	1
Leap Indicator	00
Delay (ms):	0.000
Time Offset	
Offset (ms):	-0.021
Frequency Offset	
Jitter (ms):	0.002
Jitter	

The graphs displayed in the NTP section have dynamic vertical scales. The bottom scale is the number of seconds since UTC midnight. The graph shows about 22 hours across.

1. **Time Offset Graph**

   - Reports the time offset (in scientific notation) between NTP and its selected reference.

     The vertical scales vary depending upon the actual error values so pay close attention to the labeling. Above a certain value, a decimal notation is used (such as 0.01 seconds). Once the error value decreases, the values change to scientific notation (such as 2e-06).
     The scientific breakdown is as follows:
     1e-09 = **1 ns** or 0000.000000001
     1e-08= 10 ns
     1e-07= 100ns
     1e-06= **1 microsecond** or 0000.000001000
     1e-05= 10 microseconds 0000.000010000
     1e-04= 100 microseconds or 0000.000100000
     1e-03= **1 milliseconds** or 0000.001000000
     1e-02= 10 milliseconds or 0000.01000000
     1e-01= 100 milliseconds or 0000.100000000
     1e+00=1 second or 0001.000000000
     1e+01= **10 Seconds** or 0010.000000000
     1e+02= **100 Seconds** or 0100.000000000
     1e+03= **1000 Seconds** 1000.000000000

     Note: If the first digit isn't a "1", multiply the first digit by the "time" value in the table above
     Examples
     2e-05= 20 microseconds or 0000.000020000 ("2" times "10 microseconds" is 20 microseconds)
     5e-06= 5 microseconds or 0000.000050000 ("5" times "1 microseconds" is 5 microseconds)

2. **RMS Jitter Graph**

   - Reports the variance in time offset (in seconds), from one calculation to the next
   - Official definition: The value reported by NTP is the exponential average of the square root of the sum of the squares of past offset differences

     When repeatedly reading the time, the difference may vary almost randomly. The difference of these differences (second derivation) is called jitter.

     Examples:
     0.000002 seconds = 2 microseconds
     0.0000019 seconds = 1.9 microseconds
     0.0000022 seconds = 2.2 microseconds

3. **Frequency Offset Graph**

   - Reports how much time drift our kernel is experiencing, based on the frequency disciplining of NTP.
   - This is the amount of time error our kernel time would have drifted, if NTP was not synced by a reference.
   - Our typical frequency offset appears to be around 13 PPM (about one second per day).

From http://www.ntp.org/ntpfaq/NTP-s-sw-clocks-quality.htm#AEN1230

Unfortunately all the common clock hardware is not very accurate. This is simply because the frequency that makes time increase is never exactly right. Even an error of only 0.001% would make a clock be off by almost one second per day. This is also a reason why discussing clock problems uses very fine measures: One PPM (Part Per Million) is 0.0001% (1E-6).

Real clocks have a frequency error of several PPM quite frequently. Some of the best clocks available still have errors of about 1E-8 PPM (For one of the clocks that is behind the German DCF77 the stability is told to be 1.5 s/day (1.7E-8 PPM). See http://www.ptb.de/english/org/4/43/432/real.htm or http://www.ptb.de/en/org/4/44/441/real_e.htm).

**As most people have some trouble with that abstract PPM (parts per million, 0.0001%), I'll simply state that 12 PPM correspond to one second per day roughly. So 500 PPM means the clock is off by about 43 seconds per day.

Examples

- 12PPM = about one second per day of time drift.
- 69 PPM= about six seconds per day of time drift.
- 500 PPM= about 43 seconds per day of time drift.

NTP Ref ID / Reference ID (.gps, .pps, .init, .drop, .step, etc)

- Refer to sites such as: http://www.eecis.udel.edu/~mills/ntp/html/decode.html#kiss

**.INIT

- Indicates the NTP mode of the reference has not yet been identified. (see additional info further below).
- 494e4954 in hex
- Indicates NTP is trying to reach the reference for the first time, but can't initiate communications with this reference.
- Most likely issue is the default gateway is not configured or not configured correctly , or there is a network issue with port 123.
- To troubleshoot, open a telnet or ssh session and then try pinging this reference. If no response, network issue. If it responds, verify it's a valid NTP server that is known to be up and running.

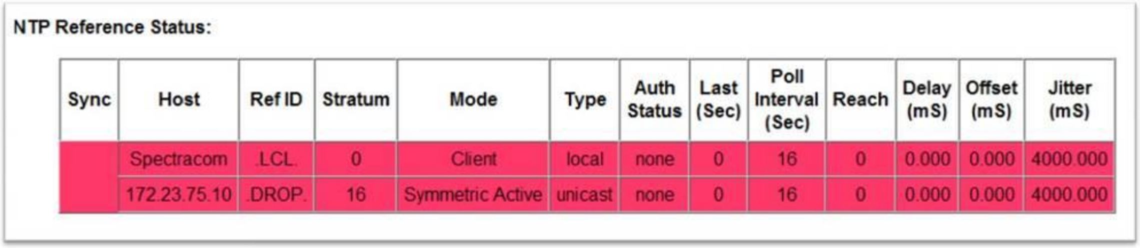
.DROP

The Reference identifier shows the word "**DROP**" in a Peer status. This appears to be due two units being peered, but when NTP starts up, only one of the two is in sync while the other is not in sync. If they both don't start at the same stratum, peering does not seem to work.

If the antenna or other reference is not connected, do not list each other as peers. Instead, list the one that is synced as a NTP server in the "Servers" table of the other unit that is not synced to a reference. Then restart NTP. Example below:

MILFORD (Antenna attached)

JEFFERSON (No Antenna)



NTP Reference Status:

Sync	Host	Ref ID	Stratum	Mode	Type	Auth Status	Last (Sec)	Poll Interval (Sec)	Reach	Delay (mS)	Offset (mS)	Jitter (mS)
	Spectracom	.LCL.	0	Client	local	none	0	16	0	0.000	0.000	4000.000
	172.23.75.10	.DROP.	16	Symmetric Active	unicast	none	0	16	0	0.000	0.000	4000.000

.USER

- “.user” is “55534552” in hex
- System Time has been manually set using the user reference.

.STEP

- A step time change in system time has occurred, but the association has not yet resynchronized.
- Time change of less than the panic threshold of 1000 seconds (16 min 40 sec) occurred.

.DENY

- NTP access was denied by the NTP server

.BCST

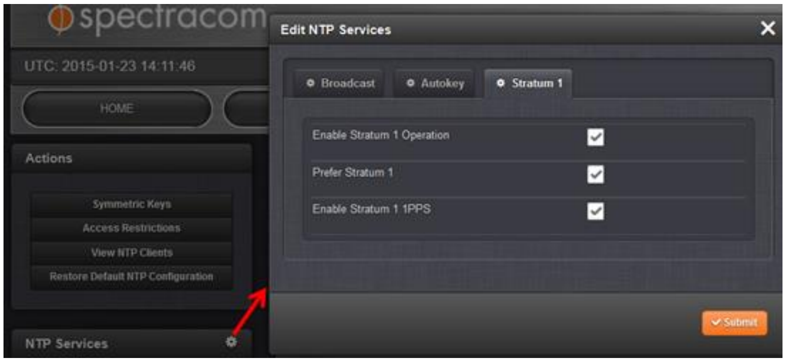
- NTP broadcast time server

**.PPS (atom clock driver/ System PPS)

- Refer to sites such as http://www.eecis.udel.edu/~mills/ntp/html/drivers/driver22.html
- “.PPS” is “50505300” in hex

web browser

Once NTP has synced to GPS inside the SecureSync (and assuming the “**Enable Stratum 1 1PPS**” checkbox is Enabled in the **Management** -> **NTP Setup** page of the browser, **Stratum 1** tab, after pressing the “gear” icon to the right of “NTP Services” as shown below), we enable another NTP input reference that uses the 1PPS generated by the GPS signal. This “PPS” reference helps stabilize/optimize the NTP functionality, if NTP decides to select it as its input. This input is known as NTP’s PPS clock driver and can be selected by NTP shortly after NTP syncs to GPS. If NTP selects it as its reference, NTP changes the Ref ID to “.PPS” to indicate this PPS clock driver had been enabled.



Enable Stratum 1 Operation ☑

Prefer Stratum 1 ☑

Enable Stratum 1 1PPS ☑

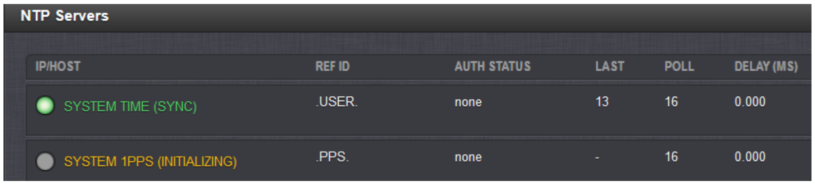
Identifying if NTP has selected the System PPS (atom clock driver)

- Using the ntpq -p command and browser

“NTP Severs” list on the NTP Setup page

System PPS (Atom clock driver) not yet selected by NTP (Ref ID not yet .pps)

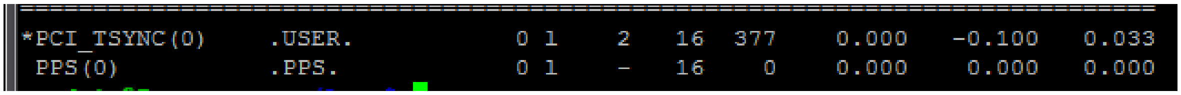
- “System Time” will be in green and “(Sync)”
- “System 1 PPS” will still be in orange and reporting “(Initializing)”



NTP Servers

IP/HOST	REF ID	AUTH STATUS	LAST	POLL	DELAY (MS)
● SYSTEM TIME (SYNC)	.USER.	none	13	16	0.000
● SYSTEM 1PPS (INITIALIZING)	.PPS.	none	-	16	0.000

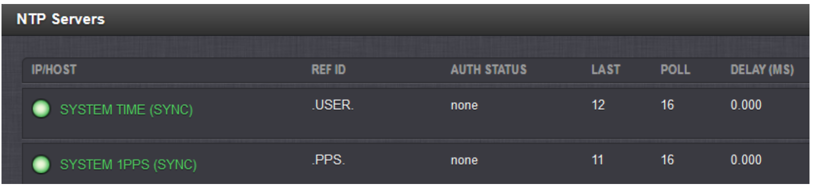
NTPQ –p command will have a “space“ in front of “PPS (0)”



```
==============================================================================
*PCI_TSYNC(0)    .USER.           0 l    2   16  377    0.000   -0.100   0.033
 PPS(0)          .PPS.            0 l    -   16    0    0.000    0.000   0.000
```

System PPS (Atom clock driver) selected by NTP (Ref ID is being as .pps)

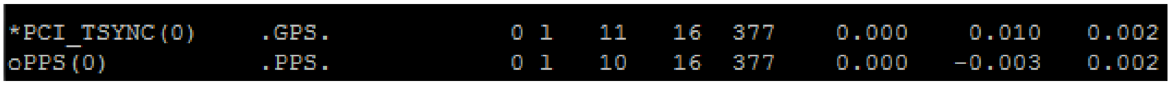
- “System Time (Sync)” will be in green
- “System 1 PPS (Sync)” will be in green



NTP Servers

IP/HOST	REF ID	AUTH STATUS	LAST	POLL	DELAY (MS)
● SYSTEM TIME (SYNC)	.USER.	none	12	16	0.000
● SYSTEM 1PPS (SYNC)	.PPS.	none	11	16	0.000

NTPQ –p command will have a “circle “in front of “PPS (0)”



```
*PCI_TSYNC(0)    .GPS.            0 l   11   16  377    0.000    0.010   0.002
oPPS(0)          .PPS.            0 l   10   16  377    0.000   -0.003   0.002
```

Ntp.log entries for selecting/de-selecting the System PPS

PKI (Public Key Infrastructure/Public Key cryptography) for NTP security

Refer to sites such as http://www.ntp.org/ntpfaq/NTP-s-algo-crypt.htm and the “NTP Security Model” Powerpoint at: https://www.eecis.udel.edu/~mills/database/brief/autokey/autokey.ppt

NTP Security Model

- NTP operates in a mixed, multi-level security environment including symmetric key cryptography, public key cryptography and unsecured.
- NTP timestamps and related data are considered public values and never encrypted.
- Time synchronization is maintained on a master-slave basis where synchronization flows from trusted servers to dependent clients possibly via intermediate servers operating at successively higher stratum levels.
- A client is authentic if it can reliably verify the credentials of at least one server and that server messages have not been modified in transit.
- A client is proventic if by induction each server on at least one path to a trusted server is authentic.

**NTP Symmetric Key Authentication (MD5/SHA1)

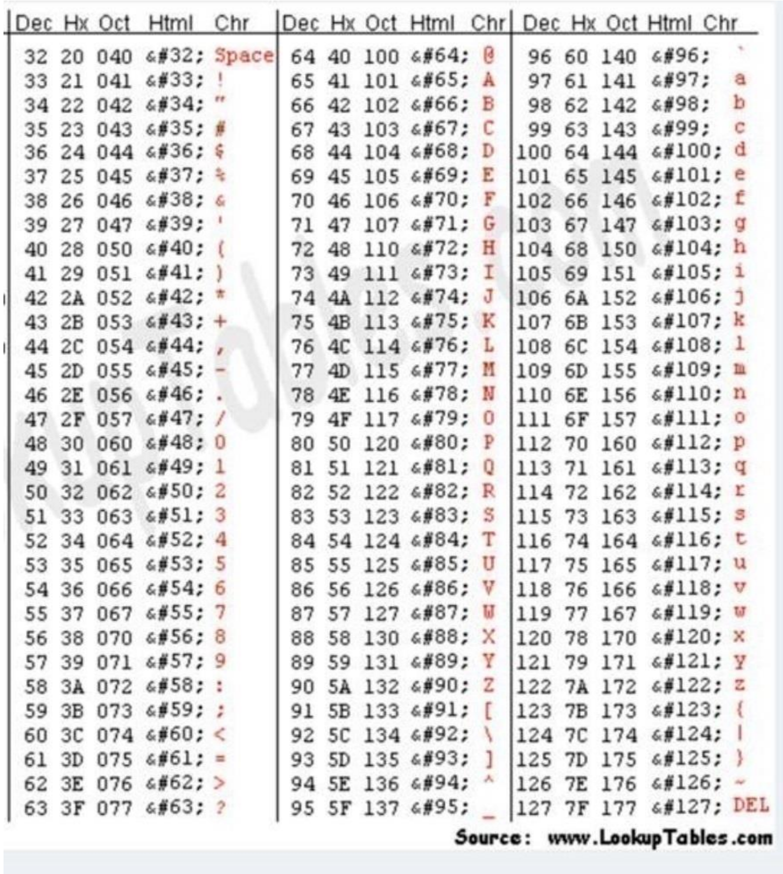
- Refer to: http://doc.ntp.org/4.2.4/authopt.html
- **Symmetric key authentication can't be used in conjunction with NTP Autokey.**

Not able to edit, create or delete symmetric keys while in Expert Mode

- Refer to Mantis case 3041
- Expert mode disables browser NTP functions, so in at least versions 5.2.0 and below, users can't get to the symmetric keys button and associated functions while expert mode is enabled.
- Workaround is to at least temporarily disable Expert mode, create new or edit existing symmetric keys and then re-enable Expert mode. Note that disabling Expert mode causes settings to be lost.

Acceptable characters (for ntp keys)

FYI- the Symmetric key should be able to be any of the following printable characters (21 through 7F, Hex) with the exception of a space and a "#" sign (these two characters are not allowed). They key length can be up to 20 characters long.



Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
32	20	040	&#32;	Space	64	40	100	&#64;	@	96	60	140	&#96;	`
33	21	041	&#33;	!	65	41	101	&#65;	A	97	61	141	&#97;	a
34	22	042	&#34;	"	66	42	102	&#66;	B	98	62	142	&#98;	b
35	23	043	&#35;	#	67	43	103	&#67;	C	99	63	143	&#99;	c
36	24	044	&#36;	$	68	44	104	&#68;	D	100	64	144	&#100;	d
37	25	045	&#37;	%	69	45	105	&#69;	E	101	65	145	&#101;	e
38	26	046	&#38;	&	70	46	106	&#70;	F	102	66	146	&#102;	f
39	27	047	&#39;	'	71	47	107	&#71;	G	103	67	147	&#103;	g
40	28	050	&#40;	(	72	48	110	&#72;	H	104	68	150	&#104;	h
41	29	051	&#41;	)	73	49	111	&#73;	I	105	69	151	&#105;	i
42	2A	052	&#42;	*	74	4A	112	&#74;	J	106	6A	152	&#106;	j
43	2B	053	&#43;	+	75	4B	113	&#75;	K	107	6B	153	&#107;	k
44	2C	054	&#44;	,	76	4C	114	&#76;	L	108	6C	154	&#108;	l
45	2D	055	&#45;	-	77	4D	115	&#77;	M	109	6D	155	&#109;	m
46	2E	056	&#46;	.	78	4E	116	&#78;	N	110	6E	156	&#110;	n
47	2F	057	&#47;	/	79	4F	117	&#79;	O	111	6F	157	&#111;	o
48	30	060	&#48;	0	80	50	120	&#80;	P	112	70	160	&#112;	p
49	31	061	&#49;	1	81	51	121	&#81;	Q	113	71	161	&#113;	q
50	32	062	&#50;	2	82	52	122	&#82;	R	114	72	162	&#114;	r
51	33	063	&#51;	3	83	53	123	&#83;	S	115	73	163	&#115;	s
52	34	064	&#52;	4	84	54	124	&#84;	T	116	74	164	&#116;	t
53	35	065	&#53;	5	85	55	125	&#85;	U	117	75	165	&#117;	u
54	36	066	&#54;	6	86	56	126	&#86;	V	118	76	166	&#118;	v
55	37	067	&#55;	7	87	57	127	&#87;	W	119	77	167	&#119;	w
56	38	070	&#56;	8	88	58	130	&#88;	X	120	78	170	&#120;	x
57	39	071	&#57;	9	89	59	131	&#89;	Y	121	79	171	&#121;	y
58	3A	072	&#58;	:	90	5A	132	&#90;	Z	122	7A	172	&#122;	z
59	3B	073	&#59;	;	91	5B	133	&#91;	[	123	7B	173	&#123;	{
60	3C	074	&#60;	<	92	5C	134	&#92;	\	124	7C	174	&#124;	|
61	3D	075	&#61;	=	93	5D	135	&#93;	]	125	7D	175	&#125;	}
62	3E	076	&#62;	>	94	5E	136	&#94;	^	126	7E	176	&#126;	~
63	3F	077	&#63;	?	95	5F	137	&#95;	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

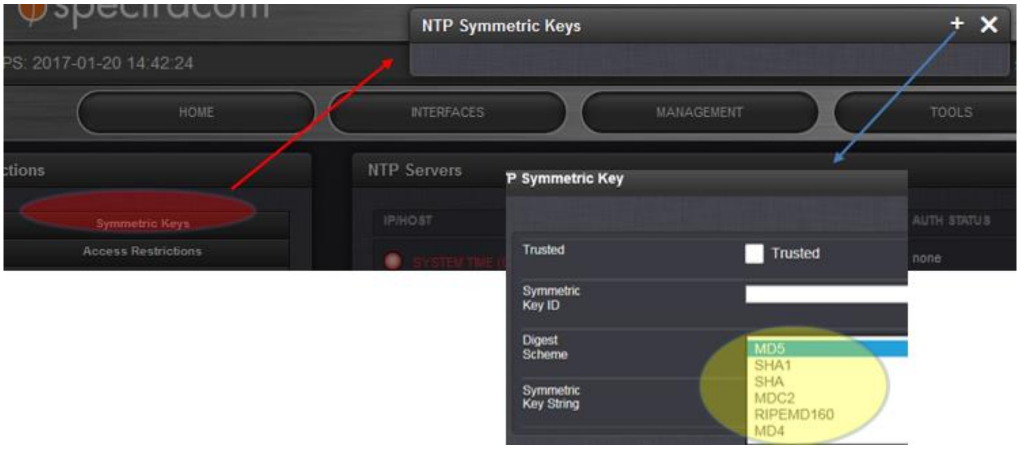
Message Digest Schemes, such as MD5, and SHA (for NTP authentication)

SHA 1 instead of MD5 authentication

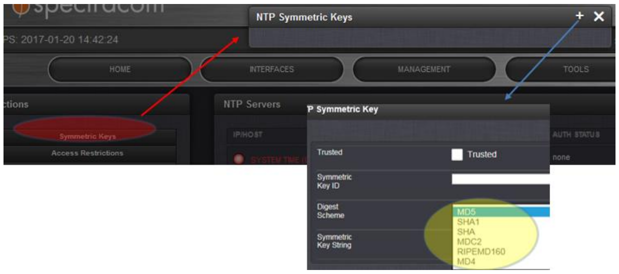
Available Message Digests in at least version 5.4.5 and above

(**Note**: Not sure in what software version the others besides MD5 were added. I couldn't find it in the Release Notes. Believe it was after v5.12 and it was before version v5.4.5).

- This configuration is not available in the classic interface browser (have to use the newewr black/charcoal browser)
- Selected in the Management -> NTP setup page of the newer browser:
  - Click on the "**Symmetric Keys**" button on the left side of the page. Then press the "+" sign in the upper-right corner of the pop-up window that opens:



Email Keith sent (20 Jan 17) The Spectracom SecureSync provides the ability to either select either MD5 or a different Message Digest schemes for NTP authentication. The below screenshot shows the available schemes (in addition to MD5) that can be configured in the **Management** -> **NTP Setup** page of the SecureSync's web browser (click on the "**Symmetric Keys**" button on the left side of the page. Then press the "+" sign in the upper-right corner of the pop-up window that opens):



2400 SecureSync Issue (at least 1.6.0): NTP "Symmetric Key String" field is limiting total characters to 16, instead of 20

- Refer to Salesforce Cases 293006 and 293838
- Refer to JIRA CAR-2288 (created Feb 2023)
- Reported by GE in Case 293838, this condition started in update v1.6.0 (but this hasn't been confirmed here, as of yet)

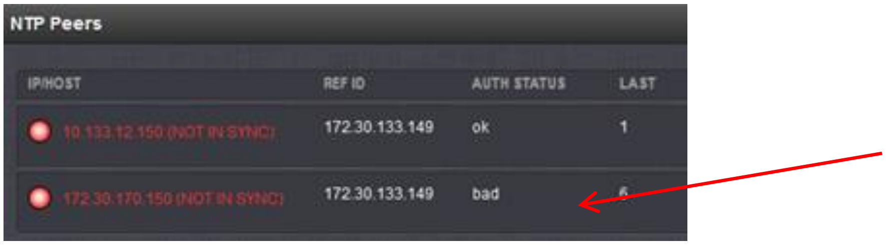
“Auth Status”

Changing a Symmetric key after NTP has started-up.

- NTP caches the symmetric keys when NTP starts-up. So, if the key changes while NTP is running, the change isn’t incorporated until NTP is restarted.
- The “Auth Status” will continue to report “ok” for authentication. But auth will fail in any other units polling this one, because NTP continues to authenticate each received packet. (NTP in other time servers will lose sync with that time server, if the key changes).

Troubleshooting/ known issues with Symmetric key Authentication

A) NTP Authentication failures (“bad” or “none” instead of “ok”)



NTP Peers

IP/HOST	REF ID	AUTH STATUS	LAST
● 10.133.12.150 (NOT IN SYNC)	172.30.133.149	ok	1
● 172.30.170.150 (NOT IN SYNC)	172.30.133.149	bad	6

“Auth Status”

Note: “Auth Status” is only updated when NTP first starts-up.

- “**none**”: Indicates authentication is not being used (no key has been specified in the specified peer/server in **Management** -> **NTP Setup** page
- “**bad**”: Indicates authentication is being used, but the authentication failed when NTP last started-up
- Either no key ID or the wrong key ID may have been specified in the specified peer/server in Management -> NTP Setup page of one or more units.
- The selected key may not have been selected as “**trusted**” in the “Symmetric Keys” table
- The selected key in the “Symmetric Keys” table may not match the same key in the other’s ntp.keys table.

Troubleshooting auth failures

- With the original web browser design (versions prior to 5.1.0) do not use characters such as a “$” (dollar sign). MD5 won’t work. (See note further below)

1. Get the logs and especially the config files from both units.
2. View the **ntp.conf** file from both units:

A) Make sure the selected key is trusted on both units (as specified next to “trustedkey”)

Example: trustedkey 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 65533 65534

1) Make sure a key for each other (peers or servers) is selected and it’s the same number specified on both units.

Specific example below of where the customer only specified a key on one but not the other (notice the second red line does not contain the word “key” so the key hadn’t been specified in the Management->NTP Setup page. I had verified from both configs that both are supposed to be using key 2

mantp
trustedkey 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 65533 65534

peer 10.133.12.150 key 2 minpoll 3 maxpoll 3
peer 172.30.170.150 *key 2* minpoll 3 maxpoll 3   (auth was reported as “bad”)
server 172.18.33.191 *key 2* minpoll 3 maxpoll 3
server 172.22.115.45 ***key 2*** minpoll 3 maxpoll 3
server 10.153.36.191 ***key 2*** minpoll 3 maxpoll 3
server 172.30.133.149 ***key 2*** minpoll 3 maxpoll 3
keysdir /etc/ntp/keys/

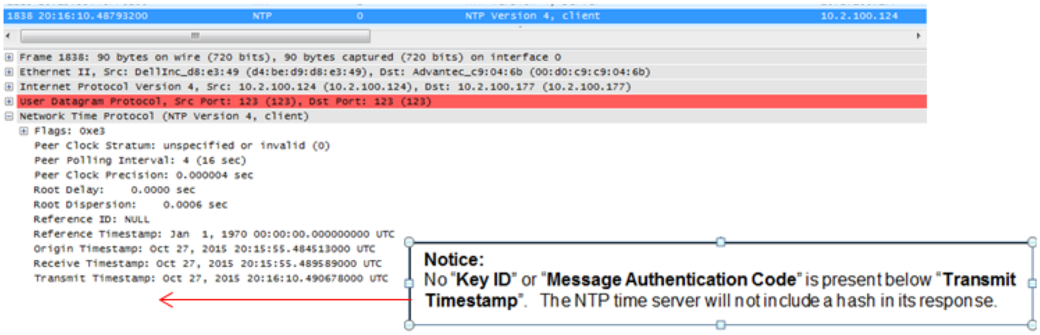
sdcntp201
trustedkey 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 65533 65534
peer 10.133.12.150 ***key 2*** minpoll 3 maxpoll 3
server 172.18.33.191 **key 2** minpoll 3 maxpoll 3
server 172.22.115.45 ***key 2*** minpoll 3 maxpoll 3
server 10.153.36.191 ***key 2*** minpoll 3 maxpoll 3
server 172.30.133.149 ***key 2*** minpoll 3 maxpoll 3
peer 10.133.10.150 minpoll 3 maxpoll 3 (auth was reported as “**none**”)   (notice the phrase “key 2” is missing from this line)

2) View the **ntp.keys** file in both config files to make sure the specified key matches verbatim the key of the other unit,

Wireshark captures of NTP authentication.

Note: In the following captures, 10.2.100.177 is the NTP server and 10.2.100.124 is the Client (using PresenTense Client software)

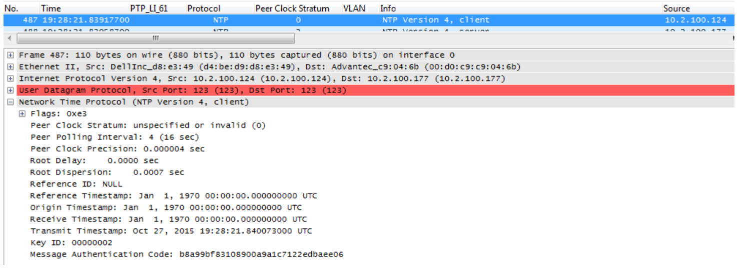
1) NTP client not sending MD5 hash in its NTP request to NTP server (Client didn’t send a hash)



```
1838 20:16:10.48793200          NTP          0          NTP Version 4, client          10.2.100.124

⊞ Frame 1838: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
⊞ Ethernet II, Src: DellInc_d8:e3:49 (d4:be:d9:d8:e3:49), Dst: Advantec_c9:04:6b (00:d0:c9:c9:04:6b)
⊞ Internet Protocol Version 4, Src: 10.2.100.124 (10.2.100.124), Dst: 10.2.100.177 (10.2.100.177)
⊞ User Datagram Protocol, Src Port: 123 (123), Dst Port: 123 (123)
⊟ Network Time Protocol (NTP Version 4, client)
  ⊞ Flags: 0xe3
    Peer Clock Stratum: unspecified or invalid (0)
    Peer Polling Interval: 4 (16 sec)
    Peer Clock Precision: 0.000004 sec
    Root Delay:     0.0000 sec
    Root Dispersion:     0.0006 sec
    Reference ID: NULL
    Reference Timestamp: Jan  1, 1970 00:00:00.000000000 UTC
    Origin Timestamp: Oct 27, 2015 20:15:55.484513000 UTC
    Receive Timestamp: Oct 27, 2015 20:15:55.489589000 UTC
    Transmit Timestamp: Oct 27, 2015 20:16:10.490678000 UTC
```

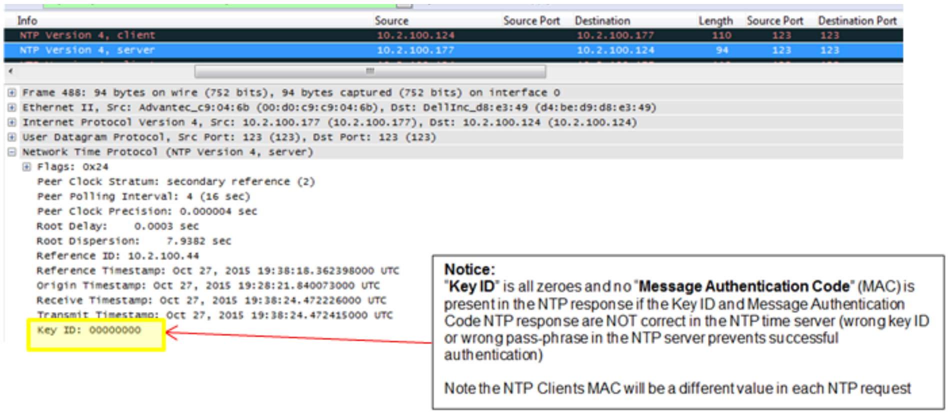
Notice:
No "**Key ID**" or "**Message Authentication Code**" is present below "**Transmit Timestamp**". The NTP time server will not include a hash in its response.

2) NTP client to NTP server sending key ID 2.



```
No.   Time                PTP_LI_61   Protocol   Peer Clock Stratum   VLAN   Info                       Source
  487 19:28:21.83917700               NTP        0                           NTP Version 4, client      10.2.100.124

⊞ Frame 487: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
⊞ Ethernet II, Src: DellInc_d8:e3:49 (d4:be:d9:d8:e3:49), Dst: Advantec_c9:04:6b (00:d0:c9:c9:04:6b)
⊞ Internet Protocol Version 4, Src: 10.2.100.124 (10.2.100.124), Dst: 10.2.100.177 (10.2.100.177)
⊞ User Datagram Protocol, Src Port: 123 (123), Dst Port: 123 (123)
⊟ Network Time Protocol (NTP Version 4, client)
  ⊞ Flags: 0xe3
    Peer Clock Stratum: unspecified or invalid (0)
    Peer Polling Interval: 4 (16 sec)
    Peer Clock Precision: 0.000004 sec
    Root Delay:     0.0000 sec
    Root Dispersion:     0.0007 sec
    Reference ID: NULL
    Reference Timestamp: Jan  1, 1970 00:00:00.000000000 UTC
    Origin Timestamp: Jan  1, 1970 00:00:00.000000000 UTC
    Receive Timestamp: Jan  1, 1970 00:00:00.000000000 UTC
    Transmit Timestamp: Oct 27, 2015 19:28:21.840073000 UTC
    Key ID: 00000002
    Message Authentication Code: b8a99bf83108900a9a1c7122edbaee06
```

3) NTP server not able to authenticate (Key ID: 000000)



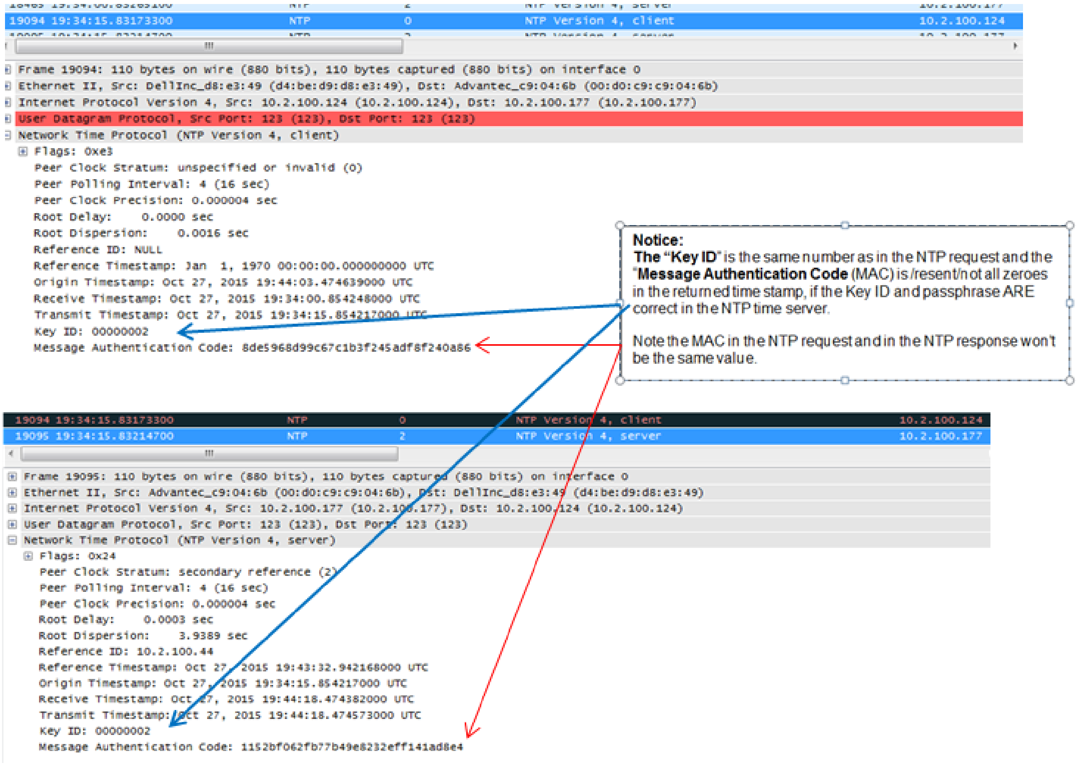
```
Info                          Source          Source Port  Destination     Length  Source Port  Destination Port
NTP Version 4, client         10.2.100.124                 10.2.100.177    110     123          123
NTP Version 4, server         10.2.100.177                 10.2.100.124    94      123          123

⊞ Frame 488: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
⊞ Ethernet II, Src: Advantec_c9:04:6b (00:d0:c9:c9:04:6b), Dst: DellInc_d8:e3:49 (d4:be:d9:d8:e3:49)
⊞ Internet Protocol Version 4, Src: 10.2.100.177 (10.2.100.177), Dst: 10.2.100.124 (10.2.100.124)
⊞ User Datagram Protocol, Src Port: 123 (123), Dst Port: 123 (123)
⊟ Network Time Protocol (NTP Version 4, server)
  ⊞ Flags: 0x24
    Peer Clock Stratum: secondary reference (2)
    Peer Polling Interval: 4 (16 sec)
    Peer Clock Precision: 0.000004 sec
    Root Delay:    0.0003 sec
    Root Dispersion:    7.9382 sec
    Reference ID: 10.2.100.44
    Reference Timestamp: Oct 27, 2015 19:38:18.362398000 UTC
    Origin Timestamp: Oct 27, 2015 19:28:21.840073000 UTC
    Receive Timestamp: Oct 27, 2015 19:38:24.472226000 UTC
    Transmit Timestamp: Oct 27, 2015 19:38:24.472415000 UTC
    Key ID: 00000000
```

Notice:
"**Key ID**" is all zeroes and no "**Message Authentication Code**" (MAC) is present in the NTP response if the Key ID and Message Authentication Code NTP response are NOT correct in the NTP time server (wrong key ID or wrong pass-phrase in the NTP server prevents successful authentication)

Note the NTP Clients MAC will be a different value in each NTP request

C. NTP client to NTP server sending key ID 2

NTP server successfully authenticated NTP client



```
19094 19:34:15.83173300    NTP    0    NTP Version 4, client    10.2.100.124

⊞ Frame 19094: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
⊞ Ethernet II, Src: DellInc_d8:e3:49 (d4:be:d9:d8:e3:49), Dst: Advantec_c9:04:6b (00:d0:c9:c9:04:6b)
⊞ Internet Protocol Version 4, Src: 10.2.100.124 (10.2.100.124), Dst: 10.2.100.177 (10.2.100.177)
⊞ User Datagram Protocol, Src Port: 123 (123), Dst Port: 123 (123)
⊟ Network Time Protocol (NTP Version 4, client)
  ⊞ Flags: 0xe3
    Peer Clock Stratum: unspecified or invalid (0)
    Peer Polling Interval: 4 (16 sec)
    Peer Clock Precision: 0.000004 sec
    Root Delay:    0.0000 sec
    Root Dispersion:    0.0016 sec
    Reference ID: NULL
    Reference Timestamp: Jan  1, 1970 00:00:00.000000000 UTC
    Origin Timestamp: Oct 27, 2015 19:44:03.474639000 UTC
    Receive Timestamp: Oct 27, 2015 19:34:00.854248000 UTC
    Transmit Timestamp: Oct 27, 2015 19:34:15.854217000 UTC
    Key ID: 00000002
    Message Authentication Code: 8de5968d99c67c1b3f245adf8f240a86
```

Notice:
The "Key ID" is the same number as in the NTP request and the "**Message Authentication Code** (MAC) is /resent/not all zeroes in the returned time stamp, if the Key ID and passphrase ARE correct in the NTP time server.

Note the MAC in the NTP request and in the NTP response won't be the same value.

```
19094 19:34:15.83173300    NTP    0    NTP Version 4, client    10.2.100.124
19095 19:34:15.83214700    NTP    2    NTP Version 4, server    10.2.100.177

⊞ Frame 19095: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
⊞ Ethernet II, Src: Advantec_c9:04:6b (00:d0:c9:c9:04:6b), Dst: DellInc_d8:e3:49 (d4:be:d9:d8:e3:49)
⊞ Internet Protocol Version 4, Src: 10.2.100.177 (10.2.100.177), Dst: 10.2.100.124 (10.2.100.124)
⊞ User Datagram Protocol, Src Port: 123 (123), Dst Port: 123 (123)
⊟ Network Time Protocol (NTP Version 4, server)
  ⊞ Flags: 0x24
    Peer Clock Stratum: secondary reference (2)
    Peer Polling Interval: 4 (16 sec)
    Peer Clock Precision: 0.000004 sec
    Root Delay:    0.0003 sec
    Root Dispersion:    3.9389 sec
    Reference ID: 10.2.100.44
    Reference Timestamp: Oct 27, 2015 19:43:32.942168000 UTC
    Origin Timestamp: Oct 27, 2015 19:34:15.854217000 UTC
    Receive Timestamp: Oct 27, 2015 19:44:18.474382000 UTC
    Transmit Timestamp: Oct 27, 2015 19:44:18.474573000 UTC
    Key ID: 00000002
    Message Authentication Code: 1152bf062fb77b49e8232eff141ad8e4
```

**NTP Autokey

- Refer to: http://doc.ntp.org/4.2.4/authopt.html
- Refer to (WP-033): S:\Engineering\Projects\Lafayette\200 Engineering Documents\Working Papers
- Consists of both authentication and encryption
- Can't **be used in conjunction with symmetric key authentication**

NTP autokey Tech Note (in progress) I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\MD5 and Autokey Ap Note

Autokey stopped being supported in newer versions of NTP (4.2.8p3 through 4.2.8p7)

- As of NTP v4.2.8p3 (update version 5.3.0 Sept 2015) NTP stopped supporting autokey

Update: NTP fixed Autokey in **version 5.4.5** (NTP v4.2.8p8) (this wasn't mentioned in the 5.4.5 Release Notes, but I confirmed this with Ron, Joe and Dave S on 28 Sept 16)

Example report from a version 5.4.1 customer:

"I'm having an issue enabling/configuring autokey for one of our SecureSync units. I've got it going on the other devices we have but for some reason I can't seem to get it configured properly on one of the units. I disabled NTP, went into the NTP config, checked the "enable" box, entered an appropriate passphrase, selected "trusted" for the certificate and clicked submit. At that point I go back into the configuration to get the GroupKey but it's always blank. When I try re-enabling NTP I get a "bad decrypt" error message (see below). I've tried rebooting the unit as well as re-applying the version 5.4.1 software. I've tried restoring the default NTP configuration as well but can't seem to get it to generate a GroupKey for the autokey. I'm at a loss for how to proceed. I've got this configured on three other devices, so I'm out of ideas at this point. I'd greatly appreciate any help."

- For more info on this condition, refer to NTP bug report http://bugs.ntp.org/show_bug.cgi?id=3005
- Version 5.3.0 update includes configs for autokey (we haven't removed them yet). But there are issues trying to use autokey starting with this version.
- As of Sept 2015, there is talk of autokey being replaced by something else, but no details available at this time
- See Ron Dries for questions about this.
- fixed in the version 5.4.5 software update. **Per email from Dave Sohn (29 Jul 16)** "Autokey in 5.4.1 is still not completely functional due to an issue within ntp itself. We just successfully tested autokey in ntp 4.2.8p8, which will be released with 5.4.5.

Support for IPv6 Autokey: Apparently, IPv6 Autokey is supported in the new version of NTP (4.2.6p5). If this is correct, since SecureSyncs with version 5.0.0 or higher have NTP v4.2.6p5, they should be compatible with IPv6. Refer to the link above for additional info on Autokey in this document.

**Need to restart NTP after changing the 1204-06 Gigabit card configs

- NTP needs to be restarted (or the unit rebooted), if the Gigabit Option Card (if installed) network port settings are changed. Otherwise, no NTP output on the ports.
- We aren't sure why this is. NTP must have some memory for storing this port info.

**NTP Log entries

- Refer to: NTP log entries

****NTP's "LOCAL (0)" reference 127.127.1.0 (to allow NTP to go to stratum 16 when no inputs available) (aka "NTP Local Clock" reference)**

- 127.127.1.0 is the NTP Local Clock driver/reference used to cause NTP to go to Stratum 16 when the time server goes out of sync (exits holdover). This entry indicates NTP went to Stratum 16

4. In SecureSync NTP Expert mode:

```
server 127.127.1.0 minpoll 4
fudge 127.127.1.0 stratum 15
```

In NTP log (when synced to Local Clock Reference): ntpd[826]: synchronized to LOCAL(0), stratum=15

- When Local Clock Reference is enabled, allows NTP to be able to go to Stratum 16
- This reference is selected if no other inputs to NTP are available.

NTP Local Clock Reference is now a dynamic reference that is only momentarily made available, as the SecureSync is going out of sync. Then the reference is removed, so that it can only be selected when SecureSync goes out of sync.

the Local clock reference is only periodically selected as the reference to NTP as the method to go to Stratum 16. The Local clock reference will no longer be displayed in the Status -> NTP page of the browser and the field to disable Local reference is no longer in the Network -> NTP setup page, NTP Servers tab.
127.127.1.0 is momentarily added to the NTP Reference table each time SecureSync exits Sync state. Then once NTP is Stratum 16, it's removed from the table. If a user happens to be viewing the NTP Status page when time sync is lost, and the page refreshes as the right moment, they may see 127.127.1.0 listed in the table. But shortly thereafter, they won't see it again, unless sync is regained and lost again.

The reason this was changed is because jittery inputs could result in NTP switching back and forth between our driver and the local driver. NTP would alternate between Stratum 1 and Stratum 16, even with the input always present. According to Paul, this newer method still lists the Local clock reference and fudge in the ntp.conf file (as was also done in the earlier versions of software). However, now NTP only periodically syncs to the local clock driver (instead of continuously) if System Time is not valid and no peers are available for sync.

Detailed info on this function. From Paul Myers (18 Dec 2013)

```
////////////////////////////////////////////////////////////////////////////////
// Function Name: DT_FudgeNTP
// Description:   This function uses NTPDC to use fudge to enable or disable
//                a Local Reference Clock Driver to set the NTP Stratum to 15
//                in the event NTP is not synchronized by the KTS with a
//                reference or by a higher NTP Stratum server. The user
//                can explicitely set a Local Reference Clock which disables
//                this feature or explicitely disable it by putting a comment
//                string in /etc/ntp/ntp.conf with the text
//                # DISABLE_AUTO_LOCAL.
//
//                The state machine for this system is shown below:
//
//               .---------------------Restart NTP------------------.
//          |                                   |
//          V                                   |
//     .-----------. Restart NTP.-----------.  NTP Sync  .-----------.
//     |           |<-----------| NTP Sync  |<---------- | NTP Out of|
//     | NTP start |            | Local Ref |----------->| Sync Local|
//     | or restart|----------->| Clock off |  NTP Out   | Ref ON    |
//     `-----------'  NTP Sync  `-----------'  of Sync   `-----------'
//
//          The NTP Sync state disabled the Local Reference Clock
//          if the user has NOT configured a Local Reference Clock
//          line in ntp.conf or has not inhibited the feature of
//          automatically enabling and fudging a local referenc clock
//          when none is present in the ntp.conf file.
//
//          If NTP goes out of sync, and NO local reference is defined and
//          this feature is NOT inhibited, a Local Reference driver
//          of stratum 15 is fudged.  If NTP enters sync the Local
//          Reference Clock driver is unconfigured.
//
// Parameters:
//    In:      None
//    In/Out:  None
//    Out:     None
//    Returns: BOOL - Returns TRUE if fudging NTP
//
////////////////////////////////////////////////////////////////////////////////
```

If desired, this function can be turned off using NTP Expert mode. More info on this from Paul Myers below.

To Disable Local Clock Reference in 5.0.0 and higher modify Expert mode file

Add line (to ntp.conf file):

```
# DISABLE_AUTO_LOCAL
```

OR

```
# 127.127.1.0
```

Or actually add the local clock reference and fudge line

```
Server 127.127.1.0
Fudge 127.127.1.0
```

NTP log entry (versions 5.0.0 and above) asserted each time the Local Clock Reference is selected

```
ntpd[26487]: 127.127.1.0 interface 127.0.0.1 -> (none)
```

Note: the five digit number in brackets will vary.

Causes of this NTP log entry being asserted

1) System Time no longer valid and no NTP peers have been configured.
2) System Time no longer valid and no configured NTP peers are available.
3) More than 3 or 4 NTP peers have been added and they are ganging up on the preferred System Time reference.

Note: This can cause NTP to disqualify all of its references, especially if the peers have high offsets from each other. If this happens, the NTP Status page may show that all references have an "x" to indicate they are not available for NTP to sync with.

**Automatic FTP of NTP Statistics

- This capability was available in the 9300s/9200s as part of the "Cachaça" project for South America.
- Not available in SecureSyncs

Q. Does the SecureSync have the option of send "Automatic FTP of Statistics", equal to 9300 series (every 30 minutes).

A (as of 28 Aug 2013 per Keith) No. This capability was not brought forward into the newer SecureSyncs.

For your information, the NTP Statistics data is still available from the SecureSync and Model 9400s. It just not automatically sent out via FTP in the newer Models. Though it's not automatically sent out, it can still be easily retrieved via a single file of bundled logs.

The NTP statistics files that are sent out in the Model 9300s are the NTP Clockstats, Peerstats and Loopstats files. These files can be easily bundled into a single file, along with the other logs and then manually extracted whenever desired, using a manual FTP connection. The instructions below to do this are specific to SecureSync, but are very similar for NetClock 9400s as well.

In order to capture the log files, simply copy/paste all of the log entries (from all of the log tabs) in the SecureSync's **Tools** -> **Logs** page of its web browser (such as all of the log entries in the "Event" tab, "Alarms" tab, "Oscillator" tab, etc). Paste all of the log entries into a single Microsoft Word document and then send us this document for our review.

Instead of copy/pasting all of the logs to a Word document, you can also bundle the logs into a single log file. Then export this bundle file from the SecureSync using an FTP or SCP session. Then, simply attach this extracted file to a reply email. Below is additional information on how to bundle and extract all of the unit's logs:

Attached you will find an example log save file. In this Text document, you will find the Clockstats, loopstats and peerstats logs (just like with the Model 9300s). Just search this file for all three of these words**.**

**NTP unicast / manycast / broadcast/ Multicast / NTP over Anycast

NTP manycast mode

- Refer to sites such as: http://doc.ntp.org/4.2.0/manyopt.html
- As of at least software version 5.2.1 (as of at least July 2015) NTP manycast mode is not supported via the web browser (but I suspect it's available via the NTP Expert Mode). Note there are not yet any tech notes available for this mode.
- We support NTP unicast, NTP broadcast, NTP multicast and NTP over Anycast modes only

What is NTP manycast (From **http://www.ntp.org/ntpfaq/NTP-s-config-adv.htm**)
This is an explanation by Professor David L. Mills: "Manycast only works in multicast mode. It uses an expanding-ring search by adjusting the TTL field. This doesn't make sense in broadcast mode, since broadcast packets do not span subnets. It might in fact be useful to implement manycast in broadcast mode without the search, but that is rather far down the to-do list." (...) "Only the * and + tattletales indicate a candidate survivor. Note that one of your servers is in process of going away, another coming onboard. This is a normal situation when first coming up and when the signatures are refreshed once per day. I assume you are using autokey; if not, no promises at all."
So basically it's a mechanism to automatically configure servers on a nearby network. Compared to broadcasting and multicasting, manycasting uses the normal server keyword, but with a multicast group address (class D) on the client. Manycast servers use the keyword manycastserver. As for broadcasts and multicasts, manycast associations on the client may come and go over time.

NTP broadcast and NTP multicast

For broadcast and multicast troubleshooting/addition info, refer to: NTP Broadcast/Multicast modes

- ➢ NTP broadcast can be enabled without stopping/restarting NTP (starts broadcasting after being enabled)
- ➢ MD5 key needs to be defined, if the NTP client requires MD5 authentication.
- ➢ NTP Broadcast can be configured to go out all Ethernet ports if the Gigabit Card 1204-06 is installed (NOTE: Need to use NTP Expert Mode. Refer to the NTP expert mode tech note: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert Mode- Broadcast and Multicast
- ➢ NTP Multicast (224.0.1.1) only goes out one Ethernet port (the first network it sees as valid, such as Eth0 for instance (if its desired to multicast to more than on network, this has to be handled outside of the SecureSync).

Note: If the NTP client can configure which multicast address it monitors, the static routes in the main default gateway page can be configured for one multicast address to be sent out one specific network interface, while another multicast address can be sent out a different interface. We can multicast any IP address, so we can multicast 224.0.1.1 (the address reserved for NTP) on one interface (such as Eth1) and 224.0.0.1 (as an example) on a different interface (such as Eth2).

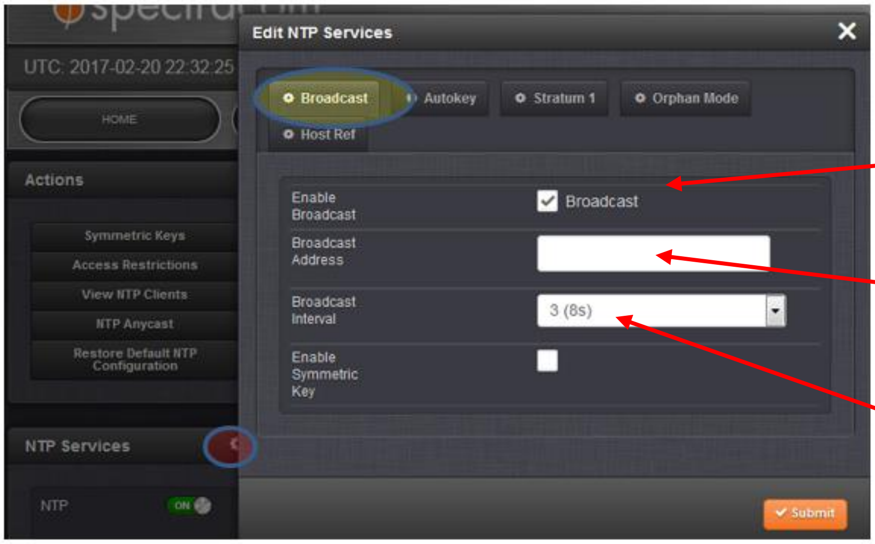
A) NTP Broadcast Mode

Ability to configure the NTP Broadcast address

- ➢ Upgrade version 5.1.5 provides the ability for a user to configure the NTP broadcast address.
- ➢ The NTP broadcast address was statically set to the factory broadcast address in previous versions.

Management -> NTP Setup page of the newer browser

- ➢ Click on the gear icon next to “NTP Services”
- ➢ Click on the Broadcast tab



Enable Broadcast ☑ Broadcast

Broadcast Address

Broadcast Interval 3 (8s)

Enable Symmetric Key □

Select this checkbox to enable Broadcast mode

Broadcast address for the particular network

Broadcast interval/rate to send NTP packets to the network’s broadcast address

Email Keith sent (20 Feb 17) The SecureSync’s Broadcast configuration provides the ability to configure the desired broadcast interval/rate. This is the rate at which NTP packets are sent to the broadcast address, with this rate determined by the requirements of the NTP clients requiring NT broadcast time stamps. the broadcast address that the packets are sent to is also configurable in this web page.

Both the network’s broadcast address that the NTP clients are listening to for the NTP packets and the interval/rate which the packets are to be sent to this address have to be configured in the SecureSync which is broadcasting the NTP packets, in order for broadcast packets to be sent out of the SecureSync.

Note the value in parenthesis for each of the broadcast interval drop-down values is the actual interval for the packets to be sent. In the example screenshot above, the interval value of “**3(8s)”** indicates the NTP packets will be automatically sent to the defined broadcast address every 8 seconds. This is the fastest rate available, with the other available values sending the packets less often.

Broadcastdelay (broadcast delay) value

Sets the typical propagation delay from this NTP server to the NTP clients receiving the NTP broadcast packets when broadcasting NTP (unlike when using unicast mode, the NTP clients can’t calculate this propagation delay when using broadcast mode. So the NTP server can be configured to include/report this value in its broadcast packets).

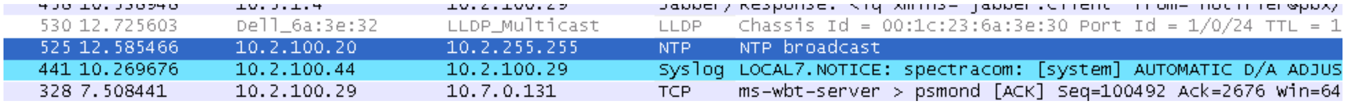
> “To compensate for any server-to-client packetlatency, you can specify an NTP broadcast delay (a time adjustment factor for the receiving of broadcastpackets by the switch)”

- This is a configuration associated with NTP broadcast mode, which is not currently available in the broadcast window of the newer web browser.
- Applicable to at least update versions 5.5.1 and below.
- Per Ron (21 Feb 17), He found NTP’s default value is -50 milliseconds.
- This config value can be changed from -50ms by adding a line to the ntp.conf file via the NTP Expert mode (note that Expert mode must remain enabled, or this value will be removed from the ntp.conf file).

Example ntp.conf file for adding broadcastdelay.

```
Server        127.127.1.0     # local clock
fudge         127.127.1.0 stratum 10
driftfile     /var/lib/ntp/drift
broadcastdelay  0.008
keys          /etc/ntp/keys
```

Packet capture of NTP broadcast packet



```
530 12.725603   Dell_6a:3e:32   LLDP_Multicast   LLDP    Chassis Id = 00:1c:23:6a:3e:30 Port Id = 1/0/24 TTL = 1
525 12.585466   10.2.100.20     10.2.255.255     NTP     NTP broadcast
441 10.269676   10.2.100.44     10.2.100.29      Syslog  LOCAL7.NOTICE: spectracom: [system] AUTOMATIC D/A ADJUS
328 7.508441    10.2.100.29     10.7.0.131       TCP     ms-wbt-server > psmond [ACK] Seq=100492 Ack=2676 Win=64
```

Email Keith sent to John Jenkins To begin, configuring the SecureSync for NTP broadcast mode is extremely easy. In fact, you don’t even need to stop and restart NTP in the process for it to start (many other NTP config changes require it to be restarted before the change takes effect).

To enable NTP broadcast mode, simply navigate to the **Network** -> **NTP setup** page of the browser, NTP Broadcasting tab. As shown below, change the “Broadcast Service” field to enabled and change the “Interval” drop-down to the desired broadcast interval (as indicated inside the parenthesis). Then hit Submit.

Note the “KEY ID” field should remain blank, unless the Harris equipment requires an MD5 authentication hash be sent with ach NTP time stamp, in order for it to accept the time stamp. If MD5 is required (as it with many Cisco devices), let Dave or I know and we can tell you more about this particular configuration.

After hitting Submit, the NTP packets will start to be transmitted at the interval specified. No other steps are required for them to go out. I just confirmed this with a wireshark capture, shown below. Wireshark capture is the best way to prove the time stamps are occurring.   The packet(s) should indicate “NTP broadcast” originating from the IP address of the NTP server and going out to the broadcast address for the network.
Are there any switches or routers in between the NTP server and the Harris equipment? As this is broadcast traffic, switches/routers may or may not pass broadcast traffic.

Lastly, most if not all NTP clients will ignore the SecureSync’s NTP packets if the SecureSync is not synced to either an external reference or to itself. To verify the SecureSync's NTP packets are useable, navigate to the **Status** -> **NTP** page of the browser. In the top row of this page is the current NTP Status. If the stratum value is a value such as 1 or 2, the NTP packets are useable. But if It indicates NTP is Stratum 16, the SecureSync is not in sync and the packets will likely be ignore by any NTP client. below is an example of NTP at Stratum 2. Its NTP packets are useable.

NTP broadcast on all four network ports (more than one isolated subnet)

- Scott will Larcan desired to broadcast NTP to all four subnets. Refer to Salesforce case 9886.
- Requires the use of NTP Expert mode (to add multiple NTP "Broadcast" lines to the ntp.conf file
- Refer to the NTP Broadcast Tech Note: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert Mode- Broadcast to more than one port

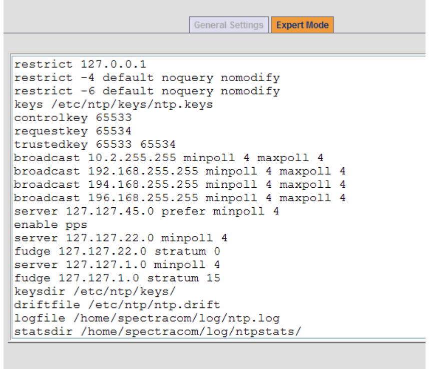
Email I sent to Scott (17 May 2013)

Regarding the Spectracom SecureSync's NTP broadcast functionality; I have some information for you. I apologize for the delay in getting back to you (there are never enough hours in a day ☹)!!!

I started trying to log in to your SecureSync, but I was doing something wrong that prevented me from getting in. Before I could contact you about it, I got pulled off in a few other directions.

This morning, instead of looking at your SecureSync, I decided to test NTP broadcast on all isolated ports using one of our SecureSyncs here at the factory. This test went VERY well.   I was able to confirm NTP is able to broadcast on every one of the four network ports, with each network port configured to be on different, isolated subnets.

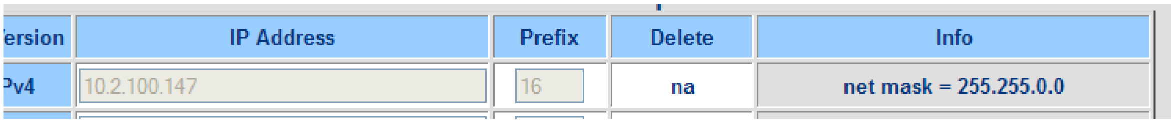
I first did the same thing that you said you did- I enabled NTP Broadcast mode (every 16 seconds to speed up the test results) and then also NTP expert mode. In the ntp.conf table, I copy/pasted the "broadcast" line three times and edited each of the pasted lines to broadcast on three additional isolated subnets. Below is a copy of the edited ntp.conf file:



```
restrict 127.0.0.1
restrict -4 default noquery nomodify
restrict -6 default noquery nomodify
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
broadcast 10.2.255.255 minpoll 4 maxpoll 4
broadcast 192.168.255.255 minpoll 4 maxpoll 4
broadcast 194.168.255.255 minpoll 4 maxpoll 4
broadcast 196.168.255.255 minpoll 4 maxpoll 4
server 127.127.45.0 prefer minpoll 4
enable pps
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
server 127.127.1.0 minpoll 4
fudge 127.127.1.0 stratum 15
keysdir /etc/ntp/keys/
driftfile /etc/ntp/ntp.drift
logfile /home/spectracom/log/ntp.log
statsdir /home/spectracom/log/ntpstats/
```

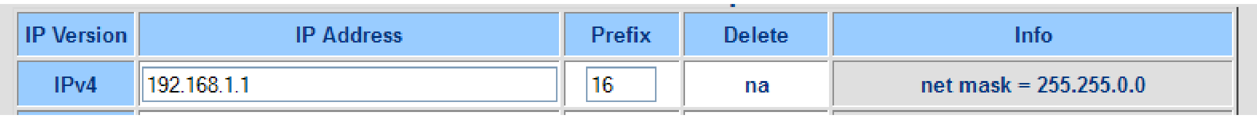
After editing the ntp.conf file, I then edited the IP addresses for Eth 0, Eth 1, Eth 2 and Eth 3 as follows:

Eth 0



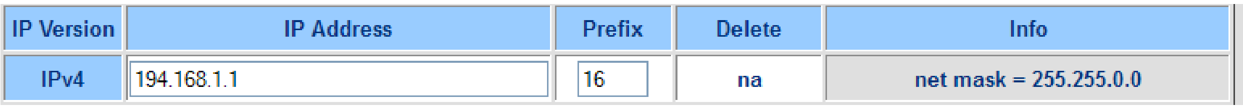
ersion	IP Address	Prefix	Delete	Info
Pv4	10.2.100.147	16	na	net mask = 255.255.0.0

Eth 1



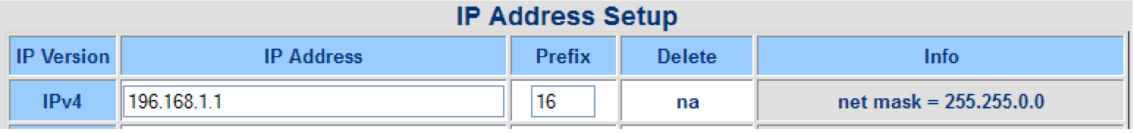
IP Version	IP Address	Prefix	Delete	Info
IPv4	192.168.1.1	16	na	net mask = 255.255.0.0

Eth 2



IP Version	IP Address	Prefix	Delete	Info
IPv4	194.168.1.1	16	na	net mask = 255.255.0.0

Eth 3



IP Address Setup

IP Version	IP Address	Prefix	Delete	Info
IPv4	196.168.1.1	16	na	net mask = 255.255.0.0

With the ntp.conf and Ethernet ports all configured, I then restarted NTP (**Network** -> **NTP Setup** page, **General Settings** tab

Once NTP restarted, and with the SecureSync in sync (this is important, in order for NTP broadcast packets to be generated), I performed a wireshark capture on all four network connections.

Attached is a copy of each of the network port captures, showing NTP broadcast packets being successfully transmitted from the same SecureSync on each isolated subnet.   The second value is the IP address for the SecureSync and the third value is the broadcast address configured in NTP, for that particular network port.

I'm not sure why you weren't receiving the NTP broadcast packets. Make sure that you restart NTP after editing NTP and the network port settings. Were you using Wireshark to capture the NTP broadcast packets, or seeing if your equipment was syncing to the packets? If you weren't using Wireshark to look for the packets, I definitely recommend you do so, especially if you try the steps above again and the equipment still doesn't sync sometime with the NTP broadcast schedule. Also make sure the Sync LED on the front of the SecureSync is green. Another good indication is the Stratum field in the first row of the Status -> NTP table should be a "1" (or a "2" if the SecureSync is synced to another NTPserver that is Stratum 1.

Please let me know that you see the NTP packets broadcast on all four networks.

B) NTP Multicast mode

- Refer to NTP Multicast Tech note: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert Mode- Broadcast and Multicast

Desire to output NTP Multicast on more than one Ethernet port (Gigabit Option card installed)

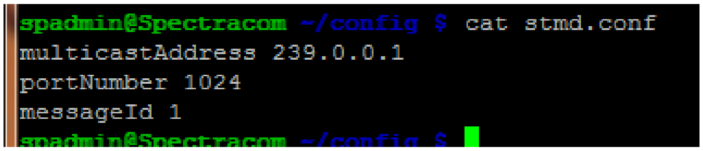
- Refer to Salesforce case 9886
- This configuration won't work – Multicast NTP can only go out one Ethernet port (not more than one). So the gigabit card won't work for this application.

Unlike NTP broadcast which goes out on all network ports, NTP Multicast (224.0.1.1) only goes out one Ethernet port (the first network it sees as valid, such as Eth0 for instance). if its desired to multicast to more than one network, this has to be handled outside of the SecureSync).

We recommended a dumb hub to repeat 224.0.1.1 on all output ports. Then use a firewall with port 123 left open, if its desired to keep subnets isolated from each other.

Configurations

NTP multicast settings are stored in the ***stmd.conf*** file (located in the **/config** directory) example entry below



```
spadmin@Spectracom ~/config $ cat stmd.conf
multicastAddress 239.0.0.1
portNumber 1024
messageId 1
spadmin@Spectracom ~/config $
```

NTP over Anycast mode (aka “high availability” or “HA”)

- Link to data sheet on our website: http://spectracom.com/documents/ntp-over-anycast
- First customer to beta test- Rachin Katti with Microsoft (Matt Loomis customer)
- Added to all SecureSyncs in software update Version 5.2.0 (Feb, 2015). This feature is not available in software versions 5.1.7 and below.
- No license file is required. Automatically enabled in all SecureSyncs with 5.2.0 or above software.
- Anycast uses two assigned addresses. One is the unique, standard Unicast address and the other is a common Anycast address that all NTP slaves can be configured to point to.
- Anycast is a form of load balancing using a special routing protocol (OSPF). All NTP clients can be pointed to
- one static IP address. This simplifies network management, especially with many NTP clients on the network.

“High Availability”/ “HA”

- Refer to salesforce case 24570

Q Question Keith sent to Matt Loomis asking what High Availalbility was (based on a question from customer: have a second NTP unit coming that I would like to set up in **High Availability**.

A Reply from Matt (28 Feb 17) Hi Keith,

High availability is a terminology we are hearing more and more in the enterprise application space. Typically most of our customers looking for “high availability” usually are interested in NTP over AnyCast. But they could also be referring to a highly redundant setups with several failover options…..

You could check with Ron or Dave S if they have any additional input.

(**Note**: Below info is from our Anycast datasheet)

Refer to sites such as:
http://en.wikipedia.org/wiki/Anycast,

https://www.pch.net/resources/papers/ipv4-anycast/ipv4-anycast.pdf

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.116.6367&rep=rep1&type=pdf

What is Anycast Anycast is a network addressing scheme in which messages are routed to one of a group of potential “receivers” via a single destination address based on a one-to-nearest association.

NTP over Anycast The NTP over Anycast feature is a combination of the time server’s ability to associate one of its network ports to an Anycast IP address and to remove itself as an available time source if there is a problem with its reference. As long as the time server is “in sync” it will be available for routing by OSPF to receive and respond to NTP requests. If the unit goes out of sync, it becomes unavailable. The request will be sent to the next nearest NTP server also configured with the NTP over Anycast address. In essence, it is the intelligence of the time server that removes the burden of this function from an NTP client so that the NTP client deployment can be simplified.

Email from Matt Loomis (10 Aug 2016)

Spectracom’s “NTP over AnyCast”:

Each of the Stratum 1 servers are synchronized locally to their Stratum 0 GNSS reference source (GPS/GNSS). At the stratum 2 level, each of the Stratum 2 servers are clients to the Stratum 1 servers and peered to other Stratum 2 servers over unicast connections. The Stratum 2 servers are additionally setup with Anycast support to provide NTP to the application servers over Anycast connections.

This setup provides reliability at all levels. Stratum 1 servers that are out of sync or degraded will be flagged as false tickers by the Stratum 2 servers and will be removed from the NTP synchronization path until resolved. The Stratum 2 servers are also peered over unicast to other Stratum 2 servers for additional reliability. The application servers connect to the Stratum 2 servers, which are configured to support NTP over Anycast connections. This reduces the burden on the application servers, which connect to the shared Anycast addresses of the Stratum 2 servers rather than setting up to individual unicast addresses. If any of the Stratum 2 servers fall out of sync or are degraded, they are removed from the Anycast network, and different Stratum 2 servers on the Anycast network respond without any configuration changes required on the application servers.

Spectracom "NTP over Anycast" Video link:
https://youtu.be/d5sSK2qV-ig

"NTP over Anycast" Tech Brief link:
http://spectracom.com/sites/default/files/document-files/NTP_over_Anycast_TB12-101_revA.pdf

"NTP over Anycast" Diagram link:
http://spectracom.com/sites/default/files/document-files/Hybrid%20Unicast-Anycast%20NTP%20Network_SD16-101%28A%29.pdf

Email from Denis Reilly to Wai Fung with Bloomberg (2 Dec 2014) We developed Anycast NTP in direct response to several customers who have asked for it. They wanted it because they wanted to make their NTP deployments in large systems easier. They wanted the ability to point all their NTP clients to a single IP address, and add and subtract server nodes without having to reconfigure all of their clients (and specifically didn't want to use round-robin DNS).

There are other ways to accomplish this, both inside and outside of NTP. Brad Knowles is correct that NTP has extensive capabilities for failover. Those capabilities are a better fit for some deployments than Anycast would be.

We've found Anycast especially useful in large networks where the possible difference between GPS-synced time servers on the same IP address is small compared to the effect that the network will have on the time – but that assumes all Anycast servers are in sync. So we've also spent some time making sure that when our server loses its GPS reference, it "shuts off" the Anycast route, forcing clients to another (presumably in-sync) server. And there are other ideas we can implement to make Anycast better if customers continue to ask for improvements.

The feature is not officially released yet but it has done well in beta testing and (assuming no issues pop up) we plan on releasing it to all customers as part of the next SecureSync update, which should be delivered in January 2015. If you own a SecureSync, you can try it out for yourself at that point.

Stub areas/NSSA stub

Q Does the appliance support stub areas? If no, how many routes can the routing table hold?
A Per Ron Dries (22 June 2015) We support nssa stub areas through expert mode configuration of the OSPF Anycast feature.

Default hello timer/dead timer

- **Hello timer**: 5 seconds
- **Dead timer**: 40 seconds

Per Ron Dries (22 June 2015) The default hello timer used in SecureSync is every 5 seconds. We typically use the default dead timer of the switch, which is 40 seconds. Other customers have done the same. The dead timer setting will determine how long clients will still be trying to query a server after it has stopped reporting a hello, so this can be configured for however sensitive you want the network to be.

Link aggregation (LACP) / NTP Anycast over more than one Ethernet interface

Q. The NTP Anycast is limited to one eth port. Can it be applied to more than one port through advanced routing somehow?

A Our web ui implementation supports NTP Anycast on a single Ethernet port. There is an expert mode configuration that allows the user to manually configure Zebra and OSPF protocols configuration files. This would allow them to configure Anycast on multiple Ethernet ports in the SecureSync had a Gigabit Ethernet option card installed. We have not tested this at this time. We recommend that Static IP addresses on separate networks would be used for any configurations.

Q.They want to have redundant eth ports on the SecureSync and mentioned LACP to allow them to have the same address on two ports to provide redundancy. Is this a feature that could be enabled somehow?

A reply from Paul Myers (30 June 15) We do not yet support LACP (Link Aggregation Control Protocol) at this time. I believe this would require some Linux kernel configuration and some changes to our software to support this. If desired can customer service enter a ECR (Engineering Change Request) describing the customer use case, customer opportunity to Product Management to be considered?

(11 Aug 15 KW) Per Dave Sohn, **link Aggregation/Ethernet Bonding** in SecureSync is feasible. It's just lower in priority right now.

**eBGP protocol and OSPF NSSA feature ("OSPF Not-So-Stubby Area (NSSA)")

- Refer to RFC 1587 (http://www.ietf.org/rfc/rfc1587.txt)
- Anycast over the BGP protocol was added in software update version 5.4.1

Summay: OSPF and BGP are both protocols to help minimize management of NTP networks, by allowing all NTP clients to be configured with one same address that all NTP servers can sync with, no matter what the other IP Addresses are for that NTP server.

So if an NTP server needs to be swapped out or another NTP server is added, no reconfiguration of the NTP clients is necessary.

Zebra (from Wikipedia)
Zeba is a routing software package that provides TCP/IP based routing services with routing protocols support such as RIP, OSPF and BGP. Zebra also supports special BGP Route Reflector and Route Server behavior. In addition to traditional IPv4 routing protocols, Zebra also supports IPv6 routing protocols. With SNMP daemon which supports SMUX protocol, Zebra provides routing protocol management information bases.

Zebra uses an advanced software architecture to provide a high quality, multi server routing engine. Zebra has an interactive user interface for each routing protocol and supports common client commands. Due to this design, new protocol daemons can be easily added. Zebra library can also be used as a program's client user interface.

A) eBGP (Exterier/External Border Gateway Protocol) (applicable only to versions 5.4.1 and above)

44. NTP Anycast over the BGP protocol was added in software update version 5.4.1

From Wikipedia: https://en.wikipedia.org/wiki/Border_Gateway_Protocol
Border Gateway Protocol (**BGP**) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet.[1] The protocol is often classified as a path vector protocol but is sometimes also classed as a distance-vector routing protocol. The Border Gateway Protocol makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator and is involved in making core routing decisions.

BGP may be used for routing within an autonomous system. In this application it is referred to as Interior Border Gateway Protocol, Internal BGP, or iBGP. In contrast, the Internet application of the protocol may be referred to as Exterior Border Gateway Protocol, External BGP, or EBGP.

eBGP (External BGP) vs iBGP (internal BGP)

- Refer to sites such as: https://supportforums.cisco.com/t5/lan-switching-and-routing/what-is-difference-between-ibgp-and-ebgp/td-p/708154
- iBGP is formed between Neighbors within the same AS, whereas eBGP is formed between neighbors in different AS.

B) OSPF (Open Shortest Path First)

- OSPF for IPv4 was added in software version 5.2.0
- OSPF for IPv6 was added in software version 5.4.1
- In at least versions 5.7.1 we support OSPF v2 (IPv4) and OSPF (IPv6)

***From Wikipedia**: http://en.wikipedia.org/wiki/Open_Shortest_Path_First*
Open Shortest Path First (**OSPF**) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008).

OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks. IS-IS, another link-state dynamic routing protocol, is more common in large service provider networks. The most widely used exterior gateway protocol is the Border Gateway Protocol (BGP), the principal routing protocol between autonomous systems on the Internet.

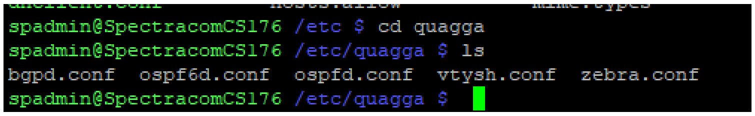
Email from Rachin Katti (18 Nov 14) We need OSPF NSSA feature enabled on the device. Our current network design doesn't align to area 0. Can you please let me know if this is something which can be done sooner? If yes, please share the timelines. Without this the NTP Anycast feature cannot be tested in our network. Thanks

NTP over Anycast configuration

About the Anycast Adddress (for both OSPF and BGP modes): this is a unique static address assigned to just one specified interface port as a "software" port for NTP clients to sync with. This address is only accessible when Anycast is configured correctly and running.
This address does not need to be on the same subnet as the physical address. This address is assigned as an "LO" (local interface) for the physical port.
This address does not need to be manually configured anywhere except within the SecureSync and the NTP clients. The SecureSync advertises it to its switch, and the switch adds this address to its routing table
Note: a troubleshotting tip is to look at the switch's routing table to see if the Anycast address is listed in this table. If NTP anycast is configured and RUNNING, it should be in this routing table.
This address should be limited to a "private" address per RFC 1918 (not a public address that is reserved for the Internet (unless it's a closed network and customer is aware that this address must remain "internal" to their private network.

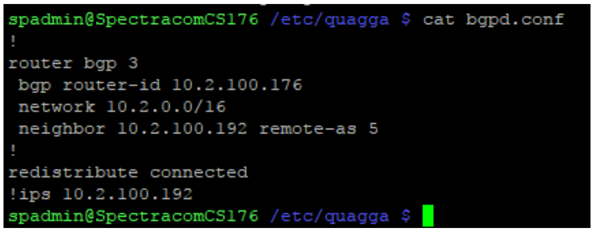
Config files for NTP over ancast

- zebra.conf, ospfd.conf and bgpd.conf are all located in /etc/quagga



```
spadmin@SpectracomCS176 /etc $ cd quagga
spadmin@SpectracomCS176 /etc/quagga $ ls
bgpd.conf  ospf6d.conf  ospfd.conf  vtysh.conf  zebra.conf
spadmin@SpectracomCS176 /etc/quagga $
```

Example bgpd.conf file



```
spadmin@SpectracomCS176 /etc/quagga $ cat bgpd.conf
!
router bgp 3
 bgp router-id 10.2.100.176
 network 10.2.0.0/16
 neighbor 10.2.100.192 remote-as 5
!
redistribute connected
!ips 10.2.100.192
spadmin@SpectracomCS176 /etc/quagga $
```

Anycast configuration is broken into two “sections”

1. **The first section is “General Settings” for Anycast mode (using OSPF or BGP).**
   - Refer to online user guide: http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/AnyCastGenSets.htm

2. **The second section is specific configuration for either OSPF or BGP modes**
   - Specific configuration for **OSPF** mode is in online guide: http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/AnyCastOSPFv4.htm?Highlight=ospf
   - Refer to “A” further below
   - Specific configuration for **BGP mode** is in online guide **applicable only to versions 5.4.1 and above)** http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/AnyCast_BGP.htm
   - Refer to “B” futher below

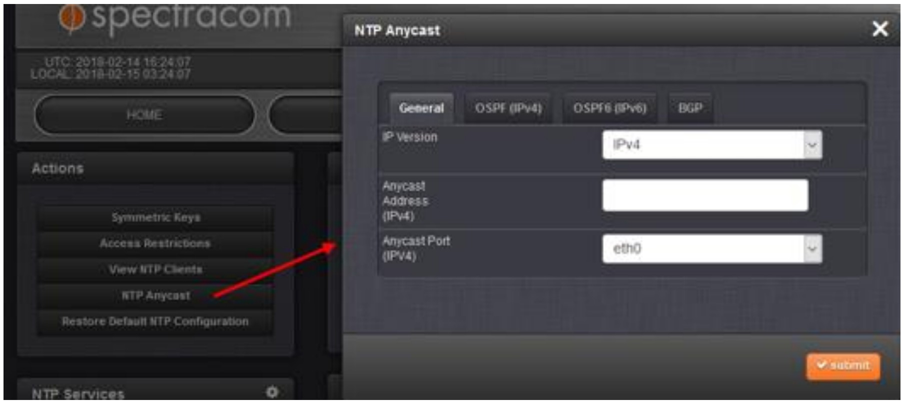
****Important note:** the SecureSync MUST be in SYNC (either to itself, or to an external reference) for the NTP Anycast configurations to be able to be accepted

Note: For example engineering software release testing of NTP over anycast mode, in Arena, refer to the ECO of the release (such as ECO 1338 for v5.7.1 https://app.bom.com/changes/detail-summary?change_id=2389346979) to find the PVP Test validation in the list of “ITEMS”

Example configs Engineering uses to test Anycast: \\rocfnp02\ICS-Eng\Projects\Lafayette\300 Verification Test Plan\Regression Test\Anycast Configuration (BGP is “zebra”?)

General configuration

1. Confirm that your existing network infrastructure is Anycast capable. Determine network specifics, such as the Anycast address and port.
2. In the SecureSync Web UI, navigate to **MANAGEMENT** > **Network** > **NTP Setup.**
3. In the Actions Panel, click “**NTP Anycast**” button (left side of page)

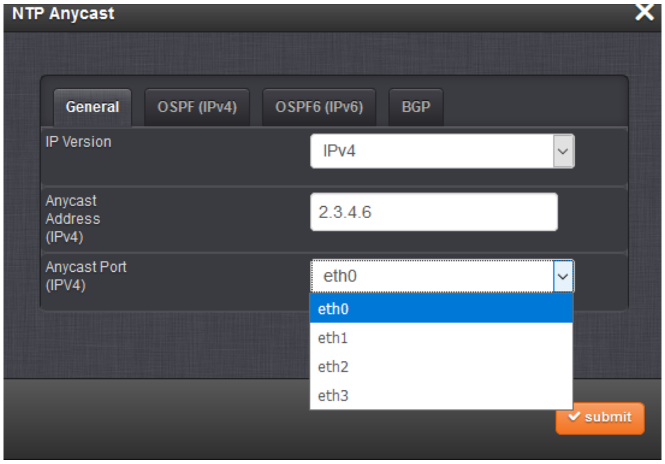


IP Version: IPv4

Anycast Address (IPv4):

Anycast Port (IPv4): eth0

4. In the **NTP Anycast** window, select the **General** tab.
5. On the General tab, select the **IP Version** you will be running Anycast service for. The options are IPv4, IPv6, or both.



IP Version: IPv4

Anycast Address (IPv4): 2.3.4.6

Anycast Port (IPV4): eth0

6. Configure the **Anycast Address** to be used.
7. Select the port to associate the Anycast service with (depending on the option card configuration of your unit, there may be only ETH0 available). If you desire IPv6 functionality, you must also select the IPv6 port address since there may be multiple IPv6 addresses on a single port.

   Note: only one interface can be selected/available for the NTP clients to get time from

8. Click Submit.

Now Proceed to either:

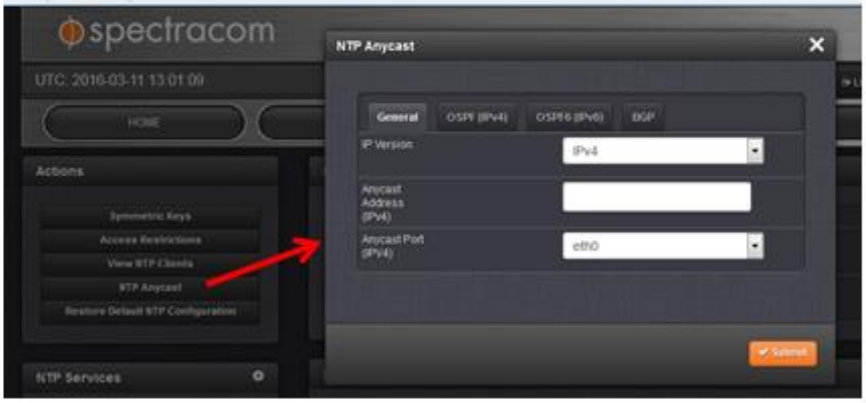
- "A" below for **OSPF** mode
- "B" further below for **BGP** mode

C) OSPF protocol (applicable to software versions 5.2.0 and above)

- http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/AnyCastOSPFv4.htm?Highlight=ospf

B.1 Configuring in software versions 5.4.0 and above (refer to “B.2” further below for versiosn 5.3.1 and below)

1. **Management** -> **NTP Setup** page of the browser and click on **NTP Anycast** (button on the left side of the page)

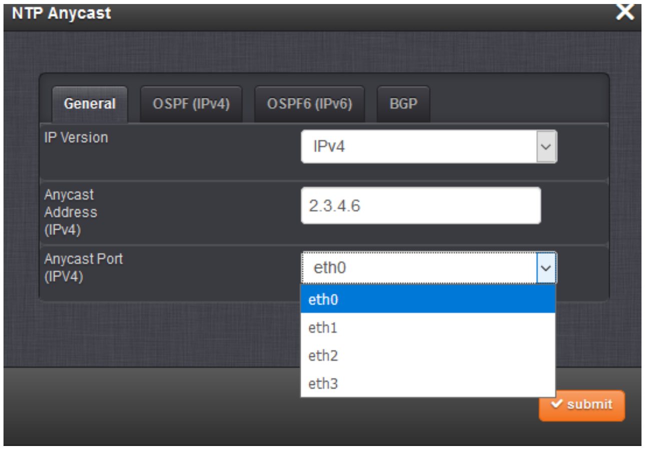


IP Version: IPv4

Anycast Address (IPv4):

Anycast Port (IPv4): eth0

2. Select the **General** tab to configure the NTP Anycast port and Anycast address



IP Version: IPv4

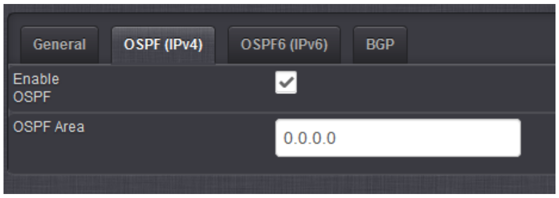
Anycast Address (IPv4): 2.3.4.6

Anycast Port (IPV4): eth0

Anycast address: common static address (not a unique “pre-set” value)

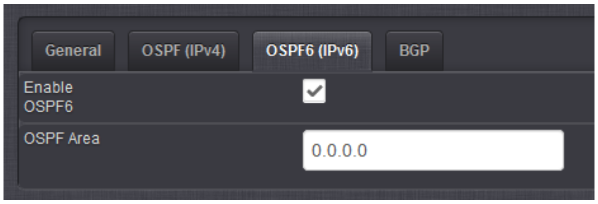
OSPF port: Which one of our Ethernet interfaces communicates with the OSPF switch.

3. Select either the “**OSPF (IPv4)”** or **(OSPF (IPv6)”** tab (as applicable) to enable NTP over Anycast and to configure the OSPF area



Enable OSPF ☑

OSPF Area: 0.0.0.0



Enable OSPF6 ☑

OSPF Area: 0.0.0.0

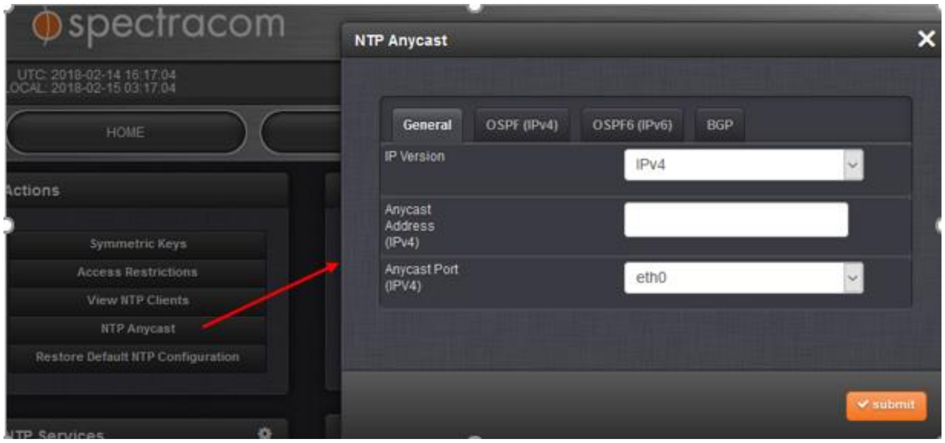
Enable: Enables Anycast mode

OSPF area: (AKA the “backbone area, area 0 or area 0.0.0.0). It’s the IP address of a main router in an area

A) BGP protocol (applicable only to versions 5.4.1 and above)

➢ http://manuals.spectracom.com/SS/Content/_Global/Topics/NTP/AnyCast_BGP.htm?Highlight=bgp

4. **Management** -> **NTP Setup** page of the browser and click on **NTP Anycast** (button on the left side of the page)

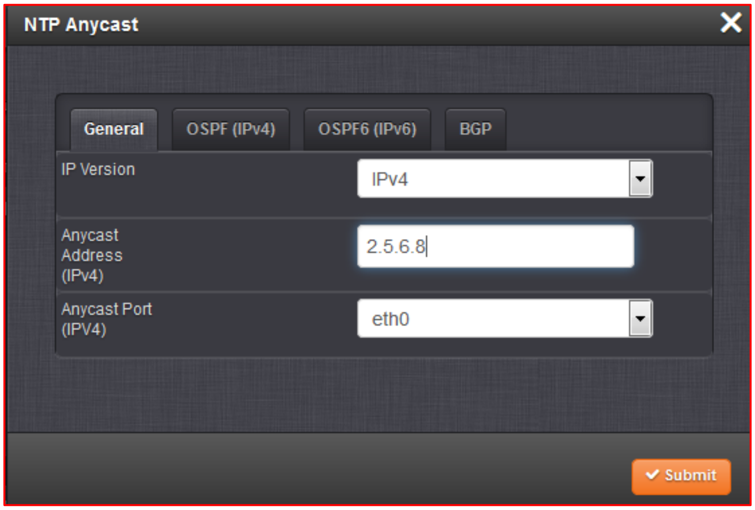


IP Version: IPv4

Anycast Address (IPv4):

Anycast Port (IPv4): eth0

5. Select the **General** tab to configure the **NTP Anycast interface** and **Anycast address**



IP Version: IPv4

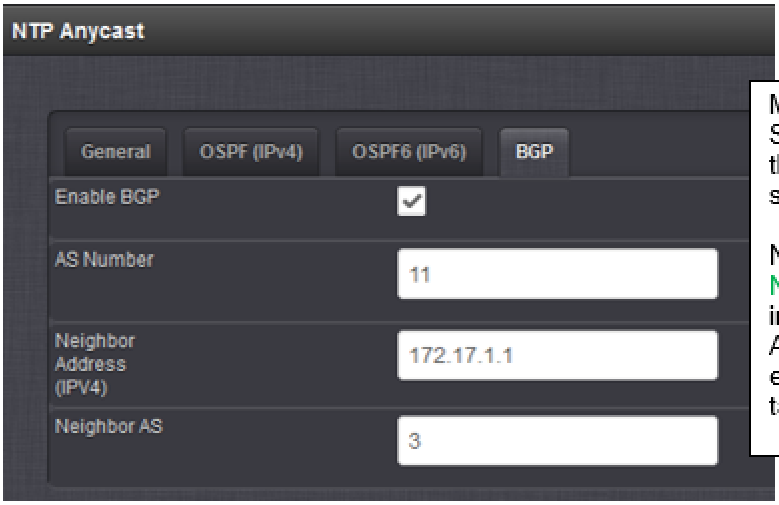
Anycast Address (IPv4): 2.5.6.8

Anycast Port (IPV4): eth0

Anycast address: common static address (not a unique “pre-set” value)

OSPF port: Which one of our Ethernet interfaces communicates with the OSPF switch.

6. Select the **BGP** tab to **enable BGP** as well as configure **AS Number** and **Neighbor info**



Enable BGP: ☑

AS Number: 11

Neighbor Address (IPV4): 172.17.1.1

Neighbor AS: 3

Make sure the AS Number (assigned to the SecureSync) and Neighbor AS (configured in the SecureSyncs immediate switch) are not the same value.

Note the values for the Neighbor Address and Neighbor AS fields are obtained from the immediate swich connected to the defined Anycast interface of the SecureSync (such as eth2 for instance) as defined in the General tab)

AS Number: unique identy value assigned to the SecureSync (cant be the same as the “Neighbor AS” value)

Neighbor Address obtained from the next network device (the switch the SecureSync is connected to) This is not info about any other NTP server on the network.

Neighbor AS: unique identity value for this next network device (usually the switch the SecureSync is connected to) as obtained from that device This is not info about any other NTP server on the network.

Q Does the SecureSync contain any internal OSPF tables such as the OSPF routers have? If so what is the capacity and will a large table slow down performance? Are there any limits to these table sizes?

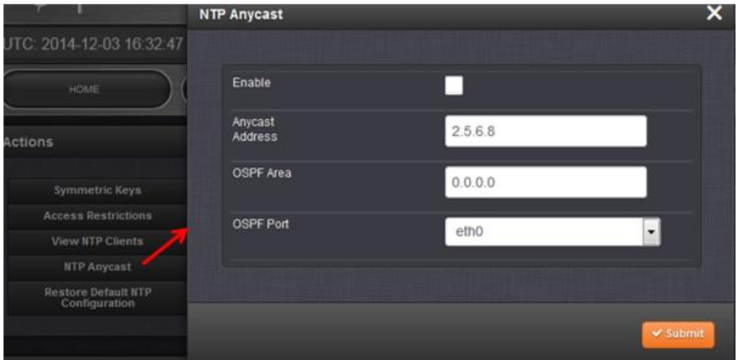
Q Another similar question (SF case 118310) How many routes can the routing table/OSPF DB hold in the SecureSync?

A I told him the SecureSync does not keep track of that and it is done in the routers but he disagreed so I said I would check.

A reply from Paul Myers (30 June 15) Our configurations of Zebra and OSPF simply setup an Anycast Interface configuration. We do not configure the SecureSync as an OSPF Anycast Router.
We participate as an endpoint in the Anycast network architecture. Zebra and OSPF collaborate with the Anycast Router using OSPF to update the routing table to let us participate in using the defined Anycast address.

B.2 Configuring OSPF in Software versions 5.3.1 and below (refer to info above for versions 5.4.1 and above)

1. **Management** -> **NTP Setup** page of the browser and click on **NTP Anycast** (button on the left side of the page)



NTP Anycast

Enable □

Anycast Address 2.5.6.8

OSPF Area 0.0.0.0

OSPF Port eth0

I confirmed my understanding with Denis Riley but will also ask Artem and CC Ron who is out on vacation if OSPF uses large internal tables.

Enable: Enables Anycast mode

Anycast address: common static address (not a unique “pre-set” value)

OSPF area: (AKA the “backbone area, area 0 or area 0.0.0.0). It’s the IP address of a main router in an area

OSPF port: Which one of our Ethernet interfaces communicates with the OSPF switch.

Any internal roouting

Q Does the SecureSync contain any internal OSPF tables such as the OSPF routers have? If so what is the capacity and will a large table slow down performance? Are there any limits to these table sizes?

A I told him the SecureSync does not keep track of that and it is done in the routers but he disagreed so I said I would check.

A reply from Paul Myers (30 June 15) Our configurations of Zebra and OSPF simply setup an Anycast Interface configuration. We do not configure the SecureSync as an OSPF Anycast Router. We participate as an endpoint in the Anycast network architecture. Zebra and OSPF collaborate with the Anycast Router using OSPF to update the routing table to let us participate in using the defined Anycast address.

NTP over Anycast Operation

Testing NTP over Anycast mode (once its been configured)

- Document describing our NTP over Anycast test: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Anycast mode

General info (OSPF and BGP)

3. OSPF

Each time a OSPF-configured SecureSync goes into sync/NTP Stratum 1, its OSPF daemon starts-upto start sending 'Hello' messages to the OSPF switches. It also sends a routing message to the switch. The OSPF switch(es) on the network then knows all the routes to its OSPF-configured SecureSyncs.

As long as each OSPF-configured SecureSync remains in sync and NTP is still in sync, the OSPF daemon will continue to send 'Hello' messages every 10 seconds, to let the switch(es) know that it's still an availalble OSPF route that can be used for NTP client requests.

When there are various subnets (cvarying number of hops between clients and the NTP servers) more than onew NTP server may be activily receiving NTP requests from NTP clients in its "area of the network". The other servers with longer routes just don't receive any NTP packets if other servers are closer and still sending their 'Hello" messages every 10 seconds.

If the SecureSync initially goes into Holdover and then out of sync, the OSPF deamon is stopped, causing the Hello messages to stop being sent out. The OSPF switch has a configurable "dead timer" delay for when the Hello messages stop to when it stops routing NTP requests to that SecureSync.
As there can be a delay between loss of sync and when the next Hello message is sent (in addition to the dead-timer delay in the switch), there may still be NTP time requests sent to the unsynced SecureSync. These NTP requests do not get re-routed to another NTP server. NTP just drops the time stamp as it usually does when OSPF isn't being used. The client will just request time again at its next poll interval,

4. BGP

- Ron Dries says SecureSync handles it internally the same way. But the network routing is handled differently.
- Per https://networklessons.com/bgp/bgp-messages, Apparently, the two BGP devices (secrureSync and Switch) first perform a tcp handshake before performing any BGP packet exchanges.

Log entries associated with NTP over Anycast mode

- Review the Daemon log for OSPF/Zebra entries (refer to troubleshooting Anycast further below)

Journal log entries for OSPF

- Refer to Mantis case 3223
- In at least version 5.3.1 (and 5.4.0) it appears Anycast config changes aren't being logged in Journal log.

SecureSync internally re-routes NTP packets based on health of NTP

- Re-routing of NTP requests when NTP is not healthy (The Server is not synced and NTP is Stratum 16) is handled internal to the SecureSyncs (not handled by the network).

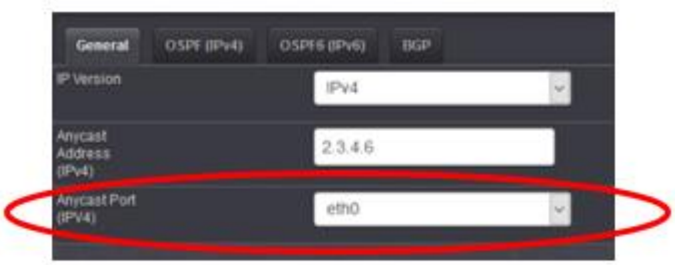
Desire to use OSPF for load balancing of thousands of NTP requests per second

- NTP over Anycast functionality is not a load balancer
- This function cannot be used as a network load balancer to increase the number of NTP requests per second that time servers can respond to each second (the SecureSyncs cannot re-route NTP requests to another NTP server if NTP is dropping packets because its capacity each second has been exceeded).

Troubleshooting NTP over Anycast not working (clients can't sync to the Anycast address

D) General troubleshooting

1. Verify the single configured/dedicated **Anycast address port** is connected to the network with the NTP slaves (anycast works only on the specific configured interface (and no others). As configured in the **Management** -> **NTP Setup** page, **NTP Anycast** button (left side of page). Then select the **General** tab



IP Version: IPv4

Anycast Address (IPv4): 2.3.4.6

Anycast Port (IPV4): eth0

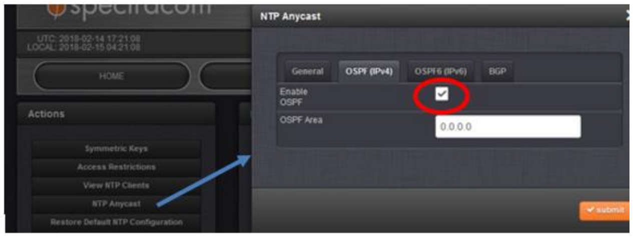
A. Verify that this interface is on the network with the NTP clients (this is the only interface which will work with the NTP Anycast address)

B. Make sure this selected netwok interface port is reachable on the network (via its assigned "physical" IP address/hostname)

C. Verify NTP slaves can succesfully sync when configured with the IP address of this physical interface (instead of configured with the Anycast address). This verifies factors such as DNS, SecureSync being in sync, port 123 blocked of firewall, etc,

2. Verify either OSPF or BGP is truly Enabled and running (via the **Enable** checkbox being selected in the **Management** -> **NTP Setup** page, **NTP Anycast** button (left side of page). Then select either the associated **BGP**,.**OSPF4** or **OSPF6** tab

OSPF4

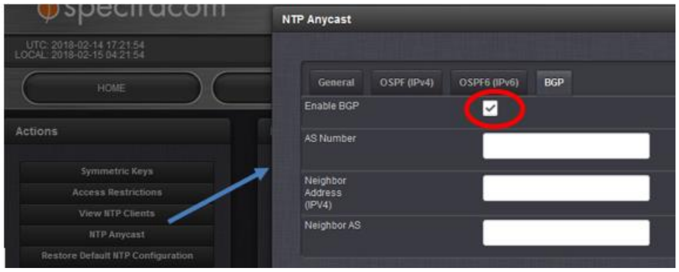


UTC: 2018-02-14 17:21:08
LOCAL: 2018-02-15 04:21:08

Enable OSPF: ☑

OSPF Area: 0.0.0.0

BGP



Enable BGP ☑

AS Number

Neighbor Address (IPV4)

Neighbor AS

3. **(BGP only**- not applicable to OSPF) in the **BGP** tab

    A. Verify the values in the **AS Number** value and **Neighbor AS** fields is not the set to the same value. They must be two different unique numbers. Below is an example Journal entry showing both AS fields set to same value (65001)

    ```
    [WEB] Enabled BGP (IPv4) Anycast: Address 100.100.100.100, Port eth2, AS Number 65001, Neighbor Address 46.235.32.1, Neighbor AS 65001 (spadmin)
    ```

4. Get a **Save log bundle**

    - Review the **Daemon** log for ospf/bgpd entries, to ensure one or the other is actually running (a couple examples below)

      ```
      Feb 13 19:00:22 Spectracom /etc/init.d/zebra[12615]: WARNING: zebra has already been started
      Feb 13 19:00:22 Spectracom /etc/init.d/bgpd[12619]: WARNING: bgpd is already starting
      ```

    - Review the journal log to check the manual configurations of Anycast mode.

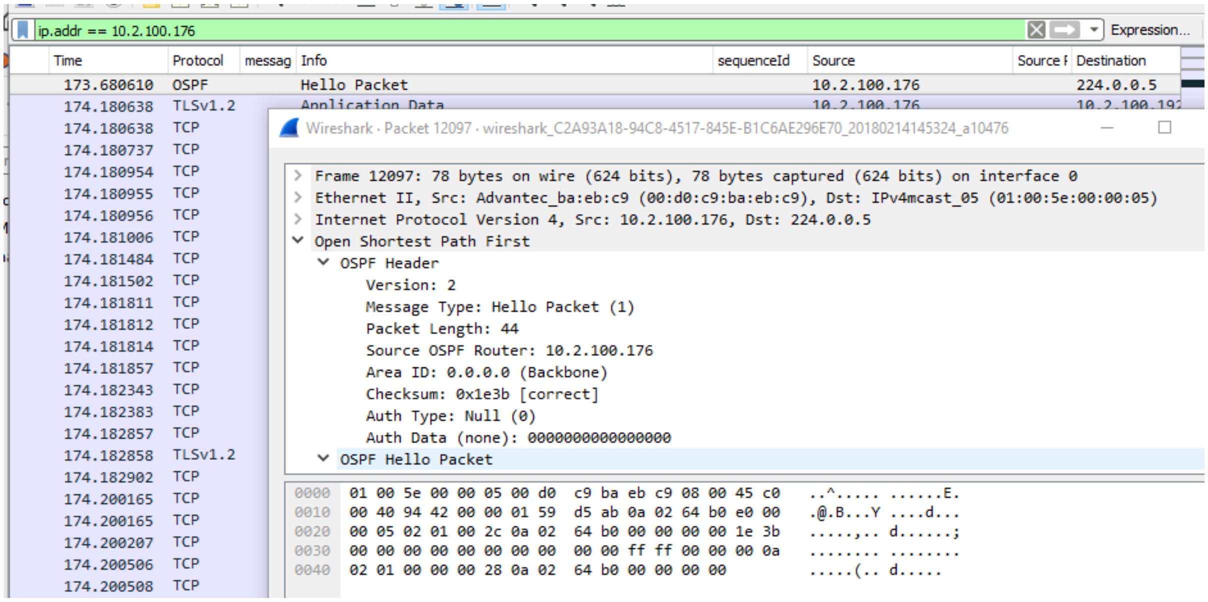
      ```
      [WEB] Enabled BGP (IPv4) Anycast: Address 100.100.100.100, Port eth2, AS Number 65001, Neighbor Address 46.235.32.1, Neighbor AS 65001 (spadmin)
      ```

5. Get a **Save Configs bundle** to review OSPF/Quagga configs

External to the SecureSync

1. look at the the **Routing table of** the SecureSync's immediate **switch connected to the Anycast port** to see if the defined Anycast address is listed in this routing table. If NTP anycast is configured and RUNNING, it should be in this routing table. Its not added or is removed from the routing table if either BGP or OSPF is not Enabled or if there is a configuration issue with Anycast mode.
2. Verify the OSPF or BGP ports are open on the switch (**OSPF is on port 89** and BGP traffic is on **TCP port 179)**
3. Use **tcpdump** or get a **packet capture** to look for '**hello'** messages (OSPF) being sent from the SecureSync to the switch every 10 seconds (see note above about network port numbers)

OSPF Enabled



```
Time         Protocol  messag  Info                 sequenceId  Source          Source F  Destination
173.680610   OSPF              Hello Packet                     10.2.100.176              224.0.0.5
174.180638   TLSv1.2           Application Data                 10.2.100.176              10.2.100.19
174.180638   TCP
174.180737   TCP
174.180954   TCP
174.180955   TCP
174.180956   TCP
174.181006   TCP
174.181484   TCP
174.181502   TCP
174.181811   TCP
174.181812   TCP
174.181814   TCP
174.181857   TCP
174.182343   TCP
174.182383   TCP
174.182857   TCP
174.182858   TLSv1.2
174.182902   TCP
174.200165   TCP
174.200165   TCP
174.200207   TCP
174.200506   TCP
174.200508   TCP
```

Wireshark · Packet 12097 · wireshark_C2A93A18-94C8-4517-845E-B1C6AE296E70_20180214145324_a10476

```
> Frame 12097: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
> Ethernet II, Src: Advantec_ba:eb:c9 (00:d0:c9:ba:eb:c9), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
> Internet Protocol Version 4, Src: 10.2.100.176, Dst: 224.0.0.5
v Open Shortest Path First
  v OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 44
      Source OSPF Router: 10.2.100.176
      Area ID: 0.0.0.0 (Backbone)
      Checksum: 0x1e3b [correct]
      Auth Type: Null (0)
      Auth Data (none): 0000000000000000
  v OSPF Hello Packet
```

```
0000  01 00 5e 00 00 05 00 d0  c9 ba eb c9 08 00 45 c0   ..^..... ......E.
0010  00 40 94 42 00 00 01 59  d5 ab 0a 02 64 b0 e0 00   .@.B...Y ....d...
0020  00 05 02 01 00 2c 0a 02  64 b0 00 00 00 00 1e 3b   .....,.. d......;
0030  00 00 00 00 00 00 00 00  00 00 ff ff 00 00 00 0a   ........ ........
0040  02 01 00 00 00 28 0a 02  64 b0 00 00 00 00         .....(.. d.....
```

BGP mode

- Per https://networklessons.com/bgp/bgp-messages, Apparently, the two BGP devices (SecureSync and Switch) first perform a tcp handshake before performing any BGP packet exchanges. So there wonlt be any “BGP protocol (tcp port 179) packets exchanged if the neighbor isnlt really a bgp enabled switch.

E) NTP over Anycast mode configs are not taking/being saved

Verify the SecureSync is in sync (to an external reference or to itself) as required by this function. It has to first be synced before it can be configured.

NTP Expert Mode

- Refer to the NTP expert mode tech note: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert Mode- Broadcast and Multicast
- Required to use for NTP multicast mode
- Required to use with the NTP/External 1PPS input reference.
- Believe it can be used to provide NTP manycast mode

NTP Setup page GUI fields not accessible while Expert mode is enabled

- Most NTP configurations in the **NTP Setup** page are not available while Expert mode is enabled. As of at least version 5.2.1:
  - **NTP autokey**: Not available while in Expert mode
  - **Symmetric key:** Can be used while in Expert mode (because ntp.keys is a different file than ntp.conf)

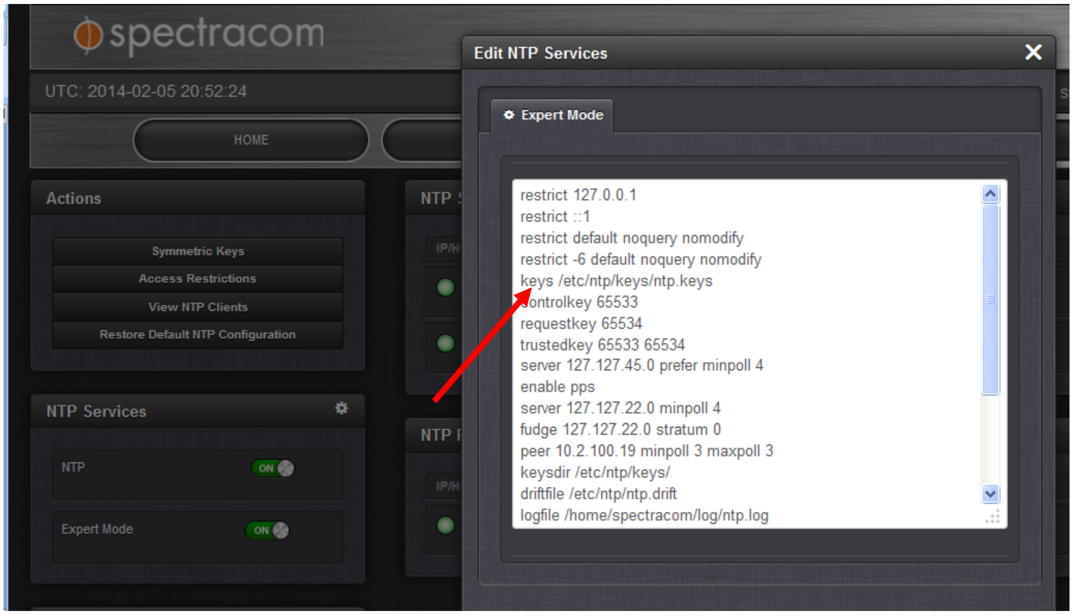
ntp.conf file in expert mode

- Uses the same ntp.conf file in both modes
- spadmin account has rights to view (cat) the ntp.conf file via telnet connection, but not with ssh onnection

Enabling Expert Mode

A) via web browser

1. Go to the Management -> NTP Setup page of the browser
2. Enable NTP Expert Mode
3. Click on the gear next to “NTP Services” to open/edit the ntp.conf file
4. Leave Expert Mode enabled to retain settings
5. Disable Expert Mode to reset ntp.conf back to factory default settings



```
restrict 127.0.0.1
restrict ::1
restrict default noquery nomodify
restrict -6 default noquery nomodify
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
server 127.127.45.0 prefer minpoll 4
enable pps
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
peer 10.2.100.19 minpoll 3 maxpoll 3
keysdir /etc/ntp/keys/
driftfile /etc/ntp/ntp.drift
logfile /home/spectracom/log/ntp.log
```

Operation as a Stratum 2 server (as of 10/20/09)

The current stratum-2 behavior will be as follows:

- The NTP running on the SecureSync will synchronize normally to the configured peers.
- Once a peer has been selected by NTP, KTS will be synchronized to that selected peer.
- When all peers are lost, the SecureSync will go into holdover and KTS will become the selected peer, synchronizing NTP using the undisciplined oscillator of the system

Note: The current design does not discipline the oscillator based on NTP, instead only steering the PPS based on NTP. That means the holdover characteristics of the unit in Stratum-2 will be based on the undisciplined oscillator of the unit.

External 1PPS input to SecureSync

- For more information, refer to: 1PPS input (epp0)

Note: As also discussed in the NTP peering and External PPS input documents, we highly recommend listing more than one NTP server to sync with. Listing just one can cause NTP to continue to toggle between NTP input and Stratum 1 input, with periodic Holdover alarms asserted.

NTP clockstats, loopstats and peerstats

Refer to (in “NTP for all products” towards the beginning of this document): NTP ClockStats, Loopstats and Peerstats

*NTP burst/iBurst mode

NTP can sync within just a couple of seconds of starting if NTP has a valid System Time reference (such as GPS or

IRIG) to sync with.

Issues related to NTP

Notifications / Email alerts /SNMP

*Notifications (SNMP traps and email alerts)/Alarms

Monitoring/Alert capabilities of installed Option Cards

Note: All of this info below is as of at least versions 5.5.1 (Feb 2017)

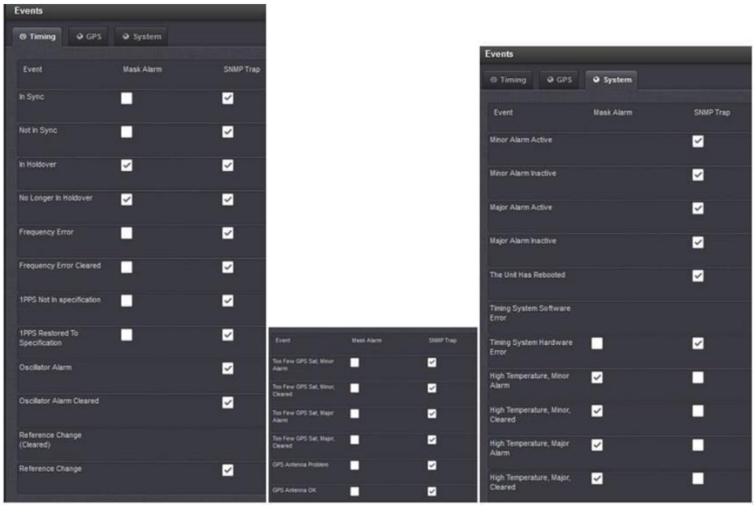
- No SNMP Traps/email alerts are directly availalble for Option Card functionality
- Only a couple of indirect (inherent) alarms/alerts are available for a loss of the currently selected input refernce, if the selected input is being provided by an Option Card (such as IRIG, PTP, havequick inputs)
  - Loss of the selected input results in either "Refernce Change" if there is another available reference which can be selected, or results in "Holdover" alert if there are no other references available for selection.

Q …need to verify that the Spectracom Secure Sync.. can in fact fault detect and fault isolate to these optional cards? and where can I find the information WRT how the system can/will notify me of such a failure requiring maintenance.,,

A response from Keith (3 Feb 17) Available SecureSync Option Cards which provide functionality for one or more outputs (such as the Model 1204-06 Gb Ethernet card, the IRIG outputs on the IRIG Option Cards, etc) and their associated output(s), are not monitored by the base SecureSync which the Option Cards are installed in. Therefore, there is no alert notification capability of the SecureSync itself, if there happens to be a problem with an output card or its particular output port. The alert would need to be provided by the other system which is connected to the SecureSync's output (an alarm/alert indicating the loss of its input signal for example).

SecureSync Option Cards which provide functionality for one or more inputs (such as the Model 1204-05 IRIG Input/Output Option Card for instance) or with each of its particular input(s), can result in indirect alerts/alarms being asserted- but only if this particular input is lost while it's the SecureSync's selected reference (alarms/alerts such as the "Reference Change" event is asserted if the SecureSync can switch to another available reference after its current reference is lost, or the Holdover alert is asserted if there are no other input references present/valid when this particular input signal is lost). Other than the alerts/alarms associated with the loss of the currently selected input reference signal, there is no continued monitoring of the Option Cards to detect if the Option Card or its particular input has a problem (the loss of a "not currently selected" input reference just results in that particular reference becoming "not valid" (unavailable for selection if the currently selected reference happens to become no longer present/becomes not valid) until the input has been restored. The loss of a "backup" reference is not an alarm/alert condition.

Note that with SNMP and/or Email alerts configured, the SecureSync can SNMP traps/email alert for many different conditions. All of these conditions (such as going into Holdover mode, loss of sync, etc), are shown in the **Management** -> **Notifications** page of the browser (via each of the three tabs at the top containing associated alerts. For your reference, Screenshots below are of the three tabs (note that each event can be individually configured to send an SNMP trap and, or an email alert but for simplicity, these screenshots are just omitting the email checkbox/email address field for each event).



Events

Event	Mask Alarm	SNMP Trap
In Sync	☐	☑
Not In Sync	☐	☑
In Holdover	☑	☑
No Longer In Holdover	☑	☑
Frequency Error	☐	☑
Frequency Error Cleared	☐	☑
1PPS Not In specification	☐	☑
1PPS Restored To Specification	☐	☑
Oscillator Alarm		☑
Oscillator Alarm Cleared		☑
Reference Change (Cleared)		
Reference Change		☑

Event	Mask Alarm	SNMP Trap
Too Few GPS Sat, Minor Alarm	☐	☑
Too Few GPS Sat, Minor, Cleared	☐	☑
Too Few GPS Sat, Major Alarm	☐	☑
Too Few GPS Sat, Major, Cleared	☐	☑
GPS Antenna Problem	☐	☑
GPS Antenna OK	☐	☑

Events

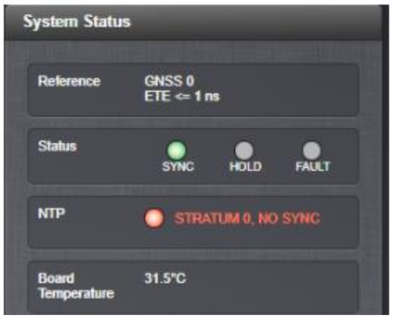
Event	Mask Alarm	SNMP Trap
Minor Alarm Active		☑
Minor Alarm Inactive		☑
Major Alarm Active		☑
Major Alarm Inactive		☑
The Unit Has Rebooted		☑
Timing System Software Error		
Timing System Hardware Error	☐	☑
High Temperature, Minor Alarm	☑	☐
High Temperature, Minor, Cleared	☑	☐
High Temperature, Major Alarm	☑	☐
High Temperature, Major, Cleared	☑	☐

Configuration for Notifications (SNMP Traps and/or Emails) to be sent

- Refer to the online 2400 SecureSync user guide: http://manuals.spectracom.com/2400/Content/NC_and_SS/Com/Topics/CONFIG/Notificat_Conf.htm

Inherent affects on the System when changes to Notifications are made (at least v5.9.2 and below)

- Refer to Salesforce cases such as 271831
- Refer to JIRA SSS-1114
- When any config changes are made to Notifications, statusd (status monitor daemon) will be restarted.
- statusd is what also monitors NTP Stratum and Sync state.
- While statusd is restarting, NTP will inherently be reported as being Stratum 0, Not in sync



System Status

Reference	GNSS 0 ETE <= 1 ns
Status	● SYNC ○ HOLD ○ FAULT
NTP	● STRATUM 0, NO SYNC
Board Temperature	31.5°C

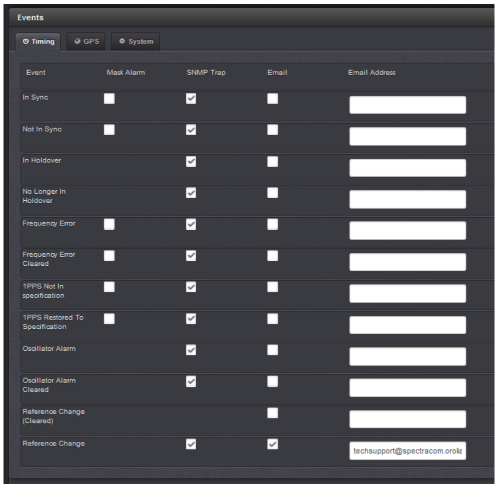
- The **System** log will assert the following entries:

  GPS Monitor daemon has restarted
  Enabling alarm mask for event: Max temperature exceeded(MAJOR) (55)
  Enabling alarm mask for event: Max temperature exceeded(MINOR) (53)
  Enabling alarm mask for event: In holdover (3)
  Notification daemon has restarted

Web browser config

Management **->** ***Notifications*** **page (three tabs at the top)**

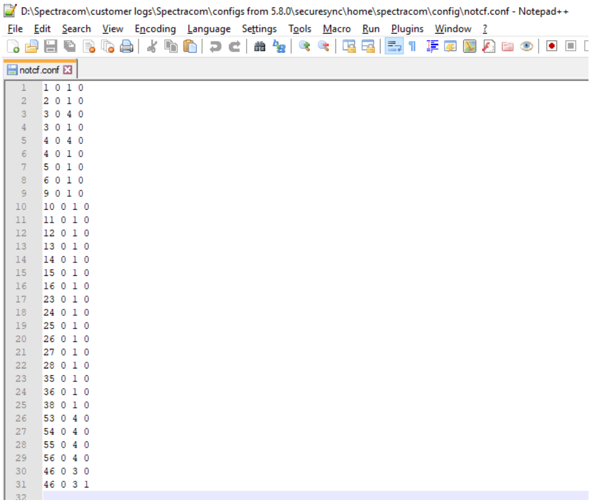
- The three tabs at the top of the page- *Timing*, *GPS* and *System*- contain the associated Notifications (these are the only notifications available to be sent from the NTP server)



Events

Event	Mask Alarm	SNMP Trap	Email	Email Address
In Sync	☐	☑	☐	
Not In Sync	☐	☑	☐	
In Holdover		☑	☐	
No Longer In Holdover		☑	☐	
Frequency Error	☐	☑	☐	
Frequency Error Cleared	☐	☑	☐	
1PPS Not In specification	☐	☑	☐	
1PPS Restored To Specification	☐	☑	☐	
Oscillator Alarm		☑	☐	
Oscillator Alarm Cleared		☑	☐	
Reference Change (Cleared)			☐	
Reference Change		☑	☑	techsupport@spectracom.orolia

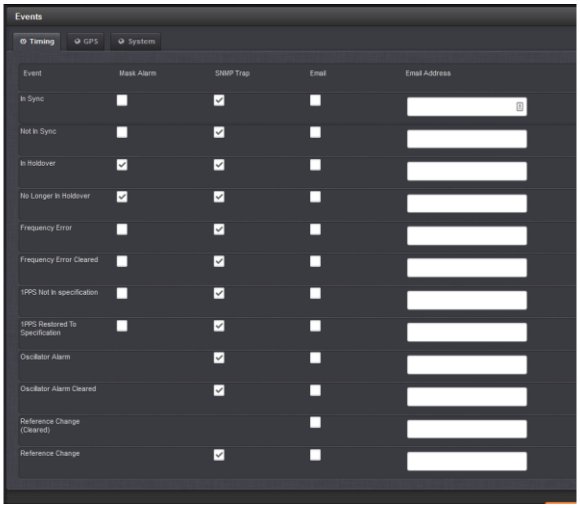
Note: These Mask Alarms *settings are stored in the* ***\home\spectracom\config\notcf.conf file*** *(as shown below):*


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 0 1 0
2 0 1 0
3 0 4 0
3 0 1 0
4 0 4 0
4 0 1 0
5 0 1 0
6 0 1 0
9 0 1 0
10 0 1 0
11 0 1 0
12 0 1 0
13 0 1 0
14 0 1 0
15 0 1 0
16 0 1 0
23 0 1 0
24 0 1 0
25 0 1 0
26 0 1 0
27 0 1 0
28 0 1 0
35 0 1 0
36 0 1 0
38 0 1 0
53 0 4 0
54 0 4 0
55 0 4 0
56 0 4 0
46 0 3 0
46 0 3 1
```

Three tabs (screenshots shown with v1.2.1 installed)

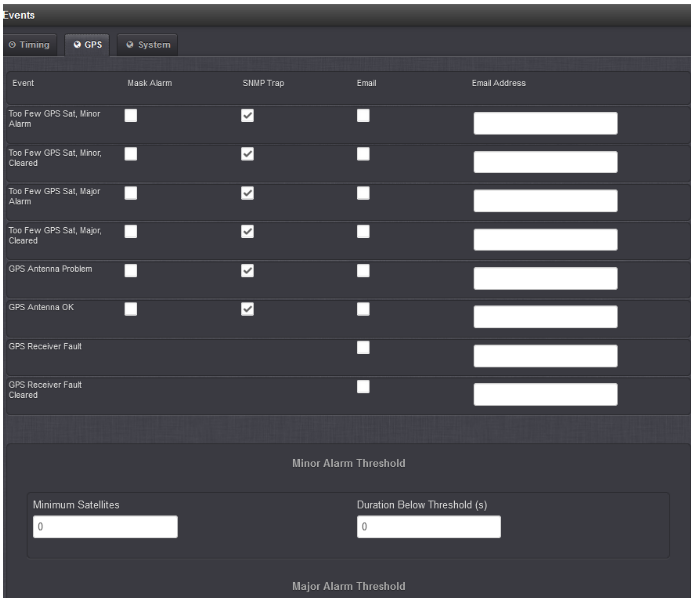
A) **TIMING** Tab



Events

Event	Mask Alarm	SNMP Trap	Email	Email Address
In Sync	□	☑	□	
Not In Sync	□	☑	□	
In Holdover	☑	☑	□	
No Longer In Holdover	☑	☑	□	
Frequency Error	□	☑	□	
Frequency Error Cleared	□	☑	□	
1PPS Not In specification	□	☑	□	
1PPS Restored To Specification	□	☑	□	
Oscillator Alarm		☑	□	
Oscillator Alarm Cleared		☑	□	
Reference Change (Cleared)			□	
Reference Change		☑	□	

B) GPS Tab (shown without Opt-BSH IDM software enabled)



Events

Event	Mask Alarm	SNMP Trap	Email	Email Address
Too Few GPS Sat, Minor Alarm	□	☑	□	
Too Few GPS Sat, Minor, Cleared	□	☑	□	
Too Few GPS Sat, Major Alarm	□	☑	□	
Too Few GPS Sat, Major, Cleared	□	☑	□	
GPS Antenna Problem	□	☑	□	
GPS Antenna OK	□	☑	□	
GPS Receiver Fault			□	
GPS Receiver Fault Cleared			□	

Minor Alarm Threshold

Minimum Satellites: 0

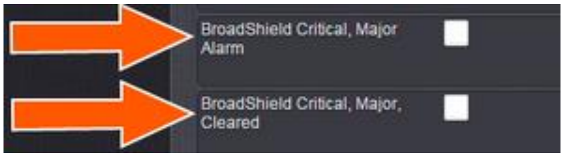
Duration Below Threshold (s): 0

Major Alarm Threshold

Opt-BSH: Broadshield notifications (with Opt-BSH enabled) in GPS tab

- ➢ These notifications are only displayed/available when Opt-BSH: BroadShield is installed/enabled

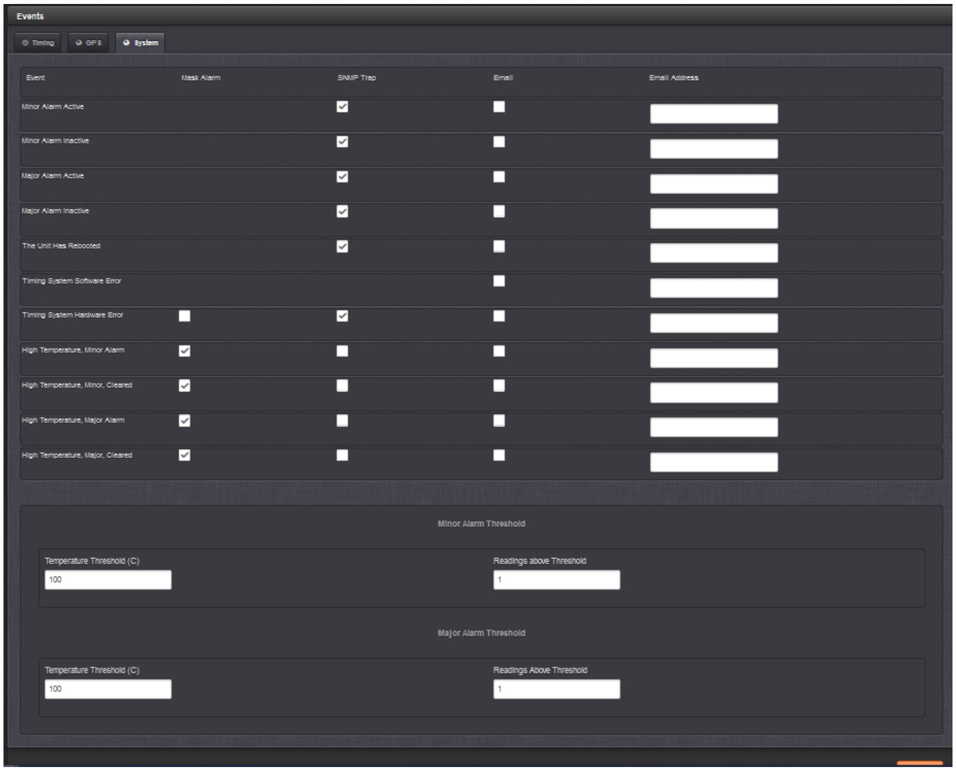
Management -> **Notifications** page of the browser



BroadShield Critical, Major Alarm □

BroadShield Critical, Major, Cleared □

C) SYSTEM Tab



Event	Mask Alarm	SNMP Trap	Email	Email Address
Minor Alarm Active		☑	□	
Minor Alarm Inactive		☑	□	
Major Alarm Active		☑	□	
Major Alarm Inactive		☑	□	
The Unit Has Rebooted		☑	□	
Timing System Software Error			□	
Timing System Hardware Error	□	☑	□	
High Temperature, Minor Alarm	☑	□	□	
High Temperature, Minor, Cleared	☑	□	□	
High Temperature, Major Alarm	☑	□	□	
High Temperature, Major, Cleared	☑	□	□	

Minor Alarm Threshold

Temperature Threshold (C): 100

Readings above Threshold: 1

Major Alarm Threshold

Temperature Threshold (C): 100

Readings Above Threshold: 1

Note (at least 1.2.1 and below): Notice there are no “Mask Alarm” checkboxes available from Major Alarm/Minor Alarm, Timing System Software Error and Reboot (these alerts cant be masked)

**Nullmailer/Email Alerts

A) Nullmailer:

From http://wiki.linuxquestions.org/wiki/Nullmailer#Running_the_daemon: "nulllmailer is a simple and secure relay-only mail transport agent

- Nullmailer is an email package automatically included in Gentoo (versions 5.0.0 and above)
- We don't configure or use Nullmailer

Refer to the **rexd.log** for Nullmailer log entries: rexd.log (daemon log) and rexd.bone log   Note that the rex.bone log MOTD time stamp gets updates each time Nullmailer runs.

B) Email Alerts

- For more information on Email alerts refer to: I:\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.
- 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)

Configure Email/SMTP setting

Refer to the Email tech note that Morgan created:

- At: \EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\SNMP
- On our website at: http://spectracom.com/sites/default/files/document-files/Email%20Notification%20Setup%20SecureSync%20and%20NetClock.pdf

Desire to send alerts to more than email address

- Limited to just one "To" email address per notification type.
- 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 settints (see below)

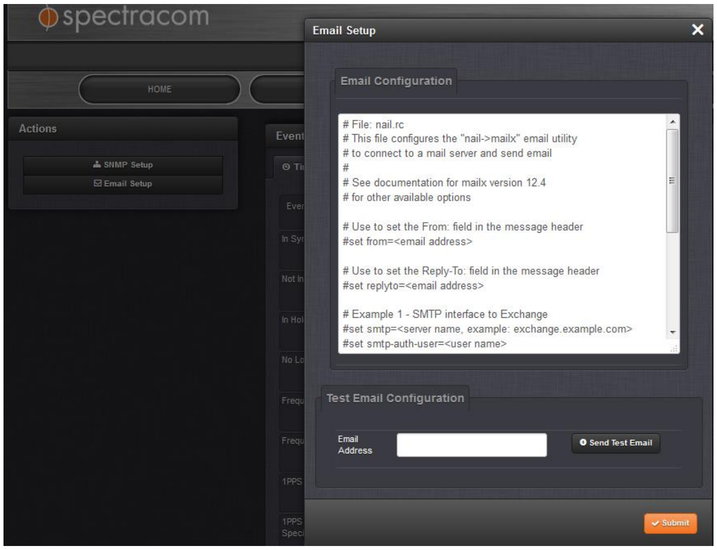
Email from Ron Dries (25 Jun 16) I just tried adding set autocc to the email configuration file and it worked. The syntax was as described in that document.

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.

A) Web browser

Management -> **Notifications** page of browser, press the "**Email Setup"** on the left side of the page.



Email Setup

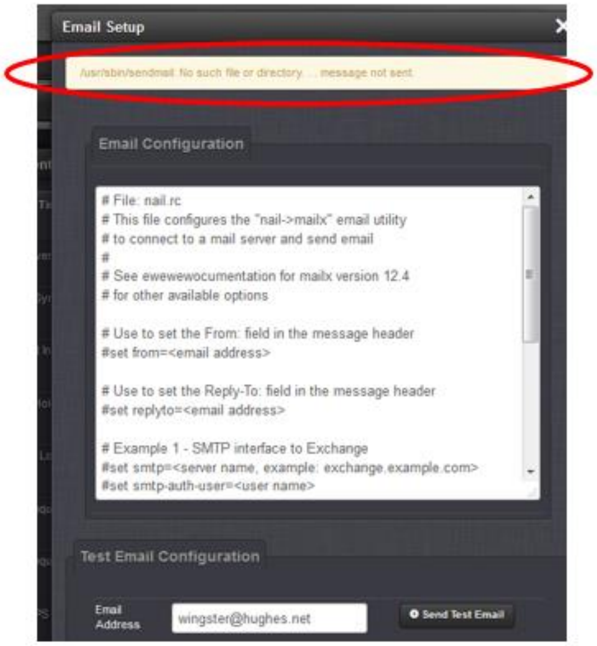
Email Configuration

```
# File: nail.rc
# This file configures the "nail->mailx" email utility
# to connect to a mail server and send email
#
# See documentation for mailx version 12.4
# for other available options

# Use to set the From: field in the message header
#set from=<email address>

# Use to set the Reply-To: field in the message header
#set replyto=<email address>

# Example 1 - SMTP interface to Exchange
#set smtp=<server name, example: exchange.example.com>
#set smtp-auth-user=<user name>
```

Test Email Configuration

Email Address:

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:



Email Setup

/usr/sbin/sendmail: No such file or directory. ... message not sent.

Email Configuration

```
# File: nail.rc
# This file configures the "nail->mailx" email utility
# to connect to a mail server and send email
#
# See ewewewocumentation for mailx version 12.4
# for other available options

# Use to set the From: field in the message header
#set from=<email address>

# Use to set the Reply-To: field in the message header
#set replyto=<email address>

# Example 1 - SMTP interface to Exchange
#set smtp=<server name, example: exchange.example.com>
#set smtp-auth-user=<user name>
```

Test Email Configuration

Email Address: wingster@hughes.net

- 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 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.

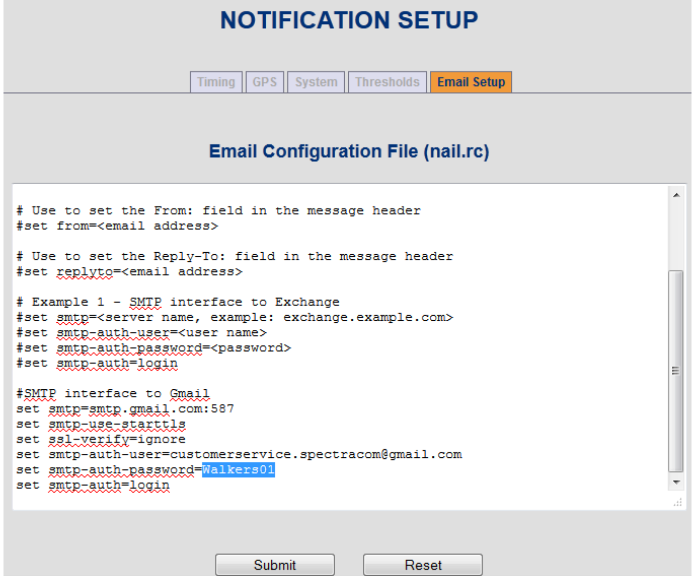
1. **Example smtp setup for Outlook 365 SMTP from a workstation that worked for Keith**

   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.orolia.com
   set smtp-auth-password=              (email still sent with no password)
   set smtp-auth=login
   set from=keith.wing@spectracom.orolia.com
   ```

   Test Email Configuration -> **“Email address”** field: keith.wing@spectracom.orolia.com or techsuport@spectracom.orolia.com

2. **Example Gmail SMTP setup that worked using the classis interface (performed by Sam Otto)**



```
# Use to set the From: field in the message header
#set from=<email address>

# Use to set the Reply-To: field in the message header
#set replyto=<email address>

# Example 1 - SMTP interface to Exchange
#set smtp=<server name, example: exchange.example.com>
#set smtp-auth-user=<user name>
#set smtp-auth-password=<password>
#set smtp-auth=login

#SMTP interface to Gmail
set smtp=smtp.gmail.com:587
set smtp-use-starttls
set ssl-verify=ignore
set smtp-auth-user=customerservice.spectracom@gmail.com
set smtp-auth-password=Walkers01
set smtp-auth=login
```

Example smtp setup for Exchange server

- ➢ Enter just one email address for each notification type to be sent to, as desired

Q. According to User Manual, it seems that we can use "Microsoft Exchange" and "Gmail" as SMTP server which we can send Email to. Can we set SMTP server other than "Microsoft Exchange" and "Gmail" in "Email setup" tab of "NOTIFICATION Setup" page?
A. Reply from Dave Lorah: The email alerts function can use any exchange server to send emails, not just MS and Gmail only.

Email to Bruce Carey 10/10/11 based on feedback from Mike Sander:
Regarding the SecureSync email alerts functionality, I have some feedback for you, from our Engineering team:

Other Notes

1) In SecureSync, we enter the short form of the user name, in your particular case, "Careyb"

2) The settings for exchange servers are tricky and in our particular case, required some back and forth with our IT group to allow it to start working.

3) The SecureSync uses a linux-based email utility called "**nail**" to send email alerts. The **Notifications**->**Email Setup** window is editing the standard "nail.rc" configuration file in the background. So you can look at documentation for "nail.rc" for advanced information about configuring email notifications (refer to sites such as http://linux.die.net/man/1/nail for example).

4) You can also invoke "nail" for a command line using either telnet (in a command prompt window, type telnet xxx.xxx.xxx.xxx - where x is the IP address of the NTP server) or the front panel serial port (connecting a PC running HyperTerminal to this port using a straight-thru serial cable- pinned 2 to 2, 3 to 3 and 5 to 5 for a minimum pinned cable). Refer to the attached Application Note regarding HyperTerminal.

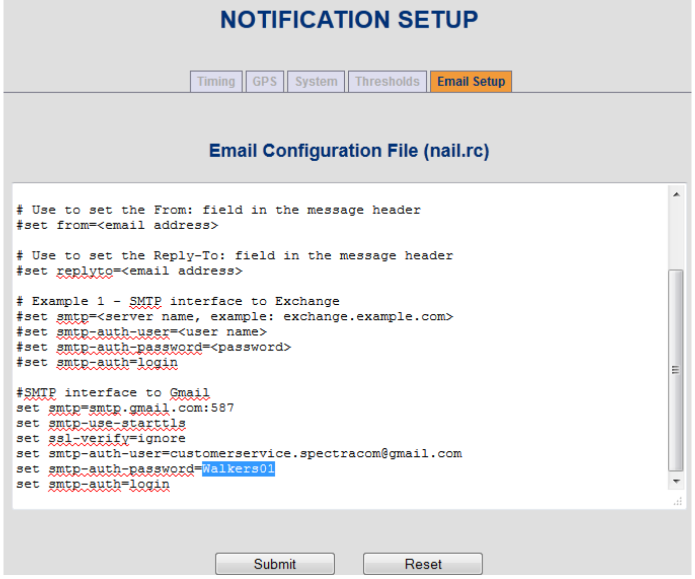
   Here's an example:

   ```
   >nail -s "test" user@XYZ.com
   Testing testing testing
   <ctrl-d>
   ```

   Nail may display a useful error.

5) You should try commenting out the "gmail configuration" and just exposing the exchange configuration. The emails can't be sent using two servers and will use the last definition in the file.

Example Gmail SMTP setup that worked (performed by Sam Otto)



```
# Use to set the From: field in the message header
#set from=<email address>

# Use to set the Reply-To: field in the message header
#set replyto=<email address>

# Example 1 - SMTP interface to Exchange
#set smtp=<server name, example: exchange.example.com>
#set smtp-auth-user=<user name>
#set smtp-auth-password=<password>
#set smtp-auth=login

#SMTP interface to Gmail
set smtp=smtp.gmail.com:587
set smtp-use-starttls
set ssl-verify=ignore
set smtp-auth-user=customerservice.spectracom@gmail.com
set smtp-auth-password=Walkers01
set smtp-auth=login
```

"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

SNMP package in SecureSync

- Like 1200 SecureSyncs and VersaSyncs, 2400 SecureSyncs 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

SecureSync System Version	Corresponding Net-SNMP Version	Notes
Versions 5.1.7 and below	5.6.1	
Versions 5.2.0 (Feb 2015) and above	5.6.2.1	In order to update SNMP to the newer version, our snmpsad subagent needed to also be updated.
Version 5.2.1	X (no change- still 5.6.2.1)	Added a patch to Net-SNMP to address SNMPD crashing. This patch didn't change the Net-SNMP version.

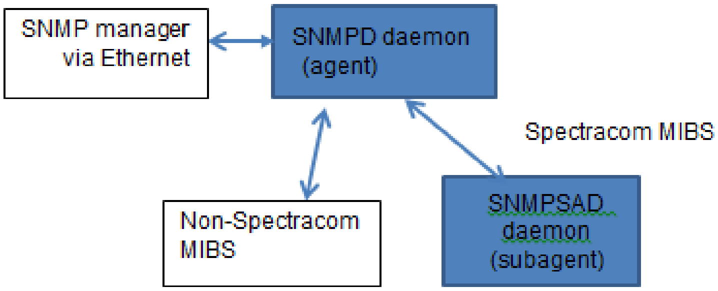
SNMP MIB files/Object IDs

- Path to the MIB files stored in the Model 9400 series: Home/Spectracom/mibs
  - The SNMP object numbers of "**.1.3.6.1.4.1.18837.**" are for the Spectracom-specific objects.
  - The SNMP object numbers of "**.1.3.6.1.4.1.8072.**" are objects associated with Net-SNMP.
  - The SNMP object numbers of "**.1.3.6.1.4.1.2.1**" are objects associated with RFC-1213.

SNMPD and SNMPSAD daemons

- There are three daemons that run for SNMP:
  - **SNMPD**: the agent running in the Linux OS
  - **SNMPSAD**: the subagent running in Spectracom application
  - **SNMPSAL**: our daemon that restarts SNMPSAD if it crashes

SNMP Basic block diagram



(Modified) email from Mark Goodlein to Morgan Stanley (7/1/12)
For SNMP:
There are 2 daemons that run, one is the agent (SNMPD) which handles snmp protocol and some published system mibs. The other is a subagent (SNMPSAD) which connects to the agent and handles the Spectracom-specific mibs.

**Remote Monitoring / SNMP configuration

Enterprise-level network monitoring tools

- Refer to the "…network monitoring tools" section of the Custserviceassistance document

SNMPd config file

- Path to the snmpd.conf file in the time server: home/spectracom/config
- Refer to: http://www.net-snmp.org/docs/man/snmpd.conf.html and

  http://www.net-snmp.org/wiki/index.php/Vacm (VACM info)

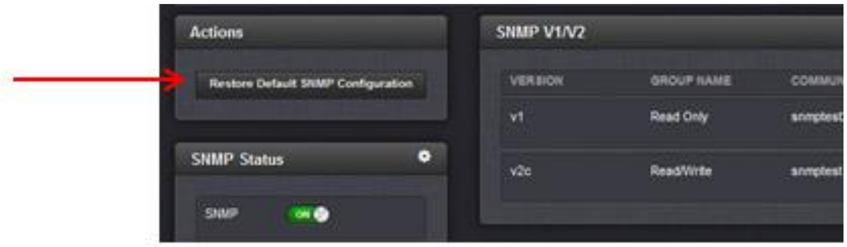
snmpd supports the View-Based Access Control Model (VACM) as defined in RFC 2575, to control who can retrieve or update information. To this end, it recognizes various directives relating to access control.

SNMP configuration

- **Refer to the SecureSync SNMP Tech Note**: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\SNMP- Notifications-email alerts\SNMP

Management -> **SNMP Setup** page

"Restore Default SNMP Configuration" button



VERSION	GROUP NAME	COMMUN
v1	Read Only	snmptest
v2c	Read/Write	snmptest

- The newer black/charcoal browser now has a "Restore Default SNMP Configuration" button in the Management -> SNMP Setup page which resets just the SNMP configs (alleviating the need to perform a full clean of all configs). Not sure what rev (either version 5.1.7 or before) this button was added to the newer browser.

- Brian Carlson with Harris was seeing weird issues with the configuration of the Notifications page and traps not being sent when they should. Using this button and reconfiguring SNMP fixed these peculiar issues.

A) SNMP User configuration (SNMP gets and sets)

1. SNMP V1/V2c user configuration

- **Unsecure**: Unlike SNMPv3, v1 and v2c do not use either encryption or authentication.

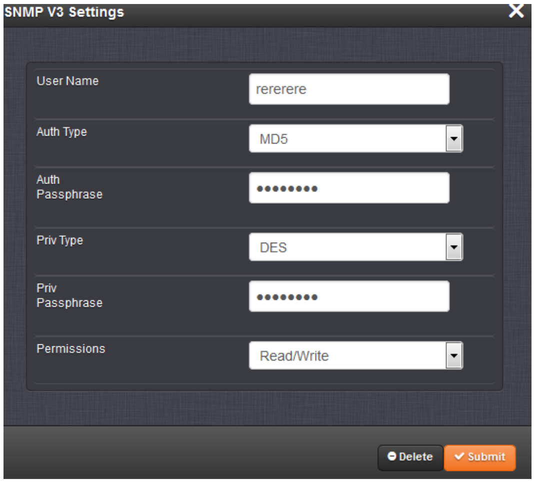
Configuration using web browser

SNMP Community/Username field

- Can be **1 to 31** characters

2. SNMPv3 user configuration

A) Newer web browser



SNMP V3 Settings

User Name	rererere
Auth Type	MD5
Auth Passphrase	••••••••
Priv Type	DES
Priv Passphrase	••••••••
Permissions	Read/Write

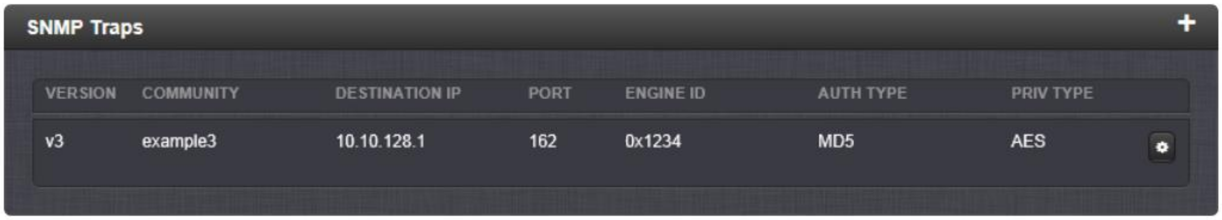
- **SNMP user names** should be **between 1 and 31** characters in length
- Auth Password must be between 1 and 31 characters in length.
- Priv Passphrase must be between 1 and 31 characters in length.

SNMP trap configuration/operation

- **Refer to S/S 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

A) SNMPV3 traps (note the SecureSync sends “traps” - not “informs)

- Refer to: http://www.net-snmp.org/tutorial/tutorial-5/commands/snmptrap-v3.html



SNMP Traps

VERSION	COMMUNITY	DESTINATION IP	PORT	ENGINE ID	AUTH TYPE	PRIV TYPE
v3	example3	10.10.128.1	162	0x1234	MD5	AES

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

- : Can be **1 to 31**

EngineID field for SNMPv3 traps

Refer also to: http://www.net-snmp.org/tutorial/tutorial-5/commands/snmptrap-v3.html for info on “Traps” versus “Informs” (SecureSync sends “Traps”- not “Informs”)., Scroll down to “**SNMPv3 TRAPs**”)

- **For SNMP Gets/Sets**: The SNMP Manager sends its EngineID to the SecureSync. There is no need to define an EngineID in the SecureSync for gets/sets
- **For SNMP traps**: The EngineID field needs to contain an EngineID value in order to send any traps. Apparently, depending on what SNMP Manager is being used, this field may need to be 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

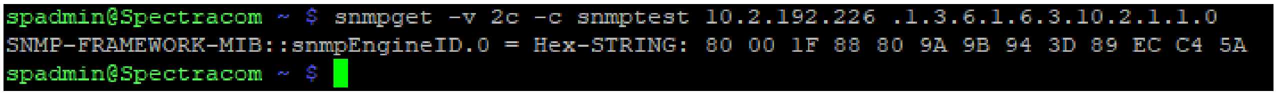
Currently,the customer must read our engineID from MIB using and SNMPGET (which is inconvenient)

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

A) 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 **snmpget -v 2c -c zzzzz xxx.xxx.xxx.xxx .1.3.6.1.6.3.10.2.1.1.0** <enter> (where "**zzzzz**" is the community name of the V2c user and where "**xxx.xxx.xxx.xxx**" is the IP address of the SecureSync).

   See the example response below (note the string **value** will vary):



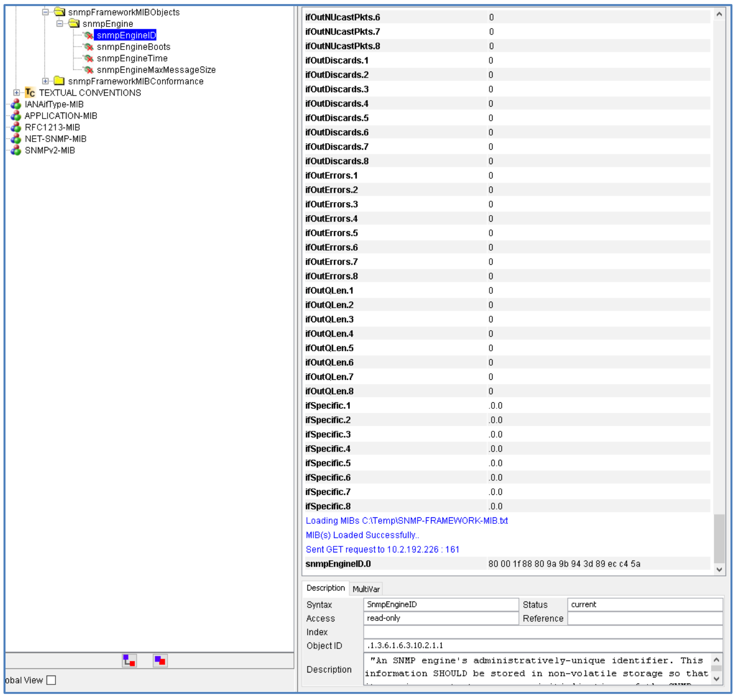
```
spadmin@Spectracom ~ $ snmpget -v 2c -c snmptest 10.2.192.226 .1.3.6.1.6.3.10.2.1.1.0
SNMP-FRAMEWORK-MIB::snmpEngineID.0 = Hex-STRING: 80 00 1F 88 80 9A 9B 94 3D 89 EC C4 5A
spadmin@Spectracom ~ $
```

4) 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"**

B) 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



ifOutNUcastPkts.6	0
ifOutNUcastPkts.7	0
ifOutNUcastPkts.8	0
ifOutDiscards.1	0
ifOutDiscards.2	0
ifOutDiscards.3	0
ifOutDiscards.4	0
ifOutDiscards.5	0
ifOutDiscards.6	0
ifOutDiscards.7	0
ifOutDiscards.8	0
ifOutErrors.1	0
ifOutErrors.2	0
ifOutErrors.3	0
ifOutErrors.4	0
ifOutErrors.5	0
ifOutErrors.6	0
ifOutErrors.7	0
ifOutErrors.8	0
ifOutQLen.1	0
ifOutQLen.2	0
ifOutQLen.3	0
ifOutQLen.4	0
ifOutQLen.5	0
ifOutQLen.6	0
ifOutQLen.7	0
ifOutQLen.8	0
ifSpecific.1	.0.0
ifSpecific.2	.0.0
ifSpecific.3	.0.0
ifSpecific.4	.0.0
ifSpecific.5	.0.0
ifSpecific.6	.0.0
ifSpecific.7	.0.0
ifSpecific.8	.0.0

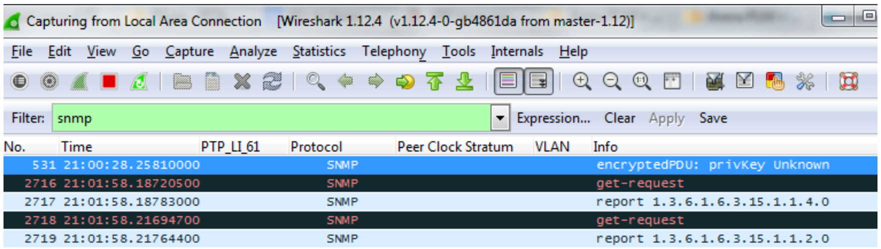
```
Loading MIBs C:\Temp\SNMP-FRAMEWORK-MIB.txt
MIB(s) Loaded Successfully..
Sent GET request to 10.2.192.226 : 161
```

snmpEngineID.0	80 00 1f 88 80 9a 9b 94 3d 89 ec c4 5a

Syntax	SnmpEngineID	Status	current
Access	read-only	Reference	
Index			
Object ID	.1.3.6.1.6.3.10.2.1.1		
Description	"An SNMP engine's administratively-unique identifier. This information SHOULD be stored in non-volatile storage so that		

1) Take the returned value,
2) Add "0x" to the front of this value and remove all the spaces between each two character value
3) Place this full value (with no spaces) in the SecureSync's SNMPv3 EngineID field

- SNMPv3 traps will only be sent from the SecureSync if an EngineID (beginning with “0x”) field has been populated when configuring v3 traps in the SecureSync. Without a valid engineID (which is then pasted into the V3 trap section of the SecureSync) no v3 traps are sent.
- in at least v5.7.1 and below, the SecureSync enforces Auth, Priv in SNMPv3 (can’t configure no auth,no priv).
- The Manager sends a message to the SecureSync when it’s being setup for SNMPv3 users in order to generate the contextID/engineID.


Capturing from Local Area Connection [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

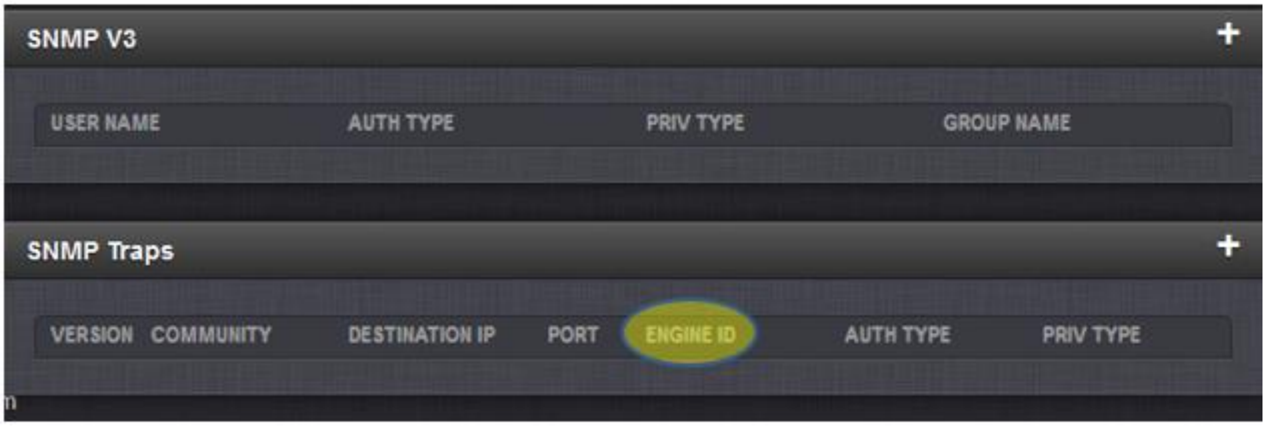
Filter: snmp

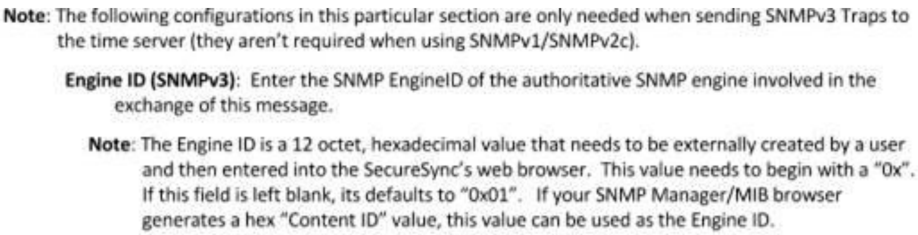
```
No.   Time               PTP_LI_61  Protocol  Peer Clock Stratum  VLAN  Info
  531 21:00:28.25810000             SNMP                                encryptedPDU: privKey Unknown
 2716 21:01:58.18720500             SNMP                                get-request
 2717 21:01:58.18783000             SNMP                                report 1.3.6.1.6.3.15.1.1.4.0
 2718 21:01:58.21694700             SNMP                                get-request
 2719 21:01:58.21764400             SNMP                                report 1.3.6.1.6.3.15.1.1.2.0
```

- The engineID can’t just be an “arbitrary” value such as “ox1a” for example.

A) Web browser

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.

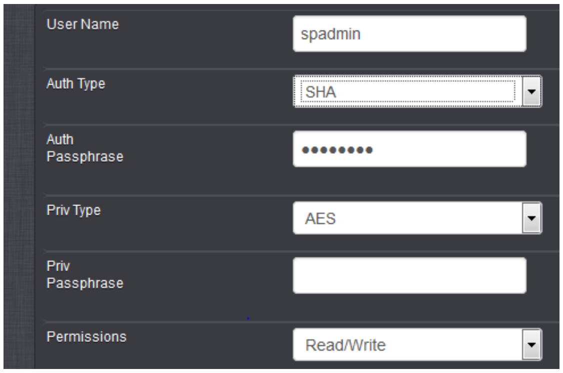
Note: The Engine ID is a 12 octet, hexadecimal value that needs to be externally created by a user and then entered into the SecureSync’s web browser. This value needs to begin with a “0x”. If this field is left blank, its defaults to “0x01”. If your SNMP Manager/MIB browser generates a hex “Content 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.~~

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

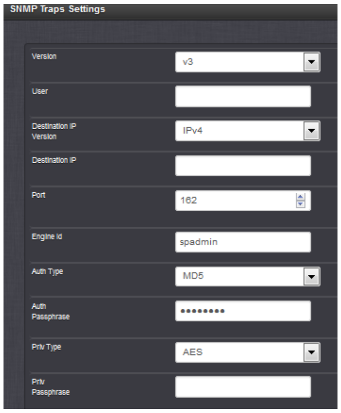
Management -> **SNMP Setup** page of the browser, to read or read/write (as shown in the screenshot below). If the user wants to setup the ‘Trap only’ user, it does not have to be reflected on the SecureSync and will need to be setup on the receiving end (SNMP Manager). The SNMP traps section of the 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



SNMP Traps Settings

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. f this capability is eliminated as a security lockdown, please let me know and I'll pass it along.

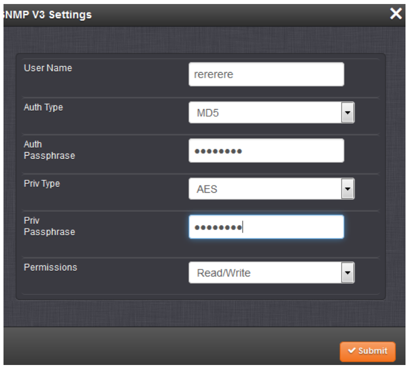
A **Keith’s response:** I believe the reason that noauth/nopriv is not supported is because it’s an unsecure connection (if a secure connection isn’t a concern, can just use SNMPv1/v2c. No need to use SNMPv3).

“User name” field

- can be **1 to 31 characters**

Setting up ManageEngine SNMP Manager to work with SNMPv3 traps from SecureSync

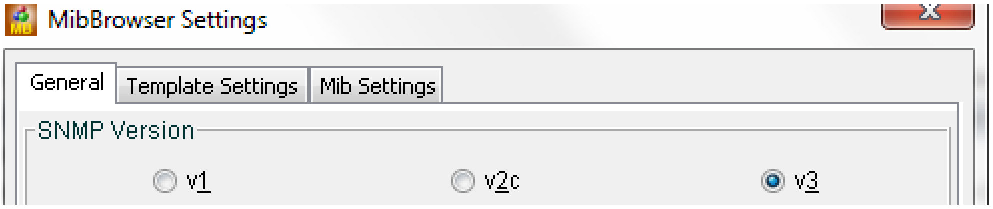
1. In the **Management** -> **SNMP** page of the SecureSync, Add/Configure a new V3 user (note this is not required to send a v3 trap that wireshark can see, but is required for the SNMP manager to be able to authenticate/see the trap). Use the same user name that is used for the V3 user name (example below uses "**rererere**")



NMP V3 Settings

User Name: rererere
Auth Type: MD5
Auth Passphrase: ••••••••
Priv Type: AES
Priv Passphrase: ••••••••
Permissions: Read/Write

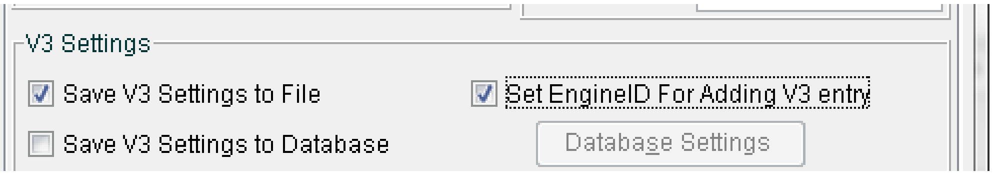
2. Select "**V3**" at the top of the top of the "General tab" of the ManageEngine GUI



MibBrowser Settings

SNMP Version: ○ v1 ○ v2c ● v3

3. Select the checkboxes for both "**Save V3 Settings to file**" and "**Set EngineID for adding V3 entry**"

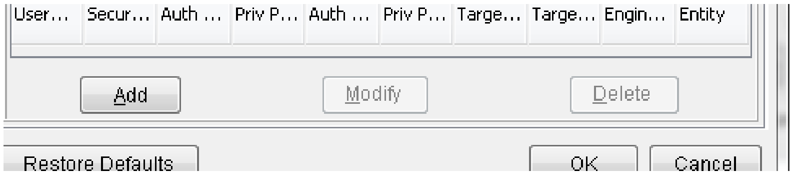


V3 Settings

☑ Save V3 Settings to File ☑ Set EngineID For Adding V3 entry

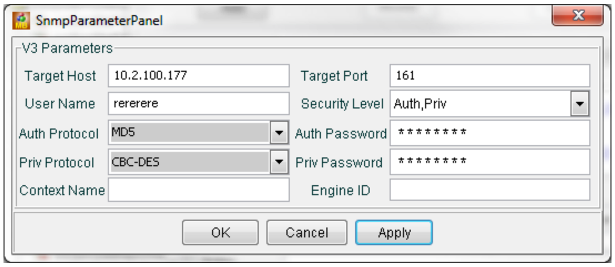
□ Save V3 Settings to Database

4. Press the "**Add**" button in the bottom left corner to add a "v3 user"



User…	Secur…	Auth …	Priv P…	Auth …	Priv P…	Targe…	Targe…	Engin…	Entity

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.

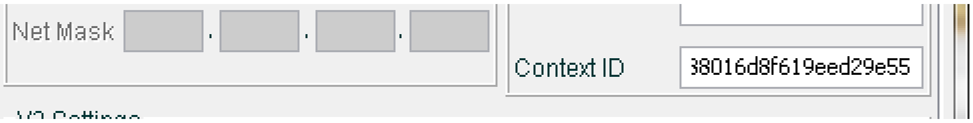


SnmpParameterPanel

V3 Parameters

Target Host	10.2.100.177	Target Port	161
User Name	rererere	Security Level	Auth,Priv
Auth Protocol	MD5	Auth Password	********
Priv Protocol	CBC-DES	Priv Password	********
Context Name		Engine ID	

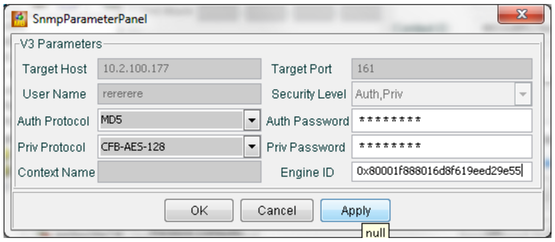
6. With Auth and Priv protocols and passwords matching the SecureSync's SNMPv3 user section, the context ID field in the main page (General tab) of the manageengine gui will be generated.



Net Mask . . .

Context ID 38016d8f619eed29e55

7. 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).

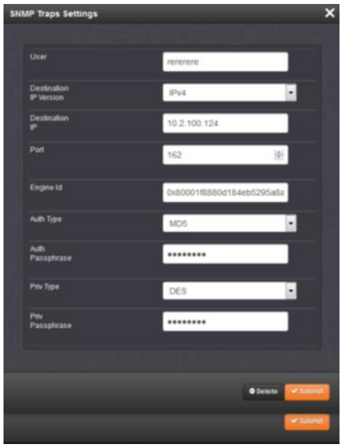


SnmpParameterPanel

V3 Parameters

Target Host 10.2.100.177
Target Port 161
User Name rererere
Security Level Auth,Priv
Auth Protocol MD5
Auth Password ********
Priv Protocol CFB-AES-128
Priv Password ********
Context Name
Engine ID 0x80001f888016d8f619eed29e55

8. 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.



SNMP Traps Settings

User rererere
Destination IP Version IPv4
Destination IP 10.2.100.124
Port 162
Engine Id 0x80001f8880d184eb5295a8a
Auth Type MD5
Auth Passphrase ••••••••
Priv Type DES
Priv Passphrase ••••••••

B) SNMPv1 and SNMPv2c

SNMP Community/User field

- 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 increaded the port restriction range:
  - [JIRA Ticket SSS-271] - SNMP Trap Port restriction should be **0-65535**, instead of 0-1023

(v4.7.0 and below only) 6/28/11 KW- In all versions prior to version 4.7.0, the SNMP trap destination value wasn't displayed or able to be changed in the web browser. It was set to port 162 without the ability to change it to another desired value.

Besides updating the software to a newer version, a work-around allowed the port value to be changed via the CLI.

Email DL sent to Todd Belcher on 6/27/11

Hello Todd,
I have some information for you. It is a description of how you can work around the bug and still send traps to a different port.

1) Log in to the unit via the command line (telnet, SSH, or serial port on front panel) as 'spadmin'
2) Change directory into the config directory (cd config)
3) Edit the snmpd.conf file using vi (vi snmpd.conf)
4) Find the "trapsess" line in the configuration file and cange the port to the desired value.
5) Save the file (:wq)
6) Disable/enable SNMP from the Web UI.

If you do not know how to use 'vi', then you will need to ftp the file off the unit, change the port with an editor you know how to use, then ftp the file back onto the unit.

Deleting a value from the Network -> SNMP Setup page, Communities tab

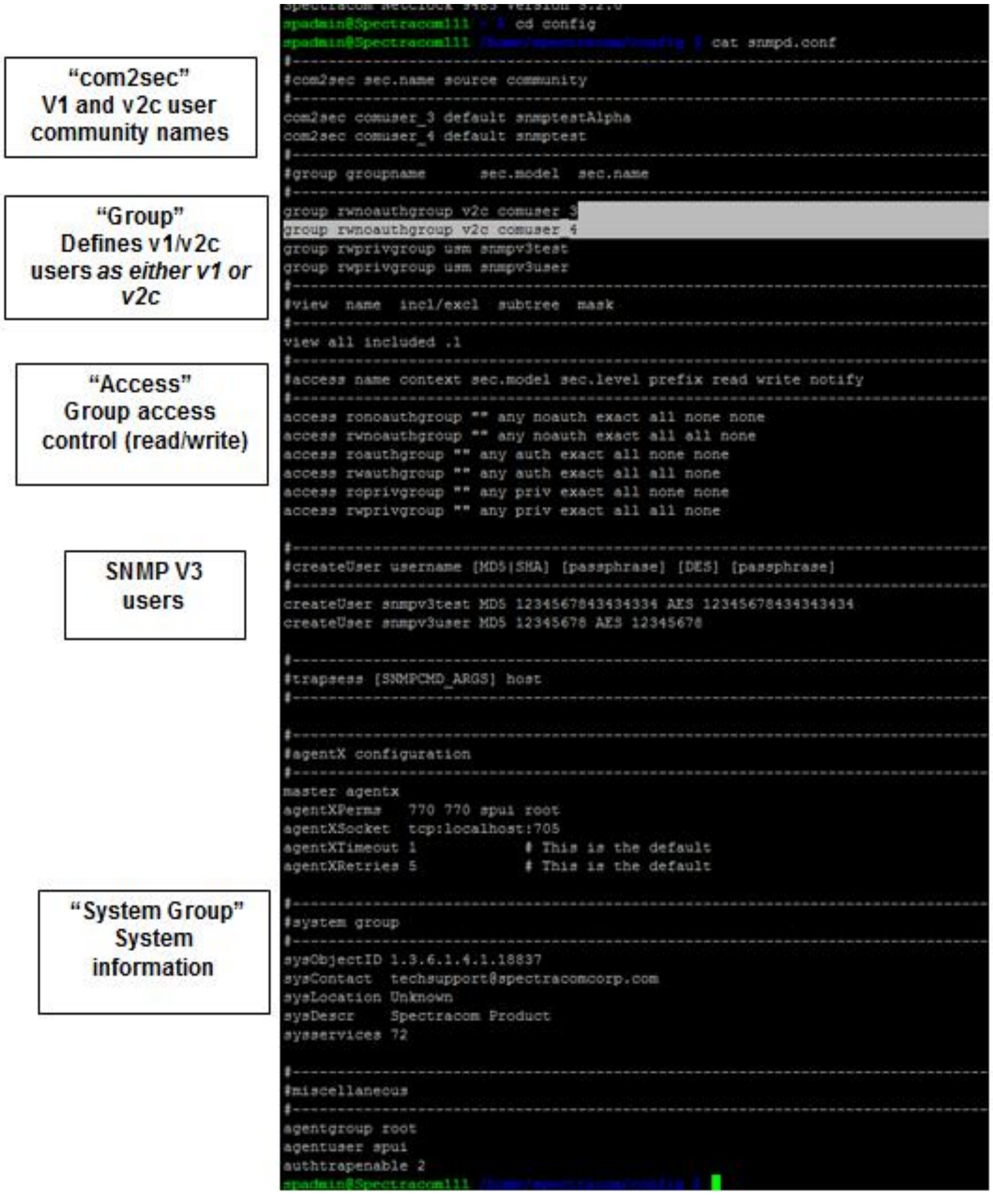
Q When we are configuring the SNMP Communities (1v/2vc), I accidentally enter an IP address into "IPv4 Network Access" field and I would like to remove the IP address. However, I am not able to remove the IP address. Please assist if this is a bug or normal behavior. Please do also advice how I can remove the unwanted IP address in the "IPv4 Network Access" field. Thus, please assist to check with Spectracom and reply asap.

A. Keith's response: I was able to enter a value in this field and then able to delete it. But it 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

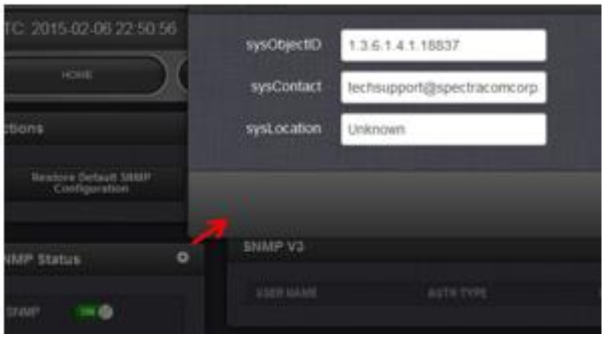
```
Spectracom NetClock 9483 version 5.2.0
spadmin@Spectracom111 ~ $ cd config
spadmin@Spectracom111 [illegible] $ cat snmpd.conf
#-------------------------------------------------------------------------------
#com2sec sec.name source community
#-------------------------------------------------------------------------------
com2sec comuser_3 default snmptestAlpha
com2sec comuser_4 default snmptest
#-------------------------------------------------------------------------------
#group groupname      sec.model  sec.name
#-------------------------------------------------------------------------------
group rwnoauthgroup v2c comuser_3
group rwnoauthgroup v2c comuser_4
group rwprivgroup usm snmpv3test
group rwprivgroup usm snmpv3user
#-------------------------------------------------------------------------------
#view  name  incl/excl  subtree  mask
#-------------------------------------------------------------------------------
view all included .1
#-------------------------------------------------------------------------------
#access name context sec.model sec.level prefix read write notify
#-------------------------------------------------------------------------------
access ronoauthgroup "" 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 roprivgroup "" 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 12345678434343434
createUser snmpv3user MD5 12345678 AES 12345678

#-------------------------------------------------------------------------------
#trapsess [SNMPCMD_ARGS] host
#-------------------------------------------------------------------------------

#-------------------------------------------------------------------------------
#agentX configuration
#-------------------------------------------------------------------------------
master agentx
agentXPerms   770 770 spui root
agentXSocket  tcp:localhost:705
agentXTimeout 1            # This is the default
agentXRetries 5            # This is the default

#-------------------------------------------------------------------------------
#system group
#-------------------------------------------------------------------------------
sysObjectID 1.3.6.1.4.1.18837
sysContact  techsupport@spectracomcorp.com
sysLocation Unknown
sysDescr    Spectracom Product
sysservices 72

#-------------------------------------------------------------------------------
#miscellaneous
#-------------------------------------------------------------------------------
agentgroup root
agentuser spui
authtrapenable 2
spadmin@Spectracom111 [illegible] $
```

***SysOlbjectID, SysContact and SysLoction fields

SysOlbjectID

- **SysObjectID**: The three values can be changed from the default values if desired.

1. Click on **Gear** icon next to “**SNMP Status**”



sysObjectID: 1.3.6.1.4.1.18837
sysContact: techsupport@spectracomcorp
sysLocation: Unknown

SysLocation field

SysName field (unit’s hostname in SNMP)

- Was made configurable (Mantis case 3095) in version 5.3.0 (I believe)
  - Wasn’t a user-configurable field in earlier versions of software.
- This field reports the assigned hostname.
- This field is only updated when the unit is rebooted, or if SNMP is stopped/restarted. If DNS changes the name thereafter, SNMP can be stopped/restarted for the new name to be updated.
  - Keith added Mantis case 3099 to have it change automatically, but Dave Sohn responded its working as it should. SNMP won’t see the change until SNMP is restarted.

Ability to enable/disable SNMP via the CLI interface

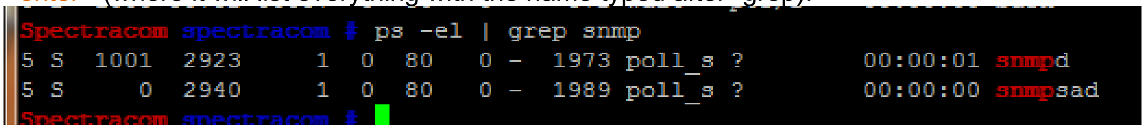
Q. (from Wade Sober) Is there a way to enable SNMP through the command line interface on SecureSync?

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 SNMPD and SNMPSAD, our sub-agent) is running, type **ps -el | grep *snmp*** <enter> (where it will list everything with the name typed after “grep):



```
Spectracom spectracom # ps -el | grep snmp
5 S  1001  2923     1  0  80   0 -  1973 poll_s ?        00:00:01 snmpd
5 S     0  2940     1  0  80   0 -  1989 poll_s ?        00:00:00 snmpsad
Spectracom spectracom #
```

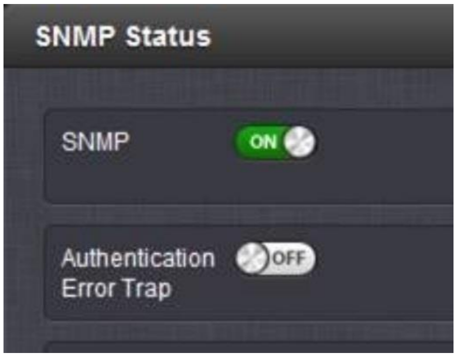
Note: when the SNMP enable/disable switch is off, both snmpd and snmpsad should be stopped (not listed)

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:



SNMP Status

SNMP ON

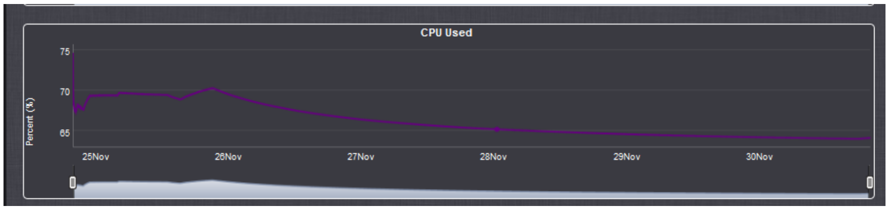
Authentication Error Trap OFF

CPU usage (CPU used) / Processor usage

- Refer to Mantis case 3029.
- CPU usage is a comparison of processor “use time” versus “rest time”.

CPU usage graph and raw data

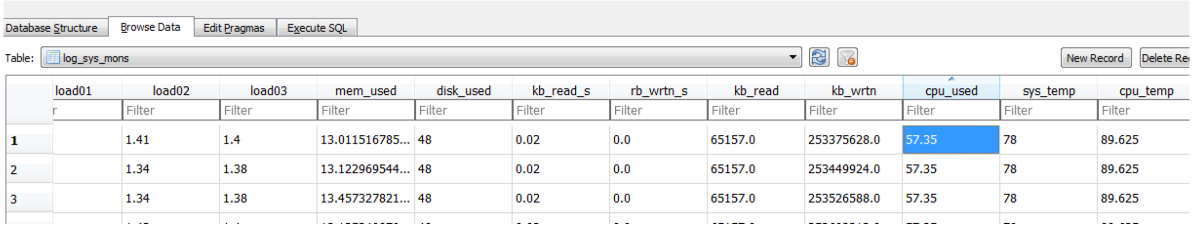
- Located at the bottom of the **Tools** ->**System Monitor** page of the newer browser (not available in classic interface).
- Graph data is captured/obtained/logged about once a minute, SO a high burst of short duration CPU activity might NOT be registered on the Log graphs/data for the database, but still occur.



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 additonal info on the database).**
  - Data for this graph is is located (can be viewed) in the “**log_sys_mons**” table, “**cpu_used**” column
  - CPU usage is captured about once a minute (at about the 30 second mark). SO a high burst of short duration

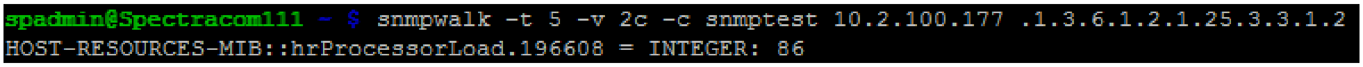
CPU activity might NOT be registered on the Log graphs/data for the database, but still occur.



	load01	load02	load03	mem_used	disk_used	kb_read_s	rb_wrtn_s	kb_read	kb_wrtn	cpu_used	sys_temp	cpu_temp
	r	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
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 snmptest 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 snmptest 10.2.100.177 .1.3.6.1.2.1.25.3.3.1.2
HOST-RESOURCES-MIB::hrProcessorLoad.196608 = INTEGER: 86
```

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

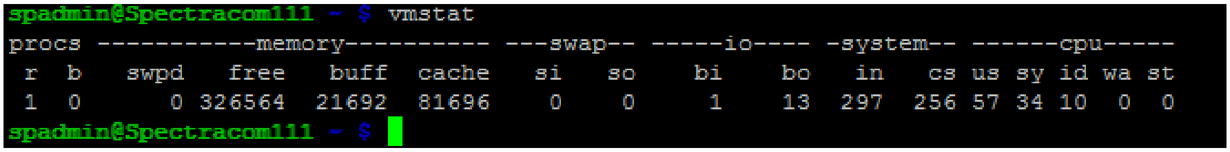
raw idle cpu time: .1.3.6.1.4.1.2021.11.53.0

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%)

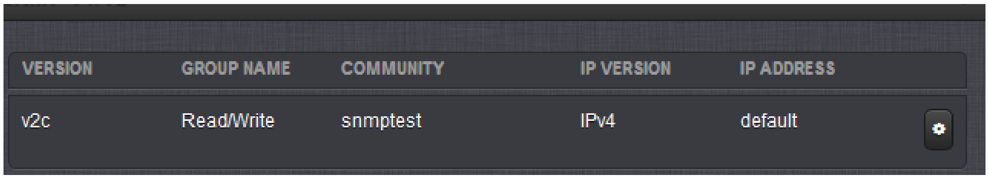
wa: Time spent waiting for IO. Prior to Linux 2.5.41, shown as zero.

**Using Linux to perform SNMPWalks SNMPGets SNMPTrap

- Note: To perform an SNMPwalk, SNMPget or receive traps in linux, use another SecureSync

(**Note**: This is also available as **spadmin**. So customers are able to use one SecureSync to hit another one via SNMP)

Important note: Make sure that the SecureSync being used to get in to the destination SecureSync is configured in the Destination SecureSync an SNMP user (or use IP address value of **default**) as shown below**:**



VERSION	GROUP NAME	COMMUNITY	IP VERSION	IP ADDRESS
v2c	Read/Write	snmptest	IPv4	default

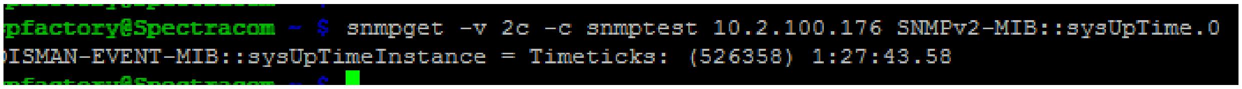
- Refer to: http://en.wikipedia.org/wiki/Net-SNMP
  https://docs.oracle.com/cd/E19201-01/820-6413-13/SNMP_commands_reference_appendix.html#50446362_54136

Example SNMPGets:

- Use the “watch –n” command at the beginning to perform the SNMPGet repeatedly

A) Get the system uptime

(Type the following): **snmpget -v 2c -c snmptest 10.2.192.226 SNMPv2-MIB::sysUpTime.0**



```
pfactory@Spectracom ~ $ snmpget -v 2c -c snmptest 10.2.100.176 SNMPv2-MIB::sysUpTime.0
ISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (526358) 1:27:43.58
pfactory@Spectracom ~ $
```

B) Get the NTP’s current status

(Type the following): **snmpget -v 2c -c snmptest 10.2.192.226 .1.3.6.1.4.1.18837.3.3.2.1.0**

Note: the numbers at the end of the snmpget (after the IP address) is the full OID number, **plus a “.0”** added to the end.

C) Desire to perform repeated SNMP Gets (same get repeatedly)

- Use linux “**watch –n**” before the snmpget command

(Example to run once per second): **watch -n1 snmpget -v 2c -c snmptest 10.2.192.226 1.3.6.1.4.1.18837.3.3.2.1.0**

Note: the time at the top will increment each second

D) 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**

E) SNMPv3bulkget

(type) **watch -n 1 snmpbulkget -v3 -t10 -u snmpv3user -l authPriv -a MD5 -A 12345678 -x AES -X 12345678 10.2.192.226 .1.3.6.1.4.1.18837**

Example SNMPWalks:

- CTRL + C to stop the output (standard for Linux) (or hold left mouse button and slide mouse either left or right to pause).
- Reports OIDs and values only (not object names)
- Can walk from any point. Whatever portion of the Object number is entered, it will get everything after that value (such as 18837.3 will find everything after this number)
- Use the “watch –n” command at the beginning to perform the walk repeatedly

(Syntax): snmpwalk -t 5 -mALL -v 2c -c public *snmp_agent_Ip_address* sysobjectID

1. Walk the entire MIBs (with a 5 second timeout)

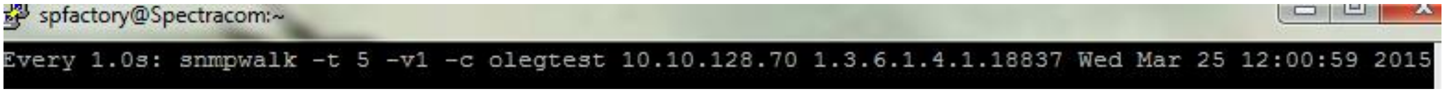
A) Just once

(Type): **snmpwalk -t5 -v2c -c snmptest 10.2.192.226 1.3.6.1.4.1.18837**

B) Example to repeatedly walk the entire MIB, once per second:

(Type): **watch -n1 snmpwalk -t5 -v2c -c snmptest 10.2.192.226 1.3.6.1.4.1.18837**

Note: the time at the top will increment each second



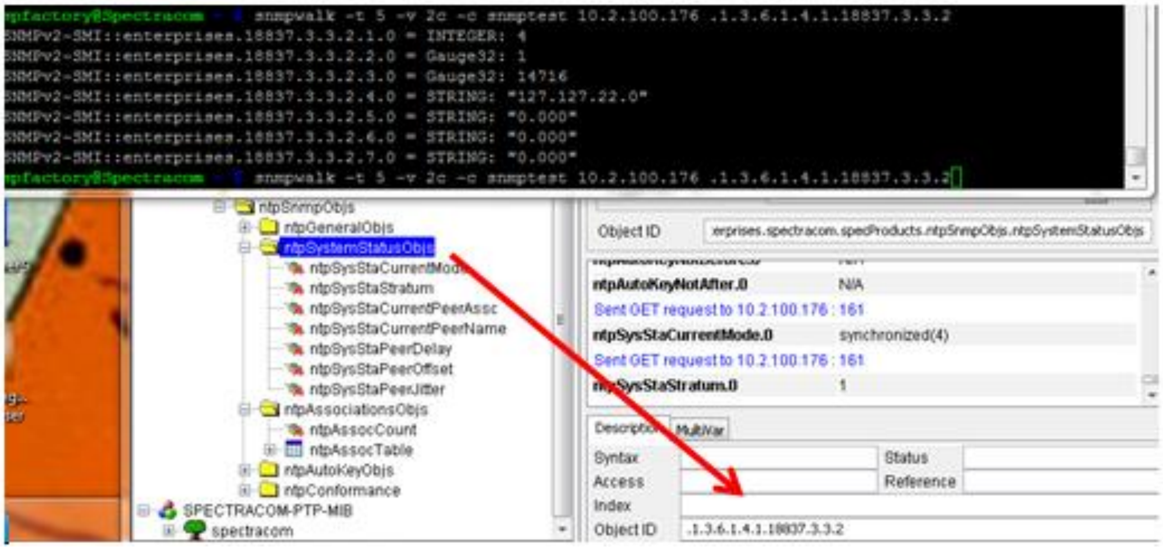
```
Every 1.0s: snmpwalk -t 5 -v1 -c olegtest 10.10.128.70 1.3.6.1.4.1.18837 Wed Mar 25 12:00:59 2015
```

C) Walk just one MIB such as NTPSystemStatysObjsMIB (with a 5 second timeout)

(Type) **snmpwalk -t 5 -v 2c -c snmptest 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)



```
pfactory@Spectracom ~ $ snmpwalk -t 5 -v 2c -c snmptest 10.2.100.176 .1.3.6.1.4.1.18837.3.3.2
SNMPv2-SMI::enterprises.18837.3.3.2.1.0 = INTEGER: 4
SNMPv2-SMI::enterprises.18837.3.3.2.2.0 = Gauge32: 1
SNMPv2-SMI::enterprises.18837.3.3.2.3.0 = Gauge32: 14716
SNMPv2-SMI::enterprises.18837.3.3.2.4.0 = STRING: "127.127.22.0"
SNMPv2-SMI::enterprises.18837.3.3.2.5.0 = STRING: "0.000"
SNMPv2-SMI::enterprises.18837.3.3.2.6.0 = STRING: "0.000"
SNMPv2-SMI::enterprises.18837.3.3.2.7.0 = STRING: "0.000"
pfactory@Spectracom ~ $ snmpwalk -t 5 -v 2c -c snmptest 10.2.100.176 .1.3.6.1.4.1.18837.3.3.2
```

```
ntpSnmpObjs
  ntpGeneralObjs
  ntpSystemStatusObjs
    ntpSysStaCurrentMode
    ntpSysStaStratum
    ntpSysStaCurrentPeerAssc
    ntpSysStaCurrentPeerName
    ntpSysStaPeerDelay
    ntpSysStaPeerOffset
    ntpSysStaPeerJitter
  ntpAssociationsObjs
    ntpAssocCount
    ntpAssocTable
  ntpAutoKeyObjs
  ntpConformance
SPECTRACOM-PTP-MIB
  spectracom
```

Object ID: erprises.spectracom.specProducts.ntpSnmpObjs.ntpSystemStatusObjs

```
ntpAutoKeyNotAfter.0                     N/A
Sent GET request to 10.2.100.176 : 161
ntpSysStaCurrentMode.0                   synchronized(4)
Sent GET request to 10.2.100.176 : 161
ntpSysStaStratum.0                       1
```

Syntax:
Status:
Access:
Reference:
Index:
Object ID: .1.3.6.1.4.1.18837.3.3.2

D) SNMPv3 walks

(type) **snmpwalk -v3 -t10 -u snmpv3user -l authPriv -a MD5 -A 12345678 -x AES -X 12345678 10.2.192.226 .1.3.6.1.4.1.18837**

E) Continuous SNMPv3 walk

(type) **watch -n1 snmpwalk -v3 -t10 -u snmpv3user -l authPriv -a MD5 -A 12345678 -x AES -X 12345678 10.2.192.226 .1.3.6.1.4.1.18837**

(type) **watch -n 1 snmpwalk -v3 -t10 -u snmpv3test -l authPriv -a MD5 -A 12345678 -x AES -X 12345678 10.2.192.226 .1.3.6.1.4.1.18837**

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?

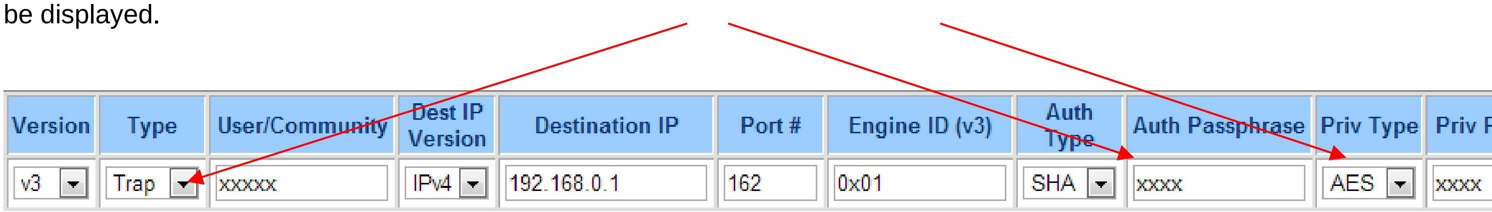
A. **Reply from Dave Sohn (10/29/12)** There is no planned mechanism to enable SNMP directly via the CLI. We are adding the capability to save and restore configurations via the CLI, which would include SNMP. Those configurations could be used as a “golden” configuration to be loaded on deployed units.

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 P
v3	Trap	xxxxx	IPv4	192.168.0.1	162	0x01	SHA	xxxx	AES	xxxx

SNMPv3 (Secure SNMP)

“EngineID” field

- Required for SNMPv3 traps
    - Not required/available for SNMPv3 Gets and Sets (not in SecureSync’s User configurations)

From Wikipedia:

The snmpEngineID has a length of 12 octets.

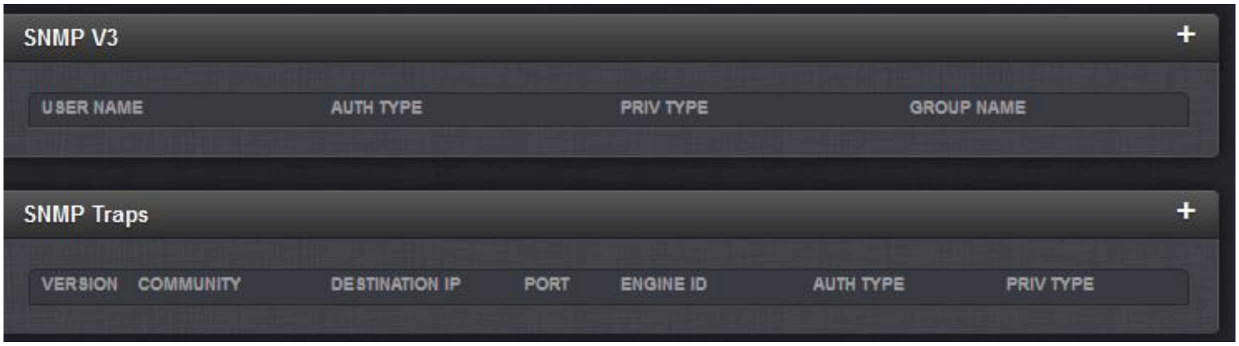
The first four octets are set to the binary equivalent of the agent's SNMP management private enterprise number as assigned by the Internet Assigned Numbers Authority (IANA). For example, if Acme Networks has been assigned {enterprises 696 }, the first four octets would be assigned '000002b8'H.

The remaining eight octets are determined via one or more enterprise-specific methods. Such methods must be designed so as to maximize the possibility that the value of this object willbe 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.

Newer browser: **Management** -> **SNMP Management** page of the browser, SNMP v3 and SNMP v3 Traps



Authentication type (AuthProtocol) / Privilege (privProtocol) terms

- SecureSync is "**authPriv**" only (in that it requires both Authentication and encryption)
  - **noAuthnoPriv:** Messages can be sent unauthenticated and unencrypted (this mode is unsecure/not supported in SecureSync)
  - "**authNoPriv**" Messages can be sent authenticated but unencrypted (this most is not completely secure/not supported in SecureSync)
  - "**authPriv**": Messages can only be sent authenticated and encrypted (This is the only one supported in SecureSync because its completely secure)

Authentication ("Auth Type" field)

- **Auth Type:** supports **MD5** or **SHA** (no selection available for '**none**')

Encryption algorithms supported ("Priv Type" field): DES or AES

- AES is 128 bit (no plans to update to 256 bit): refer to https://groups.google.com/forum/#!msg/mailing.unix.net-snmp-users/V_uVWkWUQx4/mqneIC5jC1EJ

AES support (such as 128-bit, 192-bit, 256-bit) with Net-SNMP software package
(As of at least Sept, 2017) 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"
Or 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"

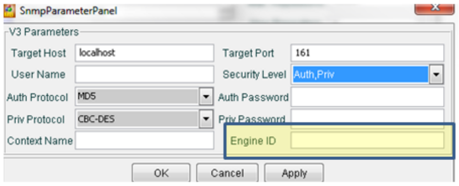
- Update: this condition was addressed in software update version 5.1.7

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.~~

“Engine ID” field with 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



Target Host: localhost
Target Port: 161
User Name:
Security Level: Auth,Priv
Auth Protocol: MD5
Auth Password:
Priv Protocol: CBC-DES
Priv Password:
Context Name:
Engine ID:

4) Enter this same value in the SNMPV3 EngineID field in the time server

Note: a default value may be entered automatically in this field. If not, can manually enter a value (such as “**80001f8880d7c92a1f7ed4b50**” for example)

Number of available EngineID characters (field length)

- **Versions 4.8.9 and above**: 50 characters
- **Versons 4.8.8 and below**: 32 characters

Obtaining unit’s Model, Serial Number and version via SNMP

- **Model info**:
- **Serial Number**:
- **Installed software version** (ssSysStaVersion):

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.

SNMP for installed Option Cards

- As of May 2013, the only Option Card with SNMP functionality is the Model 1204-12 PTP Option Card.
- One of the six MIB files we send define OID for SNMP “gets” for the PTP Card (there are no available sets or traps for this Option Cards)

Q Are there any OIDs we can poll for the info about cards inserted in these devices?
A. There are currently no SNMP OIDs associated with any of the Option Cards (there is no SNMP functionality associated with any the Option Cards nor is any planned at this time).

Update to this answer (7 May 13): As mentioned in the bullets above, the Model 1204-12 PTP Option Card does have a dedicated MIB file for SNMP gets. As of at least Nov 2014, this is the only Option Card that has PTP functionality.

Note (as of at least Dec 2014, versions 5.1.7 and below) The PTP MIB file doesn't work with the 1204-32 Gb PTP card. It is only compatible with the 1204-12 10/100 PTP card.

Desire to know if a network port is up or down

- Refer to the SecureSync SNMP Tech Note: EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\SNMP or to the NetClock SNMP tech note: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\SNMP
- Web browser doesn't report the Operational state of a port (as of at least 4.8.9 anyways).
- Port state can be read using general SNMP MIB RFC 1213 (as of at least 4.8.9, a port being down is not vailable 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

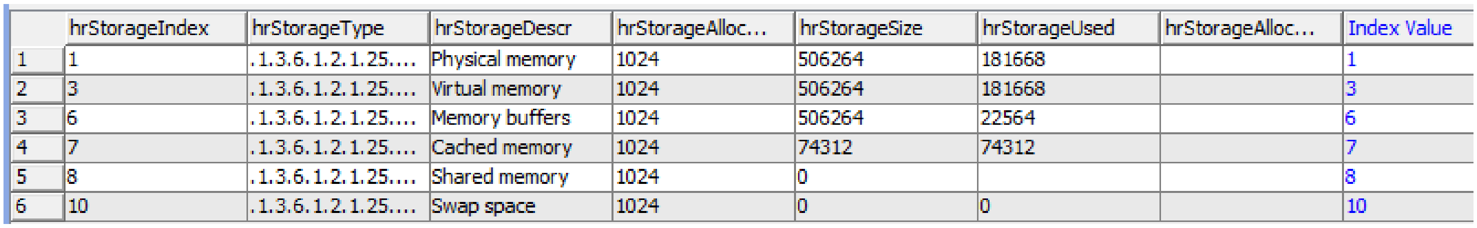
CPU:
percentage of user CPU time: .1.3.6.1.4.1.2021.11.9.0
raw user cpu time: .1.3.6.1.4.1.2021.11.50.0
percentages of system CPU time: .1.3.6.1.4.1.2021.11.10.0
raw system cpu time: .1.3.6.1.4.1.2021.11.52.0
percentages of idle CPU time: .1.3.6.1.4.1.2021.11.11.0
raw idle cpu time: .1.3.6.1.4.1.2021.11.53.0
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

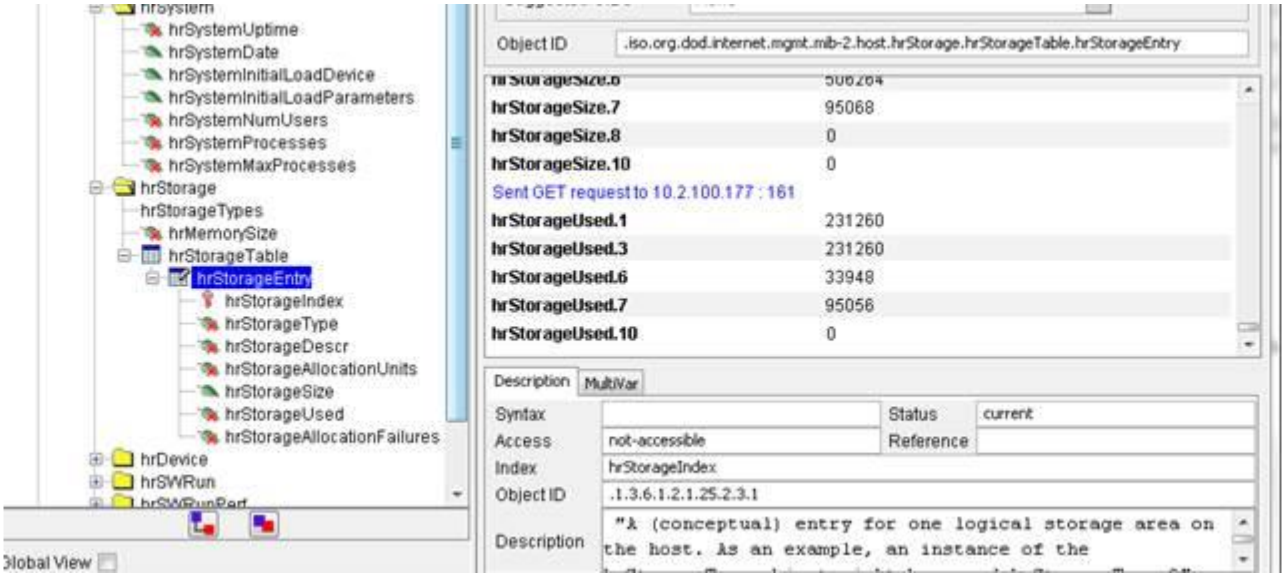


	hrStorageIndex	hrStorageType	hrStorageDescr	hrStorageAlloc…	hrStorageSize	hrStorageUsed	hrStorageAlloc…	Index Value
1	1	.1.3.6.1.2.1.25.…	Physical memory	1024	506264	181668		1
2	3	.1.3.6.1.2.1.25.…	Virtual memory	1024	506264	181668		3
3	6	.1.3.6.1.2.1.25.…	Memory buffers	1024	506264	22564		6
4	7	.1.3.6.1.2.1.25.…	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).



Object ID .iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry

```
hrStorageSize.6        506264
hrStorageSize.7        95068
hrStorageSize.8        0
hrStorageSize.10       0
Sent GET request to 10.2.100.177 : 161
hrStorageUsed.1        231260
hrStorageUsed.3        231260
hrStorageUsed.6        33948
hrStorageUsed.7        95056
hrStorageUsed.10       0
```

Syntax
Status current
Access not-accessible
Reference
Index hrStorageIndex
Object ID .1.3.6.1.2.1.25.2.3.1
Description "A (conceptual) entry for one logical storage area on the host. As an example, an instance of the

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

**Testing/Verifying SNMP/Email alerts are enabled and working inside the SecureSync

Testing SNMP traps and email alerts

A) 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.

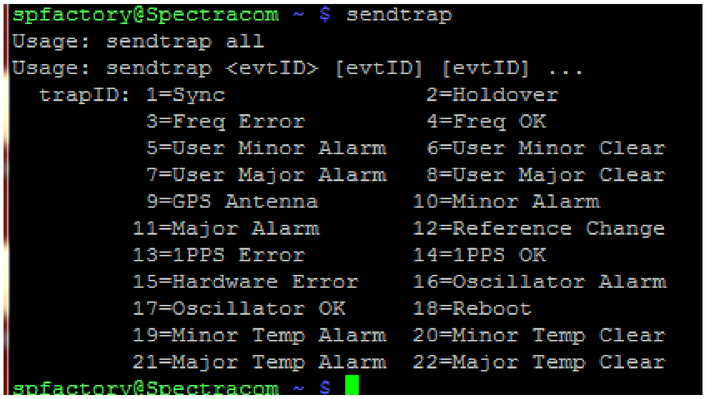
B) testevent all and testevent x commands

Note: The "**testevent**" command can be issued to send SNMP traps only! This command does not test email alerts. Refer to the SecureSync SNMP Tech note for more info on testing traps and email alerts

I believe the testevent may only work using v2 or v2c (not v1 or v3 - this is not confirmed)

1. Versions 5.6.0 and above

- Update versions v5.6.0 added **sendtrap** and **sendtrap all** commands (in addition to earlier **testevent** command)



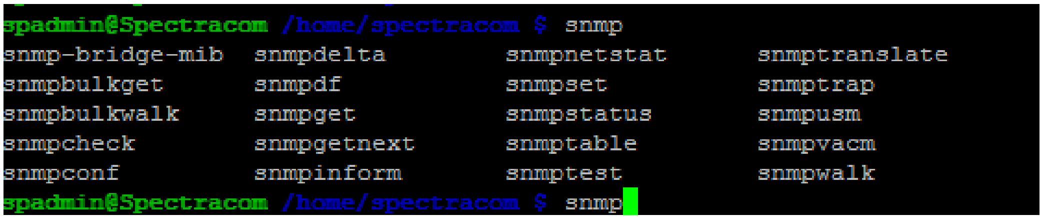
```
spfactory@Spectracom ~ $ sendtrap
Usage: sendtrap all
Usage: sendtrap <evtID> [evtID] [evtID] ...
  trapID: 1=Sync                 2=Holdover
          3=Freq Error           4=Freq OK
          5=User Minor Alarm     6=User Minor Clear
          7=User Major Alarm     8=User Major Clear
          9=GPS Antenna         10=Minor Alarm
         11=Major Alarm         12=Reference Change
         13=1PPS Error          14=1PPS OK
         15=Hardware Error      16=Oscillator Alarm
         17=Oscillator OK       18=Reboot
         19=Minor Temp Alarm    20=Minor Temp Clear
         21=Major Temp Alarm    22=Major Temp Clear
spfactory@Spectracom ~ $
```

2. Versions 5.5.1 and below

testevent and **testevent all** CLI commands

- Can include a number to send a specific trap using the testevent x command.
- Or send all available traps with the **testevent** command

The CLI allows spadmin account to perform various internal SNMP commands



```
spadmin@Spectracom /home/spectracom $ snmp
snmp-bridge-mib   snmpdelta         snmpnetstat       snmptranslate
snmpbulkget       snmpdf            snmpset           snmptrap
snmpbulkwalk      snmpget           snmpstatus        snmpusm
snmpcheck         snmpgetnext       snmptable         snmpvacm
snmpconf          snmpinform        snmptest          snmpwalk
spadmin@Spectracom /home/spectracom $ snmp
```

I recommend using either **Wireshark** on a networked Windows PC, or **tcpdump** on the SecureSync (if its hasn't since been disabled) to verify whether a trap is being sent out of the SecureSync, on the correct ethernet interface (if the Model 1204-06 three port Gb Ethernet option card is installed) with each testevent command. This test eliminates the SNMP Manager and the associated MIBS from 'the equation". Either the traps are being sent out, or not sent out.

The SecureSync (versions 5.2.1 and above) has tcpdump utility installed, allowing the ability to "sniff" the ethernet interface(s) of the SecureSync for any/all packets (such as SNMP traps) going out. Controlling tcpdump is via the CLI interface (an ssh or telnet connection):

(versions 5.2.1 and above only) Can use tcpdump in the CLI interface to see if snmp packets are being sent and which interface they are being sent from

- For additional info about using tcpdump to capture packets, refer to: TCPdump (wireshark for Linux)
  - Some examples below:

To capture data on specific Ethernet interfaces

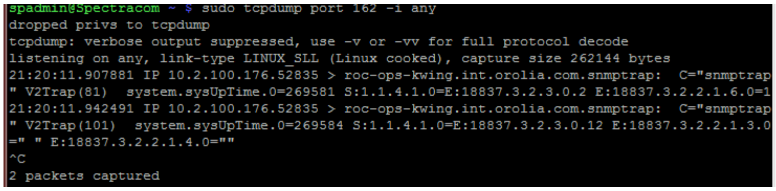
- To capture traffic on **eth1** instead of default port of eth0: **sudo tcpdump -i eth1**
- To capture traffic on more than one interface (such as **eth0 and eth1**): **sudo tcpdump -i eth0 -i eth1**
- To capture traffic on **all interfaces** **sudo tcpdump -i any**

To capture specific data type of packets (such as Radius packets only, snmp only)

Note-omit the word "sudo" in all the below commands for software versions 5.4.5 AND ABOVE

- **NTP** on eth0: **sudo tcpdump port 123** (no need to define interface as eth0 is default)
- **Radius** on eth0: **sudo tcpdump port 1812 and 1813** (no need to define interface as eth0 is default)
- **LDAP** on eth0: **sudo tcpdump port 389 and 636** (no need to define interface as eth0 is default)
- **Syslog** on eth0: **sudo tcpdump port 514** (no need to define interface as eth0 is default)
- **PTP** on eth0: **sudo tcpdump ports 319 and 320** (no need to define interface as eth0 is default)

- **SNMP Traps** sent to **any** Ethernet interface: **sudo tcpdump port 162 -i any**



```
spadmin@Spectracom ~ $ sudo tcpdump port 162 -i any
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
21:20:11.907881 IP 10.2.100.176.52835 > roc-ops-kwing.int.orolia.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.orolia.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
```

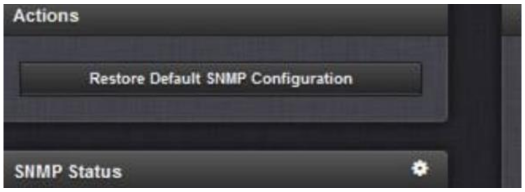
**Troubleshooting / Known issues with SNMP

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 these logs are in the **home/spectracom/log** directory).

Potential fix to SNMP issues- reset just the SNMP configs

- Button in the upper-left corner of the ***Management*** -> ***SNMP Setup*** page resets just the SNMP configs
- Automatically restarts SNMP after reconfiguring.

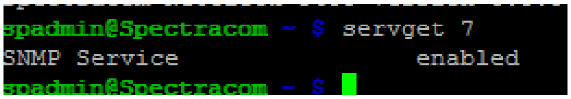
In the upper-left corner of the **Management -> SNMP Setup** page of the newer (black/charcoal) web browser, there is a "**Restore Default SNMP Configuration**" button (as shown below). Unlike a "**clean**" which resets all of the configurations in the SecureSync, this particular button just resets the configs associated with SNMP. The engineer I'm working with recommended resetting and reconfiguring just the SNMP settings. Can you try this on at least one of the SecureSyncs and then try performing the SNMPGet command again? This button won't affect any of the other settings or operations besides SNMP.



If you don't mind trying this, please let me know if an SNMPGet or walk is successful after reconfiguring SNMP. Note there is no need to reboot the unit or to turn SNMP off and back on again before or after reconfiguring SNMP.

1) Verify SNMP is Enabled via the web browser or CLI interface

- ○ **New Web browser**: **Management** -> **SNMP Setup** page
- ○ **CLI command**: **servget 7** <enter> (to disable/enable **servset 7 off** **servset 7 on**)

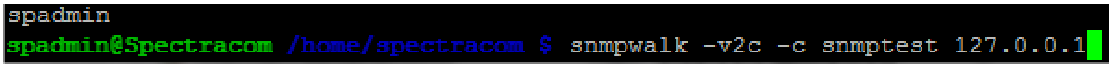


```
spadmin@Spectracom ~ $ servget 7
SNMP Service              enabled
spadmin@Spectracom ~ $
```

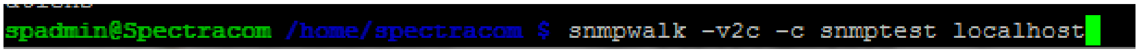
2) SNMPWalk the SecureSync from itself (from the home/spectracom directory)

Note: Spadmin has permissions to do this.

Note: for the "address" at the end of the line, can use either "**localhost**" or "**127.0.0.1**"



```
spadmin
spadmin@Spectracom /home/spectracom $ snmpwalk -v2c -c snmptest 127.0.0.1
```

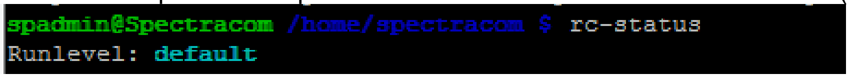


```
spadmin@Spectracom /home/spectracom $ snmpwalk -v2c -c snmptest localhost
```

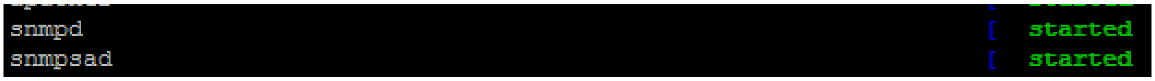
These SNMPWalk commands should walk all of the objects in the SecureSync with a "running" display

3) Perform an "rc-status"

Make sure snmpd and snmpsad are in the list and both indicate "started" (in green)



```
spadmin@Spectracom /home/spectracom $ rc-status
Runlevel: default
```

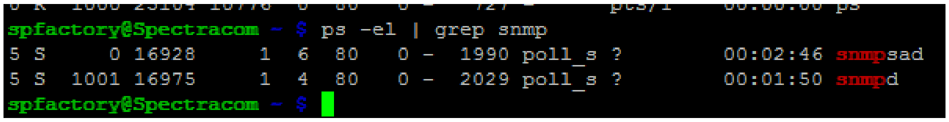


```
snmpd                                                                    [  started
snmpsad                                                                  [  started
```

- If snmp and/or snmpsad aren't listed in the response, SNMP isn't running. Go to the Management -> SNMP Setup page and see if the SNMP slider switch on the left side of the page is ON.
- If snmp and/or snmpsad indicate "crashed", SNMPD or SNMPSAD crashed. If SNMPD is crashed, likely need to update the SecureSync to version 5.2.1 (or higher). If SNMPSAD crashed, need to increase the timeout value in the device polling the SecureSync (no less than about 10 seconds) and should also update software to at least version 5.2.1.

4) Perform a "ps -el | grep snmp"

There should be two red SNMP values in the response (**snmpsad** and **snmpd**)



```
spfactory@Spectracom ~ $ ps -el | grep snmp
5 S     0 16928     1  6  80   0 -  1990 poll_s ?        00:02:46 snmpsad
5 S  1001 16975     1  4  80   0 -  2029 poll_s ?        00:01:50 snmpd
spfactory@Spectracom ~ $
```

5) Use tcpdump to verify if SNMP traps are being sent

- Note-omit the word "sudo" in all the below commands for software versions 5.4.5 AND ABOVE
  - Refer to the tcpdump section of this doc for more info
  - SNMP Traps sent to any Ethernet interface:

(Versons 5.4.5 and above) tcpdump port 162 -i any

(Versions 5.4.1 and below) sudo tcpdump port 162 -i any

Potential conditions associated with SNMP

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) 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 2c 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 http://cvsmantis.int.orolia.com/mantis/view.php?id=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)

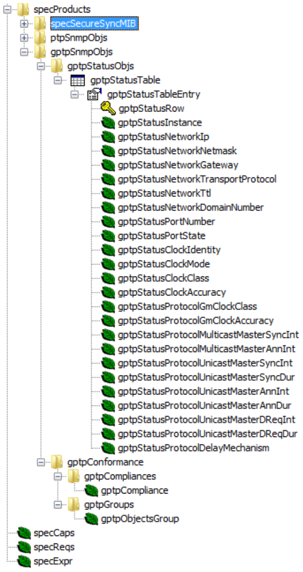
- Refer also to the SNMP Tech note (towards the end) for software changes ssociated with SNMP: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\SNMP- Notifications-email alerts\SNMP

Examples of available SNMP Gets/Sets

PTP mib file (for 1204-12 10/100 card) and GB PTP mib file (for 1204-32 card)

A) “SPECTRACOM-GPTP.mib” file/objects (starts with .1.3.6.1.4.1.18837.3.5)

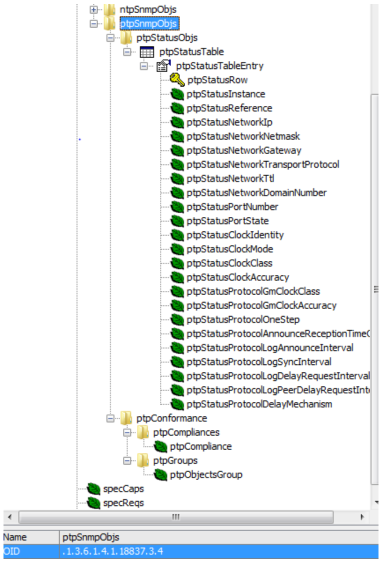
- This much more recent PTP mib file was added in software version 5.6.0 (Apr 2017) for the 1204-32 (Gb PTP Option Card)
- All of the object names begin with “gptp” (such as gptpStatusTable” for instance)



```
specProducts
  specSecureSyncMIB
  ptpSnmpObjs
  gptpSnmpObjs
    gptpStatusObjs
      gptpStatusTable
        gptpStatusTableEntry
          gptpStatusRow
          gptpStatusInstance
          gptpStatusNetworkIp
          gptpStatusNetworkNetmask
          gptpStatusNetworkGateway
          gptpStatusNetworkTransportProtocol
          gptpStatusNetworkTtl
          gptpStatusNetworkDomainNumber
          gptpStatusPortNumber
          gptpStatusPortState
          gptpStatusClockIdentity
          gptpStatusClockMode
          gptpStatusClockClass
          gptpStatusClockAccuracy
          gptpStatusProtocolGmClockClass
          gptpStatusProtocolGmClockAccuracy
          gptpStatusProtocolMulticastMasterSyncInt
          gptpStatusProtocolMulticastMasterAnnInt
          gptpStatusProtocolUnicastMasterSyncInt
          gptpStatusProtocolUnicastMasterSyncDur
          gptpStatusProtocolUnicastMasterAnnInt
          gptpStatusProtocolUnicastMasterAnnDur
          gptpStatusProtocolUnicastMasterDReqInt
          gptpStatusProtocolUnicastMasterDReqDur
          gptpStatusProtocolDelayMechanism
    gptpConformance
      gptpCompliances
        gptpCompliance
      gptpGroups
        gptpObjectsGroup
  specCaps
  specReqs
  specExpr
```

B) SPECTRACOM-PTP-MIB.mib" file/objects (starts with .1.3.6.1.4.1.18837.3.4)

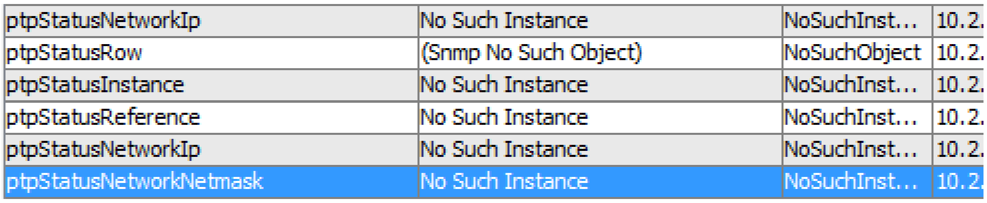
- This much earlier PTP mib file is for the Model 1204-12 (10/100 PTP Option Card)
- All of the object names begin with "ptp" (such as ptpStatusTable" for instance)



```
  ntpSnmpObjs
  ptpSnmpObjs
    ptpStatusObjs
      ptpStatusTable
        ptpStatusTableEntry
          ptpStatusRow
          ptpStatusInstance
          ptpStatusReference
          ptpStatusNetworkIp
          ptpStatusNetworkNetmask
          ptpStatusNetworkGateway
          ptpStatusNetworkTransportProtocol
          ptpStatusNetworkTtl
          ptpStatusNetworkDomainNumber
          ptpStatusPortNumber
          ptpStatusPortState
          ptpStatusClockIdentity
          ptpStatusClockMode
          ptpStatusClockClass
          ptpStatusClockAccuracy
          ptpStatusProtocolGmClockClass
          ptpStatusProtocolGmClockAccuracy
          ptpStatusProtocolOneStep
          ptpStatusProtocolAnnounceReceptionTime(
          ptpStatusProtocolLogAnnounceInterval
          ptpStatusProtocolLogSyncInterval
          ptpStatusProtocolLogDelayRequestInterval
          ptpStatusProtocolLogPeerDelayRequestInt
          ptpStatusProtocolDelayMechanism
    ptpConformance
      ptpCompliances
        ptpCompliance
      ptpGroups
        ptpObjectsGroup
  specCaps
  specReqs
```

Name	ptpSnmpObjs
OID	.1.3.6.1.4.1.18837.3.4

Note: Using the PTP Mib (10/100) file with a Gb 32 card (instead of using the GB Mib) results in the responses returnuing 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.

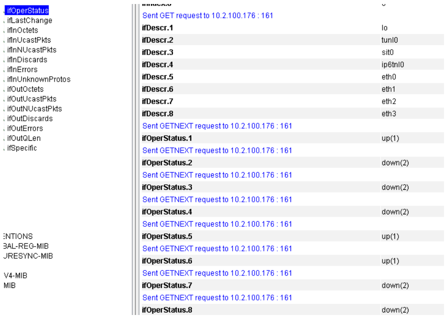
SNMP Gets available via RFC1213 MIB file

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):

- The ifDescr object lists all of the available interfaces in the time server and reports the "assigned name" for each one.



```
Sent GET request to 10.2.100.176 : 161
ifDescr.1                                   lo
ifDescr.2                                   tunl0
ifDescr.3                                   sit0
ifDescr.4                                   ip6tnl0
ifDescr.5                                   eth0
ifDescr.6                                   eth1
ifDescr.7                                   eth2
ifDescr.8                                   eth3
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.1                              up(1)
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.2                              down(2)
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.3                              down(2)
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.4                              down(2)
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.5                              up(1)
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.6                              up(1)
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.7                              down(2)
Sent GETNEXT request to 10.2.100.176 : 161
ifOperStatus.8                              down(2)
```

Note: using the

2) Configuring the Reference Priority table using SNMP Sets

Questions for Spectracom:

1. Do you expect the snmpset commands to work for the above referenced OIDs?
2. If not, why, and is there some other MIB/OID info you can provide to allow a time reference change via SNMP? SNMP is preferred because our data processor already has an SNMP interface for the PTU coded.
3. If SNMP set is not an option for this, what options other than the web GUI interface are available for doing this reference switch?

Keith's response: Section 7 (page 24) of the attached SNMP tech note discusses how to configure/reconfigure the input reference priority table using SNMP. This info is excerpted below in blue for your reference (Please especially pay particular notice to the "Note" below and in the document)

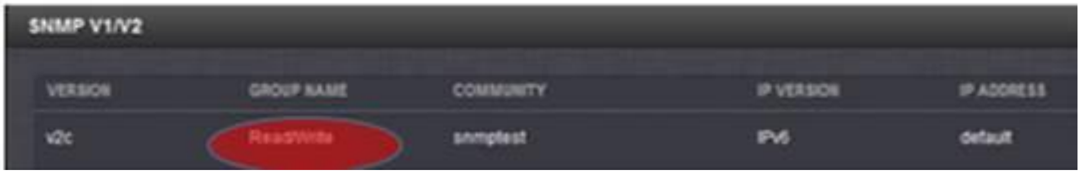
(FYI also attached is a spreadsheet I have also created which contains the more commonly used OIDs in one tab and the available SNMP traps in another tab. I hope you and your team find both the SNMP document and the spreadsheet helpful, as I suspect you will ☺!)

The "Enable/Disable" and "Priority" fields of the "Reference Priority Setup" can be configured via the SecureSync's web browser or with SNMP "Sets". The "SPECTRACOM-SECURE-SYNC-MIB.mib" file contains the applicable values for configuring this table via SNMP. Refer to "**ssReferenceMgmtObjs Objects [enterprises.18837.3.2.2.4.x]**" in this MIB file for a list of all of the values associated with this table. Refer to the SecureSync user manual for additional information on the "Reference Priority Setup" table.

Note: SNMP provides the ability to "get" the entire Reference Priority table, but only provides the ability to "set" the "State" field (Enable or Disable input references) and the "Priority" of the reference. SNMP does not allow entries to be added or deleted from the Reference Priority table.

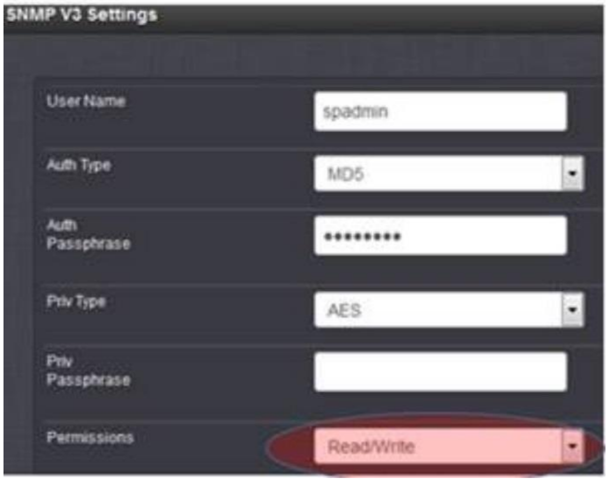
Per the "Note" above, the SecureSync's input reference priority table should initially be pre-configured (using the **Management** -> **Reference Priority** page of the web browser) with a "list" of all input references that the SecureSync could potentially be synced with. Thereafter, SNMP can then be used to change the priority assigned and/or enable/disable each of the references in this table.

[With read/write privileges enabled in both the SecureSync (**Management** -> **SNMP Setup** page of the browser as shown below) and in the SNMP Manager]:



SNMP V1/V2

VERSION	GROUP NAME	COMMUNITY	IP VERSION	IP ADDRESS
v2c	Read/Write	snmptest	IPv6	default

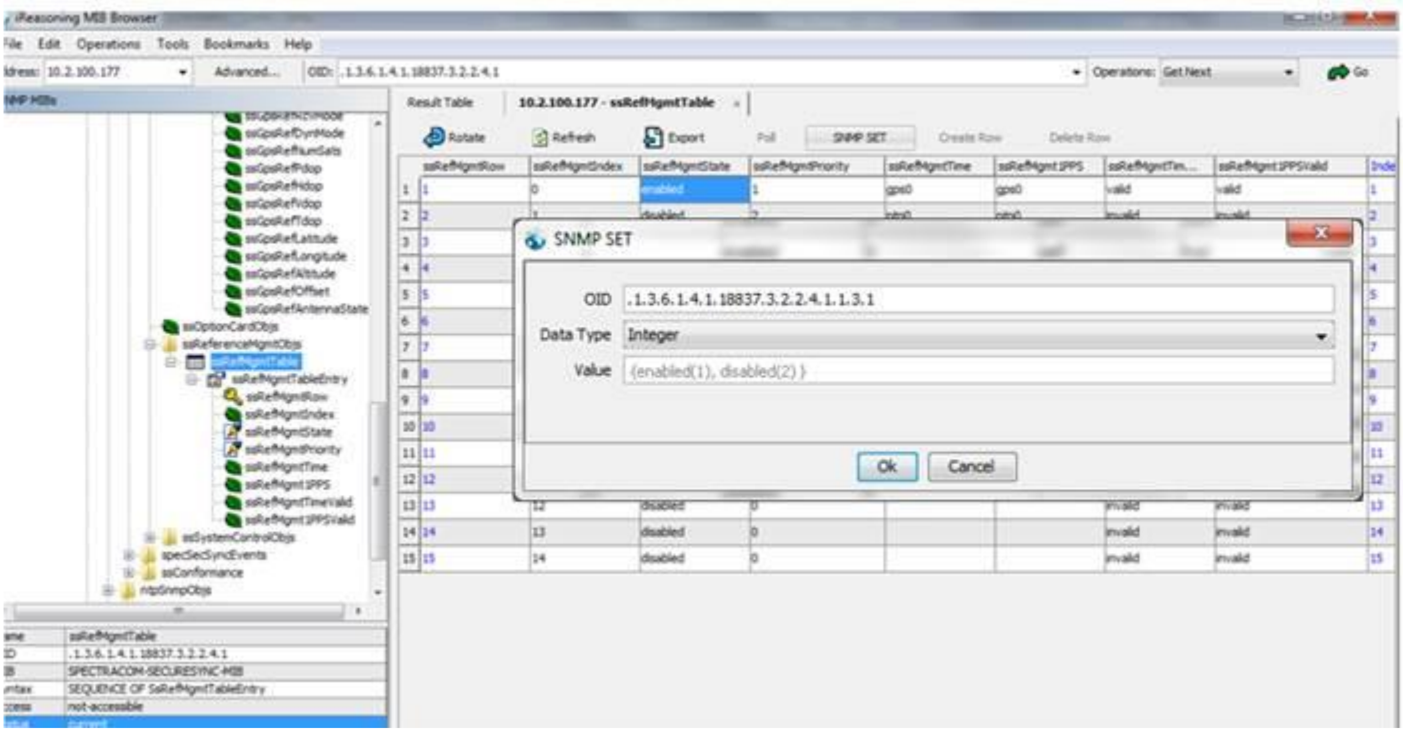


SNMP V3 Settings

User Name	spadmin
Auth Type	MD5
Auth Passphrase	•••••••••
Priv Type	AES
Priv Passphrase	
Permissions	Read/Write

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



SNMP SET

OID .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.1

Data Type Integer

Value {enabled(1), disabled(2) }

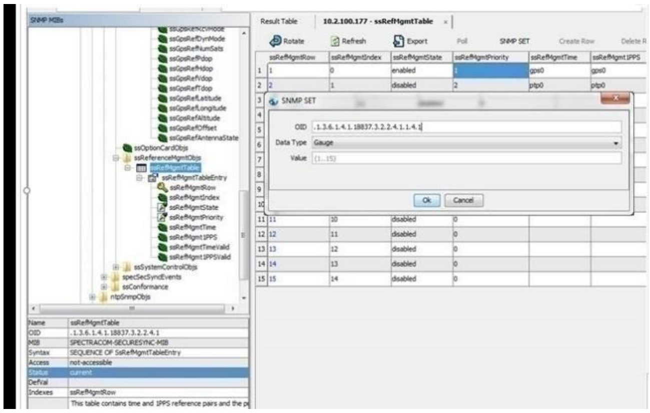
Below are the specific OIDs to enable/disable each reference.

Index (row of table)

- .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.1
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.2
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.3
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.4
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.5
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.3.6
- etc

Note that in order to disable each reference, the value of "**2**" needs to be sent.

To Change the priority of each row of the table



SNMP SET

OID .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.1

Data Type Gauge

Value (1...15)

Below are the specific OIDs to change the priority of each reference (available values are 1 through 15)
Index (row of table)

- .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.1
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.2
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.3
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.4
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.5
- .1.3.6.1.4.1.18837.3.2.2.4.1.1.4.6
- etc

System Memory, CPU and disk usage (CF card) information via the ".2021" (UCD/UCDavis) MIB file

- Per the SecureSync relese notes, ability to poll the diskstats , CPU and memory was added in version 5.2.1
  - Added ability to pull system **memory**, **CPU**, and CF card **disk usage** information from **SNMP**

Note: These system MIBs are only available with SecureSync software **versions 5.2.1** and higher installed

UCD/UC Davis MIB file ("UCD-SNMP-MIB") ".1.3.6.1.4.1.2021."

- The ".2021" MIB OIDs (such as the ones listed below) are all part of the UCD-SNMP-MIB (ucdavis) MIB file. For more information on this MIB file, which is internally supported by SecureSync, refer to: http://www.net-snmp.org/docs/mibs/ucdavis.html

TABLE 1: CPU USAGE	
OID	**FUNCTION**
.1.3.6.1.4.1.2021.11.9.0	Percentage of user CPU time
.1.3.6.1.4.1.2021.11.50.0	Raw user CPU time
.1.3.6.1.4.1.2021.11.10.0	Percentages of system CPU time
.1.3.6.1.4.1.2021.11.52.0	Raw system CPU time
.1.3.6.1.4.1.2021.11.11.0	Percentages of idle CPU time
.1.3.6.1.4.1.2021.11.53.0	raw idle CPU time
.1.3.6.1.4.1.2021.11.51.0	raw nice CPU time

TABLE 2: MEMORY USAGE	
OID	**FUNCTION**

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

TABLE 3: DISK USAGE	
OID	**FUNCTION**
.1.3.6.1.4.1.2021.9.1.2.1	Path where the disk is mounted
.1.3.6.1.4.1.2021.9.1.3.1	Path of the device for the partition
.1.3.6.1.4.1.2021.9.1.6.1	Total size of the disk/partition (kBytes)
.1.3.6.1.4.1.2021.9.1.7.1	Available space on the disk
.1.3.6.1.4.1.2021.9.1.8.1	Used space on the disk
.1.3.6.1.4.1.2021.9.1.9.1	Percentage of space used on disk
.1.3.6.1.4.1.2021.9.1.10.1	Percentage of inodes used on disk

Disk usage

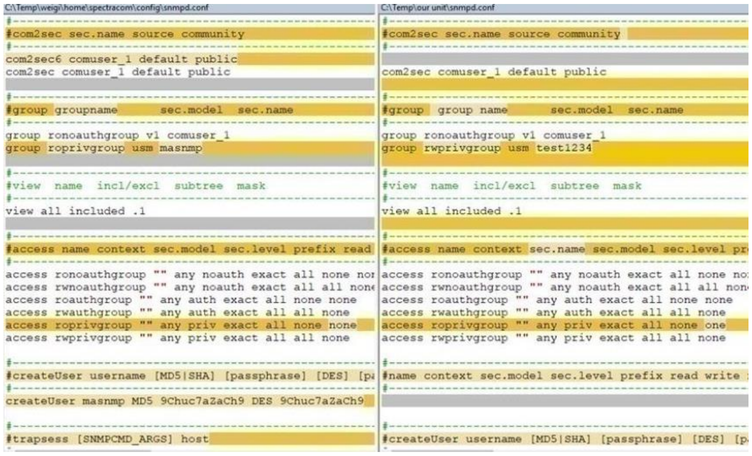
- versions prior to version 5.2.1 did not support the .**1.3.6.1.4.1.2021.9.1.7.x** objects to poll disks statis

Problem: Unable to obtain the disk stats (such as .1.3.6.1.4.1.2021.9.1.7.1) **while everything else is returned succusfully. software version well above v5.2.1**

- Refer to Salesforce case 127293
- this was caused by a customer restoring an earlier configuration bundle into a newer version of software. As shown in the snmpd.conf file comparison below, the "Miscellanious" section of the customer's snmpd.conf file was missing the "diskio" comments that we had present in our snmpd.conf file (as shown below)

FYI- I ran a diff on their snmpd.conf (left side) and our Netclock 9483 (right side)

Under **miscellaneous** (at the bottom) our unit has diskIO info, while their unit doesn't?? I think this is key, but not sure why their config would be different. Could this somehow be due to their "roprivgroup" being "**none**" and ours being "**one**"?

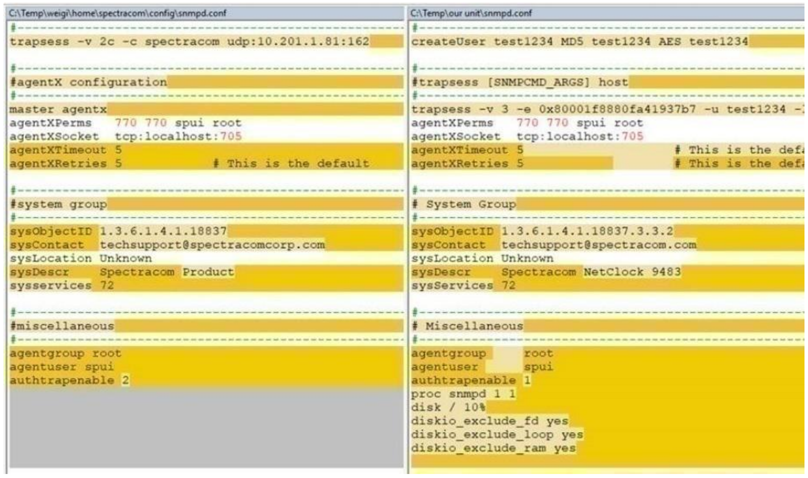


C:\Temp\weigi\home\spectracom\config\snmpd.conf

```
#-----------------------------------------------------------
#com2sec sec.name source community
#-----------------------------------------------------------
com2sec6 comuser_1 default public
com2sec comuser_1 default public

#-----------------------------------------------------------
#group groupname       sec.model  sec.name
#-----------------------------------------------------------
group ronoauthgroup v1 comuser_1
group roprivgroup usm masnmp

#-----------------------------------------------------------
#view  name  incl/excl  subtree  mask
#-----------------------------------------------------------
view all included .1

#-----------------------------------------------------------
#access name context sec.model sec.level prefix read
#-----------------------------------------------------------
access ronoauthgroup "" any noauth exact all none nor
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 roprivgroup "" any priv exact all none none
access rwprivgroup "" any priv exact all all none

#-----------------------------------------------------------
#createUser username [MD5|SHA] [passphrase] [DES] [pa
#-----------------------------------------------------------
createUser masnmp MD5 9Chuc7aZaCh9 DES 9Chuc7aZaCh9

#-----------------------------------------------------------
#trapsess [SNMPCMD_ARGS] host
```

C:\Temp\our unit\snmpd.conf

```
#-----------------------------------------------------------
#com2sec sec.name source community
#-----------------------------------------------------------

com2sec comuser_1 default public

#-----------------------------------------------------------
#group  group name       sec.model  sec.name
#-----------------------------------------------------------
group ronoauthgroup v1 comuser_1
group rwprivgroup usm test1234

#-----------------------------------------------------------
#view  name  incl/excl  subtree  mask
#-----------------------------------------------------------
view all included .1

#-----------------------------------------------------------
#access name context sec.name sec.model sec.level pr
#-----------------------------------------------------------
access ronoauthgroup "" any noauth exact all none no
access rwnoauthgroup "" any noauth exact all all non
access roauthgroup "" any auth exact all none none
access rwauthgroup "" any auth exact all all none
access roprivgroup "" any priv exact all none one
access rwprivgroup "" any priv exact all all none

#-----------------------------------------------------------
#name context sec.model sec.level prefix read write
#-----------------------------------------------------------


#-----------------------------------------------------------
#createUser username [MD5|SHA] [passphrase] [DES] [p
```



C:\Temp\weigi\home\spectracom\config\snmpd.conf

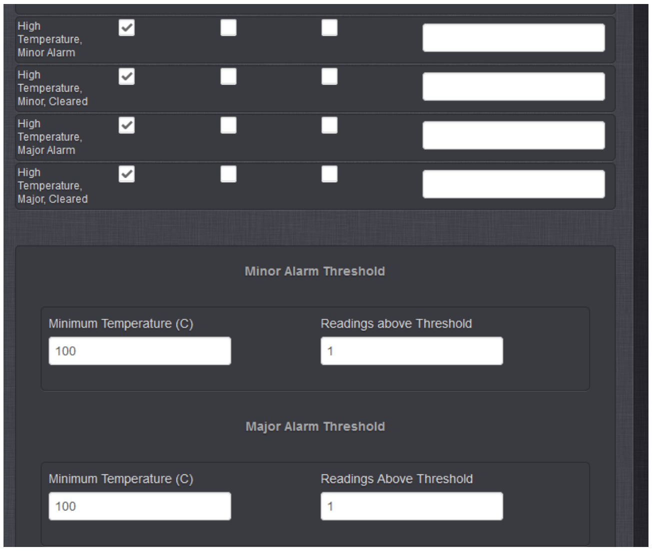
```
#-----------------------------------------------------------
trapsess -v 2c -c spectracom udp:10.201.1.81:162

#-----------------------------------------------------------
#agentX configuration
#-----------------------------------------------------------
master agentx
agentXPerms   770 770 spui root
agentXSocket  tcp:localhost:705
agentXTimeout 5
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
```

C:\Temp\our unit\snmpd.conf

```
#-----------------------------------------------------------
createUser test1234 MD5 test1234 AES test1234

#-----------------------------------------------------------
#trapsess [SNMPCMD_ARGS] host
#-----------------------------------------------------------
trapsess -v 3 -e 0x80001f8880fa41937b7 -u test1234 -
agentXPerms   770 770 spui root
agentXSocket  tcp:localhost:705
agentXTimeout 5                      # This is the defa
agentXRetries 5                      # This is the defa

#-----------------------------------------------------------
# System Group
#-----------------------------------------------------------
sysObjectID 1.3.6.1.4.1.18837.3.3.2
sysContact  techsupport@spectracom.com
sysLocation Unknown
sysDescr    Spectracom NetClock 9483
sysServices 72

#-----------------------------------------------------------
# Miscellaneous
#-----------------------------------------------------------
agentgroup     root
agentuser      spui
authtrapenable 1
proc snmpd 1 1
disk / 10%
diskio_exclude_fd yes
diskio_exclude_loop yes
diskio_exclude_ram yes
```

Temperature related notifications (added in version 5.3.1)

- ➢ Version 5.3.1 also added SNMP alerts for high temperatures (Management -> Notifications page, System tab)



High Temperature, Minor Alarm	☑	□	□	
High Temperature, Minor, Cleared	☑	□	□	
High Temperature, Major Alarm	☑	□	□	
High Temperature, Major, Cleared	☑	□	□	

Minor Alarm Threshold

Minimum Temperature (C): 100

Readings above Threshold: 1

Major Alarm Threshold

Minimum Temperature (C): 100

Readings Above Threshold: 1

The alarms are similar in behavior to the GPS Number of Satellite Major and Minor alarms. In this case the user can set a Minimum Temperature Threshold value for both the Major and Minor alarms. The user can also set a number of times the value above the threshold must be present before asserting the Major or Minor Alarm. A value of 1 means that the value was read once, a minute passed and on reading the value again, the temperature exceeded the threshold. The number of reads is user settable to allow for environmental conditions where more than 1 read is required to validate accurate temperature. Increasing the value requires N multiple consecutive reads of temperature above the minimum threshold before asserting the alarm.

Largest acceptable value for both Minimum temperature values is “100” (in at least versions 5.4.1 and below)

- Max value that should be entered in either temperature field is “100” (though in at least versions 5.4.1 and below, the browser will accept a value greater than 100 with no error messages being displayed).
- Setting either or both of the “Minimum temperature” fields to a value greater than “100” will cause statusd daemon to keep restarting (as indicated in the system.log. NTP will still be able to run, but NTP status info (stratum, sync status, etc.will be reported as “?”” because statusd will keep clearing out the values obtained from NTPQ.

Notifications/traps for SAASM receiver only

- Refer to SecureSync SAASM receiver Manual Addendum (1200-5000-0053)
    - **Note**: NOT in Arena, as it’s an FOUO document: \\rocuso.uso.oroliausa.com\us-only\Documentation\Released\Manuals\1200-xxxx-xxxx
- 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.

Testing SNMP traps and email alerts

- Refer to (in this document): **Testing/Verifying SNMP/Email alerts are enabled and working inside the SecureSync

Temporary fix to this SNMP lock-out condition

I have some new information for you, regarding the lock-out condition the SecureSync was exhibiting when you were configuring its SNMP. We have figured out what is allowing this to happen and so we can now tell you how to avoid it occurring!

In the **Network / SNMP Setup** page of the browser, "**Notifications**" tab, the **User/Community** field is a required field. If this field is empty (while other values have been entered in the same row) when you hit Submit, the empty field affects the web browser operation and will lock you out, like you have been observing. As long as there is something entered in this (preferably the correct value for your SNMP manager, but any character will work) and you hit Submit, you will no longer experience this lock-out condition.

We were only able to duplicate the symptoms, when this one field was empty and the Submit button was pressed. Because it's a required field for generating SNMP traps, we intend on modifying the software in a future release so that it ensures that the field is not empty, when editing the SNMP trap configurations.

Just thought you would like to know how to prevent the lock-out condition from occurring. I still have you record flagged in our Customer Service database to let you know when the software has been modified to check for a value in this field before accepting the changes.

To perform a CLEAN/HALT function:

- Open the web browser for the SecureSync unit
- Navigate to the TOOLS/UPGRADE/BACKUP screen
- Select the CONFIGURATION tab
- Change the Clean/Halt field from Disabled to Enabled and select SUBMIT
- This will clear out the configuration files and any erroneous settings. The unit will HALT operation and will need a power cycle to resume operation.