SecureSync®

Time and Frequency
Synchronization System

User Reference Guide

Document Part No.: 1200-5000-0050

Revision: 21

Date: 08-April-2016

spectracom.com

The information in this document has been carefully reviewed and is believed to be accurate and up-to-date. Spectracom assumes no responsibility for any errors or omissions that may be contained in this document, and makes no commitment to keep current the information in this manual, or to notify any person or organization of updates. This User Reference Guide is subject to change without notice. For the most current version of this documentation, please see our web site at spectracom.com.

Spectracom reserves the right to make changes to the product described in this document at any time and without notice. Any software that may be provided with the product described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

Spectracom Corp.

• 1565 Jefferson Road, Suite 460, Rochester, NY 14623 USA
• 3, Avenue du Canada, 91974 Les Ulis Cedex, France
• Room 208, No. 3 Zhong Guan Village South Road, Hai Dian District, Beijing 100081, China

Questions or comments regarding this User Reference Guide?

➔ E-mail: techpubs@spectracom.com

SPECTRACOM LIMITED WARRANTY

Five Year Limited Warranty

Spectracom, a business of the Orolia Group, warrants each new standard product to be free from defects in material, and workmanship for five years after shipment in most countries where these products are sold, EXCEPT AS NOTED BELOW (the “Warranty Period” and "Country Variances").

Warranty Exceptions

This warranty shall not apply if the product is used contrary to the instructions in its manual or is otherwise subjected to misuse, abnormal operations, accident, lightning or transient surge, or repairs or modifications not performed by Spectracom authorized personnel.

Items with a variance to the Five Year Warranty Period are as follows:

90 Days Warranty

TimeKeeper Software
VelaSync Hardware

One Year Limited Warranty

Timeview Analog Clock
Path Align-R Products
Bus-level Timing Boards
IRIG-B Distribution Amplifiers
Down-Up Antenna Converter (DUC)
Geo-iNav/Geo-PNT

Two Year Limited Warranty

Rubidium Oscillators
Epsilon Board EBO3
Epsilon Clock 1S, 2S/2T, 3S, 31M
Epsilon SSU
Power Adaptors
Digital and IP/POE Clocks
WiSync Wireless Clock Systems and IPSync IP Clocks
Rapco 1804, 2804, 186x, 187x, 188x, 189x, 2016, 900 series

Three Year Limited Warranty

Pendulum Test & Measurement Products GPS- 12R, CNT- 9x, 6688/6689, GPS-88/89, DA-35/36, GPS/GNSS Simulators

Country Variances

All Spectracom products sold in India have a one year warranty.

Warranty Exclusions

Batteries, fuses, or other material contained in a product normally consumed in operation.

Shipping and handling, labor & service fees EXCEPT FOR THE LIMITED WARRANTY STATED ABOVE, SPECTRACOM DISCLAIMS ALL WARRANTIES OF ANY KIND WITH REGARD TO SPECTRACOM PRODUCTS OR OTHER MATERIALS PROVIDED BY SPECTRACOM, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Spectracom shall have no liability or responsibility to the original customer or any other party with respect to any liability, loss, or damage caused directly or indirectly by an Spectracom product, material, or software sold or provided by Spectracom, replacement parts or units, or services provided, including but not limited to any interruption of service, excess charges resulting from malfunctions of hardware or software, loss of business or anticipatory profits resulting from the use or operation of the Spectracom product or software, whatsoever or howsoever caused. In no event shall Spectracom be liable for any direct, indirect, special or consequential damages whether the claims are grounded in contract, tort (including negligence), or strict liability.

Extended Warranty Coverage

Extended warranties can be purchased for additional periods beyond the standard warranty. Contact Spectracom no later than the last year of the standard warranty for extended coverage.

Warranty Claims

Spectracom's obligation under this warranty is limited to the cost of in-factory repair or replacement, at Spectracom's option, of the defective product or the product's defective component. Spectracom's Warranty does not cover any costs for installation, reinstallation, removal or shipping and handling costs of any warranted product. If in Spectracom's sole judgment, the defect is not covered by the Spectracom Limited Warranty, unless notified to the contrary in advance by customer, Spectracom will make the repairs or replace components and charge its then current price, which the customer agrees to pay.

In all cases, the customer is responsible for all shipping and handling expenses in returning product to Spectracom for repair or evaluation. Spectracom will pay for standard return shipment via common carrier. Expediting or special delivery fees will be the responsibility of the customer.

Warranty Procedure

Spectracom highly recommends that prior to returning equipment for service work, our technical support department be contacted to provide troubleshooting assistance while the equipment is still installed. If equipment is returned without first contacting the support department and "no problems are found" during the repair work, an evaluation fee may be charged.

Spectracom shall not have any warranty obligations if the procedure for warranty claims is not followed. Customer must notify Spectracom of a claim, with complete information regarding the claimed defect. A Return Authorization (RMA) Number issued by Spectracom is required for all returns.

Returned products must be returned with a description of the claimed defect, the RMA number, and the name and contact information of the individual to be contacted if additional information is required by Spectracom. Products being returned on an RMA must be properly packaged with transportation charges prepaid.

CONTENTS

CHAPTER 3

CHAPTER 4

CHAPTER 5

CHAPTER 6

CHAPTER 7

APPENDIX

BLANK PAGE.

CHAPTER 1

Introduction & Overview

The Chapter presents an **overview** of the SecureSync Time and Frequency Synchronization System, its capabilities, main technical features and functions.

The following topics are included in this Chapter:

1.1 Getting Started

Welcome to this User Reference Guide for your SecureSync unit. Whether you read this online, on paper, or in a pdf document, we sincerely hope you'll quickly find your way around.

Depending on what your objective is today, here are our recommendations on what to do next:

- If you want to install and configure a SecureSync, and have no or little experience with this technology, we suggest you
  a. browse through CHAPTER 1 first, and then
  b. familiarize yourself with the installation procedure and its variations–see "Installation and Setup Summary" on page 18.

- If you plan on installing a SecureSync unit and you are familiar with the basic technical concepts of time and frequency synchronization, as well as network administration, we suggest you start here:
  - "Installation and Setup Summary" on page 18.

- If your unit is up and running, and you consider changing a specific setting–or learning more about its features and functions–the easiest way to find the information you are looking for is
  - the TABLE OF CONTENTS, or
  - the INDEX.

- Should you experience technical problems, refer the following information sources:
  a. "Troubleshooting" on page 453
  b. "INDEX" on page i
  c. Spectracom Online Knowledge Base
  d. "Technical Support" on page 514.

1.2 Introduction

SecureSync® is a security-hardened 1-rack unit network appliance designed to meet rigorous network security standards and best practices. It ensures accurate timing through multiple references, tamper-proof management, and extensive logging. Robust network protocols are used to allow for easy but secure configuration. Features can be enabled or disabled based on your network policies. Installation is aided by DHCP (IPv4), AUTOCONF (IPv6), and a front-panel keypad and LCD display.

The unit supports multi-constellation GNSS input (SAASM GPS receivers, supporting L1/L2, available for authorized users and required for the US DoD are available), IRIG input and other input references. The unit is powered by AC on an IEC60320 connector. DC power as back-up to AC power, or as the primary input power source, is also available.

SecureSync combines Spectracom's precision master clock technology and secure network-centric approach with a compact modular hardware design to bring you a powerful time and frequency reference system at the lowest cost of ownership. Military and commercial applications alike will benefit from its extreme reliability, security, and flexibility for synchronizing critical operations.

An important advantage of SecureSync is its unique rugged and flexible modular chassis that can be configured for your specific needs. Built-in time and frequency functions are extended with up to six input/output modules.

Included with the base unit is an extremely accurate 1PPS timing signal aligned to a 10 MHz frequency signal. A variety of internal oscillators is available, depending on your requirements for holdover capability and phase noise. Choose from a variety of configurable option cards, each with an assortment of input/output timing signal types and quantity, including additional 1PPS, 10 MHz, timecode (IRIG, ASCII, HAVE QUICK), other frequencies (5MHz, 2.048 MHz, 1.544 MHz, 1MHz), Precision Timing Protocol (PTP) input/output, multi-Gigabit Ethernet (10/100/1000Base-T), telecom T1/E1 data rates and multi-network NTP, allowing SecureSync to be customized for your exact requirements.

To support network time synchronization, SecureSync supports the latest features of Network Time Protocol (NTP). An optional multi-port NTP configuration allows for operation across four LAN segments or shared operation between up to four separate/isolated networks.

Note: Some of the features described are not available on all SecureSync variants.

1.3 Inputs and Outputs

SecureSync provides multiple outputs for use in networked devices and other pieces of technology. A 1-Pulse-Per-Second (1PPS) output acts as a precise metronome, counting off seconds of System Time in the selected timescale (such as UTC, TAI or GPS). A 10 MHz frequency reference provides a precise, disciplined signal for control systems and clocks (as the inverse of time is frequency). SecureSync's outputs are driven by its inputs – most significantly, Global Navigation Satellite System (GNSS) technology as well as IRIG input from IRIG signal generators (such as Spectracom's NetClocks and bus-level timing boards) and other available input references. GNSS-equipped SecureSyncs can track up to thirty-two GNSS satellites simultaneously and synchronize to the satellite's atomic clocks. This enables SecureSync-equipped computer networks to synchronize all elements of network hardware and software (including system logs) over LANs or WANs – anywhere on the planet.

1.4 Introduction to GPS and GNSS

The United States Government operates a set of satellites providing positioning, navigation and timing services to users on Earth, in Earth's atmosphere and orbit. This satellite-based Global Positioning System is also known as "GPS Constellation". Other Global Navigation Satellite Systems (GNSS) exist e.g., the Russian GLONASS system, or the European Galileo system.

Each satellite has an internal atomic clock and transmits a signal specifying the time and satellite position. The GPS constellation consists of 24 satellites plus several spares flying in Mid-Earth Orbits (MEO, ~20,000 km), orbiting the earth at a rate of approximately twice per day.

You can determine your position on Earth by listening to four or more satellites, using a GPS receiver. Each satellite transmits a “pulse” at exactly the same time. Depending on your distance from each satellite, you will receive those “pulses” at different times, based on the propagation delay of the radio signal traveling at (near) the speed of light. For the GPS receiver, there are four unknowns in this process - x, y, and z for its position, and the time mark for the start of transmission - hence four satellites minimum are required to obtain a 3D fix by simultaneously solving four equations in order to resolve four unknowns.

The “pulse” is transmitted in the form of a spread spectrum Code Division Multiple Access (CDMA) signal with each satellite using a different Pseudo Random Noise (PRN) code. The CDMA process spreads the “pulse” energy over a long period of time by modulating it into “chips”, allowing for a weak signal to be transmitted efficiently by the satellite and reconstructed by the receiver.

The GPS satellites transmit their signals on two different frequencies, L1 (1575 MHz) and L2 (1227 MHz), using two different spread code chip rates: The Coarse/Acquisition (C/A) code is at 1M chips/sec and the Precision (P) code is at 10M/chips/sec. Many commercial receivers in use today only use the L1 C/A signal and can get sufficient accuracy, but a receiver using the P code will get higher accuracy. One that receives both frequencies can further improve accuracy by compensating for variations in propagation delay through the ionosphere.

On top of these timing signals, a low speed data stream (50 bps) is impressed containing the Almanac and Ephemeris data. The Almanac data contains the planned orbital information for each satellite and is valid for many days. The Ephemeris data contains the precise orbital positions of each satellite and is considered valid for about 4 hours. Once the receiver has the position data of the satellites in view, plus the range measurements (sometimes called “pseudo-ranges” because they are only measured estimates, not exact true ranges) to at least four of them, it can then calculate its position on earth.

For military applications, the P code is encrypted, thus guaranteeing the authenticity of the signal. A GPS receiver which has the proper decryption circuitry is called a Selective Availability/Anti-Spoofing Module (SAASM) receiver and is only available for military use.

GPS Signal Modernization

The GPS system is going through a modernization program and new satellites are being launched every year, with each new version having more capabilities. Several new signals are being created:

- **L2C** – Precise Civilian Code – This signal uses a more modern, robust modulation code and is not encrypted, giving civilian users better service. As of July 2015, it is transmitting on 16 satellites and is expected to be fully operational on 24 satellites by 2018.
- **L5** – This new signal in a new band is also intended for civilian use. It is more powerful, less prone to interference and more accurate than the current L1 civilian signal. It shares its band with the Galileo E5 signal and is fully compatible with it. Nine satellites are transmitting it today (July 2015) and it is expected to be fully operational by 2021.
- **M-code** – This is the next generation military encrypted signal which is present on 14 satellites. The new receiver that decodes this encrypted signal is sometimes referred to as the MUE – Military User Equipment. Once fully operational and all military user equipment is fully upgraded, the GPS system will be fully segregated into a civilian system and a separate military one.
- **L1C** – Future improved signal to be compatible with Galileo but no satellites are operating with this yet.

Characteristics of Other GNSS Systems

All of the global systems operate in a very similar manner to the GPS system, but each has its own unique qualities:

- **GLONASS** – Operates in the L1 and L2 bands similar to GPS, but uses a Frequency Division Multiple Access (FDMA) signal where each satellite transmits at a slightly different, higher frequency than GPS. Their orbits are optimized for slightly better accuracy at the northern latitudes, but the system still offers complete worldwide coverage. Originally a relic of the Cold War, the entire constellation was updated and is fully operational with modern equipment since 2011.
- **Galileo** – Uses more modern modulation than GPS, operating in three bands: E1, E5 and E6, and offers an encrypted Public Regulated Service and enhanced Search And Rescue (SAR) service. Only eight satellites are operational today, but birds are being launched in pairs at a faster rate, so a fully operational constellation is expected by 2019.
- **Beidou** (formerly called Compass) - This system is operational regionally over Asia today, but new satellites are being launched to offer full worldwide coverage by 2020 with 37 satellites. The new signal structure is very similar to Galileo and the new GPS signals. In Dec 2012, the Chinese published open system specs so it can be a viable system for worldwide use.
- **QZSS** – A regional navigation satellite system for the East Asia and Oceania region, operated by the Japanese Government. This system is used in combination with data from other GNSS satellites and as such is not operational by itself.

If equipped with the Multi-GNSS option, SecureSync allwos concurrent dual constellation GNSS reception, offering not only better satellite coverage and signal availability in "urban canyons" and other areas with limited view of the sky, but also offering improved reliability in the event of a fault in any single constellation.

Powering UP/DOWN a GNSS Receiver

When power is first applied to a GNSS receiver, it begins looking for satellites. It does this by searching for each satellite, individually, listening for every satellite's distinct spread-spectrum hopping sequence. This process can take several minutes, as the receiver iteratively locates satellites, refines its position, and determines for which satellites to search.

When the power is switched off, a GNSS receiver retains the last known position. This typically results in faster satellite acquisition the next time it is switched on, because the receiver will use the previously mentioned Almanac data to locate the satellites. If, however, the antenna has been moved more than a few miles, or too many days have passed since the power had been turned off, acquisition time will be longer.

1.5 Front Panel

The front panel of a SecureSync unit consists of:

- three separate illuminated status LEDs
- a front panel control keypad
- an LED time display
- an LCD information display
- an RS-232 serial interface
- and a temperature controlled cooling fan.

The LCD information display is configurable using the SecureSync Web browser user interface (also referred to as the “Web UI”) or the front panel controls. Display options include status or position information, time, date, DOY (Day of Year), GNSS information, as well as network settings and SAASM key status (available with the SAASM GPS receiver option only). The RS-232 serial interface and the front panel controls provide a means of initially configuring the unit’s network settings.

SecureSync units with the SAASM GPS receiver option module installed also have an encryption key fill connector and key zeroize switch on the left-hand side of the front panel.

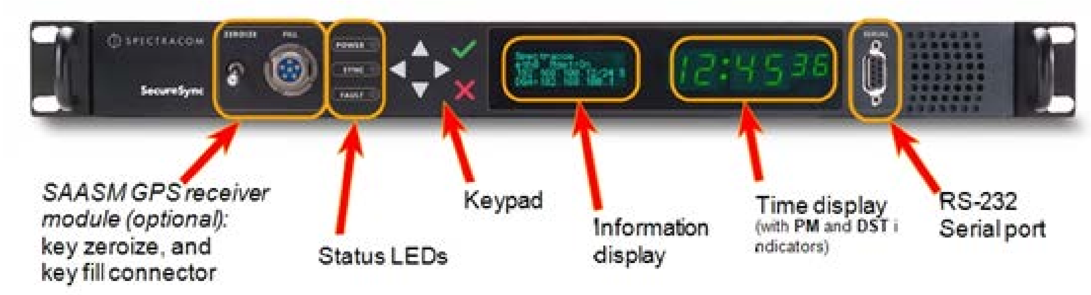


Figure 1-1: Front panel layout

1.6 Front Panel Status Indicator LEDs

The three status LEDs ("Front panel layout" on the previous page), POWER, SYNC, and FAULT, indicate whether SecureSync is synchronized, whether power is applied to the unit and if any alarms are currently asserted.

The POWER LED will not be lit, if power is not applied to the unit. It will indicate green if power **is** applied. The SYNC and FAULT lamps have multiple states:

- **POWER**: Green, always on
- **SYNC**: Tri-color LED indicates the time data accuracy
- **FAULT**: Two-color, three-state LED, indicating possible equipment fault.

At power up, the unit automatically performs a brief LED test run during which all three LEDs are temporarily lit. The following table provides an overview of the LED status indications:

Table 1-1: SecureSync front panel status indicators

LED Label	Activity/Color	Description
POWER	Off	Both AC and DC Input Power are disconnected. Or, SecureSync's AC input switch is turned off and DC input is not present.
	On/solid green	AC and/or DC Power are supplied; SecureSync detects all power inputs.
	Red	SecureSync is configured for two power inputs, but detects only one power input; or detects a power configuration error.
	Green & blinking orange 1/sec.	Power error; general power configuration fault.
SYNC	Red	Time Sync Alarm: 1) SecureSync has powered up and has not yet achieved synchronization with its inputs. 2) SecureSync was synchronized to its selected input references, but has since lost all available inputs (or the inputs were declared invalid) and the Holdover period has since expired.
	Solid green	SecureSync has valid time and 1PPS reference inputs present and is synchronized to its reference.
	Orange	SecureSync is 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.

LED Label	Activity/Color	Description
FAULT	Off	No alarm conditions are currently active.
	Blinking orange	GNSS antenna problem alarm has been asserted and is currently active. A short or open has been detected in the GNSS antenna cable. The light will automatically turn off when the alarm condition clears (Refer to "Troubleshooting via Web UI Status Page" on page 457 for troubleshooting this condition).
	Solid orange	A Minor alarm condition (other than an antenna problem alarm) has been asserted and is currently active (See "Minor and Major Alarms" on page 455 for troubleshooting this condition).
	Red	A Major alarm condition has been asserted and is currently active (See "Minor and Major Alarms" on page 455 for troubleshooting this condition).

1.7 Rear Panel

The SecureSync rear panel accommodates the connectors for all input and output references.

- Optional AC connection for the power input
- Optional DC power connector
- Ethernet and USB connections
- 1PPS output
- 10 MHz output
- Six bays for option cards
- One optional antenna connector.

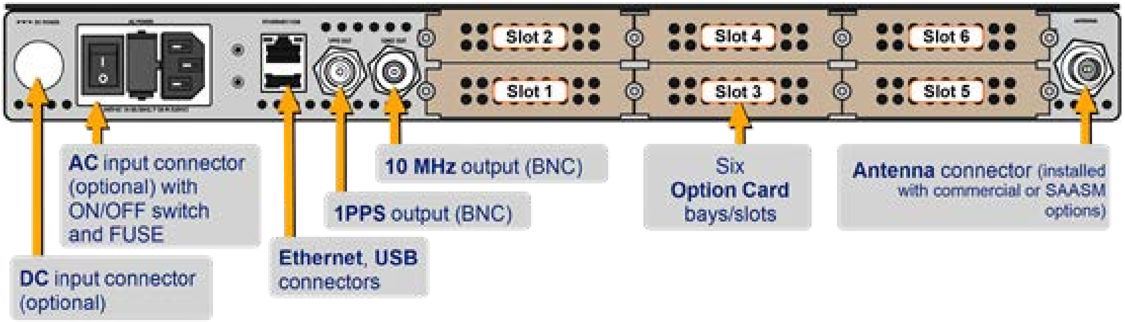

Slot 2
Slot 4
Slot 6
Slot 1
Slot 3
Slot 5
AC input connector (optional) with ON/OFF switch and FUSE
DC input connector (optional)
Ethernet, USB connectors
1PPS output (BNC)
10 MHz output (BNC)
Six Option Card bays/slots
Antenna connector (installed with commercial or SAASM options)

Figure 1-2: Standard rear panel

Typically, **option cards** will be installed at the factory. Should you purchase an extra option card at a later point, you will need to populate the next vacant slot, observing the numerical order shown above. However, not all cards can be installed in all slots. Your local Spectracom Sales Office will gladly assist you with the optimal option cards selection for your application.

The **DC Power** port connector is only installed if your unit was ordered with a DC input power option. Other optional input/output connectors depend on the installed option cards.

Note: DC input power does not have an ON/OFF switch.

- The **AC Power** connector is the input for the AC power and provides an AC power ON/OFF switch. This connector assembly is only installed if SecureSync was ordered with AC input power option.
- The **Ethernet** connector provides an interface to the network for NTP synchronization and to obtain access to the SecureSync product Web UI for system management. It 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.

LED	State	Meaning
Orange	On Off	LAN Activity detected No LAN traffic detected
Green	On Off	LAN Link established, 10 or 100 Mbps No link established

Table 1-2: Status indicators, rear panel

- The **USB** connector is reserved for future expansion.
- The **1PPS** BNC connector offers a once-per-second square-wave output signal. The 1PPS signal can be configured to have either its rising or falling edge to coincide with the system’s on-time point.
- The **10 MHz** BNC connector provides a 10 MHz sine-wave output signal.
- The optional **ANTENNA** connector is a type “N” connector for the GNSS input from your GNSS antenna via a coax cable. This connector will only be present if the standard GNSS receiver, or the optional SAASM GPS receiver module are installed.

1.8 Specifications

Note: The specifications listed herein are for the “base” SecureSync unit (not including option modules) and are based on “standard” operation, with SecureSync synchronized to valid Time and 1PPS input references (in the case of GNSS input, this is with the GNSS receiver operating in Stationary mode). Specifications for the available option modules are provided in "Option Cards Overview" on page 284.

1.8.1 GNSS Receiver

Compatible signals:

- GPS L1 C/A Code transmissions at 1575.42 MHz
- GLONASS L1 0F transmissions centered at 1602.0 MHz
- QZSS L1-SAIF (1575.42 MHz)
- BeiDou B1 (center frequency 1561.098 MHz)
- Galileo-ready E1B/C (firmware upgrade required)

Satellites tracked: Up to 72 simultaneously

Update rate: up to 2Hz (concurrent)

Acquisition time: Typically < 27 seconds from cold start

Antenna requirements: Active antenna module, +5V, powered by SecureSync, 16 dB gain minimum

Antenna connector: Type N, female

1.8.2 RS-232 Serial Port

Function: Accepts commands to locally configure the IP network parameters for initial connectivity

Connector: DB9 female, pin assignments conform to EIA/TIA-574, data communication equipment

Character structure: ASCII, 9600 baud, 1 start, 8 data, 1 stop, no parity

1.8.3 10/100 Ethernet Port

Function: 10/100 Base-T, auto-sensing LAN connection for NTP/SNTP and remote management and configuration, monitoring, diagnostics, and upgrade

Connector: RJ-45, Network IEEE 802.3

1.8.4 Protocols Supported

NTP: NTP Version 4 (Installed: Version 4.2.8p6). Provides MD5, Stratum 1 through 15 (RFC 5905). Note that NTP Autokey is currently not supported, for more information, see http://bugs.ntp.org/show_bug.cgi?id=3005.

NTP throughput: 7000 – 9000 NTP requests per second, depending on used Ethernet port/hardware configuration. Contact Spectracom for additional information.

Clients supported: The number of users supported depends on the class of network and the subnet mask for the network. A gateway greatly increases the number of users.

TCP/IP application protocols for browser-based configuration and monitoring: HTTP, HTTPS

FTP/SFTP: For remote upload of system logs and (RFC 959)

Syslog: Provides remote log storage (RFCs 3164 and 5424)

SNMP: Supports v1, v2c, and v3

Telnet/SSH: For limited remote configuration

Security features: Up to 32-character password, Telnet Disable, FTP Disable, Secure SNMP, SNMP Disable, HTTPS/HTTP Disable, SCP, SSH, SFTP

Authentication: LDAP v2 and v3, RADIUS, MD5 Passwords, NTP Autokey Protocol

1.8.5 1PPS Output

Signal: One pulse-per-second square wave (ext. reference connected to GNSS receiver)

Signal level: TTL compatible, 4.3 V minimum, base-to-peak into 50 Ω

Pulse width: Configurable pulse width (200 ms by default)

Pulse width range: 20 ns to 900 ms

Rise time: <10 ns

Accuracy: Positive edge within ±50 ns of UTC when locked to a valid 1PPS input reference

Connector: BNC female

Table 1-3: 1PPS Output accuracies

Oscillator Type	Accuracy to UTC (1 sigma locked to GPS)	Holdover (constant temp. after 2 weeks of GPS lock)	
		After 4 hours	After 24 hours
Low-phase noise Rubidium	±25 ns	0.2 µs	1 µs
Rubidium	±25 ns	0.2 µs	1 µs
Low-phase noise OCXO	±25 ns	0.5 µs	10 µs
Standard OCXO	±50 ns	1 µs	25 µs
TCXO	±50 ns	12 µs	450 µs

1.8.6 10 MHz Output

Signal: 10 MHz sine wave

Signal Waveform & Levels: +13 dBm ±2dB into 50 Ω

Harmonics: -40 dBc minimum

Spurious: -70 dBc minimum

Connector: BNC female

Table 1-4: 10 MHz output – oscillator accuracies

Oscillator Type	Accuracy
Low-phase noise Rubidium	$1x10^{-12}$ typical 24-hour average locked to GPS
	$1x10^{-11}$ per day ($5x10^{-11}$ per month) typical aging unlocked
Rubidium	$1x10^{-12}$ typical 24-hour average locked to GPS
	$1x10^{-11}$ per day ($5x10^{-11}$ per month) typical aging unlocked
Low-phase noise OCXO	$1x10^{-12}$ typical 24-hour average locked to GPS
	$2x10^{-10}$ per day typical aging unlocked
Standard OCXO	$2x10^{-12}$ typical 24-hour average locked to GPS
	$1x10^{-9}$ per day typical aging unlocked
TCXO	$1x10^{-11}$ typical 24-hour average locked to GPS
	$1x10^{-8}$ per day typical aging unlocked

Note: Oscillator accuracies are stated as fractional frequency (i.e. the relative frequency departure of a frequency source), and as such are dimensionless.

See also "Oscillator Disciplining" on page 188.

Table 1-5: 10 MHz output – oscillator stabilities

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	$5x10^{-11}$	$2x10^{-11}$	$1x10^{-11}$	$1x10^{-9}$
Standard OCXO	$5x10^{-10}$/day	$5x10^{-10}$	$5x10^{-11}$	$1x10^{-11}$	$5x10^{-9}$
TCXO	$1x10^{-8}$/day	$2x10^{-9}$	$1x10^{-9}$	$3x10^{-10}$	$1x10^{-6}$

1.8.6.1 10 MHz output – oscillator phase noise (dBc/Hz)

Oscillator Type	@ 1Hz	@ 10 Hz	@ 100 Hz	@ 1KHz	@ 10 KHz
Low-phase noise Rubidium	-100	-128	-148	-153	-155

Oscillator Type	@ 1Hz	@ 10 Hz	@ 100 Hz	@ 1KHz	@ 10 KHz
Rubidium	-80	-98	-120	-140	-140
Low-phase noise OCXO	-100	-128	-148	-153	-155
Standard OCXO	-95	-123	-140	-145	-150
TCXO	./.	./.	-110	-135	-140

1.8.7 Input Power

AC power source: 100 to 240 VAC, 50/60 Hz, +/- 10% and 100-120 VAC 400 Hz, +/- 10% via an IEC 60320 connector (power cord included)

DC input (option): 12-17 V_{DC} -15%, +20% or 21-60 VDC -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 (Rb) oscillator installed: 52 W normal (85 W start-up)

1.8.8 Fuses

Type: T 2A L 250 V

Model:

- Spectracom recommends: LITTELFUSE 0213002.MXP
- [Spectracom part number: F010R-0002-000 E FUSE,2A,SB,IEC SURGE,GLASS]

Number: 2 (two) per unit

SecureSync label on rear panel of unit:

- **"AC POWER/F 2A T 250V (2)"**
  - LEGEND:
    - F = Fuse
    - 2A = Current Rating: 2 Ampères
    - T = Speed: Time Delay (Slow-Blow)
    - L = Breaking Capacity: Low (Glass)
    - 250V = Voltage Rating
    - (2) = Fuses used: 2 (two)

Caution: Before testing fuses, remove AC power by disconnecting the AC power cord.

Note: In the event that the unit does not power up with AC power, these fuses should be tested.

1.8.9 Mechanical and Environmental Specifications

Dimensions:

- Designed for EIA 19” rack mount
- Housing w/o connectors and brackets:
  - 16.54” W x 1.72” H [1U] x 14.33” D
  - (420 mm W x 44 mm H x 365 mm D)

Weight:

- 6.0 lbs (2.72 kg)
- 6.5 lbs. (2.95 kg) for Rubidium options

Temperature:

- Operating range: -20°C to +65°C (+55°C for Rubidium option)
- Storage range: -40° to 85°C

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

Altitude:

- Operating range, (AC, 50/60 Hz): 6560 ft (2000 m)
- Operating range, (DC, 400 Hz): 13100 ft (4000 m)
- Storage range: 45000 ft (13700 m)

Shock:

- 15 g, 11 ms, half sine wave operating range
- 50 g, 11 ms, trapezoidal pulse storage range

Vibration:

- 10 to 55 Hz/0.07 g, 55 to 500 Hz/1.0 g operating range
- 10 to 55 Hz/0.15 g, 55 to 500 Hz/2.0 g storage range

MIL-STD-810F: 501.4, 502.4, 507.4, 500.4, 516.5, 514.5

1.9 Regulatory Compliance

This product has been found to be in conformance with the following regulatory publications.

FCC

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

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

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

Safety

EN 60950-1:2006/A11:2009: Safety of Information Technology Equipment, including Electrical Business Equipment

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

- UL 60950-1, 1st Edition
- CSA C22.2 No. 60950-1-07, 2nd Edition
- UL Listing no. E311040

EMC, CE:

- EN 55022:2006/A1:2007: Class A: EC Emissions Standard
- EN 55024:1998/A2:2003: EC Generic Immunity Standard
- EN 61000-3-2:2006: Harmonic Current Emissions
- EN 61000-3-3:1995/A2:2005: Voltage Fluctuations and Flicker
- The product complies with the requirements of the **Low Voltage Directive 2006/95/EC** and the **EMC Directive 2004/108/EC**.

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

EMC, ICES-003 and AS/NZS CISPR 22:

- This Class (A) digital apparatus complies with Canadian ICES-003, Issue 4.
- This Class (A) digital apparatus complies with AS/NZS CISPR 22 for radiated and conducted Emissions.

BLANK PAGE.

CHAPTER 2

INSTALLATION

This Chapter guides you through the preparation of the hardware, the installation of the SecureSync Time and Frequency Synchronization System, its hardware interfaces, and setup tasks required to be performed before configuring the product.

The following topics are included in this Chapter:

2.1 Installation and Setup Summary

This section provides an outline of the SecureSync installation process. The exact installation procedure of your unit depends on several factors:

a. The power source(s) your SecureSync is configured for.

b. Your existing infrastructure and how you plan on integrating SecureSync into it (for example, integrating it into an existing Ethernet network, or setting-up a standalone installation.)

c. How you would like to configure your SecureSync unit:

   - Via the front panel keypad and information display
   - Using a Personal Computer (PC) with a Command-Line Interpreter (CLI), connected to SecureSync via the serial port in front of the unit
   - Using the SecureSync Web User Interface ("Web UI").

   The latter is the recommended configuration tool, since it offers access to ALL configuration options. For this, you will need a PC with a standard Web browser, such as Google Chrome®, Mozilla Firefox®, or Microsoft Internet Explorer®.

   You can connect your PC to SecureSync either...

   - ...directly by means of an Ethernet cable, or
   - ...indirectly through your existing Ethernet network (using a network hub).

d. The option cards configuration of your unit: Is your SecureSync equipped with any option cards, such as additional input references, or additional signal distribution cards? If so, they need to be configured separately via the SecureSync Web UI, once the network configuration is complete.

2.1.1 Main Installation Steps

The following list is a recommendation. Deviations are possible, depending on the actual application and system configuration.

1. Unpack the unit, and take inventory: "Unpacking and Inventory" on the facing page.
2. Obtain required tools and parts: "Required Tools and Parts for Installation" on page 20.
3. Mount the unit: "Rack Mounting" on page 23.
4. Read the Safety instructions: "SAFETY" on page 20.
5. Connect your power supply/-ies: "Power Connection" on page 25.
6. Connect Input References such as your GNSS antenna, and network cable(s): "Connecting Reference Inputs, and Network Interfaces" on page 28.
7. Power up the unit: "Powering up the Unit" on page 29.

8. Configure the unit…
   1. …via front panel keypad and information display: "Network Configuration via Front Panel" on page 36
   2. …or via serial port, using a PC with a CLI: "Network Configuration via Serial Port" on page 37
   3. …or via Ethernet, using a PC with a Web browser, and the SecureSync Web UI: "DHCP Network Configuration" on page 33.
9. Register your product: "Product Registration" on page 39.

2.2 Unpacking and Inventory

Caution: Electronic equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD precautions and safeguards when handling the unit.

Unpack the equipment and inspect it for damage. If any equipment has been damaged in transit, or you experience any problems during installation and configuration of your Spectracom product, please contact your closest Spectracom Customer Service Center (see "Regional Contact" on page 515.)

Note: Retain all original packaging for use in return shipments if necessary.

The following items are included with your shipment:

- SecureSync Unit
- QuickStart Guide (printed version)
- This instruction manual, and other relevant documentation as pdf files on a CD
- Purchased Optional Equipment
- Ancillary kit (except for rack mounting items, contents of this kit, such as an AC line cord, will vary based on equipment configuration)
- Any option cards on the original purchase order have been pre-installed. See "Option Card Identification" on page 287 and "Option Cards Overview" on page 284.

2.3 Required Tools and Parts for Installation

- Phillips screwdriver to install the unit’s rack-mount ears.
- Screwdriver to mount the unit in a standard 19-inch rack.
- Ethernet cables (see "Ethernet Connection" on page 29)
- For DC power supply (if applicable), Spectracom recommends an external ON/OFF switch.

2.4 SAFETY

2.4.1 Safety: Symbols Used

Figure 2-1: Do not ignore the Safety Instructions!

Table 2-1: Safety symbos used by Spectracom in this document, or on the product

Symbol	Signal word	Definition
⚡	DANGER!	Potentially dangerous situation which may lead to personal injury or death! Follow the instructions closely.
⚠	CAUTION!	Potential equipment damage or destruction! Follow the instructions closely.
ℹ	NOTE	Tips and other useful or important information.
⚠	ESD	Risk of Electrostatic Discharge! Avoid potential equipment damage by following ESD Best Practices.
⏚	CHASSIS GROUND	This symbol is used for identifying the functional ground of an I/O signal. It is always connected to the instrument chassis.

Symbol	Signal word	Definition
⏚	Analog Ground	Shows where the protective ground terminal is connected inside the instrument. Never remove or loosen this screw!
♻	Recycle	Recycle the mentioned components at their end of life. Follow local laws.

2.4.2 SAFETY: Before You Begin Installation

This product has been designed and built in accordance with state-of-the-art standards and the recognized safety rules. Nevertheless, its use may constitute a risk to the operator or installation/maintenance personnel, if used under conditions that must be deemed unsafe, or for purposes other than the product's designated use, which is described in the introductory technical chapters of this guide.

Before you begin installing and configuring your SecureSync unit, carefully read the following important safety statements. Always ensure that you adhere to any and all applicable safety warnings, guidelines, or precautions during the installation, operation, and maintenance of your product.

DANGER! – INSTALLATION OF EQUIPMENT:

Installation of this product is to be done by authorized service personnel only. This product is not to be installed by users/operators without legal authorisation.

Installation of the equipment must comply with local and national electrical codes.

DANGER! – DO NOT OPEN EQUIPMENT, UNLESS AUTHORIZED:

The interior of this equipment does not have any user serviceable parts. Contact Spectracom Technical Support if this equipment needs to be serviced. Do not open the equipment, except to retrofit option cards, or replacement of battery. Follow Spectracom Safety Instructions, and observe all local electrical regulatory requirements.

IF THE EQUIPMENT MUST BE OPENED:
Never remove the cover or blank option card plates with power applied to this equipment. Ensure all power sources are removed from the unit prior to installing any option cards by removing both the AC and DC power cords connected to the equipment.

This unit will contain more than one power source if both the AC and DC power options are present. In this case, turning off the rear panel power switch will not remove all power sources.

DANGER! – FUSING:

The equipment has Double Pole/Neutral Line Fusing on AC power.
For continued protection against risk of fire, replace fuses only with same type and rating of fuse.

DANGER! – GROUNDING: This equipment must be EARTH GROUNDED. Never defeat the ground connector or operate the equipment in the absence of a suitably installed earth ground connection. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

The AC and DC power connectors of this equipment have a connection to the earthed conductor of the AC and DC supply earthing conductor through the AC and DC power cords. The AC source outlet must contain a protective earthing connection. This equipment shall be connected directly to the AC power outlet earthing pin or DC supply system earthing electrode conductor. The DC supply source is to be located within the same premises as this equipment: The equipment shall be located in the same immediate area (such as, adjacent cabinets) as any other equipment that has a connection to the earthing conductor of the same AC or DC supply circuit earthing conductor, and also the point of earthing of the AC or DC system. The AC or DC system shall not be earthed elsewhere.

Switches or other disconnection devices shall not be in the earthed circuit conductor between the AC and DC source and the point of the connection of the earthing electrode conductor to SecureSync's AC and DC input power connectors earthing pin.

DANGER! – BATTERY: Replace the battery only with the same or equivalent type recommended by the manufacturer. Follow Spectracom Instructions – there is a danger of a new battery exploding if it is incorrectly installed. Discard used batteries according to the manufacturer's instructions.

Caution: Electronic equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD precautions and safeguards when handling Spectracom equipment.

2.4.3 SAFETY: User Responsibilities

- The equipment must only be used in technically perfect condition. Check components for damage prior to installation. Also check for loose or scorched cables on other nearby equipment.
- Make sure you possess the professional skills, and have received the training necessary for the type of work you are about to perform.
- Do not modify the equipment.
- Use only spare parts authorized by Spectracom.
- Always follow the instructions set out in this User Reference Guide, or in other Spectracom documentation for this product.
- Observe generally applicable legal and other local mandatory regulations.

2.4.4 SAFETY: Other Tips

- Keep these instructions at hand, near the place of use.
- Keep your workplace tidy.
- Apply technical common sense: If you suspect that it is unsafe to use the product, do the following:
  - Disconnect the supply voltage from the unit.
  - Clearly mark the equipment to prevent its further operation.

2.5 Rack Mounting

If installing the unit in a rack, install the rack-mount ears on the two sides of the front panel and mount the unit in a standard 19-inch rack cabinet. The unit is intended to be installed in one orientation only. The unit should be mounted so the front panel interface keys are to the left of the display area.

The SecureSync unit will install into any EIA standard 19-inch rack. SecureSync occupies one rack unit of space for installation, however, it is recommended to leave empty space of at least one rack unit above and below the SecureSync unit to allow for best ventilation.

Rack mounting requirements:

- The maximum **ambient operating temperature** must be observed. See "Mechanical and Environmental Specifications" on page 14 for the operating temperature range specified for the type of oscillator installed in your SecureSync unit.
- If the SecureSync unit is to be installed in a closed rack, or a rack with large amounts of other equipment, a **rack cooling fan** or fans should be part of the rack mount installation.
- Installation of the unit in a rack should be such that the amount of **air flow** required for safe operation of the equipment is not compromised.
- Follow the mounting directions described below to **prevent uneven mechanical loading**, possibly resulting in a hazardous condition.
- **Do not overload power supply circuits**. Use only supply circuits with adequate overload protection. For power requirements, see "Specifications" on page 9.
- Reliable **grounding** of rack-mounted equipment must be maintained. Particular attention must be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips).

The SecureSync ancillary kit will contain the following parts needed for rack mounting:

- 2 each 1165-1000-0714 rack mounting brackets
- 2 each MP09-0003-0030 equipment rack handles
- 4 each H020-0832-0406 #8-32 flat head Phillips screws
- 6 each HM20R-04R7-0010 M4 flat head Phillips screws
- one (1) CA0R-1513-0001 AC POWER CORD.

The following **customer supplied items** are also needed:

- 4 each #10-32 pan head rack mount screws
- 1 each #2 Phillips head screwdriver
- 1 each 3/32" straight screwdriver

To rack mount the SecureSync unit:

1. Attach an MP09-0003-0030 equipment rack handle to the front of each 1165-1000-0714 rack mounting bracket, using the holes nearest the right angle bend of the 1165-1000-0714 rack mounting bracket, with the #2 size Phillips screwdriver, using 2 each of the H020-0832-0406 #8-32 flat head Phillips screws.
2. Attach the 1165-1000-0714 rack mount brackets to the sides of the SecureSync with the rack mounts ears facing outward, aligned with the front edge of the SecureSync front panel. Use the #2 Phillips screwdrivers, using 3 each of the HM20R-04R7-0010 M4 flat head Phillips screws.
3. Secure the rack mount brackets to the rack using the #10-32 rack mount screws and #2 Phillips head screwdriver, 2 each per side of the rack.

Caution: For safety reasons, the SecureSync unit is intended to be operated in a HORIZONTAL POSITION, RIGHT-SIDE-UP, that is with the keypad to the left side and the 4-line information display and the time display on the right side.

2.5.1 Desktop Operation

SecureSync units can also be operated on a desktop in a HORIZONTAL, RIGHT-SIDE-UP position. The location needs to be well-ventilated, clean and accessible.

2.6 Power Connection

Depending on the equipment configuration at time of purchase, SecureSync can be powered from an AC input, a DC input or with both AC and DC input (DC input is an option). Supplying both AC and DC input power provides redundant and automatic power switchover in case one or the other input power sources is lost.

Before connecting power to the unit, be sure that you have read all safety information detailed in section "SAFETY" on page 20.

2.6.1 Input Power Selection

As long as the AC input power is present, and SecureSync is equipped with the DC redundancy option, it will utilize the AC power source over DC power.

- If AC and DC power are both applied, AC power is used.
- If DC power is applied, but AC power is not, then DC power will be used.
- If AC and DC power are both present, but AC power is subsequently lost, SecureSync will automatically switch to using the DC power input.

DANGER! – This unit will contain more than one power source if both the AC and DC power options are present. Turning off the rear panel power switch will NOT remove all power sources.

The following sections discuss AC and DC power input. Connect AC and/or DC power, as desired.

2.6.2 Using AC Input Power

Connect the AC power cord supplied in the SecureSync ancillary kit to the AC input on the rear panel and the AC power source outlet. The AC input is fuse-protected with two fuses located in the AC power entry module (line and neutral inputs are fused). The AC power entry module also contains the main power switch for the AC power applied to the equipment.

Caution: This equipment has Double Pole/Neutral Line Fusing on AC power.

Note: Important! SecureSync is earth grounded through the AC power connector. Ensure SecureSync is connected to an AC outlet that is connected to earth ground via the grounding prong (do not use a two prong to three prong adapter to apply AC power to SecureSync).

2.6.3 Using DC Input Power

If the rear panel DC port is present, connect DC power, per the voltage and current as called out on the label that resides above the DC power connector.

Note: DC power is an option chosen at time of purchase. The rear panel DC input port connector is only installed if the DC input option is available. Different DC power input options are available (12 V_{DC} with a voltage range of 12 to 17 V at 7 A maximum or 24/48 V_{DC} input with a voltage range of 21 to 60 V at 3 A maximum). Review the DC power requirement chosen, prior to connecting DC power (when the DC port is installed, a label will be placed over the connector indicating the allowable DC input voltage range and the required current).

DANGER! GROUNDING: SecureSync is earth grounded through the DC power connector. Ensure that the unit 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.

Caution: The DC input port is both fuse and reverse polarity protected. Reversing polarity with the 24/48 V_{DC} option will not blow the fuse, but the equipment will not power-up. Reversing polarity with the 12 V_{DC} option will likely blow the internal fuse.

A DC power connector to attach DC power to SecureSync is included in the ancillary kit provided with the equipment. 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 cable clamp provided with the DC power plug for strain relief of the DC power input cable should be used when DC power is connected to SecureSync.

Note: Spectracom recommends to use a dedicated DC power supply switch to energize/de-energize SecureSync externally.

DC power connector pin-out:

SecureSync units can be ordered in a DC version that includes the following DC plug on the back panel: **DC Plug, 3-pin, chassis mount:** Amphenol P/N DL3102A10SL-3P

The DC ancillary kit includes, among other things, the following connector parts:

- **Mating DC Connector**, circular, 3-pin, solder socket, 16AWG,13A,300V: Amphenol P/N DL3106A10SL-3S; (Spectracom part no. P240R-0032-002F)

- **Cable Clamp**, circular: Amphenol part no. 97-3057-1004(621); (Spectracom part no. Spectracom part no. MP06R-0004-0001)

Pinout description, DC connector

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

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

2.7 Connecting Reference Inputs, and Network Interfaces

SecureSync can synchronize to various external inputs (including GNSS, IRIG, NTP, PTP, 1PPS, ASCII time code, HAVE QUICK, 10 MHZ and/or a user set time).

Depending on the desired operation and your specific SecureSync configuration, connect the GNSS, IRIG, 1PPS or other external references (**NTP input reference** and **User-Set Time** are software configurations that require no additional physical connection to SecureSync).

2.7.1 Connecting GNSS Input

Typical installations include GNSS as an external reference input. If the GNSS receiver is not installed or if the GNSS will not be used as a SecureSync reference, disregard the steps to install the GNSS antenna and associated cabling.

1. Install the GNSS antenna, surge suppressor, antenna cabling, and GNSS preamplifier (if required). Refer to the documentation included with the GNSS antenna for additional information regarding GNSS antenna installation.
2. Connect the GNSS cable to the rear panel antenna input jack (see illustration under "Rear Panel" on page 8).
   In the event that NO antenna is connected to the rear panel jack, SecureSync will—once it gets powered up (see "Powering up the Unit" on the facing page)—activate the **Antenna Problem** alarm, causing the front panel "**Fault**" light to be blinking orange (the **Antenna Problem** alarm indicates an open or short exists in the antenna cable.)
   Unless there is an open or short in the antenna cable, the "**Fault**" light should stop flashing orange once the GNSS antenna and coax cable are connected to the rear panel. If the "**Fault**" light does not stop flashing after connecting the antenna, refer to "Troubleshooting GNSS Reception" on page 459.

Initial synchronization with GNSS input may take up to 5 minutes (approximately) when used in the default stationary GNSS operating mode. If using GNSS, verify that GNSS is the synchronization source by navigating to **MANAGEMENT/OTHER/Reference Priority**: Confirm that GNSS is **Enabled**, and its **Status** for TIME and 1PPS is valid (green).

2.7.2 Connecting IRIG Input

With the available IRIG Input/Output option card module (Model 1204-05) installed in an option bay, IRIG time code from an IRIG generator can also be applied as an external reference input (either in addition to, or in lieu of GNSS, NTP, user set time and other available reference inputs).

If IRIG input is desired:

- Connect the IRIG time source to the BNC connector “J1” on the IRIG Input/Output module. Refer to the IRIG Input/Output module section for additional information regarding IRIG Reference input.

2.7.3 Ethernet Connection

SecureSync provides a base 10/100 Ethernet port for full NTP functionality, as well as a comprehensive Web-based user interface for configuration, monitoring and diagnostic support. Additional network ports are available with the Gigabit Ethernet option card (1204-06).

The Ethernet port is provided on the back panel for easy connection to routers, switches, or hubs.

1. Determine if you want to configure your SecureSync unit using a computer connected to the network, or a computer connected directly to your SecureSync unit.
   - When connecting to a hub, router, or network computer, use a straight-through wired, shielded CAT 5, Cat 5E or CAT 6 cable with RJ-45 connectors. Connect one end to the Ethernet port on the SecureSync rear panel, and the opposite end of the cable to a network hub or switch.
   - When connecting directly to a stand-alone Personal Computer (PC), use a network cable. Connect the cable to the NIC card of the computer.
     Since no DHCP server is available in this configuration both SecureSync, and the PC must be configured with static IP addresses that are on the same subnet (10.1.100.1 and 10.1.100.2 with a subnet value of 255.255.255.0 on both devices, for example). For more information on configuring static IP addresses, please refer to "Network Configuration Without DHCP" on page 35, and to the product documentation for the version of the operating system that you are using on the PC.
2. With input references connected, once SecureSync is powered up (see: "Powering up the Unit" below), verify that the green link light on the Ethernet port is illuminated. The amber “Activity” link light may periodically illuminate when network traffic is present.

2.8 Powering up the Unit

1. After installing your SecureSync unit, and connecting all references and network(s), verify that power is connected, turn ON the unit using the switch on the rear panel (only if equipped with AC power input), and wait for the device to boot up.

> **Note:** DC input power is not switched, so SecureSync will be powered up with DC input connected, unless you installed an external power switch.

Note: As the front panel cooling fan is internal temperature controlled, the fan may not always be in operation. However, the fan may momentarily turn on each time SecureSync is power-cycled.

2. Observe that all of the front panel LEDs momentarily illuminate (the Power LED will then stay lit) and that the Information display LCD back light illuminates.

   The time display will reset and then start incrementing the time. About 10 seconds after power-up, “Starting up SecureSync” will be displayed in the information display. After approximately 2 minutes, the information display will then show the current network settings.

   The 4-line information display shows the unit’s hostname, IPv4 address, mask, and gateway.
   The time display shows the current time: UTC, TAI, GPS or local timescale, as configured. Current time will be displayed in UTC by default.

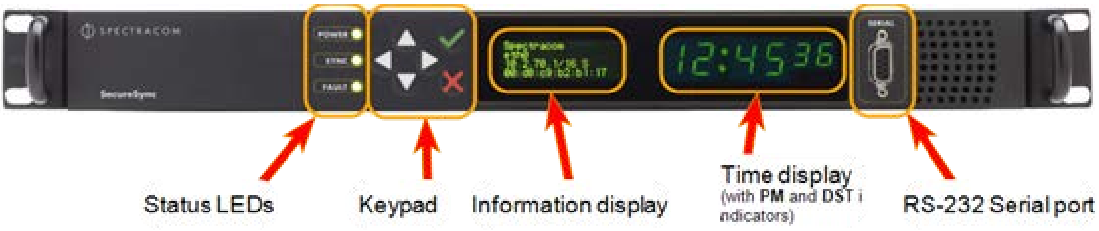


Figure 2-2: SecureSync front panel

3. Check the front panel status LED indicators:
   - The **Power** lamp should be solid green.
   - The **Sync** lamp will probably be red, since synchronization has not yet been achieved.
   - The **Fault** lamp should either be off, or solid orange, indicating a minor alarm.

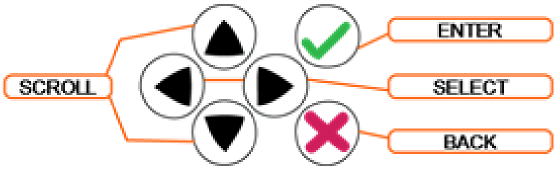
For additional information, see "Front Panel Status Indicator LEDs" on page 228 and "Status Monitoring via Front Panel" on page 228.

2.9 Using the Keypad and Information Display

To simplify operation and to allow local access to SecureSync, a keypad and LCD information display are provided on the front panel of the unit.

Among other things, the keypad and information display can be used to carry out basic network configuration tasks, such as en-/disabling DHCP, or entering an IP address and subnet mask; see below for details.

2.9.1 Keypad Description



The SecureSync front panel keypad has six buttons for making certain configuration changes or viewing status information on the LCD display. The functions of each are as follows:

- **ENTER**: Select a menu item or load a parameter when editing
- **BACK**: Return to previous display or abort an edit process
- **LEFT/RIGHT arrows**: Select a new item to the left or right, respectively
- **UP/DOWN arrows**: Scroll through parameter values in edit displays

2.9.2 Navigating the Information Display

After power initialization, press any key to go to the “Home” display. As shown in the illustration "Keypad menu tree" on the next page, several status and setup displays are accessible from the main “Home” menu. To navigate through the menus, use the arrow keys to highlight a selection and then press the ENTER button.

The main menu options and their primary functions are as follows:

- **Display**: Used to configure the information display
- **Clock**: Displaying and setting of the current date and time
- **System**: Displaying version info, system halt and reboot, reset `spadmin` password
- **Netv4**: Network interface configuration
- **Lock**: Locks the front panel keypad to prevent inadvertent operation.

2.9.3 Keypad Menu Tree

Using the front panel keypad, the 4-line information display on the unit can be configured to display various indications, including the network settings, System Status, GNSS position, GNSS signal information or the current date and time (or, it can even be configured to remain blank, if desired). The figure "Keypad menu tree" on the next page illustrates Menu Tree navigation.

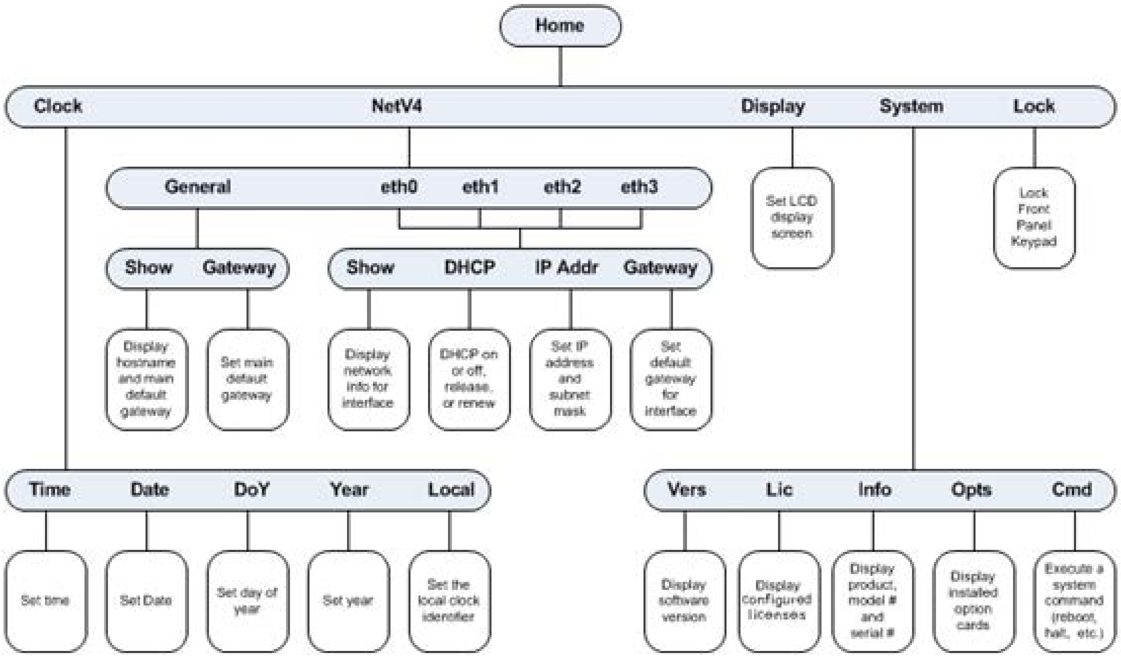

Home
Clock
NetV4
Display
System
Lock
General
eth0
eth1
eth2
eth3
Set LCD display screen
Lock Front Panel Keypad
Show
Gateway
Show
DHCP
IP Addr
Gateway
Display hostname and main default gateway
Set main default gateway
Display network info for interface
DHCP on or off, release, or renew
Set IP address and subnet mask
Set default gateway for interface
Time
Date
DoY
Year
Local
Vers
Lic
Info
Opts
Cmd
Set time
Set Date
Set day of year
Set year
Set the local clock identifier
Display software version
Display configured licenses
Display product, model # and serial #
Display installed option cards
Execute a system command (reboot, halt, etc.)

Figure 2-3: Keypad menu tree

To modify a parameter, highlight the menu option and press the ENTER button. The “O” data is the current old setting and the “N” data is the new setting. You can only change the “N” setting in all menus. Use the UP and DOWN arrow keys to scroll through all possible parameter values.

When editing a sequence of numbers, use the LEFT and RIGHT arrow keys to select other digits. When the parameter is correct, press ENTER to load the new value. You will be asked to confirm the setting change. Press ENTER to accept or BACK to cancel the parameter change. All entered values are stored in memory and restored after a power cycle.

2.9.4 Unlocking the Front Panel Keypad

If the front panel keypad is locked, the following sequence will locally unlock the keypad for use. Alternatively, the front panel can also be locked/unlocked via the SecureSync Web UI, see "Locking/Unlocking the Front Panel Keypad" on page 183.

↑ ↓ ↑ ↓ ← → ← → ✓ x ✓

2.10 DHCP Network Configuration

2.10.1 Opening the Web UI

On a network using DHCP, SecureSync's IP address will be assigned automatically once it is connected to the DHCP server. This address and other network information are displayed on the front panel when the device boots up.

1. On a computer connected to the SecureSync network, start a Web browser, and enter the above-mentioned IP address of your SecureSync into the address field of the browser.
2. Log in as an administrator (see: "The Administrator Login Password" on page 218).

Note: "Cookies" must be enabled. You will be notified, if Cookies are disabled in your browser.

Unless you are using DNS in conjunction with DHCP (with the client configured using SecureSync's hostname instead of IP address), Spectracom recommends to disable DHCP for SecureSync, and change the IP address to a static address. Failure to do this will result in a loss of time synchronization, should the DHCP server assign a new IP address to SecureSync.

If you choose to use DHCP for your SecureSync, the basic network configuration is complete, and you may proceed to "Product Configuration via the Web UI" on page 42, in order to proceed with the configuration of your SecureSync. Otherwise, proceed to "Replacing a Dynamic with a Static IP Address" on the next page

Note: Unless the user opens the Web UI using the default DNS name of “Spectracom” (instead of using the IP address to access SecureSync), the SSL certificate/security pop-up window will continue to be displayed each time the user opens the Web UI.

To prevent the security pop-up window from opening each time, a new SSL certificate needs to be created using the assigned IP address of SecureSync during the certificate generation. See "Configuring HTTPS" on page 63 for more information on creating a new SSL certificate.

Note: When configuring SecureSync without DHCP, or to configure a SecureSync unit that has not been assigned an IP address for other reasons, see "Network Configuration Without DHCP" on page 35.

2.10.2 Replacing a Dynamic with a Static IP Address

Note: During configuration it may be necessary to power down or restart SecureSync. In this case a HALT command should be issued prior to removing power from the unit. Failure to do so may cause SecureSyncto take longer to boot on the next power up cycle. After the HALT command is issued via the front panel keypad, or the Web UI, wait until the information display reads ‘Power off SecureSync’ before removing power.

Spectracom recommends assigning a static IP address to SecureSync, even if it is connected to a DHCP server. While this can be accomplished using the front panel keypad, or a PC connected to SecureSync's serial port, the most convenient way is using the SecureSync Web user interface ("Web UI"): The dynamic IP address assigned to your SecureSync unit by DHCP will allow you to readily access the Web UI, in order to carry out the desired changes.

Before continuing, obtain the following network information from your network administrator:

- **Available static IP Address**
  - This is the unique address assigned to the SecureSync unit by the network administrator. Make sure the chosen address is outside of the DHCP range of your DHCP server. The default static IP address of the SecureSync unit is 10.10.20x.1 (x= dependent on ETH port, if Ethernet Gigabit option card 1204-06 is installed).
- **Subnet mask (for the network)**
  - The subnet mask defines the number of bits taken from the IP address that are used in the network portion. The number of network bits used in the net mask can range from 8 to 30 bits.
- **Gateway address**
  - The gateway (default router) address is needed if communication to the SecureSync is made outside of the local network. By default, the gateway is disabled.

To replace DHCP network settings with a static IP address:

1. Enter the IP address shown on the front panel information display of your SecureSync unit into your browser (on a computer connected to your network). If the network supports DNS, the hostname may also be entered instead (the default hostname is "Spectracom"). The start screen of the SecureSync Web UI will be displayed.
2. Log into the Web UI as an administrator. The factory-default user name and password are:
   Username: `spadmin`
   Password: `admin123`
3. Disable DHCP, see: "Configuring Network Ports" on page 48.
4. Manually enter the desired static IP address, subnet mask, and gateway address (if required), see: "Configuring Network Ports" on page 48. For subnet mask values, see table "Subnet mask values" on page 38.

5. Enter the static IP address you assigned to your SecureSync unit, and again log into the Web UI in order to continue with the configuration; see: "Product Configuration via the Web UI" on page 42.

> **Note:** Make sure you are assigning a static IP address to your SecureSync unit that is outside of the DHCP range defined for the DHCP server. Your system administrator will be able to tell you what this range is.

2.11 Network Configuration Without DHCP

> **Note:** During configuration it may be necessary to power down or restart SecureSync. In this case a HALT command should be issued prior to removing power from the unit. Failure to do so may cause SecureSyncto take longer to boot on the next power up cycle. After the HALT command is issued via the front panel keypad, or the Web UI, wait until the information display reads 'Power off SecureSync' before removing power.

2.11.1 Assigning a Static IP Address

To configure a SecureSync that has not yet been assigned an IP address (because your network does not support DHCP, for example), there are two ways to enter the desired static IP address, subnet mask, and gateway address.:

- The front panel keypad and 4-line information display, or
- A personal or laptop computer, connected via serial cable to the serial port on the SecureSync front panel.

The keypad is the simplest method to configure the network settings. See "Using the Keypad and Information Display" on page 30 for information on using the keypad. See "Configuring Network Ports" on page 48 for steps to disable the factory-default DHCP setting, and to configure the IP address, subnet mask and gateway address.

Before continuing, obtain the following network information from your network administrator:

- **Available static IP address**
  - This is the unique address assigned to the SecureSync unit by the network administrator. Make sure the chosen address is outside of the DHCP range of your DHCP server. The default static IP address of the SecureSync unit is 10.10.20x.1 (x= dependent on ETH port, if Ethernet Gigabit option card 1204-06 is installed).
- **Subnet mask (for the network)**

- The subnet mask defines the number of bits taken from the IP address that are used in the network portion. The number of network bits used in the net mask can range from 8 to 30 bits.
- **Gateway address**
  - The gateway (default router) address is needed if communication to the SecureSync is made outside of the local network. By default, the gateway is disabled.

2.11.2 Network Configuration via Front Panel

A. **First, disable DHCP:**

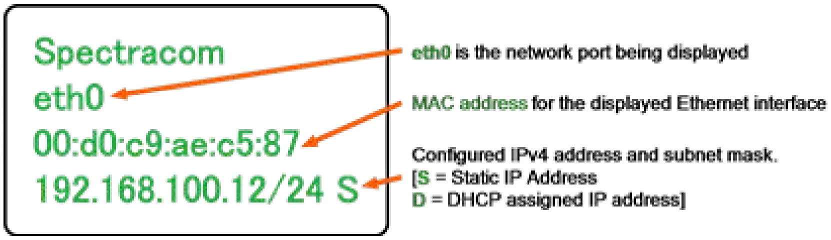
1. Press the ✓ key.
2. Using the arrow key, select `Netv4` from the menu.
   (To select a menu item, highlight it using the arrow keys, then press the ✓ key.)
3. Select the Ethernet interface for which DHCP is to be disabled, such as `eth0`.
4. Delect `DHCP` from the next menu. The display will show `State= Enabled` and `Action=Disabled`.
   Press the ✓ key once to select the action, then again to apply it.
   (The **State** is the current DHCP setting and the **Action** is the action to take. You can only change the Action setting.)
5. Press the ✓ key once to select the action, then again to apply it.

B. Then, enter IP Address and Subnet Mask:

1. Still on the `Home/Netv4/eth[0-3]` menu, select `IP Address`, and change "`N=010.010.201.001/16`" to the value of the static IP address and subnet mask/network bits to be assigned (refer to the table "Subnet mask values" on page 38 for a list of subnet mask values).
2. Press the ✓ key once to enter the setting, then again to apply the new setting.

C. Lastly, enter the Gateway Address (if required).

After all addresses are entered, press the front panel ✕ key three times to return to the main display. It should now resemble the following example:



```
Spectracom
eth0
00:d0:c9:ae:c5:87
192.168.100.12/24 S
```

eth0 is the network port being displayed

MAC address for the displayed Ethernet interface

Configured IPv4 address and subnet mask.
[S = Static IP Address
D = DHCP assigned IP address]

DNS: The Primary and Secondary DNS servers are set automatically if using DHCP. If DHCP is not available, they can be configured manually in the SecureSync Web UI via the **Network/General Setup** screen.

Note: The remainder of the configuration settings will be performed through the SecureSync Web UI (accessed through a Web browser such as Firefox® or Chrome®). For more information, see "Product Configuration via the Web UI" on page 42.

2.11.3 Network Configuration via Serial Port

Next to the keypad and 4-line information display, the front panel also contains a DB9 serial port that can be used to communicate with SecureSync. The serial port connector is a standard DB9 female connector. Communication with the serial port can be performed using a terminal emulator program (such as HyperTerminal or Procomm) using a pinned straight-thru standard DB9M to DB9F serial cable.

The serial port can be used to make configuration changes (such as the network settings), retrieve operational data (such as the GNSS receiver information) or to perform operational processes (such as resetting the admin password).

The serial port is account and password protected. Login via the serial port using the same user names and passwords as would be used to log into the SecureSync Web UI. Users with "administrative rights" can perform all available commands. Users with "user" permissions only can perform "get" commands that retrieve data, but cannot perform any "set" commands or change/reset any passwords.

Refer to "Setting up a Terminal Emulator" on page 466 for more information on the serial port connection, and "CLI Commands" on page 467 for a list and description of the available command line (CLI) commands that can be issued.

To configure SecureSync's network settings using the front panel serial port:

1. Connect a serial cable to a PC running HyperTerminal, and to your SecureSync.
2. Login to SecureSync with a user account that has "admin" group rights, such as the default `spadmin` account (the default password for `spadmin` is `admin123`).
3. To disable DHCP, type: `dhcp4set 0 off` <Enter>.

Note: If your SecureSync is configured with an Ethernet option card, use 0, 1, 2, 3 for eth0 - eth3.

4. To configure the IP address and subnet mask, type:
   - » `ip4set 0 xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy` <Enter> (where 0 is the desired interface, "`xxx.xxx.xxx.xxx`" is the desired IP address for SecureSync, and "`yyy.yyy.yyy.yyy`" is the full subnet mask for the network (refer to the table "Subnet mask values" on the next page for a list of subnet mask values).

5. Type `gw4set 0 zzz.zzz.zzz.zzz` <Enter>
(where 0 indicates which interface routing table to add the default gateway for, and "`zzz.zzz.zzz.zzz`" is the default gateway address).

> **Note:** If your SecureSync is configured with an Ethernet option card, use 0, 1, 2, 3 for eth0 - eth3.

SecureSync is now configured with a static IP address, subnet mask and gateway address. Proceed to "Product Configuration via the Web UI" on page 42.

Table 2-2: Subnet mask values

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		

2.12 Typical Post-Installation Configurations

2.12.1 Displaying Local Time

After physical product installation, a commonly requested scenario is for SecureSync to display local time on the front panel (rather than UTC time). To learn more about this configuration, see "Editing the System Time" on page 171, and "Front Panel Configuration" on page 179.

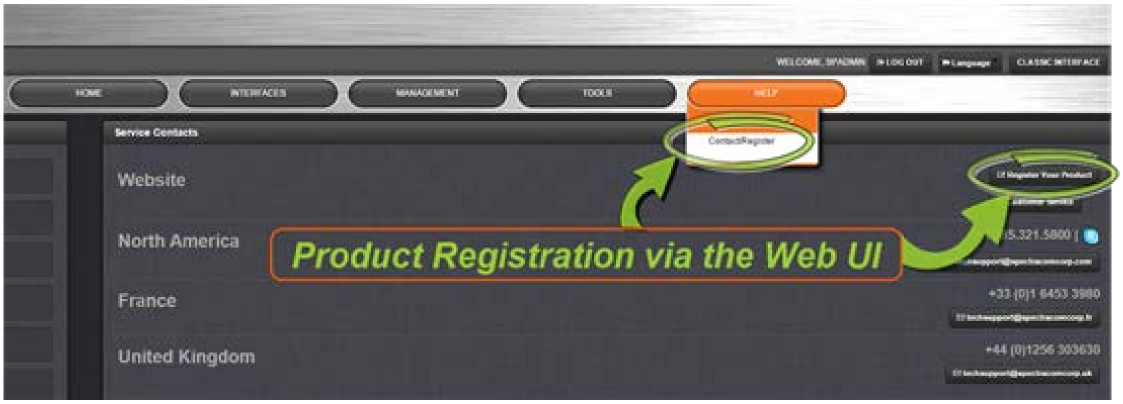
2.12.2 Synchronizing Network PCs

Frequently, network PCs have to be synchronized to SecureSync via the Ethernet port, using NTP (Network Time Protocol). A detailed description on how to synchronize Windows PCs can be found online in the Spectracom Technical Note Synchronizing Windows Computers on the Spectracom website. This document also contains information and details about using the Spectracom PresenTense NTP client software.

2.13 Product Registration

Spectracom recommends that you register your SecureSync so as to allow our Customer Service and Technical Support to notify you of important software updates, or send you service bulletins, if required.

Upon initial start of the SecureSync Web UI (see "Opening the Web UI" on page 33), you will be prompted to register your new product. It is also possible to register at a later time via the HELP menu item, or directly on the Spectracom website.



2.14 Selecting the UI Language

Spectracom continues to localize the SecureSync web user interface into languages other than English e.g., French. Other languages currently supported will be displayed under the Main menu HELP button, Once you selected a language preference, it will be maintaind across logins.

BLANK PAGE.

CHAPTER 3

CONFIGURATION

This chapter covers information on how to integrate SecureSync Time and Frequency Synchronization System into your existing infrastructure by configuring it in accordance with the requirements of your application.

The following topics are included in this Chapter:

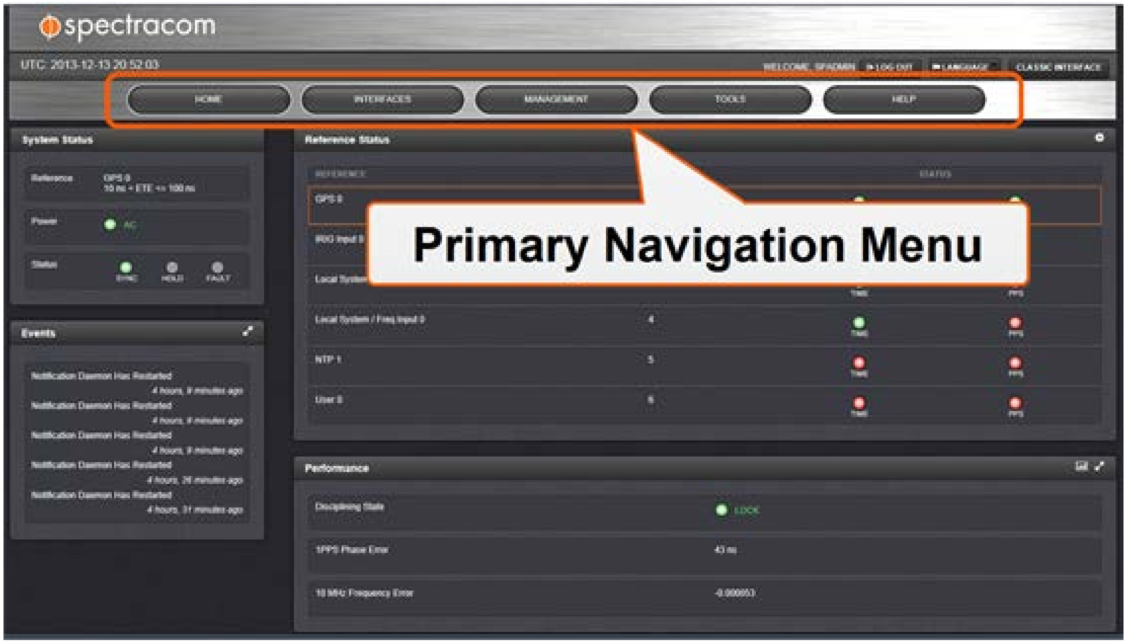
3.1 Product Configuration via the Web UI

Once you have setup and connected your SecureSync to your network, the **Web User Interface** (throughout this document referred to as “Web UI”) allows you to configure and monitor the unit.

> **Note:** Should it ever be necessary, you can restore your SecureSync's configuration to the factory settings at any time. See "Resetting the Unit to Factory Configuration" on page 220.

3.1.1 The Web UI's Main Screen

> **Note:** Screens displayed in this manual are for illustrative purposes. Actual screens may vary depending upon the configuration of your SecureSync unit (e.g., whether or not certain option cards are installed).



The Primary Navigation Menu at the top of the Web UI **Main** screen provides access to all of the Web UI's pages. The menu options are:

- **HOME**: Return to the Main screen
- **INTERFACES**: Access the configuration pages for ...

  - … references (e.g., GPS, NTP)
  - … outputs (e.g. 10 MHz, PPS, NTP) and
  - … installed option cards (e.g., GPS, PPS).
- **MANAGEMENT**: Access the NETWORK setup screens, and OTHER setup screens, e.g. to configure Reference Priorities, System Time, and the Oscillator.
- **TOOLS**: Opens a drop-down menu for access to the system maintenance screens and system logs.
- **HELP/MONITORING**: Opens a drop-down menu for access to system help and information on how to contact Spectracom for further help. (Once you have applied the optional TimeKeeper license, this button will open the TimeKeeper Monitoring menu. See also "Status Monitoring with TimeKeeper" on page 238.)

3.1.2 Default and Recommended Configurations

The factory default configuration settings were chosen for ease of initial setup. Some of the default settings may deviate from best practices recommendations, though. The following table outlines the differences between default and recommended configuration settings for your consideration:

Table 3-1: Default and recommended configurations

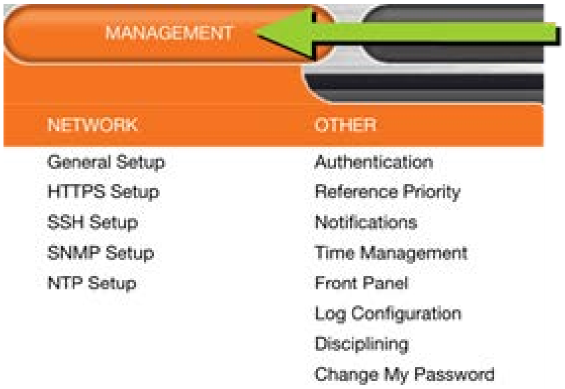
Feature	Default Setting	Recommended Setting	Where to Configure
HTTP	Enabled	Disabled	Web UI or CLI
HTTPS	Enabled (using customer-generated certificate and key or default Spectracom self-signed certificate and common public/private key SSH/SCP/SFTP enabled with unit unique 1024-bit keys)		Web UI
SNMP	Enabled	Disabled or Enabled (with SNMP v3 w/ encryption*)	Web UI
NTP	Enabled (with no MD5 values entered)	Enabled (use MD5 authentication with user-defined keys)	Web UI
Daytime Protocol	Disabled	Disabled	Web UI
Time Protocol	Disabled	Disabled	Web UI
Command Line Interface			
Serial Port	Available	Available	n/a
Telnet	Enabled	Disabled (use SSH instead)	Web UI
SSH	Enabled (default private keys provided)	Enabled	Web UI

Feature	Default Setting	Recommended Setting	Where to Configure
File Transfer			
FTP	Enabled	Disabled (use SFTP or SCP)	Web UI
SCP	Available	Disabled (use SFTP or SCP)	Web UI
SFTP	Available	Disabled (use SFTP or SCP)	Web UI

* Spectracom recommends that secure clients use only SNMPv3 with authentication for secure installations.

3.2 The MANAGEMENT Menu

The **MANAGEMENT** menu on the Web UI's Main screen provides access to SecureSync's configuration screens and menus:



Under **NETWORK**, the following setup screens can be found:

- **General** Setup
- **HTTPS** Setup
- **SSH** Setup
- **SNMP** Setup
- **NTP** Setup.

Under **OTHER**, screens can be found that are not network related:

- **Authentication**–Manage user accounts, Security Policy, LDAP Setup, RADIUS setup, Login Preference and Remote Servers. Change My Password is also available.
- **Reference Priority**–Define the order of priority for timing inputs.
- **Notifications**–Configure the notifications triggered by SecureSync’s events. A notification can be a combination of a mask alarm and/or SNMP Trap and/or email.

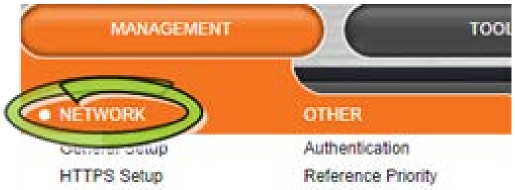
- **Time Management**–Manage the Local Clock, UTC Offset, DST Definition and Leap Second information.
- **Front Panel**–Configure the appearance of the SecureSync front panel display and keypad.
- **Log Configuration**–Manage the system logs.
- **Disciplining**–Manage oscillator disciplining.
- **Change My Password**–Configure the admin password.

3.2.1 Network Management

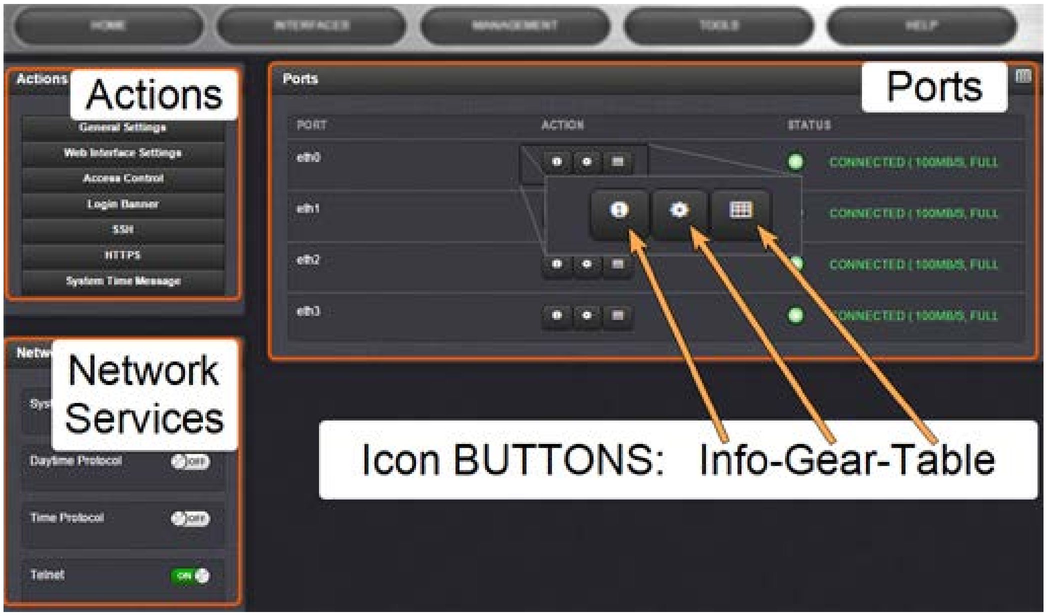
The **Network Management** screen allows you to configure your Ethernet settings and monitor your Ethernet status.

To access the **Network Management** screen:

1. Navigate to **MANAGEMENT > NETWORK**.



2. The **Network Management** screen will display. It is divided into three panels:



PORT	ACTION	STATUS
eth0		CONNECTED (100MB/S, FULL
eth1		CONNECTED (100MB/S, FULL
eth2		CONNECTED (100MB/S, FULL
eth3		CONNECTED (100MB/S, FULL

The Actions panel provides:

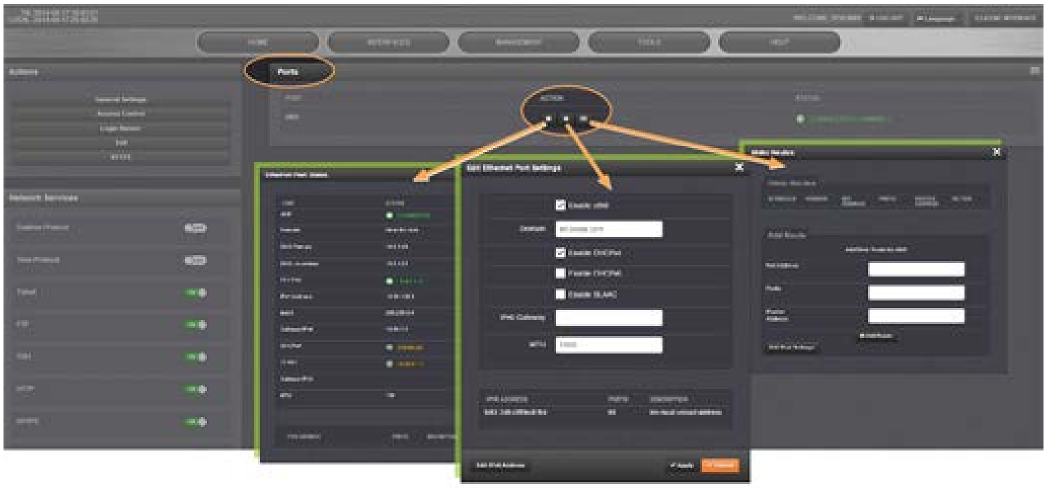
- **General Settings**: Allows quick access to the primary network settings necessary to connect SecureSync to a network. See "Network Configuration" on the next page.

- **Web Interface Settings**:
  - Web interface **timeout**: Determines on how long a user can stay logged on. For more information, see "Changing the Web UI Timeout" on page 281.
- **Access Control**: Allows the configuration of access restrictions from assigned networks/nodes.
- **Login Banner**: Allows the administrator to configure a custom banner message to be displayed on the SecureSync Web UI login page (NOTE: There is a 2000 character size limit).
- **SSH**: This button takes you to the **SSH Setup** window. For details on setting up SSH, see "Configuring SSH" on page 72.
- **HTTPS**: This button takes you to the **HTTPS Setup** window. For details on setting up HTTPS, see "Configuring HTTPS" on page 63.
- **System Time Message**: Setup a once-per-second time message to be sent to receivers via multicast. For details, see .

The Network Services panel is used to enable (ON) and disable (OFF) network services, as well as the Web UI display mode, details see: "Network Services: En-/Disabling" on page 62.

The Ports panel is used to set up and manage SecureSync’s network ports via three buttons:

- **INFO** button: Displays the Ethernet port Status window for review purposes.
- **GEAR** button: Displays the Ethernet port settings window for editing purposes.
- **TABLE** button: Displays a window that allows adding, editing, and reviewing Static Routes.

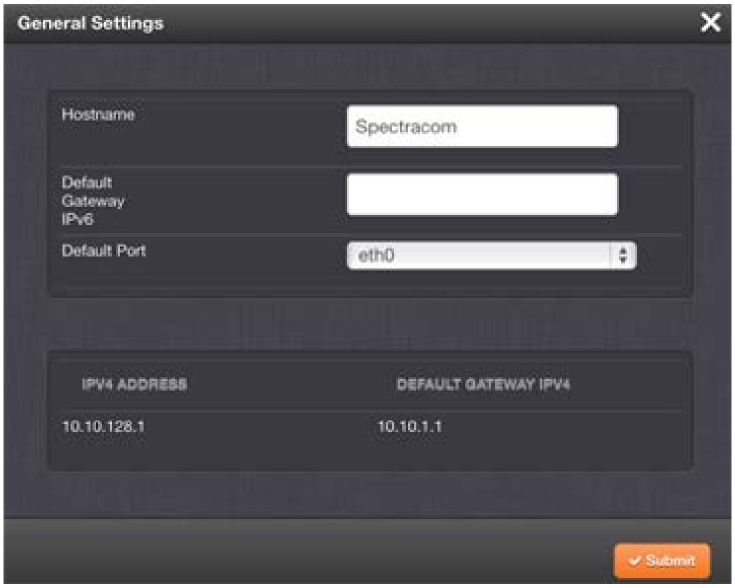


3.2.2 Network Configuration

The **Network Setup** pages are used to configure SecureSync's network connectivity. They can be accessed via the **MANAGEMENT** drop-down menu, under **NETWORK**.

3.2.2.1 General Network Settings

To facilitate network setup, SecureSync provides the **General Setings** window, allowing quick access to the primary network settings:



General Settings

Hostname: Spectracom

Default Gateway IPv6:

Default Port: eth0

IPV4 ADDRESS	DEFAULT GATEWAY IPV4
10.10.128.1	10.10.1.1

- **Hostname**–This is the server's identity on the network or IP address. The default is *Spectracom*.
- **Default Gateway IPv6**–The gateway (default router) address is needed if communication to the SecureSync is made outside of the local network. By default, the gateway is disabled. In the format "`####.####.####.####.####.####.####.####`," where each '`#`' is a hexadecimal value. When a DHCP server is not requested or is requested but not available and DHCP IPv6 is enabled, the server will use this Default Gateway.
- **Default Port**–When no specific port is identified for access to the network, the default port is used. The factory default port is *eth0*.

The **General Settings** window also displays the IPv4 address and default IPv4 gateway.

To access the **General Settings** window:

1. Navigate to **MANAGEMENT > NETWORK > General Setup**.

–OR:–

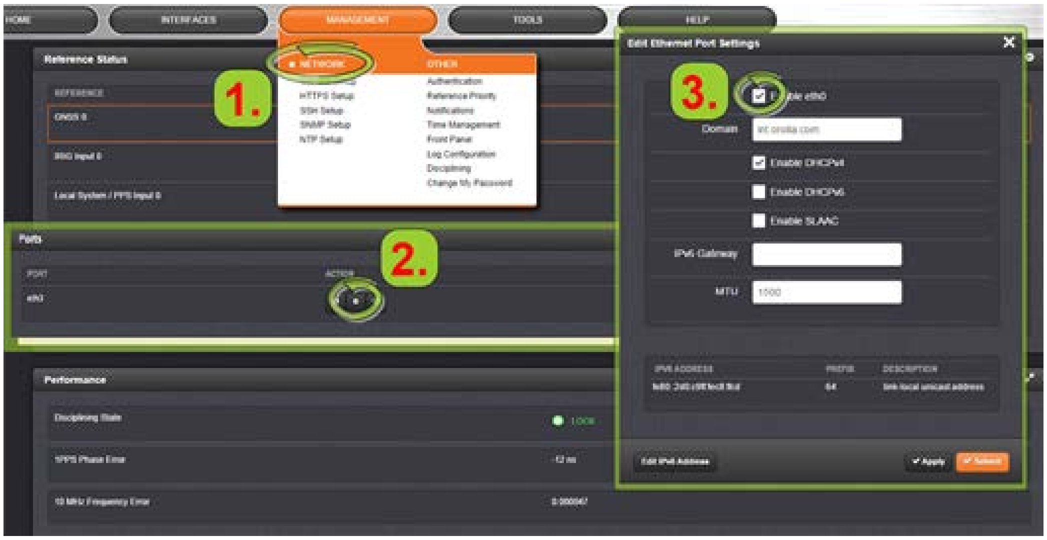
1. Navigate to **MANAGEMENT > NETWORK**. The **Network Management** screen displays. In the **Actions** panel on the left, click **General Settings**.
2. The **General Settings** window will display.

3.2.2.2 Network Ports

Configuring Network Ports

To configure a network port:

1. Navigate to the **MANAGEMENT > NETWORK** screen.
2. The **Ports** panel displays a list of the available Ethernet ports, and their connection status. Locate the port you want to configure and select the GEAR button.



Edit Ethernet Port Settings

☑ Enable eth0

Domain: int.orolia.com

☑ Enable DHCPv4

☐ Enable DHCPv6

☐ Enable SLAAC

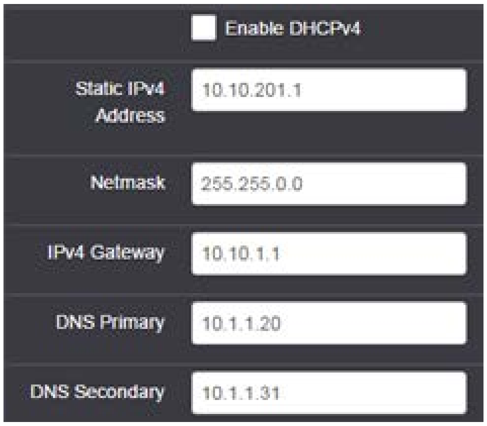
IPv6 Gateway:

MTU: 1500

IPV6 ADDRESS	PREFIX	DESCRIPTION
fe80::2a0:c9ff:fecll:8cd	64	link local unicast address

> **Note:** The eth0 port is the built-in SecureSync Ethernet port.

3. If the port is not already enabled, in the **Edit Ethernet Ports Settings** window, click the **Enable** check box. The **Edit Ethernet Ports Settings** window will expand to show the options needed to complete the port setup.
4. Fill in the fields as required:
   - **Domain**—This is the domain name to be associated with this port.
   - **Enable DHCPv4**—Check this box to enable the delivery of IP addresses from a DHCP Server using the DHCPv4 protocol. This box is checked by default. When DHCP is disabled (the box is unchecked), the following fields will display and must be completed:



□ Enable DHCPv4

Static IPv4 Address: 10.10.201.1

Netmask: 255.255.0.0

IPv4 Gateway: 10.10.1.1

DNS Primary: 10.1.1.20

DNS Secondary: 10.1.1.31

- **Static IPv4 Address**–This is the unique address assigned by the network administrator. The default static IP address of the SecureSync unit is 10.10.201.1. In the format “#.#.#.#” with no leading zeroes or spaces, where each ‘#’ is a decimal integer from the range [0,255].

Table 3-2: Default IP addresses

ETH 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

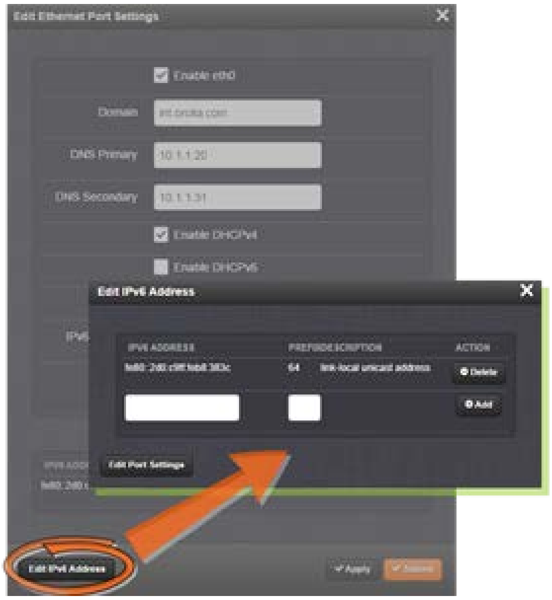
Note: The default subnet is: 255.255.0.0

- **Netmask**–This is the network subnet mask assigned by the network administrator. In the form “xxx.xxx.xxx.xxx.” See "Subnet mask values" on page 38 for a list of subnet mask values.
- **IPv4 Gateway**–The gateway (default router) address is needed if communication to the SecureSync is made outside of the local network. By default, the gateway is disabled.
- **DNS Primary**–This is the primary DNS address to be used for this port. This is set automatically if DHCP is enabled. When DHCP is disabled, DNS Primary is set manually. In the format "#.#.#.#" with no leading zeroes or spaces, where each ‘#’ is a decimal integer from the range [0,255].
- **DNS Secondary**–This is the secondary DNS address to be used for this port. This is set automatically if DHCP is enabled. When DHCP is disabled, DNS Secondary is set manually. In the format “#.#.#.#” with no leading zeroes or spaces, where each ‘#’ is a decimal integer from the range [0,255].

- **Enable DHCPv6**–Check this box to enable the delivery of IP addresses from a DHCP Server using the DHCPv6 protocol.

> **Note:** Unless you are using DNS in conjunction with DHCP (with the client configured using SecureSync's hostname instead of IP address), DHCP should be disabled and the IP address should be changed to a static address once SecureSync is properly configured.
>
> Failure to do this will result in a loss of NTP time synchronization if the DHCP server assigns a new IP address to SecureSync. Verify your setup before synchronizing the network PCs via NTP.

IPv6 addresses may be added and deleted by clicking the **Edit IPv6 Address** button at the bottom of the screen:



Edit Ethernet Port Settings

☑ Enable eth0

Domain: int.orolia.com

DNS Primary: 10.1.1.20

DNS Secondary: 10.1.1.31

☑ Enable DHCPv4

☐ Enable DHCPv6

Edit IPv6 Address

IPV6 ADDRESS	PREFIX	DESCRIPTION	ACTION
fe80::2d0:c9ff:feb8:383c	64	link-local unicast address	Delete
			Add

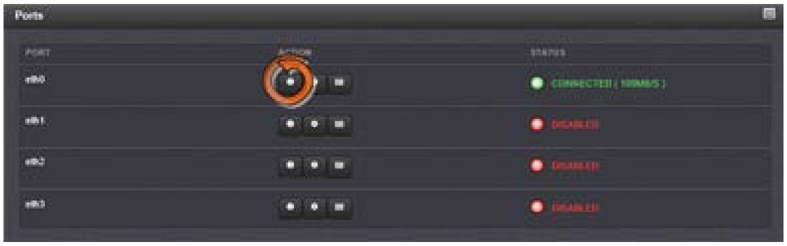
- **Enable SLAAC**–Check this box to enable stateless address auto configuration.
- **IPv6 Gateway**–The gateway (default router) address is needed if communication to the SecureSync is made outside of the local network. By default, the gateway is disabled. In the format "`####.####.####.####.####.####.####.####`," where each '`#`' is a hexadecimal value.
- **MTU**–Maximum Transmission Unit. Range (for Ethernet v2): Default: 1500 bytes. Smaller packages are recommended, if encapsulation is required, e.g. to meet encryption needs, which would cause the maximum package size to be exceeded.

To apply your changes, click **Submit** (the window will close), or **Apply**.

Viewing Network Port Settings

To view the settings of a network port:

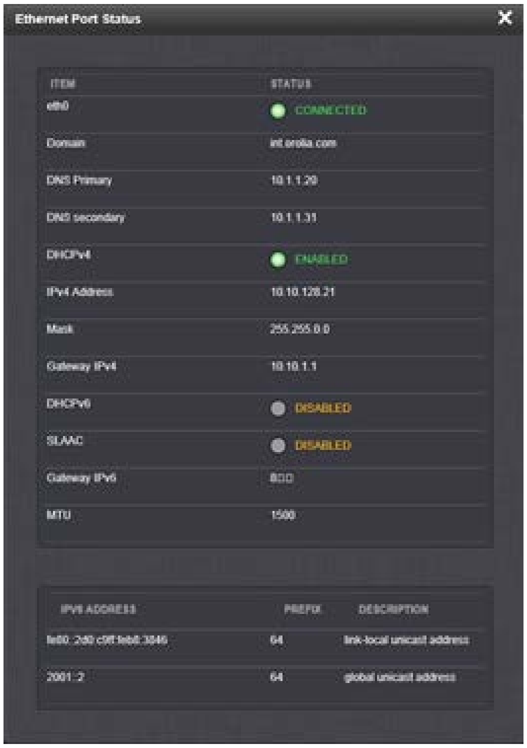
1. Navigate to the **MANAGEMENT > NETWORK** screen.
2. The **Ports** panel displays a list of the available Ethernet ports, and their connection status.



Ports

PORT	ACTION	STATUS
eth0		● CONNECTED (100MB/S)
eth1		● DISABLED
eth2		● DISABLED
eth3		● DISABLED

3. Locate the port you want to configure and click the **INFO** button. The **Ethernet Port Status** window will display:



Ethernet Port Status

ITEM	STATUS
eth0	● CONNECTED
Domain	int.orolia.com
DNS Primary	10.1.1.20
DNS secondary	10.1.1.31
DHCPv4	● ENABLED
IPv4 Address	10.10.128.21
Mask	255.255.0.0
Gateway IPv4	10.10.1.1
DHCPv6	● DISABLED
SLAAC	● DISABLED
Gateway IPv6	800
MTU	1500

IPV6 ADDRESS	PREFIX	DESCRIPTION
fe80::2d0:c9ff:feb8:3846	64	link-local unicast address
2001::2	64	global unicast address

The following configurations can be viewed:

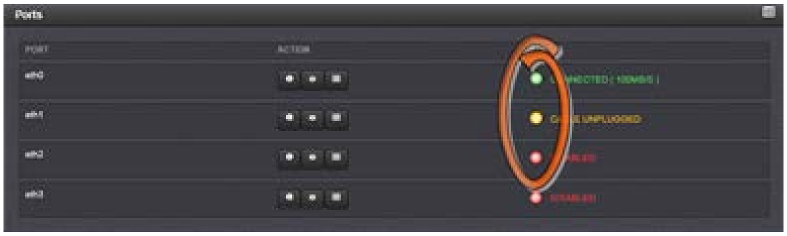
- The port number (the built in SecureSync is designated eth0). The status will be one of:
  - **CONNECTED** (showing the connection speed) in green.
  - **DISABLED** in orange.
  - **CABLE UNPLUGGED** (the port is enabled but there is not cable attached) in orange.
- **Domain**—This is the domain name associated with this port.

- **DNS Primary**–This is the primary DNS address used for this port. This is set automatically if DHCP is enabled. When DHCP is disabled, DNS Primary is set manually.
- **DNS Secondary**–This is the secondary DNS address used for this port. This is set automatically if DHCP is enabled. When DHCP is disabled, DNS Secondary is set manually.
- **DHCPv4**–This will show either “on” (“ENABLED” in green) or “off” (“DISABLED” in orange).
- **Static IPv4 Address**–This is the unique address assigned to the SecureSync unit by the network administrator to be used when DHCP is disabled.
- **Mask**–This is the network subnet mask assigned to the SecureSync unit by the network administrator to be used when DHCP is disabled.
- **Gateway IPv4**–The gateway (default router) address is needed if communication to the SecureSync is made outside of the local network to be used when DHCP is disabled. By default, the gateway is disabled.
- **DHCPv6**–This will show either “on” (“ENABLED” in green) or “off” (“DISABLED” in orange).
- **SLAAC**–This will show either “on” (“ENABLED” in green) or “off” (“DISABLED” in orange).
- **Gateway IPv6**–When a DHCP server is not requested or is requested but not available and DHCPv6 is enabled, the server will use this Default Gateway.
- **MTU**–Maximum Transmission Unit. Default: 1500 bytes. Smaller packages are recommended, if encapsulation is required, e.g.to meet encryption needs, which would cause the maximum package size to be exceeded.

Viewing the Status of a Network Port

To view the connection status of a network port:

1. Navigate to the **MANAGEMENT > NETWORK** screen.
2. The **Ports** panel displays a list of the available Ethernet ports, and their connection status.



The connection status can be:

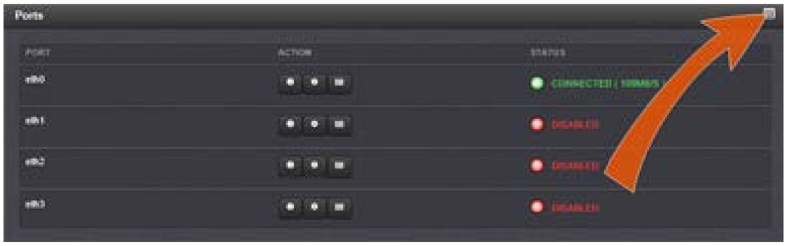
- Green: **CONNECTED** (showing the connection speed)
- Yellow: **CABLE UNPLUGGED** (the port is enabled but there is no cable attached)
- Red: **DISABLED.**

3.2.2.3 Static Routes

Viewing Static Routes

To view SecureSync's Static Routes:

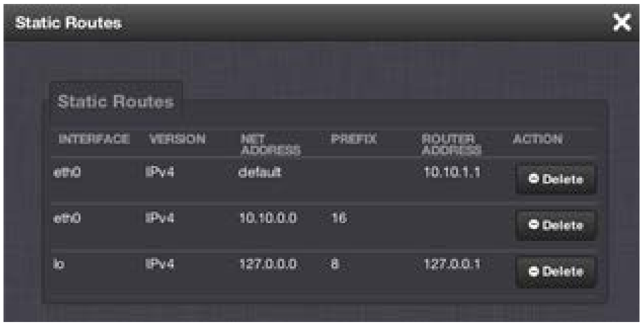
1. Navigate to the **MANAGEMENT > NETWORK** screen..
2. The **Ports** panel displays the available Ethernet ports, and their connection status.



Ports

PORT	ACTION	STATUS
eth0	● ● ▤	● CONNECTED (100Mb/S)
eth1	● ● ▤	● DISABLED
eth2	● ● ▤	● DISABLED
eth3	● ● ▤	● DISABLED

3. In the **Ports** panel, click the **TABLE** icon in the upper right-hand corner.
   The **Static Routes** table for your unit will be be displayed:



Static Routes

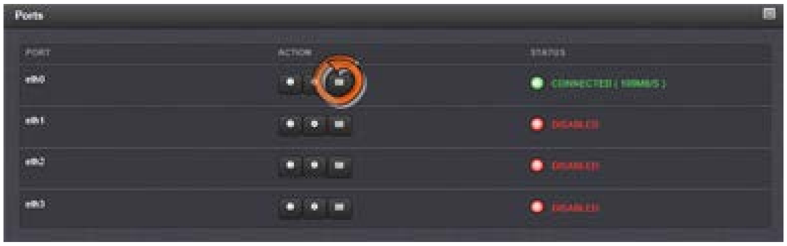
Static Routes

INTERFACE	VERSION	NET ADDRESS	PREFIX	ROUTER ADDRESS	ACTION
eth0	IPv4	default		10.10.1.1	Delete
eth0	IPv4	10.10.0.0	16		Delete
lo	IPv4	127.0.0.0	8	127.0.0.1	Delete

Adding Static Routes to the Routing Table

To add a static route to SecureSync's routing table:

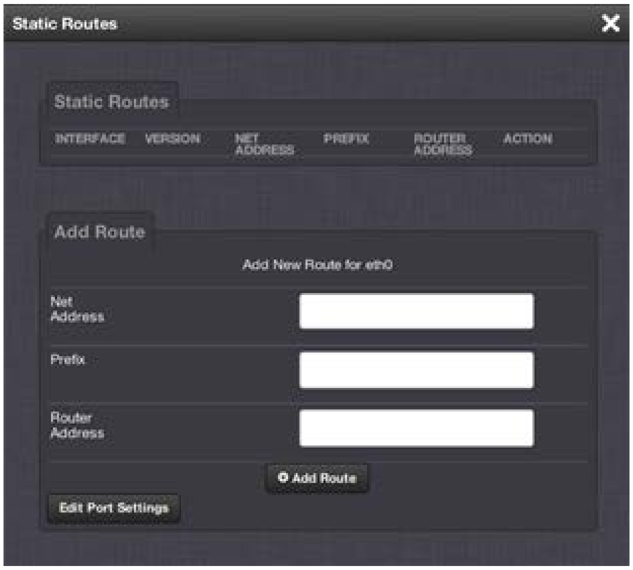
1. Navigate to the **MANAGEMENT > NETWORK** screen.
2. The **Ports** panel displays the available Ethernet ports, and their connection status.



Ports

PORT	ACTION	STATUS
eth0	● ● ▤	● CONNECTED (100Mb/S)
eth1	● ● ▤	● DISABLED
eth2	● ● ▤	● DISABLED
eth3	● ● ▤	● DISABLED

3. In the **Ports** panel, click the **TABLE** button in the row representing the port for which you wish to create a static route. The **Static Routes** window will be displayed:



Note: The eth0 port is the default port for static routing on SecureSync. If a port is not given its own static route, all packets from that port will be sent through the default.

4. In the **Add Route** panel, fill in the fields.

Note: Do not use the same route for different Ethernet port; SecureSync will reject a route that has been used elsewhere.

- **Net Address**–This is the router to which the port connects.
- **Prefix**–This is the subnet mask in prefix form. See "Network Configuration Without DHCP" on page 35 for information on subnet masks.
- **Router Address**–This is the IPv4 Gateway address.

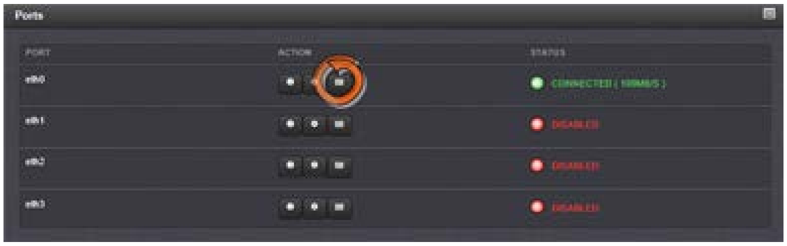
5. Click the **Add Route** button at the bottom of the screen.

Note: To set up a static route, the Ethernet connector must be physically connected to the network.

Viewing a Port’s Routing Table

To view a port’s routing table:

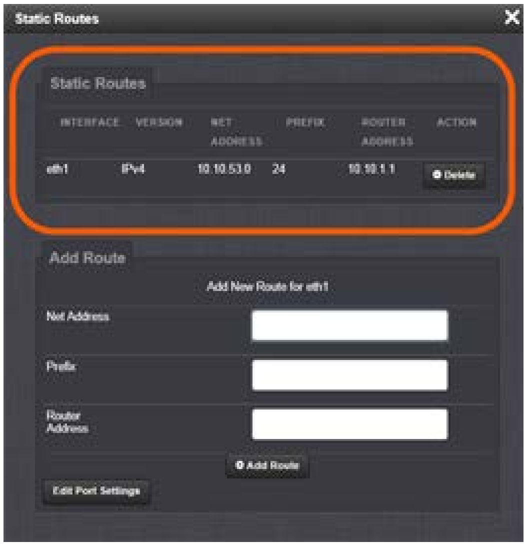
1. Navigate to the **MANAGEMENT > NETWORK** screen.
2. The **Ports** panel displays the available Ethernet ports, and their connection status.



Ports

PORT	ACTION	STATUS
eth0		● CONNECTED (100MB/S)
eth1		● DISABLED
eth2		● DISABLED
eth3		● DISABLED

3. Locate the port you want to configure, and click its **TABLE** button. The **Static Routes** window will open, with the **Static Routes** panel displaying the port’s routing table:



Static Routes

Static Routes

INTERFACE	VERSION	NET ADDRESS	PREFIX	ROUTER ADDRESS	ACTION
eth1	IPv4	10.10.53.0	24	10.10.1.1	Delete

Add Route

Add New Route for eth1

Net Address

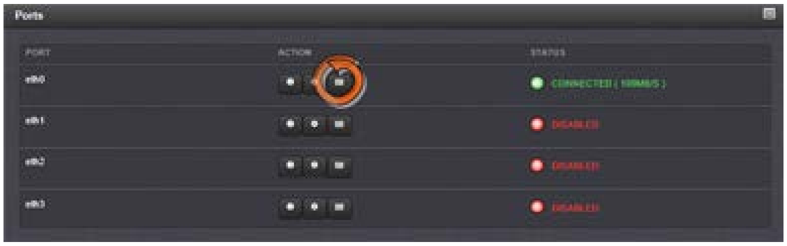
Prefix

Router Address

Assigning a Static Route to a Port

To add or edit an interface route to a port’s routing table:

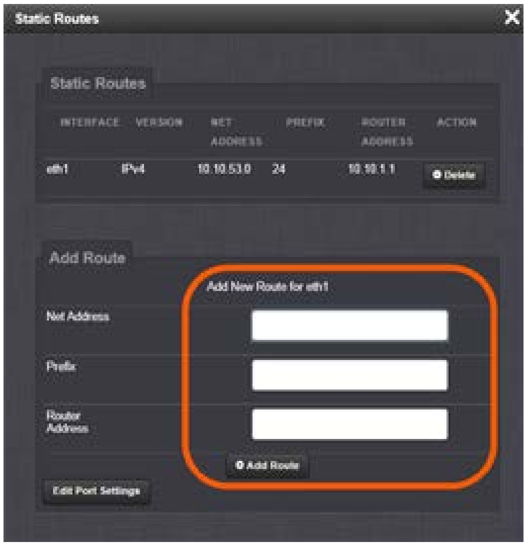
1. Navigate to the **MANAGEMENT > NETWORK** screen.
2. The **Ports** panel lists all available Ethernet ports, and their connection status:



Ports

PORT	ACTION	STATUS
eth0		● CONNECTED (100MB/S)
eth1		● DISABLED
eth2		● DISABLED
eth3		● DISABLED

3. In the **Ports** panel, locate the port you want to configure, and click the **TABLE** button. The **Static Routes** window will display:



Static Routes

Static Routes

INTERFACE	VERSION	NET ADDRESS	PREFIX	ROUTER ADDRESS	ACTION
eth1	IPv4	10.10.53.0	24	10.10.1.1	Delete

Add Route

Add New Route for eth1

Net Address

Prefix

Router Address

4. Fill in the fields as required:

> **Note:** Do not use the same route for different Ethernet ports; SecureSync will reject a route that has been used elsewhere.

- **Net Address**—This is the router to which the port connects.
- **Prefix**—This is the subnet mask in prefix form. See "Network Configuration Without DHCP" on page 35 for information on subnet masks.
- **Router Address**—This is the IPv4 Gateway address.

5. Click the **Add Route** button at the bottom of the screen.

> **Note:** In order for you to set up a static route, the Ethernet connector must be physically connected to the network.

Deleting a Static Route

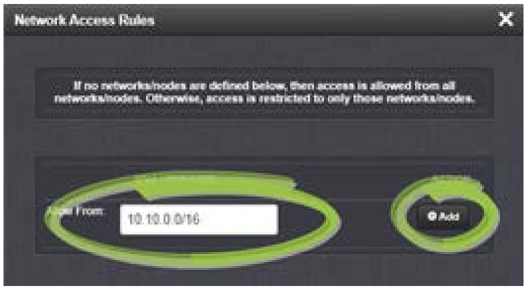
1. To delete a static address, navigate to the **MANAGEMENT > NETWORK** screen.
2. In the **Ports** panel on the right, click the **TABLE** icon in the top-right corner.
3. Click the **Delete** button on the right for the port you wish to delete.

3.2.2.4 Access Rules

Configuring Network Access Rules

To configure access restrictions from assigned networks or nodes:

1. Navigate to the **MANAGEMENT > NETWORK** screen.
2. In the **Actions** panel on the left, click on **Access Control.**
3. The **Network Access Rules** window displays:



Network Access Rules

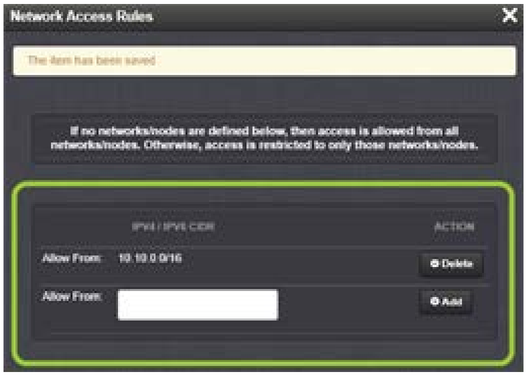
If no networks/nodes are defined below, then access is allowed from all networks/nodes. Otherwise, access is restricted to only those networks/nodes.

Allow From: 10.10.0.0/16

4. In the **Allow From** field, enter a valid IP address. The address entered can be IPv4, IPv4 CIDR, IPv6, or IPv6 CIDR addresses (meaning individual IP addresses or IP address ranges). It is not possible, however, to add direct IP addresses, but instead they must be input as blocks, i.e. you need to add `/32` at the end of an IP address to ensure that only that address is allowed. Example: `10.2.100.29/32` will allow only `10.2.100.29` access.

> **IP address nomenclature:**
>
> IPv4–`10.10.0.0/16`, where `10.10.0.0` is the IP address and `16` is the subnet mask in prefix form. See "Network Configuration Without DHCP" on page 35 for information on subnet masks.
>
> IPv6–`2001:db8::/48`, representing `2001:db8:0:0:0:0:0:0` to `2001:db8:0:ffff:ffff:ffff:ffff:ffff`.

5. Click the **Add** button in the **Action** column.
6. The established rule appears in the **Network Access Rules** window.



Network Access Rules

The item has been saved

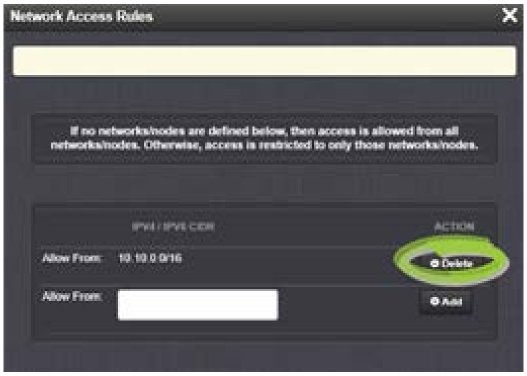
If no networks/nodes are defined below, then access is allowed from all networks/nodes. Otherwise, access is restricted to only those networks/nodes.

IPV4 / IPV6 CIDR		ACTION
Allow From:	10.10.0.0/16	Delete
Allow From:		Add

Deleting Network Access Rules

To delete access restrictions from assigned networks or nodes:

1. Navigate to the **MANAGEMENT > NETWORK** screen.
2. In the **Actions** panel on the left, click on **Access Control**.
3. In the **Network Access Rules** window, locate the rule you want to delete and click **Delete**:



Network Access Rules

If no networks/nodes are defined below, then access is allowed from all networks/nodes. Otherwise, access is restricted to only those networks/nodes.

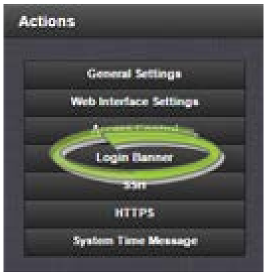
IPV4 / IPV6 CIDR		ACTION
Allow From:	10.10.0.0/16	Delete
Allow From:		Add

3.2.2.5 Login Banner

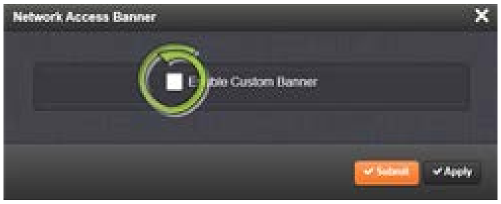
Configuring the Login Banner

To configure a custom banner message to be displayed on the SecureSync login page:

1. Navigate to the **MANAGEMENT > NETWORK** screen.
2. In the **Actions** panel, click **Login Banner**.

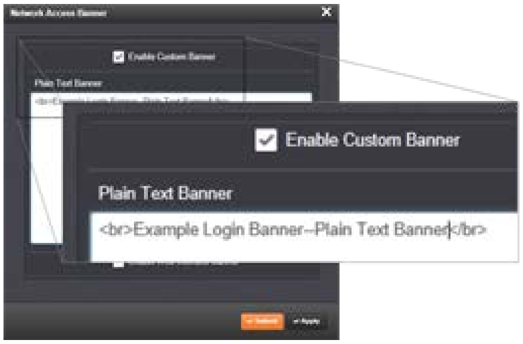


3. The **Network Access Banner** screen will display.



4. Select the **Enable Custom Banner** box.
5. In the **Plain Text Banner** text box, type in the custom text you wish to appear on the SecureSync login screen.

> **Note:** The plain text banner is used for all interactive login interfaces (Web UI, telnet, SSH, FTP, SFTP, serial, etc.). It is not required to include HTML tags. The Web UI banner is used to include a Web UI specific banner that can include HTML tags and be more complex than would be effective on other interactive interfaces.

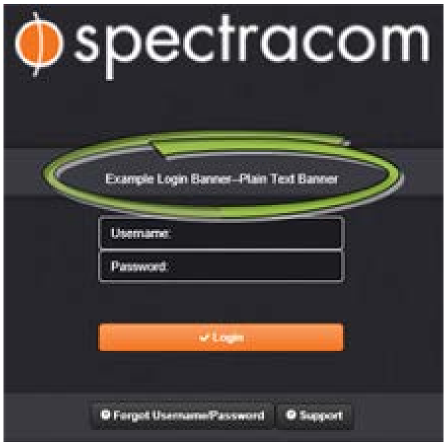


☑ Enable Custom Banner

Plain Text Banner

Example Login Banner--Plain Text Banner</br>

6. Click the **Submit** or **Apply** button at the bottom of the window.
7. To test your new banner:
   - Log out using the **LOG OUT** button at the top of the Web UI.
   - Click the **LOG IN** button at the top of the Web UI.
     - The banner will appear above the USERNAME and PASSWORD fields:

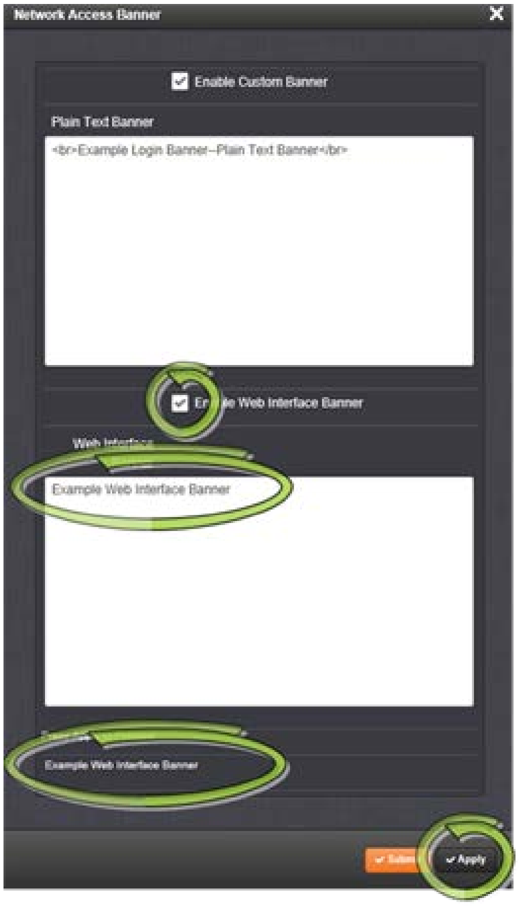


You can also set up a **Web UI banner** that does not require HTML tagging.

To set up a Web UI banner:

1. Follow steps 1 through 5 above.
2. On the **Network Access Banner** screen, select on the **Enable Web Interface Banner** button at the bottom of the screen.
3. The **Web UI** text box will display.

4. Enter the text you wish to appear on the Web UI login screen.



Network Access Banner

☑ Enable Custom Banner

Plain Text Banner

Example Login Banner--Plain Text Banner</br>

☑ Enable Web Interface Banner

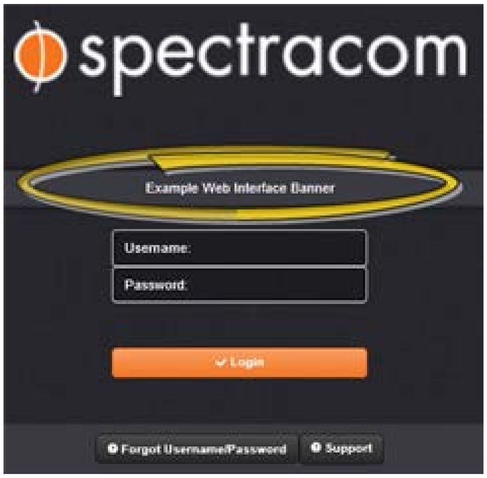
Web Interface

Example Web Interface Banner

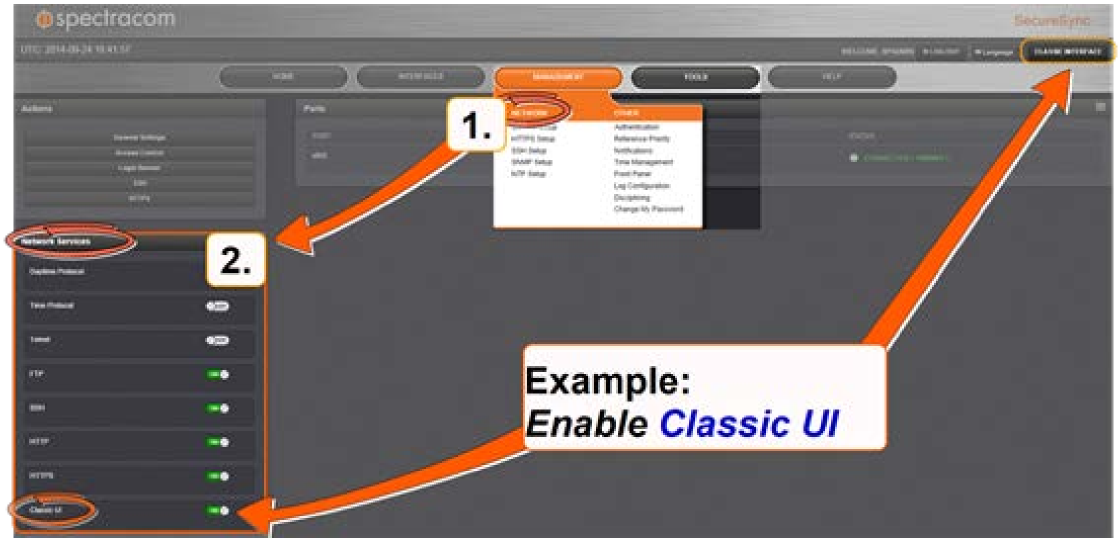
Example Web Interface Banner

5. Click the **Apply** button to see a preview of your entered text at the bottom of the window.
6. To test your new banner:
   - Log out using the **LOG OUT** button at the top of the Web UI.
   - Click the **LOG IN** button at the top of the Web UI.

- The banner will appear above the USERNAME and PASSWORD fields.



3.2.2.6 Network Services: En-/Disabling



The following **Network Services** can be toggled ON/OFF through the **Network Services** panel, which is accessible via **MANAGEMENT** > **NETWORK**:

- **System Time Message**: A once-per second Time Message sent out via Multicast; for details, see "System Time Message" on page 81.
- **Daytime Protocol, RFC867**: Network testing and measurement
- **Time Protocol, RFC 868**: Provision of machine-readable, site-independent date and time
- **Telnet**: Remote configuration
- **FTP server**: Access to logs
- **SSH**: Secure Shell cryptographic network protocol for secure data communication

- **HTTP**: Hypertext Transfer Protocol
- **HTTPS**: Hypertext Transfer Protocol Secure
- **Classic UI**: This toggle switch allows the SecureSync Classic Interface (as used in SecureSync Web UI Version 4.x and older) to be enabled or disabled. **[Default**: ENABLED] To disable, select the OFF position, and refresh the browser window (the refresh may take a moment). The **CLASSIC INTERFACE** button in the upper right hand corner of the main screen will disappear.
- **tcpdump**: A LINUX program that can be used to monitor network traffic by inspecting tcp packets. Default = ON.
  If not needed, or wanted (out of concern for potential security risks), **tcpdump** can be disabled permanently: Once toggled to OFF, and after executing a page reload, **tcpdump** will be deleted from the system: The toggle switch will be removed, and the function cannot be enabled again (even after a software upgrade).

iptables

Since Software Version 5.4.1, **iptables** is supported, allowing for customizable access restrictions. Note that **iptables** is always ON, and its policies can only be accessed via the Command Line Inteface (see "CLI Commands" on page 467) in combination with the **pseudo** command. Please also note that you need to have admin user rights to run this command.

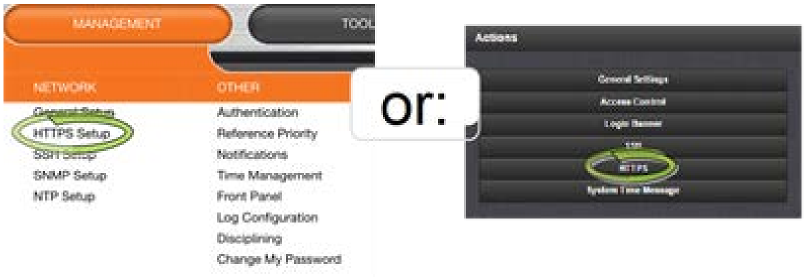
Note: A listing of network settings recommendations can be found under "Default and Recommended Configurations" on page 43.

3.2.2.7 Configuring HTTPS

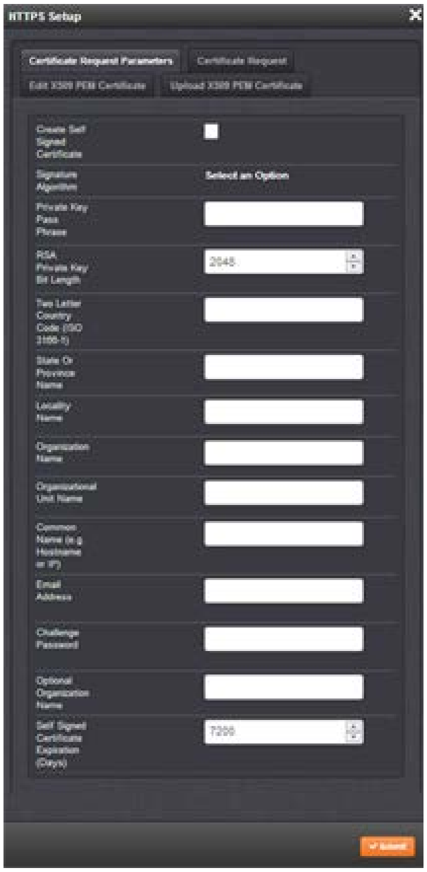
Accessing the HTTPS Setup Screen

To access the **HTTPS Setup** screen:

1. Navigate to **MANAGEMENT** > **NETWORK** > **HTTPS Setup**, or, in the **NETWORK** > **Actions** panel, select **HTTPS**.



2. The **HTTPS Setup** window will appear:



HTTPS Setup

Certificate Request Parameters
Certificate Request
Edit X509 PEM Certificate
Upload X509 PEM Certificate

Create Self Signed Certificate □

Signature Algorithm: Select an Option

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):

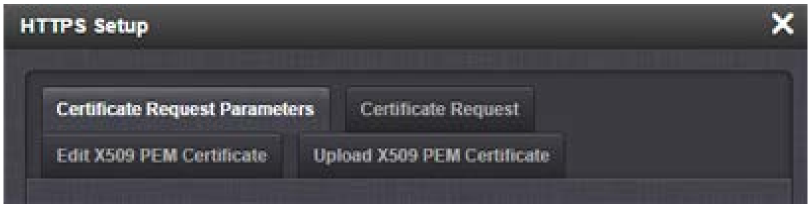
Email Address:

Challenge Password:

Optional Organization Name:

Self Signed Certificate Expiration (Days): 7200

The window contains 4 tabs:



HTTPS Setup
Certificate Request Parameters
Certificate Request
Edit X509 PEM Certificate
Upload X509 PEM Certificate

- **Certificate Request Parameters**–A GUI interface that uses the OpenSSL library to create certificate Requests and self-signed certificates.
- **Certificate Request**–A holder for the certificate request generated under the Certificates Request Parameters tab. This request is sent to the Certificate Authority.
- **Upload X509 Certificate**–The certificate returned by the Certificate Authority is uploaded under this tab.
- **Edit X509 PEM Certificate**–The certificate used by the SecureSync is stored here.

Note: You can exit the HTTPS Setup window by clicking on the X at the top right of the window or by clicking anywhere outside the window.

If you exit the HTTPS Setup window while filling out the Certificate Request Parameters form before you have hit the Submit button, any information you entered will not be retained. If you switch between tabs with the HTTPS Setup window, the information you have entered will be retained until you either leave the HTTPS Setup window or click the Submit button.

Using HTTPS

HTTPS provides secure/encrypted, web-based management and configuration of SecureSync from a PC. An SSL certificate is required to be in SecureSync in order to make this secure HTTPS connection.

SecureSync uses OpenSSL library with a simple GUI interface to create certificate requests and self-signed certificates. Users can then send these certificate requests to an external Certificate Authority (CA) for the creation of a third party verifiable certificate, or use an internal corporate Certificate Authority. If a Certificate Authority is not available, you can use the self-signed certificate that comes with the unit until it expires, or create your own self-signed certificate.

Each SecureSync comes with a default Spectracom self-signed SSL certificate. The typical life span of a certificate is about 10 years. HTTPS is available using this certificate until this certificate expires.

Note: If deleted, the HTTPS certificate cannot be restored. A new certificate will need to be generated.

Note: If the IP Address or Common Name (Host Name) is changed, you may wish to regenerate the security certificate. Otherwise you may receive security warnings from your web browser each time you login.

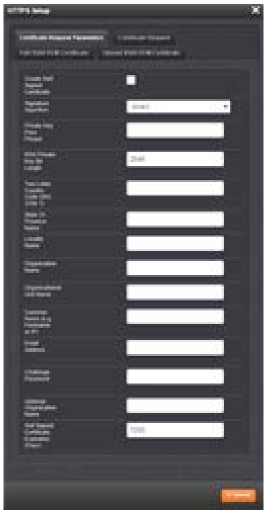
The OpenSSL library provides the encryption algorithms used for secure HTTP (HTTPS). The OpenSSL package also provides tools and software for creating X.509 Certificate Requests, Self Signed Certificates and Private/Public Keys. For more information on OpenSSL, please see www.openssl.org.

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 interface. RSA private keys are supported because they are the most widely accepted (at this time, DSA keys are not supported).

Creating an HTTPS Certificate Request

To create an HTTPS Certificate Request:

1. Navigate to the **MANAGEMENT/NETWORK/HTTPS Setup** screen and fill in the available fields.



2. Choose the **Certificate Request Parameters** tab (this should be the default page).
3. Fill in the available fields:

- **Create Self-Signed Certificate**–Check this box if the Certificate you are creating is a self-signed certificate.
- **Signature Algorithm**–Choose the algorithm to be used from:
  - MD4
  - SHA1
  - SHA256
  - SHA512
- **Private Key Pass Phrase**–This is the RSA decryption key. This must be at least 4 characters long.
- **RSA Private Key Bit Length**–2048 bits is the default. Using a lower number may compromise security and is not recommended.
- **Two-Letter Country Code**–This code should match the ISO-3166-1 value for the country in question.
- **State Or Province Name**–From the address of the organization creating up the certificate.
- **Locality Name**–Locale of the organization creating the certificate.
- **Organization Name**–The name of the organization creating the certificate.
- **Organization Unit Name**–The applicable subdivision of the organization creating the certificate.

- **Common Name (e.g. Hostname or IP)**—This is the name of the host being authenticated. The Common Name field in the X.509 certificate must match the hostname, IP address, or URL used to reach the host via HTTPS.
- **Email Address**—This is the email address of the organization creating the certificate.
- **Challenge Password**—Valid response password to server challenge.
- **Optional Organization Name**—An optional name for the organization creating the certificate.
- **Self-Signed Certificate Expiration (Days)**—How many days before the certificate expires. The default is 7200.

The user is required to select a signature algorithm, a private key passphrase of at least 4 characters, a private key bit length, the certificate expiration in days, and the rest of the remaining fields.

It is recommended that the user consult their Certificate Authority for the required fields in an X 509-certificate request. Spectracom recommends all fields be filled out and match the information given to your Certificate Authority. For example, use all abbreviations, spellings, URLs, and company departments recognized by the Certificate Authority. This helps to avoid problems the Certificate Authority might otherwise have reconciling certificate request and company record information.

If necessary, consult your web browser vendor’s documentation and Certificate Authority to see which key bit lengths and signature algorithms your web browser supports.

Spectracom recommends that when completing the Common Name field, the user provide a static IP address, because DHCP-generated IP addresses can change. If the hostname or IP address changes, the X.509 certificate must be regenerated.

It is recommended that the RSA Private Key Bit Length be a power of 2 or multiple of 2. The key bit length chosen is typically 1024, but can range from 512 to 4096. Long key bit lengths of up to 4096 are not recommended because they can take hours to generate. The most common key bit length is the value 1024.

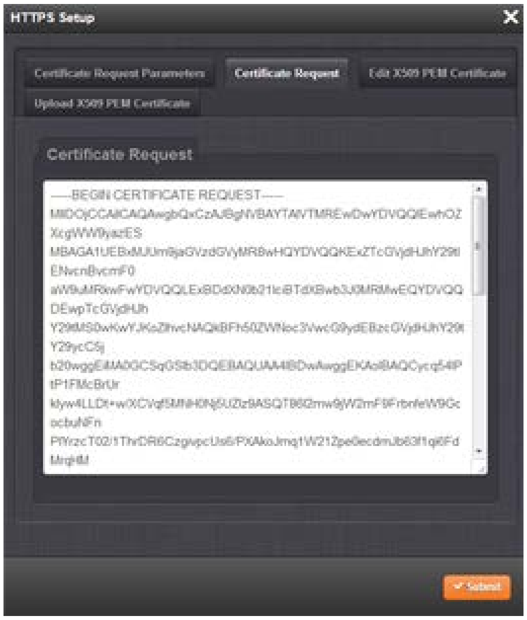
Note: The default key bit length value is 2048.

If using only self-signed certificates (see "Creating a Self-Signed Certificate" on the next page), the user should choose values based on the company’s security policy.

4. When the form is complete, click the **Submit** button. Clicking the **Submit** button automatically generates the Certificate Request in the proper format for submission to the Certificate Authority.

Note: It may take several minutes for the SecureSync to create the certificate request and the private key. The larger the key, the longer amount of time is required. If a system is rebooted during this time, the certificate will not be created.

The generated request can be seen by choosing the **Certificate Request** tab in the **HTTPS Setup** window.


HTTPS Setup
Certificate Request Parameters
Certificate Request
Edit X509 PEM Certificate
Upload X509 PEM Certificate
Certificate Request
Submit

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDOjCCAiICAQAwgbQxCzAJBgNVBAYTAlVTMREwDwYDVQQIEwhOZ
XcgWW9yazES
MBAGA1UEBxMJUm9jaGVzdGVyMRBwHQYDVQQKExZTcGVjdHJhY29tI
ENvcnBvcmF0
aW9uMRkwFwYDVQQLExBDdXN0b21lciBTdXBwb3J0MRMwEQYDVQQ
DEwpTcGVjdHJh
Y29tMS0wKwYJKoZIhvcNAQkBFh50ZWNoc3VwcG9ydEBzcGVjdHJhY29t
Y29ycC5j
b20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCycq54P
tP1FMcBrUr
klyw4LLDt+wXCVqf5MNH0Nj5UZIz9ASQT862mw9jW2mF9FrbnfeW9Gc
ocbuNFn
PlYrzcT02/1ThrDR6CzgvpcUs6/PXAkoJmq1W21Zpe0ecdmJb63f1qi6Fd
MrqHM
```

Note: If you switch between tabs while filling out the Certificate Request Parameters form, the information you entered will be retained until you exit the HTTPS Setup window or hit the Submit button.

If you exit the HTTPS Setup window, the information you entered will not be retained.

Creating a Self-Signed Certificate

To create a Self-Signed Certificate:

1. Under the Certificate Request Parameters tab in the HTTPS Setup Window, complete the form (see "Creating an HTTPS Certificate Request" on page 65).
2. Check the box marked **Create Self Signed Certificate** at the top of the form.
3. Click the **Submit** button at the bottom of the form.

A Self Signed Certificate will be generated simultaneously with the Certificate Request that is generated and then displayed under the **Certificate Request** tab. You may use Self Signed Certificate while waiting for the HTTPS Certificate from the Certificate Authority.

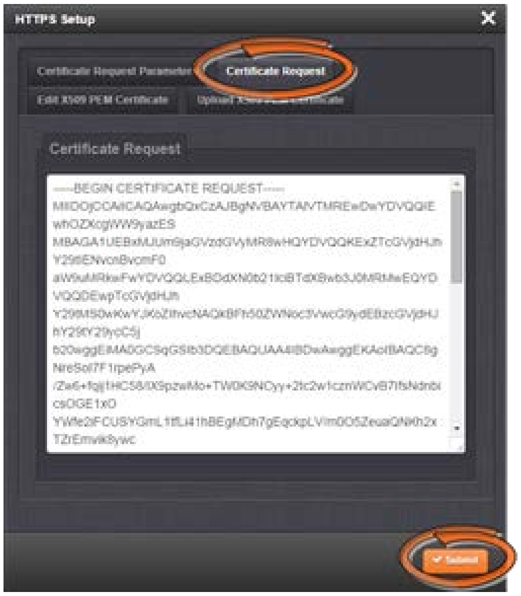
Requesting an HTTPS Certificate

To request an HTTPS Certificate:

1. Create the HTTPS Certificate Request by completing the Certificate Request Parameters form in the **MANAGEMENT/NETWORK/HTTPS Setup Window** (see "Creating an

HTTPS Certificate Request" on page 65) and click the **Submit** button.

2. Select the **Certificate Request** tab in the **HTTPS Setup** window. Clicking the **Submit** button at the bottom of the **Certificate Request Parameters** form will have generated your Certificate Request. You can view the Certificate Request in **Certificate Request** window.


HTTPS Setup
Certificate Request Parameters
Certificate Request
Edit X509 PEM Certificate
Upload X509 PEM Certificate
Certificate Request
Submit

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDOjCCAiICAQAwgbQxCzAJBgNVBAYTAlVTMREwDwYDVQQIE
whOZXcgWW9yazES
MBAGA1UEBxMJUm9jaGVzdGVyMR8wHQYDVQQKExZTcGVjdHJh
Y29tIENvcnBvcmF0
aW9uMRkwFwYDVQQLExBOdXN0b21lciBTdXBwb3J0MRMwEQYD
VQQDEwpTcGVjdHJh
Y29tMS0wKwYJKoZIhvcNAQkBFh50ZWNoc3VwcG9ydEBzcGVjdHJ
hY29tY29ycC5j
b20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC8g
NreSol7F1rpePyA
/Za6+fqjj1HC58/0XSpzwMo+TW0K9NCyy+2tc2w1czmWCvB7IfsNdnbi
csOGE1xO
YWfe2iFCUSYGmL1tfLi41hBEgMDh7gEqckpLVim0O5ZeuaQNKh2x
TZrEmvik8ywc
```

> **Note:** If you wish to create a different or additional Certificate Request, you may fill out a new form under the Certificate Request Parameters tab, and the SecureSync will automatically generate the new Certificate Request.
>
> The newly generated Certificate Request will replace the Certificate Request previously generated. Therefore, if you wish to retain your previously generated Certificate Request for any reason, you will need to copy that request and save it in text document before you generate your new Certificate Request.

3. Copy the generated Certificate Request from the Certificate Request window and submit it per the guidelines of the Certificate Authority. The Certificate Authority will issue a verifiable, authenticable third party certificate.

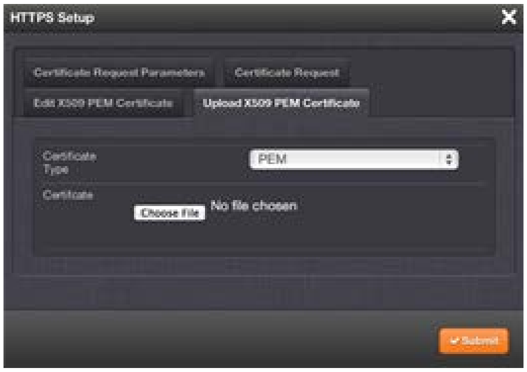
Until this certificate is received, the user’s self-signed certificate may be used (see "Creating a Self-Signed Certificate" on the previous page).

When the SecureSync Web UI is accessed from a Windows computer while the self-signed certificate is being used, the user’s web browser will present a popup window. The certificate can be viewed by the user and installed through this pop up window. Other operating systems may vary in how they install and accept certificates. External Internet access may be required by your Certificate Authority to verify your third party certificate.

Uploading the X509 PEM Certificate

After the HTTPS Certificate has been issued by the Certificate Authority (see "Creating an HTTPS Certificate Request" on page 65, and "Requesting an HTTPS Certificate" on page 68), the certificate needs to be loaded onto the SecureSync system. To upload the certificate:

1. Store the Public Keys File provided to you by the Certificate Authority in a location accessible from the computer on which you are running the Web UI.
2. Access the **MANAGEMENT/NETWORK/HTTPS Setup** window.
3. Choose the **Upload X.509 PEM Certificate** tab.


HTTPS Setup
Certificate Request Parameters
Certificate Request
Edit X509 PEM Certificate
Upload X509 PEM Certificate
Choose File
Submit

Certificate Type: PEM

Certificate: No file chosen

4. Click the **Choose File** button and locate the Public Keys File provided by the Certificate Authority in its location where you stored it in step 1.
5. Click the **Submit** button.

Once the X.509 PEM Certificate has been loaded, it can be viewed by choosing the **Edit X.509 PEM Certificate** tab in the **HTTPS Setup** window.

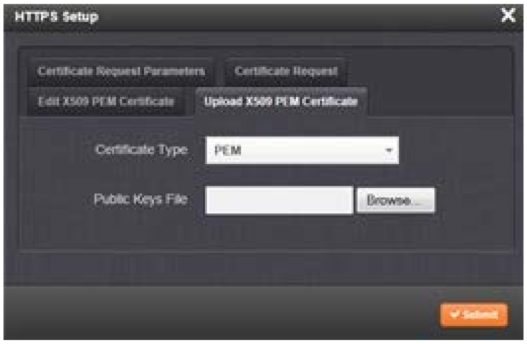
> **Note:** The text inside the text box under the Edit X.509 PEM Certificate tab is editable. However, changes should not be made to a certificate once it is imported. Instead, a new certificate should be requested. An invalid certificate may result in denial of access to the SecureSync through the Web UI. If this occurs, see "If a Secure Unit Becomes Inaccessible" on page 226.

Loading a Non-X.509 PEM Format HTTPS Certificate

After the HTTPS Certificate has been issued by the Certificate Authority (see "Creating an HTTPS Certificate Request" on page 65, and "Requesting an HTTPS Certificate" on page 68), the certificate may not be in the X.509 PEM format. To upload an HTTPS Certificate that is not in the X.509.PEM format:

1. Store the Public Keys File provided to you by the Certificate Authority in a location accessible from the computer on which you are running the Web interface.
2. Navigate to the **MANAGEMENT/NETWORK/HTTPS Setup** window.

3. Choose the **Upload X.509 PEM Certificate** tab.


HTTPS Setup
Certificate Request Parameters
Certificate Request
Edit X509 PEM Certificate
Upload X509 PEM Certificate
Browse...
Submit

Certificate Type: PEM

Public Keys File:

4. Choose the Certificate Type for the HTTPS Certificate supplied by the Certificate Authority from the **Certification Type** drop-down:

Note: The user may choose one of the following alternate certificate types:

DER
PKCS7 PEM
PKCS7 DER

5. Click the **Browse**... button and locate the Public Keys File provided by the Certificate Authority in its location where you stored it in step 1.
6. Click **Submit**.

Note: SecureSync will automatically format the certificate into the proper format.

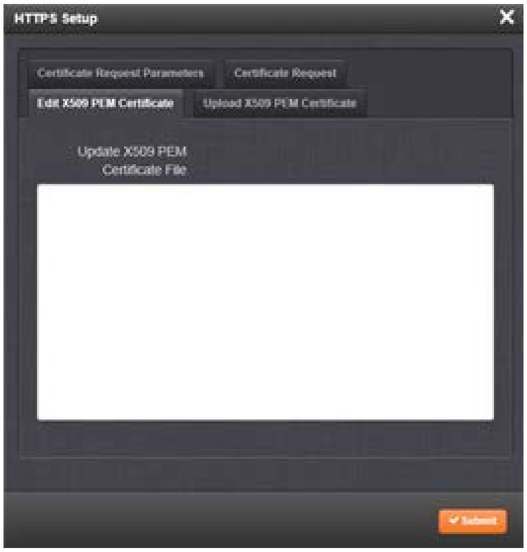
Once the X.509 PEM Certificate has been loaded, it can be viewed by choosing the **Edit X.509 PEM Certificate** tab in the **HTTPS Setup** window.

Note: The text inside the text field under the Edit X509 PEM Certificate tab is editable. However, changes should not be made to a certificate once it is imported. Instead, a new certificate should be requested. An invalid certificate may result in denial of access to the SecureSync through the Web UI. If this occurs, see "If a Secure Unit Becomes Inaccessible" on page 226.

Manually Inserting HTTPS Certificate from Text File

Many certificate authorities simply provide you with a certificate in the form of a plain text file. If your certificate is provided in this manner, and the certificate is in the X.509 PEM format, you may simply copy and paste the text into the web interface:

1. Navigate to the **MANAGEMENT/NETWORK/HTTPS Setup** window.
2. Choose the **Edit X.509 PEM Certificate** tab.


HTTPS Setup
Certificate Request Parameters
Certificate Request
Edit X509 PEM Certificate
Upload X509 PEM Certificate
Update X509 PEM Certificate File
✔ Submit

3. Copy the text of the certificate and paste it into the **Update X.509 PEM Certificate File** text field.

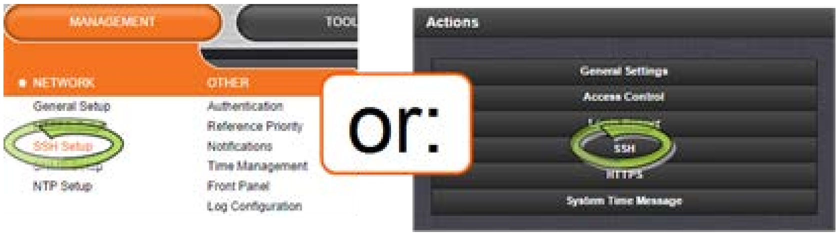
> **Note:** Only X.509 PEM Certificates can be loaded in this manner.

> **Note:** The text inside the text field under the Edit X.509 PEM Certificate tab is editable. However, changes should not be made to a certificate once it is imported.
>
> Instead, a new certificate should be requested. An invalid certificate may result in denial of access to the SecureSync through the Web UI. If this occurs, see "If a Secure Unit Becomes Inaccessible" on page 226.

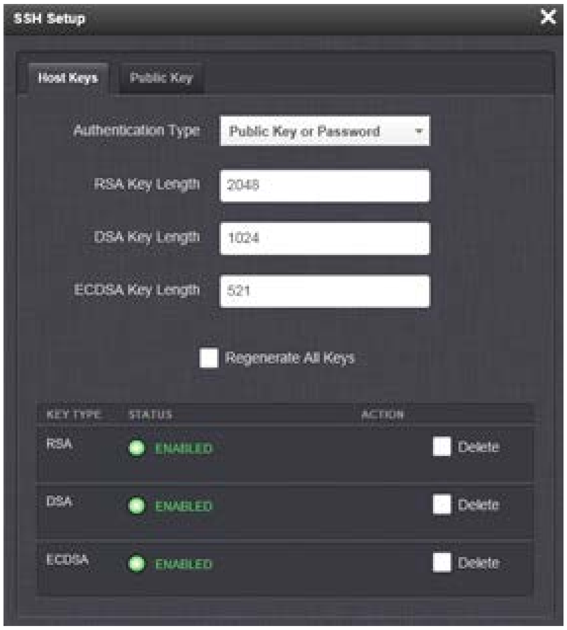
3.2.2.8 Configuring SSH

Accessing the SSH Setup Screen

To access the **SSH Setup** screen, navigate to **MANAGEMENT** > **NETWORK** > **SSH Setup**, or, in the **MANAGEMENT** > **NETWORK** > **Actions** panel, select **SSH**.



The **SSH Setup** pop-up window will display.



Authentication Type: Public Key or Password

RSA Key Length: 2048

DSA Key Length: 1024

ECDSA Key Length: 521

□ Regenerate All Keys

KEY TYPE	STATUS	ACTION
RSA	● ENABLED	□ Delete
DSA	● ENABLED	□ Delete
ECDSA	● ENABLED	□ Delete

The window contains 2 tabs:

- **Host Keys**–SSH uses Host Keys to uniquely identify each SSH server. Host keys are used for server authentication and identification.
- **Public Key**–This is a text field interface that allows the user to edit the public key files `authorized_keys` file.

Note: You can exit the SSH Setup Window by clicking on the X at the top right of the window or by clicking anywhere outside the window.

If you exit the SSH Setup window while filling out the Certificate Request Parameters form before you have hit the Submit button, any information you entered will not be retained. If you switch between tabs with the SSH Setup window, the information you have entered will be retained until you either leave the SSH Setup window or click the Submit button.

Using SSH

The SSH tools supported by SecureSync are:

- **SSH**–Secure Shell
- **SCP**–Secure Copy
- **SFTP**–Secure File Transfer Protocol

SecureSync implements the server components of SSH, SCP, and SFTP.

For more information on OpenSSH, please refer to www.openssh.org.

SSH uses Host Keys to uniquely identify each SSH server. Host keys are used for server authentication and identification. A secure unit permits users to create or delete RSA or DSA keys for the SSH2 protocol.

Note: Only SSH2 is supported. SSH1 protocol is not supported, due to vulnerabilities.

The user may choose to delete individual RSA or DSA host keys.

If the user chooses to delete the RSA or DSA key, the SSH will function, but that form of server authentication will not be available. If the user chooses to delete both the RSA and DSA keys, SSH will not function. In addition, if SSH Host Keys are being generated at the time of deletion, the key generation processes are stopped, any keys created will be deleted, and all key bit sizes are set to 0.

The user may choose to delete existing keys and request the creation of new keys, but it is often simpler to make these requests separately.

The user may create individual RSA and DSA Host Public/Private Key pairs. Host keys must first be deleted before new Host Keys can be created.

SecureSyncs have their initial host keys created at the factory. RSA host key sizes can vary between 768 and 4096 bits. The recommended key size is 1024. Though many key sizes are supported, it is recommended that users select key sizes that are powers of 2 or divisible by 2. The most popular sizes are 768, 1024, and 2048. Large key sizes of up to 4096 are supported, but may take 10 minutes or more to generate. DSA keys size support is limited to 1024 bits.

Host keys are generated in the background. Creating RSA and DSA keys, each with 1024 bits length, typically takes about 30 seconds. Keys are created in the order of RSA, DSA, RSA1. When the keys are created you can successfully make SSH client connections. If the unit is rebooted with host key creation in progress, or the unit is booted and no host keys exist the key generation process is restarted. The key generation process uses either the previously specified key sizes or if a key size is undefined, the default key bit length size used is 2048. A key with a zero length or blank key size field is not created.

The SSH client utilities SSH, SCP, and SFTP allow for several modes of user authentication. SSH allows the user to remotely login or transfer files by identifying the user's account and the target machines IP address. Users can be authenticated either by using their account passwords or by using a Public Private Key Pair. Users keep their private key secret within their workstations or network user accounts and provide the SecureSync a copy of their public key. The modes of authentication supported include:

- Either Public Key with Passphrase or Login Account Password
- Login Account Password only
- Public Key with Passphrase only

SSH using public/private key authentication is the most secure method of authenticating users for SSH, SCP or SFTP sessions.

Users are required to create private and public key pairs on their workstation or within a private area in their network account. These keys may be RSA or DSA and may be any key bit length as supported by the SSH client tool. These public keys are stored in a file in the `.ssh` directory named `authorized_keys`. The file is to be formatted such that the key is followed by the optional comment with only one key per line.

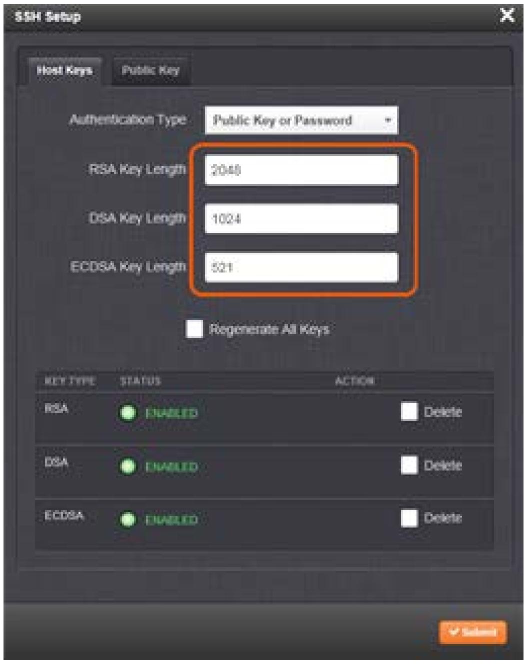
> **Note:** The file format, line terminations, and other EOL or EOF characters should correspond to UNIX conventions, not Windows.

Changing Key Length Values

The user may change the key length of the RSA host key, the DSA host key and/or the ECDSA host key.

To change the key length of a host key:

1. To access the **SSH Setup** screen, choose **MANAGEMENT/NETWORK/SSH Setup**. The window will open to the **Host Keys** tab by default.
2. Select the value of the key length you want to change.



Authentication Type: Public Key or Password

RSA Key Length: 2048

DSA Key Length: 1024

ECDSA Key Length: 521

□ Regenerate All Keys

KEY TYPE	STATUS	ACTION
RSA	● ENABLED	□ Delete
DSA	● ENABLED	□ Delete
ECDSA	● ENABLED	□ Delete

It is recommended that users select key sizes that are powers of 2 or divisible by 2. The most popular sizes are 768, 1024, and 2048. Large key sizes of up to 4096 are supported, but may take 10 minutes or more to generate. DSA keys size support is limited to 1024 bits.

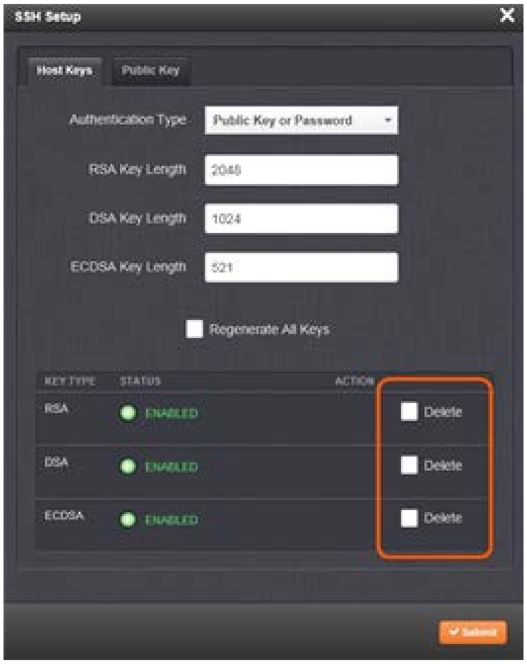
3. Click the **Submit** button at the bottom of the screen. The new values will be saved.

> Note: Changing the values and submitting them in this manner DOES NOT generate new host public/private key pairs. See "Creating Host Public/Private Key Pairs" on the facing page for information on how to create new host public/private key pairs.

Deleting Host Keys

The user may choose to delete individual RSA or DSA host keys. To delete a key:

1. To access the **SSH Setup** screen, choose **MANAGEMENT/NETWORK/SSH Setup**. The window will open to the **Host Keys** tab by default.
2. Select **Delete** in the field for the key you wish to delete.



Authentication Type: Public Key or Password

RSA Key Length: 2048

DSA Key Length: 1024

ECDSA Key Length: 521

□ Regenerate All Keys

KEY TYPE	STATUS	ACTION
RSA	● ENABLED	□ Delete
DSA	● ENABLED	□ Delete
ECDSA	● ENABLED	□ Delete

3. Press the **Submit** button at the bottom of the page.

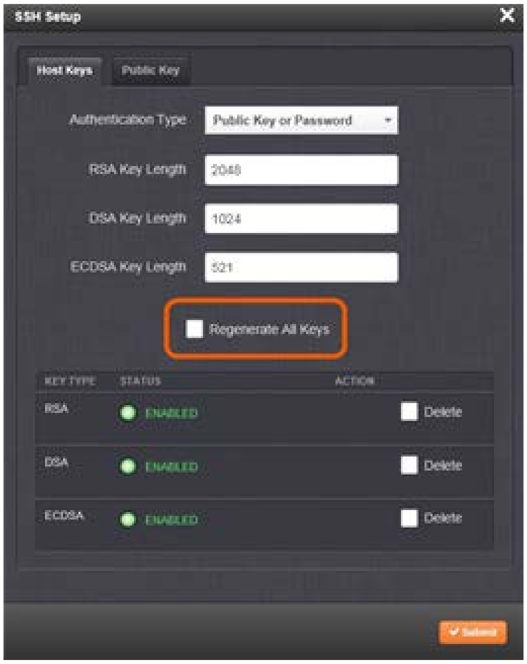
> Note: You can exit the SSH Setup Window by clicking on the X at the top right of the window or by clicking anywhere outside the window.
>
> If you exit the SSH Setup window before you have hit the Submit button, any information you entered will not be retained. If you switch between tabs with

the SSH Setup window, the information you have entered will be retained until you either leave the SSH Setup window or click the Submit button.

Creating Host Public/Private Key Pairs

The user may create individual RSA and DSA Host Public/Private Key pairs. Host keys must first be deleted before new Host Keys can be created. To create a new set of host keys:

1. To access the SSH setup screen, choose **MANAGEMENT/NETWORK/SSH Setup**. The window will open to the **Host Keys** tab by default.
2. If you want to change the key length of any host key, enter the desired length in the text field corresponding to the length you wish to change. See "Deleting Host Keys" on the previous page.



Authentication Type: Public Key or Password

RSA Key Length: 2048

DSA Key Length: 1024

ECDSA Key Length: 521

□ Regenerate All Keys

KEY TYPE	STATUS	ACTION
RSA	● ENABLED	□ Delete
DSA	● ENABLED	□ Delete
ECDSA	● ENABLED	□ Delete

3. Check the **Regenerate All Keys** box.
4. Click the **Submit** button at the bottom of the page.
   The Key Type/Status/Action table will temporarily disappear while the SecureSync regenerates the keys. The Host keys are generated in the background. Creating RSA and DSA keys, each with 1024 bits length, typically takes about 30 seconds. Keys are created in the order of RSA, DSA, ECDSA. SecureSync will generate all 3 host keys, the RSA key, the DSA key and the ECDSA key.
5. Delete any of the keys you do not want. See "Deleting Host Keys" on the previous page.

Note: If the unit is rebooted with host key creation in progress, or the unit is booted and no host keys exist, the key generation process is restarted. The key generation process uses the previously specified key sizes.

If a key size is undefined, the default key bit length size used is 2048. A key with a zero length or blank key size field is not created.

When you delete a host key and recreate a new one, SSH client sessions will warn you that the host key has changed for this particular IP address. The user will then either have to:

1. Override the warning and accept the new Public Host Key and start a new connection. This is the default. This option allows users to login using either method. Whichever mode works is allowed for logging in. If the Public Key is not correct or the Passphrase is not valid the user is then prompted for the login account password.
2. Remove the old Host Public Key from their client system and accept the new Host Public Key. This option simply skips public/private key authentication and immediately prompts the user for password over a secure encrypted session avoiding sending passwords in the clear.
3. Load a public key into SecureSync. This public key must match the private key found in the users account and be accessible to the SSH, SCP, or SFTP client program. The user must then enter the Passphrase after authentication of the keys to provide the second factor for 2-factor authentication.

Please consult your specific SSH client's software's documentation.

Public Keys: Viewing, Editing, Loading

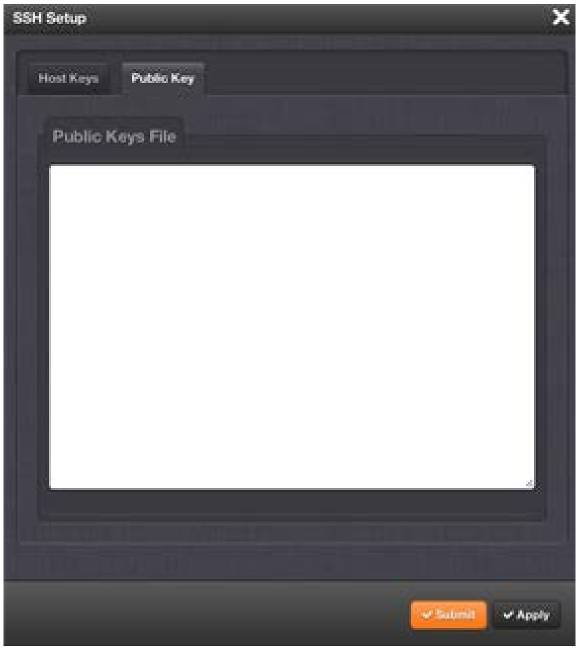
The `authorized_keys` file can be viewed and edited, so as to enable adding and deleting Public Keys. The user may also retrieve the `authorized_keys` file from the .ssh directory Using FTP, SCP, or SFTP.

If a user wants to completely control the public keys used for authentication, a correctly formatted `authorized_keys` file formatted as indicated in the OpenSSH web site can be loaded onto SecureSync. The user can transfer a new public key file using the Web UI.

To view and edit the `authorized_keys` file:

1. To access the SSH setup screen, choose **MANAGEMENT/NETWORK/SSH Setup**. The window will open to the **Host Keys** tab by default.
2. Select the **Public Key** tab. The `authorized_keys` file appears in the **Public Keys File**

window:



3. Edit the `authorized_keys` file as desired.
4. Click the **Submit** button or **Apply** button.

The file is to be formatted such that the key is followed by an optional comment, with only one key per line. The file format, line terminations, and other EOL or EOF characters should correspond to UNIX conventions, not Windows.

> **Note:** If a user deletes all Public Keys, Public/Private Key authentication is disabled. If the user has selected SSH authentication using the “Public Key with Passphrase” option, login and file transfers will be forbidden. The user must select a method allowing the use of account password authentication to enable login or file transfers using SCP or SFTP.

Editing the "authorized_key" File via CLI

Secure shell sessions using an SSH client can be performed using the admin or a user-defined account. The user may use Account Password or Public Key with Passphrase authentication. The OpenSSH tool SSH-KEYGEN may be used to create RSA and DSA keys used to identify and authenticate user login or file transfers.

The following command lines for OpenSSH SSH client tool are given as examples of how to create an SSH session.

Creating an SSH session with Password Authentication for the admin account

```
ssh spadmin@10.10.200.5
```

```
spadmin@10.10.200.5's password: admin123
```

The user is now presented with boot up text and/or a “>” prompt which allows the use of the Spectracom command line interface.

Creating an SSH session using Public Key with Passphrase Authentication for the admin account

The user must first provide the secure Spectracom product a RSA public key found typically in the OpenSSH id_rsa.pub file. The user may then attempt to create an SSH session.

```
ssh -i ./id_rsa spadmin@10.10.200.5
Enter passphrase for key './id_rsa': mysecretpassphrase
```

Please consult the SSH client tool’s documentation for specifics on how to use the tool, select SSH protocols, and provide user private keys.

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.

Perform an SCP file transfer to the device using Account Password authentication

```
scp authorized_keys scp@10.10.200.5:.ssh
spadmin@10.10.200.135's password: admin123
publickeys                                                  100%
|***************************************************| 5 00:00
```

Perform an SCP file transfer from the device using Public Key with Passphrase authentication.

```
scp -i ./id_rsa spadmin@10.10.200.5:.ssh
Enter passphrase for key './id_rsa': mysecretpassphrase
publickeys                                                  100%
|***************************************************| 5 00:00
```

Perform an SFTP file transfer to the device using Account Password authentication.

```
sftp spadmin@10.10.200.5
```

```
spadmin@10.10.200.135's password: admin123
sftp>
```

The user is presented with the SFTP prompt allowing interactive file transfer and directory navigation.

Perform an SFTP file transfer from the device using Public Key with Passphrase authentication

```
sftp -i ./id_rsa spadmin@10.10.200.5
Enter passphrase for key './id_rsa': mysecretpassphrase
sftp>
```

The user is presented with the SFTP prompt allowing interactive file transfer and directory navigation.

Recommended SSH Client Tools

Spectracom does not make any recommendations for specific SSH clients, SCP clients, or SFTP client tools. However, there are many SSH based tools available to the user at low cost or free.

Two good, free examples of SSH tool suites are the command line based tool OpenSSH running on a Linux or OpenBSD x86 platform and the SSH tool suite PuTTY.

The OpenSSH tool suite in source code form is freely available at www.openssh.org though you must also provide an OpenSSL library, which can be found at www.openssl.org.

PuTTY can be found at: http://www.chiark.greenend.org.uk/~sgtatham/putty/.

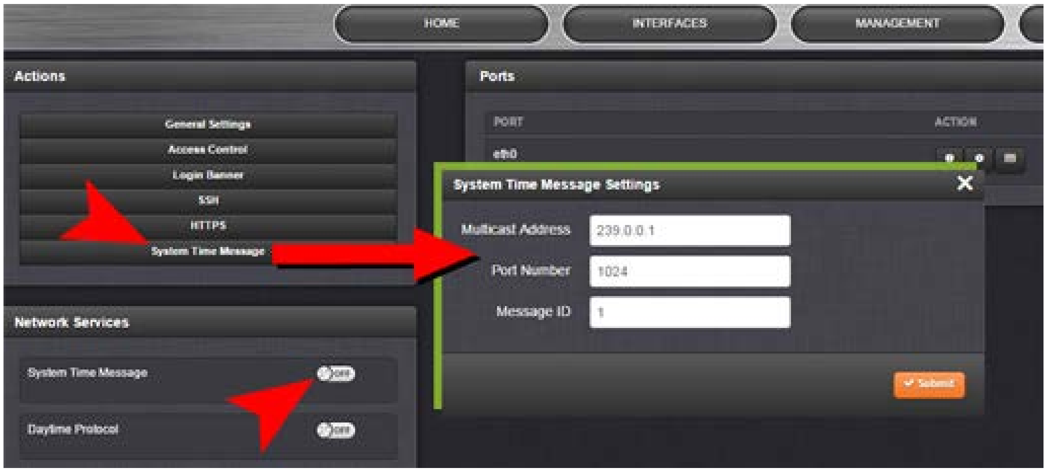
3.2.2.9 System Time Message

The **System Time Message** is a feature used for special applications that require a once-per-second time message to be sent out by SecureSync via multicast. This time message will be transmitted before every 1PPS signal, and can be used to evaluate accuracy and jitter.

To set up and enable a **System Time Message**:

1. Navigate to **MANAGEMENT** > **NETWORK** > **Actions** panel, and select S**ystem Time Message**. The **Settings** window will pop-up.
2. Populate the fields **Multicast Address**, **Port Number** and **Message ID**, and click **Submit**.

3. In the **Network Services** panel, enable the **System Time Message**.



System Time Message Settings

Multicast Address: 239.0.0.1

Port Number: 1024

Message ID: 1

System Time Message: OFF

Daytime Protocol: OFF

System Time Message Format

This message contains the time when the next 1PPS discrete will occur. It is sent once per second prior to the 1PPS discrete.

Word	Byte 3	Byte 2	Byte 1	Byte 0
1	Msg ID			
2	Msg Size			
3	Seconds			
4	nSec			
5	EOM			

Table 3-3: System Time Message format

Data Name	Data Description	Range	Resolution	Units
Message ID	UID of the message; 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

Table 3-4: System Time Message field descriptions

3.2.2.10 Configuring SNMP and Notifications

SNMP (Simple Network Management Protocol) is a widely accepted application-layer protocol for managing and monitoring network elements. It has been defined by the Internet Architecture Board under RFC 1157 for exchanging management information between network devices, and is part of the TCP/IP protocol.

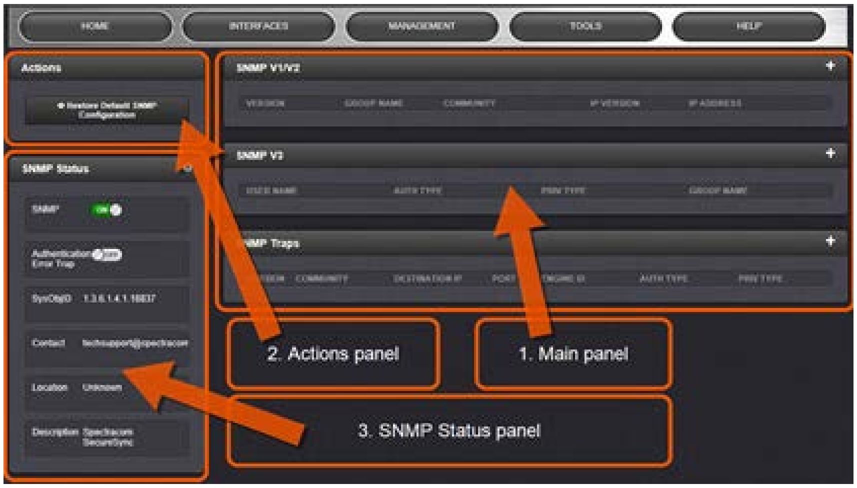
SNMP agents must be enabled and configured so that they can communicate with the network management system (NMS). The agent is also responsible for controlling the database of control variables defined in the Management Information Base (MIB).

SecureSync's SNMP functionality supports SNMP versions V1, V2c and V3 (with SNMP Version 3 being a secure SNMP protocol).

Accessing the SNMP Setup Screen

To access the **SNMP Setup** screen, navigate to **MANAGEMENT > NETWORK: SNMP Setup**.

The **SNMP** screen will display:



SNMP ON
Authentication Error Trap
SysObjID 1.3.6.1.4.1.18837
Contact techsupport@spectracom
Location Unknown
Description Spectracom SecureSync

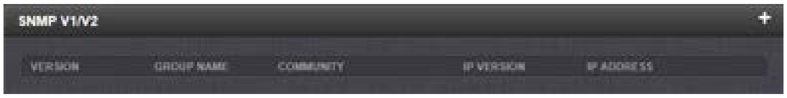
The **SNMP** screen is divided into 3 panels:

1. The **Main panel**, which is subdivided into 3 displays:
   - **SNMP V1/V2**–This panel allows configuration of SNMP v1 and v2c communities (used to restrict or allow access to SNMP). This tab allows the configurations for SNMP v1 and v2c, including the protocols allowed, permissions and Community names as well as the ability to permit or deny access to portions of the network. Clicking on the “+” symbol in the top-right corner opens the SNMP V1/V2c Settings for Access Screen. See "Configuring SNMP V1/V2 Communities" below.
   - **SNMP V3**–This panel allows configuration of SNMP v3 functionality, including the user name, read/write permissions, authorization passwords as well as privilege Types and Passphrases. Clicking on the “+” symbol in the top-right corner opens the SNMP V3 Screen. See "Configuring SNMP V3 Users" on page 86.
   - **SNMP Traps**–This panel allows the ability to define up to five different SNMP Managers that SNMP traps can be sent to over the network. This allows for SNMP Managers in different geographical areas to receive the same SNMP traps that Managers in other areas also receive. Clicking the PLUS icon in the top-right corner opens the SNMP Traps Settings Screen. See "Defining SNMP Traps (Notifications)" on page 88.
2. The **Actions panel**, which contains the **Restore Default SNMP Configuration** button.
3. The **SNMP Status panel**, which offers:
   - An **SNMP** ON/OFF switch.
   - An **Authentication Error Trap** ON/OFF switch.
   - **SysObjID**–The System Object ID number. This is editable in the SNMP Status panel (see "Configuring SNMP Status Settings" on page 90).
   - **Contact Information**–The email to contact for service. This is editable in the SNMP Status panel (see "Configuring SNMP Status Settings" on page 90).
   - **Location**–The system location. This is editable in the SNMP Status panel (see "Configuring SNMP Status Settings" on page 90).
   - **Description**–A simple product description. This is not editable in the SNMP Status.

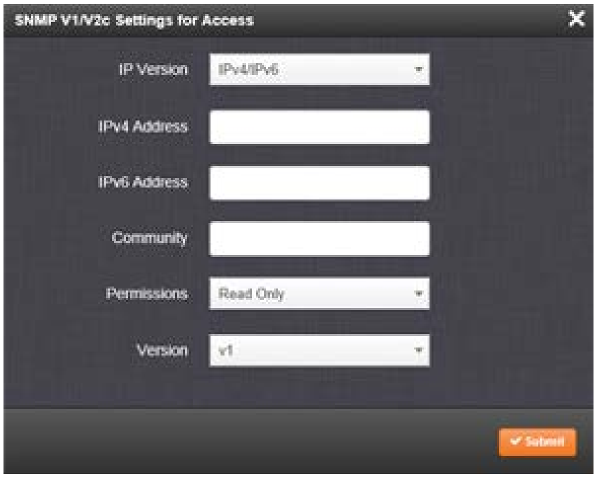
Configuring SNMP V1/V2 Communities

Creating Communities

1. Navigate to the **MANAGEMENT/NETWORK/SNMP Setup** screen.
2. In the **SNMP V1/V2** panel click the PLUS icon in the top-right corner.



3. The **SNMP V1/V2c Settings for Access** window will display.



SNMP V1/V2c Settings for Access

IP Version: IPv4/IPv6

IPv4 Address:

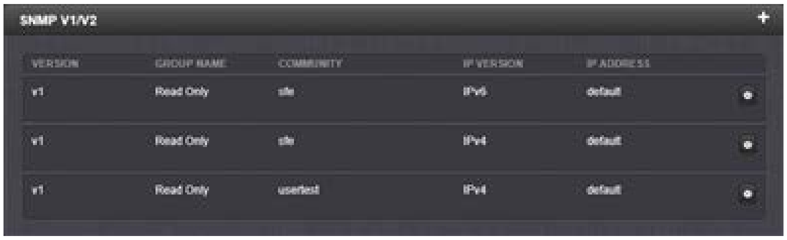
IPv6 Address:

Community:

Permissions: Read Only

Version: v1

4. Enter the required information in the fields provided
   - The **IP Version** field provides a choice of IPv4, IPV6 or both IPv4 and IPv6 (= default).
   - The choices offered below will change in context with the choice made in the **IP Version** field.
   - If no value is entered in the **IPv4** and/or **IPv6** field, SecureSync uses the system default address.
   - SNMP **Community** names should be between 4 and 32 characters in length.
   - **Permissions** may be Read Only or Read/Write
   - The **Version** field provides a choice of V1 or V2c.
5. Click the **Submit** button at the bottom of the window. Cancel any changes by clicking the **X**-icon in the top-right corner (any information entered will be lost).
6. The created communities will appear in the **SNMP V1/V2** panel.



SNMP V1/V2

VERSION	GROUP NAME	COMMUNITY	IP VERSION	IP ADDRESS
v1	Read Only	sfe	IPv6	default
v1	Read Only	sfe	IPv4	default
v1	Read Only	usertest	IPv4	default

Editing and Deleting Communities

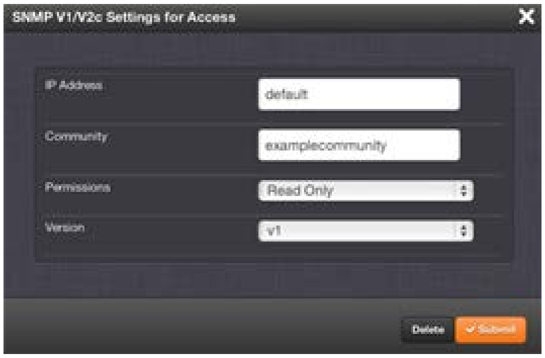
To edit or delete a community you have created:

1. Click the row of the **SNMP V1/V2** panel that displays the community you wish to edit or delete. The cursor will change from an arrow icon to a pointing finger to indicate that the

entry is clickable.

2. The **SNMP V1/V2c Settings for Access** window will display.

> **Note:** The options available for editing in the SNMP V1/V2c Settings for Access window will vary contextually according to the information in the entry chosen.


SNMP V1/V2c Settings for Access

IP Address: default

Community: examplecommunity

Permissions: Read Only

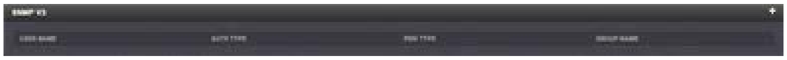
Version: v1

3. To edit the settings, enter the new details you want to edit and click the **Submit** button.
4. OR: To delete the entry, click the **Delete** button.

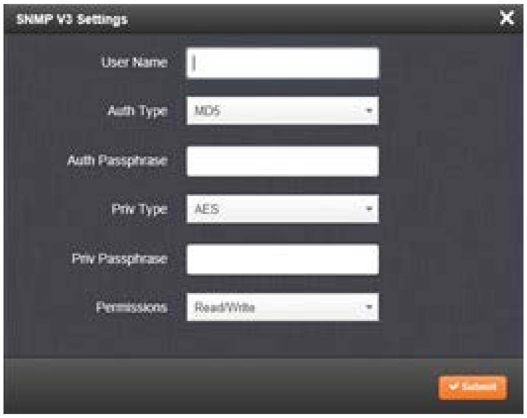
Configuring SNMP V3 Users

Creating Users

1. Navigate to the **MANAGEMENT/NETWORK/SNMP Setup** screen.
2. In the **SNMP V3** panel, click the PLUS icon in the top-right corner.



3. The **SNMP V3 Settings** window will display.


SNMP V3 Settings

User Name:

Auth Type: MD5

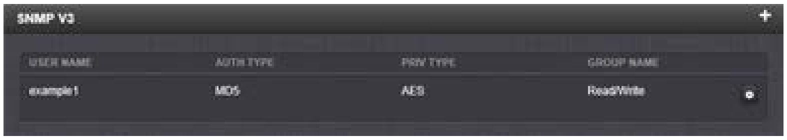
Auth Passphrase:

Priv Type: AES

Priv Passphrase:

Permissions: Read/Write

4. Enter the required information in the fields provided.
   - SNMP **User Names** and passwords are independent of users that are configured on the **Tools/Users** page.
     - User names are arbitrary. SNMP **User Names** should be between 1 and 31 characters in length.
     - The **User Name** must be the same on SecureSync and on the management station.
   - The **Auth Type** field provides a choice between MD5 and SHA.
   - The **Auth Password** must be between 8 and 32 characters in length.
   - The **Priv Type** field provides a choice between AES and DES.
   - The **Priv Passphrase** must be between 8 and 32 characters in length.
   - The **Permissions** field provides a choice between Read/Write and Read Only.
5. Click the **Submit** button at the bottom of the window. Cancel any changes by clicking the **X**-icon in the top-right corner (any information entered will be lost).
6. The created user will appear in the **SNMP V3** panel.



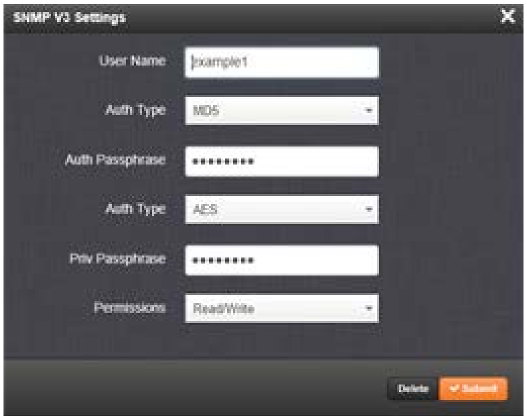
SNMP V3

USER NAME	AUTH TYPE	PRIV TYPE	GROUP NAME
example1	MD5	AES	Read/Write

Editing and Deleting Users

To edit or delete a user you have created:

1. Click the row of the **SNMP V3** panel that displays the community you wish to edit or delete. The cursor will change from an arrow icon to a pointing finger to indicate that the entry is clickable.
2. The **SNMP V3 Settings** window will display:



SNMP V3 Settings

User Name: example1

Auth Type: MD5

Auth Passphrase: ••••••••

Auth Type: AES

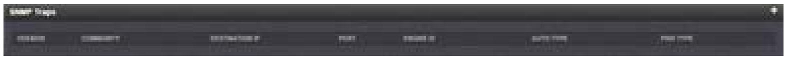
Priv Passphrase: ••••••••

Permissions: Read/Write

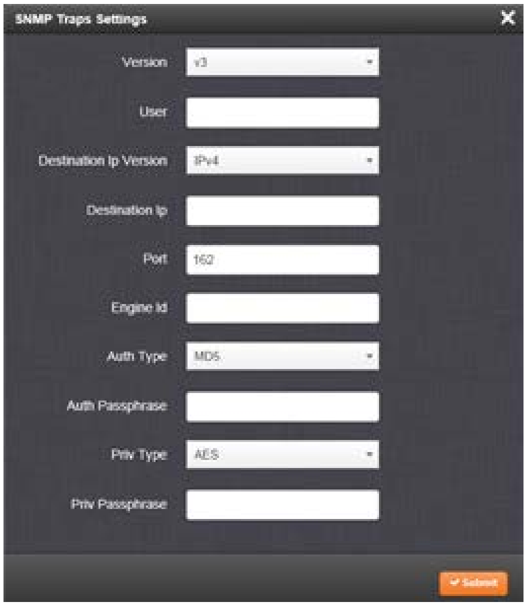
3. To edit the settings, enter the new details you want to edit and click the **Submit** button. Cancel any changes by clicking the **X**-icon in the upper right-hand corner (any information entered will be lost).
4. OR: To delete the entry, click the **Delete** button.

Defining SNMP Traps (Notifications)

1. Navigate to the **MANAGEMENT/NETWORK/SNMP Setup** screen.
2. In the **SNMP Traps** panel, click the PLUS icon in the top-right corner.



3. The **SNMP Traps Settings** window will display.


SNMP Traps Settings

Version: v3

User:

Destination Ip Version: IPv4

Destination Ip:

Port: 162

Engine Id:

Auth Type: MD5

Auth Passphrase:

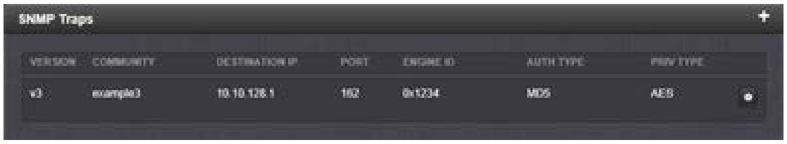
Priv Type: AES

Priv Passphrase:

4. Enter the required information in the fields provided. (Note that the options available for editing will vary contexturally according to the users's choice in the **Version** field.)
   - The **Version** field provides a choice between v1, v2c and v3 (the default)
   - SNMP **User** names should be between 4 and 32 characters in length.
   - **Destination IP Version** is a choice between IPv4 and IPv6.
   - **Destination IP** is destination address for the notification to be sent. The default Port is 162.
   - **Engine Id** must be a hexadecimal number (such as 0x1234).
   - **Auth Type** provides a choice between MD5 (the default) and SHA.
   - The **Auth Password** must be between 8 and 32 characters in length.

- » The **Priv Type** field provides a choice between AES and DES.
- » The **Priv Passphrase** must be between 8 and 32 characters in length.

5. Click the **Submit** button at the bottom of the window. Cancel any changes by clicking the **X**-icon in the top-right corner (any information entered will be lost).
6. The SNMP trap you created will appear in the **SNMP Traps** panel.



SNMP Traps

VERSION	COMMUNITY	DESTINATION IP	PORT	ENGINE ID	AUTH TYPE	PRIV TYPE
v3	example3	10.10.128.1	162	0x1234	MD5	AES

Each row of the **SNMP Traps** panel includes the version of the SNMP functionality, the User-/Community name for the trap, the IP address/Hostname of the SNMP Manager and values applicable only to SNMP v3, which include the Engine ID, the Authorization Type, the Privilege Type.

You may define up to five different SNMP Managers to whom SNMP traps can be sent over the network. This allows for SNMP Managers in different geographical areas to receive the same SNMP traps.

> **Note:** Spectracom has been assigned the enterprise identifier 18837 by the IANA (Internet Assigned Numbers Authority). Spectracom's product MIBs reside under the enterprise identifier @18837.3.

For detailed descriptions of the objects and traps supported by the SecureSync, please refer to the Spectracom SecureSync MIB files. See "Accessing the SNMP Support MIB Files" on page 91.

About SNMP Traps

SecureSync can provide SNMP traps when events occur to provide remote indications of status changes. SNMP Traps are one way to remotely monitor SecureSync status.

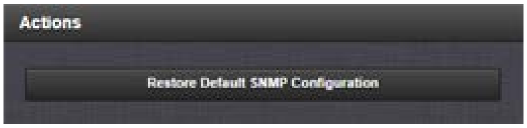
The SNMP traps indicate the status change that caused the trap to be sent and may also include one or more objects, referred to as variable-bindings, or **varbinds**. A varbind provides a current SecureSync data object that is related to the specific trap that was sent. For example, when a Holdover trap is sent because SecureSync either entered or exited the Holdover mode, the trap varbind will indicate that SecureSync is either currently in Holdover mode or not currently in Holdover mode.

For testing purposes, a command line interface command is provided. This command, `testevent`, allows one, several, or all of the traps defined in the SecureSync MIB to be generated. Refer to "CLI Commands" on page 467 for command details.

Restoring the Default SNMP Configuration

To restore the SecureSync to its default SNMP configuration:

1. Navigate to the **MANAGEMENT/NETWORK/SNMP Setup** screen.
2. In the **Actions** panel, click the **Restore Default SNMP Configuration** button.



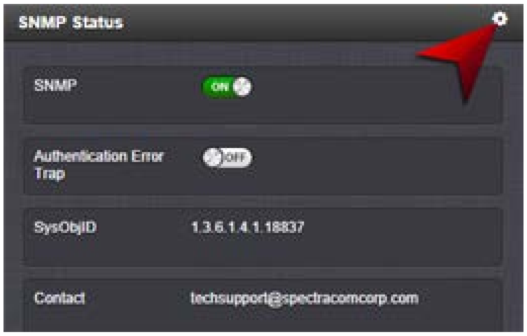
3. Confirm that you want to restore the default settings in the pop-up message.

Configuring SNMP Status Settings

The SNMP Status Settings include the **sysObjectID**, **sysContact**, and **sysLocation**.

To configure SNMP Status Settings:

1. Navigate to the **MANAGEMENT > NETWORK: SNMP Setup** screen.
2. In the **SNMP Status** panel on the left-hand side of the screen, click the GEAR icon in the top-right corner of the panel.



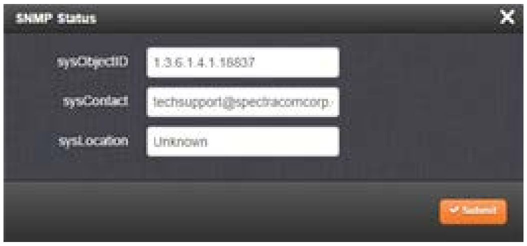
SNMP ON

Authentication Error Trap OFF

SysObjID 1.3.6.1.4.1.18837

Contact techsupport@spectracomcorp.com

3. The **SNMP Status** pop-up window will display:



sysObjectID 1.3.6.1.4.1.18837

sysContact techsupport@spectracomcorp.

sysLocation Unknown

The following settings can be configured in this window:

- In the **sysObjectID** field, enter the SNMP system object ID.
- In the **sysContact** field, enter the e-mail information for the system contact you wish to use.
- In the **sysLocation** field, enter the system location of your SecureSync unit.

4. Submit your changes by clicking the **Submit** button in the lower right-hand corner. Cancel any changes by clicking the **X**-icon in the top-right corner (any information entered will be lost).

Accessing the SNMP Support MIB Files

Spectracom's private enterprise MIB files can be extracted via File Transfer Protocol (FTP) from SecureSync using an FTP client such as Microsoft FTP, CoreFTP, or any other shareware/freeware FTP program.

To obtain the MIB files from SecureSync via FTP/SFTP:

1. Using an FTP program, log in as an administrator.
2. Through the FTP program, locate the Spectracom MIB files in the `/home/spectracom/mibs` directory.
3. FTP the files to the desired location on your PC for later transfer to the SNMP Manager.
4. Compile the MIB files onto the SNMP Manager.

Note: When compiling the MIB files, some SNMP Manager programs may require the MIB files to be named something other than the current names for the files. The MIB file names may be changed or edited as necessary to meet the requirements of the SNMP Manager. Refer to the SNMP Manager documentation for more information on these requirements.

Note: In addition to the Spectracom MIB files, there are also some net-snmp MIB files provided. Net-snmp is the embedded SNMP agent that is used in the SecureSync and it provides traps to notify the user when it starts, restarts, or shuts down. These MIB files may also be compiled into your SNMP manager, if they are not already present.

Spectracom's private enterprise MIB files can be requested and obtained from the Spectracom Customer Service department via email at techsupport@spectracomcorp.com.

Note: By default, techsupport@spectracomcorp.com is the address in the sysContact field of the SNMP Status panel of the SNMP Setup page.

3.3 Network Time Protocol (NTP)

Network Time Protocol (NTP) and Simple Network Time Protocol (SNTP) are client-server protocols for synchronizing time on IP networks. NTP provides greater accuracy and error checking than does SNTP.

NTP and SNTP are used to synchronize time on any computer equipment compatible with the Network Time Protocol. This includes Cisco routers and switches, UNIX machines, and Windows machines with suitable clients. To synchronize a single workstation, several freeware or shareware NTP clients are available on the Internet. The software running on the PC determines whether NTP or SNTP is used.

When the NTP service is enabled, SecureSync will “listen” for NTP request messages from NTP clients on the network. When an NTP request packet is received, SecureSync will send an NTP response time packet to the requesting client. Under typical conditions, SecureSync can service at least 9,000 NTP requests per second without MD5 authentication enabled, and at a somewhat lower rate with MD5 authentication enabled.

The user can either enable or completely disable the NTP Service. When NTP is disabled, no NTP time packets will be sent out to the network. When enabled, per default the NTP Service operates in Unicast mode, i.e. the NTP Service responds to NTP requests only. Also supported are a Broadcast mode in which SecureSync sends an NTP time packet to the network broadcast address, as well as an Anycast mode (see "NTP over Anycast" on page 102.)

Note: In order to configure NTP, you need to access the NTP Setup screen which requires ADMINISTRATOR rights.

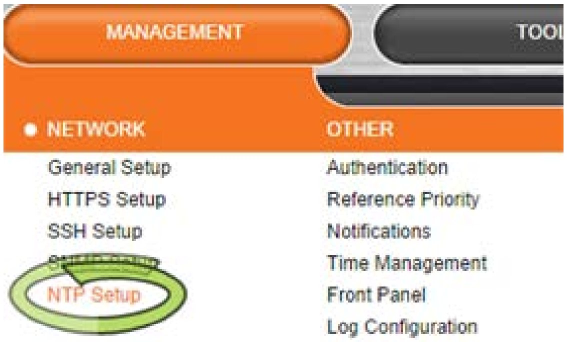
Often, it is not necessary to modify the NTP factory default configuration settings. However, most of the settings can be changed by the user in order to support specific NTP applications which may require a non-standard configuration: These features include the ability to use either MD5 authentication or NTP Autokey, to block NTP access to parts of the network and to broadcast NTP data to the network’s broadcast address.

Most of these topics listed below can also be accessed through "The NTP Setup Screen" below, which is a good starting point for 'how-to' instructions. Additional information on system monitoring can be found under "NTP Status Monitoring" on page 251.

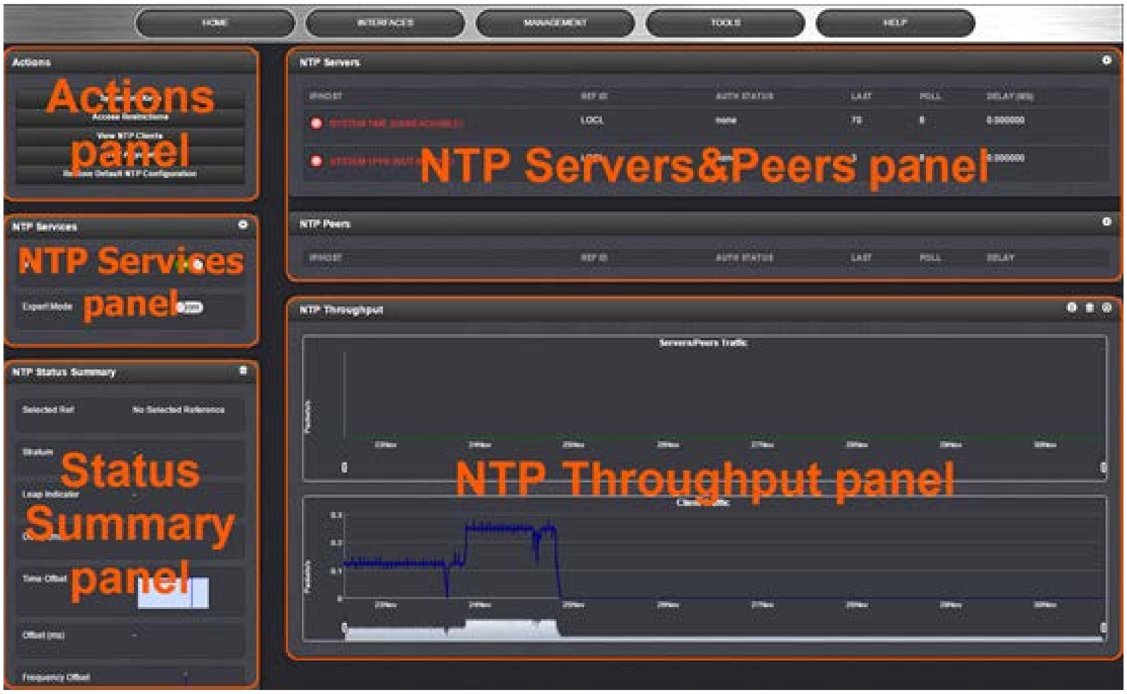
3.3.1 The NTP Setup Screen

The **NTP Setup** screen provides access to all NTP configuration settings.

To open the **NTP Setup** screen, select **MANAGEMENT > NETWORK: NTP Setup**.



The **NTP Setup** screen will be displayed; it is divided into 5 panels:



The NTP Servers and Peers panel on the right-hand side of the **NTP** screen is divided into 2 sub-panels:

» **NTP Servers**: In this display you can view the NTP Servers that SecureSync detects in your network. It is through this display that you configure external NTP references. See "NTP Servers: Adding, Configuring, Deleting" on page 113.

» **NTP Peers**: In this display you can view the NTP Peers that SecureSync detects in your network. It is through this display that you configure NTP Peer reference inputs. See "NTP Peers: Adding, Configuring, Deleting" on page 114.

For more information on NTP servers, peers, and stratums see "NTP Servers & Peers (Stratum Synchronization)" on page 95.

The NTP Throughput panel shows two graphs depicting the rate of NTP traffic from Clients and Server/Peers.

The INFO icon opens a window showing the maximum per second traffic rate from each.

The graphs maybe saved and downloaded (> ARROW icon), or deleted (> TRASHCAN icon).

This data is currently only displayed for NTP, and not for TimeKeeper.

The Actions panel in the top left-hand corner of the **NTP** screen comprises the following buttons:

> Note: The NTP Actions panel will be disabled if you applied the optional TimeKeeper license, and enabled TimeKeeper (MONITORING > TimeKeeper Service).

- **Symmetric Keys**: Click here to set up your symmetric keys for MD5 authentication. For more information on Symmetrec Keys, see "Symmetric Keys (MD5 Authentication)" on page 101.
- **Access Restrictions**: Click here to view, change or delete access restrictions to the NTP network. (See also "Configuring NTP Access Restrictions" on page 119.)
  Fields in the NTP Access Restrictions table include:
  - Type
  - IP Version
  - IP
  - IP Mask
  - Auth only
  - Enable Query
- **View NTP Clients**: Click here to reveal a table of all the clients your SecureSync is servicing. (See also "Viewing NTP Clients" on page 121)
  Information for each client includes:
  - Client IP
  - Received Packets
  - Mode
  - Version
  - Restriction Flags
  - Avg Interval
  - Last Interval
- **NTP Anycast**: Click here to enable and configure Anycast. See also "NTP over Anycast" on page 102.
- **Restore Default NTP Configuration**: Click here to restore SecureSync's NTP settings to the factory default. Any settings you have created previously will be lost. See "Restoring the Default NTP Configuration" on page 121.

The NTP Services panel is the second panel on the left-hand side of the NTP screen. It has two switches:

- **NTP ON/OFF**: This switch enables and disables NTP. See "Enabling and Disabling NTP" on page 122.

  Note: When the NTP timescale is changed or when you have changed any NTP configurations, use this switch to disable and then enable NTP.

- **Expert Mode**: Turning this switch ON enables direct access to the **NTP.conf** file, thus bypassing the SecureSync Web UI. [Default =OFF] See "NTP Expert Mode" on page 109.

Note: Spectracom Tech Support does not support the editing of the NTP configuration files in Expert Mode. For additional information on editing the NTP.-conf file, please refer to http://www.ntp.org.

Other **NTP Services** that can be configured via the **NTP Services** panel by clicking the GEAR icon are:

- Broadcast (see "Enabling/Disabling NTP Broadcasting" on page 122)
- Autokey (see "Configuring NTP Autokey" on page 123)
- Stratum 1 (see "NTP Stratum Configuration" on page 125)

The NTP Status Summary panel provides a realtime overview of your key NTP network parameters. See "NTP Status Monitoring" on page 251.

3.3.2 NTP Servers & Peers (Stratum Synchronization)

Other available NTP servers can be configured as potential input time references for System Time synchronization. A group of NTP servers at the same Stratum level (Stratum 1 time servers for example) are listed as NTP peers to each other. NTP Servers at a higher Stratum than another are configured as NTP Servers instead (Internet Time Servers should be configured as NTP Servers and not as NTP peers).

Note: IMPORTANT: In order for other NTP servers to be a valid reference, “NTP” must be enabled in the Reference Priority table (see "Configuring Input Reference Priorities" on page 155).

It is recommended to use one or more NTP Peers when you desire to provide mutual backup. Each peer is normally configured to operate from one or more time sources including reference clocks or other higher stratum servers. If a peer loses all reference clocks or fails, the other peers continue to provide time to other clients on the network.

SecureSync can be configured to receive time from one or more available NTP servers (SecureSyncs, or different models). The other NTP servers can then be valid input references for System Time synchronization. This is commonly referred to as NTP Peering.

When SecureSync is configured to obtain time from other NTP servers at the same Stratum level (configured as NTP Peers) but is currently using another input reference other than the NTP server (s) as its selected reference, SecureSync will report to the network (in the NTP time stamps) that it is a Stratum 1 time server. But, at some point, if all other input references besides the other NTP server(s) become unavailable, SecureSync will then drop to a Stratum 2 time server (with System Time being derived from the NTP time packets being received from the other NTP Peers.

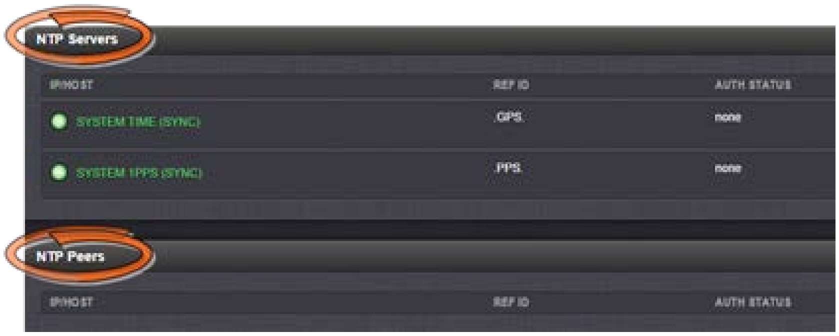
When SecureSync is configured to obtain time from other NTP servers at a higher stratum than it is (configured as NTP Servers) and is using the NTP server as its selected reference, SecureSync will report to the network (in the NTP time stamps) that it is one less Stratum than its selected reference NTP server (i.e., if SecureSync is configured to receive time from one or more Stratum 1

NTP Servers, with no other higher priority input references available, SecureSync will report to the network that it is a Stratum 2 time server).

In order for SecureSync to use other NTP servers as a valid time reference to synchronize the System Time, the input Reference Priority Setup table must be configured to allow NTP as an available reference. For more information on the input Reference Priority table, refer to "Configuring Input Reference Priorities" on page 155.

If SecureSync is synchronized to another NTP server and the other NTP server subsequently loses sync or becomes unavailable (with no other higher priority input references being present and valid) SecureSync will then go into the Holdover mode until any enabled and valid input reference becomes available again (or until the Holdover period expires, whichever one occurs first). During Holdover mode, NTP will remain at the same Stratum level it was before entering the Holdover mode and can continue to be the reference to the network. However, if no input reference becomes available before the Holdover period expires, Time Sync will be lost and shortly thereafter, NTP will report to the network that it is now at Stratum 15. A status of Stratum 15 will cause the network to ignore SecureSync as an NTP time reference. Refer to "Holdover Mode" on page 195 for information on obtaining or configuring the allowable Holdover period.

3.3.2.1 The NTP Servers and NTP Peers Panels



NTP Servers

IP/HOST	REF ID	AUTH STATUS
● SYSTEM TIME (SYNC)	GPS	none
● SYSTEM 1PPS (SYNC)	PPS	none

NTP Peers

IP/HOST	REF ID	AUTH STATUS

The **NTP Servers** and **NTP Peers** panels (see also "The NTP Setup Screen" on page 92) display which servers in the network are set up at a higher stratum (Servers) or at an equal stratum (Peers).

The **NTP Servers** panel and **NTP Peers** panel display the following information:

- **IP/HOST**
- **REF ID**–The type of input reference (for example, "GPS" indicates the reference can use GPS for its synchronization). Below is a list of potential REF IDs reported by the timing system (others may be reported by other NTP peers or servers):
  - **GPS**–GNSS reference
  - **IRIG**–IRIG reference
  - **HVQ**–HAVE QUICK reference
  - **FREQ**–Frequency reference
  - **PPS**–External 1PPS reference

  - **PTP**–PTP reference
  - **ATC**–ASCII time code reference
  - **USER**–User provided time
  - **LOCL**–Local reference (synced to itself)
  - **INIT**–NTP on server/peer is initializing
  - **STEP**–NTP on server/peer is performing initial synchronization step and restarting
- **AUTH STATUS**–Indicates if the selected reference is using MD5 authentication. “None” indicates authentication not being used.
- **LAST**–The number of seconds it’s been since this reference was last polled for its time.
- **POLL**–The poll interval, how often SecureSync is polling this NTP reference for its time.
- **DELAY (ms)**–The measured one-way delay between SecureSync and its selected reference.

Note: NTP clients of the SecureSync are viewable through the View NTP Clients option In the Actions panel of the NTP Setup screen.

Note: In order for other NTP servers to be a valid reference, “NTP” must be enabled as both the Time and 1PPS references in the Reference Priority table. See "Configuring Input Reference Priorities" on page 155.

To remove a server (and its associated configurations), select the “Clear” option at the end of its row to “Enabled” and click Submit. That particular row will then be immediately cleared.

Note: In order for NTP configuration changes to take effect, NTP should be disabled and then enabled after any configurations changes have been made. NTP can be stopped and restarted from the MANAGEMENT/NETWORK/NTP Setup page, in the NTP Service panel on the left-hand side of the page.

In the “NTP service” field, select “Disabled’, then click Submit to disable NTP, then Select “Enabled” and click Submit again to re-enable NTP. Changes made will now take effect and NTP operation will be restored shortly after this operation is performed.

If SecureSync has no valid Timing System Reference, NTP Server or NTP Peers, the NTP Stratum value is automatically increased to Stratum 15. This ensures no NTP clients can use it as a time reference when unsynchronized. This feature utilizes automatic enabling and disabling of the Local Clock Reference driver to force Stratum 15. The automatic Local Clock Reference mode is disabled in NTP Expert mode if the user configures a Local Clock Reference Driver, or if the comment `# DISABLE_AUTO_LOCAL` is added to the NTP configuration file.

3.3.3 NTP Output Timescale

The timescale for the time that is provided to the network nodes via the NTP time stamps is determined by the Timescale selected in the SecureSync System Time Setup Page, accessed through the Web UI at **MANAGEMENT/OTHER/Time Management**. See "The Time Management Screen" on page 169. If the **Timescale** in **System Time Setup** is selected as “UTC”, the network PCs will receive UTC time via NTP. If “GPS” is selected instead, the network PCs will receive GPS time via NTP. When the **Timescale** is set to “GPS”, the GPS-to-UTC offset on the Setup/Time Management page must be set correctly. Typically, UTC is the desired **Timescale** for network synchronization.

Note: IMPORTANT: Make sure the desired timescale for the NTP output is selected in the System Time Setup.

Having the incorrect timescale selected can result an undesired time error in the NTP clients that are synchronizing to SecureSync via NTP. As of July 2015, the offset between UTC and GPS time is 17 seconds.

Note: IMPORTANT: Configuration changes made to SecureSync’s NTP configurations do not take effect until the NTP Service is Disabled and then Enabled (or until SecureSync is rebooted/power cycled). The NTP service can be stopped and started from the MANAGMENT/NTP Setup in the NTP Services panel. Once NTP has been re-enabled, NTP will be available again for network synchronization within a few minutes.

The **MANAGEMENT/NETWORK/NTP Setup** page allows NTP broadcast capability to be enabled (this feature very rarely needs to be enabled) and allows the network access of the NTP time stamps to be limited to only certain clients on the network (this feature is also rarely used).

3.3.4 NTP Timing System: Reference Selection and Preference

If desired, Time and PPS References for the NTP service can be configured as **Preferred**. This provides additional “weighting” to that particular NTP input reference during the selection process, while NTP is deciding which reference it should select as its source (though “prefer” does not guarantee that reference will become the selected reference).

- The **Timing System Reference/Preferred (Enabled/Disabled)** option configures NTP to “weight” the Timing system input heavier than input from other NTP servers for its selection (The Timing System inputs are normally more accurate than other NTP servers). However, if the Timing System inputs are not normally available (such as with intermittent GNSS reception or no other inputs are available), it may be desired not to prefer the Timing System over an NTP reference, in which case this box should not be checked.
- The **Timing System 1PPS Reference (Enabled/Disabled)** option determines whether or not NTP uses the 1PPS input from the Timing System. The 1PPS input to NTP needs to

correlate with its “Time” input. If the Time and PPS inputs are originating from the same source, they will be correlated. However, if the time is originating from another NTP server, but the 1PPS is being derived by the Timing System, the two inputs may not always correlate. Without this correlation, NTP performance will be degraded. In this scenario, it is best not to use the System Time’s 1PPS as a reference.

Normally, the NTP service will obtain its Time and PPS reference inputs from the Timing System (the Timing System is the time as derived from the GNSS, IRIG, ASCII data inputs, etc.). However, if desired, NTP can also obtain time from other NTP server(s). When the Timing System references are normally available to SecureSync, the “Timing System 1PPS reference” should be enabled and the “Timing System Reference” should be Preferred (both of the boxes at the top of the page enabled). This provides NTP with the most accurate references.

In the case of Stratum synchronization (only syncing SecureSync to other NTP servers, instead of the Timing System, so that is can operate as a Stratum 2 time server, for example), the Timing System inputs are not going to be available, as the only available input will be other configured NTP servers. In this scenario, it is best to uncheck both options at the top of the page so that the Timing System is not preferred over a configured NTP server and to keep the Timing System’s 1PPS from affecting the operation of NTP (as its 1PPS will not correlate with the NTP time input being received from the other NTP servers).

Note: It is not normally recommended to enable the Timing System Reference Preferred checkbox in addition to enabling any of the Preferred boxes in the NTP Servers table.

Normally, either select the Prefer Timing System Reference and none of the Preferred boxes in the NTP servers table (if the Timing System inputs are normally available) or de-select the Prefer Timing System Reference and enable Preferred on one of the NTP servers in the NTP Servers table (if the Timing System inputs are not normally available).

It is not normally recommended to select more than one NTP Server in the NTP Servers table as being Prefer. Typically, only one NTP server in the table should be selected as Prefer (and should only be selected if the box Prefer Timing System Reference: is not checked).

The maximum number of NTP Peers (or NTP Servers) that can be configured as time references is twelve (12). For best results, more than four NTP time servers are recommended. As few as one NTP time server may be used, however, depending on your needs and network timing architecture. A specific NTP server is recommended to be configured as the preferred time reference by selecting the preferred checkbox.

For both NTP Peers and NTP Servers the Minimum and Maximum Poll rate for NTP packets can be configured. Both NTP Peers and NTP Servers support either manually configured Symmetric Key-ID/Key string pairs or the use of Auto-Key. However, these choices are mutually exclusive and must be identically configured on both the SecureSync and the NTP Peer or NTP Server. If the Symmetric Key-ID/Key string pair method is selected the Key-ID must be first defined on the Symmetric Key page.

The entry for NTP Peer or NTP Server can be deleted by selecting the Clear checkbox and pressing Submit.

The grids on the NTP Peers and Servers tabs allow the user to define, by IP address or hostname, the locations of other NTP servers to use as time references (instead of, or in addition to, the configured SecureSync's primary reference) and the locations of other NTP servers to use as peers. The maximum number of Peers allowed is twelve (12).

3.3.5 NTP Keys

3.3.5.1 NTP Autokey

Note that NTP Autokey is currently not supported, for more information, see http://bugs.ntp.org/show_bug.cgi?id=3005.

NTP Autokey–Support & Limitations

Currently, SecureSync supports only the IFF (Identify Friend or Foe) Autokey Identity Scheme. The SecureSync product web interface automates the configuration of the IFF using the MD5 digests and RSA keys and certificates. At this time the configuration of other key types or other digests is not supported.

Note: When you configure NTP Autokey, you must disable the NTP service first, and then re-enable it after Autokey configuration is completed.

NTP Autokey–IFF Autokey Support

The IFF Autokey Support is demonstrated in the figure below. The IFF identity scheme is used with Multiple Stratum NTP Time Servers. The example below shows 3 Stratum layers. Stratum 1 NTP Servers are close to the physical time references. All Stratum 1 servers can be Trusted Hosts. One of them is used to generate the IFF Group/Client Key. This defines the IFF Group.

All other group members generate Group Certificate and RSA public/private keys using MD5 digest. Each group member must share the common IFF Group/Client Key (recommended). Stratum 2 NTP servers are also members of the Group. All NTP Stratum 1 servers are Trusted Hosts. The NTP servers closest to the actual time reference (Stratum 1) should be designated trusted. A single Stratum 1 NTP server generates the IFF Group/Client Keys. There is NO group name feature supported. The Group can use the same passphrase (password) or different passphrases for each client.

An NTP Server Group member is configured by enabling Autokey and creating certificate and public/private key pair while not enabling the Client Only selection. A Client Only NTP server is configured by enabling Autokey and creating certificate and public/private key pair and enabling the Client Only selection.

Note: Passphrases can be identical for all group members and Client NTP Servers. Or passphrases can be the same for group members and a different passphrase shared between the Client Only NTP Servers.

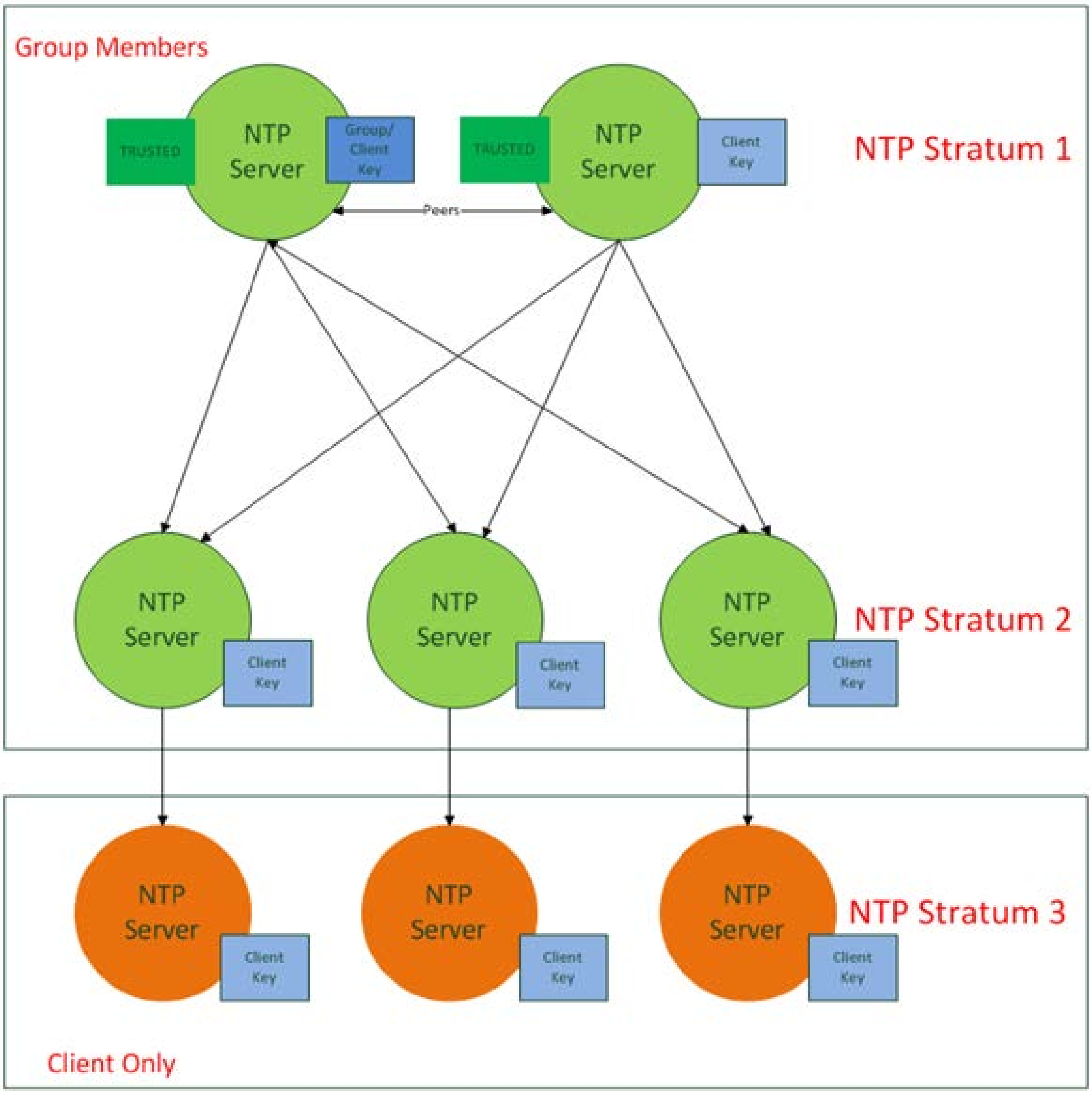


Figure 3-1: IFF Autokey configuration example

3.3.5.2 Symmetric Keys (MD5 Authentication)

SecureSync supports authenticated NTP packets using an MD5 authenticator. This feature does not encrypt the time packets, but attaches an authenticator, which consists of a key identifier and an MD5 message digest, to the end of each packet. This can be used to guarantee that NTP packets came from a valid NTP client or server, and that they were not tampered with during transmission. The Symmetrical Keys tab allows NTP to be configured to use MD5 authentication. To configure Symmetric Keys, see "Configuring NTP Symmetric Keys (MD5 Authentication)" on page 116.

3.3.6 NTP over Anycast

NTP (Network Time Protocol) is a packet network based synchronization protocol for synchronizing a client clock to a network master clock (see also "Network Time Protocol (NTP)" on page 91.)

Anycast is a network routing protocol in which messages are routed to one of a group of potential receivers via a single Anycast address, thus avoiding the need to configure every client individually.

NTP over Anycast, as implemented in SecureSync, is a combination of the two concepts, allowing SecureSync to:

I. Associate one of its network ports to an Anycast IP address, and

II. Remove itself as an available time source if its reference is lost or degraded, and vice versa.

To learn more about NTP over Anycast, see also the respective Spectracom Technology Brief (PDF).

Please note that SecureSync utilizes the OSPF (Open Shortest Path First) protocol for internal routing, and BGP (Border Gateway Protocol) for external routing..

EXAMPLE:

If an active SecureSync NTP server has removed itself as an available time source from the Anycast-capable network, the OSPF router will send a request for replacement to the next nearest NTP server, serving under the same NTP over Anycast address.

As soon as the first SecureSync server obtains a valid reference again, it will make itself available to the OSPF router, which will then use it as a time source again, based on the principle of shortest path available.

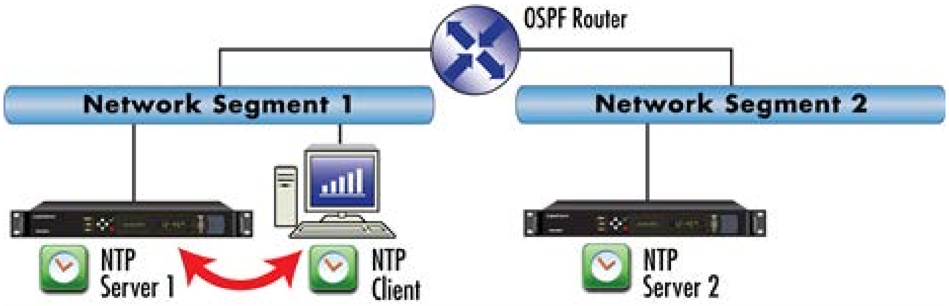


Figure 3-2: All NTP servers are synchronized

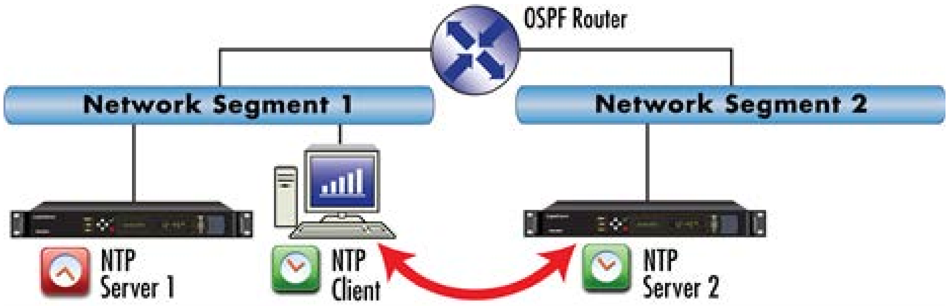


Figure 3-3: NTP server 1 is out of sync

3.3.6.1 Configuring NTP over Anycast (General Settings)

To setup the **NTP over Anycast** functionality:

1. Confirm that your existing network infrastructure is Anycast capable. Determine network specifics, such as the Anycast address and port.
2. In the SecureSync Web UI, navigate to **MANAGEMENT** > **Network** > **NTP Setup**.
3. In the **Actions Panel**, click **NTP over Anycast**.
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.
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.
8. Click **Submit**.

Note: NTP over Anycast is not compatible with TimeKeeper, i.e. these two services cannot be run simultaneously.

Note: IMPORTANT: For Anycast to function, SecureSync must be in sync to a valid reference, or to itself.

3.3.6.2 Configuring NTP over Anycast (OSPF IPv4)

To setup the **NTP over Anycast** functionality, using OSPF IPv4:

1. Confirm that your existing network infrastructure is Anycast capable, and uses OSPF Version 2 (IPv4). Determine the OSPF area.
2. In the SecureSync Web UI, navigate to **MANAGEMENT** > **Network** > **NTP Setup**.
3. In the **NTP Anycast** window, select the **General** tab.
4. On the **General** tab, select **IPv4** as the IP Version.
5. Configure the **Anycast Address** to be used.
6. Select the port to associate the Anycast service with (depending on the option card configuration of your unit, there may be only ETH0 available).
7. In the **NTP Anycast** window, navigate to the **OSPF** tab.
8. On the **OSPF** tab, check **Enable**.
9. Setup the OSPF area.
10. Click Submit.
11. Select the port address to associate the Anycast service with (because there may be multiple addresses on a single port), and click Submit. If no addresses appear, an IP address must be added to the port (see "Configuring Network Ports" on page 48).
12. Next, specify the maximum TFOM Setting (Time Figure of Merit), and the Holdover Timeout value. These two parameters determine SecureSync's accuracy "tolerance window": A small window will cause SecureSync to deliver a more accurate time window, but also will cause it to quickly withdraw from the Anycast server pool, i.e. declare itself an invalid reference. (To find out more about TFOM, see "Oscillator Disciplining Setup" on page 192.)
    Navigate to **Management** > **Disciplining**, and click the GEAR icon in the top-right corner of the **Status** panel.
13. Set the value **Maximum TFOM for Sync** to 4 (this will make SecureSync to go out of sync if the phase error is greater than 1µs).
14. Set the value for **Holdover Timeout** to 10 s, to allow SecureSync to exit holdover quickly.
15. Leave the **Phase Error Limit** at 0, and do not check any of the checkboxes (or, for more information, see "Oscillator Disciplining" on page 188).

> **Note:** NTP over Anycast is not compatible with TimeKeeper, i.e. these two services cannot be run simultaneously.

3.3.6.3 Configuring NTP over Anycast (OSPF IPv6)

To setup the **NTP over Anycast** functionality, using OSPF IPv6:

1. Confirm that your existing network infrastructure is Anycast capable, and uses OSPF Version 3 (IPv6). Determine the OSPF area.

2. In the SecureSync Web UI, navigate to **MANAGEMENT** > **Network** > **NTP Setup**.
3. In the **NTP Anycast** window, select the **General** tab.
4. On the **General** tab, select **IPv6** as the IP Version.
5. Select the port to associate the Anycast service with (depending on the option card configuration of your unit, there may be only ETH0 available).
6. Select the port address to associate the Anycast service with (because there may be multiple IPv6 addresses on a single port), and click **Submit**. If no addresses appear, an IPv6 address must be added to the port.
7. In the **NTP Anycast** window, navigate to the **OSPF** tab.
8. On the **OSPF6** tab, check **Enable**.
9. Setup the OSPF6 area.
10. Click Submit.
11. Select the port address to associate the Anycast service with (because there may be multiple addresses on a single port), and click Submit. If no addresses appear, an IP address must be added to the port (see "Configuring Network Ports" on page 48).
12. Next, specify the maximum TFOM Setting (Time Figure of Merit), and the Holdover Timeout value. These two parameters determine SecureSync's accuracy "tolerance window": A small window will cause SecureSync to deliver a more accurate time window, but also will cause it to quickly withdraw from the Anycast server pool, i.e. declare itself an invalid reference. (To find out more about TFOM, see "Oscillator Disciplining Setup" on page 192.)
    Navigate to **Management** > **Disciplining**, and click the GEAR icon in the top-right corner of the **Status** panel.
13. Set the value **Maximum TFOM for Sync** to 4 (this will make SecureSync to go out of sync if the phase error is greater than 1µs).
14. Set the value for **Holdover Timeout** to 10 s, to allow SecureSync to exit holdover quickly.
15. Leave the **Phase Error Limit** at 0, and do not check any of the checkboxes (or, for more information, see "Oscillator Disciplining" on page 188).

3.3.6.4 Configuring NTP over Anycast (BGP)

To configure **NTP over Anycast**, using **BGP** (Border Gateway Protocol):

1. Confirm that your existing network infrastructure is Anycast capable, and uses BGP. Determine the network specifics, such as your Autonomous System (AS) number, Neighbor's address and Neighbor's AS number.
2. In the SecureSync Web UI, navigate to **MANAGEMENT > Network > NTP Setup.**
3. In the **NTP Anycast** window, select the **General** tab.
4. On the **General** tab, select your desired IP Version. This selection automatically communicates with the **BGP** tab and displays the neighbor address field based on your needs.

5. 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.
6. In the **NTP Anycast** window, navigate to the **BGP** tab.
7. On the **BGP** tab, check **Enable**.
8. Input your **AS number**.
9. Input the neighbor's address.
10. Input the neighbor's AS number.
11. Click **Submit**.
12. Select the port address to associate the Anycast service with (because there may be multiple addresses on a single port), and click Submit. If no addresses appear, an IP address must be added to the port (see "Configuring Network Ports" on page 48).
13. Next, specify the maximum TFOM Setting (Time Figure of Merit), and the Holdover Timeout value. These two parameters determine SecureSync's accuracy "tolerance window": A small window will cause SecureSync to deliver a more accurate time window, but also will cause it to quickly withdraw from the Anycast server pool, i.e. declare itself an invalid reference. (To find out more about TFOM, see "Oscillator Disciplining Setup" on page 192.)
    Navigate to **Management** > **Disciplining**, and click the GEAR icon in the top-right corner of the **Status** panel.
14. Set the value **Maximum TFOM for Sync** to 4 (this will make SecureSync to go out of sync if the phase error is greater than 1µs).
15. Set the value for **Holdover Timeout** to 10 s, to allow SecureSync to exit holdover quickly.
16. Leave the **Phase Error Limit** at 0, and do not check any of the checkboxes (or, for more information, see "Oscillator Disciplining" on page 188).

3.3.6.5 Anycast Expert Mode

Advanced Anycast configuration is possible via Expert Mode, which allows you to write directly into the Anycast configuration files (`zebra.conf`, `ospfd.conf`, `ospf6d.conf` and `bgpd.conf`).

The `zebra.conf` file is required for both IPv4, and IPv6 Anycast. The `ospfd.conf` file is required for IPv4 Anycast only, the `ospf6d.conf` file is required for IPv6 Anycast only, and the `bgpd.conf` file has multiprotocol functionality, hence it can be used for both IPv4, and IPv6 Anycast.

Caution: Expert Mode should only be utilized by advanced users, as incorrectly altering the Anycast files can cause Anycast to stop working.

Caution: Any configurations made in Expert Mode will be lost as soon as Expert Mode is disabled.

1. To access Expert Mode, navigate to **MANAGEMENT > NTP Setup**.
2. Enable the switch for Expert Mode in the panel **NTP Services**.
3. Once it is enabled, click **NTP Anycast** in the **Actions Panel**. The **Expert mode** window will appear, with a separate tab for each of the three configuration files.
4. To enable OSPF IPv4 Anycast, check Enable under the **OSPF** tab. To enable OSPF IPv6 Anycast, check Enable under the **OSPF6** tab. To enable BGP Anycast, check Enable under the **BGP** tab. Then click Submit.

When the **NTP Anycast Expert Mode** window is opened, the files displayed are the configuration files in their current states. If no configuration was done outside of Expert Mode, these will be the factory default files. If Anycast configuration was already done from the Web UI, you will be able to edit the existing Anycast setup.

When editing `zebra.conf` in expert mode, you should ensure that the first line under an interface line is an `ip address` line declaring an IPv4 address (if there is one for the interface), and that the next line is an `ipv6 address` line declaring an IPv6 address (if there is one for the interface). No other lines or variations in spacing should be inserted before or between these lines. No editing restrictions exist on `ospfd.conf` or `ospf6d.conf` files.

Example `zebra.conf` file with both IPv4, and IPv6 configured on the same port:

(Interface eth0 line, followed by IPv4 line and then IPv6 line)

```
*******************************************************
!
interface eth0
ip address 10.2.100.157/16
ipv6 address 2000:10:2::157/64
!
interface lo
ip address 10.10.14.1/32
ipv6 address 2000:10:10::1/64
*******************************************************
```

Example `zebra.conf` file with IPv4, and IPv6 configured on different ports:

(Interface eth0 line, followed by only IPv4 line, because no IPv6 address is configured on that port. Interface eth1 line, followed by only IPv6 line, because no IPv4 address is configured on that port)

```
*******************************************************
```

```
!
interface eth0
ip address 10.2.100.157/16
interface eth1
ipv6 address 2000:10:2::157/64
!
interface lo
ip address 10.10.14.1/32
ipv6 address 2000:10:10::1/64
*******************************************************
```

Example `zebra.conf` file showing the default file with no addresses configured:

(Interface eth0 line, with no lines following it because no addresses are configured on the port)

```
*******************************************************
!
interface eth0
!
interface lo
*******************************************************
```

Example `ospfd.conf` file:

```
*******************************************************!
router ospf
ospf router-id 10.2.100.157
network 10.2.0.0/16 area 0.0.0.0
redistribute connected
distribute-list default out connected
!
access-list default permit 10.10.14.1/32
access-list default deny any
*******************************************************
```

Example `ospf6d.conf` file:

```
*******************************************************
!
```

```
interface eth0
!
router ospf6
router-id 10.2.100.157
interface eth0 area 0.0.0.0
redistribute connected
!
******************************************************
```

Example `bgpd.conf` file:

```
******************************************************!
router bgp 12
bgp router-id 172.17.1.12
network 172.17.0.0/16
neighbor 172.17.1.1 remote-as 3
!
redistribute connected
******************************************************
```

3.3.6.6 Testing NTP over Anycast

Note: A detailed Anycast test procedure is available from Spectracom upon request. Please contact techpubs@spectracom.com.

3.3.7 NTP Expert Mode

Advanced NTP configuration is possible via the NTP Expert Mode, which allows users to write directly into the `NTP.conf` file (the syntax is similar to the one used with CISCO routers).

Caution: NTP Expert Mode should only be utilized by advanced users, as incorrectly altering the `NTP.conf` file can cause NTP to stop working (if NTP is configured as an input reference, SecureSync could lose synchronization).

To access NTP Expert Mode, navigate to **MANAGEMENT** > **NTP Setup**. The switch for the NTP Expert Mode is in the panel **NTP Services**.

Caution: Any configurations made in NTP Expert Mode will be lost as soon as NTP Expert Mode is disabled.

NTP utilizes the `NTP.conf` file for its configuration. Normally, configuration of the `NTP.conf` file is indirectly performed by a user via the supplied configuration pages of the SecureSync Web UI. However, it may be desired in certain circumstances to edit this file directly, instead of using the web-based setup screens. When Expert Mode is enabled, the user has direct access to the `NTP.conf` file.

Caution: Spectracom Tech Support does not support the editing of the NTP configuration files while in the Expert Mode. For additional information on editing the `NTP.conf` file, please refer to http://www.ntp.org/.

Note: IMPORTANT: If an undesirable change is made to the `NTP.conf` file that affects the NTP operation, the `NTP.conf` file can be manually changed back as long as the previous configuration was known.

The `NTP.conf` file can be reset back to the factory default values by either using the procedure to restore all of the SecureSync factory default settings (see "Restoring the Default NTP Configuration" on page 121) or editing the file back to the original configuration as shown in the factory default configuration below.

Caution: If changes are made to the `NTP.conf` file while in the Expert mode, Expert mode should remain enabled from that point forward. Disabling Expert mode after changes being made to this file may result in loss of this configuration information.

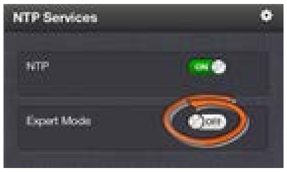
Factory default `NTP.conf` file:

```
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
peer 10.10.128.35 minpoll 3 maxpoll 3 autokey
keysdir /etc/ntp/keys/
crypto pw admin123 randfile /dev/urandom
driftfile /etc/ntp/ntp.drift
logfile /home/spectracom/log/ntp.log
statsdir /home/spectracom/log/ntpstats/
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable
```

Prior to Expert mode being enabled, the **Network/NTP Setup** page will contain various tabs for configuring different options of the NTP Service. To prevent inadvertent changes from being made to a user-edited NTP.conf file via the web pages, these NTP configuration tabs are removed from the web browser view as long as the Expert mode remains enabled (only the **Expert Mode** tab is visible in Expert Mode; all other tabs will no longer be present). Disabling the Expert mode restores these tabs to the Edit NTP Services window.

To enable the Expert Mode to edit the `NTP.conf` file directly:

1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. In the **NTP Services** panel locate the **Expert Mode** switch.



NTP Services

NTP ON

Expert Mode OFF

When enabled, the NTP Service operates in Unicast mode. In Unicast mode, the NTP Service responds to NTP requests only. The NTP Service supports a broadcast mode in which it sends a NTP time packet to the network broadcast address.

3. Click the **Expert Mode** switch.
4. Click **OK** in the dialogue box that displays.
5. Click the GEAR icon.
6. In the **Edit NTP Services** window, edit the file as desired in the text box under the **Expert Mode** tab.
7. Click the Submit button to save any changes that were made.
8. First disable and then re-enable the NTP service using the **NTP ON/OFF** switch in the **NTP Services** panel. SecureSyncwill now use the new NTP configuration per the manually edited file.

Caution: Any configurations made in NTP Expert Mode will be lost as soon as NTP Expert Mode is disabled.

3.3.8 Spectracom Technical Support for NTP

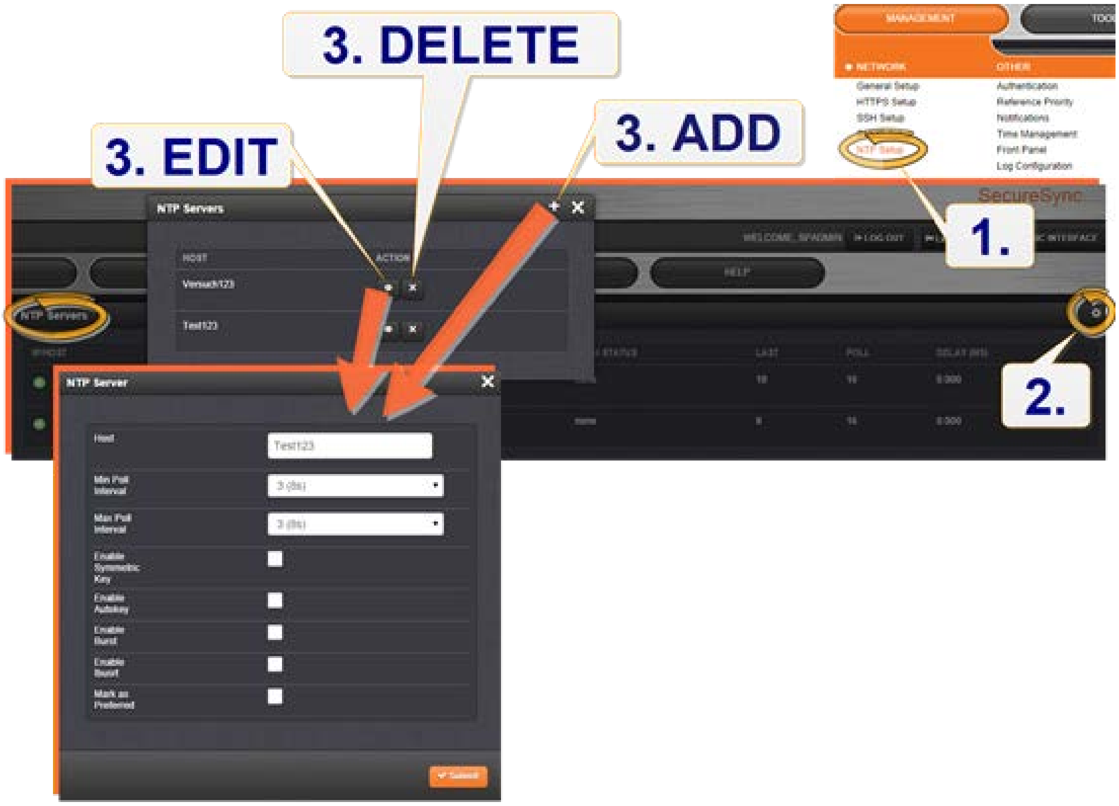
Spectracom does not provide technical assistance for configuring and installing NTP on Unix-based applications. Please refer to www.ntp.org for NTP information and FAQs. Another helpful source is the Internet newsgroup at news://comp.protocols.time.ntp.

Spectracom can provide support for Microsoft® Windows-based time synchronization. See spectracom.com for additional information, or contact Spectracom Technical Support.

Spectracom also offers an alternate Windows NTP client software package called **PresenTense**. **PresenTense** software provides many features and capabilities not included with the limited functionality of the Windows W32Time program, including alert notification and audit trails for the PC’s time.

For more information on **PresenTense**, please visit spectracom.com or contact your local Spectracom Sales Representative.

3.3.9 NTP Servers: Adding, Configuring, Deleting



NTP Servers

HOST	ACTION
Versuch123	⚙ ✕
Test123	⚙ ✕

NTP Server

Host: Test123
Min Poll Interval: 3 (8s)
Max Poll Interval: 3 (8s)
Enable Symmetric Key: □
Enable Autokey: □
Enable Burst: □
Enable Iburst: □
Mark as Preferred: □

1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**.
2. The **NTP Setup** screen appears. The **NTP Servers** panel displays a list of recognized NTP servers. Click the GEAR icon in the upper right-hand corner of the **NTP Servers** panel.
3. The **NTP Servers** pop-up window opens.

> **Note:** Should the list be empty, no servers have been added yet. In the event that added servers are not displayed in the NTP Setup screen/NTP Servers panel, they could not be resolved. Verify the IP address.
>
> System servers cannot be edited or deleted.

» To ADD a new server, click the PLUS icon in the upper right-hand corner, and proceed to the next step.

» To EDIT an existing server, click the corresponding ACTION GEAR button, or double-click anywhere on the row, and proceed to the next step.

» To DELETE an existing server, click the corresponging ACTION X-button, or double-click anywhere on the row, then confirm by clicking OK.

4. The NTP Server Edit window displays. Enter the required information into the fields:
   - **Host**–Enter is the IP address for the server to be used as host.
   - **Enable Symmetric Key**–Click to enable Symmetric Key, and then select an option from the drop down that displays.
   - **Max Poll Interval**–Select a value from the drop down.
   - **Min Poll Interval**–Select a value from the drop down.

     Note: Before you can choose an option in the Key field, you must first set up symmetric keys through the Actions Panel. See "Symmetric Keys (MD5 Authentication)" on page 101. Conversely, you may check the Autokey box below the Key field.

   - **Enable Autokey**–Click here if you want to use Autokey with this server. See "NTP Autokey" on page 100.

     Note: When you configure NTP Autokey, you must first disable the NTP service in the NTP Services panel, and then re-enable it after Autokey configuration is completed.

   - **Enable Burst**–This tells NTP to send a burst to the remote server when the server is reachable.
   - **Enable Iburst**–This tells NTP to send a burst to the remote server when the server is not reachable.
   - **Mark as Preferred**–Click here to make this server the preferred server. See "NTP Timing System: Reference Selection and Preference" on page 98.

     Note: It is not normally recommended to select more than one NTP Server in the NTP Servers table as being preferred. Typically, only one NTP server should be selected as preferred.

5. Click the **Submit** button at the bottom of the window, or press Enter.

3.3.10 NTP Peers: Adding, Configuring, Deleting

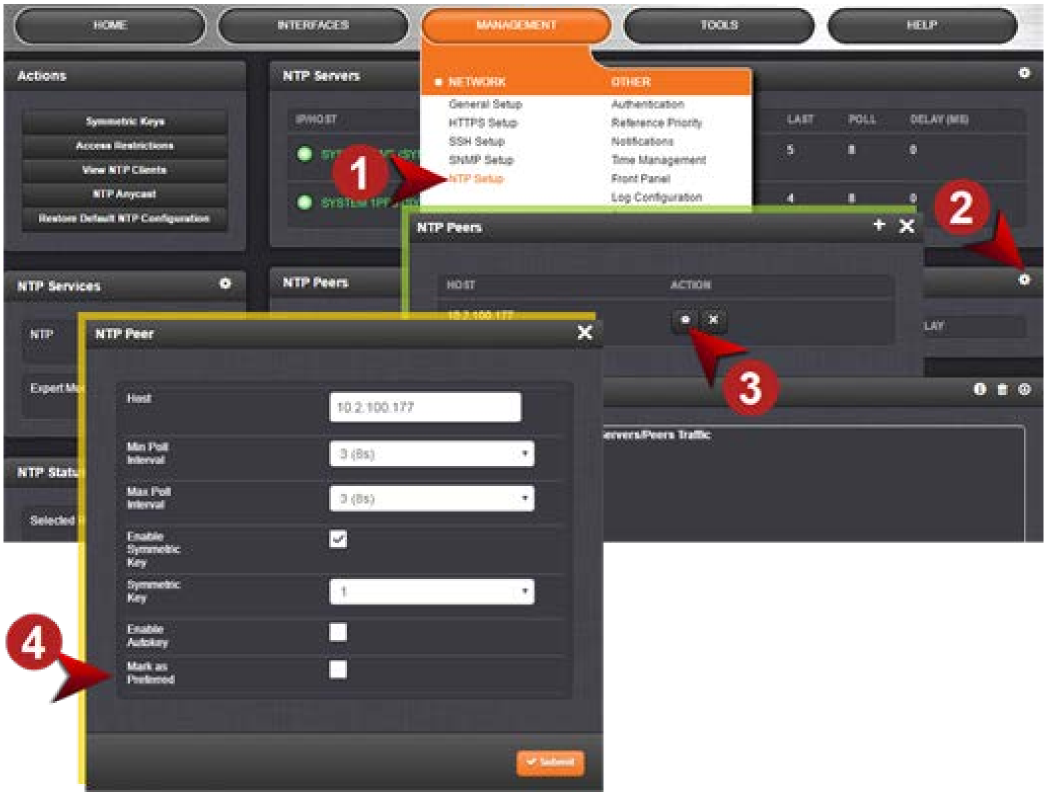
To add, edit, or delete an NTP Peer:

1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**.
2. The **NTP Setup** screen appears. The **NTP Peers** panel displays a list of recognized NTP peers.

> **Note:** Should the list be empty, no servers have been added yet. In the event that added peers are not displayed, they could not be resolved. Verify the IP address

- To EDIT the settings of an NTP Peer, click the GEAR button next to it, and proceed to Step 3 below.
- To ADD a new NTP Peer, click the PLUS icon in the top right corner of the **NTP Peers** panel.
- To DELETE an existing NTP Peer, click the X button next to it.

3. The **NTP Peers** edit window opens:



Host: 10.2.100.177
Min Poll Interval: 3 (8s)
Max Poll Interval: 3 (8s)
Enable Symmetric Key: ☑
Symmetric Key: 1
Enable Autokey: □
Mark as Preferred: □

Enter the required information in the fields:

- **Host**: Enter is the IP address for the server to be used as host.
- **Min Poll Interval**: Select a value from the drop down.
- **Max Poll Interval**: Select a value from the drop down.
- **Enable Symmetric Key**: Click the check box to enable/disable Symmetric Key. See also: "Symmetric Keys (MD5 Authentication)" on page 101.

> **Note:** Before you can edit the Key field, you must set up Symmetric Keys through the Actions Panel. See "Configuring NTP Symmetric Keys (MD5 Authentication)" below. Conversely, you may check the Autokey box below the Key field.

- **Enable Autokey**: Click the check box to enable/disable Autokey. See "NTP Autokey" on page 100 for more information on Autokey.

> **Note:** When you configure NTP Autokey, you must first disable the NTP service in the NTP Services panel, then re-enable it after Autokey configuration is completed.

- **Mark as Preferred**: Check this box to to prefer this NTP Peer over other NTP Peers. This will result in SecureSync synchronizing more frequently with this Peer.
  Please note that it is not advisable to mark more than one NTP Peer as Preferred, even though SecureSync will not prevent you from doing so.

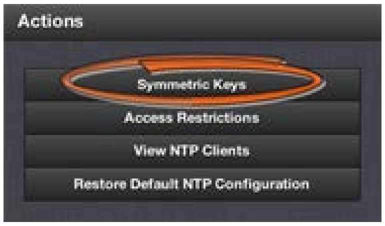
  For additional information on NTP Preferences, see "NTP Timing System: Reference Selection and Preference" on page 98.

3.3.11 Configuring NTP Symmetric Keys (MD5 Authentication)

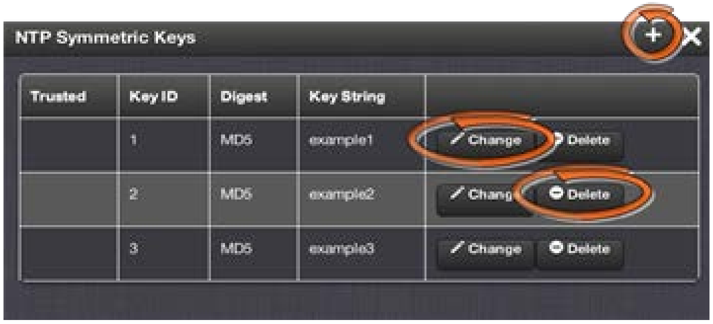
Symmetric Keys are an encryption means that NTP may utilize for authentication purposes. See also: "Symmetric Keys (MD5 Authentication)" on page 101.

To create, edit, or delete Symmetric Keys:

1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**.
2. In the **Actions** panel, click the **Symmetric Keys** button:



3. The **NTP Symmetric Keys** window will display:

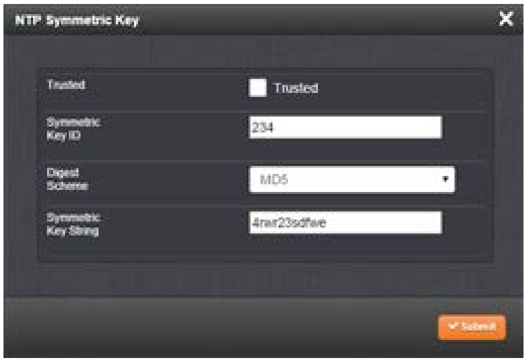


NTP Symmetric Keys

Trusted	Key ID	Digest	Key String	
	1	MD5	example1	Change Delete
	2	MD5	example2	Change Delete
	3	MD5	example3	Change Delete

- To CREATE a **Symmetric Key**, click the PLUS icon in the top-right corner, and proceed to Step 4.
- To EDIT an existing key pair, click the corresponding Change button, and proceed to Step 4.
- To DELETE a key pair, click the corresponding Delete button, and click **OK** in the dialog box to confirm and complete the procedure.

4. The **NTP Symmetric Key** window will display:



NTP Symmetric Key

Trusted	□ Trusted
Symmetric Key ID	234
Digest Scheme	MD5
Symmetric Key String	4rwr23sdfwe

Fill in, or edit the fields:

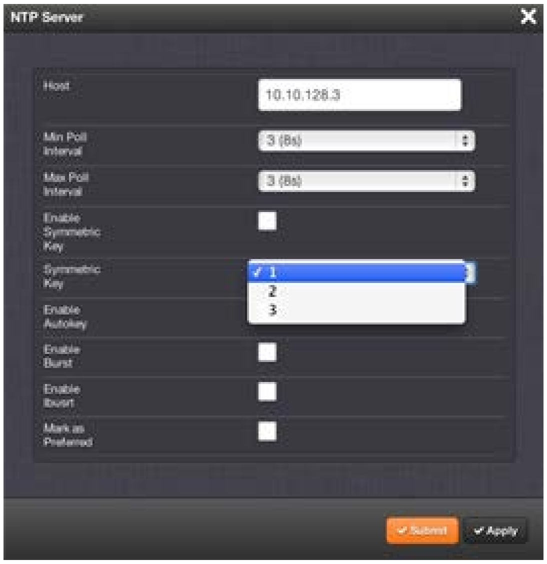
- **Trusted** (checkbox)–Check this box to use MD5 authentication with trusted key ID.

> **Note:** To use the MD5 authentication with trusted key ID, both the NTP client and the SecureSync must contain the same key ID/key string pair and the client must be set to use one of these MD5 pairs.

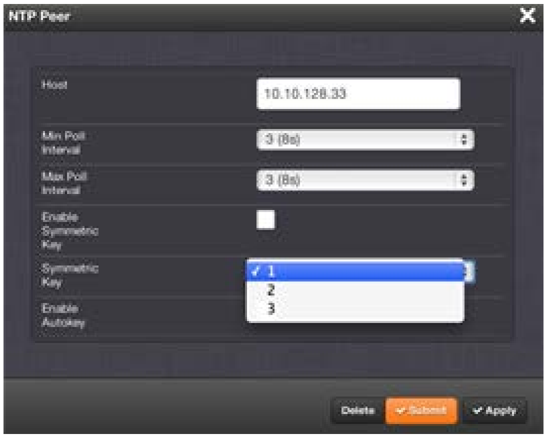
- **Key ID**–The key ID must be a number between 1 and 65532.
- **Digest Scheme**–Choose one of the options from the drop-down list. The available options are:

    - MD5 (the default)
    - SHA1
    - SHA
    - MDC2
    - MDC2
    - RIPEMD160
    - MD4
- **Key Str**–The key string must be readable ASCII and between 1 and 16 characters long.

5. Click the **Submit** button: The changes will be reflected in the table of the **NTP Symmetric Keys** window, which is displayed after clicking the **Submit** button.
6. The key(s) you have set up will now appear as options in the **Symmetric Key** field in both the **NTP Server** screen, and the **NTP Peer** screen.



Host	10.10.128.3
Min Poll Interval	3 (8s)
Max Poll Interval	3 (8s)
Enable Symmetric Key	□
Symmetric Key	✓ 1 2 3
Enable Autokey	
Enable Burst	□
Enable Iburst	□
Mark as Preferred	□



Host	10.10.128.33
Min Poll Interval	3 (8s)
Max Poll Interval	3 (8s)
Enable Symmetric Key	□
Symmetric Key	✓ 1 2 3
Enable Autokey	

Duplicate key IDs are not permitted. NTP requests received by that do not contain an authenticator containing a valid Key ID and MD5 message digest pair will be responded to, but no authentication will be performed. An NTP request with valid authenticators results in a valid NTP response with its own valid authenticator using the same Key ID provided in the NTP request.

The user may define the trusted Symmetric Keys that must be entered on both SecureSync, and any network client with which SecureSync is to communicate. The maximum number of Key-ID/Key String pairs is 15. Only those keys for which the “Trusted” box has been checked will appear in the dropdown menus on the **NTP References** screen.

Note: In order for NTP configuration changes to take effect, NTP should be disabled and then enabled after any configurations changes have been made.

NTP can be enabled and disabled through the NTP Services panel on the MANAGEMENT/NETWORK/NTP Setup page. See "Enabling and Disabling NTP" on page 122.

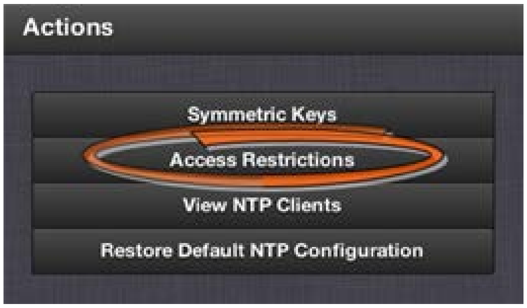
Changes made will take effect and NTP operation will be restored shortly after this operation is performed.

3.3.12 Configuring NTP Access Restrictions

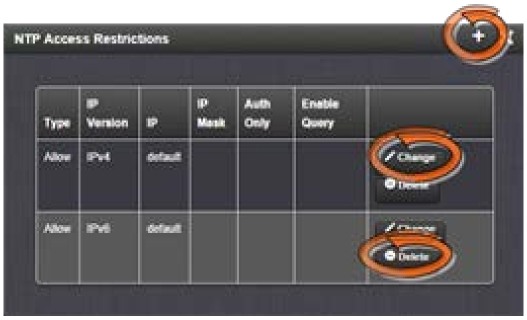
Next to encrypted authentication by means of Symmetric Keys, NTP supports a list-based means of access restriction, the use of which is also recommended to prevent fraudulent or inadvertent manipulation of a time server.

To configure NTP Access Restrictions:

1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. In the **Actions** panel, click the **Access Restrictions** button.



3. The **NTP Access Restrictions** Status window will display:

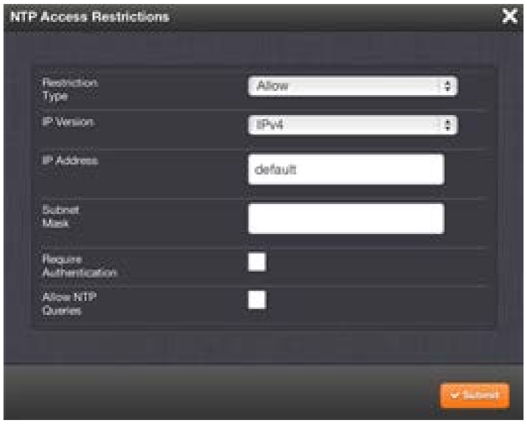


NTP Access Restrictions

Type	IP Version	IP	IP Mask	Auth Only	Enable Query	
Allow	IPv4	default				Change Delete
Allow	IPv6	default				Change Delete

- » To ADD or EDIT an access restriction, click the PLUS icon or the Change button, respectively, and proceed to the next step below.
- » To DELETE an access restriction, click the corresponding Delete button, and confirm by clicking OK.

4. The NTP Access Restrictions pop-up window will display:



NTP Access Restrictions

Restriction Type	Allow
IP Version	IPv4
IP Address	default
Subnet Mask	
Require Authentication	☐
Allow NTP Queries	☐

- » Fill in the fields:
  - » **Restriction Type**–Choose either Allow or Deny.
    If you select “Deny”, the configured portion of the network will not have NTP access to SecureSync, but the rest of the network will have access to SecureSync. If you select “allow”, the configured portion of the network will have NTP access to SecureSync, but the rest of the network will not have access to SecureSync.
  - » **IP Version**–Choose IPv4 or IPv6
  - » **IP Address**–Enter the appropriate hostname.
  - » **Subnet Mask**–Enter the appropriate IP mask.

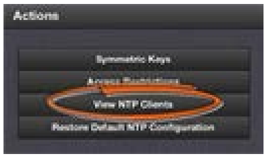
- **Require Authentication** (checkbox)–Check this box if you want the additional security of authorized access. SecureSync to accept only authenticated requests (MD5 or Autokey) from this user or network segment.
- **Allow NTP Queries** (checkbox)–Check this box if you would like to allow NTPDC or NTPQ client access. NTPDC and NTPQ are utilities for controlling NTP servers and gathering performance data from NTP servers. Modification or control of a SecureSync's NTP service through NTPDC or NTPQ is not supported.

5. Click the **Submit** button.

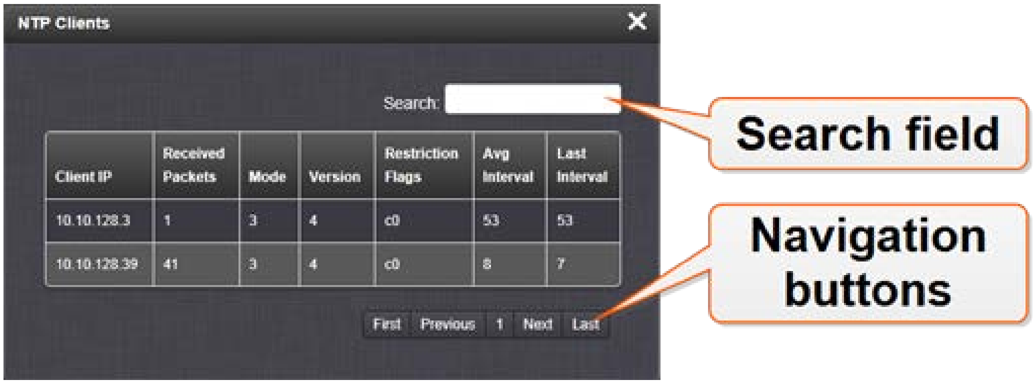
3.3.13 Viewing NTP Clients

To view the NTP clients being served by SecureSync:

1. Navigate to **MANAGEMENT> NETWORK: NTP Setup**.
2. In the **NTP Actions** panel, click **View NTP Clients**.



3. The **NTP Clients** window will display, showing a table of the clients that are synchronizing to SecureSync via NTP:



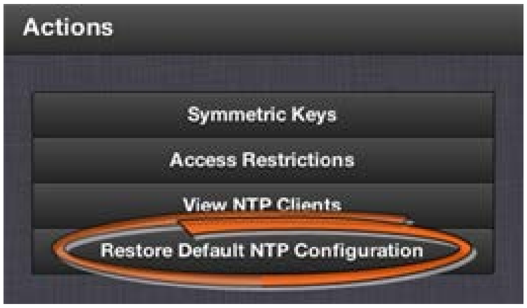
Client IP	Received Packets	Mode	Version	Restriction Flags	Avg Interval	Last Interval
10.10.128.3	1	3	4	c0	53	53
10.10.128.39	41	3	4	c0	8	7

- You can search any of the fields for specific information in the Search field at the top of the window.
- A limit of 10 entries will appear on the screen at any one time. If you have more than 10 clients, you can move through the table using the **First**, **Previous**, **Next** and **Last** navigation buttons at the bottom of the screen.

3.3.14 Restoring the Default NTP Configuration

To restore SecureSync to the default NTP configuration:

1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**.
2. In the **NTP Actions** panel, click **Restore Default NTP Configuration**.



3. In the dialog window that displays, click **OK**.

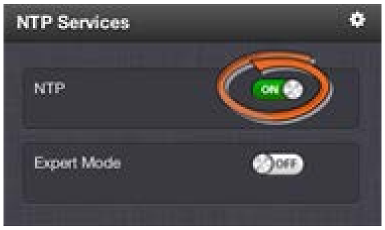
3.3.15 Enabling and Disabling NTP

After changing any of the NTP configurations, the NTP daemon needs to be disabled and then enabled for the changes to take effect.

Changes made to NTP configurations will also take effect after SecureSync is either rebooted or power cycled.

To enable or disable NTP:

1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**.
2. In the **NTP Services** panel, select the ON/OFF switch.



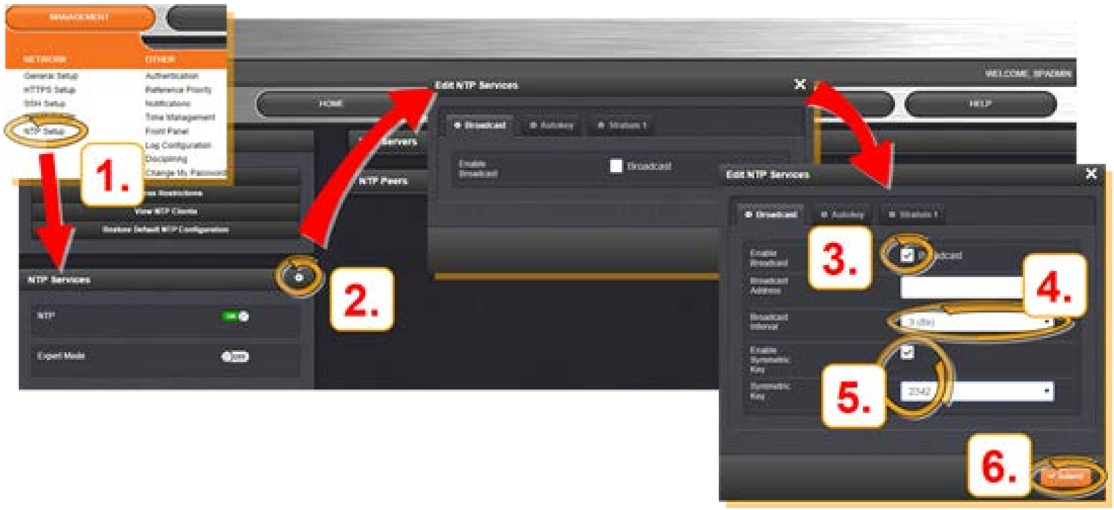
3. A 10-second pop-up notification window will confirm the status change. Clicking the X-button in the notification window will close it before the 10 seconds elapsed.

3.3.16 Enabling/Disabling NTP Broadcasting

SecureSync allows NTP service to be configured to broadcast the NTP time to the network's broadcast address at scheduled intervals. To enable NTP broadcasting:

Note: The NTP Broadcast mode is intended for one or a few servers and many clients.

As most NTP clients do not normally just “listen” for NTP data on the broadcast address (because NTP broadcast isn’t as accurate as requesting time), this capability is seldom required and rarely used.



1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**.
2. On the **NTP Services** panel, click the GEAR icon.
3. The **Edit NTP Services** window will display. Check the **Broadcast** box.
4. Select a **Broadcast Interval**. When NTP broadcasting is selected, in addition to still responding to NTP time requests sent from network appliances, SecureSync will also send unsolicited NTP time packets to the local broadcast address at a user-specified interval.
5. To utilize **MD5 Authentication**, select a **Symmetric Key** (see "Symmetric Keys (MD5 Authentication)" on page 101; to create symmetric keys, see "Configuring NTP Symmetric Keys (MD5 Authentication)" on page 116).
6. Click the **Submit** button.

If you want to disable NTP broadcasting, click the **Broadcast** box to remove the check, and then click the **Submit** button.

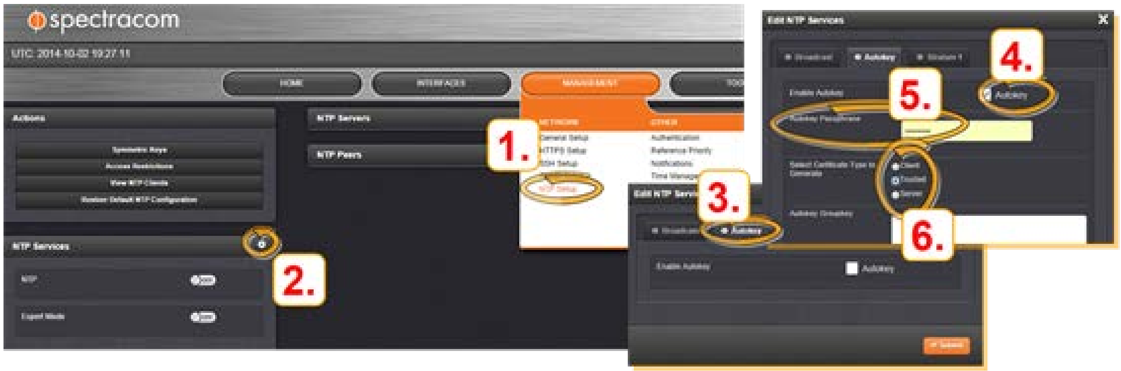
3.3.17 Configuring NTP Autokey

Note: Note that NTP Autokey is currently not supported; for more information, see http://bugs.ntp.org/show_bug.cgi?id=3005.

To configure NTP Autokey:

Note: Changing an Autokey will not take effect until the NTP Service is Disabled and then Enabled (or until SecureSync is rebooted/power cycled).

The NTP service can be stopped and started from the MANAGMENT/NTP Setup in the NTP Services panel.



1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**.
2. Click the GEAR icon in the top-right corner of the **NTP Services** panel.
3. The **Edit NTP Services** window will display
4. Click the **Autokey** tab.
5. Check the **Autokey** box.
6. Fill in the **Passphrase** field by creating a passphrase (for a **Trusted** server–see **Certificate Type** below), or by using the existing passphrase of your trusted server (for **Server** and **Client** certificates).
7. Select the **Certificate Type** for your server, by clicking the appropriate radio button for **Server**, **Client**, or **Trusted**.

TRUSTED Server:

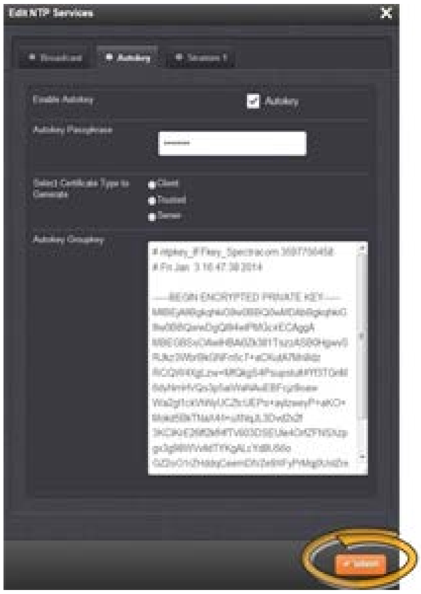
Before a server can be designated Client or Server status, one server must be designated as Trusted. When designating a server as Trusted:

1. Choose the Trusted radio button.

2. Click the Submit button.

A Groupkey is then generated for the network. This Groupkey will be pasted into the

Groupkey box to designate another server on the network as Client or Server.



```
# ntpkey_IFFkey_Spectracom.3597750458
# Fri Jan 3 16:47:38 2014

-----BEGIN ENCRYPTED PRIVATE KEY-----
[illegible]
```

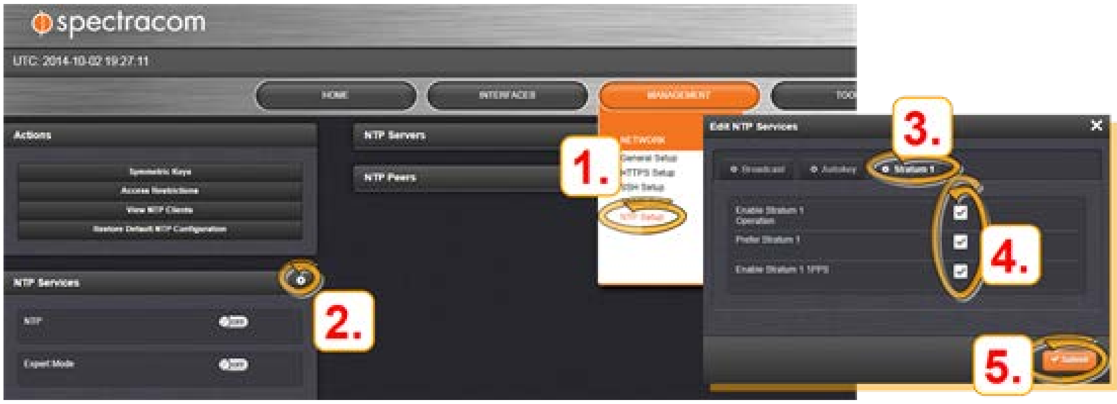
8. To designate a SecureSync as **Trusted**, click the **Submit** button. This will generate a new **Groupkey**.
9. To designate a SecureSync as a **Client** or a **Server**, paste the generated **Groupkey** into the **Groupkey** box, and click the **Submit** button.

3.3.18 NTP Stratum Configuration

3.3.18.1 Configuring Stratum-1 Status

To designate SecureSync's Stratum-1 status:

> **Note:** Configuration changes made to SecureSync's NTP configurations do not take effect until the NTP Service is Disabled and then Enabled (or until SecureSync is rebooted/power cycled). The NTP service can be stopped and started from the MANAGMENT/NTP Setup in the NTP Services panel.



1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**.
2. Click the GEAR icon in the **NTP Services** panel.
3. The **Edit NTP Services** window will display. Click the **Stratum 1** tab.
4. Choose among three options:
    - Enable Stratum 1 Operation
    - Prefer Stratum 1
    - Enable Stratum 1 1PPS.

   You may choose combination of 1, 2 or three settings. See "NTP Timing System: Reference Selection and Preference" on page 98 for information on timing systems in NTP networks.
5. Click the **Submit** button to confirm your setup.

3.3.18.2 Configuring a Stratum-1 Server as Trusted Host

To configure an NTP Stratum-1 Server as Trusted Host with IFF Group/Client key:

1. Define the Hostname of all NTP servers before proceeding. See "NTP Servers: Adding, Configuring, Deleting" on page 113.
2. Disable NTP.
    - Ensure the time is accurate to a few seconds. Use NTP or manually set the clocks to set the system time.
3. Verify this SecureSync is, in fact, NTP Stratum1, and its Time, and 1PPS synchronization to GNSS are valid.
4. Under the **Autokey** tab of the **Edit NTP Services** window:
    - **Enable Autokey**–Check the box.
    - **Autokey Passphrase**–Enter your Group members NTP Autokey password.
    - **Select Certificate Type to Generate**–Do NOT enable **Client**.

- Select **Trusted**.
- Click **Submit**.

5. Observe the **IFF Group/Client Key** appearing.
   - This is the common **IFF Group/Client Key**. This key is shared between all Group members using this NTP Servers passphrase for ALL group members.
6. Configure NTP as requiring authentication.
7. Enable NTP in the **NTP Services** panel.
8. Verify that NTP reaches occur, and that NTP eventually reaches Stratum 1.

3.3.18.3 Creating a Stratum-1 Group Member Server

To configure an NTP Stratum-1 Server, which is a Group Member, using a Client key:

1. Define the Hostname, making sure it is not the same as the trusted root server. See "NTP Servers: Adding, Configuring, Deleting" on page 113.
2. Disable NTP if enabled.
3. Manually set the time or use NTP to set the system time.
4. Under the **Autokey** tab of the **Edit NTP Services** window, enable:
   - **Enable Autokey**–Check the box.
   - **Autokey Passphrase**–Enter your Group members NTP Autokey password.
   - **Select Certificate Type to Generate**–Do NOT enable Client
5. Using the NTP Server containing the IFF Group/Common Key generate a Client Key using this NTP Server’s passphrase.
6. Cut and paste the Client Key into the **Autokey Groupkey** text box.
7. For all NTP Stratum-2 servers and higher stratum numbers, disable the following items under the **Stratum-1** tab in the **Edit NTP Services** window:
   - Prefer Stratum 1.
   - Enable Stratum-1 1PPS.
8. In the **NTP Servers** panel of the main window, add an NTP server and enable the **Autokey** option box. See "NTP Servers: Adding, Configuring, Deleting" on page 113.
9. Enable NTP in the **NTP Services** panel.
10. Wait for NTP to synchronize to the NTP References provided.

3.3.18.4 Creating a Stratum-1 Client Only Server

To create an NTP Stratum-1 'Client Only' Server with a Client key:

1. Define the Hostname, making sure that it is different from its trusted group server. See "NTP Servers: Adding, Configuring, Deleting" on page 113.
2. Disable NTP if enabled.
3. Manually set the time or use NTP to set the system time.
4. Under the Autokey tab of the **Edit NTP Services** window, enable:
   - **Enable Autokey**–Check the box.
   - **Autokey Passphrase**–Enter your Group members NTP Autokey password.
   - **Select Certificate Type to Generate**–Select **Client** to enable Client only.
5. Using the NTP Server containing the IFF Group/Client Key, copy the Group/Client key.
6. Paste this Group/Client key into the **Autokey Groupkey** text box.
7. For all NTP Stratum-2 servers and higher stratum numbers, under the **Stratum-1** tab in the **Edit NTP Services** window configure the NTP Stratum-1 references:
   - Disable Enable Stratum 1 Operation.
   - Disable Enable Stratum 1 1PPS.
8. In the **NTP Servers** panel of the main window, add an NTP server and enable the **Autokey** option box. See "NTP Servers: Adding, Configuring, Deleting" on page 113.
9. Wait for NTP to synchronize to the NTP References provided.

3.4 Configuring TimeKeeper

To **learn about TimeKeeper**, and what it can do for you, see "TimeKeeper™" on page 236.

To **activate TimeKeeper**, see "Applying a License File" on page 280.

To **turn TimeKeeper ON/OFF**, see "En-/Disabling TimeKeeper" on page 237.

3.4.1 Has TimeKeeper been activated?

FSMLabs' TimeKeeper module comes pre-installed with every SecureSync System Software Versions 5.2.0 or higher.

The TimeKeeper license must be activated by applying a License File, which can be purchased from Spectracom, either at the time when a SecureSync unit is ordered, or later. For more information, see "Applying a License File" on page 280.

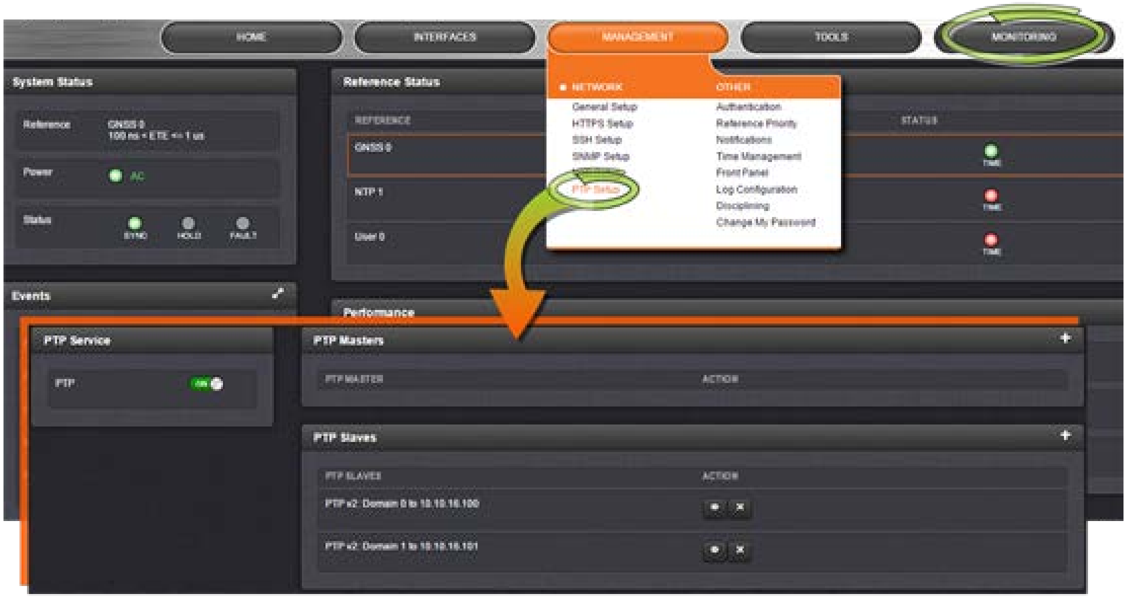
To find out if the Timekeeper license on your SecureSync has been activated:

1. In the Web UI, Select **TOOLS** > **Upgrade/Backup**.
2. In the **System Configuration** Panel, check the bottom row, under **Option**:

a. OPT-TKL TimeKeeper means that the TimeKeeper license has been activated, i.e. the license key has been purchased and applied.

b. If there is no entry under **Option**, the TimeKeeper license has not been activated.

If a TimeKeeper License is installed, you will also notice that the right button in the Main Navigation bar is labeled MONITORING (not HELP), and under **MANAGEMENT** > **NETWORK**, there is a **PTP Setup** option available:



Next, make sure that TimeKeeper is turned ON—see "En-/Disabling TimeKeeper" on page 237.

3.4.2 Configuring a TimeKeeper PTP Master

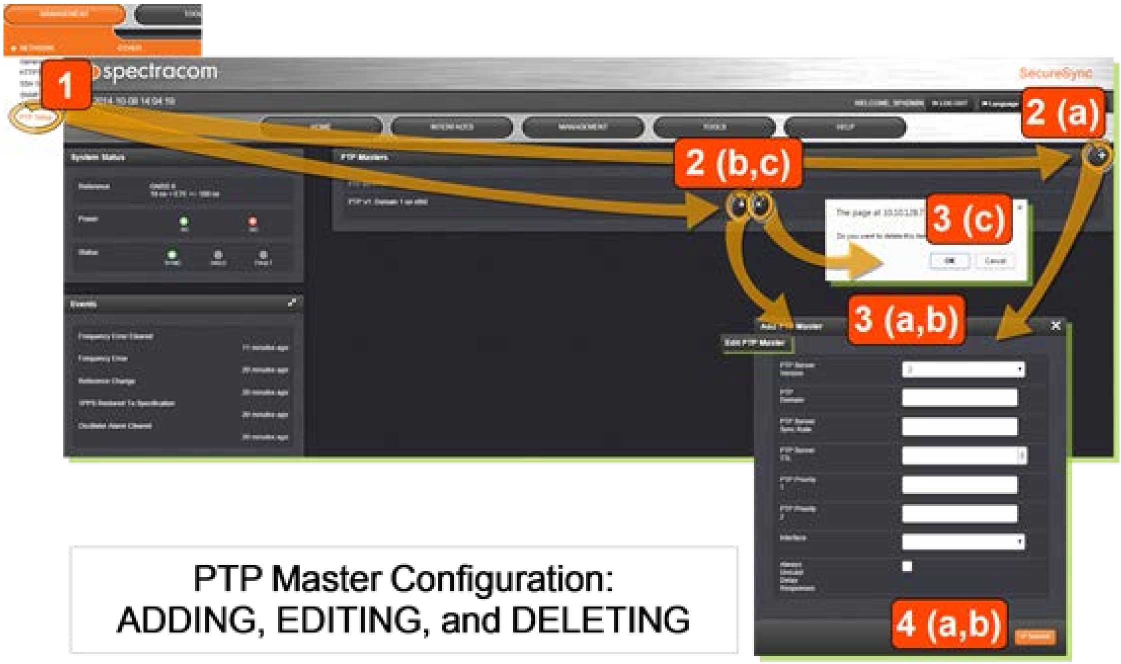
TimeKeeper is configured in the SecureSync Web UI, under **MANAGEMENT** > **PTP Setup**.

When setting up a PTP Master via TimeKeeper, the configured SecureSync interface (e.g., ETH0), detectable to the PTP network via its IP address, will send out synchronization packets under the PTP protocol.

You can setup several PTP Masters, e.g. for different interfaces (if so equipped), or to serve different domains, or one for each PTP Version.

The following explains how to configure a PTP Master. Three procedures are described below:

- Procedure a): **ADDING a PTP Master**
- Procedure b): **EDITING a PTP Master**
- Procedure c): **DELETING a PTP Master**



PTP Master Configuration:
ADDING, EDITING, and DELETING

Procedure a): ADDING a PTP Master

To add and configure a new PTP Master:

1. Navigate to the **PTP Setup** screen via the **MANAGEMENT** > **NETWORK** > **PTP Setup** menu.
2. In the **PTP Masters** panel, click the PLUS icon in the top right corner.
3. The **Add PTP Master** pop-up window displays. Fill in the applicable parameter values:

> **Note:** Not all fields need to be populated: Only the Server Version, the rest can remain blank. The new Master will output PTP data via every available ETH output.

- PTP Server Version: Ver.1 or Ver.2
- PTP Domain: Determines which domain the PTP server will broadcast on. [Range: 0-255] Default suggested domain for PTP1: 0.
- PTP Server Sync Rate: The rate at which to broadcast PTP synchronization messages (in seconds).
  - EXAMPLE: “1” will cause SecureSync to broadcast a synchronization message every second, whereas “2” will send out messages in 0.5-second intervals. [Range: 0.5-64] Suggested setting: 1

- PTP Server TTL: This numeric field determine s how long a PTP packet will live, in seconds, when routed ("Time-To-Live") Suggested setting: 1 s
- PTP Priority 1 [2]: The value set in these two fields will be broadcast by the PTP Master with announcement messages [Range: 0-255] Suggested setting: 128
- Interface: The name of the interface for PTP data this PTP Master will use.
  - The interface name must correspond with a Linux network device name. Depending on the configuration of your unit, you can select any of the ports listed in this field.

    Note: Ensure that the selected interface is enabled: Go to MANAGEMENT > Network, and click on the GEAR icon next to the port you want to use. Enable and configure the port in the Edit Ethernet Port Settings window.

- Always Unicast Delay Responses: Check this box if you would like the PTP Master to provide unicast delay responses, no matter if the client provided a unicast or a multicast delay request. When the box is unchecked, the server will respond with the same type of message as the request, that is a multicast response for a multicast request, and a unicast response for a unicast request. Recommended setting: Unchecked

4. Click **Submit**, and wait for the screen to refresh (TimeKeeper will be restarted).

Procedure b): EDITING a PTP Master

To edit the configuration of a PTP Master:

1. Navigate to the **PTP Setup** screen via the **MANAGEMENT** > **NETWORK** > **PTP Setup** menu.
2. In the **PTP Masters** table, click the GEAR button next to the PTP MASTER you wish to edit.
3. The **Edit PTP Master** pop-up window displays. Edit the desired configuration parameter(s). For additional information, see Procedure a): "ADDING a PTP Master" above.
4. Click **Submit**, and wait for the screen to refresh (TimeKeeper will be restarted).

Procedure c): DELETING a PTP Master

To delete a previously created PTP Master:

1. Navigate to the **PTP Setup** screen via the **MANAGEMENT** > **NETWORK** > **PTP Setup** menu.
2. Click the X-button next to the PTP Master you wish to delete.
3. Click **OK** in the pop-up window to confirm the deletion of the PTP Master, and wait for the screen to refresh.

Next, you may want to configure TimeKeeper PTP Slaves, see "Configuring TimeKeeper PTP Slaves" below.

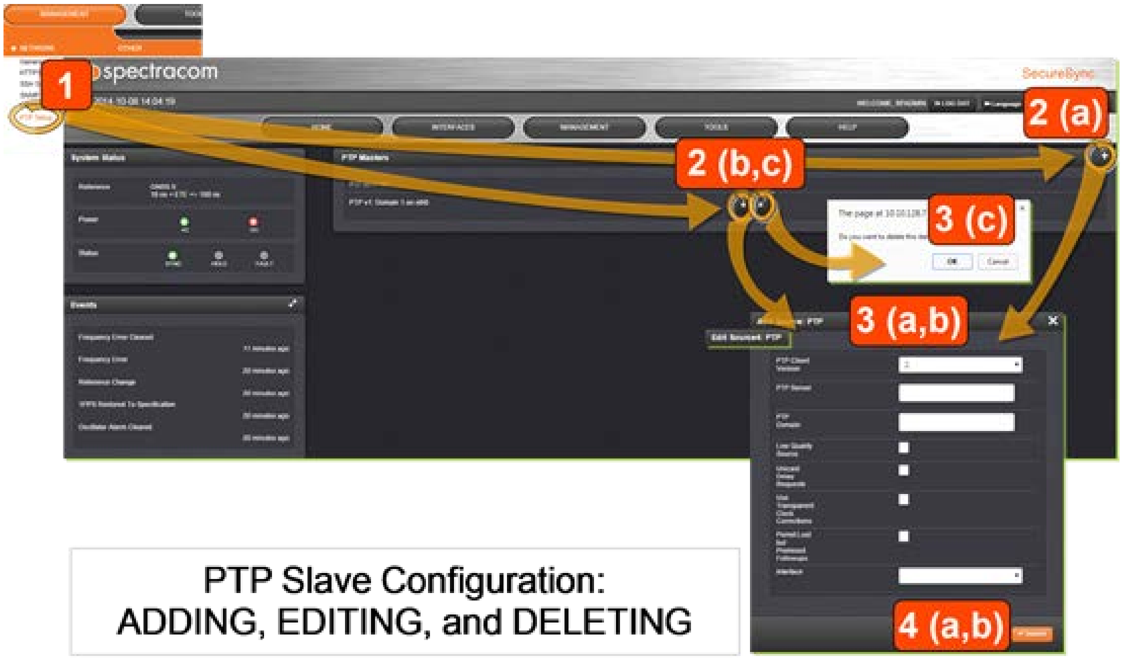
3.4.3 Configuring TimeKeeper PTP Slaves

TimeKeeper is configured in the SecureSync Web UI, under **MANAGEMENT** > **PTP Setup**.

PTP Slaves are used in a network to listen for synchronization packets from PTP Masters, and send out synchronization requests, as well as follow ups. The timing information from PTP masters are used by the system as a synchronization source if NTP is an entry in the reference priority table (it is by default), and no other reference set as a higher priority is available for synchronization. No configuration is required other than setting up PTP Slaves.

To configure a PTP Slave under TimeKeeper, follow the corresponding procedure described below:

- Procedure a): **ADDING a PTP Slave**
- Procedure b): **EDITING a PTP Slave**
- Procedure c): **DELETING a PTP Slave**



PTP Slave Configuration:
ADDING, EDITING, and DELETING

Procedure a): ADDING a PTP Slave

To add and configure a new PTP Slave:

1. Navigate to the **PTP Setup** screen via the **MANAGEMENT** > **NETWORK** > **PTP Setup** menu.
2. In the **PTP Slaves** panel, click the PLUS icon in the top right corner.

3. The **Add Source#** pop-up window displays. Fill in the applicable parameter values:
   - PTP Client Version: Ver.1 or Ver.2
   - PTP Server: The address of the PTP server (this field will be populated by TimeKeeper, if only one server has been configured).
   - PTP Domain: Determines which domain the PTP server will broadcast on. [Range: 0-255; default-suggested domain for PTP1: 0]
   - Low Quality Source: Check this box to improve tracking of low quality sources, such as NTPd. [Default: Checked]
   - Unicast Delay Requests: Enables unicast delay requests back to the server. Check this box if you would like the PTP Master to provide unicast delay responses, no matter if the client provided a unicast or a multicast delay request. When the box is unchecked, the server will respond with the same type of message as the request, that is a multicast response for a multicast request, and a unicast response for a unicast request. [Recommended setting: Unchecked]
   - Use Transparent Clock Corrections: Check to allow the slave to apply the transparent clock correction provided with PTP data. [Default: Checked]
   - Permit Lost but Promised Followups: Check this box to allow missing followup messages to handle certain network issues.
     - **Unchecked** [default]: A PTP grandmaster that promises a followup message must deliver one in order for this slave to use a given time update. (This setting is recommended, since missing followups are a good indication of an issue with PTP delivery or the grandmaster.)
     - **Checked**: A failed followup delivery will not prevent a time update.updated.
   - Interface: The name of the interface for PTP data this PTP Slave will use.
     - The interface name must correspond with a Linux network device name. Depending on the configuration of your unit, you can select any of the ports listed in this field.

       > **Note:** Ensure that the selected interface is enabled: Go to MANAGEMENT > Network, and click on the GEAR icon next to the port you want to use. Enable and configure the port in the Edit Ethernet Port Settings window.

4. Click **Submit**, and wait for the screen to refresh.

Procedure b): EDITING a PTP Slave

To edit the configuration of a PTP Slave:

1. Navigate to the **PTP Setup** screen via the **MANAGEMENT** > **NETWORK** > **PTP Setup** menu.

2. In the **PTP Slaves** table, click the GEAR button next to the PTP SLAVE you wish to edit.
3. The **Edit Source#** pop-up window displays. Edit the desired configuration parameter(s). For additional information, see **Procedure a)**: “ADDING a PTP Slave” above.
4. Click **Submit**, and wait for the screen to refresh.

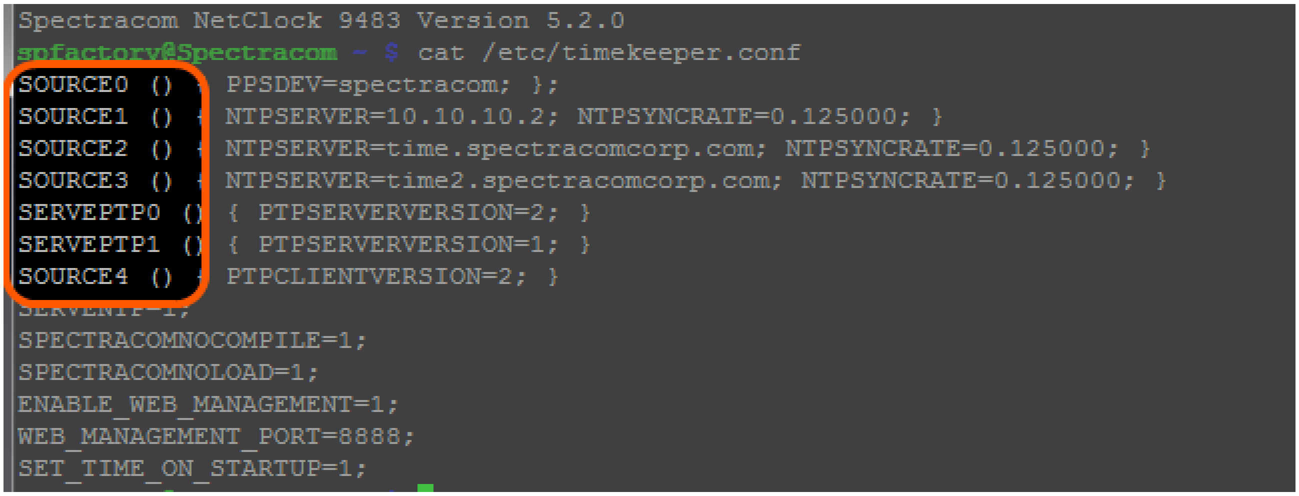
Procedure c): DELETING a PTP Slave

To delete a previously created PTP Slave:

1. Navigate to the **PTP Setup** screen through the **MANAGEMENT** > **NETWORK** > **PTP Setup** menu.
2. Click the X-button next to the PTP Slave you wish to delete.
3. Click **OK** in the pop-up window to confirm the deletion of the PTP Slave, and wait for the screen to refresh.

The Source number in the header of the ADD (EDIT) window:

The Source number shown is a result of TimeKeeper keeping track of time sources. The different sources are ranked in the TimeKeeper configuration file (see illustration below). For more information, see FSMLab's TimeKeeper documentation.



```
Spectracom NetClock 9483 Version 5.2.0
spfactory@Spectracom ~ $ cat /etc/timekeeper.conf
SOURCE0 () { PPSDEV=spectracom; };
SOURCE1 () { NTPSERVER=10.10.10.2; NTPSYNCRATE=0.125000; }
SOURCE2 () { NTPSERVER=time.spectracomcorp.com; NTPSYNCRATE=0.125000; }
SOURCE3 () { NTPSERVER=time2.spectracomcorp.com; NTPSYNCRATE=0.125000; }
SERVEPTP0 () { PTPSERVERVERSION=2; }
SERVEPTP1 () { PTPSERVERVERSION=1; }
SOURCE4 () { PTPCLIENTVERSION=2; }
SERVENTP=1;
SPECTRACOMNOCOMPILE=1;
SPECTRACOMNOLOAD=1;
ENABLE_WEB_MANAGEMENT=1;
WEB_MANAGEMENT_PORT=8888;
SET_TIME_ON_STARTUP=1;
```

3.4.4 Configuring TimeKeeper as an NTP Time Server

Note: TimeKeeper does not support NTP peering, hence NTP servers are also referred to as NTP Sources.

Similar to the concept of PTP masters as an external reference, TimeKeeper allows external NTP servers to be used by the system as a synchronization source if NTP is an entry in the reference priority table (it is by default), and no other reference set as a higher priority is available for synchronization. No configuration is required other than setting up NTP Sources.

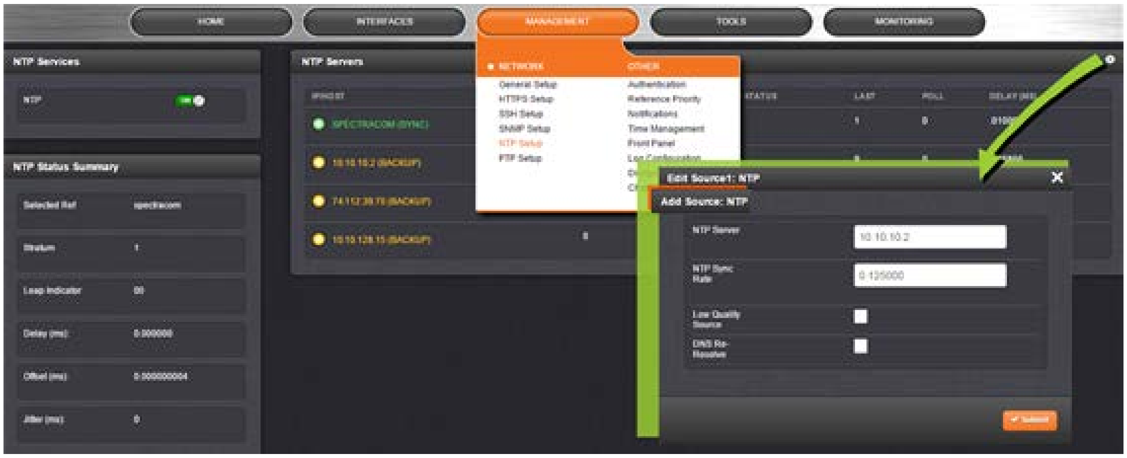
For more information on reference priorities, see "Input Reference Priorities" on page 150.

> **Note:** When TimeKeeper is enabled, the standard NTPd service is replaced by the TimeKeeper network synchronization service.

There is no configuration required of TimeKeeper to **respond to NTP client requests** that arrive at any available network ports.

To add or edit an NTP server under TimeKeeper:

1. Navigate to **MANAGEMENT** > **NETWORK/NTP Setup**.
2. In the panel **NTP Servers**, click the GEAR icon in the top-right corner to open the EDIT or ADD window (the options will change, depending on your current NTP configuration).



NTP Status Summary

Selected Ref	spectracom
Stratum	1
Leap Indicator	00
Delay (ms)	0.000000
Offset (ms)	0.000000004
Jitter (ms)	0

NTP Servers: SPECTRACOM (SYNC); 10.10.10.2 (BACKUP); 74.112.39.75 (BACKUP); 10.10.128.15 (BACKUP)

Edit Source1: NTP

Add Source: NTP

NTP Server	10.10.10.2
NTP Sync Rate	0.125000
Low Quality Source	□
DNS Re-Resolve	□

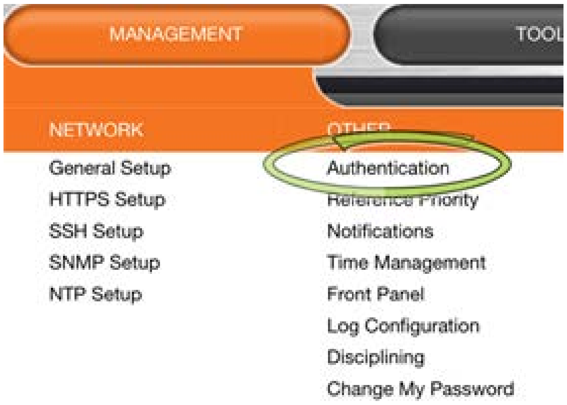
3. If requested (depending on your current NTP configuration), in the newly opened window click:
   - The PLUS icon to add a new server, or
   - The GEAR button next to an existing server, to edit it, or
   - The X-button to delete the server.
4. Populate or edit the fields:
   - **NTP Server**: The IP address or DNS name of the NTP server.
   - **NTP Sync Rate**: The rate at which to make NTP requests; a sync rate of 0.5 causes TimeKeeper to query the NTP server every 2 seconds.
   - **Low-Quality Source**: Check this box to improve tracking of a low-quality source, such as NTPd.
   - **DNS Re-Resolve**: If checked, the source will periodically re-resolve the DNS name specified for the NTP source.

3.5 OTHER Setup Pages

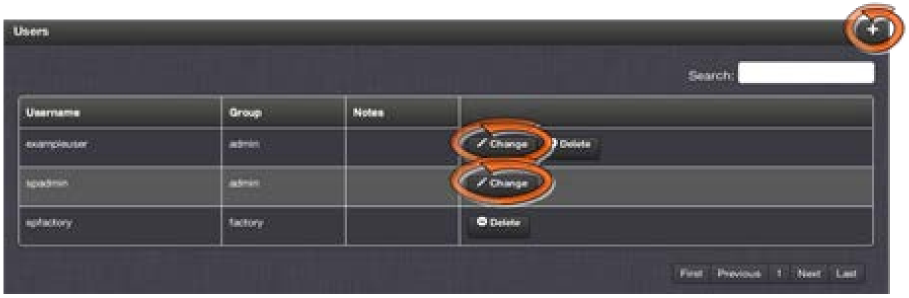
3.5.1 Authentication

3.5.1.1 User Account Management

User accounts can be created and managed from the **Users** page. The **Users** page is accessed through the **MANAGEMENT/OTHER/Authentication** menu.



The **Users** window presents a table of all user accounts showing the **Username** of each user, the **Group** to which that user account is assigned, and any **Notes** about the user account.



Username	Group	Notes	
exampleuser	admin		✎ Change ⊖ Delete
spadmin	admin		✎ Change
spfactory	factory		⊖ Delete

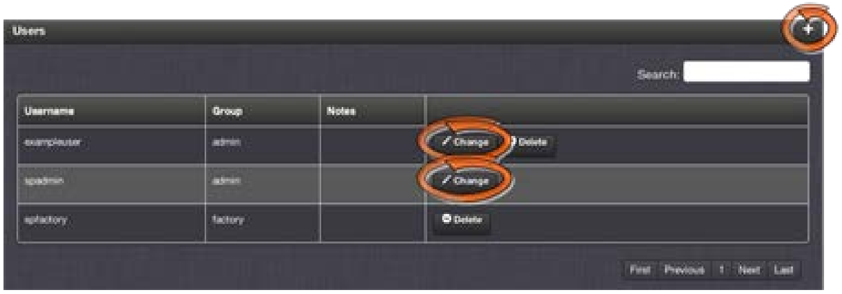
SecureSync comes with two default user accounts set up: the default administrator account (`spadmin`) and the factory service (`spfactory`) account. Additional user accounts may be added and deleted as desired.

Note: The password for the `spadmin` account can be changed (and it is recommended to do so for security reasons). However, the `spadmin` account name cannot be changed, and the account cannot be removed from SecureSync.

> **Note:** The `spfactory` account is for use by Spectracom service personnel. While the `spfactory` account can be deleted by an administrator, it should be noted that this may potentially limit remotely provided technical support.

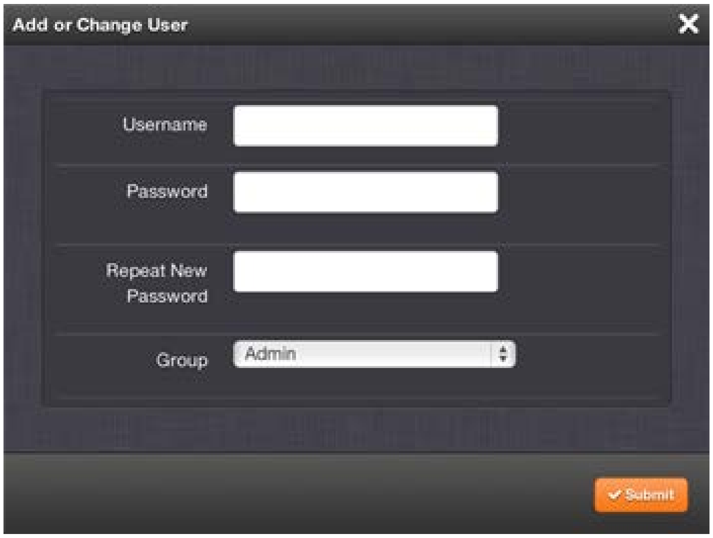
User accounts can be created to have either limited user or full administrator rights. Each user can be assigned its own login password.

- To ADD a user account, click the PLUS icon in the top-right corner of the **Users** screen.
- To DELETE a user account, click the Delete button in that account's entry on the **Users** screen.
- To APPLY CHANGES to a user account, click the Change button next to the desired user account.


Users

Username	Group	Notes	
exampleuser	admin		✓ Change ● Delete
spadmin	admin		✓ Change
spfactory	factory		● Delete

When either the Change button or the PLUS icon is clicked, the **Add or Change User** window appears:


Add or Change User

Username

Password

Repeat New Password

Group: Admin

To add a user account:

1. Enter a **Username**. The user name can be any combination of lower-case characters only (lower-case only; no upper-case characters, punctuation symbols and numbers are not

allowed). Minimum length = 3 characters, maximum length = 32 characters.

2. Enter a **Password**. The password can be any combination of upper- and lower-case characters. Minimum password length = 8 characters, maximum length = 32 characters.
3. Repeat the new **Password**.
4. In the **Group** field, choose the permission group to which you want the user to belong to:

- There are two available permission groups for each user account: user and admin. The user permission level assigns permission to access and change all settings, with the exception of the following capabilities, which are limited to the admin permission level only.
    - Changing network settings
    - Adding and deleting user accounts
    - Upgrading SecureSync system software
    - Resetting the SecureSync configuration
    - Clearing log files
    - Changing Disciplining Setup options
    - Changing configuration options for the following protocols or features:
        - NTP
        - HTTPS, SSH
        - LDAP/RADIUS
        - SNMP (with the exception of configuring SNMP notifications).

To change an existing user account:

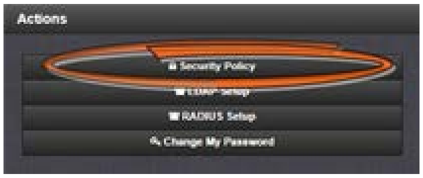
1. In the **Add or Change User** window the **Username** field will be populated.
    a. To change it, type the new name.
    b. To change the user account's password, type the new password in the **Password** field and confirm it in the **Repeat New Password** field.
    c. To change the user account's user permission group, select the group from the drop-down menu.

3.5.2 Managing Password Security

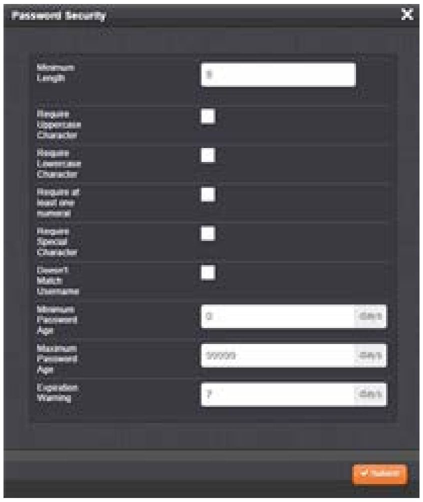
To manage password security:

1. Access the **Authentication** page through **MANAGEMENT/OTHER/Authentication** drop-down menu.

2. In the **Actions** panel, click the **Security Policy** button.



3. The **Password Security** pop-up window will display. Fill in the fields as desired.


Password Security

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

4. Click the **Submit** button at the bottom of the window.

3.5.3 Configuring LDAP Authentication

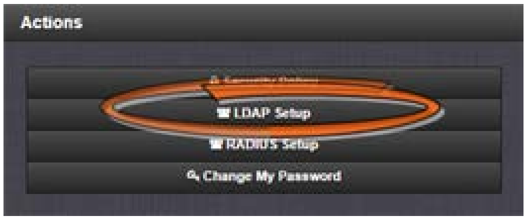
LDAP (Lightweight Directory Access Protocol) authentication provides the means to use an external LDAP server to authenticate the user account credentials when logging in to SecureSync. LDAP allows the login password for user-created accounts to be stored and maintained in a central LDAP or server on the network. This function greatly simplifies password management. Instead of having to change the password in many network appliances when a password needs to be changed, if a user password is changed in the LDAP server, it automatically changes the login password for all of the appliances that are using the LDAP server to authenticate a user login.

In order to use the LDAP authentication capability of the SecureSync, it needs to first be configured with the appropriate settings in order to be able to communicate with the LDAP server(s) on the network.

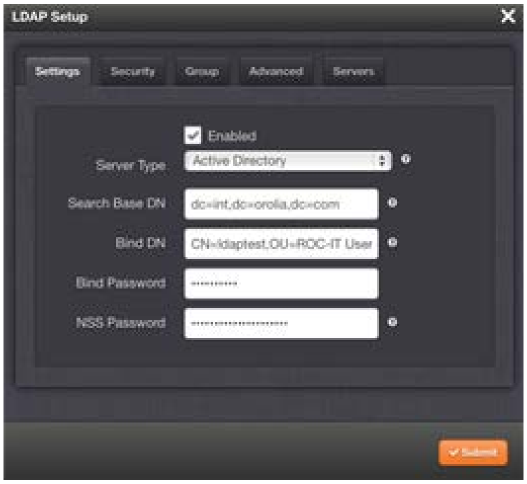
Caution: If you plan on using LDAP, configure it with diligence. If not needed, Spectracom recommends to keep LDAP disabled.

To configure LDAP authentication:

1. Navigate to **MANAGEMENT/OTHER/Authentication**.
2. In the **Actions** panel, click the **LDAP Setup** button.



3. The **LDAP Setup** window will display.



☑ Enabled

Server Type: Active Directory

Search Base DN: dc=int,dc=orolia,dc=com

Bind DN: CN=ldaptest,OU=ROC-IT User

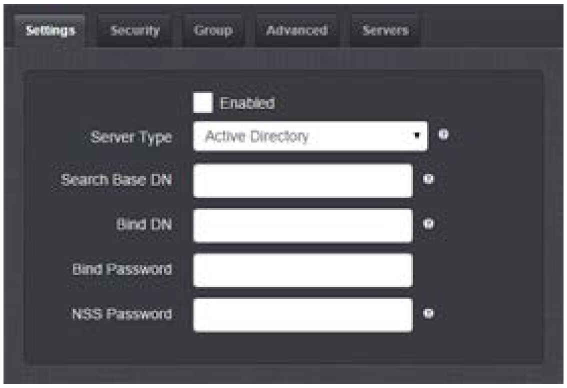
Bind Password: ••••••••••

NSS Password: ••••••••••••••••••••

4. There will be 5 tabs from which to choose:
   - **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.

3.5.3.1 LDAP Settings

Under the **LDAP Settings** tab, set:



□ Enabled

Server Type: Active Directory

Search Base DN

Bind DN

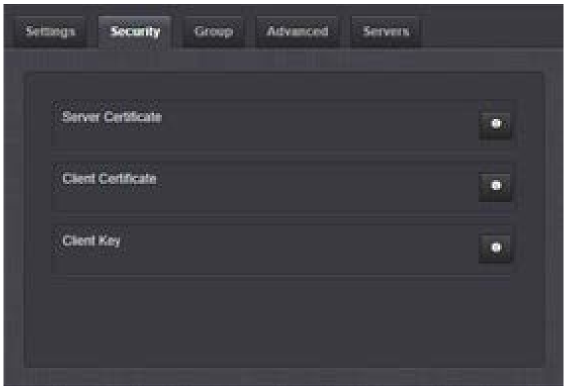
Bind Password

NSS Password

- **Server Type**—This must be the correct type—check with your LDAP server administrator if you are not sure which you are using. You have a choice of:
  - **Active Directory**—This will be used when the LDAP server is a Windows server.
  - **Open LDAP**—This will be used when the LDAP server is a Linux/UNIX server.
- **Server Base DN**—Specifies the default base distinguished name to use for searches. This is the base name to use in the database search. Typically, this is the top-level of the directory tree structure. Your LDAP server administrator will provide this information.
- **Bind DN**—Enter the Distinguished Name used to bind to (this is an optional field if the database allows anonymous simple authentication). You are able to use any same level of the tree and everything below.
  - The bind DN is the user that is permitted to search the LDAP directory within the defined search base. Most of the time, the bind DN will be permitted to search the entire directory. The role of the bind DN is to query the directory using the LDAP query filter (as specified under the **Advanced** tab) and search base for the DN for authenticating users. When the DN is returned, the DN and password are used to authenticate the user.
- **Bind Password**—Enter the password to be used to bind with the LDAP Server. Leave this field empty for anonymous simple authentication.
- **NSS Password**—Enter the password to be used for `nss_base` and `nss_shadow`. Example: `ou=People,dc=example,dc=com?one`.

3.5.3.2 LDAP Security Settings

Under the LDAP **Security** tab, you can upload and install the SSL required certificates and NTP client key.



Server Certificate

Client Certificate

Client Key

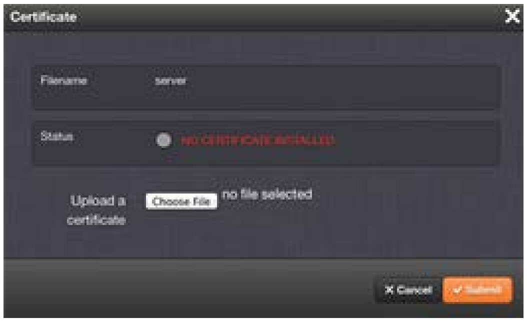
You may upload a server certificate, a client certificate, or a client key.

For each:

a. If necessary, create the desired certificate or client key. See "Creating an HTTPS Certificate Request" on page 65 for information on creating certificates and "NTP Autokey–IFF Autokey Support" on page 100 for information on client keys.

b. Click the INFO icon for the certificate you wish to upload.

c. In the **Certificate** pop-up window, click the **Choose File** button.



Certificate

Filename server

Status NO CERTIFICATE INSTALLED

Upload a certificate Choose File no file selected

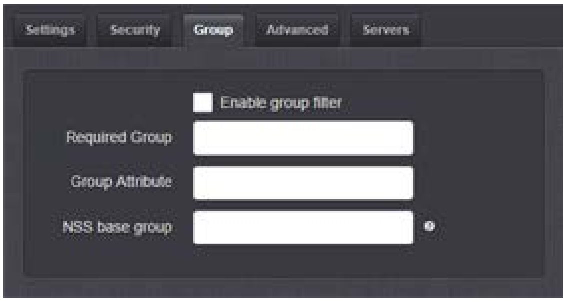
d. Locate and upload the certificate or client key file.

e. Click the **Submit** button.

The SSL certificates and/or client key you upload will be installed in the `/home/spectracom/xfer/cert/` directory.

3.5.3.3 LDAP Group Settings

Under the LDAP **Group** tab, you can filter access by group.



□ Enable group filter

Required Group

Group Attribute

NSS base group

To enable group authentication:

a. Select the **Enable group filter** checkbox.

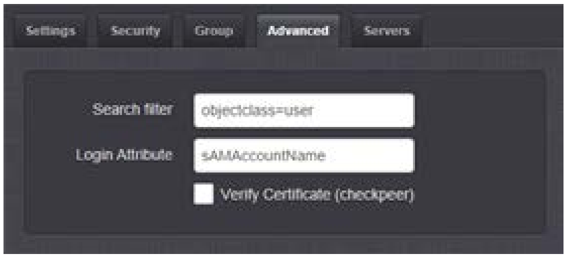
b. Enter information for:

   - **Required Group**–Enter the required group. Example. : `ou=Group, dc=example, dc=com`.
   - **Group Attribute**–Enter the group attribute. Example: `member`.
   - **NSS base group**–Enter the nss_base group. Example: ou=Group, dc=example, dc=com?one.

c. Click the **Submit** button.

3.5.3.4 LDAP Advanced Settings

Under the LDAP **Advanced** tab, you can set the search filter and the LDAP login attribute.



Search filter: objectclass=user

Login Attribute: sAMAccountName

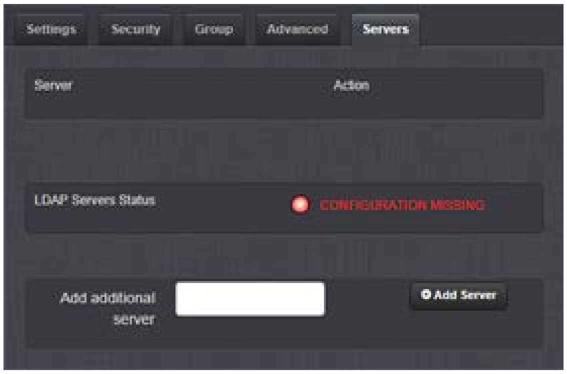
□ Verify Certificate (checkpeer)

Fill in the following fields, as desired:

- **Search filter**–This is the LDAP search filter. Example: `objectclass=user`.
- **Login Attribute**–This is the LDAP login attribute. Example: `sAMAccountName`.
- **Verify Certificate (checkpeer)**–Select this checkbox if you wish to turn on checkpeer authentication.

3.5.3.5 LDAP Servers Settings

Under the **Servers** tab, you manage the LDAP server(s) to be accessed:



Under the LDAP **Servers** tab, the window displays:

- **Server**–The hostname(s) or IP address(es) of the LDAP server(s) that have been added.
  - **Action**–After a server has been listed, it can be removed by clicking the X-button.
- **LDAP Server Status**–This will display one of the following states:
  - **PASS** (green)–An LDAP server that has been set up is available and is able to pass data.
  - **CONFIGURATION MISSING** (red)–No configuration files are available.
  - **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.
- **Add additional server**–Enter the hostname or IP address of the LDAP server to be queried. You may list multiple servers.

3.5.4 RADIUS Authentication

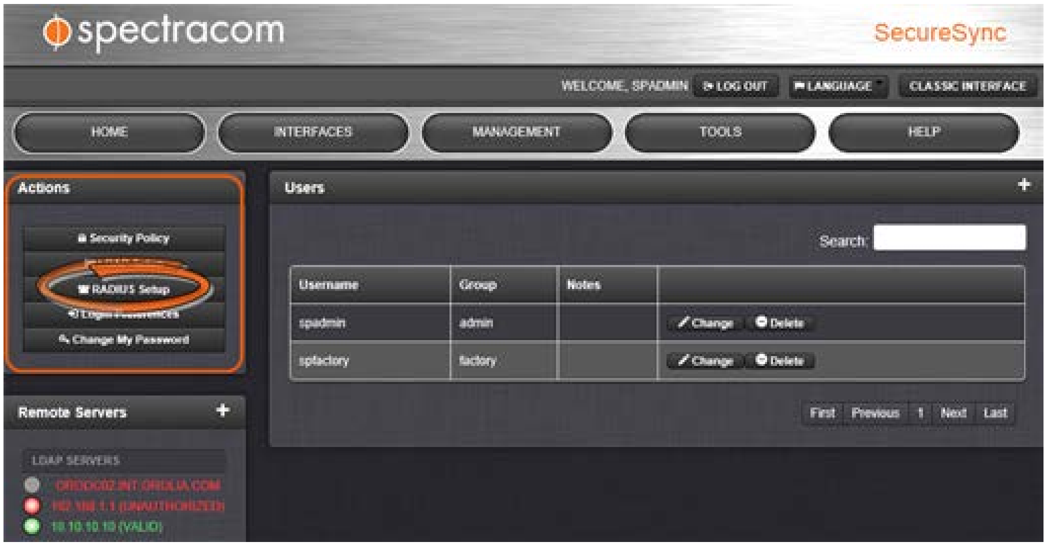
RADIUS authentication provides the means to use an external RADIUS server to authenticate the user accounts when logging in to SecureSync. RADIUS allows the login password for user-created accounts to be stored and maintained in a central RADIUS or server on the network. This function greatly simplifies password management. Instead of having to change the password in many network appliances when a password needs to be changed, if a user password is changed in the RADIUS or RADIUS server, it automatically changes the login password for all of the appliances that are using the RADIUS server to authenticate a user login.

In order to use the RADIUS authentication capability of the SecureSync, it needs to first be configured with the appropriate settings in order to be able to communicate with the RADIUS server(s) on the network.

3.5.4.1 Configuring RADIUS Authentication

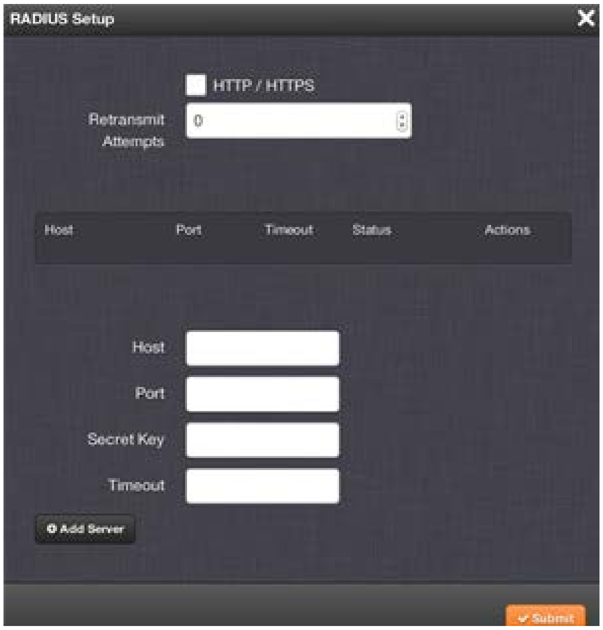
To configure RADIUS authentication:

1. Navigate to **MANAGEMENT/OTHER/Authentication**.
2. In the **Actions** panel, click the **RADIUS Setup** button.



Username	Group	Notes	
spadmin	admin		Change Delete
spfactory	factory		Change Delete

3. The **Radius Setup** window will display.



□ HTTP / HTTPS

Retransmit Attempts: 0

Host:

Port:

Secret Key:

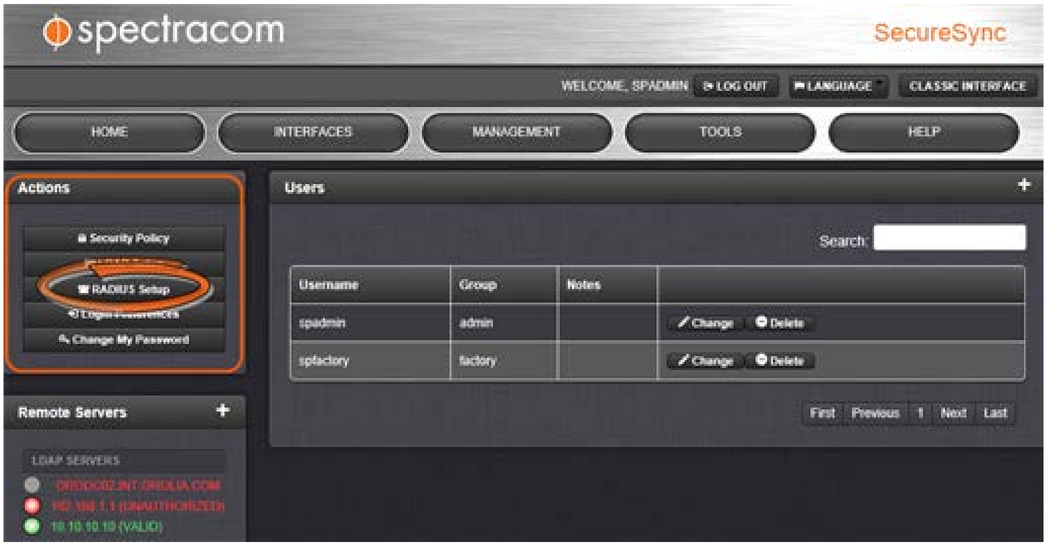
Timeout:

- If desired, select the **HTTP/HTTPS** checkbox to enable HTTPS.
- In the **Retransmit Attempts** field, select the number of retries for SecureSync to communicate with the RADIUS server.

3.5.4.2 Adding a RADIUS Server

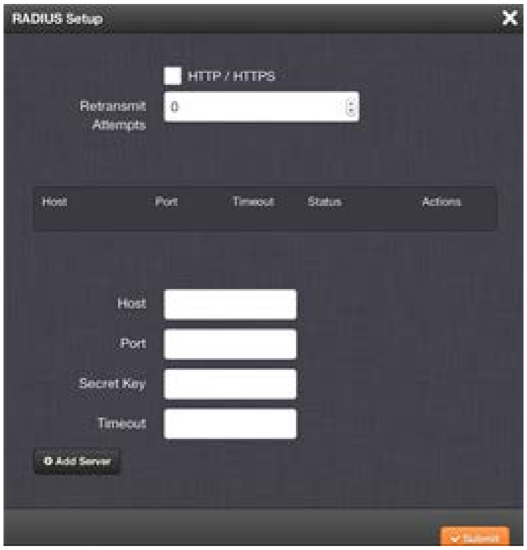
To add a RADIUS server:

1. Navigate to **MANAGEMENT/OTHER/Authentication**.
2. In the **Actions** panel, click the **RADIUS Setup** button.



Username	Group	Notes	
spadmin	admin		Change Delete
spfactory	factory		Change Delete

3. The **Radius Setup** window will display.



4. Populate the following fields as needed:
   - **Host**–Enter either the hostname or IP address of the RADIUS server on the network with which you wish SecureSync to authenticate.
   - **Port**–Defines the RADIUS Port to use. The default RADIUS Port is 1812, but this can be changed, as required.
   - **Secret key**–Enter the secret key which is shared by SecureSync and the RADIUS server (the key is used to generate an MD5 hash).

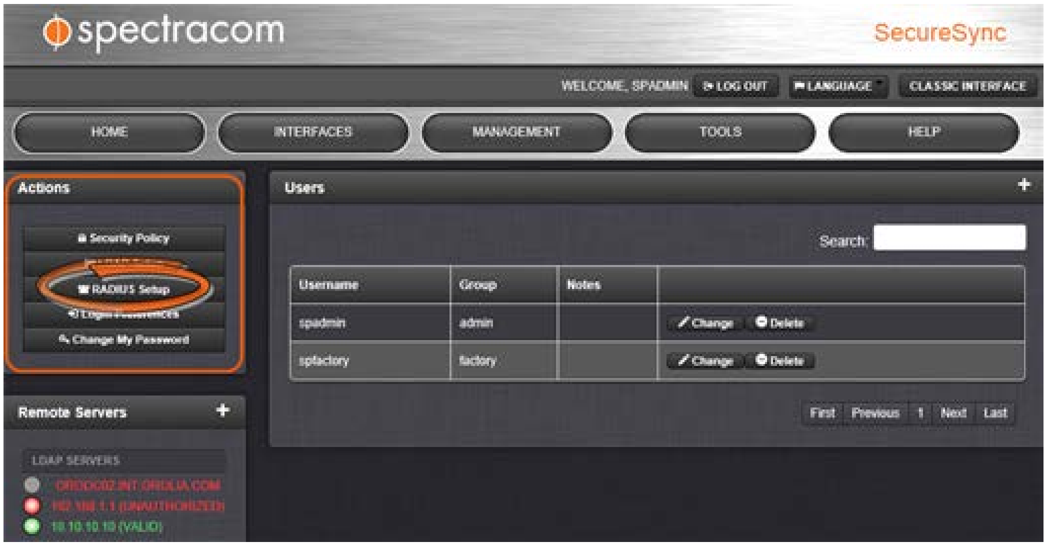
- **Timeout**–Defines the Timeout that SecureSync will wait to communicate with the RADIUS server.

5. Click the **Add Server** button.

3.5.4.3 Viewing the Status of a RADIUS Server

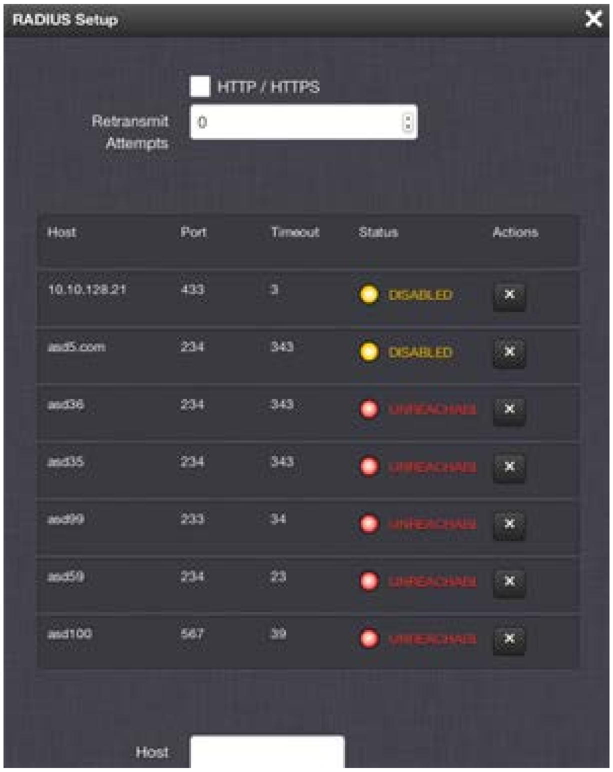
To view the status of a RADIUS server:

1. Navigate to **MANAGEMENT/OTHER/Authentication**.
2. In the **Actions** panel, click the **RADIUS Setup** button.



Username	Group	Notes	
spadmin	admin		Change Delete
spfactory	factory		Change Delete

3. The **Radius Setup** window will display.



RADIUS Setup

☐ HTTP / HTTPS

Retransmit Attempts: 0

Host	Port	Timeout	Status	Actions
10.10.128.21	433	3	● DISABLED	×
asd5.com	234	343	● DISABLED	×
asd36	234	343	● UNREACHABL	×
asd35	234	343	● UNREACHABL	×
asd99	233	34	● UNREACHABL	×
asd59	234	23	● UNREACHABL	×
asd100	567	39	● UNREACHABL	×

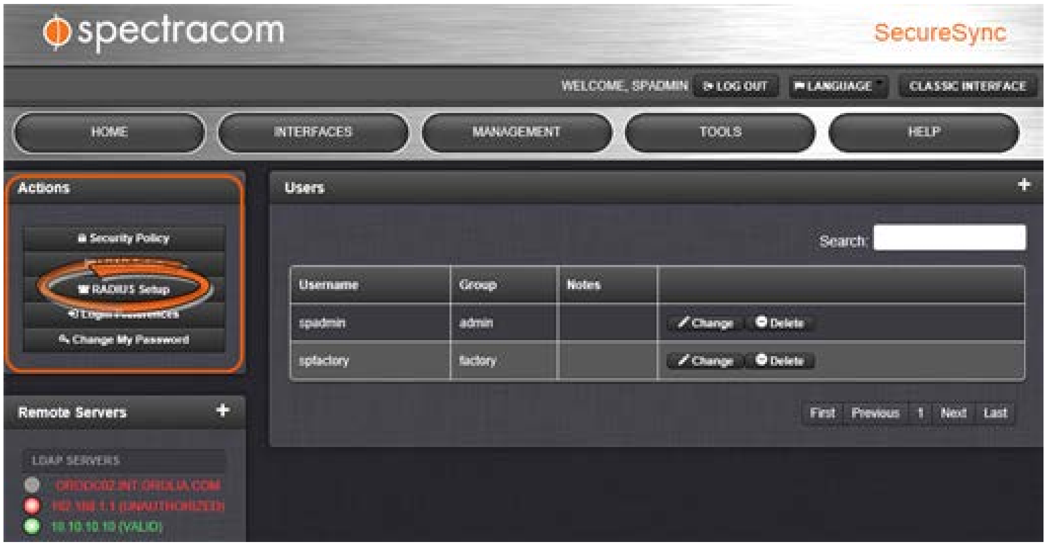
Host:

- For each RADIUS server, the following information will display:
  - **Host**–The hostname or IP address of the RADIUS server.
  - **Port**–The RADIUS port used to access the RADIUS server.
  - **Timeout**–The timeout that has been set for the RADIUS server.
  - **Status**–One of the following statuses will display:
    - **UNREACHABLE** (red, blinking)–The server is not available on the network.
    - **UNAUTHORIZED** (red)–The server is available on the network but access was denied.
    - **REACHABLE** (green)–The server is available on the network and access was allowed.
    - **DISABLED** (yellow)–The server is available on the network but RADIUS authentication is disabled on the server.
- **Actions**–Click the X-button to remove a server.

3.5.4.4 Removing a RADIUS Server

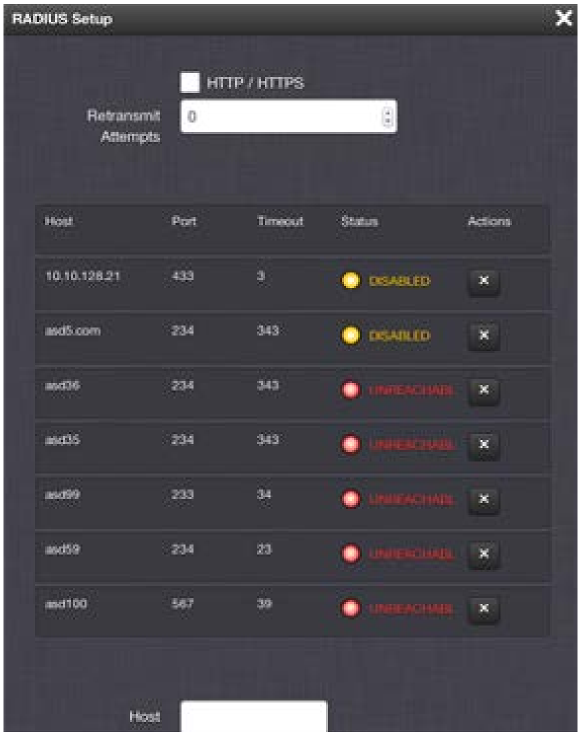
To remove a RADIUS server:

1. Navigate to **MANAGEMENT/OTHER/Authentication**.
2. In the **Actions** panel, click the **RADIUS Setup** button.



Username	Group	Notes	
spadmin	admin		Change Delete
spfactory	factory		Change Delete

3. The **Radius Setup** window will display. Click the X-button next to the RADIUS server you wish to remove.



☐ HTTP / HTTPS

Retransmit Attempts: 0

Host	Port	Timeout	Status	Actions
10.10.128.21	433	3	● DISABLED	✕
asd5.com	234	343	● DISABLED	✕
asd36	234	343	● UNREACHABL	✕
asd35	234	343	● UNREACHABL	✕
asd99	233	34	● UNREACHABL	✕
asd59	234	23	● UNREACHABL	✕
asd100	567	39	● UNREACHABL	✕

Host

3.5.5 Input Reference Priorities

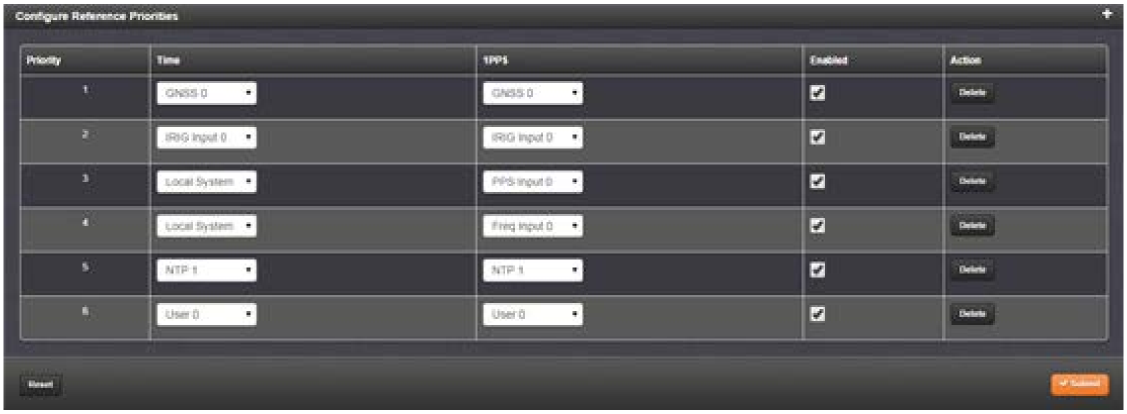
SecureSync can be synchronized to different time and frequency sources that are referred to as Input References or, sometimes just References.

References can be GNSS receivers, or other sources such as IRIG, ASCII or HAVE QUICK time codes delivered into your SecureSync unit via dedicated (mostly optional) inputs. It is even possible for the user to enter a system time manually, which SecureSync then will synchronize to.

> **Note:** Should you be installing new option cards, you will need to either manually set up the new card in the Reference Priority Table, or use the Reset to Defaults option in the Actions panel, in order to update the table with the new reference information.

In order for SecureSync to declare synchronization, it needs both a valid **PPS**, and **Time** reference.

The concept of **Reference Priority** allows the ranking of multiple references for redundancy. This allows SecureSync to gracefully fall back upon a lower ranking **PPS** or **Time** reference, in case a source with a higher priority becomes unavailable or invalid. The priority order you assign to your available references typically is a function of their accuracy and reliability.



Configure Reference Priorities

Priority	Time	1PPS	Enabled	Action
1	GNSS 0	GNSS 0	☑	Delete
2	IRIG Input 0	IRIG Input 0	☑	Delete
3	Local System	PPS Input 0	☑	Delete
4	Local System	Freq Input 0	☑	Delete
5	NTP 1	NTP 1	☑	Delete
6	User 0	User 0	☑	Delete

Each available type of **Time** and **PPS** input reference is assigned a “title” to be used in the **Reference Priority** table. The title defines the type of reference it is (e.g., “GPS 0” indicates GNSS input). These reference titles are defined in following table:

Title	Reference
ASCII Timecode	ASCII serial timecode input
External 1PPS input	External 1PPS input
Frequency	External Frequency input
GPS	GNSS input
PTP	PTP input
IRIG	IRIG timecode input

Title	Reference
Local System	Built-in clock OR internal 1PPS generation
NTP	NTP input
User	Host (time is manually set by a user)
HAVEQUICK	HAVEQUICK input

Table 3-5: Reference priority titles

Note: The number displayed indicates the number of feature inputs of that type presently installed in the SecureSync- starting with "0" representing the first feature input. For example:

-IRIG 0: 1st IRIG input instance
-Frequency 1: 2nd frequency input instance
-NTP 2: 3rd NTP input instance

The columns of the **Reference Priority** table are defined as follows:

- **Priority**–Defines the order or priority for each index (row). The range is 1 to 16, with 1 being the highest priority and 16 being the lowest priority. The highest priority reference that is available and valid is the reference that is selected.
- **Time**–The reference selected to provide the necessary "Time" reference.
- **1PPS**–The reference selected to provide the necessary "1PPS" reference.
- **Enabled**–The reference is enabled.
- **Delete**–Removes the Index (row) from the Reference Priority table.

3.5.5.1 Input Reference "User"

SecureSync allows you as the "User" to override the **System Time** (whether it is synchronized to a valid reference, or not) with a manually set time, and declare this manually set time to be a valid **System Time** (i.e., it can be used as a reference).

To this end, the following needs to be done:

I. Assign the "**User**[x]" **Time** reference to the desired Reference Priority ("1", for example), and assign a **PPS** reference to it. Click **Enable**.

II. In order for a "User" reference to become valid, user intervention is always required (contrary to "Local System" time; see "Input Reference "Local System"" on the next page): Set the **System Time** manually (**Edit System Time** > **Manual Time Set**).

Your "User[x]" Reference will then become valid.

When to use the "User" reference

The "User" reference is designed to fulfill the following use cases:

a. Temporarily, no external references are available (e.g., during system setup, or for testing/simulation purposes), or

b. No external references are required (e.g. if SecureSync is used solely to synchronize computers on a network, with no need for precise timing.)

> **Caution:** Operating SecureSync with a manually set "User" time bears the risk of inadvertently outputting an illegitimate System Time thought to be a valid reference time.

This is why the “User[x]” reference becomes invalid once SecureSync is reset or reboots, or once the Holdover Time expires (whichever occurs first), and needs to be manually set again (**Edit System Time** > **Manual Time Set**).

In order to allow use case (b.) above, two additional steps are required to override SecureSync's default settings intended to avoid outputting an illegitimate System Time as a valid reference:

i. In the **Edit System Time** window, the checkbox **Synchronize to Battery Backed Time on Startup** must be checked. This will override SecureSync's default setting to declare the System Time valid only if it is synchronized to an external reference (or a **Local System** time, see "Input Reference "Local System"" below.)

ii. In the **Oscillator Settings** window, the **Holdover Timeout** ought to be set to a duration that meets your accuracy requirements (up to 5 years): Once this **Holdover Timeout** window expires, SecureSync goes out of sync, and you need to manually set a new **System Time**.

Using the "User" reference with other reference priorities

If the “User[x]” Reference is used in conjunction with other, external reference priorities (such as GNSS or IRIG), the **System Time** should be set as accurately as possible:

Otherwise, the large time correction that needs to be bridged when switching from a lost reference to a valid reference, or from a valid reference to a higher-priority reference that has become available again, will cause NTP to exit synchronization. If the difference is under 1000 seconds, NTP will remain in sync and will "slew" (over a period of time) to the new reference time.

3.5.5.2 Input Reference "Local System"

The **Local System** Reference is a unique input reference in that it can be used as either the **Time** reference or the **PPS** reference, but never both.

When the **Time** reference is configured as **Local System**, the **Time** that SecureSync powers up with is considered valid, as long as the PPS input reference is valid. The same applies the other way round, i.e. with a **Local System PPS** reference.

The Local System configuration can be used, e.g. in a scenario with a high-quality **PPS** external reference, but an external **Time** reference that is actually less accurate than SecureSync's internal oscillator (or the other way round): In this case, the oscillator will become the higher-priority Local

System reference, and the external Time reference will serve as a lower-priority backup **Time** reference.

3.5.5.3 Reference Priorities: USE CASES

Example 1 - GNSS as Primary Reference, IRIG as Backup:

In this use case, the objective is to have:

- GNSS as the primary time and 1PPS reference
- IRIG as the backup time and 1PPS time reference.

Step-by-step procedure:

1. Move the reference which has “GPS 0” in the **Time** column and “GPS 0” in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.
2. Move the reference which has “GPS 0” in the **Time** column and “GPS 0” in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.
3. Move the reference which has “GPS 0” in the **Time** column and “GPS 0” in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.

Since both of these references are *default* references, no additional references need to be added to the **Reference Priority** table.

Example 2 - IRIG as Primary Reference, NTP Input as Backup

In this use case, the objective is to have:

- IRIG as the primary reference input
- Another NTP server as backup reference, in case the IRIG input is lost.

Step-by-step procedure:

1. Move the reference which has “IRIG 0” in both the **Time** column and “IRIG 0” in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.
2. Move the reference which has “NTP” in the **Time** column and “NTP” in the **1PPS** column to the second place in the table, with a **Priority** value of 2. Click the **Enabled** checkbox.
3. For all other references, uncheck the **Enabled** checkbox, so that they are all disabled.

Since both of these references are *default* references, no additional references need to be added to the **Reference Priority** table.

Example 3 - NTP Input as Only Available Input (“NTP Stratum 2 Synchronization”)

In this use case, the objective is to have NTP provided by another NTP server as the only available reference input.

Step-by-step procedure:

1. Move the reference which has “NTP” in the **Time** column and “NTP” in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.
2. For all other references, uncheck the **Enabled** checkbox, so that they are all disabled.

> **Caution:** When selecting NTP as an input reference, do not select another reference (such as GNSS, IRIG, etc.) to work with NTP as a reference. NTP should always be selected as both the Time and1PPS input when it is desired to use NTP as an input reference.

Example 4 - Time Set Manually by User. Other References May or May not be Available

> **Note:** In order for a manually set time to be considered valid and used to synchronize SecureSync, a “User” needs to be enabled in the Reference Priority table. See"Input Reference Priorities" on page 150 .

In this use case, the objective is to have a manually set time reference.

Step-by-step procedure:

1. If necessary (see NOTE above), create a “User.”
2. Move the reference which has “User 0” in the **Time** column and “User 0” in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.
3. For all other references, uncheck the **Enabled** checkbox, so that they are all disabled.

If the objective is to use a manually set time as a backup to other references (such as GNSS or IRIG):

1. Move the reference which has “User 0” in both the **Time** column and “User 0” in the **1PPS** column to a place in the table with a lower priority than the references the manually set reference will be backing up. Click the **Enabled** checkbox.
2. With “User” enabled, if no other higher priority references are enabled or available (or if the higher priority references have since been lost), you can simply set the **System** time to the desired value. SecureSync will go into synchronization using this set time.
3. The time can be manually set through the **System Time** panel located in the **MANAGEMENT/OTHER/Time Management** page. See "Editing the System Time" on page 171 for details on setting the time manually. Once you have set the date and time, the front panel sync light will turn green.

Note: This procedure needs to be repeated each time SecureSync is power-cycled (with no other references available,) unless synchronizing to a battery backed time on startup is enabled, or after each time all higher priority references are lost.

Example 5–Time at Power-Up ("Local System Time") to be Considered "Valid". GNSS Input to serve as 1PPS Reference

The objective of this use case is to use the time that SecureSync uses as it powers up (without the need for a user to manually set it, as would be the case with a “User” selected time). This is referred to as “Local System” time.

Since “Local System” cannot be both **Time**, and **1PPS** input together, in this use case example the GNSS input will be set as the 1PPS reference (other use cases may require using different references, e.g. IRIG.)

As there is no default entry for “Local System” and “GPS”, a new entry needs to be added to the **Reference Priorities** table in order to use this combination of references.

Step-by-step procedure:

1. Add a reference to the Reference Priority by clicking the PLUS icon. Use the following settings, then click **Submit**:
   - In the **Priority Level** text box, enter **1**. This will give this reference the highest priority.
   - In the **Time** field, select “Local System”
   - In the **PPS** field, select “GPS”.
   - Check the **Enabled** checkbox.
2. Confirm that the first reference in the **Reference Priority** table has “Local System” as the **Time** input and "GNSS" as the **1PPS** input.
3. After a power cycle or reboot, as soon as GNSS is declared valid, the System Time will automatically be used as-is, with no manual intervention required.

3.5.5.4 Configuring Input Reference Priorities

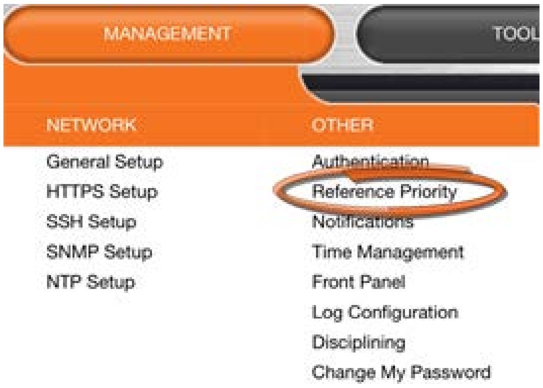
SecureSync can use numerous external time sources, referred to as "references". As external time sources may be subject to different degrees of accuracy and reliability, the user can determine in which order (= priority) SecureSync calls upon its external time and 1PPS references.

For additional information, see "Input Reference Priorities" on page 150.

Accessing the Reference Priority Screen

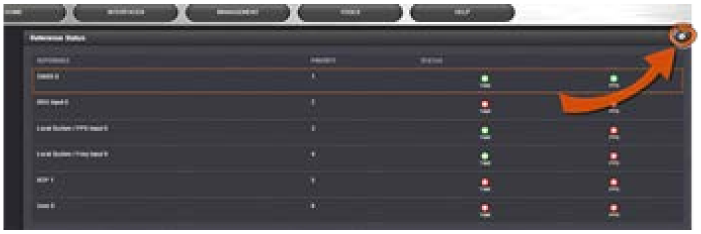
To access the **Reference Priority Setup** screen:

1. Choose **MANAGEMENT/OTHER/Reference Priority**.

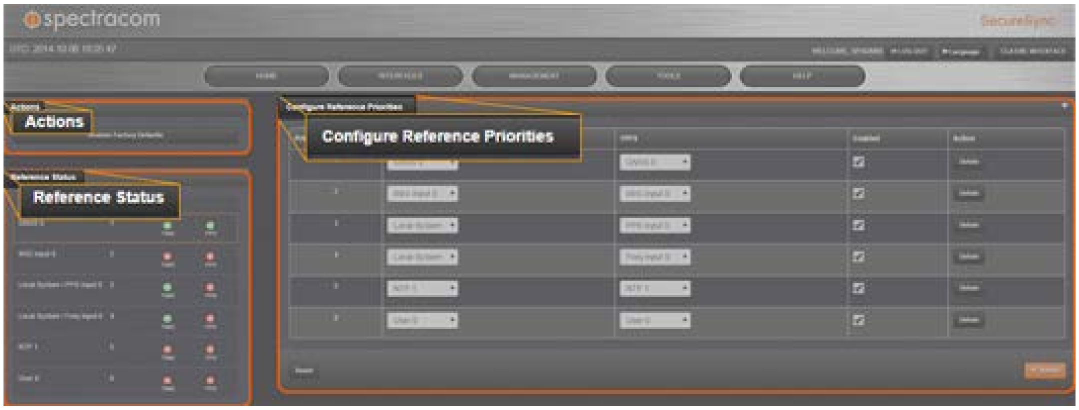


OR:

1. On the **HOME** screen, click the GEAR icon in the **Reference Status** panel.



2. The **Configure Reference Priorities** screen will display.



The **Reference Priority** screen is divided into 3 areas:

a. The **Actions** panel, which provides a single action:

   - Restore Factory Defaults

b. The **Configure Reference Priorities** panel, which displays the priority of SecureSync's references in a table form.
   In this panel you can:

- Add and configure new references
- Delete references
- Enable/disable references
- Reorder the priority of SecureSync's references

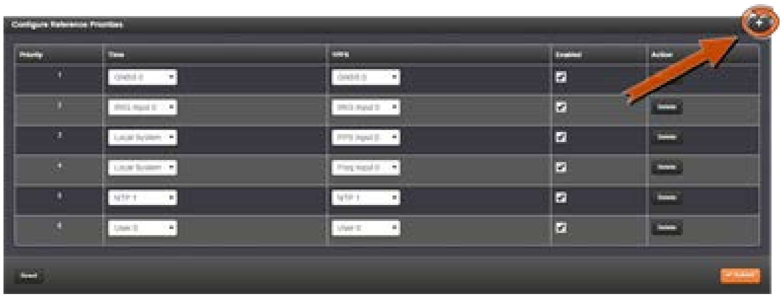
c. The **Reference Status** panel

- The **Reference Status** panel provides a real time indicator of the status of the SecureSync's references. It is the same as the **Reference Status** panel on the **HOME** screen of the Web UI.

Adding an Entry to the Reference Status Table

To add a new entry to the **Reference Status** table:

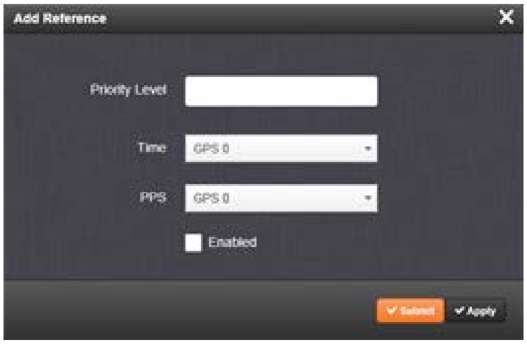
1. Navigate to the **Configure Reference Priorities** screen through the **MANAGEMENT/OTHER/Reference Priority** menu.
2. Click the PLUS icon in the upper right-hand corner of the **Configure Reference Priorities** table.



Configure Reference Priorities

Priority	Time	1PPS	Enabled	Action
1	GNSS 0	GNSS 0	☑	
2	IRIG Input 0	IRIG Input 0	☑	Delete
3	Local System	PPS Input 0	☑	Delete
4	Local System	Freq Input 0	☑	Delete
5	NTP 1	NTP 1	☑	Delete
6	User 0	User 0	☑	Delete

3. The **Add Reference** window will display:



Add Reference

Priority Level

Time: GPS 0

PPS: GPS 0

☐ Enabled

4. In the **Add Reference** window, enter:
   - **Priority Level**–This is the priority you want to give your reference.
   - **Time**–Enter the time reference.

» **PPS**–Enter the PPS reference.

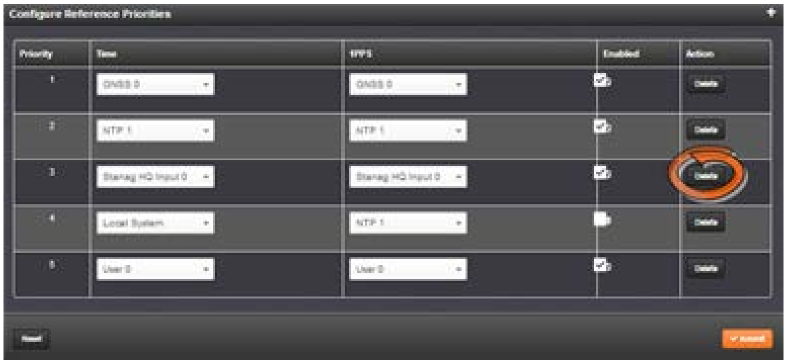
» **Enabled**–Check this box to enable the new reference.

5. Click **Apply** or **Submit**. (**Submit** will close the window.)

Deleting a Reference Entry

To delete an entry from the **Reference Status** table:

1. Navigate to the **Configure Reference Priorities** screen through the **MANAGEMENT/OTHER/Reference Priority** menu.
2. In the **Configure Reference Priorities** table click the **Delete** button on the right-hand side of the entry you wish to delete.



Configure Reference Priorities

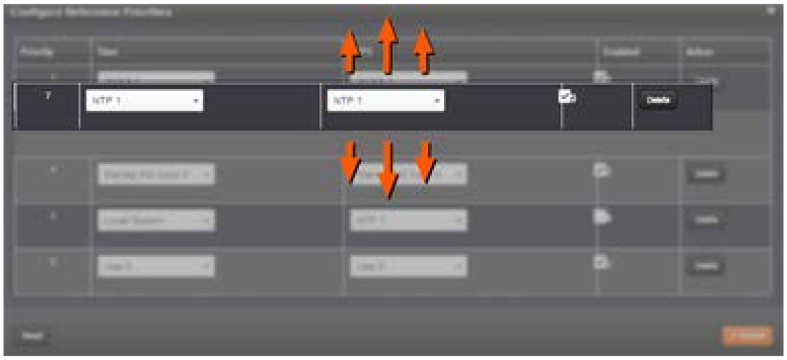
Priority	Time	1PPS	Enabled	Action
1	GNSS 0	GNSS 0	☑	Delete
2	NTP 1	NTP 1	☑	Delete
3	Stanag HQ Input 0	Stanag HQ Input 0	☑	Delete
4	Local System	NTP 1	□	Delete
5	User 0	User 0	☑	Delete

3. Click the **OK** button in the pop-up window that displays.

Reordering Reference Entries

To reorder the priority of a reference entry:

1. Navigate to the **Configure Reference Priorities** screen through the **MANAGEMENT/OTHER/Reference Priority** menu.
2. Click and hold on the item whose priority you wish to reorder.
3. Drag the item up or down to the desired place.



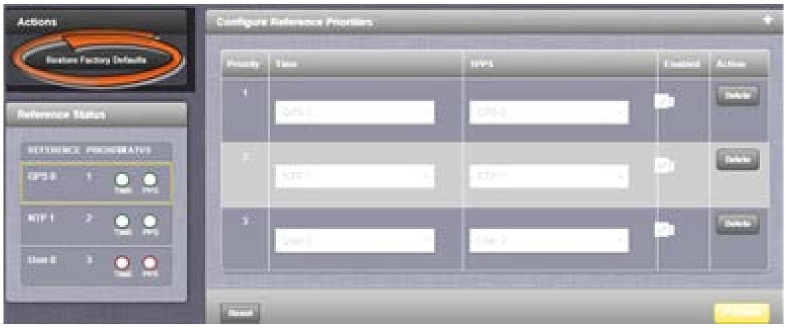
2	NTP 1	NTP 1	☑	Delete

4. Click the **Submit** button to finish the operation, or the **Reset** button to undo it.

Resetting Reference Priorities to Factory Defaults

To reset the **Reference Priority** table to the factory default configuration:

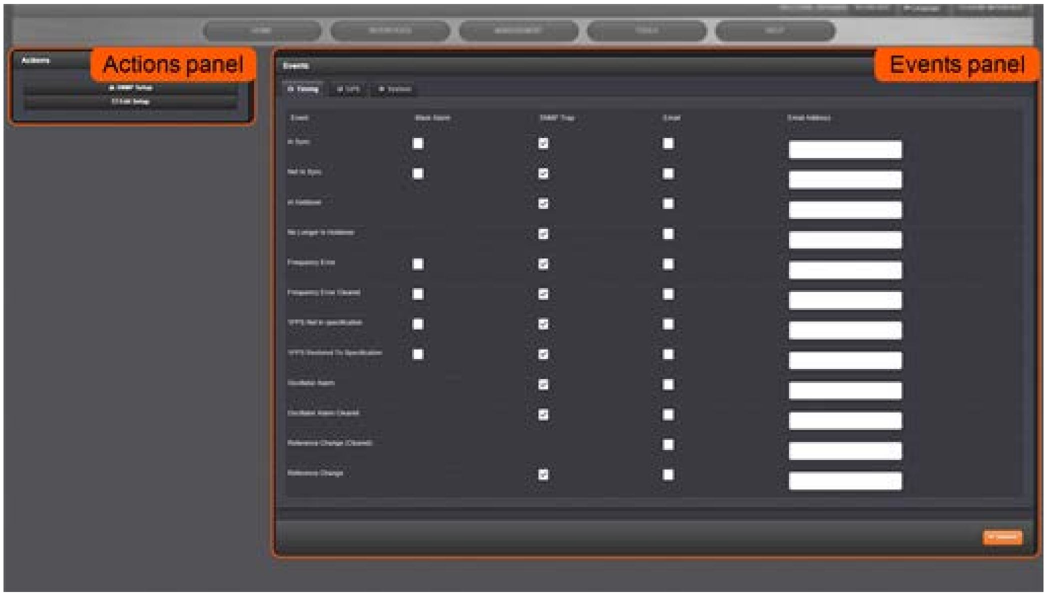
1. Navigate to the **Configure Reference Priorities** screen through the **MANAGEMENT/OTHER/Reference Priority** menu.
2. In the **Actions** panel, click the **Restore Factory Defaults** button.



3.5.6 Notifications

3.5.6.1 Accessing the Notifications Page

1. Navigate to **MANAGEMENT > OTHER: Notifications**. The **Notifications** page will display:



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		☑	□	

The **Notifications** page is divided into two panels:

- The **Actions** panel, offering two options:
  - **SNMP Setup**: Clicking this button will open the **SNMP Setup** screen. See "Configuring SNMP and Notifications" on page 83.
  - **Edit Setup**: The **Email Setup** screen provides the means to configure SecureSync with the necessary settings to interface it with Exchange email servers and Gmail.
- The **Events** panel, which includes 3 tabs:
  - **Timing**: This tab contains events for Sync Status and Holdover, Frequency error, Input references and the internal oscillator
  - **GPS**: This tab contains events related to the GNSS receiver, including antenna cabling, tracking less than the minimum number of satellites and GNSS receiver faults.
  - **Systems**: This tab contains events related to the system operation, including minor and major alarms being asserted, reboot, timing system errors and option cards.

3.5.6.2 Utilizing Notifications

SecureSync events (such as going into or out of Time Sync, into or out of Holdover mode, an antenna problem when a short or open occurs in the GNSS antenna cable, etc.) can cause a trigger to notify users that a specific event has occurred.

In some situations, two events are generated. One event occurs in the transition to a specified state and then another event occurs when transitioning back to the original state. Examples of these are losing sync and then regaining sync, or going into Holdover mode and then going out of Holdover mode. Other situations may only consist of one event. An example of this situation is switching from one input reference to another.

Notifications of each event that may occur can be via alarms, via SNMP Traps being sent to one or more SNMP Managers, via an email being sent to a specified email recipient, or a combination of the three. The Notifications page allows a user to configure whether the occurrence of each event automatically triggers an alarm to be generated, an SNMP trap to be sent out, an email to be sent out, or a combination of the three.

Also, this page allows the desired email recipient's address for that particular event to be specified. Each event can be configured with the desired email address that is specific to just that one event only. Note that only one email address can be specified in each Email Address field. If desired, the same email address can be used in all of the fields, or different addresses can be used for different events.

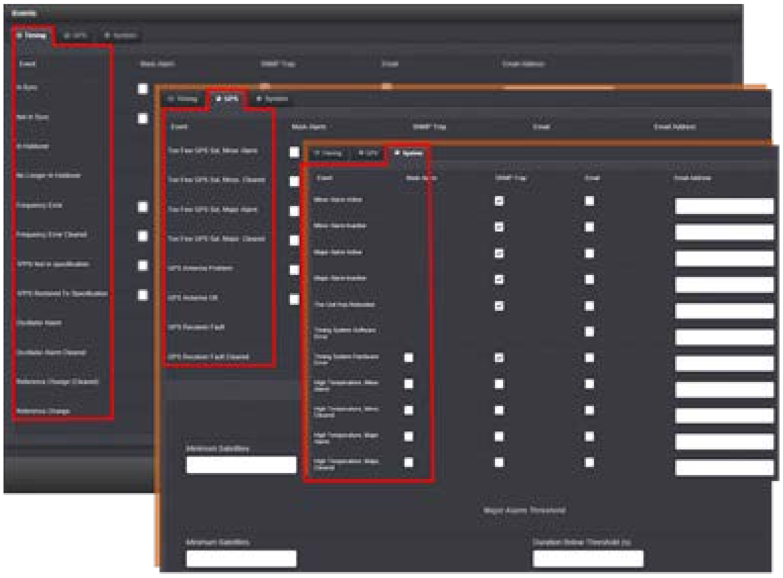
Note: Whether or not notifications are enabled/disabled for a given event, the occurrence of the event is always logged.

All available SecureSync events that can generate a notification to be sent are located in different tabs in the Notification Setup table: Timing, GPS, and System. The SecureSync Events that can automatically trigger a notification are listed in the Event column. If applicable for each specific event, the user can mask alarm generation (prevent the alarm), enable "SNMP" (to send out an SNMP trap) and/or "Email" to send an email to the address specified in the corresponding "Email Address" column.

3.5.6.3 Configuring Notifications

To configure notifications:

1. Navigate to **MANAGEMENT > OTHER: Notifications**.
2. In the **Events** table, choose the tab for **Timing**, **GPS** or **System**.



The columns under each tab are:

- **Event**–This is the event that will trigger the notification. The events under each tab will vary according to context.
- **Mask Alarm**–Check here to enable an alarm mask. Enabling an alarm mask for a given notification will prevent that notification from generating an alarm condition. Other notifications for that event and logging of the event will still occur.
- **SNMP Trap**–Check here to configure the event to trigger an SNMP Trap.
- **Email**–Check here to configure the event to trigger an email notification.
- **Email Address**–Enter the address to which the email should be sent when triggered by the event.

Note: Each event can be configured with the desired email address that is specific to just that one event only. Note that only one email address can be specified in each Email Address field.

For each event choose the notification you want and the email, if any, to which you want a notification to be sent. See "Configuring SNMP and Notifications" on page 83 for details about setting up SNMP. See "Setting Up Notification Emails" on page 165 for information on setting up notification email.

For each event, only the notification options available can be configured. For example, a mask alarm can be set for an In-Sync event, and a Not-in-Sync event, but not for an In-Holdover event.

3. Click the **Submit** button at the lower right-hand corner of the page.

Notification Events: Timing tab

Notifications can be sent upon the following **Timing Events**:

- 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

Notification Events: GPS tab

Notification events can be sent upon the following **GPS Events**:

- Too Few GPS Sat, Minor Alarm–See "Setting GPS Minor and Major Alarm Thresholds" below
- Too Few GPS Sat, Minor, Cleared
- Too Few GPS Sat, Major Alarm–See "Setting GPS Minor and Major Alarm Thresholds" below
- Too Few GPS Sat, Major, Cleared
- GPS Antenna Problem
- GPS Antenna OK
- GPS Receiver Fault
- GPS Receiver Fault Cleared

Under the **GPS Events** tab, the user also configures the **Minor** and **Major Alarm Threshold** for GNSS fault events. See the following section for information on setting these thresholds.

Notification Events: System tab

Notification events can be sent upon the following **System Events**:

- Minor Alarm Active
- Minor Alarm Inactive
- Major Alarm Active
- Major Alarm Inactive
- Unit Reboot
- Timing System Software Error
- Timing System Hardware Error
- High Temperature, Minor Alarm
- High Temperature, Minor, Cleared
- High Temperature, Major Alarm
- High Temperature, Major, Cleared

3.5.6.4 Setting GPS Minor and Major Alarm Thresholds

The **GPS Events** panel contains the definition of user-defined Minor and Major alarms for the GNSS receiver falling below a user-specified number of GNSS satellites. SecureSync itself has a pre-defined minimum number of satellites that must be tracked in order for GNSS to be considered a valid reference. However, this section allows a user to setup alerts if SecureSync tracks less than a user-specified number of satellites. This event can cause either a Minor or a Major alarm (or both) to be asserted, depending on the configuration.

Each of the two Minor and Major alarms sections contains a field to define the desired threshold for the minimum number of satellites that must be tracked that before the particular alarm is asserted. Note that the GNSS receiver must initially be tracking more than the configured number of satellites in order for this alarm to be triggered (the alarm is triggered when the receiver falls below the minimum number specified).

The **Duration Below Threshold(s)** field provides the ability to define a period of time (in seconds) that the GNSS receiver is allowed to fall below the minimum number of satellites before the particular alarm is asserted.

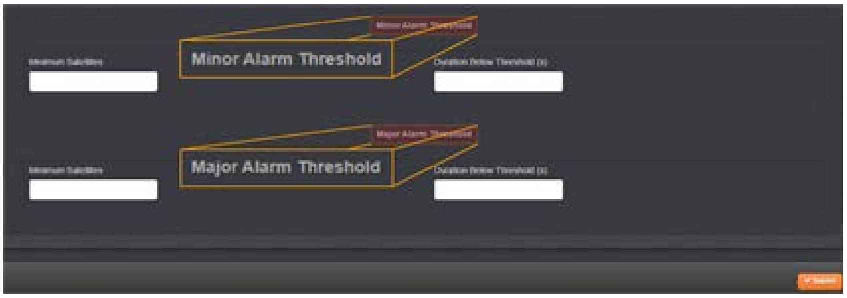


Figure 3-4: Alarm Threshold panel

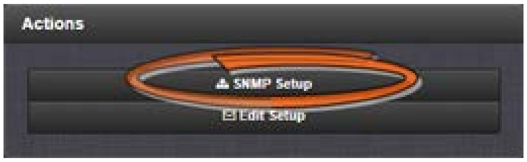
To set the **Minor Alarm Threshold** and/or **Major Alarm Threshold**:

1. If necessary, navigate to **MANAGEMENT/OTHER/Notifications** and choose the **GPS** tab.
2. At the bottom of the screen, locate the **ALARM THRESHOLD** panel.
3. In the **Minimum Satellites** field enter the minimum number of satellites that must be available before the alarm is triggered. The alarm will be triggered when the number of satellites available is **BELOW** this number.
4. In the **Duration Below Threshold(s)** field, enter the time that the system must be below the threshold set in the **Minimum Satellites** field before an alarm is triggered. The alarm will be triggered when this time is reached.

3.5.6.5 SNMP Notification Setup

To configure SNMP notifications:

1. Navigate to **MANAGEMENT > OTHER: Notifications**.
2. Near the top-left of the screen, click **SNMP Setup** in the **Actions** panel.



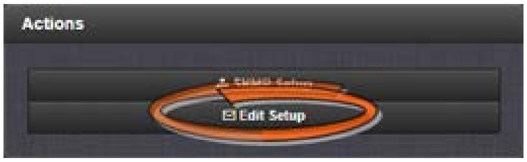
For details about setting up SNMP, see "Configuring SNMP and Notifications" on page 83.

3.5.6.6 Setting Up Notification Emails

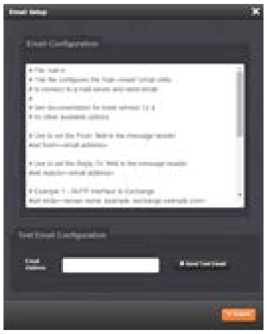
The **Email Setup** window provides the means to configure SecureSync with the necessary settings to interface it with Exchange email servers and Gmail.

To set up email:

1. Navigate to **MANAGEMENT/OTHER/Notifications**.
2. Click the **Edit Setup** button in the **Actions** panel in the top-left corner of the **Notifications** screen.

3. The **Email Setup** window will display:

The **Email Configuration** box provides two example configuration files. One is for interfacing SecureSync with an Email Exchange server; and the other is for sending emails via Gmail:

4. To configure the applicable example email configuration, delete the comments ("#") from each line and replace the "<>" with the appropriate values for your particular email server (such as the user name and password for your Email server).

Example I: SMTP interface to MS Exchange

```
#set smtp=<server name, example: exchange.example.com>
#set smtp-auth-user=<user name>
#set smtp-auth-password=<password>
#set smtp-auth=login
```

Example II: SMTP interface to Gmail

```
#set smtp=smtp.gmail.com:587
#set smtp-use-starttls
#set ssl-verify=ignore
#set smtp-auth-user=<user name, example user_xyz123@gmail.com>
```

```
#set smtp-auth-password=<password>
#set smtp-auth=login
```

5. Click the **Submit** button at the bottom of the window.
6. To test your settings:
   - In the **Test Email Address** field, enter an email address.
   - Click the **Send Test Email** button.
   - A notification that your email has been sent will appear at the top of the window.

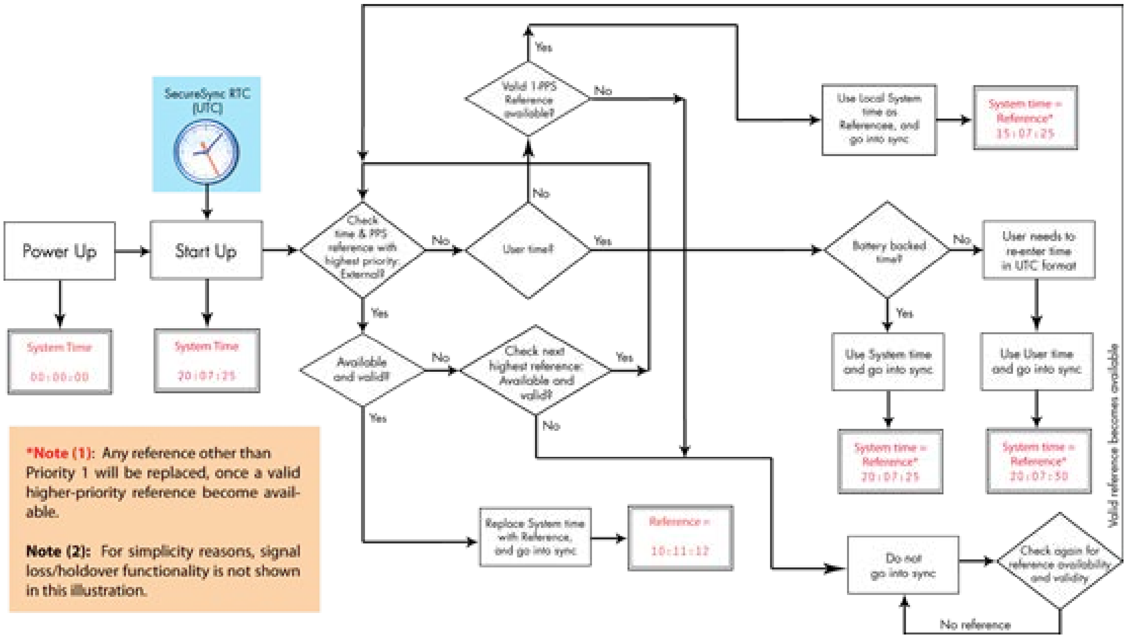
Additional information on this subject can be found in the Spectracom Technical Note "Email Notification Setup with SecureSync, NetClock".

3.5.7 System Time

The time that SecureSync maintains is referred to as the System Time. By default, the System Time is synchronized to SecureSync's input references (such as GNSS, IRIG, ASCII data, NTP, PTP, etc.).

Alternatively, the System Time can be manually configured by the user to a desired time/date, or it can be operated without external time reference (but with an external PPS reference)–this is called **Local System** reference.

The System Time is used to generate all of the available time-of-day outputs (such as the front panel LED display, NTP time stamps, time stamps in the log entries, ASCII data outputs, etc.)


SecureSync RTC (UTC)
Power Up
Start Up
System Time 00:00:00
System Time 20:07:25
Check time & PPS reference with highest priority: External?
No
Yes
User time?
No
Yes
Valid 1-PPS Reference available?
Yes
No
Use Local System time as Reference, and go into sync
System time = Reference* 15:07:25
Battery backed time?
No
Yes
User needs to re-enter time in UTC format
Use System time and go into sync
Use User time and go into sync
System time = Reference* 20:07:25
System time = Reference* 20:07:50
Available and valid?
No
Yes
Check next highest reference: Available and valid?
Yes
No
Replace System time with Reference, and go into sync
Reference = 10:11:12
Do not go into sync
Check again for reference availability and validity
No reference
Valid reference becomes available

*Note (1): Any reference other than Priority 1 will be replaced, once a valid higher-priority reference become available.

Note (2): For simplicity reasons, signal loss/holdover functionality is not shown in this illustration.

Figure 3-5: System time

The figure above illustrates how SecureSync obtains the highest available and valid reference priority, depending on whether an external source is chosen as reference, or an internal (**User[x]**, or **Local System**).

To configure the System Time, go to the **System Time** panel, which is located in the top-left corner of the **Time Management** screen (see "System Time" on the previous page).

Note: System time must be set in UTC timescale, not local time.

Note: In order for the time to be set manually by a user, and to qualify as a valid reference, the Input Reference Priority table on the Setup/Reference Priority screen must include an "Enabled" “User[x]” Time and PPS reference.

See "Input Reference Priorities" on page 150 for more information.

3.5.7.1 Timescales, Offsets and Leap Seconds

The System Time can be configured to operate in various timescales, such as UTC, GPS and TAI *(Temps Atomique International)*. All of these times are offset from each other by varying amounts, so the times are not all exactly the same.

Note: UTC Timescale is also referred to as “ZULU” time. GPS timescale is the raw GPS time as transmitted by the GNSS satellites (as of September, 2013, GPS time is currently 16 seconds ahead of UTC time. UTC timescale observes leap seconds while GPS timescale does not).

Note: The TAI timescale also does not observe leap seconds. The TAI timescale is fixed to always be 19 seconds ahead of GPS time. As of July, 2015, TAI time is 36 seconds ahead of UTC.

The System Timescale is configured through the **MANAGEMENT/OTHER/Time Management** page.

Some of the available SecureSync inputs (such as the IRIG option module’s input, ASCII data module’s inputs, etc.) won’t necessarily provide time to SecureSync in the same timescale selected in the System Time’s Timescale field. These inputs have internal conversions that allow the timescale for the inputs to also be independently defined, so that they don’t have to be provided in the same timescale. For example, the System timescale can be configured as “UTC”, but the IRIG input data stream can provide SecureSync with “local” time, with no time jumps occurring when the reference is selected.

If an output reference is using the GPS or TAI timescale, and the System Time is set to “UTC”, then the GPS Offset box in the Edit GPS Offset window must be populated with the proper timescale offset value in order for the time on the output reference to be correct. Some references (like GNSS) provide the timescale offset to the system. In the event that the input reference being used does not provide this information, it must be set in through the Offsets panel of the Time Management page. See also "System Time" on page 166.

Since the GPS and TAI offsets have a fixed relationship, only the GPS offset can be set. If only the TAI offset is known, subtract 19 from it to get the GPS offset.

Note: If the System Time is set to the UTC timescale, and all output references either use the UTC or “local” timescale, then it is not necessary to set the GPS and TAI Timescale Offsets.

Caution: It is imperative to configure any input reference’s timescales appropriately. Otherwise, a System Time error may occur!

Some of the available SecureSync outputs (such as the front panel LED display, the IRIG option module’s outputs, ASCII data module’s outputs, etc.) won’t necessarily output in the same timescale selected in the System Time’s Timescale field. These outputs have internal conversions that allow the timescale for the outputs to also be independently defined, so that they don’t have to be provided in the same timescale. For example, the System timescale can be configured as “UTC”, but the front panel LED display can be configured to still show “local” time, if desired.

Other SecureSync outputs will be provided in the same timescale that is selected in the System timescale field. The NTP output for network synchronization and the time stamps included in all log entries will be in the same timescale as the configured System Timescale. For example, if “GPS” is selected as the System timescale, the log entries and the time distributed to the network will all be in GPS time (time broadcasted directly from the GNSS constellation). But, the LED display can still be configured to show the current “local” time.

In most cases, “UTC” will be the desired Timescale to select.

3.5.7.2 DST Rule Configurations

The following examples are provided to illustrate the configuration of Daylight Savings Time (DST) when setting up SecureSync.

Example 1:

To create a Local System Clock to UTC+1 with no DST rule:

In the **Local Clock** pop-up window:

1. Assign the clock a meaningful name in the **Local Clock Name** field.

1. Select “UTC +01:00” from the **UTC Offset** pull down menu.
2. Confirm that the **Use DST Rules** checkbox is not selected.
3. Review the changes made and click the **Submit** button.
4. The SecureSync will display the status of the change.

Example 2:

To create a Local System Clock for a SecureSync installed in the Eastern Time Zone of the US, and desiring the Local Clock to automatically adjust for DST (using the post 2006 DST rules for the US).

In the **Local Clock** pop-up window:

1. Assign the clock a meaningful name in the **Local Clock Name** field.
2. Select “UTC -05:00” from the **UTC Offset** pull-down menu.
3. Select the **Use DST Rules** checkbox.
4. Select the **Set DST Rules by Region** checkbox.
5. From the **DST Region** drop-down list, select “US-Canada.”
6. Review the changes made and click the **Submit** button.
7. The SecureSync will display the status of the change.

3.5.7.3 Daylight Saving Time

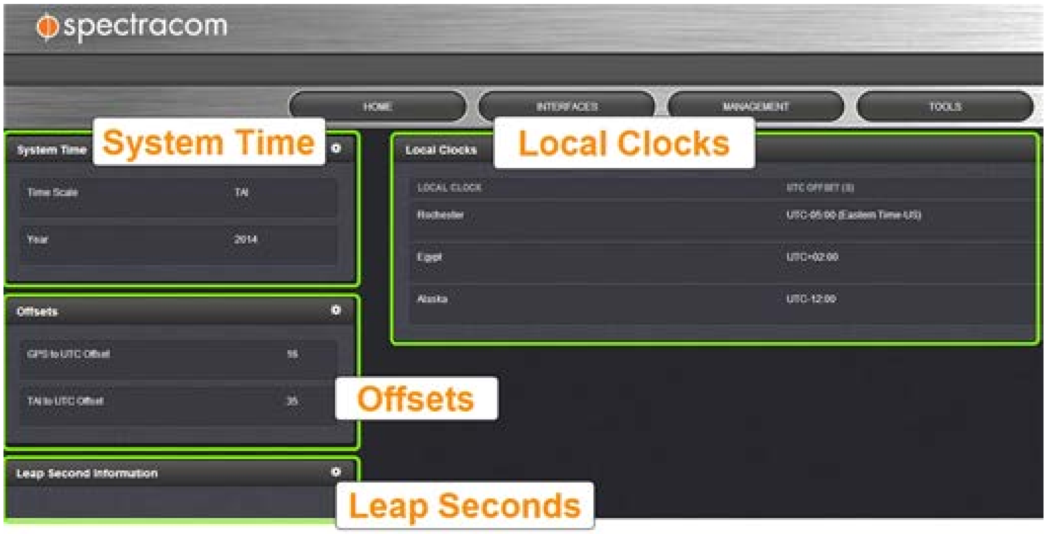
Information about time zones and DST can be found on the following web site: http://www.worldtimeserver.com/, http://webexhibits.org/daylightsaving/b.html.

3.5.7.4 The Time Management Screen

To access the **Time Management** screen:

1. Navigate to **MANAGEMENT > OTHER: Time Management**.

2. The **Time Management** screen opens. It is divided into 4 panels:



System Time

Time Scale	TAI
Year	2014

Offsets

GPS to UTC Offset	16
TAI to UTC Offset	35

Leap Second Information

Local Clocks

LOCAL CLOCK	UTC OFFSET (S)
Rochester	UTC-05:00 (Eastern Time US)
Egypt	UTC+02:00
Alaska	UTC-12:00

System Time panel

The System Time panel displays the time scale and the year, and allows access to the **Edit System Time** window via the GEAR icon in the top-right corner. This window is used to select the time scale, and to manually set a user- time, if so required.

See also: "The Time Management Screen" on the previous page

Offsets panel

The time scales UTC, TAI, and the GPS-supplied time are offset by several seconds, e.g. to accommodate leap seconds. The GPS offset may change over time, and can be managed via the GEAR icon in the top-right corner of this panel.

See also: "The Time Management Screen" on the previous page

Leap Second Info panel

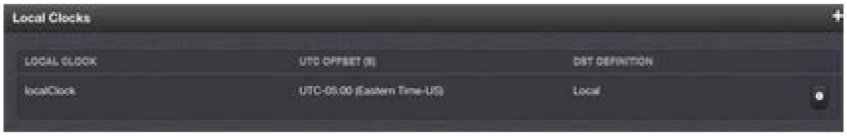
From time to time, a leap second is applied to UTC, in order to adjust UTC to the actual position of the sun. Via the **Leap Second Info** panel, leap second corrections can be applied to SecureSync’s time keeping. It is also possible to enter the exact day and time when the leap second is to be applied, and to delete a leap second.

See also: "The Time Management Screen" on the previous page

See also: "Leap Second Occurrence" on page 276

Local Clocks panel

Multiple Local Clocks with different configurations can be created, as needed. The names of all Local Clocks that have already been created are displayed table rows in the Local Clocks panel.



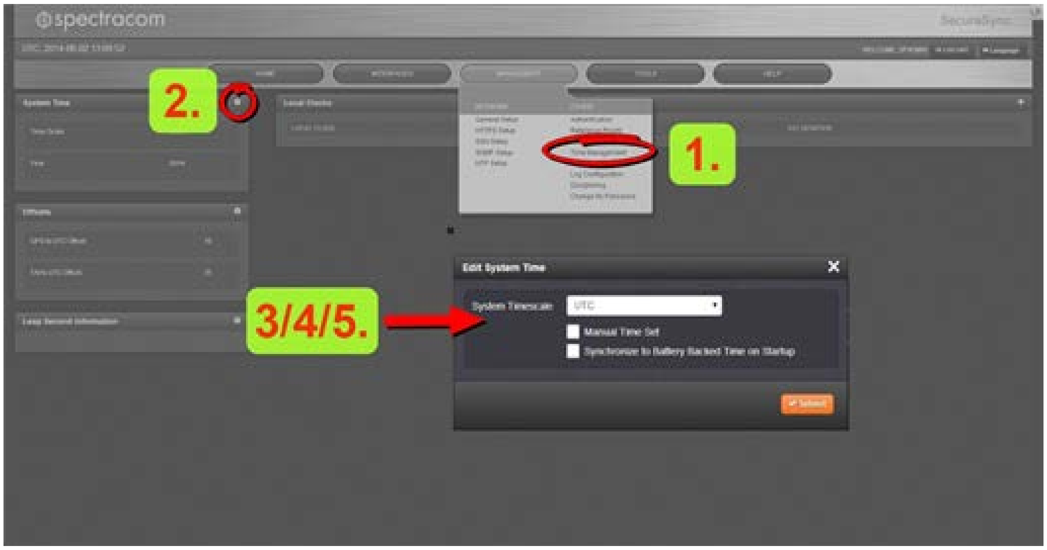
Local Clocks

LOCAL CLOCK	UTC OFFSET (S)	DST DEFINITION
localClock	UTC-05:00 (Eastern Time-US)	Local

3.5.7.5 Editing the System Time

In order to edit the System Time, SecureSync allows you to:

- Change the System Timescale
- Manually set a user-defined time, e.g. for simulation purposes, or if no external reference is available, and you want to use the unit as a valid NTP server
- Maintain the user-defined time after a system reboot by means of battery backup.



Edit System Time

System Timescale: UTC

☐ Manual Time Set

☐ Synchronize to Battery Backed Time on Startup

✓ Submit

To edit the System Time:

1. Navigate to **MANAGEMENT > OTHER: Time Management**.
2. In the **System Time** panel located in the top-left corner of the **Time Management** screen, click the GEAR icon.
3. The **Edit System Time** pop-up window will display.
4. In the **System Timescale** field select a timescale from the drop-down list. The options are:
    - **UTC**: Coordinated Universal Time (Temps Universel Coordonné); your local time zone determines the difference between UTC and local time
    - **TAI**: International Atomic Time (Temps Atomique International); the TAI time scale is based on the SI second and is not adjusted for leap seconds. As of July 2015, TAI is ahead of UTC by 36 seconds. TAI is always ahead of GPS by 19 seconds.

- **GPS**: Global Positioning System time is the time scale maintained by the GPS satellites. The time signal is provided by atomic clocks in the GPS ground control stations. GPS time follows TAI by 19 seconds.

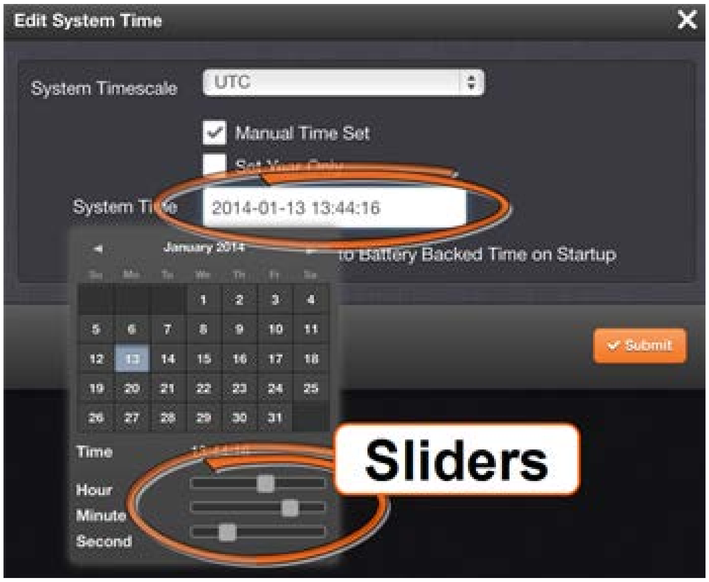
If you want to set the System Time manually, proceed with Step 5.

If you want SecureSync to use the battery-backed system time upon startup, proceed to Step 6.

Otherwise, the editing process is complete, and you can proceed to Step 7.

5. In order to override the system time with a manually set User Time, check the **Manual Time Set** checkbox.
Two additional fields will appear:

   - **Set Year Only**—Some legacy time formats do not support years. Setting this checkbox will open a data entry field to manually set the year.
   - **System Time**—If you do not select **Set Year Only**, this box will show the current time in the format: Year-Month-Day Hour:Minute:Second. To set the time manually, click anywhere in the **System Time** field. A drop-down calendar with time-setting sliders will appear:



Edit System Time

System Timescale: UTC

☑ Manual Time Set

□ Set Year Only

System Time: 2014-01-13 13:44:16

- The time in the **System Time** field will default to the current date and time. Except for testing purposes, you should not choose a date other than the current day. If you wish, you can choose an alternate day by clicking on that day in the calendar, and choose another month by using the navigation arrows on either side of the month in the calendar's heading.
- To set the time, use the *sliders* below the calendar. The time will display between the calendar and the sliders, and also next to the chosen date in the field directly above the calendar.
To close the calendar, click anywhere in the **Edit System Time** window.

If you want SecureSync to use the battery-backed system time upon startup, proceed to "Using Battery Backup Time as Startup Time" on the facing page.

Otherwise, the editing process is complete, and you can proceed to Step 7.

3. Click the **Submit** button to update the System Time, and close the window.

See also: "The Time Management Screen" on page 169.

3.5.7.6 Using Battery Backup Time as Startup Time

Upon system startup, SecureSync will, per default, not synchronize until one of the pre-defined references becomes available and valid. The functino **Synchronize to Battery Backed Time on Startup** overrides this default by declaring the battery backed time a valid reference, allowing SecureSync to transition into synchronization upon system startup, without user intervention, or waiting for external references to become available.

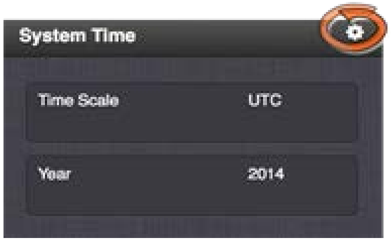
This may be useful for simulation or testing purposes, or if the synchronization state is to be reached as quickly as possible, even though the battery backed time may be less accurate than an extenal time reference.

Please note that higher priority references will take precedence over the battery backed time as soon as they become available.

Please also note that the internally maintained system time should be relatively close to the actual time, to prevent NTP synchronization problems when transitioning from one input reference to another, see also "Input Reference Priorities" on page 150.

To use battery backup time as the synchronized time at start-up:

1. Navigate to **MANAGEMENT/OTHER/Time Management**.
2. Click the GEAR icon in the **System Time** panel in the top-right corner of the **System Time** panel located on the left-hand side of the **Time Management** screen.

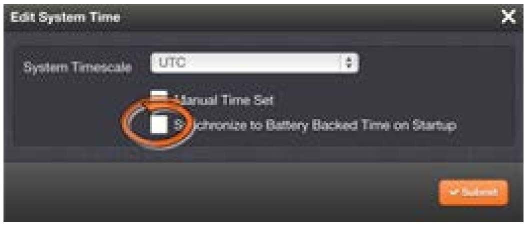


System Time

Time Scale UTC

Year 2014

3. The **Edit System Time** pop-up window will display.



Edit System Time

System Timescale UTC

□ Manual Time Set

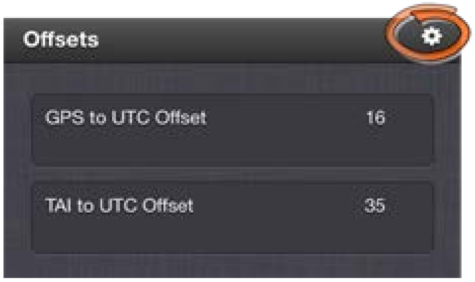
□ Synchronize to Battery Backed Time on Startup

4. Select the checkbox **Synchronize to Battery Backed Time on Startup**.
5. Click the **Submit** button.

3.5.7.7 Configuring System Time Offsets

To configure offsets to the system time:

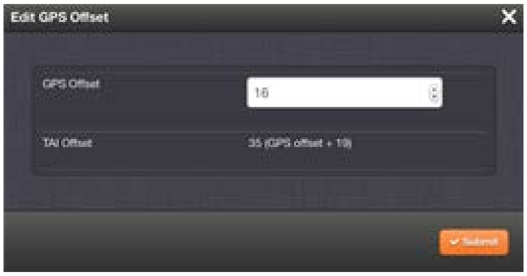
1. Navigate to **MANAGEMENT/OTHER/Time Management**.
2. Click the GEAR icon in the top-right corner of the **Offsets** panel located on the left-hand side of the **Time Management** screen.



Offsets

GPS to UTC Offset	16
TAI to UTC Offset	35

3. The **Edit GPS Offset** pop-up window will display:



Edit GPS Offset

GPS Offset	16
TAI Offset	35 (GPS offset + 19)

4. In the **GPS Offset** field enter the desired **GPS Offset** in seconds.
5. Since the GPS and TAI offsets have a fixed relationship, only the GPS offset can be set. If only the TAI offset is known, subtract 19 from it to get the GPS offset.

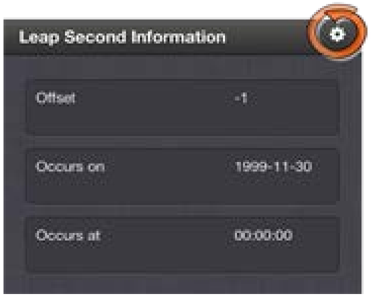
   » See also: "The Time Management Screen" on page 169.

3.5.7.8 Configuring a Leap Second Correction

To correct the System Time for a leap second:

1. Navigate to **MANAGEMENT/OTHER/Time Management**.
2. Click the GEAR icon in the **Leap Second Information** panel on the left-hand side of the

Time Management screen.

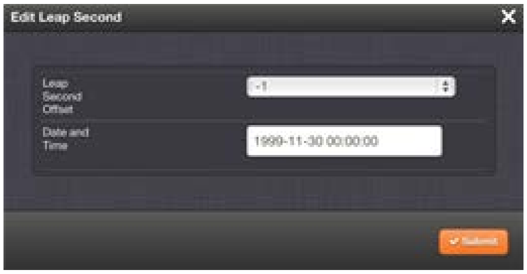


Offset -1

Occurs on 1999-11-30

Occurs at 00:00:00

3. The **Edit Leap Second** pop-up window will display.



Leap Second Offset -1

Date and Time 1999-11-30 00:00:00

4. In the **Leap Second Offset** field enter the desired GPS Offset.
5. In the **When** field, enter the date that the desired leap second should occur.
6. Click the **Submit** button at the bottom of the window.

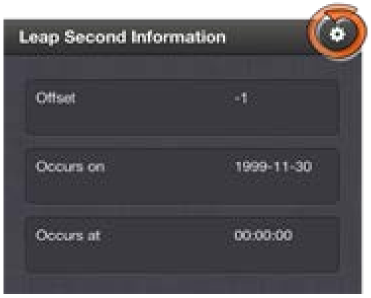
See also: "Leap Second Occurrence" on page 276.

See also: "The Time Management Screen" on page 169.

3.5.7.9 Deleting a Leap Second Correction

To delete a leap second correction:

1. Navigate to **MANAGEMENT/OTHER/Time Management**.
2. Click the GEAR icon in the **Leap Second Information** panel on the left side of the **Time Management** screen.

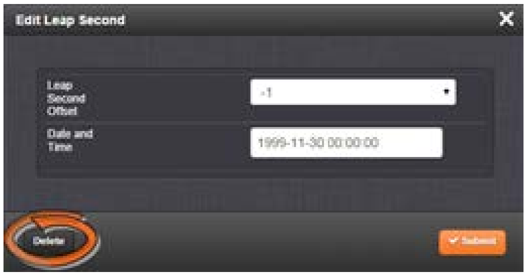


Offset -1

Occurs on 1999-11-30

Occurs at 00:00:00

3. The **Edit Leap Second** pop-up window will display:



Edit Leap Second

Leap Second Offset: -1

Date and Time: 1999-11-30 00:00:00

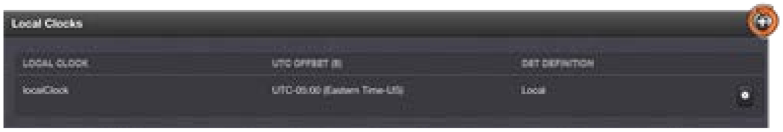
4. Click the **Delete** button at the bottom of the window.

> **Note:** The Delete button in the Edit Leap Second window will only be visible, if a leap second has been set in the first place.

3.5.7.10 Setting up a Local Clock

The **Local Clock** feature allows maintaining several times which reflect a time offset, thereby accounting for Time Zone and DST (Daylight Savings Time) correction.

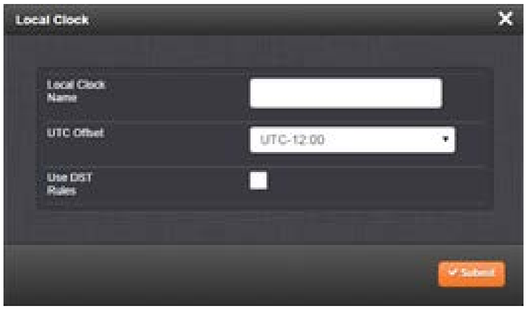
1. Navigate to **MANAGEMENT/OTHER/Time Management**.
2. Click the PLUS icon in the **Local Clocks** panel in the **Time Management** screen.



Local Clocks

LOCAL CLOCK	UTC OFFSET (I)	DST DEFINITION
localClock	UTC-05:00 (Eastern Time-US)	Local

3. The **Local Clock** pop-up window will display.



Local Clock

Local Clock Name:

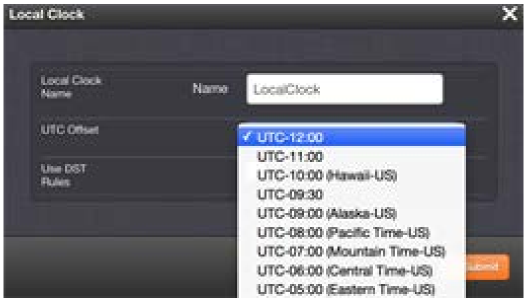
UTC Offset: UTC-12:00

Use DST Rules: □

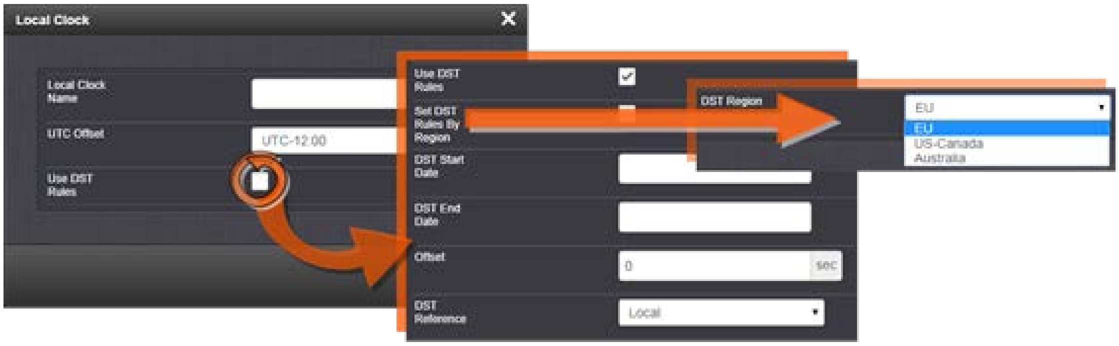
4. Enter a **Name** for your local clock.
   - The name must be between 1 and 64 characters long; spaces are allowed.
   - The name can be any meaningful name that helps you know your point of reference (for example: “New York”, “Paris” or “Eastern HQ”, etc.).

   - This name will be used as cross-reference drop-down in the applicable Input or Output port configuration. Please note the following limitations apply to this option:
      - Acceptable characters for the name include: A-Z, a-z, 0-9 and (-+_) and spaces are converted to underscores because the name must be a single word.

5. In the **UTC Offset** field, choose a **UTC Offset** from the drop-down list.



- All of the **UTC Offset** drop-downs are configured as UTC plus or minus a set number of hours.
- Examples for the US: For **Eastern**, choose UTC-05:00; for **Central**, choose UTC-06:00; for **Mountain**, choose UTC-07:00; and for **Pacific**, choose UTC-08:00.
- If you wish to use DST (Daylight Savings Time ["Summer Time"]) rules, click the **Use DST Rules** box. Otherwise the time for the local clock will always be standard time.
  DST options will appear in the **Local Clock** window:



- **Set DST Rules by Region**–Check this box to apply regional DST rules. A regions drop-down menu with the following options will display:
   - **EU (Europe**)–For if your location complies with the European DST Rule. This rule differs from all other rules because the DST changes occur based on UTC time, not local time (all time zones in Europe change for DST at precisely the same time relative to UTC, rather than offset by local time zone).
   - **US-Canada**–For if your location complies with the USA’s DST Rule (as it was changed to back in 2006, where the “DST into” date is the Second Sunday of March

and the “DST out” date is the first Sunday of November).

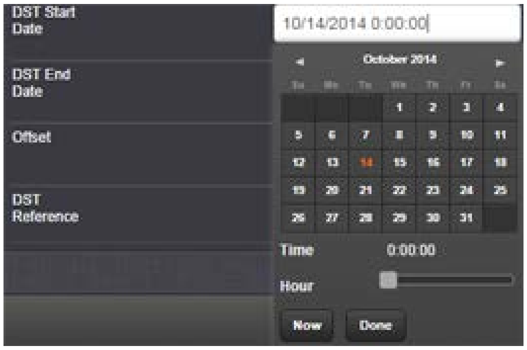
- **Australia**.

Note: If a pre-configured rule DST rule happens to be changed in the future (like the change to the US DST rule in 2006), this option allows the DST rules to be edited without the need to perform a software upgrade for a new DST rule to be defined. Select this drop-down and enter the DST parameters for the new rule.

- **DST Start Date & End Date**–Click anywhere in the **DST Start Date** field to *manually* select a start day&time, and/or end day&time for DST.

Note: The option of a manually defined DST is provided for those customers who may be in a location that does not follow any of the pre-configured DST rules. You can input start time, end time and the hour to change for the daylight saving. By selecting this option, the DST rule can be custom defined based on the weekday, week, and month of the local time you defined for this interface.

- A calendar and an hour slider will display:



DST Start Date: 10/14/2014 0:00:00

Time: 0:00:00

  - Choose a date in the calendar, and an hour with the slider.
  - The date followed by the time will display in the **DST Start Date** field. The time will display in the **Time** field between the calendar and the **Hour** slider.
  - Clicking the **Now** button will make the current time the start of DST.
  - Clicking the **Done** button will close the calendar, and accept the chosen day&time.

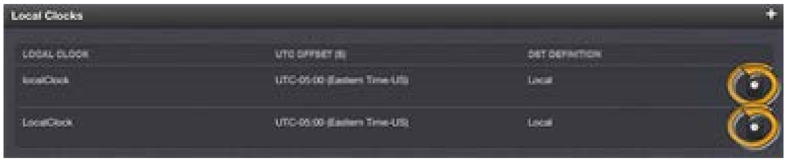
- **Offset**–In seconds. Use this field to manually define your local clock’s DST offset.
- **DST Reference**–When using a **Local Clock** with an input reference (such as IRIG input, in order to provide proper internal conversion from one Timescale to another, SecureSync needs to know if the input time is in Local Timescale or UTC Timescale. Select “Reference is **Local** time” or “Reference is **UTC**” depending on the Timescale of the Input reference this Local Clock is being used with. Additional Local Clocks may need to be created if multiple input Timescales are being submitted.

6. Click the **Submit** button at the bottom of the window. Your local clock will appear in the **Local Clocks** panel.

3.5.7.11 Local Clock: Changing Settings/Deleting

To change the settings of a Local Clock, or delete a Local Clock:

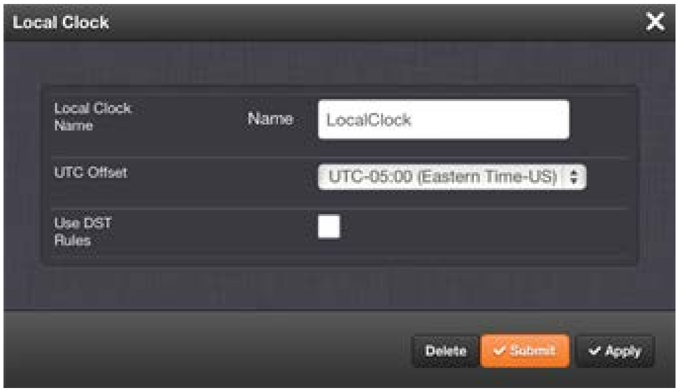
1. Navigate to **MANAGEMENT/OTHER/Time Management**.
2. In the **Local Clocks** panel, click the desired GEAR icon.



Local Clocks

LOCAL CLOCK	UTC OFFSET (S)	DST DEFINITION
localClock	UTC-05:00 (Eastern Time-US)	Local
LocalClock	UTC-05:00 (Eastern Time-US)	Local

3. The **Local Clock** pop-up window will display.



Local Clock

Local Clock Name — Name: LocalClock

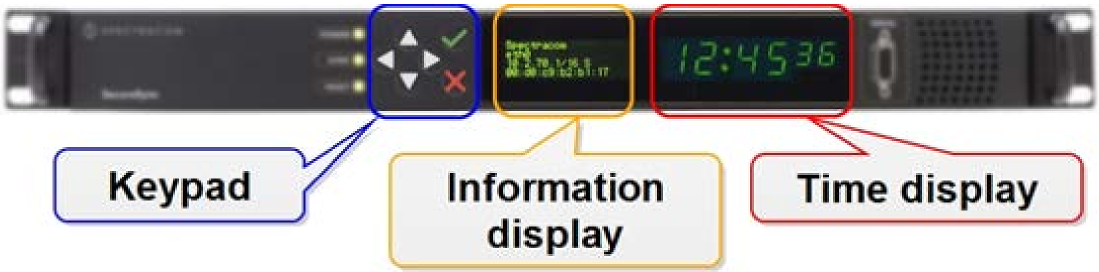
UTC Offset: UTC-05:00 (Eastern Time-US)

Use DST Rules: □

4. Apply the desired changes (see "Setting up a Local Clock" on page 176 for more information.)
5. Click **Submit**, or **Delete**.
6. The **Local Clocks** panel will reflect the change(s).

3.5.8 Front Panel Configuration

The front panel of the SecureSync unit comprises three elements which can be configured via the SecureSync Web UI:



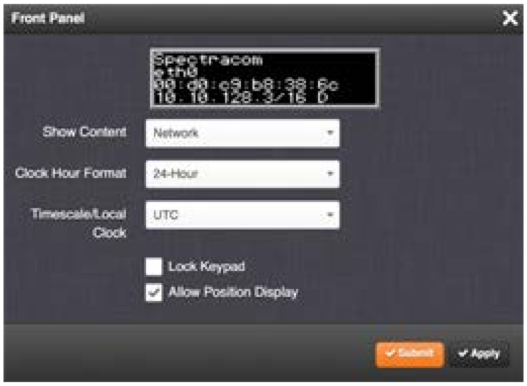
- The **keypad**, which—in conjunction with the information display—can be used to access SecureSync's main functions directly via the unit's front panel. To prevent inadvertent keypad operation, it can be locked and unlocked from the Web UI. Learn more about front panel keypad operation: "Using the Keypad and Information Display" on page 30.
- The **information display**: A 4-line LCD display that can be configured to display different screens, and that is used in conjunction with the keypad.
- The LED **time display** which can be configured to show the current time (UTC, TAI, GPS or Local time scale) in either 12- or 24-hour format. By factory default, the LED will display UTC time in 24-hour format (such as displaying “18” at 6 PM).

3.5.8.1 Accessing the Front Panel Setup Screen

SecureSync's Web UI allows you to configure the main elements on the front panel of the unit, and to see an image of the information currently displayed on the 4-line front panel information display.

To access the front panel configuration window:

1. Navigate to **MANAGEMENT > OTHER: Front Panel.**
2. The **Front Panel** configuration window will display:



Front Panel

```
Spectracom
eth0
00:d0:c9:b8:38:6c
10.10.128.3/16 D
```

Show Content: Network

Clock Hour Format: 24-Hour

Timescale/Local Clock: UTC

□ Lock Keypad

☑ Allow Position Display

- Next to the graphical near-real time representation of the 4-line front panel information display, the following functionality can be accessed in this window:
  - **Show Content**—A drop-down of the options that can be shown on the information display. This field determines what is normally displayed in the information display when the keypad is not in use. The desired screen to display can be selected with either the keypad or with this drop-down field. While switching from one screen to another either “Keypad Locked” or “Keypad Unlocked” will be displayed on the LCD (depending on the setting of the keypad “Lock” field).
  - **Clock Hour Format**—This option configures the time display on the front panel as either in 12-hour or 24-hour format.
  - **Timescale/Local Clock**—This option configures the time scale for the LED time display. The available options are:

    - **UTC** (temps universel coordonné)
    - **TAI** (Temps Atomique International)
    - **GPS**: the raw GPS time as transmitted by the GNSS satellites (as of July, 2015, GPS time is 17 seconds ahead of UTC time).
    - The **Local** timescale, which allows a Local Clock to apply a time offset for Time Zone and DST correction. This option is only available, if a Local Clock has been enabled under **MANAGEMENT/OTHER/Time Management**.

> Note: If GPS or TAI time is used, then the proper timescale offsets must be set on the MANAGEMENT/OTHER/Time Management page.

- **Lock Keypad**—If desired, the front panel keypad can be locked to prevent inadvertent operation. Locking and unlocking of the keypad can be performed either with the keypad itself, or by means of this check box. [DEFAULT = this box is NOT checked, i.e. the keypad is NOT locked]
- **Allow Position Display**—As per DEFAULT, SecureSync allows to display the geographic position of your antenna in the information display, if so configured under the **Show Content** selection menu. The option to display the position can be disabled by unchecking this box. This will cause the information display on the front panel of the unit to show the message "Not Enabled" when selecting and applying the **Position** option via the keypad.

3.5.8.2 Configuring the Front Panel Information Display

To configure the SecureSync 4-line LCD information display on the front panel of the unit:

1. Navigate to the **MANAGEMENT/OTHER/Front Panel** configuration window.
2. In the **Show Content** field, select the display you want from the drop-down list. The options are:
    - **Rotate**—This option enables sequential rotation of the content displayed in the information display as long as the keypad is not in use. Content will rotate through all enabled content for installed options. When **Rotate** is selected, a further option appears on the screen:
        - **Rotation Delay**—This option sets the duration in seconds for content display during rotation before the next content screen is displayed. [Range = between 1 and 30 seconds]
    - **Network** (the default)—This option displays the current network settings. If an option card is installed that provides additional network interfaces, there will be additional network choices (i.e., Network: eth0, Network: eth1, etc.).
    - **Status**—This option displays current key status indications (such as NTP Stratum level, TFOM -"Time Figure of Merit", Sync status and Oscillator lock status).

- **Position**–This option displays latitude, longitude and elevation of the antenna.
- **Day of Year**–This option displays the day of year (such as “Day of Year 104”).
- **GNSS**–This option displays the number of satellites currently being used (and the strongest signal strength out of all these satellites) and their relative signal strengths of all the receiver channels that are tracking satellites as a bar graph.
- **Date**–This option displays the current date (such as “16 November 2014”).

> Note: The date is based on the timescale configured for the information display. It is possible that a date other than “today’s local date” may be shown, if the configured time scale has already rolled over to its new date, though local time has not yet rolled over to its new date.

- **Keys**–This option is applicable to the SAASM GPS receiver option module only. The front panel will display “NOT SUPPORTED” unless a SAASM receiver is installed.
- **None**–This option configures the front panel 4-line information display to remain blank unless the keypad is unlocked and in use.

3. In the **Timescale/Local Clock** field, choose the timescale or local clock you wish to use as the time reference for the time shown on the front panel time display. The options available are:
   - **UTC**
   - **TAI**
   - **GPS**
   - Any **Local Clocks** you have set up. The Time Zone and DST rules, as configured under**Time Management/Local Clocks** will now be applied to the front panel time display. For more information on Local Clocks see "Setting up a Local Clock" on page 176.

> 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.

4. Select the **Lock Keypad** check box if you want to lock the front panel keypad. [DEFAULT = unlocked (unchecked)]
5. Deselect the **Allow Position Display** checkbox if you do not want to enable the option to display position data on the front panel information display. See also Allow Position Display.

3.5.8.3 Locking/Unlocking the Front Panel Keypad

To lock or unlock the keypad on the front panel of the unit (see illustration Front Panel):

1. Navigate to the **MANAGEMENT/OTHER/Front Panel** configuration window.
2. Depending on whether you want to enable or disable the keypad, check or uncheck the **Lock Keypad** checkbox.
3. Click the **Submit** button or the **Apply** button at the bottom of the window.

Note: If the keypad is unlocked, pressing any keypad key will temporarily return the information display to the “Home” menu display for keypad operation. One minute after the last keypad press, the information display will return to its configured screen.

3.5.8.4 Enabling/Disabling the Position Display Screen

To enable or disable [DEFAULT = enable] the option to display geographic position data on the information display, if so configured (see also Allow Position Display):

1. Navigate to the **MANAGEMENT/OTHER/Front Panel** configuration window.
2. Check or uncheck the **Allow Position Display** checkbox.
3. Click the **Submit** button or the **Apply** button at the bottom of the window.

3.5.9 Backing-up and Restoring Configuration Files

Once SecureSync has been configured, it may be desired to back up the configuration files to a PC for off-unit storage. If necessary in the future, the original configuration of the SecureSync can then be restored into the same unit.

The capability to backup and restore configurations also adds the ability to “clone” multiple SecureSync units with similar settings. Once one SecureSync unit has been configured as desired, configurations that are not specific to each unit (such as NTP settings, log configs, etc.) can be backed up and loaded onto another SecureSync unit for duplicate configurations.

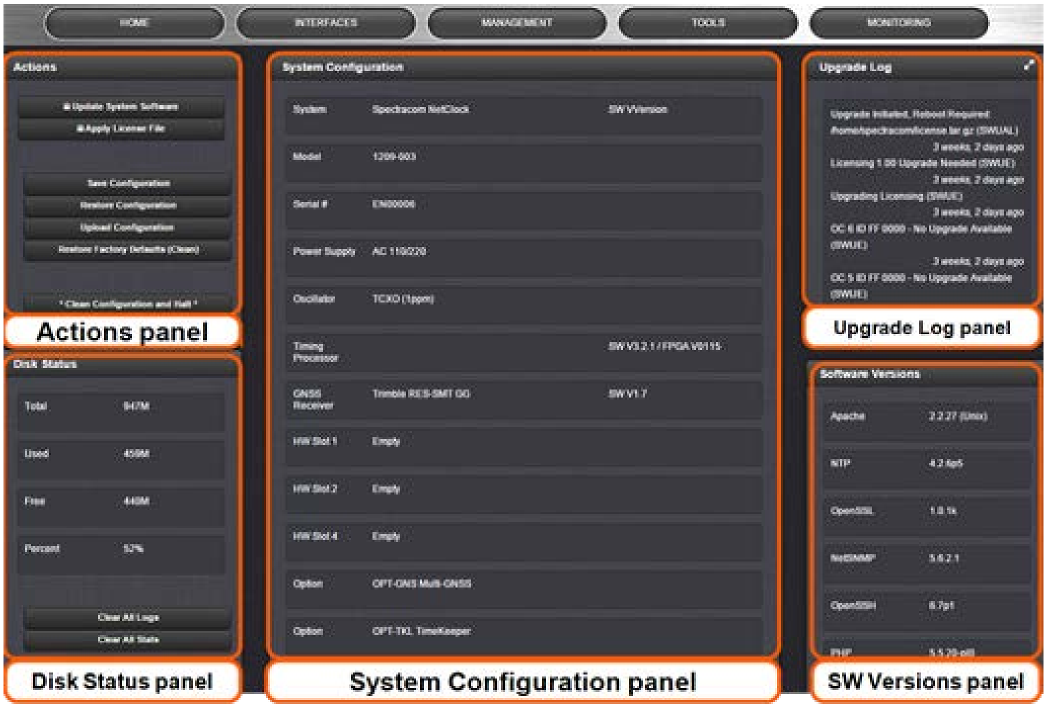
There are several configuration files that are bundled in one file for ease of handling.

Note: For security reasons, configurations relating to security of the product, such as SSH/SSL certificates, cannot be backed up to a PC.

3.5.9.1 Accessing the System Configuration Screen

To access the **System Configuration** screen:

1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. The **System Configuration** screen will display:



System	Spectracom NetClock	SW Vversion
Model	1209-003	
Serial #	EN00006	
Power Supply	AC 110/220	
Oscillator	TCXO (1ppm)	
Timing Processor		SW V3.2.1 / FPGA V0115
GNSS Receiver	Trimble RES-SMT GG	SW V1.7
HW Slot 1	Empty	
HW Slot 2	Empty	
HW Slot 4	Empty	
Option	OPT-GNS Multi-GNSS	
Option	OPT-TKL TimeKeeper	

Total	947M
Used	459M
Free	440M
Percent	52%

Upgrade Initiated, Reboot Required /home/spectracom/license.tar.gz (SWUAL)
3 weeks, 2 days ago
Licensing 1.00 Upgrade Needed (SWUE)
3 weeks, 2 days ago
Upgrading Licensing (SWUE)
3 weeks, 2 days ago
OC 6 ID FF 0000 - No Upgrade Available (SWUE)
3 weeks, 2 days ago
OC 5 ID FF 0000 - No Upgrade Available (SWUE)

Apache	2.2.27 (Unix)
NTP	4.2.6p5
OpenSSL	1.0.1k
NetSNMP	5.6.2.1
OpenSSH	6.7p1
PHP	5.5.20-pl0

The **System Configuration** screen consists of 5 panels:

The Actions panel

The **Actions** panel is used for updating the system software, managing license files, saving and restoring the configuration files, and restoring the factory defaults.

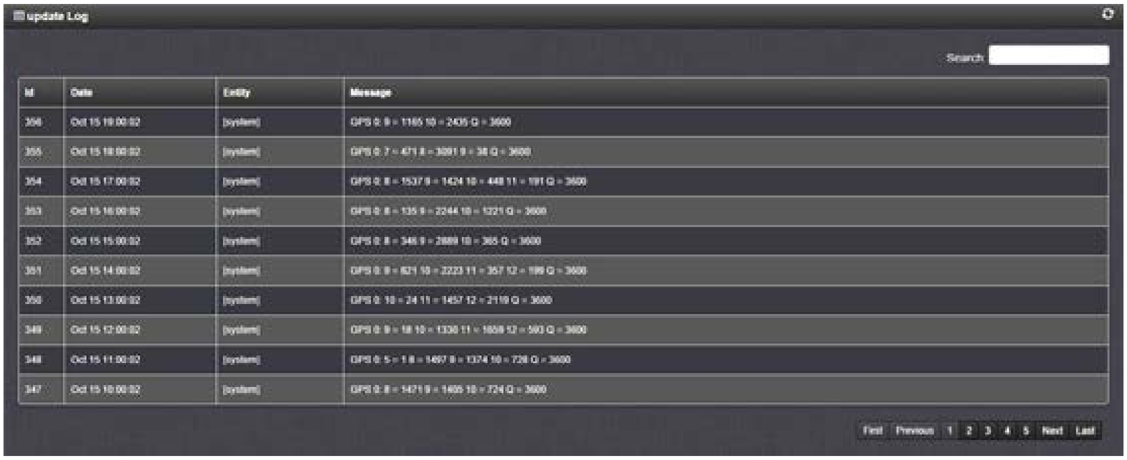
The System Configuration panel

The **System Configuration** panel provides the following information:

- **System**–The model name of this unit, and the software version currently installed.
- **Model**–The model number of this unit.
- **Serial Number**–The serial number of this unit.
- **Power Supply**–The type of power supply installed in this unit. This can be AC, DC or both.
- **Oscillator**–The type of internal timing oscillator installed in this unit.
- **GNSS Receiver**–The GNSS receiver in use with this unit.
- **HW Slots 1-6**–The Option Cards installed in this unit.

The Upgrade Log panel

The upgrade log is a running log of system upgrades, used for historical and troubleshooting purposes. It can be expanded by clicking on the DIAGONAL ARROWS icon in the top-right corner:



Id	Date	Entity	Message
356	Oct 15 19:00:02	[system]	GPS 0: 9 = 1165 10 = 2435 Q = 3600
355	Oct 15 18:00:02	[system]	GPS 0: 7 = 471 8 = 3091 9 = 38 Q = 3600
354	Oct 15 17:00:02	[system]	GPS 0: 8 = 1537 9 = 1424 10 = 448 11 = 191 Q = 3600
353	Oct 15 16:00:02	[system]	GPS 0: 8 = 135 9 = 2244 10 = 1221 Q = 3600
352	Oct 15 15:00:02	[system]	GPS 0: 8 = 346 9 = 2889 10 = 365 Q = 3600
351	Oct 15 14:00:02	[system]	GPS 0: 9 = 821 10 = 2223 11 = 357 12 = 199 Q = 3600
350	Oct 15 13:00:02	[system]	GPS 0: 10 = 24 11 = 1457 12 = 2119 Q = 3600
349	Oct 15 12:00:02	[system]	GPS 0: 9 = 18 10 = 1330 11 = 1659 12 = 593 Q = 3600
348	Oct 15 11:00:02	[system]	GPS 0: 5 = 1 8 = 1497 9 = 1374 10 = 728 Q = 3600
347	Oct 15 10:00:02	[system]	GPS 0: 8 = 1471 9 = 1405 10 = 724 Q = 3600

Each log entry is comprised of a unique ID, the date the entry was created, the originator of the entry, and the actual message. Refresh the log by clicking the CIRCLE ARROWS icon in the top-right corner. Go to the First, Last, or Previous entries by clicking the corresponding buttons in the bottom-right corner.

The Disk Status panel

The Disk Status panel provides information on the Compact Flash card memory usage. This information is relevant for troubleshooting purposes, and when preparing the system for a software update.

The Software Versions panel

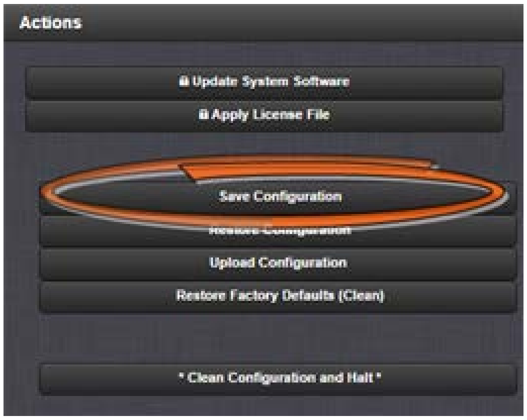
This panel provides version information on the different SW components utilized by the system.

3.5.9.2 Backing Up the System Configuration Files

To back up the system configuration files:

1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.

2. In the **Actions** panel, click the **Save Configuration** button.

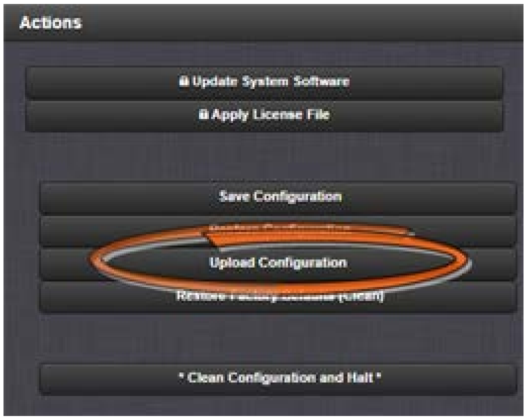


3. Click **OK** in the message window that displays.
4. Save the configuration file to a directory where it will be safe. SecureSync simultaneously saves a file at `/home/spectracom/xfer/config/`SecureSync`.conf`.

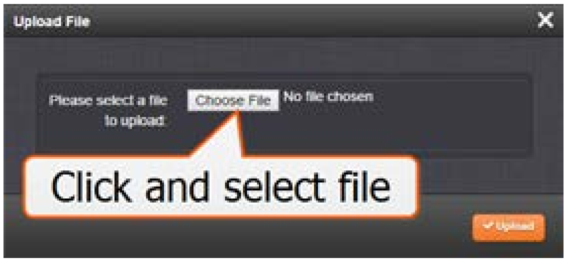
3.5.9.3 Uploading Configuration Files

To upload configuration files from a PC:

1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. In the **Actions** panel, click the **Upload Configuration** button.



3. Click **Choose File** in the window that displays, and navigate to the directory on your PC where the bundled file is stored.



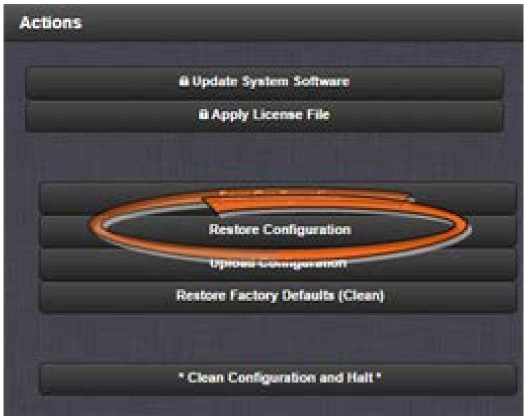
4. Click the **Upload** button. SecureSync saves the uploaded bundled file in the `/home/spectracom/xfer/config/ directory`.

Note: When uploading files remotely via long distances, or when uploading multiple files via several browser windows simultaneously, the upload process may fail to complete. In this case, cancel the upload by clicking X, and go back to Step 2.

5. To use the new configuration file for this SecureSync, click the **Restore Configuration** button, and follow the procedure described under "Restoring the System Configuration" below.

3.5.9.4 Restoring the System Configuration

1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. In the **Actions** panel, click **Restore Configuration**.



3. Click **OK** in the message window that displays. The system will restore the configuration using the bundled file stored at `/home/spectracom/xfer/config/`SecureSync`.conf`, then reboot in order to read the new configuration file. Once powered back up, SecureSync will be configured with the previously stored file.

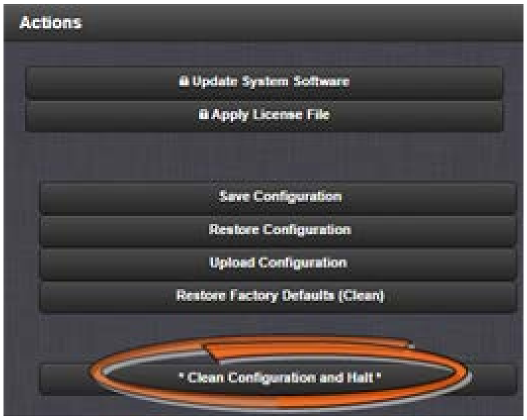
3.5.9.5 Restoring the Factory Defaults

For instructions on how to restore the SecureSync's configuration files to their factory default settings, see: "Resetting All Configurations to their Factory Defaults" on page 220.

3.5.9.6 Cleaning the Configuration Files and Halting the System

To restore the configuration files to the factory defaults and immediately halt the system:

1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. In the **Actions** panel, click ***Clean Configuration and Halt***.



3. SecureSync restores the configuration files to the factory default, and halts the system so that no changes are made to the factory default condition.

3.5.10 Oscillator Disciplining

The purpose of the internal oscillator is to provide SecureSync with an accurate and very stable frequency source. This allows SecureSync to go into a holdover mode in the event that external time or frequency references are lost or become invalid. However, the oscillator can also be used as a legitimate PPS reference during normal operation, in conjunction with an external time reference (for more information, see "Configuring Input Reference Priorities" on page 155.)

SecureSync’s internal oscillator is normally disciplined to an input reference (such as GNSS, IRIG input, 1PPS input, etc.) in order to provide the highest degree of oscillator accuracy and to account for oscillator drift. While disciplining (with a 1PPS input reference input present and valid), the oscillator’s output frequency is monitored and based on the measured frequency, the oscillator is steered to maintain a very accurate 10 MHz output. If no valid 1PPS input references are present (or input references are present but not considered valid), the oscillator will be in Freerun mode instead.

If no external input reference such as GNSS, IRIG, etc. is available (or is temporarily lost), SecureSync may become an NTP Stratum 2 or higher reference. If so configured, SecureSync can use a reference such as an NTP daemon, or TimeKeeper, referred to as a **Host Reference**. If the Host Reference becomes active, it will automatically take over the disciplining of the oscillator. This built-in functionality is referred to as **Host Disciplining**. (See also **Phase Error Limit** under

"Oscillator Status Panel" on page 191 for more information on how it is possible to influence the Host Disciplining.)

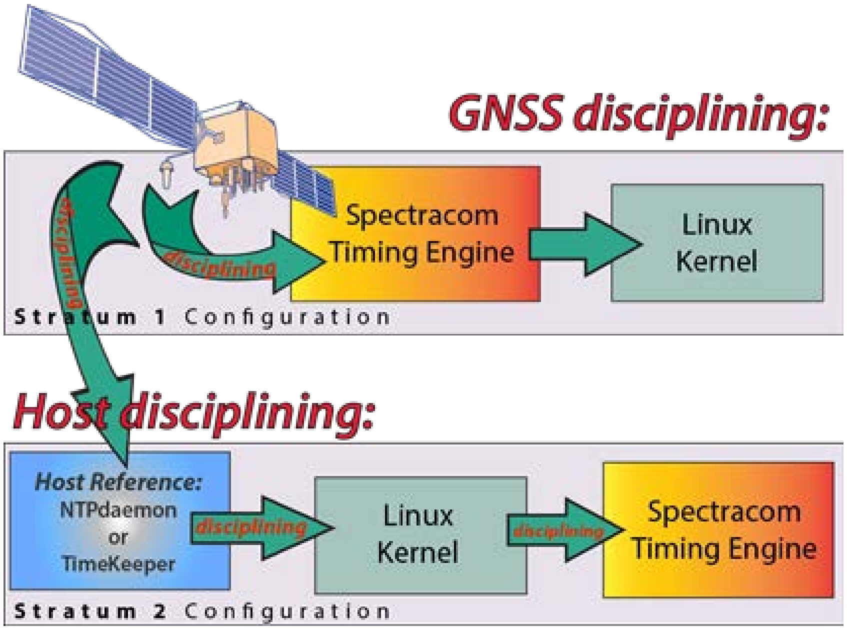


Figure 3-6: Host disciplining

Note: Host disciplining is not supported with SecureSync units that are equipped with Rubidium oscillators.

The Oscillators Settings page provides the user with some control of the disciplining process. This page is also used to configure the length of time SecureSync is allowed to remain in the Holdover mode when all references are lost.

3.5.10.1 Oscillator Types

SecureSync units are available with different types of internal oscillators:

- **TCXO** (Temperature-Compensated Crystal Oscillator)
- one of two different types of **OCXO** (Oven-Controlled Crystal Oscillator) oscillators, or
- one of two different types of **Rb** (Rubidium) oscillators.

The two different types of OCXO oscillators are a precision OCXO oscillator and a high-precision (low phase noise) OCXO oscillator. The two different types of Rubidium oscillators are a precision Rubidium oscillator and a low-phase noise Rubidium oscillator. All of these internal oscillators are self-calibrating and can be disciplined to a 1PPS input reference for maximum accuracy.

Because of its high degree of stability, the Rubidium oscillator provides the greatest ability to extend the hold-over period when input references are not present. Extending the hold-over period allows the unit to provide very accurate and useable time stamps and a 10 MHz output for a longer period of time once time synchronization has been lost.

> **Note:** Oscillators are installed at the factory, in accordance with order specifications; an oscillator cannot be swapped/retrofitted later in the product life cycle.

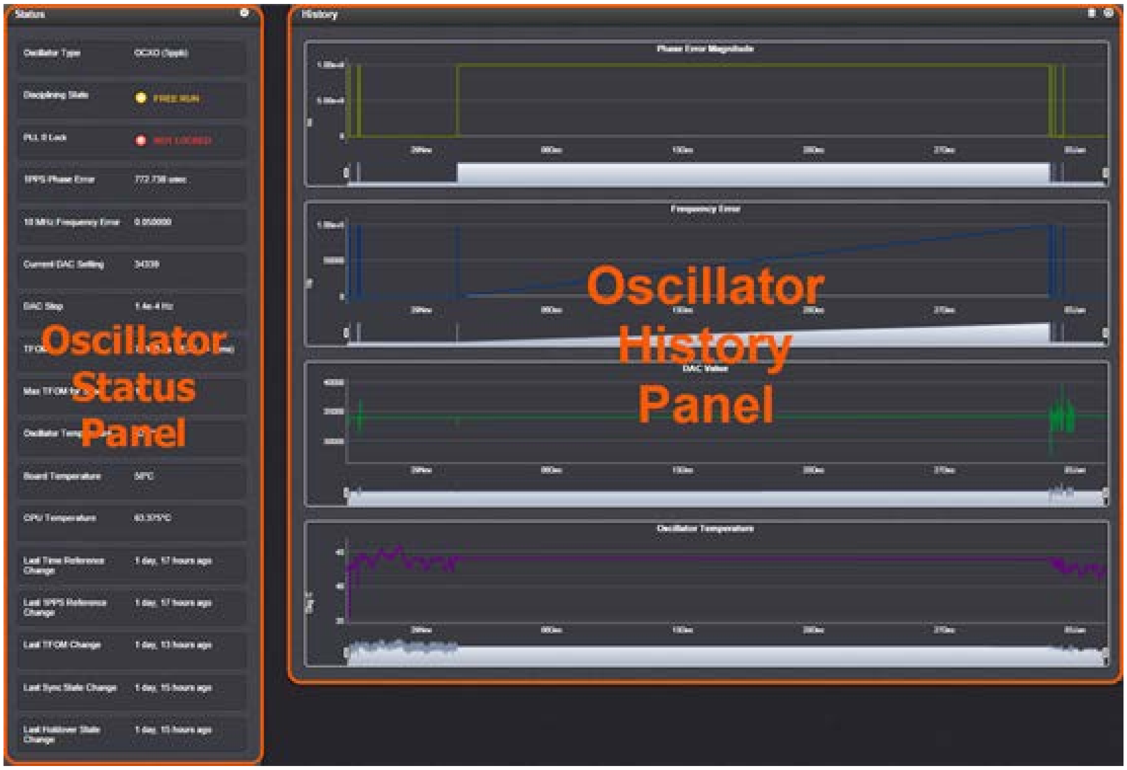
The Rubidium oscillator is atomic in nature but requires no MSDS (Material Safety Data Sheet).

For additional information on oscillator accuracies, see "10 MHz output – oscillator accuracies" on page 12.

> **Note:** External Oscillator: It is possible for an external oscillator to be locked to SecureSync's 10 MHz output via an external PLL, with the lock state of the external PLL monitored by SecureSync. Contact Spectracom for more information.

3.5.10.2 The Oscillator Disciplining Screen

1. Navigate to **MANAGEMENT > OTHER: Disciplining**.
2. The **Oscillator Management** screen will display. It consists of two panels:



Status

Oscillator Type	OCXO (5ppb)
Disciplining State	● FREE RUN
PLL 0 Lock	● NOT LOCKED
1PPS Phase Error	772.738 usec
10 MHz Frequency Error	0.000000
Current DAC Setting	34339
DAC Step	1.4e-4 Hz
TFOM	[illegible]
Max TFOM for [illegible]	[illegible]
Oscillator Temp[illegible]	[illegible]
Board Temperature	58°C
CPU Temperature	63.375°C
Last Time Reference Change	1 day, 17 hours ago
Last 1PPS Reference Change	1 day, 17 hours ago
Last TFOM Change	1 day, 13 hours ago
Last Sync State Change	1 day, 15 hours ago
Last Holdover State Change	1 day, 15 hours ago

Oscillator Status Panel

This panel provides comprehensive information on the current status of SecureSync's timing state.

- Oscillator Type: See "Oscillator Types" on page 189.
- Disciplining State: State of oscillator control and disciplining; indicates whether or not the internal oscillator is currently being disciplined (steered to an input reference). The states are: "Warm up", "Calibration", "Tracking Setup", "Lock State", "Freerun", and "Fault".
- 1PPS Phase Error: A tracking measurement [scaled time, in ns, or ms] of the internal 1PPSs' phase error with respect to the selected input reference. Long holdover periods or an input reference with excessive jitter will cause the phase error to be high. The oscillator disciplining control will gradually reduce the phase error over time. Alternatively, restarting the tracking (see "Restart Tracking" under "Oscillator Disciplining" on page 188) manually, or automatically via a pre-set Phase Error Limit, will quickly reduce the phase error.
- 10 MHz Frequency Error: An internal estimated calculation (in Hertz) of the internal oscillator's frequency error, based on the phase accuracy error at the beginning and end of a frequency measurement window (the length of this window will vary depending upon the type of oscillator installed and the oscillator adjustment algorithm).
- Current DAC Setting: Current DAC value, as determined by the oscillator disciplining system. The value is converted into a voltage that is used to discipline the oscillator. A stable value over time is desirable and suggests steady oscillator performance (see also the graph in the History Panel).
- DAC Step: Step size for adjustments to the internal oscillator, as determined by the oscillator disciplining system. Larger steps = quicker, but coarser adjustments. The step size is mainly determined by the type of oscillator.
- TFOM: The Time Figure of Merit is SecureSync’s estimation of how accurately the unit is synchronized with its time and 1PPS reference inputs, based on several factors, known as the Estimated Time Error or ETE. 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 TFOM range is 1 through 15.
- Max TFOM for Sync: Value, as set under "Oscillator Disciplining Setup" on the next page
- Temperature(s): Three temperatures are displayed:
  - **Oscillator** temperature, which has an effect on oscillator accuracy, and therefore can be used to interpret oscillator performance.
  - **Board** temperature (measured on the main board, also referred to as 'System temperature')
  - **CPU** temperature

  Ambient temperature has an effect on the accuracy of the oscillator, and therefore—in conjunction with other relevant parameters—can be used to interpret oscillator performance. The temperature data is also logged. Note that older SecureSync units may not be equipped with temperature sensors yet. (Can be retrofitted, please contact Spectracom.)

- Last Time Reference Change: [Timestamp: Last occurrence]
- Last 1PPS Reference Change: [Timestamp: Last occurrence]
- Last TFOM Change: [Timestamp: Last occurrence]
- Last Sync State Change: [Timestamp: Last occurrence]
- Last Holdover State Change: [Timestamp: Last occurrence]

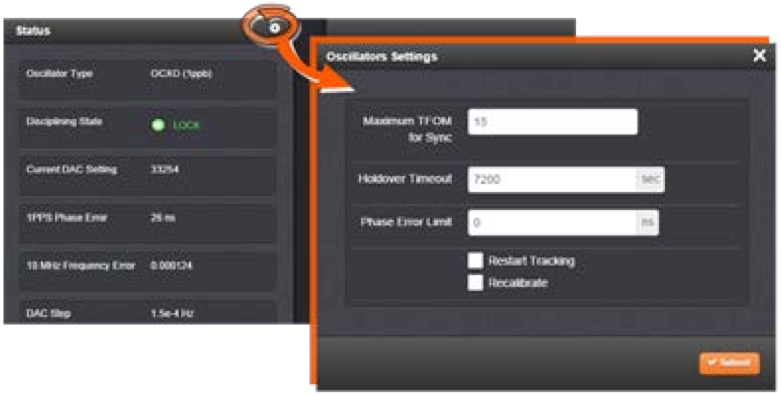
Oscillator History Panel

The graphs in the History Panel plot key oscillator-relevant data over time. See also above, and under "Oscillator Monitoring via Graphs" on page 194.

- Phase Error Magnitude
- Frequency Error
- DAC Value
- Oscillator Temperature (if equipped with temperature sensor).

3.5.10.3 Oscillator Disciplining Setup

1. To configure the oscillator settings, navigate to **MANAGEMENT > OTHER: Disciplining**.
2. Click the GEAR icon at the top of the **Status** panel. The **Oscillators Settings** window displays:



Status

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

3. Populate the fields:
   - **Maximum TFOM for Sync**: When TFOM (Time Figure of Merit, see below) is greater than Max TFOM, disciplining will still be attempted against the selected reference to improve the TFOM. If the condition persists, the system will transition to holdover, and eventually out of sync. When disciplining is performed such that TFOM is no longer greater than max TFOM, the system will transition back into sync.

     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. 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 TFOM range is 1 through 15. You may refer to the following for the TFOM to ETE conversions:

Reported 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 µsec
5	1 µsec < ETE <= 10 µsec
6	10 µsec < ETE <= 100 µsec
7	100 µsec < 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

Figure 3-7: TFOM ➔ ETE conversion

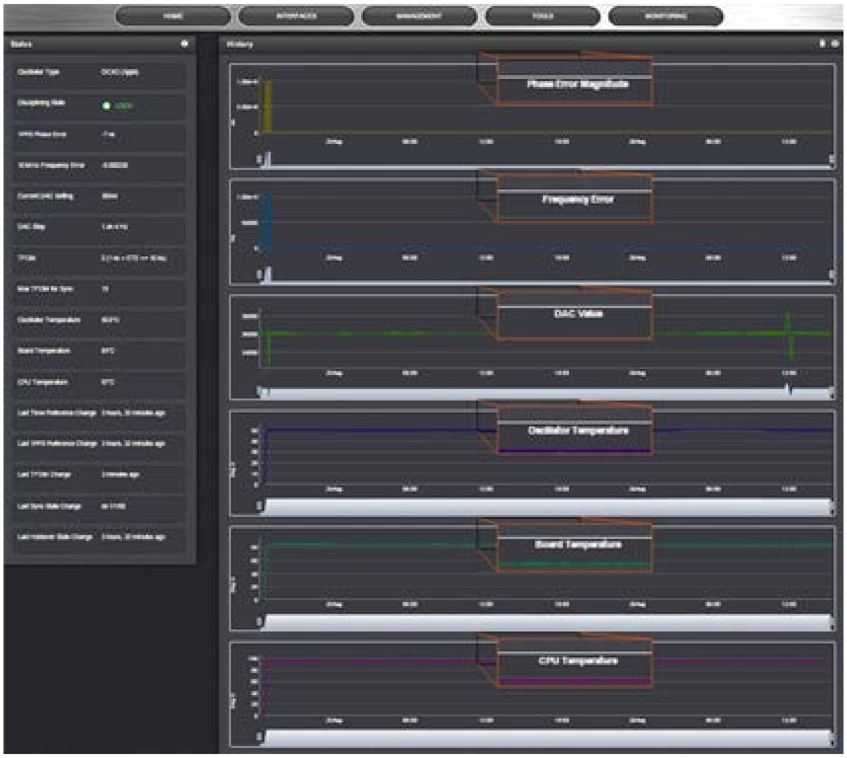
- **Holdover Timeout(s)**: The default is 7200 s (= 2 hours).
  For more information on holdover timeouts, see "Typical Holdover lengths in seconds" on page 197. For additional information on holdover, see "Holdover Timeout" on page 196.
- **Phase Error Limit**: Setting a limit (valid for +/-) for the phase error between external 1PPS reference and system 1PPS will cause the disciplining tracking to restart automatically (after a few minutes delay), if the limit is exceeded, in order to quickly re-align the system 1PPS with a reference.
  [Default=0 (disables the feature)].
  For more information on phase error, see under "Oscillator Status Panel" on page 191.
  If you are using a Host Reference as a primary or backup reference, for improved performance it is recommended to set the phase error limit for NTP to a suggested value of 100000 nsec. Adjust this value as needed, based on your accuracy requirements.

- **Restart Tracking**: Check this box, and click **Submit** if you want to manually restart disciplining tracking.
  This option causes the disciplining algorithm to stop tracking the input reference and start over (as if it was just acquired). This can be useful if there is a large phase offset between reference 1PPS and system 1PPS, as it may occur when going back into sync to the external reference after a long holdover. A **Restart Tracking** will re-align the system 1PPS with the reference 1PPS very quickly, but may cause the 1PPS output to jump.
- **Recalibrate**: In rare cases, existing calibration data may no longer be suitable to calibrate the oscillator. This function will delete the existing calibration data, and begin a new calibration process (not applicable for low phase-noise Rubidium oscillators).

4. Click the **Submit** button.

3.5.10.4 Oscillator Monitoring via Graphs

The **Oscillator Management** page offers real-time graphical monitoring of SecureSync's internal timing in the **History** panel.



This panel provides the following graphs:

- **Phase Error Magnitude**: See 1PPS Phase Error
- **Frequency Error**: See 10_MHz_Frequency_Error

- **Scaled DAC Value**: See DAC Step
- **Oscillator Temperature**: For more information, see "Oscillator Status Panel" on page 191.

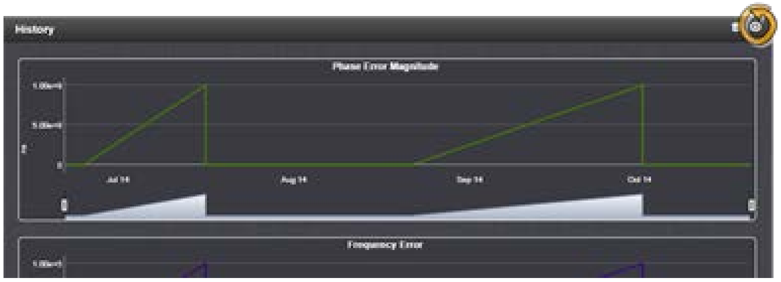
You can zoom in on any of the graphs by grabbing the handles at either end and pulling them inwards. The graph will focus in on the time interval you choose in real time.

- Clicking on the **Delete** icon in the top-right hand corner will erase all current oscillator log data.
- Clicking on the **Download** arrow icon will download the latest oscillator log data as a `.csv` file.

3.5.10.5 Oscillator Logs: Exporting/Deleting

To export, or delete the oscillator logs:

1. Navigate to **MANAGEMENT > OTHER > Disciplining**.
2. To download the log file: In the **History** panel, click the downwards pointing ARROW icon. in the top-right corner. The log file will be downloaded onto your local computer. Its name is `oscillatorStatusLog.csv`. Depending on the operating system you can open the file, or save it locally.
   To delete the log file, click the TRASH CAN icon, and confirm.



3.5.11 Holdover Mode

When input references have been supplying input to SecureSync and input from all the references has been lost, SecureSync will not immediately declare loss of time synchronization, but first will go into Holdover mode. While the unit is in Holdover mode, the time outputs are derived from an internal oscillator incrementing the System Time.

Because of the stability of the internal oscillator, accurate time can still be derived even after all the primary references are no longer valid or present. The more stable the oscillator is without an external reference, the longer this holdover period can be and have it still maintain very accurate outputs. The benefit of Holdover is that time synchronization and the availability of the time outputs is not immediately lost when input references are no longer available.

SecureSync will remain in Holdover mode until either:

a. any enabled and valid input reference becomes available again. If one or more references return and are declared valid before the Holdover period has expired (even momentarily), SecureSync exits the Holdover mode and returns to its fully synchronized state.

b. the Holdover Timeout period expires. When the Holdover Timeout period expires, declares loss of synchronization.

Holdover Mode does not persist through reboots or power cycles. If a reboot or power cycle was to occur while SecureSync is in Holdover mode, it will power-up and remain in a “not synchronized” state until at least one valid Time and 1PPS input reference becomes available again. While in this state, NTP will be Stratum 15 and outputs will not be usable. If the input references are restored and then lost or declared not valid again, SecureSync will then go back into the Holdover mode again.

Also, if the only available input reference is a manually set “user” time and SecureSync is subsequently rebooted or power cycled, time sync will be lost when SecureSync powers back-up. The time will need to be set manually again in order for SecureSync to return to its fully synchronized state. Refer to "Editing the System Time" on page 171 for more information on manually setting the time.

Holdover Timeout

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. The Holdover Timeout value can be managed from the Oscillators Settings page, accessed through the Oscillator Management screen. See "Oscillator Disciplining Setup" on page 192 for instructions on setting the Holdover Timeout value.

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.

The estimated error rates for each oscillator type, after losing the input references, are listed in the table Estimated Oscillator Error Rates during Holdover, below. Estimated typical rates are based on the oscillator being locked to a reference for 2 weeks and the ambient temperature remaining stable.

Oscillator Type	Typ. Error Rates after 4 hrs	Typ. 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 3-6: Estimated oscillator error rates during Holdover

The length of the allowed Holdover Timeout period is displayed and configured in seconds. The table below provides example conversions for typically desired Holdover periods.

Desired Holdover Length	Holdover Length (in seconds) to be entered
2 hours	7200 seconds (default value)
24 hours	86 400
7 days	604 800
30 days	2 419 200
1 year	29 030 400

Table 3-7: Typical Holdover lengths in seconds

> **Note:** Due to Leap Seconds that are periodically inserted into the UTC and Local timescales, it is not normally recommended to exceed 30 days of Holdover without an external reference that can supply Leap Second information being applied (such as GNSS).

Configuring a Holdover value exceeding 30 days could result in a one second time error in the UTC or Local timescales until an external reference (GNSS or IRIG input) is restored or a manually configured Leap Second is asserted by a user (leap seconds do not affect the GPS and TAI time scales).

If no external references (such as GNSS or IRIG) are available when a Leap Second is scheduled to occur, manual Leap Seconds can also be applied to the UTC or Local time base in the “Set Leap Second” table located in the **MANAGEMENT/OTHER/Time Management** page.

For more information on Leap Seconds, refer to "Leap Second Occurrence" on page 276 and "Configuring a Leap Second Correction" on page 174.

3.5.12 1PPS and 10 MHz Outputs

The SecureSync base model includes one 1PPS output and one 10 MHz output. Additional 1PPS and frequency outputs are available with option cards. To configure these outputs, navigate to:

- **INTERFACES/OUTPUTS,** or
- **INTERFACES/OPTION CARDS**

and select the **1PPS Output** or **10 MHz Output** you would like to see, or configure.

The 10 MHz signal is provided by the internal oscillator. External 1PPS sources ("references")—if present and valid—are utilized to discipline the oscillator, in other words to correct for oscillator drift (the oscillator cannot discipline to either NTP input, or a User set time). If no external 1PPS input references that can be used for disciplining are present, the oscillator will be in Freerun mode.

The selected 1PPS input reference (as configured with the Reference Input Priority table) is used to align SecureSync's on-time point. The on-time point serves to accurately align the outputs, such as the 1PPS output, to the correct time, based on its reference inputs.

With at least one 1PPS reference input available and considered valid, SecureSync's on-time point is initially slewed over a short duration to align itself with the 1PPS reference (this process can take a few minutes, once an input reference has become available).

SecureSync's 1PPS output is generated from the oscillator's 10 MHz output and is aligned to the on-time point. The on-time point of the 1PPS output can be configured to be either the rising or falling edge of the 1PPS signal (by default, the rising edge is the on-time point).

There is a fixed phase relationship between the 1PPS and the 10 MHz outputs, as described below:

- SecureSync equipped with **TCXO/OCXO/Low-Phase-Noise Rubidium oscillator**: With oscillator disciplining active (one or more 1PPS references available and valid) and after the on-time point has been initially slewed into alignment with the selected reference, there will always be exactly 10 million counts of the oscillator between each 1PPS output, even while in the Holdover mode (= input references are currently unavailable) and even after input references have become available again.
- SecureSync equipped with **Rubidium (Rb) oscillator**: With oscillator disciplining active (one or more 1PPS references available and valid), after the on-time point has been slewed into alignment with the selected reference, with the exception of 1PPS input reference changes occurring, there will always be exactly 10 million oscillator counts between each PPS output pulse.

  With the Rubidium oscillator installed, when a 1PPS input reference change occurs (such as switching from IRIG input to GNSS input, or switching from a reference being valid to no reference being present or valid— known as the **Holdover** mode), the oscillator counts between two 1PPS outputs may momentarily not be exactly 10 million counts. Once the reference transition has occurred, however, the counts between each PPS output pulse will return to exactly 10 million counts.

Like other types of SecureSync's signal outputs, a 1PPS output can be configured in several ways:

- **Signature Control** allows you to determine under which conditions an output signal shall be present, i.e. what SecureSync will do about a given output when an external reference is lost. See also "Signature Control" on page 201.
- The **on-time point** of the 1PPS signal: rising or falling edge

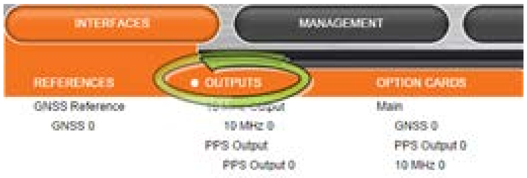
- The **pulse width**
- An **offset** can be entered to account for cable delays or other latencies.

3.5.12.1 Configuring 1PPS/10 MHz Outputs

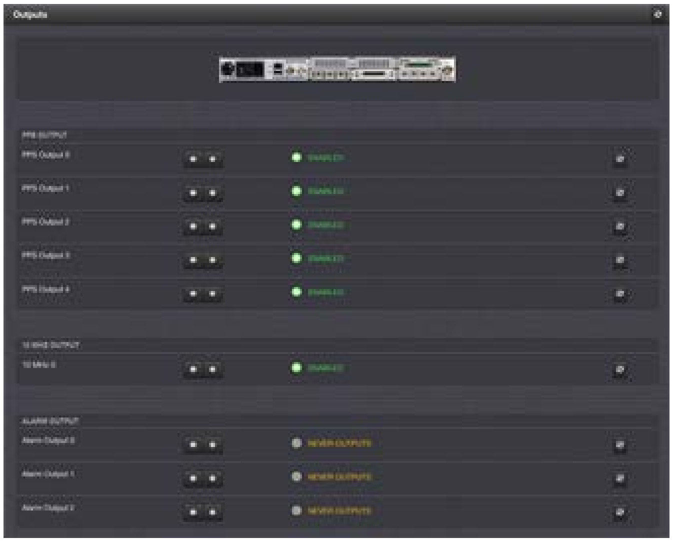
The 1PPS and 10 MHz Configuration Screens

To access the 1PPS and 10 MHz Configuration screens:

1. Navigate to **INTERFACES > OUTPUTS.**



2. The **Outputs** configuration screen will display:



Outputs

PPS OUTPUT

PPS Output 0 ENABLED

PPS Output 1 ENABLED

PPS Output 2 ENABLED

PPS Output 3 ENABLED

PPS Output 4 ENABLED

10 MHZ OUTPUT

10 MHz 0 ENABLED

ALARM OUTPUT

Alarm Output 0 NEVER OUTPUTS

Alarm Output 1 NEVER OUTPUTS

Alarm Output 2 NEVER OUTPUTS

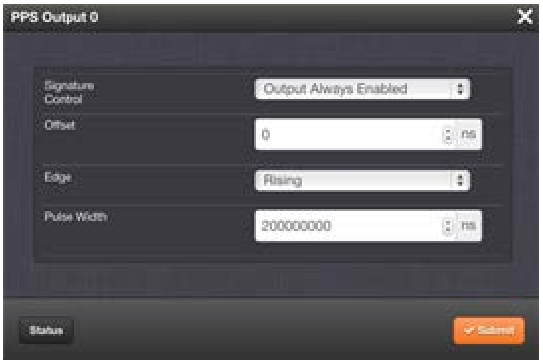
> **Note:** If you have only one output of any type, SecureSync will number that output 0. Additional outputs will be numbered 1 or above.

Configuring a 1PPS Output

To configure the 1PPS output of the main unit (i.e., not that of an option card):

1. Navigate to the **1PPS** edit screen, for example by choosing **INTERFACES/OUTPUTS** (or **INTERFACES/OPTION CARDS** for PPS outputs other than 0) to directly access the desired output, or by clicking **OUTPUTS** or **OPTION CARDS**.

2. In the latter case, click the GEAR button next to the PPS Output 0. Otherwise, click the **Edit** button.
3. The **PPS Output 0** Edit window will display, allowing the following items to be configured:



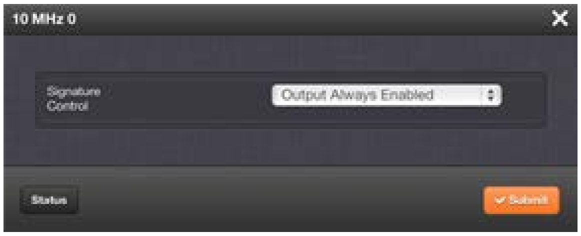
Signature Control: Output Always Enabled
Offset: 0 ns
Edge: Rising
Pulse Width: 200000000 ns

- **Signature Control**: Determines when the output is enabled. See "Signature Control" on the facing page.
- **Offset** [ns]: Allows to offset the system's 1PPS on-time point, e.g. to compensate for cable delays and other latencies [range = -500000000 to 500000000 ns = ±0.5 s]
- **Edge**: Used to determine if the on-time point of the 1PPS output is the rising or the falling edge of the signal.
  - **Rising**
  - **Falling**
- **Pulse Width** [ns]: Configures the Pulse Width of the 1PPS output.
  [range= 20 to 900000000 ns = 0.0s µs to 0.9 s]
  [default = 200 ms]

Configuring a 10 MHz Output

To configure the 10 MHz output of the main unit (i.e. not that of an option card):

1. Click the GEAR icon next to the **10 MHz** output you wish to configure.
2. The **10 MHz 0** screen will display. Choose a value from the **Signature Control** field drop-down list to determine what SecureSync shall do with the output when its input reference is lost. See also "Signature Control" on the facing page.



Signature Control: Output Always Enabled

3.5.13 Signature Control

Signature Control is a user-set parameter that controls when a SecureSync output (for example, 1PPS, or IRIG) will be present. This feature allows you to determine how closely you want to link an output to its input. This not only allows you to determine the quality of your output signal (e.g., by deactivating it, when the holdover period expires), but also offers the capability to indirectly send an input-reference-lost alarm to a downstream recipient via the presence of the signal.

> **EXAMPLES:**
>
> If you so wish, you can set signature control up such that SecureSync's built in 1PPS output goes away the moment its input reference is lost (e.g., if a valid GNSS signal is lost). Or, you can maintain your output signal while SecureSync is in holdover mode, but not in free run.

The signature-control drop-down list with its four different signature states can be found by clicking the GEAR button for any output. 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.

Table 3-8: Signature control output-presence states

Ref.	Out-of-sync, no holdover	In holdover	In-sync with external reference
I.	✓	✓	✓
II.	✗	✓	✓
III.	✗	✗	✓
IV.	✗	✗	✗

3.5.14 Configuring the GNSS Reference

With most applications, SecureSync will be setup such that it utilizes a GNSS signal as the primary (if not the only) timing reference, because the time derived from a GNSS signal is likely to be by far the most accurate time reference available. GNSS satellites (GNSS = Global Navigation

Satellite System e.g., GPS, GLONASS, Beidou, Galileo, QZSS) transmit a time signal as part of their data stream, because a very precise time is required to accurately determine your position on earth.

SecureSync has an onboard GNSS receiver that the GNSS signal received by the antenna will be supplied to.

The GNSS receiver analyzes the incoming GNSS data stream and supplies the GNSS time and 1PPS (Pulse-Per-Second) signal to SecureSync's timing system where it is processed further e.g., to enhance its stability and reliability, among other things.

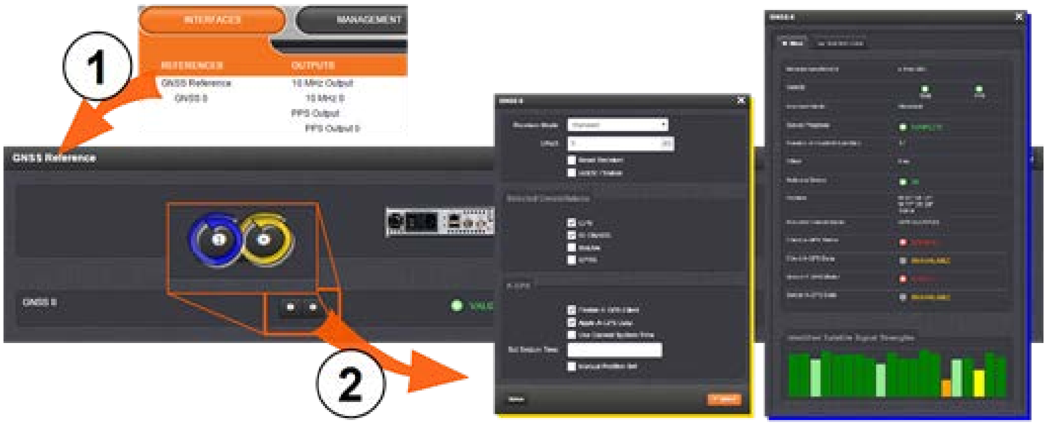
While SecureSync’s default GNSS receiver configuration will likely be adequate for most customer applications, it is advisable that you familiarize yourself with the basic configuration features so as achieve the best possible results. This is particularly true if you have only poor GNSS reception.

The GNSS Receiver settings or status can be found in these Web UI windows:

- **GNSS (0) Edit** window, and the
- **GNSS (0) Status** window.

3.5.14.1 Accessing the GNSS Reference Windows

1. Navigate to **INTERFACES** > **REFERENCES: GNSS Reference**.
2. To access the GNSS **Status** window, in the **GNSS Reference** panel, click the **INFO** button for the displayed[1] GNSS reference.
3. To access the GNSS **Edit** window, in the **GNSS Reference** panel, click the **GEAR** button.

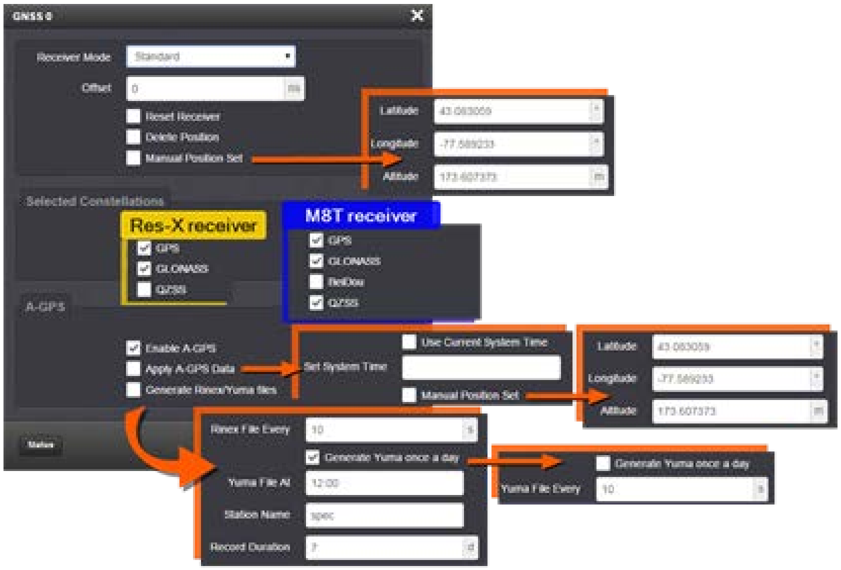


3.5.14.2 GNSS Reference Settings: Overview

The illustration below provides an overview of the available GNSS settings.

[1] Typically, there is only one GNSS reference, numbered "0". Should your equipment be configured for several receivers, they will be numbered sequentially.

Note that the options shown on your screen may be different, depending on which type of GNSS receiver is installed in your SecureSync, Res-T, Res-GG, or M8T.



GNSS 0

Receiver Mode: Standard

Offset: 0 ns

□ Reset Receiver

□ Delete Position

□ Manual Position Set

Latitude: 43.083059 °

Longitude: -77.589233 °

Altitude: 173.607373 m

Selected Constellations

Res-X receiver

☑ GPS

☑ GLONASS

□ QZSS

M8T receiver

☑ GPS

☑ GLONASS

□ BeiDou

☑ QZSS

A-GPS

☑ Enable A-GPS

□ Apply A-GPS Data

□ Generate Rinex/Yuma files

□ Use Current System Time

Set System Time:

□ Manual Position Set

Latitude: 43.083059 °

Longitude: -77.589233 °

Altitude: 173.607373 m

Rinex File Every: 10 s

☑ Generate Yuma once a day

Yuma File At: 12:00

Station Name: spec

Record Duration: 7 d

□ Generate Yuma once a day

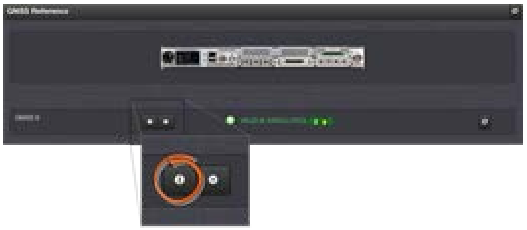
Yuma File Every: 10 s

For information on the individual settings, see "Viewing the Status of the GNSS Reference" below, and the other GNSS topics below.

3.5.14.3 Viewing the Status of the GNSS Reference

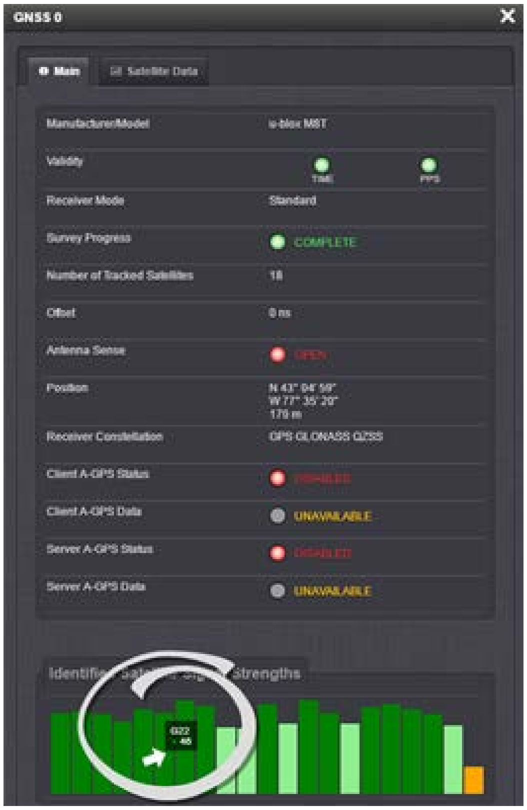
To view the current status of your GNSS reference:

1. Via **INTERFACES** > **REFERENCES: GNSS Reference**, navigate to the GNSS Reference (typically,"GNSS 0", additional GNSS references require custom hardware configuration).



2. Click the INFO button next to the **GNSS 0** reference.
3. The **GNSS 0** Status window will display. It contains two tabs:
   - **Main** (the default)

- **Satellite Data**



Manufacturer/Model	u-blox M8T
Validity	● TIME ● PPS
Receiver Mode	Standard
Survey Progress	● COMPLETE
Number of Tracked Satellites	18
Offset	0 ns
Antenna Sense	● OPEN
Position	N 43° 04' 59" W 77° 35' 20" 170 m
Receiver Constellation	GPS GLONASS QZSS
Client A-GPS Status	● DISABLED
Client A-GPS Data	● UNAVAILABLE
Server A-GPS Status	● DISABLED
Server A-GPS Data	● UNAVAILABLE

Main tab

Under the **Main** tab, the following information will display (for details, see the subsequent GNSS topics):

- **Manufacturer/Model**: The manufacturer and/or model of the GNSS receiver in your SecureSync unit.
- **Validity**: Status indicator lights for **TIME** and **1PPS** signals: “**On**” (green) indicates a valid signal, “**Off**” (red) indicates that no valid signal is available.
- **Receiver Mode:**
  - Single Satellite
  - Standard
  - Mobile
- **Survey Progress**: Current status:
  - **ACQUIRING** (x Satellites)–red
  - **SURVEYING** (x %)–yellow; remains at 1% if no satellites are in view
  - **COMPLETE**–green

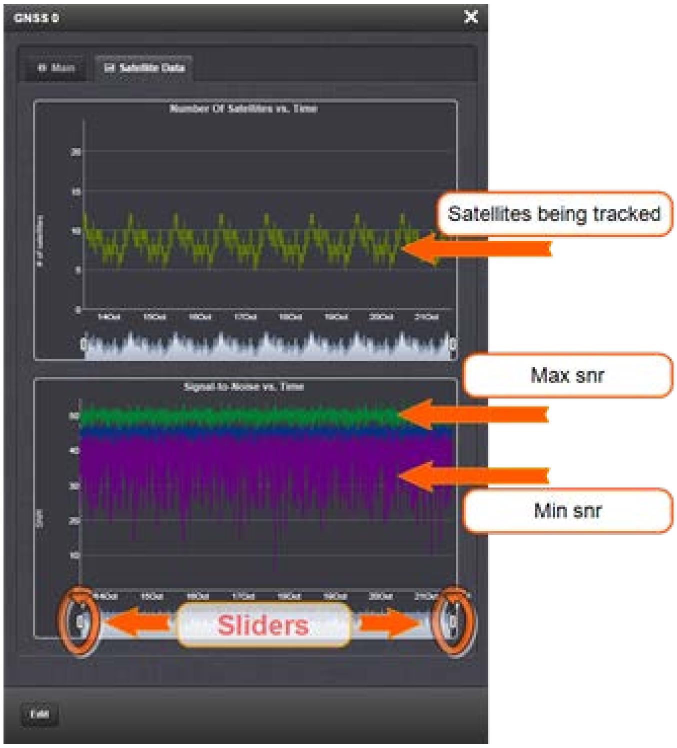
- **Number of Tracked Satellites**: The number of satellites currently being tracked.
- **Offset**: As set by the user, in nanoseconds.
- **Antenna Sense**:
    - **OK** (green)
    - **Open**: Check the antenna for the presence of an open.
    - **Short**:Check the antenna for the presence of a short.
- **Position**: SecureSync's geographic position by:
    - **Latitude**: In degrees, minutes, seconds
    - **Longitude**: In degrees, minutes, seconds
    - **Altitude**: In meters
- **Receiver Constellation**: GPS/GLONASS/Beidou/QZSS
- **Client A-GPS Status**: A-GPS is ENABLED and running, or DISABLED
- **Client A-GPS Data**: External A-GPS data is AVAILABLE, or UNAVAILABLE
- **Identified Satellite Signal Strengths**: Bar graphs for all satellites detected. Color indicates signal strength. With your mouse pointer, hover over a bar graph to display tool tip information about satellite constellation, satellite number, and signal strength.

Letter symbol	GNSS Constellation
G	GPS
R	GLONASS
E	Galileo (not yet enabled)
J	QZSS
C	BeiDou
I	IRNSS (not yet enabled)

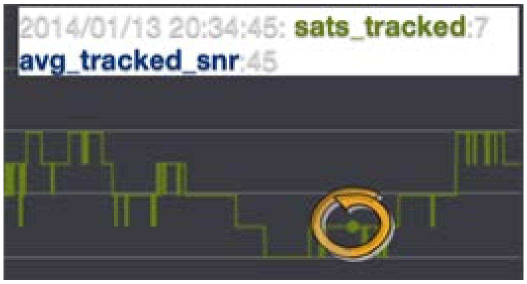
Satellite Data tab

Under the **Satellite Data** tab, there are two graphs:

- **Number of Satellites over Time**: A graphical track of how many satellites were being tracked over time.
- **SNR over Time**: A graphical track of maximum SNR, and minimum SNR.



In both graphs, to see a legend of the graphical data, and time-specific status data, click inside the graph, choosing the desired point in time. If necessary, increase the time resolution by dragging the time sliders. A pop-up window will display the legend for that graph, and the status information for the selected time.



2014/01/13 20:34:45: sats_tracked:7
avg_tracked_snr:45

3.5.14.4 GNSS Receiver Modes

When connected to a GNSS antenna that can receive a GNSS signal, SecureSync can use GNSS as an input reference. The factory default configuration allows GNSS satellites to be received/tracked with no additional user intervention required.

However, there are a few available user-configured settings for GNSS that allow a user to alter the operation of SecureSync's built-in GNSS receiver. These settings include:

- the ability to place the GNSS receiver in a **mobile mode** of operation (by default, SecureSync is optimized to operate in a stationary environment)

- the ability to apply an **offset** to account for antenna cable delays and other latencies, as well as
- the ability to **erase** the stored GNSS position information (latitude, longitude and antenna height).

The **Receiver Mode** option allows the GNSS receiver to operate in either a **stationary mode** (“**Standard**” or “Single Satellite” modes), or in a **mobile mode** environment (such as in an automobile, boat, airplane, etc.).

The Receiver Mode options are:

Standard GNSS Receiver Mode

Summary

Min. 4 satellite signals are required to determine the position and time. A survey takes 2000 seconds.

Detailed Information

The **Standard Mode** is also referred to as **Stationary Mode**. It is the most accurate, and hence the preferred GNSS receiver mode.

It therefore should always be selected, provided SecureSync's GNSS receiver will remain stationary at all times, and it will be able to track at last four satellites at all times.

In this mode a **GNSS survey** – taking about 33 minutes (2000 seconds)– will initially be performed when at least four GNSS satellites become available. During the GNSS survey, the GNSS receiver must continuously track at least four satellites. Otherwise the GNSS survey will have to start over.

Upon completion of the GNSS survey, SecureSync will go into time synchronization. Also, the GNSS receiver will lock-in the calculated GNSS position and will enter **Stationary Mode**. Once in **Stationary Mode**, the GNSS survey will only be performed again, should the equipment be relocated to another location (or if the GNSS location is manually cleared by a user).

Upon a power cycle, if the equipment has NOT been relocated, SecureSync will automatically return to **Stationary Mode** without the need to perform another GNSS survey.

In this mode, the GNSS receiver will be considered a valid input reference as long as a valid location is entered (either automatically via the GNSS survey, or manually entered by a user) and the GNSS receiver continues to track at least four qualified satellites.

Mobile GNSS Receiver Mode

Summary

SecureSync attempts to compute time in areas with poor satellite reception (such as "urban canyons"). You need to enter the antenna position under **Manual Position Set**. The calculated time may be less accurate, and less reliable than the time determined in **Standard Mode**. (NOTE: The minimum number of satellites depends on the GNSS receiver type installed in your unit.)

Detailed Information

This **Mobile Mode** (also referred to as **Continuous Mode**) should only be selected if your SecureSync unit will NOT remain stationary at all times, i.e. instead of the unit being operated in a building, it is installed in a mobile platform (such as a vehicle, ship, plane, etc.).

In this mode, no GNSS survey is performed, i.e. SecureSync will go into synchronization shortly after tracking satellites.

> **Note:** With SecureSync's GNSS Receiver configured in Mobile Mode, the specified accuracies of SecureSync will be degraded to less than three times that of Stationary Mode. Stationary Mode accuracy of the receiver is less than 50 ns to GPS/UTC (1 sigma), hence Mobile Mode is less accurate than 150 ns to GPS/UTC time (1 sigma).

Single Satellite GNSS Receiver Mode

Summary

For non-stationary applications (e.g., marine).

Detailed Information

This mode should only be used if:

- SecureSync's built-in GNSS receiver will remain stationary at all times, and if
- it is not possible for the GNSS receiver to track at least four GNSS satellites for at least 33 minutes continuously (in order to complete the GNSS survey).

The Single Satellite Mode does require a position, which the GNSS receiver most likely will not be able to obtain, if it could not complete the GNSS survey. You must therefore enter your receiver's position manually.

> **Note:** If the current position (i.e. latitude and longitude) is not known, you need to determine it by other means (see "Determining Your Position" on page 211).

SecureSync's GNSS receiver is designed to provide the most accurate time in **Standard Mode** (see above), which can only be achieved if SecureSync completed a GNSS Survey, or SecureSync's location has been entered manually, AND while tracking at least four satellites.

Hence, **Single Satellite Mode** should only be used if the GNSS survey cannot be completed.

In this mode, the GNSS receiver will be considered a valid input reference as long as:

a. a valid location has been entered by a user, and

b. the GNSS receiver continues to track at least one qualified satellite.

3.5.14.5 GNSS Receiver Offset

The **Offset** option allows you to enter an offset to the GNSS time and 1PPS reference to account for antenna cable delays or other latencies (entered and displayed in nanoseconds).

By setting the correct **Offset** value, you can offset the system’s on-time point by the **Offset** value to compensate for the antenna and in-line amplifier delays. Under typical conditions, the expected cable and amplifier delays are negligible. You can calculate the delay based on the manufacture’s specifications.

The range of the cable delay is ±50,000,000 nanoseconds. The default value is 0 nanoseconds and the resolution is 1 nanosecond.

The following formula is used to calculate the cable delay:

D = (L * C)/V

Where:

D = Cable delay in nanoseconds

L = Cable length in feet

C = Constant derived from velocity of light: 1.016

V = Nominal velocity of propagation expressed as decimal, i.e. %66 = 0.66 Value is provided by cable manufacturer.

When using LMR-400 or equivalent coax cable (such as the coax cable offered by Spectracom), this formula equates to approximately 1.2 nanoseconds of delay per every foot of cable. To calculate the Offset value (cable delay), multiply the length of the entire cable run by “1.2” and then enter this value into the Offset field.

Examples of LMR-400 (or equivalent) coax cable delays:

100 feet of cable = 120 nanoseconds of cable delay

200 feet of cable = 240 nanoseconds of cable delay

300 feet of cable = 360 nanoseconds of cable delay

3.5.14.6 Resetting the GNSS Receiver

The **Reset Receiver** command is used to erase all GNSS-relevant data from receiver memory (equivalent to a receiver cold start).

Caution: Resetting the receiver may become necessary in the rare event of internal communication issues, and is typically ONLY required if Spectracom Technical Support advises you to execute this command.

3.5.14.7 Deleting GNSS Receiver Position

The **Delete Position** option deletes the position data of the GNSS receiver in your SecureSync unit, initiating a **GNSS Self Survey** with the objective to re-determine the position of your SecureSync unit.

This function may need to be used if a SecureSync unit is relocated, and it did not self-initiate a new survey.

To ensure that no trace of position data remains on the unit, perform the following steps:

1. Disconnect SecureSync's GNSS antenna.
2. Change the **Delete Position** value to "Enabled" (the box is clicked).
3. Click the **Submit** button. SecureSync will initiate a GNSS self-survey.

Note: In Mobile Receiver Mode it is NOT possible to delete the position and start the GNSS Self Survey. This feature is only available in the Standard Mode, and the Single Satellite Mode (see "GNSS Receiver Modes" on page 206).

3.5.14.8 Manually Setting the GNSS Receiver Position

The exact geographic position (location and elevation) of your SecureSync unit—and thus its onboard GNSS receiver—is a major factor for SecureSync to calculate an accurate GNSS time.

Normally, the onboard GNSS receiver will track and adjust the antenna position during the so-called GNSS **survey**, which is performed during initial commissioning of your SecureSync unit, or re-commissioning it after it had been powered down for some time ("cold start").

Depending on where your GNSS antenna is installed and thus, how good the reception is, this survey may take several hours. With good reception, this procedure is adequate for most applications.

Setting a **Manual Position**, however, i.e. manually applying your current geographic position data (Latitude, Longitude, and Altitude) may be necessary if your GNSS receiver could not complete its survey, due to poor reception.

In some cases, setting the position manually may also help to reduce the amount of time needed for the initial position "fix", i.e. for SecureSync to synchronize with the satellites in view.

Note: When manually setting a position, SecureSync must be in one of the stationary modes, Standard or Single Satellite (see "GNSS Receiver Modes" on page 206).

Note that this position will also be used if **Apply A-GPS Data** is checked.

To manually set your position:

1. Determine your geographic position. For more information, see "Determining Your Position" below.
2. Navigate to **INTERFACES > REFERENCES: GNSS 0**. In the **GNSS 0** status window, click Edit in the lower left corner.
3. Under **Manual Position Set** accurately enter **latitude**, **longitude** (both in decimal degrees), and **altitude** (in meters) of your GNSS antenna, SecureSync can use this data during the satellite tracking/adjustment process, which typically leads to a quicker "fix". It is recommended to enter the position as accurately as possible.

Determining Your Position

In case your position is not already known, there are several ways to determine it, e.g., using a GPS-enabled device, such as a smart phone. **GoogleMaps** is another option, described below.

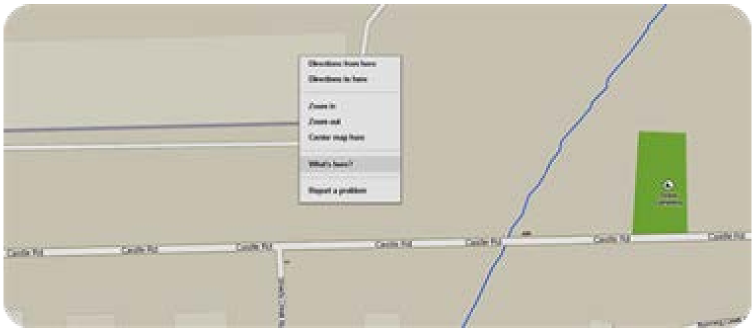
Reasons for manually entering your position

Manually entering your position may not only reduce the time to “first fix” during initial installation, it will also enable the unit to synchronize to satellite timing signals in the event that signals from less than four satellites can be received.

After manually entering the position data, SecureSync will automatically check the status of the GNSS receiver:

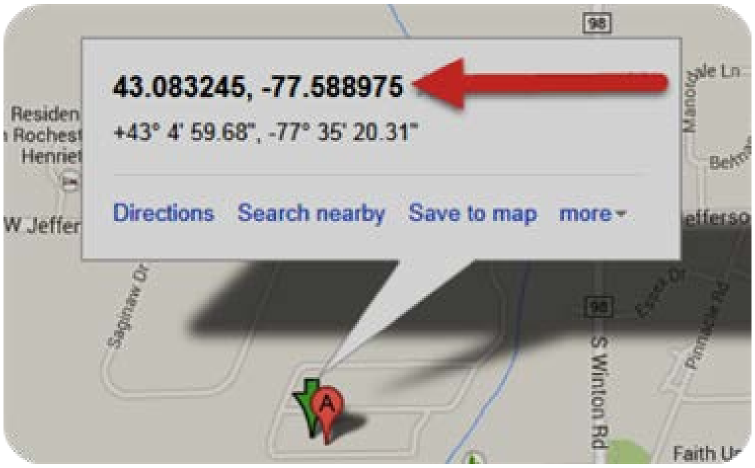
If no GNSS-based position data is available (yet), SecureSync will provide the internal GNSS receiver with the manually entered position.

1. Locate the building and the relative location in the building, using GoogleMaps™. The satellite photos may help locate the building.
2. With newer versions of GoogleMaps™, obtain the coordinates by **left**-clicking on the location: A popup window will display your coordinates. (Note: This does not work with a red pin).
3. With older versions, **right**-click the location and select **“What’s Here?”**



a. This will add a green arrow to the page.

b. Next, left-click the green arrow to expose the coordinates.



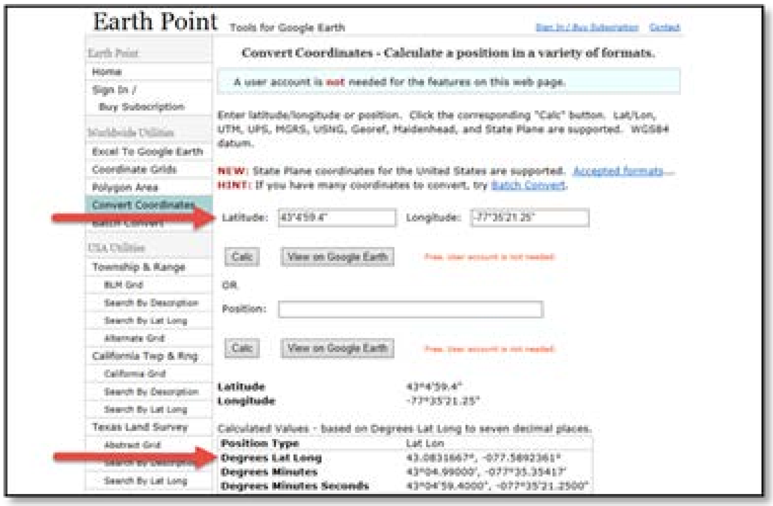
43.083245, -77.588975

+43° 4' 59.68", -77° 35' 20.31"

4. Take note of your **decimal** position.

> **Note:** Should you prefer to determine your position in a different way, and as a result, have your latitude & longitude data in degrees/minutes/seconds, you need to convert this data, e.g. by using a conversion tool, such as Earth

Point: www.earthpoint.us:



Convert Coordinates - Calculate a position in a variety of formats.

A user account is not needed for the features on this web page.

Enter latitude/longitude or position. Click the corresponding "Calc" button. Lat/Lon, UTM, UPS, MGRS, USNG, Georef, Maidenhead, and State Plane are supported. WGS84 datum.

NEW: State Plane coordinates for the United States are supported. Accepted formats...
HINT: If you have many coordinates to convert, try Batch Convert.

Latitude: 43°4'59.4" Longitude: -77°35'21.25"

Free. User account is not needed.

OR

Position:

Free. User account is not needed.

Latitude	43°4'59.4"
Longitude	-77°35'21.25"

Calculated Values - based on Degrees Lat Long to seven decimal places.

Position Type	Lat Lon
Degrees Lat Long	43.0831667°, -077.5892361°
Degrees Minutes	43°04.99000', -077°35.35417'
Degrees Minutes Seconds	43°04'59.4000", -077°35'21.2500"

5. Determine your altitude: Finding the altitude of your SecureSync's antenna position is not as crucial as finding the latitude and longitude. Looking up the altitude for the general area, the city in which the SecureSync is located in for example should be sufficient. If a more exact altitude is desired, then use a topographical map that supplies altitude information.
6. Click **Submit** to apply any changes you may have made.

3.5.14.9 Selecting GNSS Constellations

SecureSync allows you to select which GNSS constellations shall be tracked, i.e. you can determine if you want e.g., GLONASS satellites to be tracked (besides GPS). The options offered depend on the type of GNSS receiver installed in your SecureSync unit, and if a Multi-GNSS license file is installed.

To learn more about GNSS-related theory of operation, see "Introduction to GPS and GNSS" on page 4.

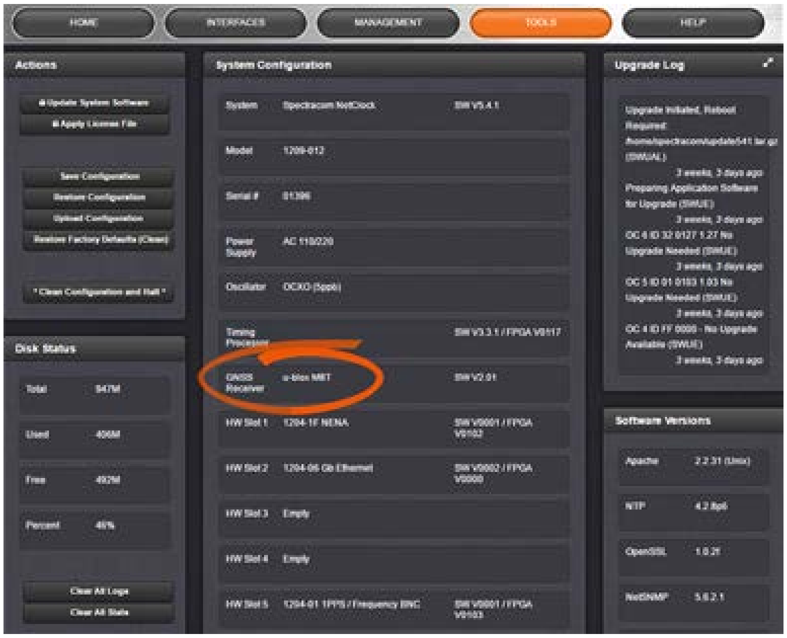
To review your current GNSS constellation selection:

1. Navigate to **INTERFACES** > **REFERENCES: GNSS Reference**.
2. Click the GEAR button next to **GNSS 0**. (For an illustration, see "Configuring the GNSS Reference" on page 201.)
3. In the newly opened **GNSS 0** window, look for the **Selected Constellations** menu.

Determining Your GNSS Receiver Model

To find out which GNSS receiver type is installed in your SecureSync:

1. Navigate to **TOOLS > Upgrade/Backup**.
2. In the **System Configuration** panel, look for **GNSS Receiver**:



System Configuration

System	Spectracom NetClock	SW V5.4.1
Model	1209-012	
Serial #	01396	
Power Supply	AC 110/220	
Oscillator	OCXO (5ppb)	
Timing Processor		SW V3.3.1 / FPGA V0117
GNSS Receiver	u-blox M8T	SW V2.01
HW Slot 1	1204-1F NENA	SW V0001 / FPGA V0102
HW Slot 2	1204-06 Gb Ethernet	SW V0002 / FPGA V0000
HW Slot 3	Empty	
HW Slot 4	Empty	
HW Slot 5	1204-01 1PPS / Frequency BNC	SW V0001 / FPGA V0103

Disk Status

Total	947M
Used	406M
Free	492M
Percent	45%

Upgrade Log

Upgrade Initiated, Reboot Required: /home/spectracom/update541.tar.gz (SWUAL)
3 weeks, 3 days ago
Preparing Application Software for Upgrade (SWUE)
3 weeks, 3 days ago
OC 6 ID 32 0127 1.27 No Upgrade Needed (SWUE)
3 weeks, 3 days ago
OC 5 ID 01 0103 1.03 No Upgrade Needed (SWUE)
3 weeks, 3 days ago
OC 4 ID FF 0000 - No Upgrade Available (SWUE)
3 weeks, 3 days ago

Software Versions

Apache	2.2.31 (Unix)
NTP	4.2.8p6
OpenSSL	1.0.2f
NetSNMP	5.6.2.1

Determining if Multi-GNSS Option Is Installed

To check if the Multi-GNSS license is installed on your SecureSync:

1. Navigate to **TOOLS** > **SYSTEM: Upgrade/Backup** (same menu as shown in the illustration above).
2. Under **System Configuration**, look for the Option OPT-GNS Multi-GNSS. (You may need to scroll to the bottom of the screen).

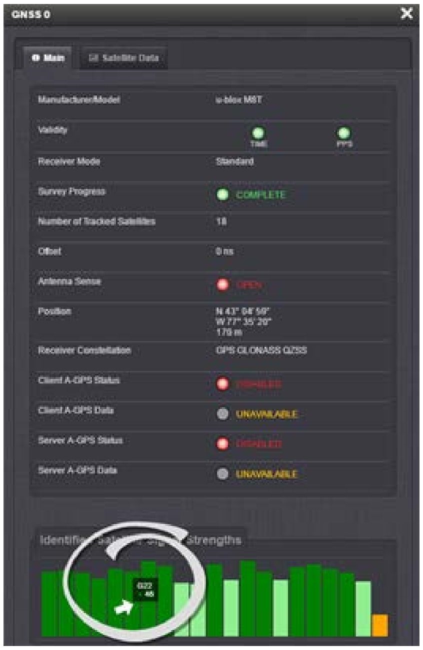
If the license is installed, proceed to "Selecting GNSS Constellations" on the facing page.

If the license is not installed, and you are interested in purchasing it, contact your local Spectracom office, or Spectracom Technical Support ("Technical Support" on page 1).

Determining Which GNSS Satellites Are Received

To see which GNSS satellites your SecureSync is currently receiving:

1. Navigate to **INTERFACES > REFERENCES: GNSS 0**.
2. Click on the INFO button next to **GNSS (0)**.



Manufacturer/Model	u-blox M8T
Validity	● TIME ● PPS
Receiver Mode	Standard
Survey Progress	● COMPLETE
Number of Tracked Satellites	18
Offset	0 ns
Antenna Sense	● OPEN
Position	N 43° 04' 50" W 77° 35' 20" 170 m
Receiver Constellation	GPS GLONASS QZSS
Client A-GPS Status	● DISABLED
Client A-GPS Data	● UNAVAILABLE
Server A-GPS Status	● DISABLED
Server A-GPS Data	● UNAVAILABLE

3. In the newly opened **GNSS 0** window, under **Identified Satellite Signal Strengths** hover with your cursor over the bars: The letter provided in each pop up text window indicates which constellation the displayed satellite belongs to:

Letter symbol	GNSS Constellation
G	GPS
R	GLONASS
E	Galileo (not yet enabled)
J	QZSS
C	BeiDou
I	IRNSS (not yet enabled)

Selecting GNSS Constellations

To review or change which GNSS constellations SecureSync's GNSS receiver shall track:

1. Navigate to **INTERFACES > REFERENCES > GNSS Reference**.
2. Click the GEAR button next to **GNSS 0**.
3. In the newly opened **GNSS Window**, under **Selected Constellations**, review which constellations are currently tracked, and apply your changes. Note the following:
   - The LEA-M8T GNSS receiver offers concurrent dual constellation reception, i.e. at any given time, **2 + QZSS** constellations can be received:

- GPS + GLONASS (plus QZSS)
- GPS + BeiDou (plus QZSS).
- GPS + Galileo (plus QZSS) [Q4 2016]

  Should you select more than 2 + QZSS constellations, you will receive a Constellation Error once you click Submit (ConstError).

With an M8T receiver and a Multi-GNSS license file installed, the following GNSS constellations are available:

- **GPS**
- **GLONASS**
- **Beidou**
- **QZSS**.

As of autumn 2016, also **Galileo** will be receivable (a GNSS receiver software update will be required for this).

Per default both GPS, and GLONASS will be enabled, in order to obtain as many satellite signals as possible. Either selection can be disabled, but not both of them (if both are turned off, no changes will be saved and the last constellation setting will be preserved).

To verify if satellite signals for the selected GNSS constellations are received, follow the procedure outlined above under "Determining Which GNSS Satellites Are Received" on page 214.

QZSS

QZSS is disabled by default. For further information, research QZSS online. In order to receive QZSS signals, you must either be located in the Japan region, or use a GNSS simulator (such as Spectracom GSG-5 or -6 Series).

QZSS is considered not a standalone constellation and while SecureSync allows you to enable only QZSS, it is recommended to use it in combination with GPS.

3.5.14.10 A-GPS

A-GPS stands for **Assisted GPS**. This widely used technology involves providing additional data to the GNSS receiver by an alternative means of communication (e.g., via IP, or by manual data entry), thereby reducing the time for the receiver to acquire and track the actual satellite signals. This may lead to a significantly shorter time for SecureSync to deliver a GNSS-based timing signal upon a “cold start” of the unit.

The **A-GPS client** is used to send assistance data to the GPS receiver. This is most useful in areas where poor GPS reception is occurring.

> **Note:** The concept of an A-GPS server also exists: This functionality allows a SecureSync to operate as a server, providing A-GPS ephemeris and almanac data

to other devices e.g., a Spectracom GSG-series GNSS simulator. Contact Spectracom for further information.

The A-GPS functionality is only available with the following GNSS receiver models:

- RES-SMT GG
- U-blox M8T

To determine which GNSS receiver is installed in your SecureSync unit, navigate to **INTERFACES** > **REFERENCES: GNSS Reference**, and click the INFO button next to **GNSS 0**. The first line item under the **Main** tab lists the receiver type.

Enable A-GPS Client

The feature **Enable A-GPS Client** will schedule assistance data to be collected and updated every hour. On startup, if data is present, it will be sent to the receiver.

Apply A-GPS Data

When this option is selected, SecureSync will **immediately** apply the time, position and satellite data to the receiver once you click Submit.

Time and position are user-configurable; SecureSync collects A-GPS satellite data from an external source automatically.

Note: Once you click Submit, any parameters entered under Apply A-GPS Data will override the system Time and Position data. Exercise caution when using this feature, since this could negatively impact the GNSS receiver operation.

Use Current System Time

Apply SecureSync's currently used system time to the GNSS receiver.

Set System Time

Enter a specific date and time, instead of the system time. This may be useful if the system time is known to be incorrect, or if you need a time in the past or future, e.g. for simulation purposes. Enter the date and time using the displayed calendar and time sliders.

Manual Position Set

By accurately entering **latitude**, **longitude** (both in decimal degrees), and **altitude** (in meters) of your antenna, SecureSync can use this data during the satellite tracking/adjustment process, which typically leads to a quicker "fix". It is recommended to enter the position as accurately as possible. For more information, see "Manually Setting the GNSS Receiver Position" on page 210.

Note: When manually setting a position, SecureSync must be in one of the stationary modes, Standard or Single Satellite (see "Receiver Mode" above).

3.6 The Administrator Login Password

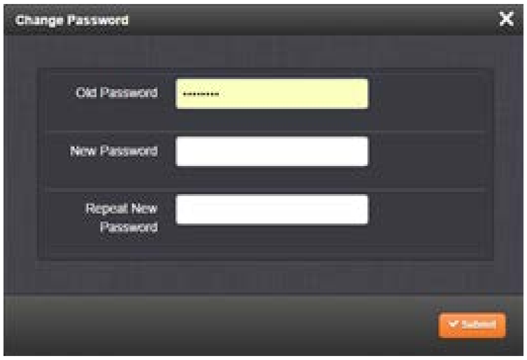
The factory default administrator password value of *admin123* can be changed from the default value to any desired value. If the current password is known, it can be changed, using the SecureSync Web UI.

Note: To follow this procedure, the user must be logged in as the `spadmin` user. If you are unable to login as `spadmin`, follow the procedure outlined in "Resetting the Administrator Password When Forgotten/Lost" on the facing page.

If the password has already been changed from the default value, but the current value is no longer known, the administrator password can be reset back to the factory default value. Once reset, it can then be changed to a new desired value via the web interface.

To change the admin password from a known value to another desired value using a web browser:

1. Navigate to **MANAGEMENT > OTHER: Change My Password**.
2. The **Change Password** pop-up window will display.



3. In the **Old Password** field, type in the current password you wish to replace.
4. In the **New Password** field, type in the new password you wish to use.

Note: The new password can be from 8 to 32 characters in length.

5. In the **Repeat New Password** field, retype the new password you wish to use.
6. Click the **Submit** button at the bottom of the screen.

3.6.1 Resetting the Administrator Password When Forgotten/Lost

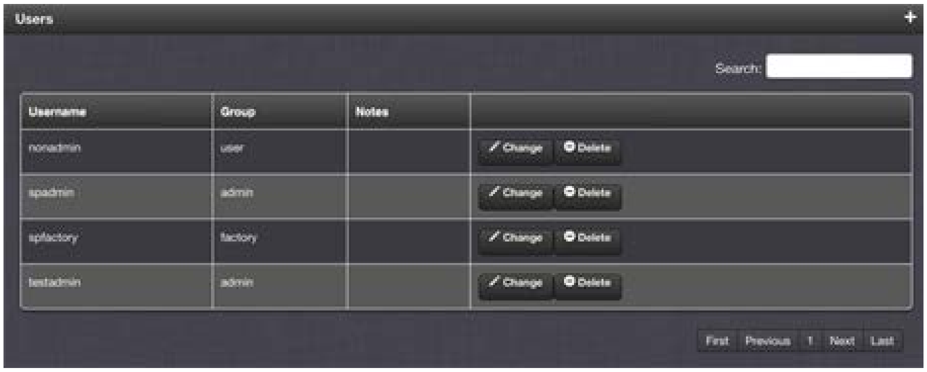
If the current *spadmin* account password has been changed from the default value and has been forgotten or lost, you can reset the *spadmin* password back to the factory default value of *admin123*.

Resetting the spadmin account password does not reset any user-created account passwords. This process only resets the *spadmin* account password.

Any user with administrator rights can reset the *spadmin* password through the **MANAGEMENT/OTHER/Authentication** window.

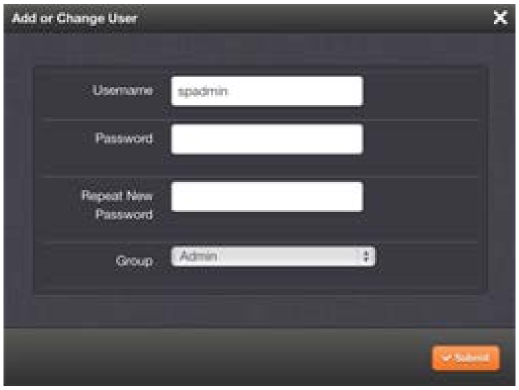
To reset the *spadmin* password through the **MANAGEMENT/OTHER/Authentication** window:

1. Navigate to the **MANAGEMENT/OTHER/Authentication** window.
2. Locate the *spadmin* entry in the **Users** table.



Username	Group	Notes
nonadmin	user	
spadmin	admin	
spfactory	factory	
testadmin	admin	

3. Click the **CHANGE** button.
4. In the **Add or Change User** window:
   a. Enter a new password.
   b. Confirm the new password.



Username: spadmin
Password:
Repeat New Password:
Group: Admin

Note: The new password can be from 8 to 32 characters in length.

5. Click the **Submit** button at the bottom of the window.

If you do not have access to SecureSync through another admin account, the *spadmin* password must be reset via the front panel keypad or using the front panel serial port.

To reset the *spadmin* account password using the keypad:

1. Use the front panel LCD and the keypad to perform a “**RESETPW**”. See also "Using the Keypad and Information Display" on page 30. (“Resetpw” is located in the **Home/System** menus).
2. You will be prompted to confirm the operation before the password is reset. The *spadmin* account password is now reset to “**admin123**”.

To reset the spadmin account password using the serial port:

1. Connect a PC to the front panel serial port, and log in using an account with admin group rights (such as the *spadmin* account).
2. Type: `resetpw` <Enter>. The *spadmin* account password is now reset.

After resetting the password follow the procedure above to change the *spadmin* password in the **MANAGEMENT/OTHER/Authentication** window.

3.7 Resetting the Unit to Factory Configuration

In certain situations, it may be desired to reset all SecureSync configurations back to the factory default configuration. The GNSS location, any SecureSync configurations and the locally stored log files can be cleared via the Web UI.

Caution: It is not possible to clear the Authentication logs and NTP logs.

Note: Restoring configurations (reloading a saved configuration), erasing the stored GNSS location and clearing the log files are separate processes. You may restore one without restoring the others.

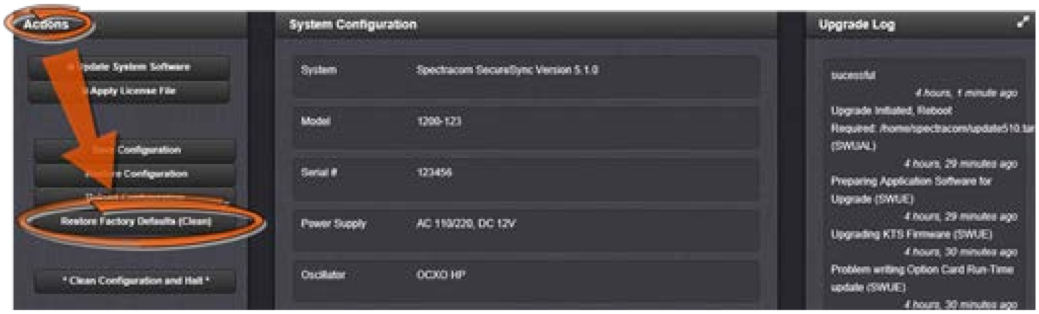
If SecureSync was assigned a static IP address before cleaning the configurations, it will be reset to DHCP after the clean has been performed. If no DHCP server is available after the clean operation, the static IP address will need to be manually reconfigured. See"Replacing a Dynamic with a Static IP Address" on page 34 or "Assigning a Static IP Address" on page 35.

3.7.1 Resetting All Configurations to their Factory Defaults

To restore the configuration files to their factory defaults:

1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.

2. In the **Actions** panel, click the **Restore Factory Defaults (Clean)** button.



System Configuration

System	Spectracom SecureSync Version 5.1.0
Model	1200-123
Serial #	123456
Power Supply	AC 110/220, DC 12V
Oscillator	OCXO HP

Upgrade Log

```
sucessful
            4 hours, 1 minute ago
Upgrade Initiated, Reboot
Required: /home/spectracom/update510.tar
(SWUAL)
            4 hours, 29 minutes ago
Preparing Application Software for
Upgrade (SWUE)
            4 hours, 29 minutes ago
Upgrading KTS Firmware (SWUE)
            4 hours, 30 minutes ago
Problem writing Option Card Run-Time
update (SWUE)
            4 hours, 30 minutes ago
```

3. SecureSync restores the configuration files to the factory settings, and then reboots in order to read the new configuration files. Once powered back up, SecureSync will be configured with the previously stored files.

> **Note:** While the GNSS position is stored and retained through power cycles, choosing Clean (Restore Factory Configuration) will erase the stored GNSS position.

Erasing the GNSS location means that the next time the GNSS antenna is connected and the GNSS receiver is able to continuously track at least four satellites, the 33 minute long GNSS survey will be performed again, so the position can be recalculated and locked-in.

3.7.2 Resetting the GNSS Receiver Position

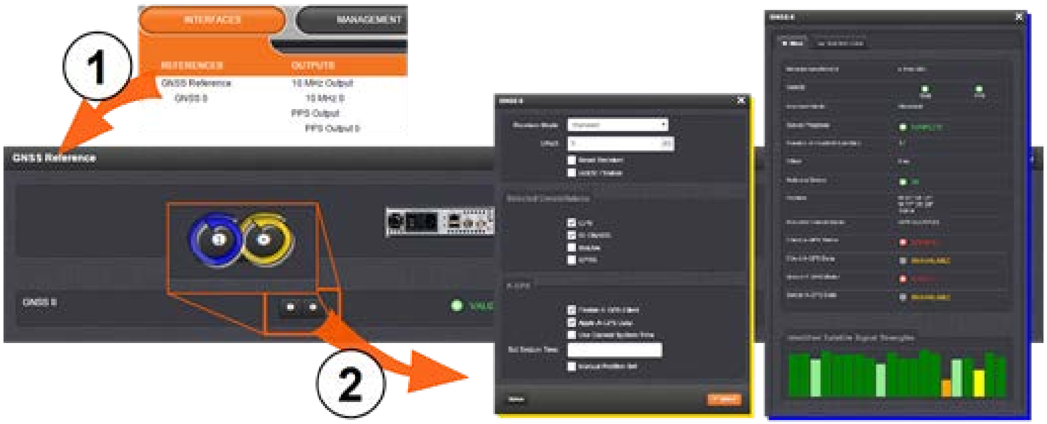
The position of the GNSS receiver your SecureSync is using is stored in the unit's memory. This data can be erased.

> **Caution:** Upon reconnecting the GNSS antenna and when the receiver is able to track continuously at least four satellites (and as long as the GNSS receiver is configured for the Standard mode), the GNSS survey will be performed again. This will take 33 minutes.

To reset the GNSS receiver position stored in your SecureSync unit:

1. Disconnect the GNSS antenna cable from the back panel antenna jack.
2. Navigate to **INTERFACES > REFERENCES: GNSS Reference**.

3. On the right side of the screen, the **GNSS Reference** panel will display.

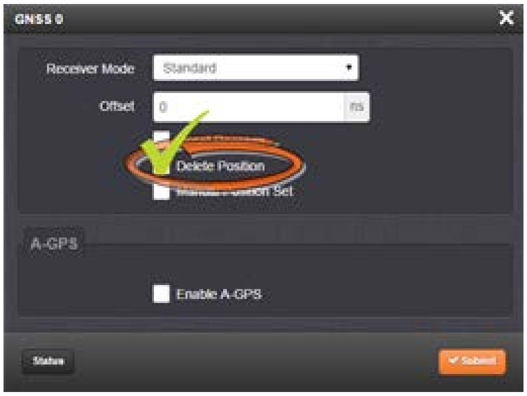


4. Click the GEAR button for the GNSS Reference you wish to configure.

> **Note:** If you choose the individual GNSS Reference directly through the INTERFACES/REFERENCES drop-down menu, the GNSS Status window will open directly. In this case, click the EDIT button at the bottom of the GNSS Status window.

> **Note:** If you have only one reference, SecureSync will number that reference 0. Additional references will be numbered 1 or above.

5. The **GNSS 0** Edit window will display.


GNSS 0

Receiver Mode: Standard

Offset: 0 ns

☑ Delete Position

□ Manual Position Set

A-GPS

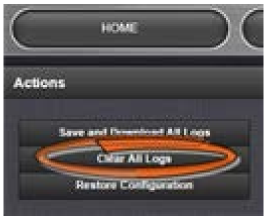
□ Enable A-GPS

6. Select the **Delete Position** check box.

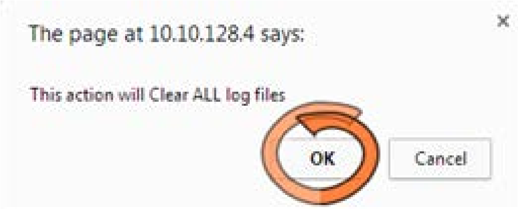
3.7.3 Clearing Locally Stored Logs: All Files

Note: Authentication and NTP logs cannot be cleared.

1. Navigate to **MANAGEMENT > OTHER: Log Configuration**.
2. On the **Logs** screen, click the **Clear All Logs** button in the **Actions** panel.



3. In the message window that displays, click **OK**.

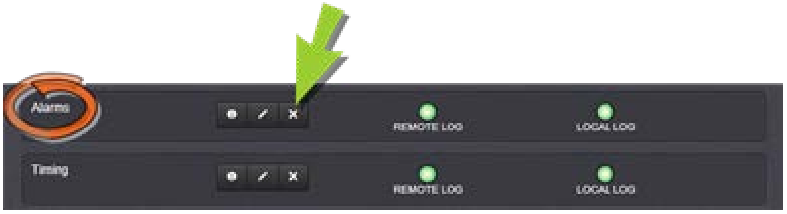

The page at 10.10.128.4 says:

This action will Clear ALL log files

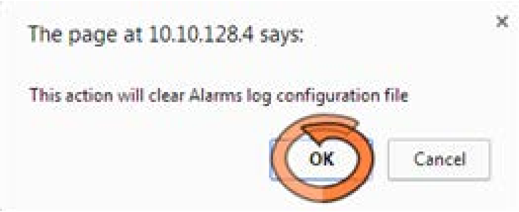
3.7.4 Clearing Locally Stored Logs: Selected Files

Note: Authentication and NTP logs cannot be cleared.

1. Navigate to **MANAGEMENT > OTHER: Log Configuration**.
2. On the **Logs** screen, for the log you wish to clear (e.g., **Alarm** log), click the X-icon.



3. In the message box that displays, click the **OK** button.



The page at 10.10.128.4 says:

This action will clear Alarms log configuration file

3.8 Issuing HALT Command Before Removing Power

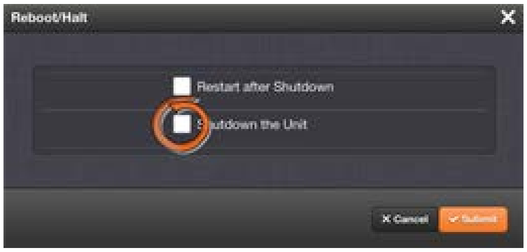
Once power is applied to the SecureSync, it should not be removed unless the HALT command is issued to the unit. Using the HALT command to shut down the system gracefully not only reduces the risk of damaging system files, but can also allow for faster startup after the next power-up of SecureSyncThe HALT command may be issued to the SecureSync through the Web UI, the front panel serial port, or the front panel keypad.

Note: Wait 30 seconds after entering the HALT command before removing power.

Once the HALT process has been initiated via the Web UI or front panel, the front panel LCD will display **Power off SecureSync,** and the front panel LED time display will stop incrementing.

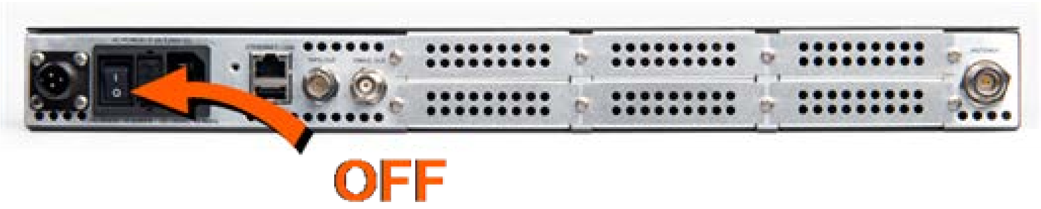
Issuing a HALT Command via the Web UI

1. Navigate to **TOOLS > SYSTEM: Reboot/Halt**.
2. The **Reboot/Halt** window will display. Select the **Shutdown the Unit** checkbox.



3. Click the **Submit** button.
4. Wait 30 seconds after entering the HALT command before switching off the SecureSync

unit.



Once the HALT process has been initiated, the front panel LCD will display **Power off** SecureSync, and the front panel LED time display will stop incrementing.

Issuing a HALT Command via Keypad/SerialPort/Telnet/SSS

The HALT command can be initiated not only via the SecureSync Web UI, but also via the keypad and LCD display. For more information on the keypad, see"Using the Keypad and Information Display" on page 30.

With a serial connection to the front panel serial port, telnet connection or SSH connection, type `halt` <Enter> to halt SecureSync for shutdown. For more information on SecureSync commands, see "CLI Commands" on page 467.

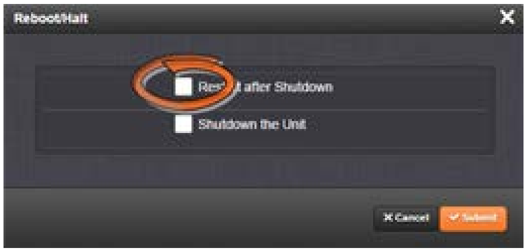
Once the HALT process has been initiated, the front panel LCD will display **Power off** SecureSync, and the front panel LED time display will stop incrementing.

Note: Wait 30 seconds after entering the HALT command before removing power.

3.9 Rebooting the System

To reboot SecureSync:

1. Navigate to **TOOLS > SYSTEM: Reboot/Halt**.
2. Select the **Restart after Shutdown** box in the **Reboot/Halt** window.



3. SecureSync will now be rebooted and be accessible again shortly thereafter.

Rebooting via LCD/Keypad, Serial Port, Telnet, SSH, SNMP

The Reboot command can be initiated not only via the SecureSync Web UI, but also via the keypad and LCD information display. See "Using the Keypad and Information Display" on page 30 for information on using the keypad to perform a system reboot.

With a serial connection to the front panel serial port, telnet connection or SSH connection, type `reboot` <Enter> to reboot SecureSync.

Reboot is also is available to be performed through an `snmpset` operation. For more information on SecureSync commands, see "CLI Commands" on page 467.

Once the Reboot process has been initiated, the front panel LCD will display a **“Power off** SecureSync**”** message, and the front panel LED time display will stop incrementing until SecureSync has started booting back up again.

Once the Reboot process has been initiated, the front panel LCD will display a **“Power off** SecureSync**”** message, and the front panel LED time display will stop incrementing until SecureSync has started booting back up again.

3.10 If a Secure Unit Becomes Inaccessible

Spectracom assumes that the customer is responsible for the physical security of the product. Spectracom secure products are recommended to be locked in a secure enclosure, cabinet or room. Unauthorized persons are not to be given access to the product nor should a serial cable and terminal program be attached unless the system administrator is configuring or performing maintenance.

Access to a secure Spectracom product can become denied, if:

- your company disables HTTPS
- loses the system passwords
- allows the certificate to expire
- deletes the certificate and private keys and deletes the host keys, or
- forgets the passphrase.

To regain access to the SecureSync unit, you must utilize the front panel keypad and LCD in order to restore the *spadmin* account’s default password.

The *spadmin* account can then be used to enable HTTPS using the “`defcert`” command. The “`defcert`” command generates a new self-signed SSL certificate.

Refer to "Using the Keypad and Information Display" on page 30 for information on using the keypad and LCD information display.

CHAPTER 4

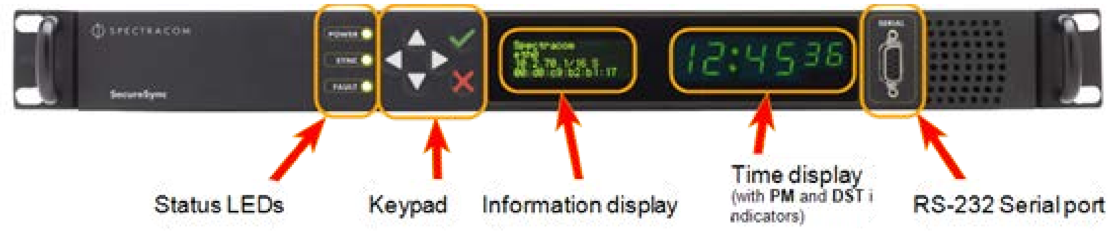
OPERATION

The Chapter OPERATION describes tasks often performed on a day-to-day basis, such as performance monitoring, and managing logs.

The following topics are included in this Chapter:

4.1 Status Monitoring via Front Panel

When you have physical access to the SecureSync front panel, you can obtain a system status overview without the need for a computer workstation with a Web browser.



4.2 Front Panel Status Indicator LEDs

The three status LEDs ("Front panel layout" on page 6), POWER, SYNC, and FAULT, indicate whether SecureSync is synchronized, whether power is applied to the unit and if any alarms are currently asserted.

The POWER LED will not be lit, if power is not applied to the unit. It will indicate green if power **is** applied. The SYNC and FAULT lamps have multiple states:

- **POWER**: Green, always on
- **SYNC**: Tri-color LED indicates the time data accuracy
- **FAULT**: Two-color, three-state LED, indicating possible equipment fault.

At power up, the unit automatically performs a brief LED test run during which all three LEDs are temporarily lit. The following table provides an overview of the LED status indications:

Table 4-1: SecureSync front panel status indicators

LED Label	Activity/Color	Description
POWER	Off	Both AC and DC Input Power are disconnected. Or, SecureSync's AC input switch is turned off and DC input is not present.
	On/solid green	AC and/or DC Power are supplied; SecureSync detects all power inputs.
	Red	SecureSync is configured for two power inputs, but detects only one power input; or detects a power configuration error.
	Green & blinking orange 1/sec.	Power error; general power configuration fault.

LED Label	Activity/Color	Description
SYNC	Red	Time Sync Alarm: 1) SecureSync has powered up and has not yet achieved synchronization with its inputs. 2) SecureSync was synchronized to its selected input references, but has since lost all available inputs (or the inputs were declared invalid) and the Holdover period has since expired.
	Solid green	SecureSync has valid time and 1PPS reference inputs present and is synchronized to its reference.
	Orange	SecureSync is in Holdover mode. SecureSync was synchronized to its selected input references, but has since lost all available inputs (or the inputs are not declared valid). SecureSync's outputs will remain useable until at least the Holdover period expires.
FAULT	Off	No alarm conditions are currently active.
	Blinking orange	GNSS antenna problem alarm has been asserted and is currently active. A short or open has been detected in the GNSS antenna cable. The light will automatically turn off when the alarm condition clears (Refer to "Troubleshooting via Web UI Status Page" on page 457 for troubleshooting this condition).
	Solid orange	A Minor alarm condition (other than an antenna problem alarm) has been asserted and is currently active (See "Minor and Major Alarms" on page 455 for troubleshooting this condition).
	Red	A Major alarm condition has been asserted and is currently active (See "Minor and Major Alarms" on page 455 for troubleshooting this condition).

4.3 Status Monitoring via the Web UI

While the SecureSync front panel status LEDs provide an indication of the current operating status of the system (see "Status Monitoring via Front Panel" on the previous page), more detailed status information can be accessed via the SecureSync **Web UI**, such as:

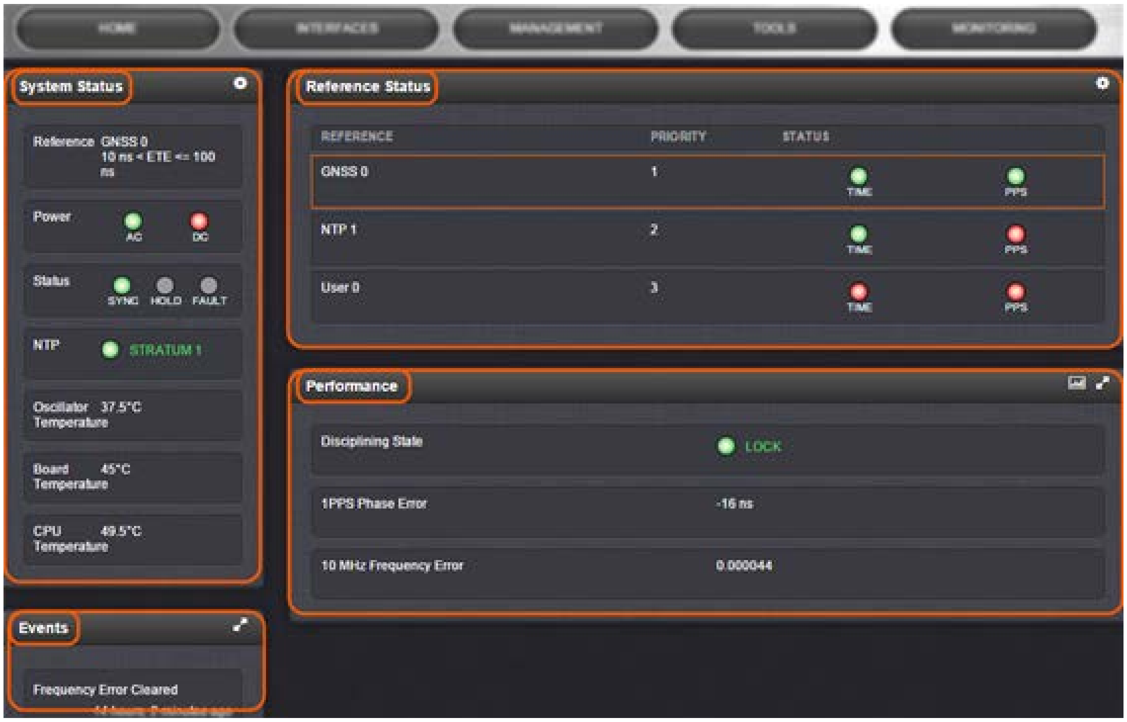
- Time synchronization status, including references
- GNSS satellites currently being tracked
- NTP sync status and current Stratum level
- Estimated time errors
- Oscillator disciplining
- Temperature monitoring
- Status of outputs and presence of DC input power.

Real-time details about SecureSync's system status can be accessed via:

- the **HOME** screen, focusing on time server functionality status
- the **TOOLS > System Monitor** screen, displaying SecureSync's internal hardware status

4.3.1 Status Monitoring via the HOME Screen

The **HOME** screen of the SecureSync Web UI provides a system status overview.



System Status

Reference	GNSS 0 10 ns < ETE <= 100 ns
Power	● AC ● DC
Status	● SYNC ● HOLD ● FAULT
NTP	● STRATUM 1
Oscillator Temperature	37.5°C
Board Temperature	45°C
CPU Temperature	49.5°C

Reference Status

REFERENCE	PRIORITY	STATUS	
GNSS 0	1	● TIME	● PPS
NTP 1	2	● TIME	● PPS
User 0	3	● TIME	● PPS

Performance

Disciplining State	● LOCK
1PPS Phase Error	-16 ns
10 MHz Frequency Error	0.000044

Events

Frequency Error Cleared

The **HOME** screen is divided into four panels:

4.3.1.1 System Status panel

- **Reference**–Indicates the status of the current synchronizing reference, if any.
- **Power**–Indicates whether the power is on and which type of power is being used. If the unit is configured for AC power, AC will appear in this panel. If the unit is configured for DC power, DC will appear in this panel. If the unit is configured for both AC and DC, AC and DC will appear in this panel.
- **Status**–Indicates the status of the network’s timing. There are three indicators in the Status field:
  - **Sync**–Indicates whether SecureSync is synchronized to its selected input references.
    - **Green** indicates SecureSync is currently synchronized to its references (The front panel **Sync** light will also be green).

    - **Orange** indicates SecureSync is not currently synchronized to its references (The front panel **Sync** light will be red).
  - **Hold**–When lit, SecureSync is in holdover mode.
  - **Fault**–Indicates a fault in the operation of the SecureSync. See "Troubleshooting via Web UI Status Page" on page 457 for instructions for troubleshooting faults.
- **Alarm Status**: If a major or minor alarm is present, it will be displayed here.
- **NTP**–Current STRATUM status of this SecureSync unit.
- **Temperature**–Oscillator, Board, and CPU temperatures are displayed in real time; for more information, see "Temperature Management" on page 257.

4.3.1.2 Reference Status panel

- **Reference**–Indicates the name type of each reference. These are determined by the inputs set up for the SecureSync
- **Priority**–Indicates the priority of each reference. This number will be between 1 and 15. References in this panel appear in their order of priority. See "Configuring Input Reference Priorities" on page 155 for more information.
- **Status**–Indicates which available input reference is acting as the **Time** reference and which available input reference is acting as the **1PPS** reference.
  - **Green** indicates that the reference is present and has been declared valid.
  - **Orange** indicates the input reference is not currently present or is not currently valid.

4.3.1.3 Performance panel

- **Disciplining State**–Indicates whether or not the internal oscillator is currently being disciplined (steered to an input reference).
- **1PPS Phase Error**–An internal measurement (in nanoseconds) of the internal 1PPSs' phase error with respect to the selected input reference (if the input reference has excessive jitter, phase error will be higher)
- **10 MHz Frequency Error**–An internal estimated calculation (in Hertz) of the internal oscillator's frequency error, based on the phase accuracy error at the beginning and end of a frequency measurement window (the length of this window will vary depending upon the type of oscillator installed and the oscillator adjustment algorithm).

Events panel

The Events panel in the bottom-left corner of the **HOME** screen is a log of SecureSync's recent activity. It updates in real time.

Note: If you know the individual reference or output whose status you wish to see, you can access the Status window of that reference or output directly through the INTERFACES/REFERENCES or INTERFACES/OUTPUTS drop-down menu.

4.3.2 Status Monitoring via the System Monitor Screen

To display status information pertaining mainly to SecureSync's current hardware status, navigate to **TOOLS > SYSTEM > System Monitor**.

The information provided on the **System Monitor** Screen is subdivided into three panels:

4.3.2.1 System Status panel

See "System Status panel" on page 230.

4.3.2.2 Disk Status panel

This panel displays:

- Total: [MB]
- Used: [MB]
- Free: [MB]
- Percent: [%]

The last item refers to Percent used. If you need to update the System Software, and this number is 70% or higher, it is recommended to clear logs and stats in order to free up memory space. (Navigate to **TOOLS > SYSTEM: Upgrade/Backup**, and click the corresponding buttons in the lower left-hand corner.)

4.3.2.3 System Monitor panel

Graphs are displayed for:

- Board Temperature
- CPU Temperature
- Memory Used
- CPU Used.

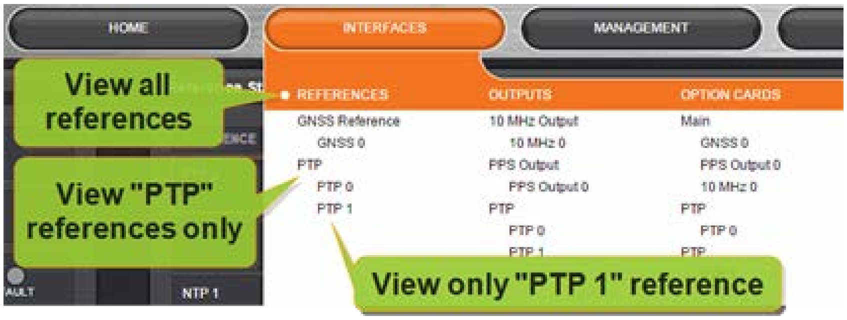
To delete the logged data used to generate the displayed graphs, click the TRASHCAN icon. (Note that re-populating the graphs with fresh data generated at a 1/min. rate will take several minutes.)

To download the logged data in .csv format, click the ARROW icon.

See also: "Temperature Management" on page 257

4.4 Status Monitoring of Input References

SecureSync's input references can be monitored in real time through the **INTERFACES** drop-down menu. The menu will populate dynamically, according to which references are available.



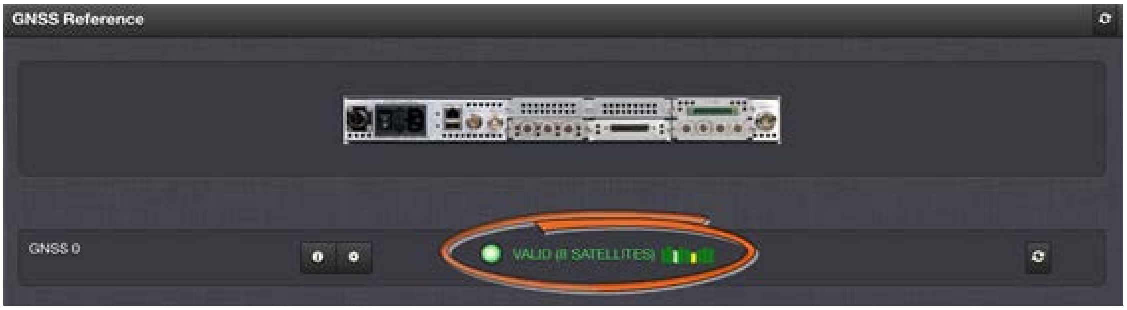
View all references

View "PTP" references only

View only "PTP 1" reference

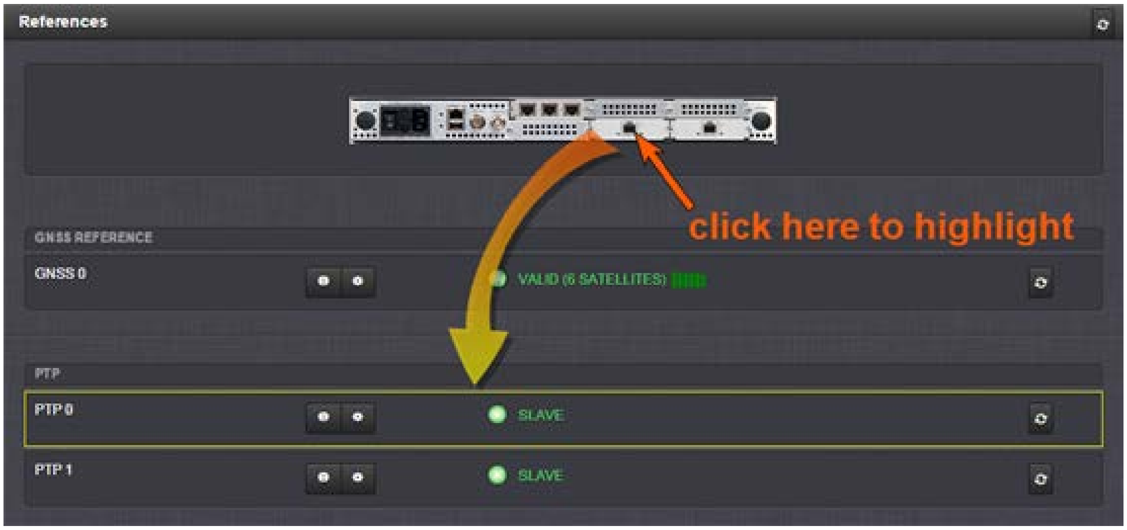
- To display **all** references, click on REFERENCES in the INTERFACES menu.
- To display all references of a **given type**, click on the entry for that reference type (not indented).

The window that opens shows the validity status for the chosen reference(s):


GNSS Reference

GNSS 0 — VALID (8 SATELLITES)

Click on any of the connectors shown in the rear panel illustration to highlight/identify the corresponding reference:


References

GNSS REFERENCE

GNSS 0 — VALID (6 SATELLITES)

PTP

PTP 0 — SLAVE

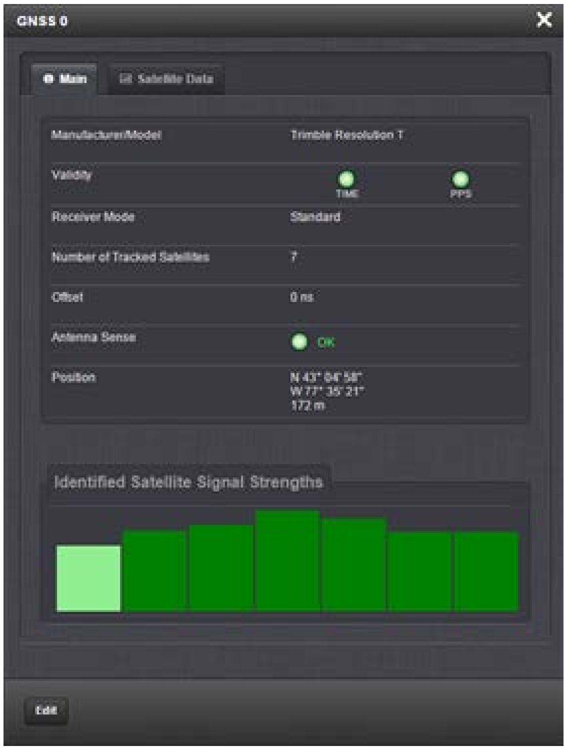
PTP 1 — SLAVE

click here to highlight

To display more status information for a particular input reference, click the corresponding INFO button:

The pop-up window being displayed will show additional status information and option-card specific settings. A particular option card might have more than one setting that can be viewed. The type of input reference, and the option card model determine which status information and option card settings will be displayed.

See "Option Cards Overview" on page 284 to learn more about the different settings of available input reference option cards.



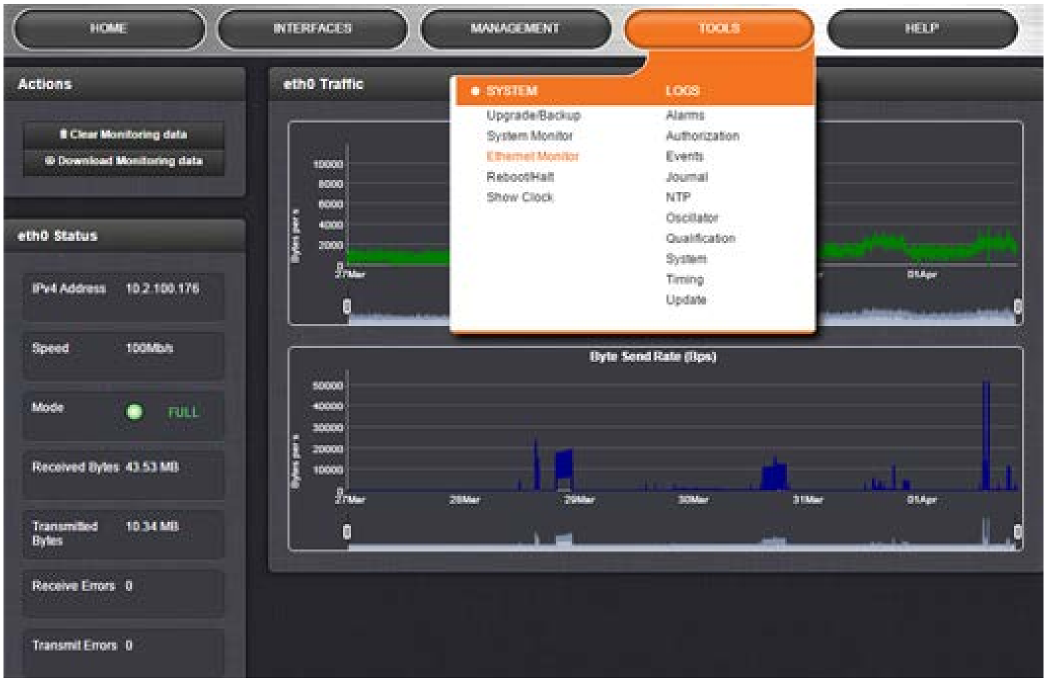
Manufacturer/Model	Trimble Resolution T
Validity	● TIME ● PPS
Receiver Mode	Standard
Number of Tracked Satellites	7
Offset	0 ns
Antenna Sense	● OK
Position	N 43° 04' 58" W 77° 35' 21" 172 m

You can access the option card's **Edit** window directly from the settings detail window by clicking on the Edit button.

4.5 Ethernet Monitoring

To monitor Ethernet status and traffic:

1. Navigate to **TOOLS > SYSTEM: Ethernet Monitor**. The Ethernet monitoring screen opens:



eth0 Status

IPv4 Address 10.2.100.176

Speed 100Mb/s

Mode FULL

Received Bytes 43.53 MB

Transmitted Bytes 10.34 MB

Receive Errors 0

Transmit Errors 0

The data displayed is linked to a specific Ethernet port e.g, ETH0. If you enable additional Ethernet ports, their throughput data will also be displayed.

In the **Traffic** pane on the right the traffic throughput in Bytes per second is displayed in two graphs. Drag the handles at the bottom of the graphs to zoom in on a particular time frame.

In the **Actions** panel on the left, you can clear or download monitoring data.

In the **Status** panel on the left, information pertaining to the given Ethernet port is displayed, including throughput statistics and error statistics. The Mode field indicates which transmission mode is being used for the given Ethernet port:

- **FULL** duplex, or
- **HALF** duplex.

Note that the Mode is auto-negotiated by SecureSync. It can be changed only via the switch SecureSync is connected to, not by using the SecureSync Web UI.

4.6 TimeKeeper™

4.6.1 What is TimeKeeper?

FSMLabs' TimeKeeper[1] is an optional module that is seamlessly integrated into the SecureSync platform, utilizing the available system components.

FSMLabs' TimeKeeper software simultaneously performs the function of an NTP Server and a PTP Master. In the absence of other references, it can synchronize to external NTP Servers, or/and PTP Masters. It also has enhanced monitoring features to help manage your network synchronization architectures.

More information on TimeKeeper Client Software can be found under FSMLab's TimeKeeper documentation.

FSMLabs' TimeKeeper Software is licensed under the Software EULA, see http://www.fsmlabs.com/Resources/tkeula/.

4.6.2 What can TimeKeeper do for me?

TimeKeeper supports NTP, and IEEE 1588 PTPv1/v2. A user interface integrated into the SecureSync Web UI allows for enhanced status and timing quality monitoring, as well as a map of the timing network, displaying all the time sources detected.

If your SecureSync has a valid synchronization reference, TimeKeeper will operate as a Stratum 1 server, using SecureSync's system time. No configuration is required for NTP. One or more instances of a PTP master can be configured.

In the event SecureSync loses its synchronization to a high-quality reference, TimeKeeper will continue to act as a time server/master during the Holdover period plus 180 seconds, and then look to synchronize for a suitable reference source on its network, qualifying one of the configured NTP servers or PTP masters to become the system's reference, if network time ("NTP") is configured accordingly in the reference priority table.

TimeKeeper does not require additional hardware, i.e. option cards, because it can operate using the built-in 10/100 Mb network interface. If installed, however, TimeKeeper will utilize the 3 additional 10/100/1000 ports offered by the 1204-06 multi-port option card (ETH1 and ETH2 can be used for hardware time stamping). Any of these ports can be configured for multiple PTP masters and slaves, and NTP sources, simultaneously.

4.6.3 Using TimeKeeper - First Steps

TimeKeeper comes pre-installed with SecureSync System Software, Version 5.2.0 and higher.

In order to utilize the TimeKeeper functionality, a License file has to be purchased from Spectracom.

[1] TimeKeeper is a registered Trademark by FSMLabs, Inc.

Getting started with TimeKeeper:

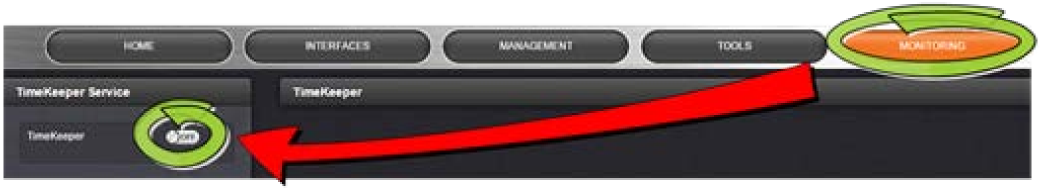
1. If the TimeKeeper license has been purchased separately, **activate** TimeKeeper by applying the License file–see "Applying a License File" on page 280. (You can skip this step, if the license was purchased with the SecureSync unit: In this case the License file will be installed in the factory.)
2. **Enable** TimeKeeper–see "En-/Disabling TimeKeeper" below.
3. **Configure** TimeKeeper, see "Configuring a TimeKeeper PTP Master" on page 129, "Configuring TimeKeeper PTP Slaves" on page 132, and/or "Configuring TimeKeeper as an NTP Time Server" on page 134.

4.6.4 En-/Disabling TimeKeeper

There are two ways to enable/disable TimeKeeper:

METHOD A:

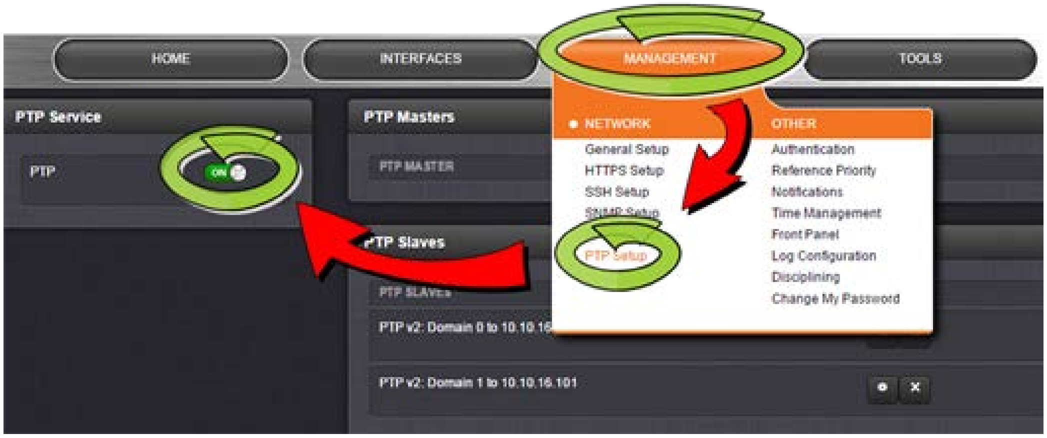
1. In the Primary Navigation menu, click on **MONITORING**.
2. In the panel **TimeKeeper Service**, slide the switch to ON (or OFF).



3. A pop-up message will briefly appear, indicating that TimeKeeper has been enabled or disabled.

METHOD B:

1. Under **MANAGEMENT** > **PTP Setup**, in the panel **PTP Service**, slide the switch to ON (or OFF).
   (Note that TimeKeeper can be enabled **only** using the **PTP Service** switch, NOT the NTP switch.)



Note: Once TimeKeeper has been enabled, the Spectracom NTPd service will be replaced by the TimeKeeper NTP service, and vice versa.

After disabling TimeKeeper, the Spectracom NTP Service must be manually enabled again (MANAGEMENT > NTP Setup: In the panel NTP Services, slide NTP to: ON).

Next, ...

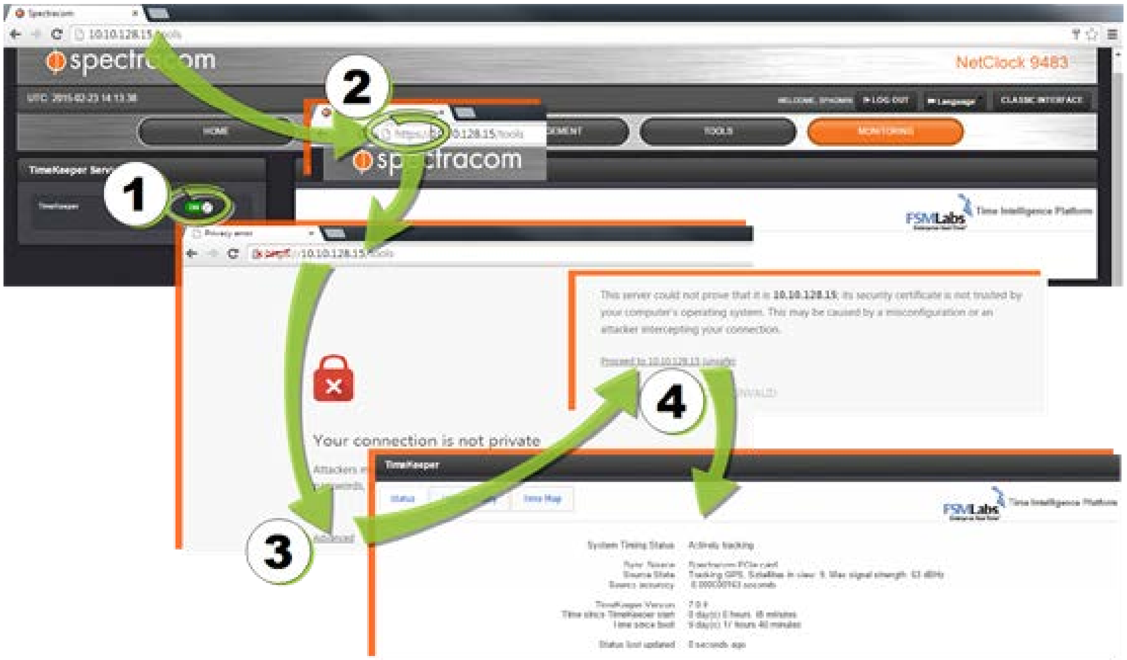
- **Configure** TimeKeeper, see "Configuring a TimeKeeper PTP Master" on page 129, or "Configuring TimeKeeper PTP Slaves" on page 132, or
- **Familiarize** yourself with the TimeKeeper functionality, see "Status Monitoring with TimeKeeper" below.

4.6.5 Status Monitoring with TimeKeeper

4.6.5.1 Enabling Status Monitoring

To display the TimeKeeper Status Monitoring functionality located on the right side of the Primary Navigation menu under the **MONITORING** tab, for security reasons you have to navigate over a secure http connection (https), see illustration below.

This login procedure must be carried out every time the browser is re-started.



Your connection is not private

This server could not prove that it is **10.10.128.15**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 10.10.128.15 (unsafe)

System Timing Status: Actively tracking

Sync Source: Spectracom PCIe card
Source State: Tracking GPS. Satellites in view: 9. Max signal strength: 43 dBHz
Source accuracy: 0.000000143 seconds

TimeKeeper Version: 7.0.9
Time since TimeKeeper start: 0 day(s) 0 hours, 18 minutes
Time since boot: 9 day(s) 17 hours 40 minutes

Status last updated: 0 seconds ago

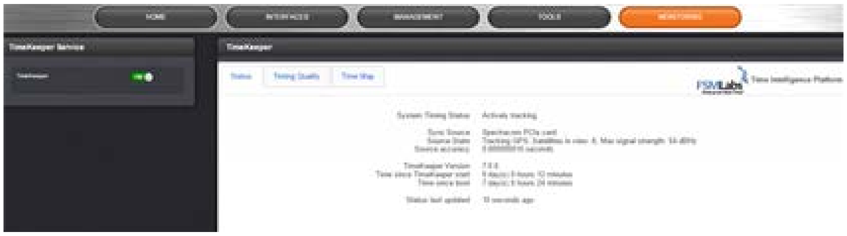
Figure 4-1: Enabling TimeKeeper Status Monitoring via https

Once the status monitoring functionality has been enabled, it can be accessed via the **MONITORING** button in the **Main Navigation** bar.

The TimeKeeper monitoring interface has three tabs: **Status**, **Timing Quality**, and **Time Map**:

4.6.5.2 TKL "Status" Tab

The Status tab provides information on the source currently tracked, as well as TimeKeeper system data, and system tracking information.



System Timing Status: Actively tracking

Sync Source: Spectracom PCIe card
Source State: Tracking GPS. Satellites in view: 8. Max signal strength: 34 dBHz
Source accuracy: 0.000000015 seconds

TimeKeeper Version: 7.0.8
Time since TimeKeeper start: 0 day(s) 0 hours, 12 minutes
Time since boot: 7 day(s) 0 hours 24 minutes

Status last updated: 10 seconds ago

Figure 4-2: TimeKeeper Status tab

4.6.5.3 TKL "Timing Quality" Tab

The Timing Quality tab offers detailed information on the quality of NTP and PTP sources, such as timing offsets and delays.

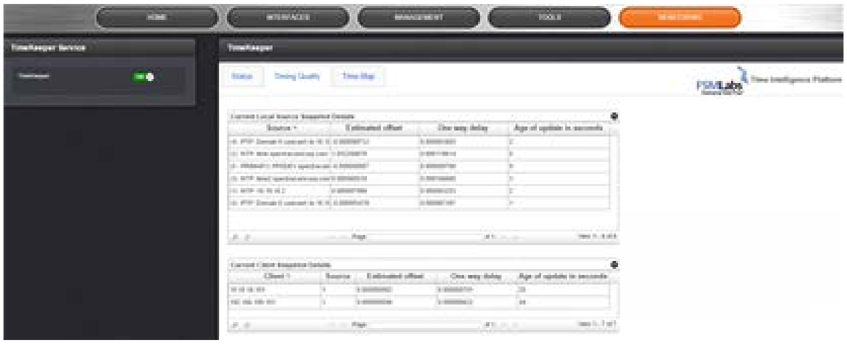


Figure 4-3: TimeKeeper Timing Quality tab

4.6.5.4 TKL "Time Map" Tab

Under the Time Map tab, TimeKeeper TKL visualizes the structure of the timing network environment, including all time sources, and other clients found on the network. Particularly with complex networks, this visualization tool can be of assistance when it comes to identifying architectural or accuracy problems.

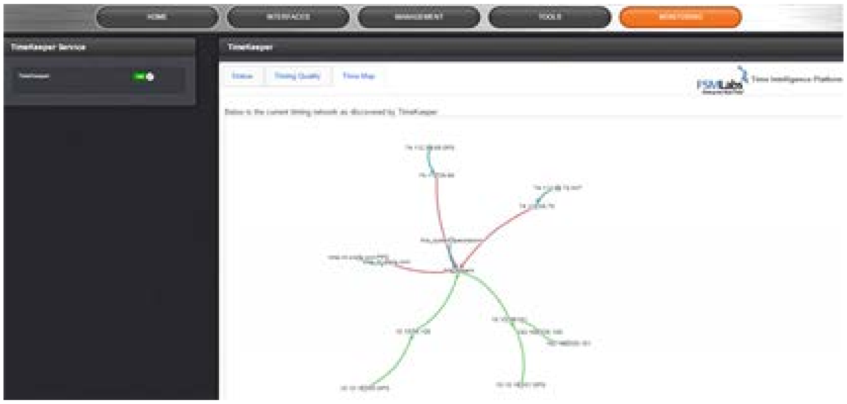


Figure 4-4: TimeKeeper Time Map tab

The connecting lines are color-coded:

- Red: NTP
- Green: PTP
- Blue: direct

Drag any node or time source with your computer mouse to adjust the graph.

Use the mouse wheel to zoom in or out.

Scroll to the bottom of the page to see additional features, such as **static display** and **hiding labels**.

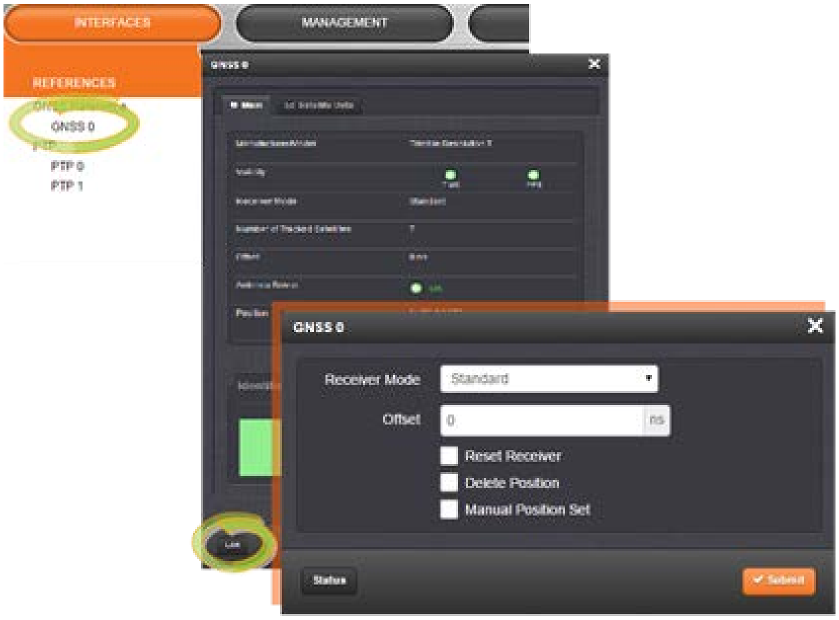
4.7 Editing the Settings of an Input Reference

Depending on the type of input reference, some of its settings may be user-editable. To access these settings for a given input reference, choose one of the two methods described below.

> **Note:** The illustrations shown below are only examples. The windows displayed in your Web UI may look differently, depending on the type of input reference (GNSS, IRIG, PNT, etc.).

There are two ways to access the settings **Status** window for an input reference:

Editing input reference settings, method 1:



Receiver Mode: Standard ▾

Offset: 0 ns

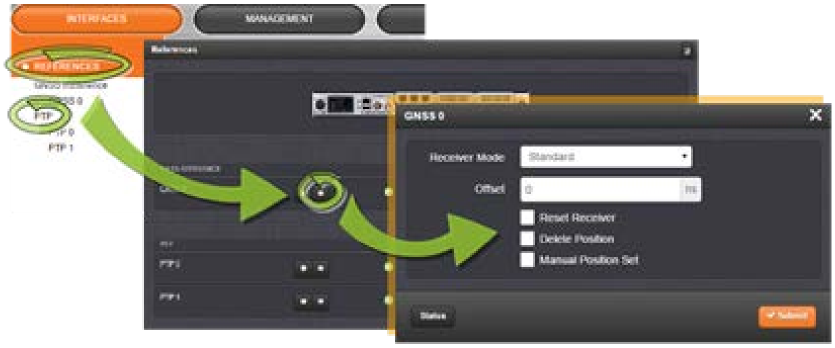
□ Reset Receiver

□ Delete Position

□ Manual Position Set

1. Under **INTERFACES/REFERENCES**, click the desired reference.
2. The Status window for the specific reference you selected will be displayed. Click the Edit button in the bottom-left corner.
3. The settings window for the chosen reference will be displayed. Edit the field(s) as desired.

Editing input reference settings, method 2:



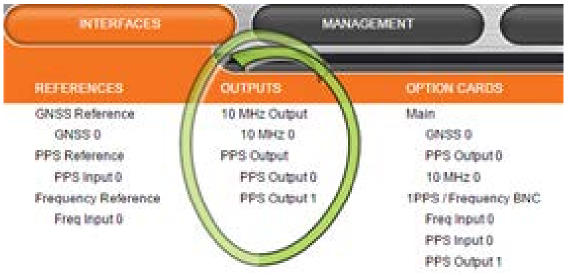
1. In the **INTERFACES/REFERENCES** drop-down menu, click **REFERENCES**, or an input reference category ("GNSS reference", for example).
2. In the pop-up Status window, click the GEAR button next to the desired input reference.
3. The settings window for the chosen reference will be displayed. Edit the field(s) as desired.

> **Note:** A particular option card might have more than one setting that can be adjusted. See "Option Cards Overview" on page 284 for the settings of any particular output or card.

4.8 Outputs Status Monitoring

Per standard configuration, SecureSync is equipped with one 1PPS and 10 MHz output interface. Additional outputs can be added by means of output option cards.

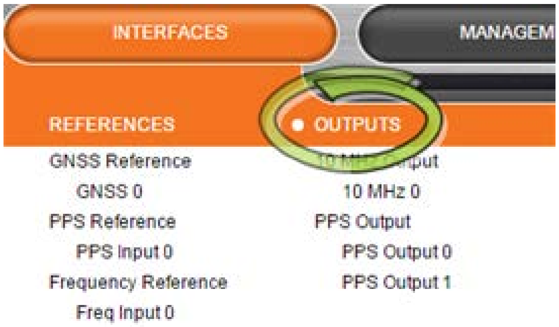
Outputs can be monitored in real time via the **INTERFACES** drop-down menu. The menu will populate dynamically, according to which outputs are installed



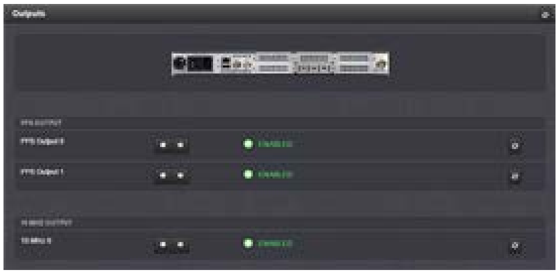
4.8.1 Monitoring the Status of All Outputs

To display a list of all the outputs installed in a SecureSync unit:

1. Select **INTERFACES** and click **OUTPUTS** in the menu heading.



2. The displayed Status window will list all the outputs installed, sorted by category.

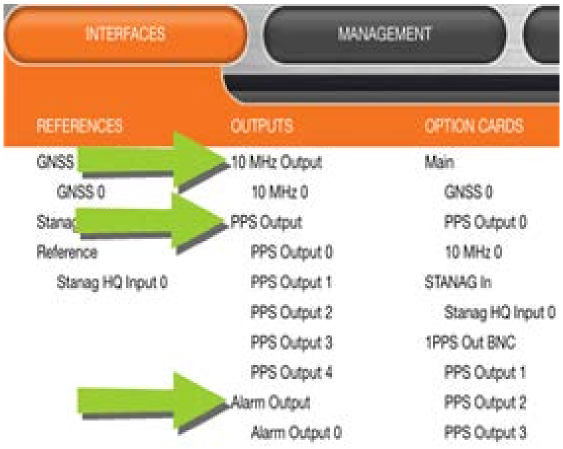


- To display more detailed information about a particular output, click the corresponding INFO button.
- To edit the settings of an output, click the GEAR button (see also "Editing Output Settings" on page 245.)
- To refresh the information displayed, click the REFRESH button (circling arrows icon).
- In the illustration of the rear panel, click on a connector to highlight the corresponding list entry.

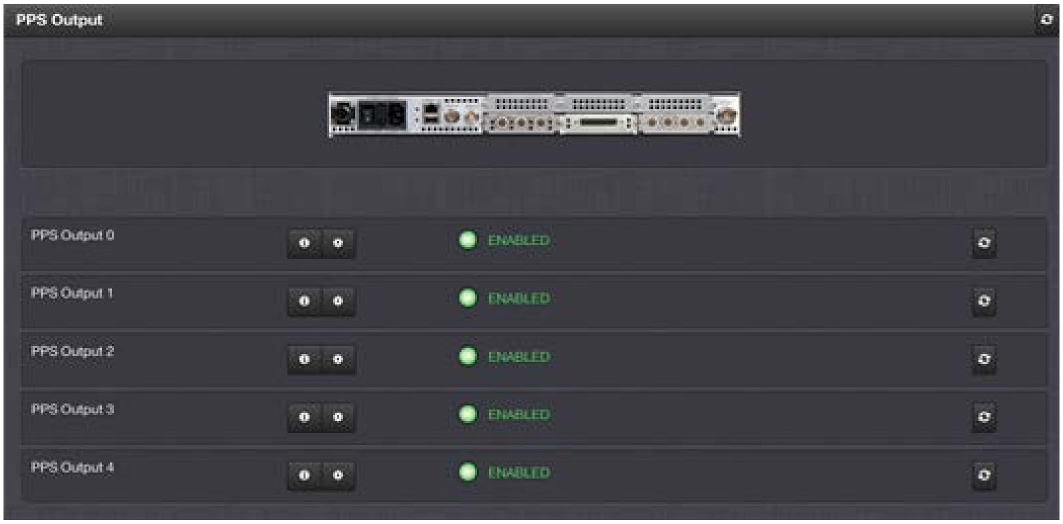
4.8.2 Monitoring all Outputs of one Type

To monitor all the outputs of a particular category (PPS, for example) simultaneously:

1. In the **INTERFACES/OUTPUTS** drop-down menu, click the desired output category (list items that are not recessed).



2. The pop-up Status window will display a list of all outputs of the selected category.



PPS Output

PPS Output 0	● ENABLED
PPS Output 1	● ENABLED
PPS Output 2	● ENABLED
PPS Output 3	● ENABLED
PPS Output 4	● ENABLED

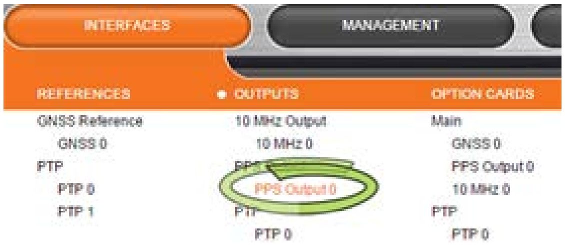
- » To display more detailed information about a particular output, click the corresponding INFO button.
- » To edit the settings of a given output, click the GEAR button (see also "Editing Output Settings" on the facing page.)
- » To refresh the information displayed, click the REFRESH button (circling arrows icon).
- » In the illustration of the rear panel, click on a connector to highlight the corresponding list entry.

4.8.3 Displaying Output Settings

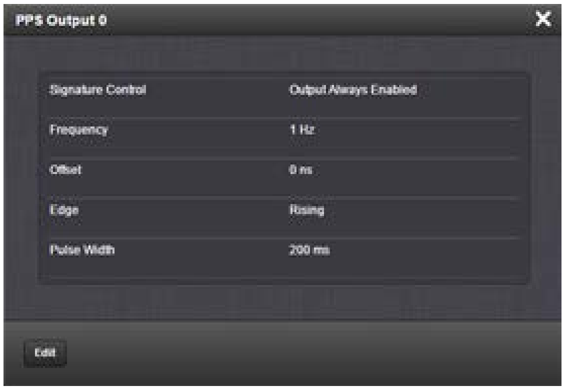
The outputs installed in your SecureSync unit have specific settings that can be reviewed, and–to some extent–edited.

To display the settings of an output:

1. In the **INTERFACES/OUTPUTS** drop-down menu, click the desired output.



2. The corresponding Status window will display.


PPS Output 0

Signature Control	Output Always Enabled
Frequency	1 Hz
Offset	0 ns
Edge	Rising
Pulse Width	200 ms

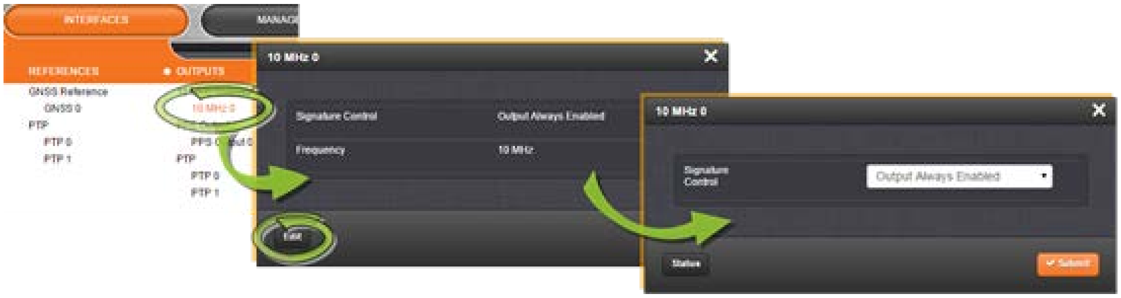
Click the Edit button in the bottom-left corner to configure settings that are user-editable. See also "Editing Output Settings" below.

4.9 Editing Output Settings

Depending on the type of output interface, some of its settings may be user-editable. To access these settings for a given output, choose one of the two methods described below.

> **Note:** The illustrations shown below are only examples. The windows displayed in your Web UI may look differently, depending on the type of output (1PPS, 10 MHz, PTP, etc.).

Editing output settings, method 1:

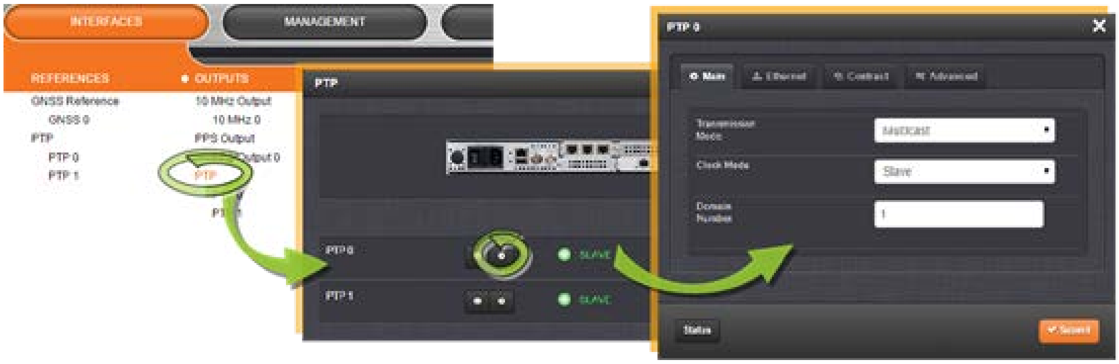


Signature Control: Output Always Enabled

Frequency: 10 MHz

1. Under **INTERFACES/OUTPUTS**, click the desired output.
2. The Status window for the specific reference you selected will be displayed. Click the **Edit** button in the bottom-left corner.
3. The settings window for the chosen output will be displayed. Edit the field(s) as desired.

Editing output settings, method 2:



Transmission Mode: Multicast

Clock Mode: Slave

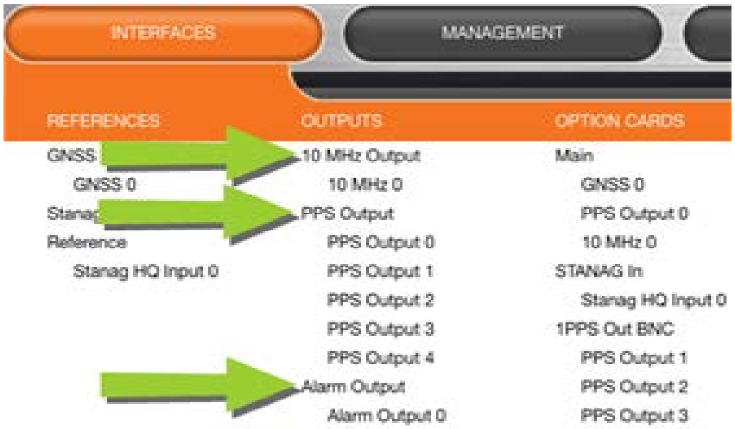
Domain Number: 1

1. In the **INTERFACES/OUTPUTS** drop-down menu, click **OUTPUTS**, or one of the output categories (not indented)
2. In the pop-up Status window, click the GEAR button next to the desired output.
3. The settings window for the chosen output will be displayed. Edit the field(s) as desired.

> **Note:** A particular option card might have more than one setting that can be adjusted. See "Option Cards Overview" on page 284 for the settings of any particular output or card.

4.10 Monitoring the Status of Option Cards

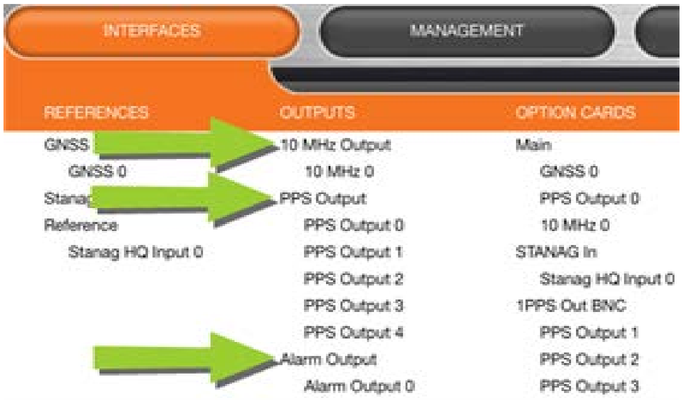
SecureSync’s installed option cards can be monitored in real time through the **INTERFACES/OPTION CARDS** drop-down menu. The menu will populate dynamically, according to which option cards are installed.



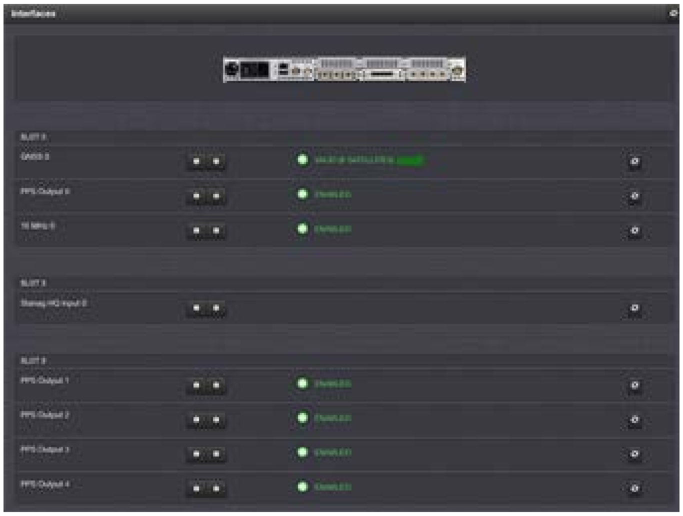
4.10.1 Monitoring the Status of ALL Option Cards

To monitor all option cards installed in your SecureSync:

1. Click on **OPTION CARDS** in the **INTERFACES** menu.



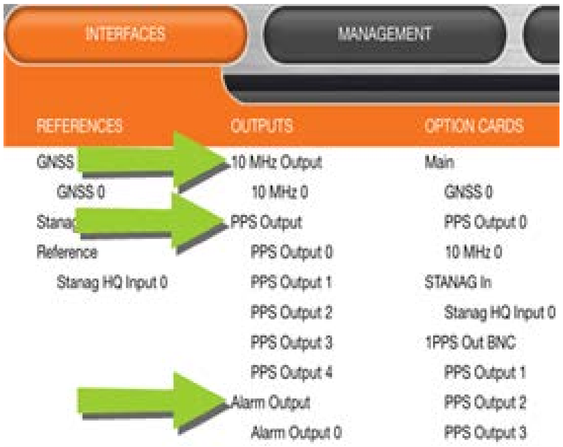
2. The resulting screen will display all installed option cards, and their current status.



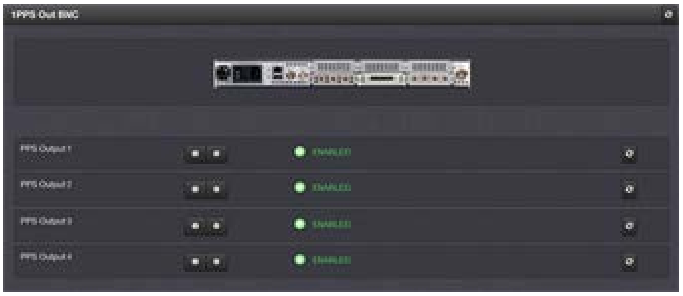
4.10.2 Monitoring the Status of a SPECIFIC Option Card

To monitor the status of a selected option card:

1. Navigate to the specific option card in the **INTERFACES/OPTION CARDS** drop-down menu.



2. The options window will display for the specific option card you chose.



1PPS Out BNC

PPS Output 1 ENABLED

PPS Output 2 ENABLED

PPS Output 3 ENABLED

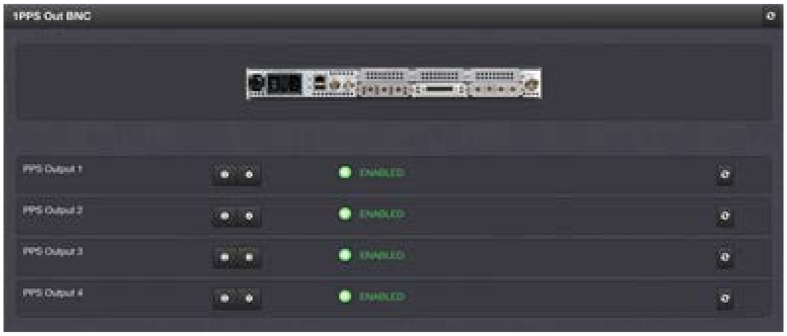
PPS Output 4 ENABLED

4.10.3 Monitoring an Option Card’s References and Outputs

To view the status of an option card’s references and outputs:

1. Navigate to the specific option card in the **INTERFACES/OPTION CARDS** drop-down menu.
2. Click on the INFO button for the reference or output whose status you wish to see.

> **Note:** A particular option card might have multiple references and/or outputs that can be viewed. See "Option Cards Overview" on page 284 for the settings of any particular option card.



1PPS Out BNC

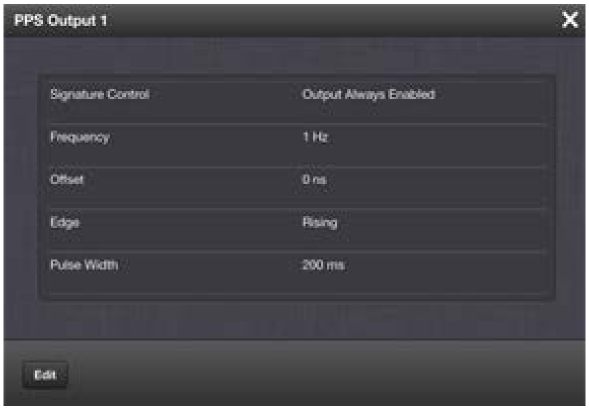
PPS Output 1 ENABLED

PPS Output 2 ENABLED

PPS Output 3 ENABLED

PPS Output 4 ENABLED

3. A **Status** window for that reference or output will display.



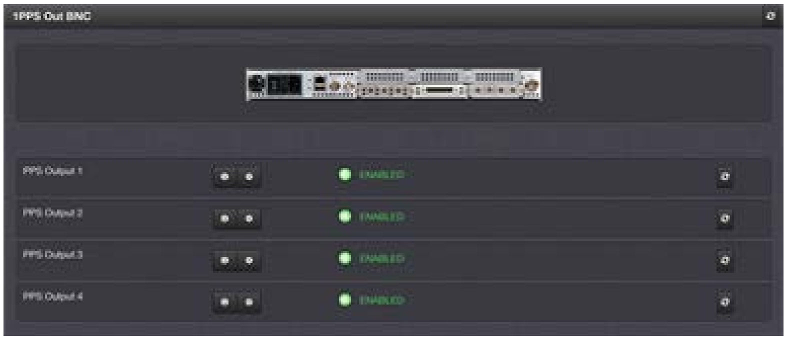
PPS Output 1

Signature Control	Output Always Enabled
Frequency	1 Hz
Offset	0 ns
Edge	Rising
Pulse Width	200 ms

4.10.3.1 Editing an Option Card’s References and Outputs

To edit the settings of an option card’s references or outputs:

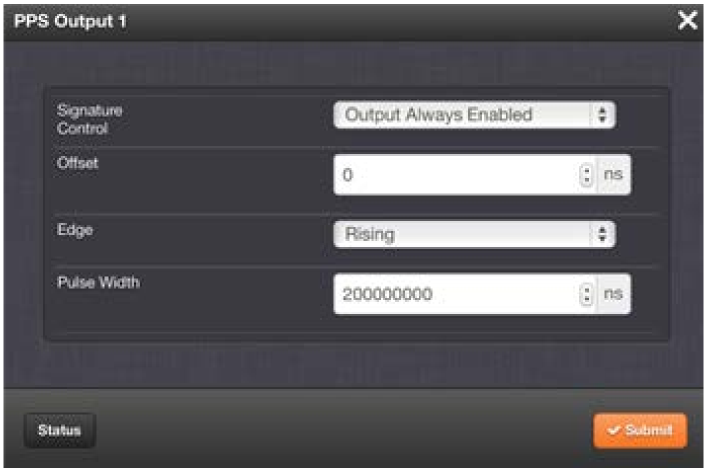
1. Navigate to the specific option card in the **INTERFACES/OPTION CARDS** drop-down menu.
2. Click on the GEAR button for the reference or output you wish to edit.



1PPS Out BNC

PPS Output 1	ENABLED
PPS Output 2	ENABLED
PPS Output 3	ENABLED
PPS Output 4	ENABLED

3. The Edit window for that reference or output will display.



PPS Output 1

Signature Control: Output Always Enabled

Offset: 0 ns

Edge: Rising

Pulse Width: 200000000 ns

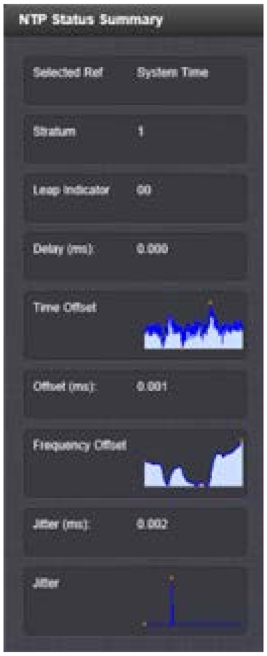
4. Edit the field(s) as desired.

> **Note:** If you know the individual reference or output whose status you wish to see, you can access the Status window of that reference or output directly through the INTERFACES/REFERENCES or INTERFACES/OUTPUTS drop-down menu.

4.11 NTP Status Monitoring

SecureSync's **NTP Status Summary** provides a means to monitor NTP status and performance parameters relevant to your SecureSync at a glance.

1. To access the **NTP Status Summary** panel, navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.



Selected Ref	System Time
Stratum	1
Leap Indicator	00
Delay (ms):	0.000
Offset (ms):	0.001
Jitter (ms):	0.002

2. The **NTP Status Summary** panel is at the lower left of the screen. The panel contains the following information:

   - **Selected Ref**—The reference SecureSync is currently using.
   - **Stratum**—This is the stratum level at which SecureSync is operating.
   - **Leap Indicator**—The leap indicator bits (usually 00). See "Leap Second Alert Notification" on page 277.
   - **Delay (ms)**—The measured one-way delay between SecureSync and its selected reference.
   - **Time Offset**—This is a graphical representation of the system time offset over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel containing a larger, more detailed view of the graph. See "The NTP Time Offset Performance Graph" on the facing page.
   - **Offset (ms)**—Displays the configured 1PPS offset values.
   - **Frequency Offset**—This is a graphical representation of the system frequency offset over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel containing a larger, more detailed view of the graph. See "The NTP Frequency Offset Performance Graph" on page 254.
   - **Jitter (ms)**—Variance (in milliseconds) occurring in the reference input time (from one poll to the next).
   - **Jitter**—This is a graphical representation of the system jitter over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel

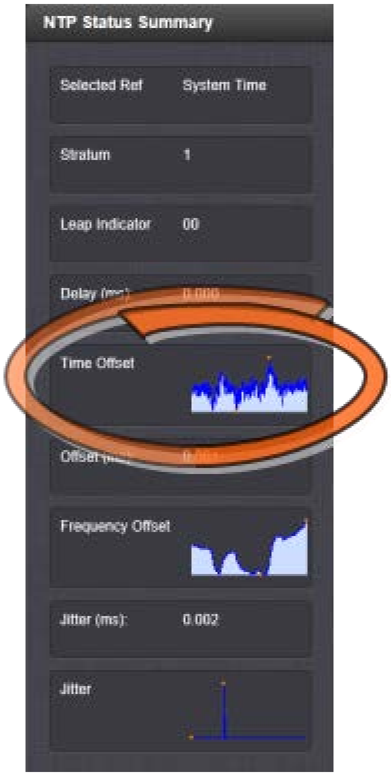
containing a larger, more detailed view of the graph. See "The NTP Jitter Performance Graph" on page 256.

> **Note:** This panel is updated every 30 seconds, or upon clicking the browser refresh button.

4.11.1 The NTP Time Offset Performance Graph

To view the NTP **Time Offset** performance graph:

1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. In the **NTP Status Summary** panel locate the **Time Offset** graph.



NTP Status Summary

Selected Ref System Time

Stratum 1

Leap Indicator 00

Delay (ms): 0.000

Time Offset

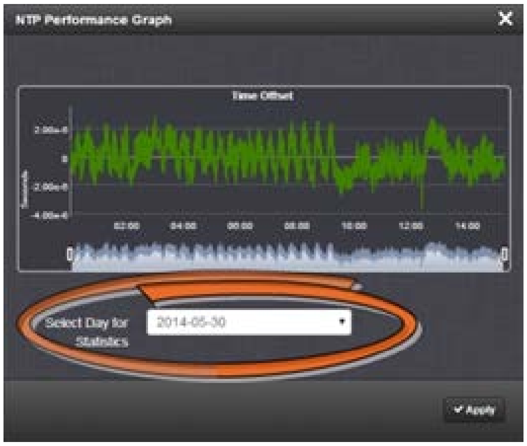
Offset (ms): [illegible]

Frequency Offset

Jitter (ms): 0.002

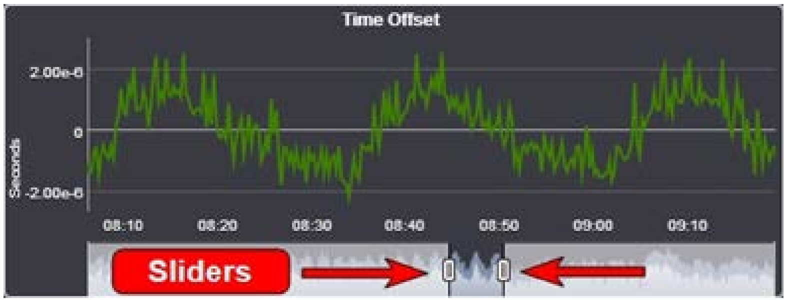
Jitter

3. Click the graph in the **NTP Status Summary** panel.
4. The **NTP Performance Graph** panel will appear.



Select Day for Statistics: 2014-05-30

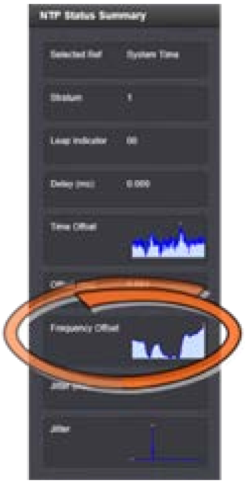
5. To select the statistics for a particular day, select a date from the drop-down list in the Select Day for Statistics field. The default date is the present date. Click **Apply**.
6. To display a higher resolution graph for a shorter time span, move one or both time sliders at the bottom of the graph inwards.



4.11.2 The NTP Frequency Offset Performance Graph

To view the NTP **Frequency Offset** performance graph:

1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. In the **NTP Status Summary** panel locate the **Frequency Offset** graph.



NTP Status Summary

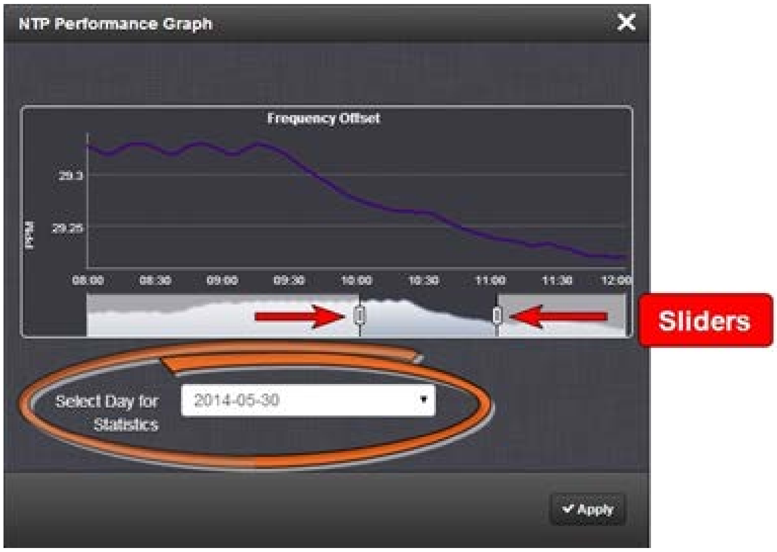
Selected Ref System Time

Stratum 1

Leap Indicator 00

Delay (ms) 0.000

3. Click the graph in the **NTP Status Summary** panel.
4. The **NTP Performance Graph** panel will appear (the data may be displayed with a delay). The X-axis represents time, the Y-axis shows the frequency offset in parts-per-million (PPM); e.g. 290 PPM is equivalent to .0290 percent.



NTP Performance Graph

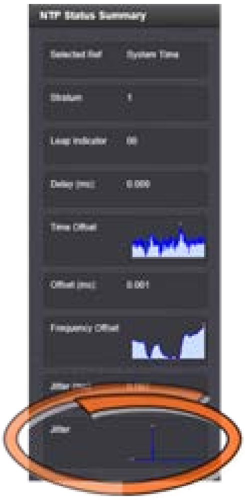
Select Day for Statistics 2014-05-30

5. To select the statistics for a particular day, select a date from the drop-down list in the **Select Day for Statistics** field (highlighted in green in the illustration above). The default date is the present date. Click the **Apply** button.
   - » To display a higher resolution graph of a shorter time frame, move one or both of the two sliders inwards.

4.11.3 The NTP Jitter Performance Graph

To view the NTP **Jitter** performance graph:

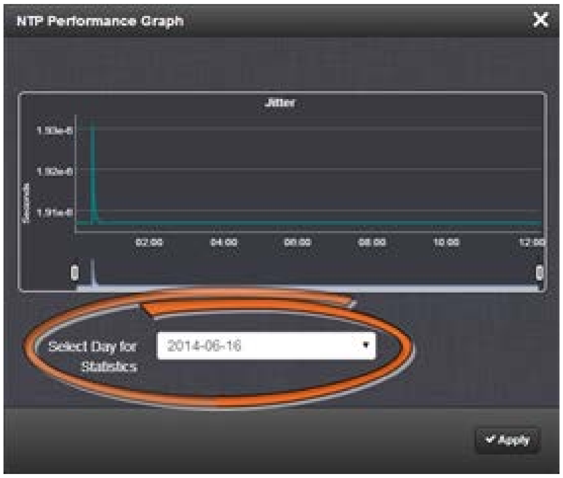
1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. In the **NTP Status Summary** panel locate the **Jitter** graph.



NTP Status Summary

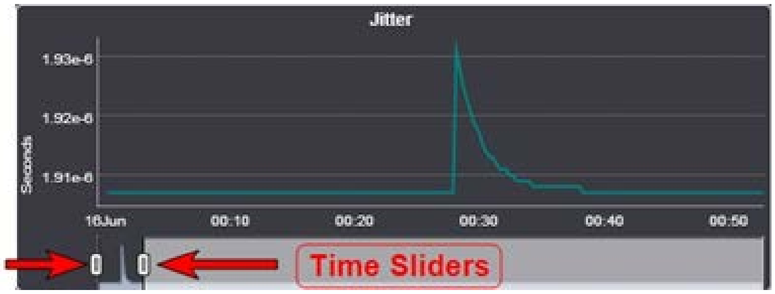
Selected Ref	System Time
Stratum	1
Leap Indicator	00
Delay (ms)	0.000
Time Offset	
Offset (ms)	0.001
Frequency Offset	
Jitter (ms)	[illegible]
Jitter	

3. Click the graph in the **NTP Status Summary** panel.
4. The **NTP Performance Graph** panel will appear.



Select Day for Statistics: 2014-06-16

5. To select the statistics for a particular day, select a date from the drop-down list in the **Select Day for Statistics** field. The default date is the present date. Click the **Apply** button.
   - » To display a higher resolution graph for a shorter time span, move one or both time sliders at the bottom of the graph inwards.



4.12 Temperature Management

SecureSync is equipped with one cooling fan, located behind the right-hand side of the front panel, and several hardware temperature sensors, including:

- the **board** temperature near the CPU
- the **CPU** temperature
- the air temperature near the **oscillator**.

Note: SecureSync units produced before 2015 may not be equipped with the oscillator sensor. They can be retrofitted, if so requested. For additional information, contact Technical Support (see "Technical Support" on page 514).

Temperature readings are performed once per minute. The temperature data is logged, and can be visualized via graphs integrated into the Web UI. The temperature readings can also be used to control the fan. For details see below.

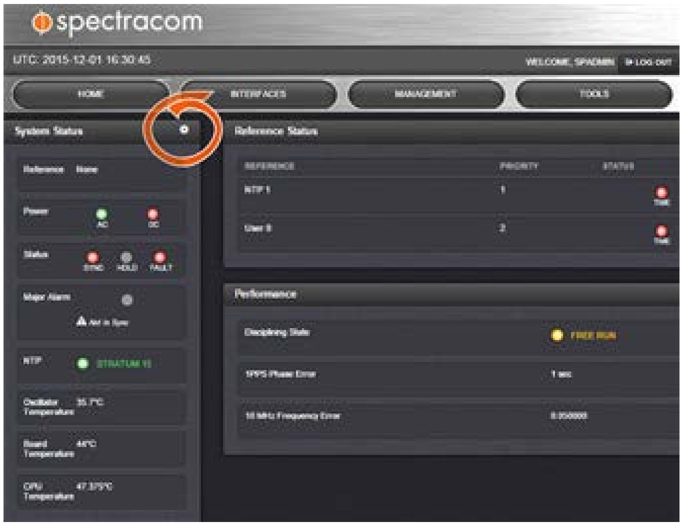
4.12.1 Fan Control Feature

Fan Control allows you to define a temperature range for the fan to turn OFF and ON.

Note: SecureSync units produced before Dec. 2015 are not equipped with the Fan Control feature.

Does my SecureSync have Fan Control?

- To find out, navigate to the **HOME** screen. Your unit is equipped with the Fan Control feature, if there is a GEAR icon displayed in the **System Status** panel:



Reference None

Power AC DC

Status SYNC HOLD FAULT

Major Alarm

Not in Sync

NTP STRATUM 15

Oscillator Temperature 35.7°C

Board Temperature 44°C

CPU Temperature 47.375°C

REFERENCE	PRIORITY	STATUS
NTP 1	1	TIME
User 0	2	TIME

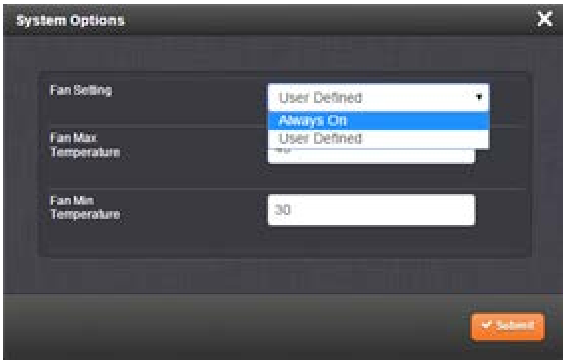
Disciplining State FREE RUN

1PPS Phase Error 1 sec

10 MHz Frequency Error 0.000000

To enable user-defined Fan Control:

The default fan setting is ALWAYS ON. To apply custom fan temperature settings, navigate to the **HOME** screen. Then, in the **System Status** panel, click the **Gear** icon in the upper right-hand corner. The **System Options** window will open:



Fan Setting: User Defined

Fan Max Temperature: 40

Fan Min Temperature: 30

Here you can choose between the **Fan Setting**s:

- **Always On** [Default]: The fan runs all the time.
- **User Defined**: You determine the:
  - **Fan Max Temperature**: The CPU temperature in °C at which the fan will turn ON. It is advisable to set this temperature no higher than 40°C.
  - **Fan Min Temperature**: The CPU temperature in °C at which the fan will turn OFF (the default is 30°C).

The temperature between the two threshold values is the range in which the temperature is allowed to rise before the fan turns on again.

In addition there is a hardware temperature sensor that will automatically turn the fan ON if the measured temperature is over 40°C.

4.12.2 Temperature Monitoring

You can monitor the unit's measured temperatures actively by inspecting the temperature graphs in the Web UI, or passively by setting up automatic alarm messages.

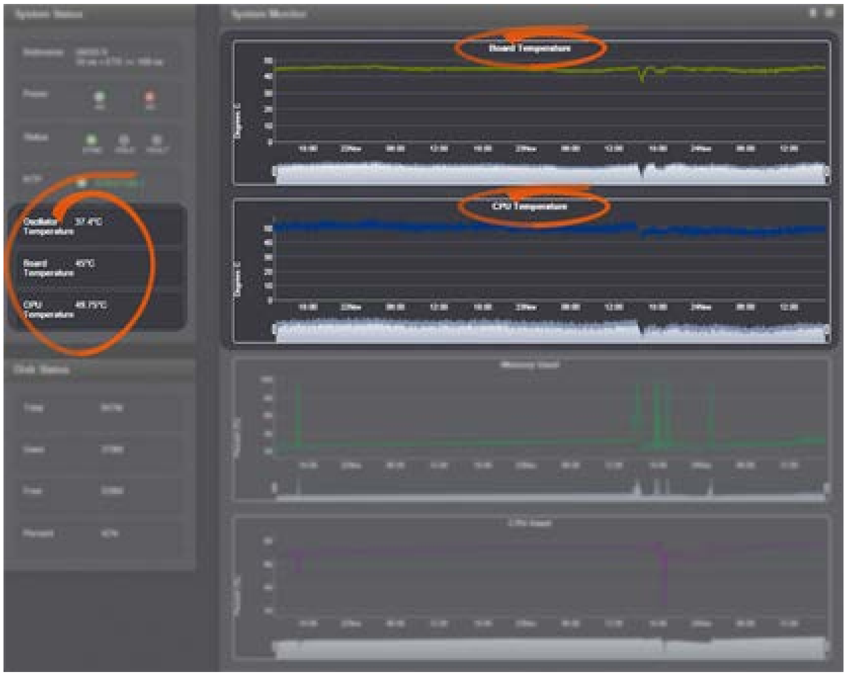
Alarm notifications can be generated via SNMP Traps and Emails, as well as log messages in the Alarm and Event Logs. The alarms may optionally be masked.

Also, it is possible to implement a delay by setting the number of times the 1/minute readings need to exceed a temperature threshold before an alarm is triggered.

4.12.2.1 Monitoring CPU and Board Temperature

Current readings for Oscillator/Board/CPU Temperature are displayed in the **System Status** panel, which can be accessed via the **HOME** screen, or via **TOOLS > System Monitor**.

CPU and Board Temperature graphs are displayed under **TOOLS > System Monitor**:

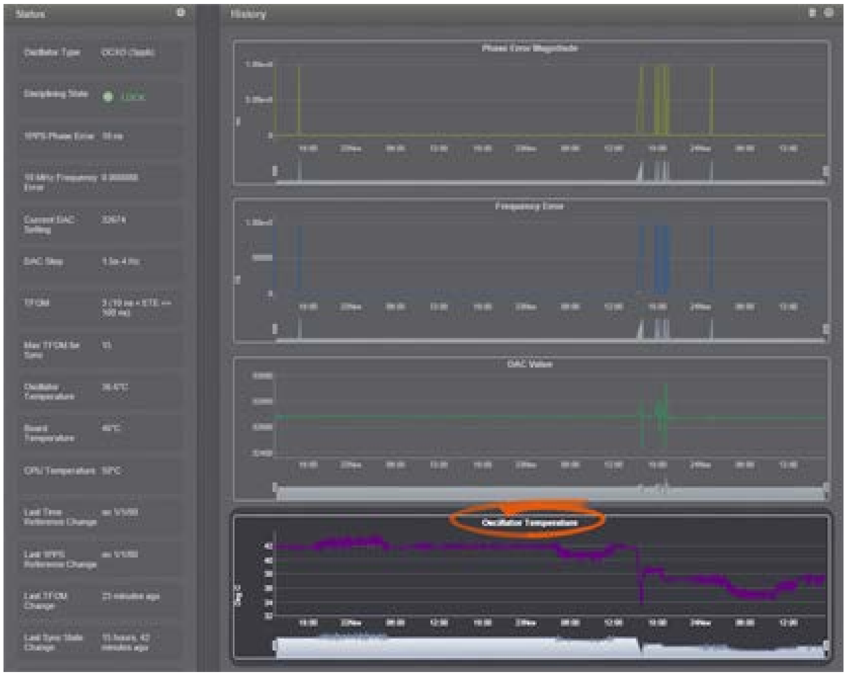


Oscillator Temperature 37.4°C

Board Temperature 45°C

CPU Temperature 49.75°C

The graph for the Oscillator Temperature is displayed under **MANAGEMENT > OTHER: Disciplining**:

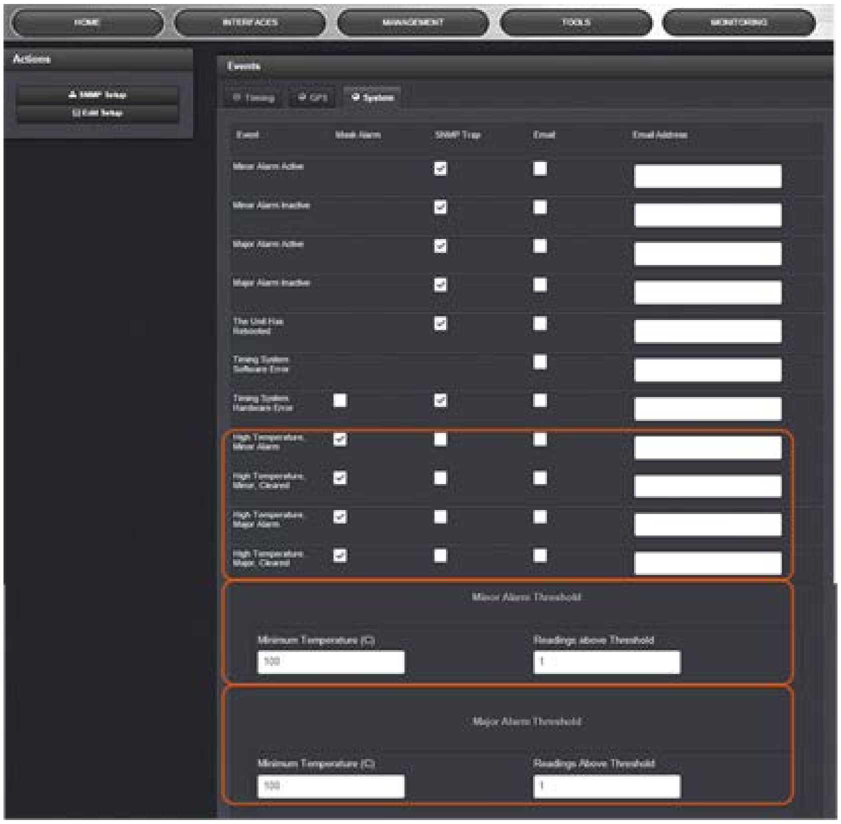


Oscillator Type	OCXO (Spab)
Disciplining State	● LOCK
1PPS Phase Error	10 ns
10 MHz Frequency Error	0.000000
Current DAC Setting	32674
DAC Step	1.5e-4 Hz
TFOM	3 (10 ns < ETE <= 100 ns)
Max TFOM for Sync	15
Oscillator Temperature	36.6°C
Board Temperature	40°C
CPU Temperature	50°C
Last Time Reference Change	on 1/1/00
Last 1PPS Reference Change	on 1/1/00
Last TFOM Change	23 minutes ago
Last Sync State Change	15 hours, 42 minutes ago

Temperature readings are subject to environmental conditions and hardware configuration e.g., oscillator type. Under normal operating conditions, all temperatures should remain fairly constant. Drastic changes may indicate e.g., a problem with the fan. Note that the oscillator temperature will have a direct impact on its accuracy, i.e. there is a strong correlation between disciplining performance and oscillator temperature.

4.12.2.2 Setting Temperature Monitoring Alarms

Navigate to **MANAGEMENT > Notifications**. In the **Events** panel, select the **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

Minimum Temperature (C): 100

Readings above Threshold: 1

Major Alarm Threshold

Minimum Temperature (C): 100

Readings Above Threshold: 1

Under the **System** tab, you can set Notifications for Minor and Major Alarms/Clearances.

Also, you can set the temperature threshold value for Minor/Major alarms, and define a retry value by determining how many readings (1/min.) the temperature must exceed the threshold value before an alarm/clearance is triggered.

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.

4.12.3 Downloading Temperature Data

It is possible to download the temperature data e.g., to plot your own temperature graphs, or because Spectracom Technical Support inquires about this data for diagnostic purposes in the event of technical problems.

» To download the logged data used to generate the displayed graphs, navigate to any panel that displays one or more graphs (see above), and click on the **Arrow** icon in the top-right corner.

A file named `systemMonitorLog.csv` file will be generated in your designated download folder.

4.12.4 Deleting Temperature Data

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.

» To delete the logged data used to generate the displayed graphs, click the TRASH CAN icon in the top-right corner of the panel.

Note that re-populating the graphs with fresh data will take several minutes.

4.12.5 Further reading

See also: "Troubleshooting the Front Panel Cooling Fan" on page 463

4.13 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 276.

4.13.1 Types of Logs

SecureSync generates log files for the following event categories:

System Log

Displays log entries related to the Timing System events and daemon events (such as the Alarms, Monitor, Notification, or SNMP daemons starting or stopping, etc.)

Events Log

Displays log entries related to GNSS reception status changes, Sync/Holdover state changes, SNMP traps being sent, etc. Examples include:

- **Reference Change**: SecureSync has switched from one input reference to another (for example, IRIG was the selected input being used, but now GNSS is the selected reference).
- **GPS Antenna Problem**: The GPS Antenna Problem alarm indicates the GNSS receiver has detected an over-current or undercurrent condition (an open or short exists in the GNSS antenna cable, or the GNSS antenna is not connected to SecureSync). The receiver will attempt to continue the normal acquisition and tracking process regardless of the antenna status. The current draw measurements that will indicate an antenna problem are:
  - Under-current indication < 8 mA
  - Over-current indication > 80 mA

Note: This alarm condition will also be present if a GNSS antenna splitter that does not contain a load to simulate an antenna being present is being used.

- **GPS Antenna OK**: The antenna coax cable was just connected or an open or short in the antenna cable was being detected but is no longer being detected.
- **Frequency Error**: The oscillator's frequency was measured and the frequency error was too large. Or, the frequency couldn't be measured because a valid input reference was not available.
- **Frequency Error cleared**: The Frequency Error alarm was asserted but was then cleared.
- **In Holdover**: Input references were available, but all input references have since been lost. If the references are not restored before the Holdover period expires, time sync will be lost.
- **No longer in Holdover**: Input references were lost at one point (or declared not valid), but have since been restored OR the Input references were not restored before the Holdover period expired (Time Sync alarm is asserted).
- **In Sync**: SecureSync is synchronized to its Time and 1PPS inputs.
- **Not In Sync**: SecureSync is not synchronized to its Time and 1PPS inputs and is not currently in Holdover. NTP will indicate to the network that it is Stratum 15 and so the time server likely be ignored as a time reference.
- **Sending trap for event 1 (SNMPSAD)**: An SNMP trap was sent by the SNMP agent to the SNMP Manager. The event number in this entry indicates which SNMP trap was sent.
- **The Unit has Rebooted**: SecureSync was either rebooted or power cycled.

Alarms Log

Displays log entries for the Timing System, for example:

- **The Unit has Rebooted**: SecureSync was either rebooted or power cycled.
- **In Holdover**: Input references were available, but all input references have since been lost. If the references are not restored before the Holdover period expires, time sync will be lost.

- **No longer in Holdover**: Input references were lost at one point (or declared not valid), but have since been restored OR the Input references were not restored before the Holdover period expired (Time Sync alarm is asserted).
- **In Sync**: SecureSync is synchronized to its selected Time and 1PPS reference inputs.
- **Not In Sync**: SecureSync is not synchronized to its Time and 1PPS inputs and is not currently in Holdover. NTP will indicate to the network that it is Stratum 15 and so the time server likely be ignored as a time reference.
- **Frequency Error**: The oscillator's frequency was measured and the frequency error was too large. Or, the frequency couldn't be measured because a valid input reference was not available.
- **Reference change**: SecureSync has selected a different Time and 1PPS input reference for synchronization. Either the previously selected input reference was declared not valid (or was lost), so a lower priority reference (as defined by the Reference Priority Setup table) is now selected for synchronization OR a valid reference with higher priority than the previous reference is now selected for synchronization.

EXAMPLE:

GNSS is the highest priority reference with IRIG input being a lower priority. SecureSync is synced to GNSS and so GNSS is the selected reference. The GNSS antenna is disconnected and IRIG becomes the selected reference. The Reference change entry is added to this log.

Timing Log

Displays log entries related to Input reference state changes (for example, IRIG input is not considered valid), antenna cable status. Examples include:

- **GRGR = GNSS Reference[1] antenna fault**: The GNSS Antenna Problem alarm indicates the GNSS receiver has detected an over-current or undercurrent condition (an open or short exists in the GNSS antenna cable, or the GNSS antenna is not connected to SecureSync). The receiver will attempt to continue the normal acquisition and tracking process regardless of the antenna status.
- **GR antenna ok**: The antenna coax cable was connected at this time or an open or short in the antenna cabling was occurring but is no longer being detected.

GPS Qualification Log

If SecureSync is connected to a GNSS antenna and is tracking satellites, this log contains a running hourly count of the number of GNSS satellites tracked each hour. This history data can be used to determine if a GNSS reception problem exists and whether this is a continuous or intermittent reception issue.

GNSS reception may be displayed as cyclic in nature. A cyclic 12 hour pattern of decreased GNSS reception typically indicates that the GNSS antenna has an obstructed view of the horizon.

[1] GR = GNSS Reference

The GNSS satellites are in a 12-hour orbit, so if part of the sky is blocked by large obstructions, at the same time every day (at approximately 12 hour intervals), the GNSS reception may be reduced or may vanish altogether. If this occurs, the antenna should be relocated to afford it an unobstructed view of the sky.

Every hour (displayed in the log as UTC time), SecureSync counts the total number of satellites that were tracked during that hour. The GNSS qualification log shows the number of satellites that were tracked followed by the number of seconds that the particular number of satellites were tracked during the hour (3600 seconds indicates a full hour). The number to the left of the "=" sign indicates the number of satellites tracked and the number to the right of the "=" sign indicates the number of seconds (out of a total of 3600 seconds in an hour) that the unit was tracking that number of satellites. For example, "0=3600" indicates the unit was tracking 0 satellites for the entire hour, while "0=2700 1=900" indicates the unit was tracking one satellite for 900 seconds, but for the remaining portion of the hour it was tracking zero satellites.

Every hourly entry in the log also contains a quality value, represented by "Q= xxxx" (where x can be any number from 0000 through 3600). The Qualification log records how many satellites were tracked over a given hour. If for every second of the hour a tracked satellite was in view, the Quality value will equal 3600. For every second SecureSync tracked less than the minimum number of satellites, the value will be less than 3600. The minimum requirement is one satellite at all times after the unit has completed the GNSS survey and indicates "Stationary". A minimum of four satellites are required in order for the GNSS survey to be initially completed.

If all entries in the qualification log are displayed as "0=3600", a constant GNSS reception problem exists, so the cause of the reception issue is continuous. If the unit occasionally shows 0=3600 but at other times shows that 1 through 12 have numbers of other than "0000", the reception is intermittent, so the cause of the reception issue is intermittent. If the Quality value normally equals 3600 but drops to lower than 3600 about every 12 hours, the issue is likely caused by the GNSS antenna having an obstructed view of the sky.

Example GPS Qualification Log Entry:

```
6 = 151 7 = 1894 8 = 480 9 = 534 10 = 433 12 = 108 Q = 3600
```

In this example, SecureSync tracked no less that 6 satellites for the entire hour. Out of the entire hour, it was tracking 6 satellites for a cumulative total of 151 seconds (not necessarily in a row). For the duration of the hour, it was tracking, 7, 8, 9, 10 and 12 satellites for a period of time. Because it was tracking at least at least one satellite for the entire hour, this Quality value is Q=3600.

Note: If SecureSync is not connected to a GNSS antenna, this log will remain empty.

Oscillator Log

Displays log entries related to oscillator disciplining. Provides the calculated frequency error periodically while synchronizing to a reference.

TimeKeeper Log

Displays log entries related to TimeKeeper (if activated).

Journal Log

Displays log entries created for all configuration changes that have occurred (such as creating a new user account, for example).

Update Log

Displays log entries related to software updates that have been performed.

Authentication Log

Displays log entries for authentication events (e.g., unsuccessful login attempts, an incorrectly entered password, etc.) that are made to SecureSync’s command line interfaces (such as the front panel setup port, telnet, SSH, FTP, etc.).

NTP Log (Not Configurable)

The NTP log displays operational information about the NTP daemon, as well as NTP throughput statistics (e.g., packets/sec.). Examples for entries in this log include indications for when NTP was synchronized to its configured references (e.g., it became a Stratum 1 time server), as well as stratum level of the NTP references.

The NTP throughput statistics data can be utilized to calculate mean values and the standard deviation.

Example log entries include:

- **Synchronized to (IP address), stratum=1**: NTP is synchronizing to another Stratum 1 NTP server.
- **ntp exiting on signal 15**: This log entry indicates NTP is now indicating to the network that it is a Stratum 15 time server because it is not synchronized to its selected reference.
- **Time reset xxxxx s**: These entries indicate time corrections (in seconds) applied to NTP.
- **No servers reachable**: NTP cannot locate any of its configured NTP servers.
- **Synchronized to PPS(0), stratum=0**: NTP is synchronized using the PPS reference clock driver (which provides more stable NTP synchronization).

4.13.2 Local and Remote Logs

SecureSync logs are all stored internally by default. With the exception of the NTP log, all logs can also be configured to be stored externally, if desired.

The log entries for the logs can also be configured to be automatically sent to a Syslog Server for external log storage. In order for these logs to be sent to a Syslog server, each desired log needs to be configured for Syslog operation. With the exception of the Authentication and NTP logs, all log setup options can be configured from the Logs Configuration page.

Note: The NTP log has no available configuration options.

In each log, entries appear with the most recent events first (i.e., in reverse chronological order, starting from the top).

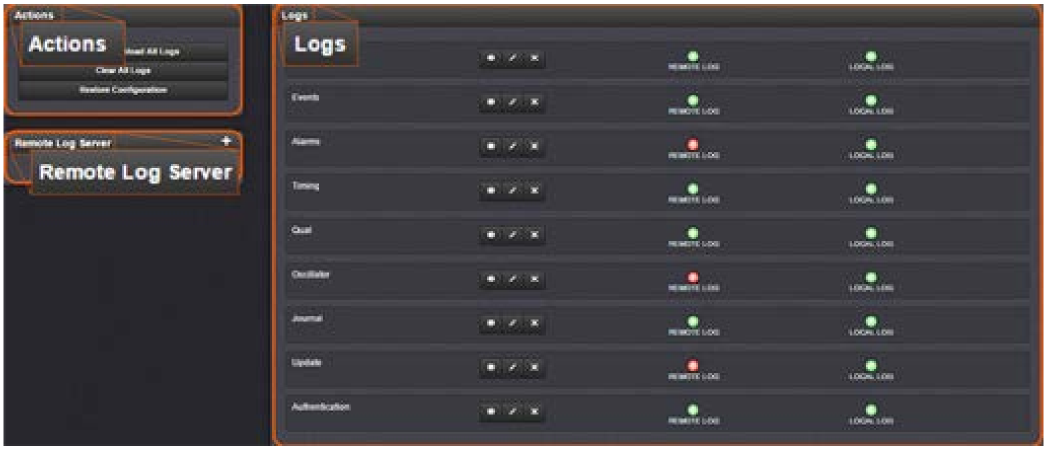
To set up a remote log server, see "Setting up a Remote Log Server" on page 274.

4.13.3 The Logs Screen

The **Logs** Screen not only provides a status overview of all log types, but also allows for all logs to be configured.

4.13.3.1 Accessing the Logs Screen

1. Navigate to **MANAGEMENT** > **OTHER**: **Log Configuration.**
2. The **Logs** screen will appear. It is divided into three panels:



The Logs panel

The **Logs** panel on the right-hand side provides a logs overview, displaying the status of all SecureSync logs.

- To read a log, click the corresponding INFO button.
- To configure a log, click the corresponding PENCIL button.
- To clear a log, click the X-button.

Note: The Clear File feature does not delete any of the logs that have been sent to and stored in a Syslog server.

A green indicator lamp shows if events of the corresponding log category are stored remotely or locally.

The Logs Actions panel

The **Actions** panel on the upper-left corner of the **Logs** screen allows you to perform batch actions on your logs:

- **Save and Download All Logs**–Save and download all the logs on SecureSync. See also: "Saving and Downloading Logs" on page 270.
- **Clear All Logs**–Clear all the logs on SecureSync. See also: "Clearing Logs" on page 276.
- **Restore Configuration**–Restore all log configurations to their factory settings. See also: "Restoring Log Configurations" on page 275.

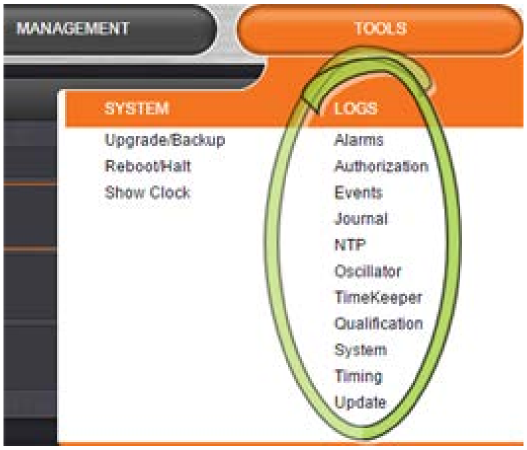
The Remote Log Server panel

The **Remote Log Server** panel, which is where you set up and manage logs on one or more remote locations. See also: "Setting up a Remote Log Server" on page 274.

4.13.4 Displaying Individual Logs

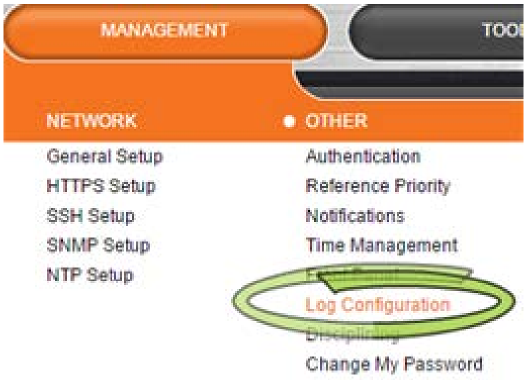
Next to displaying a **Logs** overview (see "The Logs Screen" on the previous page), it is also possible to access individual SecureSync logs:

1. From the **TOOLS** drop-down menu, select the desired **Logs** category (for example, “Alarms”, or “Events”) from the right-hand column.

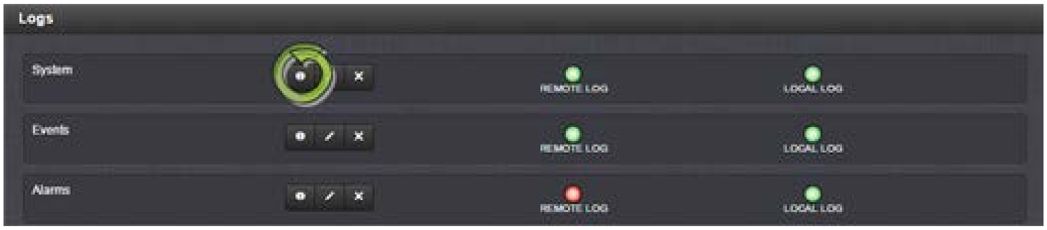


OR

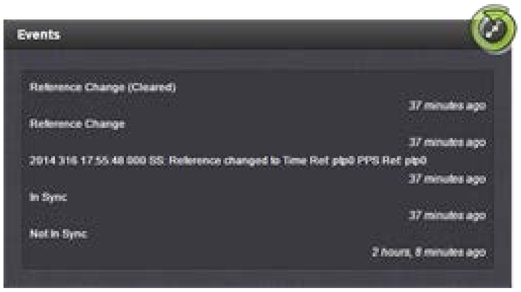
1. Access the **Logs** screen through the **MANAGEMENT/OTHER/Log Configuration** drop-down menu.



2. The **Logs** screen will be displayed:

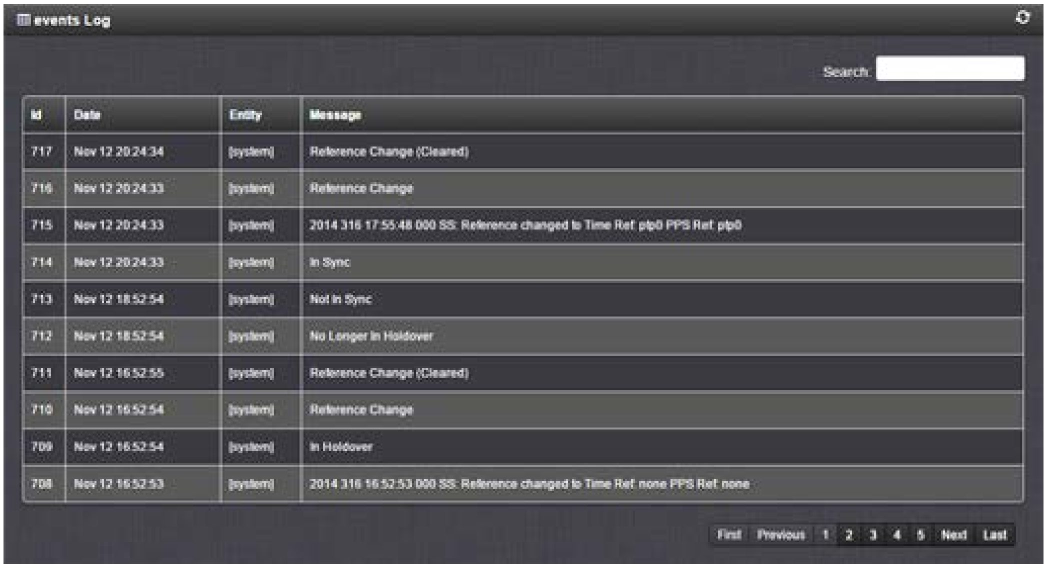


3. Click on the **INFO** button for the desired log category.



```
Reference Change (Cleared)
                                                   37 minutes ago
Reference Change
                                                   37 minutes ago
2014 316 17:55:48 000 SS: Reference changed to Time Ref: ptp0 PPS Ref: ptp0
                                                   37 minutes ago
In Sync
                                                   37 minutes ago
Not In Sync
                                               2 hours, 8 minutes ago
```

4. A short log will be displayed, showing recent entries. Click on the **ARROWS** icon in the top-right corner to expand to the full **Logs** view:



events Log

Search:

Id	Date	Entity	Message
717	Nov 12 20:24:34	[system]	Reference Change (Cleared)
716	Nov 12 20:24:33	[system]	Reference Change
715	Nov 12 20:24:33	[system]	2014 316 17:55:48.000 SS: Reference changed to Time Ref: ptp0 PPS Ref: ptp0
714	Nov 12 20:24:33	[system]	In Sync
713	Nov 12 18:52:54	[system]	Not In Sync
712	Nov 12 18:52:54	[system]	No Longer In Holdover
711	Nov 12 16:52:55	[system]	Reference Change (Cleared)
710	Nov 12 16:52:54	[system]	Reference Change
709	Nov 12 16:52:54	[system]	In Holdover
708	Nov 12 16:52:53	[system]	2014 316 16:52:53.000 SS: Reference changed to Time Ref: none PPS Ref: none

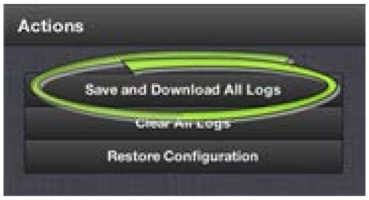
4.13.5 Saving and Downloading Logs

The SecureSync Web UI offers a convenient way to save, bundle, and download all logs in one simple step. This feature may be useful when archiving logs, for example, or for troubleshooting technical problems: Spectracom Technical Support/Customer Service may ask you to send them the bundled logs to remotely investigate a technical concern.

To save, bundle, and download all logs:

1. Navigate to **MANAGEMENT > OTHER: Log Configuration**.

2. On the left side of the screen, in the **Actions** panel, click on the **Save and Download All Logs** button.



3. Select where to save the log bundle to. The default file name is `securesync.log`.

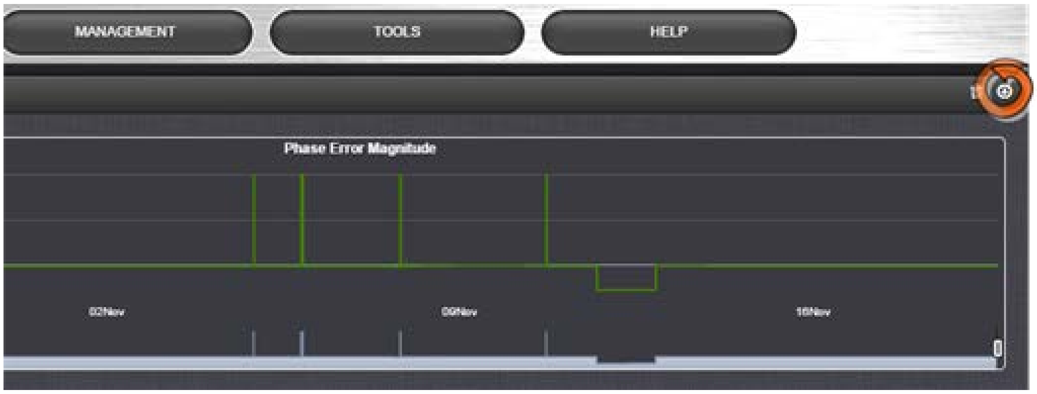
4. If so asked by Spectracom Technical Support, attach the bundled log files (typically together with the oscillator status log, see: "Saving and Downloading the Oscillator Log" on the facing page) to your email addressed to Spectracom Technical Support.

4.13.5.1 Saving and Downloading the Oscillator Log

The oscillator status log captures oscillator performance data, such as frequency error and phase error. The data can be retrieved as a comma-separated .csv file that can be read and edited with a spreadsheet software, such as Microsoft Excel®. You may want to review and/or keep this data for your own records, or you may be asked by Spectracom Technical Support to download and send the oscillator status log in the event of technical problems.

To download the oscillator status log:

1. Navigate to **MANAGEMENT > OTHER: Disciplining**.
2. Click on the ARROW icon in the top-right corner of the screen. Save the .csv file to your computer.



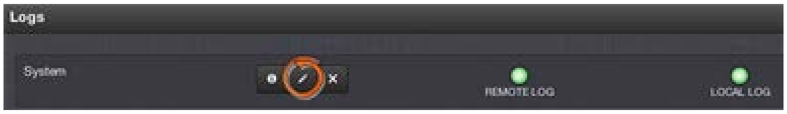
3. If so asked by Spectracom Technical Support, attach the oscillator status log file (typically together with the bundled SecureSync log files, see: "Saving and Downloading Logs" on the previous page) to your email addressed to Spectracom Technical Support.

4.13.6 Configuring Logs

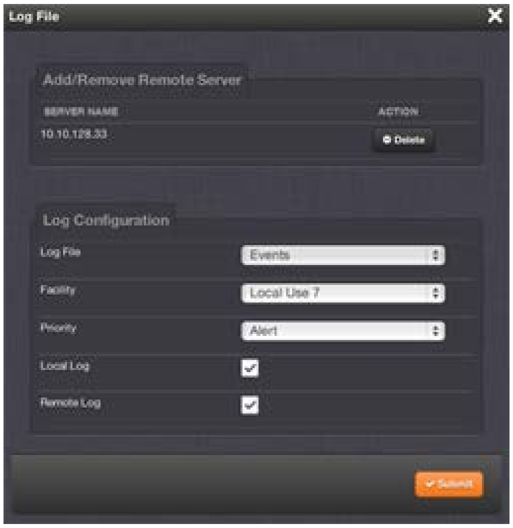
Note: The NTP log has no available configuration options.

To configure a log:

1. Navigate to **MANAGEMENT > OTHER: Log Configuration**.
1. In the **Logs** panel select the log you wish to configure, then click the corresponding PENCIL button.



2. In the **Log File** window, fill in the available fields.



10.10.128.33

Log File: Events

Facility: Local Use 7

Priority: Alert

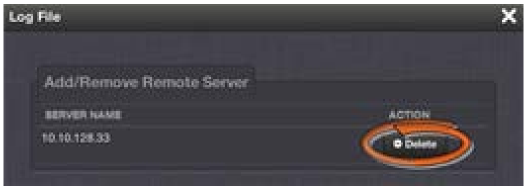
Local Log: ☑

Remote Log: ☑

The following log configuration options are available:

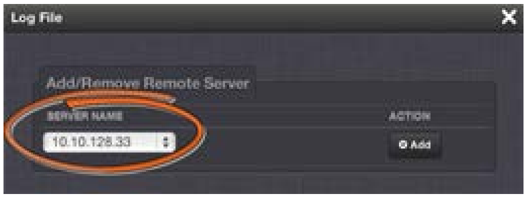
a. **Add/Remove Remote Server**–The Syslog server(s) to which remote logs are sent. This panel is only available if **Remote Log** is checked below in the **Log Configuration** panel.

If the log has a remote log server to which it writes, the name of the server will appear here. Click **Delete** to remove the remote server.



Note: Clicking the Delete button in the Log File configuration window does NOT remove the remote log server from the network. In this instance it merely deselects the server as that particular log's remote log server.

- If the log does not have a remote log server assigned, there will be a drop-down list of server choices. Click **Add** to add a remote server from the drop-down list.



- If this list is empty, you will need to set up a remote log server through the **Remote Log Server** panel. See "Setting up a Remote Log Server" on page 274.

b. **Log File**–Displays the name of the log file being configured.

c. **Facility**–Value (defined by the Syslog server) to determine where the log is stored in the Syslog server. Set this value to match the scheme used by the remote server.

d. **Priority**–Value (defined by the Syslog server) to determine where the log is stored in the Syslog server. Set this value to match the scheme used by the remote server.

> **Note:** About Facility and Priority values: In addition to configuring the log entries to be sent to a specific location in the Syslog server, the combination of these two values also determines which local log the entries are sent to inside SecureSync.
>
> Changing either or both of these values from the factory default values will alter which log the entries are sent to inside SecureSync.
>
> The table below, Factory Default Facility and Priority Codes, indicates which Log Tab the log entries will be sent to (by default), based on the configuration of these two values.

If remote logging is not being used, the Facility and Priority values should not be changed from the default values. Altering these values can cause log entries that have similar values to be sent to the same log file (combining different types of log entries into one log). The factory default settings for the Facility and Priority configurations of all logs that can be sent to a Syslog server are as follows:

Log Tab Name	Facility	Priority
Event	Local Use 7	Alert
Alarms	Local Use 7	Critical
Oscillator	Local Use 7	Debug
GPS Qualification	Local Use 7	Warning
Journal	Local Use 7	Notice
Update	Local Use 7	Information
Timing	Local Use 7	Error
System	Local Use 7	Emergency

Table 4-2: Factory default facility and priority codes

e. **Local Log**–Enable or disable this particular log being stored inside SecureSync. When this box is checked, the log will be stored in SecureSync.

f. **Remote Log**–Configure the desired Syslog servers. When this box is checked, the particular log will be sent to a Syslog server.

In order for the logs to be formatted correctly for Syslog storage, all log entries are displayed using Syslog formatting. Each log entry contains the date and time of the event, the source of the log entry, and the log entry itself.

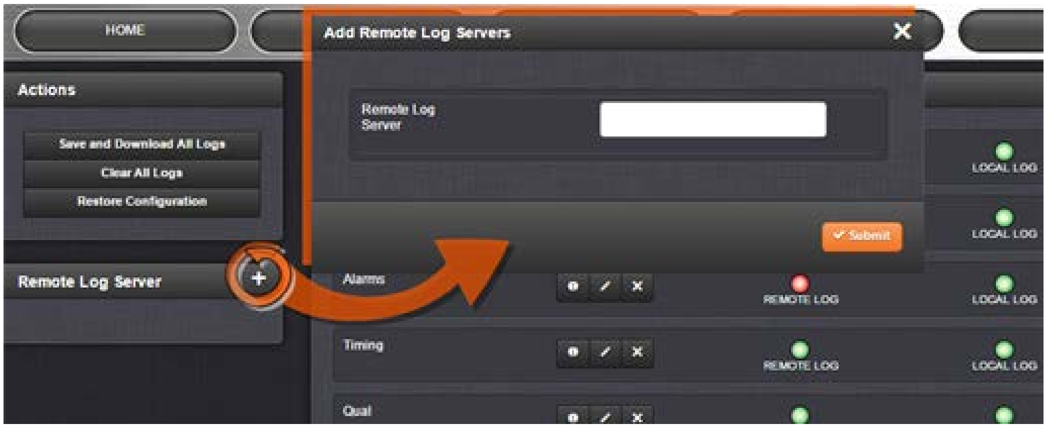
The “time” of all log entries will be in UTC, Local, TAI or GPS time, as configured in the “Time scale” field that is located in the System Time Setup page (Setup/Time Management). Refer to "Timescales, Offsets and Leap Seconds" on page 167 for information on configuring the System Timescale.

4.13.7 Setting up a Remote Log Server

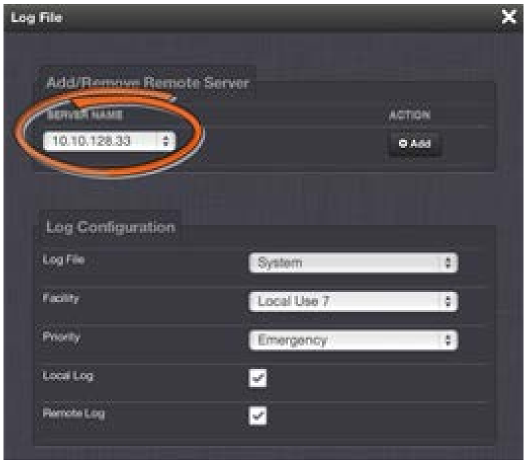
Storing log files on remote log servers supports advanced logging functionality.

To add remote log servers:

1. Navigate to **MANAGEMENT > OTHER: Log Configuration.**
2. In the **Remote Log Server** panel, click on the PLUS icon in the top-right corner of the panel. The **Add Remote Log Servers** window displays.



3. Enter the IP address or host server name (e.g. “MyDomain.com”) you wish to use as a remote log server.
4. Click the **Submit** button.
5. Your remote log server will appear in the **Remote Log Server** panel, and as a SERVER NAME in any **Log File** configuration screen:



SERVER NAME: 10.10.128.33

Log File: System

Facility: Local Use 7

Priority: Emergency

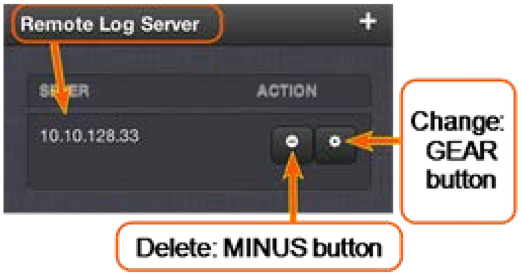
Local Log ☑

Remote Log ☑

4.13.7.1 Changing or Deleting a Remote Log Server

To change or delete a remote log server:

1. Navigate to **MANAGEMENT > OTHER: Log Configuration**.
2. In the **Remote Log Server** panel locate the remote server you wish to change or delete.



3. Choose the MINUS button to delete the remote log server. Confirm by clicking OK in the message window.

–OR–

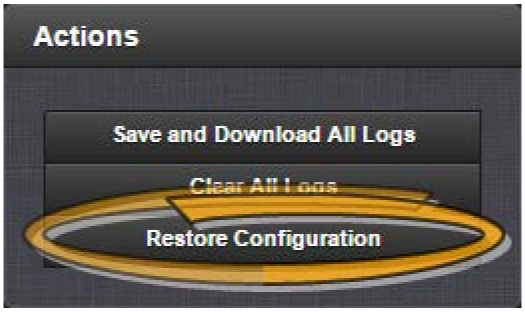
2. In the **Remote Log Server** panel, click the GEAR button to change the remote log server. Type in a new IP address or host domain server (e.g. MyDomain.com).

> Note: Clicking the Delete button in any of the Log file configuration windows does NOT remove the chosen remote log server from the network; it merely deselects the server as that particular log's remote log server.

4.13.8 Restoring Log Configurations

To restore log configurations:

1. Navigate to the **MANAGEMENT > OTHER: Log Configuration**.
2. In the **Actions** panel, click on the **Restore Configurations** button.

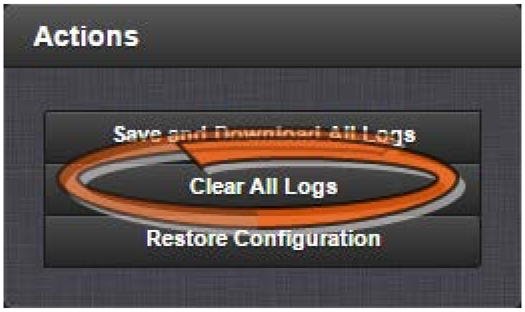


3. Click the Browse button.
4. Navigate to the directory where the configurations are stored and click **Upload**.

4.13.9 Clearing Logs

To clear all logs:

1. Navigate to **MANAGEMENT > OTHER: Log Configuration**.
2. In the **Actions** panel, click on the **Clear All Logs** button.



3. In the message window that displays, click OK.

4.14 Leap Second Occurrence

4.14.1 Reasons for a Leap Second Correction

A Leap Second is an intercalary[1] one-second adjustment that keeps broadcast standards for time of day close to mean solar time. Leap seconds are required to synchronize time standards with civil calendars, thus keeping UTC time in sync with the earth's rotation.

If it has been determined by the International Earth Rotation and Reference Systems Service (IERS) that a Leap Second needs to applied, this time correction occurs only at the end of a UTC month, and has only ever been inserted at the end of June 30 or December 31. A Leap Second may be either added or removed, but in the past, the leap seconds have always been added because the earth's rotation is slowing down.

Historically, Leap seconds have been inserted about every 18 months. However, the Earth's rotation rate is unpredictable in the long term, so it is not possible to predict the need for them more than six months in advance.

Note: Leap seconds only apply to the "UTC" and "Local" timescales. Leap seconds do not affect the "GPS" and "TAI" timescales. However, a leap second event will change the GPS to UTC and TAI to UTC offsets. When a leap second occurs, SecureSync will automatically change these offsets by the proper amount, no matter which timescale is currently being used by the system.

[1] Intercalary: (of a day or a month) inserted in the calendar to harmonize it with the solar year, e.g., February 29 in leap years.

SecureSync can be alerted of impending leap seconds by any of the following methods:

- **GNSS Receiver** (if available as an input reference)–The GNSS satellite system transmits information regarding a Leap second adjustment at a specific Time and Date an arbitrary number of months in advance.
- **Input references other than GNSS**–Some of the other available input references (e.g., IRIG) can also contain pending Leap Second notification in their data streams.
- **Manual user input**–SecureSync can be manually configured with the date/time of the next pending leap second. On this date/time, the System Time will automatically correct for the leap second (unless the System Time's timescale is configured as either GPS or TAI).

The date/time of a pending leap second can be set manually. See "Configuring a Leap Second Correction" on page 174.

4.14.2 Leap Second Alert Notification

SecureSync will announce a pending Leap Second adjustment by the following methods:

1. Data Formats 2 and 7 available from the ASCII Data option modules contain a Leap Second indicator. During the entire calendar month preceding a Leap Second adjustment, these Formats indicate that at the end of the current month a Leap Second Adjustment will be made by using the character 'L' rather than a '_ ' [space] in the data stream. Note that this does not indicate the direction of the adjustment as adding or removing seconds. These formats always assume that the Leap Second will be added, not removed.
2. NTP Packets contain two Leap Indicator Bits. In the 24 hours preceding a Leap Second Adjustment, the Leap Indicator Bits (2 bits) which normally are 00b for sync are 01b (1) for Add a Leap Second and 10b (2) for remove a Leap Second. The bit pattern 11b (3) indicates out of sync and in this condition NTP does NOT indicate Leap seconds. The Sync state indicates leap seconds by indicating sync can be 00b, 01b, or 02b.

Note: It is the responsibility of the client software utilizing either the Data Formats or NTP time stamps to correct for a Leap Second occurrence. SecureSync will make the correction at the right time. However, because computers and other systems may not utilize the time every second, the Leap second correction may be delayed until the next scheduled interval, unless the software properly handles the advance notice of a pending Leap Second and applies the correction at the right time.

4.14.3 Leap Second Correction Sequence

The following is the time sequence pattern in seconds that SecureSync will output at UTC midnight on the scheduled day (Note: This is NOT local time midnight; the local time at which the adjustment is made will depend on which Time Zone you are located in).

A. Sequence of seconds output when **adding a second** ("positive leap second"):

   - 56, 57, 58, 59, **60**, 0, 1, 2, 3 ...

B. Sequence of seconds output when **subtracting a second** ("negative leap second"):

- 56, 57, **58, 0**, 1, 2, 3, 4 ...

4.15 Upgrades and Licenses

4.15.1 Software Updates

Spectracom periodically releases new versions of software for SecureSync. These updates[1] are offered for free and made available for download from the Spectracom website. If you register your product, you will be notified of software updates.

To download a software update for your SecureSync as it becomes available, click here.

This web page also offers detailed instructions on how to perform a software update.

General Notes:

SecureSync will save system configurations across upgrades but will not save other information. In particular, update files may not be retained after a successful update.

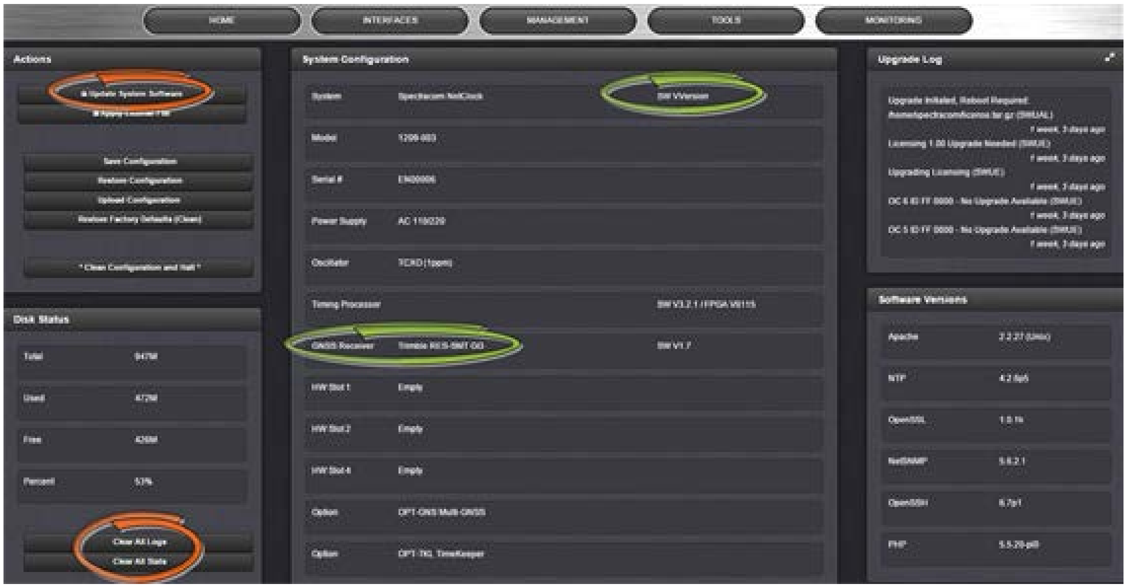
All system elements will be forced to the versions in the update file, and all configuration information will be erased as part of the update. See "Backing-up and Restoring Configuration Files" on page 183 for details.

To “roll back” system elements to an earlier version, select the older **Update File** in the **Choose File** pull-down, select both **Update System** and **Force Update**, and click **Update**. All system elements will be “forced” to the version in the update file.

Step-by-Step Instructions:

Note: These instructions apply to updates to recent software. Updates to software versions older than 5.0.x may require additional steps. These will be covered in the SWUI (Software Update Instructions) documents, which can be found under the above-mentioned link.

[1] The terms update and upgrade are both used throughout Spectracom technical literature, as software releases may include fixes and enhancements, as well as new features.



System Configuration

System	Spectracom NetClock	SW VVersion
Model	1209-003	
Serial #	E9000006	
Power Supply	AC 110/220	
Oscillator	TCXO (1ppm)	
Timing Processor		SW V3.2.1 / FPGA V0115
GNSS Receiver	Trimble RES-SMT GG	SW V1.7
HW Slot 1	Empty	
HW Slot 2	Empty	
HW Slot 4	Empty	
Option	OPT-GNS Multi-GNSS	
Option	OPT-TKL TimeKeeper	

Disk Status

Total	947M
Used	472M
Free	426M
Percent	53%

Upgrade Log

```
Upgrade Initiated, Reboot Required:
/home/spectracom/license.tar.gz (SWUAL)
                                1 week, 3 days ago
Licensing 1.00 Upgrade Needed (SWUE)
                                1 week, 3 days ago
Upgrading Licensing (SWUE)
                                1 week, 3 days ago
OC 6 ID FF 0000 - No Upgrade Available (SWUE)
                                1 week, 3 days ago
OC 5 ID FF 0000 - No Upgrade Available (SWUE)
                                1 week, 3 days ago
```

Software Versions

Apache	2.2.27 (Unix)
NTP	4.2.8p5
OpenSSL	1.0.1k
NetSNMP	5.6.2.1
OpenSSH	6.7p1
PHP	5.5.20-pl0

1. In the Web UI, under **Tools** > **Upgrade/Backup**, determine the System software version and the type of GNSS receiver. Proceed if your existing software is V5.1.5 or higher, AND you have a RES-SMT GG receiver.
(Otherwise, consult the above-mentioned instructions for updating SecureSync software.)

2. Free up disk space, if needed:
Under **Tools** > **Upgrade/Backup** > **Disk Status**, check **Percent Used**: If the number is greater than 70%, free up disk space.
(NOTE: If required, existing logs can be archived; for details consult the above-mentioned instructions for updating SecureSync software.)
To free up disk space:
    a. Delete old log files: **Tools** > **Upgrade/Backup** > **Disk Status** > **Clear All Logs**.
    b. Delete old statistics files: [~] > **Clear All Stats**.
    c. Delete previous Upgrade files: : **Tools** > **Upgrade/Backup** > **Actions** > **Update System** > **Delete Upgrade File**(s). Note that **Delete Upgrade File** and **Update System** cannot be selected at the same time.

3. Download the upgrade software bundle onto your PC.

4. Check if you have any of the following option cards installed:
    - Simulcast (Model 1204-14)
    - PTP (Model 1204-12)
    - Gigabit Ethernet (Model 1204-06)

   If this is the case, see above-mentioned instructions for updating SecureSync software (unless this has been addressed at an earlier update).

5. Perform the actual upgrade by navigating to **TOOLS** > **Upgrade/Backup** > **Actions**: **Update System File**: Upload the upgrade software bundle previously downloaded onto your PC (`updateXYZ.tar.gz`), and carry out the upgrade, as instructed.
6. Verify that the upgrade was successful: **Tools** > **Upgrade/Backup**, confirm the new SW version.

> **Note:** In case the update failed, see"Troubleshooting Software Update" on page 464 for additional information.

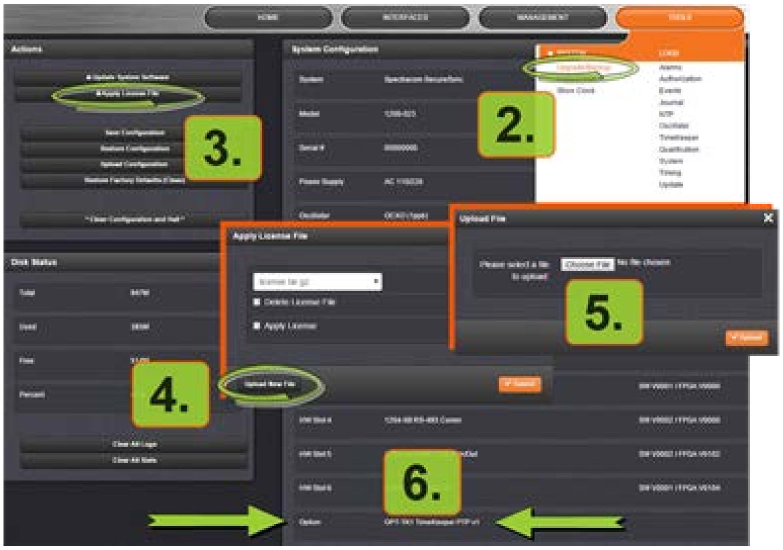
4.15.2 Applying a License File

Software options like TimeKeeper, or Multi-GNSS must be activated by applying a license file:

Typically, SecureSync units are shipped with the license file pre-installed, reflecting the system configuration as ordered. If a feature is to be activated after delivery of the SecureSync unit, please contact Spectracom Support or your local representative to have a license file generated. License files are archive files with a `tar.gz` extension. One license file may contain multiple licenses for multiple products.

To apply the license file, you need to upload it into your SecureSync unit and install it:

1. Save the license file `license.tar.gz` to a location on your PC (which needs to be connected to the same network SecureSync is.)
2. Open the SecureSync Web UI, and navigate to **Tools** > **Upgrade/Backup**:



3. In the **Actions** panel, click **Apply License File**.
4. In the **Apply License File** window, click **Upload New File**.

5. In the **Upload File** window, click **Choose File**. Using the Explorer window, navigate to the location mentioned under the first step, select the license file, and monitor the installation progress in the **Status Upgrade** window until the application has rebooted.
6. Refresh the browser window, and login to the Web UI again. Re-navigate to **Tools** > **Upgrade/Backup**, and confirm that the newly installed Option is listed in the **System Configuration** panel.

Next ...

After completion of the procedure, in the case of TimeKeeper you now can enable the new option, see "En-/Disabling TimeKeeper" on page 237.

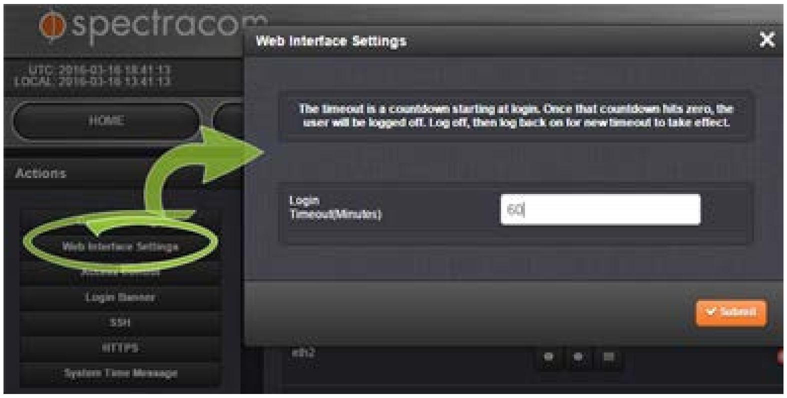
4.16 Changing the Web UI Timeout

For security reasons, the Web UI will automatically timeout after a set number of minutes, i.e. you will be logged out by the system, regardless of activity, and need to actively login again.

- **Minimum** timeout duration: 10 minutes
- **Maximum** timeout duration: 1440 minutes (24 hours)
- **Default** timeout duration: 60 minutes.

To change the time after which the Web UI will timeout:

1. Navigate to the **MANAGEMENT > NETWORK** screen.
2. In the **Actions** panel on the left, click on **Web Interface Settings**.



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.

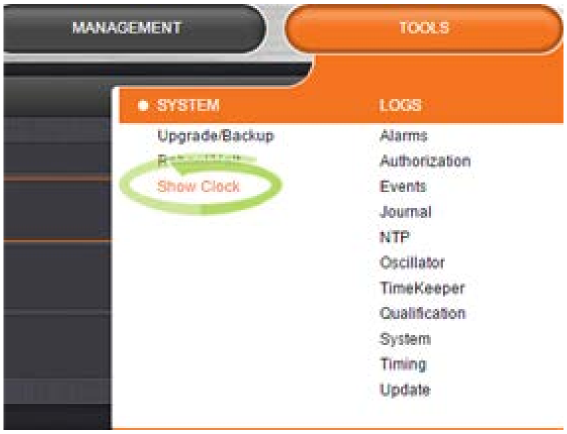
Login Timeout(Minutes) 60

3. In the **Web Interface Settings** window, enter the desired value in minutes.

In order for a new setting to take effect, you need to log off, and then log back on again. This setting affects all users, i.e. not just the user changing the value.

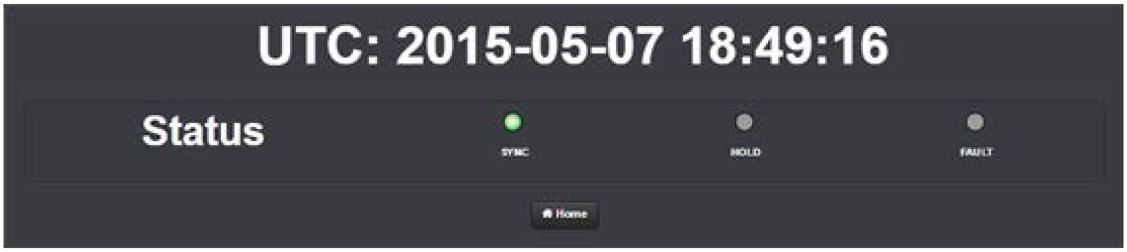
4.17 Show Clock

To display a large screen clock instead of the Web UI, navigate to **TOOLS** > **SYSTEM/Show Clock**:



Next to the system status, the screen clock will display the UTC time, and the SecureSync front panel time (if the front panel time is configured to display UTC, then only UTC will be shown—see image below).

To configure the front panel time, navigate to **MANAGEMENT** > **OTHER/Front Panel**, and under **Timescale/Local Clock** select UTC, TAI, GPS, or a local clock (see also "Front Panel Configuration" on page 179).



UTC: 2015-05-07 18:49:16

CHAPTER 5

Option Cards

Option cards allow for custom configuration of SecureSync 9483.

This Chapter lists all option cards currently available, their features and specifications.

The following topics are included in this Chapter:

5.1 Option Cards Quick Reference Guide

This section describes signals, connectors and specifications, relevant to SecureSync option cards. Also covered are commonly used Web UI procedures for the configuration of installed option cards, and the status review of option card inputs and outputs.

5.1.1 Option Cards Overview

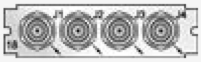
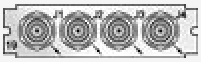
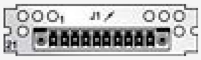
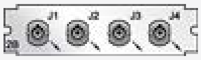
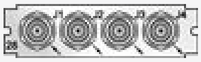
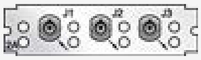
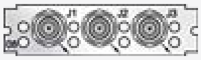
The table below lists all SecureSync option cards available at the time of publication of this document, **sorted by their function**.

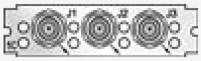
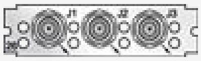
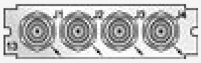
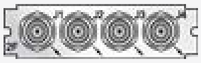
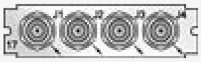
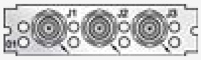
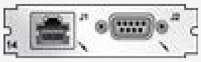
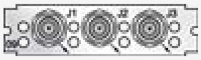
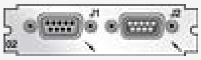
The column "Name in UI" [UI = Web User Interface] refers to the names under which the cards installed in a SecureSync unit are listed in the **INTERFACES/OPTION CARDS** drop-down menu.

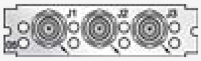
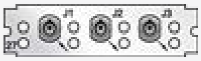
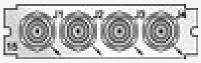
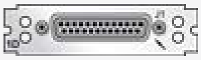
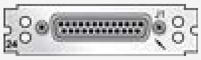
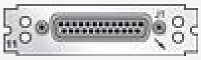
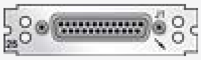
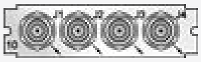
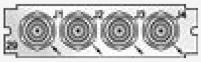
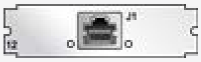
The main purpose of the table below is to assist with the identification of the card(s), and to list its key input/output specifications.

Detailed information on every card can be found in its own chapter, see hyperlinks in table "Option cards listed by their ID number" on page 290.

> **Note:** * Every option card has a 2-digit ID number that can be found on its cover plate, and in the center column below. The ID number is comprised of the two center digits of your option card's Spectracom Part Number: 1204-0180-0600.

Function	Name in UI	Illustration	ID*	Inputs	Outputs	Conn.'s
Time and Frequency Cards						
Quad 1PPS out (TTL)	1PPS Out BNC		**18**	0	1PPS, TTL (4x)	BNC (4x)
Quad 1PPS out (10 V)	1PPS Out 10V		**19**	0	1PPS, 10 V (4x)	BNC (4x)
Quad 1PPS out (RS-485)	1PPS Out, RS-485		**21**	0	1PPS, RS-485 (4x)	Terminal block, 10-pin
Quad 1PPS out (fiber optic)	1PPS Out, Fiber		**2B**	0	1PPS, F/O (4x)	ST Fiber optic (4x)
1in/3out 1PPS (TTL [BNC])	1PPS/Frequency RS-485		**28**	1PPS (1x)	1PPS (3x)	BNC (4x)
1in/2out 1PPS/-freq (fiber optic)	1PPS In/Out, Fiber		**2A**	1PPS (1x)	1PPS (2)	ST Fiber optic (3x)
5MHz out	5MHz Out		**08**	0	5MHz (3x)	BNC (3x)

Function	Name in UI	Illustration	ID*	Inputs	Outputs	Conn.'s
10 MHz out	10 MHz Out		1C	0	10 MHz (3x)	BNC (3x)
10 MHz out	10 MHz Out		38	0	10 MHz (3x)	TNC (3x)
1MHz out	1MHz Out		26	0	1MHz (3x)	BNC (3x)
Progr. frequ. out (Sine Wave)	Prog Freq Out, Sine		13	0	progr. clock, sine (4x)	BNC (4x)
Progr. frequ out (TTL)	Prog Freq Out, TTL		2F	0	progr. clock, TTL/sq. (4x)	BNC (4x)
Prog frequ out (RS-485)	Prog Freq Out, RS-485		30	0	progr. clock, RS-485 (4x)	Terminal block, 10-pin
Square Wave out	Sq Wv Out, BNC		17	0	square wave, TTL (4x)	BNC (4x)
1PPS in/out + frequ. in	1PPS/Frequency BNC		01	Var. frequ. + 1PPS	1PPS (TTL)	BNC (3x)
1PPS in/out + frequ. in	1PPS/Frequency RS-485		03	10 MHz + 1PPS	1PPS	Terminal block, 10-pin
CTCSS, Data Sync/Clock	Simulcast		14	0	data clock, CTCSS frequ., 1PPS, 1 alarm (3x)	RJ-12 & DB-9
Telecom Timing Cards						
E1/T1 data, 75 Ω	E1/T1 Out BNC		09	0	1.544/2.048 MHz (1x) unbal. E1/T1 (2x)	BNC (3x)
E1/T1 data, 100/120 Ω	E1/T1 Out Terminal		0A	0	1.544/2.048 MHz (1x) unbal. E1/T1 (2x)	Terminal block, 10-pin
Time Code Cards						
ASCII Time Code RS-232	ASCII Timecode RS-232		02	RS-232	RS-232	DB-9 (2x)
ASCII Time Code RS-485	ASCII Timecode RS-485		04	1	1	Terminal block, 10-pin

Function	Name in UI	Illustration	ID*	Inputs	Outputs	Conn.'s
IRIG BNC	IRIG In/Out BNC		05	1	2	BNC (3x)
IRIG Fiber Optic	IRIG In/Out, Fiber		27	1	2	ST Fiber optic (3x)
IRIG out, BNC	IRIG Out BNC		15	0	4	BNC (4x)
IRIG out, fiber optic	IRIG Out, Fiber		1E	0	4	ST Fiber optic (4x)
IRIG out, RS-485	IRIG Out, RS-485		22	0	4	Terminal block, 10-pin
STANAG input	STANAG In		1D	2x	1x	DB-25 (1x)
STANAG in, isol.	STANAG In, Isolated		24	2x	1x	DB-25 (1x)
STANAG out	STANAG Out		11	0	2x STANAG, 1x 1PPS	DB-25 (1x)
STANAG out, isol.	STANAG Out, Isolated		25	0	2x STANAG, 1x 1PPS	DB-25 (1x)
HAVE QUICK out BNC	HAVE QUICK Out, BNC		10	0	4 (TTL)	BNC (4x)
HAVE QUICK out RS-485	HAVE QUICK Out, RS-485		1B	0	4	Terminal block, 10-pin
HAVE QUICK	HAVE QUICK		29	1	3	BNC (4x)
Networking Cards						
Gigabit Ethernet	Gb Ethernet		06	(3, OR output)	(3, OR input)	RJ-45 (3x)
10/100 Mb PTP: Master or slave	PTP		12	(1, OR output)	(1, OR input)	RJ-45 (1x)
1Gb PTP: Master only	Gb PTP		32	0	1PPS (1x BNC), SFP (1x)	BNC (1x), SFP (1x)
Communication and Specialty Cards						

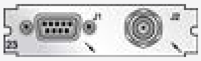
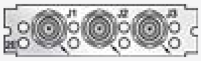
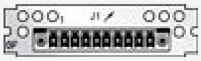
Function	Name in UI	Illustration	ID*	Inputs	Outputs	Conn.'s
Event in, Broadcast out	Event Broadcast		23	BNC: Event trigger	DB-9: Event broadcast	DB-9 + BNC (1x each)
Revertive Selector ("Failover")	n/a		2E	Frequ. or 1 PPS: (2x)	Frequ. or 1PPS (1x)	BNC (3x)
Alarm Relay Out	Relay Output		0F	0	Relay Out (3x)	Terminal block, 10-pin
Bidir. Communication	RS-485 Comm		0B	Yes	Yes	Terminal block, 10-pin

Table 5-1: Option cards overview

5.1.2 Option Card Identification

There are several ways to identify which option card(s) are installed in your SecureSync unit:

a. Using the Web UI, navigate to the **INTERFACES/OPTION CARDS** drop-down menu, and compare the list displayed in your UI with the table "Option cards overview" above

b. If you have physical access to the actual SecureSync unit, inspect its rear panel, and compare the 2-digit ID number printed in the lower left-hand corner on each option card with the table below.

5.1.2.1 Option Card Identification by ID/Part Number

The table below will help you to locate information specific to an option card.

Note: * Every option card has a 2-digit ID number that can be found on its cover plate, and in the left column below. The ID number is comprised of the two center digits of your option card's Spectracom Part Number: 1204-0180-0600.

The table lists all option cards available at the publication date of this documentation, **sorted by their ID number**. Locate the option card ID number on its cover plate, and follow the corresponding hyperlink in the right-hand column.

Card ID*	Card Name	Name in UI	See ...
01	1 PPS/freq input (TTL levels) module	1PPS/Frequency BNC	"1PPS In/Out, 10 MHz In [1204-01, -03]" on page 307

Card ID*	Card Name	Name in UI	See ...
02	ASCII Time Code module (RS-232)	ASCII Timecode RS-232	"ASCII Time Code In/Out [1204-02, -04]" on page 381
03	1 PPS/freq input (RS-485 levels) module	1PPS/Frequency RS-485	"1PPS In/Out, 10 MHz In [1204-01, -03]" on page 307
04	ASCII Time Code module (RS-485)	ASCII Timecode RS-485	"ASCII Time Code In/Out [1204-02, -04]" on page 381
05	IRIG module, BNC (1 input, 2 outputs)	IRIG In/Out BNC	" IRIG In/Out [1204-05, -27]" on page 342
06	Gigabit Ethernet module (3 ports)	Gb Ethernet	"Gigabit Ethernet [1204-06]" on page 392
08	5 MHz output module (3 outputs)	5 MHz Out	"Frequency Out [1204-08, -1C, -26, -38]" on page 314
09	T1-1.544 (75 Ω) or E1-2.048 (75 Ω) module	E1/T1 Out BNC	"T1/E1 Out [1204-09, -0A]" on page 332
0A	T1-1.544 (100 Ω) or E1-2.048 (120 Ω) module	E1/T1 Out Terminal	"T1/E1 Out [1204-09, -0A]" on page 332
0B	Bidirectional Communication module	RS-485 Comm	"Bi-Directional Communication, RS-485 [1204-0B]" on page 435
0F	Alarm module	Relay Output	"Alarm Relay Out [1204-0F]" on page 422
10	HaveQuick output module (TTL)	HAVE QUICK Out, BNC	"HAVE QUICK Out [1204-10, -1B]" on page 369
11	STANAG output module	STANAG Out	"STANAG Out [1204-11, -25]" on page 355
12	10/100 Mb PTP module	PTP	"PTP Master/Slave [1204-12]" on page 407
13	Programmable Frequency Output module (Sine Wave)	Prog Freq Out, Sine	"Programmable Frequency Out [1204-13, -2F, -30]" on page 318
14	CTCSS, Data Sync/Clock module ("Simulcast")	Simulcast	"Simulcast (CTCSS/Data Clock) [1204-14]" on page 325
15	IRIG module, BNC (4 outputs)	IRIG Out BNC	"IRIG Out [1204-15, -1E, -22]" on page 337
17	Square Wave (TTL) output module	Sq Wv Out, BNC	"Programmable Square Wave Out [1204-17]" on page 322
18	Quad 1 PPS output module (TTL)	1PPS Out BNC	"1PPS Out [1204-18, -19, -21, -2B]" on page 298
19	Quad 1 PPS output module (10 V)	1PPS Out 10V	"1PPS Out [1204-18, -19, -21, -2B]" on page 298

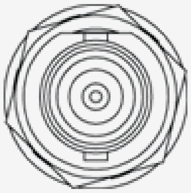
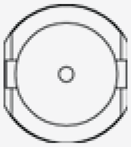
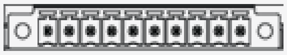
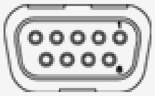
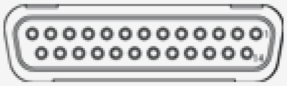
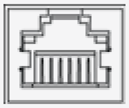
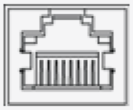
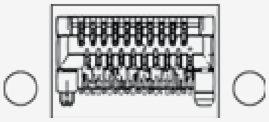
Card ID*	Card Name	Name in UI	See ...
1B	HaveQuick output module (RS-485)	HAVE QUICK Out, RS-485	"HAVE QUICK Out [1204-10, -1B]" on page 369
1C	10 MHz output module (3 outputs)	10 MHz Out	"Frequency Out [1204-08, -1C, -26, -38]" on page 314
1D	STANAG input module	STANAG In	"STANAG In [1204-1D, -24]" on page 362
1E	IRIG module, Fiber Optic (4 outputs)	IRIG Out, Fiber	"IRIG Out [1204-15, -1E, -22]" on page 337
21	Quad 1 PPS output module (RS-485 [terminal block])	1PPS Out, RS-485	"1PPS Out [1204-18, -19, -21, -2B]" on page 298
22	IRIG module, RS-485 (4 outputs)	IRIG Out, RS-485	"IRIG Out [1204-15, -1E, -22]" on page 337
23	Event Broadcast module	Event Broadcast	"Event Broadcast [1204-23]" on page 426
24	STANAG isolated input module	STANAG In, Isolated	"STANAG In [1204-1D, -24]" on page 362
25	STANAG isolated output module	STANAG Out, Isolated	"STANAG Out [1204-11, -25]" on page 355
26	1 MHz output module (3 outputs)	1MHz Out	"Frequency Out [1204-08, -1C, -26, -38]" on page 314
27	IRIG module, Fiber Optic (1 input, 1 outputs)	IRIG In/Out, Fiber	" IRIG In/Out [1204-05, -27]" on page 342
28	1-in/3-out 1 PPS module (TTL [BNC])	1PPS/Frequency RS-485	"1PPS In/Out [1204-28, -2A]" on page 302
29	1-in/3-out HaveQuick module (TTL [BNC])	HAVE QUICK	"HAVE QUICK In/Out [1204-29]" on page 374
2A	1-in/3-out 1 PPS module (Fiber Optic)	1PPS In/Out, Fiber	"1PPS In/Out [1204-28, -2A]" on page 302
2B	Quad 1 PPS output module (Fiber Optic)	1PPS Out, Fiber	"1PPS Out [1204-18, -19, -21, -2B]" on page 298
2F	Programmable Frequency Output module (TTL)	Prog Freq Out, TTL	"Programmable Frequency Out [1204-13, -2F, -30]" on page 318
2E	Revertive Selector module ("Failover")	n/a	"Revertive Selector Card [1204-2E]" on page 425
30	Programmable Frequency Output module (RS-485)	Prog Freq Out, RS-485	"Programmable Frequency Out [1204-13, -2F, -30]" on page 318
32	1Gb PTP module	Gb PTP	"PTP Grandmaster [1204-32]" on page 393
38	10 MHz output module (3 x TNC outputs)	10 MHz Out	"Frequency Out [1204-08, -1C, -26, -38]" on page 314

Table 5-2: Option cards listed by their ID number

5.1.3 Connectors

The table below lists the connector types used in SecureSync option cards.

Table 5-3: Option card connectors

Connector	Illustration	Electr. Signals	Timing signals
BNC		Differential TTL xV, sine wave, programm. square wave, AM sine wave, DCLS	1 PPS, frequency, IRIG, HAVE QUICK, PTP
ST Fiber Optic		AM sine wave, DCLS	IRIG, 1 PPS
Terminal Block [Recommended mating connector: Phoenix Contact, part no. 182 7787]		RS-485	1 PPS,frequency, ASCII time code, IRIG,HAVEQUICK, Alarm, T1/E1
DB-9		RS-232, RS-485	ASCII time code, GPS NMEA, data clocks, CTCSS frequ., 1 PPS, Alarm signal
DB-25		Differential TTL xV, RS-485	STANAG
RJ-12		RS-485	data clock, CTCSS frequ., 1 PPS,Alarm
RJ-45		Gb-Ethernet	PTP timing signal
SFP		Ethernet	PTP

5.1.4 Web UI Navigation: Option Cards

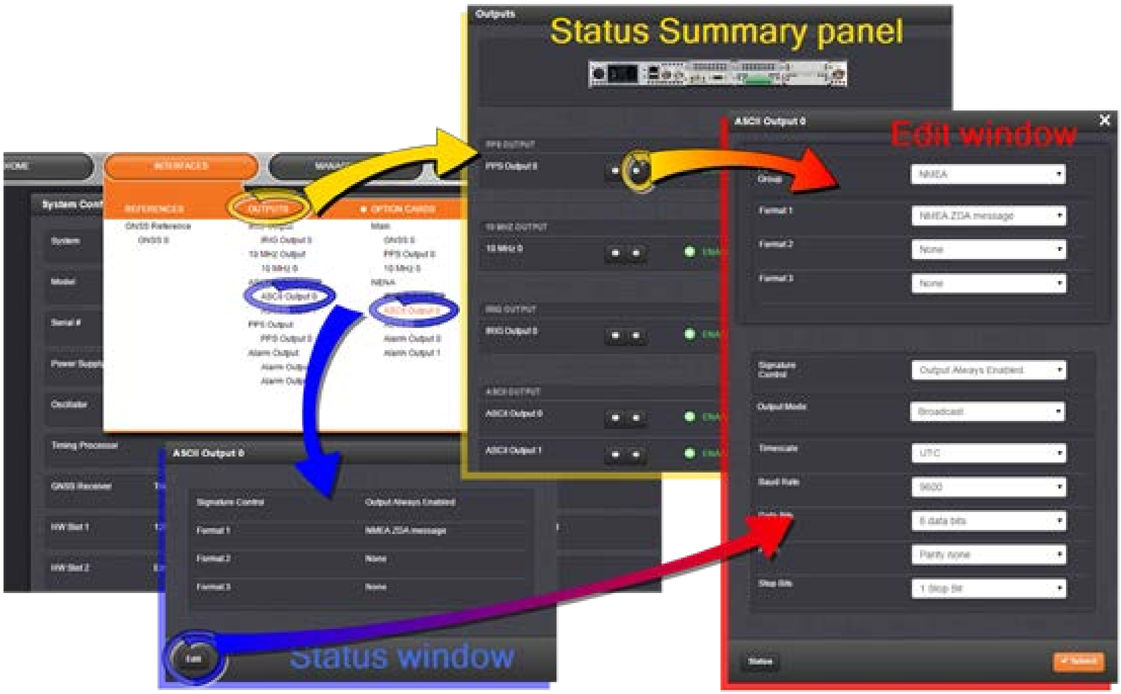


Figure 5-1: Option card navigation

To view or edit option card settings in the SecureSync Web UI (see also image above):

Status Summary panel

- Under **INTERFACES/OPTION CARDS**, clicking the superordinate list entry will open the Status Summary panel, which provides a status overview, as well as access to the Status window and the Edit window.

Status window

- Under **INTERFACES/OPTION CARDS**, clicking subordinate (indented) entries will open the Status window, providing detailed option card status information.

Edit window

- To edit option card settings, either click the **Edit** button in the lower-left corner of the Status window, or click the GEAR button in the Status Summary panel: The Edit window will open.

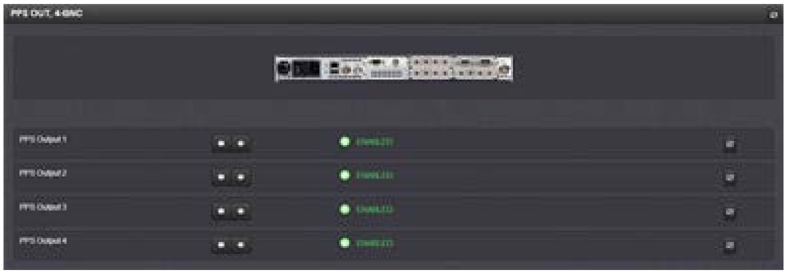
5.1.5 Viewing the Configuration of an Input or Output

The configurable settings of any SecureSync input or output interface can be viewed in its **Status window**. The Status window can be accessed in several ways; the procedure below describes the standard way:

1. Identify the name of the option card, (e.g., **PPS OUT, 4-BNC**) and the name of the input or output you want to configure (e.g., **PPS Output 1**).

   > **Note:** If you have only one input or output of any type, SecureSync will number that input or output 0. Additional inputs or outputs will be numbered 1 or above.

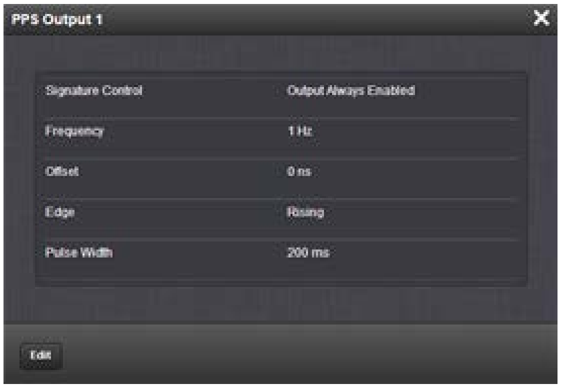
2. Navigate to the **INTERFACES/OPTION CARDS** drop-down menu, and click the list entry of the option card identified above. The option card's Status Summary panel opens:



PPS OUT, 4-BNC

PPS Output 1	ENABLED
PPS Output 2	ENABLED
PPS Output 3	ENABLED
PPS Output 4	ENABLED

3. Click on the INFO button next to the input or output whose settings you wish to review. The Status window of the input or output opens:

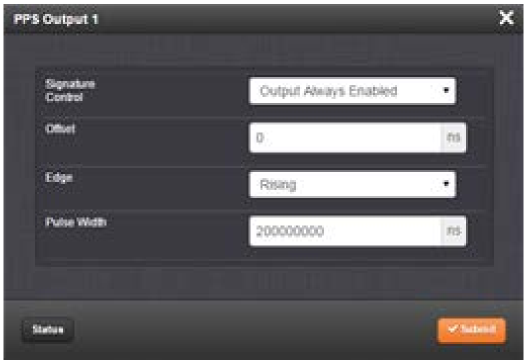


PPS Output 1

Signature Control	Output Always Enabled
Frequency	1 Hz
Offset	0 ns
Edge	Rising
Pulse Width	200 ms

4. Information about the settings of a specific interface can be found in the corresponding option card section, see "Option cards listed by their ID number" on page 290.
   If you want to change any of the settings shown in the Status window, click the **Edit** button

in the lower-left corner, in order to open the **Edit** window:



PPS Output 1

Signature Control: Output Always Enabled
Offset: 0 ns
Edge: Rising
Pulse Width: 200000000 ns

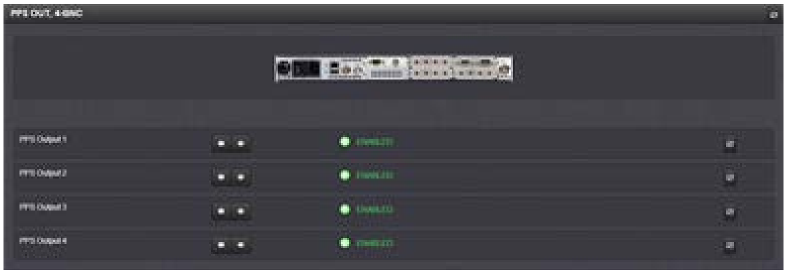
5.1.6 Configuring the Settings of an Input or Output

The configurable settings of any SecureSync input or output interface are accessible through the Edit window of the option card to which the input or output belongs. The Edit window can be accessed in several ways; the procedure below describes the standard way:

1. Identify the name of the card, (e.g., **PPS OUT, 4-BNC**), and verify the name of the input or output you want to configure (e.g., **PPS Output 1**).

   Note: If you have only one input or output of any type, SecureSync will number that input or output 0. Additional inputs or outputs will be numbered 1 or above.

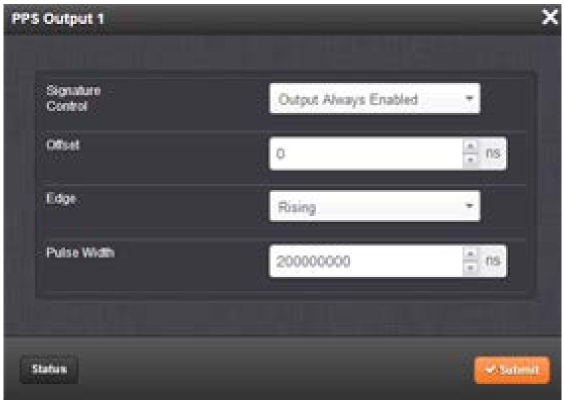
2. Navigate to the **INTERFACES/OPTION CARDS** drop-down menu, and click the list entry of the option card identified above. The option card's Status Summary panel opens:



PPS OUT, 4-BNC

PPS Output 1	● ENABLED
PPS Output 2	● ENABLED
PPS Output 3	● ENABLED
PPS Output 4	● ENABLED

3. Click on the GEAR button next to the input or output you wish to configure (as verified in Step 1 of this procedure). The Edit window of the input or output opens:



PPS Output 1

Signature Control: Output Always Enabled

Offset: 0 ns

Edge: Rising

Pulse Width: 200000000 ns

4. Information about the settings of a specific interface can be found in the corresponding option card section, see "Option cards listed by their ID number" on page 290.

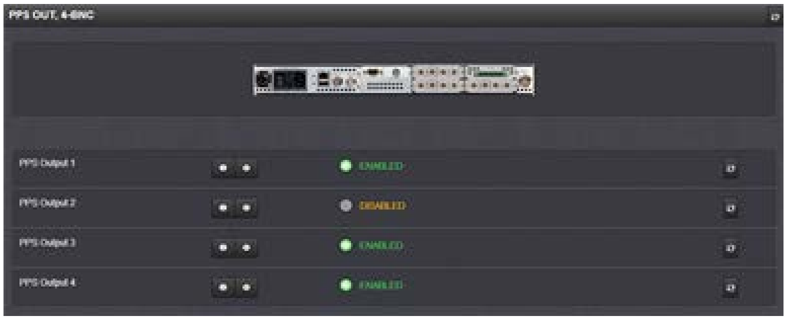
5.1.7 Viewing the Signal State of an Input or Output

To view if an input or output is currently enabled or disabled, go to the option card's Status Summary panel:

1. Identify the name of the option card, (e.g., **PPS OUT, 4-BNC**), and the name of the input or output you want to configure (e.g., **PPS Output 1**).

> **Note:** If you have only one input or output of any type, SecureSync will number that input or output 0. Additional inputs or outputs will be numbered 1 or above.

2. Navigate to the **INTERFACES/OPTION CARDS** drop-down menu, and click the list entry of the option card identified above. The option card's Status Summary panel opens:



PPS OUT, 4-BNC

PPS Output 1 ● ENABLED

PPS Output 2 ● DISABLED

PPS Output 3 ● ENABLED

PPS Output 4 ● ENABLED

All the inputs and/or outputs of this option card are listed in the Status Summary panel.

In accordance with the Signature Control setting, and the Lock Status, the current signal state for an output is indicated as:

- **ENABLED** (green); or
- **DISABLED** (orange)

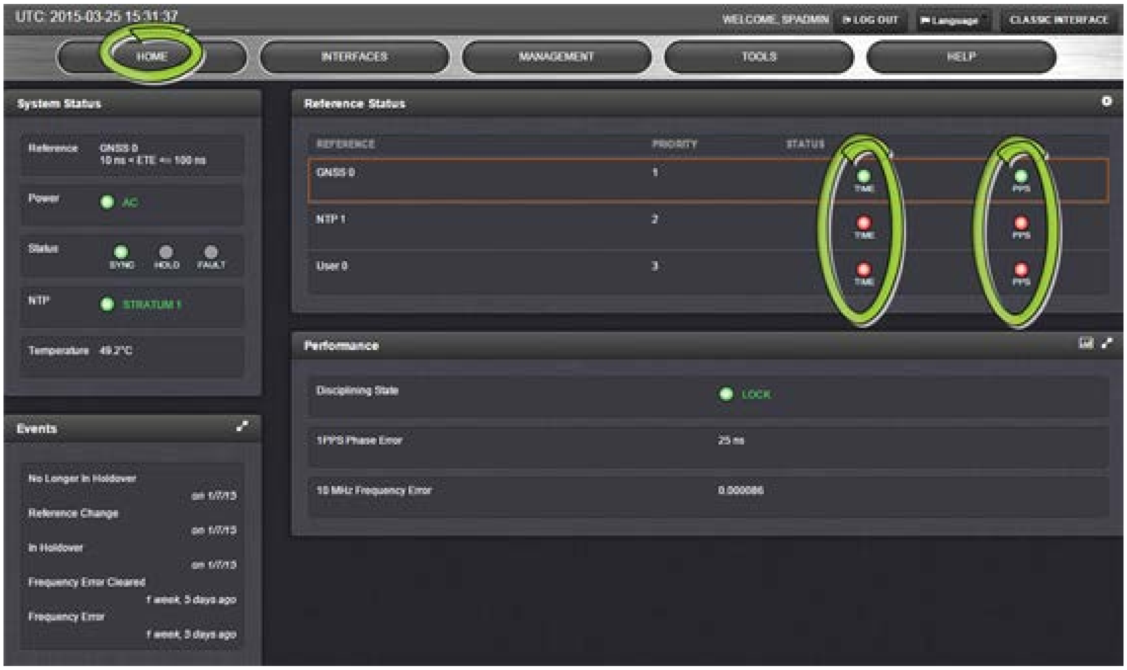
The current state of an input signal is indicated as:

- **VALID** (in green); or
- **INVALID** (in red)

The Status Summary panel will be refreshed automatically every 30 seconds. Click the **Refresh** button (circling arrows) on the right to refresh the status instantaneously. A slight refreshment delay is normal (the duration depends on the configuration of your system.)

5.1.8 Verifying the Validity of an Input Signal

The **HOME** Page of the SecureSync Web UI provides quick access to the status of all inputs via its **Reference Status** panel.



Reference GNSS 0
10 ms < ETE <= 100 ms

Power ● AC

Status ● SYNC ● HOLD ● FAULT

NTP ● STRATUM 1

Temperature 49.2°C

REFERENCE	PRIORITY	STATUS	
GNSS 0	1	● TIME	● PPS
NTP 1	2	● TIME	● PPS
User 0	3	● TIME	● PPS

Disciplining State ● LOCK

1PPS Phase Error 25 ns

10 MHz Frequency Error 0.000086

No Longer In Holdover
on 1/7/13

Reference Change
on 1/7/13

In Holdover
on 1/7/13

Frequency Error Cleared
1 week, 3 days ago

Frequency Error
1 week, 3 days ago

If an INPUT is not present, or not valid, and qualified, the **1PPS Validity** and **Time Validity** fields will be "**Not Valid**" (orange).

If an INPUT is present, and the signal is considered valid, and qualified, the two indicators will then turn "Valid" (Green).

5.2 Time and Frequency Option Cards

This section contains technical information and Web UI procedures relevant to SecureSync option cards designed to deliver time and frequency signals.

5.2.1 1PPS Out [1204-18, -19, -21, -2B]

5.2.1.1 1PPS Output Modules (TTL, 10V, RS-485)

The 1PPS output module provides four additional 1PPS outputs on BNC connectors or terminal block for the SecureSync platform.

5.2.1.2 Model 1204-18 1PPS Output (TTL): Specifications

- **Outputs:** (4) 1PPS output
- **Signal Type and Connector:** TTL (BNC)
- **Output Load Impedance:** 50 Ω
- **Rise Time to 90% of Level:** <10 ns
- **Programmable Pulse Width:** 100 ns to 900 ms with 20 ns resolution
- **Absolute Phase Error:** ±50 ns (1σ)
- **Programmable Phase Shift:** ±5ns to 500 ms with 5ns resolution
- **Maximum Number of Cards:** 6
- **Ordering Information:** 1204-18 1PPS TTL output module, BNC connector

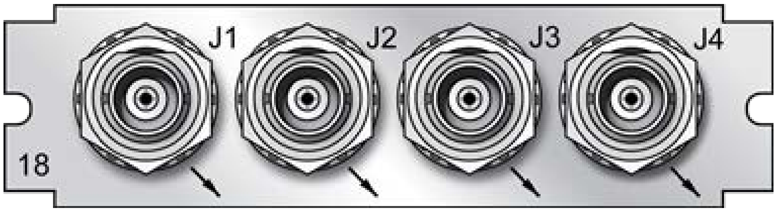


Figure 5-2: Model 1204-18 option card rear plate

5.2.1.3 Model 1204-19 1PPS Output (10 V): Specifications

- **Outputs:** (4) 1PPS output
- **Signal Type and Connector:** 10 V (BNC)
- **Output Load Impedance:** 50 Ω
- **Rise Time to 90% of Level:** <30 ns
- **Programmable Pulse Width:** 100 ns to 900 ms with 20 ns resolution
- **Absolute Phase Error:** ±50 ns (1σ)
- **Programmable Phase Shift:** ±5ns to 500 ms with 5ns resolution
- **Maximum Number of Cards:** 6
- **Ordering Information:** 1204-19 1PPS 10 V output module, BNC connector

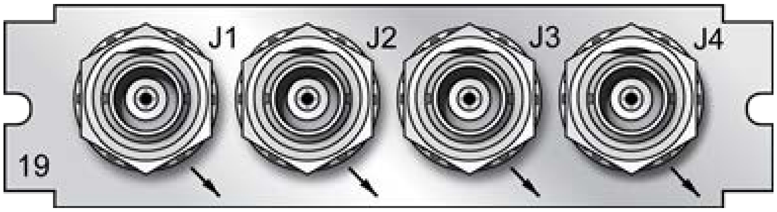


Figure 5-3: Model 1204-19 option card rear plate

5.2.1.4 Model 1204-21 1PPS Output (RS-485): Specifications

- **Inputs/Outputs:** (4) 1PPS output
- **Signal Type and Connector:** RS-485 (terminal block)
- **Output Load Impedance:** 120 Ω
- **Rise Time to 90% of Level:** <10 ns
- **Programmable Pulse Width:** 100 ns to 900 ms with 20 ns resolution
- **Absolute Phase Error:** ±50 ns (1σ)
- **Programmable Phase Shift:** ±5ns to 500 ms with 5ns resolution
- **Maximum Number of Cards:**6
- **Ordering Information:** 1204-21 1PPS RS-485 output module, terminal block

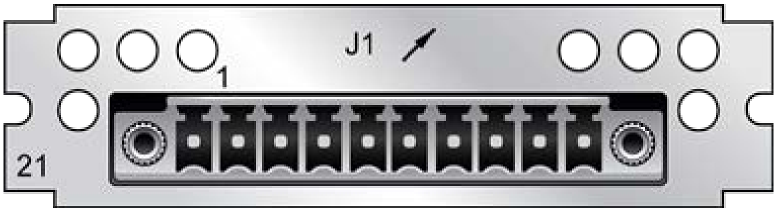


Figure 5-4: Model 1204-21 option card rear plate

Pin Assignments

Pin No.	Function
1	1PPS Output 1 +
2	1PPS Output 1 -
3	GND
4	1PPS Output 2 +
5	1PPS Output 2 -
6	1PPS Output 3 +

Pin No.	Function
7	1PPS Output 3 -
8	GND
9	1PPS Output 4 +
10	1PPS Output 4 -

Table 5-4: Model 1204-21 terminal block pin assignments

5.2.1.5 Model 1204-2B 1PPS Output (Fiber Optical): Specifications

- **Inputs/Outputs:** (4) 1PPS output
- **Operating Wavelength:** 820/850 nm
- **Optical Power:** -15 dBm average into 50/125 fiber
- **Fiber Optic Compatibility:** 50/125 µm, 62.5/125 µm multi-mode cable
- **Optical Connector:** ST
- **Programmable Pulse Width:** 100 ns to 900 ms with 20 ns resolution
- **Absolute Phase Error:** ±50 ns (1σ)
- **Programmable Phase Shift:** ±5ns to 500 ms with 5ns resolution
- **Maximum Number of Cards:** 6
- **Ordering Information:** 1204-12B 1PPS Fiber Optic output module, ST connector

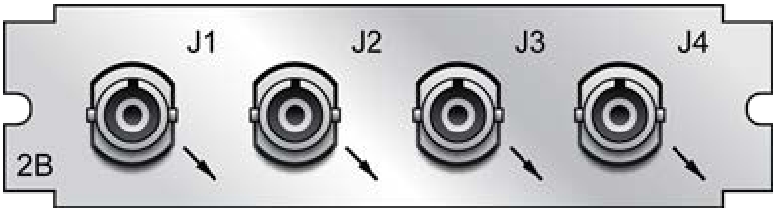


Figure 5-5: Model 1204-2B option card rear plate

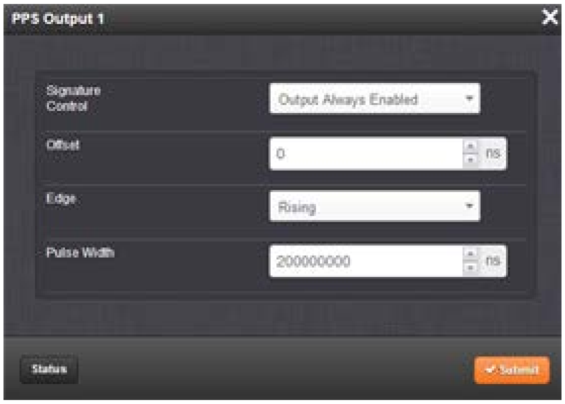
5.2.1.6 PPS Output: Edit Window

To configure the settings of a **PPS Output**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entries for these option cards are:

- 1PPS OUT, 4-BNC
- 1PPS OUT, 10V
- 1PPS OUT, RS-485
- 1PPS OUT, Fiber

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Signature Control: Output Always Enabled

Offset: 0 ns

Edge: Rising

Pulse Width: 200000000 ns

The Edit window allows the configuration of the following settings:

- **Signature Control:** Used to control when the 1PPS output signal will be present. See "Signature Control" on page 201.
- **Offset:** Used to account for 1PPS cable delays or other latencies in the 1PPS output. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.
- **Edge:** The operator can select if the output signal is a positive (reference on the rising edge) or a negative (reference on the falling edge) pulse.
- **Pulse Width:** Configures the Pulse Width of the 1PPS output. The Pulse Width is entered and displayed in nanoseconds (ns). The default Pulse Width is 200 milliseconds.

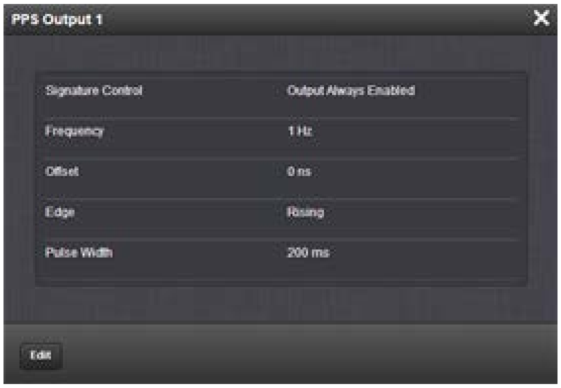
5.2.1.7 1PPS Output: Status Window

To view the current settings of a **PPS Output**, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entries for these option cards are:

- 1PPS OUT, 4-BNC
- 1PPS OUT, 10V
- 1PPS OUT, RS-485
- 1PPS OUT, Fiber

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Signature Control	Output Always Enabled
Frequency	1 Hz
Offset	0 ns
Edge	Rising
Pulse Width	200 ms

The Status window displays the following settings:

- **Signature Control:** Displays the current configuration of Signature Control; see "Signature Control" on page 201.
- **Frequency:** Indicates the configured frequency of the 1PPS output signal.
- **Offset:** Displays the configured Offset (to account for cable delays or other latencies).
- **Edge:** Shows if the on-time point of the 1PPS output is the rising or falling edge of the pulse.
- **Pulse Width:** Displays the configured Pulse Width of the 1PPS output. The Pulse Width is displayed in nanoseconds (ns). The default Pulse Width is 200 milliseconds.

5.2.2 1PPS In/Out [1204-28, -2A]

These 1PPS input/output cards provide one 1PPS input, and three or two additional 1PPS outputs on BNC or ST connectors for the SecureSync platform.

5.2.2.1 Model 1204-28 1PPS Input/Output: Specifications

- **Inputs/Outputs**: (1) 1PPS input/(3) 1PPS output
- **Signal Type and Connector**: TTL (BNC)
- **Input Impedance**: 50 Ω
- **Output Load Impedance**: 50 Ω
- **Rise Time to 90% of Level**: <10 ns
- **Programmable Pulse Width**: 100 ns to 900 ms with 20 ns resolution
- **Absolute Phase Error**: ±50 ns (1σ)
- **Programmable Phase Shift**: ±5ns to 500 ms with 5ns resolution
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-28: 1PPS 1-input/3-output, BNC connectors

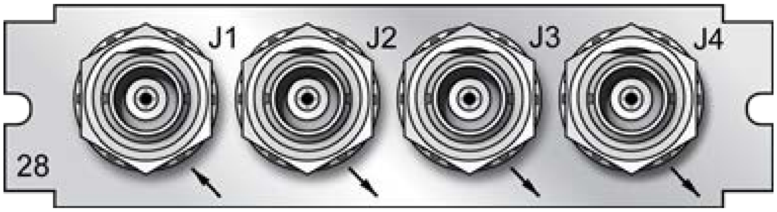


Figure 5-6: Model 1204-28 option card rear plate

5.2.2.2 Model 1204-2A 1PPS Input/Output: Specifications

- **Inputs/Outputs**: (1) 1PPS input/(2) 1PPS output
- Operating Wavelength: 820/850 nm
- **Optical Input Minimum Sensitivity**: -25 dBm @ 820 nanometers
- **Optical Output Power**: -15 dBm average into 50/125 fiber
- **Fiber Optic Compatibility**: 50/125 µm, 62.5/125 µm multi-mode cable
- **Optical Connector**: ST
- **Output Programmable Pulse Width**: 100 ns to 900 ms with 20 ns resolution
- **Output Absolute Phase Error**: ±50 ns (1σ)
- **Output Programmable Phase Shift**: ±5ns to 500 ms with 5ns resolution
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-2A: 1PPS 1-in/2-output, ST connectors

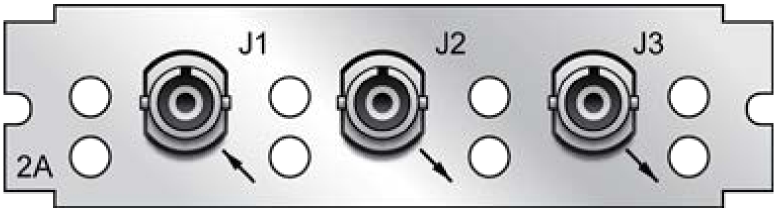


Figure 5-7: Model 1204-2A option card rear plate

5.2.2.3 1PPS Input or Output: Viewing Signal State

To quickly view if the 1PPS inputs and outputs of this option card are currently enabled or disabled, go to the option card’s **Status Summary** panel. For instructions, see: "Viewing the Signal State of an Input or Output" on page 296.

5.2.2.4 1PPS Output: Edit Window

To configure the settings of a **1PPS output**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

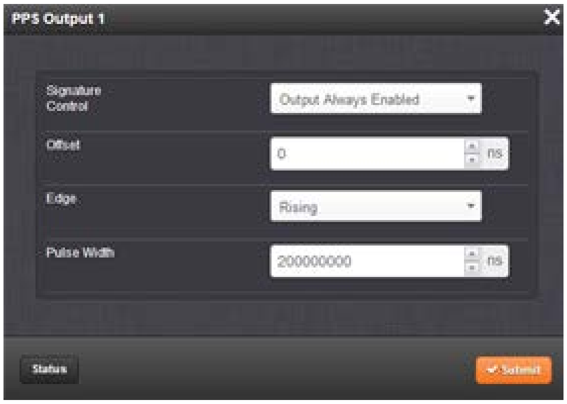
The Web UI list entries for these cards are:

- 1PPS In/Out
- 1PPS In/Out, Fiber

The connector numbers are:

- J2, J3, J4 (model -28)
- J2, J3 (model -2A)

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



PPS Output 1

Signature Control: Output Always Enabled

Offset: 0 ns

Edge: Rising

Pulse Width: 200000000 ns

The fields available are:

- **Signature Control**: Used to control when the 1PPS output signal will be present. See: "Signature Control" on page 201.
- **Offset**: Used to account for 1PPS cable delays or other latencies in the 1PPS output. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.
- **Edge**: The operator can select if the output signal is a positive (reference on the rising edge) or a negative (reference on the falling edge) pulse.
- **Pulse Width**: Configures the Pulse Width of the 1PPS output. The Pulse Width is entered and displayed in nanoseconds (ns). The default Pulse Width is 200 milliseconds.

5.2.2.5 1PPS Output: Status Window

To view the current settings of a **1PPS output**, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

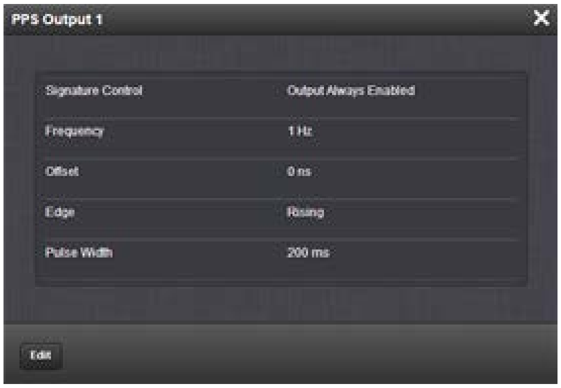
The Web UI list entries for these cards are:

- 1PPS In/Out
- 1PPS In/Out, Fiber

The connector numbers are:

- J2, J3, J4 (model -28)
- J2, J3 (model -2A)

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



PPS Output 1

Signature Control	Output Always Enabled
Frequency	1 Hz
Offset	0 ns
Edge	Rising
Pulse Width	200 ms

The fields displayed are:

- **Signature Control**: Displays the current configuration of Signature Control. See "Signature Control" on page 201.
- **Frequency**: Indicates the configured frequency of the 1PPS output signal.
- **Offset**: Displays the configured Offset (to account for cable delays or other latencies).
- **Edge**: Shows if the on-time point of the 1PPS output is the rising or falling edge of the pulse.
- **Pulse Width**: Displays the configured Pulse Width of the 1PPS output. The Pulse Width is displayed in nanoseconds (ns). The default Pulse Width is 200 milliseconds.

5.2.2.6 1PPS Input: Edit Window

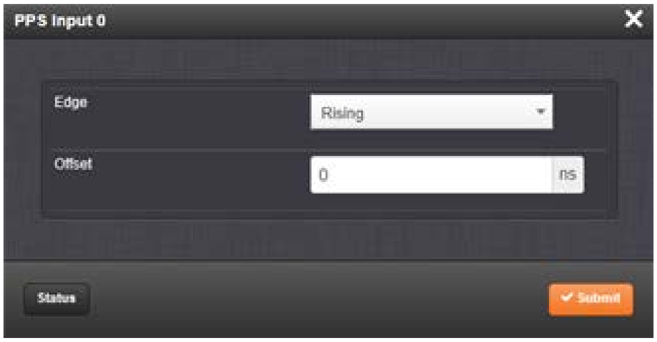
To configure the settings of the **PPS Input** (also referred to as ‘Reference’), go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entries for these cards are:

- 1PPS In/Out
- 1PPS In/Out, Fiber

The connector number for the input is: J1

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).


PPS Input 0

Edge: Rising

Offset: 0 ns

The Edit window allows the configuration of the following settings:

- **Edge**: The operator can select either the rising or the falling edge as the input time reference (defines the on-time point of the signal).
- **Offset**: It is possible to add an offset to the input signal (to account for cable delays), with a resolution of 5ns and a positive or negative value of 500 ms maximum.

5.2.2.7 1PPS Input: Status Window

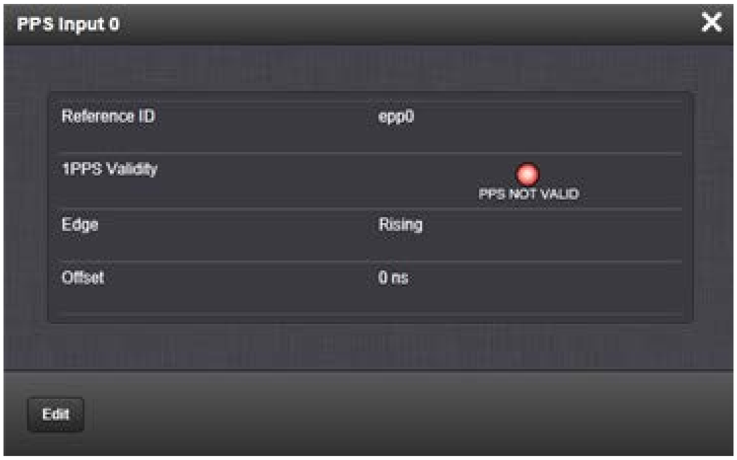
To view the current settings of the **PPS Input** (also referred to as 'Reference'), go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entries for these cards are:

- 1PPS In/Out
- 1PPS In/Out, Fiber

The connector number for the input is: J1

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).


PPS Input 0

Reference ID	epp0
1PPS Validity	● PPS NOT VALID
Edge	Rising
Offset	0 ns

The Status window displays the following settings:

- **Reference ID**: Name used to represent this 1PPS input reference in the Reference Priority table. See also: "Configuring Input Reference Priorities" on page 155.
- **1PPS Validity**: Indicates “OK” (green) if the 1PPS input signal is present and valid. Indicates “Not Valid” (orange) if the 1PPS input signal is either not present or is not considered valid.
- **Edge**: Displays the selected Edge (rising of falling) of the 1PPS input that defines the on-time point.
- **Offset**: Displays the configured 1PPS offset values.

The 1PPS Input signal is analyzed and an absence of the signal triggers a “Not Valid” indication.

5.2.3 1PPS In/Out, 10 MHz In [1204-01, -03]

5.2.3.1 Model 1204-01, 1PPS/Freq Input (TTL): General Specifications

- **Inputs/Outputs**: One Frequency Input (=J1), one 1PPS Input (=J2), one 1PPS Output
- **Signal Type And Connector**: TTL/Sine (BNC into 50 Ω)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-01: 1PPS/Freq input (TTL levels) module

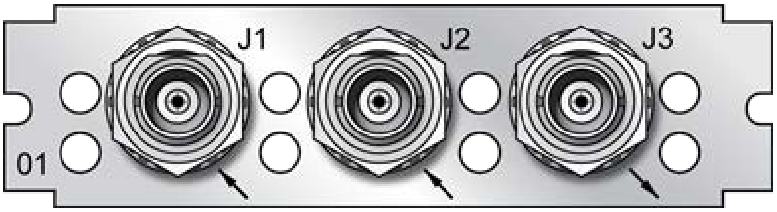


Figure 5-8: Model 1204-01 option card rear plate

5.2.3.2 Model 1204-03, 1PPS/Freq Input (RS-485): General Specifications

- **Inputs/Outputs**: (1) 1PPS Input, (1) Freq Input (1) 1PPS Output. All input and output signals are RS-485 compatible.
- **Signal Type And Connector**: Balanced RS-485 (3.8 mm terminal block)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-03: 1PPS/Freq input (RS-485 levels) module

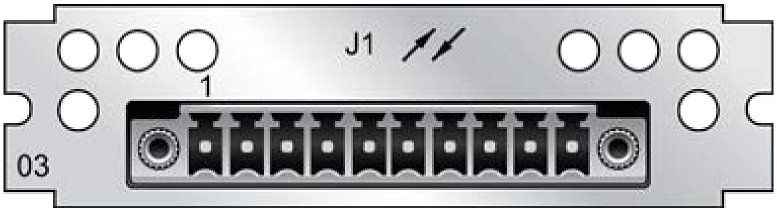


Figure 5-9: Model 1204-03 option card rear plate

Pin assignment, RS-485 connector

Pin No.	Signal	Function
1	GND	Ground
2	FREQIN_RS485+	RS-485 Frequency Input +
3	FREQIN_RS485-	RS-485 Frequency Input -
4	GND	Ground
5	PPSIN_RS485+	RS-485 1PPS Input +
6	PPSIN_RS485-	RS-485 1PPS Input -
7	GND	Ground
8	PPSOUT_RS485+	RS-485 1PPS Output +
9	PPSOUT_RS485-	RS-485 1PPS Output -
10	GND	Ground

Table 5-5: Model 1204-03 1PPS/Freq Input: Connector pin assignment

5.2.3.3 Models 1204-01,-03: Input/Output Specifications

FREQ Input Specifications

- **Signal Type And Connector**: Sine wave (BNC)
- **Detected Level**: +13 dBm to -6dBm
- **Frequency Setting**: 1KHz...10 MHz in 1Hz steps

1PPS Input Specifications

- **Input Impedance**: 50 Ω
- **Minimum Pulse Width detected**: 100 ns
- **Input Signal Jitter**: <±500 ns t o achieve oscillator lock, <±50 ns to achieve system performance
- **Programmable Phase Shift**: ±5ns to 500 ms with 5ns resolution

1PPS Output Specifications

- **Signal Type And Connector**: TTL level (BNC)
- **Output Load Impedance**: 50 Ω
- **Rise Time to 90% of Level**: <10 ns
- **Programmable Pulse Width**: 100 ns to 900 ms with 20 ns resolution

- **Absolute Phase Error**: ±50 ns (1σ)
- **Programmable Phase Shift**: ±5ns to 500 ms with 5ns resolution

5.2.3.4 1PPS Input and Output: Viewing Signal State

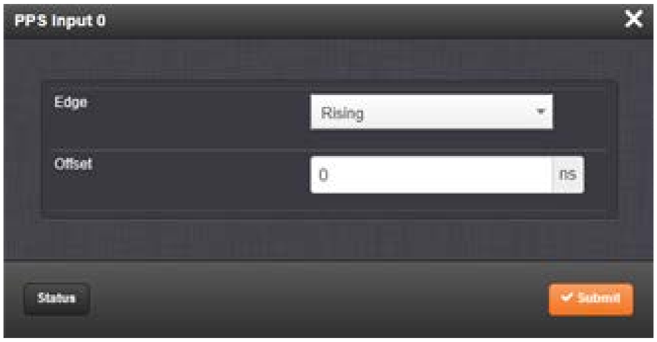
To quickly view if the PPS inputs and outputs of this option card are currently enabled or disabled, go to the option card's Status Summary panel. For instructions, see: "Viewing the Signal State of an Input or Output" on page 296.

5.2.3.5 1PPS Input: Edit Window

To configure the settings for the **1PPS Input** (also referred to as 'Reference'), go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entries for these cards are: **1PPS/Frequency BNC** and **1PPS/Frequency RS-485**. The connector number is: J2 (Model 1204-03: RS-485 connector: Pins 5 and 6)

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).


PPS Input 0

Edge: Rising

Offset: 0 ns

The Edit window allows the configuration of the following settings:

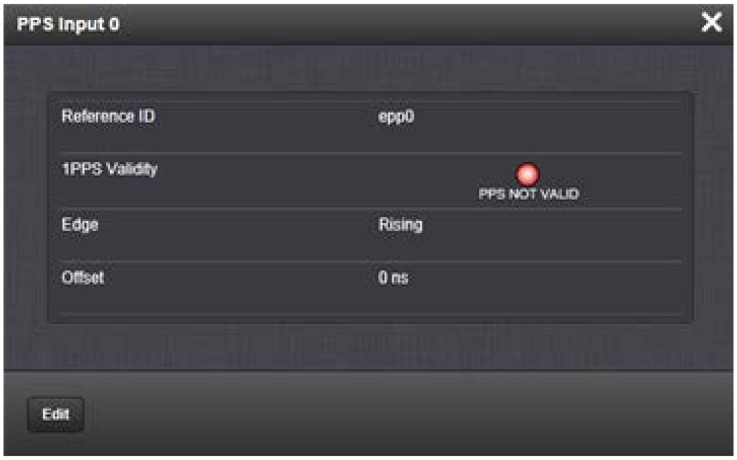
- **Edge**: The operator can select either the rising or the falling edge as the input time reference (defines the on-time point of the signal).
- **Offset**: It is possible to add an offset to the input signal (to account for cable delays), with a resolution of 5ns and a positive or negative value of 500 ms maximum.

5.2.3.6 1PPS Input: Status Window

To view the current settings of the **PPS Input** (also referred to as 'Reference'), go to its Status window. For instructions, see: "Verifying the Validity of an Input Signal" on page 297.

The Web UI list entries for these cards are: 1PPS/Frequency BNC and 1PPS/Frequency RS-485. The connector number is: J2 (Model 1204-03: RS-485 connector: Pins 5 and 6)

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Reference ID	epp0
1PPS Validity	PPS NOT VALID
Edge	Rising
Offset	0 ns

The Status window displays the following settings:

- **Reference ID**: Name used to represent this 1PPS input reference in the Reference Priority table; see "Configuring Input Reference Priorities" on page 155 for more information on reference priority configuration.
- **1PPS Validity**: Indicates “OK” (green) if the 1PPS input signal is present and valid. Indicates “Not Valid” (orange) if the 1PPS input signal is either not present or is not considered valid.
- **Edge**: Displays the selected Edge (rising of falling) of the 1PPS input that defines the on-time point.
- **Offset**: Displays the configured 1PPS offset values.

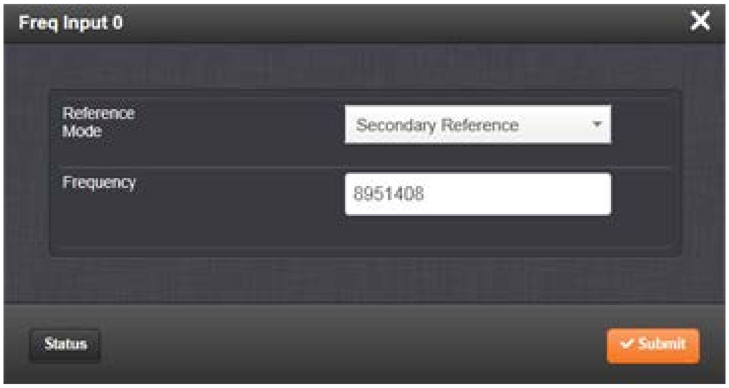
The 1PPS Input signal is analyzed and an absence of the signal triggers a “Not Valid” indication.

5.2.3.7 Frequency Input: Edit Window

To configure the settings for the **Frequency Input** (also referred to as ‘Reference’), go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entries for these cards are: 1PPS/Frequency BNC and 1PPS/Frequency RS-485. The connector number is: J1 (BNC card); J1 (RS-485 card).

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Freq Input 0

Reference Mode: Secondary Reference

Frequency: 8951408

The Edit window allows the configuration of the following settings:

- **Reference Mode**: Used to control how the reference mode operates in determining its validity. Values are:
  - **Primary Reference**–Allows the frequency reference to be valid based solely on its own presence.
  - **Secondary Reference**–Requires another valid reference to synchronize the system before the frequency reference can be determined to be valid. This is used when the frequency reference is intended to operate as a backup reference to a different primary reference source.
- **Frequency**: Used to configure the frequency (in Hertz) of the input signal. The available Frequency range is 1KHz...10 MHz in 1Hz steps.

The input frequency is measured versus internal frequency and compared to the setup value. If the discrepancy is larger than 1kHz, the input is disqualified and not considered valid. The frequency reference does not inherently provide an on-time point, so it relies on the current on-time point of the system prior to its taking over for synchronization.

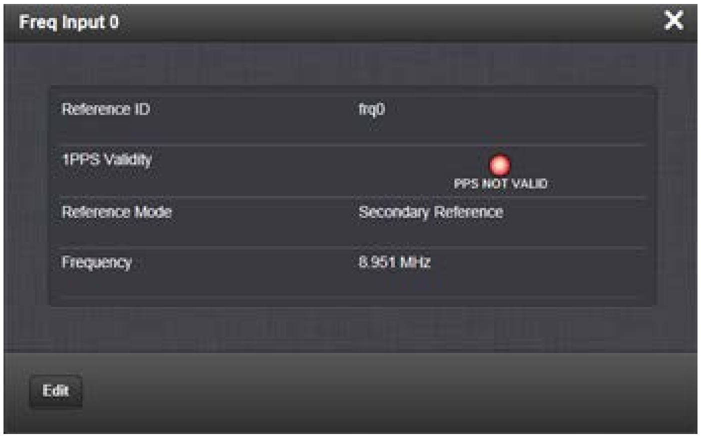
5.2.3.8 Frequency Input: Status Window

To view the current settings of the **Frequency Input** (also referred to as 'Reference'), go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entries for these cards are: 1PPS/Frequency BNC and 1PPS/Frequency RS-485.

The connector number is: J1 (BNC card); J1 (RS-485 card).

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



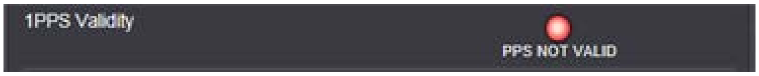
Freq Input 0

Reference ID	frq0
1PPS Validity	● PPS NOT VALID
Reference Mode	Secondary Reference
Frequency	8.951 MHz

The Status window displays the following settings:

- **Reference ID**: Name used to represent this 1PPS input reference in the Reference Priority table; see "Configuring Input Reference Priorities" on page 155 for more information on reference priorities.
- **1PPS Validity**: Indicates “OK” (green) if the 1PPS input signal is present and valid. Indicates “Not Valid” (orange) if the 1PPS input signal is either not present or is not considered valid.
- **Reference Mode**: Displays how the reference mode operates in determining its validity.
- **Frequency**: Displays (in Hertz) the configured frequency of the input frequency signal.

The 1PPS Input signal is analyzed and an absence of the signal triggers a “Not Valid” indication.



1PPS Validity ● PPS NOT VALID

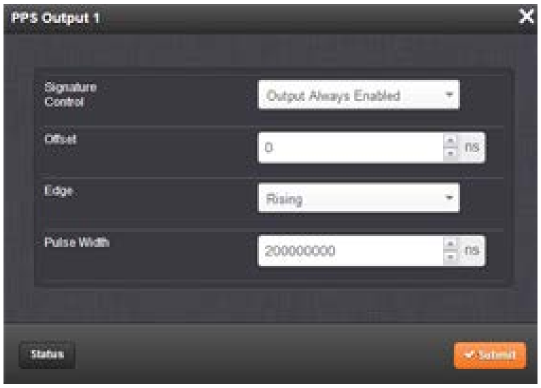
5.2.3.9 1PPS Output: Edit Window

To configure the settings of the **1PPS output**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entries for these cards are: 1PPS/Frequency BNC and 1PPS/Frequency RS-485.

The connector number is: J3 (BNC card); J1 (RS-485 card).

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



PPS Output 1

Signature Control: Output Always Enabled

Offset: 0 ns

Edge: Rising

Pulse Width: 200000000 ns

The Edit window allows the configuration of the following settings:

- **Signature Control**: Used to control when the 1PPS output signal will be present. See "Signature Control" on page 201 for more information.
- **Offset**: Used to account for 1PPS cable delays or other latencies in the 1PPS output. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.
- **Edge**: The operator can select if the output signal is a positive (reference on the rising edge) or a negative (reference on the falling edge) pulse.
- **Pulse Width**: Configures the Pulse Width of the 1PPS output. The Pulse Width is entered and displayed in nanoseconds (ns). The default Pulse Width is 200 milliseconds.

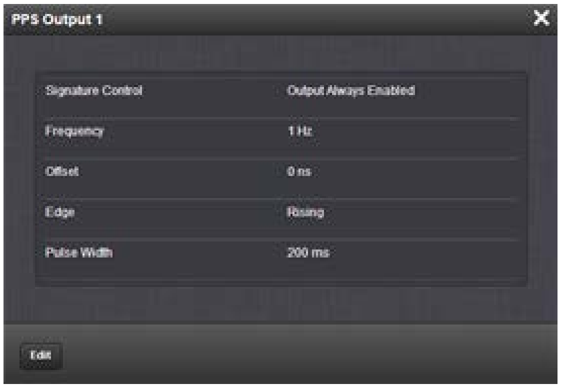
5.2.3.10 PPS Output: Status Window

To view the current settings of the **1PPS output**, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entries for these cards are: 1PPS/Frequency BNC and 1PPS/Frequency RS-485.

The connector number is: J3 (BNC card); J1 (RS-485 card).

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Signature Control	Output Always Enabled
Frequency	1 Hz
Offset	0 ns
Edge	Rising
Pulse Width	200 ms

The Status window displays the following settings:

- **Signature Control**: Displays the current configuration of Signature Control. See also: "Signature Control" on page 201.
- **Frequency**: Indicates the configured frequency of the 1PPS output signal.
- **Offset**: Displays the configured Offset (to account for cable delays or other latencies).
- **Edge**: Shows if the on-time point of the 1PPS output is the rising or falling edge of the pulse.
- **Pulse Width**: Displays the configured Pulse Width of the 1PPS output. The Pulse Width is displayed in nanoseconds (ns). The default Pulse Width is 200 milliseconds.

5.2.4 Frequency Out [1204-08, -1C, -26, -38]

5.2.4.1 Frequency Out [1204-08, -1C, -26, -38]: Specifications

- **Outputs**: (3) 1MHz, (3) 5MHz, or (3) 10 MHz Outputs
- **Signal Type and Connector**:
  - (10 MHz) +13 dBm into 50 Ω, BNC, or TNC (-38)
  - (5MHz) +10 dBm into 50 Ω, BNC, or TNC (-38)
  - (1MHz) +10 dBm into 50 Ω, BNC, or TNC (-38)
- **1MHz or 5MHz Phase Noise** (with OCXO or low phase noise Rubidium oscillator):
  - -115 dBc/Hz @ 10 Hz
  - -130 dBc/Hz @ 100 Hz
  - -140 dBc/Hz @ 1kHz
- **1MHz or 5MHz Phase noise** (with Rubidium oscillator):
  - -85 dBc/Hz @ 10 Hz
  - -110 dBc/Hz @ 100 Hz
  - -130 dBC/Hz @ 1kHz

- **10 MHz Phase Noise** (with TCXO oscillator):
  - -110 dBc/Hz @ 100 Hz
  - -135 dBc/Hz @ 1kHz
  - -140 dBc/Hz @ 10 kHz
- **10 MHz Phase Noise** (with OCXO oscillator) [Numbers in brackets represent Low Phase Noise OCXO option]:
  - -95 [-100] dBc/Hz @ 1Hz
  - -123 [-128] dBc/Hz @ 10 Hz
  - -140 [-148] dBc/Hz @ 100 Hz
  - -145 [-153] dBc/Hz @ 1kHz
  - -150 [-155] dBc/Hz @ 10 kHz
- **Harmonics**: -40 dBc minimum
- **Spurious**:
  - -60 dBc minimum (1MHz)
  - -50 dBc minimum (5MHz)
  - -70 dBc minimum (10 MHz)
- **Accuracy**: See "10 MHz output – oscillator accuracies" on page 12
- **Maximum Number of Cards**:
  - (4)
- **Ordering Information**:
  - 1204-1C: 10 MHz output (3X) Module
  - 1204-38: 10 MHz TNC output (3X) Module
  - 1204-08: 5MHz output (3X) Module
  - 1204-26: 1MHz output (3X) Module

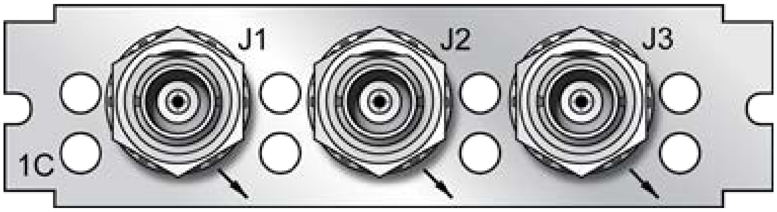


Figure 5-10: Model 1204-1C option card rear plate

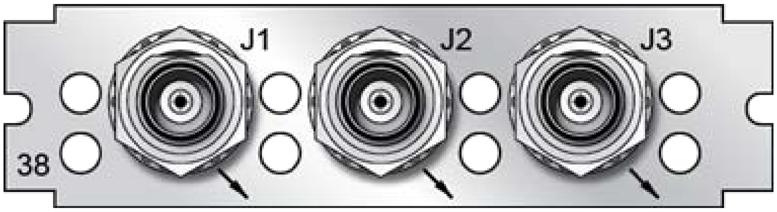


Figure 5-11: Model 1204-38 option card rear plate

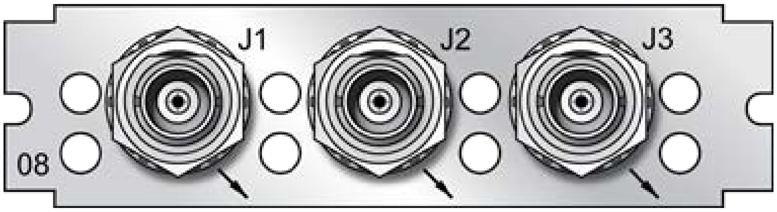


Figure 5-12: Model 1204-08 option card rear plate

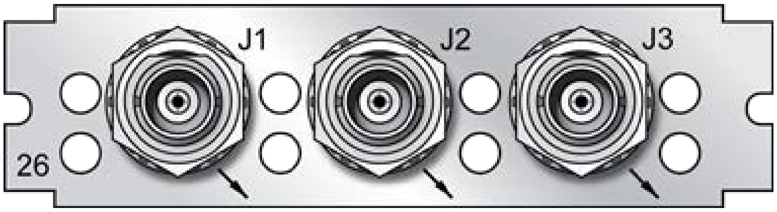


Figure 5-13: Model 1204-26 option card rear plate

The Frequency Out option cards each have 3 outputs, distributing a 1MHz signal, 5MHz or 10 MHz signal (depending on the card model). All 3 outputs are configured as a single output and will appear as such in the SecureSync Web UI, numbered sequentially by card instance, starting with 0 (except the 10 MHz option card, which starts with no.1 because of the built-in 10 MHz output.)

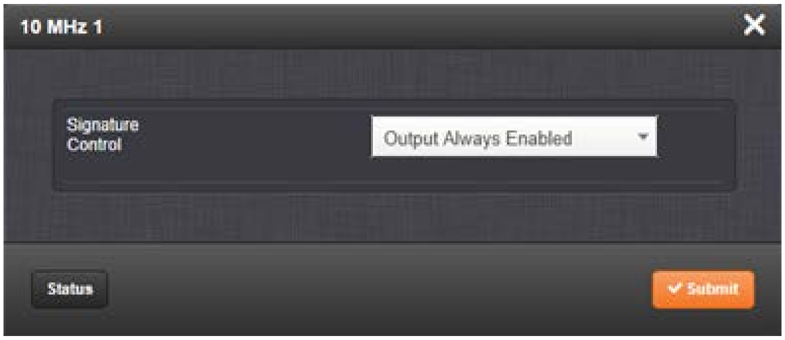
5.2.4.2 Frequency Output: Edit Window

To configure the settings of a **Frequency Output**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The list entry for this card is named: 1/5/10 MHz BNC (or: TNC)

The connector numbers are: J1...J3.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Signature Control: Output Always Enabled

The Edit window allows the configuration of the following settings:

- **Signature Control**: Controls when the output will be present; see "Signature Control" on page 201.

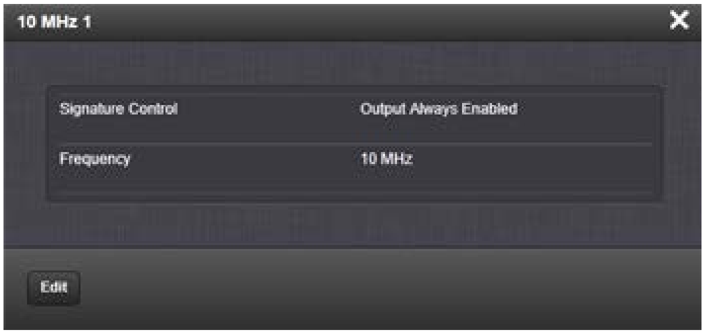
5.2.4.3 Frequency Output: Status Window

To view the settings of a **Frequency output**, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entry for this card is named: 1/5/10 MHz BNC (or: TNC).

The connector numbers are: J1...J3.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Signature Control	Output Always Enabled
Frequency	10 MHz

The Status window displays the following settings:

- **Signature Control**: Controls when the output will be present. See also: "Signature Control" on page 201.
- **Frequency**: The frequency of the output: 1MHz, 5MHz or 10 MHz, depending on the card model.

For more information on monitoring installed option cards, see: "Monitoring the Status of Option Cards" on page 247.

5.2.5 Programmable Frequency Out [1204-13, -2F, -30]

Programmable Frequency Output option modules provide output square waves at programmable pulse rates, or sine waves at programmable frequencies. The output frequency, which is adjustable via the SecureSync Web UI, is locked to the SecureSync system-disciplined oscillator.

These option cards can be used for a variety of applications requiring programmable frequency outputs. The RS-485 model of this card can be operated as an N.8 frequency synthesizer.

Depending on your card model number, the outputs are available in different formats:

- RS-485 on a pluggable terminal block
- TTL square wave on BNC, or
- Sine wave on BNC

Each output can be phase-offset between 0-360° in 0.1°-increments.

5.2.5.1 Programmable Frequency Card 1204-13 (Sine Wave, BNC): Specifications

- **Outputs**: (4) independently programmable sine wave outputs
- **Signal Type**: +13 dBm
- **Wave Form**: sine
- **Connector**: BNC
- **Output Load Impedance**: 50 Ω
- **Output Pulse/Frequency Rates**: 1Hz to 25 MHz in 0.1-Hz increments
- **Accuracy**: Function of input synchronization source (GPS, IRIG, 1 PPS, etc.)
- **Synchronization**: Output frequency locked to SecureSync disciplined 10 MHz
- **Jitter**, cycle-to-cycle: n/a
- **Phase Noise**:
  - -120 dBc/Hz @ 1kHz offset
  - -130 dBc/Hz @ 10-kHz offset
  - -140 dBc/Hz @ 100-kHz offset
- Harmonics: <-30 dBc
- **Spurious**: <-60 dBc
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-13, Programmable Frequency Card, sine wave, BNC

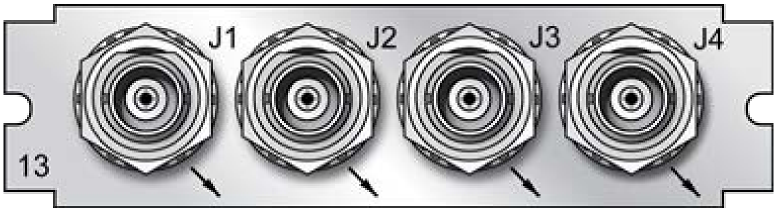


Figure 5-14: Model 1204-13 option card rear plate

5.2.5.2 Programmable Frequency Card 1204-2F (TTL, BNC): Specifications

- **Outputs**: (4) independently programmable square wave outputs
- **Signal Type**: TTL (BNC)
- **Wave Form**: square
- **Connector**: BNC
- **Output Load Impedance**: 50 Ω
- **Output Pulse/Frequency Rates**: 1PPS to 25 MPPS in 0.1-PPS increments
- **Accuracy**: Function of input synchronization source (GPS, IRIG, 1 PPS, etc.)
- **Synchronization**: Output frequency locked to SecureSync disciplined 10 MHz
- **Jitter**, cycle-to-cycle: <10 ns
- **Phase Noise**: n/a
- **Harmonics**: n/a
- **Spurious**: n/a
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204–2F, Programmable Frequency Card, TTL, BNC

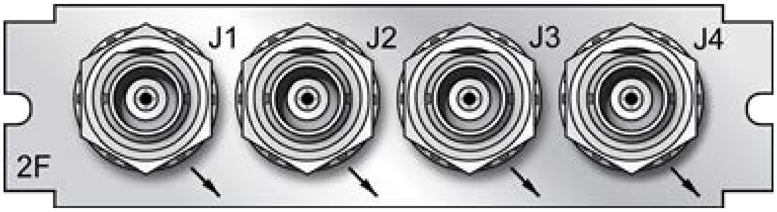


Figure 5-15: Model 1204-2F option card rear plate

5.2.5.3 Progr. Frequ. Card 1204-30 (TTL, RS-485): Specifications

- **Outputs**: (4) independently programmable square wave outputs
- **Signal Type**: RS-485
- **Wave Form**: square
- **Connector**: Terminal block
- **Output Load Impedance**: n/a
- **Output Pulse/Frequency Rates**: 1PPS to 25 MPPS in 0.1-PPS increments
- **Accuracy**: Function of input synchronization source (GPS, IRIG, 1 PPS, etc.)
- **Synchronization**: Output frequency locked to SecureSync disciplined 10 MHz

- **Jitter**, cycle-to-cycle: <10 ns
- **Phase Noise**: n/a
- **Harmonics**: n/a
- **Spurious**: n/a
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204–30, Programmable Frequency Card, TTL, RS-485

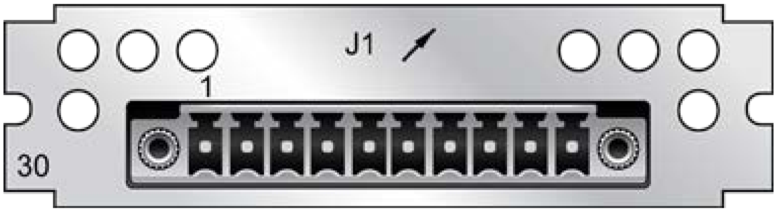


Figure 5-16: Model 1204-30 option card rear plate

Pin No.	Function
1	Frequ. Output 1 +
2	Frequ. Output 1 -
3	GND
4	Frequ. Output 2 +
5	Frequ. Output 2 -
6	Frequ. Output 3 +
7	Frequ. Output 3 -
8	GND
9	Frequ. Output 4 +
10	Frequ. Output 4 -

Table 5-6: Model 1204-30 terminal block pin assignments

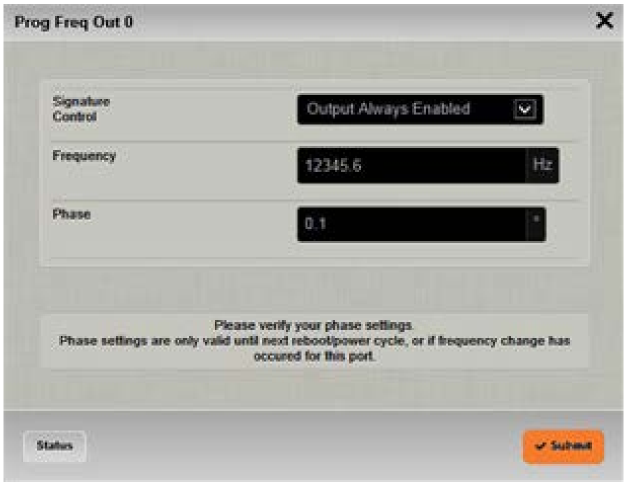
5.2.5.4 Programmable Frequency Output: Edit Window

To configure a **Programmable Frequency Output**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entry for this card is: Prog Freq Out, Sine [or: TTL, or: RS-485, respectively].

The connector numbers are: J1...J4 [J1 for the RS-485 model].

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Prog Freq Out 0

Signature Control: Output Always Enabled

Frequency: 12345.6 Hz

Phase: 0.1 °

Please verify your phase settings.
Phase settings are only valid until next reboot/power cycle, or if frequency change has occured for this port.

The Edit window allows the configuration of the following settings:

- **Signature Control**: Controls when the output will be present. See also: "Signature Control" on page 201.
- **Frequency**: Enter the desired output frequency. The ranges are as follows:
  - Sine wave output frequency (model no. 1204-13): 1 to 25,000,000 Hz
  - Pulse rate output in Hertz (model no.'s 1204-2F/-30): 1 to 25,000,000 PPS
- **Phase**: Adjust the phase by entering a phase offset (0.1 to 360°), if required.

> **Note:** The phase offset will lose its reference at a SecureSync reboot, and hence the value will be reset to 0 (ZERO).
>
> The reference will also be lost if you enter a new output frequency for a port - however in this case, the value will not be reset to 0, but instead remain unchanged. In both cases you will need to re-enter the required phase offset value.

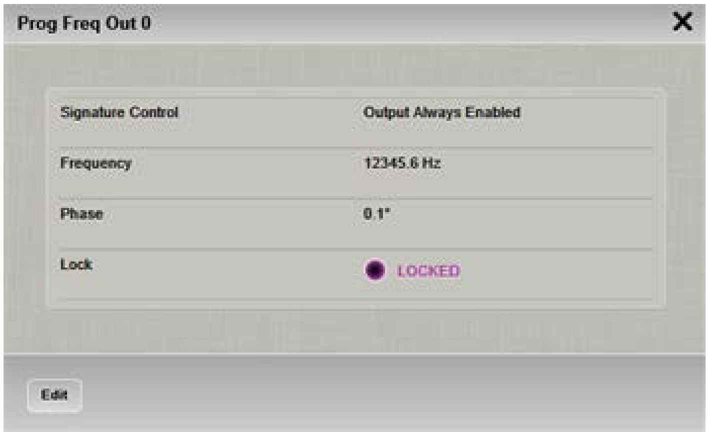
5.2.5.5 Programmable Frequency Output: Status Window

To view the settings of a **Programmable Frequency Output**, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entry for this card is named: Prog Freq Out, Sine [or: TTL, or: RS-485, respectively].

The connector numbers are: J1...J4 [J1 for the RS-485 model].

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Prog Freq Out 0

Signature Control	Output Always Enabled
Frequency	12345.6 Hz
Phase	0.1°
Lock	● LOCKED

The Status window displays the following settings:

- **Signature Control**: Controls when the output will be present. See also: "Signature Control" on page 201.
- **Frequency**: Indicates the configured frequency.
- **Phase**: Displays the configured phase offset (e.g., to account for delays caused by different cable lengths, or other latencies).
- **Lock**: Shows, if the output frequency is locked to the SecureSync system-disciplined oscillator.

> **Note:** Even if an output frequency status is LOCKED, it will not be available at the output port, if the Signature Control for that port has been DISABLED.

5.2.6 Programmable Square Wave Out [1204-17]

The Model 1204-17 Square Wave output Option Card provides four programmable square wave outputs for the SecureSync platform.

- **Inputs/Outputs**: (4) Programmable square wave outputs
- **Signal Type and Connector**: TTL (BNC)
- **Accuracy**: ±50 ns (1σ)
- **Output Load Impedance**: 50 Ω
- **Rise Time to 90% of Level**: <10 ns
- **Programmable Period**: 100 ns to 1,000,000,000 ns in 5ns steps, to 60,000,000 µs in 1µs steps
- **Programmable Pulse Width**: 20 ns to 900 ms with 5 ns resolution
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-17: Square Wave Out

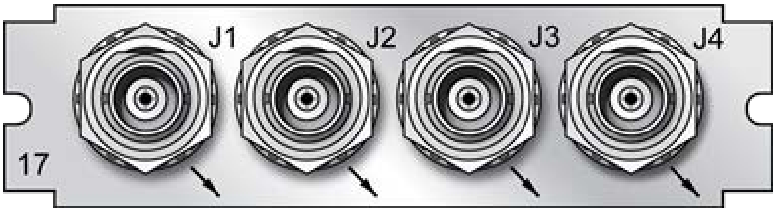


Figure 5-17: Model 1204-17 option card rear plate

5.2.6.1 Square Wave Output: Signal State

To quickly view if the **Square Wave Outputs** of this option card are currently enabled or disabled, go to the option card's Status Summary panel. For instructions, see: "Viewing the Signal State of an Input or Output" on page 296.

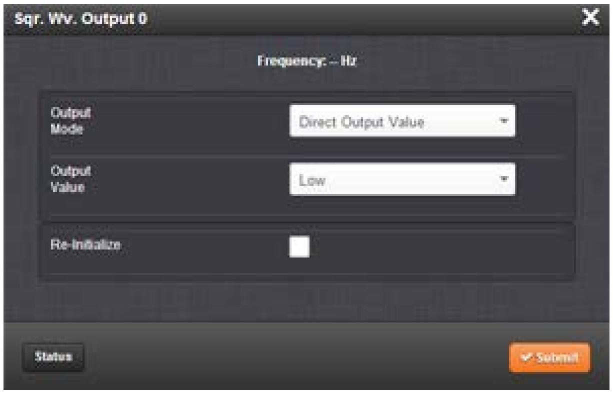
5.2.6.2 Square Wave Output: Edit Window

To configure one of the **Square Wave Outputs**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entry for this card is named: Sq Wv Out, BNC.

The connector numbers are: J1...J4.

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Sqr. Wv. Output 0

Frequency: -- Hz

Output Mode: Direct Output Value

Output Value: Low

Re-Initialize □

The Edit window allows the configuration of the following settings:

- **Output Mode**: This is a drop-down list, offering the following options:
- **Output Value**: Determines the output level (low or high).
- **Re-Initialize**: Reinitializes square wave generation and aligns to 1PPS.

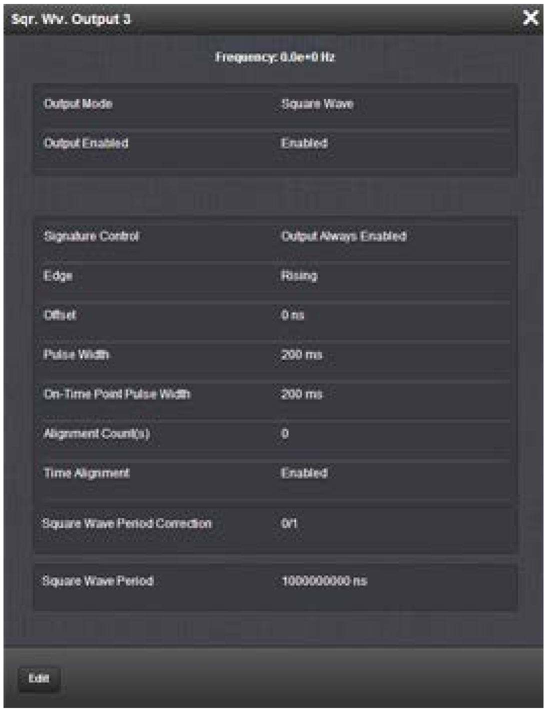
5.2.6.3 Square Wave Output: Status Window

To view the current settings of a **Square Wave Output**, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entry for this card is named: Sq Wv Out, BNC.

The connector numbers are: J1...J4.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Frequency: 0.0e+0 Hz

Output Mode	Square Wave
Output Enabled	Enabled
Signature Control	Output Always Enabled
Edge	Rising
Offset	0 ns
Pulse Width	200 ms
On-Time Point Pulse Width	200 ms
Alignment Count(s)	0
Time Alignment	Enabled
Square Wave Period Correction	0/1
Square Wave Period	1000000000 ns

The Status window displays the following settings: (The fields viewable are contextually determined according to the output mode.)

- **Output Mode**–This is a drop-down list, offering the following options:
  - Direct Output Value–Output will be low or high determined by the output value selection.
    - 1PPS
    - 1PPM
  - Square Wave–Output will generate a programmable square wave determined by the configuration.
  - Custom
- **Output Enabled**–Disables or enables output.

- **Signature Control**–Controls when the output will be present. See also: "Signature Control" on page 201.
- **Edge**–Used to determine if the on-time point of the output is the rising or falling edge of the signal.
- **Offset**–Accounts for cable delays and other latencies, entered in nanoseconds.
- **Pulse Width**–Defines the pulse width of the output (entered in nanoseconds).
- **On-Time Point Pulse Width**–The on-time point pulse width is the pulse width of the first square wave pulse aligned to the 1PPS On-Time Point. This is only active when the alignment count is non-zero. (Entered in nanoseconds).
- **Alignment Count(s)**–The alignment counter determines how often (in seconds) the square wave will be aligned back to the 1PPS. Setting zero will disable PPS alignment beyond the initial alignment.
- **Time Alignment**–(Enabled/Disabled) The time alignment enable changes the function of the alignment counter to align the square wave whenever the current time's seconds value is a multiple of the alignment count. For example: If time alignment is enabled and alignment count is set to 15 seconds, the square wave will be aligned to the 1PPS when the seconds value on the time display equals 00, 15, 30, 45.
- **Period Correction**– Period correction allows for the generation of more precise frequencies at the expense of additional period jitter. An additional clock cycle is added for numerator periods every denominator periods. Over a length of time, the true square wave period comes to:
  - Period + (numerator/denominator)] * 5 nsec
- **Period**–Sets the period of the square wave (in ns or us scale).
  - The wave's frequency will display at the top of the window once you have configured the output. The frequency is calculated based on the Period and Period Correction settings.

5.2.7 Simulcast (CTCSS/Data Clock) [1204-14]

The Simulcast CTCSS/Data Sync/Data Clock Option Card provides CTCSS, data clock, and alarm outputs through relays for the SecureSync platform through one DB-9 and one RJ-12 connector. The maximum number of cards installed is six (6).

a. **Connector**: DB-9
   - **Outputs**:
     - (3) RS-485 Outputs (Data Clocks, CTCSS frequencies, 1PPS)
     - (1) Alarm
   - **Voltage**:
     - Alarms: GND normally, high impedance when Alarm

b. **Connector**: RJ-12

- **Outputs**:
  - (1) RS-485 Outputs (Data Clocks, CTCSS frequencies, 1PPS)
  - (2) Alarm
- **Voltage**:
  - Alarms: 5V pulled up through 10 kΩ normally, GND when Alarm

Note: By factory default, all CTCSS outputs are DISABLED.

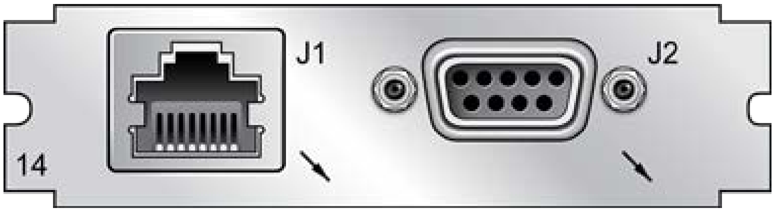


Figure 5-18: Model 1204-14 option card rear plate

5.2.7.1 Pin Assignment: DB-9 Connector

Outputs: Alarm0, CTC0 Out, CTC1 Out, CTC2 Out (with only one Simulcast option card installed)

Note: Alarm Output 0 through Alarm Output 3 are reserved by SecureSync. In the Web UI, numbering for alarm outputs for this option card will begin at Alarm 4, which is available on the DB-9 output, while Alarms 5 and 6 are assigned to the RJ-12 connector.

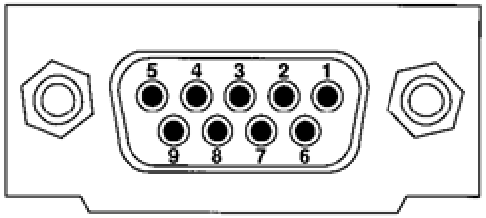


Figure 5-19: DB-9 connector pin-out

PIN	NOTES	SIGNAL	819x Mapping	819x Option17 Mapping
1	RS-485 + Terminal	Output 0+	+9.6 kHz	+CTCSS #1

PIN	NOTES	SIGNAL	819x Mapping	819x Option17 Mapping
2	RS-485 + Terminal	Output 1+	+18 kHz	+18 kHz
3	RS-485 + Terminal	Output 2+	+1 PPS	+CTCSS #2

4	Ground = Normal
	OPEN = ALARM
		Major Alarm	Major Alarm	Major Alarm

5	Cable Shield	Ground	Ground	Ground
6	RS-485 - Terminal	Output 0 -	-9.6 kHz	-- CTCSS #1
7	RS-485 - Terminal	Output 1 -	-18 kHz	- 18 kHz
8	RS-485 - Terminal	Output 2 -	-1PPS	- CTCSS #2
9	Cable Shield	GROUND	GROUND	GROUND

Table 5-7: DB-9 pin-out

5.2.7.2 Pin Assignment: RJ-12 Connector

Outputs: Alarm1, Alarm2, CTC3 Out, (with only one Simulcast option card installed)

> **Note:** Alarm Output 0 through Alarm Output 3 are reserved by SecureSync. In the Web UI, numbering for alarm outputs for this option card will begin at Alarm 4, which is available on the DB-9 output, while Alarms 5 and 6 are assigned to the RJ-12 connector.

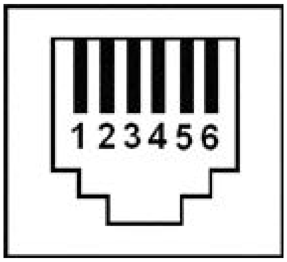


Figure 5-20: RJ-12 connector pin-out

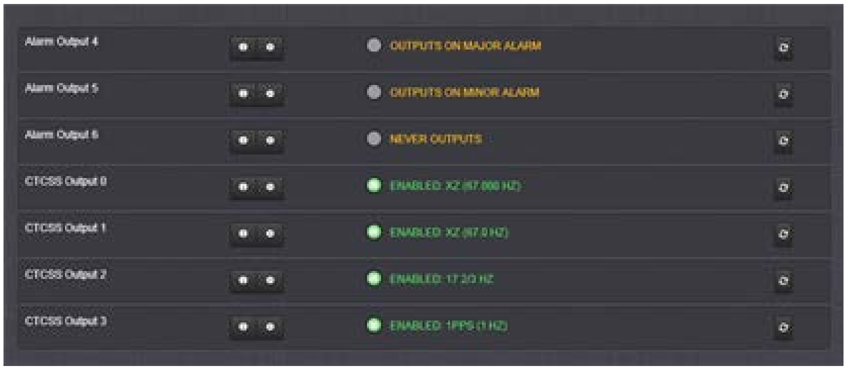
PIN	NOTES	SIGNAL	938x SP360 Mapping
1	Cable Shield	GROUND	GROUND
2	5V = NORMAL GROUND = ALARM	MAJOR ALARM RELAY	MAJOR ALARM RELAY
3	RS-485 + Terminal	Output 3+	+ 1PPS
4	RS-485 - Terminal	Output 3-	- 1PPS

PIN	NOTES	SIGNAL	938x SP360 Mapping
5	5V = NORMAL GROUND = ALARM	MINOR ALARM RELAY	MINOR ALARM RELAY
6	Cable Shield	GROUND	GROUND

Table 5-8: RJ-12 pin assignments

5.2.7.3 CTCSS and Alarm Outputs: Viewing Signal States

To quickly view the current signal state of the 1204-14 **Simulcast outputs**, go to the option card's Status Summary panel. For instructions, see: "Viewing the Signal State of an Input or Output" on page 296.



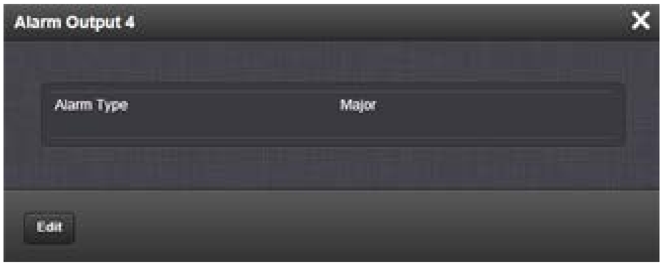
Alarm Output 4	OUTPUTS ON MAJOR ALARM
Alarm Output 5	OUTPUTS ON MINOR ALARM
Alarm Output 6	NEVER OUTPUTS
CTCSS Output 0	ENABLED: X2 (67.000 HZ)
CTCSS Output 1	ENABLED: X2 (67.0 HZ)
CTCSS Output 2	ENABLED: 17 2/3 HZ
CTCSS Output 3	ENABLED: 1PPS (1 HZ)

All outputs are listed, displaying their current output states. For a listing of the states, see "CTCSS Outputs: Edit Window" on the facing page, and "Alarm Outputs: Edit Window" on page 330.

To view the settings of *one* of the **Alarm Outputs** or **CTCSS Outputs**, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entry for this card is named: **Simulcast**.

> **Note:** Alarm Output 0 through Alarm Output 3 are reserved by SecureSync. Numbering for alarm outputs from the option card will begin at Alarm 4, which is available on the DB-9 output, while Alarms 5 and 6 are assigned to the RJ-12 connector.



Alarm Output 4

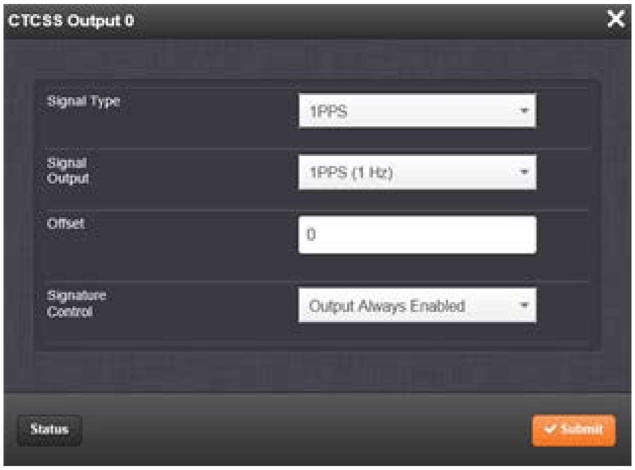
Alarm Type: Major

Figure 5-21: Simulcast Alarm Output Status window

5.2.7.4 CTCSS Outputs: Edit Window

To configure a **CTCSS output**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entry for this card is named: **Simulcast**.



CTCSS Output 0

Signal Type: 1PPS

Signal Output: 1PPS (1 Hz)

Offset: 0

Signature Control: Output Always Enabled

The Edit window allows the configuration of the following settings:

- **Signal Type**: Allows selection of the desired signal type. Available options include:
  - Disabled
  - CTCSS 1/3 Tones
  - CTCSS 1/10 Tones
  - Data Clocks
  - 1PPS
- **Signal Output**:
  - CTCSS 1/3 Tones (see also: "CTCSS 1/3 Tones" on page 331)
  - CTCSS 1/10 Tones (see also: "CTCSS 1/10 Tones" on page 331)
  - Data Clocks (see also: "Data Clock Signals" on page 332)
  - 1PPS (see also: "1PPS Duty Cycle" on page 332)
- **Offset**: Value (in nanoseconds) that can be used to adjust for cable delays or latencies.
- **Signature Control**: Controls when the output will be present. For more information, see "Signature Control" on page 201.

5.2.7.5 819x Option 17 Mapping

To replicate settings used in Series 819x devices, use the following information to configure option card no. 1204-14 for compatible CTCSS operation:

- **DB-9 Output Index 0**: Set to desired CTCSS 1/10 or CTCSS 1/3 tone
- **DB-9 Output Index 1**: Set to 18 KHz Data Clock
- **DB-9 Output Index 2**: Set to desired CTCSS 1/10 or CTCSS 1/3 tone.

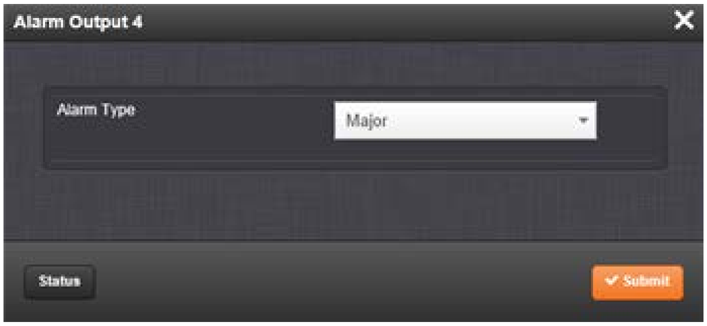
5.2.7.6 Alarm Outputs: Edit Window

To configure one of the **ALARM Outputs**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entry for this card is named: **Simulcast**.

> Note: Alarm Output 0 through Alarm Output 3 are reserved by SecureSync. Numbering for alarm outputs from the option card will begin at Alarm 4, which is available on the DB-9 output, while Alarms 5 and 6 are assigned to the RJ-12 connector.

> Note: You can configure the alarm type (None, Minor, or Major) for both the DB-9 and RJ-12 connectors. For additional information on alarm types, see "Minor and Major Alarms" on page 455.


Alarm Output 4

Alarm Type: Major

The Edit window allows the configuration of the following settings:

- **Alarm Type**:
  - None–Will not output for an alarm
  - Minor–Will output on a minor alarm
  - Major–Will output on a major alarm.

5.2.7.7 CTCSS Encoding Tables, Signal Data

Table 5-9: CTCSS 1/3 Tones

Code	Tone Freq.	Code	Tone Freq.	Code	Tone Freq.
		1A	103.666	6A	174.000
		1B	107.333	6B	180.000
XZ	67.000	2Z	111.000	7Z	186.333
WZ	69.333	2A	115.000	7A	193.000
XA	72.000	2B	119.000	M1	203.666
WA	74.333	3Z	123.000	8Z	206.666
XB	77.000	3A	127.333	M2	210.666
WB	79.666	3B	132.000	M3	218.333
YZ	82.666	4Z	136.666	M4	225.666
YA	85.333	4A	141.333	9Z	229.000
YB	88.666	4B	146.333	M5	233.666
ZZ	91.666	5Z	151.333	M6	242.000
ZA	95.000	5A	156.666	M7	250.333
ZB	97.333	5B	162.333	0Z	254.000
1Z	100.000	6Z	168.000		

Table 5-10: CTCSS 1/10 Tones

Code	Tone Freq.	Code	Tone Freq.	Code	Tone Freq.
XZ	67.0	1B	107.2	6A	173.8
WZ	69.3	2Z	110.9	6B	179.9
XA	71.9	2A	114.8	7Z	186.2
WA	74.4	2B	118.8	7A	192.8
XB	77.0	3Z	123.0	M1	203.5
WB	79.7	3A	127.3	8Z	206.5
YZ	82.5	3B	131.8	M2	210.7
YA	85.4	4Z	136.5	M3	218.1
YB	88.5	4A	141.3	M4	225.7
ZZ	91.5	4B	146.2	9Z	229.1
ZA	94.8	5Z	151.4	M5	233.6
ZB	97.4	5A	156.7	M6	241.8

Code	Tone Freq.	Code	Tone Freq.	Code	Tone Freq.
1Z	100.0	5B	162.2	M7	250.3
1A	103.5	6Z	167.9	0Z	254.1

Table 5-11: Data Clock Signals

Output	Duty Cycle
9.6 kHz, 18.0 kHz, 64.0 kHz	50% ±2%
17 2/3 Hz	888 microsecond pulse width
26 2/3 Hz	25% low, 75% high
33 1/3 Hz	208 microsecond pulse width

Table 5-12: 1PPS Duty Cycle

Output	Duty Cycle
1PPS	20% ±5%

5.3 Telecom Option Cards

This section contains technical information and Web UI procedures relevant to SecureSync option cards commonly used in the telecommunications industry.

5.3.1 T1/E1 Out [1204-09, -0A]

The E1/T1 option card provide 1.544 MHz or 2.048 MHz and E1 or T1 data outputs for the SecureSync platform. SecureSync meets G.812 Type I when installed with a Rubidium option, and G.811 when installed with a Rubidium option and synchronized with GNSS.

Note: Rubidium oscillators are recommended for the E1/T1 option card.

5.3.1.1 Model 1204-09 E1/T1 (75 Ω): Specifications

- **Outputs**:
  - (1) 1.544/2.048 MHz Output
  - (2) Unbalanced E1/T1 Outputs

- **T1 mode**:
  - 1.544 MHz (square wave) frequency output
  - (2) 1.544 Mb/sec data rate outputs:
    - Outputs are DS1 framed all ones
    - Supports Super Frame (SF or D4) and Extended Super Frame (ESF)
    - SSM support
- **E1 mode**:
  - 2.048 MHz (square wave) frequency output
  - (2) 2.048 Mb/sec data rate outputs:
    - Outputs are E1 frame all ones
    - Supports CRC4 and CAS Multiframe
    - SSM support
- **Connector and Signal Type**: BNC
  - 1.544/2.048 MHz TTL into 50 Ω
  - T1 according to GR-499-CORE (75 Ω)
  - E1 according to ITU-T G703 (75 Ω)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-09: T1/E1 (75 Ω) module

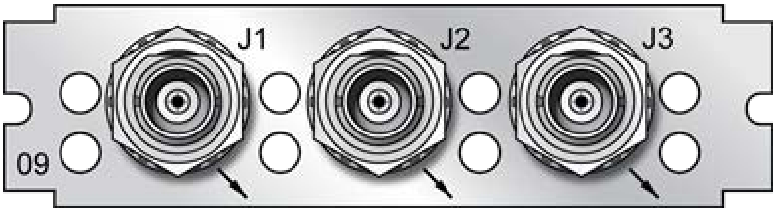


Figure 5-22: Model 1204-09 option card rear plate

5.3.1.2 Model 1204-0A E1/T1 (100/120 Ω): Specifications

- **Outputs**:
  - (1) 1.544/2.048 MHz RS-485 Outputs
  - (2) Balanced E1/T1Outputs

- **T1 mode**:
    - 1.544 MHz (square wave) frequency output
    - (2) 1.544 Mb/sec data rate outputs:
        - Outputs are DS1 framed all ones
        - Supports Super Frame (SF or D4) and Extended Super Frame (ESF)
        - SSM support
- **E1 mode**:
    - 2.048 MHz (square wave) frequency output
    - (2) 2.048 Mb/sec data rate outputs:
        - Outputs are E1 frame all ones
        - Supports CRC4 and CAS Multiframe
        - SSM support
- **Connector and Signal Type**: Terminal block
    - 1.544/2.048 MHz RS-485
    - T1 according to GR-499-CORE (100 Ω)
    - E1 according to ITU-T G703 (120 Ω)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-0A: T1/E1 (100/120 Ω) module

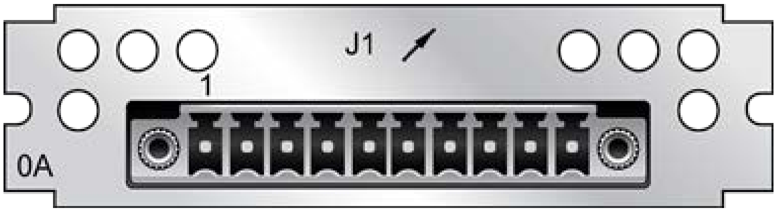


Figure 5-23: Model 1204-0A option card rear plate

Pin Assignments			
Pin No.	**Signal**	**Function**	**Description**
1	GND	Ground	Ground
2	1.544MHz/2.048MHz	RS-485 A Terminal	Square wave
3	1.544MHz/2.048MHz	RS-485 B Terminal	Square wave
4	GND	Ground	Ground
5	T1/E1 output A1	GR-499/G.703	Tip
6	T1/E1 output B1	GR-499/G.703	Ring

Pin Assignments			
Pin No.	**Signal**	**Function**	**Description**
7	GND	Ground	Ground
8	T1/E1 output A2	GR-499/G.703	Tip
9	T1/E1 output B2	GR-499/G.703	Ring
10	GND	Ground	Ground

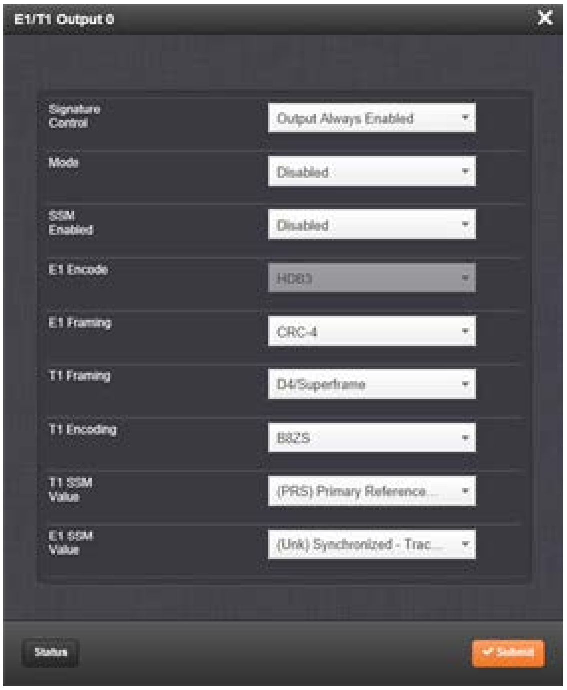
Table 5-13: 1204-0A option card pin assignments

5.3.1.3 E1/T1 Output: Edit Window

To configure an E1/T1 **data output** (1.544/2.048 MHz clock on J1 BNC connector and unbalanced E1/T1 outputs on J2 to J3 BNC connectors, or all terminal block J1 outputs), navigate to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

In the Web UI this card is listed under: **E1/T1 Out BNC** and **E1/T1 OUT Terminal**.

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Signature Control: Output Always Enabled

Mode: Disabled

SSM Enabled: Disabled

E1 Encode: HDB3

E1 Framing: CRC-4

T1 Framing: D4/Superframe

T1 Encoding: B8ZS

T1 SSM Value: (PRS) Primary Reference...

E1 SSM Value: (Unk) Synchronized - Trac...

The Edit window allows the configuration of the following settings:

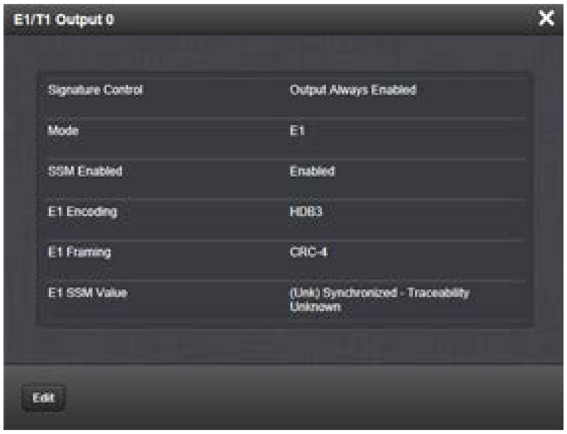
- **Signature Control**: Controls when the output will be present. For more information, see "Signature Control" on page 201.
- **Mode**: This option selects T1, E1, or disabled mode. For T1 mode, the clock output will be 1.544 MHz, and for E1 the clock output will be 2.048 MHz.
- **SSM Enabled**: Enables or disables Sync Status Messaging (SSM). T1 SSM is not valid with D4/Superframe or AIS framing. E1 SSM is not valid with AIS framing.
- **E1 Encode**: HDB3 only.
- **E1 Framing**: This option selects the framing standard (CRC-4, No CRC-4, or AIS).
- **T1 Framing**: This option selects the framing standard (D4/Superframe, Extended Superframe [CRC-6/no CR C-6], or AIS).
- **T1 Encoding**: This option selects the encoding method (B8ZS or AMI).
- **T1SSM Value**: This option selects the SSM quality level transmitted when SSM is enabled.
- **E1 SSM Value**: This option selects the SSM quality level transmitted when SSM is enabled.

5.3.1.4 E1/T1 Output: Status Window

To view the configuration settings of the **E1 OUT** or **T1 OUT** output, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entries for these cards are: **E1/T1 Out BNC** and **E1/T1 OUT Terminal**.

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Signature Control	Output Always Enabled
Mode	E1
SSM Enabled	Enabled
E1 Encoding	HDB3
E1 Framing	CRC-4
E1 SSM Value	(Unk) Synchronized - Traceability Unknown

The E1/T1 Output 0 Status Screen will vary according to whether the output signal mode is E1 or T1.

The Status windows display the following settings:

- **Signature Control**: Controls when the output will be present; see "Signature Control" on page 201.
- **Mode**: This option selects T1, E1, or disabled mode. For T1 mode, the clock output will be 1.544 MHz, and for E1 the clock output will be 2.048 MHz.
- **SSM Enabled**: Enables or disables Sync Status Messaging (SSM). T1 SSM is not valid with D4/Superframe or AIS framing. E1 SSM is not valid with AIS framing.
- **E1 Encoding**: HDB3 only.
- **E1 Framing**: This option selects the framing standard (CRC-4, No CRC-4, or AIS).
- **T1 Framing**: This option selects the framing standard (D4/Superframe, Extended Superframe [CRC-6/no CR C-6], or AIS).
- **T1 Encoding**: This option selects the encoding method (B8ZS or AMI).
- **T1 SSM Value**: This option selects the SSM quality level transmitted when SSM is enabled.
- **E1 SSM Value**: This option selects the SSM quality level transmitted when SSM is enabled.

5.4 Time Code Option Cards

This section contains technical information and SecureSync Web UI procedures for option cards designed to deliver timing data in time code formats, e.g. IRIG, HAVE QUICK, or STANAG.

5.4.1 IRIG Out [1204-15, -1E, -22]

These IRIG Output option cards provide SecureSync with four IRIG outputs. Available with BNC connectors, Fiber Optic ST connectors, or RS-485 terminal block.

5.4.1.1 IRIG Out (BNC): Specifications

- **Inputs/Outputs**: (4) IRIG Outputs
- **Signal Type and Connector**: IRIG A, B, E, G, NASA 36, amplitude modulated; 0.5 V to 6V_{p-p} into 50 Ω
- **Accuracy**: see "IRIG Output Accuracy Specifications" on page 513
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-15 Four IRIG Output Module, BNC

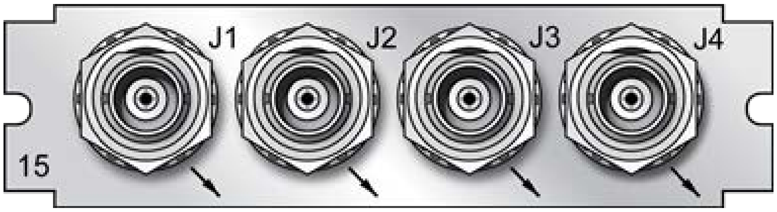


Figure 5-24: Model 1204-15 option card rear plate

5.4.1.2 IRIG Out (Fiber Optic): Specifications

- **Inputs/Outputs**: (4) IRIG Outputs
- **Signal**: IRIG A, B, E, G or NASA-36
- **Operating Wavelength**: 820/850 nm
- **Optical Power**: -15 dBm average into 50/125 fiber
- **Fiber Optic Compatibility**: 50/125 µm, 62.5/125 µm multi-mode cable
- **Optical Connector**: ST
- **Signal Type**: DC Level Shift (unmodulated)
- **Accuracy**: see "IRIG Output Accuracy Specifications" on page 513
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-1E Four IRIG Output Module, Fiber Optic

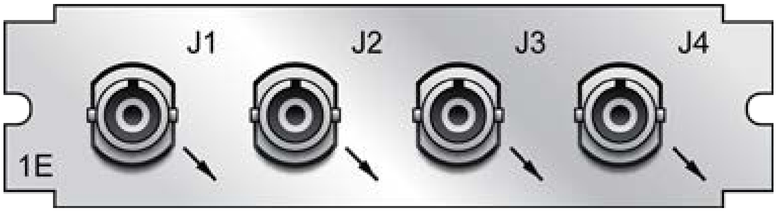


Figure 5-25: Model 1204-1E option card rear plate

5.4.1.3 IRIG Out (RS-485): Specifications

- **Inputs/Outputs**: (4) IRIG Outputs
- **Signal**: IRIG A, B, E, G or NASA-36
- **Signal Type and Connector**: RS-485 levels (terminal block)
- **Output Load Impedance**: 120 Ω
- **Accuracy**: see "IRIG Output Accuracy Specifications" on page 513
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-22 Four IRIG Output Module, RS-485

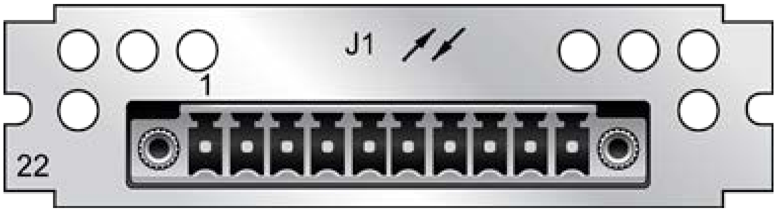


Figure 5-26: Model 1204-22 option card rear plate

Pin Assignments

J1 Pin No.	Function
1	IRIG Output 1 +
2	IRIG Output 1 -
3	GND
4	IRIG Output 2 +
5	IRIG Output 2 -
6	IRIG Output 3 +
7	IRIG Output 3 -
8	GND
9	IRIG Output 4 +
10	IRIG Output 4 -

Table 5-14: 1204-22 terminal block pin-out

5.4.1.4 IRIG Output: Viewing Signal State

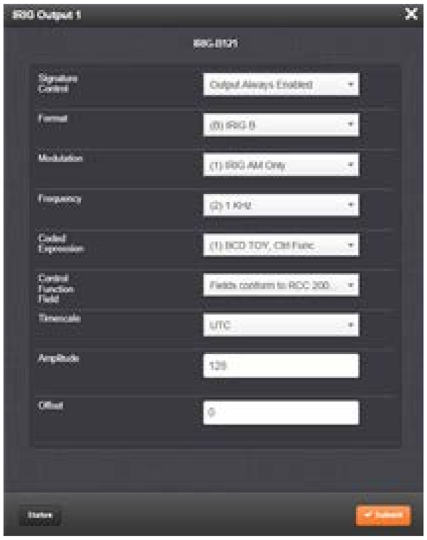
To quickly view if an IRIG output is enabled or disabled, go to the option card's Status Summary panel. For instructions, see: "Viewing the Signal State of an Input or Output" on page 296.

5.4.1.5 IRIG Output: Edit Window

To configure an **IRIG Output**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entries for these option cards are: **IRIG Out BNC, IRIG Out Fiber, IRIG Out RS-485**.

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



IRIG Output 1

IRIG-B121

Signature Control	Output Always Enabled
Format	(B) IRIG B
Modulation	(1) IRIG AM Only
Frequency	(2) 1 KHz
Coded Expression	(1) BCD TOY, Ctrl Func
Control Function Field	Fields conform to RCC 200...
Timescale	UTC
Amplitude	128
Offset	0

The Edit window allows the configuration of the following settings:

- **Signature Control**: Used to control when the IRIG modulation will be present. This function allows the modulation to stop under certain conditions; see also "Signature Control" on page 201.
- **Format**: Used to configure the desired IRIG output formatting. The available choices are:
  - IRIG A
  - IRIG B
  - IRIG G
  - IRIG E
  - NASA-36
- **Modulation**: Changes the type of output signal modulation. The available choices are:
  - IRIG DCLS: TTL-modulated output
  - IRIG AM: Amplitude-modulated output. The amplitude of the output is determined by the value entered in the **Amplitude** field.
- **Frequency**: The IRIG modulation frequency. This is determined by the configuration of Format and Modulation Type. See "IRIG Carrier Frequencies" on page 500 for details.
- **Coded Expression**: Defines the data structure of the IRIG signal, where:
  - BCD = Binary Coded Decimal
  - TOY = Time of Year
  - CF = Control Field
  - SBS = Straight Binary Seconds

> **Note:** The available options will vary according to the values of Format and Modulation Type.

- **Control Function Field**: IRIG signals have an optional section in the data stream that can be used to include additional information (such as the present year, for example). This field allows the Control Field section of the IRIG output to be defined. The available configurations are:
  - Fields conform to **RCC 200-04**: IRIG spec 200-04 specified a location for year value, if included in this field.
  - Fields conform to **IEEC 37.118-2005** (IEEE 1344): Control Field contains year, leap second and daylight savings time information.
  - Fields conform to **Spectracom Format**: Year is included in Control Field but not in the same location as RCC-2004 output (year is offset by one position).
  - Fields conform to **Spectracom FAA Format**: A unique IRIG output Control Field that contains satellite lock status and time error flags.
  - Fields conform to **NASA Formats**: Variants of IRIG B
  - Fields confirm to **Spectracom IEEE C37.118-2005**: Has been extended to support one-month leap second notification

> **Note:** The available options will vary according to the configurations of Format and Modulation Type.

- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International
  - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC)
  - A **local clock** set up through the Time Management Page: This option will appear under the name of the local clock you have set up. See "Setting up a Local Clock" on page 176 for more information. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.
- **Amplitude**: The peak-to-peak output voltage level into a 600 Ω load is adjusted by entering a digital control value in this field. The level adjustment has no effect on TTL outputs, only on AM formats. The value of 128 will cause the Mark amplitude to be about $5V_{p-p}$ into high impedance. A value of 200 results in an output amplitude of about $9V_{p-p}$ into high impedance.

Note: These are nominal values only. Actual values will vary from unit to unit. To adjust the level precisely, connect an oscilloscope to the output connector when adjusting.

- **Offset**: Provides the ability to account for IRIG cable delays or other latencies in the IRIG input. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.

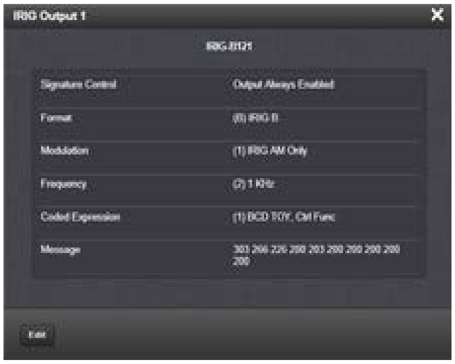
For IRIG frequency and output specifications, see "IRIG Standards and Specifications" on page 500.

5.4.1.6 IRIG Output: Status Window

To view the specifications of an **IRIG Output**, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entries for these option cards are: **IRIG Out BNC, IRIG Out Fiber, IRIG Out RS-485**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



IRIG Output 1

IRIG B121

Signature Control	Output Always Enabled
Format	(0) IRIG B
Modulation	(1) IRIG AM Only
Frequency	(2) 1 KHz
Coded Expression	(1) BCD TOY, Ctrl Func
Message	303 266 226 200 203 200 200 200 200 200

Descriptions of the settings shown in the Status window can be found "IRIG Output: Edit Window" on page 339. For IRIG frequency and output specifications, see "IRIG Standards and Specifications" on page 500.

5.4.2 IRIG In/Out [1204-05, -27]

The IRIG Input/Output option card provides SecureSync with one IRIG input and two IRIG outputs. The IRIG input can be used as the primary SecureSync time and 1PPS reference input for synchronization. Or, it can also be used in conjunction with other primary references (such as GNSS and NTP) to synchronize SecureSync. Available with BNC or Fiber Optic ST connectors.

5.4.2.1 IRIG In/Out, BNC [1204-05]: Input Specifications

- **Input Signal**: IRIG A, B, G or NASA-36;
  amplitude modulated sine wave (AM) OR pulse-width-coded (DCLS); user-selectable, with automatic switching of load on input
- **AM Carrier**: IRIG B 1000 Hz, IRIG A 10 kHz and G 100 kHz
- **AM Signal Level**: 500 mV to 10 V_{p-p} (modulated 2:1 to 6:1); 50 Ω load
- **DCLS Signal Level**: TTL; 0.8V max., 2.3V min fail.; >10 kΩ load
- **Connector**: AM and DCLS: BNC female
- **Accuracy**: n/a
- **Number of Cards**: Up to 6
- **Ordering Information**: 1204-05, IRIG module, BNC Connector

5.4.2.2 IRIG In/Out, BNC [1204-05]: Output Specifications

- **Output Signal**: IRIG A, B, G, E or NASA-36, amplitude modulated sine wave (AM), 0.5V to 6V_{p-p} into 50 Ω; or pulse-width-coded (DCLS). User-selectable.
- **AM Carrier**: IRIG B 1000 Hz, IRIG A and G 100 or 100
- **AM Signal Level**: 500 mV to 10 V_{p-p} [high Z]; (modulated 2:1 to 6:1).
- **DCLS Signal Level**: >10 kΩ TTL
- **Connector**: AM and DCLS: BNC female
- **Accuracy**: see "IRIG Output Accuracy Specifications" on page 513
- **Number of Cards**: Up to 6
- **Ordering Information**: 1204-05, IRIG module, BNC Connector

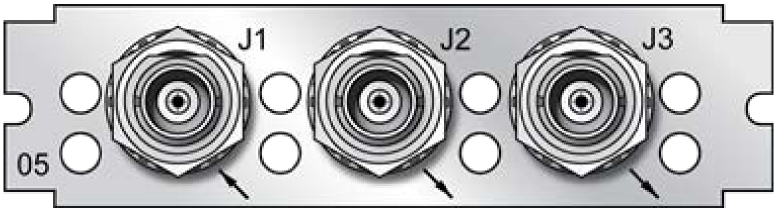


Figure 5-27: Model 1204-05 option card rear plate

5.4.2.3 IRIG In/Out, Fiber Opt. [1204-27]: Input Specifications

- **Signal**: IRIG A, B, G or NASA-36, (DCLS only, unmodulated)
- **Operating Wavelength**: 820/850 nm
- **Optical Minimum Sensitivity**: -25 dBm @ 820 nm

- **Fiber Optic Compatibility**: 50/125 µm, 62.5/125 µm multi-mode cable
- **Optical Connector**: ST
- **Accuracy**: n/a
- **Number of Cards**: Up to 6
- **Ordering Information**: 1204-27, IRIG module, Fiber Optic ST Connector

5.4.2.4 IRIG In/Out, Fiber Opt. [1204-27]: Output Specifications

- **Signal**: IRIG A, B, E, G or NASA-36, (DCLS only, unmodulated)
- **Operating Wavelength**: 820/850 nm
- **Optical Power**: -15 dBm average into 50/125 fiber
- **Fiber Optic Compatibility**: 50/125 µm, 62.5/125 µm multi-mode cable
- **Optical Connector**: ST
- **Accuracy**: see "IRIG Output Accuracy Specifications" on page 513
- **Number of Cards**: Up to 6
- **Ordering Information**: 1204-27, IRIG module, Fiber Optic ST Connector

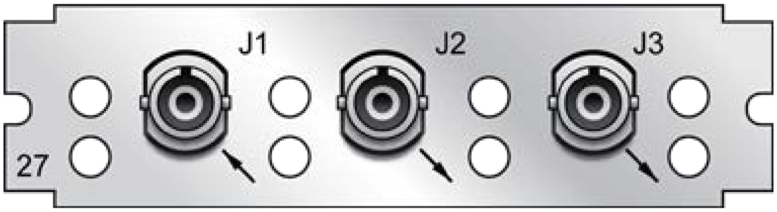


Figure 5-28: Model 1204-27 option card rear plate

5.4.2.5 Supported IRIG Formats

The IRIG option cards models 1204-05 and -27 support IRIG input and output formats A, B, and G (DCLS and AM). Additionally, the cards support inputs with frequency/resolution values of no carrier/index count interval, 1kHz/1ms, 10 kHz/0.1 ms, and 100 kHz/10 ms, as well as IRIG input coded expressions of the fields BCD_{TOY}, CF, SBS, and BCD_{YEAR}.

The IRIG inputs support the following coded expression combinations for BCD_{TOY}, CF, SBS, and BCD_{YEAR} fields:

- 0 - BCD_{TOY}, CF, SBS
- 1 - BCD_{TOY}, CF
- 2 - BCD_{TOY}
- 3 - BCD_{TOY}, SBS
- 4 - BCD_{TOY}, BCD_{YEAR}, CF, SBS
- 5 - BCD_{TOY}, BCD_{YEAR}, CF

The cards support synchronization with the following analog and DCLS IRIG input formats:

Provided IRIG Code Format	Code Description
A-DCLS	
A000	IRIG A, DCLS, BCD, CF, SBS
A001	IRIG A, DCLS, BCD, CF
A002	IRIG A, DCLS, BCD
A003	IRIG A, DCLS, BCD, SBS
A004	IRIG A, DCLS, BCD_{TOY}, BCD_{YEAR}, CF, SBS
A005	IRIG A, DCLS, BCD_{toy}, BCD_{year}, CF
A006	IRIG A, DCLS, BCD_{toy}, BCD_{year}
A007	IRIG A, DCLS, BCD_{toy}, BCD_{year}, SBS
A-AM	
A130	IRIG A, AM, 10kHz, BCD, CF, SBS
A131	IRIG A, AM, 10kHz, BCD, CF
A132	IRIG A, AM, 10kHz, BCD
A133	IRIG A, AM, 10kHz, BCD, SBS
A134	IRIG A, AM, 10kHz, BCD_{TOY}, BCD_{YEAR}, CF, SBS
A135	IRIG A, AM, 10kHz, BCD_{toy}, BCD_{year}, CF
A136	IRIG A, AM, 10kHz, BCD_{toy}, BCD_{year}
A137	IRIG A, AM, 10kHz, BCD_{toy}, BCD_{year}, SBS
B-DCLS	
B000	IRIG B, DCLS, BCD, CF, SBS
B001	IRIG B, DCLS, BCD, CF
B002	IRIG B, DCLS, BCD
B003	IRIG B, DCLS, BCD, SBS
B004	IRIG B, DCLS, BCD_{TOY}, BCD_{YEAR}, CF, SBS
B-AM	
B120	IRIG B, AM, BCD, CF, SBS
B121	IRIG B, AM, BCD, CF
B122	IRIG B, AM, BCD
B123	IRIG B, AM, BCD, SBS

Provided IRIG Code Format	Code Description
B124	IRIG B, AM, BCD_{TOY}, BCD_{YEAR}, CF, SBS
B125	IRIG B, AM, 1kHz, BCD_{toy}, BCD_{year}, CF
B126	IRIG B, AM, 1kHz, BCD_{toy}, BCD_{year}
B127	IRIG B, AM, 1kHz, BCD_{toy}, BCD_{year}, SBS
G-DCLS	
G001	IRIG G, DCLS, BCD, CF
G002	IRIG G, DCLS, BCD
G005	IRIG G, DCLS, BCD_{TOY}, BCD_{YEAR}, CF
G006	IRIG G, DCLS, BCD_{toy}, BCD_{year}
G-AM	
G141	IRIG G, AM, 100kHz, BCD,CF
G142	IRIG G, AM, 100kHz, BCD
G145	IRIG G, AM, 100kHz, BCD_{TOY}, BCD_{YEAR}, CF
G146	IRIG G, AM, 100kHz, BCD_{toy}, BCD_{year}

Table 5-15: Accepted IRIG input reference formats

5.4.2.6 IRIG Output: Signal State

To quickly view if an **IRIG output** is enabled, or disabled, navigate to the option card's Status Summary panel. For instructions, see: "Viewing the Signal State of an Input or Output" on page 296.

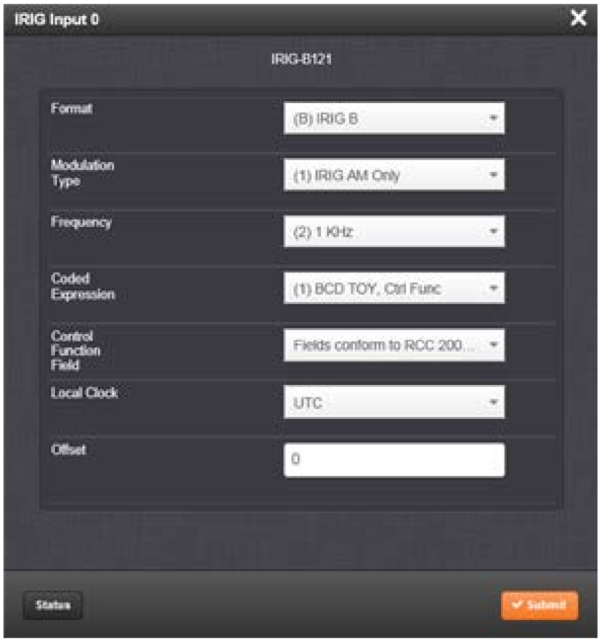
5.4.2.7 IRIG Input: Edit Window

To configure the IRIG Input (also referred to as 'Reference'), navigate to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entries for these cards are: **IRIG In/Out BNC** and **IRIG In/Out Fiber**.

The connector number is: J1.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Format: (B) IRIG B

Modulation Type: (1) IRIG AM Only

Frequency: (2) 1 KHz

Coded Expression: (1) BCD TOY, Ctrl Func

Control Function Field: Fields conform to RCC 200...

Local Clock: UTC

Offset: 0

The Edit window allows the configuration of the following settings:

- **Format**: Sets the formatting of the IRIG input signal, as defined by the IRIG generator time source. The available choices are:
  - IRIG A
  - IRIG B
  - IRIG G
  - NASA-36
- **Modulation Type**: Configures the type of input signal modulation. The choices are:
  - IRIG DCLS–A TTL (Phase) modulated signal.
  - IRIG AM–An amplitude modulated signal.
- **Frequency**: The IRIG modulation frequency. This is determined by the configuration of Format and Modulation Type. See "IRIG Carrier Frequencies" on page 500 for details.
- **Coded Expression**–Defines the data structure of the IRIG signal, where:
  - BCD = Binary Coded Decimal
  - TOY = Time of Year
  - CF = Control Field
  - SBS = Straight Binary Seconds
  - The available options will vary according to the configurations of Format and Modulation Type.
- **Control Function Field**: IRIG signals have an optional section in the data stream that can be used to include additional information (such as the present year, for example). This field

allows the Control Field section of the IRIG output to be defined. The available configurations are:

- Fields conform to **RCC 200-04**: IRIG spec 200-04 specified a location for year value, if included in this field.
- Fields conform to **IEEC 37.118-2005** (IEEE 1344): Control Field contains year, leap second and daylight savings time information.
- Fields conform to **Spectracom Format**: Year is included in Control Field but not in the same location as RCC-2004 output (year is offset by one position).
- Fields conform to **Spectracom FAA Format**: A unique IRIG output Control Field that contains satellite lock status and time error flags.
- Fields conform to **NASA Formats**: Variants of IRIG B
- Fields confirm to **Spectracom IEEE C37.118-2005**: Has been extended to support one-month leap second notification

The available options will vary according to the configurations of Format and Modulation Type.

Note: If the Format value is changed, the Control Field and Coded Expression change to the default values for the given Format value. The user can only change the Control Field field and Coded Expression field to allowed values for the Format field.

It is recommended that the SecureSync administrator/operator only use this if they do not know what the IRIG Input Format is, and they wish to identify the signal type, or to determine if a signal is present.

- **Local Clock**: The incoming IRIG input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display.
- **Offset**: Provides the ability to account for IRIG cable delays or other latencies in the IRIG input. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.

5.4.2.8 Configuring the IRIG Input Year

The IRIG time source may be able to provide SecureSync with the current year information via the IRIG input data stream. As the year value is not a required field in the IRIG data stream, (and if the year value is present, it may not always be in the same location of the Control Field), if the year value is contained in the control field section of the IRIG data stream, the control field “layout” needs to be defined in SecureSync (as determined by the Coded Expressions and Control Field values). If the year value is not present in the IRIG input signal, the year value will need to be manually set in SecureSync when using IRIG input as the only input Time reference.

Note: By default, the "year" fields in the IRIG message are ignored and a user-defined value is used.

Note: By default, the "year" fields in the IRIG message are ignored and a user-defined value is used. Make sure the year is set correctly when the SecureSync is installed. If the year is not set correctly before NTP achieves time synchronization, it will use the value entered. The unit will also default to the year entered if it is powered down during the rollover of the year. If the SecureSync was not switched on during the rollover, this value must be updated.

Note: When the IRIG Input year is updated, NTP must be restarted from the Web UI NTP page (or the SecureSync unit rebooted) for the New Year value to take effect.

The current year value can be manually entered from the MANAGEMENT/OTHER/Time Management page. The year value only needs to be manually entered once, as it will automatically increment to the next year each New Year's day. See "Editing the System Time" on page 171 for instructions on manually setting the current year.

5.4.2.9 Verifying IRIG Input Signal Validity

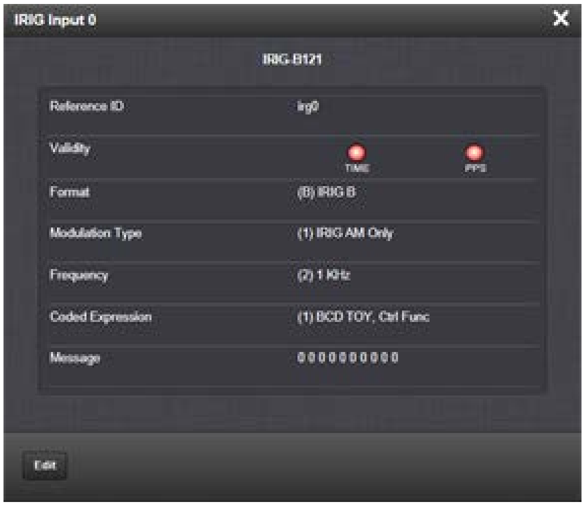
See: "Verifying the Validity of an Input Signal" on page 297.

5.4.2.10 IRIG Input: Status Window

To view the current settings of the **IRIG Input** (also referred to as 'Reference'), go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entries for these cards are: **IRIG In/Out BNC** and **IRIG In/Out Fiber**. The connector number is: J1.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



IRIG-B121

Reference ID	irg0
Validity	● TIME ● PPS
Format	(B) IRIG B
Modulation Type	(1) IRIG AM Only
Frequency	(2) 1 KHz
Coded Expression	(1) BCD TOY, Ctrl Func
Message	0000000000

The Status window displays the following settings:

- **Reference ID**: If you have only one IRIG card installed, SecureSync will number that card 0 and it will be identified as irg0. Additional cards will be numbered irg1 or above.
- **Validity**: If the IRIG input is not present, or is not considered valid and qualified, the "1PPS Validity" and "Time Validity" fields will be considered "Not Valid" (Orange).

- Once the IRIG input has been supplied and the signal is considered valid and qualified, the two indicators will then turn "Valid" (Green).
- **Format**: Identifies the formatting of the IRIG input signal, as defined by the IRIG generator time source. The possible values are:
  - IRIG A
  - IRIG B
  - IRIG G
  - NASA-36
- **Modulation Type**: Identifies the type of input signal modulation. The possible values are:
  - IRIG DCLS–A TTL (Phase) modulated signal.
  - IRIG AM–An amplitude modulated signal.
  - Frequency–The IRIG modulation frequency. This is determined by the configuration of Format and Modulation Type. See also: "IRIG Carrier Frequencies" on page 500.
- **Coded Expression**: Defines the data structure of the IRIG signal, where:
  - BCD = Binary Coded Decimal
  - TOY = Time of Year

  - CF = Control Field
  - SBS = Straight Binary Seconds
- **Message**: The IRIG message.

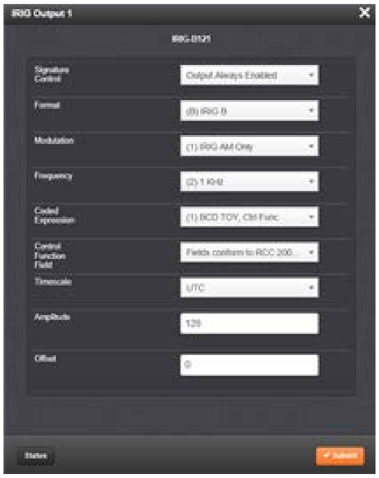
5.4.2.11 IRIG Output: Edit Window

To configure the settings of one of the two **IRIG Outputs**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entries for these cards are: **IRIG In/Out BNC** and **IRIG In/Out Fiber**.

The connector numbers are: J2 and J3.

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



IRIG Output 1

IRIG-B121

Signature Control	Output Always Enabled
Format	(B) IRIG B
Modulation	(1) IRIG AM Only
Frequency	(2) 1 KHz
Coded Expression	(1) BCD TOY, Ctrl Func
Control Function Field	Fields conform to RCC 200...
Timescale	UTC
Amplitude	128
Offset	0

The Edit window allows the configuration of the following settings:

- **Signature Control**: Is used to control when the IRIG modulation will be present. This function allows the modulation to stop under certain conditions; see also "Signature Control" on page 201.
- **Format**: Used to configure the desired IRIG output formatting. The available choices are:
  - IRIG A
  - IRIG B
  - IRIG G
  - IRIG E
  - NASA-36

- **Modulation**: Changes the type of output signal modulation. The available choices are:
  - IRIG DCLS–A TTL-modulated output.
  - IRIG AM–An amplitude modulated output. The amplitude of the output is determined by the value entered in the Amplitude field.
  - Frequency–The IRIG modulation frequency. This is determined by the configuration of Format and Modulation Type. See also "IRIG Carrier Frequencies" on page 500.
- **Coded Expression**: Defines the data structure of the IRIG signal, where:
  - BCD = Binary Coded Decimal
  - TOY = Time of Year
  - CF = Control Field
  - SBS = Straight Binary Seconds
  - The available options will vary according to the values of Format and Modulation Type.
- **Control Function Field**: IRIG signals have an optional section in the data stream that can be used to include additional information (such as the present year, for example). This field allows the Control Field section of the IRIG output to be defined. The available configurations are:
  - Fields conform to **RCC 200-04**: IRIG spec 200-04 specified a location for year value, if included in this field.
  - Fields conform to **IEEC 37.118-2005** (IEEE 1344): Control Field contains year, leap second and daylight savings time information.
  - Fields conform to **Spectracom Format**: Year is included in Control Field but not in the same location as RCC-2004 output (year is offset by one position).
  - Fields conform to **Spectracom FAA Format**: A unique IRIG output Control Field that contains satellite lock status and time error flags.
  - Fields conform to **NASA Formats**: Variants of IRIG B
  - Fields confirm to **Spectracom IEEE C37.118-2005**: Has been extended to support one-month leap second notification

  The available options will vary according to the configurations of Format and Modulation Type.
- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**–Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**–Temps Atomique International

  - **GPS**–The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC time).
  - A **local clock** set up through the Time Management Page–This option will appear under the name of the local clock you have set up. See "Editing the System Time" on page 171 for more information. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.
- **Amplitude**: The peak-to-peak output voltage level into a 600 Ω load is adjusted by entering a digital control value in this field. The level adjustment has no effect on TTL outputs, only on AM formats. The value of 128 will cause the Mark amplitude to be about 5V_{p-p} into high impedance. A value of 200 results in an output amplitude of about 9V_{p-p} into high impedance.

> **Note:** These are nominal values only. Actual values will vary from unit to unit. To adjust the level precisely, connect an oscilloscope to the output connector when adjusting.

- **Offset**: Provides the ability to account for IRIG cable delays or other latencies in the IRIG input. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.

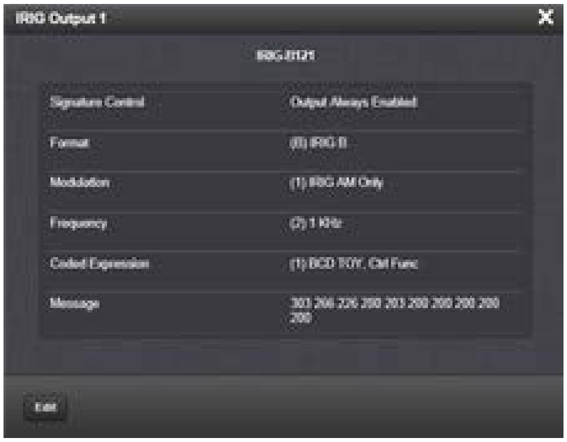
For IRIG frequency and output specifications, see "IRIG Standards and Specifications" on page 500.

5.4.2.12 IRIG Output: Status Window

To view the current settings of one of the **IRIG Outputs**, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entries for these cards are: **IRIG In/Out BNC** and **IRIG In/Out Fiber**. The connector numbers are: J2 and J3.

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



IRIG Output 1

IRIG B121

Signature Control	Output Always Enabled
Format	(B) IRIG B
Modulation	(1) IRIG AM Only
Frequency	(2) 1 KHz
Coded Expression	(1) BCD TOY, Ctrl Func
Message	303 266 226 200 203 200 200 200 200 200

The Status window displays the following settings:

- **Signature Control**: is used to control when the IRIG modulation will be present. This function allows the modulation to stop under certain conditions; see also "Signature Control" on page 201.
- **Format**: Used to configure the desired IRIG output formatting. The possible values are:
  - IRIG A
  - IRIG B
  - IRIG G
  - IRIG E
  - NASA-36
- **Modulation**: Changes the type of output signal modulation. The possible values are:
  - IRIG DCLS–A TTL-modulated output.
  - IRIG AM–An amplitude modulated output. The amplitude of the output is determined by the value entered in the Amplitude field.
  - Frequency–The IRIG modulation frequency. This is determined by the configuration of Format and Modulation Type. See also: "IRIG Carrier Frequencies" on page 500.
- **Coded Expression**: Defines the data structure of the IRIG signal, where:
  - BCD = Binary Coded Decimal
  - TOY = Time of Year
  - CF = Control Field
  - SBS = Straight Binary Seconds
  - The possible values will vary according to the values of Format and Modulation Type
- **Message**: The IRIG message of the output.

For IRIG frequency and output specifications, see "IRIG Standards and Specifications" on page 500.

5.4.3 STANAG Out [1204-11, -25]

The STANAG Output option card models 1204-11 and 1204-25 provide (2) configurable STANAG outputs and (1) 1PPS output for the SecureSync platform.

5.4.3.1 STANAG Out [1204-11, -25]: Specifications

- **Outputs**: (2) STANAG Outputs, (1) 1PPS Output
- **Signal Type and Connector**: 5V or 10 V or RS-485 level (user selectable) for STANAG and 1PPS output. DB-25 connector.
- **Formats Supported**:
  - STANAG 4246 HAVE QUICK I
  - STANAG 4246 HAVE QUICK II
  - STANAG 4372 HAVE QUICK IIA
  - STANAG 4430 Extended HAVE QUICK
  - STANAG 4430 Standard Time Message (STM)
  - ICD-GPS-060A BCD Time Code
  - ICD-GPS-060A HAVE QUICK
  - DOD-STD-1399 BCD Time Code
- **Programmable Pulse Width** (1PPS Output): 100 ns to 500 ms with 20 ns resolution
- **Accuracy**: ±50 ns (1σ)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-11 (for non-isolated board); 1204-25 (for isolated board)

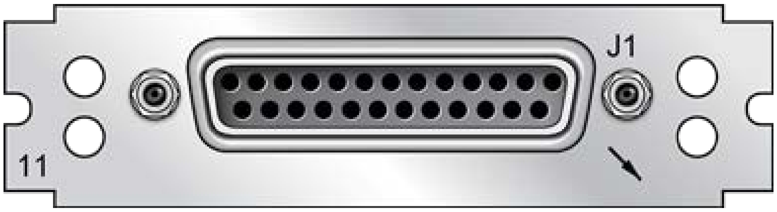


Figure 5-29: Model 1204-11 option card rear plate

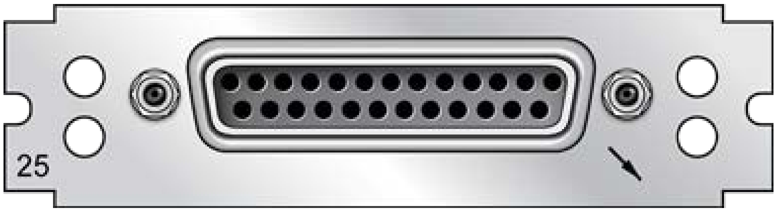


Figure 5-30: Model 1204-25 option card rear plate

Pin Assignments

Pin No.	Signal	Function	Pin No.	Signal	Function
1	GND	Ground	14	TOD1-	TOD1 RS-485- Out
2	TOD1+	TOD1 RS-485+ Out	15	NC	-
3	NC	-	16	NC	-
4	TOD2+	TOD2 RS-485+ Out	17	TOD2-	TOD2 RS-485- Out
5	NC	-	18	NC	-
6	GND	Ground	19	NC	5 MHz Out (1204-11 Only)
7	GND	Ground	20	NC	-
8	NC	-	21	1PPS-	1PPS RS-485- Out
9	1PPS+	1PPS RS-485+ Out	22	NC	-
10	TFD	Time Fault Discrete	23	GND	Ground
11	TOD1	TOD1 TTL Out	24	1PPS	1PPS TTL Out
12	GND	Ground	25	GND	Ground
13	TOD2	TOD2 TTL Out			

Table 5-16: Models 1204-11, -25: DB-25 pin-out

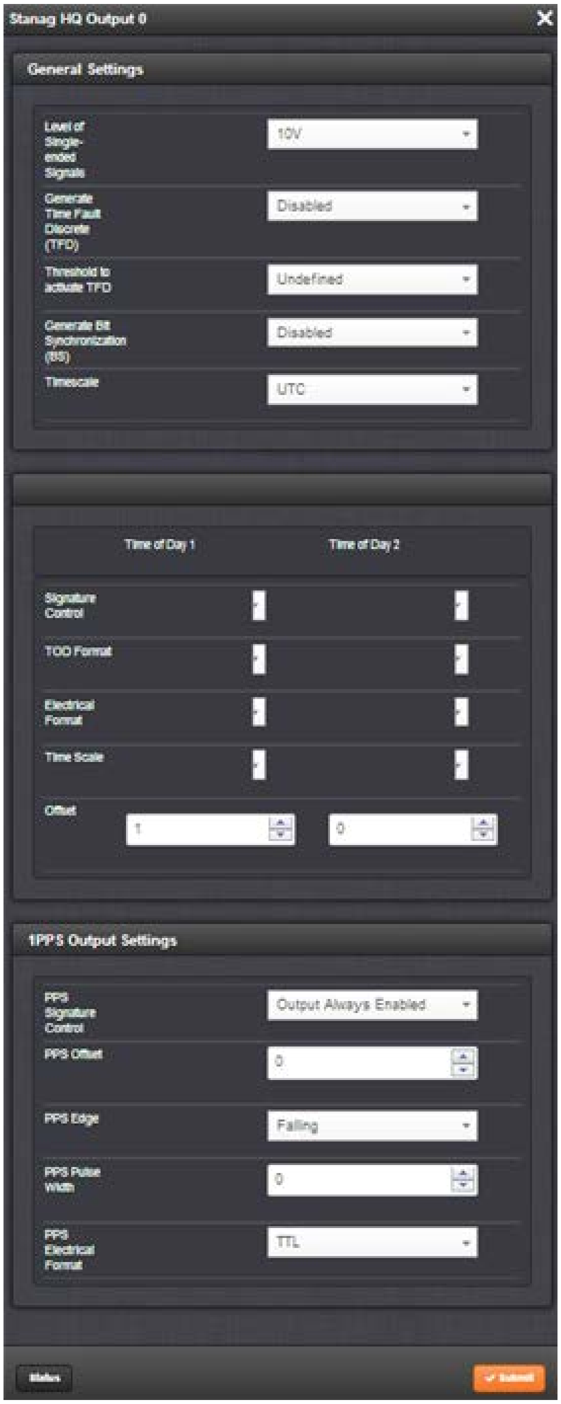
5.4.3.2 STANAG Output: Edit Window

To configure a **STANAG output**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entries for these cards are: **STANAG Out** and **STANAG Out, Isolated**.

The outputs are named: **Stanag HQ Output [number]**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



General Settings

Level of Single-ended Signals	10V
Generate Time Fault Discrete (TFD)	Disabled
Threshold to actuate TFD	Undefined
Generate Bit Synchronization (BS)	Disabled
Timescale	UTC

	Time of Day 1	Time of Day 2
Signature Control		
TOD Format		
Electrical Format		
Time Scale		
Offset	1	0

1PPS Output Settings

PPS Signature Control	Output Always Enabled
PPS Offset	0
PPS Edge	Falling
PPS Pulse Width	0
PPS Electrical Format	TTL

The Edit window allows the configuration of the following settings:

Under **General Settings**:

- **Level of Single-ended Signals**: 10 V or 5V can be selected for the TOD 1 and 1PPS Output.

- **Generate Time Fault Discrete (TFD)**:
  - Enabled: The TFD signal uses the “Threshold to activate” value to provide the level of TFD.
  - Disabled: The TFD signal is always valid.
- **Threshold to activate TFD**: If the TFD is activated, the user can select the TFOM value threshold. Below this value, the TFD is high, otherwise the TFD is low.
- **Generate Bit Synchronization (BS)**:
  - **Enabled**: The second STANAG signal (TOD 2) is used to send the BS (Bit Stream) signal used with STANAG 4430-STM. When BS is active, the configuration of TOD 2 is superseded and only used for BS.
  - **Disabled**: The second STANAG signal (TOD 2) can be used to send an independent TOD.
- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**—Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**—Temps Atomique International
  - **GPS**—The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC time)
  - A **local clock** set up through the Time Management Page—Refer to "The Time Management Screen" on page 169 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the **Timescale** field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to "Setting up a Local Clock" on page 176 for more information on Local Clocks.

Configurable settings for each **Time of Day** are:

- **Signature Control**: Used to control when the signal will be present. This function allows the modulation to stop under certain conditions, see also "Signature Control" on page 201.
- **TOD Format**: The user-selectable format to be used. Available formats include:
  - STANAG 4246 HQI
  - STANAG 4246 HQII
  - STANAG 4372 HQIIA
  - STANAG 4430 STM
  - STANAG 4430 XHQ

  - ICD-GPS-060A BCD
  - ICD-GPS-060A HQ
  - DOD-STD-1399 BCD
- **Electrical Format**: Selects signaling on either RS-485 or TTL (supporting up to 10 V levels) signal lines.
- **Time Scale**: Used to set the desired time scale (UTC, TAI, GPS, or Local). See above.
- **Offset (ns)**: Provides the ability to account for STANAG Line (TOD1 and TOD2 independently) cable delays or other latencies in the STANAG output. Available Offset range is -500 to +500 ms in 5ns steps.

Configurable settings under **1PPS Output** are:

- **PPS Signature Control**: Used to control when the signal will be present. This function allows the modulation to stop under certain conditions, see also "Signature Control" on page 201.
- **PPS Offset (ns)**: Used to account for 1PPS cable delays or other latencies in the 1PPS output. Available Offset range is -500 to +500 ms in 5ns steps.
- **PPS Edge**: The operator can select if the output signal is a rising or falling edge pulse.
- **PPS Pulse Width**: Configures the Pulse Width of the 1PPS output. The Pulse Width is entered and displayed in nanoseconds (the default Pulse Width is 200 ms).
- **PPS Electrical Format**: Selects signaling on either RS-485 or TTL (supporting up to 10 V levels) signal lines.

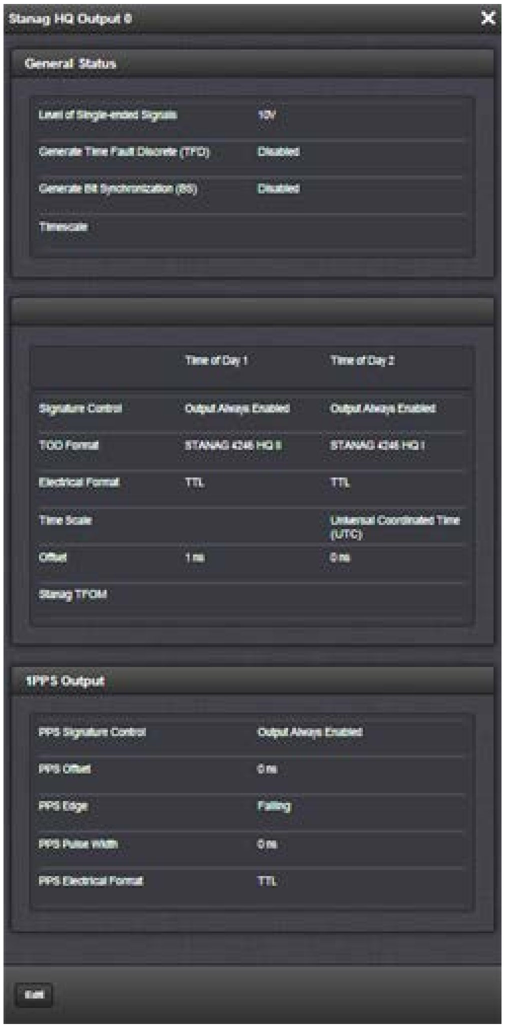
5.4.3.3 STANAG Output: Status Window

To view the current settings of a **STANAG Output**, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entries for these cards are: **STANAG Out** and **STANAG Out, Isolated**.

The outputs are named: **Stanag HQ Output [number]**.

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Stanag HQ Output 0

General Status

Level of Single-ended Signals	10V
Generate Time Fault Discrete (TFD)	Disabled
Generate Bit Synchronization (BS)	Disabled
Timescale	

	Time of Day 1	Time of Day 2
Signature Control	Output Always Enabled	Output Always Enabled
TOD Format	STANAG 4246 HQ II	STANAG 4246 HQ I
Electrical Format	TTL	TTL
Time Scale		Universal Coordinated Time (UTC)
Offset	1 ns	0 ns
Stanag TFOM		

1PPS Output

PPS Signature Control	Output Always Enabled
PPS Offset	0 ns
PPS Edge	Falling
PPS Pulse Width	0 ns
PPS Electrical Format	TTL

The Status window displays the following settings:

Under **General Status**:

- **Level of Single-ended Signals**: 10 V or 5V will be indicated for the TOD 1 and 1PPS Output.
- **Generate Time Fault Discrete (TFD)**:
  - **Enabled**: The TFD signal uses the "Threshold to activate" value to provide the level of TFD.
  - **Disabled**: The TFD signal is always valid.
- **Threshold to activate TFD**: If the TFD is activated, indicates the TFOM value threshold. Below this value, the TFD is high, otherwise the TFD is low.
- **Generate Bit Synchronization (BS)**:
  - **Enabled**: The second STANAG signal (TOD 2) is used to send the BS (Bit Stream) signal used with STANAG 4430-STM. When BS is active, the configuration of TOD

2 is superseded and only used for BS.

  - **Disabled**: The second STANAG signal (TOD 2) can be used to send an independent TOD.

- **Timescale**: Indicates the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**–Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**–Temps Atomique International
  - **GPS**–The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC time).
  - A **local clock** set up through the Time Management Page–Refer to "The Time Management Screen" on page 169 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to "Setting up a Local Clock" on page 176 for more information on Local Clocks.

For each **Time of Day** the following settings are displayed:

- **Signature Control**: Indicates when the signal is present. This function allows the modulation to stop under certain conditions, see "Signature Control" on page 201.
- **TOD Format**: The user-selectable format being used. Available formats include:
  - STANAG 4246 HQI
  - STANAG 4246 HQII
  - STANAG 4372 HQIIA
  - STANAG 4430 STM
  - STANAG 4430 XHQ
  - ICD-GPS-060A BCD
  - ICD-GPS-060A HQ
  - DOD-STD-1399 BCD
- **Electrical Format**: Selects signaling on either RS-485 or TTL (supporting up to 10 V levels) signal lines.
- **Time Scale**: Used to set the desired time scale (UTC, TAI, GPS, or Local). See above.
- **Offset (ns)**: Provides the ability to account for STANAG Line (TOD1 and TOD2 independently) cable delays or other latencies in the STANAG output. Available Offset range is

-500 to +500 ms in 5ns steps.

- **STANAG TFOM**: The Time Figure of Merit for the output.

Under **1PPS Output**, the following settings are displayed:

- **PPS Signature Control**: Indicates whether the signal will be present. This function allows the modulation to stop under certain conditions, see "Signature Control" on page 201.
- **PPS Offset (ns)**: Used to account for 1PPS cable delays or other latencies in the 1PPS output. Available Offset range is -500 to +500 ms in 5ns steps.
- **PPS Edge**: Indicates whether the output signal is a rising or falling edge pulse.
- **PPS Pulse Width**: Indicates the Pulse Width of the 1PPS output. The Pulse Width is entered and displayed in nanoseconds (the default Pulse Width is 200 ms).
- **PPS Electrical Format**: Indicates signaling on either RS-485 or TTL (supporting up to 10 V levels) signal lines.

5.4.4 STANAG In [1204-1D, -24]

The STANAG Input option cards 1204-1D and 1204-24 STANAG provide (2) configurable STANAG inputs and (1) 1PPS input for the SecureSync platform.

5.4.4.1 STANAG In [1204-1D, -24]: Specifications

- **Inputs**: (2) STANAG Inputs, (1) 1PPS Input
- **Signal Type and Connector**: TTL or RS-485 level (user selectable) for STANAG and 1PPS input. DB25.
- **Formats Supported**:
  - STANAG 4246 HAVE QUICK I
  - STANAG 4246 HAVE QUICK II
  - STANAG 4372 HAVE QUICK IIA
  - STANAG 4430 Extended HAVE QUICK
  - STANAG 4430 Standard Time Message (STM)
  - ICD-GPS-060A BCD Time Code
  - ICD-GPS-060A HAVE QUICK
  - DOD-STD-1399 BCD Time Code
- **Accuracy**: 100 ns
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-1D (for non-isolated board); 1204-24 (for isolated board)

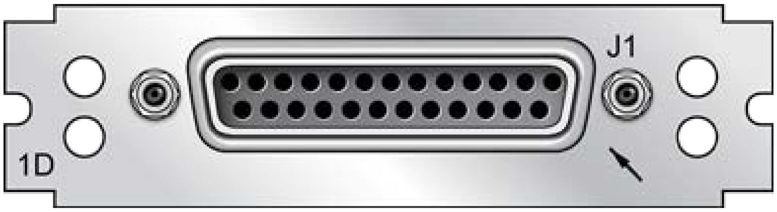


Figure 5-31: Model 1204-1D option card rear plate

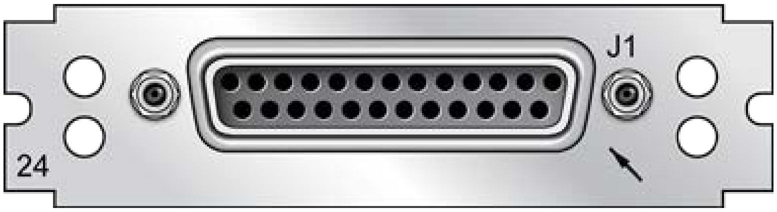


Figure 5-32: Model 1204-24 option card rear plate

Pin Assignments

Pin No.	Signal	Function	Pin No.	Signal	Function
1	GND	Ground	14	TOD1-	TOD1 RS-485- Input
2	TOD1+	TOD1 RS-485+ Input	15	NC	-
3	NC	-	16	NC	-
4	TOD2+	TOD2 RS-485+ Input	17	TOD2-	TOD2 RS-485- Input
5	NC	-	18	NC	-
6	GND	Ground	19	NC	-
7	GND	Ground	20	NC	-
8	NC	-	21	1PPS-	1PPS RS-485- Input
9	1PPS+	1PPS RS-485+ Input	22	NC	-
10	TFD	Time Fault Discrete	23	GND	Ground
11	TOD1	TOD1 TTL Input	24	1PPS	1PPS TTL Input
12	GND	Ground	25	GND	Ground
13	TOD2	TOD2 TTL Input			

Table 5-17: 1204-1D, 1204-24 option cards: DB-25 pin-outs

5.4.4.2 STANAG Input: Edit Window

To configure a **STANAG Input** (also referred to as 'Reference'), go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

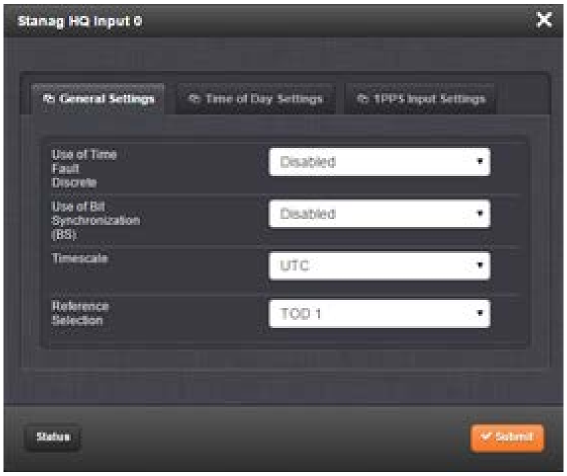
The Web UI list entries for this card are: **STANAG In** and **STANAG In, Isolated**.

The inputs are named: **Stanag HQ Input [number]**.

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).

The configurable settings are grouped under the following three tabs:

General Settings tab



Use of Time Fault Discrete	Disabled
Use of Bit Synchronization (BS)	Disabled
Timescale	UTC
Reference Selection	TOD 1

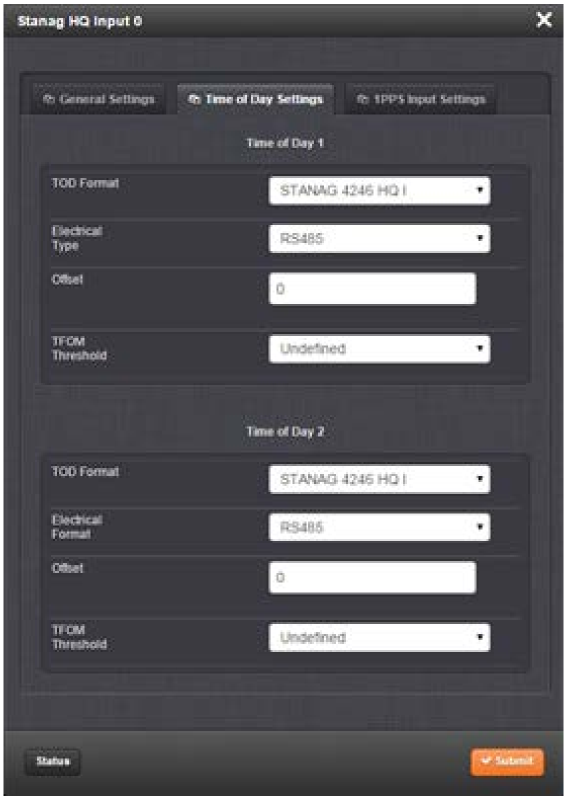
- **Use of Time Fault Discrete**: There are two options:
  - **Enabled**: The TFD input signal is used to validate the STANAG input.
  - **Disabled** (default): The TFD input signal is ignored.
- **Use of Bit Synchronization (BS)**: There are two options:
  - **Enabled**: The second STANAG input (TOD 2) is used to receive the BS (Bit Stream) signal used with STANAG 4430-STM. When BS is active, the configuration of TOD2 is superseded and only used for BS.
  - **Disabled**: The second STANAG input (TOD 2) can be used to receive an independent TOD.
- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International
  - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC time).

- A **local clock** set up through the Time Management Page: Refer to "The Time Management Screen" on page 169 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

  The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to "Setting up a Local Clock" on page 176 for more information on Local Clocks.

- **Reference Selection**: Selects TOD 1 or TOD 2 (configured below) which TOD signal is used for synchronization.

Time of Day Settings tab



Time of Day 1

TOD Format: STANAG 4246 HQ I

Electrical Type: RS485

Offset: 0

TFOM Threshold: Undefined

Time of Day 2

TOD Format: STANAG 4246 HQ I

Electrical Format: RS485

Offset: 0

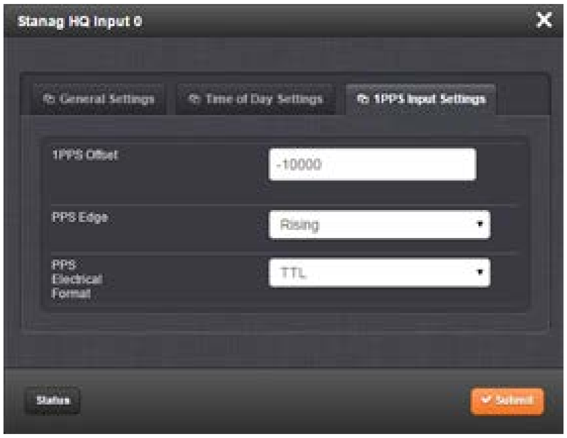
TFOM Threshold: Undefined

For **Time of Day 1** and **Time of Day 2(** (STANAG content supports two ToD streams).

- **ToD Format**: The user-selectable format to be used. Available formats include:
  - STANAG 4246 HAVE QUICK I
  - STANAG 4246 HAVE QUICK II
  - STANAG 4372 HAVE QUICK IIA

   - STANAG 4430 Extended HAVE QUICK
   - STANAG 4430 Standard Time Message (STM)
   - ICD-GPS-060A BCD Time Code
   - ICD-GPS-060A HAVE QUICK
   - DOD-STD-1399 BCD Time Code
- **Electrical Type**: Selects synchronization to either RS-485 or TTL (supporting up to 10 V levels) signal lines.
- **Offset**: Provides the ability to account for STANAG Line (TOD1 and TOD2 independently) cable delays or other latencies in the STANAG input. Available Offset range is -500 to +500 ms in 5ns steps.
- **TFOM Threshold**: Under STANAG protocol, the TFOM (Time Figure of Merit) threshold value can be utilized as a means to validate timing data based on the TFOM. For more information on TFOM, see under "Oscillator Disciplining Setup" on page 192.

1PPS Input Settings tab



1PPS Offset: -10000

PPS Edge: Rising

PPS Electrical Format: TTL

- **1PPS Offset**: Used to account for 1PPS cable delays or other latencies in the 1PPS input. Available Offset range is -500 to +500 ms in 5ns steps
- **PPS Edge**: The operator can select if the output signal is a rising or falling edge pulse.
- **PPS Electrical Format**: Selects synchronization to either RS-485 or TTL (supporting up to 10 V levels) signal lines.

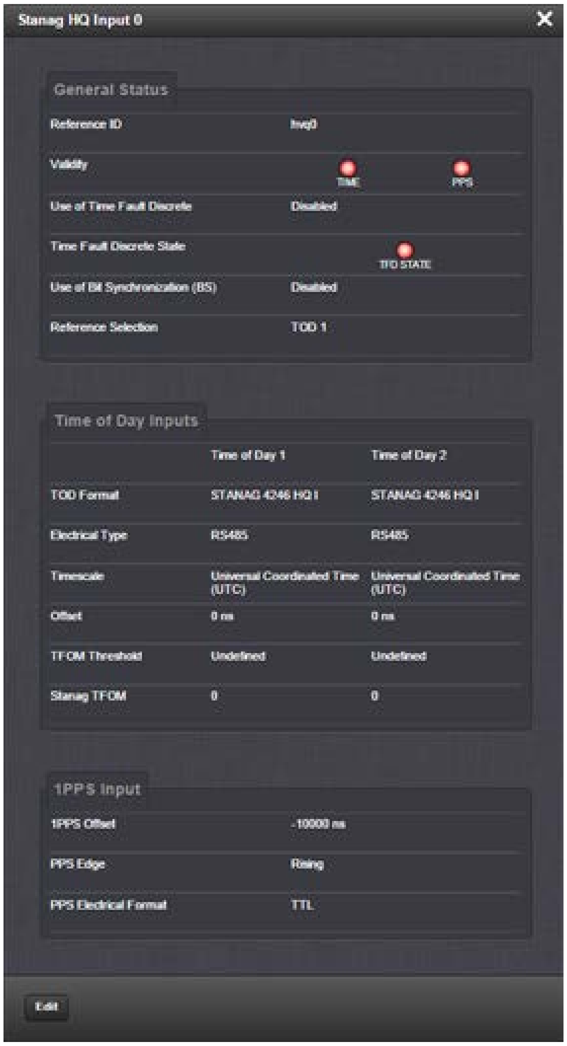
5.4.4.3 STANAG Input: Status Window

To view the current settings of a **STANAG Input** (also referred to as 'Reference'), go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entries for this card are: **STANAG In** and **STANAG In, Isolated**.

The inputs are named: **Stanag HQ Input [number]**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).


Stanag HQ Input 0

General Status

Reference ID	hvq0	
Validity	● TIME	● PPS
Use of Time Fault Discrete	Disabled	
Time Fault Discrete State	● TFD STATE	
Use of Bit Synchronization (BS)	Disabled	
Reference Selection	TOD 1	

Time of Day Inputs

	Time of Day 1	Time of Day 2
TOD Format	STANAG 4246 HQ I	STANAG 4246 HQ I
Electrical Type	RS485	RS485
Timescale	Universal Coordinated Time (UTC)	Universal Coordinated Time (UTC)
Offset	0 ns	0 ns
TFOM Threshold	Undefined	Undefined
Stanag TFOM	0	0

1PPS Input

1PPS Offset	-10000 ns
PPS Edge	Rising
PPS Electrical Format	TTL

The Status window displays the following settings:

Under General Status:

- **Reference ID**: This is the identifier given to the input by SecureSync.
- **Validity**: Indicates the validity of the Time input and the PPS input. If the input signal is valid the indicator will be green. If the signal is not valid, the indicator will be orange.

- **Use of Time Fault Discrete**: There are two options:
  - **Enabled**: The TFD input signal is used to validate the STANAG input.
  - **Disabled** (default): The TFD input signal is ignored.
- **Time Fault Discrete State**: If this is valid, the indicator will be green. If it is not valid, the indicator will be orange.
- **Use of Bit Synchronization (BS)**: There are two options:
  - **Enabled**: The second STANAG input (TOD 2) is used to receive the BS (Bit Stream) signal used with STANAG 4430-STM. When BS is active, the configuration of TOD2 is superseded and only used for BS.
  - **Disabled**: The second STANAG input (TOD 2) can be used to receive an independent TOD.
- **Reference Selection**: Indicates which TOD signal is used for synchronization. This will be either TOD 1 or TOD 2.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to "Setting up a Local Clock" on page 176 for more information on Local Clocks.

Under **Time of Day Inputs**:

- **TOD Format**: The user-selectable format being used. Available formats include:
  - STANAG 4246 HAVE QUICK I
  - STANAG 4246 HAVE QUICK II
  - STANAG 4372 HAVE QUICK IIA
  - STANAG 4430 Extended HAVE QUICK
  - STANAG 4430 Standard Time Message (STM)
  - ICD-GPS-060A BCD Time Code
  - ICD-GPS-060A HAVE QUICK
  - DOD-STD-1399 BCD Time Code
- **Electrical Type**: Either RS-485 or TTL (supporting up to 10 V levels) signal lines.
- **Time Scale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time

    TAI: Temps Atomique International

GPS: The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC time).

A **local clock** set up through the Time Management Page: Refer to "The Time Management Screen" on page 169 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

- **Offset**: Provides the ability to account for STANAG Line (TOD1 and TOD2 independently) cable delays or other latencies in the STANAG input. Available Offset range is -500 to +500 ms in 5ns steps.
- **Stanag TFOM**: The Time Figure of Merit for the input.

Under **1PPS Input**:

- **1PPS Offset**: Used to account for 1PPS cable delays or other latencies in the 1PPS input. The available Offset range is -500 to +500 ms in 5ns steps.
- **PPS Edge**: Indicates whether the output signal is a rising or falling edge pulse.
- **PPS Electrical Format**: Indicates whether the signal is synchronized to RS-485 or TTL (supporting up to 10 V levels) signal lines.

5.4.5 HAVE QUICK Out [1204-10, -1B]

The HAVE QUICK option cards provide (4) HAVE QUICK outputs for the SecureSync platform.

5.4.5.1 HAVE QUICK Out, BNC [1204-10]: Specifications

- **Outputs**: (4) HAVE QUICK
- **Signal Type and Connector**: TTL levels (BNC)
- **Formats Supported**:
  - STANAG 4246 HAVE QUICK I
  - STANAG 4246 HAVE QUICK II
  - STANAG 4372 HAVE QUICK IIA
  - STANAG 4430 Extended HAVE QUICK
  - STANAG 4430 Standard Time Message (STM)
  - ICD-GPS-060A BCD Time Code
  - ICD-GPS-060A HAVE QUICK
  - DOD-STD-1399 BCD Time Code
- **Output Load Impedance**: 10 kΩ
- **Start of Signal**: <10 µs after 1PPS output
- **Programmable Phase Shift**: ±5ns to 500 ms with 5ns resolution

- **Accuracy**: ±50 ns (1σ)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-10 HAVE QUICK outputs, BNC

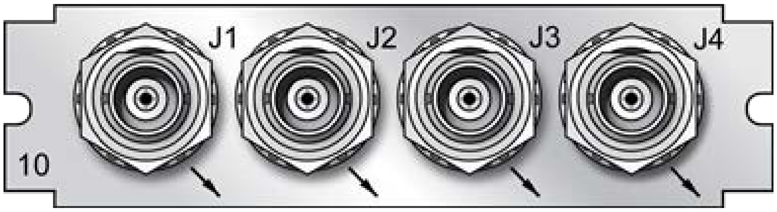


Figure 5-33: Model 1204-10 option card rear plate

5.4.5.2 HAVE QUICK Out, RS-485 [1204-1B]: Specifications

- **Outputs**: (4) HAVE QUICK outputs
- **Signal Type and Connector**: RS-485 levels (terminal block)
- **Formats Supported**:
  - STANAG 4246 HAVE QUICK I
  - STANAG 4246 HAVE QUICK II
  - STANAG 4372 HAVE QUICK IIA
  - STANAG 4430 Extended HAVE QUICK
  - STANAG 4430 Standard Time Message (STM)
  - ICD-GPS-060A BCD Time Code
  - ICD-GPS-060A HAVE QUICK
  - DOD-STD-1399 BCD Time Code
- **Output Load Impedance**: 120 Ω
- **Start of Signal**: <10 µs after 1PPS output
- **Programmable Phase Shift**: ±5ns to 500 ms with 5ns resolution
- **Accuracy**: ±50 ns (1σ)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-1B HAVE QUICK outputs, RS-485

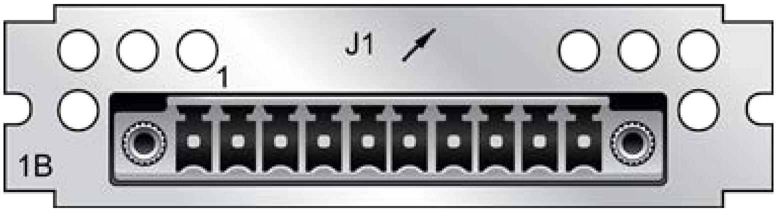


Figure 5-34: Model 1204-1B option card rear plate

Pin Assignments

Pin No.	Function
1	HAVE QUICK Output 1 +
2	HAVE QUICK Output 1 -
3	GND
4	HAVE QUICK Output 2 +
5	HAVE QUICK Output 2 -
6	HAVE QUICK Output 3 +
7	HAVE QUICK Output 3 -
8	GND
9	HAVE QUICK Output 4 +
10	HAVE QUICK Output 4 -

Table 5-18: 1204-1B terminal block pin-out

5.4.5.3 HAVE QUICK Output: Viewing Signal State

To quickly view if a **HAVE QUICK Output** is enabled or disabled, go to the option card's Status Summary panel. For instructions, see: "Viewing the Signal State of an Input or Output" on page 296.

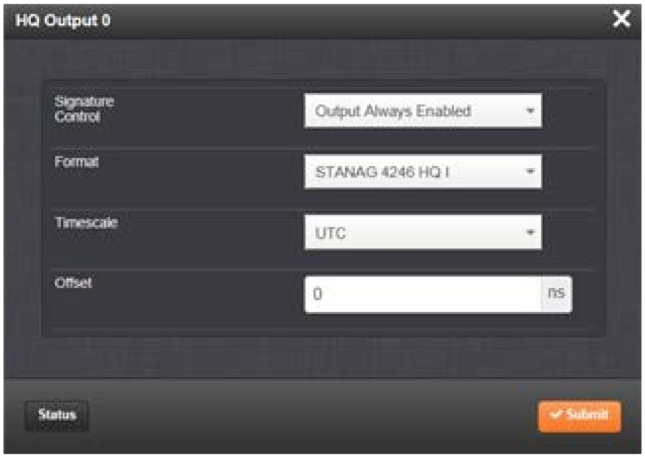
5.4.5.4 HAVE QUICK Output: Edit Window

To configure a **HAVE QUICK Output**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entries for this card are: **HAVE QUICK out, BNC** and **HAVE QUICK Out, RS-485**.

The outputs are named: **HQ Output [number]**.

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



HQ Output 0

Signature Control: Output Always Enabled

Format: STANAG 4246 HQ I

Timescale: UTC

Offset: 0 ns

The Edit window allows the configuration of the following settings:

- **Signature Control**: Signature Control is used to control when the HAVE QUICK modulation is present; see also "Signature Control" on page 201.
- **Format**: Used to configure the formatting of the four available HAVE QUICK outputs. The available output formats are as follows:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 Ext HQ (Extended HAVE QUICK)
  - STANAG 4430 STM (Standard Time Message)
  - ICD-GPS-060A BCD
  - ICD-GPS-060A HQ
  - DOD-STD-1399 BCD
- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International
  - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC time)
  - A **local clock** set up through the Time Management Page: This option will appear under the name of the local clock you have set up. Refer to "The Time Management Screen" on page 169 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to "Setting up a Local Clock" on page 176 more information on Local Clocks.

- **Offset**: Provides the ability to account for HAVE QUICK cable delays or other latencies in the HAVE QUICK outputs. The Offset values are entered in nanoseconds (ns). The available Offset range is -500 to +500 ms.

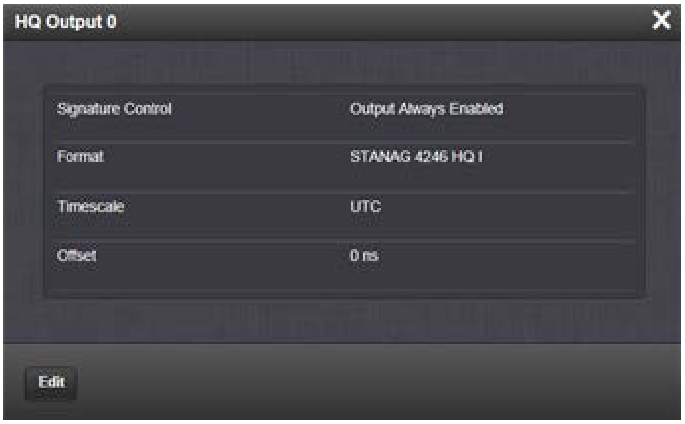
5.4.5.5 HAVE QUICK Output: Status Window

To view the current settings of a **HAVE QUICK Output**, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entries for this card are: **HAVE QUICK out, BNC** and **HAVE QUICK Out, RS-485**.

The outputs are named: **HQ Output [number]**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Signature Control	Output Always Enabled
Format	STANAG 4246 HQ I
Timescale	UTC
Offset	0 ns

The Status window displays the following settings:

- **Signature Control**: Signature Control is used to control when the HAVE QUICK modulation is present, see "Signature Control" on page 201.
- **Format**: Used to configure the formatting of the four available HAVE QUICK outputs. The available output formats are as follows:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 Ext HQ (Extended HAVE QUICK)

    - STANAG 4430 STM (Standard Time Message)
    - ICD-GPS-060A BCD
    - ICD-GPS-060A HQ
    - DOD-STD-1399 BCD
- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
    - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
    - **TAI**: Temps Atomique International
    - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC time)
    - A **local clock** set up through the Time Management Page: This option will appear under the name of the local clock you have set up. Refer to "The Time Management Screen" on page 169 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to "Setting up a Local Clock" on page 176 for more information on Local Clocks.

- **Offset**: Provides the ability to account for HAVE QUICK cable delays or other latencies in the HAVE QUICK outputs. The Offset values are entered in nanoseconds (ns). The available Offset range is -500 to +500 ms.

5.4.6 HAVE QUICK In/Out [1204-29]

The HAVE QUICK input/output option card 1204-29 provides SecureSync with (1) HAVE QUICK input and (3) HAVE QUICK outputs.

5.4.6.1 HAVE QUICK In/Out [1204-29]: Specifications

- **Inputs/Outputs**: (1) HAVE QUICK input/(3) HAVE QUICK outputs
- **Signal Type and Connector**: TTL levels (BNC)
- **Output Load Impedance**: 50 Ω
- **Start of Signal**: <10 µs after 1PPS output
- **Programmable phase shift**: ±5ns to 500 ms with 5ns resolution
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-29: HAVE QUICK Input/Output

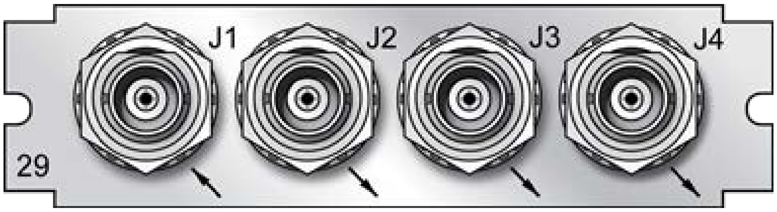


Figure 5-35: Model 1204-29 option card rear plate

5.4.6.2 HAVE QUICK Output: Viewing Signal State

To quickly view if a **HAVE QUICK Output** is enabled or disabled, go to the option card’s Status Summary panel. For instructions, see: "Viewing the Signal State of an Input or Output" on page 296.

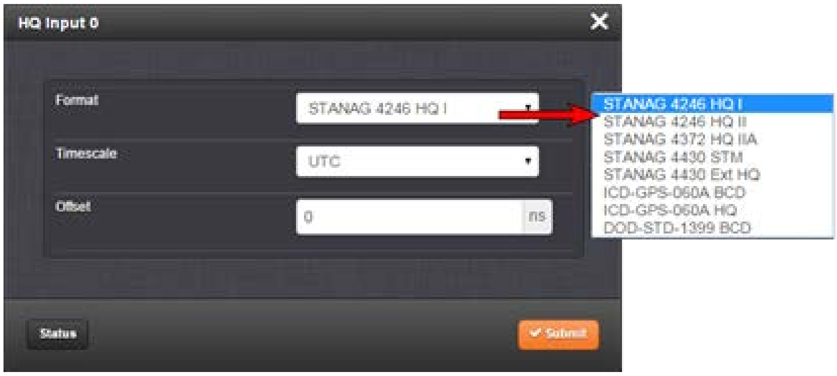
5.4.6.3 HAVE QUICK Input: Edit Window

To configure the settings of the **HAVE QUICK Input** (also referred to as ‘Reference’), go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entry for this card is: **HAVE QUICK In/Out**.

The input is named: **HQ Input [number]**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



HQ Input 0

Format: STANAG 4246 HQ I

Timescale: UTC

Offset: 0 ns

The Edit window allows the configuration of the following settings:

- **Format**: Used to configure the formatting of the four available HAVE QUICK outputs. The available output formats are as follows:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II

- STANAG 4430 STM
- STANAG 4430 Ext HQ
- ICD-GPS-060A BCD
- ICD-GPS-060A HQ
- DOD-STD-1399 BCD

- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - UTC: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - TAI: Temps Atomique International
  - GPS: The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC time)
  - Offset: Provides the ability to account for HAVE QUICK cable delays or other latencies in the HAVE QUICK outputs. The Offset values are entered in nanoseconds (ns). The available Offset range is -500 to +500 ms.

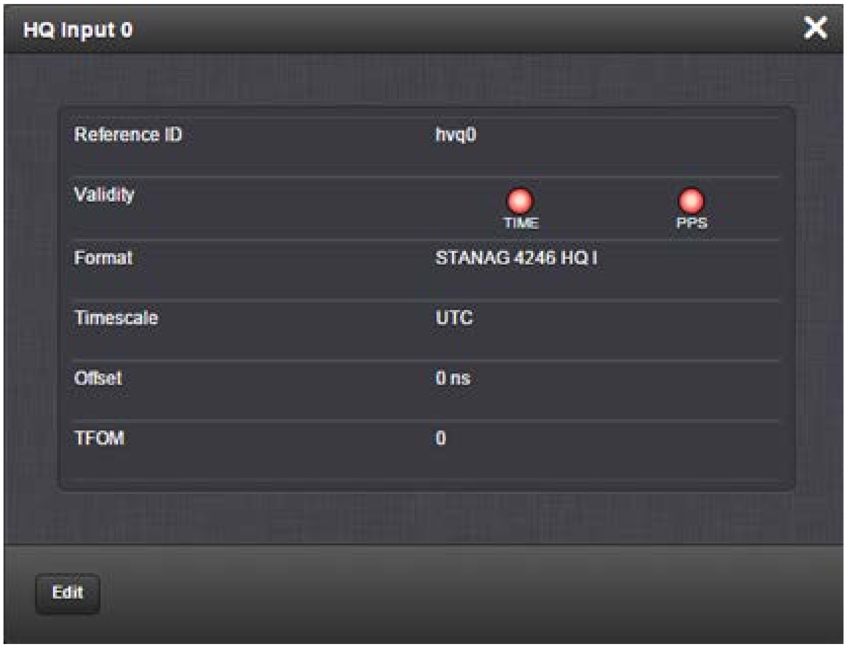
5.4.6.4 HAVE QUICK Input: Status Window

To view the current settings of the **HAVE QUICK Input** (also referred to as ‘Reference’), go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entry for this card is: **HAVE QUICK In/Out**.

The input is named: **HQ Input [number]**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Reference ID	hvq0
Validity	TIME PPS
Format	STANAG 4246 HQ I
Timescale	UTC
Offset	0 ns
TFOM	0

The Status window displays the following settings:

- **Reference ID**: Indicates the letters used in the Input Reference Priority table for this particular input reference.
- **Validity**: [TIME, PPS] Indicates the validity of the Time input and the PPS input. If the input signal is valid the indicator will be green. If the signal is not valid, the indicator will be orange.
- **Format**: Used to configure the formatting of the four available HAVE QUICK outputs. The available output formats are as follows:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4430 STM
  - STANAG 4430 Ext HQ
  - ICD-GPS-060A BCD
  - ICD-GPS-060A HQ
  - DOD-STD-1399 BCD
- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International

- **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC time).

- **Offset**: Provides the ability to account for HAVE QUICK cable delays or other latencies in the HAVE QUICK outputs. The Offset values are entered in nanoseconds (ns). The available Offset range is -500 to +500 ms.
- **TFOM**: The Time Figure of Merit for the input.

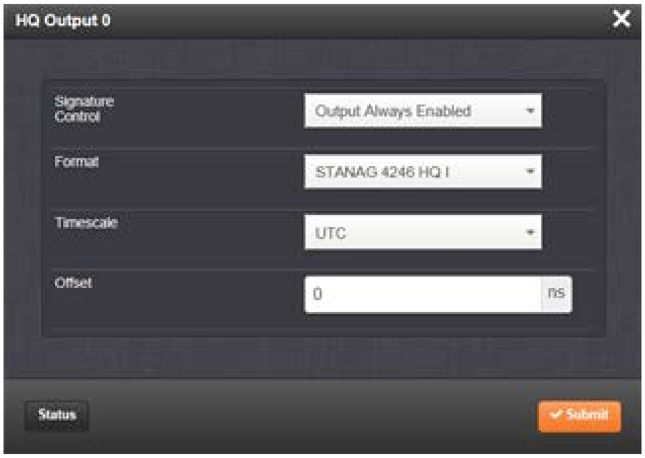
5.4.6.5 HAVE QUICK Output: Edit Window

To configure the settings of a **HAVE QUICK Output**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entry for this card is: **HAVE QUICK In/Out**.

Outputs are named: **HQ Output [number]**.

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



HQ Output 0

Signature Control	Output Always Enabled
Format	STANAG 4246 HQ I
Timescale	UTC
Offset	0 ns

The Edit window allows the configuration of the following settings:

- **Signature Control**: Signature Control is used to control when the HAVE QUICK modulation is present, see "Signature Control" on page 201.
- **Format**: Used to configure the formatting of the four available HAVE QUICK outputs. The available output formats are as follows:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 Ext HQ (Extended HAVE QUICK)
  - STANAG 4430 STM (Standard Time Message)

  - ICD-GPS-060A BCD
  - ICD-GPS-060A HQ
  - DOD-STD-1399 BCD
- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International
  - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC time).
  - A **local clock** set up through the Time Management Page: This option will appear under the name of the local clock you have set up. Refer to "The Time Management Screen" on page 169 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

  The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to "Setting up a Local Clock" on page 176 for more information on Local Clocks.
- **Offset**: Provides the ability to account for HAVE QUICK cable delays or other latencies in the HAVE QUICK outputs. The Offset values are entered in nanoseconds (ns). The available Offset range is -500 to +500 ms.

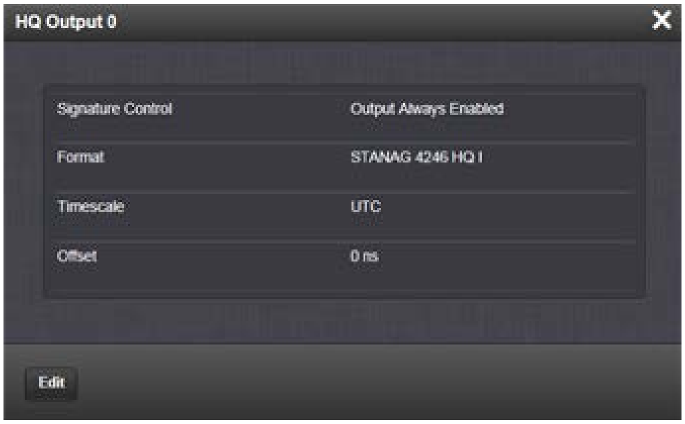
5.4.6.6 HAVE QUICK Output: Status Window

To view the current settings of a **HAVE QUICK Output**, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entry for this card is: **HAVE QUICK In/Out**.

Outputs are named: **HQ Output [number]**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Signature Control	Output Always Enabled
Format	STANAG 4246 HQ I
Timescale	UTC
Offset	0 ns

The Status window displays the following settings:

- **Signature Control**: Signature Control is used to control when the HAVE QUICK modulation is present, see "Signature Control" on page 201.
- **Format**: Used to configure the formatting of the four available HAVE QUICK outputs. The available output formats are as follows:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 Ext HQ (Extended HAVE QUICK)
  - STANAG 4430 STM (Standard Time Message)
  - ICD-GPS-060A BCD
  - ICD-GPS-060A HQ
  - DOD-STD-1399 BCD
- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International
  - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC time)
  - A **local clock** set up through the Time Management Page: This option will appear under the name of the local clock you have set up. Refer to "The Time Management Screen" on page 169 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to "Setting up a Local Clock" on page 176 for more information on Local Clocks.

- **Offset**: Provides the ability to account for HAVE QUICK cable delays or other latencies in the HAVE QUICK outputs. The Offset values are entered in nanoseconds (ns). The available Offset range is -500 to +500 ms.

5.4.7 ASCII Time Code In/Out [1204-02, -04]

The ASCII Time Code Option Card, **Model 1204-02 (RS-232)** provides:

- one male DB-9 RS-232 input connector (J2),
- and one female DB-9 RS-232 output connector (J1)

The ASCII Time Code Option Card, **Model 1204-04 (RS-485)** consists of one RS-485 input, and one RS-485 output, integrated in a shared terminal block connector.

The interfaces accept Asynchronous Serial signals including date and time information. The input and output Data Formats are selected among predefined formats.

ASCII input

The ASCII input provides a serial data interface between an ASCII time generator (e.g., another SecureSync unit), serving as an input reference for Time and 1PPS in order to synchronize SecureSync (in conjunction with, or in lieu of, other available inputs, such as GNSS and/or IRIG).

ASCII ouput

The ASCII output provides SecureSync with the ability to output one, two or three back-to-back ASCII time code data streams that can be provided to peripheral devices which accept an ASCII RS-232 input data stream for either their external time synchronization or for data processing. See "ASCII Time Code Data Formats" on page 474 for a description of all supported time code formats.

The **RX signal** on an output interface is used for triggering the output ASCII message output when a configured character is received from the peripheral device.

When SecureSync is configured to output only one format message (the second and third formats configured as “None”), the one configured message will be available on the output port as either a broadcast message or only upon a request character being received. SecureSync has the ability to output one or two additional data stream messages immediately following the first message. In this configuration, only the first message determines the on-time point for the entire output string. The on-time points for the second and third messages that are provided at the same time as the first message are discarded. This unique capability allows SecureSync to be able to simultaneously provide multiple pieces of data from different selected format messages.

An example of selecting multiple formats is selecting “NMEA GGA” as the first format, “NMEA RMC” as the second format and “NMEA ZDA” as the third format. Depending on the setting of the “Mode” field (which determines if the data streams are available every second or upon a request character being received), at the next second or the receipt of the next request character, the output port will provide the GGA message followed immediately by the corresponding RMC message for that same second, followed immediately by the corresponding ZDA message for that same second. The first GGA message will provide the on-time point for the entire output data stream.

5.4.7.1 ASCII Time Code, RS-232 [1204-02]: Specifications

- **Inputs/Outputs**: (1) Input, (1) Output
- **Signal Type and Connector**:
  - **Connector J1** – (RS-232 Output) RS-232 DB-9 F
  - **Connector J2** – (RS-232 Input) RS-232 DB-9 M
- **Accuracy**: ±100...1000 µs (format dependent)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-02: ASCII Time Code Module (RS-232)

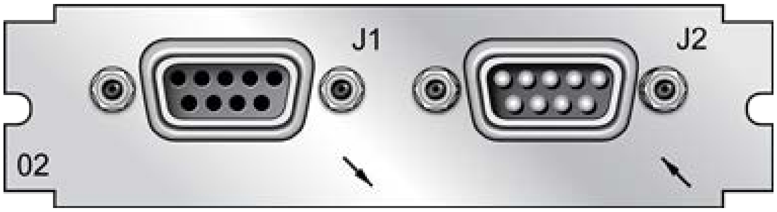


Figure 5-36: Model 1204-02 option card rear plate

Pin Assignments: OUTPUT connector J1

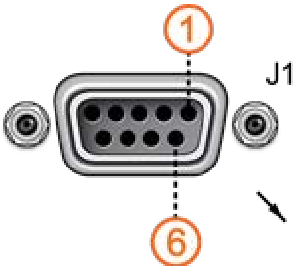


Figure 5-37: OUTPUT connector J1

Pin Number	Signal	Function
Top row of 5 pins		
1	PPS_OUT	1PPS output
2	SERIAL_OUT_TX	RS-232 Transmit data
3	SERIAL_IN_RX	RS-232 Receive data
4	NC	No connection

Pin Number	Signal	Function
5	GND	Ground
Bottom row of 4 pins		
6	NC	No connection
7	NC	No connection
8	NC	No connection
9	NC	No connection

Table 5-19: Pin-out, OUTPUT connector "J1"

Pin Assignments: INPUT connector J2

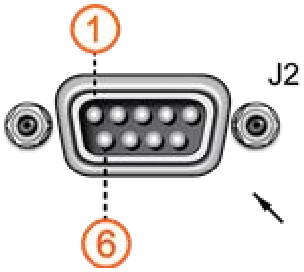


Figure 5-38: INPUT connector J2

Pin Number	Signal	Function
Top row of 5 pins		
1	PPS_IN	1PPS input
2	SERIAL_IN_RX	RS-232 Receive data
3	SERIAL_IN_TX	RS-232 Transmit data
4	NC	No connection
5	GND	Ground
Bottom row of 4 pins		
6	NC	No connection
7	NC	No connection
8	NC	No connection
9	NC	No connection

Table 5-20: Pin-out, INPUT connector "J2"

5.4.7.2 ASCII Time Code, RS-485 [1204-04]: Specifications

- **Inputs/Outputs**: (1) Input, (1) Output
- **Signal Type and Connector**: (1) RS-485 terminal block for both Input and Output
- **Accuracy**: ±100...1000 µs (format dependent)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-04 ASCII Time Code Module (RS-485)

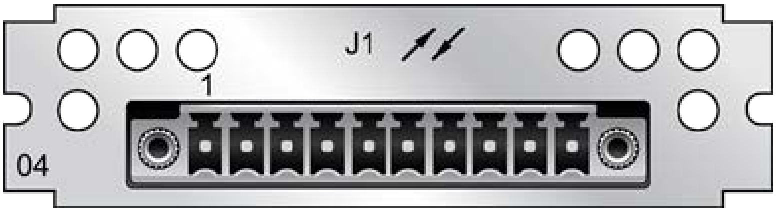


Figure 5-39: Model 1204-04 option card rear plate

Pin Assignments

Table 5-21: Pin-out, RS-485 terminal block connector J1

Pin No.	Signal	Function
1 (left)	SERIALTX_RS485+	+ RS-485 data output
2	SERIALTX_RS485-	- RS-485 data output

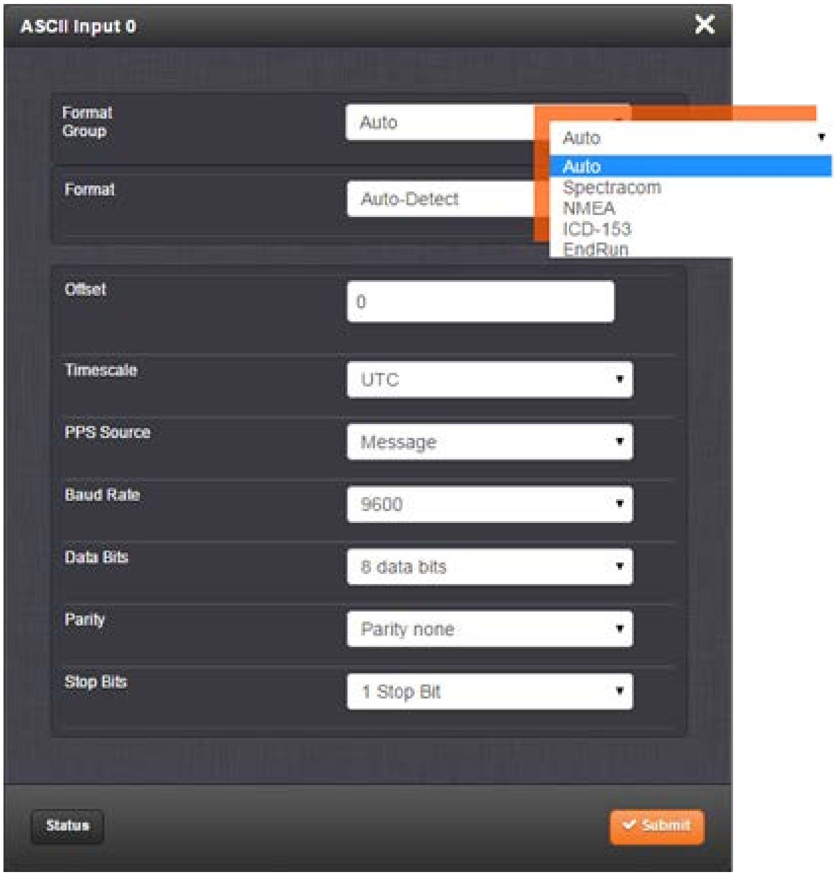
Pin No.	Signal	Function
3	GND	Ground
4	PPS_OUT_RS485+	+ 1PPS output
5	PPS_OUT_RS485-	- 1PPS output
6	SERIALRX_RS485+	+ RS-485 data input
7	SERIALRX_RS485-	- RS-485 data input
8	GND	Ground
9	PPS_IN_RS485+	+ 1PPS input
10 (right)	PPS_IN _RS485-	- 1PPS input

5.4.7.3 ASCII Time Code Input: Edit Window

To configure the **ASCII Input** (also referred to as ‘Reference’), go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entries for this card are: **ASCII TIMECODE RS-232** and **ASCII TIMECODE RS-485**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



ASCII Input 0

Format Group: Auto

Format: Auto-Detect

Offset: 0

Timescale: UTC

PPS Source: Message

Baud Rate: 9600

Data Bits: 8 data bits

Parity: Parity none

Stop Bits: 1 Stop Bit

The Input Edit window allows the configuration of the following settings:

- **Format Group**: Determines the time code message format category (see also "ASCII Time Code Data Formats" on page 474.) Choices are:
  - Auto
  - Spectracom
  - NMEA
  - ICD-153
  - EndRun
- **Format**: Once a **Format Group** has been selected, one or more **Format** fields may appear, allowing you to select one or more time code **Formats**. For more information on time code formats, see "ASCII Time Code Data Formats" on page 474.

Note: If Auto is chosen as the format group, the format will automatically be Auto-detect. SecureSync will attempt to identify the format of the incoming ASCII message.

- **Offset**: Provides the ability to account for ASCII input cable delays or other latencies in the ASCII input. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.
- **Timescale**: Used to select the time base for the incoming ASCII time code data. The entered Timescale is used by the system to convert the time in the incoming ASCII data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International
  - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC time)
  - A **local clock** set up through the Time Management Page: This option will appear under the name of the local clock you have set up. Refer to "The Time Management Screen" on page 169 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

    The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. See "Setting up a Local Clock" on page 176 for more information on Local Clocks.

> **Note:** The Timescale of the ASCII input (as configured in the ASCII time source) must be set correctly, especially if other input references are enabled. Failure to configure the Timescale of the ASCII input correctly could result in time jumps occurring in the System Time when input reference changes occur. These time jumps could affect NTP and normal operation of the system.

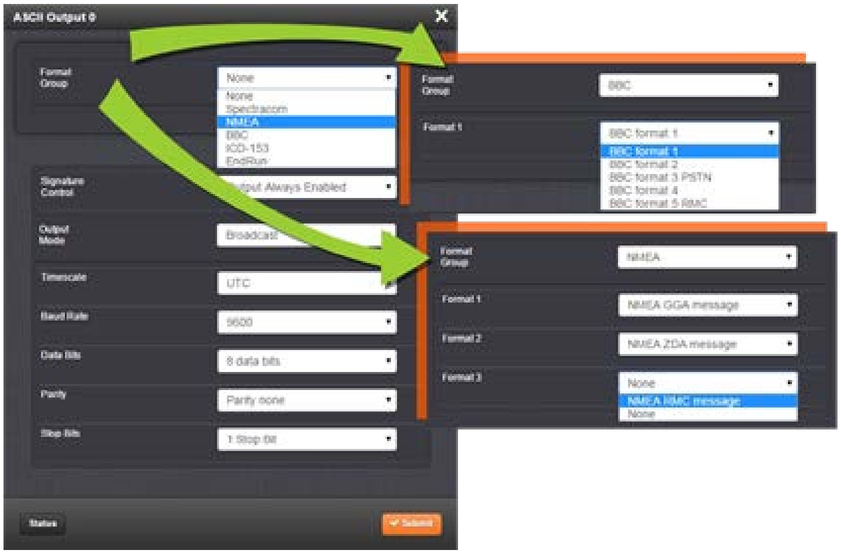
- **PPS Source** - choices are:
  - **Message**: The 1PPS on time point is extracted from the ASCII message received.
  - **1PPS Pin**: The origin of the 1PPS on-time-point is the connector 1PPS input.
- **Baud Rate**: Determines the speed at which the input port will operate.
- **Data Bits**: Defines the number of Data Bits for the input output.
- **Parity**: Configures the parity checking of the input port.
- **Stop Bits**: Defines the number of Stop Bits for the input port.

5.4.7.4 ASCII Time Code Output: Edit Window

To configure the **ASCII Output**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entries for this card are: **ASCII TIMECODE RS-232** and **ASCII TIMECODE RS-485**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



ASCII Output 0

Format Group: None

Signature Control: Output Always Enabled

Output Mode: Broadcast

Timescale: UTC

Baud Rate: 9600

Data Bits: 8 data bits

Parity: Parity none

Stop Bits: 1 Stop Bit

Format Group: BBC

Format 1: BBC format 1

Format Group: NMEA

Format 1: NMEA GGA message

Format 2: NMEA ZDA message

Format 3: None

The Output Edit window allows the configuration of the following settings:

- **Format Group** - configures the message format type. Choices are:
  - None (no message will be output)
  - Spectracom
  - NMEA
  - BBC
  - ICD-153
  - EndRun

  Once selected, the **Format Group** may offer a choice of **Formats**. For more information on supported **Formats**, see "ASCII Time Code Data Formats" on page 474.
- **Format 1**: Selects either the first of up to three, or the only format message to be output.
- **Format 2**: Selects the second consecutive format message to be outputted. Select “None” if only one output format is desired. “None” will be the only choice available if Format 1 is “None.”

- **Format 3**: Selects the third consecutive format message to be outputted. Select “None” if only one output format is desired. “None” will be the only choice available if Format 2 is “None.”
- **Signature Control**: Signature Control controls when the selected ASCII data output format will be present; see "Signature Control" on page 201.
- **Output Mode**: This field determines when the output data will be provided. The available Mode selections are as follows:
  - **Broadcast**: The format messages are automatically sent out on authorized condition (Signature control), every second a message is generated in sync with the 1PPS.
  - **Request (On-time)**: A format message is generated in sync with 1PPS after the configured request character has been received.
  - **Request (Immediate)**: A format message is generated as soon as the request character is received. As this selection does not correlate the output data to the on-time point for the message, in Data Formats that do not provide sub-second information (such as Formats 0 and 1 whereas Format 2 provides sub-second information), it should be noted that the output data can be provided immediately, but a time error could occur when using the on-time point of the message in addition to the data for timing applications.

    Note: The choices available in this field are determined by the choices of Format Group and Format.
- **Time Scale**: Used to select the time base for the incoming data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International
  - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is currently 17 seconds ahead of UTC time).

  If GPS or TAI time is used, then the proper timescale offsets must be set on the **MANAGEMENT/OTHER/Time Management** page. (See "The Time Management Screen" on page 169 for more information on how to configure and read the System Time). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.
  - A **local clock** set up through the **Time Management** Page: This option will appear under the name of the local clock you have set up. See "Setting up a Local Clock" on page 176 for more information. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. See "Setting up a Local Clock" on page 176 for more information on Local Clocks.

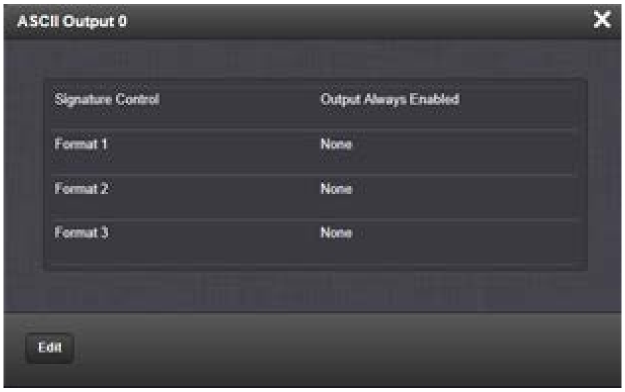
- **Baud Rate**: Determines the speed at which the output port will operate.
- **Data Bits**: Defines the number of Data Bits for the output port.
- **Parity**: Configures the parity checking of the output port.
- **Stop Bits**: Defines the number of Stop Bits for the output.

5.4.7.5 ASCII Time Code Output: Status Window

To view the current settings of the **ASCII Output**, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entries for this card are: **ASCII TIMECODE RS-232** and **ASCII TIMECODE RS-485**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).


ASCII Output 0

Signature Control	Output Always Enabled
Format 1	None
Format 2	None
Format 3	None

The Status window displays the following settings:

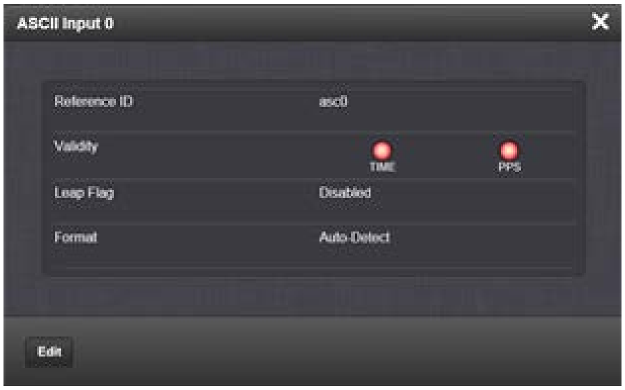
- **Signature Control**: Indicates whether Signature Control is enabled (Signature Control determines when the ASCII data stream will be enabled to be present). See also: "Signature Control" on page 201.
- **Format 1**: Indicates the configured format of the ASCII time code input data stream.
- **Format 2**: Indicates the configured format of the second consecutive ASCII time code input data stream.
- **Format 3**: Indicates the configured format of the third consecutive ASCII time code input data stream.

5.4.7.6 ASCII Time Code Input: Status Window

To *view* the current settings of the **ASCII Input** (also referred to as ‘Reference’), go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entries for this card are: **ASCII TIMECODE RS-232** and **ASCII TIMECODE RS-485**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



ASCII Input 0

Reference ID	asc0	
Validity	● TIME	● PPS
Leap Flag	Disabled	
Format	Auto-Detect	

The Status window displays the following settings:

- **Reference ID**: Indicates the letters used in the Input Reference Priority table for this particular input reference.
  - **Validity**: Indicates whether the ASCII input data is present and considered valid for Time and 1PPS references.
    - A **green** light indicates a valid reference.
    - An **orange** light indicates the reference is not considered valid.
- **Leap Flag**: Displays whether the incoming data stream is indicating that a pending leap second is to be added to the UTC timescale at the end of the month. See "Configuring a Leap Second Correction" on page 174.
- **Format**: Indicates the configured format of the ASCII time code input data stream.

5.5 Network Interface Option Cards

This section contains technical information and SecureSync Web UI procedures pertaining to option cards designed as Ethernet network interfaces using, e.g. the PTP format.

5.5.1 Gigabit Ethernet [1204-06]

This option card provides SecureSync with three 10/100/1000 Base-T network interfaces, in addition to the standard 10/100 Base-T network interface.

5.5.1.1 Gigabit Ethernet [1204-06]: Specifications

- **Inputs/Outputs**: (3) Gigabit Ethernet (10/100/1000 Base-T)
- **Connectors**: RJ-45 (3x)
- **Management**: Enabled or Disabled (NTP server only)
- **Maximum Number of Cards**: 1
- **Ordering Information**: 1204-06: Gigabit Ethernet (3X) Module

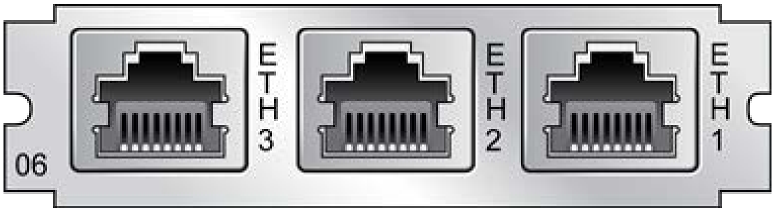
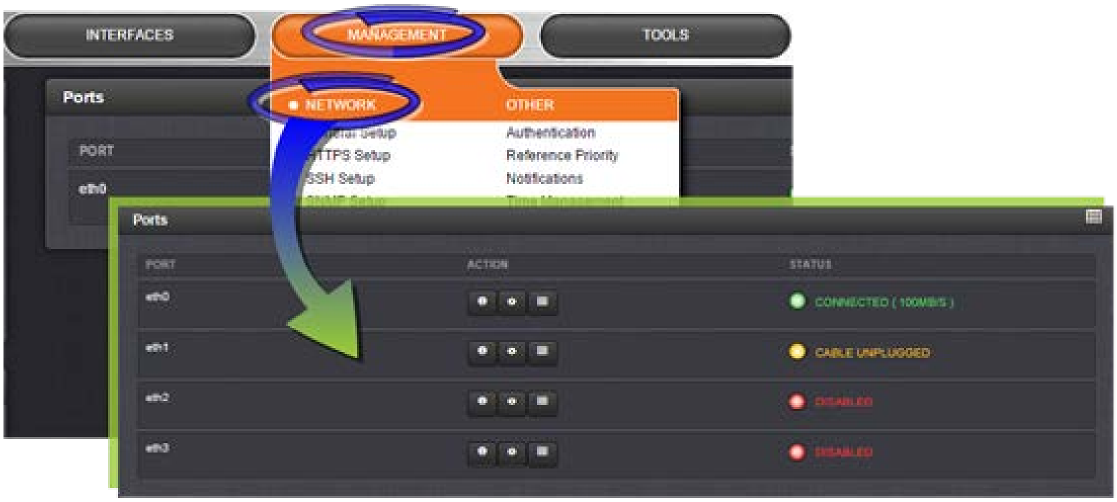


Figure 5-40: 1204-06 option card rear plate

5.5.1.2 Accessing the Network Management Screen

In order to monitor and manage Ethernet on SecureSync:

- Via **MANAGEMENT > NETWORK**, navigate to the **Network Management** screen: On the right, the **Ports** panel will display the available Ethernet ports, and their connection status:



Ports

PORT	ACTION	STATUS
eth0		● CONNECTED (100MBIT/S)
eth1		● CABLE UNPLUGGED
eth2		● DISABLED
eth3		● DISABLED

Eth0 is the built-in SecureSync Ethernet port. **Eth1** through **eth3** are the ports provided by the 1204-06 card.

For information on managing Ethernet on SecureSync, see "Network Management" on page 45.

5.5.1.3 Routing Tables

There are five (5) routing tables in the system: one for each network interface, and one main routing table.

- **Main Routing Table**: This routing table is used when network traffic is generated from the server. It will generally have the same default gateway as the routing table for **eth0**, unless configured otherwise.
- **Interface Routing Tables**: These routing tables are specific to each interface. They are named **t0** (for eth0 interface) though **t3** (for eth3 interface).
  The system is configured by default with rules to use the individual routing table for each interface for all network traffic being received or transmitted from or to the corresponding interface. For example, when an NTP request is received on interface **eth2**, it is tagged as such and the response will use routing table **t2** when sending the NTP response packet.
  Each routing table has a default gateway that is used when there is no explicit routing table entry that matches the destination address for a given network packet.

For information on configuring routing tables see "Adding Static Routes to the Routing Table" on page 53, and see Spectracom Tech Note Routing of Data with Multiple Networks.

Domains and Domain Name Servers (DNS)

Each network interface may exist on a separate domain and therefore have a different domain name and domain name servers from the other interfaces.

The system supports a single domain name and up to 2 DNS addresses per network interface. These may be assigned via DHCP or configured manually via the Web UI configuration screen for each network interface.

Configuring Ethernet Ports

For information on configuring Ethernet ports, see "Configuring Network Ports" on page 48.

5.5.2 PTP Grandmaster [1204-32]

Precision Time Protocol (PTP) is a protocol that can be used to synchronize computers on an Ethernet network. The Precision Time Protocol (PTP) option module supports PTP Version 2, as specified in the IEEE 1588-2008 standard (PTP Version 1 is not supported), via one (1) Ethernet port.

The PTP option module implements a PTP Ordinary Clock that can be configured to run as a Master Clock only. It transmits PTP packets via the Ethernet port, with information about the current time and synchronization reference selected by the SecureSync device.

5.5.2.1 PTP Grandmaster [-32]: Specifications

- **Inputs/Outputs**: (1) Configurable as Input or Output
- **Signal Type and Connector**: Ethernet via SFP, and 1PPS Output via BNC
- **Management**: Web UI
- **Resolution**: 8ns (±4ns) packet time stamping resolution
- **Accuracy**: 30 ns accuracy (3σ) Master to Slave, via crossover cable
- **Network Speeds**: 100 Mb/s, or 1Gb/s, depending on SFP module used
- **PTP Version** supported: PTP 2 (IEEE 1588-2008)
- **PTP Profiles** supported: Default, Telecom, Enterprise
- **Transmission modes**: Unicast [default], Multicast
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-32: PTP/Precision Timing Protocol Option Module

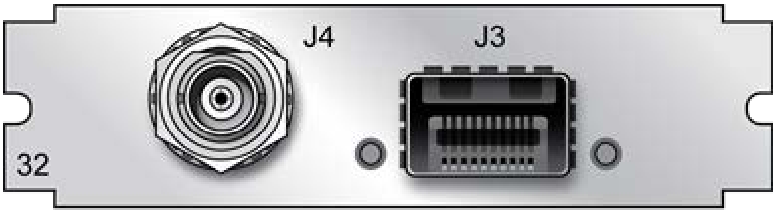
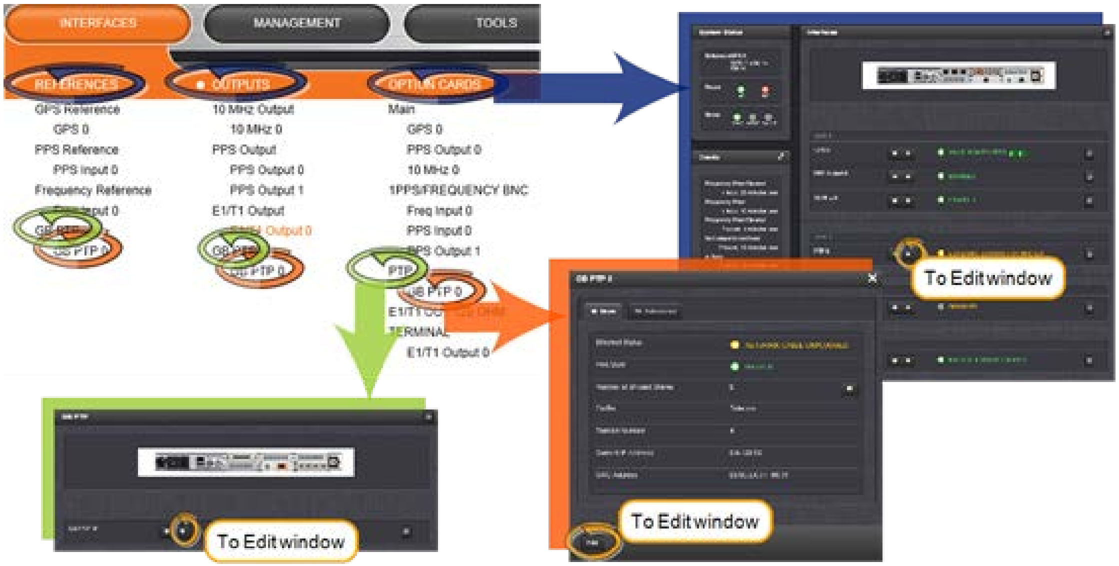


Figure 5-41: Model 1204-32 option card rear plate

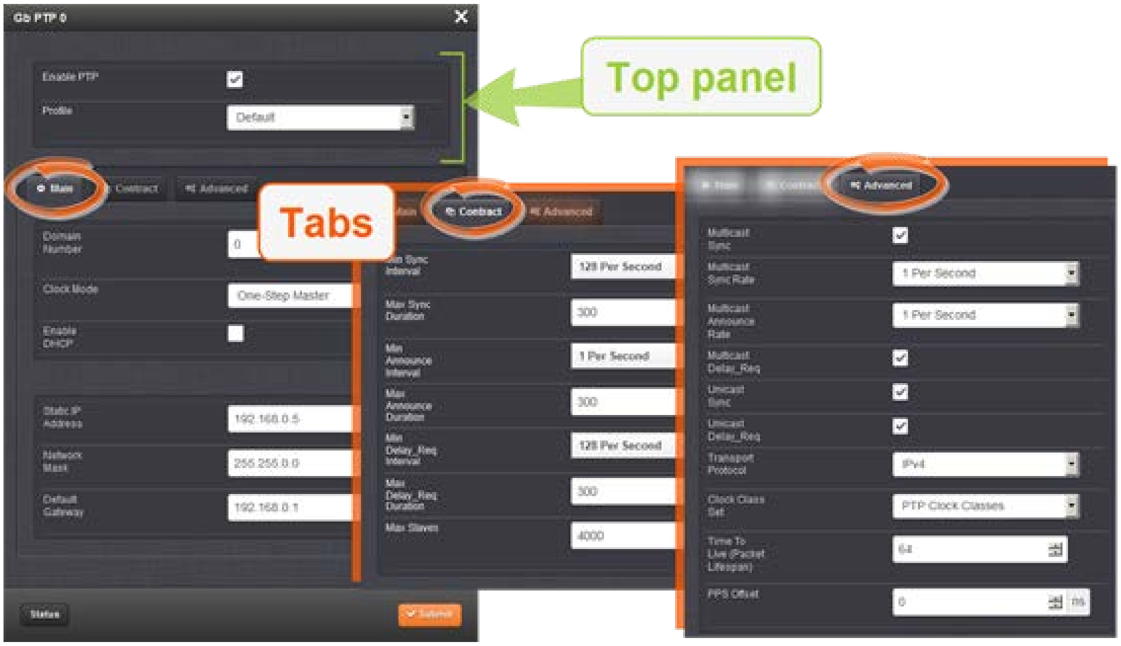
5.5.2.2 PTP Grandmaster [-32]: Edit Window

1. To configure this option card, go to its **Edit** window. For instructions, see "Configuring the Settings of an Input or Output" on page 295.



Note: If you have only one input or output of any type, SecureSync will number that input or output 0. Additional inputs or outputs will be numbered 1 or above.

2. The **Gb PTP Edit window** will display. It includes the **top panel**, and offers access to three different **tabs**, described below:



Enable PTP	☑
Profile	Default

Domain Number	0
Clock Mode	One-Step Master
Enable DHCP	□
Static IP Address	192.168.0.5
Network Mask	255.255.0.0
Default Gateway	192.168.0.1

Min Sync Interval	128 Per Second
Max Sync Duration	300
Min Announce Interval	1 Per Second
Max Announce Duration	300
Min Delay_Req Interval	128 Per Second
Max Delay_Req Duration	300
Max Slaves	4000

Multicast Sync	☑
Multicast Sync Rate	1 Per Second
Multicast Announce Rate	1 Per Second
Multicast Delay_Req	☑
Unicast Sync	☑
Unicast Delay_Req	☑
Transport Protocol	IPv4
Clock Class Set	PTP Clock Classes
Time To Live (Packet Lifespan)	64
PPS Offset	0 ns

Top panel settings

- **Enable PTP**: Enables/Disables PTP. Check the box to enable PTP. Uncheck it to disable PTP.
- **Profile** – offers a choice of:
  - Default (incl. Enterprise)
  - Telecom

Bottom panel: tabs

- **Main**: These settings pertain to network connectivity.
- **Contract**: These settings pertain to the unicast contract.
- **Advanced**: These setting pertain to time Sync information.

Main tab settings

- **Domain Number**: Sets the current PTP Domain Number, as defined in IEEE Std 1588-2008 Section 7.1
- **Clock Mode**: PTP has two ways to transmit the initial T1 timestamp of the Sync packet transmission from the Master to the Slave:
    - **One-Step** Master: The Sync packet is timestamped, then the timestamp is inserted into the Sync packet in real-time, as it is transmitted.
    - **Two-Step Master**: The Sync packet is timestamped, but the timestamp value in the Sync packet is ignored. The actual T1 value is transmitted in a "Follow-Up" packet after the Sync packet.

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

- **Enable DHCP**: This is a checkbox to enable or disable the delivery of IP addresses from a DHCP Server. The default setting is enabled (the box is checked).
- **Static IP Address**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this IP address. In the format “#.#.#.#” with no leading zeroes or spaces, where each ‘#’ is a decimal integer from the range [0,255].
- **Network Mask**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this Network Mask. In the format “#.#.#.#” with no leading zeroes or spaces, where each ‘#’ is a decimal integer from the range [0,255].
- **Default Gateway**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this Default Gateway. In the format “#.#.#.#” with no leading zeroes or spaces, where each ‘#’ is a decimal integer from the range [0,255].

Contract tab settings

> **Note:** The settings under this tab only apply to Unicast mode.

[Default settings in parenthesis]

- **Min Sync Interval**: The minimum value of Sync interval granted by the Master Clock. In packets per second. [128 Per Second]
- **Max Sync Duration**: The maximum value of Sync interval granted by the Master Clock. In seconds. [10000]
- **Min Announce Interval**: The minimum value of the Announce interval granted by the Master Clock. In packets per second. [128 Per Second

- **Max Announce Duration**: The maximum value of the Announce interval granted by the Master Clock. In seconds. [10000]
- **Min Delay_Req Interval**: In packets per second. [128 Per Second]
- **Max Delay_Req Duration**: In seconds. [10000]
- **Max Slaves**: The maximum number of slaves the card will serve. [4000]

Advanced tab settings

About… PTP Transmission Modes

The PTP Card is able to transmit the PTP packets in three transmission modes:

• **Multicast Mode**: This is the default mode. PTP packets are transmitted to all PTP Clocks by means of Multicast IP addresses dedicated to the PTP protocol (224.0.1.129, 224.0.0.107). PTP packets received by the PTP Clocks are then filtered from the Domain Number, the Port Identity (Clock Identity + Port Number) of the transmitter, the packet identifier (Sequenced).When the Master Clock is set in Multicast mode, this module will deny the requests from the Slaves Clocks to run in Unicast mode. When the Master Clock is set in Unicast mode, it doesn't transmit any PTP messages until a Slave has been granted to run in Unicast mode.

• **Unicast Mode**: This is a Point-to-Point transmission mode between two PTP Clocks by means of the unique IP address assigned to each PTP Clock.

NOTE: The Unicast mode is only implemented for the following PTP packets:

Announce, **Sync** and **Follow-Up**, **Delay_Req** and **Delay_Resp**.

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

____

• **Minicast/Hybrid Mode**: The Minicast/Hybrid mode is a method to minimize the PTP packets payload on the network, where: The transmissions initiated by the Master (Announce, Sync/Follow-Up) run in Multicast mode.

The transmissions initiated by the Slaves (Delay_Req/Delay_Resp) run in Unicast mode.

- **Multicast Sync**: Activating this option will cause the PTP Master to broadcast Sync and Announce messages to the Multicast address (as long as it is the Best Master on the network). Deactivating this option will remove the messages. When the PTP module is set in multicast mode, this will deny the requests from the Slaves Clocks to running in unicast mode.

    - Checking this box will cause two additional fields to display that will allow you to configure the:
        - Multicast Sync Rate
        - Multicast Announce Rate
- **Multicast Delay_Req**: Activating this option will cause the PTP Master to respond to multicast Delay Requests (as long as it is the Best Master on the network). Deactivating this option will prevent the Master from responding to these.
- **Unicast Sync**: The PTP Master will always respond to attempts from Unicast slaves to communicate with it, provided the Slaves use the proper Unicast Auto-Negotiation process. This setting is always enabled.
- **Unicast Delay_Req**: The PTP Master will always respond to attempts from Unicast slaves to communicate with it, provided the Slaves use the proper Unicast Auto-Negotiation process. This setting is always enabled.
- **Transport Protocol**: Selects the transport protocol used for PTP packets.
- **Clock Class Set**: Parameter broadcast in a PTP profile, indicating the quality of the attached reference; PTP [default], ARB, ITU (Telecom]
- **Time To Live (Packet Lifespan)**: Sets the TTL field for PTP packets except for Peer-to-Peer packets for which TTL is forced to 1 as specified in IEEE Std 1588-2008 Annex D.3.
- **1PPS Offset**: The 1PPS signal of this option card can be offset from the main System 1PPS. This offset will be applied to all timestamps created by this card. It can be set in 8ns increments. Range is -500 ms to +500 ms.
- **Priority 1**: See IEEE 1588-2008, Section 8.10.1, 8.10.2.
- **Priority 2**: See IEEE 1588-2008, Section 8.10.1, 8.10.2.
- **Enable SyncE**: If checked, allows access to the synchronous Ethernet settings. There will always be an ESMC message broadcast if Enable SyncE is checked.
    - **Enable ESMC**: [checkbox]
        - **ESMC Signal Control**: Determines which SSM to use in the ESMC message. One of two messages will be broadcast: either the message selected in the SSM Code dropdown or the QL_DNU code. The user may set one of the following broadcasting options:
            - **Output Always Enabled**: Always broadcasts the selected SSM code, even when SecureSync is not synchronized to its references.
            - **Output Enabled in Holdover**: The output uses the selected SSM code unless SecureSync is not synchronized to its references (the output is present while in the Holdover mode). While SecureSync is not synchronized, QL-DNU SSM code will be broadcast.
            - **Output Disabled in Holdover**: The output uses the selected SSM code unless the SecureSync references are considered not qualified

and invalid (the output is not present while in the Holdover mode). While references are invalid, QL-DNU SSM code will be broadcast.

- **Output Always Disabled**: The output is not present, even if any SecureSync references are present and considered qualified. QL-DNU SSM code is broadcast.

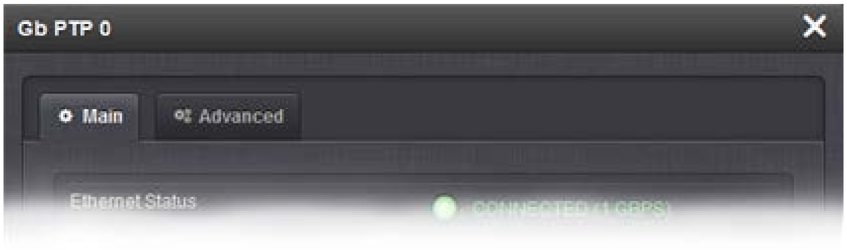
- **SSM Code**: The Sync Status Messaging (SSM) code to be utilized. Choice of code is made through the drop-down list.

> **Note:** Some parameters define a PTP packets throughput. They use the “log2 seconds“, defined as follows.

  - **Positive Value**: n => 2n seconds between two successive PTP packets
  - **Negative Value**:-n => 2(-n) = (1/2n) => 2n PTP packets per second

5.5.2.3 PTP Grandmaster [-32]: Status Window

To view the status of a PTP interface, go to its Status window. For instructions, see "Viewing the Configuration of an Input or Output" on page 293.



Ethernet Status CONNECTED (1 GBPS)

The **GB PTP** Status window contains two tabs: Main and Advanced.

Main tab: Status information

- **Ethernet Status**: Whether the module is connected to a network through Ethernet.
  - **Green**=Connected. The speed of the connection is indicated.
  - **Orange**=Not connected.
- **Port State**: Reports the current state of the PTP State Machine:
  - **Disabled**: PTP Ethernet port is Disabled. See PTP Setup/Network page, PTP Network Settings options.
  - **Initializing**: Ethernet link is unplugged/PTP Module is in power-up state. A Master Clock doesn’t leave this state while it can’t get the current time and synchronization references from the SecureSync to synchronize with it.
  - **Listening**: PTP module is looking for a Master Clock.
  - **Master**: PTP Master has become the active Master Clock on the network.

- **Passive**: PTP Module has become a Passive Master Clock. (There is another Master Clock on the network with better quality or higher priority). This Master will wait until the Best Master Clock Algorithm determines it should become the best Master Clock, and then it will transition to the Master Clock state.
- **Uncalibrated**: PTP Slave has selected a Master Clock on the network attempts to synchronize with it using sync packets.

- **Number of Unicast Slaves**: Number of PTP Slaves that have been granted by the PTP Master to run in unicast mode.
- **Profile**: Whether the profile is the default or Telecom.
- **Domain Number**: The current PTP Domain Number.
- **Clock Mode**: See "Main tab settings" on page 396.
- **Current IP Address**: The IP address currently being used by the PTP interface.
- **MAC Address**: The MAC address currently being used by the PTP interface.

Advanced tab: Status information

Time Properties:

- **UTC Offset**: The Master’s current offset between UTC time and TAI time. Units: seconds.
- **UTC Offset Valid**: Indicates whether or not the Master’s UTC Offset is valid.
- **Leap Second**: The Leap second correction as set on the **Time Management** page.
- **Time Traceable**: Indicates whether the Master’s time is traceable (Enabled) to a primary reference or not (Disabled).
- **Frequency Traceable**: Indicates whether the Master’s Frequency is traceable (Enabled) to a primary reference or not (Disabled).
- **PTP Time Scale**: Indicates the timescale that the Master is using to broadcast its time. TAI is the default PTP timescale.
- **Time source**: The Time Source that the Master is using. Refer to IEEE Standard 1588-2008, Section 7.6.2.6.

Clock Quality:

- **Clock Accuracy**: A number describing the accuracy of the oscillator in the Master relative to its UTC reference (see IEEE Standard 1588-2008, Section 7.6.2.5).
- **Offset Scaled Variance**: A constant value based on the variance of the oscillator installed in the SecureSync unit.
- **Clock Class**: A number describing the state of the time and 1pps references of the PTP Clock.
  See table below for Clock Class definitions (see also: IEEE Standard 1588-2008, Section 7.6.2.4, Table 5).

PTP Time Scale	Arbitrary Time Scale	Clock Class Definition
6	13	Time and 1pps references are synchronized with the host references and PTP clock shall not be a slave to another clock in the domain.
7	14	Time and 1pps references are in holdover state, within specifications and PTP clock shall not be a slave to another clock in the domain.
52	58	Time and 1pps references are in holdover state, not within specifications, and PTP clock shall not be a slave to another clock in the domain. Then, applied to Master Clocks who have just powered on and have not yet achieved a suitable TFOM value.
187	193	Time and 1pps references are in holdover state, not within specifications, and PTP clock may be a slave to another clock in the domain.
255	255	Class assigned to “Slave-Only” clocks.
248	248	“Unknown” class.

Table 5-22: Clock class definitions

Ethernet Status

- **Current IP Address**: The IP address currently being used by the PTP interface.

Note: If the PTP Module is set up for DHCP but fails to obtain an IP address, it will use the Static IP instead. To reacquire a DHCP address, reset the module via the Main tab in the PTP settings window.

- **Current Network Mask**: The Network Mask currently being used by the PTP interface.
- **Current Gateway**: The Gateway address currently being used by the PTP interface.

Port Status

- **Port State**: Reports the current state of the PTP State Machine:
  - **Disabled**: PTP Ethernet port is Disabled. See PTP Setup/Network page, PTP Network Settings options.
  - **Initializing**: Ethernet link is unplugged/PTP Module is in power-up state. A Master Clock doesn’t leave this state while it can’t get the current time and synchronization references from SecureSync to synchronize with it.
  - **Listening**: PTP module is looking for a Master Clock.
  - **Master**: PTP Master has become the active Master Clock on the network.
  - **Passive**: PTP Module has become a Passive Master Clock. (There is another Master Clock on the network with better quality or higher priority). This Master will

wait until the Best Master Clock Algorithm determines it should become the best Master Clock, and then it will transition to the Master Clock state.

- **Uncalibrated**: PTP Slave has selected a Master Clock on the network attempts to synchronize with it using sync packets.
- **One Step Mode**: Determines the number of steps in the PTP protocol. Will be one of the following:
  - **Disabled**: Two-Step Mode is enabled
  - **Enabled**: One-Step Mode is enabled
    [Default=Disabled]

  Note: One-Step Mode is not supported with the Peer-to-Peer Delay Mechanism.

  The current implementation of one-step mode involves a software oriented timestamping. The two-step mode imlements a hardware oriented timestamping, insensitive to software execution time variations. The Two-step mode is recommended, as it increases the PTP Clock's accuracy
- **Delay Mechanism**: Will be one of the following:
  - **E2E**: End-to-End Delay Mechanism
  - **P2P**: Peer-to-Peer Mechanism
  - **Disabled**: No Delay Mechanism
    Default setting: E2E

    Note: Peer-to-Peer Delay Mechanism is only applicable on networks equipped with Transparent Clocks (switches/routers IEEE 1588 compatible). Peer-to-Peer Delay Mechanism is not supported in Unicast transmission mode.
- **PPS Offset**: See "Advanced tab settings" on page 397.

Module Information

- **Software Version**: Version number of embedded software
- **Hardware Version:** Version number

5.5.2.4 Configuration – General Steps

- Ensure that SecureSync's PTP port is connected to the network (check the Link Status in the **PTP Status/Network** page).

- Ensure the PTP port speed is 100 Mb/s (see: **PTP Status** page > **Advanced** tab > **Port Speed**).
- Be sure that valid time and 1PPS references are currently selected (go to **MANAGEMENT/OTHER/Time Management**).

In order to operate properly as a Master Clock, SecureSync must be synchronized to a non-PTP reference. Confirm that the chosen reference transmits the following information (as reported by the Time Properties on the **PTP Status** page, under the **Advanced** tab):

- The proper TAI or UTC time (including the current year)
- The current TAI to UTC offset (required even if the reference's time is in TAI)
- Pending leap second information at least a day in advance.

If the reference does not transmit this information, it must be provided by the user in order for the Master Clock to function properly.

The built-in GNSS reference provides all information needed with no user intervention.

5.5.2.5 Configuration – PTP-Specific Steps

Confirm that:

- The PTP Port Activity is enabled (check the **Port Status** on the **PTP Status** page under the **Advanced** tab). If not, enable it from the **Port Activity** of the **PTP Setup/Network** page).
- The clock is set to be a Master-Only clock (check the **Clock Mode** on the **PTP Setup/Clock** page).
- A valid IP address is currently being used (check the **Ethernet Settings** on the **PTP Setup/Network** page).

When the PTP Module is set to be a Master Clock, the module will immediately attempt to become the active Master Clock on the network (**PTP Port State** = **Master**). If it does, it will start to transmit PTP packets (even if SecureSync is not yet synchronized).

There are several reasons why the PTP Module may not become the active Master Clock, or may not be broadcasting the correct time, even if it is set to be a Master Clock:

a. If using any reference other than self for 1PPS, SecureSync will not become an active Master Clock until the **Time Figure of Merit (TFOM)** value of the system is less than 15. After first going into sync after power-up, it may take a minute or two for the Time Figure of Merit (TFOM) value to fall to an acceptable level. The current Time Figure of Merit (TFOM) value is available in the Time Properties panel under the **Advanced** tab on the **Status** page.

b. PTP uses the TAI timescale to transfer time. Many timing references communicate time in the UTC timescale. UTC is offset from TAI by a small amount which changes every time a leap second occurs. The TAI to UTC Offset is part of the PTP Specification and must be provided to a Master Clock. If no active reference can provide that information, the offset must be provided by the Host. The TAI to UTC Offset can be set from the **MANAGEMENT/OTHER/Time Management** page (while setting the GPS to UTC Offset).

c. The PTP Protocol also provides for the transfer of Leap Second information. If the active time reference does not provide Leap Second information, it must be added by the user through the **MANAGEMENT/OTHER/Time Management** page. If this is not done, the PTP network will have the incorrect UTC time after a leap second event.

d. If there are multiple multicast Master Clocks on the network, the PTP Module uses the Best Master Clock (BMC) algorithm specified in the PTP Specification to decide whether or not to become the active Master Clock. The BMC algorithm selects the Best Master Clock on the network from the following criteria:

   i. The BMC algorithm first selects the clock having the higher Priority1 parameter (a lowest value means a higher priority)

   ii. If the BMC cannot be determined from the previous parameter, the BMC algorithm selects the clock having the higher Clock Quality (Clock Class, Clock Accuracy, Clock Variance)

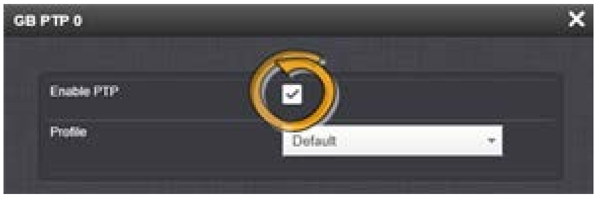
   iii. If the BMC cannot be determined from the previous parameters, the BMC algorithm selects the clock having the higher Priority2 parameter

The Master Clock selected by the BMC algorithm as the Best Master Clock will transition into the Master state to become the active Master Clock on the network. It will then start to transmit Sync packets to the Slave Clocks. The other Master Clocks will transition into the Passive state.

Enabling PTP

To enable PTP:

1. Navigate to the Top panel of the GB PTP Edit window.
2. Check the **Enable PTP** box.



GB PTP 0

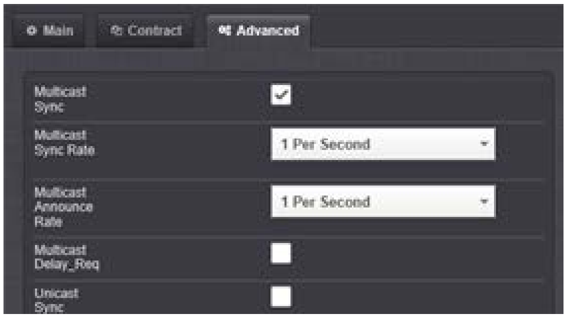
Enable PTP ☑

Profile Default

Configuring Multicast Mode

To enter Multicast mode, perform the following steps:

1. In the **GB PTP** Edit window, navigate to the **Advanced** tab.
2. Select the **Multicast Sync** checkbox.
3. Select the **Multicast Sync Rate** from the drop-down list.
4. Select the **Multicast Announce Rate** from the drop-down list.

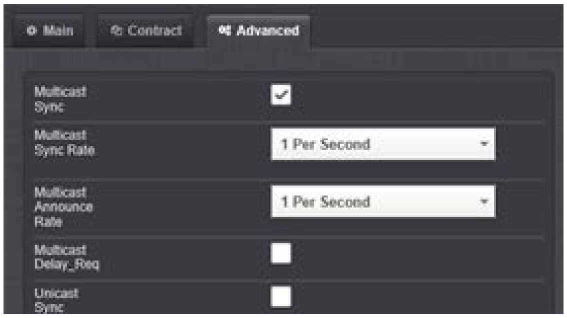


Multicast Sync	☑
Multicast Sync Rate	1 Per Second
Multicast Announce Rate	1 Per Second
Multicast Delay_Req	□
Unicast Sync	□

Configuring Unicast Mode

To enter the Unicast mode, perform the following steps:

1. In the GB PTP **Edit** window, navigate to the **Advanced** tab.
2. Confirm that **Unicast Sync** is checked. The 1204-32 PTP module should always respond to unicast negotiations.

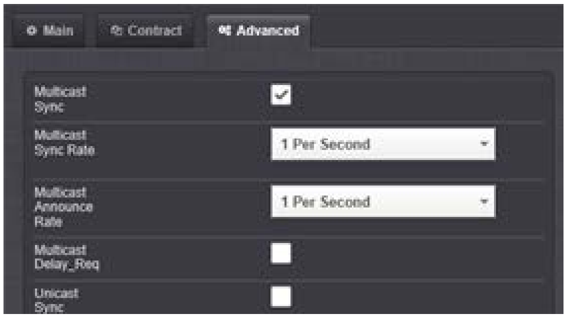


Multicast Sync	☑
Multicast Sync Rate	1 Per Second
Multicast Announce Rate	1 Per Second
Multicast Delay_Req	□
Unicast Sync	□

Configuring Minicast/Hybrid Mode

To enter the Minicast/Hybrid mode, perform the following steps:

1. In the GB PTP Edit window, navigate to the **Advanced** tab.
2. Select the **Multicast Sync** checkbox.
3. Select the **Multicast Sync Rate** from the drop-down list.
4. Select the **Multicast Announce Rate** from the drop-down list.
5. Confirm that the Unicast Sync checkbox is checked. The 1204-32 PTP module should always respond to unicast negotiations.



Multicast Sync ☑

Multicast Sync Rate: 1 Per Second

Multicast Announce Rate: 1 Per Second

Multicast Delay_Req □

Unicast Sync □

Configuring PTP on the Network

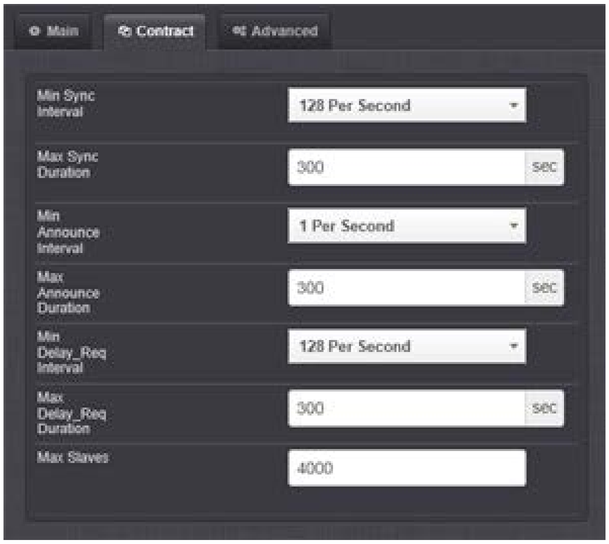
To configure PTP on the network:

1. In the GB PTP **Edit** window, navigate to the **Main** tab.
2. Under the **Main** tab of the **GB PTP** Edit window, make the following settings:

- **Domain Number**: Sets the current PTP Domain Number, as defined in IEEE Std 1588-2008 Section 7.1
- **Clock Mode**: See under "Main tab settings" on page 396.
- **Enable DHCP**: This is a checkbox to enable or disable the delivery of IP addresses from a DHCP Server. The default setting is enabled (the box is checked).
- **Static IP Address**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this IP address. In the format “#.#.#.#” with no leading zeroes or spaces, where each ‘#’ is a decimal integer from the range [0,255].
- **Network Mask**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this Network Mask. In the format “#.#.#.#” with no leading zeroes or spaces, where each ‘#’ is a decimal integer from the range [0,255].
- **Default Gateway**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this Default Gateway. In the format “#.#.#.#” with no leading zeroes or spaces, where each ‘#’ is a decimal integer from the range [0,255].

Configuring PTP Contracts

1. Navigate to the **Contract** tab of the **GB PTP** Edit window.



Min Sync Interval: 128 Per Second

Max Sync Duration: 300 sec

Min Announce Interval: 1 Per Second

Max Announce Duration: 300 sec

Min Delay_Req Interval: 128 Per Second

Max Delay_Req Duration: 300 sec

Max Slaves: 4000

2. Under the **Contract** tab of the GB PTP Edit window, make the following settings:

- **Min Sync Interval**: The minimum value of Sync interval granted by the Master Clock. In packets per second.
- **Max Sync Duration**: The maximum value of Sync interval granted by the Master Clock. In seconds.
- **Min Announce Interval**: The minimum value of the Announce interval granted by the Master Clock. In packets per second.
- **Max Announce Duration**: The maximum value of the Announce interval granted by the Master Clock. In seconds.
- **Min Delay_Req Interval**: In packets per second.
- **Max Delay_Req Duration**: In seconds.
- **Max Slaves**: The maximum number of slaves to be served. The 1204-32 module can serve up to 4000 slaves.

5.5.3 PTP Master/Slave [1204-12]

Precision Time Protocol (PTP) is a protocol that can be used to synchronize computers on an Ethernet network. The 10/100 PTP Master/Slave option card supports PTP Version 2, as specified in the IEEE 1588-2008 standard (PTP Version 1 is not supported), via one (1) Ethernet port.

The PTP option card implements a PTP Ordinary Clock that can be configured to run as:

- A **Master Clock**, in which case it transmits PTP packets via the Ethernet port, with information about the current time and synchronization reference selected by SecureSync.
- A **Slave Clock**, in which case it provides to the SecureSync device a time and synchronization reference retrieved from information carried by the PTP packets received via the Ethernet port.

- A **Master/Slave Clock**, in which case the PTP option card can change mode according to priority and quality criteria compared with the other PTP Clocks on the network.

5.5.3.1 PTP Master/Slave[1204-12]: Specifications

- **Inputs/Outputs**: (1) Configurable as Input or Output
- **Signal Type and Connector**: RJ-45
- **Management**: Web UI
- **Resolution**: 8ns (±4ns) packet time stamping resolution
- **Accuracy**: 30 ns accuracy (3σ) Master to Slave, via crossover cable
- **Networking speeds**: 10 Mb/s, 100 Mb/s
- Supported **PTP Versions**: PTP 2 (IEEE 1588-2008)
- **PTP Profiles** supported: Default
- **Transmission modes**: Unicast, Multicast [default]
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-12: PTP/Precision Timing Protocol Option Module

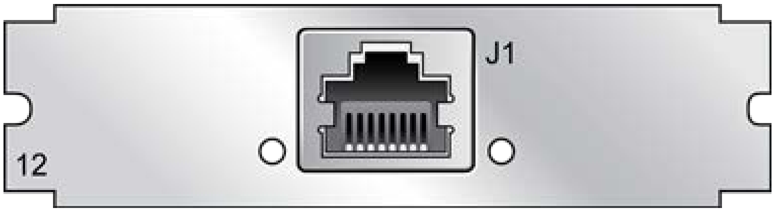
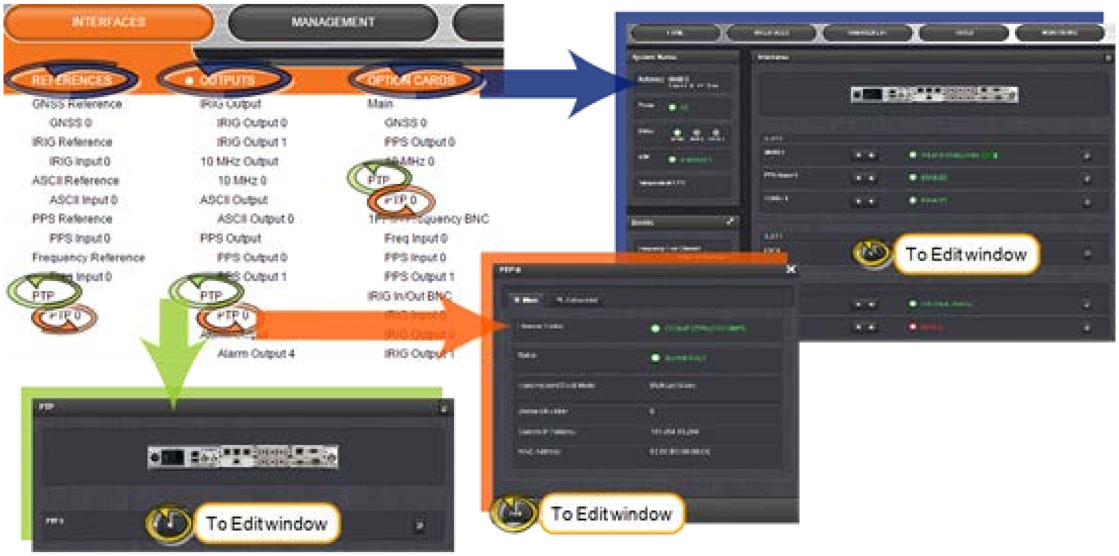


Figure 5-42: Model 1204-12 option card rear plate

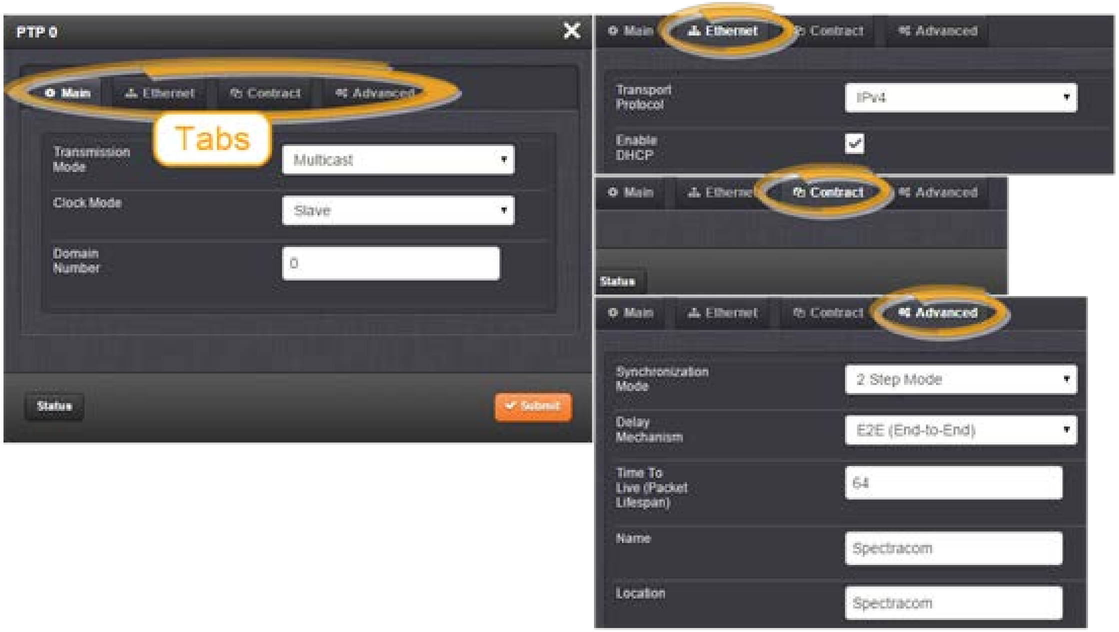
5.5.3.2 PTP Master/Slave [-12]: Edit Window

1. To configure this option card, go to its **Edit** window. For instructions, see "Configuring the Settings of an Input or Output" on page 295.



> **Note:** If you have only one input or output of any type, SecureSync will number that input or output 0. Additional inputs or outputs will be numbered 1 or above.

2. The **PTP Edit window** will display. It offers access to four different **tabs**, described below:



Transmission Mode: Multicast
Clock Mode: Slave
Domain Number: 0

Transport Protocol: IPv4
Enable DHCP: ☑

Synchronization Mode: 2 Step Mode
Delay Mechanism: E2E (End-to-End)
Time To Live (Packet Lifespan): 64
Name: Spectracom
Location: Spectracom

Main tab settings

Settings to configure under the **Main** tab:

- **Transmission Mode**: (See also: "Transmission Modes" on page 421)
  - Unicast
  - Multicast
  - Minicast
- **Clock Mode**: The Master/Slave Mode of the PTP Module. Will be one of:
  - Slave
  - Master
  - Disabled

  The default value is **Slave**.
- **Domain Number**: Sets the current PTP Domain Number, as defined in IEEE Std 1588-2008 Section 7.1. Range: [0,255]. Default setting: 0
- **Master Clock IP Address**: Static IP address of the unicast Master Clock. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].

Ethernet tab settings

Settings to configure under the **Ethernet** tab:

- **Transport Protocol**: Selects the transport protocol used for PTP Packets. Possible values are:
  - IPv4 (The default): Internet Protocol version 4 (Layer 3 protocol).
  - 802.3/Ethernet: IEEE802.3/Ethernet Protocol (Layer 2 protocol).

  Operating limitations: The IEEE802.3/Ethernet Protocol is not supported in Unicast transmission mode.
- **Enable DHCP**: This is a checkbox to enable or disable the delivery of IP addresses from a DHCP Server. The default setting is enabled (the box is checked).
- **Static IP Address**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this IP address. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].
- **Network Mask**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this Network Mask. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].
- **Default Gateway**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this Default Gateway. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].

Contract tab settings

Note: The settings under this tab only apply to Unicast Mode.

Settings to configure under the **Contract** tab:

- **Min Sync Interval**: The minimum value of Sync interval granted by the Master Clock. In packets per second.
- **Max Sync Duration**: The maximum value of Sync interval granted by the Master Clock. In seconds.
- **Min Announce Interval**: The minimum value of the Announce interval granted by the Master Clock. In packets per second.
- **Max Announce Duration**: The maximum value of the Announce interval granted by the Master Clock. In seconds.
- **Min Delay_Req Interval**: In packets per second.
- **Max Delay_Req Duration**: In seconds.
- **Max Slaves**: The maximum number of slaves the card will serve.

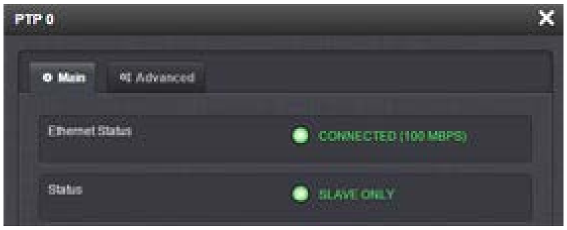
Advanced tab settings

Settings to configure under the **Advanced** tab:

- **Synchronization Mode**: Determines the number of steps in the PTP protocol. Will be either 1-Step Mode, or 2-Step Mode.
- **Delay Mechanism**: Determines how the protocol calculates delay [Default: End-to-End]
- **Time-To-Live** (Packet Lifespan): Ethernet characteristic, determining the number of routers a packet will go through [Spectracom default: 64].
- **Name**: Assign a name to this option card (Note: Used only by Managament Profile]
- **Location**: Assign a location to this option card (Note: Used only by Managament Profile]

5.5.3.3 PTP Master/Slave [-12]: Status Window

To view the status of a PTP interface, go to its Status window. For instructions, see "Viewing the Configuration of an Input or Output" on page 293.

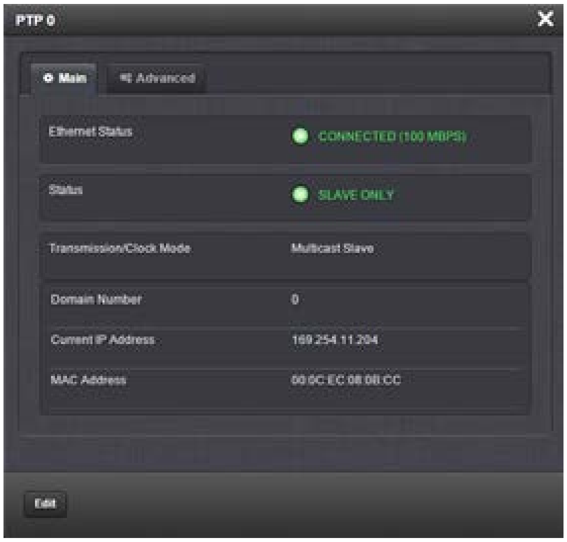


Ethernet Status ● CONNECTED (100 MBPS)

Status ● SLAVE ONLY

The **GB PTP** Status window contains two tabs: Main and Advanced.

Main tab: Status information

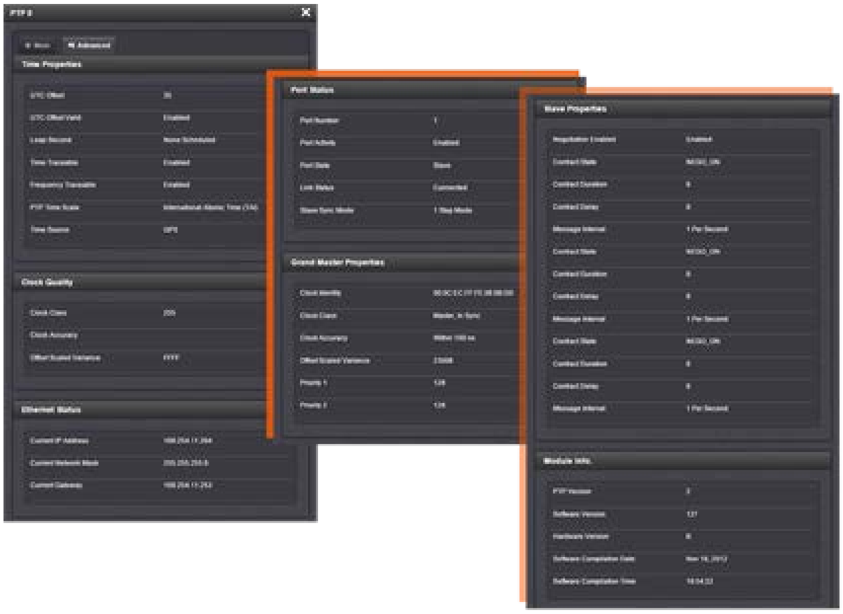


Ethernet Status	● CONNECTED (100 MBPS)
Status	● SLAVE ONLY
Transmission/Clock Mode	Multicast Slave
Domain Number	0
Current IP Address	169.254.11.204
MAC Address	00:0C:EC:08:08:CC

The **Main** tab provides the following information:

- **Ethernet Status**: Whether the module is connected to a network through Ethernet.
  - Green=Connected. The speed of the connection is indicated.
  - Orange=Not connected.
- **Status**: Master/Slave mode of the card.
- **Transmission/Clock Mode**: Transmission mode and master/slave mode.
- **Domain Number**: The current PTP Domain Number.
- **Current IP Address**: The IP address currently being used by the PTP interface.
- **MAC Address**: The MAC address currently being used by the PTP interface.

Advanced tab: Status information



Time Properties

UTC Offset	35
UTC Offset Valid	Enabled
Leap Second	None Scheduled
Time Traceable	Enabled
Frequency Traceable	Enabled
PTP Time Scale	International Atomic Time (TAI)
Time Source	GPS

Clock Quality

Clock Class	255
Clock Accuracy	
Offset Scaled Variance	FFFF

Ethernet Status

Current IP Address	169.254.11.254
Current Network Mask	255.255.255.0
Current Gateway	169.254.11.253

Port Status

Port Number	1
Port Activity	Enabled
Port State	Slave
Link Status	Connected
Slave Sync Mode	1 Step Mode

Grand Master Properties

Clock Identity	00:0C:EC:FF:FE:0B:0B:C0
Clock Class	Master, In Sync
Clock Accuracy	Within 100 ns
Offset Scaled Variance	23008
Priority 1	128
Priority 2	128

Slave Properties

Negotiation Enabled	Enabled
Contract State	NEGO_ON
Contract Duration	0
Contract Delay	0
Message Interval	1 Per Second
Contract State	NEGO_ON
Contract Duration	0
Contract Delay	0
Message Interval	1 Per Second
Contract State	NEGO_ON
Contract Duration	0
Contract Delay	0
Message Interval	1 Per Second

Module Info.

PTP Version	2
Software Version	121
Hardware Version	6
Software Compilation Date	Nov 16, 2012
Software Compilation Time	18:54:22

The **Advanced** tab provides the following information:

Time Properties:

- **UTC Offset**: The Master's current offset between UTC time and TAI time. Units: seconds.
- **UTC Offset Valid**: Indicates whether or not the Master's UTC Offset is valid.
- **Leap Second**: The Leap second correction as set on the **Time Management** page.
- **Time Traceable**: Indicates whether the Master's time is traceable (Enabled) to a primary reference or not (Disabled).
- **Frequency Traceable**: Indicates whether the Master's Frequency is traceable (Enabled) to a primary reference or not (Disabled).
- **PTP Time Scale**: Indicates the timescale that the Master is using to broadcast its time. TAI is the default PTP timescale.
- **Time source**: The Time Source that the Master is using. Refer to IEEE Standard 1588-2008, Section 7.6.2.6.

Clock Quality

- **Clock Accuracy**: A number describing the accuracy of the oscillator in the Master relative to its UTC reference. (See IEEE Standard 1588-2008, Section 7.6.2.5).
- **Offset Scaled Log Variance**: (Defined in IEEE Standard 1588-2008, Section 1.6.3)
- **Clock Class**: A number describing the state of the time and 1pps references of the PTP Clock.

Refer to the following table for Clock Class information (see IEEE standard 1588-2008, Table 5, Section 7.6.2.4).

PTP Time Scale	Arbitrary Time Scale	Clock Class Definition
6	13	Time and 1pps references are synchronized with the host references and PTP clock shall not be a slave to another clock in the domain.
7	14	Time and 1pps references are in holdover state, within specifications and PTP clock shall not be a slave to another clock in the domain.
52	58	Time and 1pps references are in holdover state, not within specifications, and PTP clock shall not be a slave to another clock in the domain. Then, applied to Master Clocks who have just powered on and have not yet achieved a suitable TFOM value.
187	193	Time and 1pps references are in holdover state, not within specifications, and PTP clock may be a slave to another clock in the domain.
255	255	Class assigned to “Slave-Only” clocks.
248	248	“Unknown” class.

Table 5-23: Clock Class definitions

Ethernet Status

- **Current IP Address**: The IP address currently being used by the PTP interface.

> Note: If the PTP Module is set up for DHCP but fails to obtain an IP address, it will use the Static IP instead. To reacquire a DHCP address, reset the module via the Main tab in the PTP settings window.

- **Current Network Mask**: The Network Mask currently being used by the PTP interface.
- **Current Gateway**: The Gateway address currently being used by the PTP interface.

Port Status

- **Port Number**: The PTP Port Number, as defined in the IEEE 1588-2008 Specification, Section 7.5.2.3. Always set to 1 for our Ordinary Clock.
- **Port Activity**: Reports whether or not the network interface is active for PTP (Enabled) or not (Disabled).
- **Port State**: Reports the current state of the PTP State Machine:
  - Disabled: PTP Ethernet port is Disabled. See PTP Setup/Network page, PTP Network Settings options.

  - Initializing: Ethernet link is unplugged/PTP Module is in power-up state. A Master Clock doesn't leave this state while it can't get the current time and synchronization references from the SecureSync to synchronize with it.
  - Listening: PTP module is looking for a Master Clock.
  - Master: PTP Master has become the active Master Clock on the network.
  - Passive: PTP Module has become a Passive Master Clock. (There is another Master Clock on the network with better quality or higher priority). This Master will wait until the Best Master Clock Algorithm determines it should become the best Master Clock, and then it will transition to the Master Clock state.
  - Uncalibrated: PTP Slave has selected a Master Clock on the network attempts to synchronize with it using sync packets.
- **Link Status**: Indicates whether or not the Ethernet link for PTP is active (Connected) or not (Disconnected).
- **Slave Sync Mode**: Determines the number of steps in the PTP protocol. Will be one of the following:
  - Two-Step Mode
  - One-Step Mode

  > **Note:** One-Step mode is not supported with the Peer-to-Peer Delay Mechanism.

  The current implementation of one-step mode involves a software-oriented timestamping. Two-step mode implements a hardware oriented timestamping, insensitive to software execution time variations. **Two-step mode is recommended**, as it increases the PTP Clock's accuracy.

> **Note:** Peer-to-Peer Delay Mechanism is only applicable on networks equipped with Transparent Clocks (switches/routers IEEE 1588 compatible). Peer-to-Peer Delay Mechanism is not supported in Unicast transmission mode.

Grandmaster Properties

Reports information from the current Grandmaster Clock. If the PTP Module is currently a Master, this will report information on the current module.

- **Clock Identity**: Displays the clock identity of the current Grandmaster Clock on the network.
- **Clock Class**: A number describing the state of the clock (see Table 5 of Section 7.6.2.4 of IEEE Standard 1588-2008).

- **Clock Accuracy**: A number describing the accuracy of the oscillator in the Grandmaster Clock (see IEEE Standard 1588-2008, Section 7.6.2.5).
- **Offset Scaled Log Variance**: See IEEE Standard 1588-2008 Section 7.6.3.
- **Priority1**: See IEEE Standard 1588-2008, Section 7.6.3.
- **Priority2**: See IEEE Standard 1588-2008, Section 7.6.3.

Slave Properties

- **Negotiation Enabled**: Reports whether the Unicast Negotiation option is Enabled or Disabled.
- **Contract State**: Reports the unicast contract state.
  - NEGO_OFF: Unicast negotiation option is Disabled.
  - NEGO_ON: Unicast negotiation option is Enabled.
  - REQUESTED: Unicast contract has been requested to the PTP Master.
  - GRANTED: Unicast contract has been granted by the PTP Master.
  - RENEWED: Renewal of the unicast contract has been requested to the PTP Master.
  - CANCELED: Cancellation of the unicast contract has been requested to the PTP Master.
- **Contract Duration**: Duration of the unicast contract. Units: Seconds.
- **Contract Delay**: Delay before the end of the unicast contract. Units: Seconds.
- **Message Interval**: Announce Interval negotiated for the unicast mode. Units: log2 seconds.
- **Contract State**: Reports the unicast contract state (see above ‘Announce Contract State’).
- **Contract Duration**: Duration of the unicast contract. Units: Seconds.
- **Contract Delay**: Delay before the end of the unicast contract. Units: Seconds.
- **Message Interval**: Sync Interval negotiated for the unicast mode. Units: log2 seconds.
- **Contract State**: Reports the unicast contract state (see above ‘Announce Contract State’).
- **Contract Duration**: Duration of the unicast contract. Units: Seconds.
- **Contract Delay**: Delay before the end of the unicast contract. Units: Seconds.
- Log Message Interval: Delay_Resp Interval negotiated for the unicast mode. Units: log2 seconds

Master Properties

- **Unicast Negotiation**: Reports whether the Unicast Negotiation option is Enabled or Disabled.
- **Number of Slave Clocks Connected**: Number of PTP Slaves that have been granted by the PTP Master to run in unicast mode.

Module Info

- **PTP Version**: Current version of PTP being used.
- **Software Version**: Current software revision level
- **Hardware Version**: Current hardware revision level.
- **Software Compilation Date**: Date the software was compiled.
- **Software Compilation Time**: Time the software was compiled

5.5.3.4 Configuring the [-12] PTP Master/Slave Card

Configuration as a Slave Clock

By default, the PTP card is configured to function as a Multicast PTP Slave, which allows a SecureSync to be able to synchronize to a Multicast PTP Master (such as another SecureSync unit with a PTP module option card configured as a Master) when configured with the following parameters:

- **Announce Interval** = once every 4 seconds or faster (This is set in the **PTP Edit** window, under the **Contract** tab).
- **Delay Mechanism** = End-to-End (This is set in the **PTP Edit** window, under the **Advanced** tab).
- **Transmission Mode** = Multicast (This is set in the **PTP Edit** window, under the **Main** tab).
- **Synchronization Mode** = Two-Step Mode faster (This is set in the **PTP Edit** window, under the **Advanced** tab).

When first connected to a network that contains an active Master Clock, it may take up to a minute for the Port State to change to the “slave” state. After that, it will take up to two minutes for the PTP connection to be accepted as a valid reference by SecureSync.

If SecureSync is not entering the “Slave” Port state (as reported by the **Main** tab on the **PTP Status** page), check the following:

- From the **PTP** Status window under the **Main** tab, check that **Ethernet Status** indicates “Connected.”
- From the **PTP** Status window under the **Advanced** tab, check that **Port Activity** indicates “Enabled.”
- From the **PTP** Status window under the **Main** tab, check that the **Ethernet Status** indicates a speed of 100 Mb/s.
- From the **PTP** Status window under the **Main** tab, check that the clock is set to be a **Slave Only**.
- From the **PTP** Status window under the **Main** tab, check that the **Transmission/Clock Mode** is a **Slave** mode and that multicast/unicast/minicast state is correct.

- Check that the **Ethernet Transport Protocol** set for the **Slave Clock** is the same as the Transport Protocol of the Master Clock to which the Slave Clock must be synchronized with. (Check the **Transport Protocol** on the **PTP** Edit window, under the **Ethernet** tab.)
- Check that the **Domain Numbe**r set for the **Slave Clock** is the same as the Domain Number of the Master Clock to which the Slave Clock must be synchronized with. (Check the Domain Number on the **PTP** Status window, under the **Main** tab.)
- From the **PTP** Status window, under the **Advanced** tab, check that the **Current IP Address** is valid.
- From the **PTP** Edit window under the **Advanced** tab, check that the **Time To Live** (TTL) for PTP packets is compatible with the network.
- If in **Multicast** mode, check that the switches/routers are transparent to multicast frames
- From the **PTP** Status window under the **Advanced** tab, check that the **Clock Class** is “Master, In Sync.”

Note: If DHCP is enabled and PTP was not successful in obtaining an IP address, DHCP will need to be restarted to retry. To restart DHCP:

1. In the **PTP** Edit window under the **Ethernet** tab, select the **Enable DHCP** checkbox.
2. Click the Submit button at the bottom of the window.

Configuration as a Master Clock

To configure the IEEE-1588 (PTP) Module as a Master Clock, perform these steps:

General configuration steps:

- Ensure the PTP port is connected to the network (check the **Link Status** in the **PTP Status/Network** page).
- Ensure the PTP port speed is 100 Mb/s (check the **Port Speed** in the **PTP** Status page under the **Advanced** tab).
- Be sure that valid time and 1PPS references are currently selected (go to **MANAGEMENT/OTHER/Time Management**).

In order to operate properly as a Master Clock, SecureSync must be synchronized to a non-PTP reference. Confirm that the chosen reference transmits the following information (as reported by the Time Properties on the **PTP** Status page, under the **Advanced** tab):

- The proper TAI or UTC time (including the current year)
- The current TAI to UTC offset (required even if the reference’s time is in TAI)
- Pending leap second information at least a day in advance.

If the reference does not transmit this information, it must be provided by the user in order for the Master Clock to function properly.

The built-in GNSS reference provides all information needed with no user intervention.

PTP-specific configuration steps:

Confirm that:

- From the **PTP** Status window under the **Advanced** tab, check that **PTP Port Activity** is enabled (if not, enable it from the PTP Edit window, under the Ethernet tab).
- From the **PTP** Edit window under the **Main** tab, check that the clock is set to be a **Master**.
- From the **PTP** Status window under the **Main** tab, check that a valid IP address is currently being used.

When the PTP Module is set to be a Master Clock, the module will immediately attempt to become the active Master Clock on the network (**Port State = Master**). If it does, it will start to transmit PTP packets (even if the SecureSync is not yet synchronized).

There are several reasons why the PTP Module may not become the active Master Clock, or may not be broadcasting the correct time, even if it is set to be a Master Clock:

a. If using any reference other than self for 1PPS, the SecureSync will not become an active Master Clock until the **Time Figure of Merit** (**TFOM**) value of the system is less than 15. After first going into sync after power-up, it may take a minute or two for the Time Figure of Merit (TFOM) value to fall to an acceptable level. The current Time Figure of Merit (TFOM) value is available in the **Time Properties** panel under the **Advanced** tab on the **PTP Status** window page.

b. PTP uses the TAI timescale to transfer time. Many timing references communicate time in the UTC timescale. UTC is offset from TAI by a small amount which changes every time a leap second occurs. The TAI to UTC Offset is part of the PTP Specification and must be provided to a Master Clock. If no active reference can provide that information, the offset must be provided by the Host. The TAI to UTC Offset can be set from the **MANAGEMENT/OTHER/Time Management** page (while setting the GPS to UTC Offset).

c. The PTP Protocol also provides for the transfer of Leap Second information. If the active time reference does not provide Leap Second information, it must be added by the user through the **MANAGEMENT/OTHER/Time Management** page. If this is not done, the PTP network will have the incorrect UTC time after a leap second event.

d. If there are multiple multicast Master Clocks on the network, the PTP Module uses the Best Master Clock (BMC) algorithm specified in the PTP Specification to decide whether or not to become the active Master Clock. The BMC algorithm selects the Best Master Clock on the network from the following criteria:

   i. The BMC algorithm first selects the clock having the higher Priority1 parameter (a lowest value means a higher priority)

   ii. If the BMC cannot be determined from the previous parameter, the BMC algorithm selects the clock having the higher Clock Quality (Clock Class, Clock Accuracy, Clock Variance)

   iii. If the BMC cannot be determined from the previous parameters, the BMC algorithm selects the clock having the higher Priority2 parameter

The Master Clock selected by the BMC algorithm as the Best Master Clock will transition into the Master state to become the active Master Clock on the network. It will then start to transmit Sync packets to the Slave Clocks. The other Master Clocks will transition into the Passive state.

Configuring Unicast Mode

For information on Unicast mode, see "Transmission Modes" on the facing page.

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

To enter the Unicast mode, perform the following steps:

On the Master side:

- In the **PTP** Edit window under the **Main** tab, select **Multicast** for the **Transmission Mode**. Enable the **Unicast** mode.

On the Slave side:

- In the **PTP** Edit window under the **Main** tab, select **Multicast** for the **Transmission Mode**. Enable the **Unicast** mode.

When the Master Clock is set in multicast mode, this one will deny the requests from the Slaves Clocks to run in Unicast mode.

When the Master Clock is set in Unicast mode, it does not transmit any PTP messages until a Slave has been granted to run in Unicast mode.

The Model 1204-12 card can grant up to 128 Unicast contracts (i.e., it can handle up to a total of 128 PTP clients). [Note that the 1204-32 Gb PTP card can handle up to 4000 Unicast contracts.]

The Model 1204-12 does not support mixing Unicast and Multicast clients on the same domain (Unlike the 1204-32 Option Card). When using the 1204-12 PTP card with Unicast clients, all clients need to be configured to use Unicast mode.

Note: The Unicast mode is only implemented for the following PTP packets:

- Announce
- Sync and Follow-Up
- Delay_Req and Delay_Resp

Configuring Master/Slave Mode

The PTP Master/Slave option card [-12] also supports a combined Master/Slave mode. The Master/Slave mode works best in a SecureSync which is not synchronized to any other reference. When the module is plugged into the PTP network, it will become a slave to the Best Master Clock on the network.

If all Master Clocks are removed from the network, the SecureSync containing the Master/Slave module will go into Holdover mode. However, the module will use that Holdover time to become the Best Master Clock on the network, and it will provide time to the network until the SecureSync's **Holdover Timeout** expires. If another Master Clock comes online and becomes the

Best Master Clock, the Master/Slave module will become a Passive Master Clock until the SecureSync's Holdover Timeout expires.

For more information on Holdover Mode, refer "Holdover Mode" on page 195.

Note: The Master/Slave mode is NOT supported in Unicast transmission mode.

Configuring Minicast Mode

For information on Minicast mode, see "Transmission Modes" below.

On the Master side:

» In the **PTP** Edit window under the **Main** tab, select **Multicast** for the **Transmission Mode**. Enable the **Minicast** mode.

On the Slave side:

» In the **PTP** Edit window under the **Main** tab, select **Multicast** for the **Transmission Mode**. Enable the **Minicast** mode.

5.5.3.5 Transmission Modes

Multicast Mode

This is the default mode. PTP packets are transmitted to all PTP Clocks by means of multicast IP addresses dedicated to the PTP protocol (224.0.1.129, 224.0.0.107). PTP packets received by the PTP Clocks are then filtered from the Domain Number, the Port Identity (Clock Identity + Port Number) of the transmitter, the packet identifier (Sequenced).
When the Master Clock is set in multicast mode, this module will deny the requests from the Slaves Clocks to run in unicast mode.

When the Master Clock is set in Unicast mode, it doesn't transmit any PTP messages until a Slave has been granted to run in unicast mode.

Unicast Mode

This is a Point-to-Point transmission mode between two PTP Clocks by means of the unique IP address assigned to each PTP Clock.

Note: The Unicast mode is only implemented for the following PTP packets:

- Announce
- Sync and Follow-Up
- Delay_Req and Delay_Resp

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

Minicast/Hybrid Mode

The Minicast/Hybrid mode is a method to minimize the PTP packets payload on the network, where:

- The transmissions initiated by the Master (Announce, Sync/Follow-Up) run in multicast mode.
- The transmissions initiated by the Slaves (Delay_Req/Delay_Resp) run in unicast mode.

5.6 Miscellaneous Option Cards

This section contains technical information and SecureSync Web UI procedures pertaining to option cards that do not fall into other categories, e.g. cards that serve as signal relays.

5.6.1 Alarm Relay Out [1204-0F]

The Model 1204-0F Alarm Relay Option Card provides three (3) configurable relay outputs for the SecureSync platform.

5.6.1.1 Alarm Relay Out [1204-0F]: Specifications

- **Inputs/Outputs**: (3) three contact relay connections (NC, common, NO)
- **Signal Type and Connector**: Terminal block
- **Contacts** switch under max. load of 30 VDC, 2A
- **Contacts** rated to switch: 220 VDC
- Nominal **Switch Capacity**: 30 V, 2A
- Maximum **switch voltage**: 220 VDC
- Maximum **switch power**: 60 W
- Maximum **switch current**: 2A
- **Breakdown voltage**: 1000 VDC between contacts
- **Switch time**: 4ms, max.
- **Maximum Number of Cards**: 1
- **Ordering Information**: 1204-0F: Relay Outputs Module

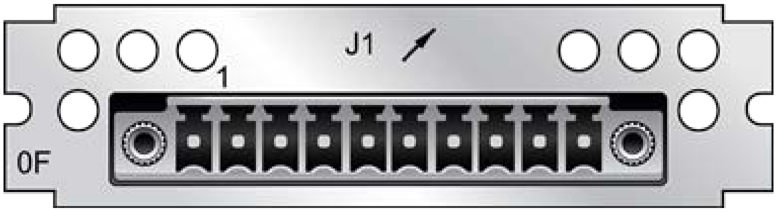


Figure 5-43: Model 1204-0F option card rear plate

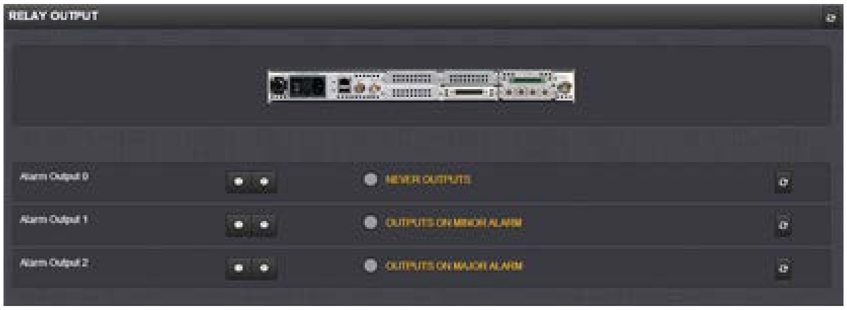
Pin Assignments

PIN	SIGNAL
1	GND
2	Relay 0 NO
3	Relay 0 NC
4	Relay 0 COMMON
5	Relay 1 NO
6	Relay 1 NC
7	Relay 1 COMMON
8	Relay 2 NO
9	Relay 2 NC
10	Relay 2 COMMON

Table 5-24: Terminal block pin-out, alarm relay out

5.6.1.2 Alarm Relay Output: Viewing Signal State

To quickly view the signal state of all three alarm outputs, see: "Viewing the Signal State of an Input or Output" on page 296.



RELAY OUTPUT

Alarm Output 0	NEVER OUTPUTS
Alarm Output 1	OUTPUTS ON MINOR ALARM
Alarm Output 2	OUTPUTS ON MAJOR ALARM

Each alarm output will be in one of these 3 states:

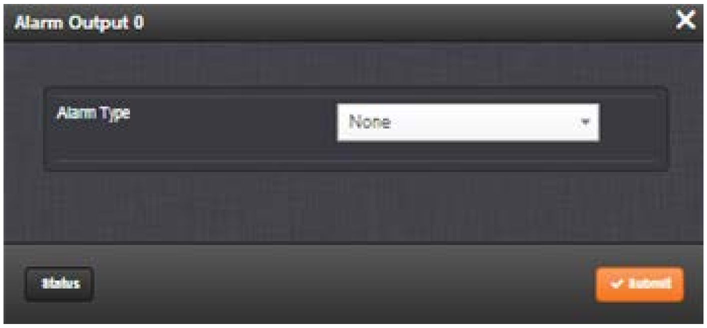
- NEVER OUTPUTS
- OUTPUTS ON MINOR ALARM
- OUTPUTS ON MAJOR ALARM

5.6.1.3 Alarm Relay Output: Edit Window

To configure the Alarm Relay Output, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entry for this card is: **Relay Output**. The name of the output is: **Alarm Output [number].**

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).


Alarm Output 0

Alarm Type: None

The Edit window allows the configuration of the following settings:

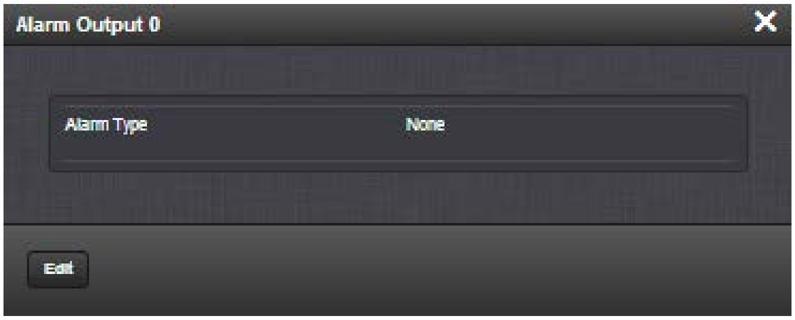
- **Alarm Type**:
  - None–Will not output for an alarm.
  - Minor–Will output on a minor alarm.
  - Major–Will output on a major alarm.

5.6.1.4 Alarm Relay Output: Status Window

To view the current settings of an Alarm Relay Output, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entry for this card is: **Relay Output**. The name of the output is: **Alarm Output [number]**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).


Alarm Output 0

Alarm Type None

The Status window displays the following settings:

- **Alarm Type**:
  - None–Will not output for an alarm.
  - Minor–Will output on a minor alarm.
  - Major–Will output on a major alarm.

5.6.2 Revertive Selector Card [1204-2E]

The Revertive Selector Option Card provides automatic failover capability, using one option card slot for a single output signal.

Operating Principle

The output follows the selected input. Signals can be 1PPS, 10 MHz, 5MHz or 1MHz.

Input “A” is selected if present and valid. If input “A” disappears, or if power to host SecureSync is interrupted, input “B” is presented at output “OUT”.

As soon as input “A” becomes valid again, the output switches back to use “A” as source.

At power-up or module reset, there is a timed delay before input “A” is presented. This allows reference at input “A” to stabilize before being used.

5.6.2.1 Model 1204-2E Specifications

- **Inputs/Outputs**:
  - (2) Inputs - Unselected input terminated with 50 Ω
  - (1) Output
- **Connectors**: 3 BNC
- **Signal Type**: User selected (jumper switch):
  - >1MHz
  - 1MHz to 100 Hz
  - 1PPS
- **Signal Level**:
  - Sine Wave, 0.5 V to 30 V_{p-p}
  - TTL (50 Ω)
- **Default Power-on Switch State**:
  Initially, **input “B”**; until a valid signal on input "A" is detected, causing the switch state to change to **"A"**.
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-2E: Revertive Selector Option Module

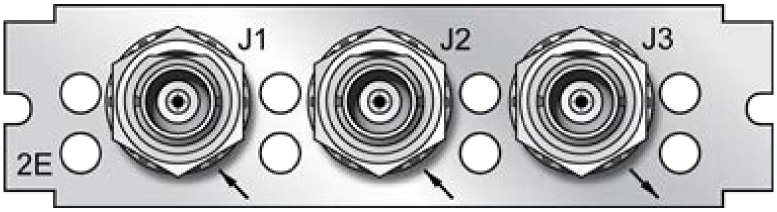


Figure 5-44: Model 1204-2E option card rear plate

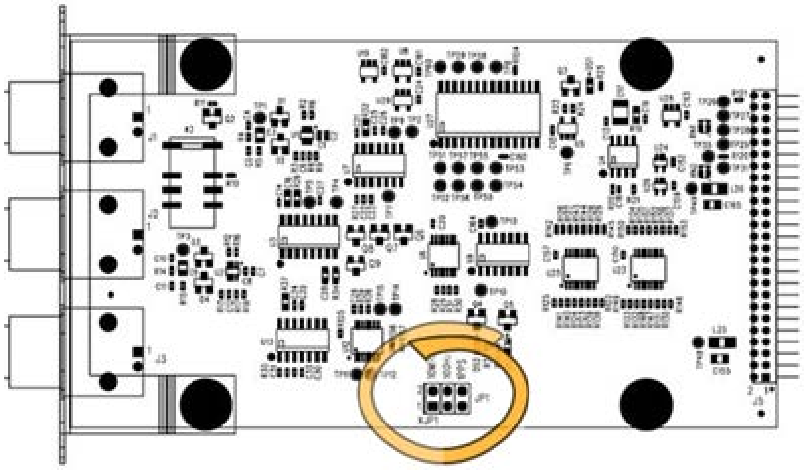


Figure 5-45: Location of jumper switches

5.6.3 Event Broadcast [1204-23]

The Event Broadcast Module (RS-232) provides a BNC connection for an Event Trigger Input and a RS-232 connector for an ASCII message output.

When the defined signal edge is detected on the **Event Input** BNC Connector, an ASCII message is created containing the current time.

ASCII messages are stored in a **Message Buffer**. The message buffer can store 512 entries before overflowing. Messages may be lost if the buffer overflows.

Messages can be output in one of two ways:

- If the **Mode** is set to Broadcast, messages in the **Message Buffer** will be output immediately through the RS-232 Output port. If another event is captured while a message is being sent, it will be queued in the buffer until the first message completes, then the next message will be sent.
- If the **Mode** is set to Request, messages in the **Message Buffer** are only sent when the Request Character is received.

The output format used is selected among a small group of formats with the capability to output data at 5ns resolution. Event Broadcast Output formats are detailed in "ASCII Time Code Data Formats" on page 474.

5.6.3.1 Event Broadcast [1204-23]: Specifications

- **Inputs/Outputs**: (1) Event Trigger Input, (1) Event Broadcast Output
- **Signal Type and Connector**:
  - Connector J1 - (RS-232 Output) RS-232 DB9F
  - Connector J2 - (Event Input) TTL BNC
- **Event Resolution**: 5ns
- **Minimum Time Between Events**: 20 ns
- **Message Buffer Size**: 512 messages
- **Ordering Information**: 1204-23: Event Broadcast

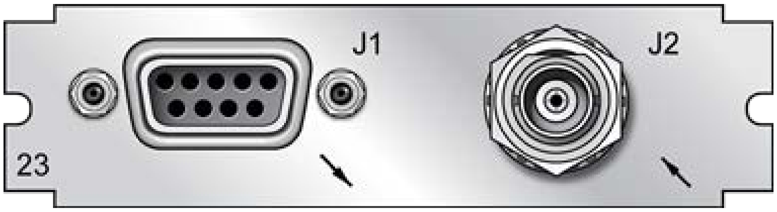


Figure 5-46: Model 1204-23 option card rear plate

Output Port: Pin Assignments

Pin Number	Signal Name	Function
Top row of 5 pins		
1	NC	No Connection
2	SERIAL_OUT_TX	RS-232 Transmit data
3	SERIAL_OUT_RX	RS-232 Receive data
4	NC	No connection
5	GND	Ground
Bottom row of 4 pins		
6	NC	No connection
7	NC	No connection
8	NC	No connection
9	NC	No connection

Table 5-25: Output connector DB-9: pin-out

5.6.3.2 Viewing the State of Event Broadcast and Event Input

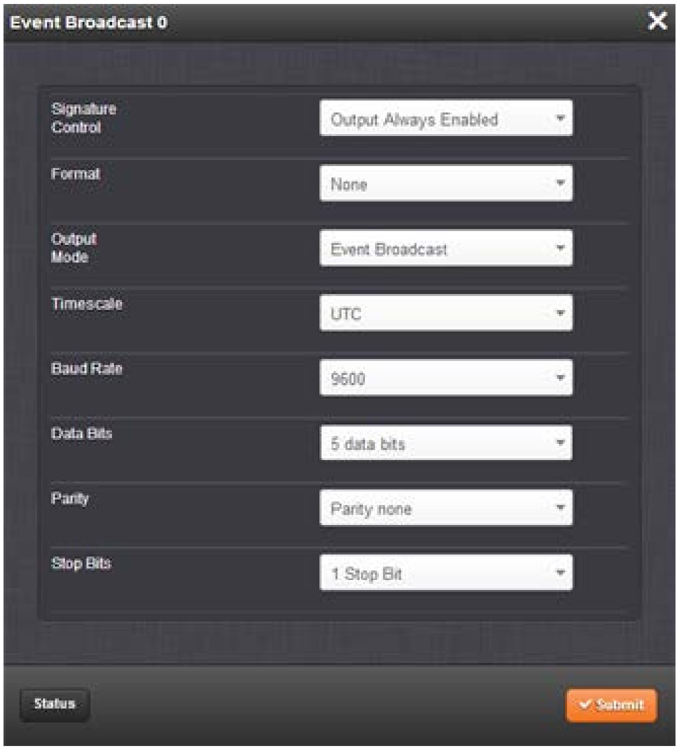
To view the Status of Event Broadcast and Event Input, see "Viewing the Signal State of an Input or Output" on page 296.

5.6.3.3 Event Broadcast Output: Edit Window

To configure the **Event Broadcast Output**, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entry for this card is: **Event Broadcast**.

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Signature Control	Output Always Enabled
Format	None
Output Mode	Event Broadcast
Timescale	UTC
Baud Rate	9600
Data Bits	5 data bits
Parity	Parity none
Stop Bits	1 Stop Bit

The Edit window allows the configuration of the following settings:

- **Signature Control**: Signature Control controls when messages will be broadcast in response to events on the Event Input (J2) port when events are enabled and the card is in "broadcast" mode. (Events are still queued even if they are not broadcast, and are transmitted once the signature control conditions permit.) For more information on Signature Control, see "Signature Control" on page 201.
- **Format**: Selects the format of the message to be outputted. Refer to "ASCII Time Code Data Formats" on page 474 for a description of all of the available formats.
  The Event Broadcast card only supports two formats (Event Broadcast Format 0 and Event Broadcast Format 1), and only supports the output of one message per event. If format is set to "None", no messages will be queued in the Message Buffer.
- **Output Mode**: This field determines when the output data will be provided. Available Mode selections are as follows:
  - **Broadcast**–Event Messages are automatically broadcast when they are created by an event. If a new event happens while an older message is being broadcast, the new message will be queued in a "First-in, First-out" manner. When the message has finished, the next message out of the queue will be broadcast.
  - **Request**–Event Messages are only broadcast in response to a Request Character. New messages will be queued in a "First-in, First-out" manner.
- **Request character**: This field defines the character that SecureSync needs to receive in order for a message to be provided when in "Request" mode. This field will only appear if the Output Mode is set as "Request Broadcast."

- **Timescale**–Used to select the time base for the incoming ASCII time code data. The entered Timescale is used by the system to convert the time in the incoming ASCII data stream to UTC time for use by the System Time. The available choices are:
- **UTC**–Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
- **TAI**–Temps Atomique International
- **GPS**–The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC time)
- A **local clock** set up through the Time Management Page–This option will appear under the name of the local clock you have set up. Refer to "The Time Management Screen" on page 169for more information on configuring and reading the System Clock. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

> Note: The Timescale of the input (as configured in the ASCII time source) must be set correctly, especially if other input references are enabled. Failure to configure the Timescale of the input correctly could result in time jumps occurring in the System Time when input reference changes occur. These time jumps could affect NTP and normal operation of the system.

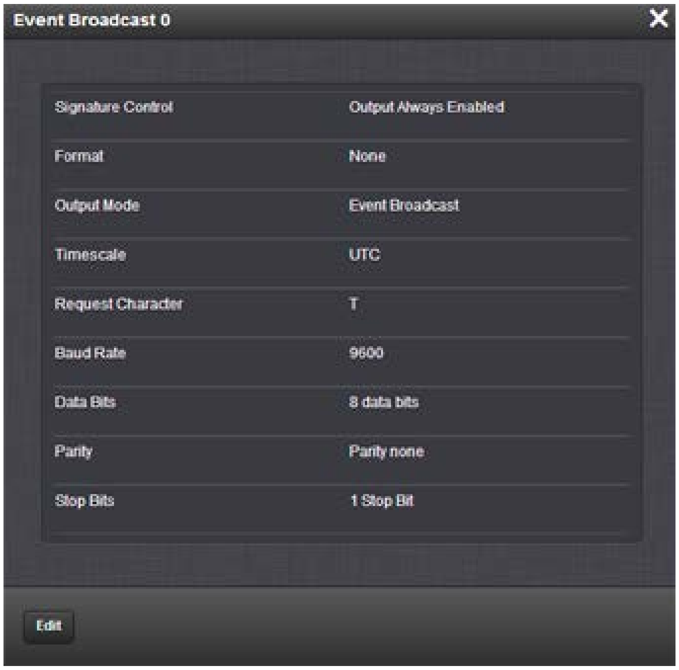
- **Baud Rate**: Determines the speed that the output port will operate at.
- **Data Bits**: Defines the number of Data Bits for the output port.
- **Parity**: Configures the parity checking of the output port.
- **Stop Bits**: Defines the number of Stop Bits for the output.

5.6.3.4 Event Broadcast Output: Status Window

To view the current settings of the **Event Broadcast Output**, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entry for this card is: **Event Broadcast**.

> Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Event Broadcast 0

Signature Control	Output Always Enabled
Format	None
Output Mode	Event Broadcast
Timescale	UTC
Request Character	T
Baud Rate	9600
Data Bits	8 data bits
Parity	Parity none
Stop Bits	1 Stop Bit

The Status window displays the following settings:

- **Signature Control**: Signature Control controls when messages will be broadcast in response to events on the Event Input (J2) port when events are enabled and the card is in “broadcast” mode. (Events are still queued even if they are not broadcast, and are transmitted once the signature control conditions permit.) For more information on Signature Control, see "Signature Control" on page 201.
- **Format**: The format of the message to be output. Refer to "ASCII Time Code Data Formats" on page 474 for a description of all of the available formats.
  The Event Broadcast card only supports two formats (Event Broadcast Format 0 and Event Broadcast Format 1), and only supports the output of one message per event. If format is set to “None”, no messages will be queued in the Message Buffer.
- **Output Mode**: When the output data will be provided. Available Mode selections are as follows:
  - **Broadcast**–Event Messages are automatically broadcast when they are created by an event. If a new event happens while an older message is being broadcast, the new message will be queued in a “First-in, First-out” manner. When the message has finished, the next message out of the queue will be broadcast.
  - **Request**–Event Messages are only broadcast in response to a Request Character. New messages will be queued in a “First-in, First-out” manner.
- **Timescale**: The time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - UTC–Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time

- TAI–Temps Atomique International
- GPS–The raw GPS time as transmitted by the GNSS satellites (as of July, 2015, this is 17 seconds ahead of UTC time).
- A local clock set up through the Time Management Page–This option will appear under the name of the local clock you have set up. Refer to "The Time Management Screen" on page 169 for more information on configuring and reading the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

Note: The Timescale of the input (as configured in the time source) must be set correctly, especially if other input references are enabled. Failure to configure the Timescale of the ASCII input correctly could result in time jumps occurring in the System Time when input reference changes occur. These time jumps could affect NTP and normal operation of the system.

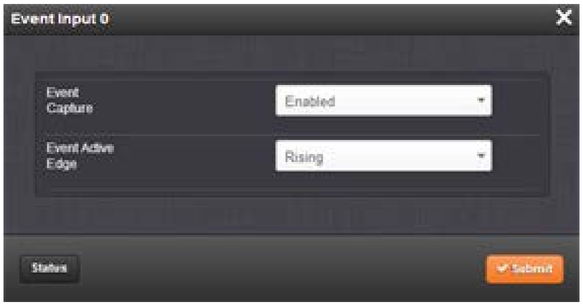
- **Request character**: This field defines the character that SecureSync needs to receive in order for a message to be provided when in “Request” mode. This field will only appear if the Output Mode is set as “Request Broadcast.”
- **Baud Rate**: The speed that the output port will operate at.
- **Data Bits**: The number of Data Bits for the output port.
- **Parity**: The parity checking of the output port.
- **Stop Bits**: The number of Stop Bits for the output.

5.6.3.5 Event Broadcast Input: Edit Window

To configure the **Event Broadcast Input** (also referred to as ‘**Reference**’), go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entry for this card is: **Event Broadcast**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Event Input 0

Event Capture: Enabled

Event Active Edge: Rising

The Status window displays the following settings:

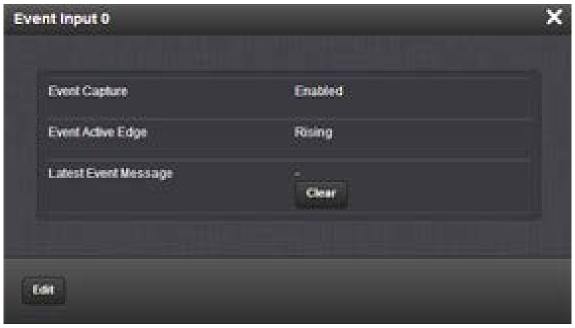
- **Event Capture**: Enables the processing of events on the Event Input port J2. When set to “Disabled”, no event messages will be queued. When set to “Enabled”, event messages will be triggered (if a valid Format is selected).
- **Event Active Edge**: Selects the signal edge used for triggering events on Event Input port J2.

5.6.3.6 Event Broadcast Input: Status Window

To view the current settings of the **Event Broadcast Input**, (also referred to as ‘**Reference**’), go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entry for this card is: **Event Broadcast**.

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



Event Input 0

Event Capture	Enabled
Event Active Edge	Rising
Latest Event Message	-

The Status window displays the following settings:

- **Event Capture**: The processing of events on the Event Input port J2. When set to “Disabled”, no event messages will be queued. When set to “Enabled”, event messages will be triggered (if a valid Format is selected).
- **Event Active Edge**: The signal edge used for triggering events on Event Input port J2.
- **Latest Event Message**: The last message sent. This can be cleared with the Clear button.

5.6.3.7 Event Broadcast Time Code Formats

The following ASCII-based time code formats are used with the Event Broadcast option card (see "Event Broadcast [1204-23]" on page 426.

Event Broadcast Format 0

Example message:

SSSSSSSSSS.XXXXXXXXX<CR><LF>

Where:

SSSSSSSSSS	10-digit Seconds Time (references from January 1st, 1970)
.	Decimal Point Separator
XXXXXXXXX	9-digit Sub-Seconds Time (5 ns resolution)
CR	Carriage Return
LF	Line Feed

Event Broadcast Format 1

Example message

YYYY DDD HH:MM:SS.XXXXXXXXX<CR><LF>

Where:

YYYY	Year
	Space Separator
DDD	Day of Year (001-366)
	Space Separator
HH	Hour of the Day (00-23)
:	Colon Separator
MM	Minutes of the Hour (00-59)
:	Colon Separator
SS	Seconds (00-59), (00-60 for leap second)
.	Period Separator
XXXXXXXXX	9-digit Sub-Seconds Time (5 ns resolution)
CR	Carriage Return
LF	Line Feed

5.6.4 Bi-Directional Communication, RS-485 [1204-0B]

- **Inputs/Outputs**: Bi-directional Communication Port
- **Signal Type and Connector**: Balanced RS-485 (3.8 mm terminal block)
- **Maximum Number of Cards**: 1
- **Ordering Information**: 1204-0B: RS-485 Communications Module

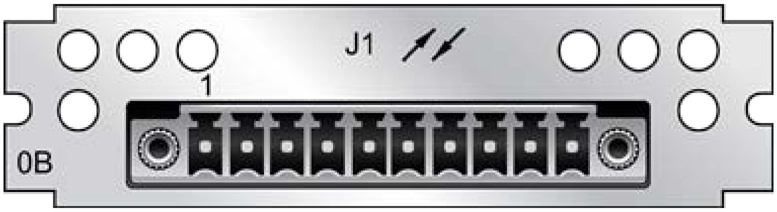


Figure 5-47: Model 1204-0B option card rear plate

Pin Assignments	
Pin No.	Signal
1	GND
2	RS-485 IN+
3	RS-485 IN-
4	GND
5	RS485 OUT+

Pin Assignments	
Pin No.	Signal
6	RS485 OUT-
7	GND
8	NC
9	NC
10	NC

Table 5-26: Model 1204-0B: RS-485 pin-out

Once an address has been assigned to it, the communication port can be operated as input or output (via CLI).

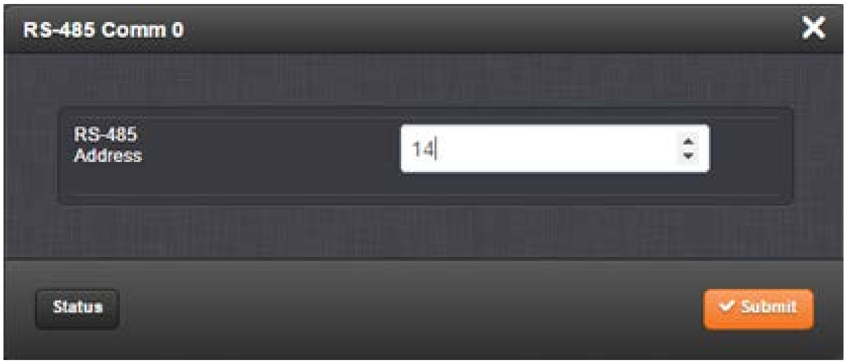
5.6.4.1 Communication Input/Output: Edit Window

To configure the Communication port's settings, go to its Edit window. For instructions, see: "Configuring the Settings of an Input or Output" on page 295.

The Web UI list entry for this card is: **RS-485 Comm**.

The name of the Input/Output is: **RS-485 Comm [number]**.

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



RS-485 Comm 0

RS-485 Address: 14

The Edit window allows the configuration of the following settings:

- **RS-485 Address**: [0-31]

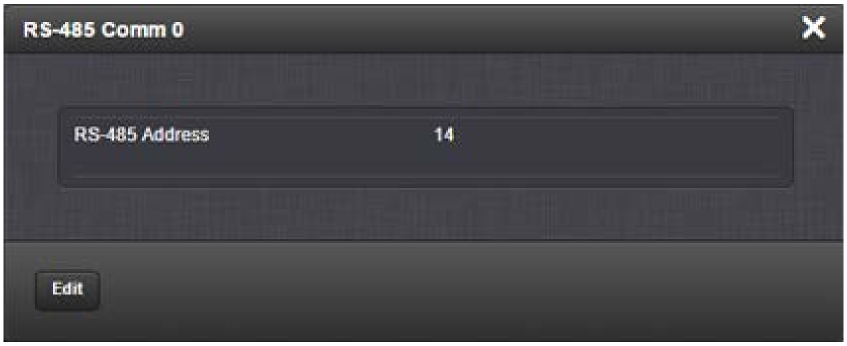
Communication Input/Output: Status Window

To view the address of an RS-485 communication input/output, go to its Status window. For instructions, see: "Viewing the Configuration of an Input or Output" on page 293.

The Web UI list entry for this card is: **RS-485 Comm**.

The name of the Input/Output is: **RS-485 Comm [number]**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



The Status window displays the following settings:

- **RS-485 Address**: [0-31]

5.7 Option Card Field Installation Guide

Typically, SecureSync units are shipped with custom-ordered option cards pre-installed at the factory. In the event that an option card is purchased at a later time, it must be installed in the SecureSync unit in the field by the customer.

This option card field installation guide contains information and instructions for installing option cards in Spectracom SecureSync units.

5.7.1 Introduction

SecureSync time and frequency synchronization system offers customizability and expandability via the addition of a range of modular option cards. Up to 6 option cards can be accommodated to offer not only synchronization to a variety of input references, but also numerous types of output signals, supporting an extensive number of traditional and contemporary timing protocols including:

- digital and analog timing and frequency signals (1PPS, 1MHz/5MHz/10 MHz)
- timecodes (IRIG, STANAG, ASCII)
- high accuracy and precision network timing (NTP, PTP)
- telecom timing (T1/E1), and more.

Note: The installation procedure varies, depending on the type of option card and the installation location.to be installed.

5.7.2 Outline of the Installation Procedure

The general steps necessary for installing SecureSync option cards are as follows:

1. If adding or removing option cards that provide a reference, optionally backup your SecureSync configuration (refer to Section: “PROCEDURE 2: Saving Reference Priority Configuration”, if applicable to your scenario or environment)
2. Safely power down the SecureSync unit and remove chassis cover.
3. Determine which slot the option card will be installed into.
4. Prepare slot (if required), and plug card into the slot.
5. Connect any required cables and secure option card into place.
6. Replace chassis cover, power on unit.
7. Log in to the SecureSync web interface; verify the installed card is identified.
8. Restore SecureSync configuration (if it had been backed up before, see above).

5.7.3 Safety

Before beginning any type of option card installation, please carefully read the safety statements and precautions under "SAFETY: Before You Begin Installation" on page 21.

5.7.4 PROCEDURE 1: Unpacking

On receipt of materials, unpack and inspect the contents and accessories (retain all original packaging for use in return shipments, if necessary).

The following additional items are included with the ancillary kit for the field installation of option card(s). Some of the parts listed below will be required for the installation (depending upon option card model, and installation location).

Item	Quant.	Part Number
50-pin ribbon cable	1	CA20R-R200-0R21
Washer, flat, alum., #4, .125 thick	2	H032-0440-0002
Screw, M3-5, 18-8SS, 4 mm, thread lock	5	HM11R-03R5-0004
Standoff, M3 x 18 mm, hex, M-F, Zinc-pl. brass	2	HM50R-03R5-0018
Standoff, M3 x 12 mm, hex, M-F, Zinc-pl. brass	1	HM50R-03R5-0012
Cable tie	2	MP00000

Table 5-27: Ancillary kit parts list [1204-0000-0700]

5.7.4.1 Additional Equipment Needed For Installation

In addition to the parts supplied with your option card ancillary kit, the following items may be required for installation:

- #1 Philips head screwdriver
- Cable tie clipper
- 6-mm hex wrench

5.7.5 PROCEDURE 2: Saving Refererence Priority Configuration

Note: This step is optional.

When adding or removing option cards with reference inputs such as IRIG Input, ASCII Timecode Input, HAVE QUICK, 1-PPS Input, Frequency Input, etc., any user-defined Reference Priority configuration will be reset back to the factory default state for the SecureSync hardware configuration. This means that you will need to re-configure the Reference Priority table at the end of the installation procedure.

To avoid this manual re- configuration, you can save the current SecureSyncconfiguration BEFORE beginning with the hardware installation, see: "Backing Up the System Configuration Files" on page 185.

After completion of the hardware installation, the SecureSync configuration can be restored (see PROCEDURE 12).

5.7.6 PROCEDURE 3: Determining the Correct Installation Procedure

The installation procedure for the option cards varies, depending on the type of your card. Determine the procedure for your card as follows:

a. Identify the first eight digits of the part number of your option card (see label on bag).

b. Inspect the back of the SecureSync housing, and select an empty slot for the new card. If the card is to be installed in one of the upper slots, take note if the corresponding lower slot is occupied.

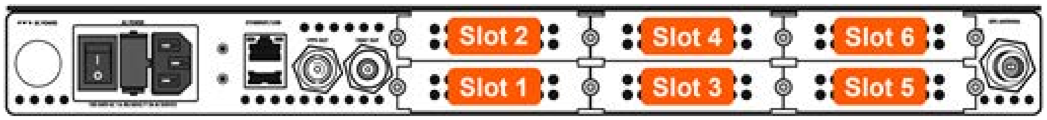


Figure 5-48: Unit rear view

c. See table "Installation steps" below:

   i. Find your part number in the left-hand column

   ii. Choose your installation location (as determined above)

   iii. When using an upper slot, choose the row bottom slot “empty” or “populated”

   iv. Continue with the installation by following the PROCEDURES listed in the corresponding row on the right hand side.

> **Note:** Follow only the PROCEDURES listed for your option card and installation scenario!

Part No. Option Card	Card function	Installation location	Bottom slot	PROCEDURES
1204-0080-0600 1204-0260-0600 1204-01C0-0600 1204-00C0-0600	Frequency output	Slot 2, 4, or 6	empty	(1), 2, 3, 5, 7, 11, (12)
			populated	(1), 2, 3, 6, 7, 11, (12)
		Slot 1, 3, or 5	(1), 2, 3, 4, 7, 11, (12)	
1204-00F0-0600	Alarm relay	Slot 2, 4, or 6	empty	(1), 2, 3, 5, 7, 10, 11, (12)
			populated	(1), 2, 3, 6, 7, 10, 11, (12)
		Slot 1, 3, or 5	(1), 2, 3, 4, 7, 10, 11, (12)	
1204-0060-0600	Gigabit Ethernet	Slot 2	empty	(1), 2, 3, 8, 11, (12)
			populated	(1), 2, 3, 9, 11, (12)
all other Part Numbers	miscellaneous	Slot 2, 4, or 6	empty	(1), 2, 3, 5, 11, (12)
			populated	(1), 2, 3, 6, 11, (12)
		Slot 1, 3, or 5	(1), 2, 3, 4, 11, (12)	

Table 5-28: Installation steps

5.7.7 PROCEDURE 4: Bottom Slot Installation

This section provides instructions for installing an option card into a bottom slot (**1**, **3**, or **5**) of the SecureSync unit.

a. Safely power down your SecureSync unit and remove chassis cover. Save the screws.

b. Remove the blank option card plate, or the existing option card in the slot. Save the screws. If a card is populating the slot above the bottom slot your option card is to be installed into, remove it.

c. Insert the card into the bottom slot by carefully pressing its connector into the mainboard connector (see Figure below), and lining up the screw holes on the card with the chassis.

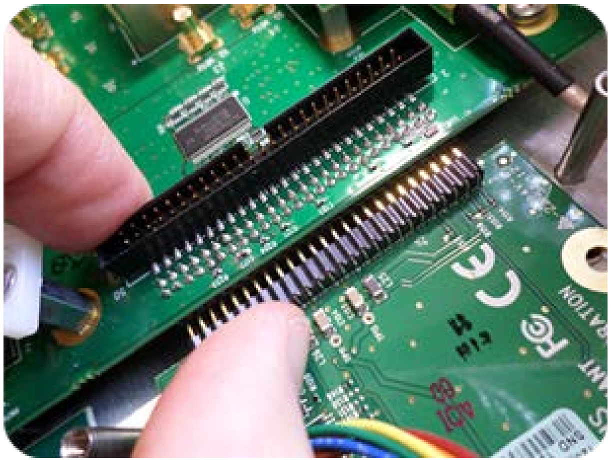


Figure 5-49: Connector installation

d. Using the supplied M3 screws, screw the board, and the option card plate into the chassis, applying a torque of 0.9 Nm/8.9 in-lbs.

> **Caution:** Ensure that screw holes on the card are properly lined up and secured to the chassis before powering the unit up, otherwise damage to the equipment may result.

5.7.8 PROCEDURE 5: Top Slot Installation, Bottom Slot Empty

This section provides instructions for installing an option card into an upper slot (**2**, **4**, or **6**) of the SecureSync unit, with no card populating the bottom slot.

a. Safely power down your SecureSync unit and remove the chassis cover. Save the screws.

b. Remove blank option card plate, or existing option card. Save the screws.

c. Place one of the supplied washers over each of the two chassis screw holes (see Figure below), then screw the 18 mm standoffs (= the longer standoffs) into the chassis (see Figure below), applying a torque of 0.9 Nm/8.9 in-lbs.

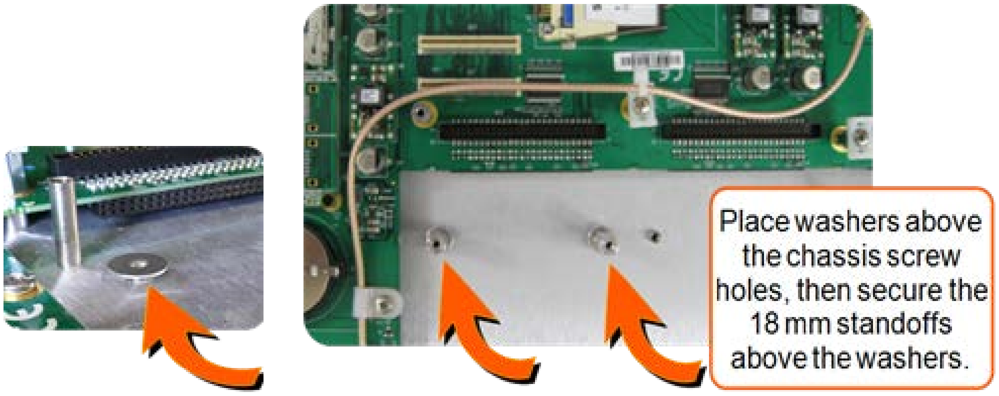

Place washers above the chassis screw holes, then secure the 18 mm standoffs above the washers.

Figure 5-50: Washers & standoffs secured to chassis screw holes

d. Insert option card into the slot, lining up the screw holes on the card with the standoffs.

e. Using the supplied M3 screws, screw the board into the standoffs, and the option card plate into the chassis, applying a torque of 0.9 Nm/8.9 in-lbs.

f. Take the supplied 50-pin ribbon cable and carefully press it into the connector on the mainboard (lining up the red sided end of the cable with PIN 1 on the mainboard), then into the connector on the option card (see Figure below).

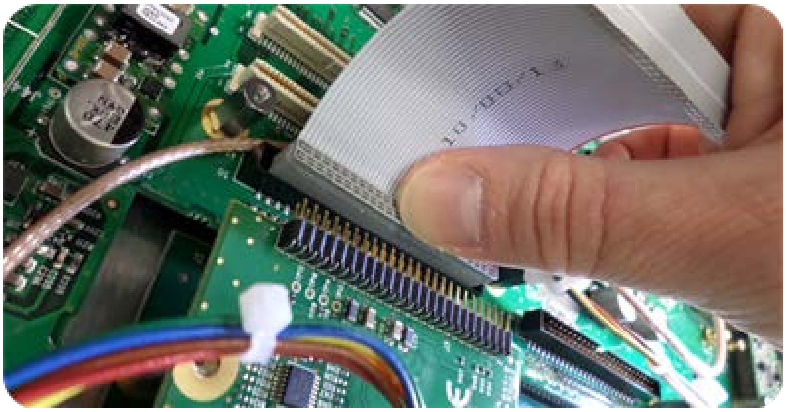


Figure 5-51: Ribbon cable installation

Caution: Ensure that the ribbon cable is aligned and fastened properly to all pins on the connector of the card. Otherwise, damage to the equipment may occur during power-up.

5.7.9 PROCEDURE 6: Top Slot Installation, Bottom Slot Occupied

This section provides instructions for installing an option card into an upper slot (**2**, **4**, or **6**) of the SecureSync unit, above a populated bottom slot.

a. Safely power down the SecureSync unit, and remove the chassis cover. Save the screws.

b. Remove the blank option card plate, or the existing option card. Save the screws.

c. Remove screws securing the card already populating the bottom slot. Save the screws.

d. Screw the 18-mm standoffs into the option card populating the bottom slot (see Figure below) , applying a torque of 0.9 Nm/8.9 in-lbs.

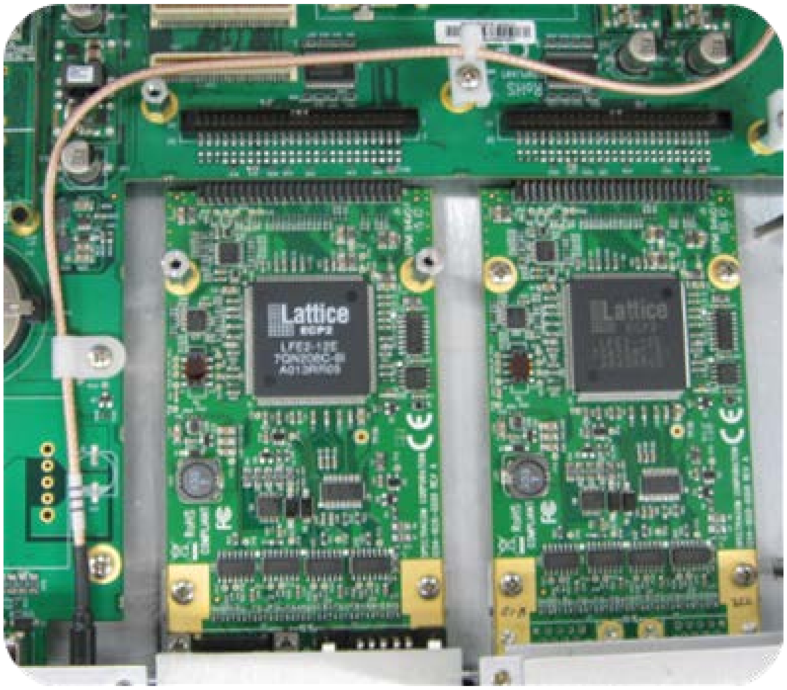


Figure 5-52: Bottom card with standoffs installed

e. Insert option card into the slot above the existing card, lining up the screw holes with the standoffs.

f. Using the supplied M3 screws, screw the board into the standoffs, and the option plate into the chassis, applying a torque of 0.9 Nm/8.9 in-lbs.

g. Take the supplied 50-pin ribbon cable and carefully press it into the connector on the mainboard (lining up the red sided end of the cable with PIN 1 on the mainboard), then into the connector on the option card (see Figure below).

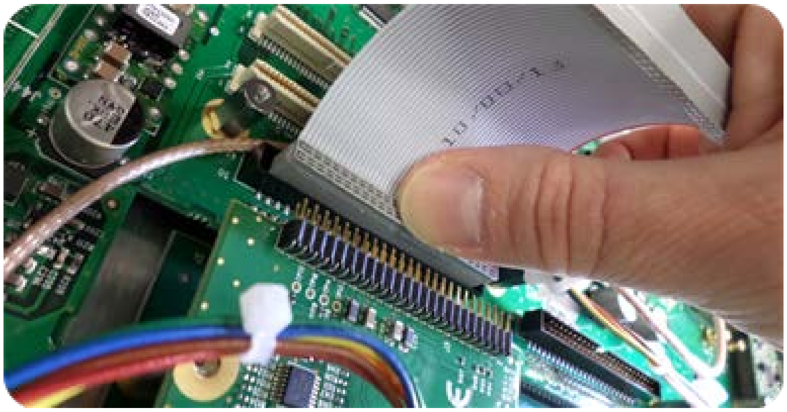


Figure 5-53: Ribbon cable installation

> **Caution:** Ensure that the ribbon cable is aligned and fastened properly to all pins on the connector of the card. Otherwise, damage to equipment may result during power up.

5.7.10 PROCEDURE 7: Frequency Output Cards: Wiring

This procedure includes additional installation instructions for the following option card types:

- Frequency Output cards:
  - 1MHz (PN 1204-0260-0600)
  - 5MHz (PN 1204-0080-0600)
  - 10 MHz (PN 1204-00C0-0600)
  - 10 MHz (PN 1204-01C0-0600)

For the cable installation, follow the steps detailed below:

a. Install the coax cable(s) onto the main PCB, connecting them to the first available open connectors, from J1... J4. See figure below:

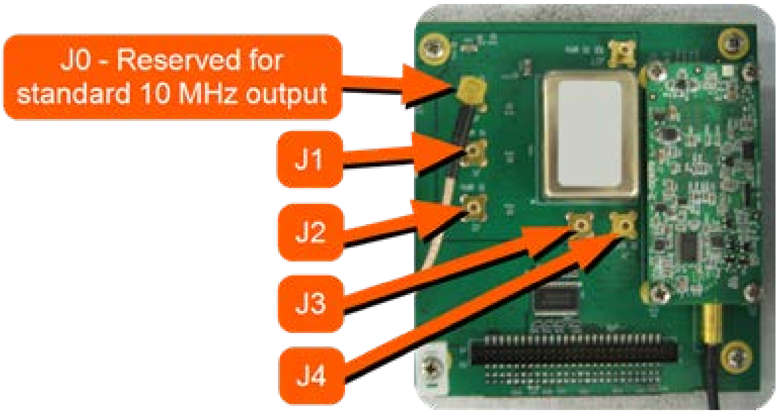


Figure 5-54: J Connectors

> **Note:** For 10 MHz option cards with 3 coax cables: From the rear of the option card, outputs are labeled J1, J2, J3.
>
> Start by connecting the cable attached to J1 on the card to the first available open connector on the SecureSync mainboard, then connect the cable attached to J2, then J3, etc.

b. Using the supplied cable ties, secure the coax cable from the option card to the white nylon cable tie holders fastened to the mainboard.

5.7.11 PROCEDURE 8: Gb ETH Card Installation, Slot1 Empty

This procedure describes the installation of the Gigabit Ethernet module card (PN 1204-0060-0600), if slot 1 is empty.

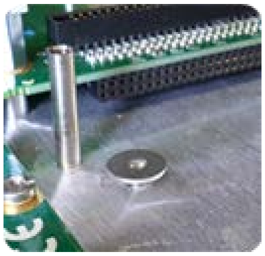
> **Note:** The Gigabit Ethernet option card must be installed in Slot 2. If there is a card already installed in Slot 2, it must be relocated to a different slot.

a. Safely power down the SecureSync unit and remove the chassis cover. Save the screws.

b. Remove the blank option card plate, or the existing option card. Save the screws.

Figure 5-55: Washer placement

c. Take the supplied washers and place them over the chassis screw holes (see figure below).



d. Screw the supplied 18-mm standoffs into place above the washers (see figure below), applying a torque of 0.9 Nm/8.9 in-lbs.

e. On the SecureSync mainboard, remove the screw located under the J11 connector and replace with the supplied 12-mm standoff (see figure below).

f. Insert the Gigabit Ethernet option card into Slot 2, and carefully press down to fit the connectors on the bottom of the Gigabit Ethernet card to the connectors on the mainboard.

g. Secure the option card by screwing the supplied M3 screws into:

- both standoffs on the chassis
- the standoff added onto the mainboard
- and into the rear chassis. Apply a torque of 0.9 Nm/8.9 in-lbs.

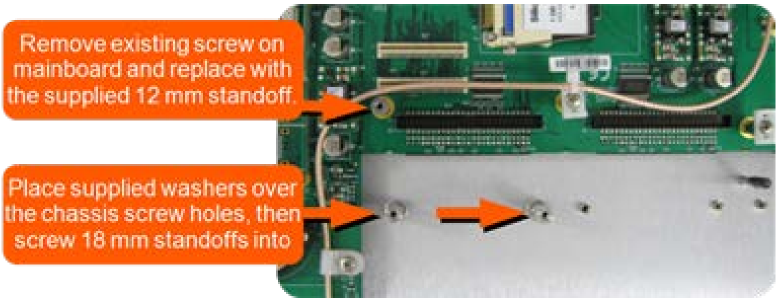

Remove existing screw on mainboard and replace with the supplied 12 mm standoff.
Place supplied washers over the chassis screw holes, then screw 18 mm standoffs into

Figure 5-56: Gigabit Ethernet option card installation

5.7.12 PROCEDURE 9: Gb ETH Card Installation, Slot1 Occupied

This procedure describes the installation of the Gigabit Ethernet card (PN 1204-0060-0600), if there is an option card installed in slot 1.

The Gigabit Ethernet option card must be installed in Slot 2. If there is a card already installed in Slot 2, it must be relocated to a different slot.

a. Safely power down the SecureSync unit and remove chassis cover. Save the screws.

b. Remove the blank option card panel, or the existing option card. Save the screws.

c. Remove the two screws securing the lower card (not the panel screws). Save the screws.

d. Screw the supplied 18-mm standoffs into place, applying a torque of 0.9 Nm/8.9 in-lbs.

e. On the SecureSync mainboard, remove the screw located under the J11 connector and replace with the supplied 12-mm standoff (see figure below).

f. Insert the Gigabit Ethernet option card into Slot 2, and carefully press down to fit the connectors on the bottom of the card to the connector on the mainboard.

g. Secure the option card by screwing the supplied M3 screws into
- both standoffs on the chassis
- the standoff added onto the mainboard
- and into the rear chassis. Apply a torque of 0.9 Nm/8.9 in-lbs.

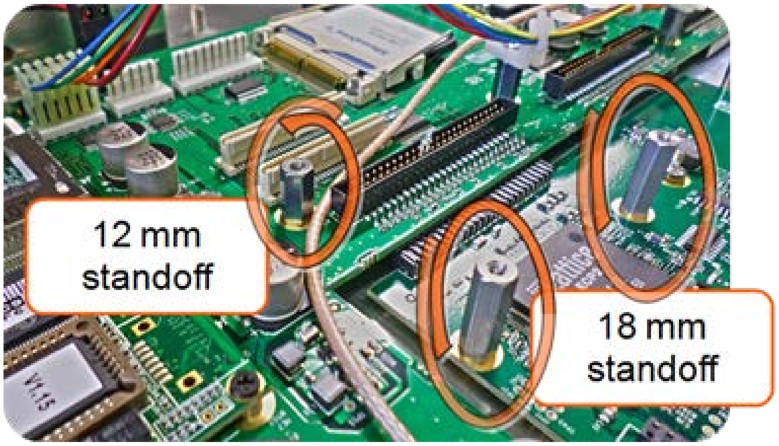


Figure 5-57: Gigabit Ethernet option card installation

5.7.13 PROCEDURE 10: Alarm Relay Card, Cable Installation

This procedure describes additional steps for the installation of the Alarm Relay Output card (PN 1204-00F0-0600).

a. Connect the supplied cable, part number 8195-0000-5000, to the mainboard connector J19 “RELAYS”.

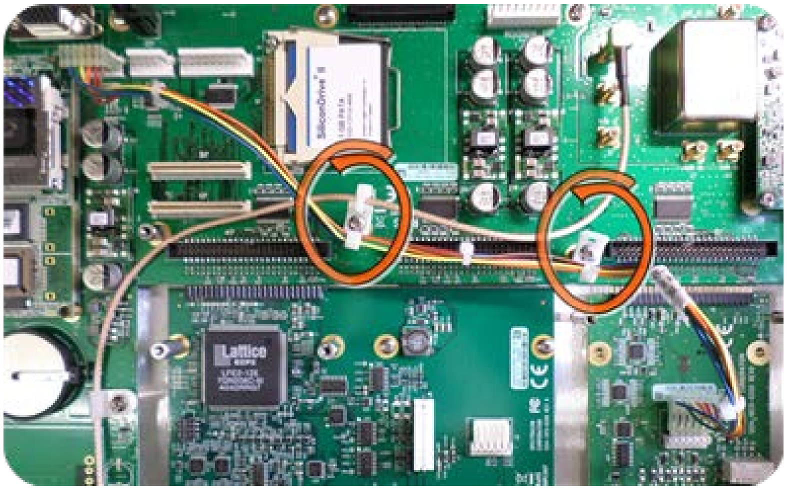


Figure 5-58: Cable routing

b. Using the supplied cable ties, secure the cable, part number 8195-0000-5000, from the option card to the white nylon cable tie holders fastened to the mainboard (see figure above).

5.7.14 PROCEDURE 11: Verifying Successful Installation

Prior to beginning managing any features or functionality provided by the new card, it is advisable to verify the successful installation by ensuring the card has been detected by the SecureSync unit.

> **Caution:** Ensure that screw holes on the card are properly lined up and secured to the chassis before powering the unit up, otherwise damage to the equipment may result.

a. Replace the chassis cover, and power on the unit.

b. To verify that the option card has been installed successfully and is being correctly recognized by SecureSync:

SecureSync Web UI, ≤ Version 4.x

Open a Web browser, and log in to the SecureSync Web UI. Navigate to the STATUS/INPUTS and/or STATUS/OUTPUTS pages. Information displayed on these pages will vary depending upon your option module card/SecureSync configuration (for example, the Multi-Gigabit Ethernet option module card has both input and output functionality, and so is displayed in both pages).

Note: If after an installation the card does not appear to be properly identified, it may be necessary to update the SecureSync system software to the latest available version.

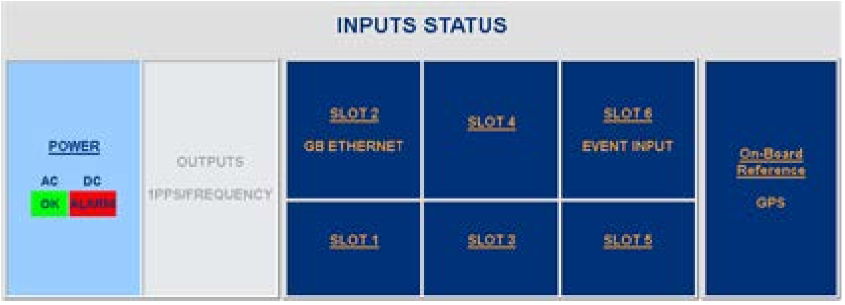


Figure 5-59: Example STATUS/INPUTS page - SecureSync Web UI

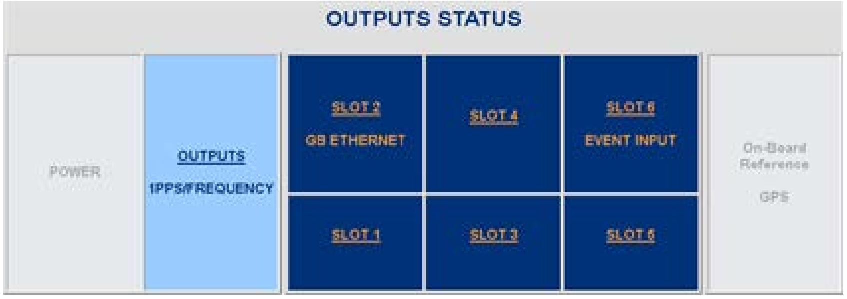


Figure 5-60: Example STATUS/OUTPUTS page - SecureSync Web user interface

SecureSync Web UI, ≥ Version 5.0

Open a web browser, log in to the SecureSync Web UI, and navigate to INTERFACES/OPTION CARDS: The new card will be displayed in the SLOT list.

Note: If after an installation the card does not appear to be properly identified, it may be necessary to update the SecureSync system software to the latest available version.

5.7.15 PROCEDURE 12: Restoring Reference Priority Configuration (optional)

Prior to configuring the new card in the Web UI, the System Configuration Files need to be restored, if you saved them under **PROCEDURE 2**.

Please see "Restoring the System Configuration" on page 187 for how-to information.

Card-specific configuration instructions may be found in the Option Cards Guide, see "Option Card Identification" on page 287.

BLANK PAGE.

CHAPTER 6

Troubleshooting

The front panel LEDs and the Web UI provide SecureSync status information that can be used to help troubleshoot failure symptoms that may occur.

The following topics are included in this Chapter:

6.1 Troubleshooting Using the Status LEDs

The front panel Status LEDs can provide “local” status information about SecureSync. Observe the front panel Status LEDs and use the table below to find the recommended troubleshooting steps or procedure for the observed condition.

LED	Current Status	Indication	Troubleshooting
Power	LED is blank (not lit).	SecureSync has no AC and/or DC input power applied.	1) Verify AC power is connected to an AC source and AC power switch is ON. 2) Verify DC power (within the correct voltage range, as stated on the DC connector) is applied to the DC power connector. 3) See "Unpacking and Inventory" on page 19
Sync	LED is off	No valid Reference inputs available since power-up.	1) Make sure the Input Reference Priority table has the desired inputs enabled, based on desired priority. 2) Make sure the desired input references are connected to the correct port of SecureSync. 3) See "Configuring Input Reference Priorities" on page 155
Sync	LED is orange	Holdover mode: All available inputs have been lost.	1) Make sure the Input Reference Priority table still has the desired inputs enabled, based on desired priority. See "Configuring Input Reference Priorities" on page 155. 2) Make sure desired input references are still connected to the correct port of SecureSync. 4) Verify GNSS antenna installation (if applicable). See "Troubleshooting GNSS Reception" on page 459.
Sync	LED is red	Time Sync alarm: SecureSync was just powered-up and has not yet synced to its references. Or, all available reference inputs have been lost and the Holdover mode has since expired.	Note: If SecureSync was just recently powered-up or rebooted and input references are applied, no troubleshooting may be necessary. Allow a few minutes for the input reference to be declared valid (allow 35 - 40 minutes for a new install with GNSS input). 1) Make sure the Input Reference Priority table still has the desired inputs enabled, based on desired priority. Refer to "Configuring Input Reference Priorities" on page 155. 2) Make sure desired input references are still connected to the correct port of SecureSync. 3) Verify GNSS antenna installation (if applicable). Make sure the antenna has a clear view of the sky.

LED	Current Status	Indication	Troubleshooting
Fault	LED is blinking orange	GNSS Antenna problem alarm is asserted	1) Verify GNSS antenna is connected to SecureSync GNSS input connector 2) Check antenna cable for presence of an open or a short. Refer to XXX for additional information.
Fault	LED is solid red	Major alarm is asserted	Refer to XXX
Fault	LED is solid orange	Minor alarm is asserted	Refer to XXX

Table 6-1: Troubleshooting SecureSync, using the front panel Status LED indications

6.1.1 Minor and Major Alarms

Major Alarm

There are several conditions that can cause the front panel Fault lamp, or 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.
- **System 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 Spectracom technical support if the error continues.

Minor Alarm

There are several conditions that can cause the front panel Fault lamp, or Web UI status lights to indicate a Minor alarm has been asserted. These conditions include:

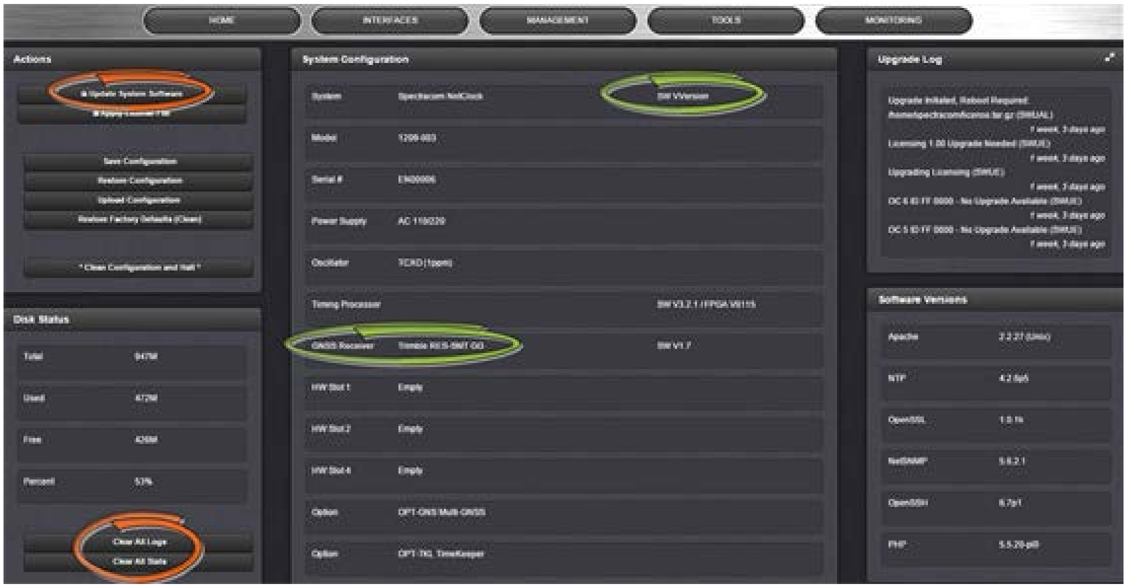
- **Too few GPS satellites, 1st threshold**: The GNSS receiver has been tracking less than the minimum number of satellites for too long of a duration. Refer to "Troubleshooting GNSS Reception" on page 459 for information on troubleshooting GNSS reception issues.

6.2 Troubleshooting: System Configuration

One of the first tasks when troubleshooting a unit is to read out the current system configuration (you may also be asked for this when contacting Spectracom Technical Support.)

In the Web UI, select **TOOLS** > **Upgrade/Backup**: The screen displayed will provide information on:

- System configuration
- Disk status, memory status
- Software versions, and
- Recent log entries.



System Configuration

System	Spectracom NetClock	SW VVersion
Model	1200-003	
Serial #	EN00006	
Power Supply	AC 110/220	
Oscillator	TCXO (1ppm)	
Timing Processor		SW V3.2.1 / FPGA V0115
GNSS Receiver	Trimble RES-SMT GG	SW V1.7
HW Slot 1	Empty	
HW Slot 2	Empty	
HW Slot 4	Empty	
Option	OPT-GNS Multi-GNSS	
Option	OPT-TKL TimeKeeper	

Disk Status

Total	947M
Used	472M
Free	426M
Percent	53%

Upgrade Log

```
Upgrade initiated, Reboot Required.
/home/spectracom/license.tar.gz (SWUAL)
                                1 week, 3 days ago
Licensing 1.00 Upgrade Needed (SWUE)
                                1 week, 3 days ago
Upgrading Licensing (SWUE)
                                1 week, 3 days ago
OC 6 ID FF 0000 - No Upgrade Available (SWUE)
                                1 week, 3 days ago
OC 5 ID FF 0000 - No Upgrade Available (SWUE)
                                1 week, 3 days ago
```

Software Versions

Apache	2.2.27 (Unix)
NTP	4.2.8p5
OpenSSL	1.0.1s
NetSNMP	5.6.2.1
OpenSSH	6.7p1
PHP	5.5.20-pl0

6.2.1 System Troubleshooting: Browser Support

Spectracom recommends using one of the following Web browsers to run the SecureSyncWeb UI on: Google Chrome, Mozilla Firefox, Internet Explorer > Ver. 8.

Using different or older browsers may lead to some incompatibility issues.

6.3 Troubleshooting - Unable to Open Web UI

With SecureSync connected to either a stand-alone or networked PC and with the network configuration correct, it should be possible to connect to the Web UI.

Verify	Current Status	Indication	Troubleshooting
LEDs on network connector	Green “Good link” is not solid green	SecureSync ICMP test is failing. SecureSync is not connected to PC via Ethernet connection	1) Verify one end of standard network cable is connected to SecureSync’s Ethernet port and other end is connected to a hub/switch. Or a network cable is connected to SecureSync and a stand-alone PC. 2) Verify network settings of SecureSync are valid for the network/PC it is connected with (IP address is on the same subnet as the other PC).
	Green “Good Link” is solid green on both SecureSync and other end of network cable.	SecureSync ICMP test is passing. SecureSync is connected to PC via Ethernet connection	1) Disconnect SecureSync’s network cable and ping its assigned address to ensure no response (no duplicate IP addresses on the network). 2) Try accessing SecureSync from another PC on the same network. 3) Network Routing/firewall issue. Try connecting directly with a PC and network cable.

Table 6-2: Troubleshooting network connection issues

6.4 Troubleshooting via Web UI Status Page

SecureSync’s Web UI includes pages that provide current “remote” status information about SecureSync. The following table includes information that can be used as a troubleshooting guidance if status fault indications or conditions occur.

Web UI Page location	Current Status	Indication	Troubleshooting
HOME page, System Status panel, Status row	SYNC indicator is not “lit” (not Green).HOLD indicator is “lit” (Orange).–OR–FAULT indicator is “lit” (Red). Below the System Status panel there is an Out of Sync alarm statement	SecureSync is in Holdover mode–OR–SecureSync is now out of Time Sync	All available Input References have been lost. The Reference Status table on the HOME page will show the current status of all inputs (Green is valid and Red is invalid or not present). 1. Make sure the Input Reference Priority table still has the desired reference inputs Enabled, based on the desired priority. See "Configuring Input Reference Priorities" on page 155. 2. Make sure the desired input references are still connected to the correct input port of SecureSync. 3. Verify GNSS antenna installation (if applicable). See "Troubleshooting GNSS Reception" on page 459.

Web UI Page location	Current Status	Indication	Troubleshooting
HOME page, System Status panel, Power row	AC and/or DC indicator is red instead of greenNOTE: The AC indicator will only display on the HOME screen if SecureSync is equipped with an AC power input.The DC indicator will only display on the HOME screen if SecureSync is equipped with a DC power input.	Specified AC and/or DC input power is not present.	Refer to Section "Power Connection" on page 25 for AC and DC power connection information: If AC indicator is red: 1. Verify AC power cord is connected to an AC outlet. 2. Verify AC power input switch is ON. 3. Check the two fuses in the AC power module. If DC indicator is red: 1. Verify DC power source is within range specified at the DC power connector. 2. Verify DC power is present at the input connector. 3. Verify DC input polarity.
MANAGEMENT/ NTP Setup page NTP Status Summary panel Stratum row	Stratum 15	NTP is not synchronized to its available input references (SecureSync may have been in Holdover mode, but Holdover has since expired without the return of valid inputs)	Note: If SecureSync was just recently powered-up or rebooted and input references are applied, no troubleshooting may be necessary. Allow at least 10-20 minutes for the input references to be declared valid and NTP to align to the System Time (allow an additional 35-40 minutes for a new install with GNSS input). 1. Verify in the Configure Reference Priorities table that all available references enabled. See "Configuring Input Reference Priorities" on page 155. 2. Verify that the Reference Status on the HOME page shows “OK” (Green) for all available references. 3. Verify NTP is enabled and configured correctly. See "NTP Stratum Configuration" on page 125.
MANAGEMENT/ NETWORK page	Cannot login or access the Web UI.	The following error message is displayed: “Forbidden You don’t have permission to access/ on this server”	This message is displayed when any value has been added to the Network Access Rules table and your PC is not listed in the table as an Allow From IP address.To restore access to the Web UI, either 1. Login from a PC that is listed as an Allow From in this table; or 2. If it is unknown what PCs have been listed in the Access table, perform an `unrestrict` command to remove all entries from the Network Access Rules table. This will allow all PCs to be able to access the Web UI.

Table 6-3: Troubleshooting using the Web UI Status indications

6.5 Troubleshooting GNSS Reception

If SecureSync reports Holdover and/or Time Sync Alarms caused by insufficient GNSS reception:

When a GNSS receiver is installed in SecureSync, a GNSS antenna can be connected to the rear panel antenna connector via a coax cable to allow it to track several satellites in order for GNSS to be an available input reference. Many factors can prevent the ability for the GNSS receiver to be able to track the minimum number of satellites.

With the GNSS antenna installed outdoors, with a good view of the sky (the view of the sky is not being blocked by obstructions), SecureSync will typically track between 5-10 satellites (the maximum possible is 12 satellites). If the antenna’s view of the sky is hindered, or if there is a problem with the GNSS antenna installation, the GNSS receiver may only be able to a few satellites or may not be able to track any satellites at all.

When GNSS is a configured time or 1PPS input reference, if the GNSS receiver is unable to continuously track at least four satellites (until the initial GNSS survey has been completed) or at least one satellite thereafter, the GNSS signal will not be considered valid. If no other inputs are enabled and available, SecureSync may not initially be able to go into time sync. Or, if GNSS reception is subsequently lost after initially achieving time sync, SecureSync will go into the Holdover mode. If GNSS reception is not restored before the Holdover period expires (and no other input references become available) SecureSync will go out of sync. The GNSS reception issue needs to be troubleshot in order to regain time sync.

For additional information on troubleshooting GNSS reception issues with SecureSync, please refer to the **GNSS Reception Troubleshooting Guide**, available here on the Spectracom website.

6.6 Troubleshooting - Keypad Inoperative

The SecureSync front panel keypad can be locked in order to prevent inadvertent operation. It can be locked and unlocked using either the keypad or the Web UI. When locked, the keypad operation is disabled until it is unlocked using either of the two following processes:

» To unlock the front panel keypad using the keypad (locally):

1. Perform the following key sequence:

↑ ↓ ↑ ↓ ← → ← → ✓ X ✓

» To unlock the front panel keypad using the Web UI (remotely):

1. Open the SecureSyncWeb UI, and navigate to the **Setup/Front Panel** page.
2. Change the **Lock** from “Enabled” to “Disabled”.
3. Click the **Submit** button.

6.7 Troubleshooting - 1PPS, 10 MHz Outputs

If the 1PPS and/or the 10 MHz output(s) are not present, input power may not be applied. Or SecureSync is not synchronized to its input references and Signature Control is enabled.

Web UI Page	Current Status	Indication	Troubleshooting
HOME page	Reference Status Table	One or more input references indicate "Not Valid" (red)	All available Input References have been lost. The Reference Status table on this same page will show the current status of all inputs (Green is valid and red is not valid, or not present). If Signature Control is enabled in this state, the output may be disabled, see "Configuring 1PPS/10 MHz Outputs" on page 199. 1. Make sure the Input Reference Priority table still has the desired inputs enabled, based on desired priority. 2. Make sure desired input references are still connected to the correct input port of SecureSync. 3. Verify GNSS antenna installation (if applicable).
Navigate to INTERFACES/OUTPUTS/ PPS Output page	Select the PPS Output screen. See "Configuring 1PPS/10 MHz Outputs" on page 199.	Signature Control will show "Output Always Enabled", "Output Enabled in Holdover", "Output Disabled in Holdover" or "Output Always Disabled".	1. With "Output Always Enabled" selected, the selected output will be present no matter the current synchronization state.2. Any other configured value will cause the applicable output to be halted if SecureSync is not fully synchronized with its input references.

Table 6-4: Troubleshooting 1PPS and/or 10 MHz outputs not being present

6.8 Troubleshooting - Blank Information Display

If the front panel 4-line LCD Information Display is blank:

As long as input power is applied (as indicated by the power light being green and the LED time display incrementing) the 4-line LCD Information Display is capable of displaying data. The Information Display can be configured to display different data while the keypad is not in use. One available configuration is to have the Information Display show a blank page when not in use. The Information Display operation can be verified and can also be configured via the Web UI, or the front panel keypad.

A. **Using the front panel keypad to verify the LCD Information Display is configured to display a blank page:**

To verify the front panel LCD Information Display is configured to display a blank page, just press any keypad button. As long as the keypad is unlocked, the **Home** screen will be displayed (after one minute of not pushing any keys, the screen will go back to blank).

Note: The information that is selected, is the page that is normally displayed in the LCD window, beginning one minute after the keypad is no longer being used.

B. **Using the front panel keypad to change the information normally displayed in the LCD when the keypad is not in use:**
To use the front panel keypad to reconfigure the LCD Information Display to show something other than a blank page (such as GNSS information, network configuration, etc.), see "Using the Keypad and Information Display" on page 30.

C. **Using the Web UI to change the information normally displayed in the LCD Information Display when the keypad is not in use:**
To use the Web UI to reconfigure the LCD Information Display to show something other than a blank page (such as GNSS information, network configuration, etc.), refer to "Front Panel Configuration" on page 179.

6.9 Troubleshooting the Front Panel Serial Port

The front panel serial port can be used for SecureSync configuration or to obtain select data. The serial port is a standard DB9 female port. Communication with this port is via a standard DB9 F to DB9M serial cable (minimum pinout is pin 2 to 2, pin 3 to 3 and pin 5 to 5) connected to a PC running a terminal emulator program such as Tera Term or Microsoft HyperTerminal. The port settings of the terminal emulator should be configured as 9600, N, 8, 1 (flow control setting does not matter).

If the terminal emulator program does not display any data when the keyboard <Enter> key is pressed, either SecureSync is not powered up or there is a problem with the connection between SecureSync and the PC.

Using a multimeter, ring out the pins from one end of the serial cable to the other. Verify the cable is pinned as a straight-thru serial cable (pin 2 to 2, pin 3 to 3 and pin 5 to 5) and not as a null-modem or other pin-out configuration.

Disconnect the serial cable from SecureSync. Then, jumper (using a wire, paperclip or car key, etc.) pins 2 and 3 of the serial cable together while pressing any character on the PC’s keyboard. The character typed should be displayed on the monitor. If the typed character is not displayed, there is a problem with either the serial cable or with the serial COM port of the PC.

Refer to "Setting up a Terminal Emulator" on page 466 for more information on using a terminal emulator software to communicate with SecureSync via serial port.

6.10 Troubleshooting the Front Panel Cooling Fan

The cooling fan (located on the front panel, to the right of the LED time display) is a temperature controlled cooling fan. Temperature sensor(s) determine when the cooling fan needs to turn on and off. It is normal operation for the cooling fan to not operate the entire time SecureSync is running. It may be turned off for long periods at a time, depending on the ambient and internal temperatures.

To verify the cooling fan is still operational, power cycle SecureSync unit (if AC and DC power are both applied, momentarily turn off the AC power switch and disconnect the DC power connector).

> **Note:** If the internal temperature in the unit is below 30 degrees Celsius, the fan may not turn on as part of the power-up sequence. In this case, it is recommended to let the unit “warm up” for approximately 30 minutes, in order to allow the unit to get to the appropriate temperature.

See also: "Temperature Management" on page 257

6.11 Troubleshooting - Network PCs Cannot Sync

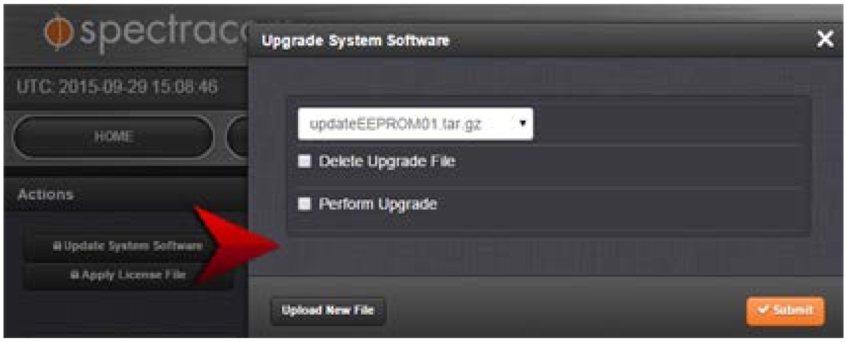
In order for clients on the network to be able to sync to SecureSync, several requirements must be met:

1. The PC(s) must be routable to SecureSync. Make sure you can access SecureSync Web UI from a PC that is not syncing. If the PC cannot access the Web UI, a network issue likely exists. Verify the network configuration.
2. The network clients have to be configured to synchronize to SecureSync's address. For additional information on syncing Windows PC's, visit the Support pages on the Spectracom website (spectracom.com), and download/view the document titled “*Synchronizing Windows Computers”*. The last section of this document also contains troubleshooting assistance for Windows synchronization. For UNIX/Linux computer synchronization, please visit http://www.ntp.org/.
3. If at least one PC can sync to SecureSync, the issue is likely not with SecureSync itself. The only SecureSync configurations that can prevent certain PCs from syncing to the time server are the NTP Access table and MD5 authentication. Refer to Sections "Configuring NTP Access Restrictions" on page 119 and "Configuring NTP Symmetric Keys (MD5 Authentication)" on page 116 respectively. A network or PC issue likely exists. A firewall may be blocking Port 123 (NTP traffic), for example.
4. NTP in SecureSync must be “in sync” and at a higher Stratum level than Stratum 15 (such as Stratum 1 or 2, for example). This requires SecureSync to be either synced to its input references or in Holdover mode. Verify the current NTP stratum level and the sync status.

6.12 Troubleshooting Software Update

When experiencing slow data transmission rates, or other network issues, it may be possible that a system software update will be aborted due to a web server timeout during the transfer.

In such an event, the **Upload New File** window will disappear, and the **Upgrade System Software** window will be displayed again instead.



- Should this happen repeatedly, you can transfer the update file using a file transfer protocol such as scp, sftp or ftp, if security is not a concern. The update can then be initiated from the Web UI or Command Line.
- Disk Status: In the event of an aborted update process, under **Tools** > **Upgrade/Backup** > **Disk Status**, check **Percent Used**: If the number is greater than 70%, free up disk space, before starting another attempt to update the System Software.

Software Versions older than 5.3.0:

Note that failed update attempts may result in lost Disk Space on the SecureSync. Reboot the system to erase unwanted update files.

Software Version 5.3.0:

In the event that an update process becomes aborted, clicking Update System Software will automatically erase unwanted update files.

CHAPTER 7

Command-Line Interface

A terminal emulation program is used to emulate a video terminal, so as to access SecureSync's CLI (Command-Line Interface) remotely via a serial cable. This may be required, if no other means of remotely accessing SecureSync are available, for example if Ethernet ports are used otherwise or have been disabled (for security reasons, or similar).

The following topics are included in this Chapter:

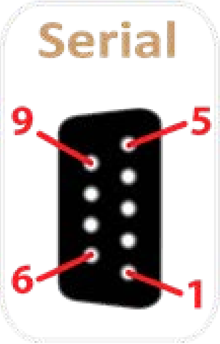
7.1 Setting up a Terminal Emulator

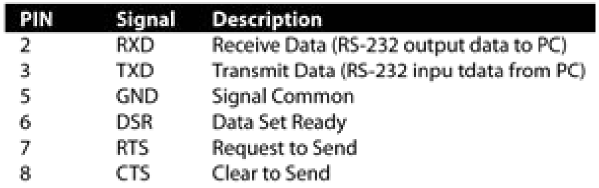
If no other means are available to access SecureSync, a terminal emulation program can be used to carry out certain configuration changes by accessing SecureSync's CLI (command-line interface) via a serial port connection. An application example for this scenario is to enable a network port so that the SecureSync Web UI can be used. While it is also possible to retrieve selected logs, a terminal emulator does not replace the SecureSync Web UI.

Spectracom does not distribute or support its own terminal emulator, and newer Microsoft operating systems no longer include HyperTerminal, however, there are several third-party open-source programs available, such as **Tera Term** or **PuTTY**. The example below illustrates the use of TeraTerm. The setup procedure is similar when using other terminal emulation programs.

Required tools and parts:

I. A standard, one-to-one pinned RS-232 serial cable; this cable has one male and one female DB-9 connector. Do NOT use a Null Modem cable. If you do not have a standard RS-232 cable at hand, follow the pin-out configuration described below when building a cable. It is required to wire at least pins number 2, 3, and 5.





PIN	Signal	Description
2	RXD	Receive Data (RS-232 output data to PC)
3	TXD	Transmit Data (RS-232 inpu tdata from PC)
5	GND	Signal Common
6	DSR	Data Set Ready
7	RTS	Request to Send
8	CTS	Clear to Send

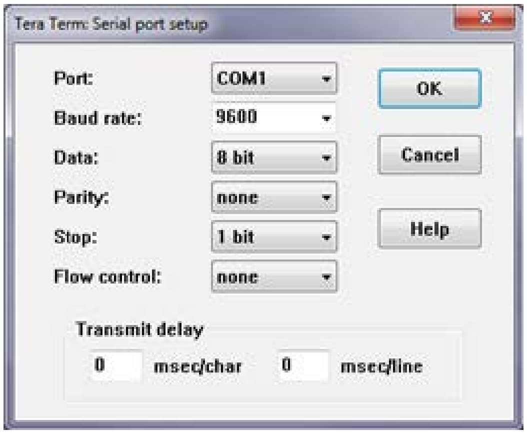
Figure 7-1: Serial port pin-out

II. Personal Computer with terminal emulator program installed.

Procedure:

1. Connect the personal computer to the SecureSync front panel serial connector, using the serial cable.
2. Configure your terminal emulation program, using the following settings:
   - **Port**: COM1
   - **Bits per second**: 9600
   - **Data bits**: 8
   - **Parity**: None

- **Stop bits**: 1
- **Flow control**: None



Port: COM1
Baud rate: 9600
Data: 8 bit
Parity: none
Stop: 1 bit
Flow control: none
Transmit delay: 0 msec/char, 0 msec/line

3. Depending on which network protocol you are using (SSH, Telnet), you will need to enter authentication upon establishment of the connection either in a separate authentication window, or the Terminal window: The default user name is `spadmin`, and the password `admin123`.
4. Using the Terminal window, you can now configure the desired parameters. See "CLI Commands" below for a list of commands.

7.2 CLI Commands

SecureSync features a suite of command-line interface (CLI) commands that can be used to configure parameters and retrieve status information or log files via a remote connection, using the `telnet` or `ssh` (if enabled) protocol.

This section includes a list of some of the supported commands.

Notes:

a. The command "`helpcli`" will provide a list of all available commands and their syntax (**Note**: Typing "`help`" will output bash shell help only and will not provide useful information).

b. You can scroll up or scroll down through the output by using the Page Up/Page down keys, or the arrow keys.

c. Type "`q`" (lower-case) to quit.

d. Pressing the up/down keys scrolls through previously typed commands.

e. Commands need to be typed in all lower-case letters.

f. Where eth0 is the base network port and eth1 (and higher) are used with the optional Gigabit Ethernet module for multiple network interfaces.

g. User accounts with “user” group permissions can perform “get” commands but cannot perform any “set” commands or change/reset passwords. Only user accounts with “admin” group permissions can perform “set” commands or change/reset password. Refer to "User Account Management" on page 136 for user account setup information.

Command	Description
clean	Restores SecureSync configuration to factory defaults and reboots
cleanhalt	Restores SecureSync configuration to factory defaults and halts
clearlogs	Clears all logs
clearstats	Clears all statistical data (NTP, and oscillator/disciplining)
dateget	Displays current date (for example, 15 APR 2015)
dateset	Used to set the current date
defcert	Used to create a new Spectracom self-signed SSL certificate for HTTPS in case of expiration of the original certificate
dhcp4get	Displays whether DHCP is enabled
dhcp4set	Used to enable or disable DHCP
dns4get	Displays the configured DNS servers
dns4set	Used to configure the DNS servers
dhcp6get	Displays whether DHCPv6 is enabled
dhcp6set	Used to enable or disable DHCPv6
doyget	Used to obtain the current Day of Year
doyset	Used to set the current Day of Year
gpsdop	Displays GNSS receiver positional accuracy estimates
gpsinfo	Applicable to SAASM-equipped SecureSync units only
gpsloc	Displays GNSS latitude, longitude and antenna height
gpsmdl	Displays the GNSS Manufacturer and Model
gpssat	Displays GNSS satellites tracked and maximum signal strength being received
gw4get	Displays IPv4 gateway addresses
gw4set	Used to configure the IPv4 gateway addresses
gw6get	Displays IPv6 gateway address
gw6set	Used to configure the IPv6 gateway address
halt	Used to Halt the system for shutdown
helpcli	Provides list of available commands and syntax

Command	Description
hostget	Displays the DNS hostname
hostset	Sets the DNS hostname
hotstart	Initiate a hot start operation on the SAASM GPS receiver
ip4get	Displays IPv4 Ethernet port information (IP address net mask and gateway)
ip4set	Used to set IPv4 Ethernet port information (IP address net mask and gateway)
ip6add	Used to add IPv6 Ethernet port information (IP address net mask and gateway)
ip6del	Used to delete IPv6 IP address
ip6get	Used to obtain the IPv6 IP address
iptables	See "Network Services: En-/Disabling" on page 62 for more information.
licenses	Displays configured licenses installed (if any)
list	Outputs a list of commands
loadconf	Restore a saved configuration and reboot
localget	Used to obtain the configured local clock
locallist	Used to display local clocks
localset	Used to configure local clocks
model	Displays the Serial Number of the unit
net	Displays network settings
netnum	Displays the number of general-purpose network interfaces
net4	Displays IPv4 network settings
net6	Displays IPv6 network settings
options	Displays configured options installed (if any)
oscget	Displays the installed system oscillator
portget	Display whether network port is enabled (for example, "portget ETH2")
portset	Enable or disable a network port: "portset x on" where "x" is the port number (for example, "ETH2") "portset X off" [NOTE: Available since Web UI Revision no. 5.1.2]
portstate	Display the current state for a network port
ppsctrl	Enable/disable individual 1PPS output signals
priorset	Sets the priority of an entry in the reference priority table
radius setretry	<value> Sets how many radius login retries will be attempted
radius getretry	<value> Gets the number of radius login retry attempts

Command	Description
radius server list	Lists radius servers
radius server add	<host> <port> <key> <timeout> Adds radius server
radius server del	<id> Deletes radius server number <id>
reboot	Used to warm-boot the unit without having to disconnect or reconnect power
reftable	Displays reference priority table
release4	Used with DHCP to release the IPv4 address
release6	Used with DHCPv6 to release the IPv6 address
renew4	Used with DHCP to renew the assigned IPv4 address
renew6	Used with DHCPv6 to renew the assigned IPv6 address
resetpw	Resets the administrator account (spadmin) password back to the default value "`admin123`"
routes4	Displays the current IPv4 routing table(s)
routes6	Displays the current IPv6 routing table(s)
rt4add	Adds an IPv4 static route
rt4del	Deletes an IPv4 static route
rt4get	Displays the configured IPv4 static routes
rt6add	Adds an IPv6 static route
rt6del	Deletes an IPv6 static route
rt6get	Displays the configured IPv6 static routes
saveconf	Generate archive of current configuration
savelog	Generate archive of all log files
scaleget	Displays configured system timescale
scaleset	Used to configure the system timescale
services	Displays the state of services (enabled/disabled)
servget	Displays the state of individual services
servset	Enable or disable specific services
slaacget	Displays whether SLAAC is enabled
slaacset	Used to enable or disable SLAAC
Stateset	Enable or disable an entry in the reference priority table. index = 0...15. state = 0 (disable), 1 (enable)

Command	Description
status	Displays information about the oscillator disciplining
syncstate	Display timing system synchronization state
sysupgrade	Performs system upgrade using the update bundle provided
testevent	Generates SNMP events in the enterprise MIB
tfomget	Displays current estimated system time error (TFOM - Time Figure of Merit)
timeget	Displays current system time (time is displayed in the configured timescale - See `scaleget` command to retrieve the configured timescale)
timeset	Used to manually set the current time (hours, minutes in seconds); time is entered based on the configured timescale - See `scaleget` command to retrieve the configured timescale
unrestrict	Used for clearing access control restrictions to SecureSync
version	Displays the installed main SecureSync and timing system software versions
yearget	Displays the current year
yearset	Used to set the current year
zeroize	Applicable to SAASM-equipped SecureSync units only

BLANK PAGE.

APPENDIX

Appendix

The following topics are included in this Chapter:

8.1 ASCII Time Code Data Formats

This section describes the different time code data format selections available for use with SecureSync option cards that accept ASCII data streams as inputs or outputs via their RS-485 and RS-232 interfaces.

Supported are formats like NMEA, BBC, Spectracom, GSSIP, and Endrun.

8.1.1 NMEA GGA Message

The GGA Format provides essential fix data which includes 3D location and accuracy data.

Example message:

```
$GPGGA,123519.00,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,*47
```

Where:

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 = GNSS 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	Checksum data, always begins with *

8.1.2 NMEA RMC Message

NMEA Message Format RMC, (Recommended Minimum) provides fix information, speed over ground and Magnetic Variance information.

Example message:

```
$GPRMC,123519.00,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A
```

Where:

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	Checksum data, always begins with *

8.1.3 NMEA ZDA Message

The Format ZDA Data message provides Date and Time information.

Example message:

```
$GPZDA,HHMMSS.00,DD,MM,YYYY,XX,YY*CC
```

Where:

HHMMSS.00	HrMinSec(UTC)
DD,MM,YYYY	Day, Month, Year
XX	Local zone hours -13...13
YY	Local zone minutes 0...59
*CC	Checksum

8.1.4 Spectracom Format 0

Format 0 includes a time synchronization status character, day of year, time reflecting Time Zone Offset and DST corrections when enabled. Format 0 also includes the DST/Standard Time indicator, and the Time Zone Offset value. Format 0 data structure is shown below:

Example message:

```
CR LF I ^ ^ DDD ^ HH:MM:SS ^ DTZ=XX CR LF
```

Where:

CR	Carriage Return
LF	Line Feed

I	Time Sync Status (space, ?, *)
^	Space separator
DDD	Day of Year (001-366)
HH	Hours (00-23)
:	Colon separator
MM	Minutes (00-59)
SS	Seconds (00- 60)
D	Daylight Saving Time indicator (S,I,D,O)
TZ	Time Zone
XX	Time Zone offset (00-23)

The leading edge of the first character (CR) marks the on-time point of the data stream.

The time synchronization status character (I) is defined as described below:

(Space)	Whenever the front panel time synchronization lamp is green.
?	When the receiver is unable to track any satellites and the time synchronization lamp is red.
*	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The Daylight Saving Time indicator (D) is defined as:

S	During periods of Standard time for the selected DST schedule.
I	During the 24-hour period preceding the change into DST.
D	During periods of Daylight Saving Time for the selected DST schedule.
O	During the 24-hour period preceding the change out of DST.

Example:

271 12:45:36 DTZ=08

The example data stream provides the following information:

Sync Status	Time synchronized to GNSS
Date	Day 271

Time	12:45:36 Pacific Daylight Time
D	DST, Time Zone 08 = Pacific Time

8.1.5 Spectracom Format 1

Format 1 converts the received day of year data (001-366) to a date consisting of day of week, month, and day of the month. Format 1 also contains a time synchronization status character, year, and time reflecting time zone offset and DST correction when enabled.

Available Formats 1 and 1S are very similar to each other. Most external systems utilizing Data Format 1 will look for a single-digit day of the month for day 1 through day 9, with a space in front of each digit (^1, ^2, ^3 ... 10, 11...), whereas other systems need to see a two digit day of the month for all days 1 through 9 with a leading 0 instead of a space (01, 02, 03... 10, 11...).

- If your device requires the two digit day of the month for days 1 through 9 (i.e. 01, 02 etc.), select Format 1.
- If your device requires the single digit day of the month for days 1 through 9 (i.e. ^1, ^2, etc.), select Format 1S instead. Refer to "Spectracom Format 1S" on page 480 for information on Format 1S.

Format 1 data structure:

CR LF I ^ WWW ^ DDMMMYY ^ HH:MM:SS CR LF

Where:

CR	Carriage Return
LF	Line Feed
I	Time Sync Status (space, ?, *)
^	Space separator
WWW	Day of Week (SUN, MON, TUE, WED, THU, FRI, SAT)
DD	Numerical Day of Month (01-31)
MMM	Month (JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC)
YY	Year without century (99, 00, 01, etc.)
HH	Hours (00-23)
:	Colon separator
MM	Minutes (00-59)
SS	Seconds (00-60)

The leading edge of the first character (`CR`) marks the on-time point of the data stream.

The time synchronization status character (`I`) is defined as described below:

(Space)	Whenever the front panel time synchronization lamp is green.
?	When the receiver is unable to track any satellites and the time synchronization lamp is red.
*	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

Example:

FRI 20APR01 12:45:36

The example data stream provides the following information:

Sync Status	The clock is not time synchronized to GNSS. Time is derived from the battery backed clock or set manually
Date	Friday, April 23, 2015
Time	12:45:36

8.1.6 Spectracom Format 1S

Format 1S (Space) is very similar to Format 1, with the exception of a space being the first character of Days 1 through 9 of each month (instead of the leading “0” which is present in Format 1).

Most external systems utilizing Data Format 1 will look for a single digit day of the month for day 1 through day 9, with a space in front of each digit (^1, ^2, ^3 ... 10, 11...) whereas other systems need to see a two digit day of the month for all days 1 through 9 with a leading 0 instead of a space (01, 02, 03... 10, 11...).

- If your device requires the single digit day of the month for days 1 through 9 (i.e. 1, 2, etc.), select Format 1S.
- If your device requires the two digit day of the month for days 1 through 9 (i.e. 01, 02, etc.), select Format 1 instead. Refer to "Spectracom Format 1" on page 478 for information on Format 1.

Example message:

CR LF I ^ WWW ^ DDMMMYY ^ HH:MM:SS CR LF

Where:

CR	Carriage Return
LF	Line Feed
I	Time Sync Status (space, ?, *)
^	Space separator
WWW	Day of Week (SUN, MON, TUE, WED, THU, FRI, SAT)
DD	Numerical Day of Month (1-31)
MMM	Month (JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC)
YY	Year without century (99, 00, 01, etc.)
HH	Hours (00-23)
:	Colon separator

MM	Minutes (00-59)
SS	Seconds (00-60)

The leading edge of the first character (CR) marks the on-time point of the data stream.

The time synchronization status character (I) is defined as described below:

(Space)	Whenever the front panel time synchronization lamp is green.
?	When the receiver is unable to track any satellites and the time synchronization lamp is red.
*	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

Example:

FRI 20APR15 12:45:36

The example data stream provides the following information:

Sync Status	The clock is not time synchronized to GNSS. Time is derived from the battery backed clock or set manually.
Date	Friday April, 23, 2015
Time	12:45:36

8.1.7 Spectracom Format 2

This format provides a time data stream with millisecond resolution. The Format 2 data stream consists of indicators for time synchronization status, time quality, leap second and Daylight Saving Time. Time data reflects UTC time and is in the 24-hour format. Format 2 data structure is shown below:

Note: Format 2 cannot be configured for a Time Zone Offset or with automatic Daylight Saving Time adjustment. Attempting to configure a Local clock using Data Format 2 with either a Time Zone Offset or automatic DST rule will result in an error message.

Example message:

CR LF IQYY ^ DDD ^ HH:MM:SS.SSS ^ LD

Where:

CR	Carriage Return
LF	Line Feed
I	Time Sync Status (space, ?, *)
Q	Quality Indicator (space, A, B, C, D)
YY	Year without century (99, 00, 01, etc.)
^	Space separator
DDD	Day of Year (001-366)
HH	Hours (00-23 UTC time)
:	Colon separator
MM	Minutes (00-59)
:	Colon separator
SS	(00-60)
.	Decimal separator
SSS	Milliseconds (000-999)
L	Leap Second indicator (space, L)
D	Daylight Saving Time Indicator (S,I,D,O)

The leading edge of the first character (`CR`) marks the on-time point of the data stream.

The time synchronization status character (`I`) is defined as described below:

(Space)	Whenever the front panel time synchronization lamp is green.
?	When the receiver is unable to track any satellites and the time synchronization lamp is red.
*	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The quality indicator (`Q`) provides an inaccuracy estimate of the output data stream. When the receiver is unable to track any GNSS satellites, a timer is started. "Quality indicators" on the facing page lists the quality indicators and the corresponding error estimates based upon the GNSS receiver 1PPS stability, and the time elapsed tracking no satellites. The Tracking Zero Satellites timer and the quality indicator reset when the receiver reacquires a satellite.

Quality	Time (hours)	TXCO Error (milliseconds)	OCXO Error (milliseconds)	Rubidium Error (microseconds)
Space	Lock	<1	<0.01	<0.3
A	<10	<10	<0.72	<1.8
B	<100	<100	<7.2	<18
C	<500	<500	<36	<90
D	>500	>500	>36	>90

Table 8-1: Quality indicators

The leap second indicator (L) is defined as:

(Space)	When a leap second correction is not scheduled for the end of the month.
L	When a leap second correction is scheduled for the end of the month.

The Daylight Saving Time indicator (D) is defined as:

S	During periods of Standard time for the selected DST schedule.
I	During the 24-hour period preceding the change into DST.
D	During periods of Daylight Saving Time for the selected DST schedule.
O	During the 24-hour period preceding the change out of DST.

Example:

?A15 271 12:45:36.123 S

The example data stream provides the following information:

Sync Status	The clock has lost GNSS time sync. The inaccuracy code of "A" indicates the expected time error is <10 milliseconds.
Date	Day 271 of year 2015.
Time	12:45:36 UTC time, Standard time is in effect.

8.1.8 Spectracom Format 3

Format 3 provides a format identifier, time synchronization status character, year, month, day, time with time zone and DST corrections, time difference from UTC, Standard time/DST indicator, leap second indicator and on-time marker. The Format 3 data structure is shown below:

Example message:

FFFFI^YYYYMMDD^HHMMSS±HHMMD L # CR LF

Where:

FFFF	Format Identifier (0003)
I	Time Sync Status (Space, ?, *)
^	Space separator
YYYY	Year (1999, 2000, 2001, etc.)
MM	Month Number (01-12)
DD	Day of the Month (01-31)
HH	Hours (00-23)
MM	Minutes (00-59)
SS	Seconds (00-60)
±	Positive or Negative UTC offset (+,-) Time Difference from UTC
HHMM	UTC Time Difference Hours Minutes (00:00-23:00)
D	Daylight Saving Time Indicator (S,I,D,O)
L	Leap Second Indicator (space, L)
#	On time point
CR	Carriage Return
LF	Line Feed

The time synchronization status character (`I`) is defined as described below:

(Space)	Whenever the front panel time synchronization lamp is green.
?	When the receiver is unable to track any satellites and the time synchronization lamp is red.
*	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The time difference from UTC, ±HHMM, is selected when the Serial Com or Remote port is configured. A time difference of -0500 represents Eastern Time. UTC is represented by +0000.

The Daylight Saving Time indicator (`D`) is defined as:

S	During periods of Standard time for the selected DST schedule.
I	During the 24-hour period preceding the change into DST.
D	During periods of Daylight Saving Time for the selected DST schedule.
O	During the 24-hour period preceding the change out of DST.

The leap second indicator (L) is defined as:

(Space)	When a leap second correction is not scheduled for the end of the month.
L	When a leap second correction is scheduled for the end of the month.

Example:

0003 20150415 124536-0500D #

The example data stream provides the following information:

Data Format	3
Sync Status	Day 271 of year 2015.
Date	April 15, 2015.
Time	12:45:36 EDT (Eastern Daylight Time). The time difference is 5 hours behind UTC.
Leap Second	No leap second is scheduled for this month.

8.1.9 Spectracom Format 4

Format 4 provides a format indicator, time synchronization status character, modified Julian date, time reflecting UTC with 0.1 millisecond resolution and a leap second indicator. Format 4 data structure is shown below:

Example:

FFFFIMJDXX^HHMMSS.SSSS^L CR LF

Where:

FFFF	Format Identifier (0004)
I	Time Sync Status (Space, ?, *)

MJDXX	Modified Julian Date
^	Space separator
HH	Hours (00-23 UTC time)
MM	Minutes (00-59)
SS.SSSS	Seconds (00.0000-60.0000)
L	Leap Second Indicator (space, L)
CR	Carriage Return
LF	Line Feed

The start bit of the first character marks the on-time point of the data stream.

The time synchronization status character (`I`) is defined as described below:

(Space)	Whenever the front panel time synchronization lamp is green.
?	When the receiver is unable to track any satellites and the time synchronization lamp is red.
*	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The leap second indicator (`L`) is defined as:

(Space)	When a leap second correction is not scheduled for the end of the month.
L	When a leap second correction is scheduled for the end of the month.

Example:

0004 50085 124536.1942 L

The example data stream provides the following information:

Data format	4
Sync Status	Time synchronized to GNSS.
Modified Julian Date	50085
Time	12:45:36.1942 UTC
Leap Second	A leap second is scheduled at the end of the month.

8.1.10 Spectracom Format 7

This format provides a time data stream with millisecond resolution. The Format 7 data stream consists of indicators for time synchronization status, leap second and Daylight Saving Time. Time data reflects UTC time and is in the 24-hour format. Format 7 data structure is shown below:

Note: Format 7 cannot be configured for a Time Zone Offset or with automatic Daylight Saving Time adjustment. Attempting to configure a Local clock using Data Format 7 with either a Time Zone Offset or automatic DST rule will result in an error message.

Example message:

CR LF I^YY^DDD^HH:MM:SS.SSSL^D CR LF

Where:

CR	Carriage Return
LF	Line Feed
I	Time Sync Status (space, ?, *)
YY	Year without century (99, 00, 01, etc.)
^	Space separator
DDD	Day of Year (001-366)
HH	Hours (00-23 UTC time)
:	Colon separator
MM	Minutes (00-59)
SS	Seconds (00-60)

.	Decimal Separator
SSS	Milliseconds (000-999)
L	Leap Second Indicator (space, L)
D	Daylight Saving Time Indicator (S,I,D,O)

The leading edge of the first character (CR) marks the on-time point of the data stream.

The time synchronization status character (I) is defined as described below:

(Space)	Whenever the front panel time synchronization lamp is green.
?	When the receiver is unable to track any satellites and the time synchronization lamp is red.
*	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The leap second indicator (L) is defined as:

(Space)	When a leap second correction is not scheduled for the end of the month.
L	When a leap second correction is scheduled for the end of the month.

The Daylight Saving Time indicator (D) is defined as:

S	During periods of Standard time for the selected DST schedule.
I	During the 24-hour period preceding the change into DST.
D	During periods of Daylight Saving Time for the selected DST schedule.
O	During the 24-hour period preceding the change out of DST.

Example:

? 15 271 12:45:36.123 S

The example data stream provides the following information:

Sync Status	The clock has lost GNSS time sync.
Date	Day 271 of year 2015.
Time	12:45:36 UTC time, Standard time is in effect.

8.1.11 Spectracom Format 8

Format 8 includes a time synchronization status character, the four digit year, day of year, time reflecting Time Zone Offset and DST corrections when enabled. Format 8 also includes the

DST/Standard Time indicator, and the Time Zone Offset value. Format 8 data structure is shown below:

Example:

CR LF I ^ ^YYYY^ DDD ^ HH:MM:SS ^ D+XX CR LF
or
CR LF I ^ ^YYYY^ DDD ^ HH:MM:SS ^ D-XX CR LF

Where:

CR	Carriage Return
LF	Line Feed
I	Time Sync Status (space, ?, *)
YYYY	Four digit year indication
^	Space separator
DDD	Day of Year (001-366)
HH	Hours (00-23)
:	Colon separator
MM	Minutes (00-59)
SS	Seconds (00-60)
D	Daylight Saving Time indicator (S,I,D,O)
XX	Time Zone Switch Setting (±00…12)

The leading edge of the first character (`CR`) marks the on-time point of the data stream. Time sync status character (`I`) is described below:

(Space)	When SecureSync is synchronized to UTC source.
*	When SecureSync time is set manually.
?	When SecureSync has not achieved or has lost synchronization to UTC source.

The time and date can be set to either local time or UTC time, depending upon the configuration of the output port.

8.1.12 Spectracom Format 9

Format 9 provides Day-of-Year and Time information.

Example message:

<SOH>DDD:HH:MM:SSQ<CR><LF>

Where:

SOH	Start of header (ASCII Character 1)
DDD	Day of Year (001-366)
:	Colon Separator
HH	Hours (00-23)
MM	Minutes (00-59)
SS	Seconds (00-59) (00-60 for leap second)
Q	Time Sync Status [as INPUT] space = SYNC ‘.’ = SYNC ‘*’=NOT IN SYNC ‘#’ = NOT IN SYNC “?” = NOT IN SYNC
Q	Time Sync Status [as OUTPUT] space = Time error is less than time quality flag 1's threshold (TFOM < or = 3) “.” = Time error has exceeded time quality flag 1's threshold (TFOM = 4) “*” = Time error has exceeded time quality flag 2's threshold (TFOM = 5) “#” = Time error has exceeded time quality flag 3's threshold (TFOM = 6) “?” = Time error has exceeded time quality flag 4's threshold OR a reference source is unavailable (TFOM >=7)
CR	Carriage Return (ASCII Character 13)
LF	Line Feed (ASCII Character 10)

The leading edge of the first character (`CR`) marks the on-time point of the data stream.

8.1.13 Spectracom Epsilon Formats

8.1.13.1 Spectracom Epsilon TOD 1

This message corresponds to the TOD 1 format provided by EPSILON 2S/3S Series products on RS232/422 ports.

The structure of this format is as follows:

- <space>DD/MM/YYYY<space>HH:MM:SST(CR)(LF)

Length=23 bytes

Where:

<space>	separator
DD	2-digit Day of month
</>	separator
MM	2-digit Month
</>	separator
YYYY	4-digit Year
<space>	separator
HH	2-digit Hour
:	separator
MM	2-digit Minutes
:	separator
SS	2-digit Seconds
T	1-digit Timescale ('N' None, 'G' GPS, 'U' UTC, 'A' TAI, 'L' Local, 'M' Manual)
(CR)	Carriage Return (ASCII Character 13 0x0D)
(LF)	Line Feed (ASCII Character 10 0x0A)

8.1.13.2 Spectracom Epsilon TOD 3

This message corresponds to the TOD 3 format provided by EPSILON 2S/3S Series products on RS232/422 ports.

The structure of this format is as follows:

- <space>DOY/YYYY<space>HH:MM:SS<space>T(CR)(LF)

Length=22 bytes

Where:

<space>	separator
DOY	3-digit Day of year
</>	separator
YYYY	4-digit Year

</>	separator
YYYY	4-digit Year
<space>	separator
HH	2-digit Hour
:	separator
MM	2-digit Minutes
:	separator
SS	2-digit Seconds
T	1-digit Timescale ('N' None, 'G' GPS, 'U' UTC, 'A' TAI, 'L' Local, 'M' Manual)
(CR)	Carriage Return (ASCII Character 13 0x0D)
(LF)	Line Feed (ASCII Character 10 0x0A)

8.1.14 BBC Message Formats

8.1.14.1 Format BBC-01

This format is based on string ASCII characters, and is sent once per second. It provides year, month, day, day of week, day of month, hours, minutes, and seconds.

Number of characters: 24 (including CRLF and '.')

Example message:

```
T:ye:mo:da:dw:ho:mi:sc
```

Where:

T	Indicates the synchronous moment for the time setting.
ye	Year (00-99)
mo	Month (01-12)
da	Day of month (01-31)
dw	Day of week (01=Monday to 7=Sunday)
ho	Hours (00-23)
mi	Minutes (00-59)
sc	Seconds (00-59)

8.1.14.2 Format BBC-02

This is a hexadecimal frame/message sent twice per second. The message should be sent such that the final "99" occurs at 0 msec and 500 msec.

Number of bytes: 26

Format:

START		Year		Month	Day	Hour	Min	Sec.
AA	AA	07	DA	06	16	13	59	01

Millisecond		Time Zone		Daylight	Leap-second Sign	Leap-second Month	Leap-second Zone	GPS Week	
02	BA	80	00	00	00	00	00	1A	2A

GPS Second			GPS to UTC Offset	Check-sum	END	
09	3A	7E	12	FE	99	99

Where:

Leap Second Sign:

- 01=Positive
- FF=Negative
- 00=No leap second

Leap Second Month:

- 00=None scheduled
- 03=March
- 06=June
- 09=September
- 0C=December

Leap Second Zone:

- 0=Out of zone
- 1=Within zone
- Zone is 15 minutes before to 15 minutes after a leap second.

GPS Week:

- Up to FFFF

GPS Second:

- Second of week 000000 up to 093A7F (604799 decimal)

GPS to UTC offset:

- 2's complement binary signed integer, seconds

Checksum:

- Sum of all bytes up to and including the checksum (sum includes the AAAA start identifier but excludes the 9999 end identifier)

8.1.14.3 Format BBC-03 PSTN

The third format is a string ASCII characters and is sent on a received character.

The message should be advanced by an appropriate number such that the stop bit of each <CR> occurs at the start of the next second. For example, at 300 baud, 8 data bits, 1 stop bit, and no parity, each byte takes 10/300 s=33 ms, so the <CR> byte should be advanced by 33 ms in order for the <CR>'s stop bit to line up with the start of the next second.

Time information is available in UTC format or UK TOD format.

‘t’ command

Input format: t<CR>

Output format:

Current Second	Second + 1	Second + 2	Second + 3
<CR>	HHMMSS<CR>	HHMMSS<CR>	HHMMSS<CR>

Number of characters: 7 (including CR)

Each HHMMSS filed refers to the time at the start of the next second. The data transmitted by SecureSync is timed so that the stop bit of each <CR> ends at the start of the next second.

‘d’ command

SecureSync transmits the date on request.

Input format: d<CR>

Output format: YYMMDD<CR>

Number of output characters: 7 (including CR)

‘s’ command

SecureSync transmits the status information on request.

Input format: s<CR>

Output Format: status

Number of output characters: 1

Where returned, values for status are:

- G = System Good
- D = Failure of SecureSync internal diagnostics
- T = SecureSync does not have correct time

‘l’ command

The loopback command will cause SecureSyncto echo the next character received back to the caller. This may be used by a caller’s equipment to calculate the round trip delay across the PSTN connection in order to apply a correction to the received time data.

Input format: l<CR>

Output format: (Next character received)

‘hu’ command

The hang up command will cause SecureSync to drop the line immediately and terminate the call.

Input format: `hu<CR>`

8.1.14.4 Format BBC-04

This format is a string of ASCII characters and is sent once per second.

Number of characters: 18 (including CRLF)

Example message:

```
T:ho:mi:sc:dw:da:mo:ye:lp:cs<CR><LF>
```

Where:

T	Indicates the synchronous moment for the time setting.
ho	Hours (00-23)
mi	Minutes (00-59)
sc	Seconds (00-59)
dw	Day of week (01=Monday to 7=Sunday)
da	Day of month (01-31)
mo	Month (01-12)
ye	Year (00-99)
lp	0 (for 60s, no leap) or 1 (for 61s, leap)
cs	Checksum. This is calculated from the start of the message, including start identifier and excluding CRLF. It is created by adding all the 1s. If the sum is even, 0 is returned. If the sum is odd, 1 is returned. This is mathematically the same as sequentially running an XOR on each bit of each byte.

Standard Serial configuration is:

- RS-232 format
- 9600 baud
- 8 data bits

- 1 stop bit
- No parity

8.1.14.5 Format BBC-05 (NMEA RMC Message)

The NMEA Message Format RMC, (Recommended Minimum) provides fix information, speed over ground and Magnetic Variance information. Note that this RMC Message is not 100% identical to the official NMEA RMC MESSAGE (that corresponds to the 3.01 NMEA 0183 standard and is another time code format supported by SecureSync.)

The BBC RMC message (BBC-05) corresponds to Version 2 of the NMEA 0183 standard, following the description below:

Example message:

```
$GPRMC,123519,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A
```

Where:

RMC	Recommended Minimum sentence C
123519	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
22.4	Speed over the ground in knots
84.4	Track angle in degrees True
230394	Date–23rd of March 1994
003.1,W	Magnetic Variation
*6A	The checksum data, always begins with *

8.1.15 GSSIP Message Format

The GSSIP[1] format includes 3 ICD-GPS-153C messages which are used to support emulation of a SAASM GPS used in a SINCGARS interface. The messages are the Buffer Box (253), Time Transfer (5101), and the Current Status (5040).

[1] GSSIP = GPS STANDARD SERIAL INTERFACE PROTOCOL

The ICD-GPS-153C protocol defines the format of these messages. The Current Status and Time Transfer are sent once per second (1Hz). The Buffer Box is sent once every 6 seconds (1/6 Hz).

The purpose of these three messages is to emulate a SINCGARS interface connection to a SAASM GPS. SecureSync generates these messages emulating the Time and 1PPS transfer behavior of the SINCGARS interface. An external device compatible with the SINCGARS interface can attach to an ASCII Output from SecureSync and receive time and 1PPS as if communicating with and ICD-GPS-153C compatible SAASM GPS.

These commands are emulated only and contain only time information; position and velocity information is zeroed out. No controlled data is included in the messages, hence no SAASM GPS receiver is required.

The ASCII Output supports two configurations for supporting SINCGARS:

A configuration of Time Transfer as Message Format1 and Current Status as Format2 causes the SINCGARS protocol to be emulated and the machine state to be initializated.

- **Format1**: Time Transfer (5101)
- **Format2**: Current Status (5040)
- **Format3**: Buffer Box (253)

A configuration of Current Status as Message Format1 and Time Transfer as Format2 results in broadcasting of the messages Current Status (1Hz), Time Transfer (1Hz), and Buffer Box (1/6Hz) at their default rates.

- **Format1**: Current Status (5040)
- **Format2**: Time Transfer (5101)
- **Format3**: Buffer Box (253)

8.1.16 EndRun Formats

The following formats provide compatibility with **EndRun** technology.

8.1.16.1 EndRun Time Format

Example message:

T YYYY DDD HH:MM:SS zZZ m<CR><LF>

Where:

T	Time Figure of Merit character (TFOM), limited to the range 6 to 9: 9 indicates error >±10 milliseconds, or unsynchronized condition 8 indicates error <±10 milliseconds 7 indicates error <±1 millisecond 6 indicates error <±100 microseconds
YYYY	Year
DDD	Day of Year (001-366)
HH	Hour of the day (00-23)
:	Colon Separator
MM	Minutes of the hour
SS	Seconds (00-59), (00-60 for leap second)
z	The sign of the offset to UTC, + implies time is ahead of UTC
ZZ	The magnitude of the offset to UTC in units of half-hours. If ZZ = 0, then z = +

m	Time mode character, is one of:
	G = GPS
	L = Local
	U = UTC
	T = TAI

CR	Carriage Return
LF	Line Feed

8.1.16.2 EndRunX (Extended) Time Format

The **EndRunX** format is identical to the **EndRun** format, with the addition of two fields: the current leap second settings and the future leap second settings.

The following example message string is sent once each second:

```
T YYYY DDD HH:MM:SS zZZ m CC FF<CR><LF>
```

Where:

T	Time Figure of Merit character (TFOM), limited to the range 6 to 9: 9 indicates error >±10 milliseconds, or unsynchronized condition 8 indicates error <±10 milliseconds 7 indicates error <±1 millisecond 6 indicates error <±100 microseconds
YYYY	Year
DDD	Day of Year (001-366)
HH	Hour of the day (00-23)
:	Colon Separator
MM	Minutes of the hour
SS	Seconds (00-59), (00-60 for leap second)
z	The sign of the offset to UTC, + implies time is ahead of UTC
ZZ	The magnitude of the offset to UTC in units of half-hours. If ZZ = 0, then z = +

m	Time mode character, is one of:
	G = GPS
	L = Local
	U = UTC
	T = TAI

CC	The current leap seconds
FF	The future leap seconds, which will show a leap second pending 24 hours in advance
CR	Carriage Return
LF	Line Feed

8.2 IRIG Standards and Specifications

8.2.1 IRIG Carrier Frequencies

Each IRIG code specifies a carrier frequency that is modulated to encode date and time, as well as control bits to time-stamp events. Initially, IRIG applications were primarily military and government associated. Today, IRIG is commonly used to synchronize voice loggers, recall recorders, and sequential event loggers found in emergency dispatch centers and power utilities.

Format	Encoding	Modulation	Carrier	Coded Expressions	Bit rate	Time Frame Interval
			IRIG-A			
IRIG-A	A000	DCLS	N/A	BCD_{TOY}, CF and SBS	1000 pps	0.1 sec
IRIG-A	A001	DCLS	N/A	BCD_{TOY}, CF	1000 pps	0.1 sec
IRIG-A	A002	DCLS	N/A	BCD_{TOY}	1000 pps	0.1 sec
IRIG-A	A003	DCLS	N/A	BCD_{TOY}, SBS	1000 pps	0.1 sec
IRIG-A	A004	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, CF and SBS	1000 pps	0.1 sec
IRIG-A	A005	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and CF	1000 pps	0.1 sec
IRIG-A	A006	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}	1000 pps	0.1 sec
IRIG-A	A007	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and SBS	1000 pps	0.1 sec
IRIG-A	A130	AM	10 kHz	BCD_{TOY}, CF and SBS	1000 pps	0.1 sec
IRIG-A	A131	AM	10 kHz	BCD_{TOY}, CF	1000 pps	0.1 sec
IRIG-A	A132	AM	10 kHz	BCD_{TOY}	1000 pps	0.1 sec
IRIG-A	A133	AM	10 kHz	BCD_{TOY}, SBS	1000 pps	0.1 sec
IRIG-A	A134	AM	10 kHz	BCD_{TOY}, BCD_{YEAR}, CF and SBS	1000 pps	0.1 sec
IRIG-A	A135	AM	10 kHz	BCD_{TOY}, BCD_{YEAR}, and CF	1000 pps	0.1 sec
IRIG-A	A136	AM	10 kHz	BCD_{TOY}, BCD_{YEAR}	1000 pps	0.1 sec
IRIG-A	A137	AM	10 kHz	BCD_{TOY}, BCD_{YEAR}, and SBS	1000 pps	0.1 sec
			IRIG-B			

Format	Encoding	Modulation	Carrier	Coded Expressions	Bit rate	Time Frame Interval
IRIG-B	B000	DCLS	N/A	BCD$_{TOY}$, CF and SBS	100 pps	1 sec
IRIG-B	B001	DCLS	N/A	BCD$_{TOY}$, CF	100 pps	1 sec
IRIG-B	B002	DCLS	N/A	BCD$_{TOY}$	100 pps	1 sec
IRIG-B	B003	DCLS	N/A	BCD$_{TOY}$, SBS	100 pps	1 sec
IRIG-B	B004	DCLS	N/A	BCD$_{TOY}$, BCD$_{YEAR}$, CF and SBS	100 pps	1 sec
IRIG-B	B005	DCLS	N/A	BCD$_{TOY}$, BCD$_{YEAR}$, and CF	100 pps	1 sec
IRIG-B	B006	DCLS	N/A	BCD$_{TOY}$, BCD$_{YEAR}$	100 pps	1 sec
IRIG-B	B007	DCLS	N/A	BCD$_{TOY}$, BCD$_{YEAR}$, and SBS	100 pps	1 sec
IRIG-B	B120	AM	1 kHz	BCD$_{TOY}$, CF and SBS	100 pps	1 sec
IRIG-B	B121	AM	1 kHz	BCD$_{TOY}$, CF	100 pps	1 sec
IRIG-B	B122	AM	1 kHz	BCD$_{TOY}$	100 pps	1 sec
IRIG-B	B123	AM	1 kHz	BCD$_{TOY}$, SBS	100 pps	1 sec
IRIG-B	B124	AM	1 kHz	BCD$_{TOY}$, BCD$_{YEAR}$, CF and SBS	100 pps	1 sec
IRIG-B	B125	AM	1 kHz	BCD$_{TOY}$, BCD$_{YEAR}$, and CF	100 pps	1 sec
IRIG-B	B126	AM	1 kHz	BCD$_{TOY}$, BCD$_{YEAR}$	100 pps	1 sec
IRIG-B	B127	AM	1 kHz	BCD$_{TOY}$, BCD$_{YEAR}$, and SBS	100 pps	1 sec
IRIG-E						
IRIG-E	E000	DCLS	N/A	BCD$_{TOY}$, CF and SBS	10 pps	1 sec
IRIG-E	E001	DCLS	N/A	BCD$_{TOY}$, CF	10 pps	1 sec
IRIG-E	E002	DCLS	N/A	BCD$_{TOY}$	10 pps	1 sec
IRIG-E	E003	DCLS	N/A	BCD$_{TOY}$, SBS	10 pps	1 sec
IRIG-E	E004	DCLS	N/A	BCD$_{TOY}$, BCD$_{YEAR}$, CF and SBS	10 pps	1 sec
IRIG-E	E005	DCLS	N/A	BCD$_{TOY}$, BCD$_{YEAR}$, and CF	10 pps	1 sec

Format	Encoding	Modulation	Carrier	Coded Expressions	Bit rate	Time Frame Interval
IRIG-E	E006	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}	10 pps	1 sec
IRIG-E	E007	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and SBS	10 pps	1 sec
IRIG-E	E110	AM	100 Hz	BCD_{TOY}, CF and SBS	10 pps	1 sec
IRIG-E	E111	AM	100 Hz	BCD_{TOY}, CF	10 pps	1 sec
IRIG-E	E112	AM	100 Hz	BCD_{TOY}	10 pps	1 sec
IRIG-E	E113	AM	100 Hz	BCD_{TOY}, SBS	10 pps	1 sec
IRIG-E	E114	AM	100 Hz	BCD_{TOY}, BCD_{YEAR}, CF and SBS	10 pps	1 sec
IRIG-E	E115	AM	100 Hz	BCD_{TOY}, BCD_{YEAR}, and CF	10 pps	1 sec
IRIG-E	E116	AM	100 Hz	BCD_{TOY}, BCD_{YEAR}	10 pps	1 sec
IRIG-E	E117	AM	100 Hz	BCD_{TOY}, BCD_{YEAR}, and SBS	10 pps	1 sec
IRIG-E	E120	AM	100 Hz	BCD_{TOY}, CF and SBS	10 pps	1 sec
IRIG-E	E121	AM	1kHz	BCD_{TOY}, CF	10 pps	10 sec
IRIG-E	E122	AM	1kHz	BCD_{TOY}	10 pps	10 sec
IRIG-E	E123	AM	1kHz	BCD_{TOY}, SBS	10 pps	10 sec
IRIG-E	E124	AM	1kHz	BCD_{TOY}, BCD_{YEAR}, CF and SBS	10 pps	10 sec
IRIG-E	E125	AM	1kHz	BCD_{TOY}, BCD_{YEAR}, and CF	10 pps	10 sec
IRIG-E	E126	AM	1kHz	BCD_{TOY}, BCD_{YEAR}	10 pps	10 sec
IRIG-E	E127	AM	1kHz	BCD_{TOY}, BCD_{YEAR}, and SBS	10 pps	10 sec
IRIG-G						
IRIG-G	G001	DCLS	N/A	BCD_{TOY}, CF	10000 pps	10 msec
IRIG-G	G002	DCLS	N/A	BCD_{TOY}	10000 pps	10 msec

Format	Encoding	Modulation	Carrier	Coded Expressions	Bit rate	Time Frame Interval
IRIG-G	G005	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and CF	10000 pps	10 msec
IRIG-G	G006	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}	10000 pps	10 msec
IRIG-G	G141	AM	100 kHz	BCD_{TOY}, CF	10000 pps	10 msec
IRIG-G	G142	AM	100 kHz	BCD_{TOY}	10000 pps	10 msec
IRIG-G	G145	AM	100 kHz	BCD_{TOY}, BCD_{YEAR}, and CF	10000 pps	10 msec
IRIG-G	G146	AM	100 kHz	BCD_{TOY}, BCD_{YEAR}	10000 pps	10 msec
NASA-36	N/A	AM	1msec	UNKNOWN	100 pps	1 sec
NASA-36	N/A	DCLS	10 msec	UNKNOWN	100 pps	1 sec

Table 8-2: Available IRIG output signals

The Spectracom IRIG formats use the control functions for BCD year information and a Time Sync Status bit and in format E the control functions are used for straight binary seconds (SBS). Refer to individual IRIG Time Code description figures and text. IRIG Standard 200-98 format B had 27 control bits and format E had 45 bits for control functions. These control bits could be used for any use and there was no defined function. Spectracom used the control function element at index count 55 as the TIME SYNC STATUS and the sub-frame after position identifiers P6 and P7 as the year info and for format E the sub-frame after P8 and P9 for the straight binary seconds (SBS). The position of the BCD year information does not conform to the newer IRIG Standard 200-04. IRIG Standard 200-04 incorporated the year information after P5 and reduced the allocated control bits to 18 for format B and 36 for format E.

Note: DCLS is DC Level Shifted output, pulse width modulated with a position identifier having a positive pulse width equal to 0.8 of the reciprocal of the bit rate, a binary one (1) having a positive pulse width equal to 0.5 of the reciprocal of the bit rate and a binary zero (0) having a positive pulse width equal to 0.2 of the reciprocal of the bite rate.

SecureSync can provide IRIG A, IRIG B, IRIG E and IRIG G code in amplitude modulated (AM) or pulse width coded (TTL) formats. A signature control feature may be enabled for any IRIG output. Signature control removes the modulation code when a Time Sync Alarm is asserted.

8.2.2 IRIG B Output

The IRIG B Time Code description follows.

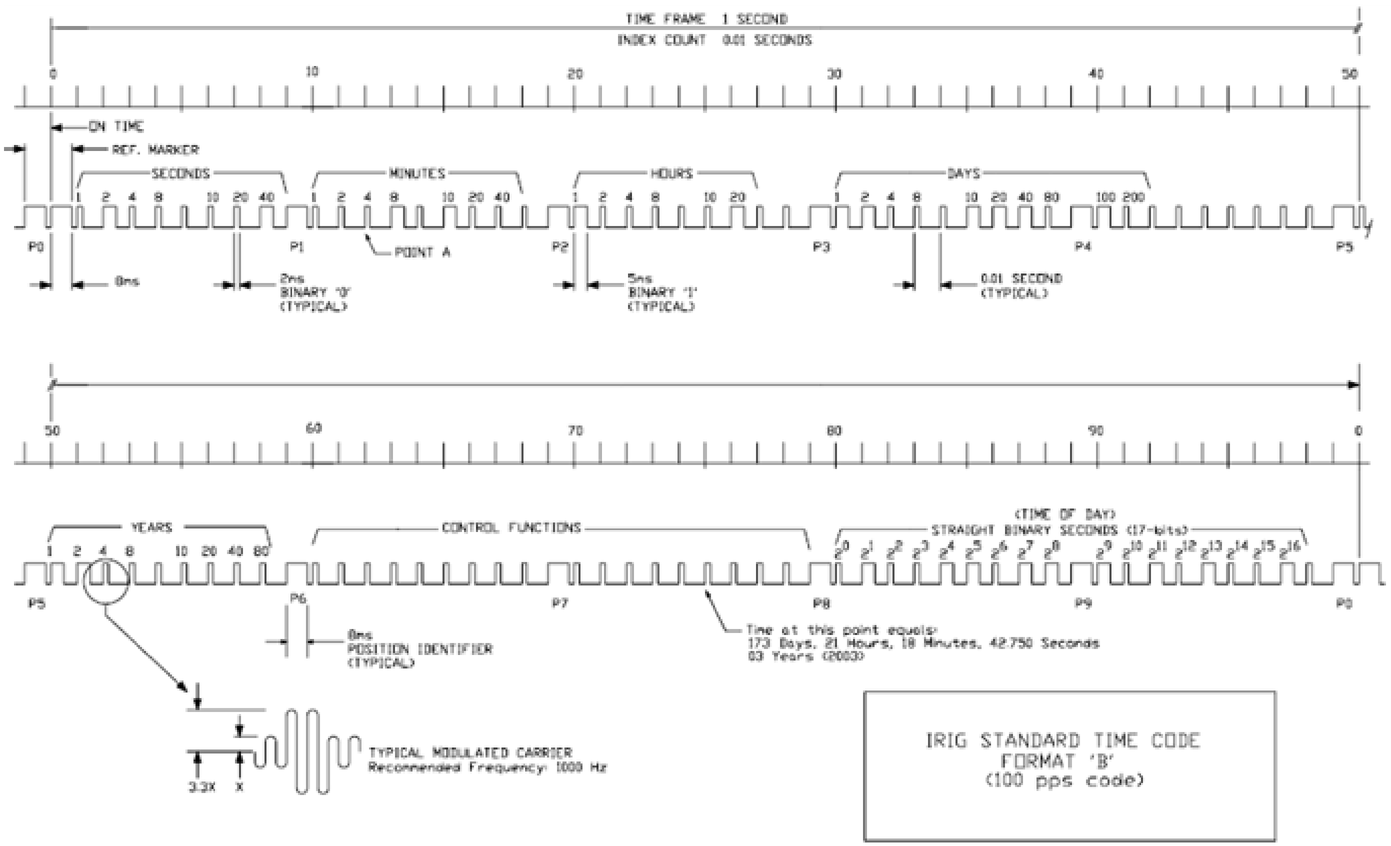


Figure 8-1: IRIG B time code description

The IRIG B code contains the Binary Coded Decimal (BCD) time of year, Control Function (CF) field and the Straight Binary Seconds time of day. The following figure illustrates the IRIG B data structure. The BCD time of year provides the day of the year, 1-366, and the time of day including seconds. The hour of the day is expressed in 24 hour format. The SBS time is the number of seconds elapsed since midnight. The Control Function field contains year information and a time synchronization status bit.

1. Time frame: 1.0 seconds.
2. Code digit weighting:
   A. Binary Coded Decimal time-of-year.
   - Code word - 30 binary digits.
   - Seconds, minutes hours, and days.
   - Recycles yearly.

   B. Straight Binary Seconds time-of-day.
   - Code word - 17 binary digits.
   - Seconds only, recycles daily.
3. Code word structure:

- **BCD**: Word seconds digits begin at index count 1. Binary coded elements occur between position identifier elements P0 and P5 (7 for seconds, 7 for minutes, 6 for hours, and 10 for days) until the code word is complete. An index marker occurs between decimal digits in each group to provide separation for visual resolution. Least significant digit occurs first.
- **CF**: IRIG formats reserve a set of elements known as Control Functions (CF) for the encoding of various control, identification, or other special purpose functions. IRIG B has 27 Control Functions located between elements 50 and 78. The SecureSync uses the Control Functions to encode year information and time synchronization status.

The table below lists the Control Function Field and the function of each element.

- Element 55 is the time synchronization status bit. Element 55 is a Binary 1 when the front panel time synchronization lamp is green, and a Binary 0 when the lamp is red.
- Year information consists of the last two digits of the current year (i.e. 97, 98, 99 etc.). Elements 60 through 63 contain the binary equivalent of year units. Elements 65 through 68 contain the binary equivalent of tens of years. In keeping with IRIG formats, the least significant bit occurs first. All unused Control Functions are filled with a space (Binary 0).
- **SBS**: Word begins at index count 80. Seventeen Straight Binary Coded elements occur with a position identifier between the 9th and 10th binary coded elements. Least significant digit occurs first.

- Pulse rates:
  - Element rate: 100 per second.
  - Position identifier rate: 10 per second.
  - Reference marker rate: 1 per second.
- Element identification: The "on time" reference point for all elements is the pulse leading edge.
  - Index marker (Binary 0 or uncoded element): 2 millisecond duration.
  - Code digit (Binary 1): 5 millisecond duration.
  - Position identifier: 8 millisecond duration.
- Reference marker, 1 per second. The reference marker appears as two consecutive position identifiers. The second position identifier marks the on-time point for the succeeding code word.
- Resolution:
  - Pulse width coded signal: 10 milliseconds.
  - Amplitude modulated signal: 1 millisecond.
- Carrier frequency: 1 kHz when modulated.

C.F. Element #	Digit #	Function
50	1	Space
51	2	Space
52	3	Space
53	4	Space
54	5	Space
55	6	Time Sync Status
56	7	Space
57	8	Space
58	9	Space
59	PID P6	Position Identifier
60	10	Years Units Y1
61	11	Years Units Y2
62	12	Years Units Y4

C.F. Element #	Digit #	Function
63	13	Years Units Y8
64	14	Space
65	15	Years Tens Y10
66	16	Years Tens Y20
67	17	Years Tens Y40
68	18	Years Tens Y80
69	PID P7	Position Identifier
70	19	Space
71	20	Space
72	21	Space
73	22	Space
74	23	Space
75	24	Space
76	25	Space
77	26	Space
78	27	Space

Table 8-3: IRIG B control function field

8.2.3 IRIG E Output

The IRIG E code contains the Binary Coded Decimal (BCD) time of year and Control Functions. The figure IRIG E Time Code Description illustrates the IRIG E data structure. The BCD time of year provides the day of year, 1-366, and time of day to tens of seconds. The hour of the day is expressed in 24 hour format. The Control Function field includes a time synchronization status bit, year information and SBS time of day.

- Time frame: 10 seconds.
- Code Digit Weighting:
  - Binary Coded Decimal time of year.
  - Code world - 26 binary digits.

- Tens of seconds, minutes, hours, and days.
- Recycles yearly.

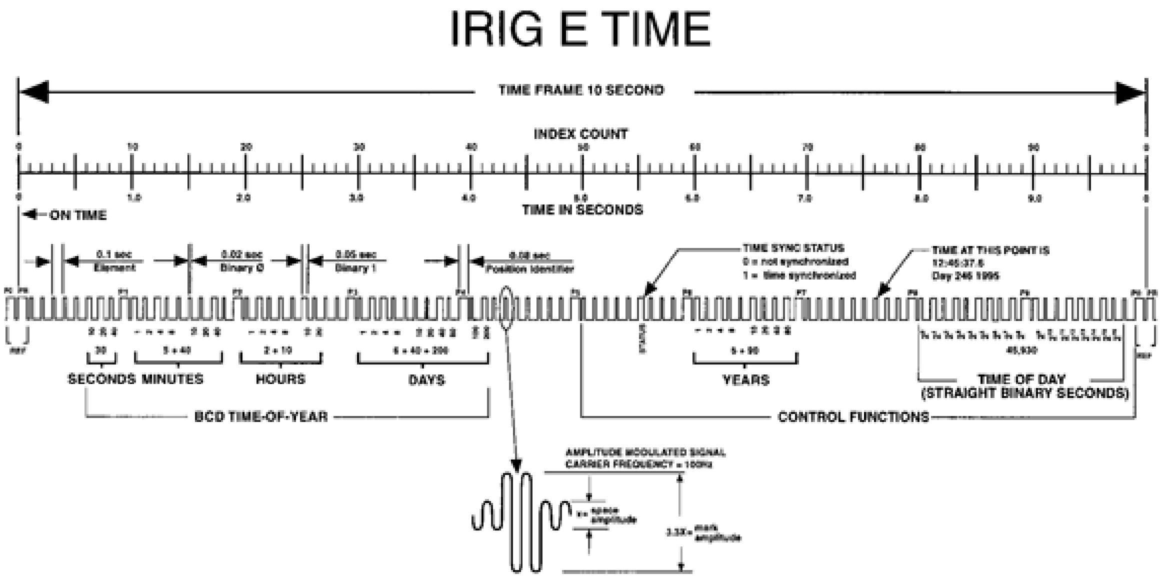
- **Code Word Structure**: BCD word tens of seconds digits begin at index count 6. Binary coded elements occur between position identifier elements P0 and P5 (3 for seconds, 7 for minutes, 6 for hours, and 10 for days) until the code word is complete. An index marker occurs between decimal digits in each group to provide separation for visual resolution. Least significant digit occurs first.
- **Control Functions**: IRIG formats reserve a set of elements known as Control Functions (CF) for the encoding of various control, identification, or other special purpose functions. IRIG E has 45 Control Functions located between elements 50 and 98. The SecureSync uses the Control Function field to encode year data, time synchronization status, and SBS time data. Table B-2 lists the Control Function Field and each element's function.

Element 55 is the time synchronization status bit. Element 55 is a Binary 1 when the front panel time synchronization lamp is green, and a Binary 0 when the lamp is red.

Year information consists of the last two digits of the current year (i.e. 98, 99, etc.). Elements 60 through 63 contain the binary equivalent of year units. Elements 65 through 68 contain the binary equivalent of tens of years. In keeping with IRIG formats, the least significant bit occurs first.

Elements 80 through 97 are encoded with the Straight Binary Seconds (SBS) time data. The SBS time data is incremented in 10-second steps and recycles every 24 hours.

- Pulse rates:
  - Element rate: 10 per second.
  - Position identifier rate: 1 per second.
  - Reference marker rate: 1 per 10 seconds.
- Element identification: The "on time" reference point for all elements is the pulse leading edge.
- Index marker (Binary 0 or uncoded element): 20 millisecond duration.
- Code digit (Binary 1): 50 millisecond duration.
- Position identifier: 80 millisecond duration.
- Reference marker: 80 millisecond duration, 1 per 10 seconds. The reference marker appears as two consecutive position identifiers. The second position identifier or reference marker is the on-time point for the succeeding code word.



Specific

The beginning of each 10 second time frame is identified by two consecutive 80 ms elements (P_0 and P_R). The leading edge of the second 80 ms element (P_R) is the "on time" reference point for the succeeding time code. 1 pps position identifiers P_0, P_1,......P_9 (80 ms duration) occur 0.1 second before 1 pps "on time" and refer to the leading edge of the succeeding element.

The time code word and the control functions presented during the time frame are pulse width coded. The binary "zero" and index markers have a duration of 20 ms, and the binary "one" has a duration of 50 ms. The leading edge is the 10 pps "on time" reference point for all elements.

The binary coded decimal (BCD) time-of-year code word consists of 26 digits beginning at index count 6. The binary coded subword elements occur between position identifiers P_0 and P_5 (3 for seconds; 7 for minutes; 6 for hours; 10 for days) until the code word is complete. An index marker occurs between the decimal digits in each subword to provide separation for visual resolution. The least significant digit occurs first. The BCD code recycles yearly.

Forty-five control functions occur between position identifiers P_5 and P_9. Any control function element or combination of control function elements can be programmed to read a binary "one" during any specified number of time frames. Each control element is identified on the Control Function Field Table.

Figure 8-2: IRIG E time code description

BIT No.	CF ELEMENT No.	FUNCTION
50	1	SPACE

BIT No.	CF ELEMENT No.	FUNCTION
51	2	SPACE
52	3	SPACE
53	4	SPACE
54	5	SPACE
55	6	TIME SYNC_STATUS
56	7	SPACE
57	8	SPACE
58	9	SPACE
59	PID P6	POSITION IDENTIFIER
60	10	YEAR UNITS Y1
61	11	YEAR UNITS Y2
62	12	YEAR UNITS Y4
63	13	YEAR UNITS Y8
64	14	SPACE
65	15	YEAR TENS Y10
66	16	YEAR TENS Y20
67	17	YEAR TENS Y40
68	18	YEAR TENS Y80
69	PID P7	POSITION IDENTIFIER
70	19	SPACE
71	20	SPACE
72	21	SPACE
73	22	SPACE
74	23	SPACE
75	24	SPACE
76	25	SPACE
77	26	SPACE
78	27	SPACE

BIT No.	CF ELEMENT No.	FUNCTION
79	PID P8	POSITION IDENTIFIER
80	28	SBS 20
81	29	SBS 21
82	30	SBS 22
83	31	SBS 23
84	32	SBS 24
85	33	SBS 25
86	34	SBS 26
87	35	SBS 27
88	36	SBS 28
89	PID P9	POSITION IDENTIFIER
90	37	SBS 29
91	38	SBS 210
92	39	SBS 211
93	40	SBS 212
94	41	SBS 213
95	42	SBS 214
96	43	SBS 215
97	44	SBS 216
98	45	SPACE
99	PID P0	POSITION IDENTIFIER

Table 8-4: IRIG E control function field

8.2.4 IRIG Output Accuracy Specifications

The IRIG outputs of the Spectracom Option Cards 1204-15, -1E, -22, and 1204-05, -27 deliver signals with the following 1PPS accuracy:

IRIC DCLS

Signal Category	Measured Accuracy
IRIG A	30 ns
IRIG B	30 ns
IRIG G	30 ns
IRIG NASA	30 ns
IRIG E	30 ns

IRIG AM

Signal Category	Measured Accuracy
IRIG A	200 ns
IRIG B	800 ns
IRIG G	200 ns
IRIG NASA	800 ns
IRIG E	1.5 µs

8.3 Technical Support

To request technical support for your SecureSync unit, please go to the "Support" page of the Spectracom Corporate website, where you can not only submit a support request, but also find additional technical documentation.

Phone support is available during regular office hours under the telephone numbers listed below.

To speed up the diagnosis of your SecureSync, please send us:

- the current **product configuration** (see "Option Card Identification" on page 287 to find out which option cards are installed in your unit), and
- the **events log** (see "Saving and Downloading Logs" on page 270).

Thank you for your cooperation.

8.3.1 Regional Contact

Spectracom operates globally and has offices in several locations around the world. Our main offices are listed below:

Country	Location	Phone
China	Beijing	+86-10-8231 9601
France	Les Ulis, Cedex	+33 (0)1 6453 3980
USA	Rochester, NY	+1.585.321.5800

Table 8-5: Spectracom contact information

Additional regional contact information can be found on the Contact Us page of the Spectracom corporate website.

8.4 Return Shipments

Please contact Spectracom Technical Support before returning any equipment to Spectracom. Technical Support must provide you with a Return Material Authorization Number (RMA#) prior to shipment.

When contacting Technical Support, please be prepared to provide your equipment serial number (s) and a description of the failure symptoms or issues you would like resolved.

Freight to Spectracom is to be prepaid by the customer.

Note: Should there be a need to return equipment to Spectracom, it must be shipped in its original packing material. Save all packaging material for this purpose.

8.5 License Notices

8.5.1 NTPv4.2.6p5

Copyright Notice
jpg "Clone me," says Dolly sheepishly.
Last update: 1-Jan-2011 08:34 UTC
____

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

The following individuals contributed in part to the Network Time Protocol Distribution Version 4 and are acknowledged as authors of this work.

1. [1]Takao Abe <takao_abe@xurb.jp> Clock driver for JJY receivers
2. [2]Mark Andrews <mark_andrews@isc.org> Leitch atomic clock controller
3. [3]Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial line and PCI-bus devices
4. [4]Viraj Bais <vbais@mailman1.intel.com> and [5]Clayton Kirkwood <kirkwood@striderfm.intel.com> port to WindowsNT 3.5
5. [6]Michael Barone <michael,barone@lmco.com> GPSVME fixes
6. [7]Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
7. [8]Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT port. Clean up recvbuf and iosignal code into separate modules.
8. [9]Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
9. [10]Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver, Trimble PARSE support
10. [11]Nelson B Bolyard <nelson@bolyard.me> update and complete broadcast and crypto features in sntp
11. [12]Jean-Francois Boudreault <Jean-Francois.Boudreault@viagenie.qc.ca> IPv6 support
12. [13]Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
13. [14]Steve Clift <clift@ml.csiro.au> OMEGA clock driver
14. [15]Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
15. [16]Sven Dietrich <sven_dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port.
16. [17]John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
17. [18]Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
18. [19]Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
19. [20]John Hay <jhay@icomtek.csir.co.za> IPv6 support and testing
20. [21]Dave Hart <davehart@davehart.com> General maintenance, Windows port interpolation rewrite
21. [22]Claas Hilbrecht <neoclock4x@linum.com> NeoClock4X clock driver
22. [23]Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
23. [24]Mike Iglesias <iglesias@uci.edu> DEC Alpha port

24. [25]Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
25. [26]Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
26. [27]Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or [28]<H.Lambermont@chello.nl> ntpsweep
27. [29]Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
28. [30]Frank Kardel [31]<kardel (at) ntp (dot) org> PARSE <GENERIC> driver (>14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup, dynamic interface handling
29. [32]William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
30. [33]Dave Katz <dkatz@cisco.com> RS/6000 AIX port
31. [34]Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
32. [35]George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
33. [36]Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
34. [37]Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
35. [38]Danny Mayer <mayer@ntp.org>Network I/O, Windows Port, Code Maintenance
36. [39]David L. Mills <mills@udel.edu> Version 4 foundation: clock discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbiter, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG
37. [40]Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
38. [41]Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
39. [42]Tom Moore <tmoore@fievel.daytonoh.ncr.com> i386 svr4 port
40. [43]Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
41. [44] Derek Mulcahy <derek@toybox.demon.co.uk> and [45] Damon Hart- Davis <d@hd.org> ARCRON MSF clock driver
42. [46]Rob Neal <neal@ntp.org> Bancomm refclock and config/parse code maintenance
43. [47]Rainer Pruy <Rainer.Pruy@informatik.uni- erlangen.de> monitoring/trap scripts, statistics file handling
44. [48]Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
45. [49]Wilfredo Sánchez <wsanchez@apple.com> added support for NetInfo
46. [50]Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
47. [51]Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
48. [52]Ray Schnitzler <schnitz@unipress.com> Unixware1 port
49. [53]Michael Shields <shields@tembel.org> USNO clock driver
50. [54]Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
51. [55]Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
52. [56]Kenneth Stone <ken@sdd.hp.com> HP-UX port
53. [57]Ajit Thyagarajan <ajit@ee.udel.edu>IP multicast/anycast support
54. [58]Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK clock driver
55. [59]Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver

56. [60]Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

____

References

1. mailto:%20takao_abe@xurb.jp
2. mailto:%20mark_andrews@isc.org
3. mailto:%20altmeier@atlsoft.de
4. mailto:%20vbais@mailman1.intel.co
5. mailto:%20kirkwood@striderfm.intel.com
6. mailto:%20michael.barone@lmco.com
7. mailto:%20karl@owl.HQ.ileaf.com
8. mailto:%20greg.brackley@bigfoot.com
9. mailto:%20Marc.Brett@westgeo.com
10. mailto:%20Piete.Brooks@cl.cam.ac.uk
11. mailto:%20nelson@bolyard.me
12. mailto:%20Jean-Francois.Boudreault@viagenie.qc.ca
13. mailto:%20reg@dwf.com
14. mailto:%20clift@ml.csiro.au
15. mailto:casey@csc.co.za
16. mailto:%20Sven_Dietrich@trimble.COM
17. mailto:%20dundas@salt.jpl.nasa.gov
18. mailto:%20duwe@immd4.informatik.uni-erlangen.de
19. mailto:%20dennis@mrbill.canet.ca
20. mailto:%20jhay@icomtek.csir.co.za
21. mailto:%20davehart@davehart.com
22. mailto:%20neoclock4x@linum.com
23. mailto:%20glenn@herald.usask.ca
24. mailto:%20iglesias@uci.edu
25. mailto:%20jagubox.gsfc.nasa.gov
26. mailto:%20jbj@chatham.usdesign.com
27. mailto:Hans.Lambermont@nl.origin-it.com
28. mailto:H.Lambermont@chello.nl
29. mailto:%20phk@FreeBSD.ORG
30. http://www4.informatik.uni-erlangen.de/%7ekardel
31. mailto:%20kardel(at)ntp(dot)org
32. mailto:%20jones@hermes.chpc.utexas.edu
33. mailto:%20dkatz@cisco.com
34. mailto:%20leres@ee.lbl.gov
35. mailto:%20lindholm@ucs.ubc.ca
36. mailto:%20louie@ni.umd.edu
37. mailto:%20thorinn@diku.dk
38. mailto:%20mayer@ntp.org
39. mailto:%20mills@udel.edu

40. mailto:%20moeller@gwdgv1.dnet.gwdg.de
41. mailto:%20mogul@pa.dec.com
42. mailto:%20tmoore@fievel.daytonoh.ncr.com
43. mailto:%20kamal@whence.com
44. mailto:%20derek@toybox.demon.co.uk
45. mailto:%20d@hd.org
46. mailto:%20neal@ntp.org
47. mailto:%20Rainer.Pruy@informatik.uni-erlangen.de
48. mailto:%20dirce@zk3.dec.com
49. mailto:%20wsanchez@apple.com
50. mailto:%20mrapple@quack.kfu.com
51. mailto:%20jack@innovativeinternet.com
52. mailto:%20schnitz@unipress.com
53. mailto:%20shields@tembel.org
54. mailto:%20pebbles.jpl.nasa.gov
55. mailto:%20harlan@pfcs.com
56. mailto:%20ken@sdd.hp.com
57. mailto:%20ajit@ee.udel.edu
58. mailto:%20tsuruoka@nc.fukuoka-u.ac.jp
59. mailto:%20vixie@vix.com
60. mailto:%20Ulrich.Windl@rz.uni-regensburg.de

---

[53]gif.

[54]David L. Mills <mills@udel.edu>

References

1. mailto:marka@syd.dms.csiro.au
2. mailto:altmeier@atlsoft.de
3. mailto:vbais@mailman1.intel.co
4. mailto:kirkwood@striderfm.intel.com
5. mailto:michael.barone@lmco.com
6. mailto:karl@owl.HQ.ileaf.com
7. mailto:greg.brackley@bigfoot.com
8. mailto:Marc.Brett@westgeo.com
9. mailto:Piete.Brooks@cl.cam.ac.uk
10. mailto:reg@dwf.com
11. mailto:clift@ml.csiro.au
12. mailto:casey@csc.co.za
13. mailto:Sven_Dietrich@trimble.COM
14. mailto:dundas@salt.jpl.nasa.gov
15. mailto:duwe@immd4.informatik.uni-erlangen.de
16. mailto:dennis@mrbill.canet.ca
17. mailto:glenn@herald.usask.ca

18. mailto:iglesias@uci.edu
19. mailto:jagubox.gsfc.nasa.gov
20. mailto:jbj@chatham.usdesign.com
21. mailto:Hans.Lambermont@nl.origin-it.com
22. mailto:H.Lambermont@chello.nl
23. mailto:phk@FreeBSD.ORG
24. http://www4.informatik.uni-erlangen.de/~kardel
25. mailto:Frank.Kardel@informatik.uni-erlangen.de
26. mailto:jones@hermes.chpc.utexas.edu
27. mailto:dkatz@cisco.com
28. mailto:leres@ee.lbl.gov
29. mailto:lindholm@ucs.ubc.ca
30. mailto:louie@ni.umd.edu
31. mailto:thorinn@diku.dk
32. mailto:mills@udel.edu
33. mailto:moeller@gwdgv1.dnet.gwdg.de
34. mailto:mogul@pa.dec.com
35. mailto:tmoore@fievel.daytonoh.ncr.com
36. mailto:kamal@whence.com
37. mailto:derek@toybox.demon.co.uk
38. mailto:d@hd.org
39. mailto:Rainer.Pruy@informatik.uni-erlangen.de
40. mailto:dirce@zk3.dec.com
41. mailto:wsanchez@apple.com
42. mailto:mrapple@quack.kfu.com
43. mailto:jack@innovativeinternet.com
44. mailto:schnitz@unipress.com
45. mailto:shields@tembel.org
46. mailto:pebbles.jpl.nasa.gov
47. mailto:harlan@pfcs.com
48. mailto:ken@sdd.hp.com
49. mailto:ajit@ee.udel.edu
50. mailto:tsuruoka@nc.fukuoka-u.ac.jp
51. mailto:vixie@vix.com
52. mailto:Ulrich.Windl@rz.uni-regensburg.de
53. file://localhost/backroom/ntp-stable/html/index.htm
54. mailto:mills@udel.edu

8.5.2 OpenSSH

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1) Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland

All rights reserved

As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details. [However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY

GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2) The 32-bit CRC implementation in crc32.c is due to Gary S. Brown. Comments in the file indicate it may be used for any purpose without restrictions: COPYRIGHT (C) 1986 Gary S. Brown. You may use this program, or code or tables extracted from it, as desired without restriction.

3) The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license. Cryptographic attack detector for ssh - source code Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky <futo@core-sdi.com><http://www.core-sdi.com>

4) ssh-keygen was contributed by David Mazieres under a BSD-style license. Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.

Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

5) The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license: @version 3.0 (December 2000) Optimised ANSI C code for the Rijndael cipher (now AES) @author Vincent Rijmen vincent.rijmen@esat.kuleuven.ac.be @author Antoon Bosselaers antoon.bosselaers@esat.kuleuven.ac.be @author Paulo Barreto <paulo.barreto@terra.com.br>

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6) One component of the ssh source code is under a 4-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code. The Regents of the University of California have declared that term 3 is no longer enforceable on their source code, but we retain that license as is.Copyright (c) 1983, 1990, 1992, 1993, 1995 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

7) Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl, Theo de Raadt, Niels Provos, Dug Song, Aaron Campbell, Damien Miller, Kevin Steves, Daniel Kouril, Per Allansson

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS ORIMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIESOF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8.5.3 OpenSSL

LICENSE ISSUES

==============

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

==

Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that

EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties. Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2004, Sparta, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE

This open software is available for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

8.6 List of Tables

8.7 List of Images

8.8 Document Revision History

Rev	ECO	Description	Date
A	2451	First-generation product manual.	May 2010

Rev	ECO	Description	Date
B	2504	Edits to include software changes implemented in the latest software version.	August 2010
C	2513	3rd Revision.	September 2010
D	2542	Edits to include changes implemented in the latest software version. Updated option card information, additional maintenance.	November 2010
E	2548	Edits to include changes implemented in the latest software version. Updated available option module card information, additional maintenance.	December 2010
F	2643	Edits to include changes implemented in the latest software version. Updated option module cards sections, PTP, SNMP, NTP sections, additional maintenance and editorial corrections.	April 2011
G	2680	Edits added to reflect changes in latest software version. Added new sections covering multi-Ethernet gigabit & routing functionality, new ASCII format information, and new security/access restrictions feature. Numerous additional minor updates, corrections, and document maintenance.	July 2011
H	2742	Updates to reflect changes in latest software version. Added new section covering new RS-485 Communications and Event Broadcast option modules. Updated supported IRIG output format tables. Added new supported CLI commands. Numerous additional minor maintenance updates & corrections.	October 2011
J	2804	Updates to reflect changes in new software version release. Updated warranty information. Updated IRIG input information, network setup pages, added new info regarding battery backed-up time synchronization, added new STANAG option module card information, numerous additional maintenance updates.	December 2011
K	2868	Updates to reflect changes in new software version release including new option card information, enhanced user management security enhancements, hardware configuration updates, additional document maintenance.	February 2012
L	2952	General updates, enhancements coinciding with latest software release.	June 2012
M	3019	Updates coinciding with latest software release. Added new feature descriptions, updated warranty information, updated specifications, added new option module card information, updated PTP feature information, adjusted IRIG reference information.	September 2012
N	3103	General updates, enhancements coinciding with latest software release.	December 2012

Rev	ECO	Description	Date
P	3250	General updates, enhancements coinciding with latest release: Multi-GNSS, Failover option card, Option Licensing, NTP update	January 2013
Q	3397	General updates to reflect new software release and new optional module 1204-32.	February 2014
R	3442	Changes pertaining to A-GPS/Software version 5.1.3	March 2014
16	0081	Addition of Programmable Frequency Module information. Web UI modifications, V 5.1.4: MTU field addition, NTP graph modifications, Classic UI functionality change. Modifications in Chapter “System Time”. Addition of fuse specifications. Option Module Card 1204-32: Correction of Step Mode Specifications Errata implementation.	June 2014
17	0340	Comprehensive overhaul of all existing content. New content: NTP over Anycast, TimeKeeper, oscillator disciplining features, option card installation procedure Changed content: option card reference information, consolidation of several UI procedures Errata implementation.	March 2015
18	0436	Implementation of newly released features under SW release 5.2.1: A-GPS Rinex Server functionality, tcpdump functionality, new IRIG control field for advanced leap second notifications (Spectracom IEEE C37), Show Clock page, and minor corrections throughout the manual.	May 2015
19	0486	Implementation of newly released features under SW release 5.3.0: AnyCast IPv6, GNSS receiver SW update, temperature monitoring, host disciplining Errata implementation	August 2015
20	0693	Added topic "Temperature Management". Content modifications under Notification Configuration. Content modifications under GNSS receiver configuration. Document maintenance and errata implementation.	December 2015

Rev	ECO	Description	Date
21	DOC000010	Edits to include changes implemented in the latest software version. Content modifications: GNSS theory of operation; GNSS receiver specifications, NTP throughput specifications; login timeout (new); Ethernet monitoring (new); NTP Peer preference; iptables support (new); language support; NTP Autokey (not supported under 4.2.8p6); configuration of network access rules; NTP over Anycast: OSPF (changes), BGP (new); Expert Mode (new)	April 2016

INDEX