SecureSync®

INSTRUCTION MANUAL

1565 Jefferson Road
Rochester, NY 14623
Phone: US +1.585.321.5800
Fax: US +1.585.321.5219

spectracom

www.spectracomcorp.com
Part Number 1200-5000-0050
Rev. P
September 2013

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

One Year Limited Warranty

Timeview Analog Clock
Path Align-R Products
Bus-level Timing Boards
IRIG-B Distribution Amplifiers

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.

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 instruction manual, 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.

Contents

List of Figures

Underwriters Laboratory (UL) has not tested the performance or reliability of the Global Positioning System (GPS) hardware, operating software, or other aspects of this product. UL has only tested for fire, shock, or casualties as outlined in UL's Standard(s) for Safety for Information Technology Equipment, UL60950-1. UL Certification does not cover the performance or reliability of the GPS hardware and GPS operating software.

UL MAKES NO REPRESENTATIONS, WARRANTIES, OR CERTIFICATIONS WHATSOEVER REGARDING THE PERFORMANCE OR RELIABILITY OF ANY GPS RELATED FUNCTIONS OF THIS PRODUCT.

Section 1: SecureSync

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 & 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.

1.1 Introduction

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 6 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 are 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 (5 MHz, 2.048 MHz, 1.544 MHz), 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. For security purposes, system management can be restricted to a dedicated management LAN.

SecureSync is a security-hardened 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 1 rack unit high (1RU) chassis supports 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.

> ***NOTE:*** *All features described are not available on all SecureSync variants.*

1.2 Inputs and Outputs: What Can SecureSync Do for You?

Spectracom 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.

1.3 SecureSync Front Panel

The front panel of the SecureSync unit consists of three separate, illuminated status LEDs, front panel control keypad, an LED time display, an LCD display, an RS-232 serial interface, and a temperature controlled cooling fan. The LCD is configurable using the web browser user interface (also referred to as the "web interface" or "web UI") or front panel controls. Display options include status or position information, time, date, DOY (Day of Year), GNSS information, network settings and SAASM key status (available with the SASSM 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.

When the SAASM GPS receiver option module is installed, an encryption key fill connector and key Zeroize switch are also located on the left side of the front panel.

The status LEDs ("Sync", "Power" and "Fault") indicate whether the 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. It will indicate green if power is applied. The Sync and Fault lamps have multiple states (refer to the following "*Front Panel LED Indicators*" section for descriptions of the different LED status indications).

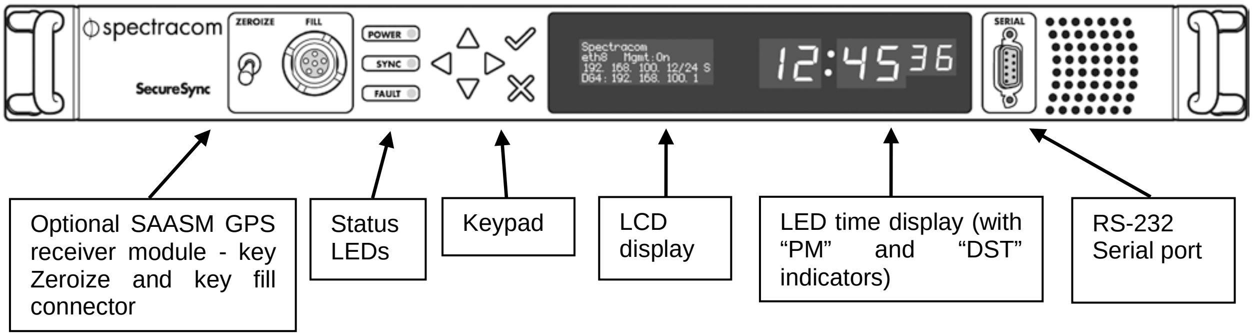


Figure 1-1: SecureSync Front Panel

1.3.1 Front Panel LED Indicators

Power: Green, always on.
Sync: Tri-color LED indicates the time data accuracy.
Fault: Indicates equipment fault.

At power up, a quick LED test is run which illuminates all three LEDs. The following table provides an overview of the LED status indications:

Label	Activity / 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 as present.
	Red	SecureSync detecting only one of its possible power inputs, or detecting a power configuration error.
	Green, but blinking Orange once per second	Indicates power error condition; 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	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 Section *9.4* for troubleshooting this condition).
	Solid orange	A Minor alarm condition (other than an antenna problem alarm) has been asserted and is currently active (Refer to Section *9.1.2*: "*Fault light - Minor Alarm*" for troubleshooting this condition).
	Red	A Major alarm condition has been asserted and is currently active (Refer to Section *9.1.1*: "*Fault Light - Major Alarm*" for troubleshooting this condition).

Table 1-1: SecureSync Front Panel Status Indicators

1.4 SecureSync Rear Panel

The SecureSync rear panel provides several different outputs for interfacing the unit to various systems. The rear panel has an optional AC connection for the power input (DC Power optional), Ethernet and USB connections, 1PPS and 10MHz outputs, six available option module card bay slots, and GNSS antenna (GNSS configuration is optional).

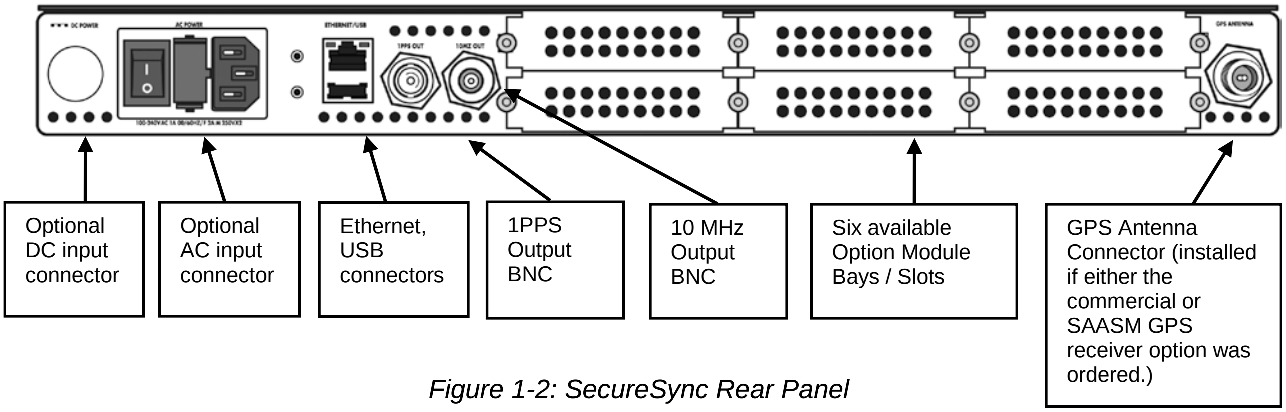

DC POWER
AC POWER
ETHERNET/USB
1PPS OUT
10MHZ OUT
GPS ANTENNA
Optional DC input connector
Optional AC input connector
Ethernet, USB connectors
1PPS Output BNC
10 MHz Output BNC
Six available Option Module Bays / Slots
GPS Antenna Connector (installed if either the commercial or SAASM GPS receiver option was ordered.)

Figure 1-2: SecureSync Rear Panel

The **DC Power** port connector is only installed if SecureSync was ordered with DC input power option. Note: DC input power does not have an ON/OFF switch.

The **AC Power** connector is the input for the AC power and provides and AC power ON/OFF switch. This connector 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 interface for system management. It has two small indicator lamps, “Good Link” (green LED), and “Activity” (orange LED). The “Good Link” link light indicates a connection to the network is present. The “Activity” link light will illuminate when network traffic is detected.

Ethernet	Yellow	On Off	LAN Activity detected. No LAN traffic detected.
Ethernet	Green	On Off	LAN Link established, 10 or 100 Mb/s. No link established.

Table 1-2: Status Indicators, Rear Panel

The **USB connector** is reserved for future expansion.

The **1PPS Output** provides a once-per-second square-wave output via BNC output connector. The 1PPS output can be configured to have either the rising or falling edge of the signal to be coincident with the system’s on-time point.

The **10 MHz Output** provides a 10 MHz sine-wave output via BNC output connector.

The **GPS ANTENNA** connector is a type “N” type connector for the GNSS input from the GNSS antenna and coax cabling. This connector won’t be present if the standard GNSS receiver (or the optional SAASM GPS receiver module) is not installed.

1.4.1 Option Module Card Slot Layout

The **six option module card bay slots** are designated as **Slot 1** – **Slot 6**, as shown in the following figure:

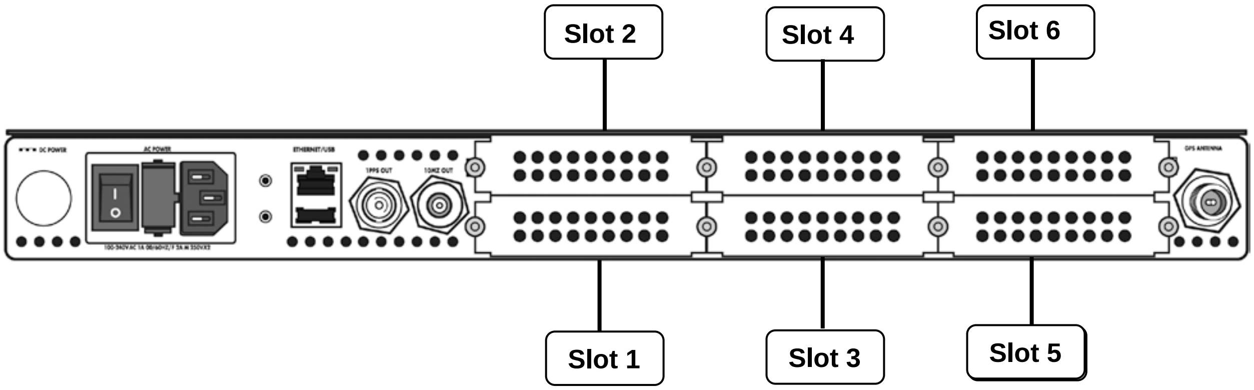


Figure 1-3: SecureSync Rear Panel Option Module Bays

1.5 Technical and Customer Support

If you require assistance with the configuration or operation of your product, or have questions or issues that cannot be resolved using the information in this document, please contact Spectracom Technical & Customer Support at either our North American or European service centers, or visit the Spectracom website at www.spectracomcorp.com.

NOTE: Premium Support Customers can refer to their service contracts for emergency 24-hour support.

North America		
Phone	+1 585.321.5800	
email	techsupport@spectracom.orolia.com	
Europe		
France		**United Kingdom**
Phone	+33 (0)1 6453 3980	44 (0)1256 303630
email	techsupport-france@spectracom.orolia.com	techsupport@spectracom.co.uk

Also visit Spectracom's website for general product information, Application and Technical Notes, notices regarding the availability of software updates for your products, and more.

1.5.1 Return Shipments

Please contact Customer Service before returning any equipment to Spectracom. Customer Service must provide you with a Return Material Authorization Number (RMA#) prior to shipment. When contacting Customer Service, 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.

1.6 Compliance

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

The product complies with the requirements of the **Low Voltage Directive 2006/95/EC** and the **EMC Directive 2004/108/EC**.

1.7 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 Section *1.8*: “*Available Option Modules*”.

1.7.1 GNSS Receiver

Received Standard:	L1 C/A Code transmitted at 1575.42 MHz
Satellites Tracked:	Up to 32 simultaneously.
Acquisition Time:	Typically <4 minutes from a cold start.
Antenna Requirements:	Active antenna module, +5V, powered by the SecureSync unit, 16 dB gain minimum.
Antenna Connector:	Type N, female.

1.7.2 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 standard, data communication equipment.
Character Structure:	ASCII, 9600 baud, 1 start, 8 data, 1 stop, no parity.

1.7.3 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.

1.7.4 Protocols Supported

NTP:	NTP v4.2.6p5. Provides MD5 and Autokey, Stratum 1 or higher (RFC 5905).
Loading:	~7,000 NTP requests per second, typical.
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.
HTTP, HTTPS Servers:	For browser-based administration, configuration and monitoring using Internet Explorer 7 or higher with JavaScript support, Mozilla Firefox 3 or higher (per RFCs 1945 and 2068), with JavaScript support.
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.

1.7.5 1PPS Output

Signal:	One pulse-per-second square wave derived from the GNSS receiver.
Signal Level:	TTL compatible, 4.3 V minimum, base-to-peak into 50 Ω.
Pulse Width:	Configurable Pulse Width (200 milliseconds by default).
Pulse Width Range:	200 - 900 nanoseconds
Rise Time:	<10ns
Accuracy:	Positive edge within ± 50 nanoseconds of UTC when locked to a valid 1PPS input reference.
Connector:	BNC Female
Signature Control:	Positive edge within ± 50 nanoseconds of UTC when locked to a valid 1PPS input reference.

1.7.6 10 MHz Output

Signal:	10 MHz sinewave.
Signal Level:	+13 dBm +/- 2dB into 50 Ω.

Harmonics:	-40 dBc minimum.
Spurious:	-70 dBc minimum.
Oscillator Types & Accuracy:	**TCXO:** 1x10^{-11} typical 24-hour average locked to GPS, 1x10^{-8} per day typical aging unlocked. **OCXO (standard performance):** 2x10^{-12} typical 24-hour average locked to GPS, 5x10^{-10} per day typical aging unlocked. **OCXO Low Phase Noise (Option):** 1x10^{-12} typical 24-hour average locked to GPS, 2x10^{-10} per day typical aging unlocked. **Rubidium (Option):** 1x10^{-12} typical 24-hour average locked to GPS; 5x10^{-11} per month (3x10^{-11} per month typical) aging unlocked. **Rubidium Low Phase Noise (Option):** 1x10^{-12} typical 24-hour average locked to GPS; 5x10^{-11} per month (3x10^{-11} per month typical) aging unlocked.
Connector:	BNC Female
Signature Control:	This configurable feature removes the output signal whenever a major alarm condition or loss of time synchronization condition is present. The output is restored when the fault condition is corrected.

1.7.7 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):	12-17VDC -15%, +20% or 21-60 VDC -15%, +20%, secure locking device.
Maximum Power Draw:	TCXO/OCXO oscillator installed - 40W normal (50W start-up) Rubidium (Rb) oscillator installed - 50W normal (80W start-up)

1.7.8 Mechanical and Environmental

Dimensions:	Designed for EIA 19” rack mount 16.75” W x 1.72” H [1U] x 14.00” D actual (425 mm W x 44 mm H x 356 mm D) actual
Weight:	6.0 lbs (2.72 kg) 6.5 lbs. (2.95 kg) for Rubidium option
Temperature:	-20°C to +65°C operating range

	(+ 55°C for Rubidium option) -40° to 85°C storage range
Humidity:	10% - 95% relative humidity, non-condensing @ 40° C
Altitude:	100-240VAC - 6,561ft (2000m) operating range 100-120VAC – 13,100ft (4000m) operating range 45000ft (13700m) storage range
Shock:	15g/0.53oz, 11ms, half sine wave operating range 50g/1.76oz, 11ms, trapezoidal pulse storage range
Vibration:	10-55Hz/0.07g, 55-500Hz/1.0g operating range 10-55Hz/0.15g, 55-500Hz/2.0g storage range
MIL-STD-810F:	501.4, 502.4, 507.4, 500.4, 516.5, 514.5

1.8 Available Option Modules

Add the features you need by selecting SecureSync option module cards. Up to six (6) modules can be accommodated per unit. In some cases, the number of modules of any one type that can be installed may be restricted (see "Maximum number of cards" for each type of module). For detailed information on a specific option module card (including setup, configuration), refer to Section 8: "Option Modules".

1.8.1 1204-01, 1204-03: 1PPS/Freq Input and 1PPS Output Modules

Use external timing or frequency signals as a system reference. Also adds additional 1PPS output.

Inputs / Outputs:	(1) 1PPS Input, (1) Freq Input, (1) 1PPS Output
1PPS Output Rise Time:	<10ns
Signal Type and Connector:	Sine (BNC into 50 Ω) or RS-485 (3.8 mm terminal block).
Input Signal Jitter:	< +/- 500 ns to achieve oscillator lock, < +/- 50 ns to achieve system performance
Maximum Number of Cards:	6
Ordering Information:	1204-01: 1PPS/Freq input (TTL levels) module 1204-03: 1PPS/Freq input (RS-485 levels) module

1.8.2 1204-02, 1204-04: ASCII Time Code Modules (RS-232, RS-485)

Inputs / Outputs:	(1) Input, (1) Output
Signal Type and Connector:	RS-232 on DB-9 or RS-485 on terminal block
Accuracy:	+/- 100-1000 microseconds (format dependant)
Maximum Number of Cards:	6
Ordering Information:	1204-02: ASCII Time Code Module (RS-232) 1204-04 ASCII Time Code Module (RS-485)

1.8.3 1204-05, 1204-27: IRIG Input/Output Module

Inputs / Outputs:	(1) IRIG Input, (2) IRIG Output
Signal Type and Connector:	Input: IRIG A, B, G, E, NASA 36

	BNC Connector: Amplitude Modulated (0.5v to 6v peak to peak into 50 Ω) or DC Level Shift (unmodulated), user selectable Fiber Optic, ST Connector: DC Level Shift Only (unmodulated)
Accuracy:	+/- 2 to 200 microseconds (IRIG Format dependant)
Maximum Number of Cards:	6
Ordering Information:	1204-05: IRIG module, BNC Connector 1204-27: IRIG module, Fiber Optic ST Connector

1.8.4 1204-06: Multi-Gigabit Ethernet Module

Inputs / Outputs:	(3) Gigabit Ethernet (10/100/1000 Base-T)
Signal Type and Connector:	RJ-45
Management:	Enabled or Disabled (NTP server only)
Maximum Number of Cards:	1
Ordering Information:	1204-06: Gigabit Ethernet (3X) Module

1.8.5 1204-08, 1204-0C, 1204-1C, 1204-26: Frequency Output Modules

Inputs / Outputs:	(3) 1 MHz, (3) 5 MHz, or (3) 10 MHz Outputs
Signal Type and Connector:	(10 MHz) +13dBm into 50 Ω, BNC (5 MHz) +10dBm into 50 Ω, BNC (1 MHz) +10dBm into 50 Ω, BNC
1 MHz or 5 MHZ Phase noise (with OCXO or low phase noise Rubidium oscillator):	-115 dBc/Hz @ 10Hz -130 dBc/Hz @ 100Hz -140 dBc/Hz @ 1kHz
1 MHz or 5 MHZ Phase noise (with Rubidium oscillator):	-85 dBc/Hz @ 10Hz -110 dBc/Hz @ 100Hz -130 dBC/Hz @ 1kHz
10 MHz Phase noise (with TCXO oscillator):	-110 dBc/Hz @ 100Hz -135 dBc/Hz @ 1kHz -140 dBc/Hz @ 10kHz
10 MHz Phase noise (with OCXO oscillator):	-100 [-95] dBc/Hz @ 1Hz -128 [-123] dBc/Hz @ 10Hz

	-148 [-140] dBc/Hz @ 100Hz -153 [-145] dBc/Hz @ 1kHz -155 [-150] dBc/Hz @ 10kHz
10 MHz Phase noise (with Rubidium oscillator):	-100 [-80] dBc/Hz @ 1Hz -128 [-98] dBc/Hz @ 10Hz -148 [-120] dBc/Hz @ 100Hz -153 [-140] dBc/Hz @ 1kHz -155 [-140] dBc/Hz @ 10kHz
Harmonics:	-40 dBc minimum
Spurious:	-60 dBc minimum (1 MHz) -50 dBc minimum (5 MHz) -70 dBc minimum (10 MHz)
Accuracy:	**TCXO:** 1x10^{-11} typical 24-hour average locked to GPS, 1x10^{-8} per day typical aging unlocked. **OCXO (standard performance):** 2x10^{-12} typical 24-hour average locked to GPS, 5x10^{-10} per day typical aging unlocked. **OCXO Low Phase Noise (Option):** 1x10^{-12} typical 24-hour average locked to GPS, 2x10-10 per day typical aging unlocked. **Rubidium (Option):** 1x10^{-12} typical 24-hour average locked to GPS; 5x10^{-11} per month (3x10^{-11} per month typical) aging unlocked. **Rubidium Low Phase Noise (Option):** 1x10^{-12} typical 24-hour average locked to GPS; 5x10^{-11} per month (3x10^{-11} per month typical) aging unlocked.
Maximum Number of Cards:	4 (1204-08, 1204-1C, or 1204-26) 1 (1204-0C)
Ordering Information:	1204-08: 5 MHz output (3X) Module 1204-0C: 10 MHz output (3X) Module 1204-1C: 10 MHz output (3X) Module 1204-26: 1 MHz output (3X) Module

1.8.6 1204-09, 1204-0A: T1 / E1 Output Modules

Outputs:	T1 mode: • 1.544MHz (square wave) frequency output • (2) 1.544 Mb/sec data rate outputs: o Outputs are DS1 framed all ones. o Supports Super Frame (SF or D4) and Extended Super Frame (ESF). o SSM support E1 mode: • 2.048MHz (square wave) frequency output • (2) 2.048 Mb/sec data rate outputs:

	o Outputs are E1 frame all ones. o Supports CRC4 and CAS Multiframe. o SSM support
Maximum Number of Cards:	6
Ordering Information:	1204-09: T1 / E1 (75 Ω) module 1204-0A: T1 / E1 (100 / 120 Ω) module

1.8.7 1204-0B: RS-485 Communications Module

Inputs / Outputs:	Bi-directional Communication Port
Signal Type and Connector:	Balanced RS-485 (3.8mm terminal block)
Maximum Number of Cards:	1
Ordering Information:	1204-0B: RS-485 Communications Module

1.8.8 1204-1D, 1204-24: STANAG Input Modules

Inputs:	(2) STANAG Inputs, (1) 1PPS Input
Signal Type and Connector:	TTL or RS-485 level (user selectable) for STANAG and 1PPS input. SUB-D 25.
Formats Supported:	STANAG 4246 HAVE QUICK I STANAG 4246 HAVE QUICK II STANAG 4372 HAVE QUICK IIA STANAG 4430 Extended HAVE QUICK ICD-GPS-060A HAVE QUICK
Accuracy:	100ns
Maximum Number of Cards:	6
Ordering Information:	1204-1D (for non-isolated board) 1204-24 (for isolated board)

1.8.9 1204-11, 1204-25: STANAG Output Modules

Outputs:	(2) STANAG Outputs, (1) 1PPS Output
Signal Type and Connector:	5V or 10V or RS-485 level (user selectable) for STANAG and 1PPS output. SUB-D 25.

Formats Supported:	STANAG 4246 HAVE QUICK I STANAG 4246 HAVE QUICK II STANAG 4372 HAVE QUICK IIA STANAG 4430 Extended HAVE QUICK ICD-GPS-060A HAVE QUICK
Programmable Pulse Width (1PPS Output):	100ns to 500ms with 20ns resolution
Accuracy:	±50ns (1σ)
Maximum Number of Cards:	6
Ordering Information:	1204-11 (for non-isolated board) 1204-25 (for isolated board)

1.8.10 1204-0F: Relay Outputs Module

Inputs / Outputs:	(3) Three contact relay connections (NC, common, NO)
Signal Type and Connector:	Terminal block Contacts Switch under max. load of 30VDC, 2A Contacts rated to switch 220VDC Breakdown voltage of 1000VDC between contacts Switch time 4 msec, max.
Maximum Number of Cards:	1
Ordering Information:	1204-0F: Relay Outputs Module

1.8.11 1204-10, 1204-1B: HAVE QUICK Module

Inputs / Outputs:	(4) HAVE QUICK Outputs
Signal Type and Connector:	TTL (BNC into 10k Ω) RS-485 (Terminal Block into 120 Ω)
Formats:	STANAG 4246 HAVE QUICK I STANAG 4246 HAVE QUICK II STANAG 4372 HAVE QUICK IIA STANAG 4430 Extended HAVE QUICK ICD-GPS-060A HAVE QUICK
Accuracy:	±50ns (1σ)
Maximum Number of Cards:	6
Ordering Information:	1204-10 HAVE QUICK outputs

	1204-1B RS-485 HAVE QUICK outputs

1.8.12 1204-12: Precision Time Protocol Module

Inputs / Outputs:	(1) Configurable as Input or Output
Signal Type and Connector:	RJ-45
Management:	PTP Management Protocol Only
Resolution:	8 nS (+/- 4 nS) packet timestamping resolution
Accuracy:	30 nS accuracy (3σ) Master to Slave via crossover cable
Maximum Number of Cards:	6
Ordering Information:	1204-12: PTP / Precision Timing Protocol Option Module

1.8.13 1204-14: CTCSS / Data Sync / Data Clock

Connector: **DB-9**	
Outputs:	(3) RS-485 Outputs (Data Clocks, CTCSS frequencies, 1PPS) (1) Alarm
Voltage:	Alarms: GND normally, high impedance when Alarm
Connector: **RJ-12**	
Outputs:	(1) RS-485 Outputs (Data Clocks, CTCSS frequencies, 1PPS) (2) Alarm
Voltage:	Alarms: 5V pulled up through 10k Ω normally, GND when Alarm

1.8.14 1204-15, 1204-1E: Four IRIG Output

Inputs / Outputs:	(4) IRIG Output
Signal Type and Connector:	IRIG A, B, E, G, NASA 36 BNC Connector: Amplitude Modulated (0v to 5v peak to peak into 50 Ω) or DC Level Shift (unmodulated), user selectable. Fiber Optic, ST Connector: DC Level Shift Only (unmodulated)

Accuracy:	+/- 2 to 200 microseconds (IRIG Format dependant)
Maximum Number of Cards:	6
Ordering Information:	1204-15: IRIG output module, BNC Connector 1204-1E: IRIG output module, Fiber-ST Connector

1.8.15 1204-17: Four Square Wave Out Module

Inputs / Outputs:	(4) Programmable square wave outputs
Signal Type and Connector:	TTL (BNC into 50 Ω)
Accuracy:	±50ns (1σ)
Programmable Period:	100ns to 1,000,000,000ns in 5 ns steps, to 60,000,000us in 1us steps
Programmable Pulse Width:	20ns to 900ms with 5ns resolution
Maximum Number of Cards:	6
Ordering Information:	1204-17: Square Wave Out

1.8.16 1204-18, 1204-19, 1204-21, 1204-2B: 1PPS Output Module

Inputs / Outputs:	(4) 1PPS outputs
Signal Type and Connector:	TTL or 10V (BNC into 50 Ω) RS-485 (Terminal Block into 120 Ω)
Accuracy:	±50ns (1σ)
Maximum Number of Cards:	6
Ordering Information:	1204-18 1PPS TTL output module, BNC connector 1204-19 1PPS 10V output module, BNC connector 1204-21 1PPS RS-485 output module, terminal block 1204-2B 1PPS Fiber Optic output module, ST connector

1.8.17 1204-23: Event Broadcast Module

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:	5 nanoseconds
Minimum Time Between Events:	20 nanoseconds
Message Buffer Size:	512 messages
Ordering Information:	1204-23: Event Broadcast

1.8.18 1204-28, 1204-2A: 1PPS Input/Output

Inputs / Outputs:	(1) 1PPS input / (3) 1PPS output (TTL Option) (1) 1PPS input / (2) 1PPS output (Fiber Option)
Signal Type and Connector:	TTL (BNC) Fiber (ST)
Input Impedance:	50 Ω (TTL Option)
Output Load Impedance:	50 Ω (TTL Option)
Rise time to 90% of level:	<10ns (TTL Option)
Programmable pulse width:	100ns to 500ms with 20ns resolution
Absolute phase error:	±50ns (1σ)
Programmable phase shift:	±5ns to 500ms with 5ns resolution
Maximum Number of Cards:	6
Ordering Information:	1204-28: 1PPS 1-input/3-output, BNC connectors 1204-2A: 1PPS 1-in/2-out, Fiber Optic, ST connectors

1.8.19 1204-2E: Failover Option Module

Inputs / Outputs:	(2) Inputs – Unselected input terminated with 50 Ω (1) Output
Connector:	3 BNC
Signal Type:	User selected: • >1 MHz • 1MHz to 100Hz • 1PPS

Signal Level:	• Sine Wave, 0.5V to 30V pp • TTL
Default Power-on Switch State:	Input “B”
Maximum Number of Cards:	6
Ordering Information:	1204-2E: Failover Module

1.8.20 1204-29: HAVE QUICK Input/Output Module

Inputs/Outputs:	(1) HAVE QUICK input / (3) HAVE QUICK outputs
Signal Type and Connector:	TTL levels (BNC)
Output Load Impedance:	10k Ω
Start of signal:	<10µs after 1PPS output
Programmable phase shift:	±5ns to 500ms with 5ns resolution
Maximum Number of Cards:	6
Ordering Information:	1204-29: HAVE QUICK Input/Output

Section 2: Installation

To begin the installation of your product, follow the steps and information outlined in this section.

2.1 Safety

Before beginning, 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.

⚠	**WARNING**
	Installation of this product is to be done by authorized service personnel only. This product is not to be installed by the user/operator. *Installation of the equipment must comply with local and national electrical codes.* *DO NOT OPERATE THIS EQUIPMENT WITH THE COVER OR BLANK PLATES COVERING UNUSED OPTION CARD SLOTS REMOVED.*
	CAUTION
	Electronic equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD precautions and safeguards when handling Spectracom equipment.
⚠	**WARNING**
	The interior of this equipment does not have any user serviceable parts. Contact Spectracom Technical Support if this equipment needs to be serviced. *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.* *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.* *Never remove the cover or blank option card plates with power applied to this equipment.* *This equipment has Double Pole/Neutral Line Fusing on AC power.*
⚠	**WARNING**
	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.* *This 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.* *The DC supply source is to be located within the same premises as this equipment.* *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.*
⚠	**CAUTION**
	For continued protection against risk of fire, replace fuses only with same type and rating of fuse. *There is a danger of a new battery exploding if it is incorrectly installed. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.*

2.2 Unpacking & Inventory

Unpack and inspect the unit and accessories. The following items are included with your shipment:

- SecureSync Unit
- QuickStart Guide
- 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 options on the original purchase order have been pre-installed. ***Note:*** Retain all original packaging for use in return shipments if necessary.

2.3 Required Tools and Cables for Installation

1. Phillips screwdriver to install the unit's rack-mount ears.
2. Screwdriver to mount the unit in a standard 19-inch rack.
3. Ethernet cables (refer to Section *2.12*: "*Ethernet Network Cabling*").

2.4 Installation Summary

This section provides an overview summary of the installation process. The installation of the SecureSync consists of the following steps. Refer to the table of contents in this document for specific section references detailing how these summarized steps are accomplished.

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.

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.

2.5 Rack Mounting

The SecureSync will install into any EIA standard 19 inch rack. The 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 for best ventilation of the SecureSync.

- The SecureSync maximum ambient operating temperature must be kept to the maximum value specified in Section *1.7.8*: "*Mechanical and Environmental*" of this document for the oscillator option purchased. If the SecureSync 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 SecureSync in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- Mounting of the SecureSync in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Consideration should be given to the connection of the SecureSync to the supply circuit and the effect that overloading of the circuits might have on over current protection and supply wiring. Appropriate consideration of SecureSync nameplate ratings should be used when addressing this concern.
- Reliable earthing of rack-mounted equipment should be maintained. Particular attention should 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

The following customer supplied items are also needed:

- 4 each #10-32 pan head rack mount screws
- 1 each #2 Phillips head screwdriver

To rack mount the SecureSync:

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.

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.

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. ***NOTE:*** For safety purposes, the SecureSync is intended to be operated in the upright position only, with the keypad to the left side and the LCD and time displays on the right side.

2.6 Power Connection

2.6.1 Input Power Selection:

As long as the AC input power is present, AC power will be selected.

- If AC and DC power are both applied, AC power is used.
- If DC power is applied, but AC power is not, the 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.

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

2.6.2 If AC Input Power is Desired:

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.

WARNING: 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 If DC Input Power is Desired:

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 (12vdc with a voltage range of 12-17V at 7A maximum or 24/48vdc input with a voltage range of 21-60V at 3A 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).

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

NOTE: The DC input port is both fuse and reverse polarity protected. Reversing polarity with the 24/48vdc option will not blow the fuse, but the equipment will not power-up. Reversing polarity with the 12vdc 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.

DC power connector pin-out:

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

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

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

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

2.6.4 SecureSync Power-up

If AC input is connected, turn the rear panel AC power switch on (DC input power is not switched, so SecureSync will be powered up with DC input connected) and observe that all of the front panel LEDs momentarily illuminate (the Power LED will then stay lit) and that the LCD display backlight illuminates. The LED time display will reset and then start incrementing the time. About 10 seconds after power-up, “Starting up SecureSync” will be displayed in the LCD window. After approximately 2 minutes, the LCD will then display the current network settings.

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

2.7 Power and Ground Connection Safety

⚠	**WARNING** ***The interior of this equipment does not have any user serviceable parts. Contact Spectracom Technical Support if this equipment needs to be serviced.*** *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.* *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.* *Never remove the cover or blank option card plates with power applied to this equipment.* *This equipment has Double Pole/Neutral Line Fusing on AC power.*
⚠	**WARNING** *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.* *This 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.* *The DC supply source is to be located within the same premises as this equipment.* *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.*

2.8 Common Post-Installation Configuration Scenarios

After physical product installation, a commonly desired scenario is for the SecureSync to display local time on the front panel (rather than UTC time). If this configuration is desired for your environment, refer to Section 3.11.7: "Example - Applying Local Clock to Front Panel or ASCII Outputs" for steps and additional information.

2.9 Connecting Reference Inputs and Network Interface

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 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. These two reference inputs are discussed later in this manual).

1. **GNSS Reference 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, just disregard the steps to install the GNSS antenna and associated cabling.

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.

Connect the GNSS cable to the rear panel antenna input jack (refer to Figure 1-2). Until the GNSS antenna is connected to the rear panel jack, the Antenna Problem alarm is asserted, 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 Section *9.4*.

2. **IRIG Reference input:** With the available IRIG Input/Output module (Model 1204-5) 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). When 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.

3. **Network interface to LAN:** Obtain the following network information from your network administrator before continuing:

Available static IP Address	This is the unique address assigned to the SecureSync unit by the network administrator. The default static IP address of the SecureSync unit is 10.10.200.1.
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.

Table 2-1: Required Network information

If your network does not support DHCP, use the front panel LCD and keypad (refer to Section 2.10) to input the desired static IP, subnet mask, and gateway address.

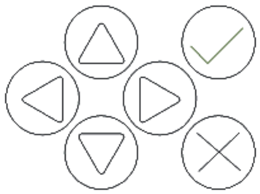
Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
30	255.255.255.252	18	255.255.192.0
29	255.255.255.248	17	255.255.128.0
28	255.255.255.240	16	255.255.0.0
27	255.255.255.224	15	255.254.0.0
26	255.255.255.192	14	255.252.0.0
25	255.255.255.128	13	255.248.0.0
24	255.255.255.0	12	255.240.0.0
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		

Table 2-2: Subnet mask values

2.10 Front Panel Keypad/LCD Operation

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

2.10.1 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 arrow (←): Select a new item to the left

RIGHT arrow (→): Select a new item to the right

DOWN arrow (↓): Scroll through parameter values in edit displays

UP arrow (↑): Scroll through parameter values in edit displays

2.10.2 Navigating the Keypad Display

After power initialization, press any key to go to the “Home” display. As illustrated in Figure 2-1, 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 LCD 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.

2.10.3 Unlocking the Front Panel Keypad

If the front panel keypad is locked, the following sequence will locally unlock the keypad for use (note that the front panel can also be locked / unlocked via the SecureSync web user interface. Refer to Section *3.12*: “*Front Panel LED / LCD Display and Keypad Configuration*”):

↑ ↓ ↑ ↓ ← → ← → ✓ x ✓

2.10.4 Editing Options from the Keypad

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.

Figure 2-1 displays the navigation tree for the keypad/LCD operation.

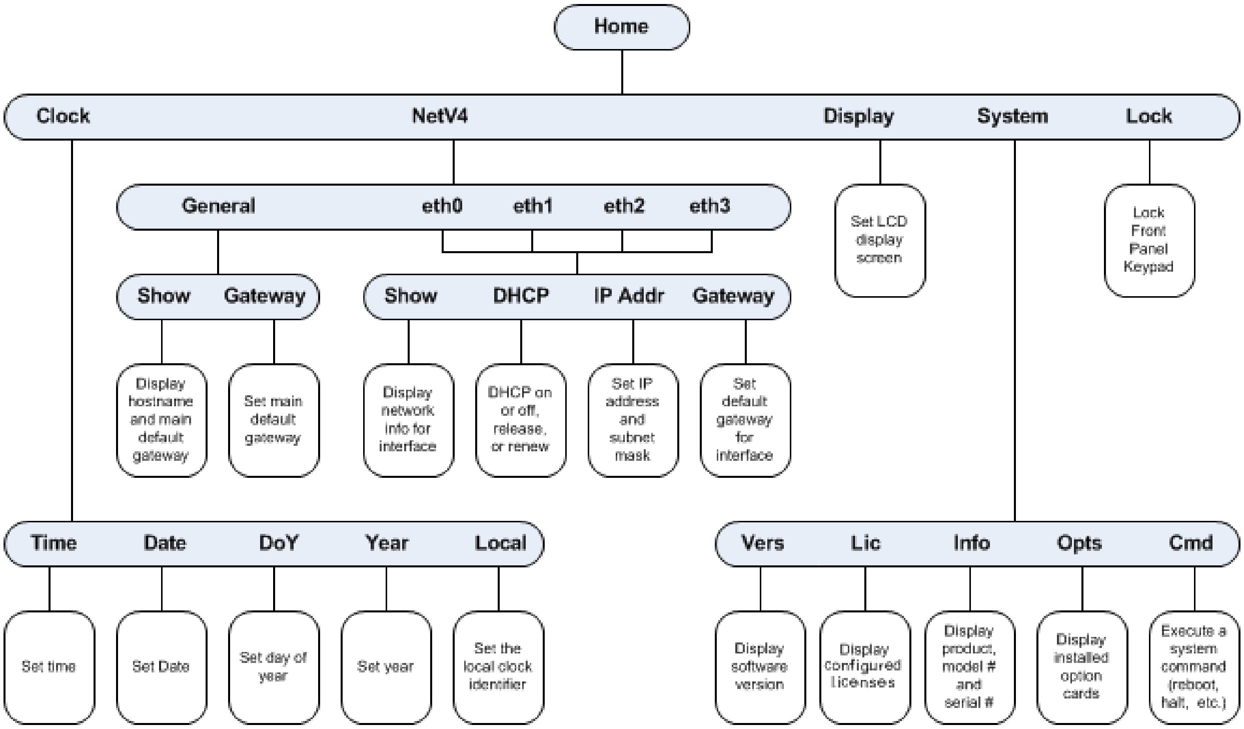

Home
Clock
NetV4
Display
System
Lock
General
eth0
eth1
eth2
eth3
Set LCD display screen
Lock Front Panel Keypad
Show
Gateway
Show
DHCP
IP Addr
Gateway
Display hostname and main default gateway
Set main default gateway
Display network info for interface
DHCP on or off, release, or renew
Set IP address 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 2-1: Keypad/LCD Navigation Tree

Using the keypad, the LCD display window 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).

2.11 Front Panel Serial Port

In addition to the available front panel keypad and LCD 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 interface. 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 *Section 10*: for more information on the serial port connection and *Section 11*: for a list and description of the available command line (CLI) commands that can be issued.

2.11.1 To Disable DHCP using Front Panel

1. Press the ✓ key.
2. Using the arrow keys, select **`Netv4`** from the menu.

NOTE: *To select a menu item, highlight it using the arrow keys and press the ✓ key.*

3. Select the Ethernet interface for which DHCP is to be disabled, such as “**`eth0`**”.
4. Select “**`DHCP`**” from the next menu.
   The display will show “**`State=Enabled`**” and “**`Action=Disabled`**”.

NOTE: *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.

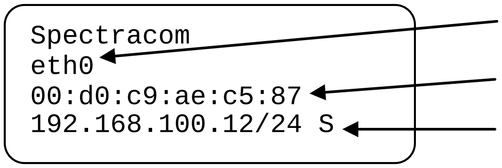
2.11.2 To Enter IP Address and Subnet Mask

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.
2. Press the ✓ key once to enter the setting, then again to apply the new setting.

2.11.3 To Enter the Gateway Address (if Required)

1. Still on the **`Home / Netv4 / eth[0-3]`** menu, select **`Gateway`**, and change “**`N=010.010.201.254`**” to the value of the default gateway to be assigned to this interface.
2. Press the ✓ key once to enter the setting, then again to apply the new setting.

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 from the **Network / General Setup** page of the SecureSync web interface.

NOTE: *The remainder of the configuration settings will be performed through the SecureSync product web-based user interface (accessed through a web browser such as .*

Determine whether configuration will be done on a computer attached to the network or a computer connected directly to the SecureSync unit. For a network computer, connect a shielded CAT 5, Cat 5E or CAT 6 cable with RJ-45 connectors to the Ethernet port on the SecureSync rear panel (refer to Figure 1-2). Connect the opposite end of the cable to a network hub or switch. For connection with a stand-alone computer, this cable should be pinned as a network-crossover cable and should be connected to the NIC card of the computer. Verify the green link light on the Ethernet port is illuminated. The amber "Activity" link light may periodically illuminate when network traffic is present.

Connect to the SecureSync unit using a web browser (such as Internet Explorer or Mozilla Firefox) directed to either the static IP address or the address assigned by DHCP, as displayed on the front panel LCD. If the network supports DNS, the hostname may also be entered instead (the default hostname is "Spectracom"). You can now manage and configure your product through the SecureSync product web interface. Refer to Section *3.3*: "*Product Configuration Using the Web User Interface*" for additional information.

NOTE: *The factory-default user name and password are:*

Username: `spadmin`
Password: `admin123`

With input references connected, verify the SecureSync's front panel Sync lamp is green. Initial synchronization with GNSS input may take up to 35 minutes (approximately) when used in the default stationary GNSS operating mode. If using GNSS, verify that GNSS is the sync source by navigating to the **Status / Time and Frequency Status** page and viewing the "Selected Time Reference Source" in the table. The Selected Time Reference Source for GNSS is "GPS 0".

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

Synchronize the network PCs via NTP using the Ethernet port as desired. For a more description of synchronizing Windows PC's, please visit the Spectracom website (www.spectracomcorp.com), and from the main site navigation menu select **Support > Library > Installation and Troubleshooting Guides**, and download / review the document titled *Synchronizing Windows Computers*. This document also contains information and details about using the Spectracom PresenTense NTP client software.

During configuration of the various options it may be necessary to power down or restart the unit. In this case a 'Halt' command should be issued prior to removing power from the unit. Failure to do so may cause the SecureSync unit to take longer to boot on the next power up cycle. After the 'halt' command is issued via the web interface or front panel, wait until the LCD reads 'Power off SecureSync' before removing power (refer to Section *3.9*: *Rebooting the System* for additional information).

2.12 Ethernet Network Cabling

Spectracom SecureSync provides a base 10/100 Ethernet port for full NTP functionality, as well as a full web-based user interface for configuration, monitoring and diagnostic support. Additional network ports are available with the Gigabit Ethernet option module (refer to Section 8 for additional information).

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

Use shielded CAT 5 or CAT 6 cable with RJ-45 connectors.

When connecting to a hub or router use a straight-through wired cable.

When connecting directly to a Windows PC, use a crossover wired network cable. Since no DHCP server is available in this configuration, both SecureSync and the Windows 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 the product documentation for the version of the Windows operating system that you are using.

2.13 Product Registration

Spectracom periodically releases important software updates for our products. If you would like to be notified of these updates as they become available, the Spectracom website provides a product registration page. To register your email address for automatic notifications of software updates, please visit www.spectracomcorp.com. Product registration can be accessed from the "**Support**" menu.

NOTE: If SecureSync has access to the Internet, the **Tools / "Contact/Register**" page of the SecureSync web interface provides the direct link to register your product & contact information.

Section 3: Product Configuration

NOTE: Screens displayed in this manual are for illustrative purposes. Actual screens may vary depending upon your particular SecureSync configuration (e.g., whether or not certain option cards are installed, etc).

After installing SecureSync, verify that power is connected and wait for the device to boot up.

The front panel display provides certain configuration data on start-up. The LED window displays the current time (UTC, TAI, GPS or local timescale, as configured. Current time will be displayed in UTC by default). The LCD window displays the unit's hostname, IPv4 address, mask, and gateway.

NOTE: If using DHCP, the IP address will be assigned automatically and displayed on the front panel. You may use a web browser to connect to this IP address and configure the SecureSync through the web browser user interface. Refer to *"Network Configuration with DHCP"*.

When configuring a SecureSync without DHCP, or to configure a SecureSync that has not been assigned an IP address, refer to Network Configuration, Section *3.2*.

3.1 Network Configuration with DHCP

Once connected to the DHCP server through the network, the SecureSync is assigned an IP address. This address and other network information are displayed on the front panel when the device boots up. Enter the IP address in your browser (on a computer connected to the network) and log in as an administrator. The HTTP session will be redirected automatically to an HTTPS session and a security certificate pop-up window will be displayed. Accept the certificate by clicking "OK."

NOTE: Unless you are using DNS in conjunction with DHCP (with the client configured using SecureSync's hostname instead of IP address), DHCP must be disabled and the IP address must be changed to a static address once the SecureSync is properly configured. Failure to do this will result in a loss of time synchronization if the DHCP server assigns a new IP address to the SecureSync.

NOTE: Unless the user opens the web interface 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 interface. 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. Refer to Section *3.5.4* for more information on creating a new SSL certificate.

3.2 Network Configuration without DHCP

NOTE: The IP address assignment in this configuration may be performed even if your network has a DHCP server. There may be times when you do not wish DHCP to automatically assign an IP address for the SecureSync.

To configure a SecureSync without a DHCP server available on the network or to configure a SecureSync that has not been assigned an IP address; you can use either the front panel keypad and LCD display or a serial cable to connect a PC or laptop computer to the serial port on the front of the SecureSync. The keypad is the simplest method to configure the network settings. Refer to Section *2.10* for information on using the keypad. Refer to Sections *2.11.1*, *2.11.2* and *2.11.3* for steps to disable DHCP and to configure the IP address, Subnet Mask and Gateway address.

If you desire to use the front panel serial port instead of the keypad, after making this connection, use a terminal emulator program (such as HyperTerminal) to log into the SecureSync as an administrator. Use the Command Line Interface (CLI) in the terminal program to configure initial values and determine the SecureSync's network address. Refer to *Section 10:* for more information on the serial port connection and *Section 11*: for a list and description of the available serial port commands that can be issued.

A) To configure SecureSync's network settings using the front panel serial port:
1) Connect a serial cable to a PC running HyperTerminal and to 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 Table 2-2 for a list of subnet mask values).
5) Type **`gw4set 0 zzz.zzz.zzz.zzz`** <Enter> (where 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.

3.3 Product Configuration Using the Web User Interface

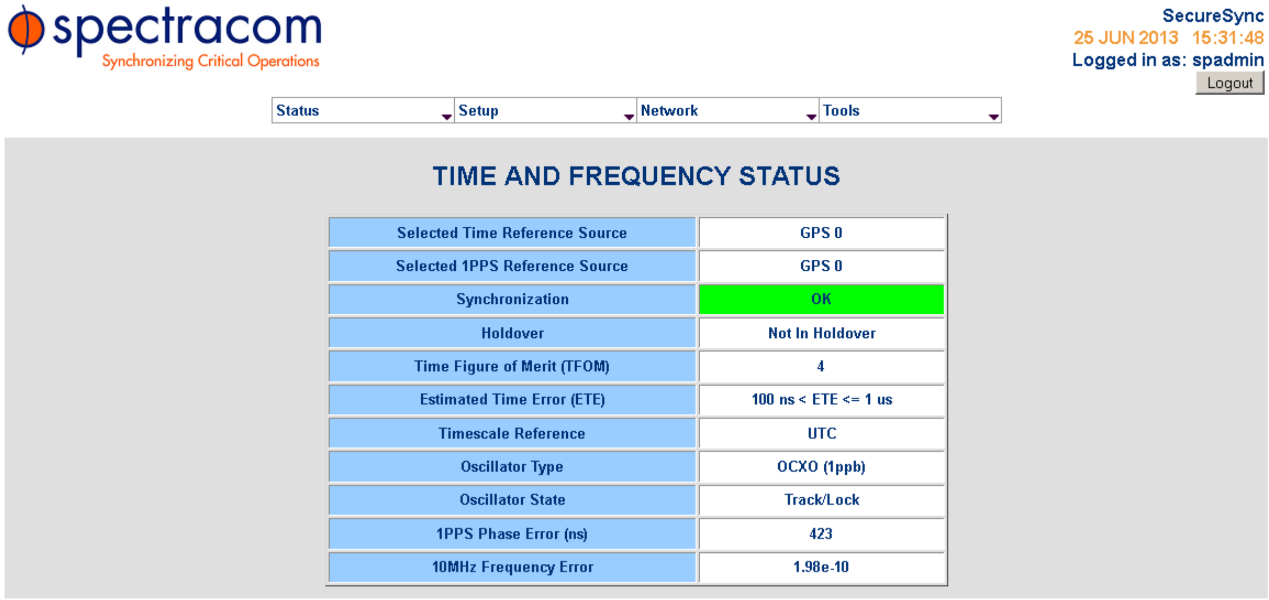
Once the SecureSync has been configured with the appropriate network settings and connected to the network, you may configure it, change its operating settings, check status, and generate reports from the web user interface (or "web UI") as needed. All web interface pages are accessible from the primary navigation menu at the top of the main SecureSync page, which is displayed after a successful login. These pages, their functions, and example configurations (where applicable) are presented in this section.

NOTE: At any time during configuration in the web interface, click the "Submit" button to save the settings or "Reset" button to restore the settings to their previous state.

The SecureSync web interface automatically refreshes about every 30 seconds. This allows status changes to be monitored without the need for the administrator to manually reload the page. ***Note:*** After 15 minutes of idle time, the operator is automatically logged off the web interface session.

Primary-level navigation menu options include **Status**, **Setup**, **Network** and **Tools**, and are located in a horizontal row near the top of the product web interface. All primary-level menu options have sub-menus (or secondary-level) options. Select an item from any of the sub-menus to access the page for that particular option. Some pages also contain tabs that can be selected which group options into logical sections. For ease, this document defines which page to navigate to using the format: "**XXXX / YYYY**", where "**XXXX**" is the primary-level menu selection and "**YYYY**" is the drop-down menu option to be selected (refer to Figure 3-1).

In certain instances, the second page viewed will allow access to other web pages. So, another specific page may need to be selected. This may be indicated in the manual as "**XXXX / YYYY / ZZZZ**" where "**ZZZZ**" is the next page selection to choose.



SecureSync
25 JUN 2013 15:31:48
Logged in as: spadmin

TIME AND FREQUENCY STATUS

Selected Time Reference Source	GPS 0
Selected 1PPS Reference Source	GPS 0
Synchronization	OK
Holdover	Not In Holdover
Time Figure of Merit (TFOM)	4
Estimated Time Error (ETE)	100 ns < ETE <= 1 us
Timescale Reference	UTC
Oscillator Type	OCXO (1ppb)
Oscillator State	Track/Lock
1PPS Phase Error (ns)	423
10MHz Frequency Error	1.98e-10

Figure 3-1: SecureSync Web Interface

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

Status: Obtain current SecureSync status to include input AC/DC power, Time Sync/Holdover, NTP Stratum level, option modules (if installed) as well as input references being present and valid.

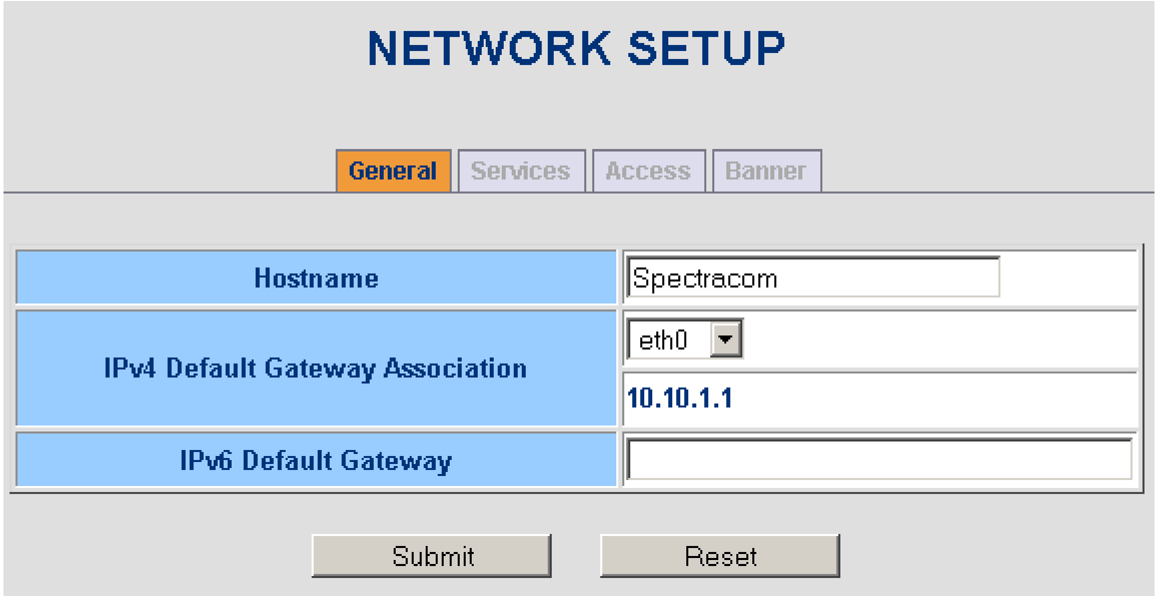
Setup: Configure input references (GNSS, IRIG, NTP, manually set time, etc), view/set date and time, configure front panel display and option modules (if installed), configure logs and oscillator disciplining.

Network: Configuration including general network settings (hostname, gateway, static routes, services, access security), individual interface network settings (DHCP, DNS, Domain, IP address/netmask, gateway, static routes), HTTPS/SSH setup (certificates & keys), NTP (enable NTP, NTP Access), SNMP, LDAP, RADIUS and IPSec configuration.

Tools: Setup user accounts, configure notifications, review logs, perform software updates and backup configurations, reboot / halt the appliance, display version information, register the product for notifications of software updates.

3.4 Network Setup Pages

From the main navigation menu in the SecureSync web interface, network setup options can be accessed from the **Network** menu item.



Hostname	Spectracom
IPv4 Default Gateway Association	eth0 10.10.1.1
IPv6 Default Gateway	

Figure 3-2: Network Setup Page (1 of 2)

The **Network / General Setup** page contains the following tabs:

General: Allows configuration of the SecureSync hostname (default: “Spectracom”), IPv4 and IPv6 default gateways. IPv4 main default gateway is specified by associating an interface, which then provides the main default gateway.

Services: Allows the configuration of various services (Daytime Protocol Service, Time protocol service, FTP, SSH, HTTP, HTTPS). ***Note:*** Disabling individual services closes the associated port for that particular service.

Access: From this tab, the following options can be configured:

IPv4/IPv6 CIDR Access Tables:

Allows the configuration of access restrictions from assigned networks / nodes. Examples:

1) Enter nothing: No restrictions
2) 10.10.0.0/16: Limit access to machines on 10.10.x.x network.

To delete an entry, check the “Delete” checkbox for that item, and click Submit.

Web Session, Strict IP Check:

When enabled, a web UI session will be restricted to a client (web browser) using a single IP address. Complex networks using network address translation, load balancing, or load sharing can present multiple IP addresses for a single web client. In those situations, strict IP checking must be disabled. Select the desired value from the dropdown list and click Submit.

Banner: Allows the administrator to configure a custom banner message to be displayed on the SecureSync login page (Note: there is a 2000 character size limit).

The **Network / Interfaces** page displays the configurable settings for the SecureSync network interfaces (with each available interface displayed and managed on a separate tab). ***Note:*** The number of tabs displayed is generated dynamically depending upon what available interfaces exist (i.e., a tab is only displayed if the interface is installed).

The following common values are configurable for each of the network interface tabs:

MAC Address: Displays the physical layer / MAC address for that particular interface.

DHCP Setup: Allows management of DHCP services for that particular interface. DHCP may be enabled or disabled (On / Off), or the IP configuration (lease) for that interface may be released or renewed (Release / Renew).

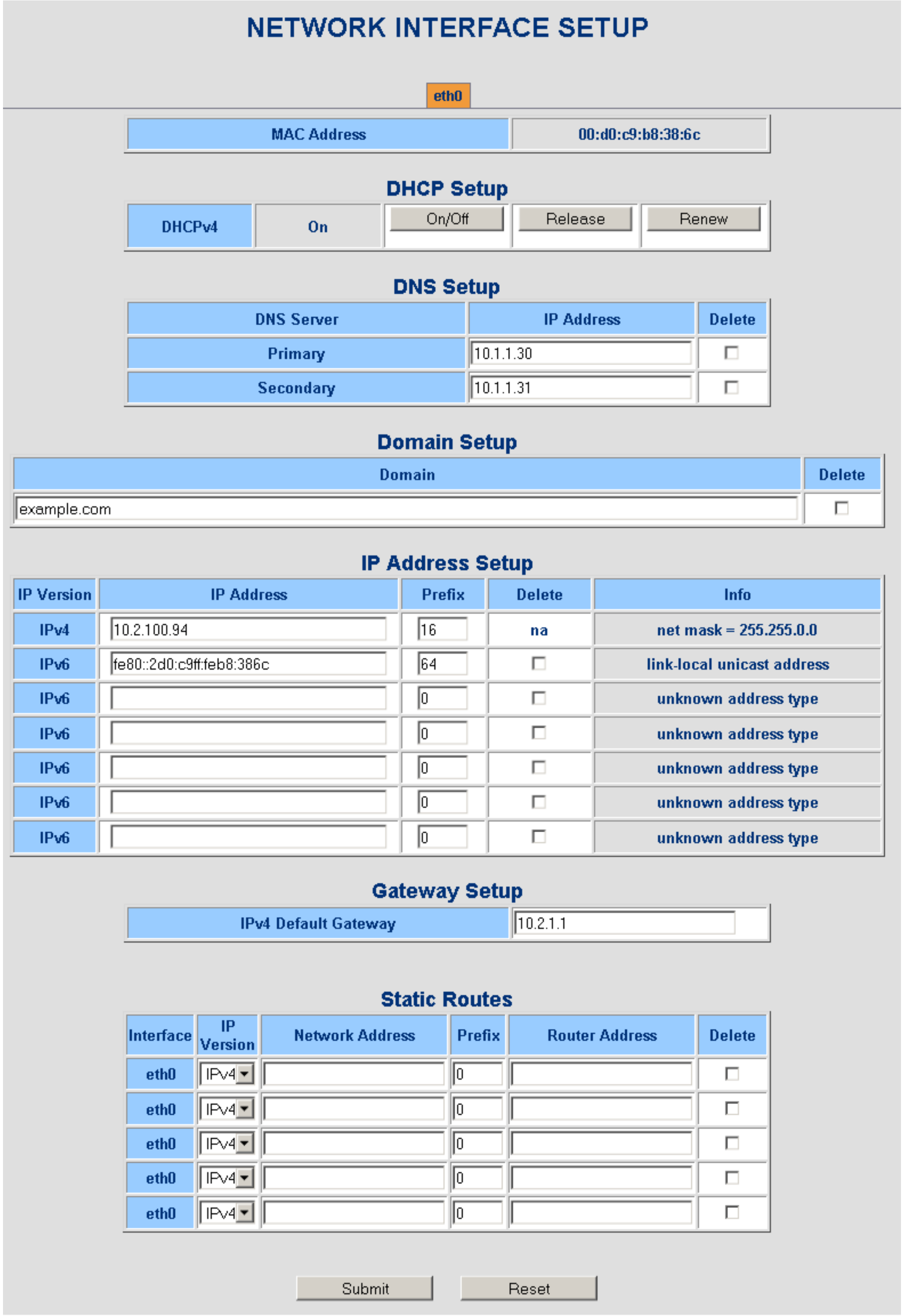
DNS Setup: Allows manual configuration of the IPv4 DNS servers for that particular interface.

Domain Setup: Allows manual configuration of the domain name for that particular interface.

IP Address Setup: Allows manual configuration of IPv4 and IPv6 settings for the selected network interface, including IP Address, and network prefix. To delete an entry, check the appropriate “Delete” box and select “Submit”. The Reset option undoes any changes since the last submit.

Gateway Setup: Allows manual configuration of IP protocol default gateways in the routing table for that particular interface.

Static Routes: Allows manual configuration of static routes in the routing table for that particular interface.



NETWORK INTERFACE SETUP

eth0

MAC Address	00:d0:c9:b8:38:6c

DHCP Setup

DHCPv4	On	On/Off	Release	Renew

DNS Setup

DNS Server	IP Address	Delete
Primary	10.1.1.30	□
Secondary	10.1.1.31	□

Domain Setup

Domain	Delete
example.com	□

IP Address Setup

IP Version	IP Address	Prefix	Delete	Info
IPv4	10.2.100.94	16	na	net mask = 255.255.0.0
IPv6	fe80::2d0:c9ff:feb8:386c	64	□	link-local unicast address
IPv6		0	□	unknown address type
IPv6		0	□	unknown address type
IPv6		0	□	unknown address type
IPv6		0	□	unknown address type
IPv6		0	□	unknown address type

Gateway Setup

IPv4 Default Gateway	10.2.1.1

Static Routes

Interface	IP Version	Network Address	Prefix	Router Address	Delete
eth0	IPv4		0		□
eth0	IPv4		0		□
eth0	IPv4		0		□
eth0	IPv4		0		□
eth0	IPv4		0		□

Submit Reset

Figure 3-3: Network Setup Page (2 of 2)

3.5 Configuring Network Security

Spectracom SecureSync uses OpenSSH and OpenSSL. OpenSSH is the Open Source version of the Secure Shell; which provides a set of server side tools allowing secure remote telnet like access and secure file transfer using remote copy (like SCP and FTP/SFTP). OpenSSL is the Open Source version of Secure Sockets Library; which is used to provide the encryption libraries. Together, OpenSSH and OpenSSL provide industrial strength encryption allowing for secure remote administration via command line, HTTPS web pages and secure file transfers.

The user is permitted to enable or disable HTTPS and SSH. The product can be configured to allow access only via NTP and the secure protocols such as HTTPS or SSH, or to operate in a less secure mode.

3.5.1 Configuring SSH

SSH can be configured from the **Network /** "**HTTPS/SSH**" setup page of the SecureSync web interface (select the SSH tab). The tools supported are SSH – secure shell, SCP – secure copy, and SFTP – secure file transfer protocol. The 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. The secure Spectracom product permits users to create or delete RSA or DSA keys for the SSH2 protocol.

NOTE: Due to vulnerabilities in SSH1 protocol, it is not supported. Only SSH2 is supported.

The user may choose to delete individual RSA or DSA host keys. To delete a key, simply select "Enabled" in the field for the key you wish to delete and press submit at the bottom of the page.

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. To create a new set of host keys first delete the old keys, then select the create host keys checkbox and enter the key sizes you desire. Then select the "Submit" button at the bottom of the screen.

SecureSync units 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 up to 4096 are supported, but may take ten 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 and finally 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.

Note also that 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 either have to override the warning and accept the new Public Host Key and start a new connection or they may need to remove the old Host Public Key from their client system and accept the new Host Public Key. Please consult your specific SSH client's software's documentation.

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 by either 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

The first option allows users to login using either method. This is the default. 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. The second 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. Finally the last option requires the user to load a public key into the 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.

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

The web browser user interface provides the means for the user to view and edit the **`authorized_keys`** file, to add Public Keys. Using FTP, SCP, or SFTP the user may also retrieve the **`authorized_keys`** file from the.ssh directory.

An example of a user adding a public key to the **`authorized_keys`** file is shown below.

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

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.
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 the product. The user can transfer a new public key file using the web interface.

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.

3.5.2 Secure File Transfer

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.

1. 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
   ```

2. 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
   ```

3. 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.

4. 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.

3.5.3 Recommended SSH Client Tools

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

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

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.

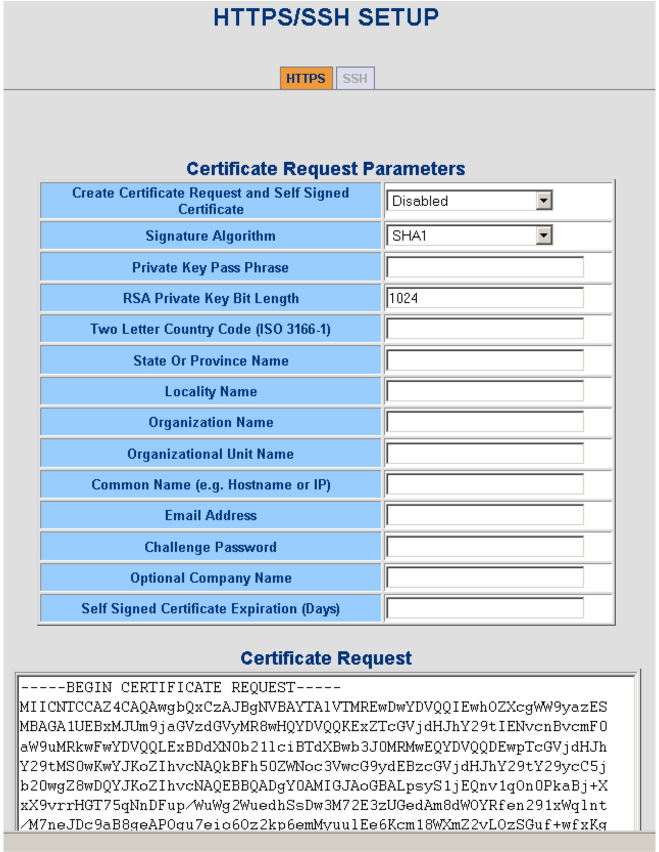
The putty SSH tools and instructions regarding their use can be found at: http://www.chiark.greenend.org.uk/~sgtatham/putty/

3.5.4 Configuring HTTPS

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

Each SecureSync comes with a default Spectracom self-signed SSL certificate. The typical expiration of the certificate is about 10 years. HTTPS is available using this certificate until this certificate expires. If deleted however, this certificate cannot be restored (a new certificate will need to be generated).

The OpenSSL library provides the encryption algorithms used for secure HTTP (HTTPS). The OpenSSL package also provides tools and software, which is used to create X.509 Certificate Requests, Self Signed Certificates and Private/Public Keys. The 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 CA. If a Certificate Authority is not available the user can simply use the self-signed certificate that comes with the unit until it expires or create their own self-signed certificates to allow the use of HTTPS.



Certificate Request Parameters

Create Certificate Request and Self Signed Certificate	Disabled
Signature Algorithm	SHA1
Private Key Pass Phrase	
RSA Private Key Bit Length	1024
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 Company Name	
Self Signed Certificate Expiration (Days)	

Certificate Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIICNTCCAZ4CAQAwgbQxCzAJBgNVBAYTAlVTMREwDwYDVQQIEwhOZXcgWW9yazES
MBAGA1UEBxMJUm9jaGVzdGVyMR8wHQYDVQQKExZTcGVjdHJhY29tIENvcnBvcmF0
aW9uMRkwFwYDVQQLExBDdXN0b21lciBTdXBwb3J0MRMwEQYDVQQDEwpTcGVjdHJh
Y29tMS0wKwYJKoZIhvcNAQkBFh50ZWNoc3VwcG9ydEBzcGVjdHJhY29tY29ycC5j
b20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALpsyS1jEQnv1q0n0PkaBj+X
xX9vrrHGT75qNnDFup/WuWg2WuedhSsDw3M72E3zUGedAm8dW0YRfen291xWqlnt
/M7neJDc9aB8geAPOqu7eio60z2kp6emMyuulEe6Kcm18WXmZ2vL0zSGuf+wfxKg
```

Figure 3-4: HTTPS Configuration

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.

For more information on OpenSSL, please see www.openssl.org.

The SecureSync's software supports X.509 DER and PEM and P7 PKCS#7 PEM and DER formatted certificates. The user can create a customer specific X.509 self-signed certificate, an RSA private key and X.509 certificate request using the web interface. RSA private keys are supported because they are the most widely accepted (at this time, DSA keys are not supported).

3.5.5 Requesting Certificate Authority Certificates

Once the processing to create the certificate request, RSA private key, and self-signed certificate is completed, the SecureSync will display the certificate request through the web interface.

The user can submit this certificate request to the company's Certificate Authority for a verifiable, authenticable third party certificate. Until this certificate is received, the user's self-signed certificate, displaying the information shown herein, can be used.

The SecureSync will load this new self-signed certificate and private key after the user selects a few more web page options or when the user selects the "Exit connection to product" button at the top of the screen. You will see a pop up window in Windows operating systems. The certificate can be installed or viewed using 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.

3.5.6 Updating X.509 PEM Certificate Files Using the Web Interface

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 in avoiding issues with the Certificate Authority having issues to reconciling certificate request and company record information.

NOTE: When generating a certificate, select **Apache** when prompted for information on the Web server's software. This should result in the preferred X.509 PEM certificate format.

The Common Name field 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. This field should be filled with the hostname or IP address of the SecureSync. Spectracom recommends using 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. If using only self-signed certificates, the user should choose values based on the company's security policy.

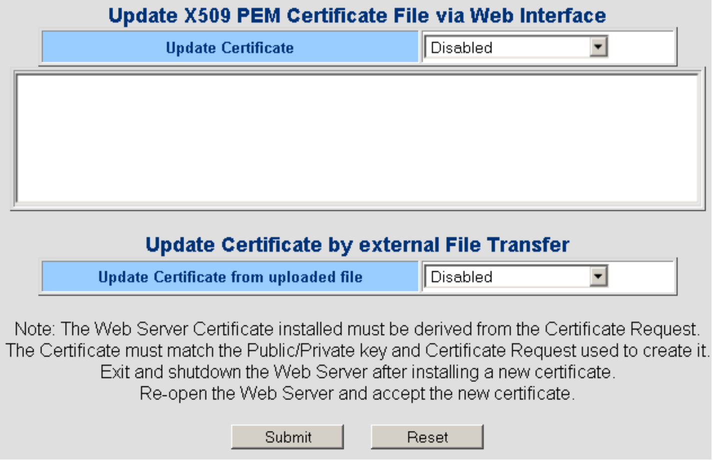
Many certificate authorities simply provide you with a certificate in the form of a plain text file. If your certificate is provided in this manner, and the certificate is provided in the X.509 PEM format, you may simply copy and paste the text into the web interface. Paste the text into the "Update Certificate" box, make sure that the Update Certificate checkbox is selected, and submit your changes.

NOTE: Only X.509 PEM certificates can be loaded from the web interface.

3.5.7 Updating X.509 PEM Certificate Files through External File Transfer

If you are provided with a certificate file and the certificate is ***not*** in the X.509 PEM format, you may use an alternative method to update the certificate. Name the file using the following scheme:

File Type	File Name
X.509 PEM	`cert.pem`
X.509 DER	`cert.der`
pkcs7 PEM	`certpem.p7c`
pks7c DER	`certder.p7c`



Update X509 PEM Certificate File via Web Interface

Update Certificate	Disabled

Update Certificate by external File Transfer

Update Certificate from uploaded file	Disabled

Note: The Web Server Certificate installed must be derived from the Certificate Request.
The Certificate must match the Public/Private key and Certificate Request used to create it.
Exit and shutdown the Web Server after installing a new certificate.
Re-open the Web Server and accept the new certificate.

Figure 3-5: Update HTTPS certificate

Next, use an FTP, SCP, or SFTP program to connect to the SecureSync. Copy your certificate to the default FTP starting directory. Then select the "Update Certificate from uploaded file" checkbox, select the appropriate file name in the associated drop-down box, and click "Submit". The default directory to place the file is "**`home/spectracom`**".

Be aware that it may take several minutes for the certificate request, the private key, and self-signed certificate are created. The larger the key, the longer amount of time is required. It is recommended that a 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.

The user is provided with several signature algorithm choices, including MD5, SHA1, SHA256 and SHA512. The signature algorithm or message digest is most commonly MD5. Other secure options include SHA1 and RMD160.

If necessary, consult your web browser vendor's documentation and Certificate Authority for key bit lengths and signature algorithms supported.

If a system is rebooted during this time, the certificate will not be created. When the operation is completed, the user will see a certificate request in the certificate request text box. A digital file copy of the certificate request can be found in the root directory with the file name `cert.csr`. This file can be retrieved using FTP, SCP or SFTP. The certificate request can also be copied / pasted from the certificate request text box in the web interface.

3.5.8 If You Cannot Access a Secure SecureSync

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.

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, access to the secure Spectracom product can become denied.

To restore access to SecureSync, you must utilize the front panel keypad and LCD 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 Section *2.10* for information on using the keypad and LCD display.

3.5.9 Default and Recommended Configurations

The factory default configuration settings were chosen for ease of initial setup. Refer to the recommended settings listed here as applicable for your unit.

Option / Feature	Default Setting	Recommended Setting	Where to Configure
HTTP	Enabled	Disabled	Web User Interface or Command Line Interface
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 User Interface
SNMP	Disabled	Disabled or Enabled (with SNMP v3 w/ encryption*)	Web User Interface
NTP	Enabled (with no MD5 values entered)	Enabled (use MD5 authentication with user-defined keys)	Web User Interface
Daytime Protocol	Disabled	Disabled	Web User Interface
Time Protocol	Disabled	Disabled	Web User Interface
Command Line Interface			
Serial Port	Available	Available	Not Applicable
Telnet	Enabled	Disabled (use SSH instead)	Web User Interface
SSH	Enabled (default private keys provided)	Enabled	Web User Interface
File Transfer			
FTP	Enabled	Disabled (use SFTP or SCP)	Web User Interface
SCP	Available	Available	Not Applicable
SFTP	Available	Available	Not Applicable

**We recommend secure clients use only SNMPv3 with authentication for secure installations.*

Table 3-1: Default and Recommended Configurations

3.6 Resetting SecureSync to Factory Default Configuration

In certain situations, it may be desired to reset all SecureSync configurations back to the factory default configuration. The GNSS position, as either calculated by the GNSS receiver (if a GNSS receiver is installed) or manually entered by a user, will be stored and retained through power cycles. SecureSync configurations, GNSS location and the locally stored log files (with the exception of the Authentication and NTP logs which can't be cleared) can be erased via the web interface. Restoring configurations (reloading a saved configuration), erasing the stored GNSS location and clearing the log files are separate processes ("clean" configuration also erases the stored GNSS position). It may be desired to perform one without performing 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. Refer to Section 2.9.

If the GNSS location is erased, the next time that 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.

A) To reset all configurations back to the factory default settings:

1) Go to the **Tools / "Upgrade/Backup"** page and select the **Configuration** tab.
2) Change the "**Clean Configuration**" option to "**Enabled**", then click Submit. SecureSync will reboot with "`Starting up SecureSync`" displayed in the front panel LCD.

B) To reset the GNSS receiver position:

1) Disconnect the GNSS antenna cable from the back panel antenna jack.
2) Navigate to the **Setup / Inputs / GPS** page.
3) Change the "**Position Clear**" option to "**Enabled**", then click Submit. Verify the "**Manual Position Setup**" on this page are now set to all 0's.

The GNSS receiver's position information has now been erased and is no longer stored. Upon reconnecting the GNSS antenna and when the receiver is able to track at least four satellites (and as long as the GNSS receiver is configured for the Standard mode), the GNSS survey will be performed again.

C) To clear all local log files stored on the SecureSync (with the exception of the authentication and NTP logs, which can't be cleared):

1) Navigate to the **Setup / Logs** page and select the "**General Settings**" tab.
2) Click "**Clear All Log Files**".
3) Click Submit.

D) To clear only a particular category of log files stored on the SecureSync (with the exception of the authentication and NTP logs which can't be cleared):

1) Navigate to the **Setup / Logs** page and click on the applicable tab name for the desired log file to be cleared.
2) Change the "**Clear File**" checkbox to "**Enabled**", then click Submit.

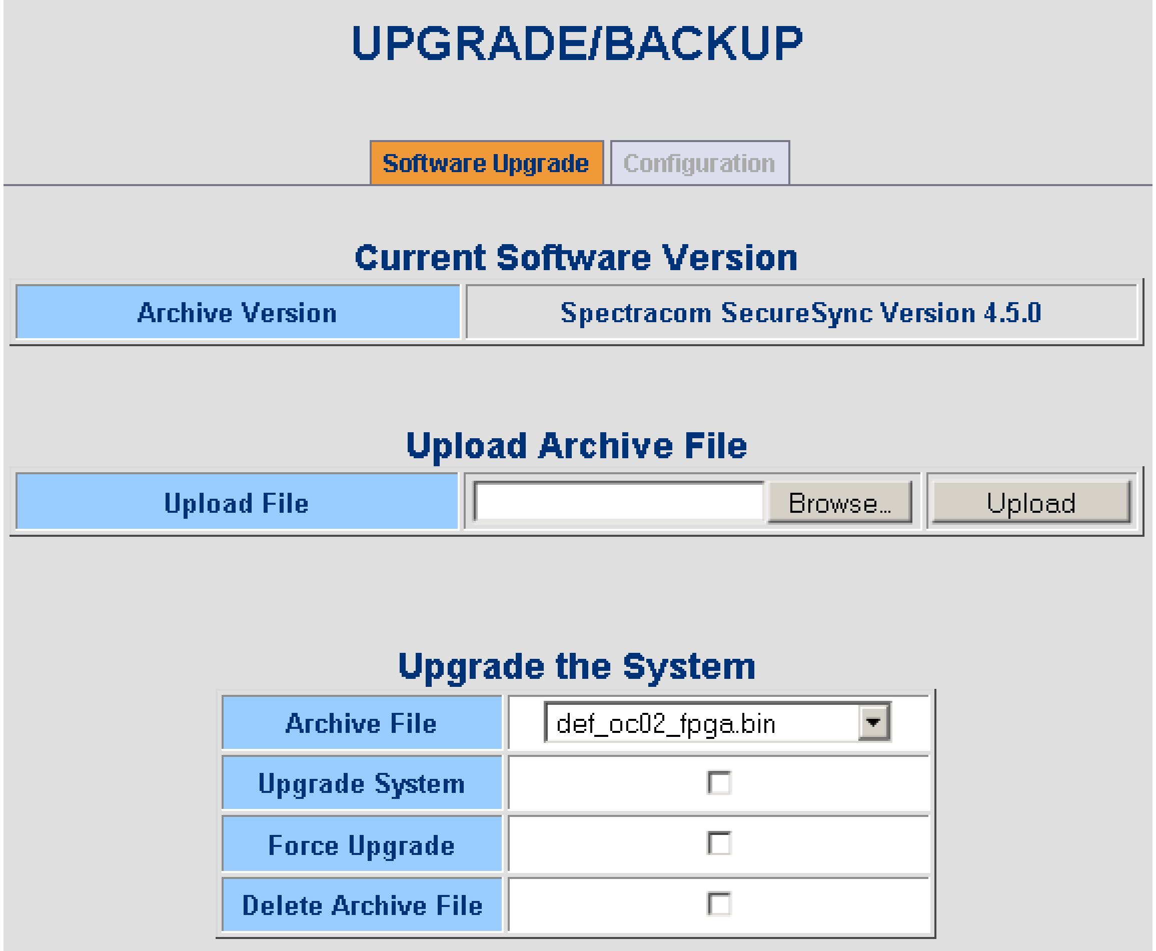
3.7 Backing-up and Restoring Configuration Files

Once SecureSync has been configured, it may be desired to backup 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.

NOTE: For security reasons, configurations relating to security of the product, such as SSH/SSL certificates are not backed up to a PC.

The **Configuration tab** on the **Tools / "Upgrade/Backup"** page allows the configuration and log files to be saved, or backed up to and restored from a PC. Refer to the following figure.



UPGRADE/BACKUP

Current Software Version

Archive Version	Spectracom SecureSync Version 4.5.0

Upload Archive File

Upload File	Browse...	Upload

Upgrade the System

Archive File	def_oc02_fpga.bin
Upgrade System	□
Force Upgrade	□
Delete Archive File	□

Figure 3-6: Example Upgrade/Backup page

A) To save SecureSync Log Files to a PC:

1) Navigate to the **Tools / Upgrade/Backup** page and select the **Configuration** tab.
2) Change the "**Save Log Files**" option to "**Enabled**", then click "Submit". A message will display:

"`Creating Log Archive at /home/spectracom/xfer/log/securesync.log`".

You can then use your preferred method to connect to the SecureSync unit (SFTP/FTP, etc) to access the saved logs.

B) To save SecureSync Configuration Files to a PC:

1) Navigate to the **Tools / "Upgrade/Backup"** page and select the "**Configuration**" tab.
2) Change the "**Save Configuration**" option to "**Enabled**", then click "Submit". A new file will be created on the SecureSync unit, located at: **`/home/spectracom/xfer/config/securesync.conf`.**
3) FTP/SFTP into the SecureSync and navigate to this specified file location. Transfer this file to the desired location on your PC.

C) To restore / clone SecureSync Configuration Files from a PC:

1) Open an FTP/SFTP session with the SecureSync unit you wish to transfer the files to (the **`securesync.conf`** should be located on this PC).
2) Navigate to the location **`/home/spectracom/xfer/config/`** and transfer the **"`securesync.conf`"** file from the directory it is located on this PC into this SecureSync directory.
3) From the SecureSync web interface, navigate to the **Tools / "Upgrade/Backup"** page and select the "**Configuration**" tab.
4) Change the "**Restore Configuration**" option to "**Enabled**" and click "Submit".

After enabling the "**Restore Configurations**" option, SecureSync will automatically transfer the **`securesync.conf`** file from the **`/home/spectracom/xfer/config`** directory to a new location. SecureSync will then reboot in order to read the new configuration files. Once powered back up, SecureSync will be configured with the previously stored file.

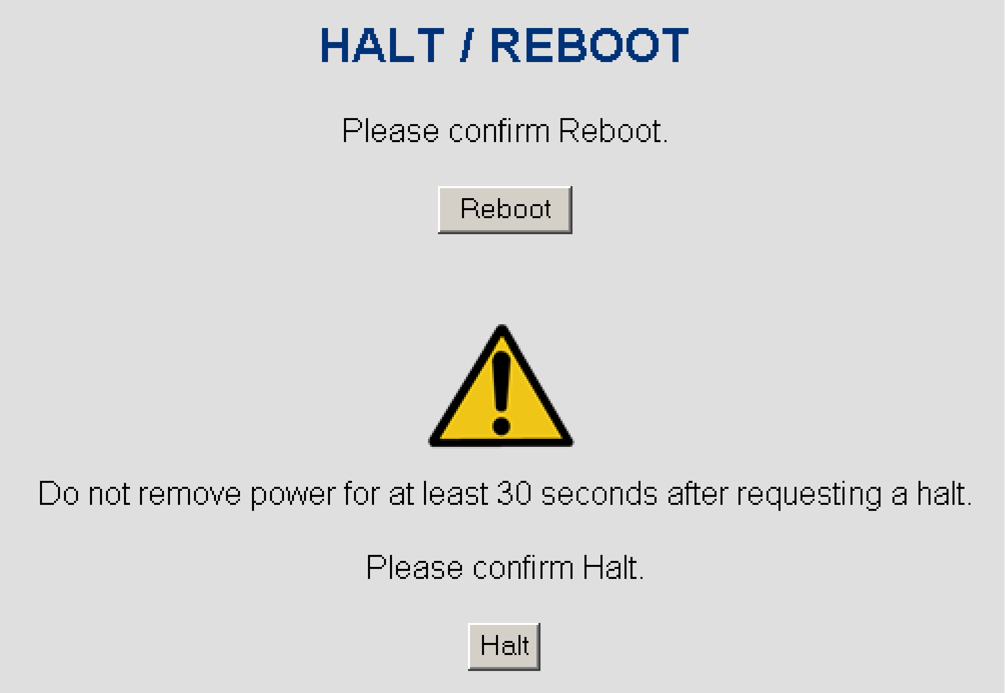
3.8 Issuing the HALT Command before Removing Power

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 can allow for faster startup after the next power-up of SecureSync.

NOTE: The HALT command may be issued to the SecureSync through the web interface, the front panel serial port, or the front panel keypad.

3.8.1 Issuing the HALT Command through the Web User Interface

From the **Tools / "Reboot/Halt"** page, click the Halt button. Wait 30 seconds after making the Halt request before removing power to the unit. The system may also be rebooted from this page. To Halt SecureSync for power-down, click the "Halt" button.



HALT / REBOOT

Please confirm Reboot.

Do not remove power for at least 30 seconds after requesting a halt.

Please confirm Halt.

Figure 3-7: System Reboot/Halt Screen

3.8.2 Issuing HALT Command through the LCD/Keypad or the Serial Port

The Halt command can be initiated via the Keypad and LCD display. Refer to Section 2.10 for information on using the keypad to perform a Halt.

With a serial connection to the front panel serial port, type **`halt`** <Enter> to halt the SecureSync for shutdown.

> ***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.

3.9 Rebooting the System

SecureSync can also be rebooted from the **Tools / "Reboot/Halt"** page. Click the "Reboot" button. SecureSync will now be rebooted and be accessible again shortly thereafter.

3.9.1 Issuing the REBOOT Command through the LCD/Keypad or Serial Port

The Reboot command can be initiated via the Keypad and LCD display. Refer to section 2.10 for information on using the keypad to perform a system reboot.

With a serial connection to the front panel serial port, type **`reboot`** <Enter> to reboot the SecureSync.

Once the Reboot process has been initiated via the SecureSync web interface or front panel, the front panel LCD will display a "*Power off SecureSync*" message, and the front panel LED time display will stop incrementing until it has started booting back up again.

3.10 Changing or Resetting 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 from the SecureSync web interface.

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 the **Tools / Users** page.
2) Select the **"Manage User Accounts"** tab.
3) In the row that has the Username "**`spadmin`**", enter the desired new password into the "Password" textbox.

   NOTE: The new password can be from 8 to 32 characters in length.

4) Retype the desired password in the "Retype Password" textbox.
5) Check the "Update Account" box to "Enabled".
6) Click the "Submit" button.

If the current **`spadmin`** account password has since been changed from the default value and is no longer a known value, 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. Since the unknown administrator password would be required to login to the web browser in order to change it via the web browser, this password needs to be reset via the front panel keypad (or with the front panel serial port). Perform either of the two following to reset the password:

To reset the `spadmin` account password from an unknown value back to the factory default value using the keypad, perform the following:

1) Use the front panel LCD and the keypad to perform a "**RESETPW**". Refer to Section *2.10* regarding the use of the front panel keypad. ("Resetpw" is located in the **Home/System** menus). 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 from an unknown value back to the factory default value using the serial port, perform the following:

1) Connect a PC to the front panel serial port and login 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 previous procedure to change the password from a known value to another value (by logging into the SecureSync web interface with the default password of “`spadmin`” and the default password “`admin123`”. Then navigate to the **Tools / Users** page, **Manage User Accounts** tab).

3.11 Configuring and Reading the "System Time"

SecureSync has an "internal clock", referred to as the "System Time". The System Time is synchronized to its input references (such as GNSS, IRIG, ASCII data, NTP, PTP, etc) or it can be manually configured by a user to a desired time/date. The System Time is then 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).

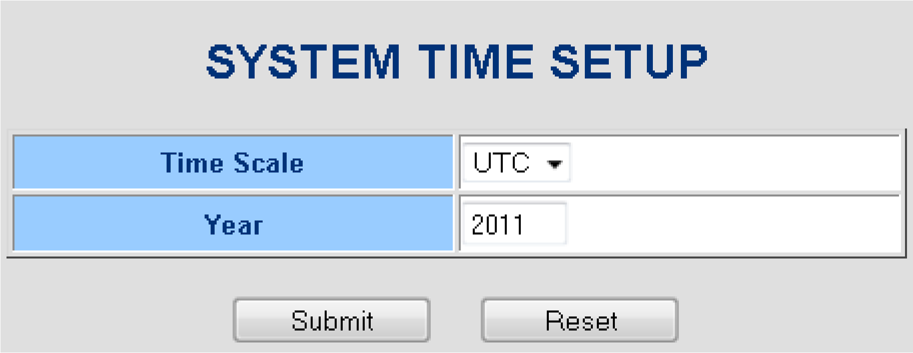
3.11.1 Configuring the System Time Timescale

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 September, 2013, TAI time is 35 seconds ahead of UTC.

The System Timescale is configured in the "System Time Setup" located on the **Setup / Time Management** page. Refer to the following figure:



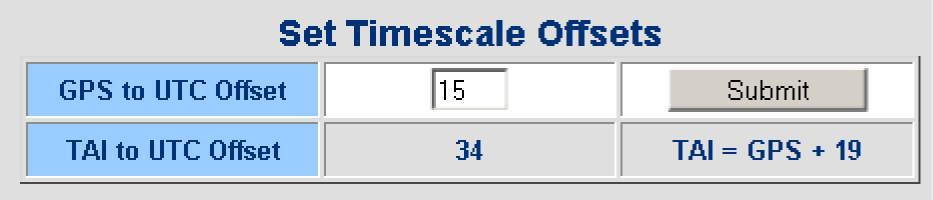
SYSTEM TIME SETUP

Time Scale	UTC
Year	2011

Figure 3-8: System Time Setup

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 "Set Timescale Offsets" box 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 the “Set Timescale Offsets” section of the **Setup / Time Management** page:



Set Timescale Offsets

GPS to UTC Offset	15	Submit
TAI to UTC Offset	34	TAI = GPS + 19

Since the GPS and TAI offsets have a fixed relationship, only the GPS offset can be set on this page. 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.

IMPORTANT NOTE: 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.

3.11.2 Reading and Manually Setting the System Time

The current System Time can be either obtained or manually set using the “**Set Manual Date/Time**” options from the **Setup / Time Management** page. These fields will display the current time, Day of Year (DOY) and current year that System Time is using to generate the SecureSync’s available outputs (Note that the current System Time and date are also displayed in the top right-hand corner of the web interface, above the main menus).

The System Time can also be manually set by a user, if desired. Once the time and/or date has been manually set, this manually set System Time will be synchronized to these values and the values will be used for the generation of the outputs (NTP, Log entries, front panel display, etc).

NOTE: System time must be set in UTC timescale, not local time.

In order for the time to be able to be manually set by a user and used for synchronization, the Input Reference Priority table on the **Setup / Reference Priority** page needs to have this capability enabled. The Index row of this table that has "user" in both the Time and 1PPS columns needs to be configured as "Enabled".

Refer to Section *3.17* for more information on configuring the Reference Priority table. A "**USE CASE Example**" provides additional information on manually setting the System Time.

Once the System Time has been manually set, it will continue to use this incrementing time as the System reference, unless a valid, higher priority input reference becomes available (a higher priority input reference will cause the System Time to change to the input reference's time/date) or until SecureSync is rebooted/power cycled.

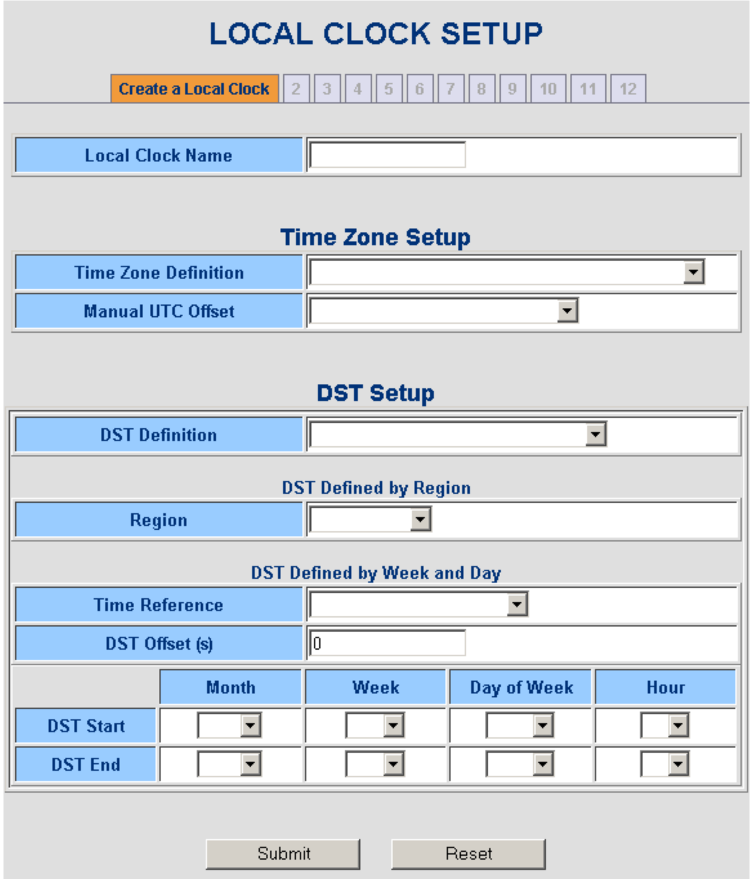
System Time is "maintained" during power-down and should be fairly close to the correct time upon power-up. It is also possible to use this "start-up" time as the synchronized time by enabling synchronization to the battery backed time. Refer to Section *3.17* for more information on synchronizing to the battery backed time. The "start-up" time can also be used when a valid 1PPS input is also applied. This is referred to as "Local System" reference. A "**USE CASE Example**" provides additional information on using "Local System" reference.

IMPORANT NOTE: Disable NTP before setting user time, and re-enable NTP after time is set. If it is desired to use the NTP output with a user set time/date (instead of it being synchronized to an external reference such as GNSS or IRIG input), it is highly recommended that either the time/date be very accurately set to the current time/date, or that all other input references in the Input Reference Priority table be set to "Disabled". If another higher priority input reference becomes available with the reference input being enabled, the user set System Time's time/date values will automatically be corrected to the incoming reference. The time jump that would occur if the System Time was not set at least fairly close to the input reference when the reference syncs the System would prevent NTP from using System Time as a reference, until the NTP Service is either manually disabled and then re-enabled, or until SecureSync is rebooted/power-cycled.

3.11.3 Local Clock Setup

The selected TimeScale for System Time defines the Timescale of the System. As the System Time is the basis for the time of all outputs, it may be desired to output the time with an offset for “Local time” (Time Zone offset and Daylight Saving Time adjusted). The Local Clock provides the means to apply a time offset for local time to various outputs. Local Clocks are only used in conjunction with the UTC timescale (Local Clocks do not apply to the GPS and TAI Timescales).

The **Setup / Local Clock** page provides the means to create one or more local clocks that can be shared with many of the SecureSync inputs and outputs that support local time capability (such as the front panel LED time display, IRIG input / output, etc).



DST Offset (s): 0

Figure 3-9: Local Clock Setup

Multiple Local Clocks with different configurations can be created, as needed. The names of all Local Clocks that have already been created are displayed as tabs across the top of the page.

3.11.4 Creating a New Local Clock

Local Clock Name: Enter any name you wish for the Local Clock Name (up to 64 characters long and spaces between names are allowed). It 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:

1. 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.
2. Built-in Timescales are displayed as Local Clocks, UTC, TAI, GPS
3. User-created Local Clocks are displayed after built-in local clocks in the local clock dropdown boxes.

Time Zone Definition: Under Time Zone Setup, there are two choices:

- Automatically configure to unit's physical locality
- Manually defined UTC offset

Automatically Configure to Unit's Physical Locality
By selecting this option, the unit will compute the Time Zone Offset automatically based on the location of the unit provided by the GNSS receiver (if installed) or manually entered by a user (refer to Section *3.19.1*).

If you select this feature before the GNSS receiver completes the position calculation, a message will be displayed to explain that this feature is not valid until the position is available. If you select this feature after the GNSS receiver determines its position, the computed Time Zone Offset information will be shown.

Once this option has been selected and submitted, the SecureSync software will determine the values for the appropriate manual fields. These manual definitions will be displayed when the defined clock is edited.

NOTE: Automatic time zone calculations are imprecise because the time zones are determined by local political boundaries that may change.

Manually Defined: By selecting "Manually Defined", the user can specify a number of hours added or subtracted from UTC for the desired time zone. The desired number of hours to offset is defined in the "Manual UTC Offset" field below this field.

Manual UTC Offset: All of the Time Zone Offset drop-downs in the web UI user interface 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.

DST Setup

The Local Clock can be configured to automatically adjust for DST (Daylight Saving Time change), if applicable in your area. A few pre-configured DST Rules are available, including DST rules for Australia, Canada, Europe and the US. The DST rule can also be manually configured for other areas or other DST rules.

DST Definition

Daylight Saving Time (DST) observance varies with locality and application. Choose the configuration that reflects your location and needs. Under the DST SETUP, you will see three choices:

- No DST rule, always standard time
- Manually defined by region
- Manually defined by week and day

No DST Rule, Always Standard Time

When this option is selected, this Local Clock will not observe DST time changes. An output assigned to use this Local Clock will always output the time as Standard time.

Manually Defined by Region

From this dropdown box, the user may select commonly defined geographic regions that share DST rules. There may be exceptions based on your location. The options include the following:

- EU (Europe)
- US-Canada (post-2006)
- Australia

Select "**EU" (Europe)** 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).

Select "**US-Canada"** 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).

DST Manually Defined by Week and Day

This option is provided for those customers that 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.

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.

Time 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 inputted.

A Manually Defined by Week and Day configuration table exists in the Defined by Week and Day section of this page. These fields allow each portion on the DST Rules to be manually defined.

The DST Rules consist of a DST Start date/time and a DST End date/time. The DST Start date defines when the location switches from Standard to DST time. The DST End date defines when the location switched from DST to Standard time. This table provides drop-down fields to set the Month, which week of the Month and which day of the month the DST adjustment should occur, and a field to enter at what time the adjustment should occur.

3.11.5 Examples - DST Rule Configurations

Example 1: To create a Local System Clock to UTC+1 with no DST rule:

1) Assign the clock a meaningful name for this clock in “Local Clock Name”.
2) Select “Manually defined” for the Time Zone Definition.
3) Select “UTC +01:00” from the “Manual UTC Offset” pull down menu.
4) In the “DST Definition” field, select “No DST rule, always standard time”.
5) Review the changes made and click “Submit”.
6) 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).

1) Select “Enabled” for the “Create a Local Clock”.
2) Assign the clock a meaningful name for this clock in “Local Clock Name”.
3) Select “Manually defined” for the Time Zone Definition.
4) Select “UTC -05:00” from the “Manual UTC Offset” pull down menu.
5) In the “DST Definition” field, select “Manually defined by region”.
6) In the “Region” field, select “Canada-US”.
7) Review the changes made and click “Submit”.
8) The SecureSync will display the status of the change.

3.11.6 Example - Editing a Previously Created Local Clock

Any previously created Local Clock can be edited as desired. Select the name of the Local Clock from the top of the **Setup / Local Clock** page. Edit the desired value(s) in the Local Clock setup requiring modification and click Submit.

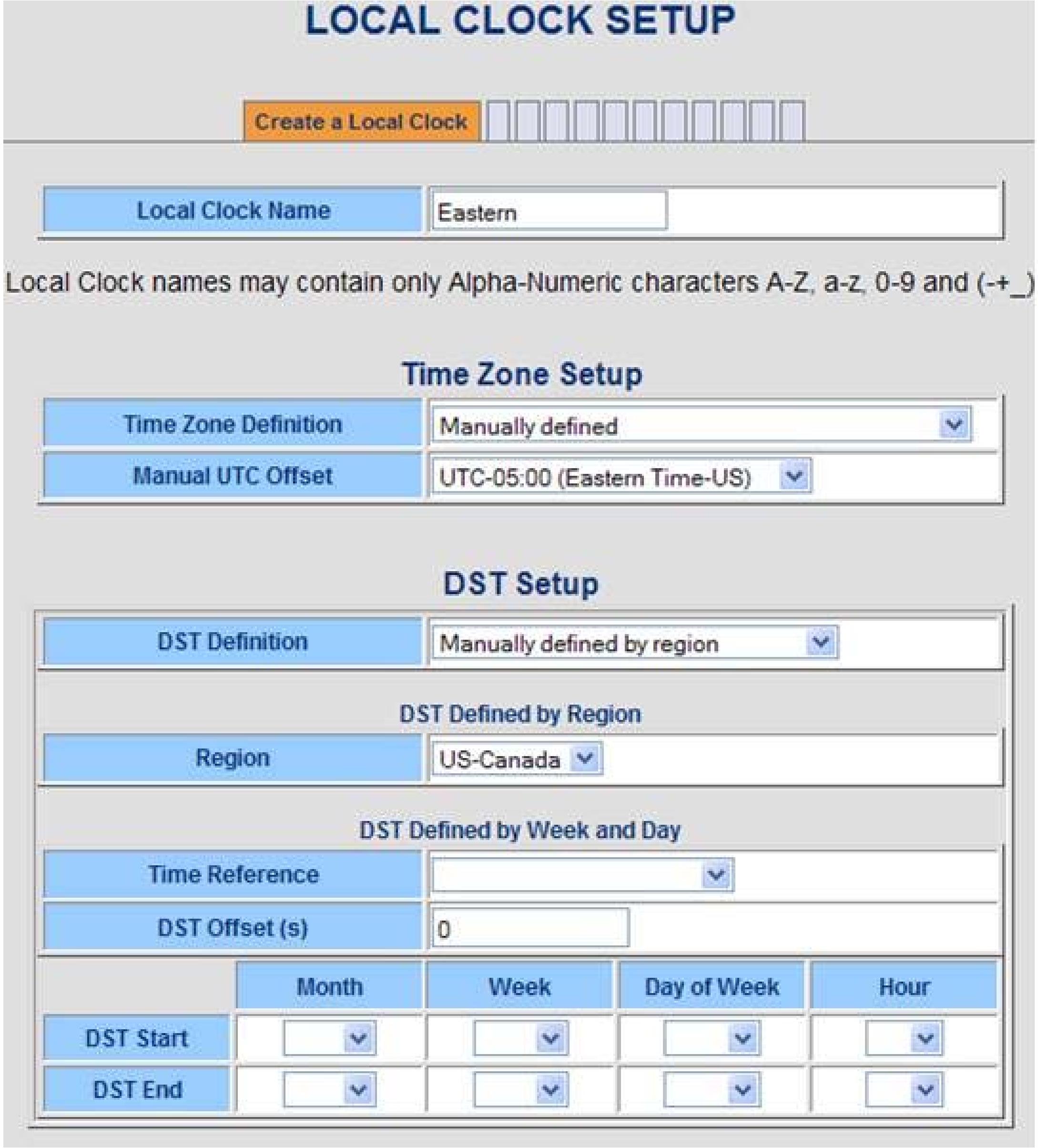
The modifications made will affect the DST correction/computations for all inputs and outputs that are configured to use the name of the just edited Local Clock.

3.11.7 Example - Applying Local Clock to Front Panel or ASCII Outputs

The following example scenario includes steps that can be used to apply a local clock to the SecureSync front panel or to ASCII outputs to show local time.

A. Creating a Local Clock:

1. From the SecureSync web interface, verify a Local Clock has already been created. Navigate to the **Setup / Local Clock** page and configure the Local Clock options as described in the following example:



LOCAL CLOCK SETUP

Create a Local Clock

Local Clock Name	Eastern

Local Clock names may contain only Alpha-Numeric characters A-Z, a-z, 0-9 and (-+_)

Time Zone Setup

Time Zone Definition	Manually defined
Manual UTC Offset	UTC-05:00 (Eastern Time-US)

DST Setup

DST Definition	Manually defined by region

DST Defined by Region

Region	US-Canada

DST Defined by Week and Day

Time Reference	
DST Offset (s)	0

	Month	Week	Day of Week	Hour
DST Start				
DST End				

Local Clock Name: Enter an arbitrary name for the Local Clock. The name can be used as a cross reference for the output ports that can be configured to display local time (such as the front panel).

2. Under the **Time Zone Setup** section, set the options as follows:

   a. **Time Zone Definition:** Set to "**Manually defined**"

b. **Manual UTC Offset:** Set to the appropriate Time Zone Offset for your region. Note that US States use the values with a dash character (“-“), such as: “**UTC-05:00**” for **Eastern** or “**UTC-06:00**” for **Central**, etc.

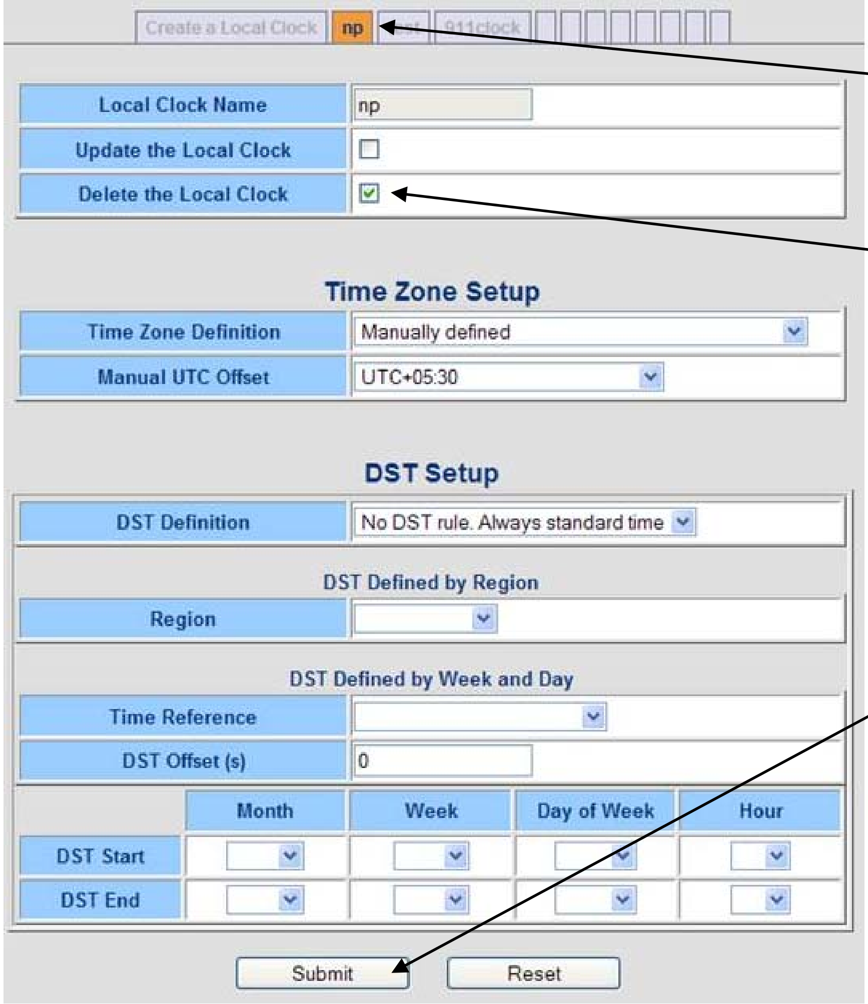
3. Under the **DST Setup** section, set the options as follows:

    a. **DST Definition:** For US States / Regions that observe Daylight Saving Time (DST) rules, select “**Manually defined by region**”. If not applicable to your region, leave this option set to “**No DST Rule. Always standard time**”.
    b. Under the **DST Defined by Region** section: Set the **Region** option depending on whether or not your region observes Daylight Saving Time (DST) rules. For example: for US States / Regions, select “**US-Canada**”.
    c. Under the **DST Defined by Week and Day** section: For US States / Regions that observe US DST rules (and have “**US-Canada**” defined for the **Region** option), there is no need to set the Time Reference, DST Offset(s), DST Start, or **DST End** options – the values will automatically populate after clicking “Submit”.

4. After defining the DST Setup options, click “Submit”. A message stating “`Configuration Successful`” should be displayed.

    NOTE: If a message stating “`Validation Error`” is displayed, the local clock was not successfully created. Perform the following steps to delete and recreate the Local Clock:

    1. From the SecureSync web interface, navigate to the **Setup / Local Clock** page.
    2. Click on the first tab to the right of the “**Create a Local Clock**” tab (note: there may or may not be a name displayed on the tab – refer to the following example).
    3. After this tab has been selected, click the checkbox for the “**Delete the Local Clock**” option. Refer to the following example.



Local Clock Name	np
Update the Local Clock	□
Delete the Local Clock	☑

Time Zone Setup

Time Zone Definition	Manually defined
Manual UTC Offset	UTC+05:30

DST Setup

DST Definition	No DST rule. Always standard time

DST Defined by Region

Region	

DST Defined by Week and Day

Time Reference	
DST Offset (s)	0

	Month	Week	Day of Week	Hour
DST Start				
DST End				

1. Click the first tab to the right of the "**Create a Local Clock**" tab.

2. Click the "**Delete the Local Clock**" checkbox.

3. Click "**Submit**".

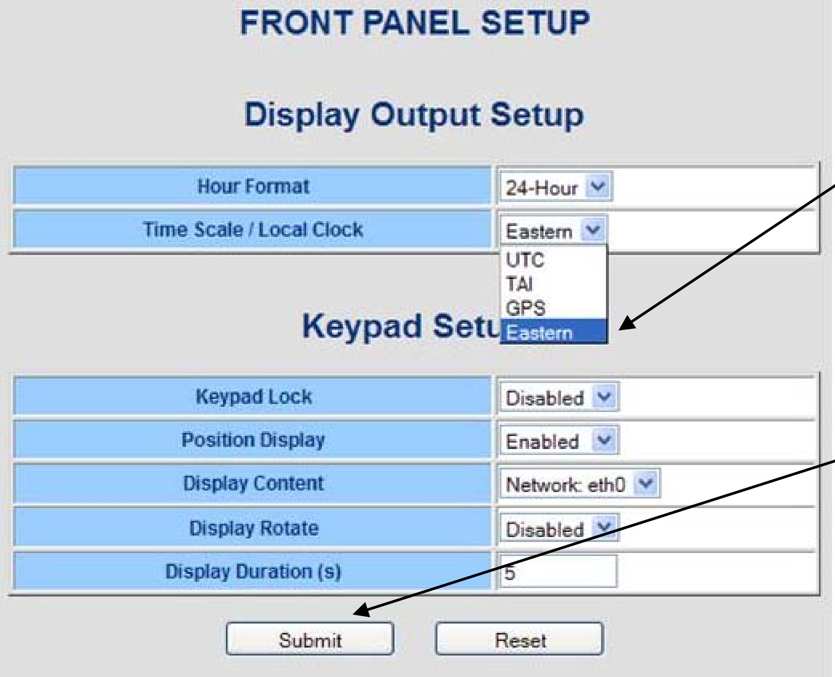
4. After deleting the Local Clock, you will need to create a new one. Click to select the "**Create a Local Clock**" tab at the top of the page. Create a new Local Clock using the same, previous values. Once the Local Clock has been recreated, any "`Validation Error`" messages should no longer appear.

B. Configure Front Panel to Display Local Time (Instead of Factory Default UTC time)

Once a Local Clock has been created, you can set the front panel time display to also show local time. To do this, take the following steps:

1. From the SecureSync web interface, navigate to the **Setup / Front Panel** page.
2. Under the **Display Output Setup** section, locate the **Time Scale / Local Clock** option, and select your desired Local Clock from the drop-down list. (Note: The names of all created Local Clocks will be displayed in this list).
3. If desired, set the **Hour Format** option to display in either a 12 or 24 hour format.

Once you've completed your configuration of the Display Output Setup options, click "Submit". The front panel should now display the correct local time. Refer to the following example.



FRONT PANEL SETUP

Display Output Setup

Hour Format	24-Hour
Time Scale / Local Clock	Eastern

Keypad Setu

Keypad Lock	Disabled
Position Display	Enabled
Display Content	Network: eth0
Display Rotate	Disabled
Display Duration (s)	5

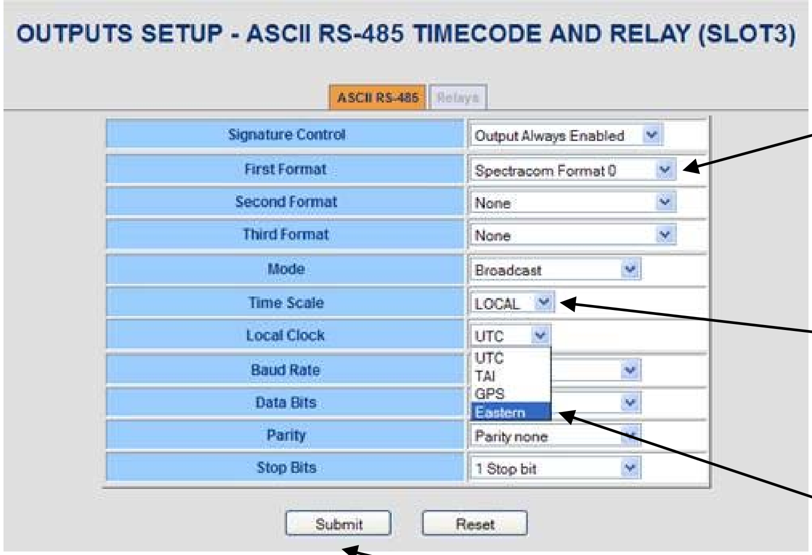
1. For the **Time Scale / Local Clock** option, select the name of the desired custom Local Clock from the drop-down list.

2. Click "**Submit**".

C. If there are any Spectracom TimeView digital display clocks connected to the Remote RS-485 output of the NetClock, configure the Remote output port for Format 0, 9600, local time output, every second:

1. From the SecureSync web interface, navigate to the **Setup / Outputs** page and select the Slot where the IRIG RS-485 & Relays option module card is installed. Ensure the "**ASCII RS-485**" tab is selected.
2. Set the First Format option to "**Spectracom Format 0**"
3. Set the Time Scale option to "**Local**"
4. Set the Local Clock option to the desired custom Local Clock

After defining the DST Setup options, click "Submit". A message stating "`Configuration Successful`" should be displayed. Refer to the following example.



OUTPUTS SETUP - ASCII RS-485 TIMECODE AND RELAY (SLOT3)

Signature Control	Output Always Enabled
First Format	Spectracom Format 0
Second Format	None
Third Format	None
Mode	Broadcast
Time Scale	LOCAL
Local Clock	UTC
Baud Rate	
Data Bits	
Parity	Parity none
Stop Bits	1 Stop bit

1. For the **First Format** option, select "**Spectracom Format 0**" from the drop down list

2. For the **Time Scale** option, select "**Local**" from the drop-down list

3. For the **Local Clock** option, select the desired custom Local Clock

4. Click "**Submit**".

3.11.8 Reference Information about Daylight Saving Time Change

The general Time Zone and DST rule information can be found from the following web sites: http://www.worldtimeserver.com/, http://webexhibits.org/daylightsaving/b.html.

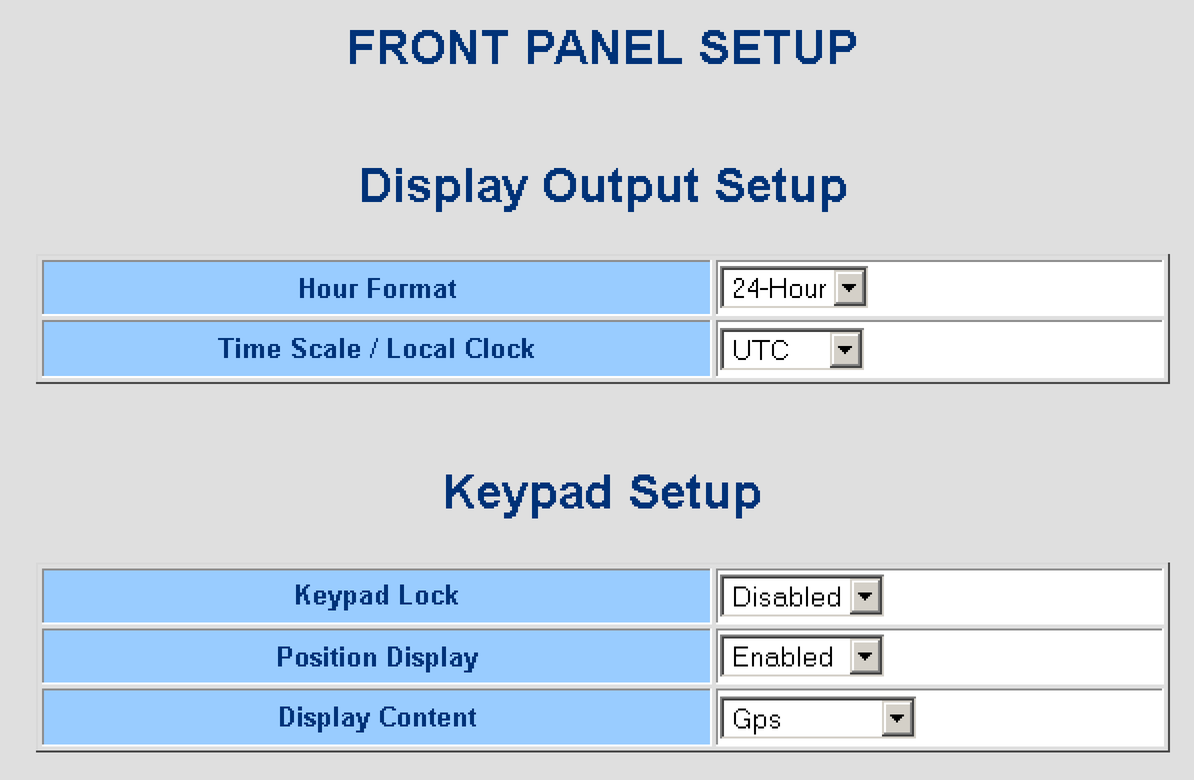
3.12 Front Panel LED / LCD Display and Keypad Configuration

The Front Panel LED time display, LCD display and the keypad operation can be configured from the **Setup / Front Panel** page from the SecureSync web interface.

The SecureSync front panel contains an 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 6PM).

The SecureSync front panel also features an LCD display. Besides being used in conjunction with the keypad, the LCD window can be configured to display different screens when the keypad is not in use. To prevent inadvertent keypad operation, it can be locked and unlocked from the web interface.

The front panel setup page is divided into two sections: **Display Output Setup** and **Keypad Setup**. The configurable front panel options in these sections are detailed herein.



FRONT PANEL SETUP

Display Output Setup

Hour Format	24-Hour
Time Scale / Local Clock	UTC

Keypad Setup

Keypad Lock	Disabled
Position Display	Enabled
Display Content	Gps

Figure 3-10: Front Panel Setup screen

Display Output Setup

Hour Format: This drop-down configures the LED time display to show the current time in either 12 hour format (such as displaying “6” for 6PM) or 24 hour format (such as displaying “18” at 6PM).

NOTE: While configured as 12 hour format and during “PM” hours (noon until midnight), a “PM indicator” (decimal point) will be displayed to the bottom-right of the hours portion of the LED time display. The “PM indicator” extinguishes during “AM” hours.

Time Scale / Local Clock: This option configures the time scale for the LED time display. The available options are UTC, TAI (Temps Atomique International), GPS and Local. UTC is also referred to as ZULU time. GPS 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). If GPS or TAI time is used, then the proper timescale offsets must be set on the **Setup / Time Management** page. (Refer to Section *3.11.1* for more information). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

Local Clock: The System Time may be configured as the UTC timescale (default configuration), but it may be desired to display local time on the front panel instead. With the Timescale field set to “Local”, select the name of a previously created Local Clock in the drop-down. The Time Zone and DST rules, as configured in the Local Clock will now be applied to the front panel time display. Refer to Section *3.11.3* for more information on Local Clocks.

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.

Keypad Setup

Keypad Lock: 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 or with this drop-down field. When Lock is configured as “Disabled”, the front panel keypad operation is available.

Position Display: Disables the front panel position display screen. If it is currently selected, the front panel display screen is set to “none”.

Display Content: Determines what is normally displayed in the LCD window 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).

If the keypad is unlocked, pressing any keypad key will temporarily return the LCD display to the “Home” menu display for keypad operation. A minute after the last keypad press, the configured LCD screen will be displayed again.

Several LCD screen displays are available for selection, including:

> **Network:** 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: Displays current key status indications (such as NTP Stratum level, TFOM – "Time Figure of Merit", Sync status and Oscillator lock status).

Position: Displays current latitude, longitude and antenna height.

Day of Year: Displays the day of year (such as "Day of Year 104")

GPS: 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: Displays the current date (such as "16 April 2012").

> ***NOTE:*** The date is based on the configured LCD's timescale. 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: (*Applicable to SAASM GPS receiver option module only*): Will display "`NOT SUPPORTED`" unless a SAASM receiver is installed.

None: Configures the LCD window to remain blank unless the keypad is unlocked and in use.

Display Rotate: Enables rotation of the content display in the LCD window when the keypad is not in use. Content will rotate through all enabled content for installed options.

Display Duration (s): Sets the duration in seconds for content display during rotation before the next content screen is displayed. Valid duration range is between 1 and 30 seconds.

3.13 User Accounts

In addition to the available default administrator (**`spadmin`**) account, up to 64 more user accounts can be created, each having its own assigned login password. User accounts can be created to have either limited user or full administrator rights.

User accounts can be created and managed from the **Tools / Users** page. The "**Create a User Account**" tab allows for new accounts to be created while the "**Manage User Accounts**" tab allows current user accounts to be managed.

To create a new user account, click on the "**Create a User Account**" tab. Configurable options are described below.

Username: Enter the desired user name. The user name can be any combination of lower-case characters only (upper-case characters, punctuation symbols and numbers are not allowed). The minimum username length is 3 characters and the maximum is 32 characters.

Password: Enter the desired login password for this account. The password can be any combination of upper and lower-case characters. The minimum password length is 8 characters and the maximum length is 32 characters.

Retype Password: Please retype the password to verify the desired value.

Group: 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
    - IPSec
    - LDAP / RADIUS
    - SNMP (with the exception of configuring SNMP notifications)

To manage user accounts that have already been created, open the “**Manage User Accounts**” tab. From this tab, the administrator can define group memberships, change passwords, and remove (delete) user accounts from SecureSync.

NOTE: The “**Manage User Accounts**” tab includes a number inside of the parenthesis “()”. This indicates how many user accounts currently exist.

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.

Security-related user setup options can be managed from the “**Security**” tab. Configurable options are as follows:

Idle Timeout

Idle Timeout (minutes): Defines the number of minutes without activity before the SecureSync will require the user to log back in. A value of “0” means the idle timeout feature is disabled.

Password Aging

Password Aging is a feature that can be used to require a user to change their password periodically.

Minimum before change (days): Defines the minimum number of days after a user has changed a password before they are allowed to change it again. ***Note:*** The default value for this option is 0, which means there is no restriction.

Maximum before expiry (days): Defines the number of days before the password expires and the user will be required to change it. ***Note:*** The default value for this option is 99,999, which means the passwords will never expire.

Warning before expiry (days): Defines how many days before the expiry the user will be given an indication that the password will expire. ***Note:*** Warnings will not apply unless the expiry is enabled.

NOTE: If a user ignores the warnings or does not log in during the warning period, they will no longer be able to log into the SecureSync web interface. In this case, one of the following steps will restore access:

- An "admin" level user can change the user's password
- The user can log in to the command line interface via **`telnet`**, **`ssh`**, or the front panel serial connection. During the login process the user will be required to change their password.
- As a special case, the **`spadmin`** account password can be reset from the front panel keypad, under the menu **Home > System > ResetPW**.

Password Length

Minimum Length: Allows for a user-defined minimum length / number of characters for password length. ***Note:*** Default minimum length is 8, and maximum length is 32 characters.

Complex Passwords

The complex passwords options allow for the configuration of various password complexity requirements. The following options can be enabled or disabled:

- **Require uppercase**
- **Require lowercase**
- **Require number**
- **Not based on a user name**
- **Require special character:** If enabled, every password must have at least one of each of the following character types:
  - Letters (a-z or A-Z)
  - Numbers (0-9)
  - Special characters (~ @ # % ^ & * ( ) _ - + = { } [ ] : ; < > . |)

The following special characters are <u>NOT</u> allowed: single quote, double quote, dollar sign, comma, backslash, exclamation mark, and apostrophe.

Additionally, the username may not be included in the password.

Default Accounts

The SecureSync ships with a default "`spfactory`" account that users with strict security requirements may want to permanently remove. The factory account is not essential for any support or repair functions, but is sometimes used for those purposes as a convenience.

> **Remove Factory Account:** To permanently remove the default factory account, click the check box for this option and select Submit. ***Note:*** ***<u>This action cannot be reversed.</u>***

3.14 Oscillator Disciplining

SecureSync can be purchased with various types of internal ovenized oscillators. The available oscillators consist of a 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) oscillator. 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 OCXO 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.

The purpose of the internal oscillator is to provide SecureSync with an accurate 10 MHz output that is extremely stable, even when input references aren't available. The oscillator also provides a very accurate internal time base in case reference inputs are either lost or declared not valid. The oscillator is also used to generate the 1PPS output.

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: The SecureSync must be ordered with the desired oscillator installed at the time of the initial purchase. The oscillators cannot be swapped after the SecureSync has been shipped from the factory.

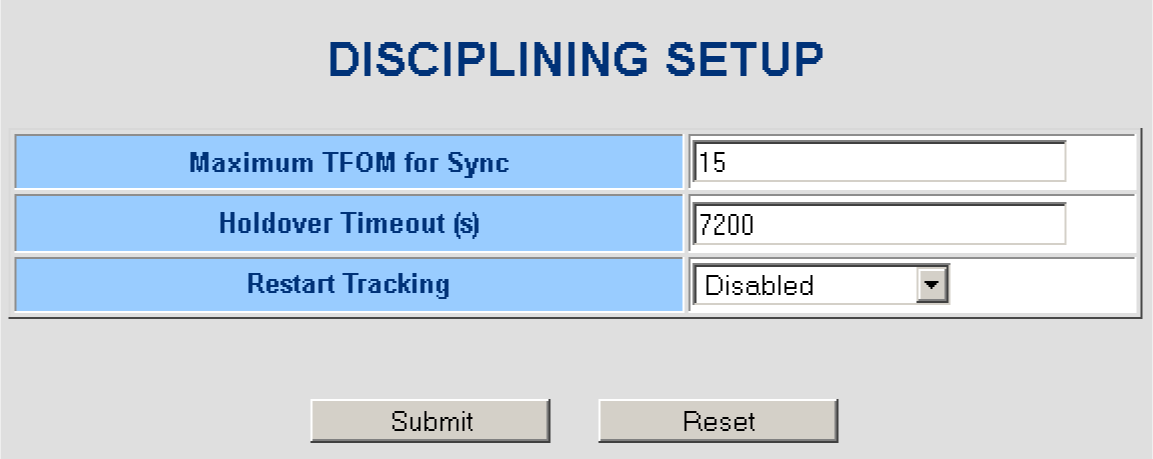
The Rubidium oscillator is atomic in nature but requires no MSDS (Material Safety Data Sheet).

10 MHZ Frequency Output:

Low phase noise Rubidium oscillator:	1x10^{-12} typical 24-hour average locked to GPS. 1x10^{-11} per day (5x10^{-11} per month) typical aging unlocked.
Rubidium oscillator:	1x10^{-12} typical 24-hour average locked to GPS. 1x10^{-11} per day (5x10^{-11} per month) typical aging unlocked.
High performance OCXO oscillator:	1x10^{-12} typical 24-hour average locked to GPS. 2x10^{-10} per day typical aging unlocked.
Standard OCXO oscillator:	2x10^{-12} typical 24-hour average locked to GPS. 1x10^{-9} per day typical aging unlocked.
TCXO oscillator:	1x10^{-11} typical 24-hour average locked to GPS. 1x10^{-8} per day typical aging unlocked.

The 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.

The **Setup / Disciplining** 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.



DISCIPLINING SETUP

Maximum TFOM for Sync: 15

Holdover Timeout (s): 7200

Restart Tracking: Disabled

Figure 3-11: Oscillator Disciplining

Maximum TFOM for Sync (Time Figure of Merit): Defines the largest TFOM value (TFOM is SecureSync's estimation of how accurately it is synchronized with its time and 1PPS reference inputs, based on several factors - known as the estimated time error or "ETE") that is allowed before disciplining is no longer performed on the oscillator. The larger the TFOM value, the less accurate SecureSync believes it is aligned with its 1PPS input that is used to perform disciplining. If this estimated error is too large, it could adversely affect the performance of oscillator disciplining. The available TFOM range is 1 through 15. You may refer to the following table (also available in Section 4.2) 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 usec
5	1 usec < ETE <= 10 usec
6	10 usec < ETE <= 100 usec
7	100 usec < ETE <= 1 msec
8	1 msec < ETE <= 10 msec
9	10 msec < ETE <= 100 msec
10	100 msec < ETE <= 1 sec
11	1 sec < ETE <= 10 sec

12	10 sec < ETE <= 100 sec
13	100 sec < ETE <= 1000 sec
14	1000 sec < ETE <= 10000 sec
15	ETE > 10000 sec

3.15 Holdover Mode

Holdover Timeout: The time interval between the loss of all valid 1PPS or Time input references and the moment that the SecureSync declares loss of time synchronization is known as the *Holdover Mode*. While the unit is in Holdover mode, the time outputs are derived from an internal oscillator incrementing the System Time.

The Holdover Timeout value can be managed from the **Setup / Disciplining** page.

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.

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.

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 “not synchronized” until at least one valid Time and 1PPS input reference becomes available again. While in this state, NTP will be Stratum 16 and outputs will not be useable. 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 “user” manually set time and SecureSync is subsequently rebooted or power cycled, time sync will be lost when it powers back-up. The time will need to be manually set by a user again in order for SecureSync to return to its fully synchronized state. Refer to Section *3.11.2* for more information on manually setting the time.

SecureSync has a user configurable variable holdover period so that it can be adjusted for personal requirements and desires. A user can change the length of time that SecureSync will operate in the Holdover mode before loss of time synchronization occurs (the factory default Holdover period is 2 hours). The estimated error rates for each oscillator type, after losing the input references, are listed in Table 3-2 (estimated rates are based on the oscillator being locked to a reference for 2 weeks and the ambient temperature remaining stable).

Oscillator Type	Typical Error Rates after 4 hrs	Typical Error Rates after 24 hrs
Low Phase noise Rb (Rubidium)	0.2 microseconds (nominal)	1 microseconds (nominal)
Rb (Rubidium)	0.2 microseconds (nominal)	1 microseconds (nominal)
High performance OCXO	0.5 microseconds (nominal)	10 microseconds (nominal)
Standard OCXO	1 microseconds (nominal)	25 microseconds (nominal)
TXCO	12 microseconds (nominal)	450 microseconds (nominal)

Table 3-2: Estimated Oscillator Error Rates during Holdover

If SecureSync is currently in time sync, the changes will take effect immediately. If the unit is in Holdover, the changes will not take effect until the next Holdover. To force the changes to take effect immediately, reboot the SecureSync.

The length of the allowed Holdover timeout period is displayed and configured in seconds. Table 3-3 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	86400
7 days	604,800
30 days	2,419,200
1 year	29,030,400

Table 3-3: Holdover value conversions

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).

Having a configured 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 **Setup / Time Management** page.

For more information on Leap Seconds, refer to Section *7.1*: “*Leap Second Occurrence*”.

Restart Tracking: This option can be configured from the **Setup / Disciplining** page and 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, in which case it will re-align the system 1PPS with the reference 1PPS very quickly but may cause the 1PPS output to jump.

3.16 System On-time Point, 1PPS / 10 MHz Frequency Output Generation and Configuration

The base Model of SecureSync includes one (1) 1PPS output and one (1) 10 MHZ output (additional 1PPS and 5 MHZ /10 MHz frequency outputs are available with option modules). To manage options for these outputs, navigate to the **Setup / Outputs** page and select **OUTPUTS: 1PPS/Frequency**.

The 10 MHz output is provided by the internal oscillator. With certain 1PPS input References being present and considered valid, the internal oscillator is disciplined to correct for oscillator drift (the oscillator cannot discipline to either NTP input or a user set time). If no 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 the SecureSync's on-time point (the on-time point is used 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, the 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 becomes available).

The 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:

TCXO/OCXO/Low Phase Noise Rubidium oscillator installed: 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 10,000,000 counts of the oscillator between each 1PPS output, even while in the Holdover mode (input references not currently available) and even after input references have become available again.

Rubidium (Rb) oscillator installed: 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 10,000,000 counts of the oscillator between each 1PPS output.

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 will momentarily not be exactly 10,000,000 counts . Once the reference transition has occurred, the counts between each 1PPS output will return to exactly 10,000,000 counts in between each output.

The 1PPS output can be configured to use Signature Control, to define the rising or falling edge of the 1PPS as the on-time point, the pulse width of the 1PPS can be defined and an offset can be entered to account for cable delays or other latencies. The 10 MHz output can be configured to use Signature Control as desired.

The available 1PPS output configurations are defined as follows:

Signature Control
Signature Control controls when the 1PPS output will be present.

Output Always Enabled: The 1PPS output is present, even when SecureSync is not synchronized to its references.

Output Enabled in Holdover: The 1PPS output is present unless SecureSync is not synchronized to its references (the 1PPS output is present while in the Holdover mode).

Output Disabled in Holdover: The 1PPS output is present unless the SecureSync references are considered not qualified and invalid. (the 1PPS output is not present while in the Holdover mode).

Output Always Disabled: The 1PPS output is not present, even if any SecureSync references are present and considered qualified.

Edge
Used to determine if the on-time point of the 1PPS output is the rising or falling edge of the signal.

Pulse Width
Configures the Pulse Width of the 1PPS output. The Pulse Width is entered and displayed in nanosecond (default Pulse Width is 200 milliseconds).

Offset
Displays the currently configured 1PPS Offset (accounts for cable delays and other latencies). The Offset is entered and displayed in nanoseconds.

Frequency Output
The 10 MHz (Frequency) output can be configured with Signature Control, as desired.

Output Always Enabled: The 10 MHz output is present, even when SecureSync is not synchronized to its references.

Output Enabled in Holdover: The 10 MHz output is present unless SecureSync is not synchronized to its references (the 10 MHz output is present while in the Holdover mode).

Output Disabled in Holdover: The 10 MHz output is present unless the SecureSync references are considered not qualified and invalid (the 10 MHz output is not present while in the Holdover mode).

Output Always Disabled: The 10 MHz output is not present, even if any SecureSync references are present and considered qualified.

3.17 Reference Priority Input Configuration

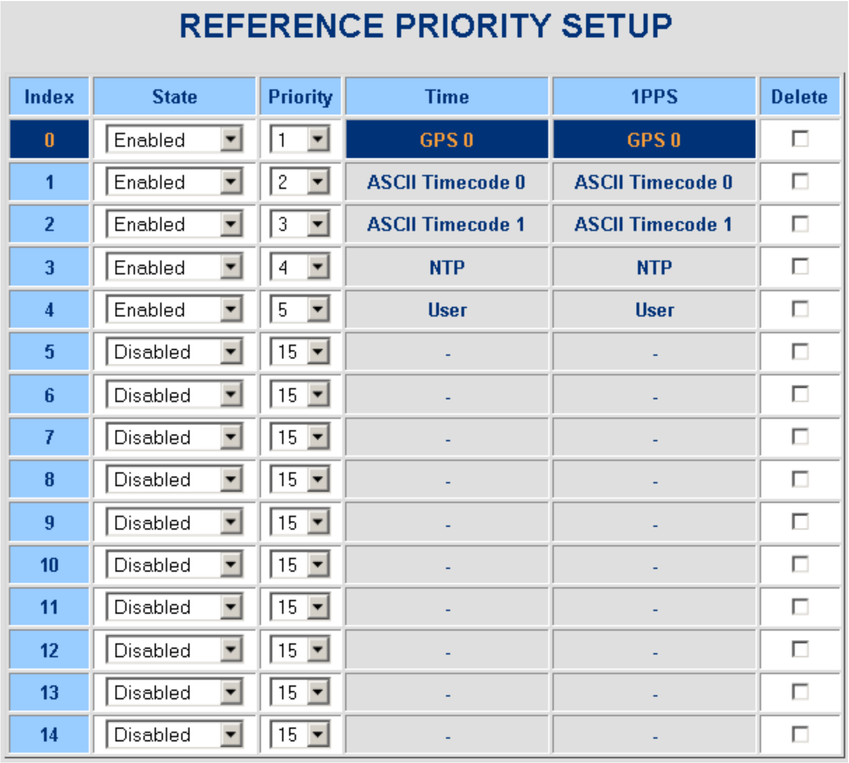
SecureSync can be synchronized by many different external time sources such as GNSS, IRIG input (IRIG input requires the IRIG Input/Output module be installed), 1PPS input, 10 MHz, HAVE QUICK (HAVE QUICK input requires the HAVE QUICK module be installed), PTP or another NTP server. Or, a user can enter the system time manually, which SecureSync can synchronize as the current time.

NOTE: If you are installing any new option module cards, you will need to either manually set up the desired card in the Reference Priority Table, or use the "**Reset to Defaults / Reset Table**" option on the **Reference Priority Setup** section in order to update the table with the new reference information.

In order for SecureSync to declare synchronization, it needs both valid 1PPS and valid time reference inputs. The Time and 1PPS references can be obtained from input references such as GNSS input, IRIG input, NTP input, 1PPS input or a user-set time.

Multiple references can be used to provide redundant inputs. The Reference Priority table allows multiple references to be defined in the order of priority desired. If the highest priority reference in available, it is selected. But if it's not available, the next lower priority reference will be selected, as long as it is available.

The Reference Priority Setup page (**Setup / Reference Priority**) options are used to define the priority order for the desired inputs.



REFERENCE PRIORITY SETUP

Index	State	Priority	Time	1PPS	Delete
0	Enabled	1	GPS 0	GPS 0	☐
1	Enabled	2	ASCII Timecode 0	ASCII Timecode 0	☐
2	Enabled	3	ASCII Timecode 1	ASCII Timecode 1	☐
3	Enabled	4	NTP	NTP	☐
4	Enabled	5	User	User	☐
5	Disabled	15	-	-	☐
6	Disabled	15	-	-	☐
7	Disabled	15	-	-	☐
8	Disabled	15	-	-	☐
9	Disabled	15	-	-	☐
10	Disabled	15	-	-	☐
11	Disabled	15	-	-	☐
12	Disabled	15	-	-	☐
13	Disabled	15	-	-	☐
14	Disabled	15	-	-	☐

Figure 3-12: Reference Priority Input Table

Each available type of available Time and 1PPS 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	External 1PPS input
Frequency	External Frequency input
GPS	GNSS input
PTP	PTP input
IRIG	IRIG timecode input
Local System	SecureSync’s built-in clock OR internal 1PPS generation
NTP	NTP input
User	Host (time is manually set by a user)
HAVEQUICK	HAVEQUICK input

Table 3-4: Reference Priority Input Names

NOTE: The number displayed indicates the number of feature inputs of that type presently installed in the SecureSync - starting with “0” representing the 1st 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:

Index: (Row number) Provide a sequential list of available references and their priority.

State: Enables or disables that Index (row) of the table.

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.

Delete: Removes the Index (row) from the Reference Priority table.

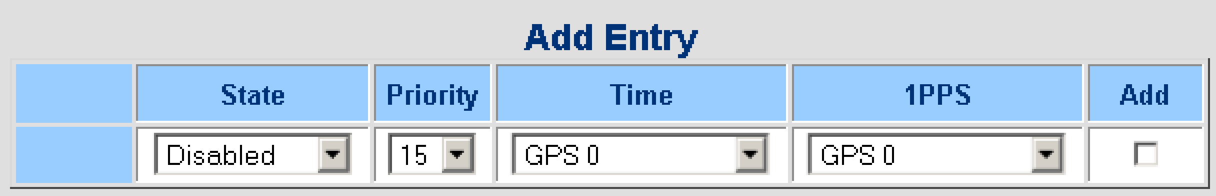
Battery Backed Time Synchronization

Below the Reference Priority Setup table is a "**Synchronize to Battery Backed Time on Startup**" enable option. Enabling this allows the system to write the battery backed time into the timing system for synchronization. This mechanism utilizes the "User" reference, so it requires an enabled "User" entry in the table.

NOTE: Synchronization accuracy and traceability are not specified when utilizing battery backed time.

Add Entry Table

The "Add Entry" table allows the Reference Priority Setup table to be customized with additional entries not included by default. The entries created in this table are appended into the Reference Priority Setup table as additional input references being available. This allows different combinations of references to be available as the reference Time and 1PPS inputs. To modify the entry table, select a value from any of the drop-down boxes.



Add Entry

	State	Priority	Time	1PPS	Add
	Disabled	15	GPS 0	GPS 0	□

Figure 3-13: Add Entry to Reference Priority Table

Reset Table: This option returns the Reference Priority Table to default configuration values.

Example: Desire the Ability to use "User Set Time" for the Input Time Reference, but want to use IRIG as the Input 1PPS Input:

1) From the Add Entry table, change the State option to "Enabled"
2) Set the Priority for this new Index (1-15 with the lower the number, the higher its priority as the input).
3) Set the Time field to "User" (this is the input Time reference).
4) Set the 1PPS field to "IRIG" (this is the input 1PPS reference).
5) Click the "Add" button.
6) Click "Submit".
7) Observe a new entry has been added to the Reference Priority Setup table. This new entry can be edited as desired directly in the Reference Priority table.

Reset to Defaults

The Reference Priority table can be reset to the factory default configuration by clicking on "Reset Table" box option and then pressing Submit.

Important Information Regarding "User" Input Reference (Manually Set Time):

The "User" reference input provides a "one-time-only" ability to use a manually set time as the system time. It requires manual intervention each time it is to be used (just having this "User" reference enabled does not automatically allow the current time to be considered valid and used as a reference). In order for the time to be considered valid, the user needs to "set" the time.

If a higher priority reference is enabled and the input reference goes away with no other external time references being available, the user needs to set the time manually in order for the SecureSync to continue to be synchronized. Or, if SecureSync is power cycled anytime thereafter, with no other references enabled or available, the time must be manually set to be considered valid, before being used to synchronize SecureSync.

For example, GNSS input is enabled and present, and configured as a higher priority than "User". If GNSS is then lost, in order for the time to remain synced, the user has to "set" the time manually. Having "User" enabled in the Reference table allows the ability for the user to set the time manually. If GNSS is restored and because GNSS is configured as a higher priority than the "User" (manually set time), GNSS will become the selected time reference. If GNSS goes away again, the user has to once again "set" the time manually again in order for the time to remain synchronized.

In this example, if GNSS reception is lost and if the time is not manually set by the user, and if no other references are available, SecureSync will go into the Holdover mode the moment GNSS is lost. If GNSS is not restored or the time is not manually set before the Holdover period expires, Time Sync is lost and the outputs may become unusable (the length of available Holdover is configured in the **Setup / Disciplining** page).

Also, if no other external references are available after a power cycle, the time needs to be manually set again in order for SecureSync to be synced unless battery backed time synchronization is enabled. After a power cycle, SecureSync cannot return to the Holdover mode until a reference is available and then all of those reference(s) are subsequently lost. After power-up SecureSync will remain in Time Sync alarm until either external references are restored or the time is manually set with "User" enabled in the Reference table.

NOTE: When using "User" with another higher priority reference (such as GNSS or IRIG) being enabled (so that it could become an available reference if it's declared valid), the System Time should be set as accurately as possible. If the input reference was to switch from "User" to another available reference (such as GNSS) and a large time correction was needed to be applied because the System Time error was too large, NTP will go out of sync.

If this time jump is excessive, (greater than 1000 seconds), NTP will exit synchronization and will not correct for the time jump until the NTP service is either stopped and then restarted or until SecureSync is rebooted. If the time difference between the "User" set time and the higher priority reference when its selected is less than 1000 seconds, NTP will remain in sync and will slew (over a period of time) to the new reference time.

Note: Selecting "Local System" as an Input Reference

"Local System" input reference is a unique input reference in that in can be used as either the Time input reference or the 1PPS input reference, but can never be both. It must be used in conjunction with another input reference (such as "GPS" or "IRIG" for example).

When the Time reference is configured as "Local System" (with the 1PPS reference configured as a different input reference), the Time that SecureSync powers up with is considered valid time, as long as the 1PPS input reference is valid.

When 1PPS reference is configured as “Local System” (with the Time reference configured as a different input reference), the SecureSync’s internal 1PPS will be used as a valid 1PPS input reference as long as the Time reference is valid.

3.17.1 Reference Priority Input USE CASE Examples:

Example 1 (GNSS as primary references, IRIG as backup):
It is desired to have GNSS as the primary time and 1PPS reference with IRIG input being the backup time and 1PPS time reference. For this configuration the Index row which has “GPS 0” in both the Time and 1PPS columns would be set to the “Enabled” state with a Priority value of “1”. Then the Index row which has “IRIG 0” in the Time and 1PPS columns would be set to the “Enabled” state with a Priority value of “2”. All other Index rows should be set to “Disabled”. Since these are both default Indexes, no additional entries need to be added to the Reference table.

Example 2 (IRIG as Primary Reference, NTP Input as Backup):
It may be desired to have IRIG as the primary reference input but to be able to have another NTP server be the backup reference in case the IRIG input is lost. For this configuration the Index row which has “IRIG 0” in both the Time and 1PPS columns would be set to the Enabled state with a Priority value of “1”. Then the Index row which has “NTP” in both the Time and 1PPS columns would be set to the “Enabled” state with a Priority value of “2”. All other Index rows should be set to “Disabled”. Since these are both default Indexes, no additional entries need to be added to the Reference table.

Example 3 (NTP Input as Only Available Input, also Referred to as “NTP Stratum 2 Synchronization”):
It may be desired to have NTP (provided by another NTP server) as the only available reference input. For this configuration, the Index row which has “NTP” in both the Time and 1PPS columns would be set to the “Enabled” state with a Priority value of “1”. All other Index rows should be set to “Disabled”.

Important Note: 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 (User Desires to Manually Set the Time. Other References may or may not be Available):
In order for a manually set time to be considered valid and used to synchronize SecureSync, user needs to be enabled in the Reference Priority table. The Index row which has “user” in both the Time and 1PPS columns should be set to the “Enabled” state. If no other references are connected, the Priority value should be set to “1” and all other Index rows should be set to “Disabled”.

If it is desired to use manually set time as a backup to other references (such as GNSS or IRIG), the appropriate Index rows for those desired references should be set to “Enabled” and the Index row which has “user” in both the Time and 1PPS columns should be set to a lower priority than the other references.

With "user" enabled, if no other higher priority references are enabled or available (or if the higher priority references have since been lost), simply set the System time to the desired value. SecureSync will go into synchronization using this set time. The time can be manually set in the "**Set Manual Date/Time**" table located in the **Setup / Time Management** page. Set the desired date/time and then click Submit. The front panel sync light will turn green.

NOTE: This process needs to be repeated each time SecureSync is power cycled (with no other references available) unless "**Synchronize to Battery Backed Time on Startup**" is enabled or after each time all higher priority references are lost.

Example 5 (User Desires to use the time that SecureSync Powers up with as the Valid Time. The 1PPS Input Reference will be Derived from GNSS Input):

It may be desired to just use the time that SecureSync powers up with (without the need for a user to manually set it, as would be done with "User" selected). This is referred to as "Local System". Because "Local System" can't be both Time and 1PPS input together, GNSS will be the 1PPS reference input.

Because there is no default Index for "Local System" and "GPS", a new Entry needs to be added to the Reference table in order to use this combination of references. In the Add Entry table (below the Reference Priority table), Change the State to "Enabled", set the Priority to 1 (for this to be the highest level priority), change Time field to "Local System" and change the 1PPS field to "GPS". Select the **Add** box and click "Submit".

A new Index will now be added to the Reference Priority table that has "Local System" as the Time input and GNSS as the 1PPS input. After a power cycle or reboot, as soon as GNSS is declared valid, the System Time will be automatically be used as-is with no manual intervention being required.

3.18 Configuring NTP

3.18.1 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 (**Setup / Time Management** page). 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.

Important Note: 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 September 2013, the offset between UTC and GPS time is 16 seconds.

If it is desired to change the NTP timescale from one value to another, either NTP should be "Disabled" and then "Enabled" after this change has been made, or SecureSync should be rebooted/power cycled to have this timescale change take effect.

NTP settings can be configured from the **Network / NTP Setup** page.

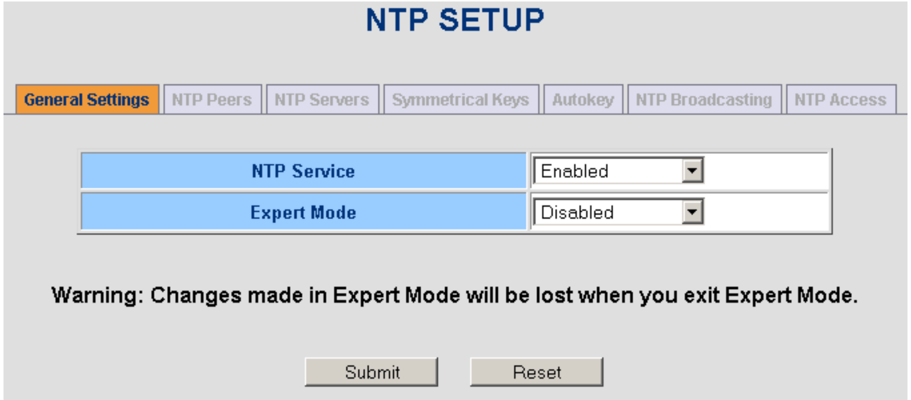
Important Note: Configuration changes made to SecureSync's NTP configurations do not take effect until the NTP Service is Disabled and then Enabled (or until SecureSync is rebooted/power cycled). The NTP service can be stopped and started from the **Network / NTP Setup** page → **General Settings** tab. Once NTP has been re-enabled, NTP will be available again for network synchronization within a few minutes.

Typically, the factory default configurations of the NTP settings do not need to be modified for NTP operation. However, NTP has configurations available that allow the normal operation of NTP to be altered for unique applications. These features include the ability to use either MD5 authentication or NTP Autokey, to block NTP access to parts of the network or to broadcast NTP data to the network's broadcast address.

The **Network / NTP Setup** page allows the NTP Service to be enabled and disabled, 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). Refer to Figure 3-14.

3.18.2 General Settings Tab

The **General Settings tab** provides the ability to either stop (Disable) or start (Enable) the NTP daemon. After changing any 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.



NTP SETUP

NTP Service	Enabled
Expert Mode	Disabled

Warning: Changes made in Expert Mode will be lost when you exit Expert Mode.

Figure 3-14: NTP Setup page

The user can either enable or completely disable the NTP Service. When disabled, no NTP time packets will be sent out to the network. 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.

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 7,000 NTP requests per second without MD5 authentication enabled (and a somewhat lower rate with MD5 authentication enabled).

The General Settings tab also offers an "**Expert Mode**" for NTP configuration. 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.

Important Note: The Expert Mode should only be used by those individuals that are extremely familiar with NTP operation, including the `NTP.conf` file settings. Incorrectly altering the `NTP.conf` file can cause NTP to stop working (if NTP is configured as an input reference, SecureSync could lose synchronization).

Important Note: 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/.

Important Note: 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 or editing the file back to the original configuration as shown in the factory default configuration below. Refer to Section *3.6* for more information on restoring all SecureSync configurations back to factory default settings.

Important Note: 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 -4 default noquery nomodify
restrict -6 default noquery nomodify
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
server 127.127.45.0 prefer minpoll 4
enable pps
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
server 127.127.1.0 minpoll 4
fudge 127.127.1.0 stratum 15
keysdir /etc/ntp/keys/
driftfile /etc/ntp/ntp.drift
logfile /home/spectracom/log/ntp.log
statsdir /home/spectracom/log/ntpstats/
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 "**General Settings**" and "**Expert Mode**" tabs remain visible while in Expert Mode (all other tabs will no longer be present). Disabling the Expert mode restores these tabs to this page of the SecureSync web interface.

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

1) Enable the "Expert Mode" in the **General Settings** tab.
2) Click on the "Expert Mode" tab.
3) Edit the file as desired.
4) After editing this file, click "Submit" to save any changes that were made.
5) From the **Network / NTP Setup** page → **General Settings** tab, first disable and then re-enable the NTP Service to start using the new NTP configuration per the edited file.

3.18.3 Configuring NTP Peers and NTP Servers (Stratum Synchronization)

SecureSync can be configured to receive time from one or more available NTP servers (such as other SecureSyncs, or Spectracom Model 9300 series NTP servers). The other NTP servers can then be a valid input reference for System Time synchronization. This is commonly referred to as NTP Peering.

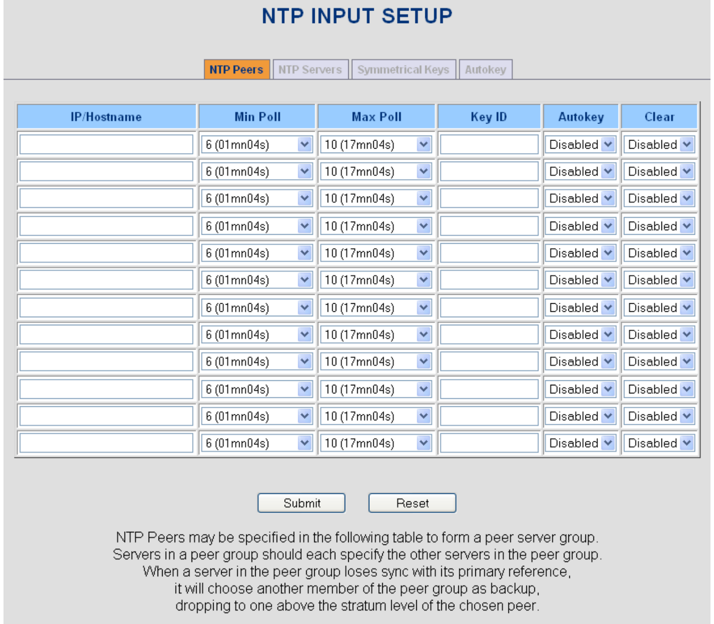
When SecureSync is configured to obtain time from other NTP servers at the same Stratum level (configured as NTP Peers) but is currently using another input reference other than the NTP server(s) as its selected reference, SecureSync will report to the network (in the NTP time stamps) that it is a Stratum 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 Section *3.17*.

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 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 16. Stratum 16 will cause the network to ignore SecureSync as an NTP time reference. Refer to Section *3.15* for information on obtaining or configuring the allowable Holdover period.

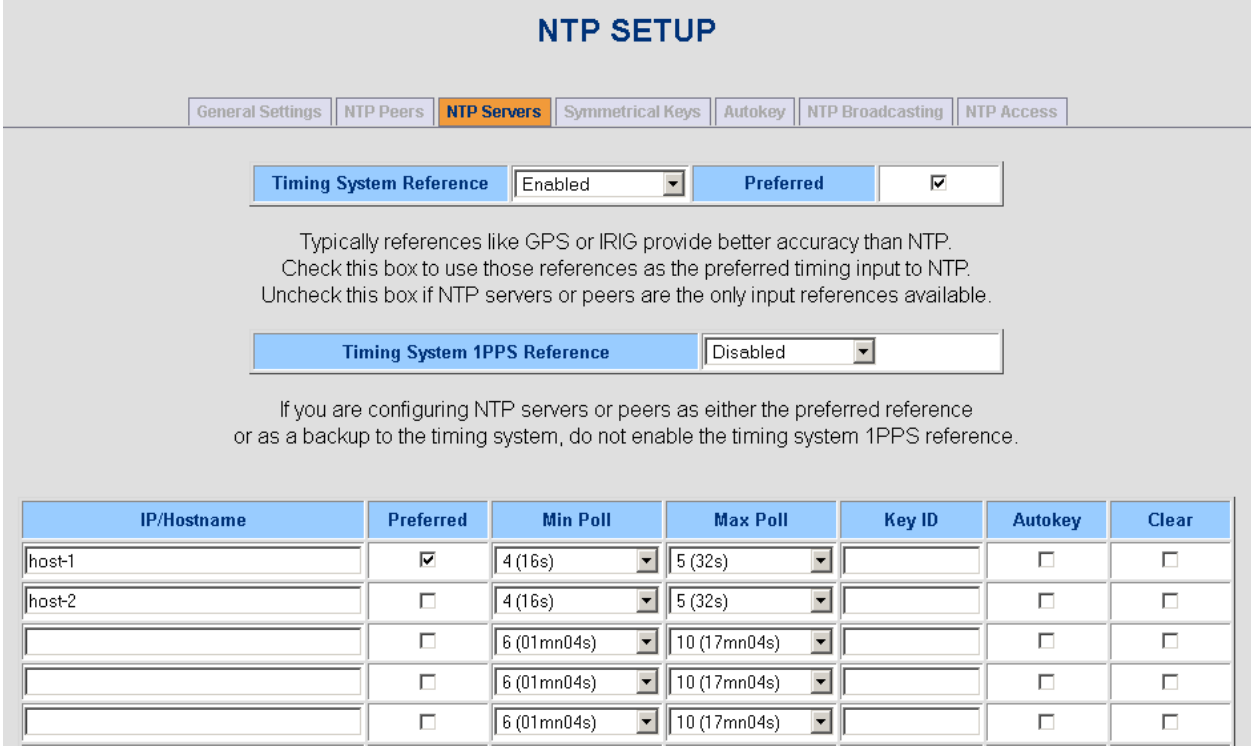
The **NTP Peers** and **NTP Servers** tabs located on the **Network / NTP** page allow NTP to be configured with external NTP reference inputs.



IP/Hostname	Min Poll	Max Poll	Key ID	Autokey	Clear
	6 (01mn04s)	10 (17mn04s)		Disabled	Disabled
	6 (01mn04s)	10 (17mn04s)		Disabled	Disabled
	6 (01mn04s)	10 (17mn04s)		Disabled	Disabled
	6 (01mn04s)	10 (17mn04s)		Disabled	Disabled
	6 (01mn04s)	10 (17mn04s)		Disabled	Disabled
	6 (01mn04s)	10 (17mn04s)		Disabled	Disabled
	6 (01mn04s)	10 (17mn04s)		Disabled	Disabled
	6 (01mn04s)	10 (17mn04s)		Disabled	Disabled
	6 (01mn04s)	10 (17mn04s)		Disabled	Disabled
	6 (01mn04s)	10 (17mn04s)		Disabled	Disabled
	6 (01mn04s)	10 (17mn04s)		Disabled	Disabled
	6 (01mn04s)	10 (17mn04s)		Disabled	Disabled

NTP Peers may be specified in the following table to form a peer server group.
Servers in a peer group should each specify the other servers in the peer group.
When a server in the peer group loses sync with its primary reference,
it will choose another member of the peer group as backup,
dropping to one above the stratum level of the chosen peer.

Figure 3-15: Configuring NTP Peers



Timing System Reference	Enabled	Preferred	☑

Typically references like GPS or IRIG provide better accuracy than NTP.
Check this box to use those references as the preferred timing input to NTP.
Uncheck this box if NTP servers or peers are the only input references available.

Timing System 1PPS Reference	Disabled

If you are configuring NTP servers or peers as either the preferred reference
or as a backup to the timing system, do not enable the timing system 1PPS reference.

IP/Hostname	Preferred	Min Poll	Max Poll	Key ID	Autokey	Clear
host-1	☑	4 (16s)	5 (32s)		□	□
host-2	□	4 (16s)	5 (32s)		□	□
	□	6 (01mn04s)	10 (17mn04s)		□	□
	□	6 (01mn04s)	10 (17mn04s)		□	□
	□	6 (01mn04s)	10 (17mn04s)		□	□

Figure 3-16: Configuring NTP Servers

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 can be used to synchronize the 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.

NTP Peers and NTP Servers Tabs

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).

> **Important 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 (Refer to Section *3.17*).

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 looses all reference clocks or fails, the other peers continue to provide time to other clients on the network.

Timing System Reference Preferred and **Enable Timing System 1PPS Reference Options:** 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 "Preferred". Typically, only one NTP server in the table should be selected as "Preferred" (and should only be selected if the "Prefer Timing System Reference: box 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).

Key ID: If you want to use MD5 authentication with the configured NTP server, enter the desired MD authentication Key ID number (from the **Network / NTP Setup** page, "Symmetrical Keys" tab). MD5 authentication will occur when SecureSync obtains time from the listed server.

The **Min Poll** and **Max Poll** options in the NTP References grids allow the user to choose, from within the available ranges, how often the SecureSync will poll the defined servers for timing information. Check with your network administrator for guidelines regarding network traffic and recommended polling intervals, if any.

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 **Network / NTP Setup** page → **General Settings** tab. 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.

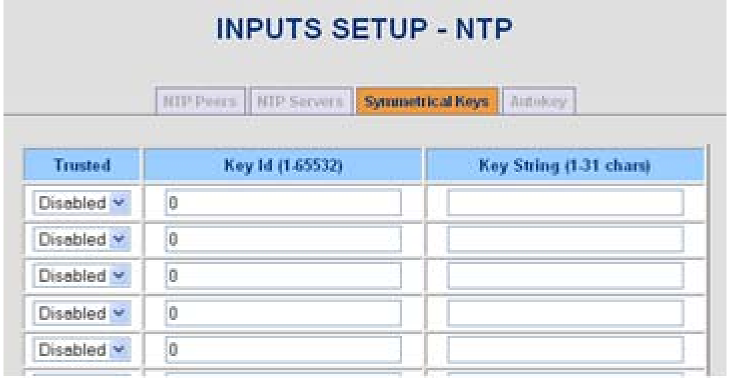
If the SecureSync has no valid Timing System Reference, NTP Server or NTP Peers, the NTP Stratum value is automatically increased to Stratum 15. This ensures no NTP clients can use it as a time reference when unsynchronized. This feature utilizes automatic enabling and disabling of the Local Clock Reference 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.

3.18.4 Symmetrical 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 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. The key ID must be a number between 1 and 65532; the key string must be readable ASCII and between 1 and 16 characters long. Duplicate key IDs are not permitted. NTP requests received by SecureSync 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. NTP requests with valid authenticator result in a valid NTP response with its own valid authenticator using the same Key ID provided in the NTP request.

From the Symmetrical Keys screen (Figure 3-17), the user may define the trusted symmetrical keys that must be entered on both the SecureSync and any network client with which the 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.



Trusted	Key Id (1-65532)	Key String (1-31 chars)
Disabled	0	
Disabled	0	
Disabled	0	
Disabled	0	
Disabled	0	

Figure 3-17: NTP Symmetrical Keys (MD5) 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 stopped and restarted from the **Network / NTP Setup** page → **General Settings** tab. 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.

3.18.5 NTP Autokey

3.18.5.1 Overview

The SecureSync provides an NTP version 4.2.6p5 which supports the Autokey Protocol. The Autokey Protocol uses the OpenSSL library which provides security capabilities including message digests, digital signatures and encryption schemes. The Autokey Protocol provides a means for NTP to authenticate and establish a chain of trusted NTP servers.

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

3.18.5.3 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 closes 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.

A 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.

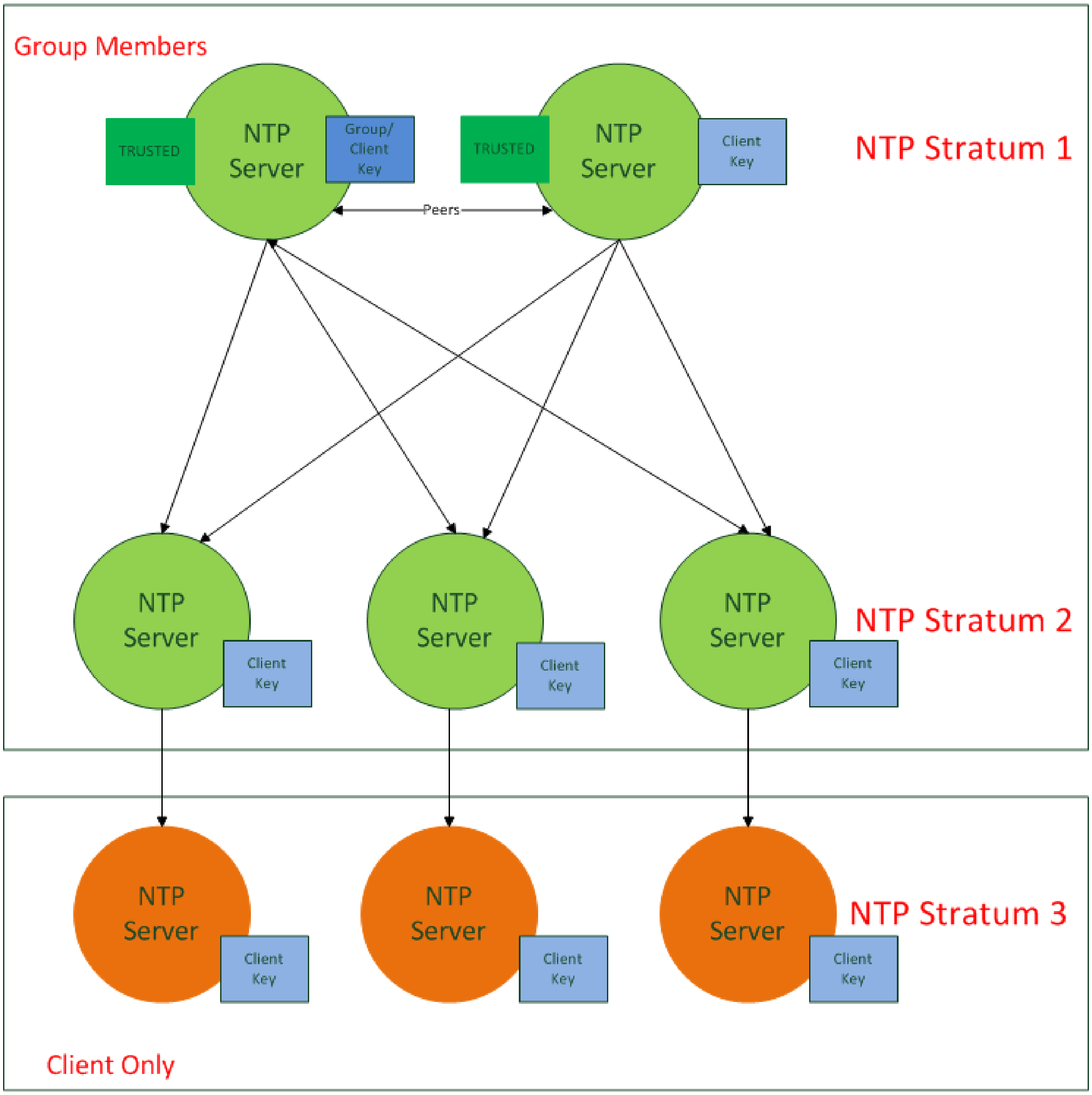


Figure 3-18: IFF Autokey Configuration Example

Configuring NTP Autokey
Use the following instructions to configure each type of NTP Server shown above.

Create a NTP Stratum 1 Trusted Host with IFF Group/Client Key
The steps to configure a NTP Stratum 1 Server acting a Trusted Host with an IFF Group/Client key are shown below.

1. Define Hostname of all NTP servers before proceeding.
2. Disable NTP.

Ensure the time is accurate to a few seconds. Use NTP or handset the clocks to set the system time.

3. Verify all NTP Stratum 1 SecureSync are in Time/1PPS Sync.
4. Enable Autokey selecting the following options on the Autokey tab
    a. Autokey Service Enabled
    b. Passphrase - <your NTP server's password>
    c. Do NOT enable Client only.
    d. Enable Trusted
    e. Select under the Autokey Group Key pull-down the option "Generate"
5. Observe the IFF Group/Client Key appearing with the selection "Keep Current Group Key" enabled.
    a. 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 Autokey under the NTP Access tab.
7. Enable NTP under the General Settings tab.
8. Verify NTP reaches occur and NTP eventually reaches Stratum 1.

Create a NTP Stratum 1 Group Member Server with a Client Key

The steps to configure a NTP Stratum N Server which is a Group Member using a Client key are detailed below.

1. Define the Hostname, making sure it is not the same as the trusted root server.
2. Disable NTP if enabled.
3. Handset the time or use NTP to set the system time.
4. Enable Autokey selecting the following options on the Autokey tab
    a. Autokey Service Enabled
    b. Passphrase - < your Group members NTP Autokey password >
    c. Do NOT enable Client only
5. Using the NTP Server containing the IFF Group/Common Key generate a Client Key using this NTP Server's passphrase.
6. Under the Auto Group Key selection choose "Upload" and cut and paste this exported key into the text box.
7. For all NTP Stratum 2 servers and higher stratum numbers disable the following items on the NTP Server tab and configure NTP Stratum 1 references.
    a. Disable "Prefer Timing System Reference"
    b. Disable "Enable Timing System 1PPS Reference"
    c. Add an IP/Hostname of NTP servers.
    d. Enable the Autokey option box.
8. Enable NTP on the General Settings tab.
9. Wait for NTP to synchronize to the NTP References provided.

Create a 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.
2. Disable NTP if enabled.
3. Handset the time or use NTP to set the system time.
4. Enable Autokey selecting the following options on the Autokey tab.
    a. Autokey Service Enabled
    b. Passphrase - <your client's NTP Autokey password>
    c. You must select to enable Client only.

5. Using the NTP Server containing the IFF Group/Client Key, copy the Group/Client key.
6. Under the Auto Group Key selection choose "Upload" and cut and paste this copied key into the text box.
7. For all NTP Stratum 2 servers and higher stratum numbers disable the following items on the NTP Server tab and configure NTP Stratum 1 references.
    a. Disable "Prefer Timing System Reference"
    b. Disable "Enable Timing System 1PPS Reference"
    c. Add an IP/Hostname of NTP servers.
    d. Enable the Autokey option box.
8. Enable NTP on the General Settings tab.
9. Wait for NTP to synchronize to the NTP References provided.

3.18.6 NTP Broadcasting Tab

The **NTP Broadcasting** tab allows NTP service to be configured to broadcast the NTP time to the network's broadcast address at scheduled intervals. 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).

If desired to broadcast NTP time packets to the network, select "Enable" for "NTP Broadcast Service" drop-down to enable broadcast mode and select an interval at which to broadcast from the dropdown box. The NTP Broadcast mode is intended for one or a few servers and many clients. NTP broadcast mode can utilize MD5 authentication. Select a single trusted MD5 key to use for broadcast from the pull-down menu. Use of MD5 authentication requires that MD5 symmetrical keys already be defined on the NTP Symmetrical Keys page.

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. The broadcast intervals available are included in the "**Interval**" dropdown menu.

When using MD5 authentication in broadcast mode, one MD5 key ID Number needs to be selected from the Symmetrical Keys table (**Symmetrical keys** tab) to be sent with the NTP broadcast message. This MD5 key to be used with the NTP broadcast is identified by the Key ID number and entered into the **Key ID** field.

3.18.7 NTP Access Tab

The **NTP Access** tab allows the user to enable or disable all IPv4 and IPv6 requests, as well as to ability allow or deny users or network segments. Selecting "Enabled" in the "Auth Only" drop-down box on each line where a user or network segment is defined will prompt the SecureSync to accept only authenticated requests (MD5 or Autokey) from this user or network segment.

When the "Service all IPv4 requests…" and the "Service all IPv6 requests…" boxes are Enabled, SecureSync will respond to all NTP requests. You may also specify options on a per client basis. Instead of providing blanket access, you may either specify which IP Addresses or hostnames have access to NTP, or you can restrict NTP access to certain IP addresses or hostnames.

To limit NTP access to SecureSync, first change both of the "Service all IPv4 and IPV6 requests" to "Disabled". Then in the NTP Access table, change the "Type" drop-down to either "Allow," or to "Deny." Enter the appropriate hostname and IP Mask. If you wish for the additional security of authorized access, enable "Auth Only." 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.

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.

If you would like to allow any NTPDC or NTPQ client access over IPv4, enable “Allow Queries from NTPDC or NTPQ over IPv4.” If you would like this for IPv6 NTPDC or NTPQ, enable “Allow queries from NTPDC or NTPQ.”

To require all requests for NTPDC or NTPQ to be allowed over IPv4 or IPv6, enable “Allow Queries from NTPDC or NTPQ over IPv4” or “Allow queries from NTPDC or NTPQ over IPv6.”

3.18.8 NTP Support

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 good source for support is the Internet newsgroup at news://comp.protocols.time.ntp.

Spectracom can provide support for Windows NT, Windows 2000, Windows XP, Windows Vista, Windows Server 2003/2008, and Windows 7 time synchronization. Refer to www.spectracomcorp.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 the PresenTense software, please visit www.spectracomcorp.com or contact our Sales department.

3.19 Configuring GNSS Input

When connected to a GNSS antenna that can receive a GNSS signal, SecureSync can use GNSS as one of its selected references. 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 the 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 GNSS receiver's configuration can be accessed via the **Setup / Inputs** page.

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 available selections are detailed herein:

Standard: This mode should always be selected if the GNSS receiver will remain stationary at all times and will be able to track at last four satellites at all times. In this mode, a GNSS survey, taking about 33 minutes, 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 Sync. Also, the GNSS receiver will lock-in the calculated GNSS position and will enter the "Stationary" mode. Once in Stationary mode, the GNSS survey will only be performed again if the equipment is then 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 return to the 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 from that point forward.

"Mobile": This mode should only be selected if the SecureSync will not remain stationary at all times (instead of SecureSync being installed in a building, it is instead installed in a mobile platform (such as a vehicle, ship, plane, etc). In this mode, the GNSS survey is not performed. SecureSync will go into synchronization shortly after tracking satellites.

NOTE: With the GNSS Receiver configured in "Continuous" (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 50ns to GPS/UTC (1 sigma), so mobile mode is less than 150ns to GPS/UTC time (1 sigma).

"1 satellite" (also known as the "Single Satellite mode"): This mode should only be used if the GNSS receiver will remain stationary at all times and it is impossible for the GNSS receiver to track at least four GNSS satellites for at least 33 minutes continuously (in order to complete the GNSS survey) and the current latitude and longitude is not known. As the GNSS receiver is designed to provide the best timing in the Stationary mode (stationary mode can only be achieved if the GNSS Survey can be completed or the location is manually entered) while tracking at least four satellites, “Single Satellite” mode should only be used if the GNSS survey cannot be completed and the current latitude and longitude are not known (and therefore, can’t be manually entered by a user).

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 one qualified satellite from that point forward.

The “**Offset**” option allows a user 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 (also known as “antenna cable delay”), the system’s on-time point can be offset 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

The **Position Clear** option allows the user to delete the SecureSync’s GNSS position and restart the GNSS Self Survey on command. To ensure that no trace of position data remains on the unit, perform the following steps:

- Disconnect the SecureSync’s GNSS antenna.
- Change the **Position Clear** value to “Enabled”.
- Click the “Submit” button. The SecureSync will initiate a GNSS self-survey.

NOTE: You cannot delete position and restart the GNSS Self Survey when in the "Continue" (mobile) Receiver mode. This option is for use with "Standard" and "1 Satellite" Receiver modes ONLY.

The **Constellation Selection** option allows the user to select which GNSS constellations are used. This setting appears only when SecureSync is equipped with a Multi-GNSS receiver. In addition, the selection of constellations other than GNSS requires the Multi-GNSS option to be installed on the product.

3.19.1 Manual Position Setup Table

This table allows the current latitude, longitude and antenna height to be either viewed or manually entered. While in the Stationary mode of operation, the GNSS Survey is the best method for the GNSS receiver to accurately and automatically calculate the latitude, longitude and antenna height values.

However, if the GNSS survey cannot be completed because less than four GNSS satellites can be received, manually entering a fairly accurate location into the GNSS receiver can also place it into the "Stationary" mode of operation, thereby increasing the accuracy of the GNSS receiver. Use this table to enter the current latitude and longitude if required.

The location input by the user may only help to speed up the time to the first fix during the initial installation. The unit will automatically check the status of the GNSS receiver after receiving the location input from the user. Based on the status of the GNSS receiver, the unit will either tell the user that the GNSS receiver already has finished the first fix and the input was abandoned, or send the location to the GNSS receiver.

3.20 Configuring SNMP and Notifications

3.20.1 SNMP

SNMP (Simple Network Management Protocol) is a set of standards for managing network devices, which includes a protocol, a database structure specification, and a set of data objects. The communication protocol involves one or more network management stations monitoring one or more network devices. SNMP enabled devices must have an SNMP agent application that is capable of handling network management functions requested by a network manager. The agent is also responsible for controlling the database of control variables defined in the product's Management Information Base (MIB).

SecureSync's SNMP functionality supports SNMP versions V1, V2c and v3 (with SNMP version 3 being a secure SNMP protocol).

SNMP is configured in the **Network / SNMP Setup** page. This page consists of four tabs:

3.20.1.1 General Settings Tab

The following options are configurable from this tab:

The **SNMP Service** option allows SNMP to be either Enabled or Disabled. When disabled, the SNMP port is closed and no SNMP functionality will be available.

When enabled, the **Authentication Error Trap** will send an SNMP trap each time a user tries to access SNMP, but the attempt fails (wrong community name is used, for example).

sysObjectID, sysContact, and **sysLocation** are SNMP options (default SNMP values will be displayed initially, but the values are configurable by the administrator).

3.20.1.2 Communities (v1/v2) Tab

This tab 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.

3.20.1.3 Users (v3) Tab

This tab allows configuration of SNMP v3 functionality, including the user name, read/write permissions, authorization passwords as well as privilege Types and Passphrases.

NOTE: User names are arbitrary. The user name must be the same on SecureSync and on the management station. SNMP user names and passwords are independent of users that are configured on the **Tools / Users** page.

3.20.1.4 Notifications (Traps) Tab

This tab 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 and Managers in other areas also receive.

Each row of the notifications page includes the version of the SNMP functionality, the User/Community name for the trap, the IP address/Hostname of the SNMP Manager (and whether the address is IP4 or IPv6), as well as values applicable only to SNMP v3 which include the Engine ID, the Authorization Type/password, the Privilege Type, and the password.

NOTE: When selecting an engine ID for SNMPv3, pick an arbitrary hexadecimal number (such as 0x1234).

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

For detailed descriptions of the objects and traps supported by the SecureSync, please refer to the Spectracom SecureSync MIB files, discussed in Section 3.20.3.

3.20.2 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 a “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 the 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 *Section 11:* for command details.

3.20.3 SNMP Support

Spectracom’s private enterprise MIB files can be requested and obtained from the Spectracom Customer Service department via email. They can also be obtained 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, using an FTP program, log in as an administrator. The Spectracom MIB files are located in the **`/home/spectracom/mibs`** directory. FTP the files to the desired location on your PC for later transfer to the SNMP Manager. The MIB files may then be compiled 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 name 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.

3.20.4 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 **Tools / Notification** 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 (note that only one email address can be specified in each "**Email Address**" field). Each event can be configured with the desired email address that is specific to just that one event only. If desired, the same email address can be used in all of the fields, or different addresses can be used for different events.

All available SecureSync events that can generate a notification to be sent are located in different tabs in the **Notification Setup** table, including **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.

NOTE: Whether or not notifications are enabled / disabled for a given event, the occurrence of the event is always logged.

The types of events in each tab are as follows:

Timing: This tab contains events for Sync Status and Holdover, Frequency error, Input references and the internal oscillator.

GPS: Contains events related to the GNSS receiver, including antenna cabling, tracking less than the minimum number of satellites and GNSS receiver faults.

System: This tab contains events related to the system operation, including minor and major alarms being asserted, reboot, timing system errors and option cards.

The **Thresholds** tab 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 asserted (the alarm is asserted when the receiver falls below the minimum number specified).

The "Duration below threshold" 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.

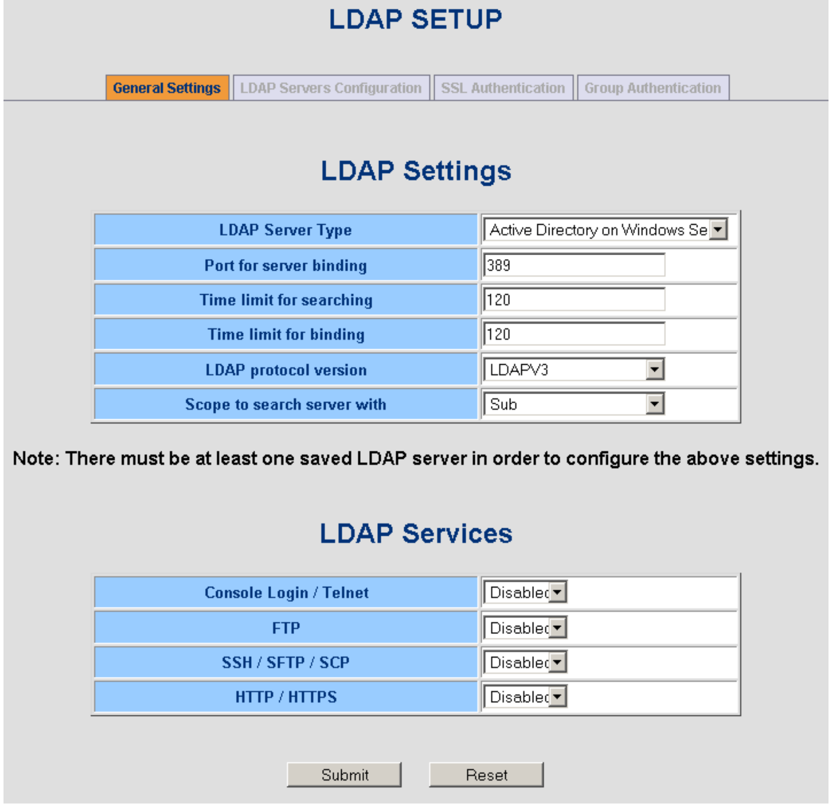
The **Email Setup** tab provides the means to configure SecureSync with the necessary settings to interface it with Exchange email servers and Gmail. The "Email Configuration" box in this tab provides two example configuration files. One is for interfacing SecureSync with an Email Exchange server and the other is for sending emails via Gmail. 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).

3.21 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.

The **Network / LDAP Setup** page (refer to Figure 3-19) provides the LDAP configuration options for SecureSync. The user may define the LDAP server type (this must be the correct – check with your LDAP server administrator if you are not sure) and also choose the types of services allowed to request authentication from the LDAP server.



LDAP Settings

LDAP Server Type	Active Directory on Windows Se
Port for server binding	389
Time limit for searching	120
Time limit for binding	120
LDAP protocol version	LDAPV3
Scope to search server with	Sub

Note: There must be at least one saved LDAP server in order to configure the above settings.

LDAP Services

Console Login / Telnet	Disablec
FTP	Disablec
SSH / SFTP / SCP	Disablec
HTTP / HTTPS	Disablec

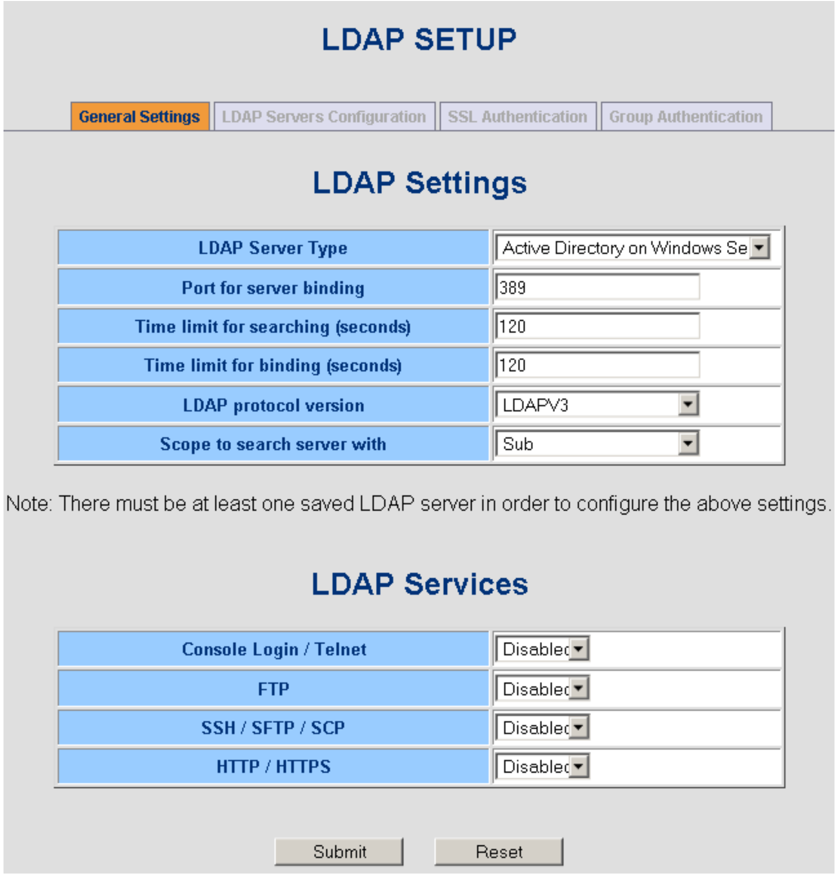
Figure 3-19: Security LDAP Client Configuration Screen (1 of 2)

The LDAP screen contains four tabs. These tabs are "General Settings", "OpenLDAP on Linux/Unix", "SSL Authentication" and "Group Authentication".

The "**General Settings"** tab provides the ability to enable or disable LDAP operation and configures SecureSync with the type of LDAP service(s) to be used. It also provides the means to define which login services will use LDAP authentication (such as Telnet, FTP, SSH/SFTP/SCP and HTTP/HTTPS). Refer to the LDAP Setup figure below.

Notice: We highly recommend enabling LDAP with only ONE listed service to begin (**Security / LDAP General** page), until it has been confirmed that your LDAP configuration is correct. It is recommended that you leave HTTP/HTTPS unchecked, and instead enable any of the other services (such as FTP).

Once you can confirm that you can perform this connection method (such as creating an FTP session), then you can go back in and enable the other services as desired. We always recommend holding off on enabling the HTTPS box so that you don't get locked out of the web interface because one or more of the attributes were not initially entered correctly.



LDAP SETUP

LDAP Settings

LDAP Server Type	Active Directory on Windows Se
Port for server binding	389
Time limit for searching (seconds)	120
Time limit for binding (seconds)	120
LDAP protocol version	LDAPV3
Scope to search server with	Sub

Note: There must be at least one saved LDAP server in order to configure the above settings.

LDAP Services

Console Login / Telnet	Disablec
FTP	Disablec
SSH / SFTP / SCP	Disablec
HTTP / HTTPS	Disablec

Figure 3-20: Open LDAP on Linux/Unix tab

The "**Open LDAP on Linux/Unix**" tab allows the user to specify the addresses or hostnames of the LDAP server(s) and inputs other fields that must be provided by the

LDAP server administrator. One of the servers (and one only) must be defined as the main LDAP server. The other servers are replicas. Refer to Figure 3-20.

Besides creating the user account, the criteria for the LDAP server needs to be defined in SecureSync. These values are specific to your LDAP server. The following section contains descriptions of the configurable LDAP attributes along with example configurations:

Distinguished name of the search base (known as DN): This is the base name to use in the database search. Typically, this is the top-level of the directory tree structure.

Distinguished Name to bind server with (known as Bind DN): The bind DN is the user on the external LDAP server 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 and search base for the DN (distinguished name) for authenticating users. When the DN is returned, the DN and password are used to authenticate the user. Enter The DN to use 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.

Credential to bind server with: Either the necessary password to bind with the LDAP Server or leave this field empty for anonymous simple authentication.

Login attribute used for search: A string of data that provides additional filter (UID) information.

Search base for password: Helps the LDAP Server determine the starting point in the directory tree to start searching for the password. Think of the search base as the "top" of the directory for your LDAP users, although it may not always be the top of the directory itself. The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.

A example configuration for an OpenLDAP server would be as follows:

DN for search base	`dc=spectracomcorp,dc=com`
Bind DN	`cn=manager,dc=spectracomcorp,dc=com`
Bind password	`test`
Search filter	`objectclass=posixaccount`
Login attribute	`uid`
DN for password	`ou=people,dc=spectracomcorp,dc=com?one`
Group DN	`cn=engineer,ou=group,dc=spectracomcorp,dc=com`
Group member attribute	`member`

A example configuration for Active Directory would be as follows:

DN for search base	**dc=test,dc=spectracomcorp,dc=com**
Bind DN	**cn=administrator,cn=users,dc=test,dc=spectracomcorp,dc=com**
Bind password	**test**
Search filter	**objectclass=User**
Login attribute	**sAMAccountName**
DN for password	**ou=users,dc=test,dc=spectracomcorp,dc=com?one**
Group DN	**cn=engineer,cn=users,dc=test,dc=spectracomcorp,dc=com**
Group member attribute	**member**

The “**SSL Authentication**” tab provides the means to encrypt the data sent to the LDAP server.

If “**Enable SSL for simple authentication**” is disabled, cleartext is sent to the LDAP server. However, if “Enable SSL for simple authentication” is enabled, text sent to the LDAP server is encrypted.

Server CA certificate verification level: This value specifies the full path to the file with the certificates for the set of acceptable CAs.

CA certificate for server certificate verification: This value specifies the full path to the client public key certificate.

CA client key: This value specifies the full path to the file with the client private key certificate.

The “**Group Authentication**” tab provides the means to authenticate groups of users.
To utilize group authentication, set the “**Enable group based authentication**” value to “Enabled “

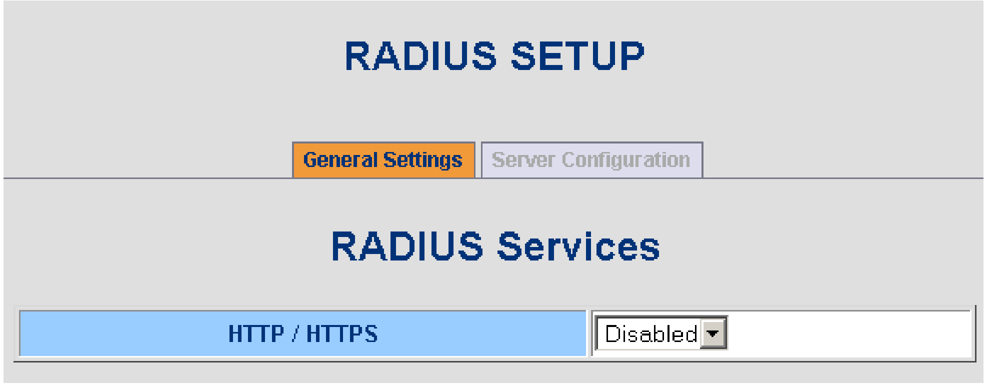
3.22 Configuring RADIUS Authentication

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 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.

The **Network / RADIUS Setup** page (Refer to Figure 3-21) provides the RADIUS configuration options for SecureSync.

The RADIUS Setup page consists of two tabs: "**General Settings**", and "**Server Configuration**".



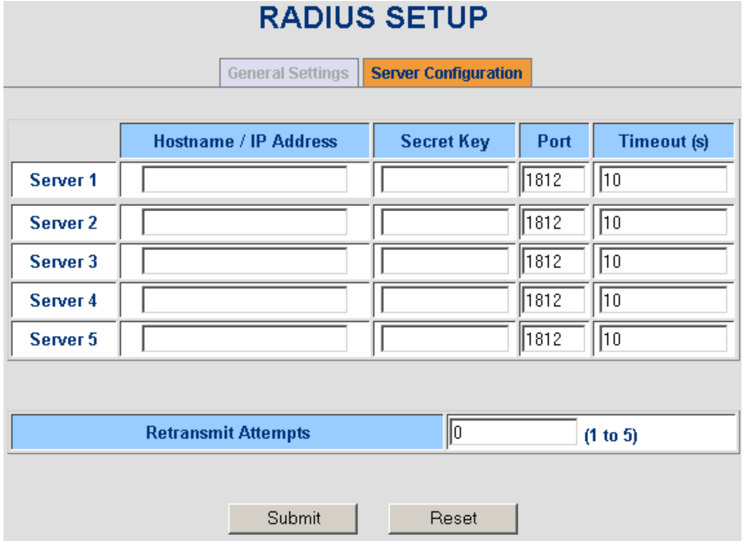
RADIUS SETUP

RADIUS Services

HTTP / HTTPS	Disabled

Figure 3-21: RADIUS Client Configuration Screen (1 of 2)

The "**General Settings**" tab provides the ability to enable or disable RADIUS functionality and provides the means to define which login services will use RADIUS authentication (either HTTP/HTTPS).



	Hostname / IP Address	Secret Key	Port	Timeout (s)
Server 1			1812	10
Server 2			1812	10
Server 3			1812	10
Server 4			1812	10
Server 5			1812	10

Retransmit Attempts 0 (1 to 5)

Figure 3-22: RADIUS Client Configuration

The **Server Configuration** tab allows the user to specify the addresses or hostnames of the RADIUS server(s). Also configured in this tab is a secret key which is shared by SecureSync and the RADIUS server.

Hostname/IP address: Enter either the hostname or IP address of up to five desired Radius servers on the network in which SecureSync can authenticate with.

Secret key: Enter the secret key which is shared by Secure/Sync and the RADIUS server (the key is used to generate an MD5 hash).

Port: Defines the RADIUS Port in which to use. The default RADIUS Port is 1812, but this can be changed, as required.

Timeout: Defines the Timeout that SecureSync will wait to communicate with the RADIUS server.

Retransmit Attempts: Defines the number of retries for SecureSync to communicate with the RADIUS server.

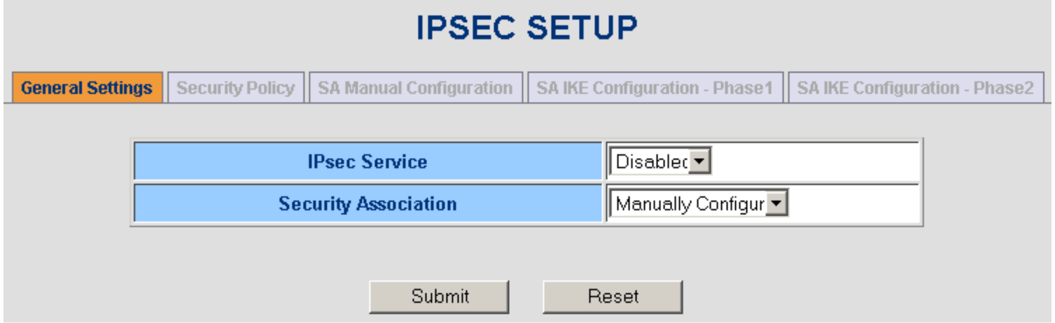
3.23 Configuring IPSec

Internet Protocol Security (IPSec) is a suite of IP protocols that authenticates and encrypts network communications. IPSec supports IPv6 and IPv4 as of this writing.

IPSec defines a Security Association (SA), consisting of secured communications between two network devices. Configuring IPSec requires us to define SA Policy (SAP) and SA Descriptors (SAD). SAP determines what network traffic can or must be secured through IPSec. SAD describes actively secured conversations. All network traffic for an SA contains an identical Security Parameter Index (SPI).

IPSec configuration is performed via the **Network / IPSEC** page, which contains the following tabs:

General Settings
Allows the IPSec function / port to be enabled or disabled as desired. It also allows the Security Association to be defined as either manually configured or using IKE instead.



IPsec Service	Disablec
Security Association	Manually Configur

Figure 3-23: General Settings page

3.23.1 AH vs. ESP

An Authentication Header (AH) and an Encapsulating Security Payload (ESP) are the primary protocols used by IPSec. They authenticate (AH) or authenticate and encrypt (ESP) the data across that connection. Typically, they are used independently, but it is possible to use them together. The SecureSync supports both protocols.

3.23.2 Transport Mode vs. Tunnel Mode

Transport mode provides a secure connection between two endpoints by encapsulating the IP payload. Tunnel mode encapsulates the entire IP packet.

NOTE: Tunnel mode is used to form a traditional Virtual Private Network (VPN), in which the tunnel creates a secure path across a distrusted Internet connection. The SecureSync supports *Transport mode ONLY.*

3.23.3 MD5 vs. SHA-1 vs. DES vs. 3DES vs. AES

An IPSec connection can use two or three encryption choices from among those available. Authentication calculates an Integrity Check Value (ICV) over the data packet's contents. It is usually built on a hash algorithm (for example, MD5 or SHA-1). It uses a secure key known to both endpoints, allowing the recipient to compute the ICV as the sender has computed it. If the recipient gets the same value, the sender has effectively authenticated itself.

3.23.4 IKE vs. Manual Keys

To communicate, the devices at both endpoints must possess the same secure keys. Keys can be entered manually. They may also be generated dynamically between two hosts through Internet Key Exchange (IKE). The SecureSync supports both IKE and manual keys.

3.23.5 Main Mode vs. Aggressive Mode

The initial IKE exchange may be efficient or it may be secure. This tradeoff is governed by the exchange mode, Main or Aggressive. Main mode is completely secure and requires six packets to be sent between the two devices. Aggressive mode requires only three packets be sent between the two devices, but it is less secure.

NOTE: The SecureSync supports both Main and Aggressive modes. Aggressive mode is NOT recommended because of the security risks involved.

3.23.6 Configuring IPSec (IKE SA)

To establish an IPSec connection between the Spectracom SecureSync and an IPv4 addressed host ("A") using IKE SA configuration, we must first configure the IPSec IKE to communicate with host A. To do this, navigate to the IPSEC IKE SA Configuration screen (Figure 3-26).

Exchange Mode defines the mode for Phase 1 (when the IKE daemon is the initiator). You may select all three options (meaning the SecureSync supports Main, Aggressive, and Base Exchange modes) or you may select one or two modes to support. The IKE daemon uses the Main exchange mode when it is the initiator.

Life Time defines the lifetime of the Phase 1 SA proposal.

DH group defines the group used for Diffie-Hellman exponentiations. This directive must be defined using one of the following:

Group 1 - Modp768
Group 2 - Modp1024
Group 5 - Modp1536
Group 14 - Modp2048

NOTE: When using Aggressive mode, the DH group defined for each proposal must be the same.

Encryption Algorithm specifies the algorithm used for Phase 1 negotiation. Choose DES, 3DES, or AES as desired (or as specified by your network administrator).

Hash Algorithm defines another algorithm used for Phase 1 negotiation. Select HMAC-MD5 or HMAC-SHA1 as desired or required.

Authentication Method defines the means of Phase 1 authentication used (preshared keys or X.509 certificates).
Preshared Keys

The easiest way to authenticate using the IKE daemon is through preshared keys. These keys must be defined in a file uploaded to the location specified in the Using Preshared key located in field.

NOTE: After the file is uploaded, its file privileges will be changed automatically to deny unauthorized users access to the preshared keys. This means you will not be able to access the file after uploading it. Always keep an extra copy of the file on hand in another location.

The preshared key file should have the following syntax:

```
192.168.2.100          password1
5.0.0.1                password2
3ffe:501:ffff::3       password3
```

This file is organized in columns. The first column holds the identity of the peer authenticated by the preshared key. The second column contains the keys.

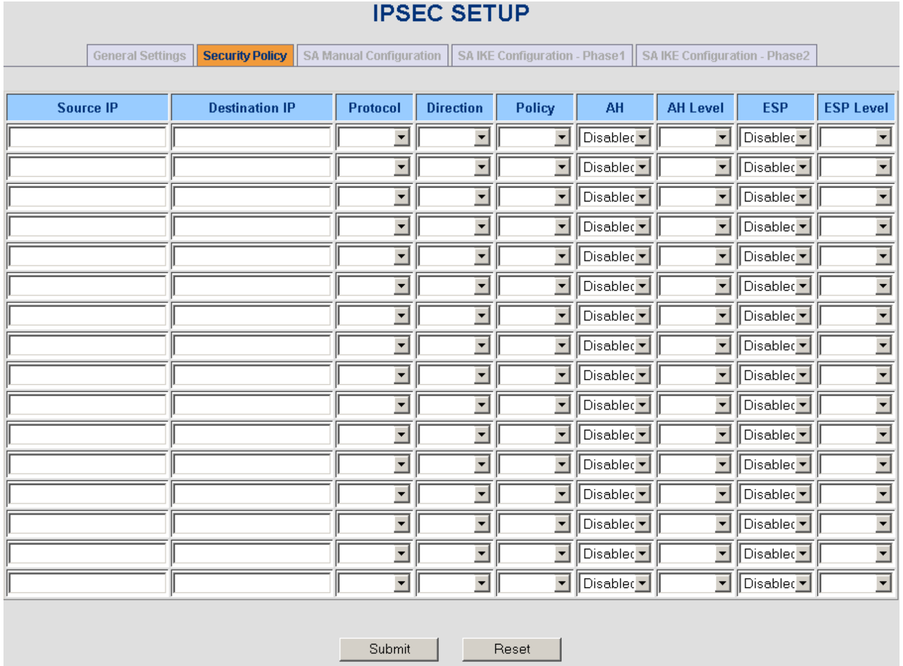
X.509 Certificates

The IKE daemon supports the use of X.509 certificates for authentication. Spectracom supplies two means of providing the public/private key pair to the SecureSync.

The first approach is through the user interface on the IPSec IKE SA Configuration screen. Specify the Certificate Files Path and Peer's Certificate File name, then select Md5 or Sha1 to specify the Signature Algorithm. You must also specify the RSA Private Key Length to use when generating the key pair.

Alternatively, you may generate elsewhere and upload to the SecureSync your key pair(s). Specify the directory and the name of the key pairs uploaded to it. Regardless of the method used, however, you must upload the peer's public key to the SecureSync and provide the directory and file name to the SecureSync in the IPSec IKE SA Configuration pagen.

Security Policy Tab



Source IP	Destination IP	Protocol	Direction	Policy	AH	AH Level	ESP	ESP Level
					Disablec		Disablec	
					Disablec		Disablec	
					Disablec		Disablec	
					Disablec		Disablec	
					Disablec		Disablec	
					Disablec		Disablec	
					Disablec		Disablec	
					Disablec		Disablec	
					Disablec		Disablec	
					Disablec		Disablec	
					Disablec		Disablec	
					Disablec		Disablec	
					Disablec		Disablec	
					Disablec		Disablec	
					Disablec		Disablec	
					Disablec		Disablec	

Figure 3-24: IPSec Security Policy Screen

Select *ANY* as the desired protocol to apply for IPSec security protection (unless a specific protocol is desired; these can be selected from the drop-down list).

NOTE: When using IKE over IPv6, do NOT select ANY. There are protocols that do not work well with IKE under IPv6 with IKE. Select one of the specific protocols listed in the dropdown menu, as desired or required.

Select *Both* for the Direction, which means IPSec security protection is required for both incoming and outgoing packets. Security protection may also be applied to incoming packets only, or to outgoing packets only (from the drop-down list).

Select *IPSec* to use IPSec as the security policy. (You may also select *None* or *Discard*. Selecting *None* means that IPSec operation will not take place on the packet, while selecting *Discard* means the packet matching indexes will be discarded.

You may choose to check either or both AH and ESP to set them as *Require*, *Use*, *Default*, or *Unique*.

- *Default* means the kernel consults the system-wide default for the protocol specified.
- *Use* means the kernel uses an SA if it is available, while the kernel keeps normal operation otherwise.
- *Require* means an SA is required whenever the kernel sends a packet matched with the policy.

- *Unique* is nearly functionally identical to *Require*, but allows the policy to match the unique outbound SA.

SA Manual Configuration Tab
To establish an IPSec connection between SecureSync and an IPv6 addressed host (“B”) using manual SA configuration, refer to the IPSec Manual SA Configuration screen.

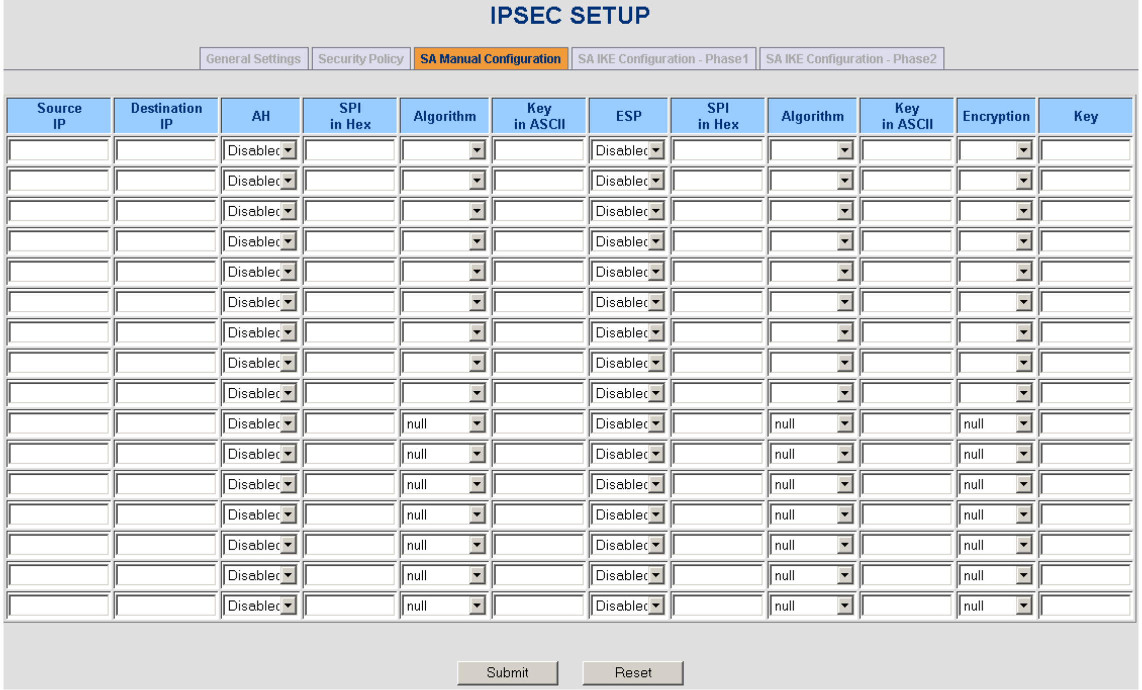
3.23.7 Manual Security Associations

Input the SecureSync IP address as the Source IP and host B’s IP address as the Destination IP.

The Security Parameter Index (SPI) must be a hexadecimal number without the “0x” prefix. Enter the desired values manually.

NOTE: SPI values between 0 and 255 are reserved and cannot be used at this time.

Make sure to check the AH or ESP boxes for the key configurations used. If the appropriate box is not checked, information following the AH or ESP inputs will be ignored by the update page.



IPSEC SETUP

Source IP	Destination IP	AH	SPI in Hex	Algorithm	Key in ASCII	ESP	SPI in Hex	Algorithm	Key in ASCII	Encryption	Key
		Disablec				Disablec					
		Disablec				Disablec					
		Disablec				Disablec					
		Disablec				Disablec					
		Disablec				Disablec					
		Disablec				Disablec					
		Disablec				Disablec					
		Disablec				Disablec					
		Disablec				Disablec					
		Disablec		null		Disablec		null		null	
		Disablec		null		Disablec		null		null	
		Disablec		null		Disablec		null		null	
		Disablec		null		Disablec		null		null	
		Disablec		null		Disablec		null		null	
		Disablec		null		Disablec		null		null	
		Disablec		null		Disablec		null		null	

Figure 3-25: IPSec Manual SA Configuration

3.23.8 Configure IPSec Security Policy

Configure the IPSec security policy from the IPSec General Setting screen (Figure 3-23).

NOTE: The manual SA values must be configured BEFORE the manual SA option is enabled from the IPSec General screen (Figure 3-24). If the feature is enabled before it is configured from the IPSec Manual SA Configuration screen, the SA and SP tables will not update correctly.

Select ANY as the desired protocol to apply for IPSec security protection (unless a specific protocol is desired; these can be selected from the drop-down list).

Select *Both* for the Direction, which means IPSec security protection is required for both incoming and outgoing packets. Security protection may also be applied to incoming packets only, or to outgoing packets only (from the drop-down list).

Select *IPSec* to use IPSec as the security policy. You may also select *None* or *Discard*. Selecting *None* means that IPSec operation will not take place on the packet, while selecting *Discard* means the packet matching indexes will be discarded.

You may choose to check either or both AH and ESP to set them as *Require*, *Use*, *Default*, or *Unique*.

- *Default* means the kernel consults the system-wide default for the protocol specified.
- *Use* means the kernel uses an SA if it is available, while the kernel keeps normal operation otherwise.
- *Require* means an SA is required whenever the kernel sends a packet matched with the policy.
- *Unique* is the same as *Require*, but allows the policy to match the unique outbound SA.

SA IKE Configuration - Phase 1 Tab

Compression Algorithm defaults to “deflate.” It is not configurable at this time.

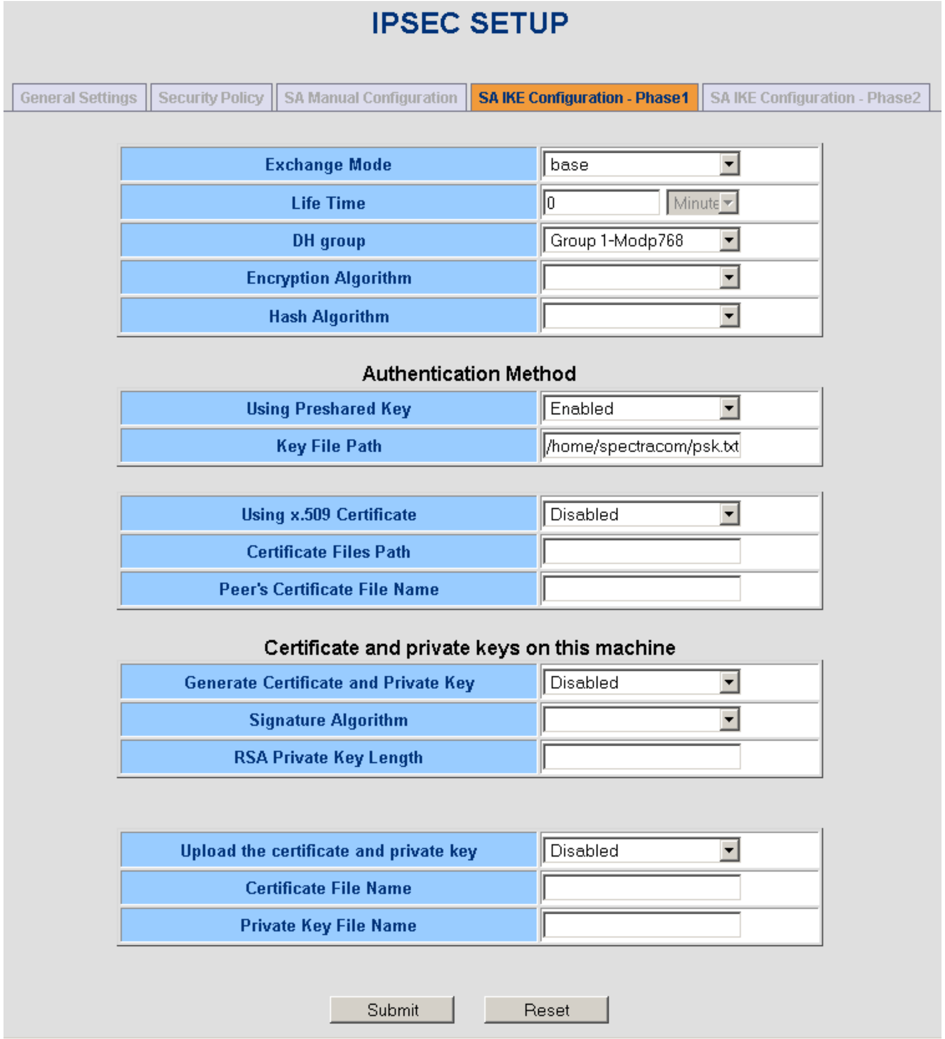
NOTE: After completing and submitting changes in the IPSec IKE SA Configuration screen, check to make sure IPSec is enabled and IKE is selected for use with IPSec. The IKE Log (refer to *Logs and Status Reporting*) is helpful in troubleshooting this condition.

3.23.9 Configure IPSec Security Policy

To configure IPSec security policy options, navigate to the **Network / IPSec Setup** page, **Security Policy** tab.

NOTE: Always configure IKE BEFORE enabling the IKE option. If IKE is not configured, the IKE daemon won’t start correctly when the Security Association is enabled.

From the IPSec General Screen, enable (or disable) the IPSec service and specify the Security Association (IKE if already configured, or Manually Configure). In the Security Policy table, input the SecureSync’s IP address as the Source IP and host A’s address as the Destination IP.



Exchange Mode	base
Life Time	0 Minute
DH group	Group 1-Modp768
Encryption Algorithm	
Hash Algorithm	

Authentication Method

Using Preshared Key	Enabled
Key File Path	/home/spectracom/psk.txt

Using x.509 Certificate	Disabled
Certificate Files Path	
Peer's Certificate File Name	

Certificate and private keys on this machine

Generate Certificate and Private Key	Disabled
Signature Algorithm	
RSA Private Key Length	

Upload the certificate and private key	Disabled
Certificate File Name	
Private Key File Name	

Figure 3-26: IPSEC IKE SA Configuration Screen (1 of 2)

The SA IKE Configuration - Phase 2 Tab

Life Time defines how long an IPSec SA will be used.

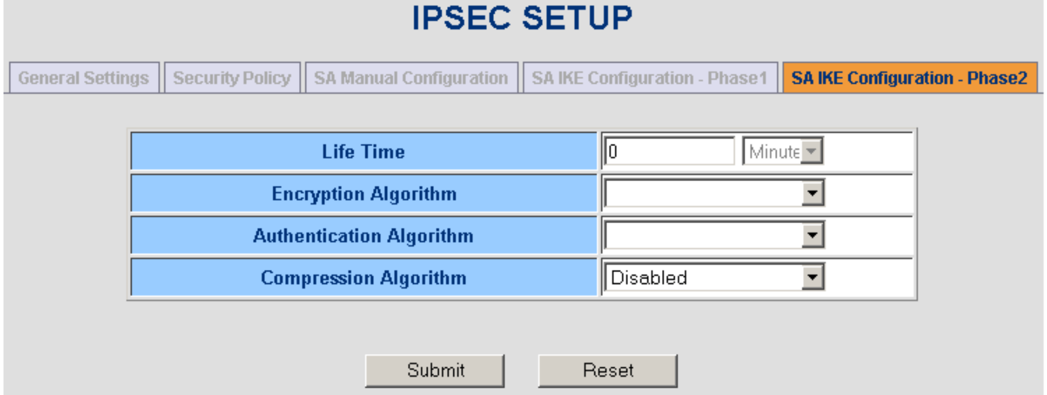
Encryption Algorithm defines the group used for Diffie-Hellman exponentiations. This directive must be defined using one of the following:

Group 1 - Modp768
Group 2 - Modp1024
Group 5 - Modp1536
Group 14 - Modp2048

NOTE: When using Aggressive mode, the DH group defined for each proposal must be the same.

Encryption Algorithm specifies the algorithm used for Phase 2. Select DES, 3DES, AES (used with ESP) or NULL as desired (or as required by your network administrator).

Authentication Algorithm defines another algorithm used for Phase 2. Select HMAC-SHA1 or HMAC-MD5 as required.



Life Time	0 Minute
Encryption Algorithm	
Authentication Algorithm	
Compression Algorithm	Disabled

Figure 3-27: IPSEC IKE SA Configuration Screen (2 of 2)

Section 4: SecureSync Status Indications

In addition to the available SecureSync logs, status information about the unit can be viewed and monitored several ways. These status indications include the time synchronization with its selected references, GNSS satellites currently being tracked, estimated time errors, oscillator disciplining, NTP sync status and current Stratum level, status of outputs and presence of DC input power.

4.1 Front Panel LED Status Indications

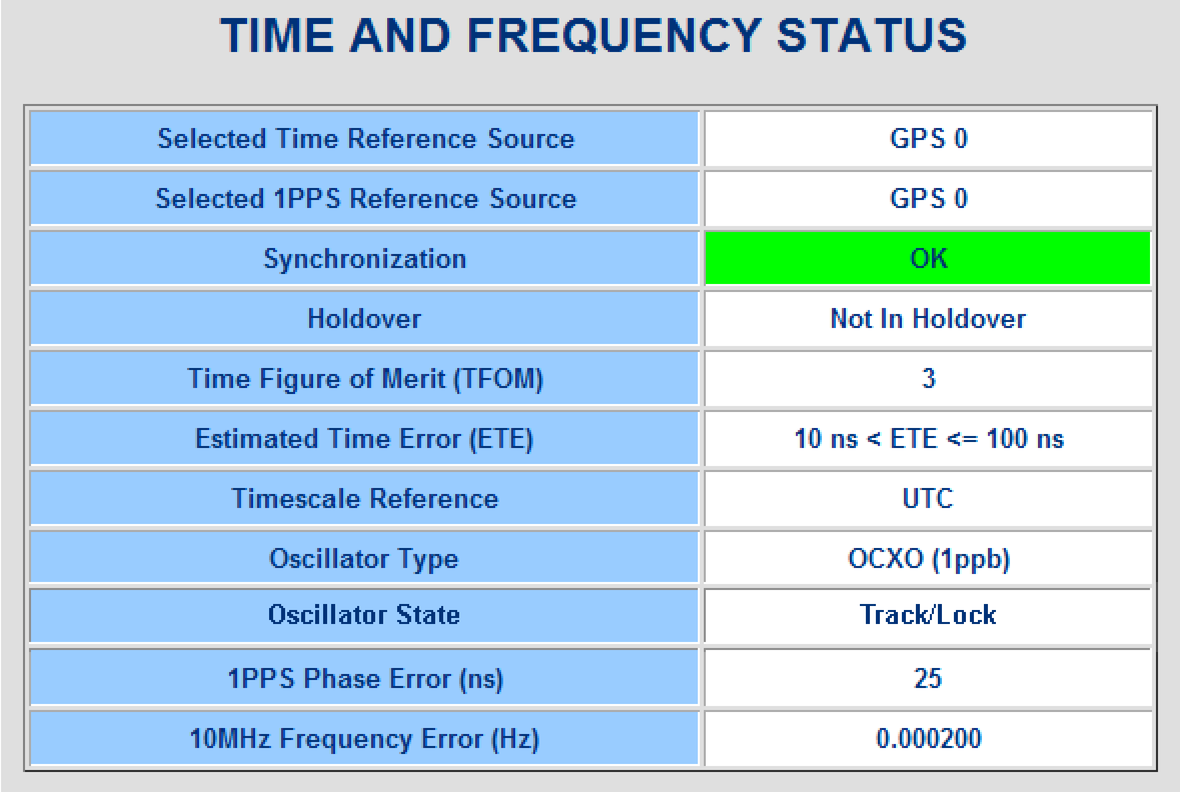
The SecureSync front panel status LEDs are one indication of the current operational status. For detailed information, refer to the table in Section *1.3.1*: "*Front Panel LED Indicators*".

4.2 Web Interface Status Indications

Current status information is also available via the "**Status**" dropdown option from the main navigation menu of the SecureSync web user interface. Available status pages include **Time and Frequency**, **Inputs**, **Outputs**, **Disciplining**, **NTP**, and **Power**. This section details the information displayed on each of these status pages.

4.2.1 Status / Time and Frequency Page

The **TIME AND FREQUENCY STATUS** table (accessible from **Status / Time and Frequency**) provides the status of reference inputs and the system timing.



TIME AND FREQUENCY STATUS

Selected Time Reference Source	GPS 0
Selected 1PPS Reference Source	GPS 0
Synchronization	OK
Holdover	Not In Holdover
Time Figure of Merit (TFOM)	3
Estimated Time Error (ETE)	10 ns < ETE <= 100 ns
Timescale Reference	UTC
Oscillator Type	OCXO (1ppb)
Oscillator State	Track/Lock
1PPS Phase Error (ns)	25
10MHz Frequency Error (Hz)	0.000200

Figure 4-1: Time and Frequency Status

Status information displayed on this page is as follows:

Selected Time Reference Source: This field indicates which available input reference has been selected to be the Time reference for the System Time.

- “OK” (Green) indicates the reference is present and has been declared valid.
- “Not Valid” (Orange) indicates the reference is not currently present or is not currently valid.

Selected 1PPS Reference Source: This field indicates which available input reference has been selected to be the 1PPS reference for the System Time.

- “OK” (Green) indicates the reference is present has been declared valid.
- “Not Valid” (Orange) indicates the input reference is not currently present or is not currently valid.

Synchronization: Indicates if SecureSync is currently synchronized with its selected references.

- “OK” (Green) indicates SecureSync is currently synchronized to its references (The front panel Sync light will also be green).
- “Not Valid” (Orange) indicates SecureSync is not currently synchronized to its references (The front panel Sync light will also be red).

Holdover: Holdover is a mode of operation that begins when all of the references defined in the Reference Status table are either declared invalid or are no longer present. During Holdover mode, the internal oscillator is used to increment the system time very accurately. Holdover mode ends when an available reference is restored (SecureSync returns to "Synchronized") or if the references are not restored before the configured holdover period expires (SecureSync will no longer be "Synchronized"). During Holdover, all outputs are still fully useable. If the Holdover period expires without the references being restored, Time Sync is lost and the outputs may not be unusable.

Holdover indicating "Disabled" indicates that either both of the Time and 1PPS references are currently valid or that one or both of the references were lost and the Holdover period has since expired. "Enabled" indicates Holdover mode is currently active (one or both of the references has been lost and the Holdover period has not yet expired).

The default maximum allotted Holdover time is 2 hours, but this value can be customized as desired (based on timing requirements). The maximum length of Holdover is configured from the **Setup / Disciplining** page. Refer to Section *3.15* for more information on configuring Holdover mode.

Oscillator Type: Indicates the installed oscillator type of the unit and the stability of the oscillator.

Oscillator State: Indicates whether or not the internal oscillator is currently being disciplined (steered to an input reference).

- When "Disciplining State" indicates "Track/Lock", Freerun will indicate "Not in Freerun".
- When "Disciplining State" indicates "Not locked", Freerun will indicate "In Freerun".

Time Figure of Merit (TFOM): A report that indicates SecureSync's estimation of how accurately it is synchronized with its time and 1PPS reference inputs, based on several factors. The TFOM range is 1through 15, with the lower the TFOM number, the more closely SecureSync believes it's aligned with its inputs. Refer to the following table.

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 usec
5	1 usec < ETE <= 10 usec
6	10 usec < ETE <= 100 usec
7	100 usec < ETE <= 1 msec
8	1 msec < ETE <= 10 msec
9	10 msec < ETE <= 100 msec
10	100 msec < ETE <= 1 sec
11	1 sec < ETE <= 10 sec
12	10 sec < ETE <= 100 sec
13	100 sec < ETE <= 1000 sec
14	1000 sec < ETE <= 10000 sec
15	ETE > 10000 sec

Table 4-1: TFOM values

Estimated Time error (ETE): SecureSync's estimate on its internal time error, based on its available time input references. The estimated error is between the two stated values.

TimeScale Reference: Displays the currently configured time scale for the System Time. This Timescale defines what Timescale that the time entries in all of the logs and the NTP time stamps will be provided as. If Timescale is configured as "UTC", the timestamps in the logs and the NTP output will be in UTC timescale.

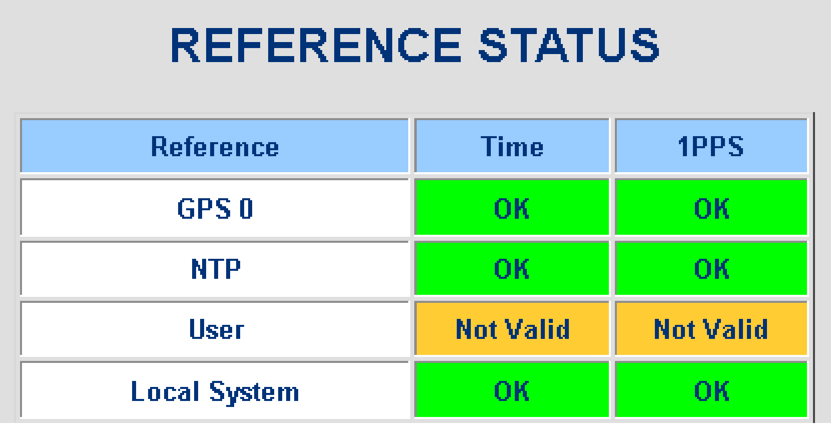
Oscillator Type: Displays the oscillator type.

Oscillator State: Displays the current oscillator disciplining state.

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).

10MHz 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).

The **REFERENCE STATUS** table provides the current status (presence and validity) of all configured time and 1PPS input references (such as GNSS, IRIG, NTP, 10 MHz, HAVE QUICK, external 1PPS input and user set time).



REFERENCE STATUS

Reference	Time	1PPS
GPS 0	OK	OK
NTP	OK	OK
User	Not Valid	Not Valid
Local System	OK	OK

Figure 4-2: Reference Status Table

The **Time** and **1PPS** columns will show the configured input references for that Index.

- "OK" (Green) indicates the reference is both present and valid.
- "Not Valid" (Orange) indicates the reference is either not valid or not present.

Each input reference is assigned a designated name that indicates the type of reference it is (e.g., "GPS 0" indicates the reference is GNSS input). Refer to Section *3.17* for more information on configuring the Input references and a list of the designated names.

The example Reference Status table (refer to Figure 4-2) shows that both the GNSS and Local System inputs are both currently enabled and are providing valid time and 1PPS input (as indicated by the green "OK" boxes). However, NTP and User are not currently providing valid time or 1PPS input (as indicated by the "Not Valid" messages).

4.2.2 Status / Inputs Page

The **Status / Inputs** page provides access to the status of different sections of SecureSync, including input power and the input status for any installed option modules (Slots) that have input status available.

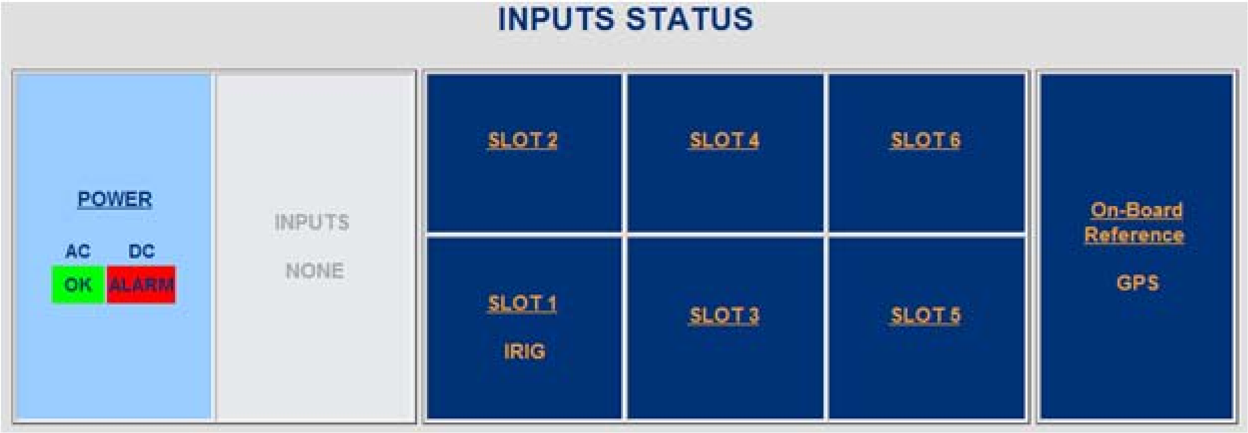


Figure 4-3: Example Inputs Status page

Power: The Power box displays whether AC and DC power are currently present (Note: clicking on "Power" here opens another page displaying the same information, but in a different view).

- "OK" (Green) indicates AC or DC power is currently present.
- "ALARM" (Red) indicates the AC or DC power is not present.

Option Modules: Any Slot that has an option module installed which contains input status (such as the IRIG module for example) will be displayed in the corresponding Slot number on this page. Select this Slot to see the input status for that particular module.

Slots: The "Slot" boxes (Slot 1 through Slot 6) will indicate which option modules (if any) are currently installed in that particular Slot location. Slot numbers are displayed in the same orientation as they are physically located on the rear panel, and the name of the installed option modules are displayed below the Slot number.

Clicking on a particular Slot that indicates an option module in installed will access the input status page for that particular module. When clicked, if no modules are currently installed in that Slot, the message "*This slot is empty*" will be displayed. Or, if the installed module has no input configuration available (some option modules have no input configuration and only have output configuration available), the message "*This card does not have inputs*" will be displayed instead.

NOTE: The Input Status pages of the various Option Modules are discussed in the corresponding Option Module chapters, located in Section 8:.

GPS: The "GPS" box displays whether the 1PPS and Time inputs being provided by the GNSS receiver are present and valid.

- "OK" (Green) indicates the GNSS input references are present and valid (the minimum number of GNSS satellites requires is currently being tracked).
- "Not Valid" (Orange) indicates the GNSS input references are either not valid or currently not present (the minimum number of GNSS satellites requires is not currently being tracked).

Clicking on "**GPS**" in this box opens the GPS Inputs Status page. Status information displayed here includes the following:

Manufacturer/Model: Displays manufacturer/model information for the installed GNSS receiver.

1PPS Validity and **Time Validity**:

Display whether the 1PPS and Time inputs being provided by the GNSS receiver are present and considered valid.

- "OK" (Green) indicates the GNSS input references are present and valid (the minimum number of GNSS satellites requires is currently being tracked).
- "Not Valid" (Orange) indicates the GNSS input references are either not valid or currently not present (The minimum number of GNSS satellites requires is not currently being tracked).

Receiver Mode: Indicate whether the GNSS receiver is configured for standard mode, 1 satellite mode, or mobile mode operation.

GPS Longitude and **GPS Latitude:** Current location of the GNSS receiver, as either calculated by GNSS or manually inputted by a user.

GPS Altitude: Current height (above sea level) of the GNSS antenna, as either calculated by GNSS or manually inputted by a user.

Survey Prog: Shows the current progression (in percent) or status of the GNSS survey. The GNSS survey is conducted in order for the GNSS receiver to calculate and lock-in an accurate GNSS fix. If the GNSS receiver is configured for the factory default "Stationary" mode (GNSS surveys are not performed while the GNSS receiver is in the mobile mode)", a GNSS survey is automatically performed when any of following conditions occur:

- Initial installation of SecureSync (GNSS has not yet been tracked).
- SecureSync has been relocated to a new location.
- The GNSS receiver's location has been manually cleared by a user.
- The receiver is reconfigured from mobile mode to stationary mode.

The GNSS survey will begin once the GNSS receiver initially starts tracking at least four GNSS satellites. The survey requires the receiver to be able to track at least four satellites continuously until the survey has completed (if the GNSS receiver drops below four satellites during the survey, it will begin again).

This field will display "**Almanac**" with no GNSS satellites presently being tracked. With GNSS reception present and a survey being required, this field will begin to show the percentage of the survey that has been completed thus far (the survey takes approximately 33 minutes to complete). Until the GNSS survey has been completed, the receiver needs to continue to track a minimum of four satellites to allow the GNSS survey to be completed.

Once the GNSS survey has completed (as indicated by "Complete" in the "Survey Prog" field) at least four satellites need to continue to be tracked in order for GNSS to be considered a valid and useable input reference. If the GNSS signal is subsequently lost or Secure Sync is rebooted, the survey does not need to be performed again (the GNSS survey will need to be performed again if SecureSync is subsequently relocated or the GNSS position data is ever manually cleared). GNSS will then be considered valid with at least four satellites being tracked.

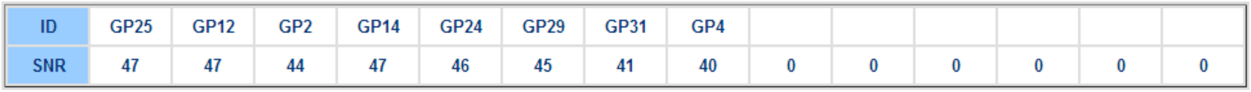
Number of Tracked Satellites: Displays the total number of satellites currently being used by the GNSS receiver for positional and timing operations.

Offset: Displays the currently configured GNSS Offset (offset accounts for antenna cable delays and other latencies).

Antenna Sense: Indicates if 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. "Open" indicates there is an open in the GNSS antenna cable and "Short" indicates there is a short in the GNSS antenna cable. "OK" indicates the GNSS antenna is connected with the expected amount of current draw being detected (no opens or shorts currently being detected in the cable).

Selected Constellations: When the product is fitted with a Multi-GNSS receiver, this field indicates constellations which are currently selected.

"ID/SNR" table: The GNSS satellite signal strengths are displayed in the smaller table located below the GNSS status table. The values shown in the fourteen horizontal ID fields correspond to the Vehicle ID numbers assigned to each of the first fourteen GNSS satellites (each satellite is assigned to one of the available GNSS receiver channels). ID is preceded by the mention "GP" or "GL", which indicates the type of satellite tracked. GP indicates GPS satellite, and GL indicates GLONASS satellite. The SNR range is 0 to 55, with typical SNR values for good GNSS reception typically being in the mid 30's to 40's range.



ID	GP25	GP12	GP2	GP14	GP24	GP29	GP31	GP4						
SNR	47	47	44	47	46	45	41	40	0	0	0	0	0	0

Figure 4-4: Example ID/SNR table output

In the example shown in the figure, eight satellites are currently being tracked (as indicated by the first eight fields of the horizontal "SNR" column have numbers other than "0" present). In this example, the satellites ID numbers being tracked are the first nine numbers in the horizontal "ID" column and the signal strengths of these satellites (SNR horizontal column) range from 40 to 47 (indicating good signal strengths).

4.2.3 Status / Outputs Page

The **Status / Outputs** page provides the current output status of the 1PPS and 10 MHz outputs that are available with all SecureSync units as well as the output statuses of any installed / available option modules.

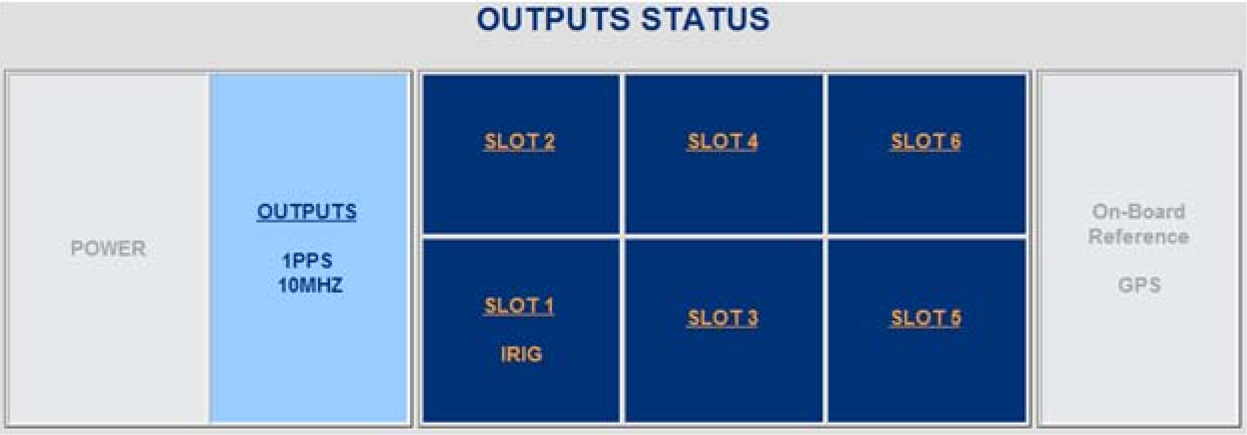
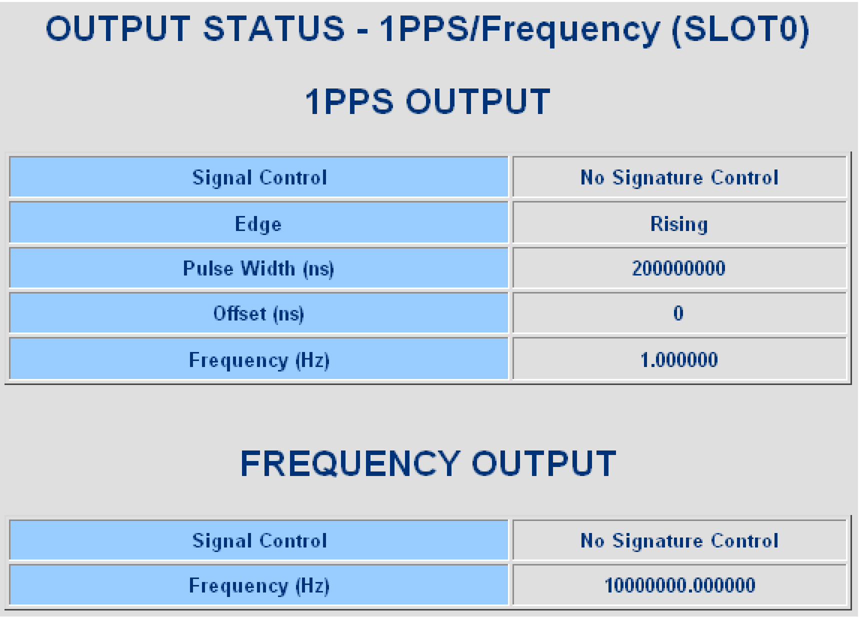


Figure 4-5: Example Outputs Status Page

Outputs (1PPS/Frequency): Clicking on "OUTPUTS" opens a page that displays the current status of the 1PPS and 10 MHz outputs, described below:



OUTPUT STATUS - 1PPS/Frequency (SLOT0)

1PPS OUTPUT

Signal Control	No Signature Control
Edge	Rising
Pulse Width (ns)	200000000
Offset (ns)	0
Frequency (Hz)	1.000000

FREQUENCY OUTPUT

Signal Control	No Signature Control
Frequency (Hz)	10000000.000000

Figure 4-6: Output Status page

Signature Control: Signature Control, when enabled, disables the 1PPS or 10 MHz output if SecureSync is not synchronized to its selected references. "**Output Always Enabled**" indicates the signal is always present as long as SecureSync is running.

Edge: Indicates if the on-time point of the 1PPS output is the rising or falling edge of the signal.

Pulse Width: Configured Pulse Width of the 1PPS output, displayed in nanoseconds.

Offset: Displays the currently configured 1PPS Offset (Offset accounts for cable delays and other latencies).

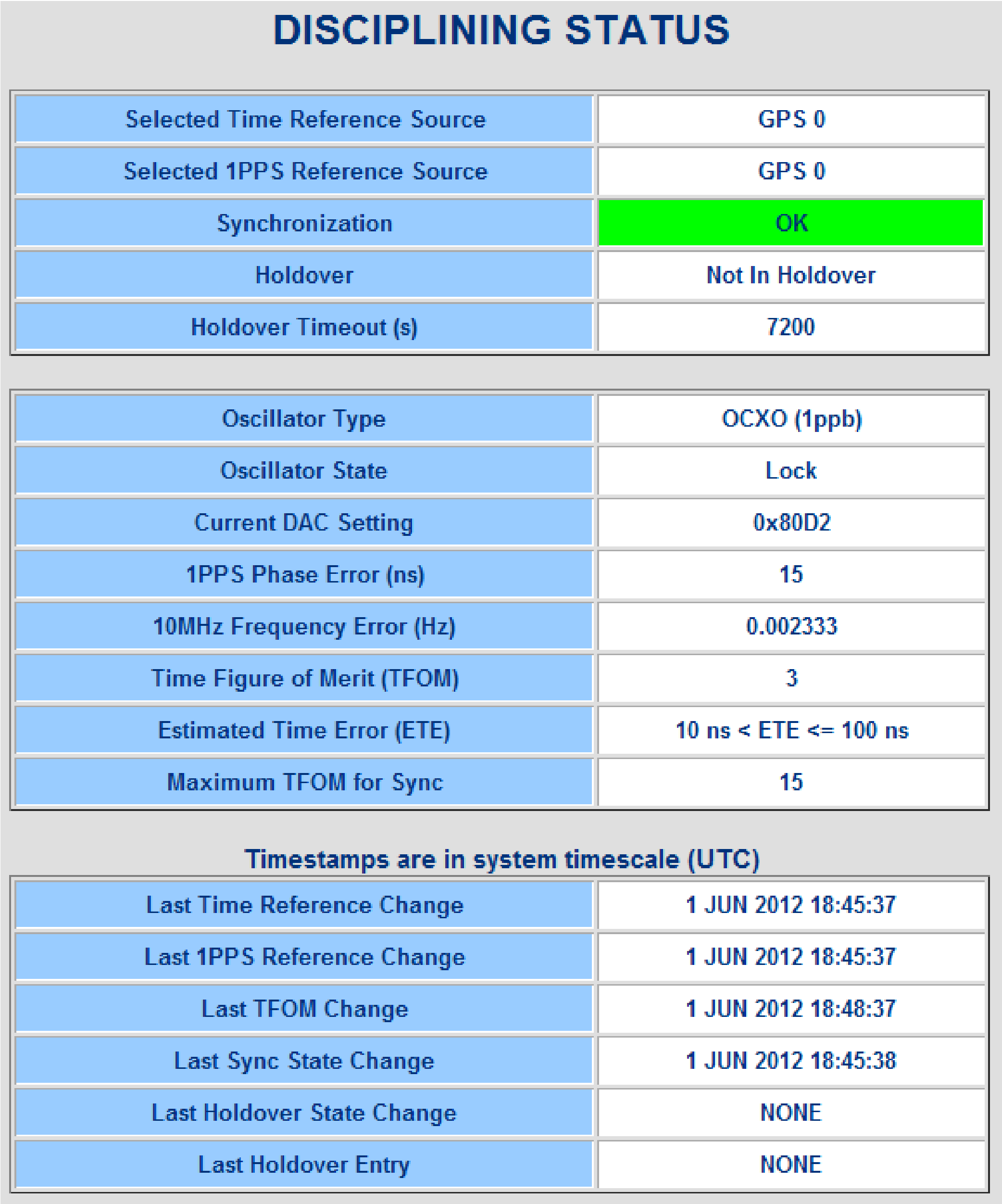
Frequency: Current frequency of the 1PPS and 10 MHz outputs.

Slots: The “Slot” boxes (Slot 1 through Slot 6) will indicate which option modules (if any) are currently installed in that particular Slot location. The name of the installed module is shown below the Slot number. The numbers of the Slot boxes are shown in the same orientation as they are located on the back panel.

Clicking on a particular Slot that indicates an option module in installed will access the output status of that particular module. When clicked, if no modules are currently installed in that Slot (or if the installed module has no output configuration available), the message “*This slot is empty*” will be displayed instead.

4.2.4 Status / Disciplining Page

Disciplining status information is available from the **Status / Disciplining Status** page. It provides additional information beyond what is available from the **Status / Time and Frequency** page.



DISCIPLINING STATUS

Selected Time Reference Source	GPS 0
Selected 1PPS Reference Source	GPS 0
Synchronization	OK
Holdover	Not In Holdover
Holdover Timeout (s)	7200

Oscillator Type	OCXO (1ppb)
Oscillator State	Lock
Current DAC Setting	0x80D2
1PPS Phase Error (ns)	15
10MHz Frequency Error (Hz)	0.002333
Time Figure of Merit (TFOM)	3
Estimated Time Error (ETE)	10 ns < ETE <= 100 ns
Maximum TFOM for Sync	15

Timestamps are in system timescale (UTC)

Last Time Reference Change	1 JUN 2012 18:45:37
Last 1PPS Reference Change	1 JUN 2012 18:45:37
Last TFOM Change	1 JUN 2012 18:48:37
Last Sync State Change	1 JUN 2012 18:45:38
Last Holdover State Change	NONE
Last Holdover Entry	NONE

Figure 4-7: Oscillator Disciplining

Status information displayed on this page is as follows:

NOTE: Much of the information displayed on this page is described in the "*Status / Time and Frequency Page*" section.

Selected Time Reference Source: See the **Status / Time and Frequency** Page section.

Selected 1PPS Reference Source: See the **Status / Time and Frequency** Page section.

Synchronization: See the **Status / Time and Frequency** Page section.

Holdover: See the **Status / Time and Frequency** Page section.

Holdover Timeout: The time interval between the loss of all valid 1PPS or Time input references and the moment that the SecureSync declares loss of time synchronization is known as the Holdover mode. While the unit is in Holdover mode, the time outputs are derived from an internal oscillator incrementing the System Time. Set on the **Setup / Disciplining** page.

Oscillator Type: See the **Status / Time and Frequency** Page section.

Oscillator State: See the **Status / Time and Frequency** Page section.

Current DAC Setting: See the **Status / Time and Frequency** Page section.

1PPS Phase Error: See the **Status / Time and Frequency** Page section.

10MHz Frequency Error: See the **Status / Time and Frequency** Page section.

Time Figure of Merit (TFOM): See the **Status / Time and Frequency** Page section.

Estimated Time error (ETE): See the **Status / Time and Frequency** Page section.

Maximum TFOM for Sync: Defines the largest TFOM value (TFOM is SecureSync's estimation of how accurately it is synchronized with its time and 1PPS reference inputs, based on several factors - known as the estimated time error or "ETE") that is allowed before disciplining is no longer performed on the oscillator. Set on the **Setup / Disciplining** page.

Last Time Reference Change: This timestamp shows the last time the **Time Reference Source** to the SecureSync changed.

Last 1PPS Reference Change: This timestamp shows the last time the **1PPS Reference Source** to the SecureSync changed.

Last TFOM Change: This timestamp shows the last time the TFOM of the SecureSync changed.

Last Sync State Change: This timestamp shows the last time the Synchronization state of the SecureSync changed.

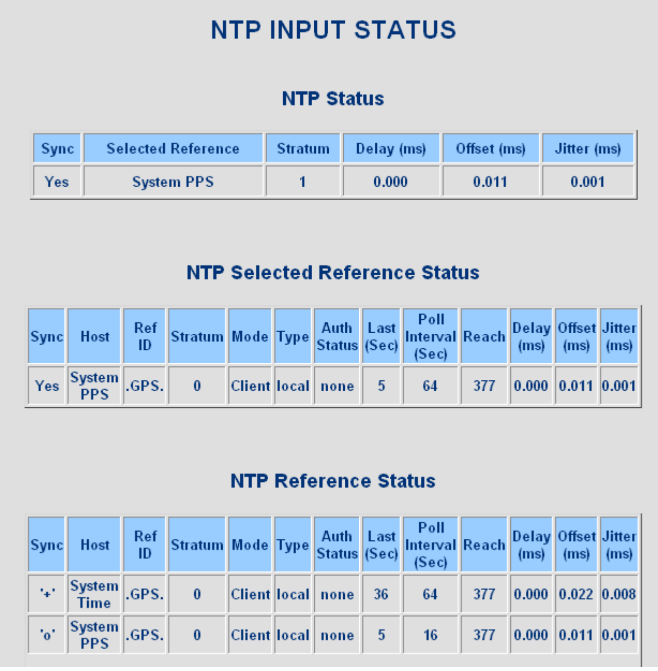
Last Holdover State Change: This timestamp shows the last time the Holdover state of the SecureSync changed.

Last Holdover Entry: This timestamp shows the last time the SecureSync entered the Holdover state.

4.2.5 Status / NTP Page

To view current NTP status information, navigate to the **Status / NTP Status** page. Other available NTP servers can be configured as NTP Peers or Servers to SecureSync (refer to Section 3.18.3 for more information on configuring other NTP servers as input references). This is known as NTP Peering and allows for NTP servers to provide time to other NTP servers at the same Stratum, or to other NTP servers at a lower stratum level.

NTP can be provided with a list of other NTP servers that it can sync to, but it can only choose one as its current selected reference. The NTP status page displays current information about the selected NTP server and the other configured NTP Peers and servers (such as reported Stratum level, sync status, jitter, offset, poll interval, etc) for any other configured NTP Peers and/or Servers that can be used as input time references for System Time synchronization.



NTP INPUT STATUS

NTP Status

Sync	Selected Reference	Stratum	Delay (ms)	Offset (ms)	Jitter (ms)
Yes	System PPS	1	0.000	0.011	0.001

NTP Selected Reference Status

Sync	Host	Ref ID	Stratum	Mode	Type	Auth Status	Last (Sec)	Poll Interval (Sec)	Reach	Delay (ms)	Offset (ms)	Jitter (ms)
Yes	System PPS	.GPS.	0	Client	local	none	5	64	377	0.000	0.011	0.001

NTP Reference Status

Sync	Host	Ref ID	Stratum	Mode	Type	Auth Status	Last (Sec)	Poll Interval (Sec)	Reach	Delay (ms)	Offset (ms)	Jitter (ms)
'+'	System Time	.GPS.	0	Client	local	none	36	64	377	0.000	0.022	0.008
'o'	System PPS	.GPS.	0	Client	local	none	5	16	377	0.000	0.011	0.001

Figure 4-8: NTP Input Status page

Status information displayed on the NTP Status page is divided into the three sections: NTP Status, NTP Selected Reference Status, and NTP Reference Status.

NTP Status: Displays SecureSync's current NTP status, including whether or not NTP is in sync, the current Stratum level being reported to the network, as well as its Delay, Offset and Jitter values (as compared to its selected input references). This section consists of the following fields:

Sync: Indicates if SecureSync is reporting to the network that NTP is in sync.

Selected Reference: Indicates what NTP is synchronized with for its reference. If NTP is internally synced to SecureSync's internal System information "System Time" will initially be displayed and then it will switch to "System PPS" being displayed in this field. Otherwise, an IP address will be displayed in this field if NTP is synced with another NTP server instead.

Stratum: The NTP Stratum level being reported to the network. This value indicates "NTP hierarchy" and also determines if the network can use the NTP packets supplied by SecureSync for its synchronization.

1. When SecureSync is currently synced with its NTP input reference selected (or went into Holdover mode after losing its NTP reference), this value will be one less than SecureSync's NTP reference. The clients on the network can use the SecureSync's NTP packets for synchronization.
2. When SecureSync is currently synced with any other reference selected (besides the NTP input reference) or SecureSync has since lost the reference and has gone into the Holdover mode, this value will indicate Stratum 1. The clients on the network can use the SecureSync's NTP packets for synchronization.
3. When SecureSync is currently not synced with any of its input references and is not currently in Holdover mode, this value will indicate Stratum 16. Stratum 16 will cause the NTP clients to ignore the SecureSync's NTP packets.

Delay: the measured one-way path delay (in milliseconds) between NTP and its selected reference (e.g., System Time).

Offset: The measured time difference (in milliseconds) between NTP and its selected reference (e.g., System Time).

Jitter: Variance (in milliseconds) occurring in the reference input time (from one poll to the next).

NTP Selected Reference Status: Displays information about the selected NTP Peer or Server that NTP is using as its reference, including the following:

Sync: A symbol that indicates if the listed reference is available for selection as a reference. Refer to the following table for details.

Symbol	Indication
o	PPS Peer (A high quality candidate for NTP reference that can be selected by NTP as its PPS reference).
+	A high quality candidate for NTP reference input that can be selected by NTP as its time reference.
*	Reference is a preferred peer.
X	Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference).
.	Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference).
-	Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference).

Table 4-2: Sync Column Symbols

Host: Indicates what the selected NTP reference is synchronized with for its reference. If NTP is internally synced to SecureSync's internal System information "System Time" or "System PPS" will be displayed in this field. Otherwise, an IP address will be displayed in this field if the NTP reference is synced with another NTP server.

Ref ID: The type of input reference (for example, "GPS" indicates the reference can use GPS for its synchronization).

LOCL (Local): Listed reference is currently synced to itself (the listed reference has not yet synced to its reference yet).

GPS: The listed reference is a GNSS-based type reference (such as another SecureSync appliance).

PPS: The listed reference is a PPS (not a Time) reference for NTP.

STC (Serial Time Code): The listed reference is an ASCII data reference.

Stratum: The Stratum level of the selected input reference.

Mode: The mode of NTP operation, where:

Client: Indicates a Client/Server relation used when communicating with another reference that is configured as a "Server".

INIT: Indicates the NTP mode of the reference has not yet been identified.

STEP: Indicates an initial time correction has been applied.

Symmetric Active: Indicates the listed reference is configured in SecureSync as an "NTP Peer" (Refer to Section *3.18.3*).

Symmetric Passive: Indicates the listed reference is configured in SecureSync as an "NTP Server" (Refer to Section *3.18.3*).

Type: "local" indicates NTP generated internal to SecureSync. "Unicast" indicates NTP received over the network.

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 Interval: How often SecureSync is polling this NTP reference for its time.

Reach: An octal counter that indicates how many of the last eight polls of the NTP server were successful (a reach value of "377" indicates all eight of the last eight polls were successful).

NOTE: If the Reach value remains at "0" for a longer duration than the displayed "Poll Interval", NTP may not be running in SecureSync, there may be a network issue between SecureSync and the other NTP reference or the configured reference is not able to provide NTP packets to SecureSync.

Delay: The measured one-way delay between SecureSync and its selected reference.

Offset: The measured time difference between SecureSync and its selected reference.

Jitter: Variance in the reference inputs time from one poll to the next.

NTP Reference Status: This table provides all of the same information as the Selected Reference Status table, but in addition to the selected reference, it also lists all of the other configured Peers and Servers that SecureSync has available to choose from as its reference.

4.2.6 Status / Power Page

The Power status page displays the same information as the Power section of the **Status / Inputs** page. This page indicates whether AC power and DC power are currently present. "OK" (Green) indicates power is present and ALARM (Red) indicates the power is not present.

If the status displayed for either the AC or DC fields is red (Alarm), refer to Section *2.4* for information on connecting AC and/or DC input power.

4.2.7 SNMP Traps

If the network has one or more SNMP Managers available, SecureSync status can also be remotely monitored with SNMP Traps, as desired. SecureSync supports SNMP, including the ability to send SNMP Traps which include status variables (varbinds) when these Traps occur. Refer to Section *3.20* for more information on configuring SNMP and SNMP Traps.

Section 5: SecureSync Logs

SecureSync generates log files for several categories, including **General Settings**, **System**, **Event**, **Alarms**, **Timing**, **GPS Qualification**, **Oscillator**, **Journal**, and **Update**. These logs are available from the SecureSync web interface via the **Setup / Logs** page. A tab is available for each type of log (however, the Authentication and NTP logs have no available configuration options).

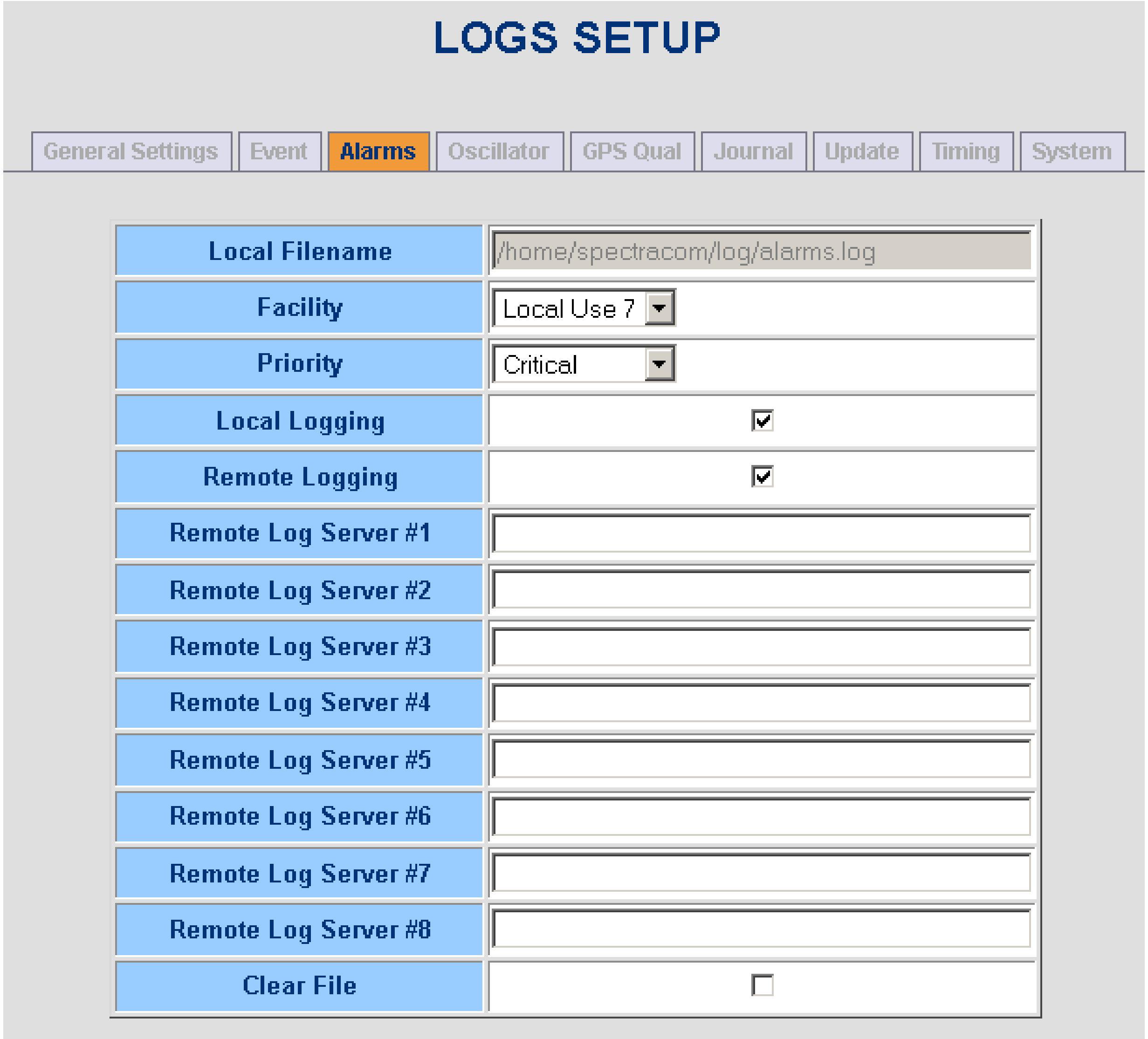
The SecureSync logs by default are all stored internally. With the exception of the Authentication and NTP logs, all logs can also be configured not to be stored internally, if desired). The log entries for these same logs can also be configured to be automatically sent to a Syslog Server for external 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 **Setup / Logs** page.

NOTE: For each type of log, entries appear with the most recent events first (i.e., in reverse chronological order, starting from the top).

The **General Settings** tab allows all of the log files to be deleted at one time. To delete all of the internal log files, enable this option and click Submit. If desired, each of the internal logs can also be individually deleted in their respective tab.

NOTE: The “Clear File” feature does not delete any of the logs that have been sent to and stored in a Syslog server.

Each of the other tabs (such as System, Event, Alarms, etc) provides the configuration options for the respective logs. Each tab includes the ability to delete the stored log, or configure the log to be stored internally and/or sent to a Syslog server (refer to Figure 5-1).



Local Filename	/home/spectracom/log/alarms.log
Facility	Local Use 7
Priority	Critical
Local Logging	☑
Remote Logging	☑
Remote Log Server #1	
Remote Log Server #2	
Remote Log Server #3	
Remote Log Server #4	
Remote Log Server #5	
Remote Log Server #6	
Remote Log Server #7	
Remote Log Server #8	
Clear File	□

Figure 5-1: Logs Setup page

The following log configuration options are common across all log types / tabs:

Local Filename: Displays where the log file is stored inside SecureSync.

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.

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.

> **Important 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. Table 5-1 displays 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 5-1: Factory Default Facility and Priority codes

Local Logging: Enable or disable this particular log being stored inside SecureSync. When this box is checked, the log will be stored in SecureSync.

Remote Logging: Configure the desired Syslog servers. When this box is checked, the particular log will be sent to a Syslog server.

Remote Log Server: Address(es) of the Syslog server(s) to send the logs to when "Remote Logging" is selected (the log files can be sent to up to five different Syslog servers).

Clear File: Allows the contents of this particular log to be deleted. Select this box and then hit Submit to delete this log's contents.

All of the available internal logs can be viewed from the **Tools / Logs** page. This page contains a tab for each available internal log. As long as the log is configured for Local Logging, the log data will be internally stored and displayed from its respective tab.

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.

NOTE: The "time" of all log entries will be in UTC, Local, TAI or GPS time, as configured in the "Timescale" field that is located in the System Time Setup page (**Setup / Time**

Management). Refer to Section 3.11.1 for information on configuring the System Timescale).

The information displayed for each log type is detailed herein.

5.1.1 System Log

Displays log entries related to the Timing system (KTS) events, and daemon events (such as the Alarms, Monitor, Notification, or SNMP daemons starting or stopping, etc).

"Updating UTC-GPS Offset value from 0 to 15": UTC is being offset by this value to account for the time differences between the UTC and GPS timescales.

5.1.2 Event Log

Displays log entries related to GNSS reception status changes, Sync/Holdover state changes, SNMP traps being sent, etc. Details for example event log entries include the following:

"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 16 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.

5.1.3 Alarms Log

Displays log entries for the KTS Timing engine (Kramden Timing System). Details for example entries include the following:

“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 16 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.

5.1.4 Authentication Log

Displays log entries for authentication events (e.g., unsuccessful login attempts, an incorrect password was entered, etc.) that are made to SecureSync's command line interfaces (such as the front panel setup port, telnet, SSH, FTP, etc).

5.1.5 Timing Log

Displays log entries related to Input reference state changes (for example, IRIG input is not considered valid), antenna cable status.

"GR 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.

5.1.6 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. 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.

5.1.7 Oscillator Log

Displays log entries related to oscillator disciplining. Provides the calculated frequency error periodically while synchronizing to a reference.

5.1.8 Journal Log

Displays log entries created for all configuration changes that have occurred (such as creating a new user account, for example).

5.1.9 Update Log

Displays log entries related to software updates that have been performed.

5.1.10 NTP Log

The NTP log displays operational information about the NTP daemon. Entries in this log include indications for when NTP was synchronized to its configured references (e.g., it became a Stratum 1 time server), stratum level of the NTP references, etc.

“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 16 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 can’t 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).

Section 6: Software Upgrades & License Installation

6.1 Software Upgrades

Spectracom periodically releases new versions of software for SecureSync as well as other products we offer. SecureSync software updates are offered for free and made available for download from the Spectracom website.

To download software updates for your SecureSync as they become available, please visit www.spectracomcorp.com, and from the website navigation menu select **Support → Software**. You can also register your email address to receive automatic notification of software updates. Refer to Section *2.13*.

Once an available software update has been downloaded from the Spectracom website, the update files can simply be transferred to the SecureSync using either a web browser via HTTPS on the **Tools / "Upgrade/Backup"** page, or the files can be transferred via FTP or SCP/SFTP.

When using the web interface to transfer the files from a PC to the SecureSync, the software update begins after the files have been transferred. Or, if the files are manually transferred using FTP or SFTP, the update can be delayed until the next time the SecureSync is either rebooted or power cycled. The update process occurs automatically with no user interaction required to the **`/home/spectracom`** directory. Multiple files can be uploaded to the unit at one time.

After the update file is uploaded to the SecureSync, the update can be applied on the **Tools / "Upgrade/Backup"** page by selecting the file in the "**Update File**" pulldown, selecting "**Update System**", and clicking **Submit**. At this point, the system will be analyzed against the files in the update. Any system element with a newer version of software in the update file will be updated.

To "roll back" system elements to an earlier version, select the older Update file in the "**Update File**" pulldown, select both "**Update System**" and "**Force Update**", and click **Submit**. All system elements will be "forced" to the version in the update file.

To delete a previously uploaded update file, select the file in the "**Update File**" pulldown, select "**Delete Update File**", and click **Submit**. Note that "**Delete Update File**" and "**Update System**" cannot be selected at the same time.

SecureSync will save system configuration across upgrades, but will not save other information. In particular, update files may not be retained after a successful update.

To erase ALL configuration information and restore the unit to the factory clean state, an update file must be loaded on the unit. Select "**Update System**", "**Force Update**", and "**Restore Factory Configuration**", and click **Submit**. 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.

The versions of software currently installed in SecureSync can be found on the **Tools / Versions** page. This page displays the software versions for the main SecureSync unit as well as the versions of software for any installed option modules.

The "**Archive Software Version**" option in the "**System Version**" table contains the high level referenced software version that all other versions of software are based on. The **Tools / "Upgrade/Backup"** page, **Software Upgrade** tab also displays the currently installed "**Archive Version**". This tab is also used for performing software upgrades where the upgrade files were transferred to the SecureSync using FTP, SFTP or SCP.

6.2 License Installation

Software options available for SecureSync have to be enabled by a license installation on the product. The license installation is made in the same way than a software upgrade. A file has to be uploaded into the product and then installed.

License files are archive files with a **`tar.gz`** extension. They could contain multiple licenses for multiple products.

Once the file is uploaded to in the product as described in the software upgrade above, select the file in the "**Update File**" pulldown. Then check both "**Update system**" and "**Force Update**", and click Submit.

Licensed software options currently installed can be found on the **Tools / Versions** page.

Section 7: Day-to-Day Operation

Operation of the SecureSync is relatively intuitive and requires little operator intervention during normal network activities.

7.1 Leap Second Occurrence

7.1.1 Reasons for a Leap Second Correction

A Leap Second is an intercalary, one-second adjustment that keeps broadcast standards for time of day close to mean solar time. Leap seconds are necessary to keep time standards synchronized with civil calendars, the basis of which is astronomical. They are used to keep 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.

The SecureSync can be alerted of impending leap seconds by any of the following methods:

1. 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.

2. Input references other than GNSS – Some of the other available input references also contain pending Leap Second notification in the data streams that can be read by SecureSync.

3. Manual user input – SecureSync can be manually configured by a user 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 manually entered from the **Setup / Time Management** page → "**Set Leap Second**" section. Configurable Leap Second options are as follows:

Leap Second Offset: Select the desired time correction, in seconds. Selectable values include: **-1**, **+0**, and **+1** (Normally, "+1" is the value to be selected). To clear or reset a previously set leap second offset value, select the **+0** value, then click "Submit".
At Date (DOY/YYYY): Enter the date of the desired Leap second to occur. The format is the Day of the Year (1 though 365) / the year of the change to occur.
At Time (HH:MM:SS): Enter the time of the desired Leap second to occur. The format is the hours, minutes, seconds (most leap seconds are asserted at 23:59:59).

7.1.2 Leap Second Alert Notification

The 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 having a 'L' rather than a ' ' (space) character 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. The 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.

7.1.3 Sequence of a Leap Second Correction Being Applied

The following is the time output sequence that the SecureSync will utilize to apply the Leap second at UTC midnight (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 leap second:

56, 57, 58, 59, 60, 0, 1, 2, 3, …

B) Sequence of seconds output when removing Leap seconds:

56, 57, 58, 0, 1, 2, 3, 4, …

Section 8: Option Modules

Spectracom offers numerous optional module cards for the SecureSync, allowing you to customize and tailor the SecureSync platform to suit your specific requirements, environment, or applications. This section contains technical details for available option module cards, and information regarding configuration and usage that can be used after installation.

Module P/N	Description	Refer to Section
1204-01, 1204-03	1PPS Frequency Input (TTL levels, RS-485 levels)	8.1.1, 8.1.9
1204-02, 1204-04	ASCII Time Code Modules (RS-232, RS-485)	8.2.1, 8.2.2
1204-05, 1204-27	IRIG Input / Output (BNC or Fiber)	8.3
1204-06	Gigabit Ethernet (3X, 10/100/1000 Base-T)	8.4
1204-08, 1204-0C, 1204-1C, 1204-26	(3X) Frequency Output (1, 5, 10 MHz)	8.5
1204-09, 1204-0A	T1 / E1 (75 Ω, 100 / 120 Ω)	8.6
1204-0B	RS-485 Communication Module	8.7
1204-1D, 1204-24	STANAG Input (2X, non-isolated or isolated)	8.8
1204-11, 1204-25	STANAG Output (2X, non-isolated or isolated)	8.9
1204-0F	Relay Outputs	8.10
1204-10, 1204-1B	HAVE QUICK Single-ended, HAVE QUICK Differential	8.11
1204-12	Precision Time Protocol (PTP)	8.12
1204-14	CTCSS / Data Sync / Data Clock	8.13
1204-15, 1204-1E	Four IRIG Output (BNC or Fiber)	8.14
1204-17	Square Wave Out	8.15
1204-18, 1204-19, 1204-21, 1204-2B	1PPS Output (TTL, 10V, RS-485, Fiber)	8.16.2, 8.16.3
1204-23	Event Broadcast	8.17
1204-28, 1204-2A	1PPS Input/Output (BNC or Fiber)	8.18
1204-2E	Failover Module	8.19
1204-29	HAVE QUICK Input/Output	8.20

NOTE: Contact sales@spectracomcorp.com for general inquiries regarding option module card functionality or availability, or for information regarding any option cards you would like to add. Before installing any new option module cards, review the "*SecureSync Option Card Installation Guide*" document for detailed option card installation steps.

8.1 Models 1204-01, 1204-03: 1PPS/Frequency Input

8.1.1 Model 1204-01: 1PPS/Freq Input (TTL Levels) Module

The 1PPS output module provides input reference interfaces to the timing system and provides an additional 1PPS output on a BNC connector.

Inputs/Outputs:	(1) 1PPS Input, (1) Freq Input (1) 1PPS output
Signal Type And Connector:	TTL/Sine (BNC into 50 Ω)
Input Signal Jitter:	< +/- 500 ns to achieve oscillator lock, < +/- 50 ns to achieve system performance
Maximum Number of Cards	6

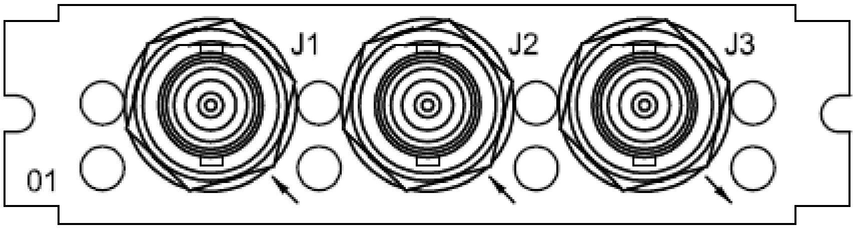


Figure 8-1: Model 1204-01 Option Card Rear Plate

8.1.2 FREQ Input Specifications

Signal Type And Connector:	Sinewave (BNC)
Detected Level:	+13dBm to -6dBm
Frequency setting:	1 KHz - 10 MHz in 1 Hz steps

8.1.3 1PPS Input Specifications

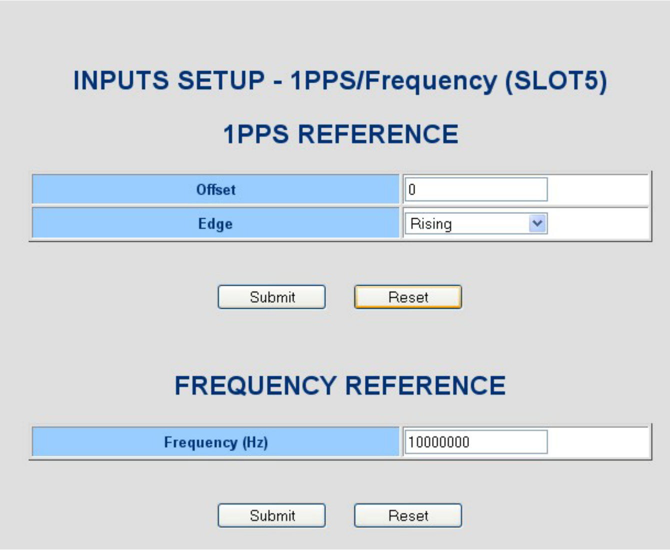
Input impedance:	50 Ω
Minimum Pulse Width detected:	100ns.
Programmable phase shift:	±5ns to 500ms with 5ns resolution
1PPS Input Minimum Pulse Width detected:	100ns

8.1.4 1PPS Output Specifications

Signal Type And Connector:	TTL level (BNC)
Output Load impedance:	50 Ω
Rise time to 90% of level:	<10ns
Programmable pulse width:	100ns to 500ms with 20ns resolution
Absolute phase error:	±50ns (1σ)
Programmable phase shift:	±5ns to 500ms with 5ns resolution

8.1.5 1PPS Input Setup / Configuration

To manage the 1PPS input (BNC Connector **J2** on the 1PPS module), navigate to the **Setup / Inputs** page and select the Slot labeled "**1PPS/Freq**". Refer to the following figure:



INPUTS SETUP - 1PPS/Frequency (SLOT5)

1PPS REFERENCE

Offset	0
Edge	Rising

FREQUENCY REFERENCE

Frequency (Hz)	10000000

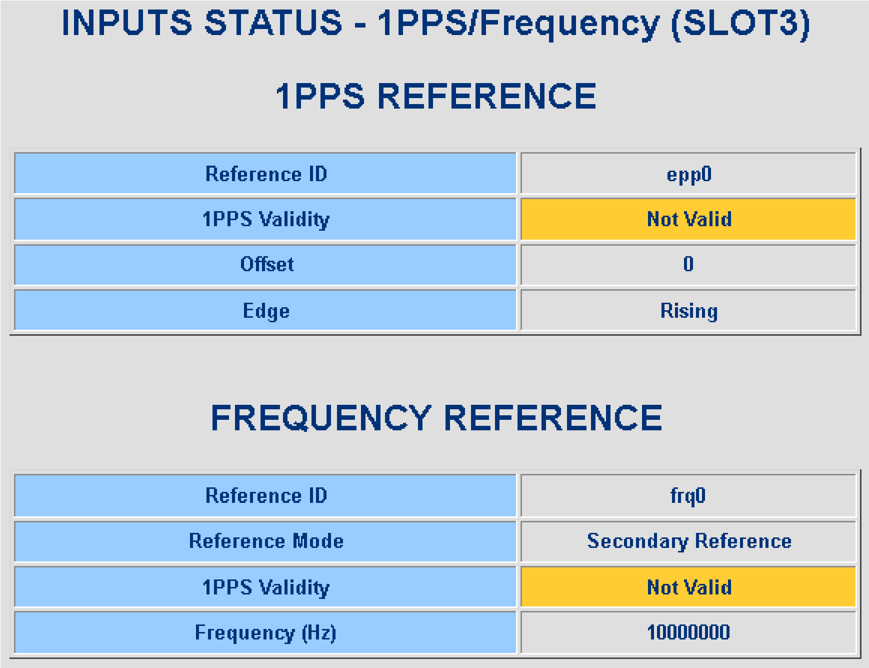
Figure 8-2: 1PPS and Frequency Inputs Setup page

Offset: It is possible to add an offset to the input signal (to account for cable delays), with a resolution of 20ns and a positive or negative value of 500ms maximum.

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).

8.1.6 1PPS Status Pages

To view 1PPS input status, navigate to the **Status / Inputs** page and select the Slot labeled “**1PPS/Freq**”. The 1PPS Input signal is analyzed and an absence of the signal triggers a “Not Valid” indication. Refer to the following figure.



INPUTS STATUS - 1PPS/Frequency (SLOT3)

1PPS REFERENCE

Reference ID	epp0
1PPS Validity	Not Valid
Offset	0
Edge	Rising

FREQUENCY REFERENCE

Reference ID	frq0
Reference Mode	Secondary Reference
1PPS Validity	Not Valid
Frequency (Hz)	10000000

Figure 8-3: 1PPS and Frequency Input Status

1PPS (Input) Reference status information displayed on this page includes the following:

Reference ID: Name used to represent this 1PPS input reference in the Reference Priority table (refer to Section *3.17* for more information on the Reference Priority Input table 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.

Offset: Displays the configured 1PPS offset values.

Edge: Displays the selected Edge (rising of falling) of the 1PPS input that defines the on-time point.

8.1.7 FREQ Input

To manage the Frequency Input (BNC Connector **J1** on the 1PPS module), navigate to the **Setup / Inputs page** and select the Slot labeled “**1PPS/Freq**”. Available options are as follows:

Reference Mode: Used to control how the reference mode operates in determining its validity.

Secondary: 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.

Primary: Allows the frequency reference to be valid based solely on its own presence.

Frequency: Used to configure the frequency (in Hertz) of the input signal. The available Frequency range is 1 KHz - 10 MHz in 1 Hz steps.

The input frequency is measured versus internal frequency and compared to the setup value. If the discrepancy is larger than 1 kHz, 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.

The "**Frequency Reference**" (Input) values displayed on the **Status / Inputs / 1PPS** page include the following:

Reference ID: Name used to represent this 1PPS input reference in the Reference Priority table (Refer to Section *3.17* for more information on the Reference Priority Input table).

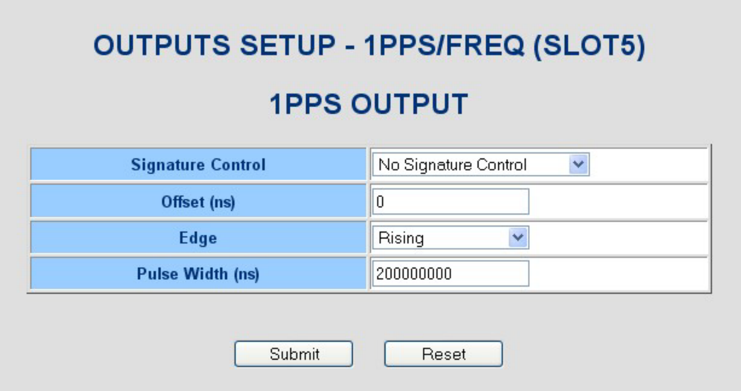
1PPS Validity: Indicates "OK" (green) if the 1PPS input signal is present and valid. Indicates "Not Valid" (orange) if the 1PPS input signal is either not present or is not considered valid.

Offset: Displays the configured 1PPS offset values (as configured from the **Setup / Inputs** page).

Frequency: Displays (in Hertz) the configured frequency of the input frequency signal.

8.1.8 1PPS Output

To manage the 1PPS Output (BNC Connector **J3** on the 1PPS module), navigate to the **Setup / Outputs** page and select the Slot labeled "**1PPS/Freq**". Available options are as follows:



OUTPUTS SETUP - 1PPS/FREQ (SLOT5)

1PPS OUTPUT

Signature Control	No Signature Control
Offset (ns)	0
Edge	Rising
Pulse Width (ns)	200000000

Figure 8-4: 1PPS Output Setup page

Signature Control: Used to control when the 1PPS output signal will be present. This function allows the modulation to stop in certain situations.

Output Always Enabled: 1PPS output is present, even when SecureSync is not synchronized to its references.

Output Enabled in Holdover: 1PPS output is present unless the SecureSync is not synchronized to its references (modulation is present while in the Holdover mode).

Output Disabled in Holdover: 1PPS output is present unless the SecureSync references are considered not qualified and invalid (modulation *is not* present while in the Holdover mode).

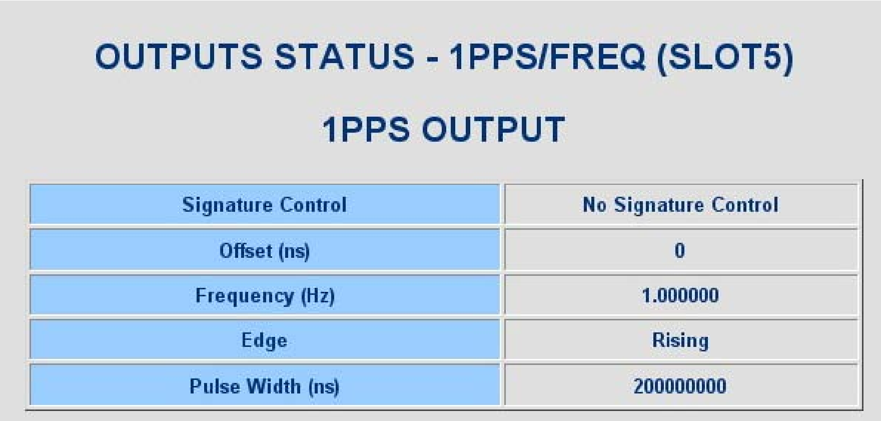
Output Always Disabled: No 1PPS output is present, even if any SecureSync input references are present and considered qualified.

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.

To view current status and configuration information of the 1PPS output signal, navigate to the **Status/Outputs** page and select the Slot labeled "**1PPS/Freq**".



OUTPUTS STATUS - 1PPS/FREQ (SLOT5)

1PPS OUTPUT

Signature Control	No Signature Control
Offset (ns)	0
Frequency (Hz)	1.000000
Edge	Rising
Pulse Width (ns)	200000000

Figure 8-5: 1PPS and Frequency Output Status page

Information displayed on this page includes the following:

Signature Control: Displays the current configuration of Signature Control.

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.

Frequency: Indicates the configured frequency of the 1PPS output signal.

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.

8.1.9 Model 1204-03: 1PPS/Freq Input (RS-485 Levels) Module

Inputs/Outputs:	(1) 1PPS Input, (1) Freq Input (1) 1PPS All input and output signals are RS-485 compatible.
Signal Type And Connector:	Balanced RS-485 (3.8 mm terminal block)
Input Signal Jitter:	< +/- 500 ns to achieve oscillator lock, < +/- 50 ns to achieve system performance
Maximum Number of Cards:	6

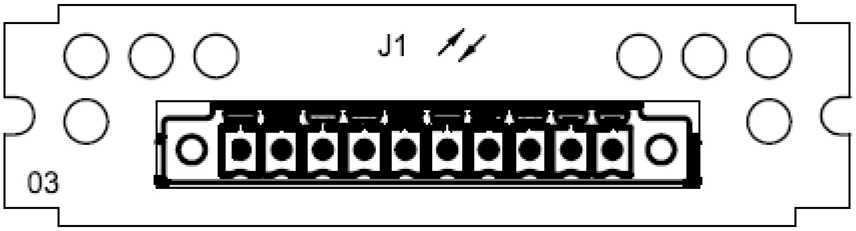


Figure 8-6: Model 1204-03 Option Module Card Rear Plate

NOTE: The operation of the Model 1204-03 1PPS/Freq Input module (RS-485 levels) is similar to the operation of the Model 1204-01 1PPS/Freq Input (TTL levels) option module. Refer to Section 8.1 for configuration information for the Model 1204-03 (RS-485) option module card.

Pin Assignment

Pin No.	Signal Name	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 8-1: Model 1204-03 1PPS/Freq Input Module Card Pin Assignment

8.2 Models 1204-02, 1204-04: ASCII Time Code

8.2.1 Model 1204-02: ASCII Time Code (RS-232)

Inputs / Outputs:	(1) Input, (1) Output
Signal Type and Connector:	Connector J1 - (RS-232 Output) RS-232 DB9F Connector J2 - (RS-232 Input) RS-232 DB9M
Accuracy:	+/- 100-1000 microseconds (format dependant)

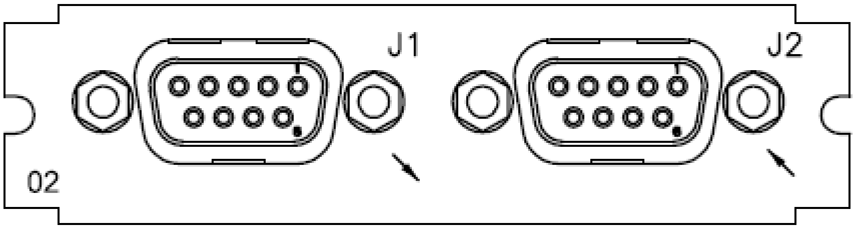


Figure 8-7: Model 1204-02 Option Module Card Rear Plate

The ASCII Time Code Module (RS-232) provides one RS-232 input interface and one RS-232 output interface for Asynchronous Serial signal including date and time information. The input and output Data Formats are selected among predefined formats.

The ASCII Time Code Module (RS-232) consists of two ports. The ASCII input connector (J2) is a DB9 Male port and the ASCII output connector (J1) is a DB9 Female port. The ASCII input port (J2) allows a serial data interface between an ASCII time generator (such as a Spectracom Model 9300 appliance or another SecureSync) to be an available Time and 1PPS input reference for SecureSync synchronization (in conjunction with, or in lieu of, other available inputs, such as GNSS and/or IRIG).

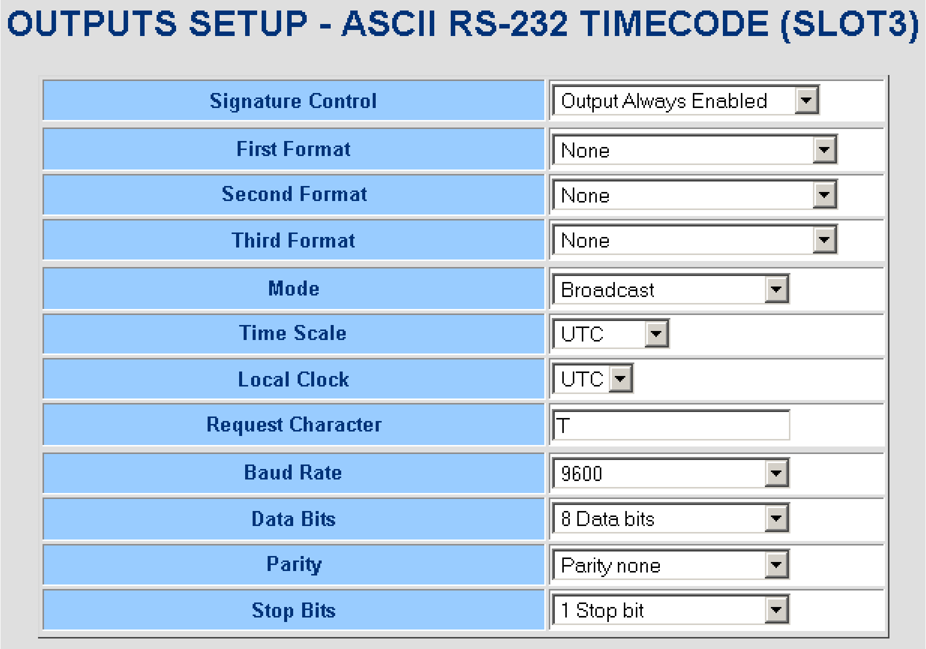
Each DB9 connector includes both TX (Transmit) and RX (Receive) signals. The RX signal on an output interface is used for triggering the output ASCII message output when a configured character is received from the peripheral device.

The ASCII output port (J1) 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 can accept an ASCII RS-232 input data stream for either their external time synchronization or for data processing. Refer to *11.1* for a description of all of the available formats.

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 point for the second and third messages 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.

8.2.1.1 ASCII Time Code Output Setup (RS-232)



OUTPUTS SETUP - ASCII RS-232 TIMECODE (SLOT3)

Signature Control	Output Always Enabled
First Format	None
Second Format	None
Third Format	None
Mode	Broadcast
Time Scale	UTC
Local Clock	UTC
Request Character	T
Baud Rate	9600
Data Bits	8 Data bits
Parity	Parity none
Stop Bits	1 Stop bit

Figure 8-8: ASCII RS-232 Time Code Output Setup

To manage the ASCII data output ports, navigate to the **Setup / Outputs** page and select the Slot labeled "**ASCII RS-232 TIMECODE**". Available options are as follows:

Signature Control: Signature Control controls when the selected ASCII data output format will be present.

Output Always Enabled: The ASCII data output format is present, even when SecureSync is not synchronized to its references.

Output Enabled in Holdover: The ASCII data output format is present unless SecureSync is not synchronized to its references (The 1PPS output is present while in the Holdover mode).

Output Disabled in Holdover: The ASCII data output format is present unless the SecureSync references are considered not qualified and invalid. (The 1PPS output is not present while in the Holdover mode).

Output Always Disabled: The ASCII data output format is not present, even if any SecureSync references are present and considered qualified.

First Format: Selects either the first of up to three or the only format message to be outputted.

NOTE: Refer to 11.1 for a description of all available formats.

Second Format: Selects the second consecutive format message to be outputted. Select "None" if only one output format is desired.

Third Format: Selects the third consecutive format message to be outputted. Select "None" if only one output format is desired.

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.

Time Scale: Used to select the time base for the incoming IRIG 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, TAI (Temps Atomique International), GPS and Local. UTC is also referred to as ZULU time. GPS is the raw GPS time as transmitted by the GNSS satellites (as of September, 2013, this is currently 16 seconds ahead of UTC time). If GPS or TAI time is used, then the proper timescale offsets must be set on the **Setup / Time Management** page. (Refer to Section 3.11.1 for more information). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

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. Refer to Section 3.11.3 for more information on Local Clocks.

Baud Rate: Determines the speed that the output port will operate at.

Data Bits: Defines the number of Data Bits for the output port.

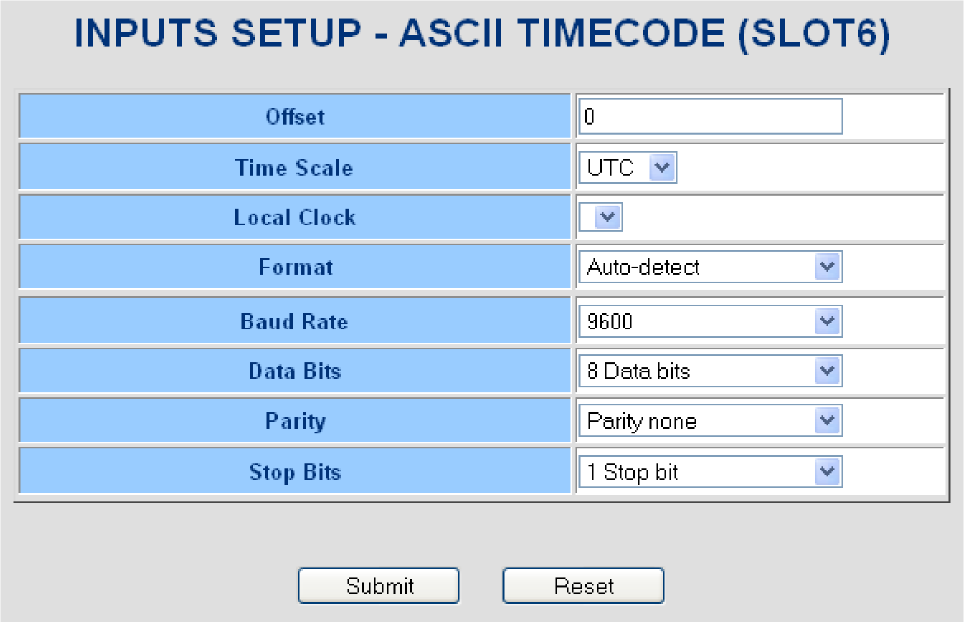
Parity: Configures the parity checking of the output port.

Stop Bits: Defines the number of Stop Bits for the output.

Pin Number	Signal Name	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
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 8-2: Output DB-9 Connector Pin-Out

8.2.1.2 ASCII Time Code Input Setup (RS-232)



INPUTS SETUP - ASCII TIMECODE (SLOT6)

Offset	0
Time Scale	UTC
Local Clock	
Format	Auto-detect
Baud Rate	9600
Data Bits	8 Data bits
Parity	Parity none
Stop Bits	1 Stop bit

Figure 8-9: ASCII RS-232 Time Code Input Setup

To manage the ASCII data input ports, navigate to the **Setup / Inputs** page and select the Slot labeled “**ASCII RS-232 TIMECODE**”. Available options are as follows:

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.

Time Scale: 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, TAI (Temps Atomique International), GPS and Local. UTC is also referred to as ZULU time. GPS is the raw GPS time as transmitted by the GNSS satellites (as of September, 2013, this is currently 16 seconds ahead of UTC time). If GPS or TAI time is used, then the proper timescale offsets must be set on the **Setup / Time Management** page. (Refer to Section *3.11.1*: *"Configuring the System Time Timescale"* for more information). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

> **Important 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.

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. Refer to Section *3.11.3*: *"Local Clock Setup"* for more information on Local Clocks.

Format: Configures the format message being provided to SecureSync's input port. Refer to *11.1* for a description of all of the available formats that can be accepted by SecureSync for its synchronization. *Note:* If "Auto-detect" is selected, SecureSync will attempt to identify the format of the incoming ASCII message.

Baud Rate: Determines the speed that the input port will operate at.

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.

Pin Number	Signal Name	Function
Top row of 5 pins		
1	PPS_IN	1PPS input
2	SERIAL_IN_RX	RS-232 Receive data
3	SERIAL_OUT_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 8-3: Input DB-9 Connector Pin-Out

8.2.1.3 ASCII Time Code Module Output Status (RS-232)

To view current output status and configuration information for this option module, navigate to the **Status / Outputs** page and select the Slot labeled **"ASCII RS-232 TIMECODE**".

The following information is displayed on this page:

Signature Control: Indicates whether Signature Control is enabled (Signature Control determines when the ASCII data stream will be enabled to be present).

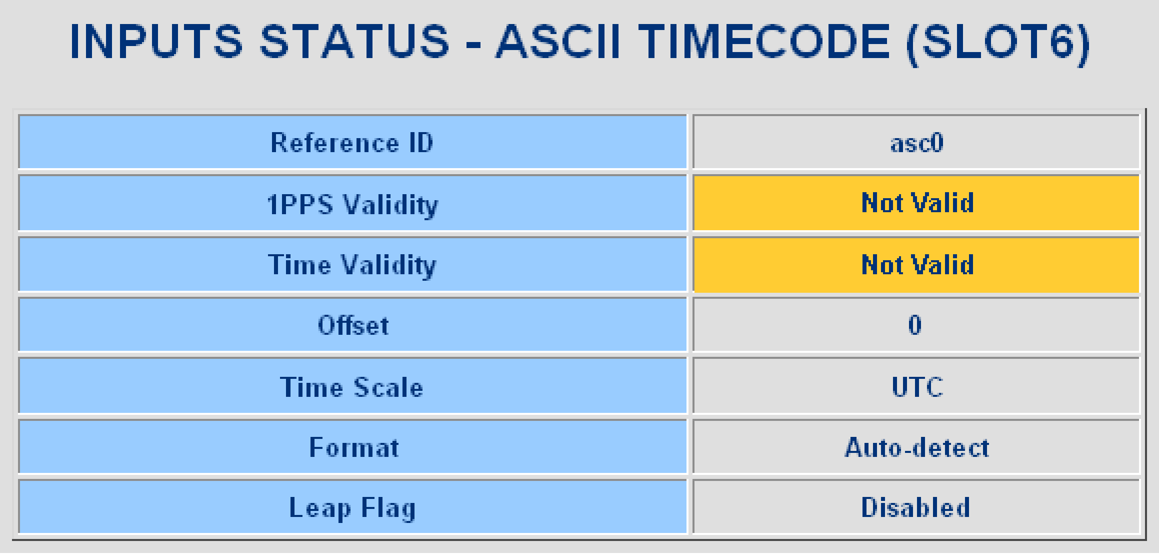
Format: Indicates the configured format of the ASCII time code input data stream.

Mode: The selected Mode determines if the data stream is broadcasted on a routine interval or is instead only provided when a configured request character is received from a peripheral device.

Time Scale: Indicates the configured timescale of the ASCII time code input data stream.

8.2.1.4 ASCII Time Code Module Input Status (RS-232)

To view current status and configuration information for the input of the ASCII module, navigate to **Status / Inputs** and select the Slot labeled "**ASCII RS-232 TIMECODE**".



INPUTS STATUS - ASCII TIMECODE (SLOT6)

Reference ID	asc0
1PPS Validity	Not Valid
Time Validity	Not Valid
Offset	0
Time Scale	UTC
Format	Auto-detect
Leap Flag	Disabled

Figure 8-10: ASCII RS-232 Time Code Input Status Page Example

The following information is displayed on this page:

Reference ID: Indicates the letters used in the Input Reference Priority table for this particular input reference.

1PPS Validity and Time Validity: Indicates whether the ASCII input data is present and considered valid 1PPS and time references. A green "OK" indicates a valid reference. An orange "Not Valid" indicates the reference is not considered valid.

Offset: Indicates the amount of configured time offset applied to the ASCII time code input data stream.

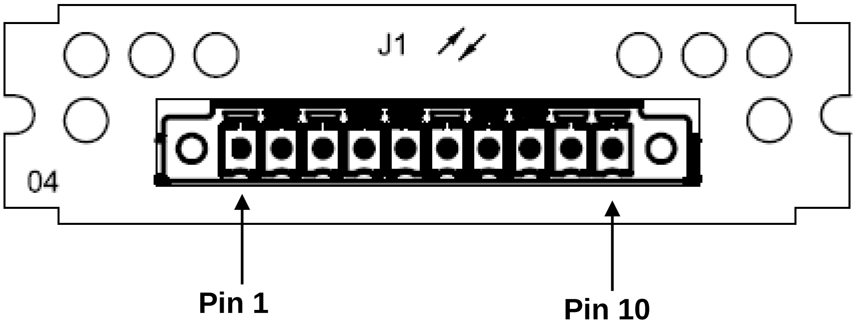
Time Scale: Indicates the configured timescale of the ASCII time code input data stream.

Format: Indicates the configured format of the ASCII time code input data stream.

Leap Flag: Displays whether the incoming data stream is indicating a pending leap second is to be added to the UTC timescale at the end of the month ("Enabled" indicates a leap second is to be applied to UTC timescale at the end of the month).

8.2.2 Model 1204-04: ASCII Time Code Module (RS-485)

Inputs / Outputs:	(1) Input, (1) Output
Signal Type and Connector:	(1) RS-485 terminal block for both Input and Output
Accuracy:	+/- 100-1000 microseconds (format dependant)



NOTE: Pin numbers for this card are arranged from Pin 1 to Pin 10, from left to right.

Figure 8-11: Model 1204-04 Option Module Card Rear Plate

The ASCII Time Code Module (RS-485) consists of one RS-485 input port and one RS-485 output port. The input and output connector is a shared terminal block connector. The ASCII input port (J1) allows a serial data interface between an ASCII time generator (such as a Spectracom Model 9300 series appliance or another SecureSync) to be an available Time and 1PPS input reference for SecureSync (in conjunction with or in lieu of other inputs, such as GNSS and/or IRIG).

The ASCII output port (J2) provides SecureSync with the ability to output a selected ASCII time code data stream that can be provided to peripheral devices (such as Spectracom wall display clocks) that can accept an ASCII RS-485 input data stream for their external time synchronization.

Pin Assignments

Pin Number	Signal Name	Function
1	SERIALTX_RS485+	+ RS-485 data output
2	SERIALTX_RS485-	- RS-485 data output
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	PPS_IN _RS485-	- 1PPS input

Table 8-4: Model 1204-04 RS-485 Terminal Block Connector Pinout

The ASCII Time Code Module (RS-485) provides one input interface and one output interface for Asynchronous Serial signal including date and time information. The input and output Data Formats are selected among predefined formats.

The ASCII Time Code Module (RS-485) consists of two ports. The ASCII input connector (J2) and the ASCII output connector (J1) are both terminal block connectors. The ASCII input port (J2) allows a serial data interface between an ASCII time generator (such as a Spectracom Model 9300 appliance or another SecureSync) to be an available Time and 1PPS input reference for SecureSync synchronization (in conjunction with, or in lieu of, other available inputs, such as GNSS and/or IRIG).

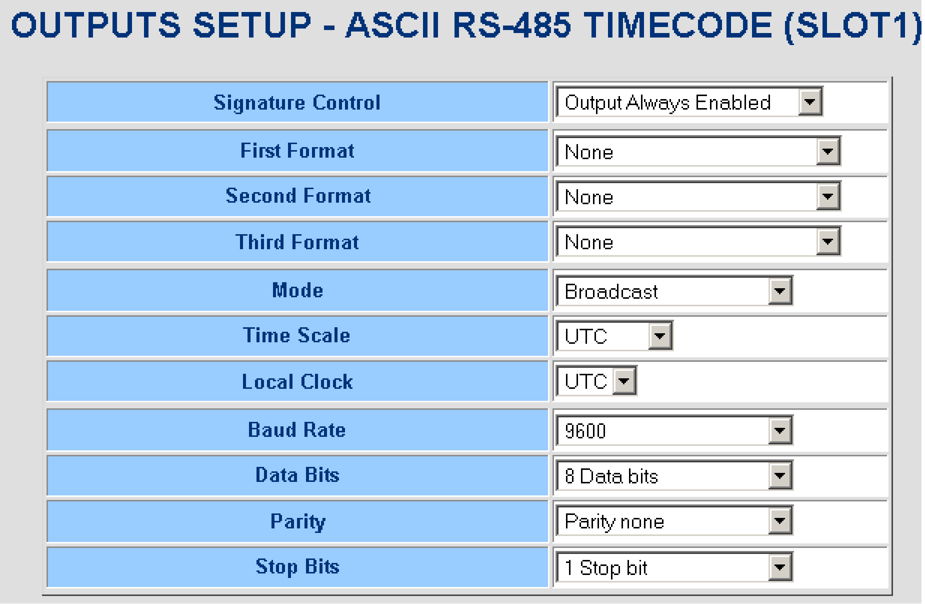
Each terminal block connector includes TX (Transmit) and RX (Receive) signals. The RX signal on an output interface is used for triggering the output ASCII message output when a configured character is received from the peripheral device.

The ASCII output port (J1) 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 that can accept an ASCII RS-232 input data stream for their external time synchronization.

When SecureSync is configured to output only one format message (the second and third formats configured as “None”), the 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 point for the second and third messages provided at the same time as the first message are disregarded. This unique capability allows SecureSync to be able to simultaneously provide multiple pieces of data from different selected messages.

An example of selecting multiple formats is selecting the NMEA GGA as the first message, NMEA RMC as the second format and NMEA ZDA as the third format. Depending on the setting of the Mode (which determines if the data streams are available every second or only 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 by the corresponding RMC message for that same second, followed 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.

8.2.2.1 ASCII Time Code Output Setup (RS-485)



OUTPUTS SETUP - ASCII RS-485 TIMECODE (SLOT1)

Signature Control	Output Always Enabled
First Format	None
Second Format	None
Third Format	None
Mode	Broadcast
Time Scale	UTC
Local Clock	UTC
Baud Rate	9600
Data Bits	8 Data bits
Parity	Parity none
Stop Bits	1 Stop bit

Figure 8-12: ASCII RS-485 Time Code Output Setup

To configure the ASCII data output ports, navigate to the **Setup / Outputs** page and select the Slot labeled “**ASCII RS-485 TIMECODE**”. Available options are as follows:

Signature Control: Signature Control controls when the ASCII data input format will be present.

> **Output Always Enabled:** The ASCII data input is present, even when SecureSync is not synchronized to its references.
>
> **Output Enabled in Holdover:** The ASCII data input is present unless SecureSync is not synchronized to its references (The ASCII output is present while in the Holdover mode).
>
> **Output Disabled in Holdover:** The ASCII data input is present unless the SecureSync references are considered not qualified and invalid. (The ASCII output is not present while in the Holdover mode).
>
> **Output Always Disabled:** The ASCII data input is not present, even if any SecureSync references are present and considered qualified.

First Format: Selects either the first of up to three or the only format message to be outputted.

> ***NOTE:*** Refer to Section 11.1 for a description of all available formats.

Second Format: Selects the second consecutive format message to be outputted. Select “None” if only one output format is desired.

Third Format: Selects the third consecutive format message to be outputted. Select “None” if only one output format is desired.

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.
>
> **On-time:** A format message is generated in sync with 1PPS after the configured request character has been received.
>
> **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, 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.

Time Scale: Used to select the time base for the incoming IRIG 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, TAI (Temps Atomique International), GPS and Local. UTC is also referred to as ZULU time. GPS is the raw GPS time as transmitted by the GPS satellites (as of September, 2013, this is currently 16 seconds ahead of UTC time). If GPS or TAI time is used, then the proper timescale offset values must be set on the **Setup / Time Management** page. (Refer to Section *3.11.1* for more information). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

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. Refer to Section *3.11.3* for more information on Local Clocks.

Baud Rate: Determines the speed that the output port will operate at.

Data Bits: Defines the number of Data Bits for the output.

Parity: Configures the parity checking of the port.

Stop Bits: Defines the number of Stop Bits for the output.

8.2.2.2 ASCII Time Code Input Setup (RS-485)

To configure the ASCII data input ports, navigate to the **Setup / Inputs** page and select the Slot labeled "**ASCII TIMECODE**". Configurable options are as follows:

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.

Time Scale: 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, TAI (Temps Atomique International), GPS and Local. UTC is also referred to as ZULU time. GPS is the raw GPS time as transmitted by the GNSS satellites (as of September, 2013, this is currently 16 seconds ahead of UTC time). If GPS or TAI time is used, then the proper timescale offsets must be set on the **Setup / Time Management** page. (Refer to Section *3.11.1* for more information). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

> **Important 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.

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. Refer to Section *3.11.3* for more information on Local Clocks.

Format: Defines the format message being provided to SecureSync's input port. Refer to Section *11.1* for a description of all of the available formats that can be accepted by SecureSync for its synchronization. Note: If "Auto-detect" is selected, SecureSync will attempt to identify the format of the incoming ASCII message.

Baud Rate: Determines the speed that the input port will operate at.

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.

8.2.2.3 ASCII Time Code Module Output Status (RS-485)

To view current output status and configuration information for this option module, navigate to the **Status / Inputs** page and select the Slot labeled "**ASCII RS-485 TIMECODE**".

The following information is displayed on this page:

Signature Control: Indicates whether Signature Control is enabled (Signature Control determines when the ASCII data stream will be enabled to be present).

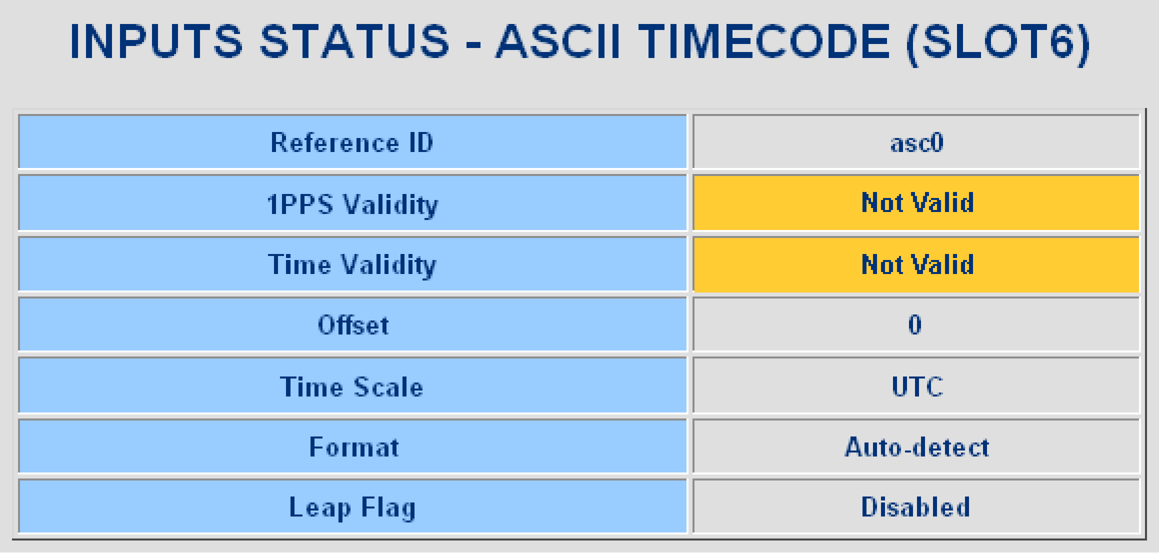
Format: Indicates the configured format of the ASCII time code input data stream.

Mode: The selected Mode determines if the data stream is broadcasted on a routine interval or is instead only provided when a configured request character is received from a peripheral device.

Time Scale: Indicates the configured timescale of the ASCII time code input data stream.

8.2.2.4 ASCII Time Code Module Input Status (RS-485)

To view current input status and configuration information for this option module, navigate to the **Status / Inputs** page and select the Slot labeled "**ASCII RS-485 TIMECODE**".



INPUTS STATUS - ASCII TIMECODE (SLOT6)

Reference ID	asc0
1PPS Validity	Not Valid
Time Validity	Not Valid
Offset	0
Time Scale	UTC
Format	Auto-detect
Leap Flag	Disabled

Figure 8-13: ASCII RS-485 Time Code Input Status Page

The following options are displayed on this page:

Reference ID: Indicates the letters used in the Input Reference Priority table for this particular input reference.

1PPS and Time Validity: Indicates whether the ASCII input data is present and considered valid 1PPS and time references. A Green "OK" indicates a valid reference. An Orange "Not Valid" indicates the reference is not considered valid.

Offset: Indicates the amount of configured time offset applied to the ASCII time code input data stream.

Time Scale: Indicates the configured timescale of the ASCII time code input data stream.

Format: Indicates the configured format of the ASCII time code input data stream.

Leap Flag: Displays whether the incoming data stream is indicating a pending leap second is to be added to the UTC timescale at the end of the month (“Enabled” indicates a leap second is to be applied to UTC timescale at the end of the month).

8.3 Model 1204-05, 1204-27: IRIG Input/Output Module

The IRIG Input/Output module provides SecureSync with one (1) IRIG input and two (2) 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.

8.3.1 IRIG Input Specifications (BNC Option)

Signal:	IRIG A, B, E, G or NASA-36, amplitude modulated sine wave (AM) or pulse-width-coded (DCLS).
AM Carrier:	IRIG B 1000 Hz, IRIG A and G 100 or 100
AM Signal Level:	500mV to 10V p-p (modulated 2:1 to 6:1).
DCLS Signal Level:	>10k Ω TTL
Connector:	AM and DCLS: BNC female

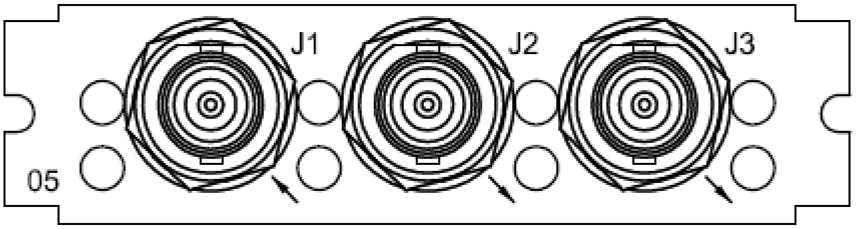


Figure 8-14: Model 1204-05 Option Module Card Rear Plate

8.3.2 IRIG Input Specifications (Fiber Optic Option)

Signal:	IRIG A, B, E, G or NASA-36, (DCLS only)
Operating Wavelength:	820/850 nm
Optical Minimum Sensitivity:	-25 dBm @ 820 nanometers
Fiber Optic Compatibility	50/125 µm, 62.5/125 µm multi-mode cable
Optical Connector:	ST

8.3.3 IRIG Output Specifications (Fiber Optic Option)

Signal:	IRIG A, B, E, G or NASA-36, (DCLS only)
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

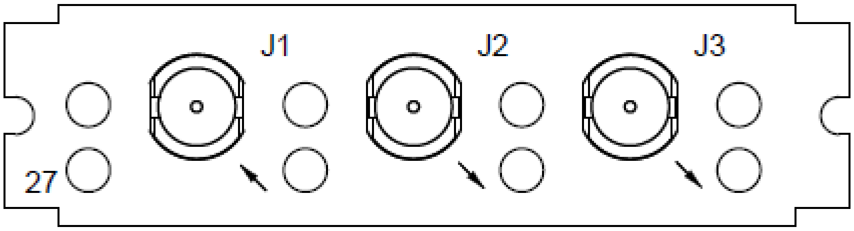


Figure 8-15: Model 1204-27 Option Module Card Rear Plate

IRIG Code Format Provided	Code Description
A000	IRIG A, DCLS, 1 kHz , BCD, CF and SBS
A001	IRIG A, DCLS, 1 kHz, BCD, CF
A002	IRIG A, DCLS, 1 kHz, BCD
A003	IRIG A, DCLS, 1 kHz, BCD and SBS
A004	IRIG A, DCLS, 1 kHz, BCD_{TOY}, BCD_{YEAR}, CF and SBS
A130	IRIG A, AM, 10kHz, BCD, CF and SBS
A131	IRIG A, AM, 10kHz, BCD, CF
A132	IRIG A, AM, 10kHz, BCD
A133	IRIG A, AM, 10kHz, BCD and SBS
A134	IRIG A, AM, 10kHz, BCD_{TOY}, BCD_{YEAR}, CF and SBS
B000	IRIG B, DCLS, BCD, CF and SBS
B001	IRIG B, DCLS, BCD, CF
B002	IRIG B, DCLS, BCD
B003	IRIG B, DCLS, BCD and SBS
B004	IRIG B, DCLS, BCD_{TOY}, BCD_{YEAR}, CF and SBS
B120	IRIG B, AM, 1 kHz , BCD, CF and SBS
B121	IRIG B, AM, 1 kHz , BCD, CF
B122	IRIG B, AM, 1 kHz, BCD
B123	IRIG B, AM, 1 kHz, BCD and SBS
B124	IRIG B, AM, 1 kHz , BCD_{TOY}, BCD_{YEAR}, CF and SBS
G001	IRIG G, DCLS, BCD, CF

G002	IRIG G, DCLS, BCD
G005	IRIG G, DCLS, BCD_{TOY}, BCD_{YEAR} and CF
G141	IRIG G, AM, 100kHz, BCD,CF
G142	IRIG G, AM, 100kHz, BCD
G145	IRIG G, AM, 100kHz, BCD_{TOY}, BCD_{YEAR} and CF

Table 8-5: Accepted IRIG Input Reference Formats

IRIG is an acronym for Inter-Range Instrumentation Group. In the late 1950s, this group created a series of time code standards suitable for use with recording oscillographs, magnetic tape, and real-time transmission.

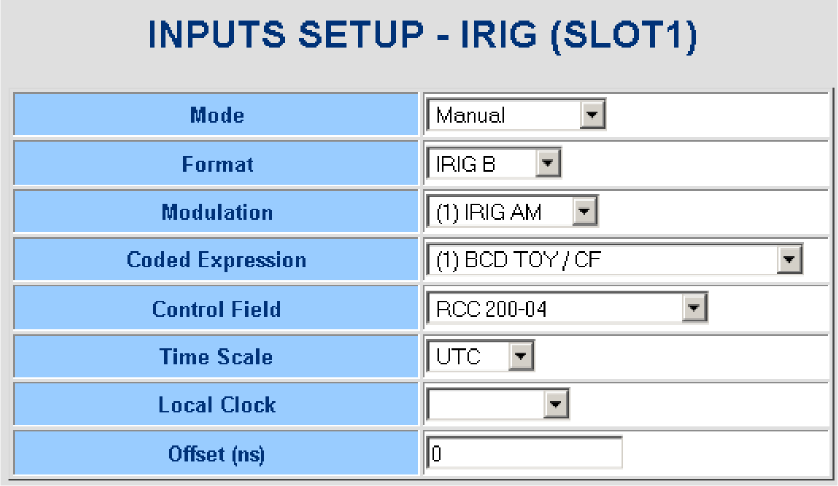
IRIG input is connector **J1** on the SecureSync's IRIG Input module. Connect the IRIG time source generator to connector **J1** for IRIG time code input.

8.3.4 IRIG Input Setup

From the IRIG Input setup page, the user may configure the source year to be used with the IRIG input time code. By default, the "year" fields in the IRIG message are ignored and a user-defined value is used.

NOTE: 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, SecureSync must be restarted from the NTP web interface page (or the SecureSync rebooted) for the New Year value to take effect.



INPUTS SETUP - IRIG (SLOT1)

Mode	Manual
Format	IRIG B
Modulation	(1) IRIG AM
Coded Expression	(1) BCD TOY / CF
Control Field	RCC 200-04
Time Scale	UTC
Local Clock	
Offset (ns)	0

Figure 8-16: IRIG Input Page

Mode: Determines the IRIG input mode selection.

Manual: SecureSync will not attempt to detect the format. It must be manually defined. Manual Mode is the default enabled mode and uses the following settings:

Format: IRIB G
Modulation: (1) IRIG AM
Coded Expression: (1) BCD TOY/CF
Control Field: RCC 200-04
Auto Detection: SecureSync will attempt to automatically determine the IRIG input format.

Format: Sets the formatting of the IRIG input signal, as defined by the IRIG generator time source. The available choices are IRIG A, B, G, E and NASA-36.

NOTE: "Automatic" and "Unknown" may also be listed values but shouldn't be selected as input selection.

Modulation: Configures the type of input signal modulation.

IRIG DCLS is a TTL (Phase) modulated signal.
IRIG AM is an amplitude modulated signal.

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

Control 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:

RCC 200-4: IRIG spec 200-04 specified a location for year value, if included in this field.
IEE 1344: Control Field contains year, Leap Second and DST information.
Spectracom Format: Year is included in Control Field but not in the same location as RCC-2004 output (year is offset by one position).
Spectracom FAA Format: A unique IRIG output Control Field that contains satellite lock status and time error flags.
NASA-36: A variant of IRIG B.

NOTE: If the **Control Field** value is changed, the **Format** and **Coded Expression** change to the default values for the given **Control Field** value. The user can only change the **Format** field and **Coded Expression** field to allowed values for the **Control 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. If no IRIG Format is detected, the value displayed will be "UNKNOWN".

Time Scale: Used to select the time base for the incoming IRIG 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, TAI (Temps Atomique International), GPS and Local. UTC is also referred to as ZULU time. GPS is the raw GPS time as transmitted by the GNSS satellites (as of September, 2013, this is currently 16 seconds ahead of UTC time). If GPS or TAI time is used, then the proper timescale offsets must be set on the **Setup / Time Management** page. (Refer to Section *3.11.1* for more information). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

> **Important Note:** The Timescale of the IRIG input (as configured in the IRIG generator) must be set correctly, especially if other input references are enabled. Failure to configure the Timescale of the IRIG 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.

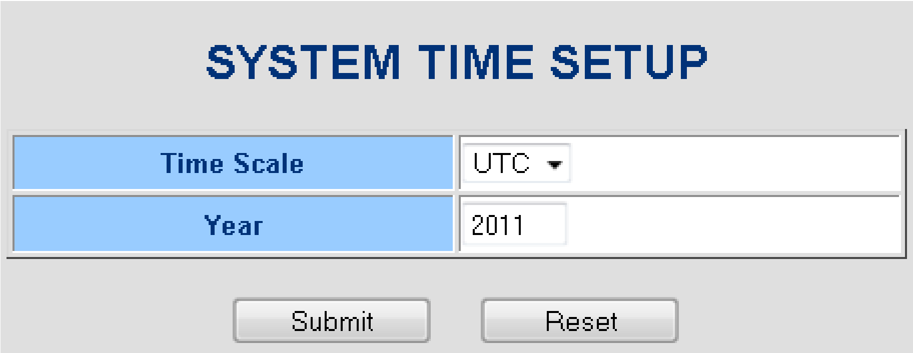
Local Clock: The incoming IRIG input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to "Local", select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to Section *3.11.3* for more information on Local Clocks.

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.

8.3.5 IRIG Input Year Configuration

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.

The current year value can be manually entered from the **Setup / 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. Enter the current year value and click Submit.



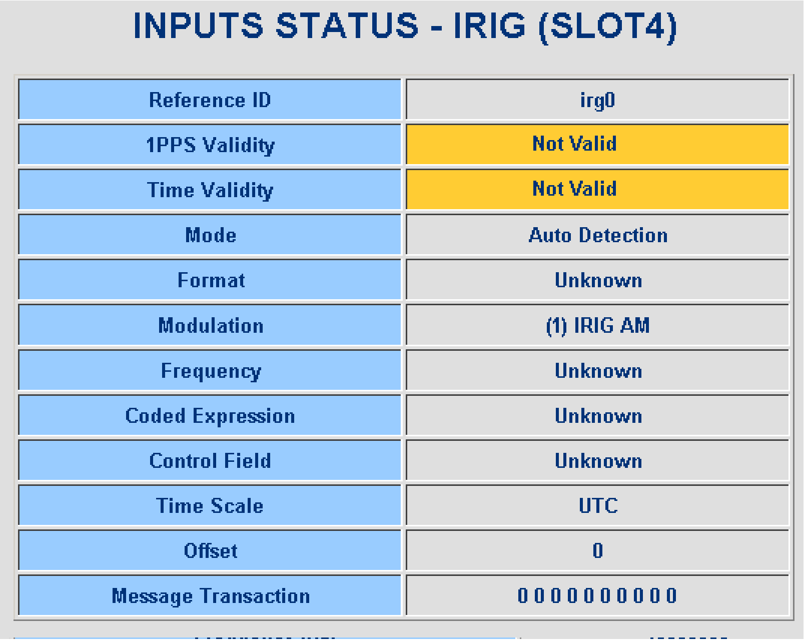
SYSTEM TIME SETUP

Time Scale	UTC
Year	2011

Figure 8-17: System Timescale and Current Year Value

8.3.6 Verifying the IRIG Input Signal Status

To view the current validity status of the IRIG input signal, navigate to the **Status / Inputs** page and select the Slot labeled “**IRIG**”.

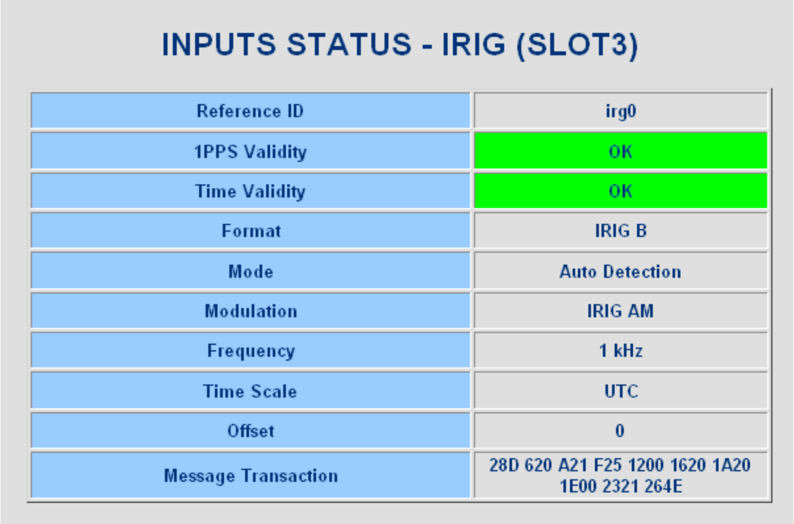


INPUTS STATUS - IRIG (SLOT4)

Reference ID	irg0
1PPS Validity	Not Valid
Time Validity	Not Valid
Mode	Auto Detection
Format	Unknown
Modulation	(1) IRIG AM
Frequency	Unknown
Coded Expression	Unknown
Control Field	Unknown
Time Scale	UTC
Offset	0
Message Transaction	0 0 0 0 0 0 0 0 0 0

Figure 8-18: IRIG Input Status with No Valid IRIG Input

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, these two fields will then turn “Valid” (Green). The parameters for the IRIG input signal configuration are also displayed in this table.



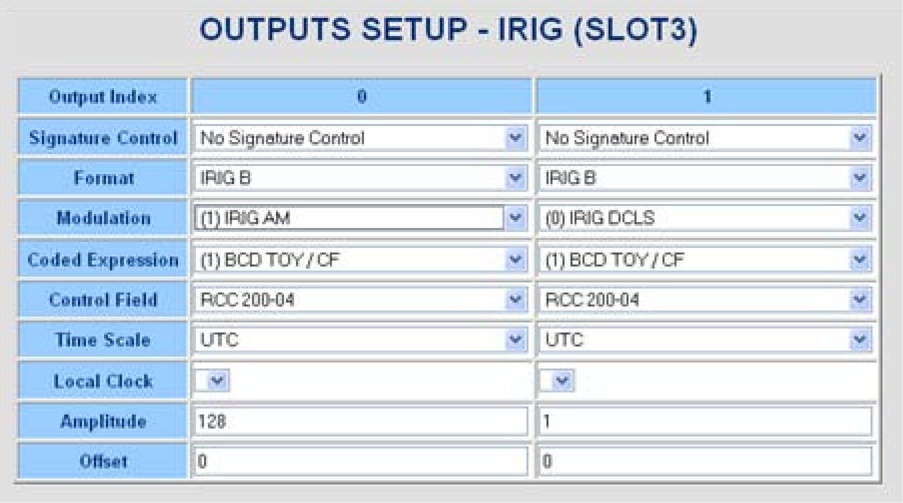
INPUTS STATUS - IRIG (SLOT3)

Reference ID	irg0
1PPS Validity	OK
Time Validity	OK
Format	IRIG B
Mode	Auto Detection
Modulation	IRIG AM
Frequency	1 kHz
Time Scale	UTC
Offset	0
Message Transaction	28D 620 A21 F25 1200 1620 1A20 1E00 2321 264E

Figure 8-19: IRIG Input Status with Valid IRIG Input

8.3.7 IRIG Output Configuration

To manage each of the two IRIG outputs (BNC Connectors **J2** and **J3** on the IRIG module), navigate to the **Setup / Outputs** page and select the Slot labeled “**IRIG**”. Configurable options are as follows:



OUTPUTS SETUP - IRIG (SLOT3)

Output Index	0	1
Signature Control	No Signature Control	No Signature Control
Format	IRIG B	IRIG B
Modulation	(1) IRIG AM	(0) IRIG DCLS
Coded Expression	(1) BCD TOY / CF	(1) BCD TOY / CF
Control Field	RCC 200-04	RCC 200-04
Time Scale	UTC	UTC
Local Clock		
Amplitude	128	1
Offset	0	0

Figure 8-20: IRIG Output Setup

- Output Index 0 is used to configure IRIG output connector J2.
- Output Index 1 is used to configure IRIG output connector J3.

Signature Control: is used to control when the IRIG modulation will be present. This function allows the modulation to stop in certain situations.

Output Always Enabled: IRIG time code modulation is present, even when SecureSync is not synchronized to its references.

Output Enabled in Holdover: IRIG time code modulation is present unless the SecureSync is not synchronized to its references (Modulation is present while in the Holdover mode).

Output Disabled in Holdover: IRIG time code modulation is present unless the SecureSync references are considered not qualified and invalid. (Modulation is not present while in the Holdover mode).

Output Always Disabled: No IRIG output modulation is present, even if any SecureSync input references are present and considered qualified.

Format: Used to configure the desired IRIG output formatting. The available choices are IRIG A, B, G, E (either 100 or 1000 Hz) and NASA-36.

Modulation: Changes the type of output signal modulation:

- **IRIG AM** is an amplitude modulated output. The amplitude of the output is determined by the value entered in the “Amplitude” field.
- **IRIG DCLS** is a TTL modulated output.

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

Control 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 as follows:

RCC-2004: IRIG spec 200-04 specifies a location for year value, if included in this field.
IEE 1344: IRIG B format with extensions. Control Field contains year (if included), Leap Second and DST information.
Spectracom Format: Year is included in Control Field but not in the same location as RCC-2004 output (year is offset by one position).
Spectracom FAA Format: A unique IRIG output Control Field that contains satellite lock status and time error flags.
NASA-36: A variant of IRIG B.

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 5vp-p into high impedance. A value of 200 results in an output amplitude of about 9vp-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.

Time Scale: Used to select the time base for the output IRIG data stream. The available choices are UTC, TAI (Temps Atomique International), GPS and Local. UTC is also referred to as ZULU time. GPS is the raw GPS time as transmitted by the GNSS satellites (as of September, 2013, this is currently 16 seconds ahead of UTC time). IF GPS or TAI time is used, then the proper timescale offsets must be set up on the **Setup / Time Management** page. (Refer to the Section: "*Configuring the System Time Timescale"* for more information). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

Local Clock: System Time may be configured as UTC time, but it might be desired to output the IRIG time as local time instead. 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 IRIG output data stream. Refer to Section *3.11.3* for more information on Local Clocks.

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.

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	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	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	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
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	1 kHz	BCD$_{TOY}$, CF	10 pps	10 sec
IRIG-E	E122	AM	1 kHz	BCD$_{TOY}$	10 pps	10 sec
IRIG-E	E123	AM	1 kHz	BCD$_{TOY}$, SBS	10 pps	10 sec
IRIG-E	E124	AM	1 kHz	BCD$_{TOY}$, BCD$_{YEAR}$, CF and SBS	10 pps	10 sec

IRIG-E	E125	AM	1 kHz	BCD$_{\text{TOY}}$, BCD$_{\text{YEAR}}$, and CF	10 pps	10 sec
IRIG-E	E126	AM	1 kHz	BCD$_{\text{TOY}}$, BCD$_{\text{YEAR}}$	10 pps	10 sec
IRIG-E	E127	AM	1 kHz	BCD$_{\text{TOY}}$, BCD$_{\text{YEAR}}$, and SBS	10 pps	10 sec
IRIG-G	G000	DCLS	N/A	BCD$_{\text{TOY}}$, CF and SBS	10000 pps	10 msec
IRIG-G	G001	DCLS	N/A	BCD$_{\text{TOY}}$, CF	10000 pps	10 msec
IRIG-G	G002	DCLS	N/A	BCD$_{\text{TOY}}$	10000 pps	10 msec
IRIG-G	G003	DCLS	N/A	BCD$_{\text{TOY}}$, SBS	10000 pps	10 msec
IRIG-G	G004	DCLS	N/A	BCD$_{\text{TOY}}$, BCD$_{\text{YEAR}}$, CF and SBS	10000 pps	10 msec
IRIG-G	G005	DCLS	N/A	BCD$_{\text{TOY}}$, BCD$_{\text{YEAR}}$, and CF	10000 pps	10 msec
IRIG-G	G006	DCLS	N/A	BCD$_{\text{TOY}}$, BCD$_{\text{YEAR}}$	10000 pps	10 msec
IRIG-G	G007	DCLS	N/A	BCD$_{\text{TOY}}$, BCD$_{\text{YEAR}}$, and SBS	10000 pps	10 msec
IRIG-G	G140	AM	100 kHz	BCD$_{\text{TOY}}$, CF and SBS	10000 pps	10 msec
IRIG-G	G141	AM	100 kHz	BCD$_{\text{TOY}}$, CF	10000 pps	10 msec
IRIG-G	G142	AM	100 kHz	BCD$_{\text{TOY}}$	10000 pps	10 msec
IRIG-G	G143	AM	100 kHz	BCD$_{\text{TOY}}$, SBS	10000 pps	10 msec
IRIG-G	G144	AM	100 kHz	BCD$_{\text{TOY}}$, BCD$_{\text{YEAR}}$, CF and SBS	10000 pps	10 msec
IRIG-G	G145	AM	100 kHz	BCD$_{\text{TOY}}$, BCD$_{\text{YEAR}}$, and CF	10000 pps	10 msec
IRIG-G	G146	AM	100 kHz	BCD$_{\text{TOY}}$, BCD$_{\text{YEAR}}$	10000 pps	10 msec
IRIG-G	G147	AM	100 kHz	BCD$_{\text{TOY}}$, BCD$_{\text{YEAR}}$, and SBS	10000 pps	10 msec
NASA-36	NA	AM	1msec	UNKNOWN	100 pps	1 sec
NASA-36	NA	DCLS	10msec	UNKNOWN	100 pps	1 sec

Table 8-6: Available IRIG Output Signals

NOTE: 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.

The 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.

Reference information about the IRIG B and IRIG E formats follows.

8.3.7.1 IRIG B Output

The IRIG B Time Code description follows.

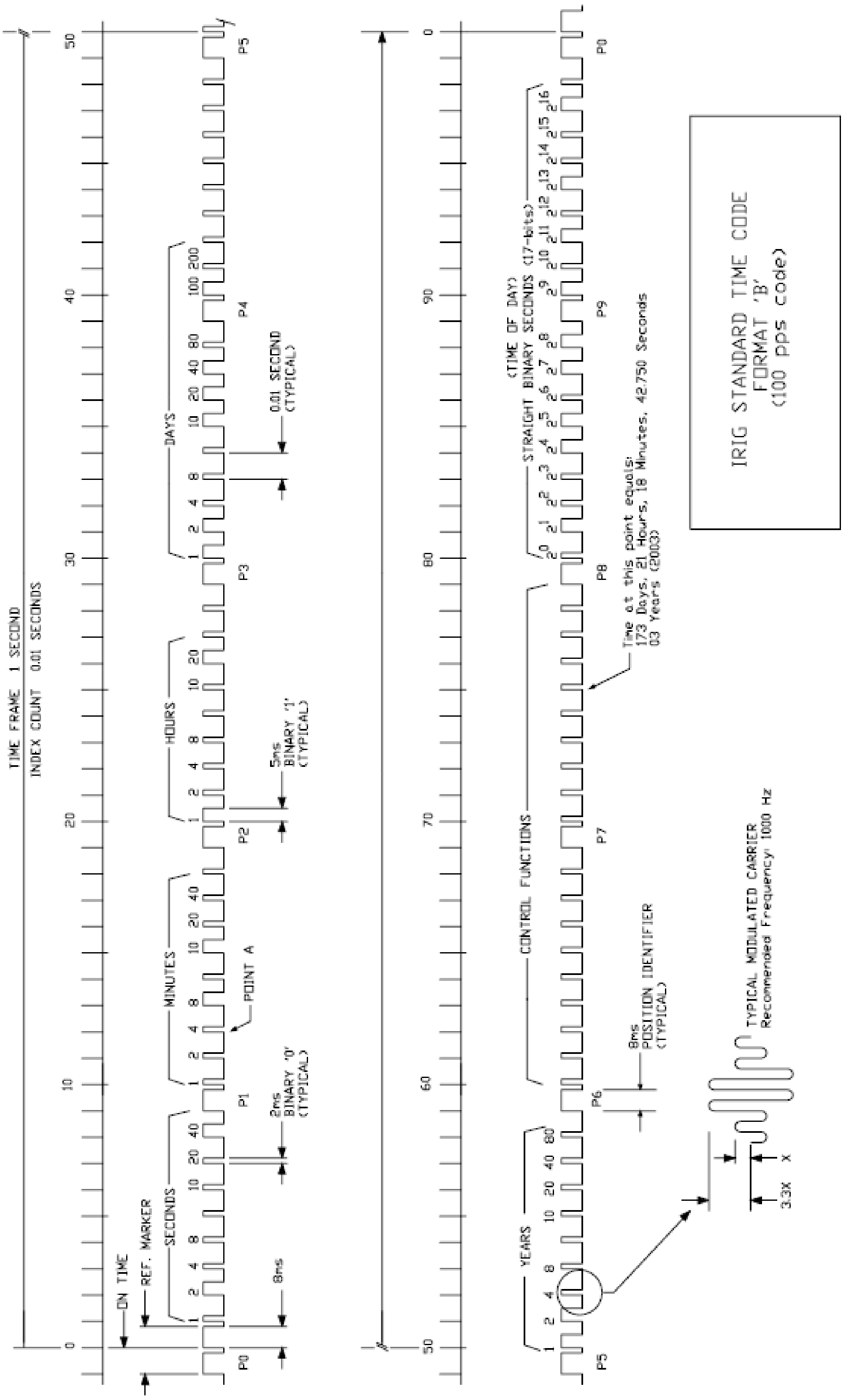


Figure 8-21: IRIG B Time Code Description

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.

Time frame: 1.0 seconds.

Code digit weighting:
Binary Coded Decimal time-of-year.
Code word - 30 binary digits.
Seconds, minutes hours, and days.
Recycles yearly.

Straight Binary Seconds time-of-day.
Code word - 17 binary digits.
Seconds only, recycles daily.

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.

Table 8-7 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. 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
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 8-7: IRIG B Control Function Field

8.3.7.2 IRIG E Output

The IRIG E code contains the Binary Coded Decimal (BCD) time of year and Control Functions. Figure 8-11 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.

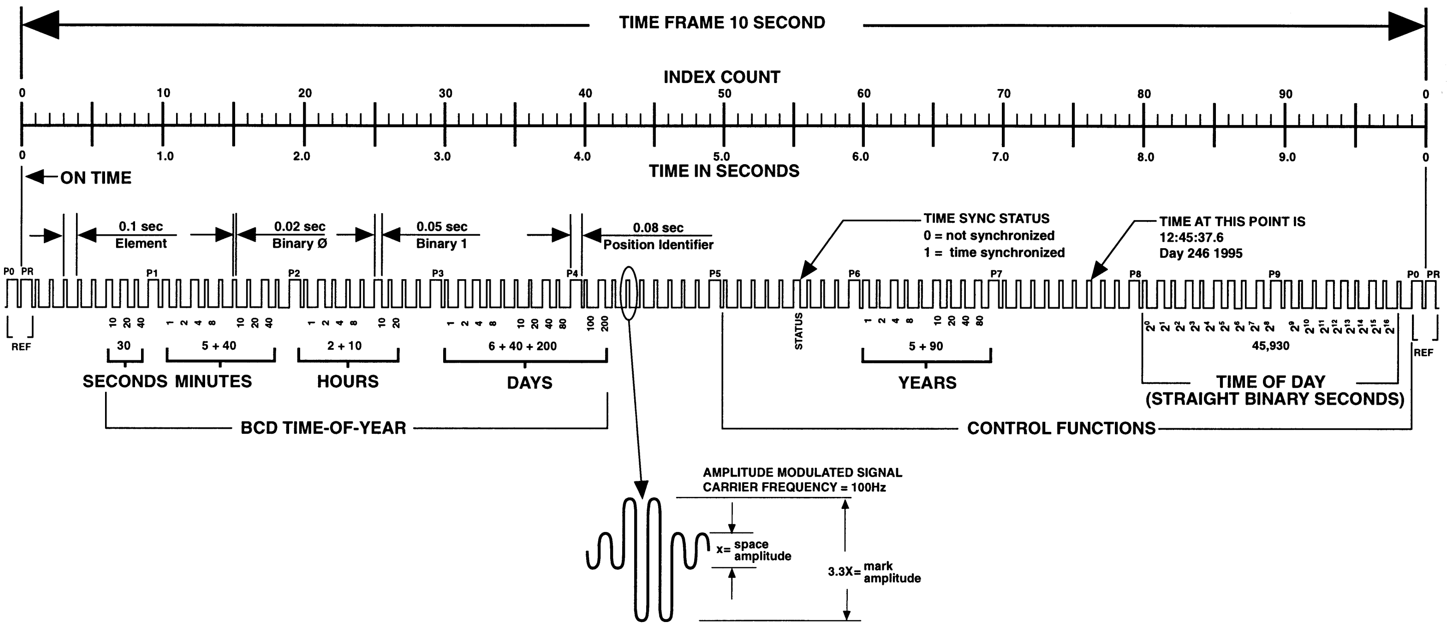
Pulse rates:
Element rate: 10 per second.
Position identifier rate: 1 per second.
Reference marker rate: 1 per 10 seconds.

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.

IRIG E TIME



Specific
The beginning of each 10 second time frame is identified by two consecutive 80 ms elements (P_O 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_0. 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.

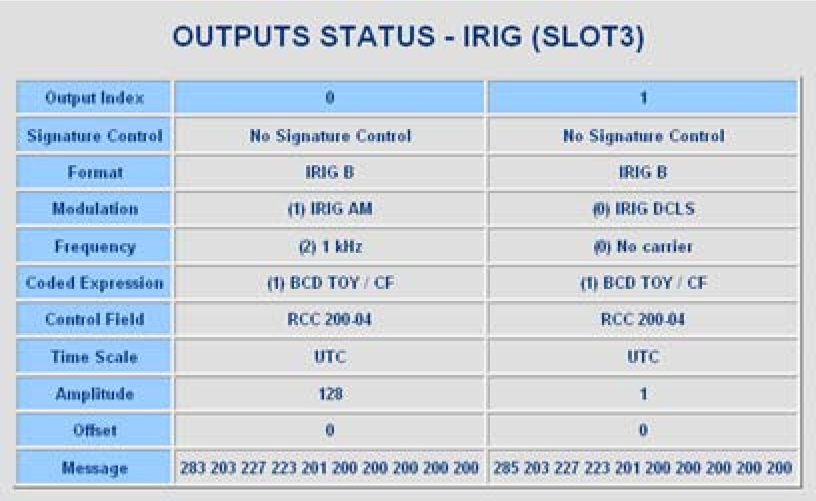
Figure 8-22: IRIG E Time Code Description

BIT #	*CF ELEMENT #*	*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	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		
79	PID P8	POSITION		IDENTIFIER
80	28	SBS		2^{0}
81	29	SBS		2^{1}
82	30	SBS		2^{2}
83	31	SBS		2^{3}
84	32	SBS		2^{4}
85	33	SBS		2^{5}
86	34	SBS		2^{6}
87	35	SBS		2^{7}
88	36	SBS		2^{8}
89	PID P9	POSITION		IDENTIFIER
90	37	SBS		2^{9}
91	38	SBS		2^{10}
92	39	SBS		2^{11}
93	40	SBS		2^{12}
94	41	SBS		2^{13}
95	42	SBS		2^{14}
96	43	SBS		2^{15}
97	44	SBS		2^{16}
98	45	SPACE		
99	PID P0	POSITION IDENTIFIER		

Table 8-8: IRIG E Control Function Field

8.3.8 IRIG Output Status

To view the current validity status of the IRIG output signal, navigate to the **Status / Outputs** page and select the Slot labeled “**IRIG**”.



OUTPUTS STATUS - IRIG (SLOT3)

Output Index	0	1
Signature Control	No Signature Control	No Signature Control
Format	IRIG B	IRIG B
Modulation	(1) IRIG AM	(0) IRIG DCLS
Frequency	(2) 1 kHz	(0) No carrier
Coded Expression	(1) BCD TOY / CF	(1) BCD TOY / CF
Control Field	RCC 200-04	RCC 200-04
Time Scale	UTC	UTC
Amplitude	128	1
Offset	0	0
Message	283 203 227 223 201 200 200 200 200 200	285 203 227 223 201 200 200 200 200 200

Figure 8-23: IRIG Output Configuration

The IRIG Output Status displays the current configurations of both IRIG outputs and the current IRIG Message.

8.4 Model 1204-06: Gigabit Ethernet (3X) Module

Inputs / Outputs:	(3) Gigabit Ethernet (10/100/1000 Base-T)
Signal Type and Connector:	RJ-45
Management:	Enabled or Disabled (NTP server only)
Maximum Number of Cards:	1
Ordering Information:	1204-6: Gigabit Ethernet (3X) Module (configured through the **Network / Interfaces** page of SecureSync web interface)

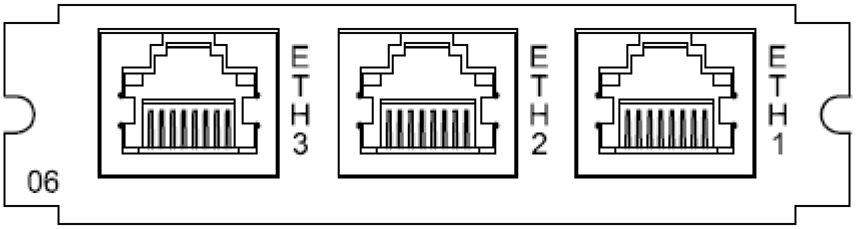


Figure 8-24: Model 1204-06 Option Module Card Rear Plate

This option module card adds three (3) 10/100/1000 Base-T network interfaces in addition to the standard 10/100 Base-T network interface.

8.4.1 Multiple Network Interface Routing

There are five (5) routing tables in the system: one for each network interface, and a 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.

8.4.2 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 interface configuration screen for each network interface.

8.5 Frequency Output Modules

8.5.1 Models 1204-08, 1204-0C, 1204-1C, 1204-26

Inputs / Outputs:	(3) 1 MHz, (3) 5 MHz, or (3) 10 MHz Outputs
Signal Type and Connector:	(10 MHz) +13dBm into 50 Ω, BNC (5 MHz) +10dBm into 50 Ω, BNC (1 MHz) +10dBm into 50 Ω, BNC
Maximum Number of Cards:	4 (1204-08, 1204-1C, or 1204-26) 1 (1204-0C)
Ordering Information:	1204-08: 5 MHz output (3X) Module 1204-0C: 10 MHz output (3X) Module 1204-1C: 10 MHz output (3X) Module 1204-26: 1 MHz output (3X) Module

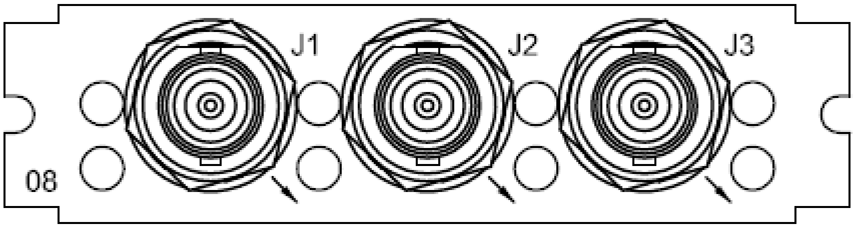


Figure 8-25: Model 1204-08 Option Module Card Rear Plate

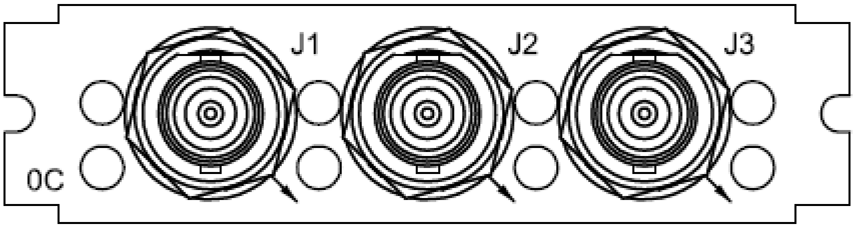


Figure 8-26: Model 1204-0C Option Module Card Rear Plate

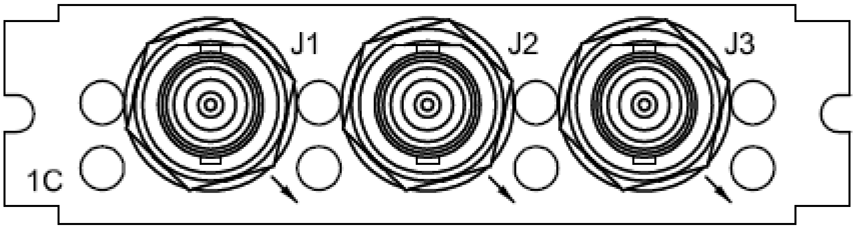


Figure 8-27: Model 1204-1C Option Module Card Rear Plate

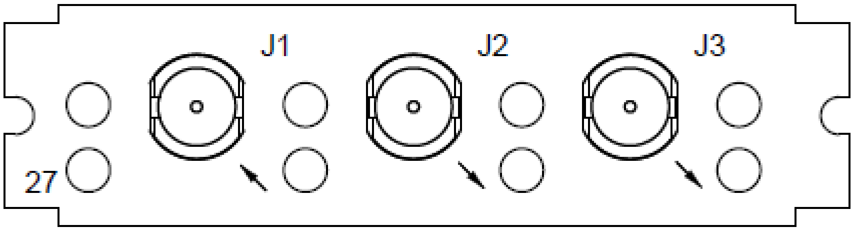


Figure 8-28: Model 1204-27 Option Module Card Rear Plate

Output Configuration:
To manage the three BNC outputs connectors on the module (labeled as "**J1**" ,"**J2**" and "**J3**"), navigate to the **Setup / Outputs** page and select the Slot labeled "**1 MHZ**", "**5 MHZ**", or "**10 MHZ**" (depending on installed option card). Configurable options are as follows:

Signature Control: Signature Control is used to control when the frequency output is present.

Output Always Enabled: Output is present, even when SecureSync is not synchronized to its reference (output is present while in the Holdover mode).

Output Enabled in Holdover: Output is present unless the SecureSync is not synchronized to its references (output is present while in the Holdover mode).

Output Disabled in Holdover: Output is present unless the SecureSync references are not considered qualified and valid (output is not present while in the Holdover mode).

Output Always Disabled: No output is present, even if the SecureSync references are present and considered qualified.

8.6 Models 1204-09, 1204-0A: T1 / E1 Module

The T1 / E1 option modules provide 1.544 MHz or 2.048 MHz and E1 or T1 data outputs for the SecureSync platform. The 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.

8.6.1 Model 1204-09 T1 / E1 (75 Ω) Specifications

Inputs / Outputs:	(1) 1.544 / 2.048 MHz Output (2) Unbalanced T1 / E1 Outputs
Signal Type and Connector:	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)

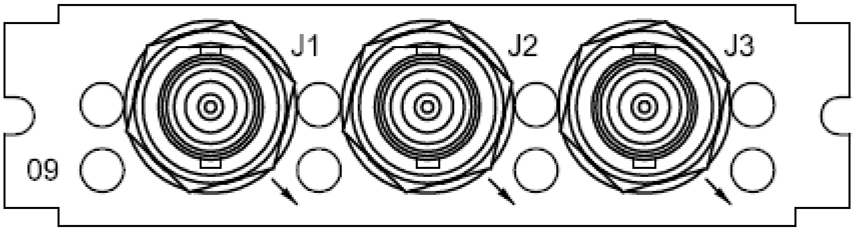


Figure 8-29: Model 1204-09 Option Module Card Rear Plate

8.6.2 Model 1204-0A T1 / E1 (100 / 120 Ω) Specifications

Inputs / Outputs:	(1) 1.544 / 2.048 MHz RS-485 Outputs (2) Balanced T1 / E1 Outputs
Signal Type and Connector:	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)

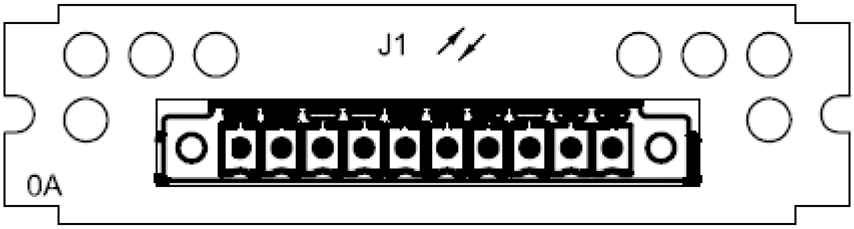


Figure 8-30: Model 1204-0A Option Module Card Rear Plate

Pin Assignments			
Pin No.	**Signal Name**	**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
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 8-9: 1204-0A Option Card Pin Assignments

8.6.3 Setup / Configuration

To manage the outputs (1.544 / 2.048 MHz clock on **J1** BNC connector and unbalanced T1 / E1 outputs on **J2** to **J3** BNC connectors, or all outputs **J1** terminal block, of the T1 / E1 module), navigate to the **Setup / Outputs** page and select the Slot labeled "**E1/T1**". Options on this page are divided into three sections, detailed here.

General

Signature Control: Controls when the output will be present. Options include the following:

Output Always Enabled: The output is present, even when SecureSync is not synchronized to its references.

Output Enabled in Holdover: The output uses the current framing mode unless SecureSync is not synchronized to its references (the output is present while in the Holdover mode). While not synchronized, the output will change SSM states if SSM is enabled, or transition to AIS.

Output Disabled in Holdover: The output uses the current framing mode unless the SecureSync references are considered not qualified and invalid (the output is not present while in the Holdover mode). While references are invalid, the output will change SSM states if SSM is enabled, or transition to AIS.

Output Always Disabled: The output is not present, even if any SecureSync references are present and considered qualified.

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 Enable: 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.

T1 Configuration

Encoding: This option selects the encoding method (**B8ZS** or **AMI**).

Framing: This option selects the framing standard (**D4/Superframe**, **Extended Superframe** [**CRC-6** / **no CRC-6**], or **AIS**).

SSM Value: This option selects the SSM quality level transmitted when SSM is enabled.

E1 Configuration

Encoding: HDB3 only.

Framing: This option selects the framing standard (**CRC-4**, **No CRC-4**, or **AIS**).

SSM Value: This option selects the SSM quality level transmitted when SSM is enabled.

8.6.4 T1 / E1 - 120 Ω Module Status Pages

To view status information for this option module card, navigate to the **Status / Outputs** page and select the Slot labeled “**E1/T1**”.

8.7 Model 1204-0B: RS-485 Communication Module

Inputs / Outputs:	Bi-directional Communication Port
Signal Type and Connector:	Balanced RS-485 (3.8mm terminal block)
Maximum Number of Cards:	1

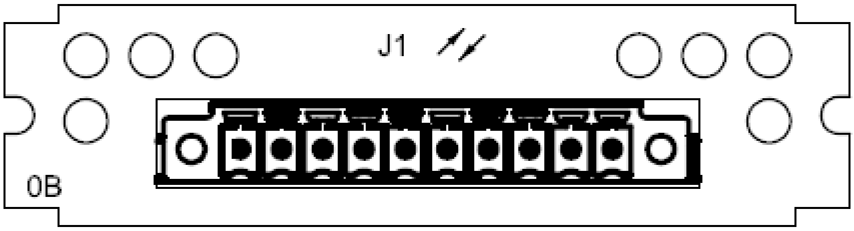


Figure 8-31: Model 1204-0B Option Module Card Rear Plate

Pin Assignments	
Pin No.	**Signal Name**
1	GND
2	RS-485 IN+
3	RS-485 IN-
4	GND
5	RS485 OUT+
6	RS485 OUT-
7	GND
8	NC
9	NC
10	NC

Table 8-10: Model 1204-0B RS-485 Communication Module Card Pin Assignment

8.8 Models 1204-1D, 1204-24: STANAG Input Modules

The Models 1204-1D and 1204-24 STANAG Input option modules provide two (2) configurable STANAG inputs and one (1) 1PPS input for the SecureSync platform.

Inputs:	(2) STANAG Inputs, (1) 1PPS Input
Signal Type and Connector:	TTL or RS-485 level (user selectable) for STANAG and 1PPS input. SUB-D 25.
Formats Supported:	STANAG 4246 HAVE QUICK I STANAG 4246 HAVE QUICK II STANAG 4372 HAVE QUICK IIA STANAG 4430 Extended HAVE QUICK ICD-GPS-060A HAVE QUICK
Accuracy:	100ns
Maximum Number of Cards:	6
Ordering Information:	1204-1D (for non-isolated board) 1204-24 (for isolated board)

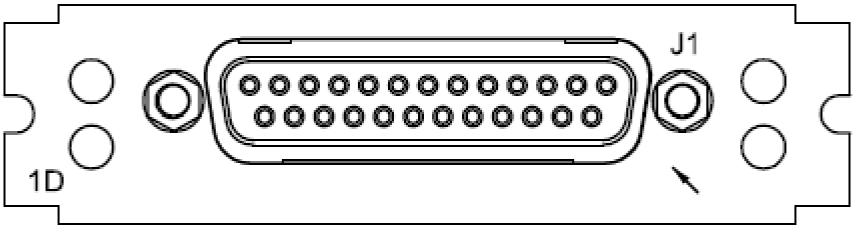


Figure 8-32: Model 1204-1D Option Module Card Rear Plate

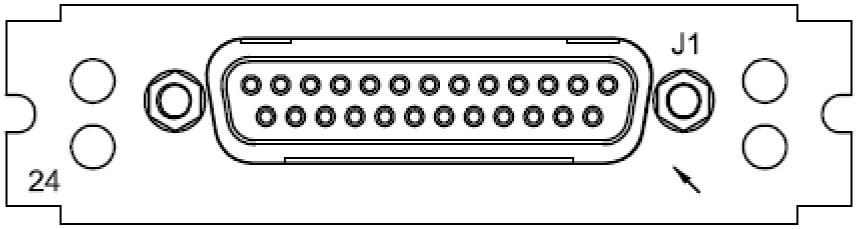


Figure 8-33: Model 1204-24 Option Module Card Rear Plate

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 8-11: 1204-1D, 1204-24 Option Card Pin Assignments

8.8.1 Setup / Configuration

To manage the features for this option module card, navigate to **Setup / Inputs** and select the Slot labeled "**STANAG INPUT**". Configurable options on this page are divided among three tabs, detailed in this section.

8.8.1.1 Setup Tab

From the **Setup** tab page, you can access three sections:

General Settings Section
The following options can be managed from this section:

Reference ID: Name used to represent this input reference in the Reference Priority table (refer to Section *3.17* for more information on the Reference Priority Input table).

Use of Time Fault Discrete:

Enabled: The TFD input signal is used to validate the STANAG input.
Disabled: The TFD input signal is ignored. By default, this option is **Disabled**.

Use of Bit Synchronization (BS):

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: (**TOD 1** / **TOD 2**)**:** Selects which TOD signal is used for synchronization.

Time of Day Reference Settings Section
The following options can be managed from this section:

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
- ICD-GPS-060A HAVE QUICK

Electrical Format: Selects synchronization to either RS-485 or TTL (supporting up to 10V levels) signal lines.

Time Scale: Used to set the desired time scale (**UTC**, **TAI**, **GPS**, or **Local**).

Offset (ns): 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 +500ms in 5ns steps.

1PPS Reference Settings Section

Offset (ns): Used to account for 1PPS cable delays or other latencies in the 1PPS input. Available Offset range is -500 to +500ms in 5ns steps.

Edge: The operator can select if the output signal is a rising or falling edge pulse.

Electrical Format: Selects synchronization to either RS-485 or TTL (supporting up to 10V levels) signal lines.

8.8.1.2 Configuration Examples Tab

This tab displays configuration examples for the option module.

8.8.1.3 SUB-D Connector Pinout Tab

This tab displays the SUB-D connector pinout information. Notice that if the Bit Synchronization (BS) is used, the TOD 2 reference cannot be selected.

8.8.2 STANAG Input Status Pages

To view status information for this option module card, navigate to **Status / Inputs** and select the Slot labeled “**STANAG INPUT**”.

8.9 Models 1204-11, 1204-25: STANAG Output Modules

The Models 1204-11 and 1204-25: STANAG Output Modules provide two (2) configurable STANAG outputs and one (1) 1PPS output for the SecureSync platform.

Outputs:	(2) STANAG Outputs, (1) 1PPS Output
Signal Type and Connector:	5V or 10V or RS-485 level (user selectable) for STANAG and 1PPS output. SUB-D 25.
Formats Supported:	STANAG 4246 HAVE QUICK I STANAG 4246 HAVE QUICK II STANAG 4372 HAVE QUICK IIA STANAG 4430 Extended HAVE QUICK ICD-GPS-060A HAVE QUICK
Programmable Pulse Width (1PPS Output):	100ns to 500ms with 20ns resolution
Accuracy:	±50ns (1σ)
Maximum Number of Cards:	6
Ordering Information:	1204-11 (for non-isolated board) 1204-25 (for isolated board)

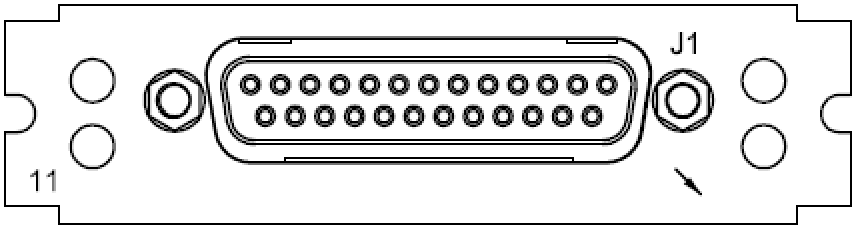


Figure 8-34: Model 1204-11 Option Module Card Rear Plate

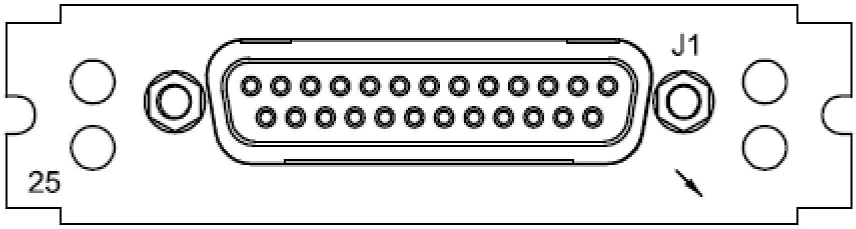


Figure 8-35: Model 1204-25 Option Module Card Rear Plate

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			

8-12: Models 1204-11, 1204-25 Option Card Pin Assignments

8.9.1 Setup / Configuration

To setup and configure this option module card, navigate to **Setup / Outputs** and select the Slot labeled “**STANAG OUTPUT**”. Configurable options on this page are divided among three tabs, detailed in this section.

8.9.1.1 Setup Tab

From the **Setup** tab page, you can access three sections:

General Settings Section

Level of Single-ended Signals: 10V 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.

Time of Day Output Settings Section

TOD 1 & TOD 2: STANAG columns 1 and 2

Signature Control: Used to control when the signal will be present. This function allows the modulation to stop in certain situations.

Output Always Enabled: STANAG signal is present, even when SecureSync is not synchronized to its references.

Output Enabled in Holdover: STANAG signal is present unless the SecureSync is not synchronized to its references (Modulation is present while in the Holdover mode).

Output Disabled in Holdover: STANAG signal is present unless the SecureSync references are considered not qualified and invalid. (Modulation is not present while in the Holdover mode).

Output Always Disabled: No STANAG signal is present, even if any SecureSync input references are present and considered qualified.

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

Electrical Format: Selects signaling on either RS-485 or TTL (supporting up to 10V levels) signal lines.

Time Scale: Used to set the desired time scale (**UTC**, **TAI**, **GPS**, or **Local**).

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 +500ms in 5ns steps.

1PPS Output Settings Section

Signature Control: Used to control when the signal will be present. This function allows the modulation to stop in certain situations.

Output Always Enabled: STANAG signal is present, even when SecureSync is not synchronized to its references.

Output Enabled in Holdover: STANAG signal is present unless the SecureSync is not synchronized to its references (Modulation is present while in the Holdover mode).

Output Disabled in Holdover: STANAG signal is present unless the SecureSync references are considered not qualified and invalid. (Modulation is not present while in the Holdover mode).

Output Always Disabled: No STANAG signal is present, even if any SecureSync input references are present and considered qualified.

Offset (ns): Used to account for 1PPS cable delays or other latencies in the 1PPS output. Available Offset range is -500 to +500ms in 5ns steps.

Edge: The operator can select if the output signal is a rising or falling edge pulse.

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 milliseconds).

Electrical Format: Selects signaling on either RS-485 or TTL (supporting up to 10V levels) signal lines.

8.9.1.2 Configuration Examples Tab

This tab displays configuration examples for the option module.

8.9.1.3 SUB-D Connector Pinout Tab

This tab displays the SUB-D connector pinout information. Notice that if the Bit Synchronization (BS) is generated, the TOD 2 output cannot be delivered.

8.9.2 Status Pages

To view status information for the STANAG Output module card, navigate to the **Status / Outputs** page and select the Slot labeled "**STANAG OUTPUT**".

8.10 Model 1204-0F: Relay Output

The Model 1204-0F Relay option module card provides three (3) configurable relay outputs for the SecureSync platform.

Inputs / Outputs:	(3) Three contact relay connections (NC, common, NO)
Signal Type and Connector:	Terminal block Contacts Switch under max. load of 30VDC, 2A Contacts rated to switch 220VDC Breakdown voltage of 1000VDC between contacts Switch time 4 msec, max.

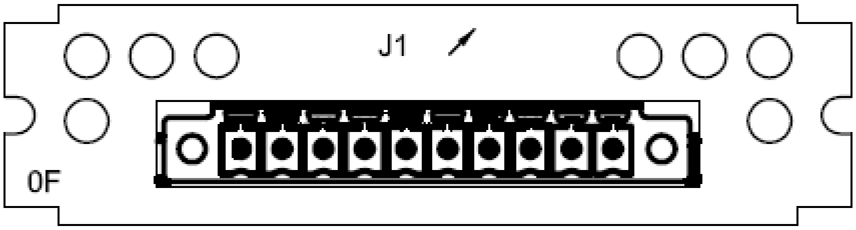


Figure 8-36: Model 1204-0F Option Module Card Rear Plate

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 8-13: Relay Output Option Card Connector Pin Assignment

8.10.1 Setup / Configuration

To manage this option module card, navigate to **Setup / Outputs** and select the Slot labeled "**RELAY OUTPUT**". Configurable options are as follows:

Alarm Type

This section allows configuration of the alarm type (**None / Disabled**, **Minor**, or **Major**) for both the DB-9 and RJ-12 connectors. Refer to Sections *9.1.2*: "*Fault light - Minor Alarm*" and *9.1.1*: "*Fault Light - Major Alarm*" for additional information on alarm types.

8.10.2 Relay Output Status Pages

To view status information pages for this option module card, navigate to **Status / Outputs** and select the Slot labeled "**RELAY OUTPUT**".

8.11 Models 1204-10, 1204-1B: HAVE QUICK Module

The HAVE QUICK modules provide four (4) available HAVE QUICK outputs for the SecureSync platform.

8.11.1 Model 1204-10 HAVE QUICK Output Specifications

Outputs:	(4) HAVE QUICK outputs
Signal Type and Connector:	TTL levels (BNC)
Output Load Impedance:	10k Ω
Start of signal:	<10µs after 1PPS output
Programmable Phase Shift:	±5ns to 500ms with 5ns resolution
Maximum Number of Cards	6

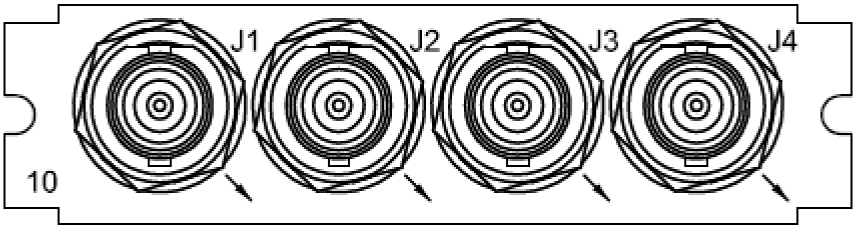


Figure 8-37: Model 1204-10 Option Module Card Rear Plate

8.11.2 Model 1204-1B: HAVE QUICK Output Specifications

Outputs:	(4) HAVE QUICK outputs
Signal Type and Connector:	RS-485 levels (terminal block)
Output Load Impedance:	120 Ω
Start of signal:	<10µs after 1PPS output
Programmable Phase Shift:	±5ns to 500ms with 5ns resolution
Maximum Number of Cards	6

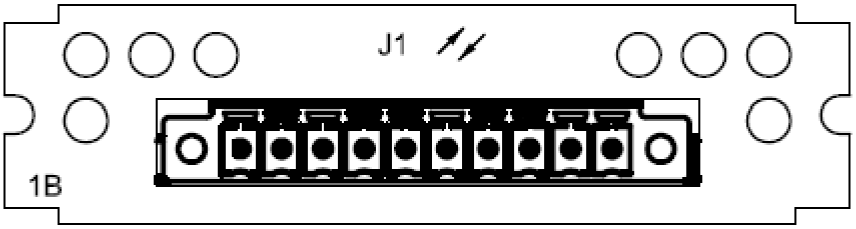


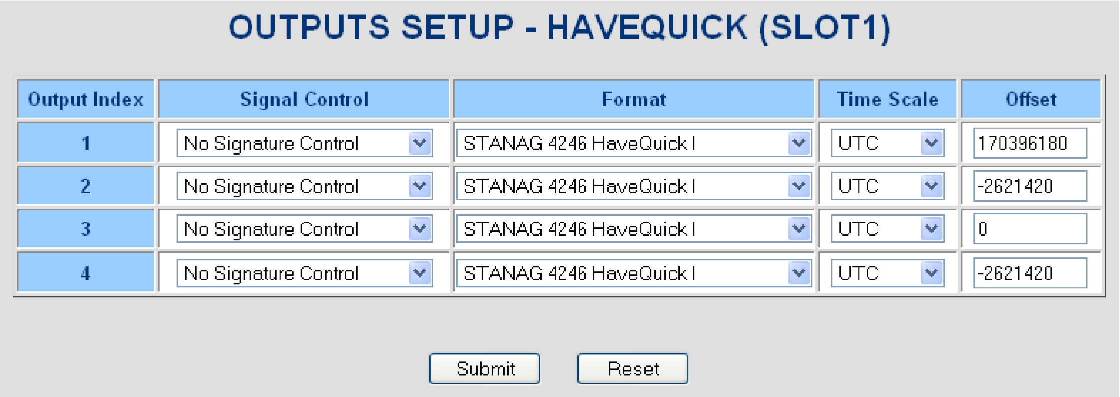
Figure 8-38: Model 1204-1B Option Module Card Rear Plate

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 8-14: Model 1204-1B HAVE QUICK Card Pin Assignments

To manage the four HAVE QUICK BNC outputs (**J1** to **J4** BNC connectors or **J1** terminal block on the HAVE QUICK module), navigate to **Setup / Outputs** and select the Slot labeled "**HAVEQUICK**".



OUTPUTS SETUP - HAVEQUICK (SLOT1)

Output Index	Signal Control	Format	Time Scale	Offset
1	No Signature Control	STANAG 4246 HaveQuick I	UTC	170396180
2	No Signature Control	STANAG 4246 HaveQuick I	UTC	-2621420
3	No Signature Control	STANAG 4246 HaveQuick I	UTC	0
4	No Signature Control	STANAG 4246 HaveQuick I	UTC	-2621420

Figure 8-39: HAVE QUICK Output Configuration

Available options are as follows:

Output Index: Correlates to the four BNC Output connectors (labeled **J1** - **J4**) on the HAVE QUICK module (left to right as viewed on the SecureSync back panel, where 1 is the left-most BNC connector).

Signature Control: Signature Control is used to control when the HAVE QUICK modulation is present.

Output Always Enabled: HAVE QUICK time code modulation is present, even when SecureSync is not synchronized to its reference (Modulation is present while in the Holdover mode).

Output Enabled in Holdover: HAVE QUICK time code modulation is present unless the SecureSync is not synchronized to its references (modulation is present while in the Holdover mode).

Output Disabled in Holdover: HAVE QUICK time code modulation is present unless the SecureSync references are not considered qualified and valid. (Modulation is not present while in the Holdover mode).

Output Always Disabled: No HAVE QUICK output modulation is present, even if the SecureSync references are present and considered qualified.

Format: Used to configure the formatting of the four available HAVE QUICK outputs. The available output formats are as follows:

- STANAG 4246 HAVE QUICK I
- STANAG 4246 HAVE QUICK II
- STANAG 4372 HAVE QUICK IIA
- STANAG 4430 Extended HAVE QUICK
- ICD-GPS-060A HAVE QUICK

Time Scale: This option configures the time scale for the LED time display. The available options are UTC, TAI (Temps Atomique International), GPS and Local. UTC is also referred to as ZULU time. GPS 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). If GPS or TAI time is used, then the proper timescale offsets must be set on the **Setup / Time Management** page. (Please refer to Section *3.11.1* for more information). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

Local Clock: System Time may be configured as UTC time, but it might be desired to output the IRIG time as local time. 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 IRIG output data stream. Refer to Section *3.11.3* 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.

8.12 Model 1204-12: Precision Time Protocol (PTP) Module

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.

Inputs / Outputs:	(1) Configurable as Input or Output
Signal Type and Connector:	RJ-45
Management:	Web interface
Resolution:	8 nS (+/- 4 nS) packet timestamping resolution
Accuracy:	30 nS accuracy (3σ) Master to Slave via crossover cable
Maximum Number of Cards:	6

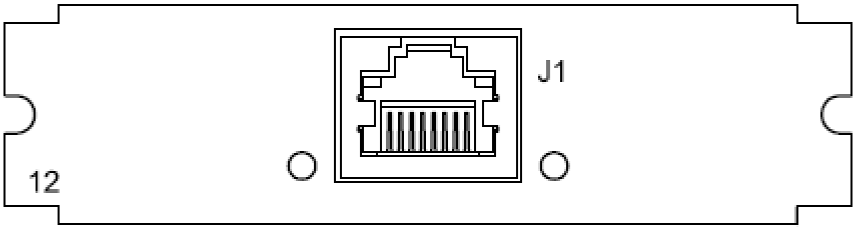


Figure 8-40: Model 1204-12 Option Module Card Rear Plate

The PTP option module 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 the SecureSync device.
- 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 module can change mode according to priority and quality criteria compared with the other PTP Clocks on the network.

8.12.1 Configuration as a Slave Clock

By default, the PTP Module is configured to function as a PTP Slave, which allows a SecureSync to be able to synchronize to a PTP Master (such as another SecureSync unit with a PTP module option card configured as a Master) when configured with the following parameters:

- Announce Rate = once every 4 seconds or faster
- Delay Mechanism = End-to-End
- Multicast operation active
- Two-Step operation

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 the SecureSync.

If the SecureSync is not entering the “Slave” Port state (as reported by the “**Network**” tab on the **PTP Status** page), check the following:

- From the **PTP Status** page / **Network** tab, check that the **Port Status** / **Link Status** indicates “Connected”
- From the **PTP Status** page / **Network** tab, check that the **Port Status** / **Port Activity** indicates “Enabled”
- Ensure PTP Port Speed is 100 Mb/s.
- From the **PTP Setup** / **Network tab**, check that the clock is set to be a Slave-Only clock.
- The clock is set to be a Slave-Only clock (check **Clock Mode** on the **PTP Setup / Clock** page)
- The **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 Setup / Network** page)
- The **Domain Number** 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 Setup / Network** page)
- The **PTP Protocol** version number of the Master Clock is 2
- A valid IP address is currently being used (check **Ethernet Settings** on the **PTP Setup / Network** page)
- The Time To Live (TTL) for PTP packets is compatible with the network topology (check the **Time To Live (TTL)** on the **PTP Setup / Network** page)
- In **Multicast mode**, the switches/routers are transparent to multicast frames
- The Master Clock is synchronized (Clock Class = 6, 7, 13 or 14 as reported by the **GrandMaster Properties** on the **PTP Status / PTP Protocol** page)

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:

- Navigate to the **PTP Setup** page and select the **Network** tab.
- From the **PTP Network Settings** section, locate the **Port Activity** option.
- Selected **Disabled**, then click **Submit**.
- Re-Enable the **Port Activity** option by selecting **Enabled**, then click **Submit**. The restart may take up to a few minutes to complete.

8.12.2 Configuration as a Master Clock

To configure the IEEE-1588 (PTP) Module as a Master Clock, perform these steps:

General SecureSync actions:

- The PTP port is Connected to the network (check the Link Status in the **PTP Status / Network** page).
- The PTP port speed is 100 Mb/s (check the **Port Speed** in the **PTP Status / Network** page).
- Be sure that valid time and 1PPS references are currently selected (check the **Status / Time and Frequency** page).

In order to operate properly as a Master Clock, the SecureSync must be synchronized to a non-PTP reference. Confirm that the chosen reference transmits the following information (as reported by the Time Properties in the **PTP Status / Clock** page):

- 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.

Specific PTP Module actions:

- The **PTP Port Activity** is Enabled (check the **Port Activity** in the **PTP Status / Network** page). 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 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:

1. 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 on the **Status / Time and Frequency** page.

2. 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 **Setup / Time Management** page (while setting the GPS to UTC Offset).

3. 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 SecureSync web interface. If this is not done, the PTP network will have the incorrect UTC time after a leap second event.

4. If there are multiple 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:

   a. The BMC algorithm first selects the clock having the higher Priority1 parameter (a lowest value means a higher priority)
   b. 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)
   c. 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.

8.12.3 Configuration in Master/Slave Mode

The IEEE-1588 (PTP) Module 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 to Section *3.15*.

NOTE: The Master/Slave mode is not supported in unicast transmission mode.

8.12.4 Transmission Modes

The PTP Module is able to transmit the PTP packets in three transmission modes:

8.12.4.1 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 (SequenceId).
To enter Multicast mode, perform the following steps:

On the Master side:

- Enable the Multicast mode (see **Transmission Mode** from the **PTP Setup / Network** page).

On the Slave side:

- Enable the Multicast mode (see **Transmission** from the **PTP Setup / Network** page).

8.12.4.2 Unicast Mode

Point-to-Point transmission mode between two PTP Clocks by means of the unique IP address assigned to each PTP Clock.

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:

- Enable the unicast mode for the Master Clock (refer to the settings for Master-Only Clock from the PTP Setup / Unicast page).

On the Slave side:

- Set the IP address of the Master Clock enabled to run in unicast mode (refer to the settings for **Slave-Only Clock** from the **PTP Setup / Unicast** page).
- Enable the unicast mode (see **Transmission Mode** from the **PTP Setup / Network** page).

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 doesn’t transmit any PTP messages
until a Slave has been granted to run in unicast mode.

NOTE: The Unicast mode is only implemented for the following PTP packets:

- Announce
- Sync and Follow-Up
- Delay_Req and Delay_Resp

8.12.4.3 Minicast Mode

Hybrid mode 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.

To enter the Minicast mode, perform the following steps:

On the Master side:

- Enable the minicast mode for the Master Clock (refer to the **Master-Only Clock** settings from the **PTP Setup / Unicast** page).

On the Slave side:

- Set the IP address of the Master Clock enabled to run in minicast mode (refer to the **Slave-Only Clock** settings from the **PTP Setup / Unicast** page).
- Enable the minicast mode (see **Transmission Mode** from the **PTP Setup / Network** page).

8.12.5 PTP Status Pages

The **PTP Status** pages are available either through the “**Inputs**” display or the “**Outputs**” display, with different tabs displaying PTP System information:

- **Clock:** Information about the PTP clock (time information)
- **Network:** Network information (MAC layer, Internet layer, PTP port information)
- **PTP Protocol:** Information about the PTP layer
- **Unicast:** Information about the Unicast transmission mode
- **Module:** General PTP module information

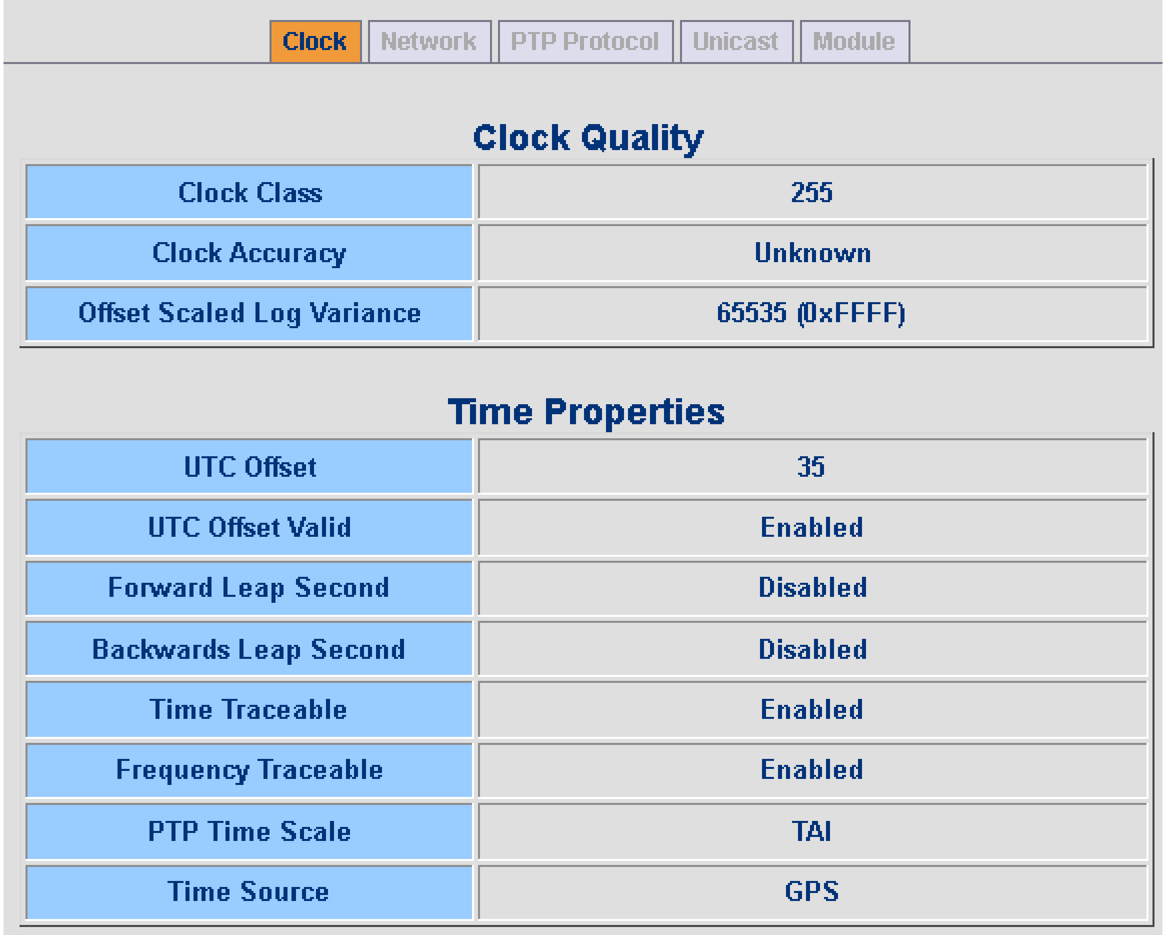
The following sections cover the information displayed on each of the **PTP Status** tabs.

NOTE: Some parameters define a PTP packets throughput. They use the “log2 seconds“, defined as follows:

- Positive Value: n => 2^n seconds between two successive PTP packets
- Negative Value: -n => $2^{(-n)}$ = ($1/2^n$) => 2^n PTP packets per second

8.12.5.1 PTP Status / Clock Tab

This tab reports the status of several key parameters about the clock provided by the PTP card.



Clock Quality

Clock Class	255
Clock Accuracy	Unknown
Offset Scaled Log Variance	65535 (0xFFFF)

Time Properties

UTC Offset	35
UTC Offset Valid	Enabled
Forward Leap Second	Disabled
Backwards Leap Second	Disabled
Time Traceable	Enabled
Frequency Traceable	Enabled
PTP Time Scale	TAI
Time Source	GPS

Figure 8-41: PTP Status / Clock Tab

Clock Quality

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 Timescale	Arbitrary Timescale	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.

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). Slaves will always report “Unknown” here.

Offset Scaled Log Variance: (Defined in IEEE Standard 1588-2008, Section 1.6.3)

Time Properties

If the module is currently a Slave, these values come from the current Master. Otherwise, these values come from the module itself.

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.

Forward Leap Second: Indicates whether or not a leap second will be removed at the end of the current 24-hour UTC day. (Enabled or Disabled).

Backwards Leap Second: Indicates whether or not a leap second will be added at the end of the current 24-hour UTC day. (Enabled or Disabled).

Time Traceable: Indicates whether the Master’s time is traceable (Enabled) to a primary reference or not (Disabled).

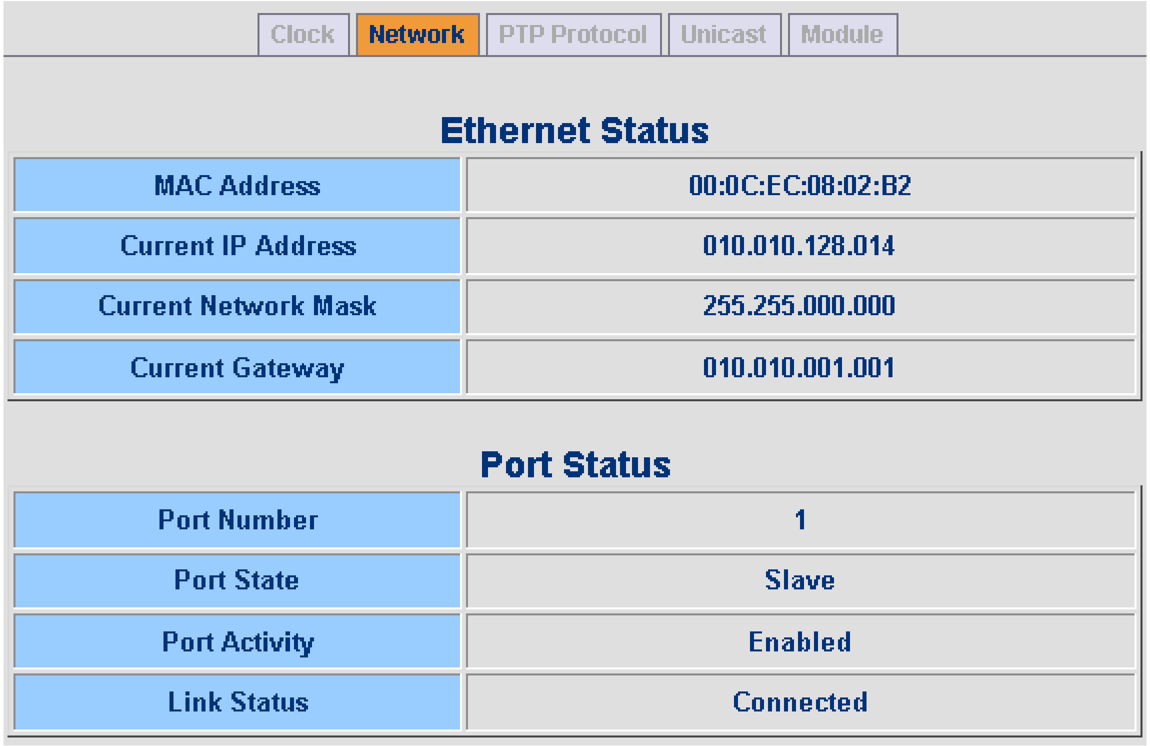
Frequency Traceable: Indicates whether the Master’s Frequency is traceable (Enabled) to a primary reference or not (Disabled).

PTP Timescale: 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.

8.12.5.2 PTP Status / Network Tab

This tab displays the current network item status for the PTP device.



Ethernet Status

MAC Address	00:0C:EC:08:02:B2
Current IP Address	010.010.128.014
Current Network Mask	255.255.000.000
Current Gateway	010.010.001.001

Port Status

Port Number	1
Port State	Slave
Port Activity	Enabled
Link Status	Connected

Figure 8-42: PTP Status / Network Tab

Ethernet Status

MAC Address: The MAC address currently being used by the PTP interface.

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 "**Network**" tab on the **PTP Setup** page.

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 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.
- **Slave:** PTP Slave is actively synchronizing to a Master Clock on the network.

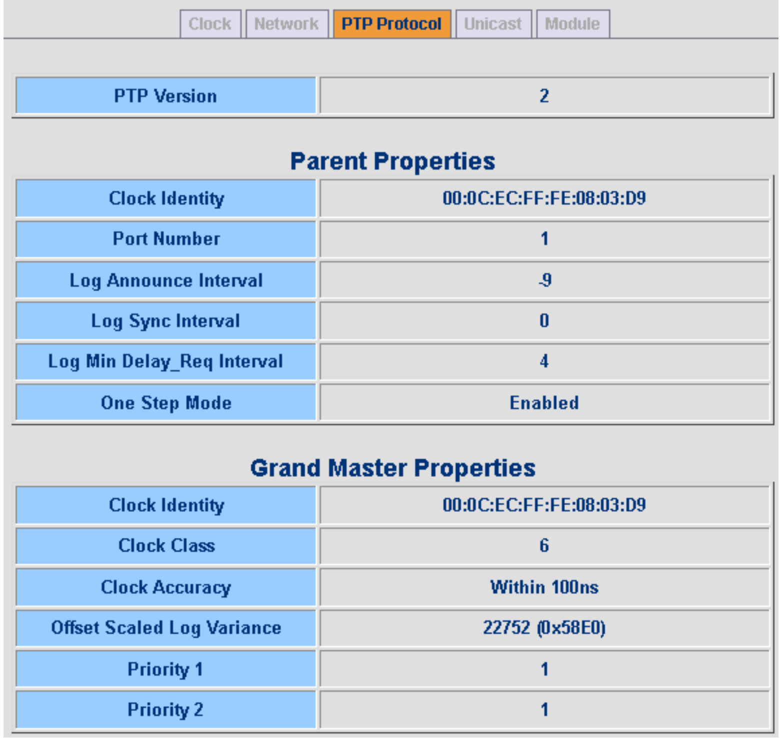
For more information on PTP Port State definitions, refer to Section 9.2.4 of the IEEE Standard 1588-2008 PTP Specification.

Port Activity: Reports whether or not the network interface is active for PTP (Enabled) or not (Disabled).

Link Connected: Indicates whether or not the Ethernet link for PTP is active (Connected) or not (Disconnected).

8.12.5.3 PTP Status / PTP Protocol Tab

This tab displays certain PTP information including PTP version, clock information, priority, etc.



PTP Version	2

Parent Properties

Clock Identity	00:0C:EC:FF:FE:08:03:D9
Port Number	1
Log Announce Interval	-9
Log Sync Interval	0
Log Min Delay_Req Interval	4
One Step Mode	Enabled

Grand Master Properties

Clock Identity	00:0C:EC:FF:FE:08:03:D9
Clock Class	6
Clock Accuracy	Within 100ns
Offset Scaled Log Variance	22752 (0x58E0)
Priority 1	1
Priority 2	1

Figure 8-43: PTP Status / PTP Protocol Tab

PTP Version: This module only supports PTP Version 2.

Parent Properties

Reports information from the Parent Clock - i.e., the Master Clock with which the PTP Module that is currently a Slave is synchronized. If the PTP Module is currently a Master, this will report information on the PTP module itself.

Clock Identity: Displays the clock identity of the current Grandmaster Clock on the network.

Port Number: Displays port number.

Log Announce Interval: Reports the current Announce Interval (for Masters). Units: log2 seconds.

Log Sync Interval: Reports the current Sync Interval for Masters. Units: log2 seconds.

Log Min Delay_Req Interval: Reports the current `Delay_Req` / Delay Request interval (for Slaves). Units: log2 seconds.

One-Step Mode: Determines whether the Master operates in one-step (Enabled) or two-step (Disabled) 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).

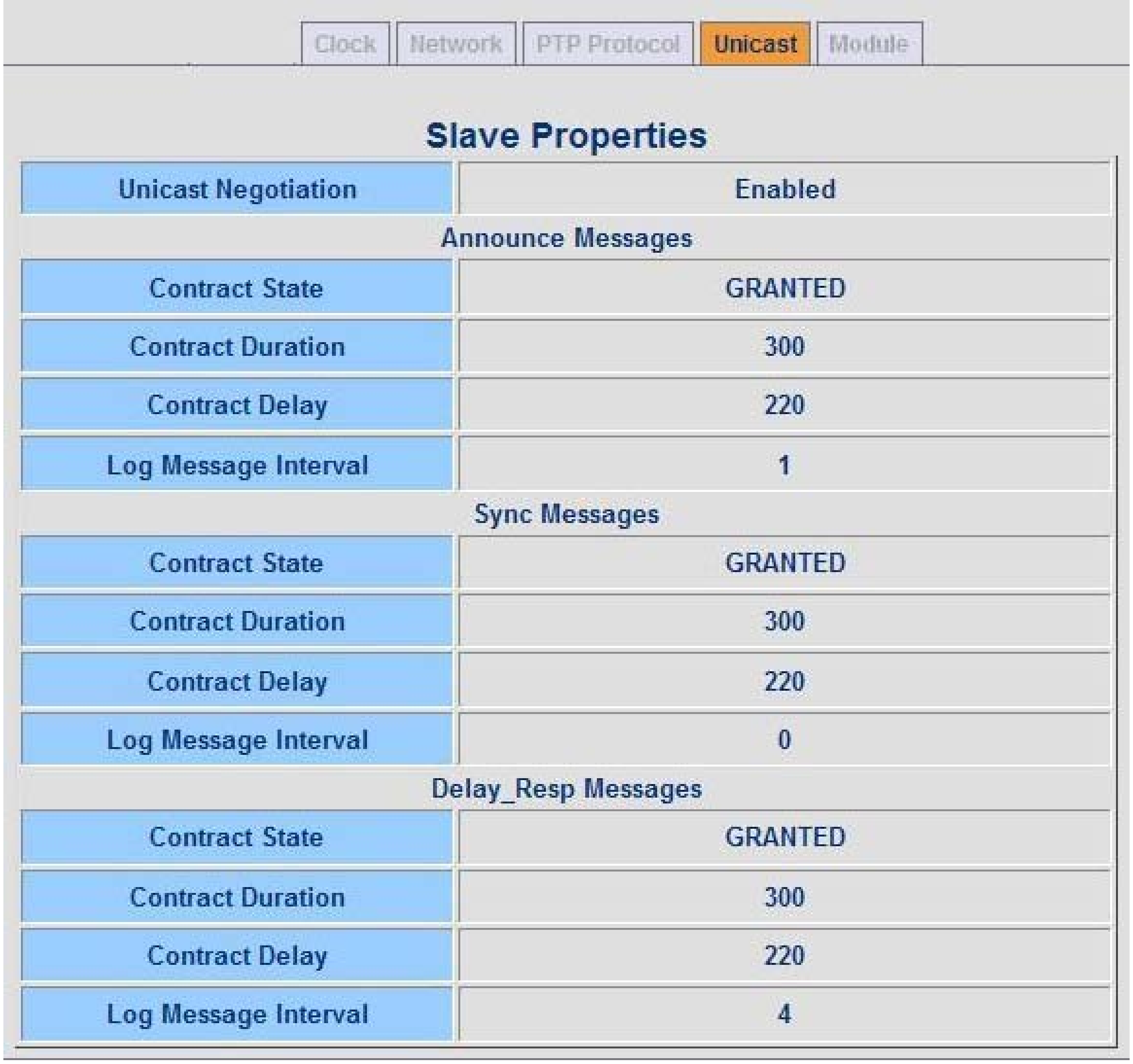
Offset Scaled Log Variance: See IEEE Standard 1588-2008 Section 7.6.3.

Priority1: See IEEE Standard 1588-2008, Section 7.6.3

Priority2: See IEEE Standard 1588-2008, Section 7.6.3

8.12.5.4 PTP Status / Unicast Tab

This tab displays the negotiation status of the unicast contracts. See IEEE Std 1588-2008, Section 16.1.



Slave Properties

Unicast Negotiation	Enabled
Announce Messages	
Contract State	GRANTED
Contract Duration	300
Contract Delay	220
Log Message Interval	1
Sync Messages	
Contract State	GRANTED
Contract Duration	300
Contract Delay	220
Log Message Interval	0
Delay_Resp Messages	
Contract State	GRANTED
Contract Duration	300
Contract Delay	220
Log Message Interval	4

Figure 8-44: PTP Status / Unicast Tab for Slave-Only Clocks

Slave Properties

Unicast Negotiation: Reports whether the Unicast Negotiation option is Enabled or Disabled.

Unicast contract for Announce Messages:

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.

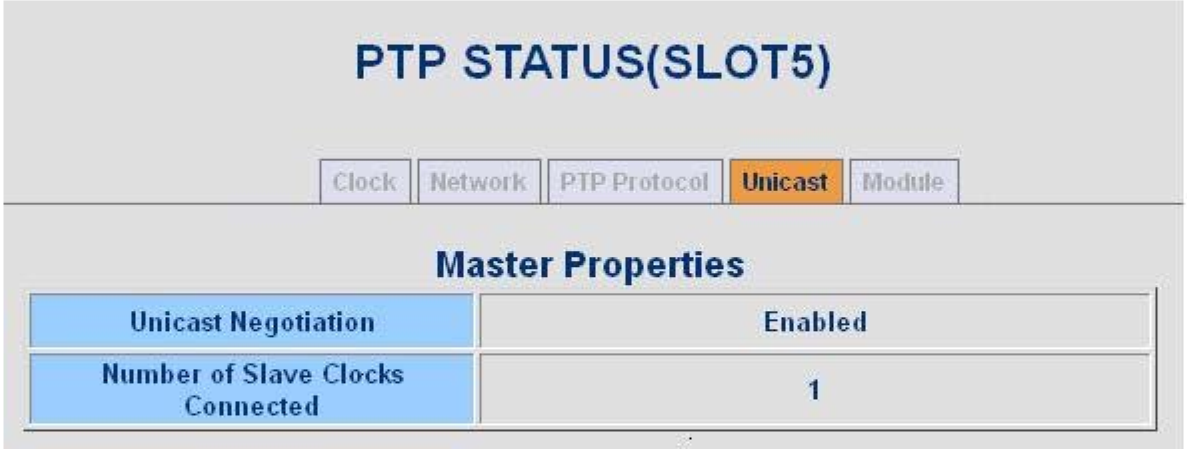
Contract Duration: Duration of the unicast contract.
Units: Seconds.
Contract Delay: Delay before the end of the unicast contract.
Units: Seconds.
Log Message Interval: Announce Interval negotiated for the unicast mode.
Units: log2 seconds.

Unicast Contract for the Sync Messages:

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: Sync Interval negotiated for the unicast mode.
Units: log2 seconds.

Unicast Contract for the Delay_Resp Messages:

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.



PTP STATUS(SLOT5)

Master Properties

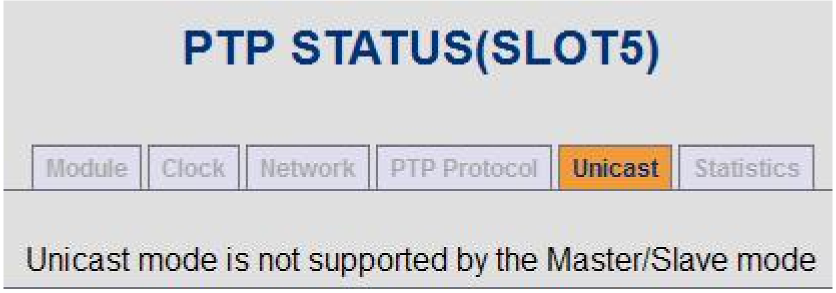
Unicast Negotiation	Enabled
Number of Slave Clocks Connected	1

Figure 8-45: PTP Status / Unicast Tab for Master-Only Clocks

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.

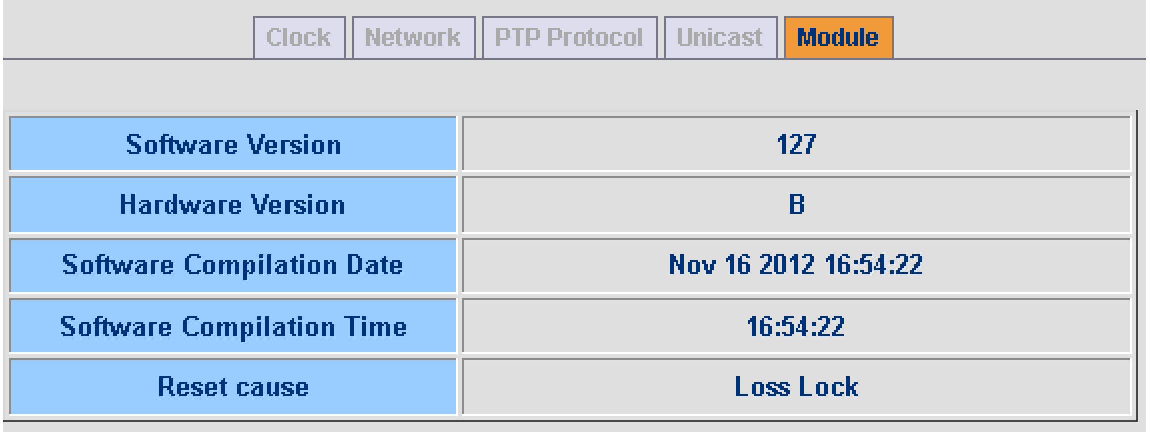


Unicast mode is not supported by the Master/Slave mode

Figure 8-46: PTP Status / Unicast Tab for Master-Slave Clocks

8.12.5.5 PTP Status / Module Information Tab

This tab displays status information on the current PTP module.



Software Version	127
Hardware Version	B
Software Compilation Date	Nov 16 2012 16:54:22
Software Compilation Time	16:54:22
Reset cause	Loss Lock

Figure 8-47: PTP Status / Module Tab

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.
Reset Cause: Information on the cause of the last reset operation.

8.12.6 PTP Setup Pages

The **PTP Setup** pages are available either through the “Inputs” display or the “Outputs” display. PTP setup options are available from the following tabs:

- **Network:** Network settings (Transport layer, Internet layer, PTP network)

- **Clock:** Settings regarding the PTP Clock
- **PTP Protocol:** General settings regarding the PTP protocol configuration
- **Unicast:** Information about the Unicast transmission mode

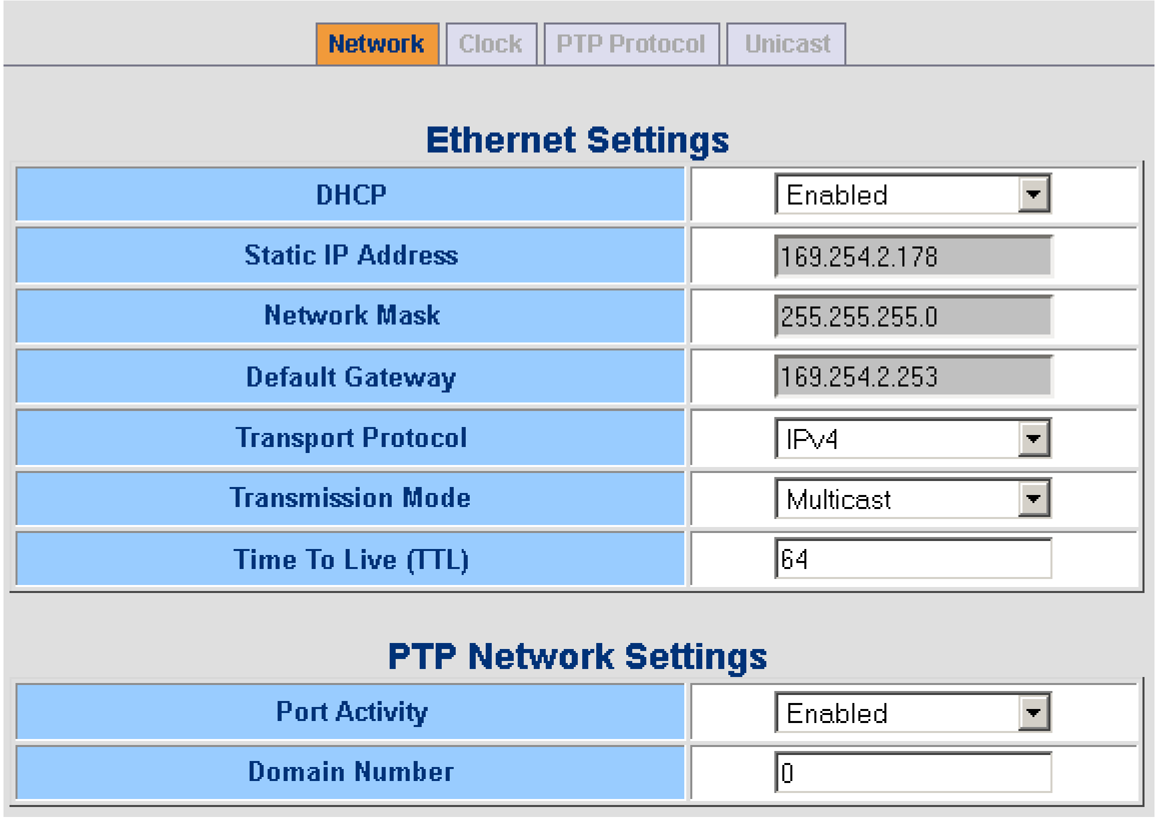
The following sections cover the configurable options for each of the **PTP Setup** tabs.

NOTE: Some parameters define a PTP packet's throughput. These use the "log2 seconds" unit, defined as follows:

- Positive Value: n => 2^n seconds between two successive PTP packets
- Negative Value: -n => $2^{(-n)}$ = $(1/2^n)$ => 2^n PTP packets per second

8.12.6.1 PTP Setup / Network Setup Tab

Networking options for the PTP device can be configured from this tab.



Ethernet Settings

DHCP	Enabled
Static IP Address	169.254.2.178
Network Mask	255.255.255.0
Default Gateway	169.254.2.253
Transport Protocol	IPv4
Transmission Mode	Multicast
Time To Live (TTL)	64

PTP Network Settings

Port Activity	Enabled
Domain Number	0

Figure 8-48: PTP Setup / Network Setup Tab

Ethernet Settings

DHCP Enable: Enables or disables the delivery of IP addresses from a DHCP Server Default setting: Enabled

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`].

Default setting: 169.254.macAddr5.macAddr6

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 setting: 255.255.255.0

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].
Default setting: 169.254.macAddr5.253

Transport Protocol: Selects the transport protocol used for PTP Packets
IPv4: Internet Protocol version 4 (Layer 3 protocol).
802.3/Ethernet: IEEE802.3/Ethernet Protocol (Layer 2 protocol).
Default setting: IPv4
Operating limitations: The IEEE802.3/Ethernet Protocol is not supported in Unicast transmission mode.

Transmission Mode: Addressing mode for IPv4 transmissions.
Multicast: PTP Module transmits PTP packets in multicast mode.
Unicast: PTP Module transmits PTP packets in unicast mode.
Minicast: Hybrid mode. PTP Module transmits in multicast mode if it is in Master state, and in unicast mode if it is in Slave state. This mode minimizes the PTP network payload.
Default setting: Multicast

Time To Live (TTL): 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.
Range: [1,255]
Default setting: 64

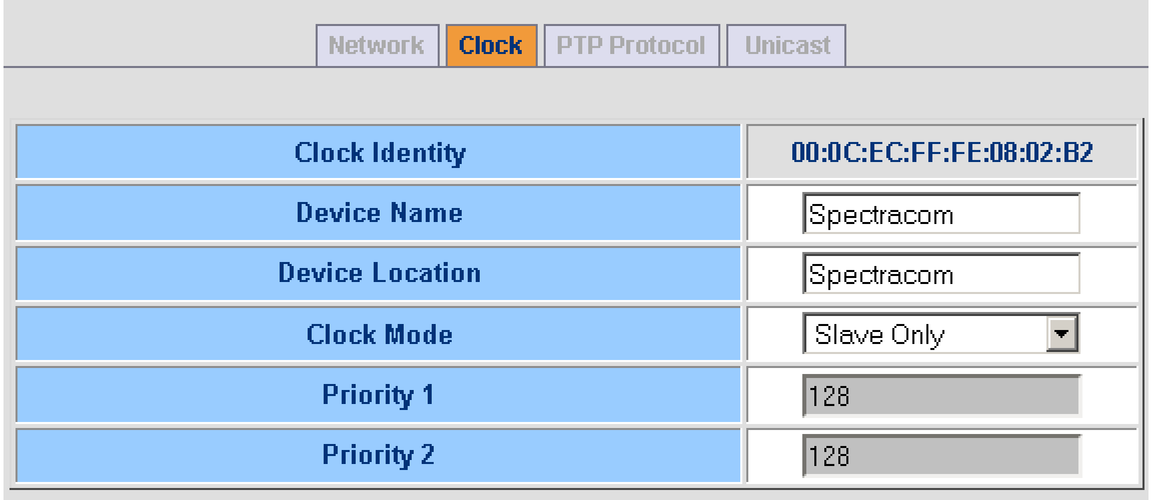
PTP Network Settings

Port Number: Enables / Disables the PTP port activity. If disabled, no PTP messages are transmitted and all PTP received messages are discarded except for management messages.
Default setting: Enabled

Domain Number: Sets the current PTP Domain Number, as defined in IEEE Std 1588-2008 Section 7.1.
Range: [0,255]
Default setting: 0

8.12.6.2 PTP Setup / Clock Setup Tab

The **Clock Setup** tab configures key operational parameters of the PTP device.



Clock Identity	00:0C:EC:FF:FE:08:02:B2
Device Name	Spectracom
Device Location	Spectracom
Clock Mode	Slave Only
Priority 1	128
Priority 2	128

Figure 8-49: PTP Setup / Clock Setup Tab

Clock Identity: A unique identifier for PTP devices, based on the MAC Address.

Device Name / Device Location: User-configurable strings for identification purposes (Default settings: `Spectracom` / `Spectracom`)

Clock Mode: The Master/Slave Mode of the PTP Module. Available options include the following:

- **Slave Only**
- **Master Only**
- **Master/Slave**

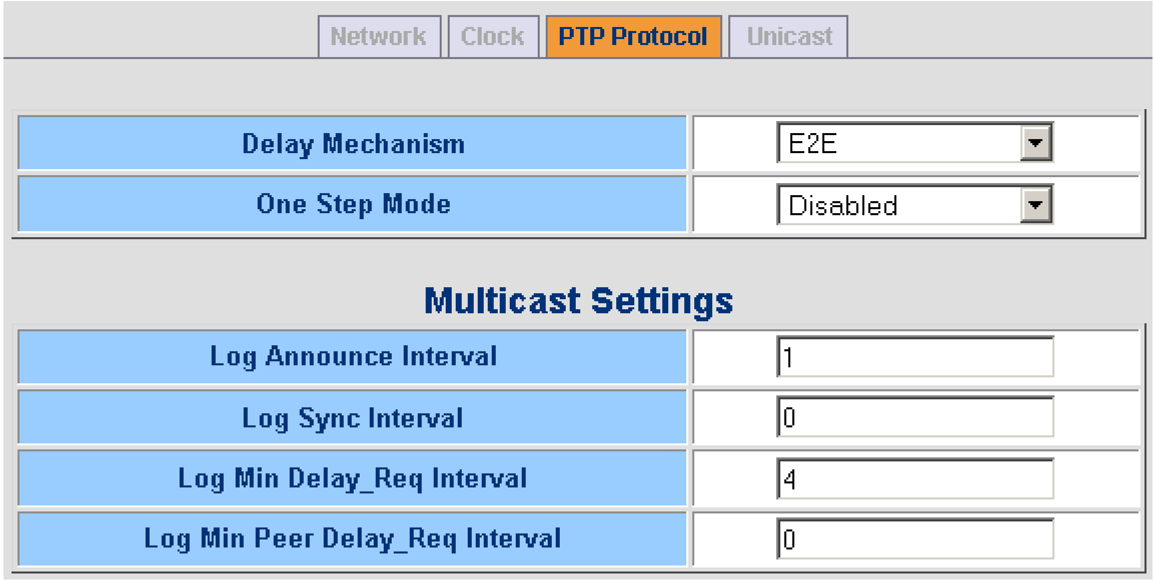
Default Setting: Slave Only
Operating Limitations: Master/Slave mode is not supported in unicast transmission mode.

Priority 1: See Section 8.10.1, 8.10.2 of IEEE 1588-2008.
Only settable for Master clocks (Master Only or Master/Slave mode). (Lower numbers mean higher priority).

Priority 2: See Section 8.10.1, 8.10.2 of IEEE 1588-2008.
Only settable for Master clocks (Master Only or Master/Slave mode).

8.12.6.3 PTP Setup / PTP Protocol Setup Tab

This tab allows configuration of various protocol-related options in **Multicast transmission mode**.



Delay Mechanism	E2E
One Step Mode	Disabled

Multicast Settings

Log Announce Interval	1
Log Sync Interval	0
Log Min Delay_Req Interval	4
Log Min Peer Delay_Req Interval	0

Figure 8-50: PTP Setup / Protocol Setup Tab

Delay Mechanism

E2E: End-to-End Delay Mechanism
P2P: Peer-to-Peer Delay Mechanism
Disabled: No Delay Mechanism
Default Setting: E2E
Operating limitations: 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.

One Step Mode: Determines the number of steps in the PTP protocol.

Disabled: Two-Step Mode is enabled
Enabled: One-Step Mode is enabled
Default setting: Disabled
Operating limitations: 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.

Log Announce Interval: A Master uses this value to determine the rate at which it sends out Announce messages in Multicast mode. The Slaves check the interval time between two consecutives Announce messages with the Announce Reception Timeout.
Units: log2 seconds. Range: [-9, 22].
Default setting: 1

Log Sync Interval: A Master uses this value to determine the rate at which Sync messages are transmitted in Multicast mode.
Units: log2 seconds. Range: [-9, 22].

Default setting: 0

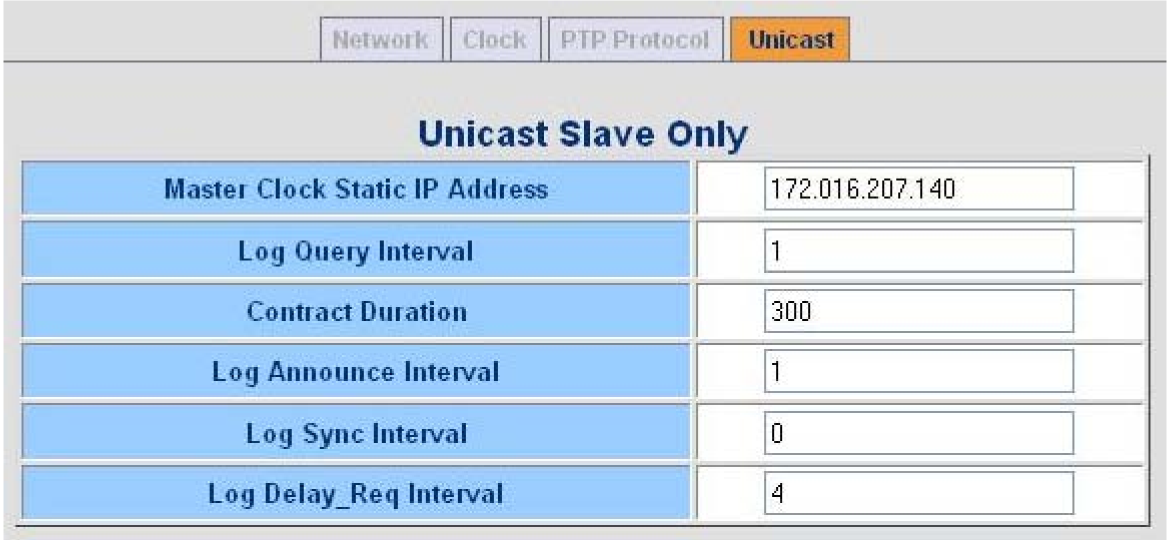
Log Min Delay_Req Interval: A Master will broadcast this value to Slaves to determine the rate at which Delay_Req messages are transmitted in Multicast mode (when the End-to-End Delay Mechanism is chosen).
Units: log2 seconds. Range: [-9, 22].
Default setting: 4

Log Min Peer Delay_Req Interval: A Master will broadcast this value to Slaves to determine the rate at which Delay_Req messages are transmitted (when the Peer-to-Peer Delay Mechanism is chosen).
Units: log2 seconds. Range: [-9, 22].
Default setting: 0

8.12.6.4 PTP Setup / Unicast Setup Tab

Settings regarding the Unicast transmission mode can be configured from this tab.

> **For a Slave-Only clock:** Settings declare a possible Master Clock with which the Slave Clock can communicate in Unicast mode.
> **For a Master-Only clock:** Settings enable the Unicast transmission mode for the Master Clock and define the operating limits of this mode.
> **For a Master/Slave clock:** Not supported.



Unicast Slave Only

Master Clock Static IP Address	172.016.207.140
Log Query Interval	1
Contract Duration	300
Log Announce Interval	1
Log Sync Interval	0
Log Delay_Req Interval	4

Figure 8-51: PTP Setup / Unicast Setup Tab for Slave-Only Clocks

Master Clock's Static 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].

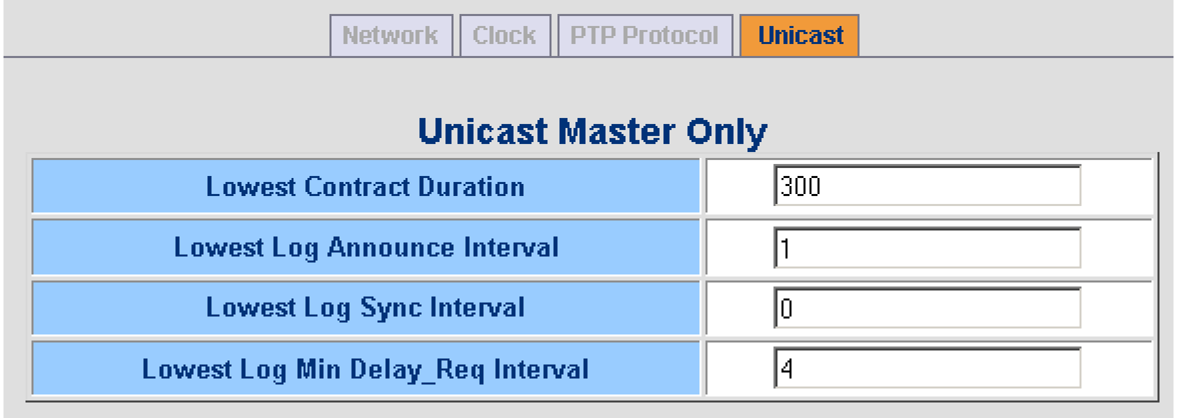
Log Query Interval: A Slave uses this value to determine the rate at which it requests for unicast contracts to the unicast Master when such requests fail.
Units: log2 seconds. Range: [-2, 22]
Default setting: 1

Contract Duration: Duration of the unicast contracts requested by Slaves to the unicast Master.
Units: seconds. Range: [10, 65535]
Default setting: 300

Log Announce Interval: Unicast Announce interval requested by Slaves to the unicast Master.
Units: log2 seconds. Range: [-3, 3]
Default setting: 1

Log Sync Interval: Unicast Sync interval requested by Slaves to the unicast Master.
Units: log2 seconds. Range: [-7, 1]
Default setting: 0

Log Min Delay_Req Interval: Unicast min Delay_Req interval requested by Slaves to the unicast Master.
Units: log2 seconds. Range: [-7, 6]
Default setting: 4



Unicast Master Only

Lowest Contract Duration	300
Lowest Log Announce Interval	1
Lowest Log Sync Interval	0
Lowest Log Min Delay_Req Interval	4

Figure 8-52: PTP Setup / Unicast Setup Tab for Master-Only Clocks

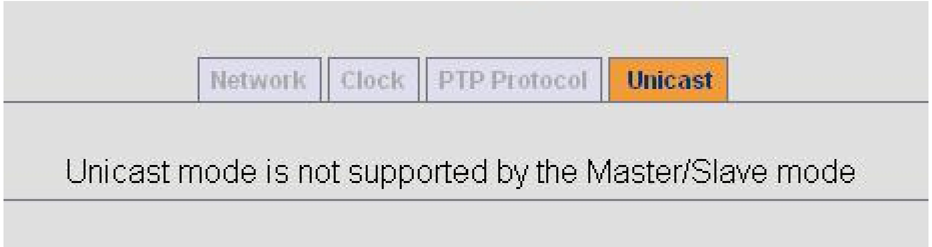
Lowest Contract Duration: Lowest value of unicast contract duration granted by the Master Clock.
Units: seconds. Range: [10, 65535]
Default setting: 300

Lowest Log Announce Interval: Lowest value of Announce interval granted by the Master Clock.
Units: log2 seconds. Range: [-3, 3]
Default setting: 1.

Lowest Log Sync Interval: Lowest value of Sync interval granted by the Master Clock.
Units: log2 seconds. Range: [-7, 1]
Default setting: 0

Lowest Log Min Delay_Req Interval: Lowest value of min Delay_Req interval granted by the Master Clock.
Units: log2 seconds. Range: [-7, 6]

Default setting: 4



Unicast mode is not supported by the Master/Slave mode

Figure 8-53: PTP Setup / Unicast Setup Tab for Master-Slave Clocks

8.13 Model 1204-14: Simulcast (CTCSS / Data Clock) Module

The CTCSS/Data Sync/Data Clock option module card provides CTCSS, data clock outputs, and alarm outputs through relays for the SecureSync platform through 1 DB-9 and 1 RJ-12 connector. The maximum number of cards installed is six (6).

Connector: **DB-9**	
Outputs:	(3) RS-485 Outputs (Data Clocks, CTCSS frequencies, 1PPS) (1) Alarm
Voltage:	Alarms: GND normally, high impedance when Alarm
Connector: **RJ-12**	
Outputs:	(1) RS-485 Outputs (Data Clocks, CTCSS frequencies, 1PPS) (2) Alarm
Voltage:	Alarms: 5V pulled up thru 10k Ω normally, GND when Alarm

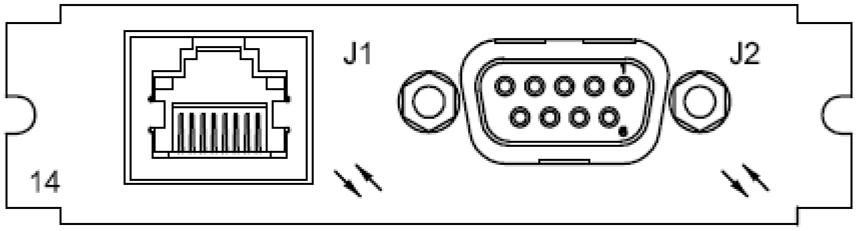


Figure 8-54: Model 1204-14 Option Module Card Rear Plate

Pin Assignments

Output #1 Connector: DB-9 Socket Timing Outputs

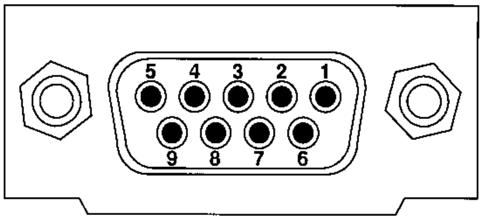


Figure 8-55: DB-9 Connector

PIN	NOTES	SIGNAL	819x Mapping	819x Option 17 Mapping
1	RS-485 + TERMINAL	OUTPUT 0+	+ 9.6 KHZ	+ CTCSS #1
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 -	- 1 PPS	- CTCSS #2
9	CABLE SHIELD	GROUND	GROUND	GROUND

Table 8-15: DB-9 Pin Assignments

Output #2 Connector: RJ-12 1PPS and Alarm Outputs

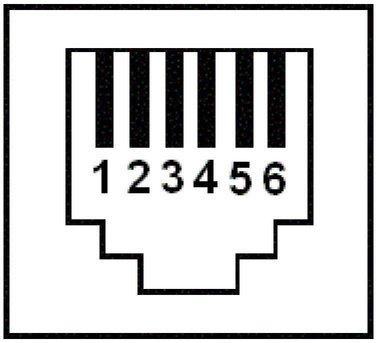


Figure 8-56: RJ-12 1PPS and Alarm Output Connector

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
5	5V = NORMAL GROUND = ALARM	MINOR ALARM RELAY	MINOR ALARM RELAY
6	CABLE SHIELD	GROUND	GROUND

Table 8-16: RJ-12 Pin assignments

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 8-17: CTCSS 1/3 Tones

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
1Z	100.0	5B	162.2	M7	250.3
1A	103.5	6Z	167.9	0Z	254.1

Table 8-18: CTCSS 1/10 Tones

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 8-19: Data Clock Signals

1PPS

Output	Duty Cycle
1PPS	20% ±5%

Table 8-20: 1PPS

8.13.1 Setup / Configuration

To manage this option module card, navigate to the **Setup / Outputs** page and select the Slot labeled “**Simulcast**”. From this page, options are available from the **Signals** and **Alarms** tabs, as detailed below.

Signals tab

Signal Type: Allows selection of the desired signal type. Available options include:

Disabled: No signal type.

CTCSS 1/3 Tones: Refer to Table 8-10: CTCSS 1/3 Tones.

CTCSS 1/10 Tones: Refer to Table 8-11: CTCSS 1/10 Tones.

Data Clocks: Refer to Data Clocks Signals section.

1PPS: 1PPS

Offset: Value (in nanoseconds) that can be used to adjust for cable delays or latencies.

Signature Control: Controls when the output will be present. Options include the following:

Output Always Enabled: The output is present, even when SecureSync is not synchronized to its references.

Output Enabled in Holdover: The output is present unless SecureSync is not synchronized to its references (the output is present while in the Holdover mode).

Output Disabled in Holdover: The output is present unless the SecureSync references are considered not qualified and invalid (the output is not present while in the Holdover mode).

Output Always Disabled: The output is not present, even if any SecureSync references are present and considered qualified.

Alarms tab

This tab allows configuration of the alarm type (**None / Disabled**, **Minor**, or **Major**) for both the DB-9 and RJ-12 connectors. Refer to sections *9.1.1* and *9.1.2* of this document for additional information on alarm types.

819x Option 17 Mapping

Use the following information for configuring option card 1204-14 for 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

NOTE: All outputs are disabled by default

8.13.2 Status Pages

To view current status and configuration information for this option module card, navigate to the **Status / Outputs** page and select the Slot labeled “**Simulcast**”.

8.14 Model 1204-15: Four IRIG Output Module

Inputs / Outputs:	(4) IRIG Output
Signal Type and Connector:	IRIG A, B, E, G, NASA 36, Amplitude Modulated (0v to 5v peak to peak into 50 Ω on BNC) or DC Level Shift (unmodulated), user selectable
Maximum Number of Cards:	6

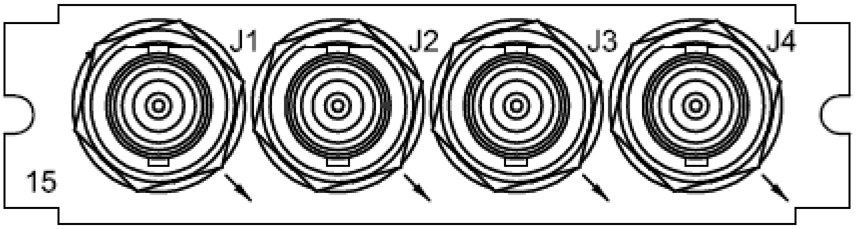
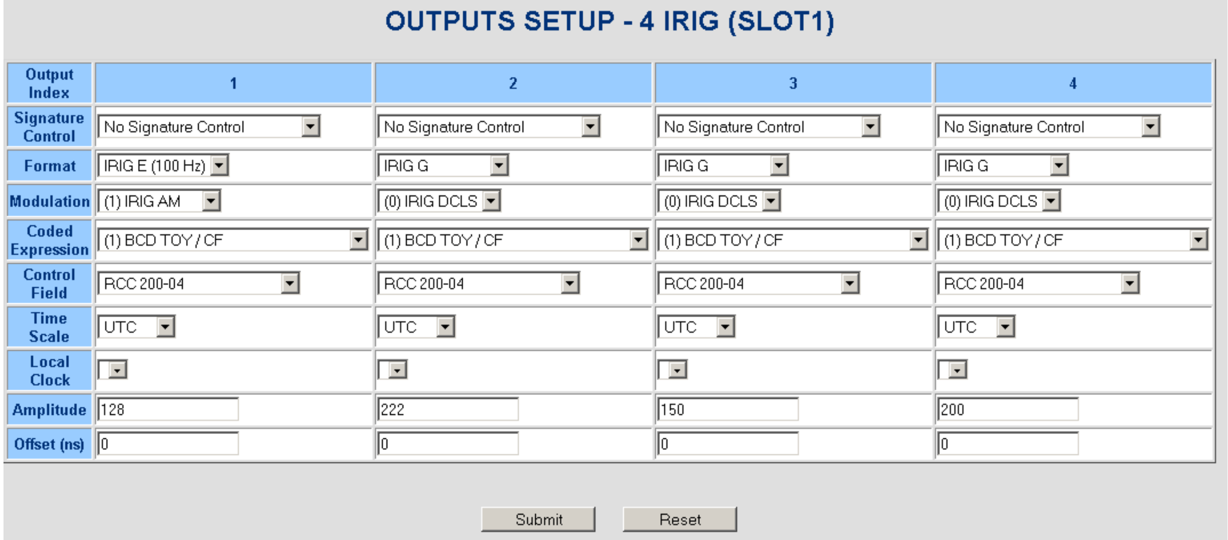


Figure 8-57: Model 1204-15 Option Module Card Rear Plate

8.14.1 IRIG Output Setup / Configuration

To manage the four IRIG outputs (BNC Connectors **J1** to **J4** on the IRIG module), navigate to the **Setup / Outputs** page and select the Slot labeled “**IRIG**”. Available options are as follows:



OUTPUTS SETUP - 4 IRIG (SLOT1)

Output Index	1	2	3	4
Signature Control	No Signature Control	No Signature Control	No Signature Control	No Signature Control
Format	IRIG E (100 Hz)	IRIG G	IRIG G	IRIG G
Modulation	(1) IRIG AM	(0) IRIG DCLS	(0) IRIG DCLS	(0) IRIG DCLS
Coded Expression	(1) BCD TOY / CF	(1) BCD TOY / CF	(1) BCD TOY / CF	(1) BCD TOY / CF
Control Field	RCC 200-04	RCC 200-04	RCC 200-04	RCC 200-04
Time Scale	UTC	UTC	UTC	UTC
Local Clock				
Amplitude	128	222	150	200
Offset (ns)	0	0	0	0

Figure 8-58: IRIG Output Setup

Signature Control: is used to control when the IRIG modulation will be present. This function allows the modulation to stop in certain situations.

> **Output Always Enabled:** IRIG time code modulation is present, even when SecureSync is not synchronized to its references.

Output Enabled in Holdover: IRIG time code modulation is present unless the SecureSync is not synchronized to its references (Modulation is present while in the Holdover mode).

Output Disabled in Holdover: IRIG time code modulation is present unless the SecureSync references are considered not qualified and invalid. (Modulation is not present while in the Holdover mode).

Output Always Disabled: No IRIG output modulation is present, even if any SecureSync input references are present and considered qualified.

Format: Used to configure the desired IRIG output formatting. The available choices are IRIG A, B, G, E (either 100 or 1000 Hz) and NASA-36.

Modulation: Changes the type of output signal modulation:

- **IRIG AM** is an amplitude modulated output. The amplitude of the output is determined by the value entered in the "Amplitude" field.
- **IRIG DCLS** is a TTL modulated output.

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

Control 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 as follows:

RCC IRIG Standard 200-4: Spectracom supports IRIG serial timecode formats A, B, G, and E, as defined by the Range Commanders Council (RCC) specification.
IEEE 1344: IRIG B format with extensions. Control Field contains year, Leap Second and DST information.
Spectracom Format: Year is included in Control Field but not in the same location as RCC-2004 output (year is offset by one position).
Spectracom FAA Format: A unique IRIG output Control Field that contains satellite lock status and time error flags.
NASA-36: A variant of IRIG B.

Amplitude: The peak-to-peak output voltage level into a 600 Ωload 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 5vp-p into high impedance. A value of 200 results in an output amplitude of about 9vp-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.

Time Scale: Used to select the time base for the output IRIG data stream. The available choices are UTC, TAI (Temps Atomique International), GPS and Local. UTC is also referred to as ZULU time. GPS is the raw GPS time as transmitted by the GNSS satellites (as of September, 2013, this is currently 16 seconds ahead of UTC time). IF GPS or TAI time is used, then the proper timescale offsets must be set up from the **Setup / Time Management** page. (Refer to Section *3.11.1*: "*Configuring the System Time Timescale*" for more information). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

Local Clock: System Time may be configured as UTC time, but it might be desired to output the IRIG time as local time instead. 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 IRIG output data stream. Refer to Section *3.11.3*: "*Local Clock Setup*" for more information on local clocks.

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). Available Offset range is -500 to +500 ms.

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	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	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	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
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	1 kHz	BCD$_{TOY}$, CF	10 pps	10 sec
IRIG-E	E122	AM	1 kHz	BCD$_{TOY}$	10 pps	10 sec
IRIG-E	E123	AM	1 kHz	BCD$_{TOY}$, SBS	10 pps	10 sec
IRIG-E	E124	AM	1 kHz	BCD$_{TOY}$, BCD$_{YEAR}$, CF and SBS	10 pps	10 sec
IRIG-E	E125	AM	1 kHz	BCD$_{TOY}$, BCD$_{YEAR}$, and CF	10 pps	10 sec
IRIG-E	E126	AM	1 kHz	BCD$_{TOY}$, BCD$_{YEAR}$	10 pps	10 sec
IRIG-E	E127	AM	1 kHz	BCD$_{TOY}$, BCD$_{YEAR}$, and SBS	10 pps	10 sec
IRIG-G	G000	DCLS	N/A	BCD$_{TOY}$, CF and SBS	10000 pps	10 msec
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
IRIG-G	G003	DCLS	N/A	BCD$_{TOY}$, SBS	10000 pps	10 msec
IRIG-G	G004	DCLS	N/A	BCD$_{TOY}$, BCD$_{YEAR}$, CF and SBS	10000 pps	10 msec
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	G007	DCLS	N/A	BCD$_{TOY}$, BCD$_{YEAR}$, and SBS	10000 pps	10 msec

IRIG-G	G140	AM	100 kHz	BCD_{TOY}, CF and SBS	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	G143	AM	100 kHz	BCD_{TOY}, SBS	10000 pps	10 msec
IRIG-G	G144	AM	100 kHz	BCD_{TOY}, BCD_{YEAR}, CF and SBS	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
IRIG-G	G147	AM	100 kHz	BCD_{TOY}, BCD_{YEAR}, and SBS	10000 pps	10 msec
NASA-36	NA	AM	1msec	UNKNOWN	100 pps	1 sec
NASA-36	NA	DCLS	10msec	UNKNOWN	100 pps	1 sec

Table 8-21: Available IRIG Output Signals

NOTE: 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.

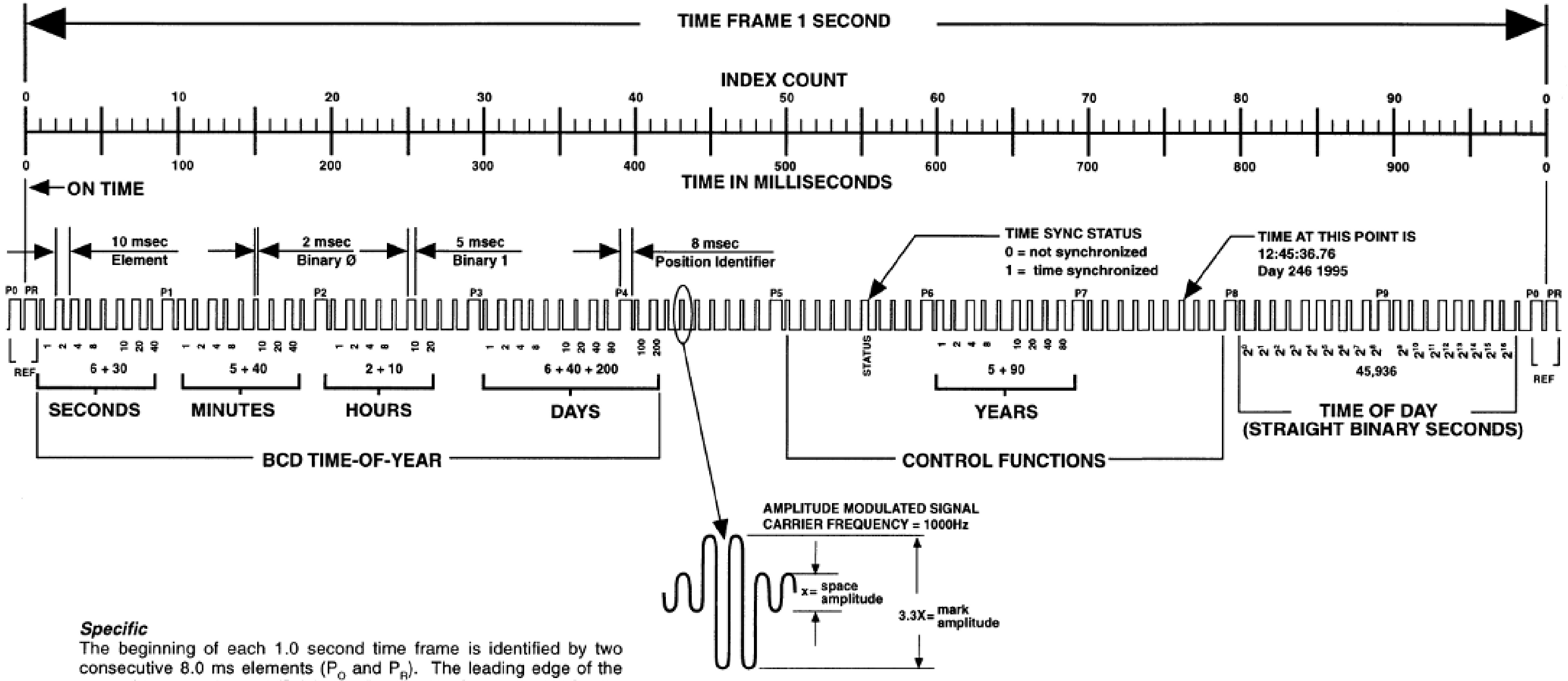
NOTE: DCLS is DC Level Shifted output, pulse width modulated with a position identifier having a positive pulse width equal to 0.8 of the reciprocal of the bit rate, a binary one (1) having a positive pulse width equal to 0.5 of the reciprocal of the bit rate and a binary zero (0) having a positive pulse width equal to 0.2 of the reciprocal of the bite rate.

The 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.

For reference, detailed information about the IRIG B and IRIG E formats follow.

8.14.1.1 IRIG B Output

IRIG B TIME



Specific
The beginning of each 1.0 second time frame is identified by two consecutive 8.0 ms elements (P_O and P_R). The leading edge of the second 8.0 ms element (P_R) is the "on time" reference point for the succeeding time code. 10 pps position identifiers P_0, P_1......P_9 (8.0 ms duration) occur 10 ms before 10 pps "on time" and refer to the leading edge of the succeeding element.

The two time code words and the control functions presented during the time frame are pulse width coded. The binary "zero" and index markers have a duration of 2.0 ms, and the binary "one" has a duration of 5.0 ms. The leading edge is the 100 pps "on time" reference point for all elements.

The binary coded decimal (BCD) time-of-year code word consists of 30 digits beginning at index count 1. The binary coded subword elements occur between position identifiers P_0 and P_5 (7 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.

Twenty-seven control functions occur between position identifiers P_5 and P_0. 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.

The straight binary (SB) time-of-day code word occurs between position identifiers P_8 and P_0. Seventeen digits give the time-of-day in seconds with the least significant digit occurring first. A position identifier occurs between the 9th and 10th binary coded elements. The straight binary code recycles every 24 hours.

Figure 8-59: 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.

Table 8-7 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. 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
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 8-22: IRIG B Control Function Field

8.14.1.2 IRIG E Output

The IRIG E code contains the Binary Coded Decimal (BCD) time of year and Control Functions. Figure 8-11 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 word - 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.

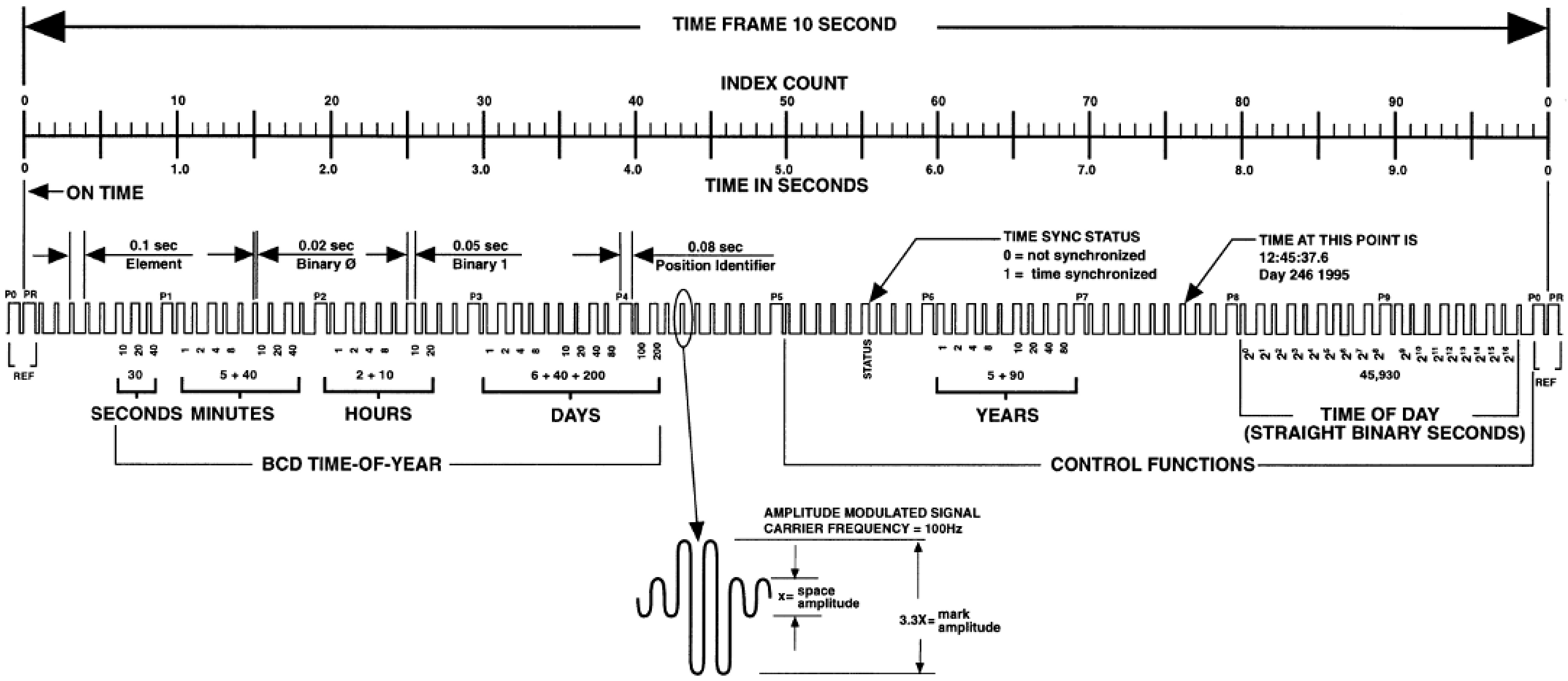
Elements 80 through 97 are encoded with the Straight Binary Seconds (SBS) time data. The SBS time data is incremented in 10-second steps and recycles every 24 hours.

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.

IRIG E TIME



Specific
The beginning of each 10 second time frame is identified by two consecutive 80 ms elements (P_O 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_0. 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.

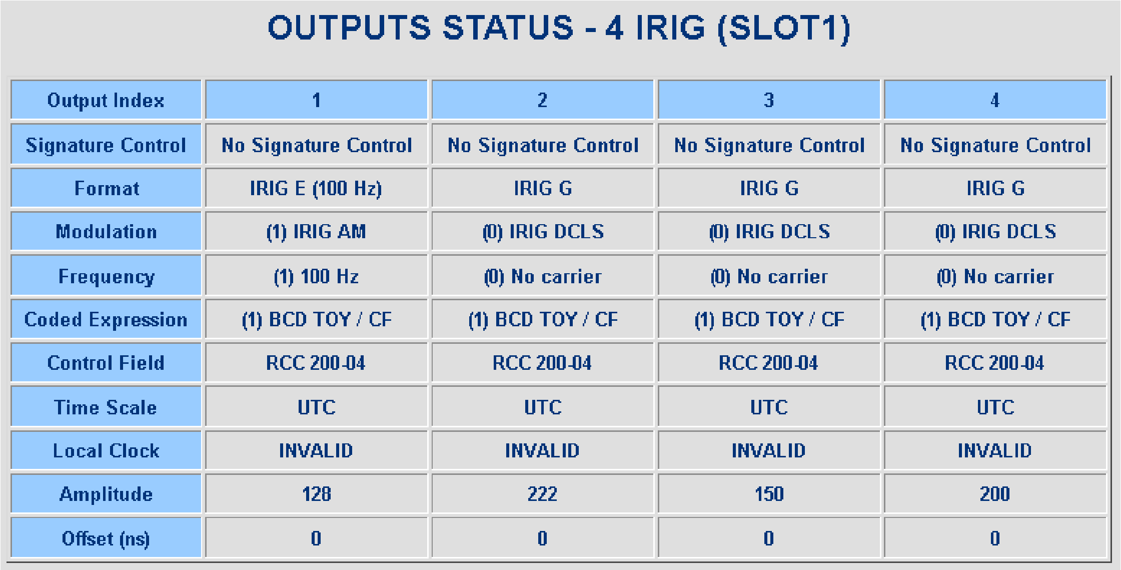
Figure 8-60: IRIG E Time Code Description

BIT #	CF ELEMENT #	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	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		
79	PID P8	POSITION		IDENTIFIER
80	28	SBS		2^{0}
81	29	SBS		2^{1}
82	30	SBS		2^{2}
83	31	SBS		2^{3}
84	32	SBS		2^{4}
85	33	SBS		2^{5}
86	34	SBS		2^{6}
87	35	SBS		2^{7}
88	36	SBS		2^{8}
89	PID P9	POSITION		IDENTIFIER
90	37	SBS		2^{9}
91	38	SBS		2^{10}
92	39	SBS		2^{11}
93	40	SBS		2^{12}
94	41	SBS		2^{13}
95	42	SBS		2^{14}
96	43	SBS		2^{15}
97	44	SBS		2^{16}
98	45	SPACE		
99	PID P0	POSITION IDENTIFIER		

Table 8-23: IRIG E Control Function Field

8.14.2 IRIG Output Status

To view current status and configuration information for this option module card, navigate to the **Status / Outputs** page and select the Slot labeled “**IRIG**”.



OUTPUTS STATUS - 4 IRIG (SLOT1)

Output Index	1	2	3	4
Signature Control	No Signature Control	No Signature Control	No Signature Control	No Signature Control
Format	IRIG E (100 Hz)	IRIG G	IRIG G	IRIG G
Modulation	(1) IRIG AM	(0) IRIG DCLS	(0) IRIG DCLS	(0) IRIG DCLS
Frequency	(1) 100 Hz	(0) No carrier	(0) No carrier	(0) No carrier
Coded Expression	(1) BCD TOY / CF	(1) BCD TOY / CF	(1) BCD TOY / CF	(1) BCD TOY / CF
Control Field	RCC 200-04	RCC 200-04	RCC 200-04	RCC 200-04
Time Scale	UTC	UTC	UTC	UTC
Local Clock	INVALID	INVALID	INVALID	INVALID
Amplitude	128	222	150	200
Offset (ns)	0	0	0	0

Figure 8-61: Example IRIG Output Status

The IRIG Output Status displays the current configurations of both IRIG outputs and the current IRIG Message.

8.15 Model 1204-17: Square Wave Out

The Model 1204-17 Square Wave output option module card provides four programmable square wave outputs for the SecureSync platform.

Inputs / Outputs:	(4) Programmable square wave outputs
Signal Type and Connector:	TTL (BNC)
Output Load Impedance:	50 Ω
Rise time to 90% of level:	<10ns
Programmable period:	100ns to 1,000,000,000ns in 5 ns steps, to 60,000,000us in 1us steps
Programmable pulse width:	20ns to 900ms with 20ns resolution
Maximum Number of Cards:	6

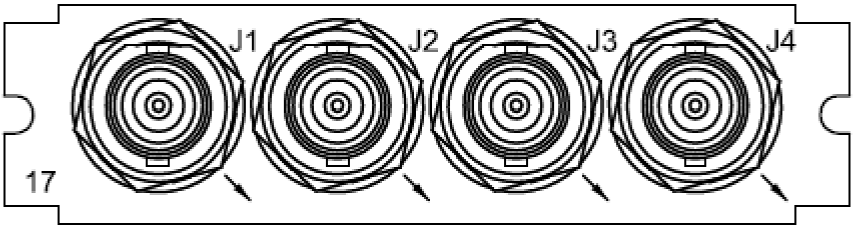


Figure 8-62: Model 1204-17 Option Module Card Rear Plate

8.15.1 Setup / Configuration

To manage the Square Wave outputs (**J1** to **J4** connectors on the Square Wave Output module), navigate to the **Setup / Outputs** page and select the Slot labeled "**SQUARE WAVE**". This page is divided into three sections: **General**, **Direct Value**, and **Square Wave**. Options in each section are as follows:

General

Output Mode

Direct Value: Output will be low or high determined by the output value selection.

Square Wave: Output will generate a programmable square wave determined by the configuration.

Output Enable: Disables or enables output.

Direct Value

Output Value: Determines the output level (low or high).

Square Wave

Signature control: Controls when the output will be present. Options include the following:

Output Always Enabled: The output is present, even when SecureSync is not synchronized to its references.

Output Enabled in Holdover: The output uses the current framing mode unless SecureSync is not synchronized to its references (the output is present while in the Holdover mode).

Output Disabled in Holdover: The output uses the current framing mode unless the SecureSync references are considered not qualified and invalid (the output is not present while in the Holdover mode).

Output Always Disabled: The output is not present, even if any SecureSync references are present and considered qualified.

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.

Period: Sets the period of the square wave (in ns or us scale).

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
```

Frequency (Hz): Calculated based on the Period and Period Correction settings.

Pulse Width (ns): Defines the pulse width of the output (entered in nanoseconds).

On-Time Point Pulse Width (ns): 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.

Re-initialize: Reinitializes square wave generation and aligns to 1PPS.

8.15.2 Status Pages

To view status information pages for this option module card, navigate to **Status / Outputs** and select the Slot labeled "**SQUARE WAVE**".

8.16 Models 1204-18, 1204-19, 1204-21, 1204-2B

8.16.1 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.

8.16.2 Model 1204-18 1PPS Output Specifications (TTL Option)

Inputs / Outputs:	(4) 1PPS output
Signal Type and Connector:	TTL (BNC)
Output Load Impedance:	50 Ω
Rise time to 90% of level:	<10ns
Programmable pulse width:	100ns to 500ms with 20ns resolution
Absolute phase error:	±50ns (1σ)
Programmable phase shift:	±5ns to 500ms with 5ns resolution
Maximum Number of Cards:	6

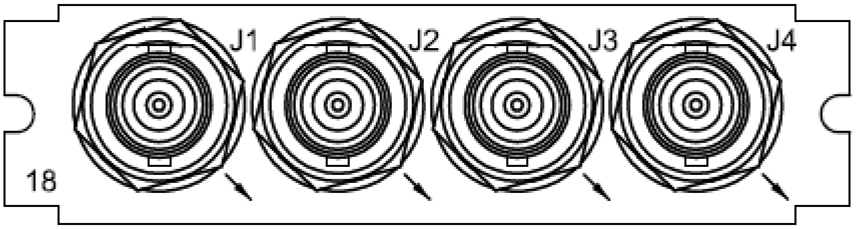


Figure 8-63: Model 1204-18 Option Module Card Rear Plate

8.16.3 Model 1204-19 1PPS Output Specifications (10V Option)

Inputs / Outputs:	(4) 1PPS output
Signal Type and Connector:	10V (BNC)
Output Load Impedance:	50 Ω
Rise time to 90% of level:	<30ns
Programmable pulse width:	100ns to 500ms with 20ns resolution
Absolute phase error:	±50ns (1σ)

Programmable phase shift:	±5ns to 500ms with 5ns resolution
Maximum Number of Cards:	6

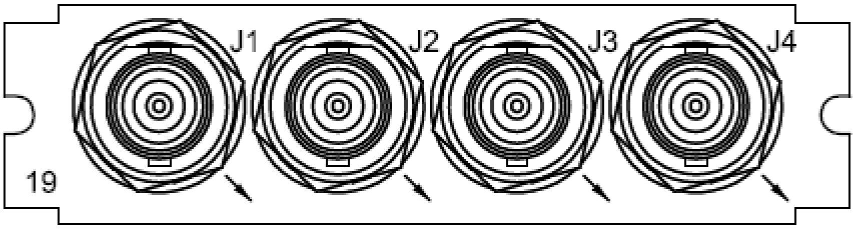


Figure 8-64: Model 1204-19 Option Module Card Rear Plate

8.16.4 Model 1204-21 1PPS Output Specifications (RS-485 Option)

Inputs / Outputs:	(4) 1PPS output
Signal Type and Connector:	RS-485 (Terminal Block)
Output Load Impedance:	120 Ω
Rise time to 90% of level:	<10ns
Programmable pulse width:	100ns to 500ms with 20ns resolution
Absolute phase error:	±50ns (1σ)
Programmable phase shift:	±5ns to 500ms with 5ns resolution
Maximum Number of Cards:	6

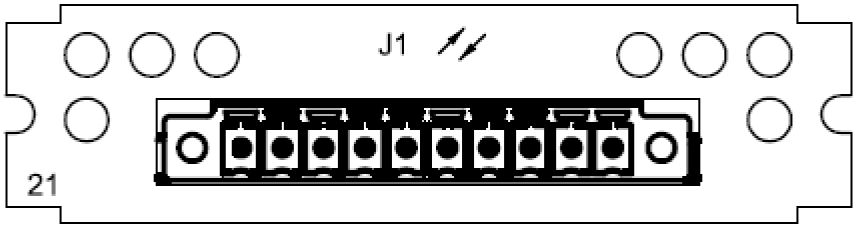


Figure 8-65: Model 1204-21 Option Module Card Rear Plate

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 +
7	1PPS Output 3 -
8	GND
9	1PPS Output 4 +
10	1PPS Output 4 -

Table 8-24: Model 1204-21 1PPS Output card Pin Assignments

8.16.5 Model 1204-2B 1PPS Output Specifications (Fiber Option)

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:	100ns to 500ms with 20ns resolution
Absolute phase error:	±50ns (1σ)
Programmable Phase Shift:	±5ns to 500ms with 5ns resolution
Maximum Number of Cards:	6

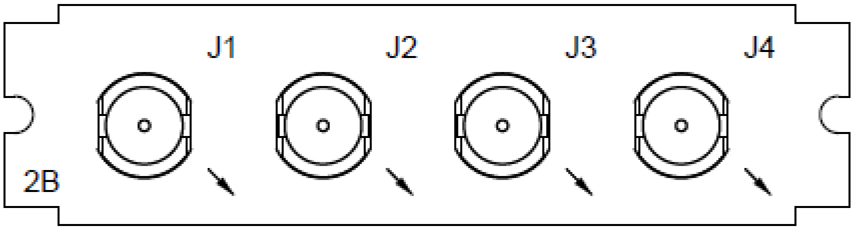
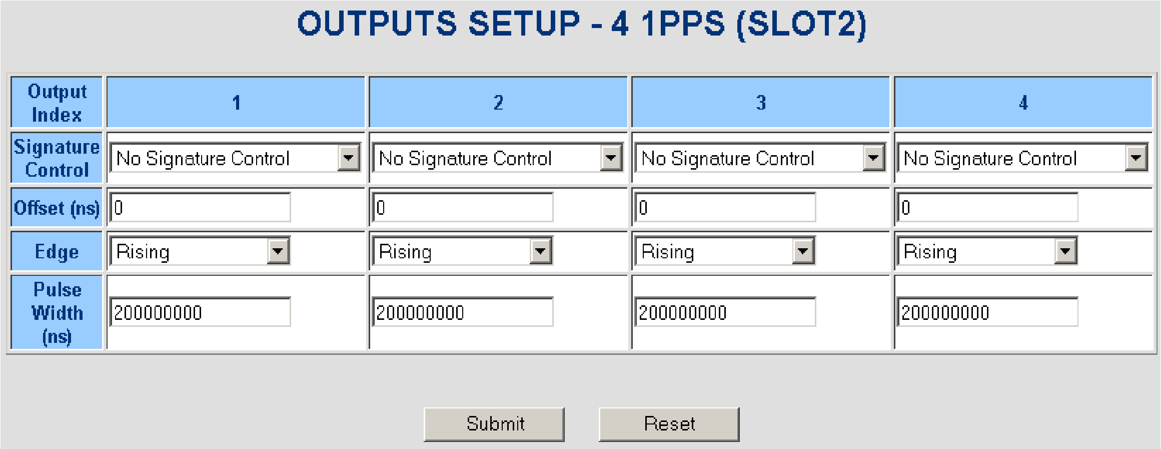


Figure 8-66: Model 1204-2B Option Module Card Rear Plate

8.16.6 1PPS Output Setup / Configuration

To manage the 1PPS outputs (**J1** to **J4** BNC connectors or **J1** terminal block on the 1PPS Output module), navigate to the **Setup / Outputs** page and select the Slot labeled “**1PPS**”. Configurable options are as follows:


OUTPUTS SETUP - 4 1PPS (SLOT2)

Output Index	1	2	3	4
Signature Control	No Signature Control	No Signature Control	No Signature Control	No Signature Control
Offset (ns)	0	0	0	0
Edge	Rising	Rising	Rising	Rising
Pulse Width (ns)	200000000	200000000	200000000	200000000

Figure 8-67: 1PPS Output setup page

Signature Control: Signature Control is used to control when the 1PPS output signal will be present. This function allows the modulation to stop in certain situations.

> **Output Always Enabled:** 1PPS output is present, even when SecureSync is not synchronized to its references.
>
> **Output Enabled in Holdover:** 1PPS output is present unless the SecureSync is not synchronized to its references (modulation is present while in the Holdover mode).
>
> **Output Disabled in Holdover:** 1PPS output is present unless the SecureSync references are considered not qualified and invalid. (Modulation is not present while in the Holdover mode).
>
> **Output Always Disabled:** No 1PPS output is present, even if any SecureSync input references are present and considered qualified.

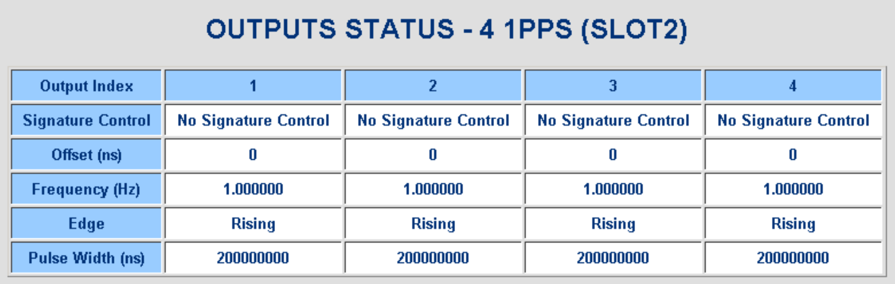
Offset: Used to account for 1PPS cable delays or other latencies in the 1PPS output.

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 (the default Pulse Width is 200 milliseconds).

8.16.7 Status Pages

To view current output status and configuration information for this option card, navigate to the **Status / Outputs** page and select the Slot labeled "**1PPS**".



OUTPUTS STATUS - 4 1PPS (SLOT2)

Output Index	1	2	3	4
Signature Control	No Signature Control	No Signature Control	No Signature Control	No Signature Control
Offset (ns)	0	0	0	0
Frequency (Hz)	1.000000	1.000000	1.000000	1.000000
Edge	Rising	Rising	Rising	Rising
Pulse Width (ns)	200000000	200000000	200000000	200000000

Figure 8-68: 1PPS and Frequency Output status page

Information displayed on this page includes the following:

Signature Control: Displays the current configuration of Signature Control.

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.

Frequency: Indicates the configured frequency of the 1PPS output signal.

Pulse Width: Displays the configured Pulse Width of the 1PPS output. The Pulse Width is displayed in nanosecond (default Pulse Width is 200 milliseconds).

8.17 Model 1204-23: Event Broadcast

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.

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:	5 nanoseconds
Minimum Time Between Events:	20 nanoseconds
Message Buffer Size:	512 messages

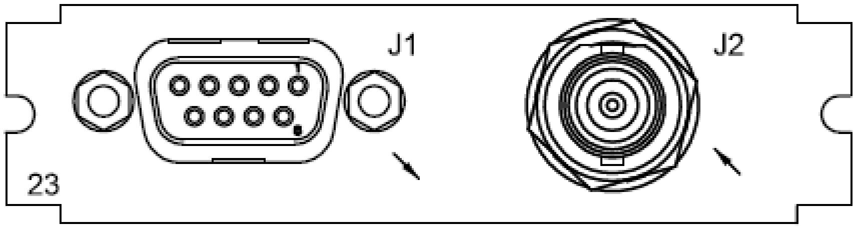


Figure 8-69: Model 1204-23 Option Module Card Rear Plate

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 5 ns resolution. Event Broadcast Output formats are detailed in *11.1*.

8.17.1 Setup / Configuration

To manage the Event Broadcast port options, navigate to the **Setup / Outputs** page and select the Slot labeled “**EVENT BROADCAST**”. Available options are as follows:

Event Enable: 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.

Reset Event Buffer: When set to “Enabled”, will discard all messages waiting in the Event Buffer.

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 is transmitted once the signature control conditions permit.)

> **Output Always Enabled:** All events are broadcast, even when SecureSync is not synchronized to its references.
>
> **Output Enabled in Holdover:** All events are broadcast unless SecureSync is not synchronized to its references.
>
> **Output Disabled in Holdover:** All events are broadcast unless the SecureSync references are considered not qualified and invalid.
>
> **Output Always Disabled:** No events are broadcast even if any SecureSync references are present and considered qualified.

ASCII Format: Selects the format of the message to be outputted. Refer to *11.1* 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.

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.

Time Scale: Used to select the time base for the output messages. 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, TAI (Temps Atomique International), GPS and Local. UTC is also referred to as ZULU time. GPS is the raw GPS time as transmitted by the GNSS satellites (as of September, 2013, this is currently 16 seconds ahead of UTC time). If GPS or TAI time is used, then the proper timescale offsets must be set on the **Setup / Time Management** page. (Refer to Section *3.11.1*: "*Configuring the System Time Timescale*" for more information). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

Local Clock: The incoming 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 event messages. Refer to Section *3.11.3*: "*Local Clock Setup*" for more information on Local Clocks.

Request character: This field defines the character that SecureSync needs to receive in order for a message to be provided when in "Request" mode.

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.

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 8-25: Output DB9 Connector Pinout

8.17.2 Event Broadcast Status Pages

To view output status information for this option module card, navigate to the **Status / Outputs** page and select the Slot labeled "**EVENT BROADCAST**".

8.18 Model 1204-28, 1204-2A: 1 PPS Input/Output

The 1PPS input/output module provides one 1PPS input, and three or two additional 1PPS outputs on BNC or ST connectors for the SecureSync platform.

8.18.1 Model 1204-28 1PPS 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:	<10ns
Programmable pulse width:	100ns to 500ms with 20ns resolution
Absolute phase error:	±50ns (1σ)
Programmable phase shift:	±5ns to 500ms with 5ns resolution
Maximum Number of Cards:	6

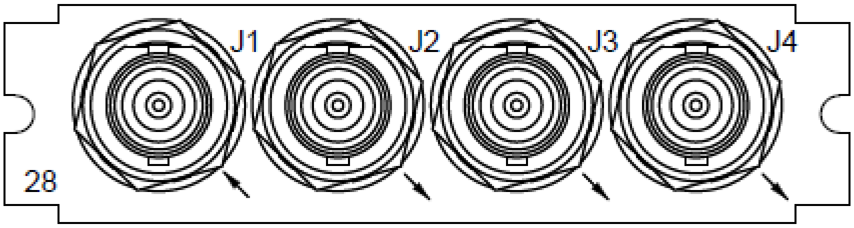


Figure 8-70: Model 1204-28 Option Module Card Rear Plate

8.18.2 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:	100ns to 500ms with 20ns resolution
Output absolute phase error:	±50ns (1σ)
Output programmable phase shift:	±5ns to 500ms with 5ns resolution
Maximum number of cards:	6

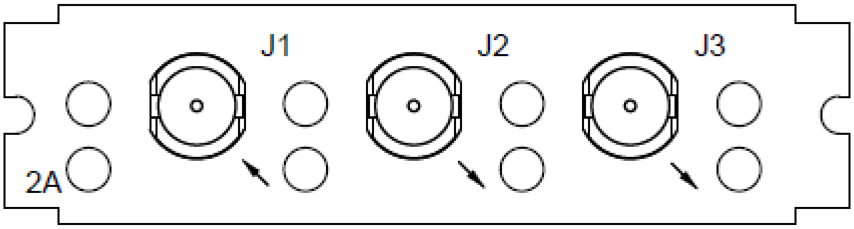


Figure 8-71: Model 1204-2A Option Module Card Rear Plate

8.18.3 1PPS Input Setup / Configuration

To configure the 1PPS input (“**J1**” connector on the 1PPS input/output module) navigate to the **Setup / Inputs** page and select the Slot labeled “**1PPS Input/Output**”. Available options are as follows:

Offset: It is possible to add an offset to the input signal (to account for cable delays), with a resolution of 20ns and a positive or negative value of 500ms maximum.

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).

To view current 1PPS input status and configuration information for this option card, navigate to the **Status / Inputs** page and select the Slot labeled “**1PPS Input/Output**”. The 1PPS Input signal is analyzed and an absence of the signal triggers a “Not Valid” indication.

Information displayed on this page includes the following:

Reference ID: Name used to represent this 1PPS input reference in the Reference Priority table (refer to Section *3.17*: “ *Reference Priority Input* Configuration” for more information on the Reference Priority Input table).

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.

Offset: Displays the configured 1PPS offset values.

Edge: Displays the selected Edge (rising of falling) of the 1PPS input that defines the on-time point.

8.18.4 1PPS Output Setup / Configuration

To configure the 1PPS outputs (**J2** to **J4** connectors on the 1PPS Input/Output module), navigate to **Setup / Outputs** and select the Slot labeled "**1PPS Input/Output**". Available options are as follows:

Signature Control: Signature Control is used to control when the 1PPS output signal will be present. This function allows the modulation to stop in certain situations.

Output Always Enabled: 1PPS output is present, even when SecureSync is not synchronized to its references.

Output Enabled in Holdover: 1PPS output is present unless the SecureSync is not synchronized to its references (modulation is present while in the Holdover mode).

Output Disabled in Holdover: 1PPS output is present unless the SecureSync references are considered not qualified and invalid. (Modulation is not present while in the Holdover mode).

Output Always Disabled: No 1PPS output is present, even if any SecureSync input references are present and considered qualified.

Offset: Used to account for 1PPS cable delays or other latencies in the 1PPS output.

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 (the default Pulse Width is 200 milliseconds).

8.18.5 Status Pages

To view status information pages for this option module card, navigate to **Status / Outputs** and select the Slot labeled "**1PPS Input/Output**".

8.19 Model 1204-2E Failover Module

Output follows selected input. Signals can be 1PPS, 10MHz, 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". When input "A" becomes valid again, 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.

8.19.1 Model 1204-2E Specifications

Inputs / Outputs:	(2) Inputs – Unselected input terminated with 50 Ω (1) Output
Connector:	3 BNC
Signal Type:	User selected: • >1 MHz • 1MHz to 100Hz • 1PPS
Signal Level:	• Sine Wave, 0.5V to 30V pp • TTL (50 Ω)
Default Power-on Switch State:	Input "B"
Maximum Number of Cards:	6
Ordering Information:	1204-2E: Failover Module

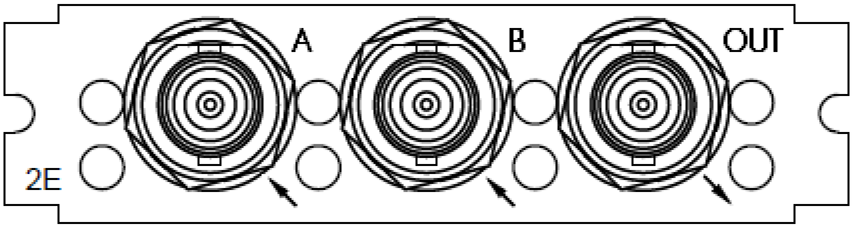


Figure 8-72. Model 1204-2E Option Module Card Rear Plate

8.20 Model 1204-29 HAVE QUICK Input/Output Module

The HAVE QUICK input / output module provides SecureSync with one available HAVE QUICK input and four available HAVE QUICK outputs.

8.20.1 Model 1204-29 HAVE QUICK Input/Output 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:	<10µs after 1PPS output
Programmable phase shift:	±5ns to 500ms with 5ns resolution
Maximum Number of Cards:	6

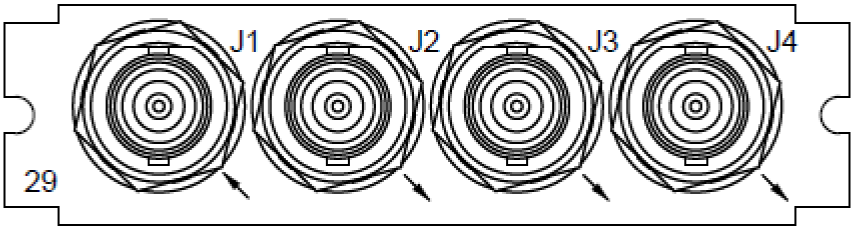


Figure 8-73: Model 1204-29 Option Module Card Rear Plate

8.20.2 HAVE QUICK Input Setup / Configuration

To configure HAVE QUICK input options for this module card (BNC connector **J1**), navigate to **Setup / Inputs** and select the Slot labeled “**HAVEQUICK IN/OUT**”.

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
- ICD-GPS-060A HAVE QUICK

Time Scale: Used to set the desired time scale (UTC, TAI, GPS, or Local).

Offset (ns): 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 +500ms in 5ns steps.

8.20.3 HAVE QUICK Output Setup / Configuration

To configure the three HAVE QUICK BNC outputs (**J2** to **J4** BNC connectors on the HAVE QUICK module), navigate to **Setup / Outputs** and select the Slot labeled "**HAVEQUICK IN/OUT**".

Output Index: Correlates to the three BNC Output connectors on the HAVE QUICK module (left to right as viewed on the SecureSync back panel, where 1 is the left-most BNC connector).

Signature Control: Signature Control is used to control when the HAVE QUICK modulation is present.

Output Always Enabled: HAVE QUICK time code modulation is present, even when SecureSync is not synchronized to its reference (Modulation is present while in the Holdover mode).

Output Enabled in Holdover: HAVE QUICK time code modulation is present unless the SecureSync is not synchronized to its references (modulation is present while in the Holdover mode).

Output Disabled in Holdover: HAVE QUICK time code modulation is present unless the SecureSync references are not considered qualified and valid. (Modulation is not present while in the Holdover mode).

Output Always Disabled: No HAVE QUICK output modulation is present, even if the SecureSync references are present and considered qualified.

Format: Used to configure the formatting of the four available HAVE QUICK outputs. Available output formats include:

- STANAG 4246 HAVE QUICK I
- STANAG 4246 HAVE QUICK II
- STANAG 4372 HAVE QUICK IIA
- STANAG 4430 Extended HAVE QUICK
- ICD-GPS-060A HAVE QUICK

Time Scale: This option configures the time scale for the LED time display. The available options are UTC, TAI (Temps Atomique International), GPS and Local. UTC is also referred to as ZULU time. GPS 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). If GPS or TAI time is used, then the proper timescale offsets must be set on the **Setup / Time Management** page. (Refer to Section *3.11.1*: *"Configuring the System Time Timescale"* for more information). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

Local Clock: System Time may be configured as UTC time, but it might be desired to output the IRIG time as local time. 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 IRIG output data stream. Refer to Section *3.11.3*: *"Local Clock Setup"* 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.

8.20.4 Status Pages

To view status information pages for this option module card, navigate to **Status / Outputs** and select the Slot labeled “**HAVEQUICK IN/OUT**”.

Section 9: General SecureSync Troubleshooting

The front panel LEDs and the web interface provide SecureSync status information that can be used to help troubleshoot failure symptoms that may occur.

9.1 Troubleshooting Front Panel LED Status Indications:

The front panel LEDs can provide “local” status information about the SecureSync. Observe the front panel 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) Refer to Section 2.2
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) Refer to Section 3.17.
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. Refer to Section 3.17. 2) Make sure desired input references are still connected to the correct port of SecureSync. 4) Verify GNSS antenna installation (if applicable). Refer to Section 9.4
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 Section 3.17. 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.

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 Section 9.4 for additional information.
Fault	LED is solid red	Major alarm is asserted	Refer to Section *9.1.1*
Fault	LED is solid orange	Minor alarm is asserted	Refer to Section *9.1.2*

Table 9-1: Troubleshooting front panel LED indications

9.1.1 Fault Light - Major Alarm

There are several conditions that can cause the front panel Fault lamp 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.
- **Too few GPS sat 2nd threshold:** The GNSS receiver is continuing to track less than the minimum number of satellites. Refer to Section *9.4*: "*Troubleshooting GNSS Reception Issues (Holdover and/or Time Sync Alarms Occurring)*:" for information on troubleshooting GNSS reception issues.
- **GPS Receiver Fault:** There was a problem with communications between SecureSync and its GNSS receiver.
- **The SAASM key has expired (applicable to the SAASM GPS receiver option module only):** Re-install new crypto keys for the SAASM receiver. The receiver will operate in commercial mode until new keys have been installed.

9.1.2 Fault light - Minor Alarm

There are several conditions that can cause the front panel Fault lamp to indicate a Minor alarm has been asserted. These conditions include:

- **Too few GPS sat 1st threshold:** The GNSS receiver has been tracking less than the minimum number of satellites for too long of a duration. Refer to Section *9.4* for information on troubleshooting GNSS reception issues.
- **The SAASM key expiring soon (applicable to the SAASM GPS receiver option module only):** A new crypto key will need to be loaded soon.
- **The unit has rebooted:** SecureSync was either rebooted or intentionally/inadvertently power cycled.

9.2 Unable to Open SecureSync Web User Interface:

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 product web interface.

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 cross-over 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 cross-over cable.

Table 9-2: Troubleshooting network connection issues

9.3 Troubleshooting Web Interface Status Page Indications

SecureSync's web user interface 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	Current Status	Indication	Troubleshooting
Status / Time and Frequency page	Synchronization is not "OK" (Orange instead of green)	SecureSync is either in Holdover mode (Holdover field will indicate "In Holdover"), or is now out of Time Sync.	All available Input References have been lost. Reference Status table on this same 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. Refer to Section 3.16 2) Make sure desired input references are still connected to the correct input port of SecureSync. 3) Verify GNSS antenna installation (if applicable). Refer to Section 9.4
Status / Inputs page - OR - **Status / Power** page	AC and/or DC indicate "ALARM" (Red instead of green)	Specified AC and/or DC input power is not present	Refer to Section 2.6 for AC and DC power connection information: If AC 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 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.
Status / **Inputs NTP** page	Stratum 16	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 **Setup / Reference Priority** table has all available references enabled. Refer to Section 3.17. 2) Verify Reference Status table in the **Status / Time and Frequency** page shows “OK“ (Green) for all available references. 3) Verify NTP is enabled and configured correctly. Refer to Section 0.
Network / General Setup / Access tab	Cannot login or access the web interface.	The following error message is displayed: “`ERROR: You are trying to access a system file, which is forbidden…`”	This message is displayed when any value has been added to this table and your PC is not listed in the table as an “allow from” IP address. To restore access to the web interface, either login from a PC that is listed as an “allow from” in this table. If it is unknown what PC’s have been listed in the Access table, perform an **`unrestrict`** command to remove all entries from the Access table. This will allow all PC’s to be able to access the web interface.

Table 9-3: Troubleshooting Web Interface Indications

9.4 Troubleshooting GNSS Reception Issues (Holdover and/or Time Sync Alarms Occurring):

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 many 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 *SecureSync GNSS Reception Troubleshooting* document, available from the Spectracom website (visit www.spectracomcorp.com and from the site navigation menu, select **Support → Library → Installation and Troubleshooting Guides**).

9.5 Front Panel Keypad is Inoperative:

The front keypad can be locked in order to prevent inadvertent operation. It can be locked and unlocked using either the keypad or the web interface. When locked, the keypad operation is disabled until it is unlocked using either of the two following processes:

A) To unlock the front panel keypad using the keypad (locally):

1) Perform the following key sequence:

↑ ↓ ↑ ↓ ← → ← → ✓ x ✓

B) To unlock the front panel keypad using the web browser (remotely):

1) Open the SecureSync web interface and navigate to the **Setup / Front Panel** page.
2) Change the "Lock" from "Enabled" to "Disabled".
3) Press the Submit button.

9.6 No 1PPS and / or 10 MHZ Output Present:

If the 1PPS and / or the 10 MHz output 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
Navigate to **Status / Time And Frequency** page	Reference Status Table	One or more input references indicate "Not Valid" (Orange)	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 orange is not valid, or not present). If Signature Control is enabled in this state, the output may be disabled: 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 **Setup / Outputs** page	Click on "Outputs: 1PPS/FREQUENCY"	Signature Control	1) With "No signature control" 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 9-4: Troubleshooting 1PPS and/or 10 MHz outputs not being present

9.7 The Front Panel LCD Window is Blank:

As long as input power is applied (as indicated by the power light being green and the LED time display incrementing) the LCD can display data. The LCD can be configured to display different information while the keypad is not in use. One available configuration is to have the LCD display a blank page when not in use. The LCD window operation can be verified and can also be configured via the web interface or the front panel keypad.

A) **Using the front panel keypad to verify the LCD is configured to display a blank page:**
To verify the front panel LCD 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 LCD display 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 to display something other than a blank page (such as GNSS information, network configuration, etc), refer to Section *2.10*.

C) **Using the web browser to change the information normally displayed in the LCD when the keypad is not in use:**

To use the web UI to reconfigure the LCD to display something other than a blank page (such as GNSS information, network configuration, etc), refer to Section *3.12*.

9.8 Front Panel Serial Port is Not Responding:

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 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.

1. 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.

2. 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.

3. Refer to *Section 10*: "*Using HyperTerminal to Connect to SecureSync*" for more information on using HyperTerminal (or similar terminal emulator software) to communicate with the SecureSync via serial port.

9.9 Front Panel Cooling Fan is Not Running:

The cooling fan (located on the front panel, to the right of the LED time display) is a temperature controlled cooling fan. An internal temperature sensor determines 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 the 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.

9.10 Network PCs are not able to Synchronize to SecureSync:

In order for clients on the network to be able to sync to SecureSync, a few factors have to be met.

1. The PC(s) must be routable to SecureSync. Make sure you can access the SecureSync product web interface from a PC that is not syncing. If the PC can't access the web interface, 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 Spectracom website (www.spectracomcorp.com), and from the main site navigation menu select **Support > Library > Installation and Troubleshooting Guides**, 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 the 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 *3.18.2* and *3.18.4*, respectively. A network or PC issue likely exists. A firewall may be blocking Port 123 (NTP traffic), for example.

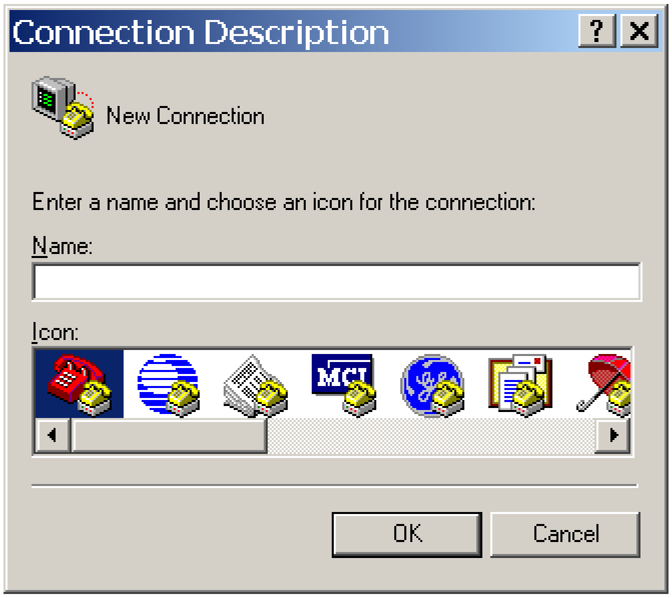
4. NTP in SecureSync must be "in sync" and at a higher Stratum level than Stratum 16 (such as Stratum 1 or 2, for example). This requires SecureSync to be either synced to its input references or in Holdover mode. Check the current NTP stratum level and the sync status. Refer to Sections *4.2.1* and *4.2.3*.

Section 10: Using HyperTerminal to Connect to SecureSync

In Microsoft Windows versions up to and including Windows XP, the HyperTerminal program is typically located under Accessories → Communications in the Windows PC Start Menu.

NOTE: Starting with the release of Windows Vista, Microsoft discontinued including the HyperTerminal program along with the operating system. For this reason, if you are using a Windows operating system that was released after Windows XP (e.g., any version of Windows Vista or Windows 7, etc), you may need to use an alternative terminal emulator program in order to establish serial port connections with the SecureSync. Many terminal emulation programs are freely available and downloadable from the web that can be used for this purpose. Once you've obtained a suitable program, the same general instructions listed in this section can be followed.

Establish a new connection using the serial port to which you have connected the SecureSync (typically COM1).

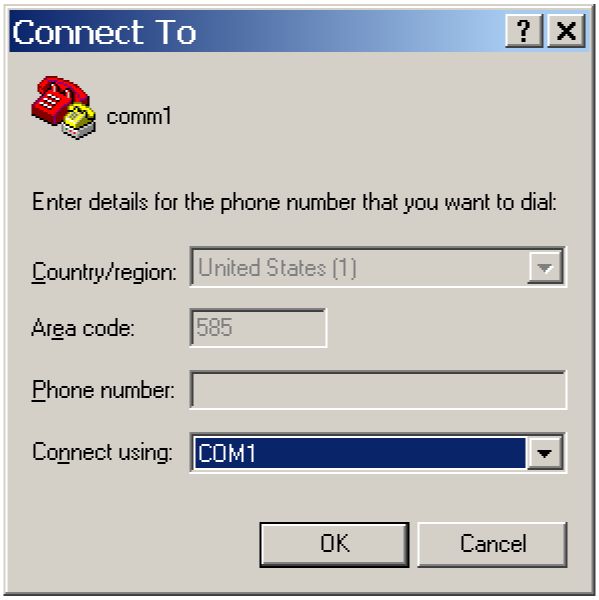


Connection Description

New Connection

Enter a name and choose an icon for the connection:

Figure 10-1: Establishing a New Terminal Connection with HyperTerminal



comm1

Enter details for the phone number that you want to dial:

Country/region: United States (1)

Area code: 585

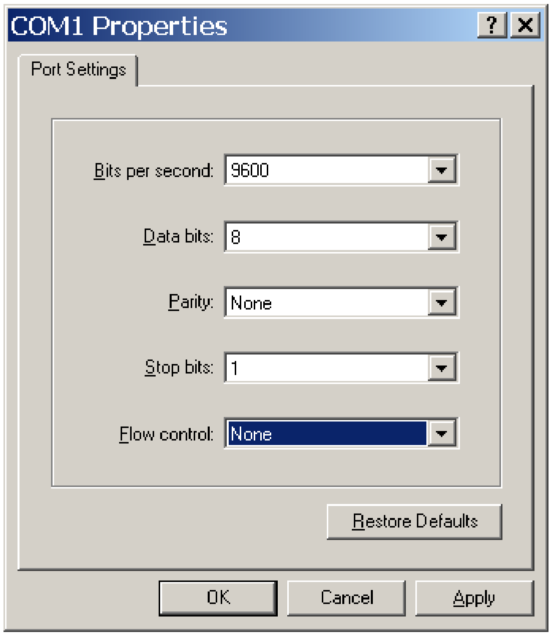
Phone number:

Connect using: COM1

Figure 10-2: Connecting to the Computer's Serial Port

Configure the COM1 properties using the following options (see Figure 10-3). Refer to *Section 11:* "*SecureSync Commands*" for a list of all available serial commands:

Bits per second:	9600
Data bits:	8
Parity:	None
Stop bits:	1
Flow control:	None



Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Figure 10-3: Configuring the Serial Port Connection Properties

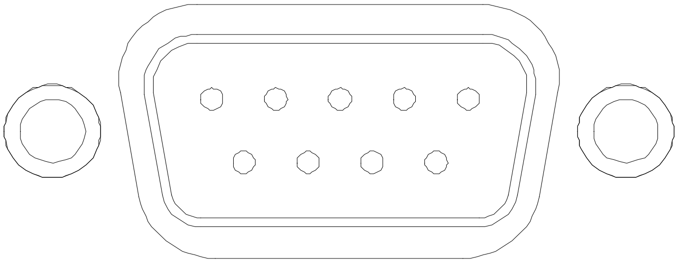


Figure 10-4: Serial Port Pin Configuration

PIN	Signal	Description
2	RXD	Receive Data (RS-232 output data to PC)
3	TXD	Transmit Data (RS-232 input data from PC)
5	GND	Signal Common
6	DSR	Data Set Ready
7	RTS	Request to Send
8	CTS	Clear to Send

Table 10-1: Setup port Cable Pin-Outs

Section 11: SecureSync Commands

The Spectracom SecureSync product features a suite of command line interface (CLI) commands that can be used to set certain options or get status information, via serial cable connections or a remote connection such as **`telnet`** or **`ssh`** (if enabled). This section includes information and details regarding the usage of these commands.

Notes:

1. Typing "**`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).
2. You can scroll up or scroll down through the output by using the Page Up / Page down keys, or the arrow keys.
3. Type "**`q`**" (lower-case) to quit.
4. Pressing the up / down keys scrolls through previously typed commands.
5. Commands need to be typed in all lower-case letters.
6. Where **`eth0`** is the base network port and **`eth1`** (and higher) are used with the optional Gigabit Ethernet module for multiple network interfaces.
7. 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 Section *3.13*: "*User Accounts*" for user account setup information.

`list:` Outputs a list of available serial port commands.

Command	Description
`clean`	Restores SecureSync configuration to factory defaults and reboots.
`cleanhalt`	Restores SecureSync configuration to factory defaults and halts.
`dateget`	Displays current date (i.e., 15 APR 2012).
`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 the IP4 Ethernet port is enabled.
`dhcp4set`	Used to enable or disable the IP4 Ethernet port.
`dns4get`	Displays the configured DNS servers.
`dns4set`	Used to configure the DNS servers.

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.
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 setIPv4 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.
licenses	Displays configured licenses installed (if any).
list	Displays a simple 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 units Serial Number.
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.
ppsctrl	Enable / disable individual 1PPS output signals.
priorset	Sets the priority of an entry in the reference priority table.
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.
renew4	Used with DHCP to keep the assigned IPv4 address.
resetpw	Resets the administrator account (spadmin) password back to the default value “`admin123`”.
routes4	Displays the current IPv4 routing table(s).
rt4add	Adds an IPv4 static route.
rt4del	Deletes an IPv4 static route.
rt4get	Displays the configured IPv4 static routes.
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

stateset	Enable or disable an entry in the reference priority table.
	index = 0..15
	state = 0 (disable), 1 (enable)

status	Displays information about the oscillator disciplining.
syncstate	Display timing system synchronization state.
sysupgrade	Performs system upgrade using the update bundle provided.
testevent	Generates SNMP events in the enterprise MIB.
tfomget	Displays current estimated system time error (TFOM - Time Figure of Merit).
timeget	Displays current system time (time is displayed in the configured timescale – See **`scaleget`** command to retrieve 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 the 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.

11.1 ASCII Data Formats for use with the ASCII RS-485 and RS-232 Input/Output Timecode Option Modules

This section describes each of the Data Format selections available for use with the ASCII Input/Output timecode option modules (these are the ASCII data streams accepted as inputs to the modules and available as outputs from the modules).

Three NMEA (National Marine Electronics Association) Formats and ten different Spectracom Data Formats are available for selection. The three available NMEA Formats are GGA, RMC and ZDA. The available Spectracom Data Formats are Formats 0, 1, 1S, 2, 3, 4, 5, 6, 7, 8 and 9.

11.2 NMEA GGA Message

Format GGA 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**	=	the checksum data, always begins with *

11.3 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**	=	The checksum data, always begins with *

11.4 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

11.5 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

11.6 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 Section *11.7* 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 20, 2001
Time:	12:45:36

11.7 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).

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 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 Section *11.6* 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 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 20, 2001
Time:	12:45:36

11.8 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. Table 6-2: Table of Quality Indicators lists the quality indicators and the corresponding error estimates based upon the GNSS receiver 1 PPS 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 8-11-1: Table of 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: **`?A01 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 2001.
Time: 12:45:36 UTC time, Standard time is in effect.

11.9 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. 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 20010415 124536-0500D #`**

The example data stream provides the following information:

Data Format: 3
Sync Status: Day 271 of year 2001.
Date: April 15, 2001.
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.

11.10 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:

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.

11.11 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: **`? 01 271 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 2001.
Time:	12:45:36 UTC time, Standard time is in effect.

11.12 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:

```
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,0)
XX	=	Time Zone Switch Setting (+/- 00 to 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 the SecureSync is synchronized to UTC source.
*****	=	When the SecureSync time is set manually.
?	=	When the 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.

11.13 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 (space = SYNC, ‘.’ = NOT IN SYNC, ‘*’=NOT IN SYNC, ‘#’ = NOT IN SYNC, “?” = NOT IN SYNC)
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.

11.14 BBC Message Formats

11.14.1 Format BBC-01

This format provides year, month, day, day of week, day of month, hours, minutes, and seconds.

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)

11.14.2 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.

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:

<u>Leap Second Sign:</u>
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)

11.14.3 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 bytes takes 10/300s=33ms, so the **<CR>** byte should be advanced by 33ms 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.

11.14.3.1 '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 the SecureSync is timed so that the stop bit of each **<CR>** ends at the start of the next second.

11.14.3.2 'd' command

The SecureSync transmits the date on request.

Input format: **d<CR>**

Output format: **YYMMDD<CR>**

Number of output characters: 7 (including CR)

11.14.3.3 ‘s’ command

The SecureSync transmits the status information on request.

Input format: **s<CR>**
Output Format: **status**

Number of output characters: 1

Where returned value for **status** are:

G = System Good
D = Failure of SecureSync internal diagnostics
T = SecureSync does not have correct time

11.14.3.4 ‘l’ command

The loopback command will cause the SecureSync to 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)

11.14.3.5 ‘hu’ command

The hang up command will cause the SecureSync to drop the line immediately and terminate the call.

Input format: **hu<CR>**

11.14.3.6 Format BBC-04

The first format is a string of ASCII characters and is sent once per second.

Example message: **T:ho:mi:sc:dw:da:mo:ye:lp<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)

Standard Serial configuration is:

- RS-232 format
- 9600 baud
- 8 data bits
- 1 stop bit
- No parity

11.15 GSSIP Message Format

The ASCII Outputs support 3 ICD-GPS-153C (GPS STANDARD SERIAL INTERFACE PROTOCOL – GSSIP) 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).

The ICD-GPS-153C 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. The 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 the 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. No Position or Velocity information is provided. No SAASM GPS receiver is required because this is emulation and no controlled data is included in the messages. Position and Velocity information is zeroed out.
The ASCII Output supports two configurations for supporting SINCGARS:

Configure Time Transfer as Message Format1 and Current Status as Format2 results in an emulation of the SINCGARS protocol and initialization state machine.

Format1: Time Transfer (5101)
Format2: Current Status (5040)
Format3: Buffer Box (253)

Configure Current Status as Message Format1 and Time Transfer as Format2 results in broadcast 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)

11.16 EndRun Formats

The following formats provide compatibility with EndRun technology.

11.16.1 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	=	Timemode character and is one of:
		G = GPS
		L = Local
		U = UTC
		T = TAI

CR	=	Carriage Return
LF	=	Line Feed

11.16.2 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 (00-59)
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	=	Timemode character and 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

11.17 Event Broadcast Formats

The following formats are used with the Event Broadcast option module card.

11.17.1 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

11.17.2 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

Section 12: License Notices

NTPv4.2.6p5

This file is automatically generated from html/copyright.html

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.

```
***********************************************************************
*                                                                     *
* Copyright (c) University of Delaware 1992-2011                      *
*                                                                     *
* Permission to use, copy, modify, and distribute this software and   *
* its documentation for any purpose with or without fee is hereby     *
* granted, provided that the above copyright notice appears in all    *
* copies and that both the copyright notice and this permission       *
* notice appear in supporting documentation, and that the name        *
* University of Delaware not be used in advertising or publicity      *
* pertaining to distribution of the software without specific,        *
* written prior permission. The University of Delaware makes no       *
* representations about the suitability this software for any         *
* purpose. It is provided "as is" without express or implied          *
* warranty.                                                           *
*                                                                     *
***********************************************************************
```

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

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".

[Tatu continues]
* 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

[The licence continues]

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 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 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.

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 both that copyright notice and this permission notice appear in
supporting documentation, and that the name of CMU and The Regents of
the University of California not be used in advertising or publicity
pertaining to distribution of the software without specific written
permission.
CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL
WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR
THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL,
INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING
FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF
CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN
CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----
Copyright (c) 2001-2003, Networks Associates Technology, 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 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 3: Cambridge Broadband Ltd. copyright notice (BSD) -----
Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
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.
* The name of Cambridge Broadband Ltd. may not be used to endorse or
promote products derived from this software without specific prior
written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``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 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 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

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 interchang

Document Revision History			
Rev	***ECN***	***Description***	***Date***
A	2451	*First-generation manual for the SecureSync product.*	May 2010
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
P	3250	*General updates, enhancements coinciding with latest release: Multi-*	September 2013

		GNSS, Failover option card, Option Licensing, NTP update	

Orolia USA, Inc.
1565 Jefferson Road, Suite 460
Rochester, NY 14623
www.spectracomcorp.com
Phone: US +1.585.321.5800
Fax: US +1.585.321.5219

An Orolia Group Business