ELECTRONICS & DEFENSE

VersaSync

User Manual

Document Part No.: 1228-5000-0050
Revision: 16.1
Date: 20-November-2025

SAFRAN

© 2025 Safran. All rights reserved.

Information furnished by Safran is believed to be accurate and reliable. However, no responsibility is assumed by Safran for its use, nor for any infringements of patents or other rights of third parties that may result from its use. Safran reserves the right to make changes without further notice to any products herein. Safran makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does Safran assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. No license is granted by implication or otherwise under any patent or patent rights of Safran. Trademarks and registered trademarks are the property of their respective owners. Safran products are not intended for any application in which the failure of the Safran product could create a situation where personal injury or death may occur. Should Buyer purchase or use Safran products for any such unintended or unauthorized application, Buyer shall indemnify and hold Safran and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable legal fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Safran was negligent regarding the design or manufacture of the part.

Safran Electronics & Defense

safran-navigation-timing.com

Safran Trusted 4D

• 45 Becker Road, Suite A, West Henrietta, NY 14586 USA
• 3, Avenue du Canada, 91974 Les Ulis, France

The industry-leading Spectracom/Orolia products you depend on are now brought to you by Safran.

Do you have questions or comments regarding this User Manual ?
➔ E-mail: techpubs@nav-timing.safrangroup.com

Blank page.

CONTENTS

CHAPTER 1

Product Description

The Chapter presents an overview of the VersaSync Time and Frequency Synchronization System, its capabilities, main technical features and specifications.

The following topics are included in this Chapter:

1.1 Getting Started

Figure 1-1: VersaSync Rugged GPS Time & Frequency Reference

Welcome to the VersaSync User Manual .

First steps:

- If you are not yet familiar with VersaSync, you may want to start here: "VersaSync Overview" below.
- If you are ready to begin the installation process, see: "Initial Network Setup" on page 34
- If your unit is already up and running, and you would like to change specific settings, see ...
  - ... "Managing Time" on page 171, or
  - ... "System Administration" on page 247.

1.2 VersaSync Overview

VersaSync is a high-performance time & frequency GPS master clock and network time server that delivers accurate, software configurable time and frequency signals under all circumstances, including GNSS-denied environments. Its compact size and high level of ruggedization make VersaSync suitable for mobile applications in harsh environments. VersaSync's small footprint allows for easy integration of the time and frequency functionality into systems architecture.

VersaSync includes all the timing functionality required in modern, network-centric applications:

- NTP/PTP precise time transfer over Ethernet, including security protocols that prevent network vulnerabilities
- Low phase noise 10 MHz frequency distribution
- Configurable pulse signals, including IRIG or HaveQuick timecodes
- Serial link Time Of Day (ToD) messages

GPS-Denied Environments

VersaSync accommodates an OCXO, Rubidium, or CSAC oscillator, allowing the unit to maintain frequency and time accuracy for long periods of GPS/GNSS outage. In addition, it can be re-synchronized by an external reference.

Reliable, Versatile, and Configurable

VersaSync physical inputs and outputs are software configurable and can adapt to various application requirements. I/O pins can be configured as TTL, 10 V pulse, RS232, RS422, and RS485. This allows VersaSync to provide a high number of outputs of the same type, while still fitting into a small form factor. However, if the combination of software configurable outputs is not enough, VersaSync can accommodate an option board (within the same form factor), designed to customer requirements to provide additional outputs of the same type or other type of interface (IRIG AM, etc...).

Due to its high level of ruggedization, VersaSync provides very high intrinsic reliability. Strong status monitoring capability, either locally or remotely, allows quick fault diagnosis. Physical alarm (dry contact) and network alarms (SNMP traps) are raised in real time. An internal, exportable log can be accessed either locally or remotely. In addition to oscillator options (OCXO, Rubidium, or CSAC), VersaSync is available with a C/A L1 GPS receiver or with an L1/L2 SAASM receiver. Pulse outputs are configurable through the web user interface ("Web UI"). An extension slot is available to accommodate additional timing interfaces.

Typical Applications

- **Airborne**: Observation payload (radars, optronics, electronic warfare), flying test bench, flight analysis
- **Ground**: Satcom On the Move (SOTM), anti-IED jamming systems, mobile radios and C3I, robotics
- **Marine**: Sensor support (radars, sonars, optronics, electronic warfare), communication networks, offshore/DSO platforms, buoys

1.3 Status LEDs

VersaSync's front panel status LEDs provide a real-time status overview: Eight (8) LEDs indicate the unit's current operating state:

The LEDs can be disabled, see "Blackout Mode" on page 6.

1.3.1 Blinking Intervals

The status LEDs can communicate five different operating states:

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

1.3.2 LED Lighting Patterns

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

Table 1-1: Common light patterns

Start-up	HEART-B.	OFF	OFF	OFF	OFF	OFF	OFF	OFF
Acquiring fix	ON	FAST	FAST	FAST	FAST	FAST	HEART-B.	FAST

Soft-ware upgrade	FAST	OFF	OFF	FAST	OFF	FAST	HEART-B.	OFF

1.3.3 Legend, individual LEDs

Table 1-2: Legend for Status LEDs

Icon	Light	Meaning
	OFF	No power
	HEARTBEAT	Booting
	ON	Powered
	OFF	No GNSS reception (0 satellites)
	HEARTBEAT	GNSS acquisition in process (≥1 satellite(s), or 1PPS OK, or Time OK
	SLOW	Jamming detected
	FAST	Antenna short circuit
	ON	GNSS is available as reference (1PPS and Time OK)
	OFF	No valid references
	FAST	Using non-primary reference
	ON	Using primary reference
	OFF	Unit is in Holdover (valid)
	ON	System Clock OK (valid)
	FAST	Invalid Time (Holdover period exceeded, or oscillator damaged)
	OFF	No output signal(s) detected/all outputs are disabled
	FAST	Malfunction detected (short circuit, or overload)
	ON	Outputs are enabled
	OFF	No network detected
	FAST	Network malfunction detected (e.g., no auto-negotiation)
	ON	Network OK, configuration OK

Icon	Light	Meaning
	OFF	Unit OK
	FAST	Unit requires attention; check other status LEDs, see Web UI
	HEARTBEAT	See table "LED Lighting Patterns" on page 4
	OFF	Temperature OK
	FAST	High temperature detected

1.3.3.1 LED Patterns during Boot Sequence

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

1.3.4 Blackout Mode

All LEDs can be turned off via the Web UI.

The LED brightness level can be set from 63 (as bright as possible) to 0 (not visable).

To disable all LED activity via the WebUI:

» Navigate to **MANAGEMENT > OTHER: LED Configuration**, and set the Brightness level to "0".

1.4 Interfaces Overview

All of VersaSync's interfaces are integrated into the unit's connectors, which are located on the front panel:

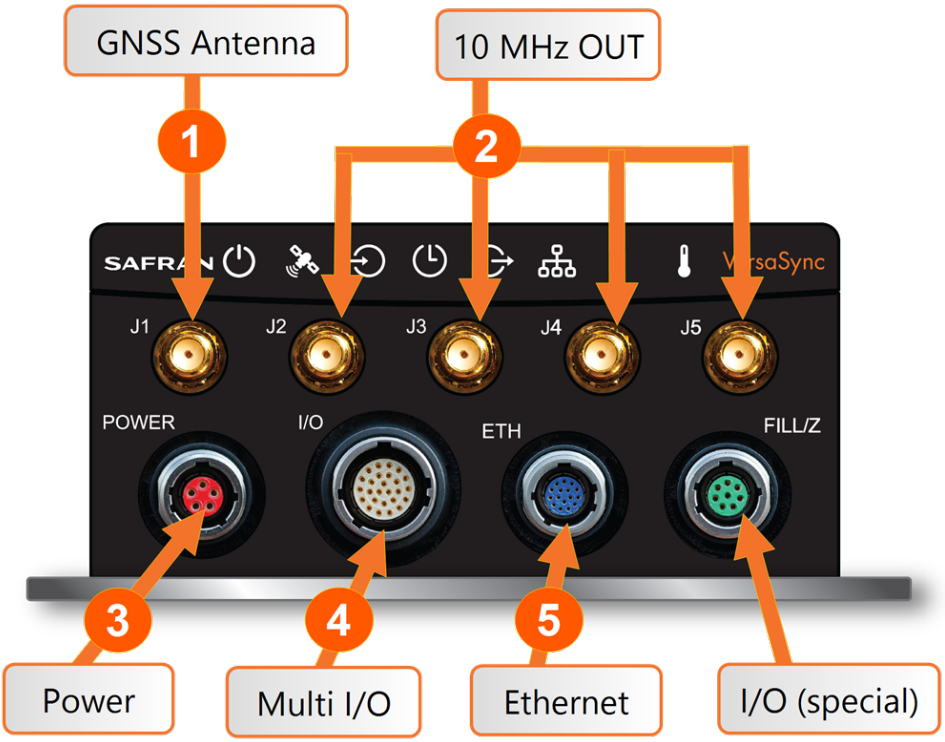


Figure 1-2: VersaSync front panel connectors

Note: VersaSync is highly configurable and the connections can be adjusted many different ways. Your interface configuration may vary based on options you selected during the ordering process.

The following interfaces are provided:

1.4.1 Input Timing Interfaces

Table 1-3: VersaSync inputs (default setup)

INPUT SIGNAL	Total available	DCLS		RS-232	RS-485	ETH	Connector No. (see Fig. above)
		TTL	10V				
1PPS	(1)	1					4
ASCII/HaveQuick/IRIG B	(1)				1		4
ASCII/NMEA	(1)			1			4

INPUT SIGNAL	Total available	DCLS		RS-232	RS-485	ETH	Connector No. (see Fig. above)
		TTL	10V				
GNSS (GPS) antenna connection	(1)	SMA					1
Network Interface (10/100/1000bT): NTP (Stratum 2), PTP	(2)					1	5

All **Multi I/O** interfaces (connector no. 4) are software-configurable, see "Assigning I/O Pins" on page 44.

1.4.2 Output Timing Interfaces

Table 1-4: VersaSync outputs (default setup)

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

All **Multi I/O** interfaces (connector no. 4) are software-configurable, see "Assigning I/O Pins" on page 44.

10 MHz outputs can be disabled. See "The 10 MHz Outputs" on page 70 for more information.

For additional information on configuring pinouts, see "Connectors and their Pinouts" on page 10 and "Configure I/O Settings" on page 51.

1.4.3 Other Interfaces

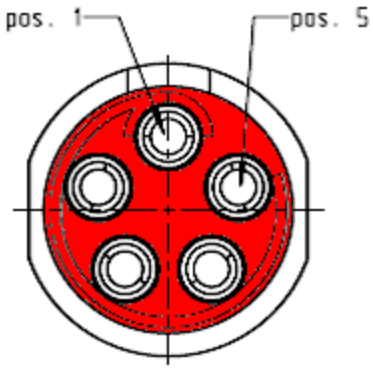
» USB serial equivalent: CLI interface (Connector 4)

Note: The rear panel contains a small breather vent designed to prevent a large pressure differential (1.4psi max) between the interior of the unit and environment. Users are advised to avoid blocking this vent.

1.5 Connectors and their Pinouts

All of VersaSync's connectors are provided at the front panel of the unit, below the Status LEDs. The Advanced Military Connectors are keyed for foolproof connectivity and offer a push-pull locking mechanism. Since the connectors are keyed, you should not need to force connectivity. Inspect all connectors and cables for damage prior to connection.

1.5.1 Power Connector



Note: View in mating direction from front.

Table 1-5: Power connector pinout

Pin	Signal
1	V_{Main} (10 to 32 V)
2	-not used-
3	$V_{Standby}$ (10 to 32 V)
4	GND (to Standby)
5	GND (to Main)

This product is designed to handle a **maximum voltage of up to 32 V_{DC}**. Power supplies with higher voltage or transient/ cranking power will require a power conditioner or surge blocker.

Caution: Reversed polarity can blow an internal fuse that protects the product from damage. Use care when building power cables.

Test any new cables to safely power the unit before connecting your VersaSync to any other inputs or outputs (such as a GNSS antenna), and before grounding your unit to a vehicle.

1.5.2 Input/Output Connector

VersaSync has a 26-pin input/output connector that offers 8 software-configurable CHANNELS, plus one fixed DCLS channel, and a USB interface. To learn more about types of interfaces and signals, and how to configure them, see "Assigning I/O Pins" on page 44.

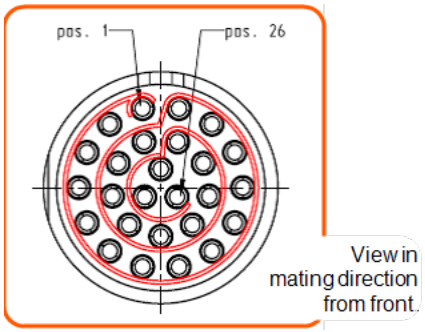
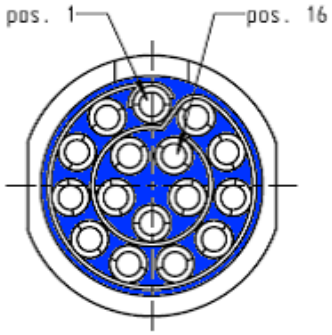


Table 1-6: Default I/O connector pinout

Pin	Channel	Signal	Pin	Channel	Signal
1	0	1PPS output (5V)	15	7	Have Quick output (RS-485 signal +)
2		GND	16		GND
3	1	Have Quick input (RS-485 signal +)	17	8	Have Quick output (RS-485 signal –)
4		GND	18		GND

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

1.5.3 Ethernet Connector



Note: View in mating direction from front.

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

Table 1-7: Ethernet connector pinout

Pin	Signal	Pin	Signal
1	Ethernet_1 A+	9	Ethernet_2 A+

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

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

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

1.5.4 Optional I/O Connector

The Optional I/O connector ("SAASM" or "FILL/Z") is used in conjunction with the Option Board that is available for VersaSync. If the unit is not equipped with an Option Board, this connector is not used.

1.5.5 Coaxial Connectors

VersaSync offers five (5) coaxial connectors. Standard configuration includes the **GNSS antenna** input connector and (4) **10 MHz sinewave** outputs. (Certain models may have variation on this setup. Refer to your purchase order for information on your VersaSync model.)

The coaxial connectors (aside from the GNSS connection) produce a 10MHz output that can be simultaneously disabled through the Web UI.

All coaxial connectors are **standard SMA connectors** (recommended torque value: 8-10 in-lbs).

Mating Connector Plugs

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

Table 1-8: Connector Part Numbers

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

1.5.5.1 ODU® ordering contact information (USA):

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

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

ETHERNET connector wiring:

- 1 through 8: A Ethernet Connect, 4 pairs, 1000bT (in the software, eth0)
- 9 through 16: B Ethernet Connect, 4 pairs, 1000bT (in the software, eth1)

POWER connector pinout

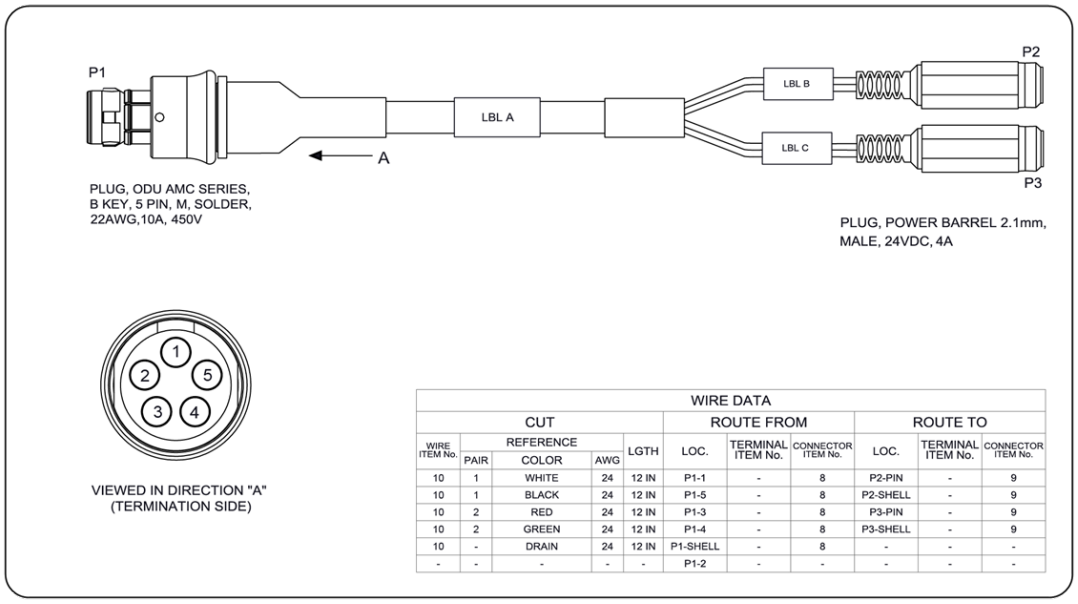
- 1: V_{Main}, 10 to 32 V_{DC}
- 2: -not used-
- 3: $V_{Standby}$, 10 to 32 V_{DC} (Standby Power)

- 4: Ground return, standby power
- 5: Ground return, main power

1.6 Included Cables

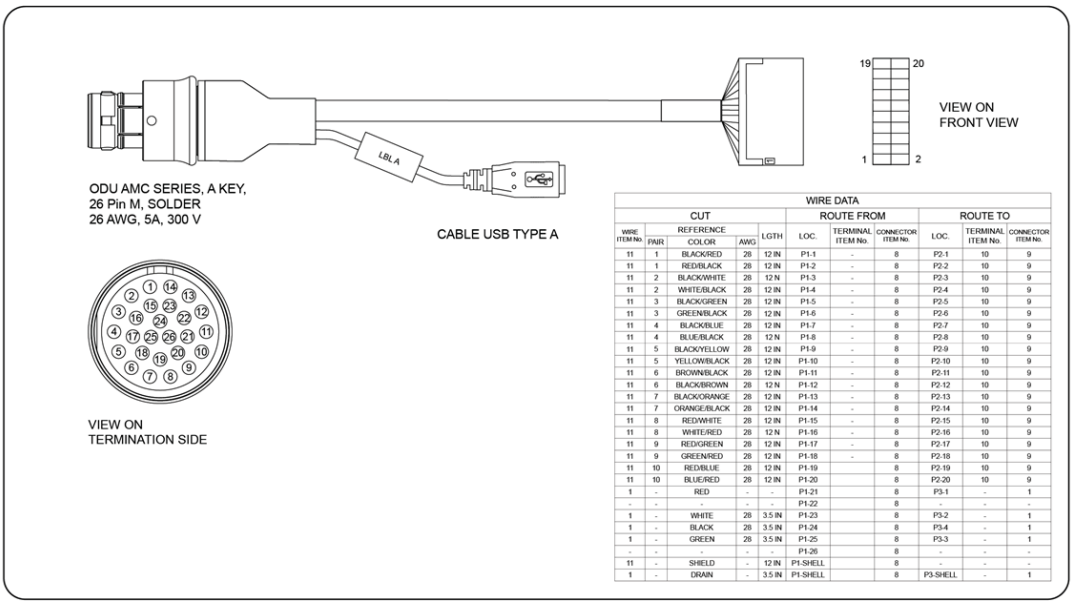
The VersaSync Evaluation Kit contains the following cables (antenna cable not shown):

Power Cable



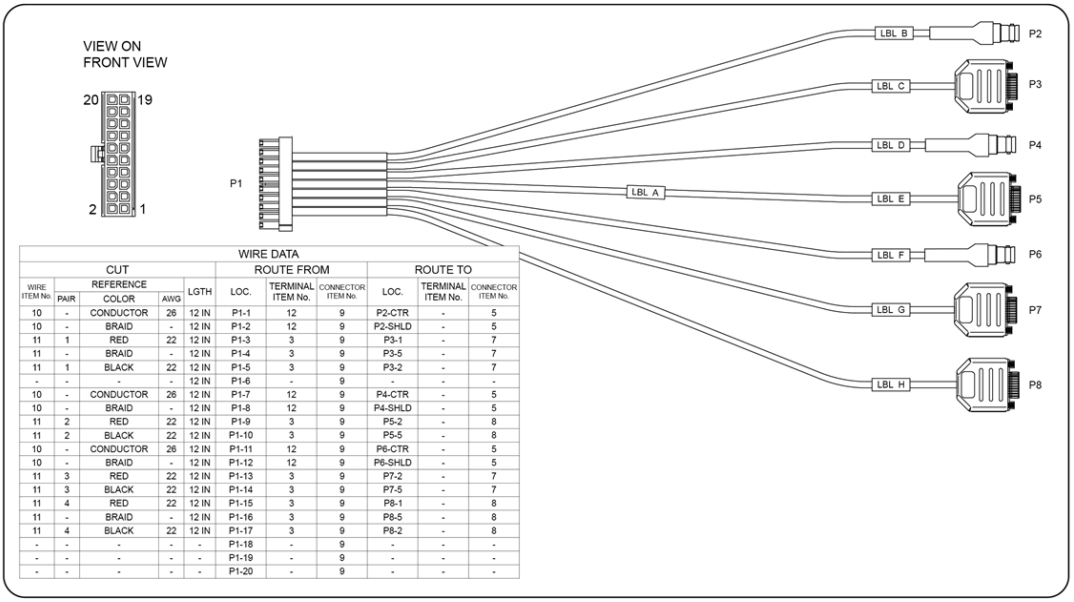
WIRE DATA										
CUT					ROUTE FROM			ROUTE TO		
WIRE ITEM No.	REFERENCE			LGTH	LOC.	TERMINAL ITEM No.	CONNECTOR ITEM No.	LOC.	TERMINAL ITEM No.	CONNECTOR ITEM No.
	PAIR	COLOR	AWG							
10	1	WHITE	24	12 IN	P1-1	-	8	P2-PIN	-	9
10	1	BLACK	24	12 IN	P1-5	-	8	P2-SHELL	-	9
10	2	RED	24	12 IN	P1-3	-	8	P3-PIN	-	9
10	2	GREEN	24	12 IN	P1-4	-	8	P3-SHELL	-	9
10	-	DRAIN	24	12 IN	P1-SHELL	-	8	-	-	-
-	-	-	-	-	P1-2	-	-	-	-	-

I/O Cable



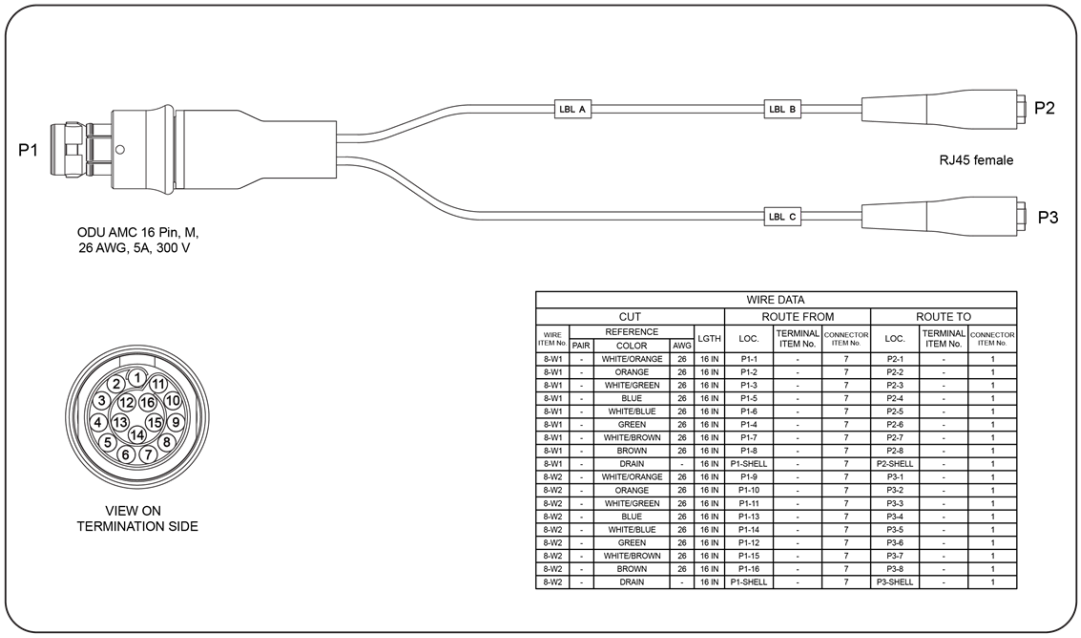
WIRE DATA											
CUT					ROUTE FROM			ROUTE TO			
WIRE ITEM No.	REFERENCE PAIR	REFERENCE COLOR	AWG	LGTH	LOC.	TERMINAL ITEM No.	CONNECTOR ITEM No.	LOC.	TERMINAL ITEM No.	CONNECTOR ITEM No.
11	1	BLACK/RED	28	12 IN	P1-1	-	8	P2-1	10	9
11	1	RED/BLACK	28	12 IN	P1-2	-	8	P2-2	10	9
11	2	BLACK/WHITE	28	12 N	P1-3	-	8	P2-3	10	9
11	2	WHITE/BLACK	28	12 IN	P1-4	-	8	P2-4	10	9
11	3	BLACK/GREEN	28	12 IN	P1-5	-	8	P2-5	10	9
11	3	GREEN/BLACK	28	12 IN	P1-6	-	8	P2-6	10	9
11	4	BLACK/BLUE	28	12 IN	P1-7	-	8	P2-7	10	9
11	4	BLUE/BLACK	28	12 N	P1-8	-	8	P2-8	10	9
11	5	BLACK/YELLOW	28	12 IN	P1-9	-	8	P2-9	10	9
11	5	YELLOW/BLACK	28	12 IN	P1-10	-	8	P2-10	10	9
11	6	BROWN/BLACK	28	12 IN	P1-11	-	8	P2-11	10	9
11	6	BLACK/BROWN	28	12 N	P1-12	-	8	P2-12	10	9
11	7	BLACK/ORANGE	28	12 IN	P1-13	-	8	P2-13	10	9
11	7	ORANGE/BLACK	28	12 IN	P1-14	-	8	P2-14	10	9
11	8	RED/WHITE	28	12 IN	P1-15	-	8	P2-15	10	9
11	8	WHITE/RED	28	12 N	P1-16	-	8	P2-16	10	9
11	9	RED/GREEN	28	12 IN	P1-17	-	8	P2-17	10	9
11	9	GREEN/RED	28	12 IN	P1-18	-	8	P2-18	10	9
11	10	RED/BLUE	28	12 IN	P1-19		8	P2-19	10	9
11	10	BLUE/RED	28	12 IN	P1-20		8	P2-20	10	9
1	-	RED	-	-	P1-21		8	P3-1	-	1
-	-	-	-	-	P1-22		8	-	-	-
1	-	WHITE	28	3.5 IN	P1-23		8	P3-2	-	1
1	-	BLACK	28	3.5 IN	P1-24		8	P3-4	-	1
1	-	GREEN	28	3.5 IN	P1-25		8	P3-3	-	1
-	-	-	-	-	P1-26		8	-	-	-
11	-	SHIELD	-	12 IN	P1-SHELL		8	-	-	-
1	-	DRAIN	-	3.5 IN	P1-SHELL		8	P3-SHELL	-	1

I/O Breakout Cable



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

Ethernet Data Cable



WIRE DATA

CUT					ROUTE FROM			ROUTE TO		
WIRE ITEM No.	REFERENCE PAIR	REFERENCE COLOR	AWG	LGTH	LOC.	TERMINAL ITEM No.	CONNECTOR ITEM No.	LOC.	TERMINAL ITEM No.	CONNECTOR ITEM No.
8-W1	-	WHITE/ORANGE	26	16 IN	P1-1	-	7	P2-1	-	1
8-W1	-	ORANGE	26	16 IN	P1-2	-	7	P2-2	-	1
8-W1	-	WHITE/GREEN	26	16 IN	P1-3	-	7	P2-3	-	1
8-W1	-	BLUE	26	16 IN	P1-5	-	7	P2-4	-	1
8-W1	-	WHITE/BLUE	26	16 IN	P1-6	-	7	P2-5	-	1
8-W1	-	GREEN	26	16 IN	P1-4	-	7	P2-6	-	1
8-W1	-	WHITE/BROWN	26	16 IN	P1-7	-	7	P2-7	-	1
8-W1	-	BROWN	26	16 IN	P1-8	-	7	P2-8	-	1
8-W1	-	DRAIN	-	16 IN	P1-SHELL	-	7	P2-SHELL	-	1
8-W2	-	WHITE/ORANGE	26	16 IN	P1-9	-	7	P3-1	-	1
8-W2	-	ORANGE	26	16 IN	P1-10	-	7	P3-2	-	1
8-W2	-	WHITE/GREEN	26	16 IN	P1-11	-	7	P3-3	-	1
8-W2	-	BLUE	26	16 IN	P1-13	-	7	P3-4	-	1
8-W2	-	WHITE/BLUE	26	16 IN	P1-14	-	7	P3-5	-	1
8-W2	-	GREEN	26	16 IN	P1-12	-	7	P3-6	-	1
8-W2	-	WHITE/BROWN	26	16 IN	P1-15	-	7	P3-7	-	1
8-W2	-	BROWN	26	16 IN	P1-16	-	7	P3-8	-	1
8-W2	-	DRAIN	-	16 IN	P1-SHELL	-	7	P3-SHELL	-	1

1.7 VersaSync Specifications

The specifications listed below apply to the current base model, during “normal” operation, with VersaSync synchronized to valid Time and 1PPS input references.

1.7.1 Supply Power

Operating Power and Standby Power: 10 to 32 V_{DC}

Power draw:

- **Operating**: 10 W typical
- **Standby**: 1.5 W

This product is not intended to operate above 32V_{DC}; power sources with transient voltage spikes and surges above 32V require an external power conditioner/power filter to ensure safe operation.

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

1.7.2 GNSS Receiver

VersaSync has an integrated state-of-the-art GNSS receiver, suitable for concurrent dual-constellation reception.

Compatible signals:

- GPS L1 C/A (center frequency 1575.42 MHz)
- GLONASS L1 0F (center frequency 1602.0 MHz)
- Galileo E1 B/C (center frequency 1575.42 MHz)
- QZSS L1-SAIF (center frequency 1575.42 MHz)
- BeiDou B1 (center frequency 1561.098 MHz)

Satellites tracked: Up to 72 simultaneously

Update rate: up to 2Hz (concurrent)

Acquisition time: Typically < 27 seconds from cold start

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

Antenna connector: SMA

1.7.3 Output References

1.7.3.1 10 MHz Output

- **Signal**: 10 MHz sine wave
- **Signal Level**: +10 dBm ±2dB into 50 Ω
- **Harmonics**: -40 dBc minimum
- **Spurious**: -60 dBc minimum OCXO
- **Connector**: SMA female
- **Signature Control**: This configurable feature removes the output signal whenever a major alarm condition or loss of time synchronization condition is present. The output will be restored once the fault condition is corrected.

Table 1-9: 10 MHz output — oscillator types and accuracies

Oscillator Type	Relative Frequency Variation with Aging:		
	24 hours	One month	One year
OCXO	$1x10^{-10}$	$3x10^{-9}$	$3x10^{-8}$
mRO-50	-	$1x10^{-10}$	$1x10^{-9}$

Table 1-10: 10 MHz output — oscillator stability

Oscillator Type	Short-Term Stability (Allan Deviation)			Relative Frequency Variation with Temperature
	1 sec.	10 sec.	100 sec.	
OCXO	$1x10^{-10}$	$3x10^{-11}$	$3x10^{-11}$	$\pm1x10^{-9}$ (-40°C to +71°C)
mRO-50	1×10^{-10}	3×10^{-11}	1×10^{-11}	$\pm1x10^{-9}$ (-10°C to 65°C)

Table 1-11: 10 MHz output — oscillator phase noise (dBc/Hz)

Oscillator Type	@ 10 Hz	@ 100 Hz	@ 1KHz	@ 100 KHz
OCXO	-115 dBc/Hz	-133 dBc/Hz	-147 dBc/Hz	-155 dBc/Hz
mRO-50	-90 dBc/Hz	-110 dBc/Hz	-135 dBc/Hz	-140 dBc/Hz

For more information, see "Configuring the Oscillator" on page 239.

1.7.3.2 1PPS Output

Signal: One pulse-per-second square wave

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

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

Pulse width range: 20 ns to 900 ms

Rise time: <10 ns

Accuracy: Positive edge within ±15 ns of UTC when locked to a valid 1PPS GNSS input reference

Signature Control: This configurable feature removes the output signal whenever a major alarm condition or loss of time synchronization condition is present. The output will be restored once the fault condition is corrected.

Table 1-12: 1PPS output accuracies

Oscillator Type	1PPS Accuracy to UTC (1 sigma, locked to GPS)	Holdover (constant temp. following 48 hours dis-ciplining)		
		After 4 hours	After 24 hours	After 7 days
OCXO	±15 ns	1.5 µs	10 µs	0.4 ms
mRO-50	±15 ns	0.2 µs	1.5 µs	20 µs

1.7.4 Mechanical & Environmental Specifications

1.7.4.1 Physical Specifications

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

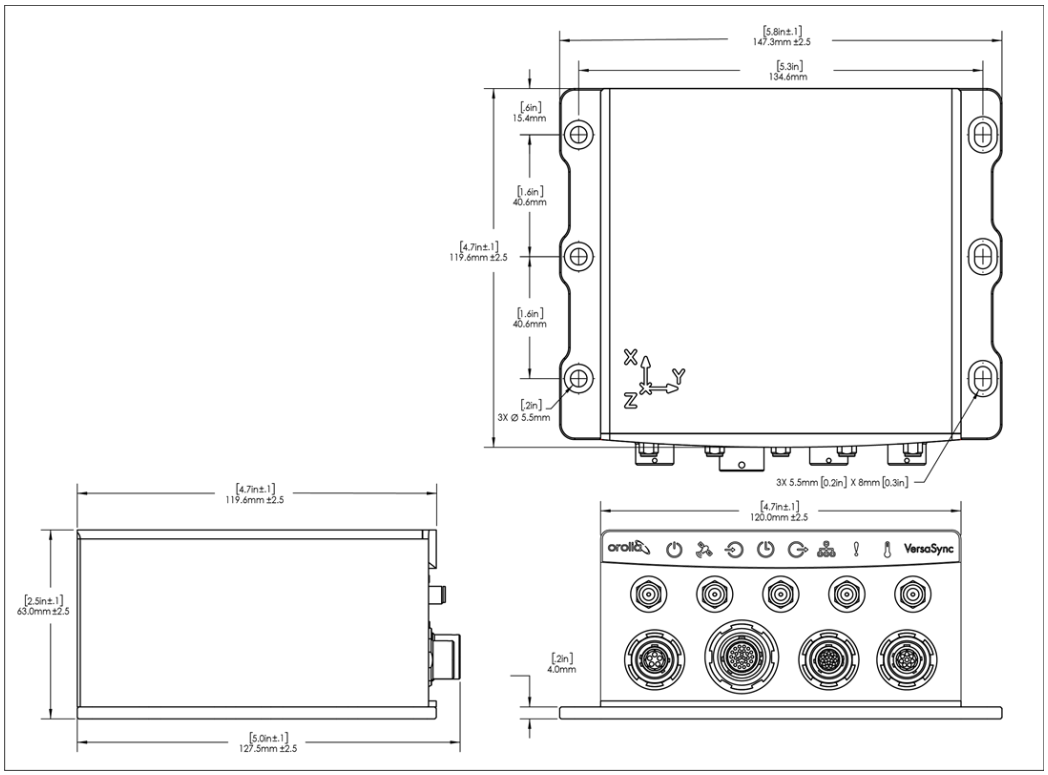


Figure 1-3: Mechanical dimensions

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

1.7.4.2 Environmental Requirements

- **Temperature, in operation**: -40°C to +71°C
- **Temperature, in storage**: -45°C to +85°C
- **Humidity**: 95% RH, non condensing at 40°C
- **Altitude**: up to 45,000 ft
- **Protection**: IP 65

- **Vibration**:
  - 7.7 g rms, 20 to 1000 Hz (in accordance with MIL-STD-810G Method 514.6E-1 and 514.6E-2 category 24 – minimum integrity tests)
- **Shock**: 20 g, 11 ms (pulse sawtooth) in accordance with MIL-STD 810G, Method 516.7 Procedure 1

1.8 Regulatory Compliance

This product has been tested and found to be in compliance with the following regulatory publications:

MIL compliance

- Tested in accordance with MIL-STD-810G:
  - MIL-STD 810G, 506.6
  - MIL-STD 810G, 509.6
  - MIL-STD 810G, 516.7
  - MIL-STD 810G, 514.7
- MIL-461F Testing (EMI/EMC):
  - MIL-STD-461F CE102 Conducted Emissions, Power Leads
    - Note: Frequency Range: 10 kHz to 10 MHz; Test Limits: Figure CE102-1
  - MIL-STD-461F CS101 Conducted Susceptibility, Power Leads
    - Note: Frequency: 30 Hz to 150 kHz; Test Levels: Figure CS101-1 (Curve #2)
  - MIL-STD-461F RE102 Radiated Emissions, Electric Field
    - Note: Frequency Range: 10 kHz to 18 GHz; Test Limits: Figure RE102-3
  - MIL-STD-461F CS114 Conducted Susceptibility, Bulk Cable Injection
    - Note: Frequency Range: 10 kHz to 200 MHz

FCC compliance

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

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

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

Other compliance

- EN 60068-2-6
- RoHS, WEEE compliant.

1.9 The VersaSync Web UI

VersaSync has an integrated web user interface (referred to as "Web UI" throughout this documentation) that can be accessed from a network-connected computer, using a standard web browser. The Web UI is the most complete way to configure and monitor the unit.

Note: If you prefer, an integrated Command-Line Interpreter interface (CLI) allows the use of a subset of commands. See "Command-Line Interface" on page 334.

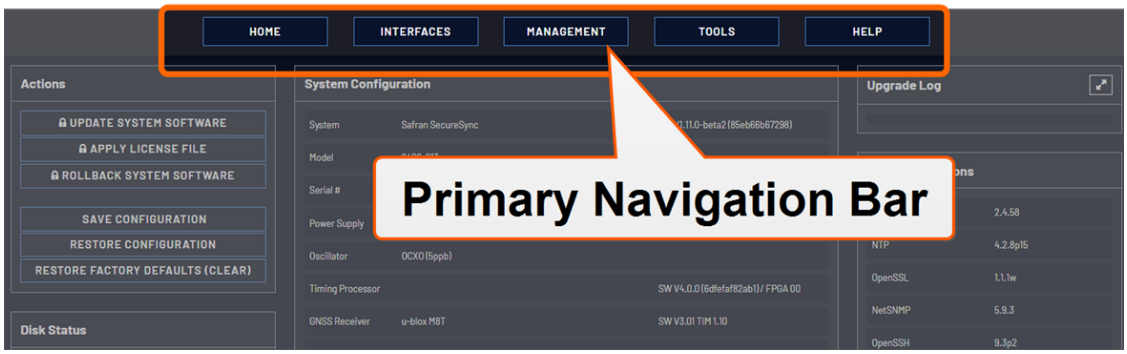
1.9.1 The Web UI HOME Screen

Note: Screens displayed in this manual are for illustrative purposes. Actual screens may vary depending upon the configuration of your product.

The **HOME** screen of the VersaSync web user interface ("Web UI") provides comprehensive status information at a glance, including:

- vital **system** information
- current status of the **references**
- key **performance**/accuracy data
- major **log events**.

The **HOME** screen can be accessed from anywhere in the Web UI, using the HOME button in the **Primary Navigation Bar**:



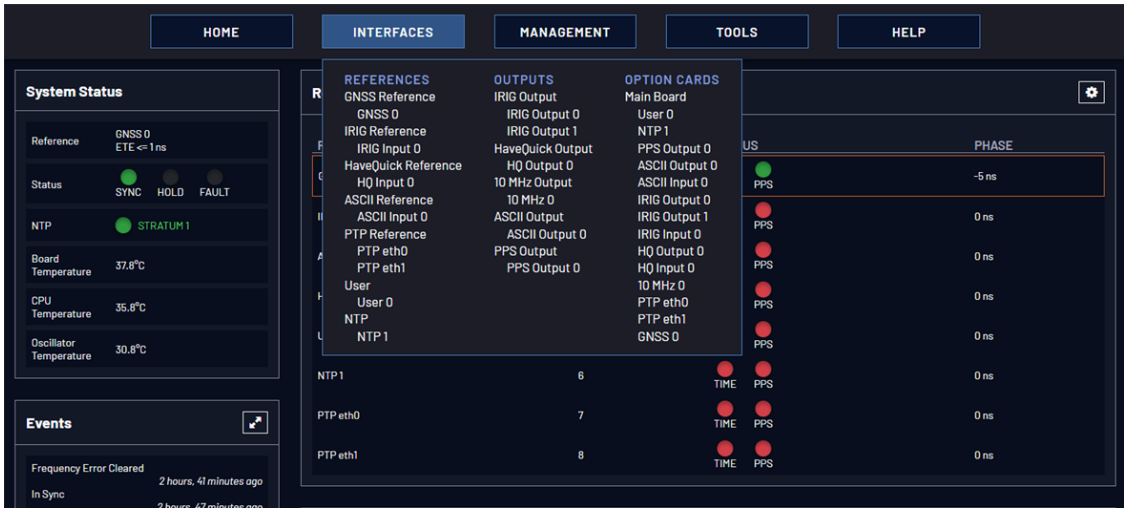
The **Primary Navigation Bar** provides access to all menus:

- **HOME**: Return to the HOME screen (see above)
- **INTERFACES**: Access the configuration pages for ...
  - ... references (e.g., GNSS, NTP)
  - ... outputs (e.g. 10 MHz, PPS, NTP) and
  - ... installed input/output option cards.
- **MANAGEMENT**: Access the NETWORK setup screens, and OTHER setup screens e.g., to configure Reference Priorities, System Time, and the Oscillator.
- **TOOLS**: Opens a drop-down menu for access to the system maintenance screens and system logs.
- **HELP**: Provides Safran Service Contact Information and high-level system configurations you may be required to furnish when contacting Safran Service.

1.9.2 The INTERFACES Menu

The **INTERFACES** menu on the Main screen provides access to VersaSync's:

- External REFERENCES e.g., the GNSS reference input
- Detected OUTPUTS, such as 10 MHz and 1PPS
- Installed OPTIONS.



Clicking on any of the line items will open a status screen, providing real-time information on the selected interface e.g., availability, performance data and events history.

To configure settings for the selected interface, click the GEAR icons or buttons provided on most of the status screens. Icons like the INFO symbol provide access to more detailed status information and history data.

The headings of each of the INTERFACES drop-down menus (white on orange) open overview status screens for the respective menu items.

1.9.3 The Configuration MANAGEMENT Menu

The **MANAGEMENT** menu on the Web UI's Main screen provides access to VersaSync's configuration screens and settings.

On the left side, under **NETWORK**, the following standard setup screens can be found:

- **Pin** Layout
- **Network** Setup
- **SSH** Setup
- **SNMP** Setup
- **NTP** Setup
- **PTP** Setup
- **GPSD** Setup

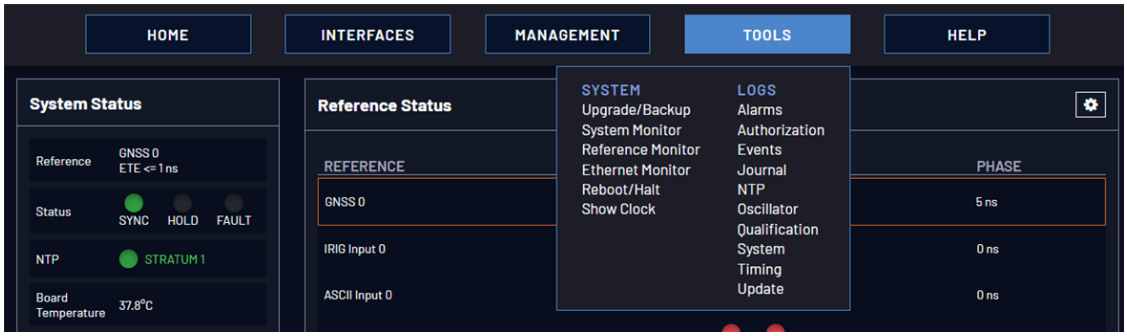
Under **OTHER**, you can access non-network related screens:

- **Authentication**: Manage user accounts, Security Policy, LDAP Setup, RADIUS setup, Login Preference and Remote Servers. Change My Password is also available.
- **Reference Priority**: Define the order of priority for timing inputs.
- **Notifications**: Configure the notifications triggered by VersaSync's events. A notification can be a combination of a mask alarm and/or SNMP Trap and/or email.
- **Time Management**: Manage the Local Clock, UTC Offset, DST Definition and Leap Second information.
- **System Time Message**: Configure a regularly delivered message of the system time.
- **Log Configuration**: Manage the system logs.
- **Disciplining**: Manage oscillator disciplining.
- **LED Configuration**: Change the LED brightness.
- **Change My Password**: Configure the admin password.

1.9.4 The TOOLS Menu

The **TOOLS** menu on the Web UI's Main screen provides access to:

- The System Upgrade screen
- System and network monitoring screens
- Miscellaneous system administration screens
- Log screens



CHAPTER 2

SETUP

The following topics are included in this Chapter:

2.1 SAFETY

Table 2-1: Safety symbols used on this product or in this document

Symbol	Signal word	Definition
	DANGER!	Potentially dangerous situation which may lead to personal injury or death! Follow the instructions closely.
	CAUTION!	Potential equipment damage or destruction! Follow the instructions closely.
	NOTE	Tips and other useful or important information.
	ESD	Risk of Electrostatic Discharge! Avoid potential equipment damage by following ESD Best Practices.
	CHASSIS GROUND	This symbol is used for identifying the functional ground of an I/O signal. It is always connected to the instrument chassis.
	Analog Ground	Shows where the protective ground terminal is connected inside the instrument. Never remove or loosen this screw!
	Recycle	Recycle the mentioned components at their end of life. Follow local laws.

2.1.1 SAFETY: Before You Begin Installation

This product may constitute a risk to the operator or installation/maintenance personnel, if used under conditions that must be deemed unsafe, or for purposes other than the product's designated use, which is described in the introductory technical chapters of this guide.

DANGER! If the equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

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

DANGER! — INSTALLATION OF EQUIPMENT:

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

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

DANGER! — DO NOT OPEN EQUIPMENT, UNLESS AUTHORIZED:

The interior of this equipment does not have any user serviceable parts. Contact Orolia Technical Support if this equipment needs to be serviced. Do not open the equipment. Follow Orolia Safety Instructions, and observe all local electrical regulatory requirements.

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

2.1.2 SAFETY: User Responsibilities

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

2.1.3 SAFETY: Other Tips

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

2.2 Installation Overview

The steps that need to be performed prior to putting VersaSync into service include:

- Installation: Hardware setup, mechanical installation, physical connections.
- Setup: Establish basic access to the unit, so as to allow the use of the web user interface ("Web UI").
- Configuration: Access the Web UI, configure the network, input and output references, protocols (e.g., NTP), other settings.

Not all of the setup steps described in this manual may apply to you. Your unit installation relative to other connected devices, the cable selection and manufacturing, your chosen power source, your project-specific infrastructure, and your planned access to your unit (either WebUI or CLI), could all affect your setup needs.

2.2.1 Hardware Connections

During the procedure described below, you will connect the **Power** cable, the **Multi I/O** cable, and the **Ethernet** cable.

The step-by-step instructions below outline the VersaSync installation and configuration process:

1. **Install VersaSync** in the designated vehicle:
   - The mounting plate should be in direct contact with the unit base plate, so as to conduct heat.
   - For more detail on mounting your unit, see "Mounting" on page 32.

2. **Connect the power supply**. The unit will power up, and the ON/OFF status LED will pulsate.

Requirement	Action	Evaluation kit cable
Power up	Connect 12 V_{DC} to the power connector.	Attach a cable and apply 12 V_{DC} to the plug labeled "Main" (CA08R-CRPB-0002)

> **Caution:** If your unit does not power up, and this is your first installation using your cables, check the polarity of the wires and confirm that the unit will power up normally before proceeding with these steps or making any other connections.

3. **Install the GNSS antenna**(s). Follow your antenna manufacturer's instructions. :

   For additional information on GNSS antenna installation considerations, including cabling, an Orolia tech note is available here.

4. **Wire the antenna cables and interface cables**. Most customers will require the Multi I/O and Ethernet cables for these connections, as well as a PC..

Requirement	Action	Evaluation kit cable
USB connection	Connect USB to the Multi I/O connector.	Connect the USB connector to a PC with a terminal emulator program (CA08R-CRUB-0002)
Network connection	Connect at least one of the two Ethernet connectors to a network.	Connect the RJ45 jack labeled ETH0 or ETH1 to a network hub/switch or directly to a PC (CA08R-CRET-0002)

   - USB: Connect the **Multi I/O** connector to the VersaSync unit. If you are using the Evaluation Kit, connect the Multi I/O USB output to a PC. Install a **terminal emulator** program on the PC (e.g., TeraTerm® or PuTTY®).
   - Ethernet: Connect the **Ethernet** cable to one of the ETH ports of the unit. If you are using the Evaluation Kit, connect at least one of the two I/O cable Ethernet ports (ETH0 or ETH1) to a network switch/hub, or to the PC mentioned above (using a standard Ethernet patch cable, or a crossover cable).

   For pinout tables, see "Connectors and their Pinouts" on page 10 and "Configuring Inputs/Outputs" on page 43.

5. **Establish a network connection** so as to allow access to the web user interface ("Web UI"). See "Initial Network Setup" on page 34 for information on the USB driver installation and network address configuration.

   Note: You can also use Zeroconf to access the Web UI (see "Zero Configuration Setup" on page 39).

6. Using the Web UI, **configure** the following:
   - Software-configurable I/O pins, see "Assigning I/O Pins" on page 44.
   - Other VersaSync INTERFACES settings and MANAGEMENT settings e.g., network settings, reference priorities (see "Configuring Network Settings" on page 72).

2.2.2 Mounting

2.2.2.1 Selecting a Mounting Location

The unit is to be mounted on a plate, using six (6) through holes. The mounting location must offer sufficient space to accommodate the unit and the cable connectors, and it must be within cable reach to other connected devices, such as the GNSS antenna. The unit can be mounted horizontally, or at any angle. The chosen environment must not fall below IP 65 ingress protection standards.

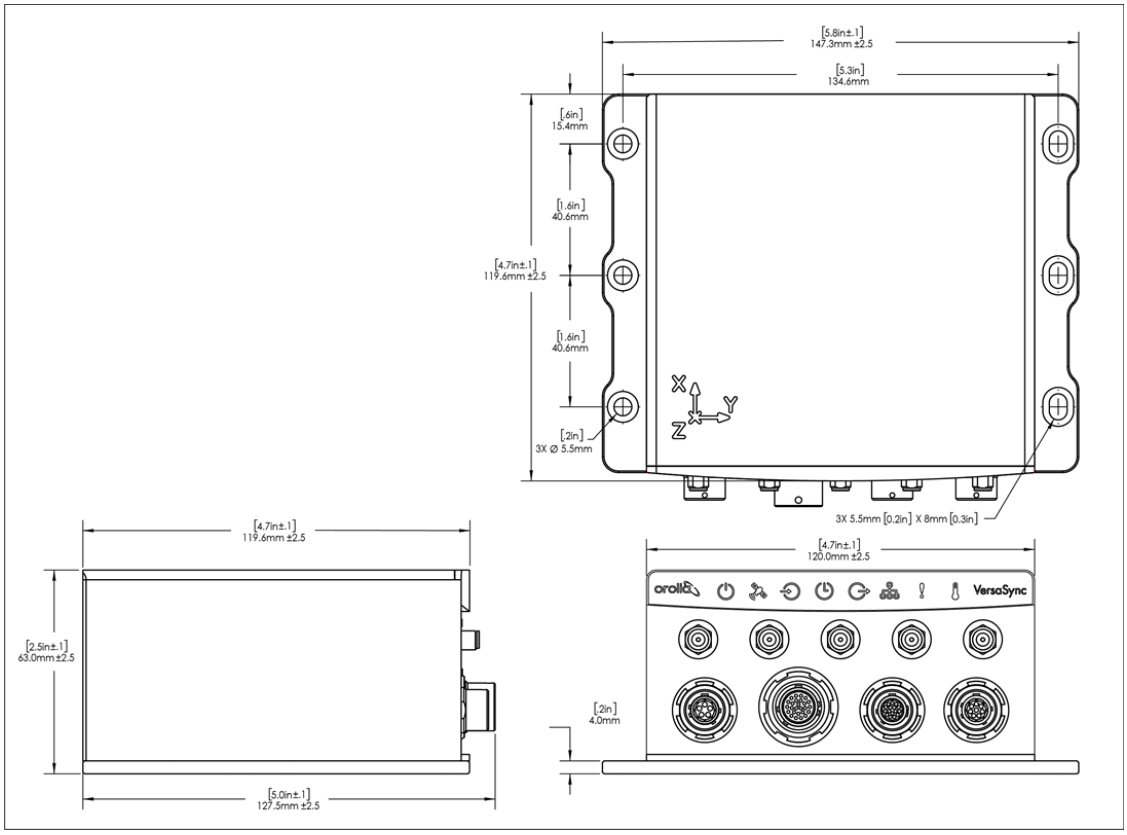


Figure 2-1: Mechanical dimensions

2.2.2.2 Heat Dissipation

The aluminum base plate of the unit acts as a heat drain, conducting heat away from VersaSync's interior components. When considering a mounting location, it is crucial that:

- the operating temperature of the mounting surface does not exceed 71°C/149°F.
- the mounting surface is even and heat conductive. Do not use any insulator material e.g., rubber gaskets or similar.
- the ambient air temperature meets is within the specified range, i.e. -40°C to +71°C.

2.2.2.3 Fasteners

Orolia recommends to observe the VITA 75 standard regarding mounting the unit, and fastener selection.

2.2.2.4 Grounding

The VersaSync's DC power is not isolated from the chassis; during operation, the negative DC of the power source becomes the ground of the VersaSync and its chassis. Typical AC "earth ground" measures are unnecessary because of this design.

Should you opt to ground your VersaSync directly to your vehicle, connect the DC negative terminals of the power connector to the chassis of the unit and to the vehicle metallic structure. Doing so will send the negative DC directly to the vehicle, rather than the power supply. Use a grounding strap if the baseplate can't make metal-to-metal contact with the mounting surface.

2.3 Initial Network Setup

After making the hardware connections outlined in the Installation Overview list, the following information will help you to establish a network connection. Your connection instructions will vary depending on your chosen physical connections.

- If your unit is connected to your network, you can quickly find and communicate with your VersaSync **web user interface** ("Web UI", used to configure and monitor the unit)
  - via the default IP address, and a PC configured with the same subnet mask (255.255.255.0)
  - using a DHCP-assigned address and a PC also connected to your network. For more information, see "Zero Configuration Setup" on page 39.
- If your unit is connected directly to a PC via the USB connection or an Ethernet port: VersaSync has a **Command Line Interpreter** ("CLI"). **You will need a terminal emulator program** installed on the PC that will be used to configure VersaSync in order to communicate. Follow the instructions below, or see "Setting up a Terminal Emulator" on page 334 for more detailed instructions and a list of CLI commands. Using the serial CLI connection, you can set up access to the **Web UI** by setting or identifying an IP address on your network. (See "Assigning a Static IP Address" on page 41).

Default settings:

VersaSync network settings default to static IP addresses. The Ethenet ports come preconfigured with IP addresses as follows:

Eth0 - 192.168.1.1

Eth1 - 192.168.1.2

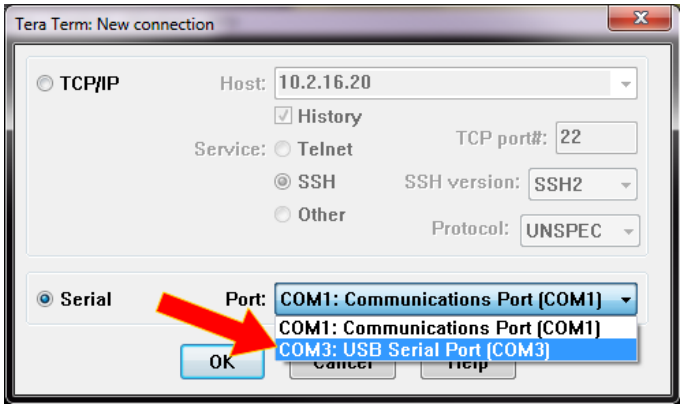
Default subnet mask: 255.255.255.0

2.3.1 USB Driver

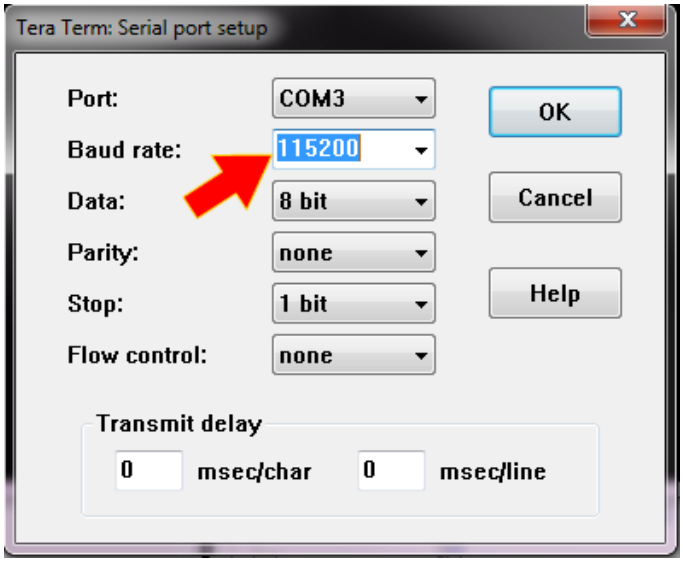
» If you are using a USB connection through the multi I/O connector, driver installation may be necssary. On the PC connected to the unit, new hardware (the USB interface) will be detected. The correct driver should be installed automatically. If not, download the driver from www.ftdichip.com/Drivers/VCP.htm, and install it manually via the instructions for your operating system.

2.3.2 Network Connection

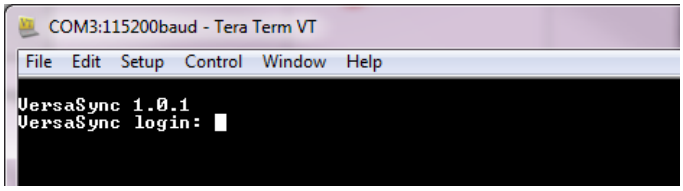
a. Start the terminal emulator program on the PC. Select the COM port that is assigned to the USB interface:



Access the CLI via ssh or telnet: The required port configuration is 115200 8N1:



Press the **Return** key, and enter the login credentials:



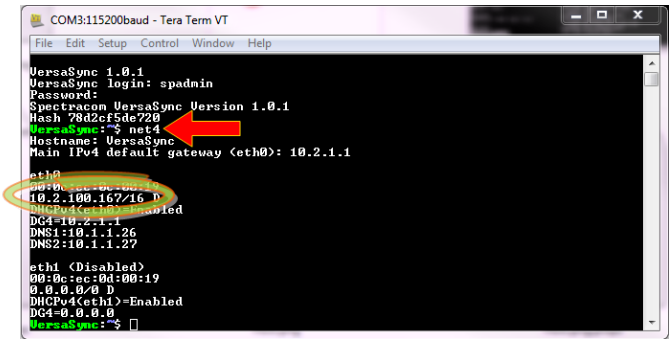
Note: The default login credentials are:
User name = spadmin
Password = admin123 (will not be displayed on the screen)

Note: For your reference, the command helpcli produces a list of available commands. Press the space key to display the next page, or the b key to display the previous page.

Note: Should it become necessary to leave the command help mode (indicated by a command line prompt ":"), press Q, or Ctrl C.

b. If you are on a DHCP-enabled network, you can assign an IP address by enabling DHCP on your unit. Use the `dhcp4set <x> on` command, (x being 0/1 for ETH0 and ETH1, respectively).

Retrieve the IP address assigned to VersaSync by typing the `net4` command. The command should return the network settings, including the IP address.



You can use this IP address to login to the VersaSync Web UI and then set a static IP address, subnet mask and gateway. (This can also be done via the CLI and a terminal emulator. See "Assigning a Static IP Address" on page 41).

c. If you are NOT on a DHCP-enabled network, your unit's IP address is set to the default for each Ethernet port, unless you have assigned a new static IP address.

For more detailed information about setting a static IP address for your unit, see "Setting up an IP Address" on page 40

Or, proceed to "Accessing the Web UI" below (it is recommended that you have identified or set your unit IP address for this step).

2.4 Accessing the Web UI

VersaSync's Web UI is the recommended tool to interact with the device, since it provides access to nearly all configurable settings, and obtain comprehensive status information without having to use the Command Line Interpreter (CLI).

You can access the Web UI either by using the default IP address, an automatically assigned DHCP IP address, or by using a manually set static IP address (see "Assigning a Static IP Address" on page 41).

1. On a PC connected to VersaSync via ETH1 or ETH0, start a web browser.
2. Navigate to the IP address assigned or identified in "Initial Network Setup" on page 34.

3. Log into the Web UI as an administrator. The factory-default administrator user name and password are:

   Username: `spadmin`

   Password: `admin123`

   Note: For security reasons, it is advisable to change the default credentials; see: "Managing Passwords" on page 263.

4. Upon initial login, you will be asked to register your product. Orolia recommends to register your VersaSync, so as to receive software updates and services notices. See also "Product Registration" on page 422.

2.5 Zero Configuration Setup

As an alternative to conventional network configuration, VersaSync can also be set up using the zero-configuration networking technology ("zeroconf").

Note: You can use Zeroconf on either Ethernet port if DHCP is enabled. Zeroconf must be used with a DHCP server.

When using zeroconf, a TCP/IP network will be created automatically, i.e. without the need for manual configuration: Once VersaSync's ETH connector is connected to a network, you can directly access the VersaSync Web UI, using a standard web browser, without any configuration.

Zeroconf can be used to connect to the unit through the Web UI:

- when you need to identify the IP address assigned to your unit through DHCP (DHCP must be enabled through the Web UI or CLI)
- in circumstances when your unit is not connected directly to a PC
- when you wish to access the Web UI of your VersaSync without using the CLI commands or serial connection
- anytime the IP address of a unit is not known

Zeroconf Requirements

Prior to using zeroconf, ensure the following requirements are met:

- Your network is DHCP enabled, and DHCP is enabled on the individual ETH port you are using.
- The PC you will use to communicate with your unit is connected to the same network as your VersaSync.
- Windows 7/8 users should install Bonjour Print Services, otherwise access to `*.local` addresses will not be possible.
- Windows 10 already supports mDNS and DNS-SD, hence there is no need to install additional software.

2.5.1 Using Zeroconf

Connect to the Web UI of your VersaSync unit in these steps:

1. Check the serial number label on the side of the unit, and write down the last 6 digits of the **MAC 0** address: e.g., "`0C 00 19`". Note that you will use the same MAC address for either Ethernet port.
2. Connect the VersaSync to a router on your LAN via the ETH connector (see "Initial Network Setup" on page 34).
3. Connect the power supply to the VersaSync unit.
4. On a connected computer, open your web browser and in the URL field type the following:

   versasync-[xxxxxx].local/

   where the [xxxxxx] of the hostname are the last six digits of the MAC 0 address you copied from the serial number label on the unit.

   You should now be prompted for a username and password. The factory default credentials are:

   Username: **spadmin**

   Password: **admin123**

Note: If you do not have physical access to the unit, you can obtain the MAC 0 address by accessing VersaSync's CLI via the I/O connector USB port, using e.g., the `ifconfig` command.

Once you logged into the VersaSync via zeroconf, you can retrieve the DHCP address for future use:

» Navigate to **MANAGEMENT: NETWORK > Network Setup**. In the **Ports** panel, click on the information button next to each Ethernet port. The popup window will display the assigned DCHP IP address for the selected port.

See "Setting up an IP Address" below or "Accessing the Web UI" on page 37 for more information.

2.6 Setting up an IP Address

In order for VersaSync to be accessible via your network, you need to assign an IP address to VersaSync, as well as a subnet mask and gateway, unless you are

using an address assigned by a DHCP server.

Before you continue ...

... please obtain the following information from the system network administrator:

- **Available static IP address**
  - This is the unique address your network administrator will assign to your VersaSync unit. Make sure the chosen address is outside of the DHCP range of your DHCP server.
- **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 VersaSync is made outside of the local network. By default, the gateway is disabled.

2.6.1 Assigning a Static IP Address

There are two ways to setup a permanent static IP address, after connecting VersaSync to a network:

Assigning a Static IP Address Using the CLI:

Note: For your reference, the command helpcli produces a list of available commands. Press the space key to display the next page, or the b key to display the previous page. To leave the command help file, press Q or Ctrl C.

Open the serial console, using a terminal emulator program

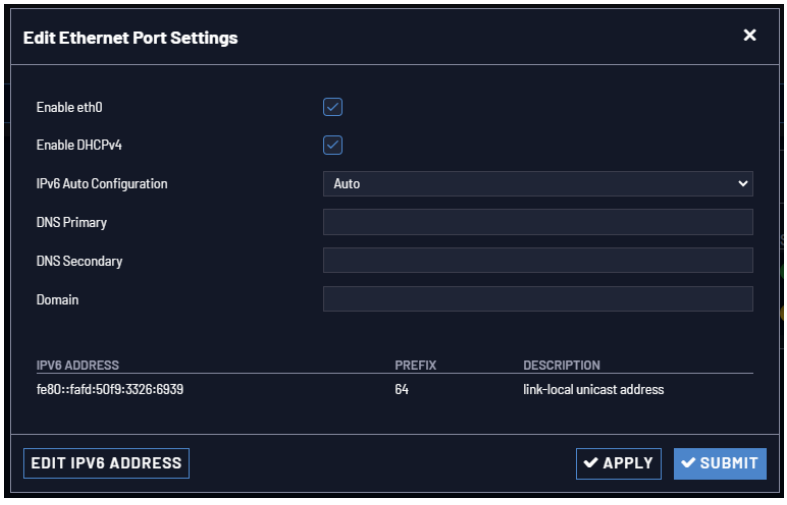
1. If necessary, disable DHCP – Command: `dhcp4set <x> off` (**where x is 0/1 for ETH0 and ETH1**, respectively).
2. Set the static IP address – Command: `ip4set <x>.<IP address>.<subnet mask>` Example: `ip4set 0 10.2.100.245 255.255.0.0`

   If required, also set your gateway address: `gw4set <x> <gateway address>`
3. Verify that the address has been accepted – Command: `net4`
4. If so required, turn DHCP back on – Command: `dhcp4set [x] on`

Assigning a Static IP Address Using the Web UI:

1. Enter the IP address identified during setup ("Initial Network Setup" on page 34) into the address field of your browser (on a computer connected to the VersaSync network). If the network supports DNS, the hostname may also be entered instead (the default hostname is "Spectracom"). The start screen of the VersaSync Web UI will be displayed.
2. Log into the Web UI as an administrator. The factory-default user name and password are:
   Username: `spadmin`
   Password: `admin123`
3. If necessary, disable DHCP by navigating to **MANAGEMENT > Network Setup**. In the **Ports** panel on the right, click the GEAR icon next to the Ethernet Port you are using. In the **Edit Ethernet Port Settings** window, uncheck the **Enable DHCPv4** field. Do NOT click Submit or Apply until you complete the next step to avoid error messages.
4. In the fields below the **Enable DHCPv4** checkbox, enter the desired Static IP address, Netmask, and Gateway address (if required). Click Submit.

   For subnet mask values, see "Subnet Mask Values" on page 421.



5. To verify that the address has been accepted, enter the static IP address into the address field of the browser and log into the Web UI again.
6. To continue with your configuration; see: "Configuring Network Settings" on page 72.

2.7 Configuring Inputs/Outputs

This Section covers the configuration of the inputs and outputs of the I/O connector and SMA connectors on the front panel..

When you configure an input our output via the I/O connector, you will need to adjust both the pin configuration ("Assigning I/O Pins" on the next page) and (for some types) the settings for that input or output via the Web UI ("Configure I/O Settings" on page 51).

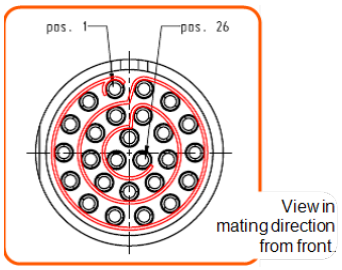


Figure 2-2: I/O connector

For more information on the I/O connector, see "Connectors and their Pinouts" on page 10.

Note: For instructions on how to configure the GNSS input reference, see "The GNSS Reference" on page 209 in the Chapter MANAGING TIME.

Note: The Network Ports eth0 and eth1 can be configured under MANAGEMENT > Network Setup. For more information, see "Configuring Network Settings" on page 72.

2.7.1 Assigning I/O Pins

VersaSync's I/O connector is software configurable, i.e. the pin interfaces and the signal modulations can be configured by the user via the VersaSync Web UI.

The software-configurable 26-pin I/O connector comprises 9 user-configurable Channels, plus one fixed USB interface. Channels can be used for the following input or output interfaces:

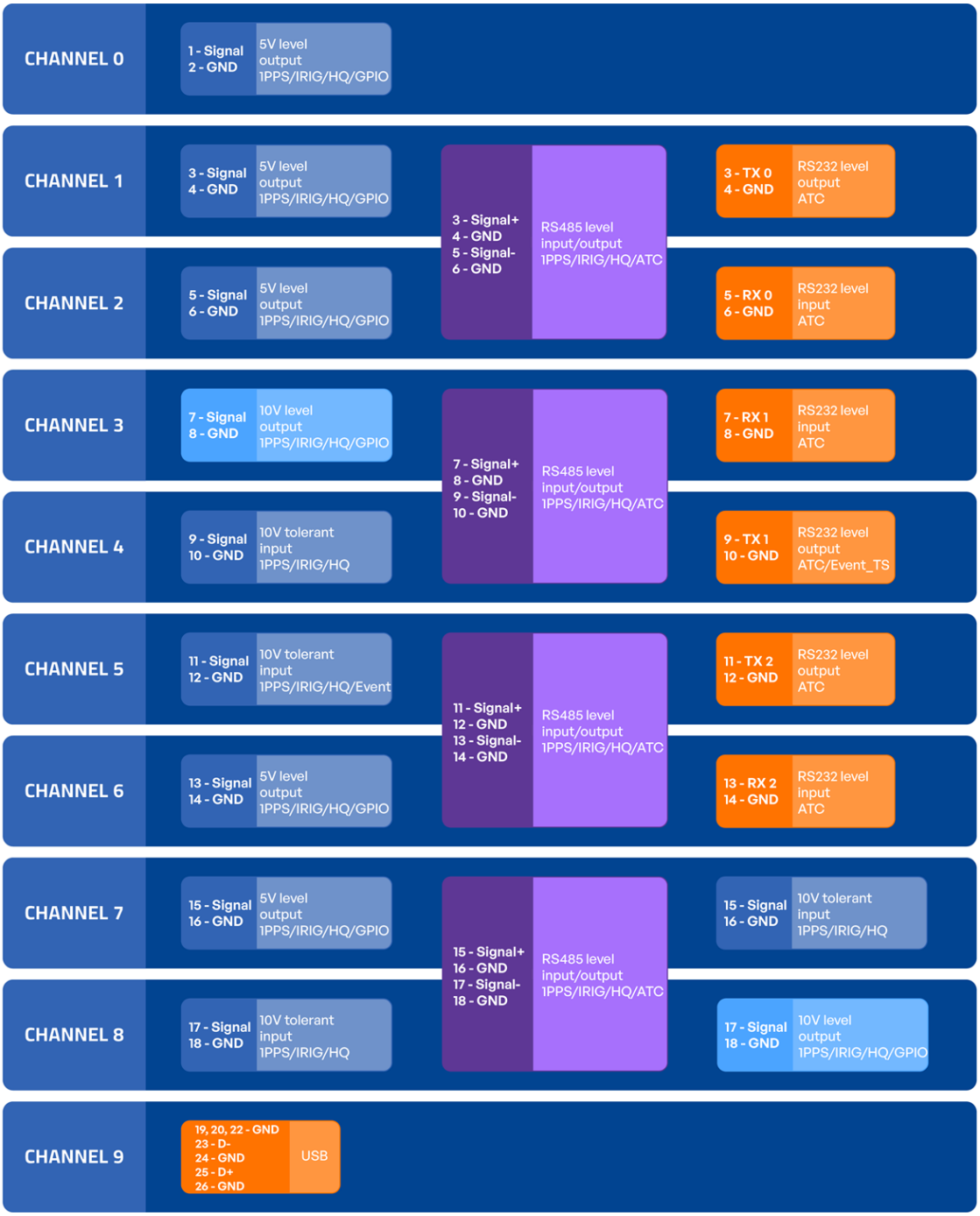


Figure 2-3: I/O configuration options for VersaSync models 1228-1610 and 1228-1311

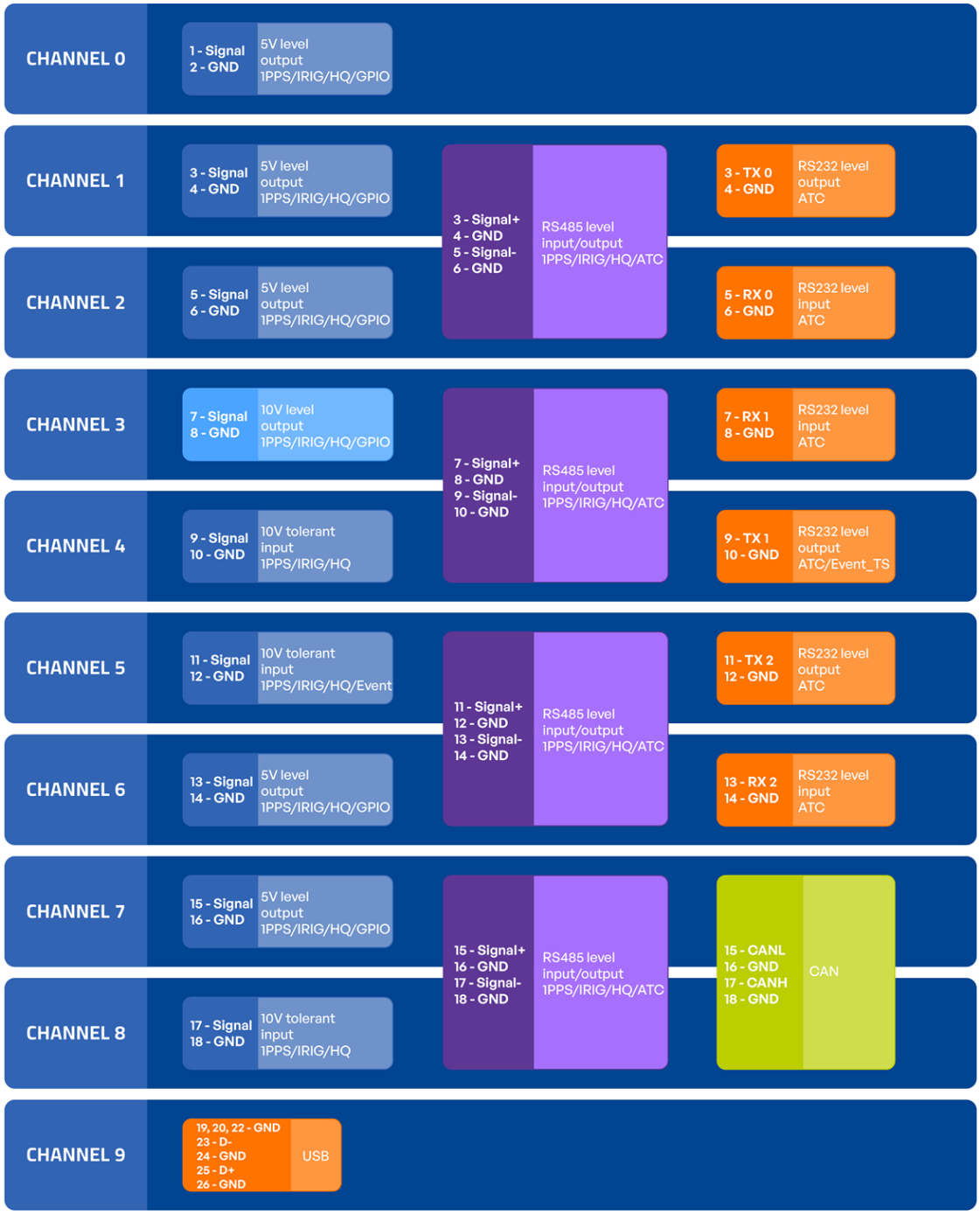


Figure 2-4: I/O configuration options for all other VersaSync models

2.7.1.1 Signal Types

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

Table 2-2: Available signal types for VersaSync models 1228-1610 and 1228-1311

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

Table 2-3: Available signal types for all other VersaSync models

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

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

DCLS Signal Lines

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

Single-ended Serial Lines

VersaSync provides up to 3 RX and 3 TX **RS232** interfaces for e.g., ASCII..

Differential Serial Lines

Up to four differential serial lines are available. Each of them can be set to **RS485** electrical standard, and used as input or output. PPS or Time-of-Day messages are available, as well as HAVE QUICK and other formats. Note that this kind of interface uses two Channels.

Non-Configurable Pins

Channel # 0 provides a DCLS TTL output signal that is not user-configurable.

Also note that **pins # 19 through 26** are reserved for the USB command line interface.

2.7.1.2 I/O Signal Mapping Table

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

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

Table 2-4: I/O signal mapping to Channels

					Channel											
					0	1	2	3	4	5	6	7	8	7	8	9
					Pin Position											
												Models 1228-1610 & 1228-1311		All Other Models		
	Signal Message Type	I/O	Type Filter	Electr. Level	1 & 2	3 & 4	5 & 6	7 & 8	9 & 10	11 & 12	13 & 14	15 & 16	17 & 18	15 & 16	17 & 18	19-25
Time & Frequency	PPS	out	DCLS	TTL	Y	Y	Y				Y	Y		Y		
	IRIG	out	DCLS	TTL	Y	Y	Y				Y	Y		Y		
	HQ	out	DCLS	TTL	Y	Y	Y				Y	Y		Y		
	GPIO	out	DCLS	TTL	Y	Y	Y				Y	Y		Y		
	ATC	out	RS232			Y			Y	Y						
	PPS	out	RS485			Y		Y		Y		Y		Y		
	IRIG	out	RS485			Y		Y		Y		Y		Y		
	HQ	out	RS485			Y		Y		Y		Y		Y		
	ATC	out	RS485			Y		Y		Y		Y		Y		
	PPS	in	RS485			Y		Y		Y		Y		Y		
	PPS	in	RS485	Load		Y		Y		Y		Y		Y		
	IRIG	in	RS485			Y		Y		Y		Y		Y		
	IRIG	in	RS485	Load		Y		Y		Y		Y		Y		
	HQ	in	RS485			Y		Y		Y		Y		Y		
	HQ	in	RS485	Load		Y		Y		Y		Y		Y		
	ATC	in	RS485			Y		Y		Y		Y		Y		
	ATC	in	RS485	Load		Y		Y		Y		Y		Y		
	ATC	in	RS232				Y	Y			Y					
	PPS	out	DCLS	10V				Y					Y			
	IRIG	out	DCLS	10V				Y					Y			
	HQ	out	DCLS	10V				Y					Y			
	GPIO	out	DCLS	10V				Y					Y			
	PPS	in	DCLS	10V					Y	Y		Y	Y			
	IRIG	in	DCLS	10V					Y	Y		Y	Y			
	HQ	in	DCLS	10V					Y	Y		Y	Y			
	PPS	in	DCLS	TTL					Y	Y		Y	Y		Y	
	IRIG	in	DCLS	TTL					Y	Y		Y	Y		Y	
	HQ	in	DCLS	TTL					Y	Y		Y	Y		Y	
	OPTION CARD					Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
	ATC EVENT	out	RS232						Y							
	GPIO EVENT	in	DCLS	TTL						Y						
	CAN BUS	in/out												Y		
																Occupied - USB

Notes:

Pins to Channels (e.g., pins 3 & 4= Channel 1)
green = Signal Message Type can be assigned to this Channel (RS485 requires two Channels)
red = This Signal Message type cannot be assigned to this Channel
ATC = ASCII Time Code

Note: Applying changes to the pin configuration will reset the reference priority table. See also "Configuring Input Reference Priorities" on page 189.

Configuring a new Input or Output

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

Restoring the Default I/O Configuration

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

The following illustration shows the **default I/O pin configuration**:

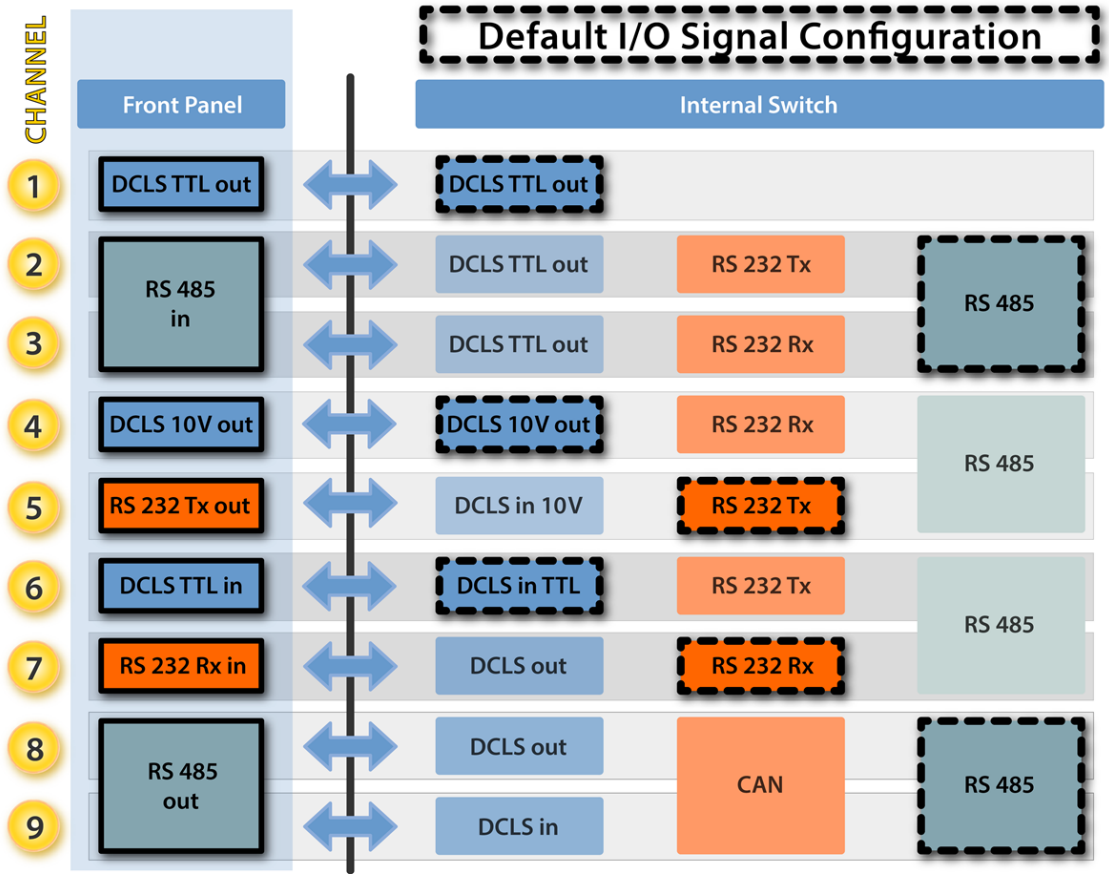


Figure 2-5: Default I/O configuration

To restore the default I/O pin configuration:

A. Navigate to the **MANAGEMENT: NETWORK > Pin Layout** screen.

B. In the **Actions** panel on the left, click **Restore Default Layout**.

Reloading the Current I/O Configuration

To reload the currently used I/O configuration after adding pin layout changes, but before clicking **Apply Changes**:

A. Navigate to the **MANAGEMENT: NETWORK > Pin Layout** screen.

B. In the **Actions** panel on the left, click **Reload Layout**.

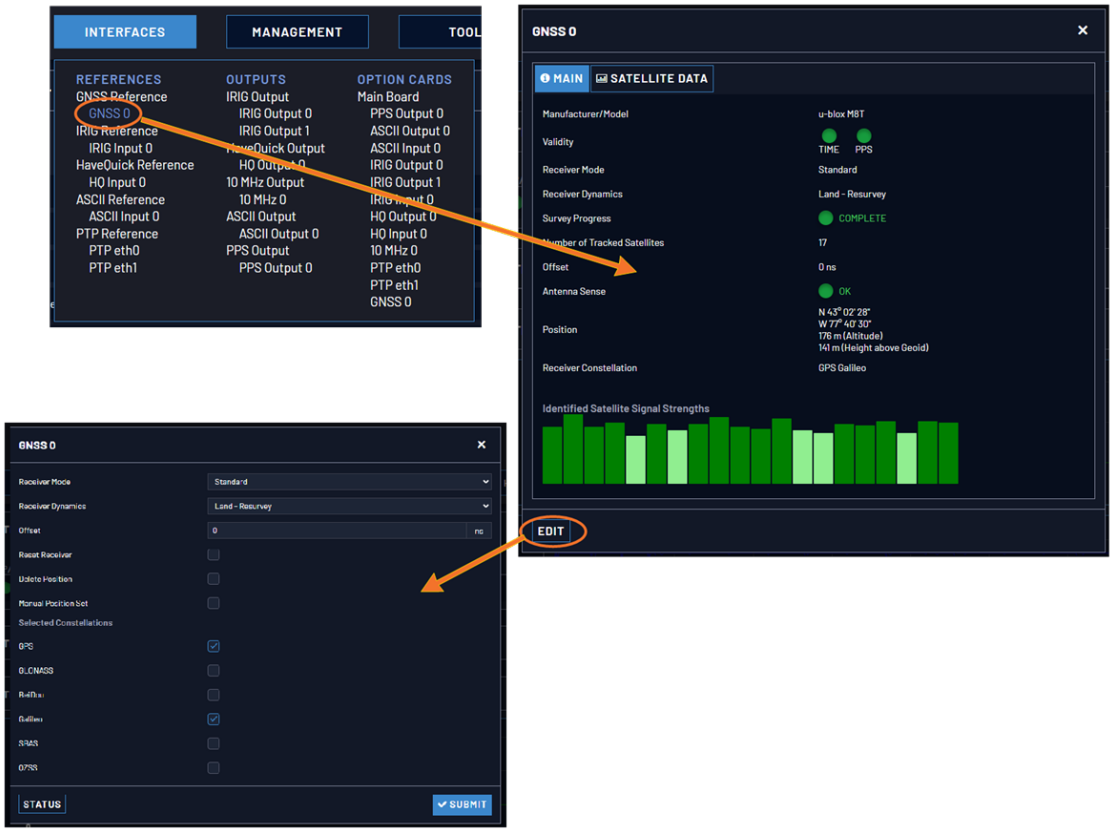
2.7.2 Configure I/O Settings

> **Note:** Illustrations shown below are examples; the windows displayed in your Web UI may look differently.

2.7.2.1 How to Configure an Input Reference

To access the user-editable settings of an Input Reference, choose one of these two methods:

Configuring the settings of an input reference, method 1:



1. Under **INTERFACES > REFERENCES**, click the desired reference.
2. The Status window for the specific reference you selected will be displayed. Click the Edit button in the bottom-left corner.
3. The settings window for the chosen reference will be displayed. Edit the field(s) as desired.

Configuring the settings of an input reference, method 2:

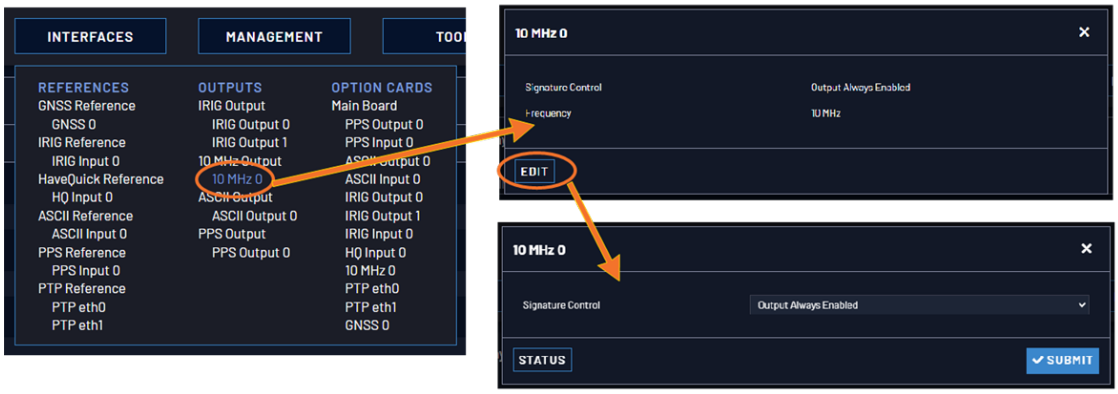
1. In the **INTERFACES > REFERENCES** drop-down menu, click **REFERENCES** (white on orange), or an input reference category (e.g., "GNSS reference").
2. In the Status window, click the GEAR button next to the desired input reference.
3. The settings window for the chosen reference will be displayed. Edit the field(s) as desired.

   For more information, see "Managing References" on page 187.

2.7.2.2 How to Configure an Output

To access the user-editable settings of an Output, choose one of these two methods:

Configuring the settings of an output, method 1:



1. Under **INTERFACES > OUTPUTS**, click the desired output.
2. The Status window for the specific reference you selected will be displayed. Click the **Edit** button in the bottom-left corner.
3. The settings window for the chosen output will be displayed. Edit the field(s) as desired.

   Configuring the settings of an output, method 1:Under **INTERFACES > OUTPUTS**, click the desired output. The Status window for the specific reference you selected will be displayed. Click the **Edit** button in the bottom-left corner. The settings window for the chosen output will be displayed. Edit the field(s) as desired.

Configuring the settings of an output, method 2:

1. In the **INTERFACES > OUTPUTS** drop-down menu, click OUTPUTS, or one of the output categories (**not** indented to the right)
2. In the Status window, click the GEAR button next to the desired output.
3. The settings window for the chosen output will be displayed. Edit the field (s) as desired.

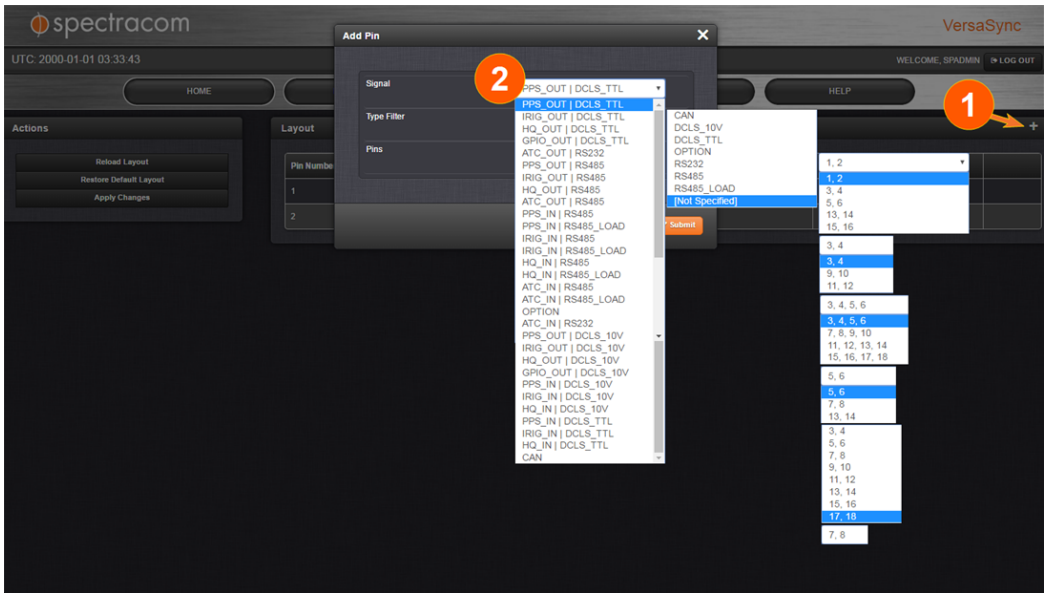
Note: Offset values for outputs are set in 20 ns increments and will round to the nearest multiple of 20 if not set to one exactly.

2.7.3 Example: Configuring a 20 PPS Output

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

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

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

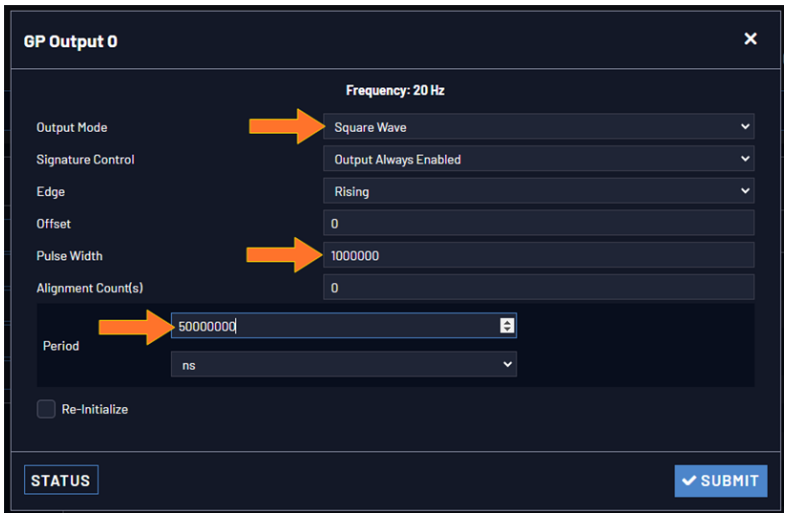


2. Prior to assigning the new output, identify a pin pair in the Pin Layout table that is not used (Signal = "None") or not needed. You can **Delete** it, but you may also simply assign the new PPS Output as described below, thus over-writing the existing Input or Output.
3. Add a pin configuration by clicking the PLUS icon in the top-right corner (1). The **Add Pin** window will display.
4. Start with the **Type Filter** drop-down menu (second line in the window) and select **DCLS_TTL**.
5. From the **Signal** drop-down menu, select **GPIO_OUT DCLS_TTL**.

6. From the **Pins** drop-down menu in line 3, select e.g., pins **1,2**.
7. Click **Submit**.
8. In the **Actions** panel, click **Apply Changes**.

Then, configure the settings for the newly created output:

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



13. Click Submit.

2.7.4 Configurable I/Os

2.7.4.1 Configuring a 1PPS Input

To configure a 1PPS Input:

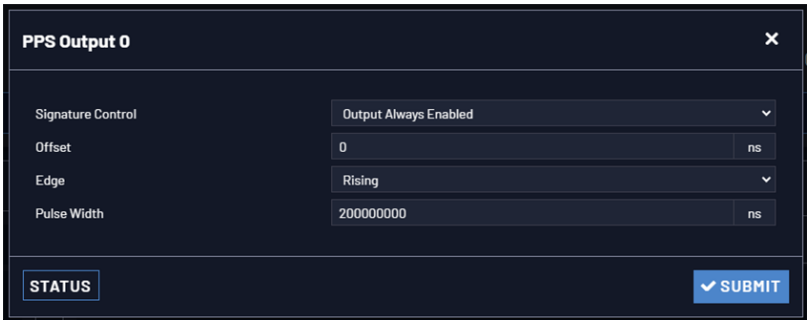
1. Navigate to **INTERFACES > REFERENCES: PPS Input 0** (or: **INTERFACES > OPTION CARDS: PPS Input 0**).
2. The PPS Input 0 Status window displays. Click Edit to open the configuration window:

3. Apply your settings for:
   - **Edge**: [Rising, Falling] The on-time point of the 1PPS input can be configured to be either the rising or falling edge of the 1PPS signal (by default, the rising edge is the on-time point).
   - **Offset**: [-500000000 to 500000000 ns = ±0.5 s] Allows to offset the system's 1PPS on-time point, e.g. to compensate for cable delays and other latencies
4. Click Submit.

2.7.4.2 Configuring a 1PPS Output

To configure a 1PPS output:

1. Navigate to **INTERFACES: OUTPUTS**, or to **INTERFACES: OPTION CARDS** (white on orange).
2. In the panel on the right, click the GEAR button next to the **1PPS Output** you want to edit.
3. The **1PPS Output** Edit window will display, allowing the following items to be configured:



- **Signature Control**: Determines when the output is enabled. For more information, see "Signature Control" on page 71.

- **Offset** [ns]: Allows to offset the system's 1PPS on-time point, e.g. to compensate for cable delays and other latencies [range = –500000000 to 500000000 ns = ±0.5 s]
- **Edge**: Used to determine if the on-time point of the 1PPS output is the rising or the falling edge of the signal.
  - **Rising**
  - **Falling**
- **Pulse Width** [ns]: Configures the Pulse Width of the 1PPS output.

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

4. Click Submit.

2.7.4.3 Configuring an ASCII Input

To configure an **ASCII Input** (ATC = ASCII Time Code):

1. Navigate to **INTERFACES > REFERENCES: ASCII Input 0** (or: **INTERFACES > OPTION CARDS: ASCII Input 0**). The status window will open, providing information on the current Reference ID, input Validity, ASCII Format, and if a pending Leap Second will be added to the UTC timescale at the end of the month. (See also "Local Clock(s), DST" on page 184.)
2. Click Edit to open the configuration window:

The following settings are editable:

- **Format Group**: Determines the time code message format category (see also "Time Code Data Formats" on page 343.) Choices are:

- Auto
- Spectracom
- NMEA
- EndRun

- **Format**: Once a **Format Group** has been selected, one or more **Format** fields may appear, allowing you to select one or more time code **Formats**. For detailed specifications and limitations on the supported time code formats, see "Time Code Data Formats" on page 343.

  Note: If Auto is chosen as the format group, the format will automatically be Auto-detect. VersaSync will attempt to identify the format of the incoming ASCII message.

- **Offset**: Provides the ability to account for ASCII input cable delays or other latencies in the ASCII input. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is –500 to +500 ms.
- **Timescale**: Used to select the time base for the incoming ASCII time code data. The entered Timescale is used by the system to convert the time in the incoming ASCII data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International
  - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of 20-November-2025, this is 18 seconds ahead of UTC time)
  - A **local clock** set up through the Time Management Page: This option will appear under the name of the local clock you have set up. Refer to "The Time Management Screen" on page 172 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.
    The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so

internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. See for more information on Local Clocks.

Note: The Timescale of the ASCII input (as configured in the ASCII time source) must be set correctly, especially if other input references are enabled. Failure to configure the Timescale of the ASCII input correctly could result in time jumps occurring in the System Time when input reference changes occur. These time jumps could affect NTP and normal operation of the system.

- **PPS Source**: Choices are:
  - **Message**: The 1PPS on time point is extracted from the ASCII message received.
  - **1PPS Pin**: The origin of the 1PPS on-time-point is the 1PPS input connector.
- **Baud Rate**: Determines the speed at which the input port will operate.
- **Data Bits**: Defines the number of Data Bits for the input output.
- **Parity**: Configures the parity checking of the input port.
- **Stop Bits**: Defines the number of Stop Bits for the input port.

3. Click Submit.

2.7.4.4 Configuring an ASCII Output

About the ASCII Format Outputs

The ASCII outputs (ATC = ASCII Time Code) provide VersaSync with the ability to output one, two or three back-to-back ASCII time code data streams that can be provided to peripheral devices which accept an ASCII RS-232 or RS-485 input data stream for either their external time synchronization or for data processing. See "Time Code Data Formats" on page 343 for a description of all supported time code formats.

The **RX signal** on an output interface is used for triggering the output ASCII message output when a configured character is received from the peripheral device.

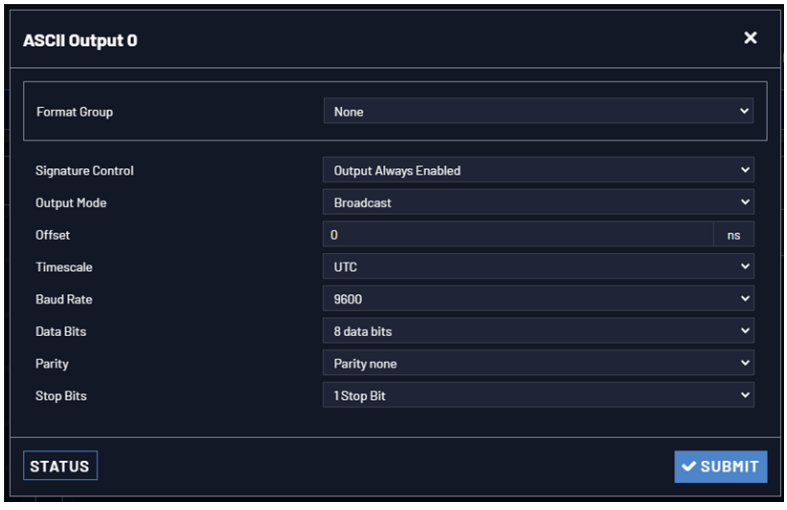
When VersaSync is configured to output only one format message (the second and third formats configured as “None”), the one configured message will be available on the output port as either a broadcast message or only upon a

request character being received. VersaSync has the ability to output one or two additional data stream messages immediately following the first message. In this configuration, only the first message determines the on-time point for the entire output string. The on-time points for the second and third messages that are provided at the same time as the first message are discarded. This unique capability allows VersaSync 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.

To configure an **ASCII Output**:

1. Navigate to **INTERFACES > OUTPUTS: ASCII Output 0**, or to **INTERFACES > OPTION CARDS: ASCII Output 0**. The status window will display, providing information on Signature Control and the message format (s).
2. Click the Edit button to open the configuration window:



The Edit window allows the configuration of the following settings:

- **Format Group**: configures the message format type. Choices are:
  - None (no message will be output)
  - Spectracom

- NMEA
- BBC
- ICD-153
- EndRun

Once selected, the **Format Group** may offer a choice of **Formats**. For more information on supported **Formats**, see "Time Code Data Formats" on page 343.

- **Format 1**: Selects either the first of up to three, or the only format message to be output.
- **Format 2**: Selects the second consecutive format message to be outputted. Select “None” if only one output format is desired. “None” will be the only choice available if Format 1 is “None.”
- **Format 3**: Selects the third consecutive format message to be outputted. Select “None” if only one output format is desired. “None” will be the only choice available if Format 2 is “None.”

- **Signature Control**: Signature Control controls when the selected ASCII data output format will be present; see "Signature Control" on page 71.
- **Output Mode**: This field determines when the output data will be provided. The available Mode selections are as follows:
  - **Broadcast**: The format messages are automatically sent out on authorized condition (Signature control), every second a message is generated in sync with the 1PPS.
  - **Request (On-time)**: A format message is generated in sync with 1PPS after the configured request character has been received.
  - **Request (Immediate)**: A format message is generated as soon as the request character is received. As this selection does not correlate the output data to the on-time point for the message, in Data Formats that do not provide sub-second information (such as Formats 0 and 1 whereas Format 2 provides sub-second information), it should be noted that the output data can be provided immediately, but a time error could occur when using the on-time point of the message in addition to the data for timing applications.

- 

  Note: The choices available in this field are determined by the choices of Format Group and Format.

- **Timescale**: Used to select the time base for the incoming data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International
  - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of 20-November-2025, this is currently 18 seconds ahead of UTC time).

  If GPS or TAI time is used, then the proper timescale offsets must be set on the **MANAGEMENT: OTHER > Time Management** page. (See "The Time Management Screen" on page 172 for more information on how to configure and read the System Time). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.
  - A **Local Clock** can be set up through the **Time Management** page: This option will appear under the name of the local clock you have set up. See for more information. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.
    The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock.
- **Baud Rate**: Determines the speed at which the output port will operate.
- **Data Bits**: Defines the number of Data Bits for the output port.
- **Parity**: Configures the parity checking of the output port.
- **Stop Bits**: Defines the number of Stop Bits for the output.

3. Click Submit.

2.7.4.5 Event Broadcast (ASCII Output)

The Event Broadcast functionality is available without a license through the multi-I/O connector and configured through the WebUI. The Event Broadcast system consists of an Event Input and an Event Broadcast output. Both the input and output for this fuctionality have settings and options.

When the defined signal edge is detected on the **Event Input** GPIO Connector, an ASCII message is created containing the current time, and **Event Broadcast** through the RS-232 Output port.

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. If another event is captured while a message is being sent, it will be queued in the buffer until the first message completes, then the next message will be sent.
- If the **Mode** is set to Request, messages in the **Message Buffer** are only sent when the Request Character is received.

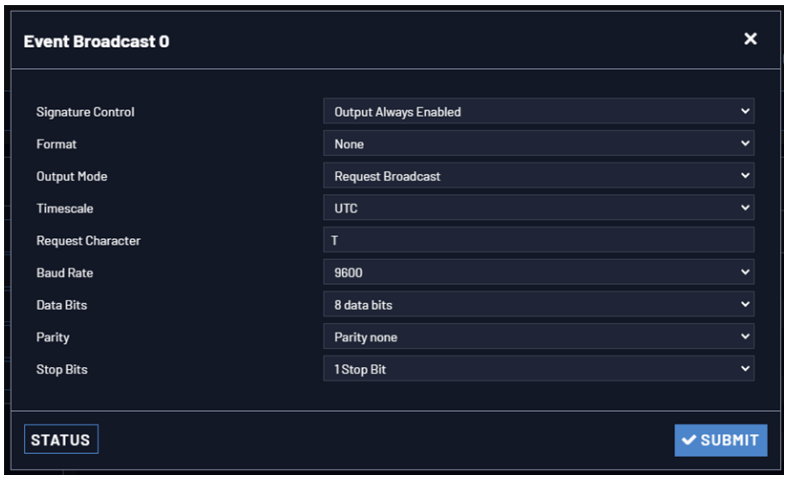
The output format used is selected among a small group of formats with the capability to output data at 5ns resolution. Event Broadcast Output formats are detailed in "Event Broadcast Time Code Formats" on page 401.

To configure the Event Broadcast functionality:

1. Configure the multi-I/O connector pinout to create the Event Input and Event Broadcast ports:
   - Enable the **Event Broadcast** output. Navigte to **MANAGEMENT** > **NETWORK** > **Pin Layout**. Click on the plus sign on the layout screen and scroll down the Signal Type until you select **ATC_OUT | RS232_EVENT**. This option must be configured on the 9 & 10 pins. Click submit.
   - Enable the **Event Input**. Click on the plus sign again, scroll down the Signal Type and select **GPIO_IN | DCLS_TTL**. This option must be configured on the 11 & 12 pins. Click submit.
2. Configure the input settings. Navigate to **INTERFACES** > **REFERENCES** > **EVENT INPUT 0**, or to **INTERFACES** > **OPTION CARDS**: **Event Input 0**. The status window will display, providing information on the current settings: the Event Capture and Event Active Edge settings, as well as the Last Event Message.
3. Click the Edit button to open the configuration window:

- **Event Capture**: Enables the processing of events on the Event Input (pins 11 & 12). 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, either rising or falling.

4. Click Submit.
5. Configure the output settings. Navigate to **INTERFACES > OUTPUTS: Event Broadcast 0**, or to **INTERFACES > OPTION CARDS: Event Broadcast 0**. The status window will display, providing information on the current settings.
6. Click the Edit button to open the configuration window:



The Edit window allows the configuration of the following settings:

- **Signature Control**: Signature Control controls when messages will be broadcast in response to events on the Event Input (J2) port when events are enabled and the card is in “broadcast” mode. (Events are still queued even if they are not broadcast, and are transmitted once the signature control conditions permit.) For more information on Signature Control, see "Signature Control" on page 71.
- **Format**: Selects the format of the message to be outputted. Refer to "Event Broadcast Time Code Formats" on page 401 for a description of all of the available formats.
  Event Broadcast only supports two formats (Event Broadcast Format 0 and Event Broadcast Format 1), and only supports the output of one message per event. If format is set to “None”, no messages will be queued in the Message Buffer.

- **Output Mode**: This field determines when the output data will be provided. Available Mode selections are as follows:
  - **Broadcast**—Event Messages are automatically broadcast when they are created by an event. If a new event happens while an older message is being broadcast, the new message will be queued in a "First-in, First-out" manner. When the message has finished, the next message out of the queue will be broadcast.
  - **Request**— [default: **t**] Event Messages are only broadcast in response to a Request Character. New messages will be queued in a "First-in, First-out" manner.
- **Timescale**—Used to select the time base for the incoming ASCII time code data. The entered Timescale is used by the system to convert the time in the incoming ASCII data stream to UTC time, in order to produce the Event Broadcast (always in UTC). The available choices are:
  - **UTC**— Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**—Temps Atomique International
  - **GPS**—The raw GPS time as transmitted by the GNSS satellites (as of 20-November-2025, this is 18 seconds ahead of UTC time)
- **Request character**: This field defines the character that VersaSync needs to receive in order for a message to be provided when in "Request" mode. This field will only appear if the Output Mode is set as "Request Broadcast."
- **Baud Rate**: 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.

7. Click Submit.

2.7.4.6 Configuring a GPIO Output

VersaSync can support up to five (5) programmable square-wave pulse outputs through the I/O connector. They are software-configurable via the VersaSync Web UI.

Note: When changing the offset value, the offset may not take effect immediately. It may take up to a minute or two depending on how high the alignment count is set to.

Specifications

- **Inputs/Outputs**: up to (5) programmable square wave outputs
- **Signal Type and Connector**: TTL (software-selectable Main I/O connector pins)
- **Accuracy**: ±50 ns (1σ)
- **Output Load Impedance**: 50 Ω
- **Rise Time to 90% of Level**: <10 ns
- **Programmable Period**: 100 ns to 1,000,000,000 ns in 5ns steps, to 60,000,000 µs in 1µs steps
- **Programmable Pulse Width**: 20 ns to 900 ms with 5 ns resolution

To configure one of the GPIO Outputs:

1. Navigate to **INTERFACES > OUTPUTS: GP Output [x]**.

   Note: I/O ports are numbered starting with 0.

   The **GP Output** Status window will display. It provides information on the Output Mode, if the output is Enabled, and its Current Value (i.e., low or high output level).

2. Click the Edit button in the lower left corner. The **GP Output** Edit will open, offering the following settings:
   - **Output Mode**: This is a drop-down list, offering the following options:
     - **Direct Output Value**: Output will be low or high determined by the **Output Value** selection below.
     - **1PPS**: Output will occur at a rate of one pulse per second.
     - **1PPM**:Output will occur at a rate of one pulse per minute.
     - **5MPPS/1PPS**: Composite setting with a 5 MHz clock with an extended pulse at the one second mark.
     - **Square Wave**: Output will generate a programmable square wave determined by the configuration.

- **Custom**: Output will be customized according to specific parameters.

- **Output Enabled**: Check this box to enable or disable the output. If Enabled, additional configurable parameters will be displayed.

If Direct Output mode is selected:

- **Signature Control**: Controls when the output will be present. See also: "Signature Control" on page 71.
- **Output Value**: Determines if the output level shall be **High** or **Low**.
- **Re-Initialize**: Re-initializes square wave generation and aligns to 1PPS.

If 1PPS or 1PPM is selected:

- **Signature Control**: Controls when the output will be present. See also: "Signature Control" on page 71.
- **Edge**: Used to determine if the on-time point of the output is the Rising or Falling edge of the signal.
- **Offset**: [ns] Accounts for cable delays and other latencies.
- **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.
- **Pulse Width**: [ns] Defines the pulse width. (For an application example, see "Example: Configuring a 20 PPS Output" on page 53.)
- **Re-Initialize**: Re-initializes square wave generation and aligns to 1PPS.

If Square Wave output mode is selected:

- **Signature Control**: Controls when the output will be present. See also: "Signature Control" on page 71.
- **Edge**: Used to determine if the on-time point of the output is the Rising or Falling edge of the signal.
- **Offset**: [ns] Accounts for cable delays and other latencies.
- **Pulse Width**: [ns] Defines the pulse width. (For an application example, see "Example: Configuring a 20 PPS Output" on page 53.)
- **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.

- **Period**: Sets the period of the square wave (in ns or µs scale).
  - The wave's frequency will display at the top of the window once you have configured the output. The frequency is calculated based on the Period and Period Correction settings.
- **Re-Initialize**: Re-initializes square wave generation and aligns to 1PPS.

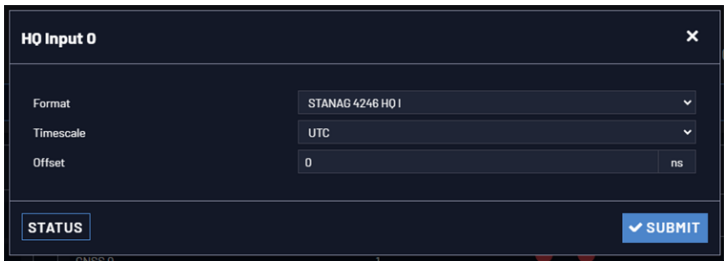
If Custom is selected:

- **Signature Control**: Controls when the output will be present. See also: "Signature Control" on page 71.
- **Edge**: Used to determine if the on-time point of the output is the Rising or Falling edge of the signal.
- **Offset**: [ns] Accounts for cable delays and other latencies.
- **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.
- **Pulse Width**: [ns] Defines the pulse width. (For an application example, see "Example: Configuring a 20 PPS Output" on page 53.)
- **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) This changes the function of the alignment counter to align the square wave whenever the current time's seconds value is a multiple of the alignment count. For example: If time alignment is enabled and alignment count is set to 15 seconds, the square wave will be aligned to the 1PPS when the seconds value on the time display equals 00, 15, 30, 45.
- **Period**: Sets the period of the square wave (in ns, µs, ms, or s scale).
  - The wave's frequency will display at the top of the window once you have configured the output. The frequency is calculated based on the Period and Period Correction settings.
- **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 ns
- **R7e-Initialize**: Re-initializes square wave generation and aligns to 1PPS.

2.7.4.7 Configuring a HaveQuick Input

To configure a HaveQuick input:

1. Navigate to **INTERFACES > REFERENCES: HQ Input 0** (or: **INTERFACES > OPTION CARDS: HQ Input 0**). The **Status** window will open, displaying information on the current Reference ID, input Validity, TOD Format, Time Scale, Offset, and TFOM. (For more information on TFOM, see "Time Figure of Merit (TFOM)" on page 241.)
2. Click **Edit** to open the **Configuration** window.



The following settings are configurable:

- **ToD Format**: The user-selectable format to be used. Available formats include:
  - STANAG 4246 HAVE QUICK I
  - STANAG 4246 HAVE QUICK II
  - STANAG 4372 HAVE QUICK IIA
  - STANAG 4430 Extended HAVE QUICK
  - STANAG 4430 Standard Time Message (STM)
  - ICD-GPS-060A BCD Time Code
  - ICD-GPS-060A HAVE QUICK
  - DOD-STD-1399 BCD Time Code
- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International

- **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of 20-November-2025, this is 18 seconds ahead of UTC time).
- A **local clock** can be set up through the Time Management Page; see "Local Clock(s), DST" on page 184. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

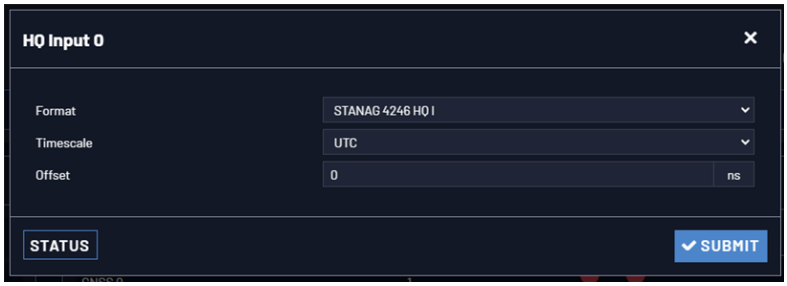
- **Offset**: Provides the ability to account for STANAG Line (TOD1 and TOD2 independently) cable delays or other latencies in the STANAG input. Available Offset range is –500 to +500 ms in 5ns steps.

3. Click Submit.

2.7.4.8 Configuring a HaveQuick Output

To configure a HaveQuick output:

1. Navigate to **INTERFACES > OUTPUTS: HQ Output 0**, or to **INTERFACES > OPTION CARDS: HQ Output 0**. The Status window will display, providing information on Signature Control, message Format, Timescale, and Offset.
2. Click Edit. The Configuration window will display.



The following settings are configurable:

- **Signature Control**: Used to control when the signal will be present. This function allows the modulation to stop under certain conditions, see also "Signature Control" on page 71.
- **TOD Format**: The user-selectable format to be used. Available formats include:
  - STANAG 4246 HQI
  - STANAG 4246 HQII
  - STANAG 4372 HQIIA

- STANAG 4430 STM
- STANAG 4430 XHQ
- ICD-GPS-060A BCD
- ICD-GPS-060A HQ
- DOD-STD-1399 BCD

- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**— Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**—Temps Atomique International
  - **GPS**—The raw GPS time as transmitted by the GNSS satellites (as of 20-November-2025, this is 18 seconds ahead of UTC time)
  - A **local clock** set up through the Time Management Page—Refer to "The Time Management Screen" on page 172 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.
- **Offset (ns)**: Provides the ability to account for STANAG Line (TOD1 and TOD2 independently) cable delays or other latencies in the STANAG output. Available Offset range is –500 to +500 ms in 5ns steps.

3. Click Submit.

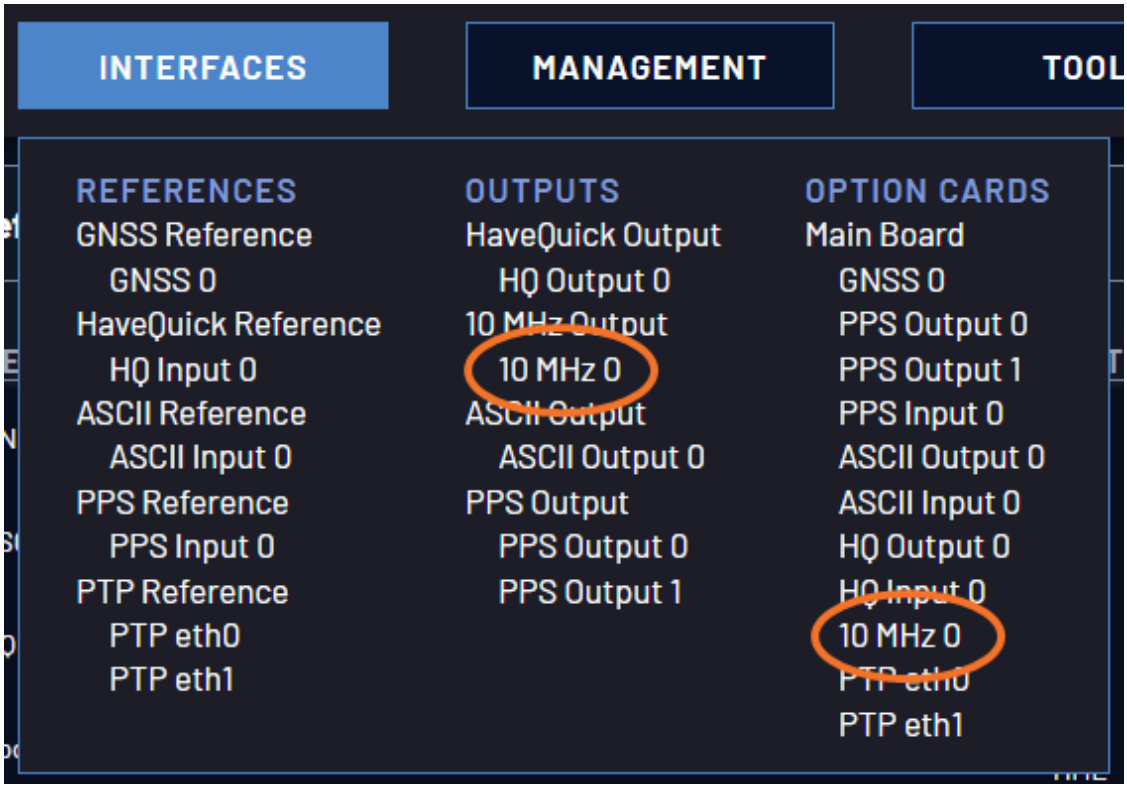
2.7.4.9 The 10 MHz Outputs

The 10 MHz signal is provided by the internal oscillator. Depending on the product configuration placed at the time of ordering, VersaSync offers up to four 10 MHz outputs.

The four 10 MHz outputs are all controlled via one setting (for example, all SMA outputs are off). To configure these outputs, navigate to:

- **INTERFACES > OUTPUTS,** or
- **INTERFACES > OPTION CARDS > Main**

and select the **10 MHz Output 0**.



In the **10 MHz 0** Status Page, choose Edit, and select your designated Signature Control to select the behavior of all the SMA outputs. (See "Signature Control" below for more information).

Submit your changes.

2.7.5 Signature Control

Signature Control is a user-set parameter that controls under which output states an output will be present. This feature allows you to determine how closely you want to link an output to the status of the active input reference e.g., by deactivating it after holdover expiration. It is also offers the capability to indirectly send an input-reference-lost-alarm to a downstream recipient via the presence of the signal.

EXAMPLES:

You can setup Signature Control such that VersaSync's built in 1PPS output becomes disabled the moment its input reference is lost (e.g., if a valid GNSS signal is lost).

Or, you can setup your output signal such that remains valid while VersaSync in holdover mode, but not in free run.

The available options are:

I. **Output Always Enabled**—The output is present, even if VersaSync is not synchronized to its references (VersaSync is free running).

II. **Output Enabled in Holdover**—The output is present unless VersaSync is not synchronized to its references (VersaSync is in Holdover mode).

III. **Output Disabled in Holdover**—The 1PPS output is present unless the VersaSync references are considered not qualified and invalid (the output is NOT present while VersaSync is in Holdover mode.)

IV. **Output Always Disabled**—The output is never present, even if VersaSync references are present and valid.

Table 2-5: Signature control output-presence states

Ref.	Out-of-sync, no holdover	In holdover	In-sync with external reference
I.	✓	✓	✓
II.	✗	✓	✓
III.	✗	✗	✓
IV.	✗	✗	✗

Configuring Signature Control for an Output

To review or configure the Signature Control setting for any output:

1. Navigate to **INTERFACES > OUTPUTS** and click the output you want to configure.
2. In the **Outputs** panel, click the GEAR button for the desired output. Ehe **Edit** window will open with the current Signature Control setting, and a drop-down list to change it.

2.8 Configuring Network Settings

Before configuring the network settings, you need to setup access to VersaSync web user interface ("Web UI"). This can be done by assigning a static IP address,

or using a DHCP address. For more information, see "Assigning a Static IP Address" on page 41.

Once you have assigned the IP address, login to the Web UI. For more information, see "Accessing the Web UI" on page 37.

To configure network settings, or monitor your network, navigate to VersaSync's **Network Setup** screen.

To access the **Network Setup** screen:

» Navigate to **MANAGEMENT > Network Setup**. The **Network Setup** screen is divided into three panels:

The Actions panel provides:

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

» **Web Interface Settings**:

  » Web interface **timeout**: Determines how long a user can stay logged on. For more information, see "Web UI Timeout" on page 266.

» **Access Control**: Allows the configuration of access restrictions from assigned networks/nodes.

» **Login Banner**: Allows the administrator to configure a custom banner message to be displayed on the VersaSync Web UI login page and the CLI (Note: There is a 2000 character size limit).

- **SSH**: This button takes you to the **SSH Setup** window. For details on setting up SSH, see "SSH" on page 91.
- **System Time Message**: Setup a once-per-second time message to be sent to receivers via multicast. For details, see "System Time Message" on page 110.
- **VLAN**: This button will reveal the **VLAN Setup** popup window. For more information, see "VLAN Support" on page 109.
- **HTTPS**: This button takes you to the **HTTPS Setup** window. For details on setting up HTTPS, see "HTTPS" on page 80.
- **DNSSEC**: This button takes you to the **DNSSEC Setup** window. For more information, see "DNSSEC" on page 111.

The Network Services panel is used to enable (ON) and disable (OFF) network services, as well as the Web UI display mode, details see: "Network Services" on page 77.

The Ports panel not only displays STATUS information, but is used also to set up and manage VersaSync's network ports via three buttons:

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

2.8.1 General Network Settings

To expedite network setup, VersaSync provides the **General Settings** window, allowing quick access to the primary network settings.

To access the **General Settings** window:

1. Navigate to **MANAGEMENT > Network Setup**. In the **Actions Panel** on the left, click **General Settings**.

2. Populate the fields:
   - **Hostname**: This is the server's identity on the network or IP address.
   - **Default IPv4 Port**: Unless you specify a specific Port to be used as Default Port, the factory default port **eth0** will be used as the gateway (default gateway).
   - **Default IPv6 Port**: Unless you specify a specific Port to be used as Default Port, the factory default port **eth0** will be used as the gateway (default gateway).

   The **General Settings** window also displays the IPv4 Address and default IPv4 Gateway.

2.8.2 Network Ports

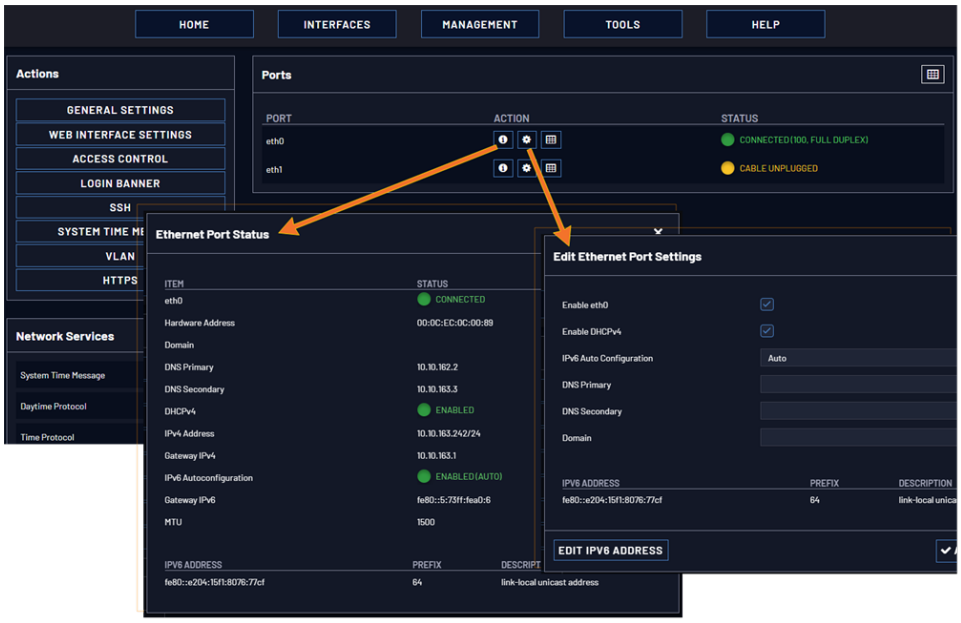
Ports act as communication endpoints in a network. The hardware configuration of your unit will determine which ports (e.g., Eth0, Eth1, ...) are available for use.

To enable & configure, or view a network port:

1. Navigate to **MANAGEMENT > NETWORK: Network Setup**.
2. The **Ports** panel on the right side of the screen lists the available Ethernet ports, and their connection STATUS:
   - **Green: CONNECTED** (showing the connection speed)
   - **Yellow: CABLE UNPLUGGED** (the port is enabled but there is no cable attached)
   - **Red: DISABLED**.

     Locate the port you want to configure (eth0 or eth1) and click the GEAR button to enable & configure the port, or the INFO button to

view the port status.



3. Ethernet ports are enabled by default. If the port is not already enabled, in the **Edit Ethernet Ports Settings** window, click the **Enable** check box. The **Edit Ethernet Ports Settings** window will expand to show the options needed to complete the port setup.

   Fill in the fields as required:

   - **Enable eth0**: [Checkbox]
   - **Enable DHCPv4**: [Checkbox] Check this box to enable the delivery of IP addresses from a DHCP Server using the DHCPv4 protocol.
   - **Static IPv4 Address**: This is the default, or the unique address assigned by the network administrator.

     Table 2-6: Default IP addresses

ETH port	Default IP address
ETH0	192.168.1.1
ETH1	192.168.1.2

     The default subnet is: 255.255.0.0

   - **Netmask**: This is the network subnet mask assigned by the network administrator. In the form "`xxx.xxx.xxx.xxx`." See "Subnet Mask Values" on page 421 for a list of subnet mask values.

- **IPv4 Gateway**: The gateway (default router) address is needed if communication to the VersaSync is made outside of the local network. By default, the gateway is disabled.
- **IPv6 Auto Configuration**: Choose between Disabled (disable auto configuration), Auto (stateless auto configuration using SLAAC and DHCP), and Stateful (auto configuration using DHCP only).
- **IPv6 Gateway**: A static IPv6 gateway is needed if IPv6 Auto Configuration is disabled.
- **Domain**: This is the domain name to be associated with this port.
- **DNS Primary**: This is the primary DNS address to be used for this port. Depending on how your DHCP server is configured, this is set automatically once DHCP is enabled. Alternatively, you may configure your DHCP server to NOT use a DNS address. When DHCP is disabled, DNS Primary is set manually, using the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].
- **DNS Secondary**: This is the secondary DNS address to be used for this port. Depending on how your DHCP server is configured, this is set automatically once DHCP is enabled, or your DHCP server may be configured NOT to set a DNS address. When DHCP is disabled, DNS Secondary is set manually, using the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].

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

2.8.3 Network Services

Several standard network services can be enabled or disabled via the easily accessible **Network Services** Panel under **MANAGEMENT** > **Network Setup**:

The **Network Services** panel has ON/OFF toggle switches for the following daemons and features:

- **System Time Message**: A once-per second Time Message sent out via Multicast; for details, see "System Time Message" on page 110.
- **Daytime Protocol, RFC-867**: A standard Internet service, featuring an ASCII daytime representation, often used for diagnostic purposes.
- **Time Protocol, RFC-868**: This protocol is used to provide a machine-readable, site-independent date and time.
- **Telnet**: Remote configuration

- **SSH + SFTP**: Secure Shell cryptographic network protocol for secure data communication and secure access to logs.
- **HTTP**: Hypertext Transfer Protocol. Default = OFF.
- **tcpdump**: A LINUX program that can be used to monitor network traffic by inspecting tcp packets. Default = ON.
  If not needed, or wanted (out of concern for potential security risks), **tcpdump** can be disabled permanently: Once Remove is selected, **tcpdump** will be deleted from the system: the Web UI section will be removed, and the function cannot be enabled again (even after a software upgrade) unless a full CLEAN upgrade is performed. Removing tcpdump on this page will also remove the PTP-specific functionality (see "The PTP Master Settings Panel" on page 165).

2.8.4 Static Routes

Static routes are manually configured routes used by network data traffic, rather than solely relying on routes chosen automatically by DHCP (Dynamic Host Configuration Protocol). With statically configured networks, static routes are in fact the only possible way to route network traffic.

To view, add, edit, or delete a static route:

1. Navigate to the **MANAGEMENT > Network Setup** screen.
2. The **Ports** panel displays the available Ethernet ports, and their connection status.
3. To view all configured Static Routes for all Ethernet Ports, or delete one or more Static Routes, click the **TABLE** icon in the top-right corner.
4. To add a new Route, view or delete an existing Route for a specific Ethernet Port, locate the Port listing you want to configure, and click the **TABLE** button next to it.
   The **Static Routes** window for the chosen Port will open, displaying its Routing Table, and an **Add Route** panel.
   - In the **Add Route** panel, populate these fields in order to assign a Static Route to a Port:
     - **Net Address**: This is the address/subnet to route to.
     - **Prefix**: This is the subnet mask in prefix form e.g., "24". See also "Subnet Mask Values" on page 421.
     - **Router Address**: This is where you will go through to get there.
   - Click the **Add Route** button at the bottom of the screen.

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

Note: Do not use the same route for different Ethernet ports; a route that has been used elsewhere will be rejected.

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

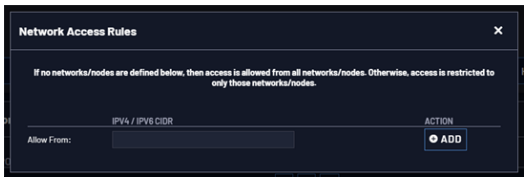
2.8.5 Access Rules

Network access rules restrict access to only those assigned networks or nodes defined. If no access rules are defined, access will be granted to all networks and nodes.

Note: In order to configure Access Rules, you need ADMINISTRATOR rights.

To configure a new, or delete an existing access rule:

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



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

IP address nomenclature:

IPv4—`10.10.0.0/16`, where `10.10.0.0` is the IP address and `16` is the subnet mask in prefix form. See the table "Subnet Mask Values" on page 421 for a list of subnet mask values.

IPv6—`2001:db8::/48`, representing `2001:db8:0:0:0:0:0:0` to `2001:db8:0:ffff:ffff:ffff:ffff:ffff`.

5. Click the **Add** button in the **Action** column to add the new rule.
6. The established rule appears in the **Network Access Rules** window. Click the **Delete** button next to an existing rule, if you want to delete it.

2.8.6 HTTPS

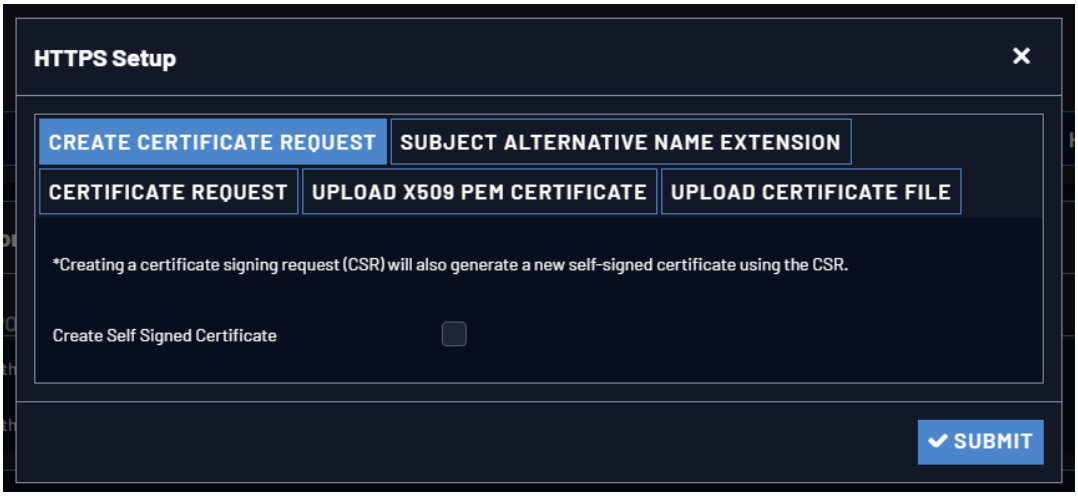
HTTPS stands for HyperText Transfer Protocol over SSL (Secure Socket Layer). This TCP/IP protocol is used to transfer and display data securely by adding an encryption layer to protect the integrity and privacy of data traffic. Certificates issued by trusted authorities are used for sender/recipient authentication.

Note: In order to configure HTTPS, you need ADMINISTRATOR rights.

Note that VersaSync supports two different modes of HTTPS operation: The **Standard HTTPS Level** (default), and a **High-Security Level**. For more information, see "HTTPS Security Levels" on page 285.

2.8.6.1 Accessing the HTTPS Setup Window

1. Navigate to **MANAGEMENT** > **NETWORK: HTTPS Setup** (or, navigate to **MANAGEMENT** > **Network Setup**, and click **HTTPS** in the **Actions** panel on the left):



The **HTTPS Setup** window has five tabs:

- **Create Certificate Request**: This menu utilizes the OpenSSL library to generate certificate Requests and self-signed certificates.
- **Subject Alternative Name Extension**: This menu is used to add alternative names to an X.509 extension of a Certificate Request.
- **Certificate Request**: A holder for the certificate request generated under the **Create Certificate Request** tab. Copy and paste this Certificate text in order to send it to your Certificate Authority.
- **Upload X.509 PEM Certificate**: Use the window under this tab to paste your X.509 certificate text and upload it to VersaSync.
- **Upload Certificate File**: Use this tab to upload your certificate file returned by the Certificate Authority. For more information on format types, see "Supported Certificate Formats" on the next page.

Exit the **HTTPS Setup** window by clicking the **X** icon in the top right window corner, or by clicking anywhere outside the window.

Should you exit the **HTTPS Setup** window while filling out the certificate request parameters form *before* clicking the Submit button, any information you entered will be lost. Exiting the **HTTPS Setup** window will not lose and Subject Alternative Names that have been entered. When switching between tabs within the **HTTPS Setup** window, the information you have entered will be retained.

2.8.6.2 About HTTPS

HTTPS provides secure/encrypted, web-based management and configuration of VersaSync from a PC. In order to establish a secure HTTPS connection, an SSL certificate must be stored inside the VersaSync unit.

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

Once you created a certificate request, submit the request to an external Certificate Authority (CA) for the creation of a third party verifiable certificate. (It is also possible to use an internal corporate Certificate Authority.)

If a Certificate Authority is not available, or while you are waiting for the certificate to be issued, you can use the default Safran self-signed SSL certificate that comes with the unit until it expires, or use your own self-signed certificate. The typical life span of a certificate (i.e., during which HTTPS is available for use) is about 10 years.

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

Note: In a Chrome web browser, if a valid certificate is deleted or changed such that it becomes invalid, it is necessary to navigate to Chrome's Settings> More Tools> Clear browsing data> Advanced and clear the Cached images and files in the history. Otherwise Chrome's security warnings may make some data unavailable in the Web UI.

Note: If the IP Address or Common Name (Host Name) is changed, you need to regenerate the certificate, or you will receive security warnings from your web browser each time you log in.

2.8.6.3 Supported Certificate Formats

VersaSync supports X.509 PEM and DER Certificates, as well as PKCS#7 PEM and DER formatted Certificates.

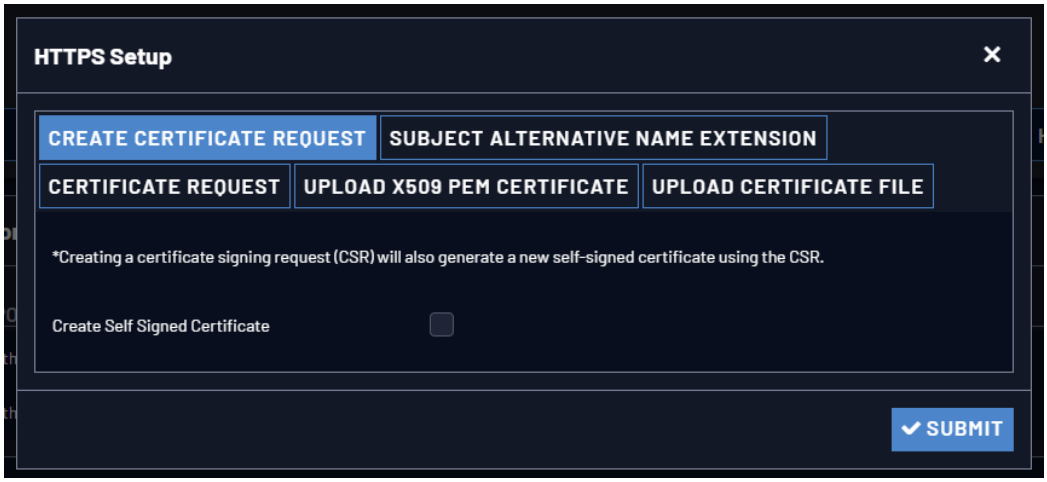
You can create a unique X.509 self-signed Certificate, an RSA private key and X.509 certificate request using the Web UI. RSA private keys are supported because they are the most widely accepted. At this time, DSA keys are not supported.

2.8.6.4 Creating an HTTPS Certificate Request

> **Caution:** If you plan on entering multiple Subject Alternative Names to your HTTPS Certificate Request, you must do so before filling out the Create Certificate Request tab to avoid losing any information. See "Adding HTTPS Subject Alternative Names" on page 86.

To create an HTTPS Certificate Request:

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



2. Click the **Create Certificate Request** tab (this is the default tab).
3. Check the box Create Self Signed Certificate, in order to open up all menu items.

   This checkbox serves as a **security feature**: Check the box **only** if you are certain about generating a new self-signed Certificate.

   > **Caution:** Once you click Submit, a previously generated Certificate (or the Safran default Certificate) will be overwritten.

   Note that an invalid Certificate may result in denial of access to VersaSync via the Web UI!

4. Fill in the available fields:
   - **Signature Algorithm**: Choose the algorithm to be used from:
     - MD4
     - SHA1
     - SHA256
     - SHA512

     Note: Due to FIPS 140-2 compliance, SHA1 will be unavailable if OpenSSL mode in the Web UI Security Dashboard page is set to Enhanced Security Core. For more information about FIPS 140-2, see "Web UI Security Dashboard" on page 281.

   - **Private Key Pass Phrase**: This is the RSA decryption key. This must be at least 4 characters long.
   - **RSA Private Key Bit Length**: 2048 bits is the default. Using a lower number may compromise security and is not recommended.
   - **Two-Letter Country Code**: This code should match the ISO-3166-1 value for the country in question.
   - **State Or Province Name**: From the address of the organization creating up the Certificate.
   - **Locality Name**: Locale of the organization creating the Certificate.
   - **Organization Name**: The name of the organization creating the Certificate.
   - **Organization Unit Name**: The applicable subdivision of the organization creating the Certificate.
   - **Common Name (e.g. Hostname or IP)**: This is the name of the host being authenticated. The Common Name field in the X.509 Certificate must match the hostname, IP address, or URL used to reach the host via HTTPS.
   - **Email Address**: This is the email address of the organization creating the Certificate.
   - **Challenge Password**: Valid response password to server challenge.
   - **Optional Organization Name**: An optional name for the organization creating the Certificate.

» **Self-Signed Certificate Expiration (Days)**: How many days before the Certificate expires. The default is 7200.

> **Caution:** No fields can be left blank. Enter an arbitrary value, as necessary, to ensure all fields have any entry before submitting. Leaving any fields blank when submitting will prevent the creation of the new Certificate Request.

You are required to select a signature algorithm, a private key passphrase of at least 4 characters, a private key bit length, and the Certificate expiration in days. The remaining fields are optional.

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

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

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

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

> **Note:** The default key bit length value is 2048.

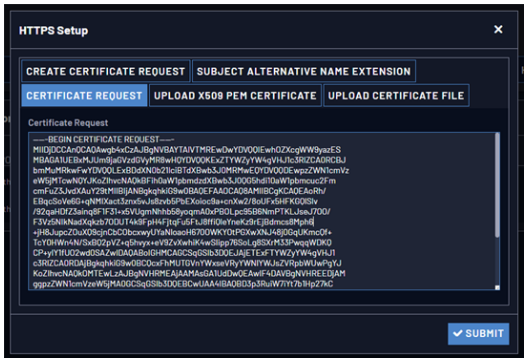
When using a self-signed Certificate, choose values based on your company's security policy.

5. When the form is complete, confirm that you checked the box **Create Self Signed Certificate** at the top of the window, then select **Submit**. Selecting the **Submit** button automatically generates the Certificate Request in the proper format for subsequent submission to the Certificate Authority.

Note: It may take several minutes for VersaSync to create the Certificate request and the private key (larger keys will require more time than small keys). If the unit is rebooted during this time, the Certificate will not be created.

Caution: In order for the Certificate Request to successfully submit, you must wait 30 seconds and refresh your browser after selecting the **Submit** button.

To view the newly generated request, in the **HTTPS Setup** window, click the **Certificate Request** tab.



When switching between tabs within the **HTTPS Setup** window, the information you have entered will be retained. If you exit the **HTTPS Setup** window before clicking Submit, the information will be lost.

2.8.6.5 Adding HTTPS Subject Alternative Names

Caution: Subject Alternative Names must be added before a new Certificate Request is generated, otherwise the Certificate Request will have to be created again to include the Subject Alternative Names. Any information entered into the Create Certificate Request tab that has not been submitted will be lost by adding, deleting, or editing Subject Alternative Names.

It is recommended that you consult your Certificate Authority regarding questions of Subject Alternative Name usage.

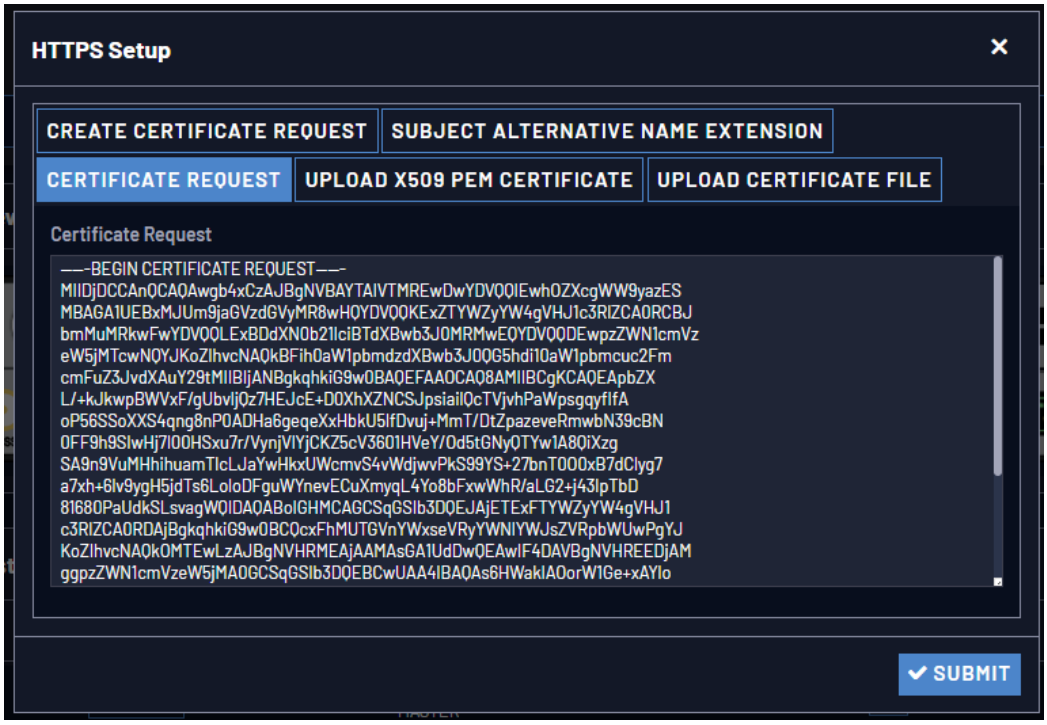
To add Subject Alternative Names to an HTTPS Certificate Request:

1. Navigate to **MANAGEMENT** > **NETWORK: HTTPS Setup** (or, navigate to **MANAGEMENT** > **NETWORK Setup**, and click **HTTPS** in the **Actions** panel.
2. In the Subject Alternative Name Extension tab, select the plus icon to access the Add Subject Alternative Name popup.
3. Fill in the available fields:
   - **Type** [DNS, IP, email, URI, RID, dirName]
   - **Name**
   - for Directory Subject Alternative Names (**dirName**), check the Directory Name box, and additional optional fields will be available:
     - Two Letter Country Code: must match ISO-3166-1 value.
     - Organization name: name of orgainzation creating certificate.
     - Organizational Unit Name: The applicable subdivision of the organization creating the certificate.
     - Common name: The name of the host being authenticated. The Common Name field in the X.509 Certificate must match the host name, IP address, or URL used to reach the host via HTTPS.
4. After completing and submitting the form, view the Subject Alternative Name tab to see existing entries. Existing Subject Alternative Names can be edited or deleted from this window.
5. After adding all the desired Subject Alternative Names, follow instructions for "Creating an HTTPS Certificate Request" on page 83.

2.8.6.6 Requesting an HTTPS Certificate

Before requesting an HTTPS Certificate from a third-party Certificate Authority, you need to create a **Certificate Request**:

1. Navigate to **MANAGEMENT > HTTPS Setup**, or to **MANAGEMENT > Network Setup > Actions** panel: **HTTPS**.
2. In the **HTTPS Setup** window, under the **Certificate Request Parameters** tab, complete the form as described under "Creating an HTTPS Certificate Request" on page 83.
3. Click Submit to generate your Certificate Request.
4. You have now created a **Certificate Request**. Navigate to the **Certificate Request** tab to view it:



5. Copy the generated Certificate Request from the **Certificate Request** window, and paste and submit it per the guidelines of your Certificate Authority. The Certificate Authority will issue a verifiable, authenticable third-party certificate.
6. OPTIONAL: While waiting for the certificate to be issued by the Certificate Authority, you may use the certificate from the Certificate Request window as a self-signed certificate (see below).

NOTE: Preventing accidental overwriting of an existing certificate:

If you plan on using a new Certificate Request, fill out a new form under the **Certificate Request Parameters** tab. Be aware, though, that the newly generated Certificate Request will replace the Certificate Request previously generated once you submit it. Therefore, if you wish to retain your previously generated Certificate Request for any reason, copy its text, and paste it into a separate text file. Save the file before generating a new request.

Using a Self-Signed Certificate

In the process of generating a Certificate Request, a self-signed certificate will automatically be generated simultaneously. It will be displayed under the **Certificate Request** tab.

You may use your self-signed certificate (or the default self-signed certificate that comes with the unit) while waiting for the HTTPS certificate from the

Certificate Authority, or – if a Certificate Authority is not available – until it expires. The typical life span of a certificate is about 10 years.

NOTE: When accessing the VersaSync Web UI while using the self-signed certificate, your Windows® web browser will ask you to confirm that you want to access this site via https with only a self-signed certificate in place. 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 certificate.

2.8.6.7 Uploading an X.509 PEM Certificate Text

Many Certificate Authorities simply issue a Certificate in the form of a plain text file. If your Certificate was provided in this manner, and the Certificate is in the X.509 PEM format, follow the procedure below to upload the Certificate text by copying and pasting it into the Web UI.

Note: Only X.509 PEM Certificates can be loaded in this manner. Certificates issued in other formats must be uploaded via the Upload Certificate tab.

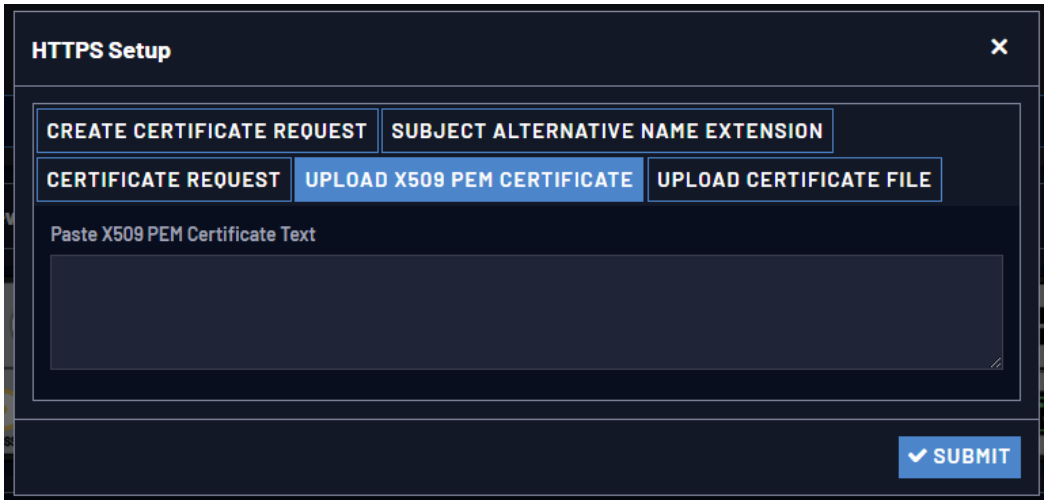
Certificate Chain

It is also possible to upload a X.509 PEM Certificate Chain by pasting the text of the second certificate behind the regular CA Certificate.

Uploading X.509 PEM certificate text

To upload an X.509 PEM Certificate text to VersaSync:

1. Navigate to **MANAGEMENT > NETWORK: HTTPS Setup**.
2. Select the **Upload X.509 PEM Certificate** tab.



3. Copy the text of the Certificate that was issued to you by your Certificate Authority, and paste it into the text field.
4. Click **Submit** to upload the Certificate to VersaSync.

NOTE: The text inside the text field under the **Edit X.509 PEM Certificate** tab is editable. However, changes should not be made to a Certificate once it is imported; instead, a new Certificate should be requested. An invalid Certificate may result in denial of access to the VersaSync through the Web UI.

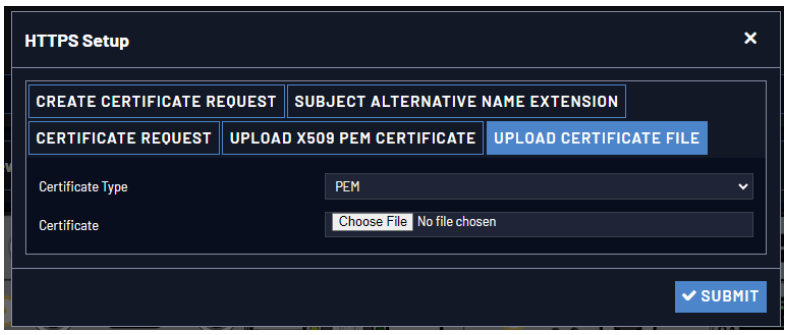
2.8.6.8 Uploading an HTTPS Certificate File

Once the HTTPS Certificate has been issued by your Certificate Authority, you have to upload the Certificate file to VersaSync, unless it is a X.509 PEM-format Certificate: In this case you may also upload the pasted Certificate text directly, see "Uploading an X.509 PEM Certificate Text" on the previous page.

Note: For more information about Certificate formats, see "Supported Certificate Formats" on page 82.

To upload an HTTPS certificate file to VersaSync:

1. Store the Public Keys File provided to you by the Certificate Authority in a location accessible from the computer on which you are running the Web UI.
2. In the Web UI, navigate to **MANAGEMENT > NETWORK: HTTPS Setup**.
3. Select the tab **Upload Certificate File**.



4. Choose the Certificate Type for the HTTPS Certificate supplied by the Certificate Authority from the **Certification Type** drop-down menu:
   - PEM
   - DER
   - PKCS #7 PEM
   - PKCS #7 DER
5. Click the **Browse...** button and locate the Public Keys File provided by the Certificate Authority in its location where you stored it in step 1.
6. Click **Submit**.

> **Note:** VersaSync will automatically format the Certificate into the X.509 PEM format.

Certificate Chain

It is possible to upload a X.509PEM Certificate Chain file. Note that there should be no character between the Certificate texts.

2.8.7 SSH

The SSH, or Secure Shell, protocol is a cryptographic network protocol, allowing secure remote login by establishing a secure channel between an SSH client and an SSH server. SSH can also be used to run CLI commands.

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

Note: Only SSH2 is supported due to vulnerabilities in the SSH1 protocol.

The SSH tools supported by VersaSync are:

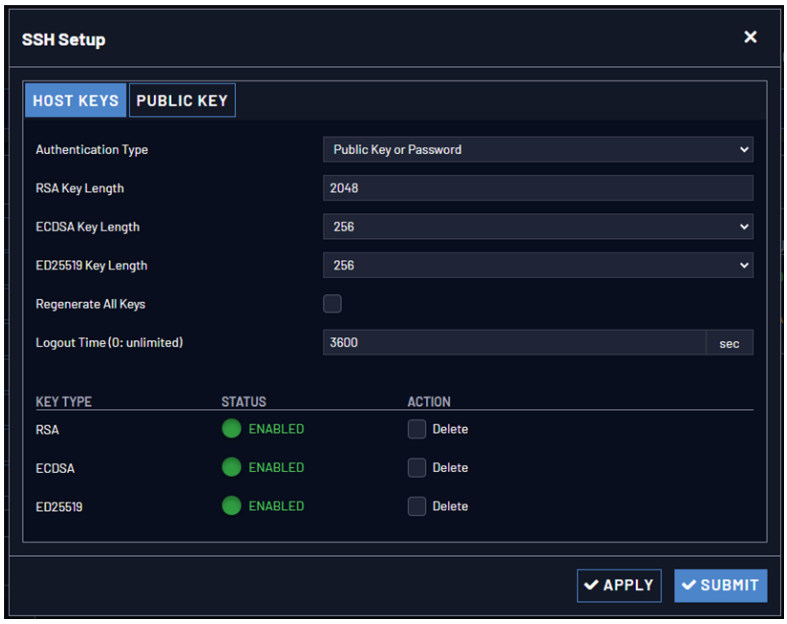
- **SSH**: Secure Shell
- **SCP**: Secure Copy
- **SFTP**: Secure File Transfer Protocol

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

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

To configure SSH:

1. Navigate to **MANAGEMENT** > **NETWORK: SSH Setup**. The **SSH Setup** window will display.



The window contains two tabs:

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

Note: Should you exit the SSH Setup window (by selecting X in the top right corner of the window, or by clicking anywhere outside of the window), while editing any configuration settings before selecting Submit, any information you entered will be lost. When switching between tabs within the SSH Setup window, however, the information you have entered will be retained.

Host Keys

You may choose to delete individual RSA or DSA host keys. Should you decide to delete the RSA or DSA key, the SSH will function, but that form of server authentication will not be available. Should you 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.

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

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

VersaSync 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 of up to 4096 are supported, but may take 10 minutes or more to generate. DSA keys size support is limited to 1024 bits.

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

The SSH client utilities SSH, SCP, and SFTP allow for several modes of user authentication. SSH allows you to remotely login or transfer files by identifying your account and the target machine's IP address. As a user you can authenticate yourself by using your account password, or by using a Public Private Key Pair.

It is advisable to keep your private key secret within your workstation or network user account, and provide the VersaSync a copy of your public key. The modes of authentication supported include:

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

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

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

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

Changing Key Length Values

You may change the key length of the RSA, DSA, ECDSA, and ED25519 type host keys.

To change the key length of a host key:

1. Navigate to **MANAGEMENT > NETWORK: SSH Setup**. The **SSH Setup** window will open to the **Host Keys** tab by default.
2. Select the **Key Length** value for the key type you want to change.

   Key sizes that are powers of 2 or divisible by 2 are recommended. The most popular sizes are 768, 1024, and 2048. Large key sizes of up to 4096 are supported, but may take 10 minutes or more to generate. DSA keys size support is limited to 1024 bits. The key type ED25519 supports 256 bits.
3. Check the **Regenerate All Keys** box.
4. Click **Submit**. The new values will be saved.

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

Deleting Host Keys

You can delete individual host keys. To delete a key:

1. Navigate to **MANAGEMENT > NETWORK: SSH Setup**. The window will open to the **Host Keys** tab by default.
2. Select **Delete** in the field for the key you wish to delete, and click **Submit**.

Creating Host Public/Private Key Pairs

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

1. To access the SSH setup screen, navigate to **MANAGEMENT > NETWORK: SSH Setup**. The window will open to the **Host Keys** tab by default.
2. Should you want to change the key length of any host key, enter the desired length in the text field corresponding to the length you wish to change.
3. Check the **Regenerate All Keys** box.
4. Click **Submit**.
   The Key Type/Status/Action table will temporarily disappear while the VersaSync regenerates the keys. The Host keys are generated in the background. Creating RSA and DSA keys, each with 1024 bits length, typically takes about 30 seconds. Keys are created in the order of RSA, DSA, ECDSA, ED25519. VersaSync will generate all 4 host keys, RSA, DSA, ECDSA, and ED25519.
5. Delete any of the keys you do not want. See "Deleting Host Keys" above.

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

> **Note:** 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 will not be created.

When you delete a host key and recreate a new one, SSH client sessions will warn you that the host key has changed for this particular IP address. You must then take one of the following actions:

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

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

Public Keys: Viewing, Editing, Loading

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

If you want 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 VersaSync. You can transfer a new public key file using the Web UI.

To view and edit the `authorized_keys` file:

1. Navigate to **MANAGEMENT > NETWORK: SSH Setup**. The **SSH Setup** window will open to the **Host Keys** tab by default.
2. Select the **Public Key** tab. The `authorized_keys` file appears in the **Public Keys File** window:

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

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

> **Note:** If you delete ALL Public Keys, Public/Private Key authentication is disabled. If you have selected SSH authentication using the Public Key with Passphrase option, login and file transfers will be forbidden. You must select a method allowing the use of account password authentication to enable login or file transfers using SCP or SFTP.

Editing the "authorized_key" File via CLI

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

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

Creating an SSH session with Password Authentication for the admin account

```
ssh spadmin@10.10.200.5
```

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

You are now presented with boot up text and/or a “>” prompt which allows the use of the Safran command line interface.

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

You must first provide the secure Safran product a RSA public key found typically in the OpenSSH id_rsa.pub file. Then you may attempt to create an SSH session.

```
ssh -i ./id_rsa spadmin@10.10.200.5
```

```
Enter passphrase for key './id_rsa': mysecretpassphrase
```

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

Secure File Transfer Using SCP and SFTP

VersaSync provides secure file transfer capabilities using the SSH client tools SCP and SFTP. Authentication is performed using either Account Passwords or Public Key with Passphrase.

Example output from OpenSSH, SCP, and SFTP client commands are shown below.

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

```
scp authorized_keys scp@10.10.200.5:.ssh
```

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

```
publickeys                                                    100%
|***********************************************| 5 00:00
```

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

```
scp -i ./id_rsa spadmin@10.10.200.5:.ssh
```

```
Enter passphrase for key './id_rsa': mysecretpassphrase
```

```
publickeys 100%
|***********************************************| 5 00:00
```

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

```
sftp spadmin@10.10.200.5
spadmin@10.10.200.135's password: admin123
```

You will be presented with the SFTP prompt allowing interactive file transfer and directory navigation.

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

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

You will be presented with the SFTP prompt allowing interactive file transfer and directory navigation.

Recommended SSH Client Tools

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

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

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

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

SSH Timeout

The keep-SSH alive timeout is configurable, in seconds, between 0 and 36000 seconds (10 hours). The default is set to 60 minutes (3600 seconds).

2.8.8 SNMP

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

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

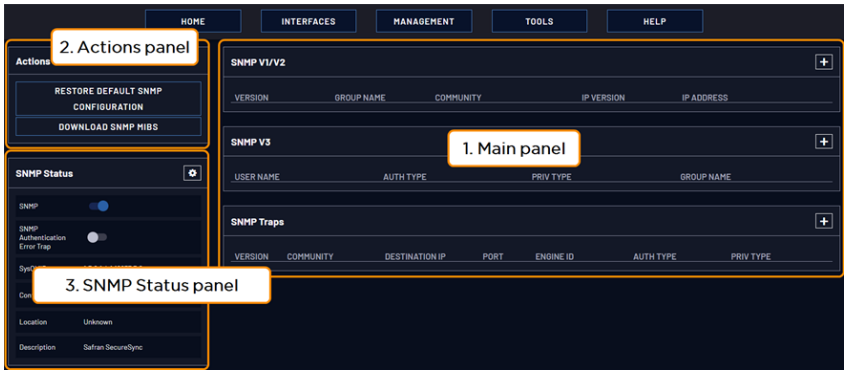
VersaSync's SNMP functionality supports SNMP versions V1, V2c and V3 (with SNMP Version 3 being a secure SNMP protocol).

Once SNMP is configured it will persist through reboot, and only needs to be reconfigured after performing a "clean" update process (thus restoring the factory default condition).

Note: In order to configure SNMP, you need ADMINISTRATOR rights.

To access the **SNMP Setup** screen:

Navigate to **MANAGEMENT > NETWORK: SNMP Setup**. The **SNMP** screen will display:



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

1. The **Main panel**, which is subdivided into 3 displays:
   - **SNMP V1/V2**: This panel allows configuration of SNMP v1 and v2c communities (used to restrict or allow access to SNMP). This tab allows the configurations for SNMP v1 and v2c, including the protocols allowed, permissions and Community names as well as the ability to permit or deny access to portions of the network. Clicking on the "+" symbol in the top-right corner opens the SNMP V1/V2c Settings for Access Screen. See "SNMP V1/V2c" on page 104.
   - **SNMP V3**: This panel allows configuration of SNMP v3 functionality, including the user name, read/write permissions, authorization passwords as well as privilege Types and

Passphrases. Clicking on the “+” symbol in the top-right corner opens the SNMP V3 Screen. See "SNMP V3" on page 105.

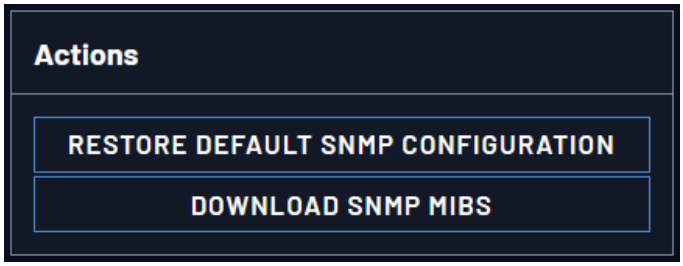
- **SNMP Traps**: This panel allows you to define different SNMP Managers that SNMP traps can be sent to over the network. This allows for SNMP Managers in different geographical areas to receive the same SNMP traps that Managers in other areas also receive. Clicking the PLUS icon in the top-right corner opens the SNMP Traps Settings Screen. See also "SNMP Traps" on page 107 and "Setting Up SNMP Notifications" on page 255.

2. The **Actions panel**, which contains the **Restore Default SNMP Configuration** button.
3. The **SNMP Status panel**, which offers:
   - An **SNMP** ON/OFF switch.
   - An **Authentication Error Trap** ON/OFF switch.
   - **SysObjID**—The System Object ID number. This is editable in the SNMP Status panel (see "Configuring the SNMP Status" on the next page).
   - **Contact Information**—The email to contact for service. This is editable in the SNMP Status panel (see "Configuring the SNMP Status" on the next page).
   - **Location**—The system location. This is editable in the SNMP Status panel (see "Configuring the SNMP Status" on the next page).
   - **Description**—A simple product description. This is not editable in the SNMP Status.

Restoring the Default SNMP Configuration

To restore the VersaSync to its default SNMP configuration:

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

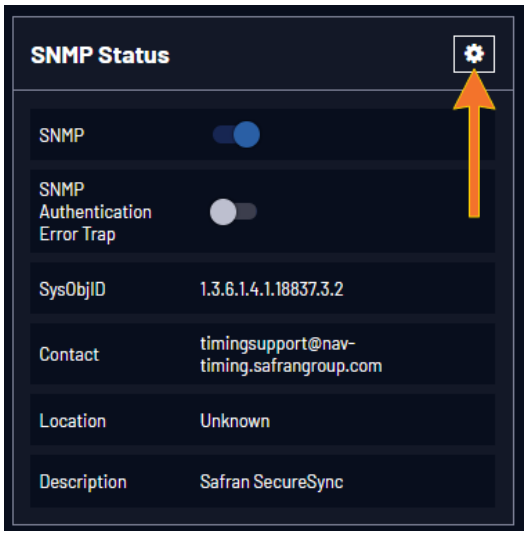


3. Confirm that you want to restore the default settings in the pop-up message.

Configuring the SNMP Status

The SNMP Status Settings are **sysObjectID**, **sysContact**, and **sysLocation**. To configure SNMP Status Settings:

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



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

The following settings can be configured in this window:

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

4. Click **Submit**, or cancel by clicking the **X**-icon in the top-right corner.

Accessing the SNMP Support MIB Files

Safran Trusted 4D (formerly Orolia/Spectracom)'s private enterprise MIB files can be downloaded via the Web UI or extracted via File Transfer Protocol (FTP) from VersaSync, using an FTP client such as FileZilla or any other shareware/freeware FTP program.

Note: Current VersaSync Time and Frequency Synchronization System software requires SFTP to ensure increased security.

To obtain the MIB files from VersaSync via the Web UI:

1. Navigate to **MANAGEMENT > NETWORK: SNMP Setup**.
2. In the Actions panel select the **Download SNMP MIBs** button.

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

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

After obtaining the MIB files, compile them onto the SNMP Manager.

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

Note: In addition to the Orolia/Spectracom MIB files, there are also some net-snmp MIB files provided. Net-snmp is the embedded SNMP agent that is used in the VersaSync 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.

Safran Trusted 4D's private enterprise MIB files can be requested and obtained from the Safran Customer Service department via email at TimingSupport@nav-timing.SafranGroup.com.

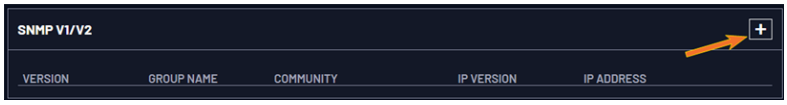
Note: By default, TimingSupport@nav-timing.safrangroup.com is the address in the sysContact field of the SNMP Status panel of the SNMP Setup page.

2.8.8.1 SNMP V1/V2c

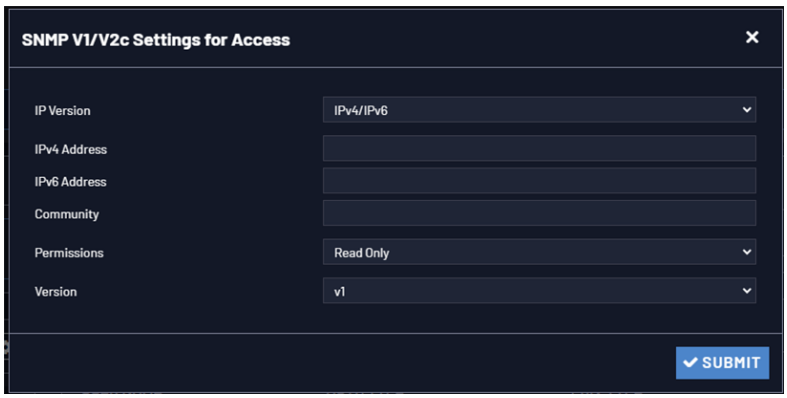
SNMP V1 is the first version of the SNMP protocol, as defined in the IETF (Internet Engineering Task Force) RFCs (Request for Comments) number 1155 and 1157. SNMP V2c is the revised protocol, but it also uses the V1 community based administration model.

Creating Communities

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



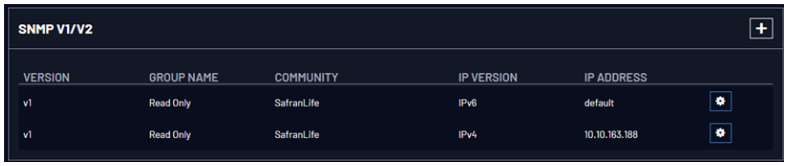
3. The **SNMP V1/V2c Settings for Access** window will display:



4. Enter the required information in the fields provided:
   - The **IP Version** field provides a choice of IPv4, IPV6 or both IPv4 and IPv6 (= default).

- The choices offered below will change in context with the choice made in the **IP Version** field.
- If no value is entered in the **IPv4** and/or **IPv6** field, VersaSync uses the system default address.
- SNMP **Community** names should be between 4 and 32 characters in length.
- **Permissions** may be Read Only or Read/Write.
- The **Version** field provides a choice of V1 or V2c.

5. Click **Submit**. The created communities will appear in the **SNMP V1/V2** panel:



Editing and Deleting Communities

To edit or delete a community you have created:

1. Navigate to **MANAGEMENT > NETWORK: SNMP Setup**.
2. Click the row of the **SNMP V1/V2** panel that displays the community you wish to edit or delete. The cursor will change from an arrow icon to a pointing finger to indicate that the entry is clickable.
3. The **SNMP V1/V2c Settings for Access** window will display.

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

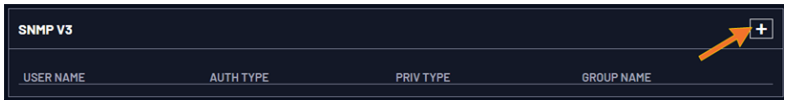
4. To edit the settings, enter the new details you want to edit and click **Submit**. OR: To delete the entry, click **Delete**.

2.8.8.2 SNMP V3

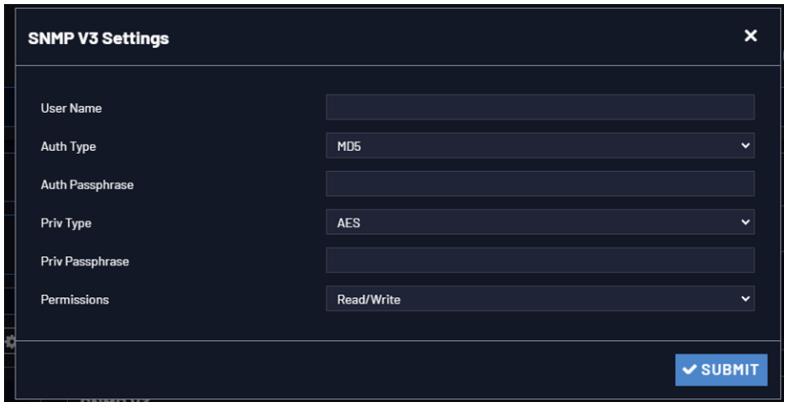
SNMP V3 utilizes a user-based security model which, among other things, offer enhanced security over SNMP V1 and V2.

Creating Users

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



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



4. Enter the required information in the fields provided.
   - SNMP **User Names** and passwords are independent of users that are configured on the **Tools/Users** page.
     - User names are arbitrary. SNMP **User Names** should be between 1 and 31 characters in length.
     - The **User Name** must be the same on VersaSync and on the management station.
   - The **Auth Type** field provides a choice between MD5 and SHA.
   - The **Auth Password** must be between 8 and 32 characters in length.
   - The **Priv Type** field provides a choice between AES, DES, and No Privacy.
   - The **Priv Passphrase** must be between 8 and 32 characters in length.
   - The **Permissions** field provides a choice between Read/Write and Read Only.
5. Click **Submit**. The created user will appear in the **SNMP V3** panel

Editing and Deleting Users

To edit or delete a user you have created:

1. Navigate to **MANAGEMENT > NETWORK: SNMP Setup**.
2. Click the row of the **SNMP V3** panel that displays the community you wish to edit or delete. The cursor will change from an arrow icon to a pointing finger to indicate that the entry is clickable.
3. The **SNMP V3 Settings** window will display.
4. Apply your changes and click **Submit**. OR: Click **Delete** to remove the User.

2.8.8.3 SNMP Traps

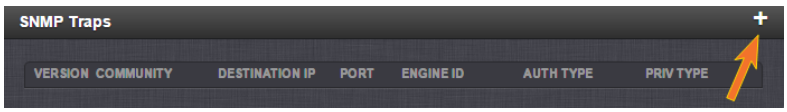
SNMP traps allow for automatic event notification, and as such are one way to remotely monitor VersaSync's status.

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

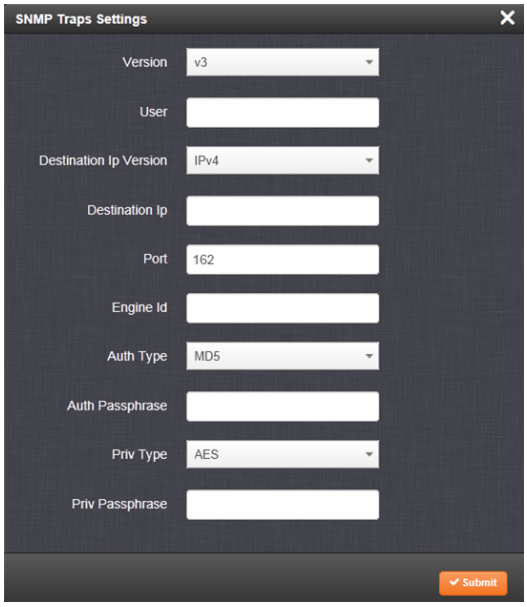
For testing purposes, a command line interface command is provided. This command, `sendtrap`, allows one, several, or all of the traps defined in the VersaSync MIB to be generated. Refer to "CLI Commands" on page 335 for command details.

To define SNMP Traps (Notifications):

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



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



4. Enter the required information in the fields provided. (Note that the options will vary contextually according to your Version.)
5.
   - The **Version** field provides a choice between v1, v2c, and v3 [= default]
   - The **Community** field for the SNMP Community string. [v1, v2c]
   - SNMP **User** names should be between 4 and 32 characters in length. [v3]
   - **Destination IP Version** is a choice between IPv4 and IPv6. [v1, v2c, v3]
   - **Destination IP** is destination address for the notification and password key to be sent. The default port is 162. [v1, v2c, v3]
   - The UDP **Port** number used by SNMP Traps [default = 162]. [v1, v2c]
   - **Engine Id** must be a hexadecimal number at least 10 digits long (such as 0x123456789A). The Id originates from the MIB Browser/SNMP Manager. [v3][1]
   - **Auth Type** provides a choice between MD5 (the default) and SHA. [v3]
   - The **Auth Password** must be between 8 and 32 characters in length. [v3]
   - The **Priv Type** field provides a choice between AES and DES. [v3]

[1]If your SNMP manager is not providing an Engine ID, you can generate one yourself according to protocols within RFC 3411 and apply it to your network manager and trap configuration.

» The **Priv Passphrase** must be between 8 and 32 characters in length. [v3]

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

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

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

Note: Safran Trusted 4D has been assigned the enterprise identifier 18837 by the IANA (Internet Assigned Numbers Authority). The product MIBs reside under the enterprise identifier @18837.3.

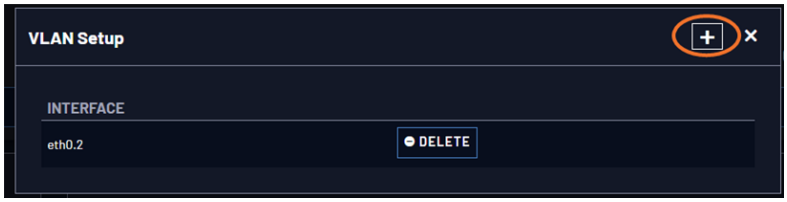
For detailed descriptions of the objects and traps supported by the VersaSync, please refer to the VersaSync MIB files. See "Accessing the SNMP Support MIB Files" on page 103.

2.8.9 VLAN Support

VLAN support in VersaSync allows you to assign a VLAN ID to a specific port to facilitate communication within your network. These VLAN interfaces have the same configuration options as the standard untagged Ethernet interfaces.

To set up VLAN interface identification tags:

1. Navigate to **MANAGEMENT** > **Network Setup**. In the **Actions** panel, select **VLAN**.
2. In the popup panel labeled **VLAN Setup**, click on the plus sign to add your VLAN interfaces. (You can also view or delete any configured VLAN tags from this panel).



3. Select the parent interface [eth0-], type in your VLAN ID, and click submit. Repeat the process as necessary.

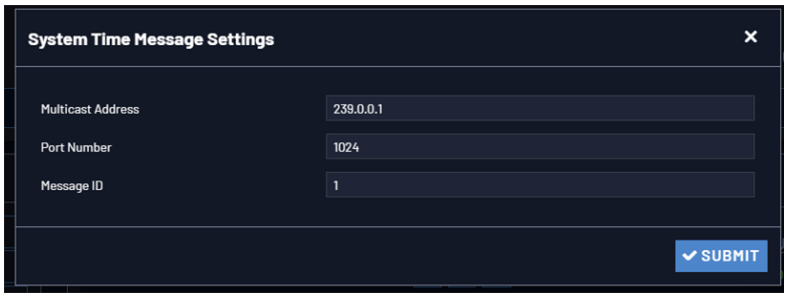
Your new VLAN interfaces will now be displayed in the VLAN Setup panel, listed as eth[#].[VLAN ID].

2.8.10 System Time Message

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

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

1. Navigate to **MANAGEMENT** > **OTHER** > **System Time Message**.
2. Populate the fields **Multicast Address**, **Port Number** and **Message ID**, and click **Submit**.
3. In the **Network Services** panel, enable **System Time Message**.



2.8.10.1 System Time Message Format

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

Table 2-7: System Time Message format

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

Table 2-8: System Time Message field descriptions

Data Name	Data Description	Range	Resolution	Units
Message ID	UID of the message; programmable	Unsigned 32 bit integer	1	n/a
Message Size	Total message size in bytes	Unsigned 32 bit integer	1	Bytes
Seconds	Seconds since epoch (00:00:00 Jan 1, 1970 UTC)	Unsigned 32 bit integer	1	Seconds
NSec	NSec within the current second	Unsigned 32 bit integer	1	nsec
EOM	End-of-message	-1	1	n/a

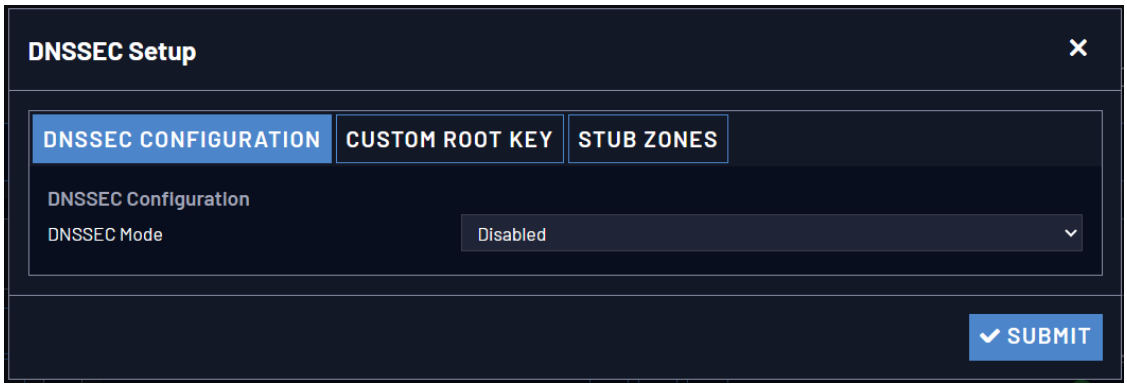
It is also possible to use the System Time Message to send NMEA over UDP. For more information about this functionality, see the NMEA over UDP App Note.

2.8.11 DNSSEC

DNSSEC (Domain Name System Security Extensions) is a set of security mechanisms that add cryptographic signatures to DNS records, ensuring data integrity and authenticity. The VersaSync DNSSEC Setup window allows for the enabling of DNSSEC and trust anchor management.

Note: In order to configure DNSSEC, you need ADMINISTRATOR rights.

To configure DNSSEC, navigate to **MANAGEMENT** > **Network Setup** and select the **DNSSEC** button in the **Actions** panel on the left:



The **DNSSEC Setup** window contains 3 tabs:

- **DNSSEC Configuration:** Allows you to set the DNSSEC mode to disabled, private (using custom root keys), or public (using IANA root key).
- **Custom Root Key:** Allows for manual trust anchor management by entering DNSSEC root keys in the text field. A list of current private keys stored on the system is also displayed, these can be removed by selecting the "REMOVE" button.
- **Stub Zones:** Allows for the configuration of stub zones by entering a zone name and DNS Server IP. A list of current configured stub zones is also displayed, these can be removed by selecting the "REMOVE" button.

Once you have configured your desired settings, select the **Submit** button to apply and initiate your changes.

Note: Only one custom root key may be entered at a time into the Custom Root Key tab text field.

Note: Should you exit the **DNSSEC Setup** window (by selecting X in the top right corner of the window, or by clicking anywhere outside of the window) while editing any configuration settings *before* selecting the **Submit** button, any information you entered will be lost. When switching between tabs within the **DNSSEC Setup** window, the information you have entered will be retained.

2.8.12 Configure NTP

Network Time Protocol (NTP) and **Simple Network Time Protocol** (SNTP) are client-server protocols that are used to synchronize time on IP networks. NTP provides greater accuracy and better error checking capabilities than SNTP does, but requires more resources.

For many applications, it is not necessary to modify the NTP factory default configuration settings. It is possible, however, to change most of the settings in order to support specific NTP applications which may require a non-standard configuration:

These features include the ability to use either MD5 authentication or NTP Autokey, to block NTP access to parts of the network and to broadcast NTP data to the network's broadcast address. NTP and SNTP are used to synchronize time on any computer equipment compatible with the Network Time Protocol. This includes Cisco routers and switches, UNIX machines, and Windows machines with suitable clients. To synchronize a single workstation, several freeware or shareware NTP clients are available on the Internet. The software running on the PC determines whether NTP or SNTP is used.

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

You can either enable or completely disable the NTP Service. When NTP is disabled, no NTP time packets will be sent out to the network. When enabled, by default, the NTP Service operates in Unicast mode, i.e. the NTP Service responds to NTP requests only.

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

2.8.12.1 Checklist NTP Configuration

The following is a list of configuration settings you may want to consider as you setup your NTP Service. (Not all items may apply to your application, or there may be other considerations not included in this list.)

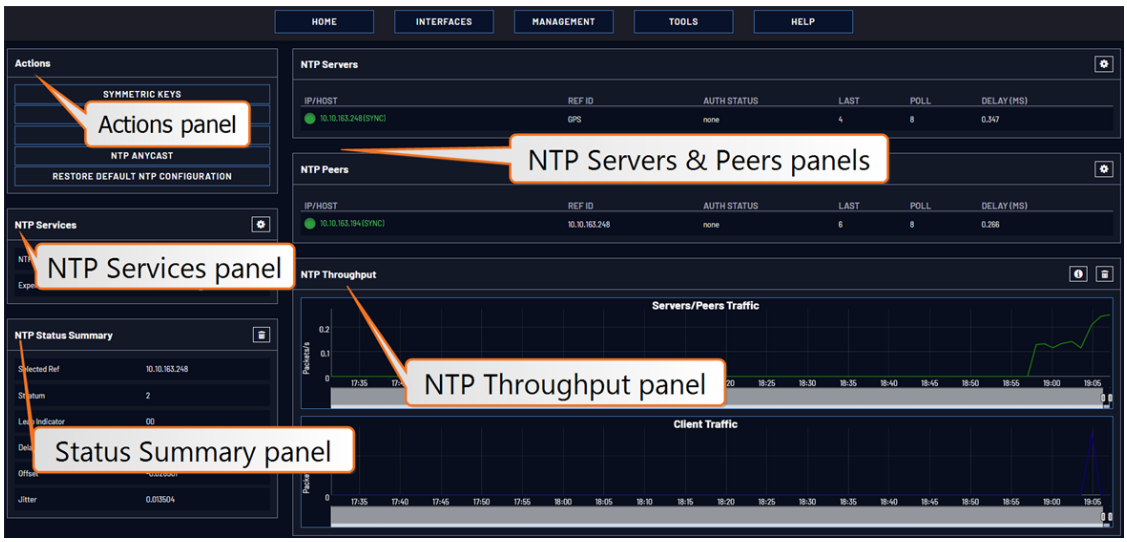
1. Did you setup your NTP Service and have it use the right **Reference(s)**?
   » See "NTP Reference Configuration" on page 120.

2. Does your NTP Service use the right **Timescale**?
   » See "NTP Output Timescale" on page 119.
3. If required, have you setup other **NTP Servers and Peers** for fallback purposes?
   » See "NTP Peers: Adding, Configuring, Removing" on page 128.

2.8.12.2 The NTP Setup Screen

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

To open the **NTP Setup** screen, navigate to **MANAGEMENT > NTP Setup**. The **NTP Setup** screen is divided into 5 panels:



The NTP Servers and Peers panels

... are located on the right-hand side of the **NTP** screen:

» **NTP Servers**: In this display you can view the NTP Servers that VersaSync detects in your network. It is through this display that you configure external NTP references. See "NTP Servers: Adding, Configuring, Removing" on page 125.

» **NTP Peers**: In this display you can view the NTP Peers that VersaSync detects in your network. It is through this display that you configure NTP Peer reference inputs. See "NTP Peers: Adding, Configuring, Removing" on page 128.

For more information on NTP servers, clients, and Stratums see "NTP Servers and Peers" on page 122.

The NTP Throughput panel

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

- The INFO icon opens a window showing the maximum per second traffic rate from each.
- The graphs maybe saved and downloaded (> ARROW icon), or deleted (> TRASH CAN icon).

The Actions panel

... is in the top left-hand corner of the **NTP** screen comprises the following buttons:

- **Symmetric Keys**: Click here to set up your symmetric keys for MD5 authentication. For more information on Symmetric Keys, see "Configuring NTP Symmetric Keys" on page 136.
- **Access Restrictions**: Click here to view, change or delete access restrictions to the NTP network. (See also "NTP Access Restrictions" on page 139.) Fields in the NTP Access Restrictions table include:
  - Type
  - IP Version
  - IP
  - IP Mask
  - Auth only
  - Enable Query
- **View NTP Clients**: Click here to reveal a table of all the clients your VersaSync is servicing. (See also "Viewing NTP Clients" on page 117.) Information for each client includes:
  - Client IP
  - Received Packets
  - Mode
  - Version
  - Restriction Flags
  - Avg Interval
  - Last Interval

» **Restore Default NTP Configuration**: Click here to restore VersaSync's NTP settings to the factory default. Any settings you have created previously will be lost. See "Restoring the Default NTP Configuration" on page 118.

The NTP Services panel

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

» **NTP ON/OFF**: This switch enables and disables NTP. See "Dis-/Enabling NTP" below.

> **Note:** When applying any changes NTP will usually restart automatically. Use this switch only to force a restart.

» **Expert Mode**: Turning this switch ON enables direct access to the **NTP.conf** file, thus bypassing the VersaSync Web UI. [Default =OFF] See "NTP Expert Mode" on page 150.

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

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

» Stratum 1 (see "NTP Reference Configuration" on page 120)

The NTP Status Summary panel

... provides a real-time overview of your key NTP network parameters. For more information, see "NTP Status Monitoring" on page 295.

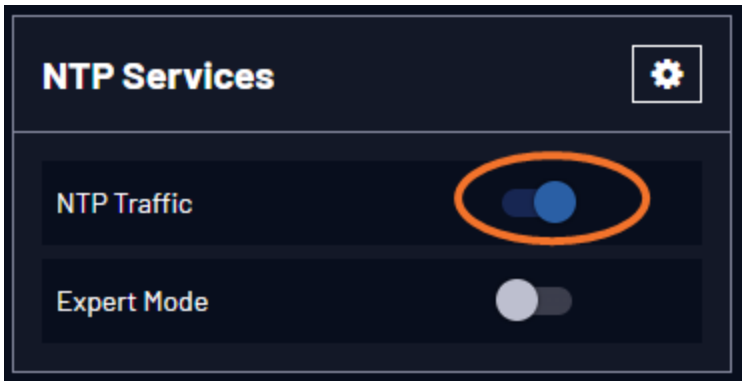
2.8.12.3 Dis-/Enabling NTP

If you applied NTP configuration changes e.g., added a new NTP Server, VersaSync usually will stop and re-start the NTP Service automatically once you clicked Submit. Changes made to NTP configurations will also take effect after VersaSync is either rebooted or power-cycled.

You can, however, also disable or enable the VersaSync NTP Service manually, e.g. with NTP Autokey.

To disable and enable your NTP Service:

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



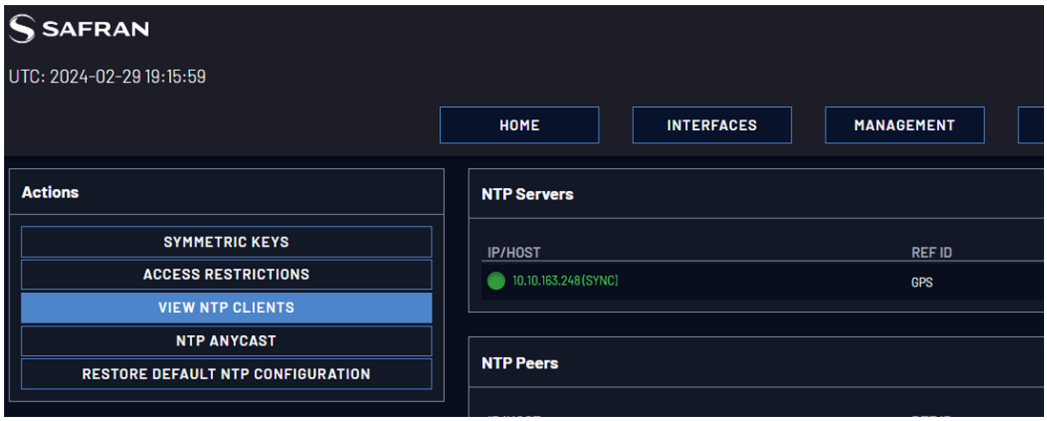
3. A notification window will confirm the status change.
4. In the **NTP Services** panel, set the ON/OFF toggle switch to ON again.

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

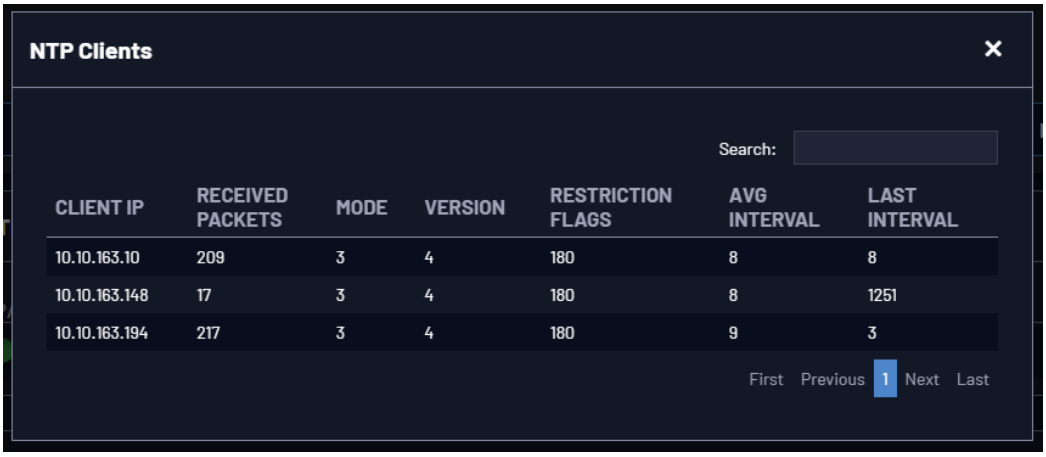
2.8.12.4 Viewing NTP Clients

To view the NTP clients being served by VersaSync:

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



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



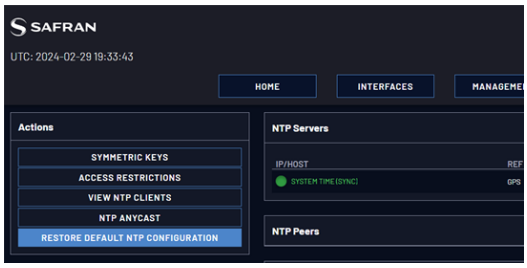
- You can search any of the fields for specific information in the Search field at the top of the window.
- A limit of 10 entries will appear on the screen at any one time. If you have more than 10 clients, you can move through the table using the **First**, **Previous**, **Next** and **Last** navigation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

2.8.12.5 Restoring the Default NTP Configuration

The VersaSync default NTP configuration can be restored at any time. It comprises basic settings such as Stratum 1 operation with no other servers or peers, no broadcasting and no access restrictions. External queries or modifications are not permitted, while generally all IPv4 and IPv6 client connections are allowed.

To restore VersaSync to its default NTP configuration:

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



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

2.8.12.6 NTP Output Timescale

You can choose the timescale VersaSync will use for the time stamps it sends out to its NTP clients and network nodes. This is done by setting VersaSync **System Time** timescale. The options are UTC, TAI and GPS. Typically, UTC is used for network synchronization.

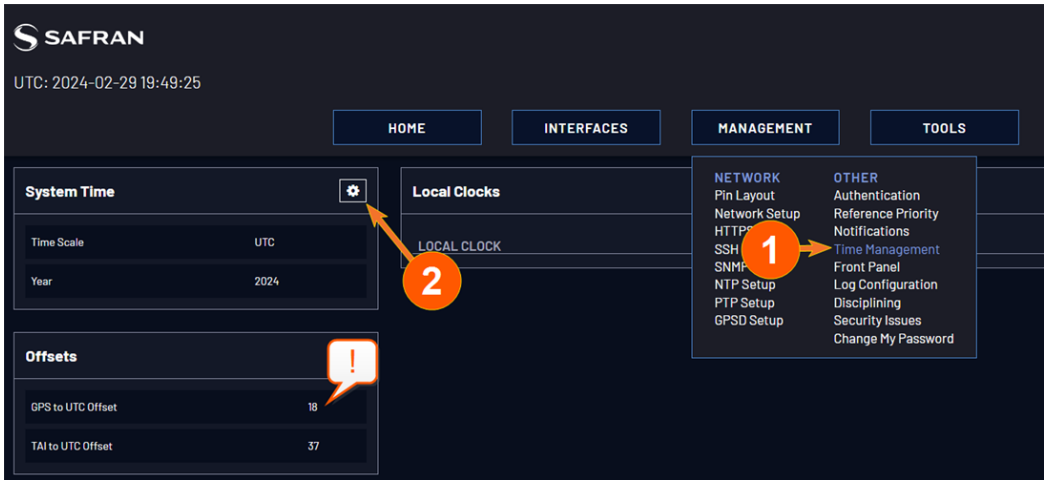
Note that the **System Time** affects not only NTP output, but also all other aspects of time management e.g., time distributed via channels other than NTP, logging, and time displayed in the Web UI.

If VersaSync is operated as a Stratum 2 server, i.e. as a client to a Stratum 1 server (see "Configuring "NTP Stratum Synchronization"" on page 121), the other server will override VersaSync's System Timescale, should it be different.

> **Note:** IMPORTANT: Make sure you select your desired timescale! Using the wrong timescale will inevitably result in an undesired time error in your NTP clients.

To change the system timescale VersaSync will use for its NTP output (and other outputs):

1. Navigate to **MANAGEMENT > OTHER: Time Management**:



2. In the **System Time** panel, click the GEAR icon.
3. In the **Edit System Time** window, select the System Timescale VersaSync will be in:
   - **UTC**: The network PCs will receive UTC time via NTP.
   - **TAI**: The network PCs will receive TAI time via NTP.
   - **GPS**: The network PCs will receive GPS time via NTP.

> **Note:** When the Timescale is set to “GPS”, the GPS to UTC Offset must be set correctly. As of 20-November-2025, the offset between UTC and GPS is 18 seconds.

2.8.12.7 NTP Reference Configuration

VersaSync's NTP Service needs to be setup such that it utilizes the time source ("input reference") you want it to use. There are two options for an NTP Server to derive its time from:

a. The NTP Service uses VersaSync's System Time, i.e. typically the GNSS reference (or IRIG, ASCII data input, etc.), and distributes that time over the NTP network. This is called **Stratum 1 Operation**, because VersaSync will be the Stratum 1 (or primary) server. This is the most common configuration.

b. It is, however, also possible for NTP to utilize the time provided by *another* NTP Server as a reference. In this case the other server would be Stratum 1, and VersaSync would be **Stratum 2** (or higher). This operating mode can be referred to as **Stratum 2 operation**, **secondary server operation**, or **NTP Stratum Synchronization**.

With a GNSS-capable time server it is possible to combine these two configurations e.g., by assigning a higher reference priority to (a.), and a lower "fallback" priority to (b.). For more information on reference priority configuration, see "Configuring Input Reference Priorities" on page 189.

The NTP Stratum Model

The NTP Stratum model is a representation of the hierarchy of time servers in an NTP network, where the **Stratum level (0-15)** indicates the device's distance to the reference clock.

Stratum 0 means a device is directly connected to e.g., a GPS antenna. **Stratum 0** devices cannot distribute time over a network directly, though, hence they must be linked to a **Stratum 1** time server that will distribute time to **Stratum 2** servers or clients, and so on. The higher the Stratum number, the more the timing accuracy and stability degrades.

The NTP protocol does not allow clients to accept time from a **Stratum 15** device, hence **Stratum 15** is the lowest NTP Stratum.

A group of NTP servers at the same Stratum level (**Stratum 2**, for example) are considered NTP Peers to each other. NTP Servers at a *higher* Stratum level, on the other hand, are referred to as NTP Servers.

Note: Internet Time Servers should be configured as NTP Servers and not as NTP Peers.

If VersaSync has no valid Timing System Reference, NTP Server or NTP Peers, the NTP Stratum value is automatically downgraded to **Stratum 15**. This ensures that its NTP clients will no longer use this VersaSync unit as a time reference.

Configuring "NTP Stratum 1" Operation

When the Timing System references of your VersaSync are normally available (rather than being unavailable most of the time e.g., in areas with poor GNSS reception), it is advisable to use the System Time as a reference to NTP, since this provides NTP with the most accurate references. This mode is called **Stratum 1** operation, since VersaSync operates as a **Stratum 1** NTP server.

To configure **Stratum 1** operation for VersaSync:

1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**:
2. Click the GEAR icon in the **NTP Services** panel.
3. The **Edit NTP Services** window will display. Click the **Stratum 1** tab.
4. Check all of the three options:
   - **Enable Stratum 1 Operation**
     Checking this option will cause the NTP Service to use the System Time provided by the Timing System input.
   - **Prefer Stratum 1**
     This option configures NTP to "weigh" 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 desirable NOT to prefer the Timing System over an NTP reference, in which case this box should not be checked.
5. Click the **Submit** button.

Configuring "NTP Stratum Synchronization"

NTP Stratum Synchronization refers to the concept of using a different NTP Server or Peer as your primary reference (instead of e.g., GNSS). This will make the VersaSync you are configuring a **Stratum 2** server, since the other server is Stratum 1.

To configure **Stratum 2** (or greater) operation for VersaSync:

1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**:
2. Click the GEAR icon in the **NTP Services** panel.
3. The **Edit NTP Services** window will display. Click the **Stratum 1** tab.
4. Uncheck all three options:
   - **Enable Stratum 1 Operation**
     Uncheck this option. When the checkbox **Enable Stratum 1** is unchecked, the system will always synchronize its .time to an NTP server.
   - **Prefer Stratum 1**
     Uncheck this option to prevent VersaSync's NTP service from "weighing" the Timing System input heavier than input from other NTP servers. Thus, during normal operation, the time provided by the external Stratum 1 NTP server will be used (unless its quality is determined to be low).

     Note: If enabled, this function would give GPS additional "weight" for NTP to select the GNSS input over other NTP Servers.
5. Click the **Submit** button.

2.8.12.8 NTP Servers and Peers

VersaSync can be configured to receive time from one or more available NTP Servers (VersaSyncs or different models). This allows for NTP Servers on a timing network to be configured as potential (fallback) input time references for VersaSync System Time synchronization. In the event that a current reference becomes unavailable, VersaSync can fallback to the other NTP Servers available on the network.

A group of NTP servers at the same Stratum level (Stratum 1 time servers, for example) are considered as NTP Peers to each other.

NTP Servers at a higher Stratum level, on the other hand, are called NTP Servers (Note that Internet Time Servers should be configured as NTP Servers and not as NTP Peers).

Note: IMPORTANT: In order for other NTP servers to be a valid reference, you must enable “NTP” in the Reference Priority table (see "Configuring Input Reference Priorities" on page 189).

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

NTP Servers at the same Stratum level

If VersaSync is configured to obtain time from other NTP Servers at the same Stratum level (i.e., NTP Peers) but is currently using a different input reference as its selected reference, VersaSync will report to the network (via the NTP time stamps) that it is a **Stratum 1** time server. Should, however, all input references except the other NTP server(s) become unavailable, VersaSync 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.

NTP Servers at a higher Stratum level

If VersaSync is configured to obtain time from another NTP Server at a higher Stratum level (i.e., NTP Servers), and it is using that NTP Server as its selected reference, VersaSync will report to the network (via the NTP time stamps) that it is one less Stratum than its selected reference NTP Server.

EXAMPLE:

If VersaSync is configured to receive time from one or more Stratum 1 NTP Servers, with no other higher priority input references available, VersaSync will report to the network that it is a Stratum 2 Server.

In order for VersaSync to use other NTP servers as a valid time reference to synchronize the System Time, the input Reference Priority Setup table must be configured to allow NTP as an available reference. For more information on the input Reference Priority table, refer to "Configuring Input Reference Priorities" on page 189.

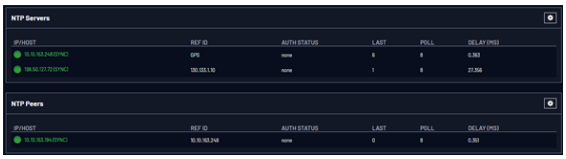
Holdover

If VersaSync is synchronized to another NTP Server or reference, and that server or reference subsequently loses sync or becomes unavailable (with no other higher priority input references being present and valid), VersaSync will then go into the Holdover mode. It will remain in Holdover mode until any enabled and valid input reference becomes available again, or until the Holdover period expires, whichever occurs first.

During Holdover mode, NTP will remain at the same Stratum level it was before entering the Holdover mode and can continue to be the reference to the network. However, if no input reference becomes available before the Holdover period expires, Time Sync will be lost and shortly thereafter, NTP will report to the network that it is now at Stratum 15. A status of Stratum 15 will cause the network to ignore VersaSync as an NTP time reference.

For more information about Holdover, see "Holdover Mode" on page 235.

The NTP Servers and NTP Peers Panels



The **NTP Servers** and **NTP Peers** panels display which servers in the network are set up at higher or equal Stratums (Servers or Peers, respectively), and their configurations. These panels are also used to add, configure, or remove NTP Servers and Peers.

Note: For information on how to view NTP Clients, see "Viewing NTP Clients" on page 117.

The **NTP Servers** and **NTP Peers** panels are part of the **NTP Setup** screen (see "The NTP Setup Screen" on page 114), which can be accessed via **MANAGEMENT > NETWORK: NTP Setup**.

Information provided in the NTP Servers and NTP Peers panels

The following columns are used to break down the status information for recognized **NTP Servers** and **NTP Peers**.

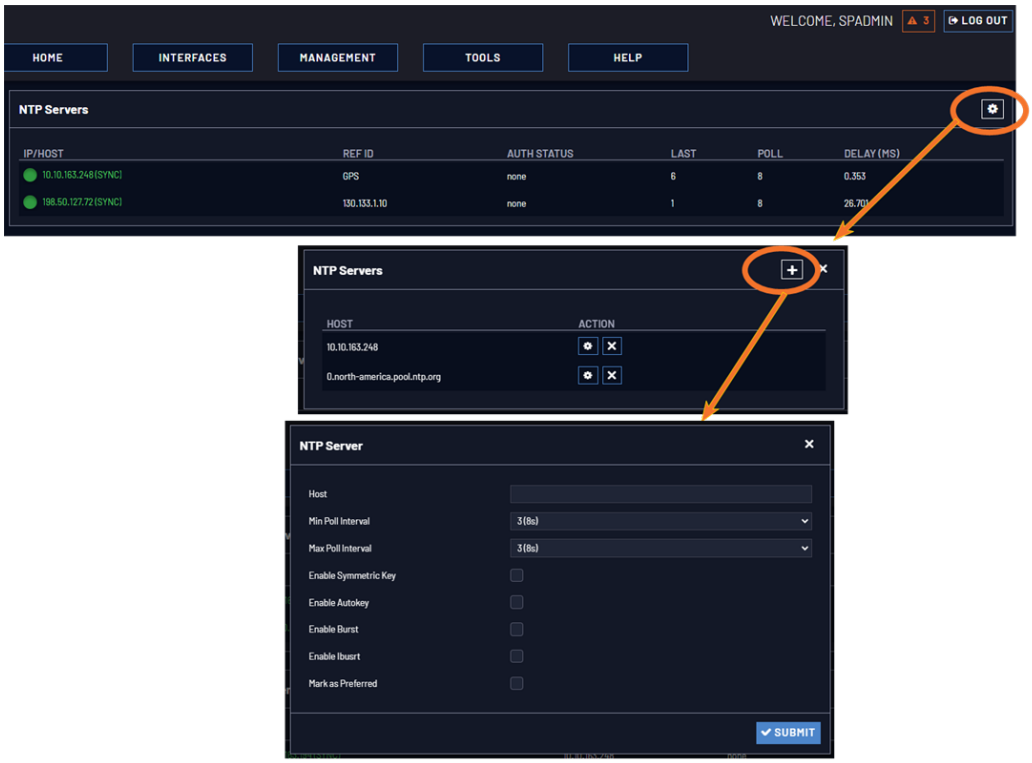
Note: Servers will be displayed in the Status view only if they can be resolved. They will, however, always be displayed in the Setup view in order to reconfigure them, if necessary.

- **IP/HOST**: Name and real-time status (color-coded)
- **REF ID**: Identifies the type of Input REFerence e.g., **GPS** indicates the reference can use GPS for its synchronization. Below is a list of potential REF IDs reported by the VersaSync Timing System (other NTP Servers and Peers may report different references):
  - **GPS**: GNSS reference
  - **IRIG**: IRIG reference
  - **HVQ**: HAVE QUICK reference
  - **FREQ**: Frequency reference
  - **PPS**: External 1PPS reference
  - **PTP**: PTP reference
  - **ATC**: ASCII time code reference
  - **USER**: User provided time
  - **LOCL**: Local reference (synced to itself)
  - **INIT**: NTP on server/peer is initializing
  - **STEP**: NTP on server/peer is performing initial synchronization step and restarting
- **AUTH STATUS**: Indicates if the selected reference is using MD5 authentication. “None” indicates authentication not being used.
- **LAST**: The number of seconds that have expired since this reference was last polled for its time.
- **POLL**: The polling interval, i.e. how often VersaSync is polling this NTP reference for its time.
- **DELAY (ms)**: The measured one-way delay between VersaSync and its selected reference.

NTP Servers: Adding, Configuring, Removing

To add, configure, or remove an NTP Server:

1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**.



2. The **NTP Setup** screen appears. The **NTP Servers** panel displays a list of recognized NTP servers. Click the GEAR icon in the upper right-hand corner of the **NTP Servers** panel.
3. The **NTP Servers** window opens. Should the list be empty, no servers have been added yet. In the event that added servers are not displayed in the NTP Setup screen/NTP Servers panel, they could not be resolved. Verify the IP address. Note that System servers cannot be edited or deleted.

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

   > **Note:** In order for other NTP Servers to be a valid reference, "NTP" must be enabled as both the Time and 1PPS references in the Reference Priority table. See "Configuring Input Reference Priorities" on page 189.

   » To EDIT an existing server, click the corresponding ACTION GEAR button, and proceed to the next step.

- To REMOVE a server (and its associated configurations), click the X-button next to it, then confirm by clicking OK.

4. The **NTP Server** Edit window displays. Enter the required information:
   - **Host**: The IP address for the server to be used as host.
   - **Min Poll Interval**: Select a value from the drop down (the default is 3 (8s)).
   - **Max Poll Interval**: Select a value from the drop down (the default is 3 (8s)). 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 VersaSync 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.
   - **Enable Symmetric Key**: Click to enable Symmetric Key, and then select an option from the drop down menu that displays.
   - 

     Note: Before you can choose an option in the Key field, you must first set up symmetric keys through the Actions panel. See "Configuring NTP Symmetric Keys" on page 136. Conversely, you may check the Autokey box below the Key field.
   - **Enable Autokey**: Click here if you want to use Autokey with this server. See "NTP Autokey" on page 130.
   - 

     Note: When you configure NTP Autokey, you must first disable the NTP service in the NTP Services panel, and then re-enable it after the Autokey configuration is completed.
   - **Enable Burst**: This tells NTP to send a burst to the remote server when the server is reachable.
   - **Enable Iburst**: The iburst function tells NTP to send a burst of queries instead of one when the remote server is not reachable for faster clock synchronization. This will occur if the connection was inter-

rupted, or upon restart of the NTP daemon. For additional information, please refer to public NTP configuration documentation.

» **Mark as Preferred**: Click here to make this server the preferred server. For more information, see "Configuring "NTP Stratum 1" Operation" on page 121.

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

5. Click Submit, or press Enter.

NTP Peers: Adding, Configuring, Removing

To add, configure, or remove an NTP Peer:

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

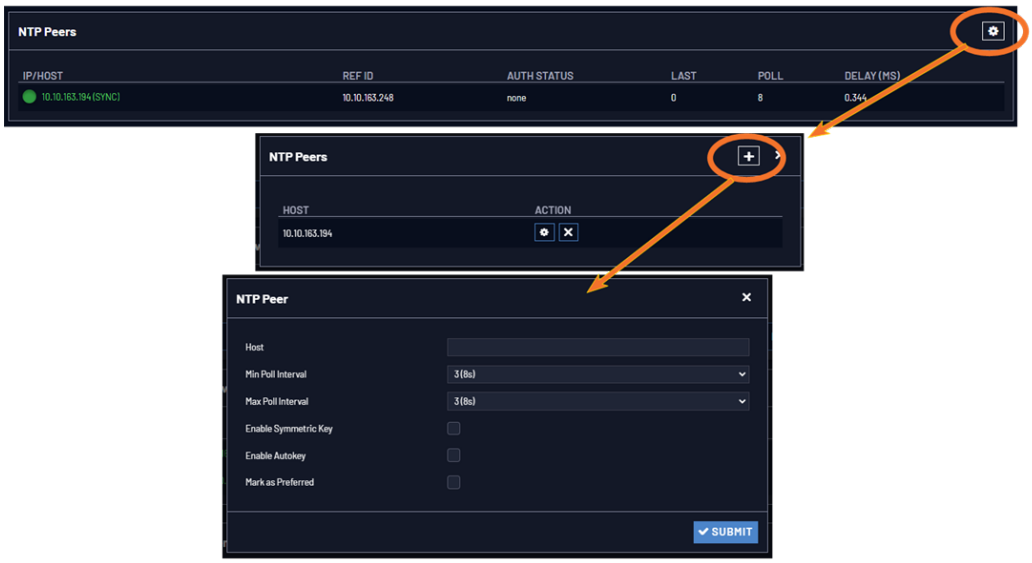
> **Note:** Should the list be empty, no servers have been added yet. In the event that added peers are not displayed, they could not be resolved. Verify the IP address

» To EDIT the settings of an NTP Peer, click the GEAR button next to it, and proceed to Step 3 below.

» To ADD a new NTP Peer, click the PLUS icon in the top right corner of the **NTP Peers** panel.

» To REMOVE an NTP Peer (and its associated configurations), click the X-button next to it.

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



4. Enter the required information into the fields:
   - **Host**: The IP address for the server to be used as host.
   - **Min Poll Interval**: Select a value from the drop down (the default is 3 (8s).
   - **Max Poll Interval**: Select a value from the drop down (the default is 3 (8s).
     For both NTP Peers, and NTP Servers the Minimum and Maximum Poll rate for NTP packets can be configured.
   - **Enable Symmetric Key**: Click the checkbox to enable/disable Symmetric Key. See also: "Configuring NTP Symmetric Keys" on page 136.

     Note: Before you can edit the Key field, you must set up Symmetric Keys through the Actions Panel. See "NTP: Symmetric Keys (MD5) " on page 136. Conversely, you may check the Autokey box below the Key field.

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

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

» **Mark as Preferred**: Check this box to prefer this NTP Peer over other NTP Peers ("NTP Peer Preference"). This will result in VersaSync synchronizing more frequently with this Peer. For additional information on NTP Preferences, see "Configuring "NTP Stratum 1" Operation" on page 121.

> **Note:** Please note that it is not advisable to mark more than one NTP Peer as Preferred, even though VersaSync will not prevent you from doing so.

5. Click Submit, or press Enter.

2.8.12.9 NTP Authentication

Since NTP information is distributed across entire networks, NTP poses a security risk: Falsified NTP time stamps or other NTP-related information can be exploited by an attacker. NTP authentication keys are used to authenticate time synchronization, thus detecting a fake time source before it can do harm.

NTP Autokey

The NTP version installed on VersaSync 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.

NTP Autokey: Support & Limitations

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

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

NTP Autokey: IFF Autokey Support

The IFF Autokey Support is demonstrated in the figure below. The IFF identity scheme is used with Multiple Stratum NTP Time Servers. The example below shows 3 Stratum layers. Stratum 1 NTP Servers are close to the physical time references. All Stratum 1 servers can be Trusted Hosts. One of them is the trusted route 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. Stratum 2 NTP servers are also members of the Group. All NTP Stratum 1 servers are Trusted Hosts. The NTP servers closest to the actual time reference (Stratum 1) should be designated trusted. A single Stratum 1 NTP server generates the IFF Group/Client Keys. There is NO group name feature supported. The Group can use the same passphrase (password) or different passphrases for each client.

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

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

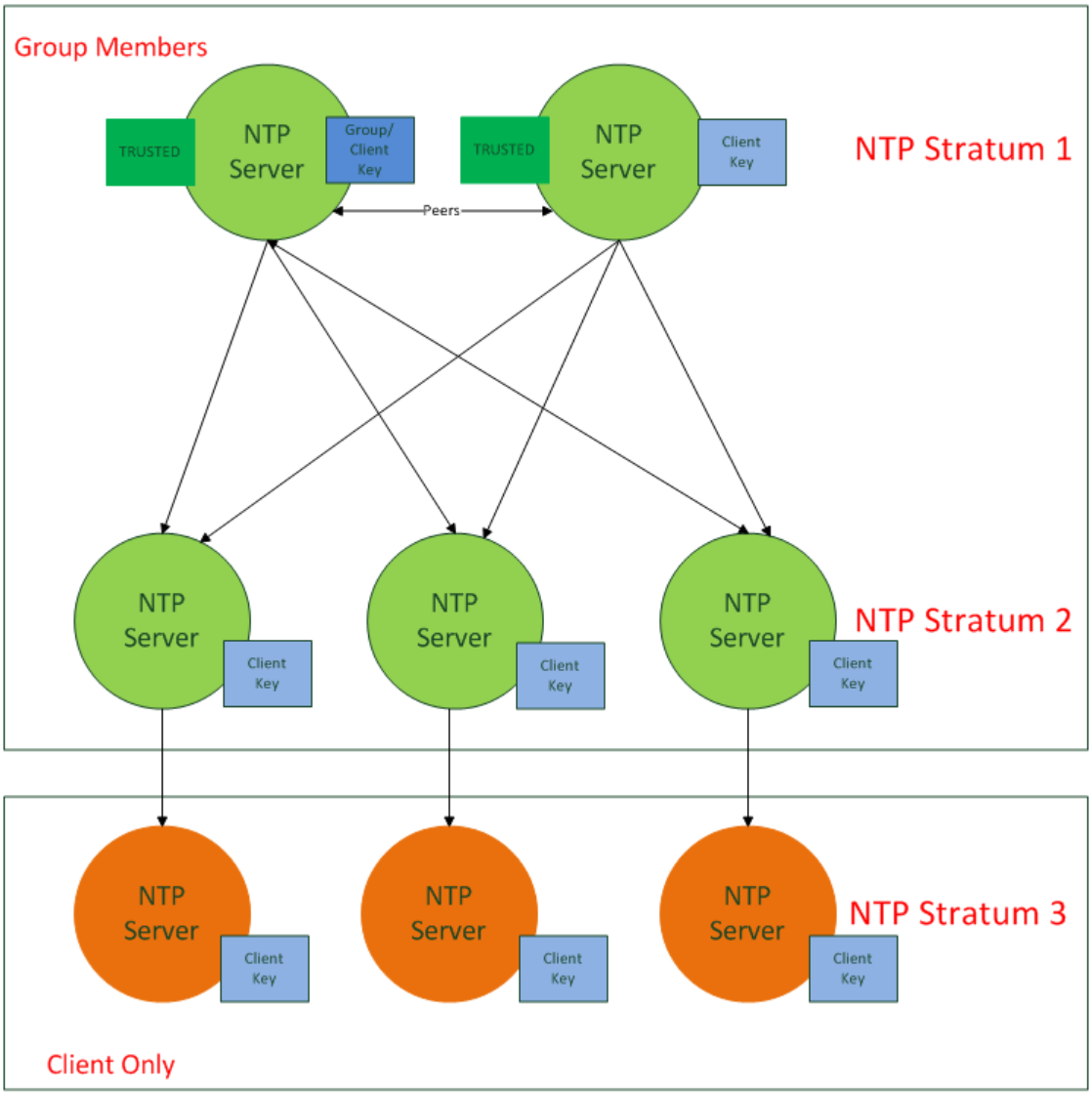


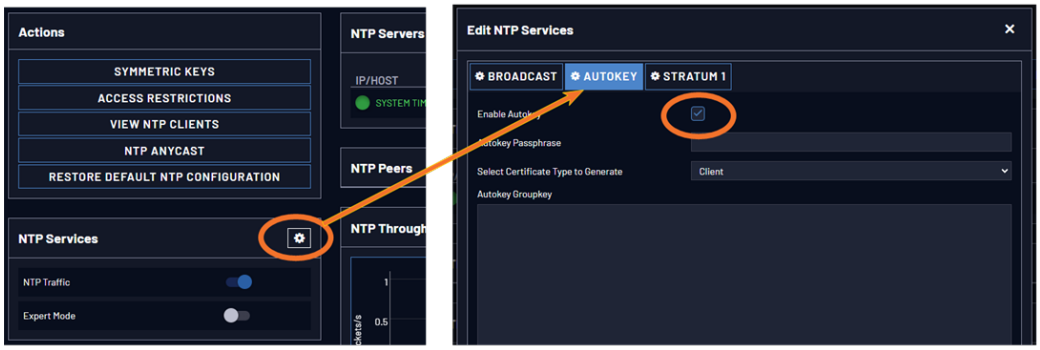
Figure 2-6: IFF Autokey configuration example

Configuring NTP Autokey

Note: When you configure NTP Autokey, you must disable the NTP Service first, and then re-enable it after Autokey configuration is completed. See "Dis-/Enabling NTP" on page 116.

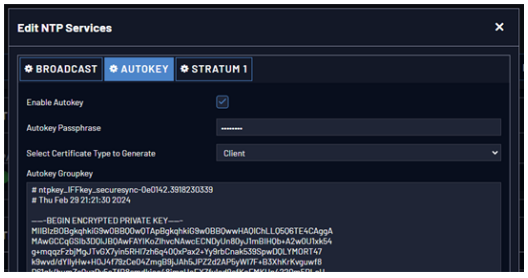
To configure NTP Autokey:

1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**.



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

> **TRUSTED Server:**
>
> Before a server can be designated Client or Server status, one server must be designated as Trusted. When designating a server as Trusted:
>
> 1. Choose the Trusted radio button.
>
> 2. Click the Submit button.
>
> A Groupkey is then generated for the network. This Groupkey will be pasted into the Groupkey box to designate another server on the network as Client or Server.



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

Configuring a Stratum-1 Server as Trusted Host

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

1. Define the Hostname of all NTP servers before proceeding. See "NTP Servers: Adding, Configuring, Removing" on page 125.
2. Disable NTP.
   - » Ensure the time is accurate to a few seconds. Use NTP or manually set the clocks to set the system time.
3. Verify this VersaSync is, in fact, NTP Stratum 1, and its Time, and 1PPS synchronization to GNSS are valid.
4. Under the **Autokey** tab of the **Edit NTP Services** window:
   - » **Enable Autokey**—Check the box.
   - » **Autokey Passphrase**—Enter your Group members NTP Autokey password.
   - » **Select Certificate Type to Generate**—Do NOT enable **Client**.
   - » Select **Trusted**.
   - » Click **Submit**.
5. Observe the **IFF Group/Client Key** appearing.
   - » This is the common **IFF Group/Client Key**. This key is shared between all Group members using this NTP Servers passphrase for ALL group members.
6. Configure NTP as requiring authentication.
7. Enable NTP in the **NTP Services** panel.
8. Verify that NTP reaches occur, and that NTP eventually reaches Stratum 1.

Creating a Stratum-1 Group Member Server

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

1. Define the **Hostname**, making sure it is unique, i.e. not the same as the trusted root server. See also "General Network Settings" on page 74.
2. Disable NTP if enabled.

3. Manually set the time or use NTP to set the system time.
4. Under the **Autokey** tab of the **Edit NTP Services** window, enable:
   - **Enable Autokey**—Check the box.
   - **Autokey Passphrase**—Enter your Group members NTP Autokey password.
   - **Select Certificate Type to Generate**—Do NOT enable Server
5. Using the NTP Server containing the IFF Group/Common Key generate a Client Key using this NTP Server's passphrase.
6. Cut and paste the Client Key into the **Autokey Groupkey** text box.
7. For all NTP Stratum-2 servers and higher stratum numbers, disable the following items under the **Stratum-1** tab in the **Edit NTP Services** window:
   - Prefer Stratum 1.
   - Enable Stratum-1 1PPS.
8. In the **NTP Servers** panel of the main window, add an NTP server and enable the **Autokey** option box. See "NTP Servers: Adding, Configuring, Removing" on page 125.
9. Enable NTP in the **NTP Services** panel.
10. Wait for NTP to synchronize to the NTP References provided.

Creating a Stratum-1 Client Only Server

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

1. Define the Hostname, making sure that it is different from its trusted group server. See "NTP Servers: Adding, Configuring, Removing" on page 125.
2. Disable NTP if enabled.
3. Manually set the time or use NTP to set the system time.
4. Under the Autokey tab of the **Edit NTP Services** window, enable:
   - **Enable Autokey**—Check the box.
   - **Autokey Passphrase**—Enter your Group members NTP Autokey password.
   - **Select Certificate Type to Generate**—Select **Client** to enable Client only.
5. Using the NTP Server containing the IFF Group/Client Key, copy the Group/Client key.
6. Paste this Group/Client key into the **Autokey Groupkey** text box.

7. For all NTP Stratum-2 servers and higher stratum numbers, under the **Stratum-1** tab in the **Edit NTP Services** window configure the NTP Stratum-1 references:
   - » Disable Enable Stratum 1 Operation.
   - » Disable Enable Stratum 1 1PPS.
8. In the **NTP Servers** panel of the main window, add an NTP server and enable the **Autokey** option box. See "NTP Servers: Adding, Configuring, Removing" on page 125.
9. Wait for NTP to synchronize to the NTP References provided.

NTP: Symmetric Keys (MD5)

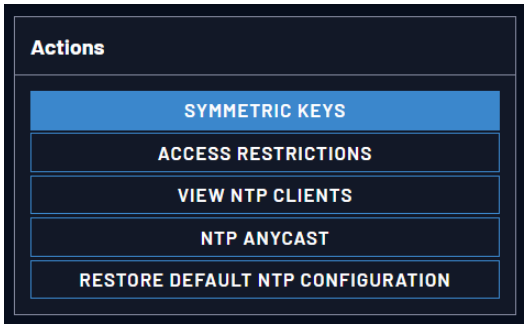
Symmetric Keys are an encryption means that can be used with NTP for authentication purposes.

VersaSync 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 Symmetric Keys tab allows NTP to be configured to use MD5 authentication.

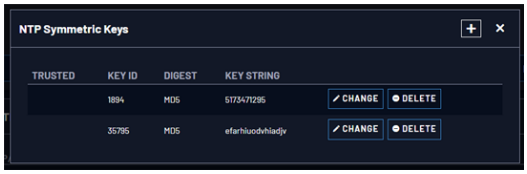
Configuring NTP Symmetric Keys

To create, edit, or delete Symmetric Keys (MD5 Authentication):

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



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



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

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

Fill in, or edit the fields:

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

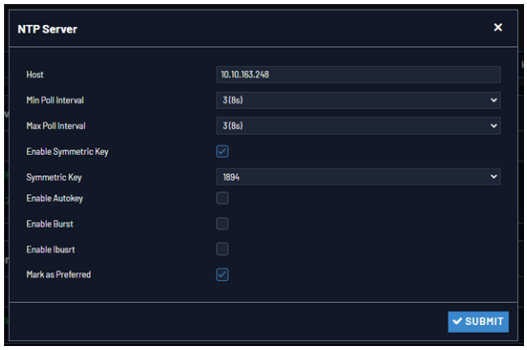
> **Note:** To use the MD5 authentication with trusted key ID, both the NTP client and the VersaSync must contain the same key ID/key string pair, the client must be set to use one of these MD5 pairs, and the key must be trusted.

- **Key ID**—The key ID must be a number between 1 and 65532.
- **Digest Scheme**—Choose one of the options from the drop-down list. The available options are:
  - MD5 (the default)
  - SHA1
  - SHA
  - SHA256
  - SHA512
  - SHA3-256
  - AES128CMAC
  - MDC2

- RIPEMD160
- MD4

- **Key Str**—The key string restrictions for different Digest schemes are as follows:
  - For MD5 type keys, you can enter in a plain text ASCII key of 20 characters or less OR a hex key of 40 characters or less.
  - For all other key types, you must enter a hex key of 40 characters or less.

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



NOTES:

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

You may define the trusted Symmetric Keys that must be entered on both VersaSync, and any network client with which VersaSync is to communicate. Only

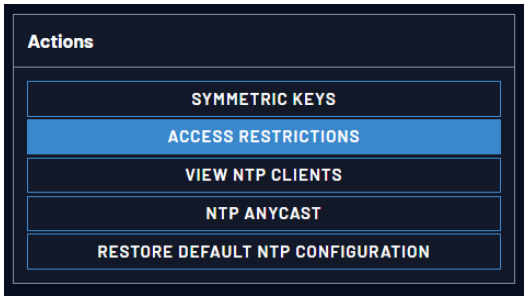
those keys for which the "Trusted" box has been checked will appear in the drop-down menus on the **NTP References** screen.

2.8.12.10 NTP Access Restrictions

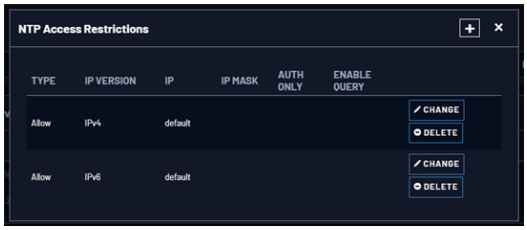
Next to encrypted authentication by means of Symmetric Keys, NTP supports a list-based means of access restriction, the use of which is also recommended to prevent fraudulent or inadvertent manipulation of a time server.

To configure NTP Access Restrictions:

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

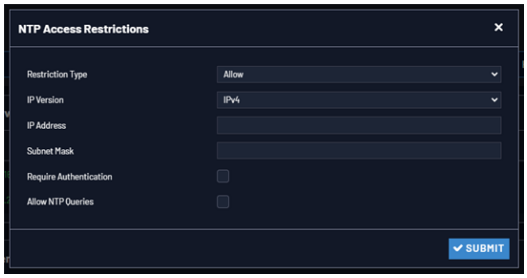


3. The **NTP Access Restrictions** Status window will display:



   - To ADD or EDIT an access restriction, click the PLUS icon or the Change button, respectively, and proceed to Step 4. below.
   - To DELETE an access restriction, click the corresponding Delete button, and confirm by clicking OK.

4. The **NTP Access Restrictions** window will display:



- Fill in the fields:
  - **Restriction Type**—Choose either Allow or Deny.
    If you select “Deny”, the configured portion of the network will not have NTP access to VersaSync, but the rest of the network will have access to VersaSync. If you select “allow”, the configured portion of the network will have NTP access to VersaSync, but the rest of the network will not have access to VersaSync. By default, VersaSync allows all IPv4 and IPv6 connections.
  - **IP Version**—Choose IPv4 or IPv6
  - **IP Address**—Enter the appropriate hostname.
  - **Subnet Mask**—Enter the appropriate IP mask.
  - **Require Authentication** (checkbox)—Check this box if you want the additional security of authorized access. VersaSync to accept only authenticated requests (MD5 or Autokey) from this user or network segment.
  - **Allow NTP Queries** (checkbox)—Check this box if you want to allow external NTP queries into VersaSync services.

5. Click the **Submit** button.

2.8.12.11 NTP over Anycast

NTP (Network Time Protocol) is a packet network based synchronization protocol for synchronizing a client clock to a network master clock (see also "Configure NTP" on page 113.)

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

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

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

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

To learn more about NTP over Anycast, see also the respective Safran Tech Note.

Please note that VersaSync utilizes the OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol).

OSPF Protocol EXAMPLE:

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

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

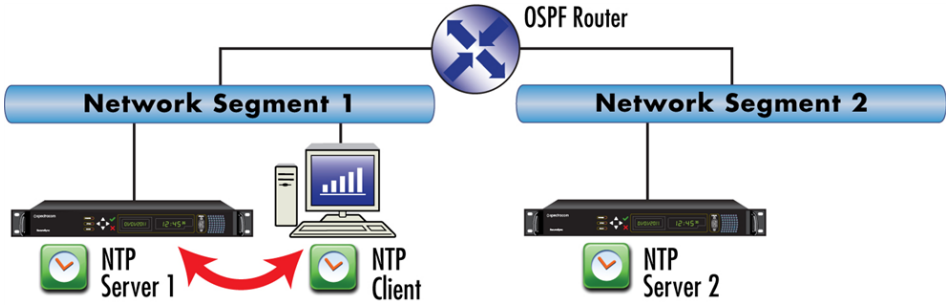


Figure 2-7: All NTP Servers are synchronized

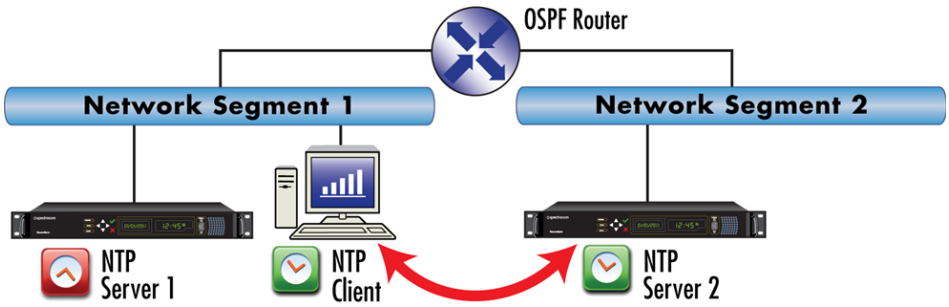


Figure 2-8: NTP Server 1 is out of sync

Configuring NTP over Anycast (General Settings)

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

1. Confirm that your existing network infrastructure is Anycast capable. Determine network specifics, such as the Anycast address and port.
2. In the VersaSync Web UI, navigate to **MANAGEMENT** > **Network** > **NTP Setup**.
3. In the **Actions Panel**, click **NTP over Anycast**.
4. In the **NTP Anycast** window, select the **General** tab.

5. On the **General** tab, select the **IP Version** you will be running Anycast service for. The options are IPv4, IPv6, or both.
6. Configure the **Anycast Address** to be used.
7. Select the port to associate the Anycast service with (depending on the option card configuration of your unit, there may be only ETH0 available). If you desire IPv6 functionality, you must also select the IPv6 port address since there may be multiple IPv6 addresses on a single port.
8. If you would like to enable the option to divert NTP Anycast traffic through the Anycast port, select the Divert Anycast Traffic Out Anycast Port check box.
9. Click **Submit**.

Note: NTP over Anycast is not compatible with DHCP, as it is designed to be used with static addresses only.

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

Note: Interfaces intended for Anycast use should be connected and fully configured for IPv4 or IPv6 communication.

Note: When NTP Anycast is configured, the Anycast interface configured from the General tab will be momentarily reloaded to apply configuration.

Configuring NTP over Anycast (OSPF IPv4)

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

1. Confirm that your existing network infrastructure is Anycast capable, and uses OSPF Version 2 (IPv4). Determine the OSPF area.
2. In the VersaSync Web UI, navigate to **MANAGEMENT** > **Network** > **NTP Setup**.
3. In the **Actions Panel**, click **NTP over Anycast**.
4. In the **NTP Anycast** window, select the **General** tab.

5. On the **General** tab, select **IPv4** as the IP Version.
6. Configure the **Anycast Address** to be used.
7. Select the port to associate the Anycast service with (depending on the option card configuration of your unit, there may be only ETH0 available).
8. In the **NTP Anycast** window, navigate to the **OSPF** tab.
9. On the **OSPF** tab, check **Enable**.
10. Setup the OSPF area.
11. Click **Submit**.
12. Select the port address to associate the **Anycast** service with (because there may be multiple addresses on a single port), and click **Submit**. If no addresses appear, an IP address must be added to the port (see "Network Ports" on page 75).
13. Next, specify the maximum TFOM Setting (Time Figure of Merit), and the Holdover Timeout value. These two parameters determine VersaSync's accuracy "tolerance window": A small window will cause VersaSync to deliver a more accurate time window, but also will cause it to quickly withdraw from the Anycast server pool, i.e. declare itself an invalid reference. (For more information about TFOM, see "Configuring the Oscillator" on page 239.)
    Navigate to **Management** > **Disciplining**, and click the GEAR icon in the top-right corner of the **Status** panel.
14. Set the value **Maximum TFOM for Sync** to 4 (this will make VersaSync to go out of sync if the phase error is greater than 1µs).
15. Set the value for **Holdover Timeout** to 10 s, to allow VersaSync to exit holdover quickly.
16. Leave the **Phase Error Limit** at 0, and do not check any of the checkboxes (or, for more information, see "Configuring the Oscillator" on page 239).

Configuring NTP over Anycast (OSPF IPv6)

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

1. Confirm that your existing network infrastructure is Anycast capable, and uses OSPF Version 3 (IPv6). Determine the OSPF area.
2. In the VersaSync Web UI, navigate to **MANAGEMENT** > **Network** > **NTP Setup**.
3. In the **Actions Panel**, click **NTP over Anycast**.
4. In the **NTP Anycast** window, select the **General** tab.
5. On the **General** tab, select **IPv6** as the IP Version.

6. Select the port to associate the Anycast service with (depending on the option card configuration of your unit, there may be only ETH0 available).
7. Select the port address to associate the Anycast service with (because there may be multiple IPv6 addresses on a single port), and click **Submit**. If no addresses appear, an IPv6 address must be added to the port.
8. In the **NTP Anycast** window, navigate to the **OSPF** tab.
9. On the **OSPF6** tab, check **Enable**.
10. Setup the OSPF6 area.
11. Click Submit.
12. Select the port address to associate the Anycast service with (because there may be multiple addresses on a single port), and click Submit. If no addresses appear, an IP address must be added to the port (see "Network Ports" on page 75).
13. Next, specify the maximum TFOM Setting (Time Figure of Merit), and the Holdover Timeout value. These two parameters determine VersaSync's accuracy "tolerance window": A small window will cause VersaSync to deliver a more accurate time window, but also will cause it to quickly withdraw from the Anycast server pool, i.e. declare itself an invalid reference. (For more information about TFOM, see "Configuring the Oscillator" on page 239.)
    Navigate to **Management** > **Disciplining**, and click the GEAR icon in the top-right corner of the **Status** panel.
14. Set the value **Maximum TFOM for Sync** to 4 (this will make VersaSync to go out of sync if the phase error is greater than 1µs).
15. Set the value for **Holdover Timeout** to 10 s, to allow VersaSync to exit holdover quickly.
16. Leave the **Phase Error Limit** at 0, and do not check any of the checkboxes (or, for more information, see "Configuring the Oscillator" on page 239).

Configuring NTP over Anycast (BGP)

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

1. Confirm that your existing network infrastructure is Anycast capable, and uses BGP. Determine the network specifics, such as your Autonomous System (AS) number, Neighbor's address and Neighbor's AS number.
2. In the VersaSync Web UI, navigate to **MANAGEMENT > Network > NTP Setup.**
3. In the **Actions Panel**, click **NTP over Anycast**.
4. In the **NTP Anycast** window, select the **General** tab.

5. On the **General** tab, select your desired IP Version. This selection automatically communicates with the **BGP** tab and displays the neighbor address field based on your needs.
6. Select the port to associate the Anycast service with (depending on the option card configuration of your unit, there may be only ETH0 available). If you desire IPv6 functionality, you must also select the IPv6 port address since there may be multiple IPv6 addresses on a single port.
7. In the **NTP Anycast** window, navigate to the **BGP** tab.
8. On the **BGP** tab, check **Enable**.
9. Input your **AS number**.
10. Input the neighbor's address.
11. Input the neighbor's AS number.
12. Click **Submit**.
13. Select the port address to associate the Anycast service with (because there may be multiple addresses on a single port), and click Submit. If no addresses appear, an IP address must be added to the port.
14. Next, specify the maximum TFOM Setting (Time Figure of Merit), and the Holdover Timeout value. These two parameters determine VersaSync's accuracy "tolerance window": A small window will cause VersaSync to deliver a more accurate time window, but also will cause it to quickly withdraw from the Anycast server pool, i.e. declare itself an invalid reference. (For more information about TFOM, see "Configuring the Oscillator" on page 239.)
    Navigate to **Management** > **Disciplining**, and click the GEAR icon in the top-right corner of the **Status** panel.
15. Set the value **Maximum TFOM for Sync** to 4 (this will make VersaSync to go out of sync if the phase error is greater than 1µs).
16. Set the value for **Holdover Timeout** to 10 s, to allow VersaSync to exit holdover quickly.
17. Leave the **Phase Error Limit** at 0, and do not check any of the checkboxes (or, for more information, see "Configuring the Oscillator" on page 239).

Configuring Anycast via NTP Expert Mode

Advanced Anycast configuration is possible via the **NTP Expert Mode** (see also "NTP Expert Mode" on page 150), which allows you to write directly into the Anycast configuration files (`zebra.conf`; `ospfd.conf`; `ospf6d.conf` and `bgpd.conf`).

The `zebra.conf` file is required for both IPv4, and IPv6 Anycast. The `ospfd.conf` file is required for IPv4 OSPF only, the `ospf6d.conf` file is required for IPv6 OSPF

only, and the `bgpd.conf` file has multiprotocol functionality, hence it can be used for both IPv4, and IPv6 Anycast.

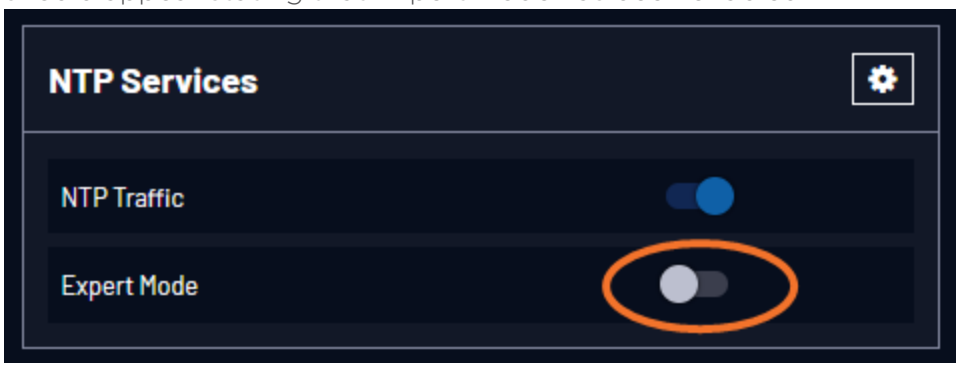
Caution: Expert Mode should only be utilized by advanced users, as incorrectly altering the Anycast files can cause Anycast to stop working.

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

Note: Interfaces intended for Anycast use should be connected and fully configured for IPv4 or IPv6 communication.

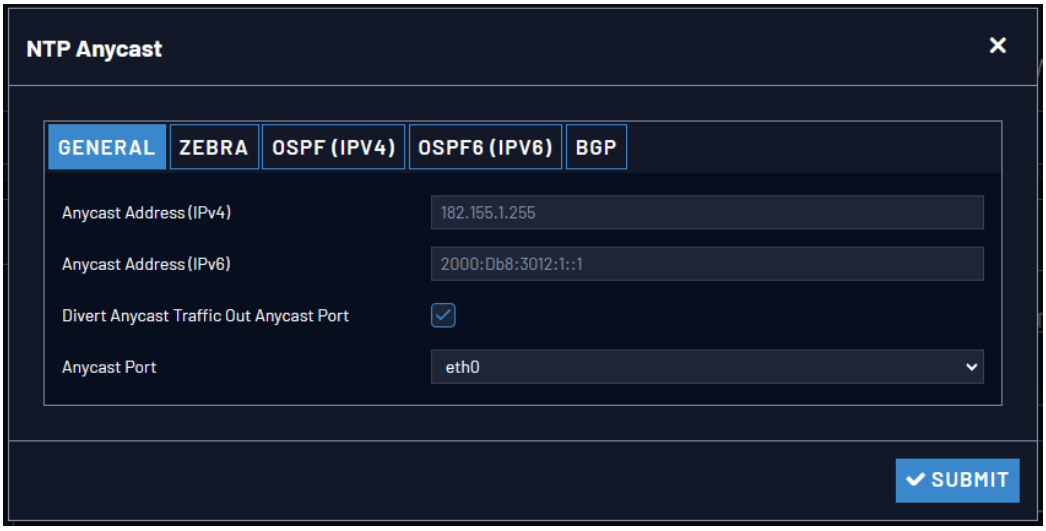
Note: When NTP Anycast is configured, the Anycast interface configured from the General tab will be momentarily reloaded to apply configuration.

1. To access Expert Mode, navigate to **MANAGEMENT > NTP Setup**.
2. Enable the switch for Expert Mode in the **NTP Services** panel, a notification should appear stating that Expert Mode has been enabled.



3. Once it is enabled, select **NTP Anycast** in the **Actions** panel. The **NTP Anycast** window will appear, with a **General** tab and separate tabs for

each of the configuration files.



4. To enable the option to divert NTP Anycast traffic through the Anycast port, navigate to the **General** tab and select the Divert Anycast Traffic Out Anycast Port check box.
5. To enable OSPF IPv4 Anycast, check Enable OSPF under the **OSPF (IPV4)** tab. To enable OSPF IPv6 Anycast, check Enable OSPF6 under the **OSPF6 (IPV6)** tab. To enable BGP Anycast, check Enable BGP under the **BGP** tab. Then select the Submit button.

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

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

Caution: Quagga services features outside of Safran base configuration settings are untested and may not interact properly within the VersaSync.

Caution: Do NOT edit the base interface IP addresses in `zebra.conf`. Doing so can cause Anycast to stop working.

zebra.conf Base configuration example

```
!
interface eth0
!
interface eth1
!
interface lo
ip address 10.10.10.10/32
ipv6 address fc00:10:10:10::10/128
!
access-list anycast permit 10.10.10.10/32
access-list anycast deny any
!
```

ospfd.conf Base configuration example

```
!
interface eth0
ip ospf area 0.0.0.0
!
!
interface lo
ip ospf area 0.0.0.0
!
!
router ospf
```

```
ospf router-id 10.10.100.200
distribute-list anycast out connected
!
```

ospf6d.conf Base configuration example

```
!
interface eth0
ipv6 ospf network broadcast
!
!
interface lo
ipv6 ospf network broadcast
!
!
router ospf6
router-id 10.10.100.200
interface eth0 area 0.0.0.0
interface lo area 0.0.0.0
!
```

bgpd.conf Base configuration example

```
router bgp 65001
bgp router-id 10.10.100.200
network 10.10.10.10/32
neighbor 10.10.100.250 remote-as 65000
neighbor fc00:10:10:100::250 remote-as 65000
!
address-family ipv6
network fc00:10:10:10::10/128
```

```
neighbor fc00:10:10:100::250 activate
exit-address-family
exit
!
```

Testing NTP over Anycast

Note: A detailed Anycast test procedure is available from Safran upon request. Please contact TimingSupport@nav-timing.safrangroup.com.

2.8.12.12 NTP Expert Mode

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

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

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

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

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

Caution: Safran Tech Support does not support the editing of the NTP configuration files while in the Expert Mode. For additional

information on editing the `NTP.conf` file, please refer to http://www.ntp.org/.

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

» The `NTP.conf` file can be reset back to the factory default values by either using the procedure to restore all of the VersaSync factory default settings (see "Restoring the Default NTP Configuration" on page 118) or editing the file back to the original configuration as shown in the factory default configuration below.

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

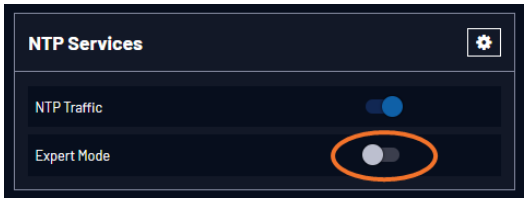
Factory default `NTP.conf` file:

```
restrict 127.0.0.1
restrict ::1
restrict default noquery nomodify
restrict -6 default noquery nomodify
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
server 127.127.45.0 prefer minpoll 4
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
peer 10.10.128.35 minpoll 3 maxpoll 3 autokey
keysdir /etc/ntp/keys/
crypto pw admin123 randfile /dev/urandom
driftfile /etc/ntp/ntp.drift
logfile /home/spectracom/log/ntp.log
statsdir /home/spectracom/log/ntpstats/
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable
```

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

To enable the Expert Mode, and edit the `NTP.conf` file:

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



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

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

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

2.8.12.13 Safran Technical Support for NTP

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

Safran can provide support for Microsoft® Windows-based time synchronization: https://safran-navigation-timing.com/document/synchronizing-windows-computers/. See safran-navigation-timing.com for additional information, or contact Safran Technical Support.

Safran 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.

2.8.13 Configuring PTP

Precision Time Protocol (PTP) is a time protocol that can be used to synchronize computers on an Ethernet network. VersaSync supports PTP Version 2, as specified in the IEEE 1588-2008 standard, via two (2) Ethernet ports.

VersaSync can be configured as a PTP Master Clock or as a PTP Slave Clock.

Next to PTP specifications, this topic describes the PTP menu items and settings, and outlines how to set up VersaSync as a PTP Master or Slave.

PTP Specifications

- **Inputs/Outputs**: (2) Ports
- **Signal Type**: Ethernet
- **Management**: Web UI
- **Network Speeds**: 10/100/1000 Mb/s
- **PTP Version** supported: PTP 2 (IEEE 1588-2008)
- **PTP Profiles** supported: (Changing the profile selection will adjust the default settings for the port to be configured):
  - Default
  - Telecom G.8265.1
  - Power Utility 61850-9-3
  - Power System C37.238
  - Enterprise
- **Transmission modes**: Unicast, Multicast (IPv4 and Ethernet), and Hybrid [default]
- **Timestamping**: VersaSync has PTP time stamp functionality which is set to use the PTP timescale.

2.8.13.1 The PTP Screen

The PTP screen provides PTP status information, and provides access to all configurable PTP settings.

To access the PTP screen, navigate to **MANAGEMENT > NETWORK: PTP Setup**. The PTP screen will open:

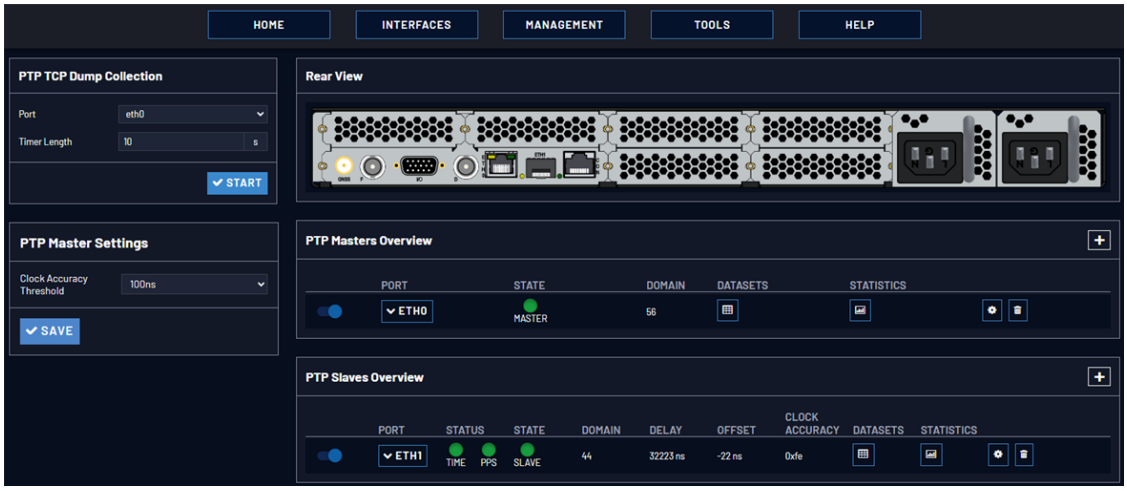


Figure 2-9: PTP setup screen

You will see the PTP Masters Panel, the PTP Slaves Panel, the PTP Master Settings Panel, and the PTP TCP Dump Collection Panel.

Note: Web UI pages refresh every 30 seconds, so if your changes aren't immediately reflected, you can try refreshing the page in your browser.

The PTP Masters Overview Panel

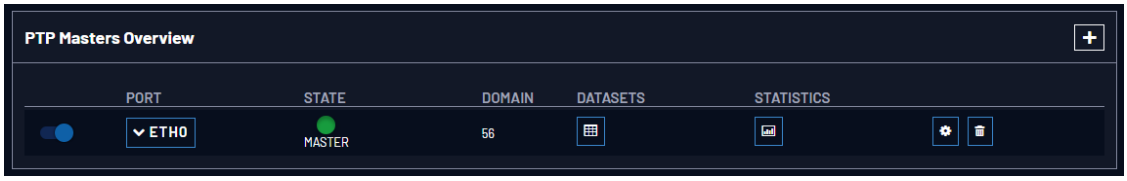


Figure 2-10: PTP Masters Overview Panel

Tip: You will not see any data in this panel if you do not have a PTP Master configured. See "Configure a New PTP Master or PTP Slave" on page 166

The PTP Masters Overview panel contains an overview of each PTP master configured on the unit, along with links to view more specific information.

The **ON/OFF toggle** will Enable/Disable PTP on the specific port.

The **Port dropdown** lists the port (eth0/eth1), and displays additional configuration information if the drop-down is selected:

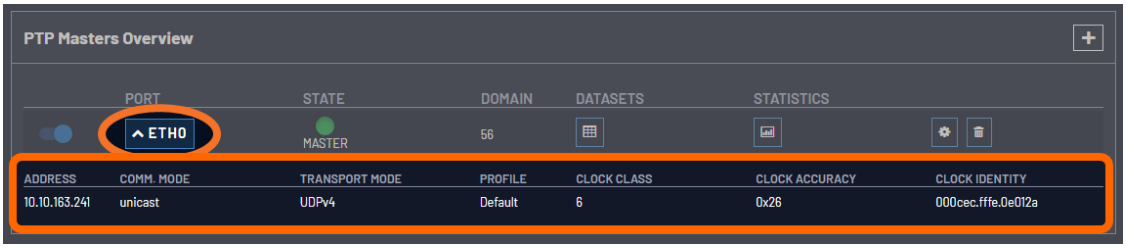


Figure 2-11: PTP Master Overview Drop Down

- Address: the IP or MAC address associated with the Ethernet port
- Comm. Mode: the PTP transmission mode configuration (Unicast, Multicast, or Hybrid).
- Transport Mode: (Ethernet, UDP on IPv4, UDP on IPv6).
- Profile: the currently selected PTP profile.
- Clock Class: as reported by the PTP data.
- Clock Accuracy: as reported by the PTP data.
- Clock Identity: a unique identifier for the PTP instance.

The **State** displays the current PTP master state. The LED will change according to the current state:

- Green: Master
- Yellow: Listening, Passive
- Red: Faulty
- Grey: Disabled, Unknown

The **Domain** displays based on the current configuration.

The **Datasets button** displays the Datasets popup window (see "The PTP Datasets Panel " on page 161).

The **Statistics button** displays the Statistics popup window (see "The PTP Statistics Panel" on page 162).

The **Settings button** brings up the popup window to edit settings (see "The Edit PTP Settings Panel" on page 158).

The **Delete button** removes the configuration on a given Ethernet port and will return all settings to default.

The **Plus symbol** adds a new PTP Master and brings up the Edit PTP Settings popup window..

The PTP Slaves Overview Panel

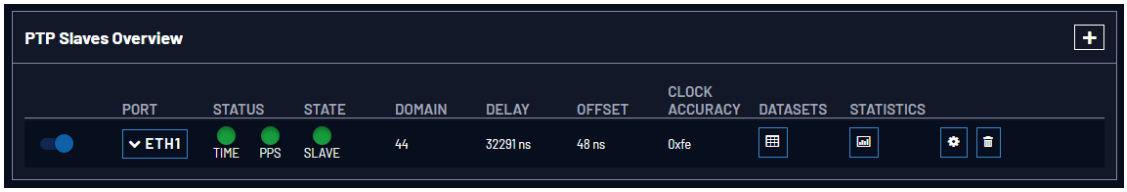


Figure 2-12: PTP Slaves Overview Panel

> Tip: You will not see any data in this panel if you do not have a PTP Slave configured. See"Configure a New PTP Master or PTP Slave" on page 166

The PTP Slaves Overview panel contains an overview of each PTP slave configured on the unit, along with links to view more specific information.

The **ON/OFF toggle** will Enable/Disable PTP on the specific port.

The **Port dropdown** lists the port (eth0/eth1), and displays additional configuration information if the drop-down is selected:

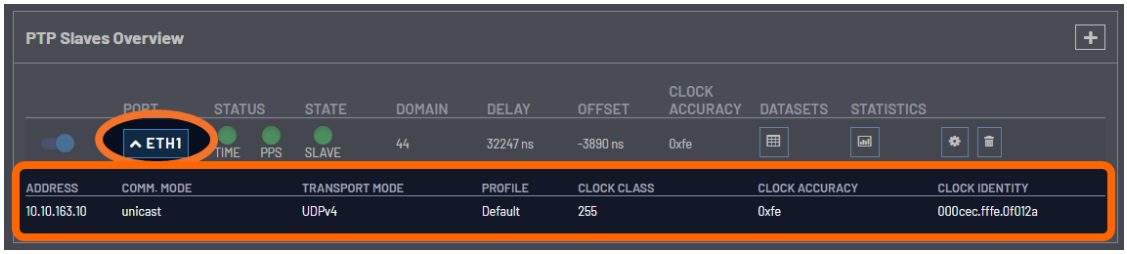


Figure 2-13: PTP Slaves Overview Drop Down

- Address: the IP or MAC address associated with the Ethernet port.
- Comm. Mode: the PTP transmission mode configuration (Unicast, Multicast, or Hybrid).
- Transport Mode: (Ethernet, UDP on IPv4, UDP on IPv6).
- Profile: the currently selected PTP profile.
- Clock Class: as reported by the PTP data.
- Clock Accuracy: as reported by the PTP data.
- Clock Identity: a unique identifier for the PTP instance.

The **Status** LEDs display the Validity for the Time and PPS provided by the PTP Master associated with this slave.

The **State** displays the current PTP slave state. The LED will change according to the current state:

- Green: Slave
- Yellow: Listening, Uncalibrated
- Red: Faulty
- Grey: Disabled

The **Domain** displays based on the current configuration.

The **Delay** reflects the path delay between master and slave.

The **Offset** is the current offset to Master.

The **Clock Accuracy** displays as reported by the PTP data.

The **Datasets button** displays the Datasets popup window (see "The PTP Datasets Panel " on page 161).

The **Statistics button** displays the Statistics popup window (see "The PTP Statistics Panel" on page 162).

The **Settings button** brings up the popup window to edit settings (see "The Edit PTP Settings Panel" below).

The **Delete button** removes the configuration on a given Ethernet port and will return all settings to default.

The **Plus symbol** adds a new PTP Slave and brings up the Edit PTP Settings popup window.

The Edit PTP Settings Panel

The Edit PTP Settings Panel displays when the plus symbol to add a new Master or Slave is selected, or when the Settings button next to a configured PTP Ethernet port is selected. The settings panel provides access to the configuration settings, as described below. When you are finished with your configuration, select **Submit** (you could also choose to **Restore defaults**).

Note: The PTP settings fields visible will change based on profile selection and other choices made in the configuration process.

Note: The Restore Defaults button in each PTP Settings panel will only apply to the configuration of the Ethernet port that is currently open.

Settings changed by the user will be maintained when the PTP service is stopped and started, and between reboots and power cycles.

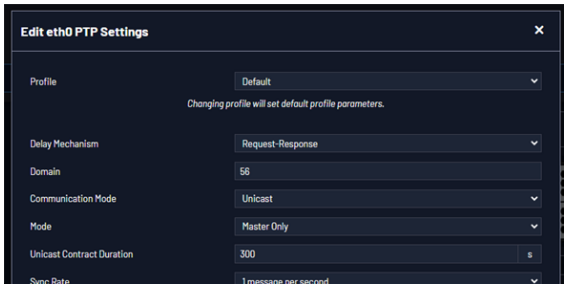


Figure 2-14: Edit PTP Settings panel

- **Profile**: PTP profile selection beyond Default will result in new fields, parameters, and default values.
  - **Default** Standard presets and defaults for PTP functionality.
  - **Telecom G.8265.1**: Defaults: Unicast is required, Domain is set to 4.
  - **Power Utility 61850-9-3**: Defaults: Peer Delay Mechanism, with an announce rate of 1 message per second, Ethernet Network Transport, and available Peer MAC Address field.
  - **Power System C37.238-2017**: Defaults: Peer Delay Mechanism, with an announce rate of 1 message per second, Ethernet Network Transport, available Peer MAC Address and Alt Timescale Display Name fields. Domain is set to 254.
  - **Enterprise**: Defaults: Request-Response Delay Mechanism, Multicast or Hybrid is required, UDP on IPv4 or IPv6 Network Transport, Announce Rate set to 1 message per second, and Best Master Clock Algorithm On.
- **Delay Mechanism**: [Request-Response or Peer] Set for propagation delay measurements.
- **Domain**: [defaults very for Profile selection] Sets the current PTP Domain Number, as defined in IEEE Std 1588-2008 Section 7.1
- **Communication Mode**: Select multicast, hybrid, or unicast mode.

About… PTP Transmission Modes

The PTP Card is able to transmit the PTP packets in three transmission modes:

• **Multicast Mode**: PTP packets are transmitted to all PTP Clocks by means of Multicast IP addresses. PTP packets received by the PTP Clocks are then filtered from the Domain Number, the Port Identity (Clock Identity + Port Number) of the transmitter. When the Master Clock is set in Multicast mode, this module will deny the requests from the Slaves Clocks to run in Unicast mode. When the Master Clock is set in Unicast mode, it doesn't transmit any PTP messages until a Slave has been granted to run in Unicast mode.

• **Unicast Mode**: This is a Point-to-Point transmission mode between two PTP Clocks by means of the unique IP address assigned to each PTP Clock.

• **Hybrid Mode**: [default] This mode uses Multicast messages for Sync, Follow-Up, and Announce packets from the Master. Slaves are expected to send Delay Request messages to the Master in Unicast, and the Master responds in Unicast. No Unicast Negotiation grants are necessary.

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.

- **Mode**: Master Only or Slave Only.
- **Unicast Contact Duration**: [10 to 1000 s] Unicast communication mode only. Duration of the Unicast contract, in seconds.
- **Sync Rate**: The rate at which Sync messages are sent, in packets per second.
- **Announce Rate**: [see Sync Rate above] The rate at which Announce messages are sent, in packets per second.
- **Delay Req Rate**: (Request-Response Delay Mechanism Only). Interval between request messages sent by the slave to the master, in packets per second.
- **Peer Delay Req Rate**: (Peer Delay Mechanism Only). Interval between request messages sent between peers, in packets per second.
- **Best Master Clock Algorithm**: [On or OFF] Only available with Multicast and Hybrid modes. When set to ON, the Master will listen for traffic from other Masters and become passive if another master on the network has better credentials according to the Best Master Clock Algorithm (Section 9.3 of IEEE 1588-2008). A passive master will not transmit any protocol

messages as long as another Master is active as the Best Master on the network. If the unit is synchronized but the oscillator is not yet locked to the primary reference, then the BMCA will transition to slave until the end of that condition.
When set to OFF, the Master will act as an active master no matter whether or not other masters are present. This may be required for certain PTP profiles.

- **Clock Priority 1**: [0 to 255] (0 is highest priority. Default is **128** for both priority values. This is usually the priority value that a Slave is set to.) See IEEE 1588-2008, Section 8.10.1, 8.10.2.
- **Clock Priority 2**: [0 to 255] (same as above).
- **Network Transport**: [Ethernet, IPv4/UDP, IPv6/UDP] Selects the transport protocol used for PTP packets.
- **MAC Address**: [default: 01:1B:19:00:00:00] Default, Power Utility 61850-9-3 and Power System C37.238 profiles only. The address protocol messages are sent to.
- **Peer MAC Address**: [default: 01:80:C2:00:00:0E] Default, Power Utility 61850-9-3 and Power System C37.238 profiles only.
- **Alt Timescale Display Name**: Power System C37.238 profile only. Display name of the alternative timescale (optional).
- **Multicast Ttl**: [1 through 255] Time-to-live (packet lifespan) — Sets the TTL field for PTP packets except for Peer-to-Peer packets for which TTL is forced to 1 as specified in IEEE Std 1588-2008 Annex D.3.
- **Delay Asymmetry**: [-2147483648 to 2147483648] Sets the time difference (in nanoseconds) of the transmit and receive paths in networks with a constant asymmetry (default of 0). The values should be positive when the master-to-slave propagation time is longer and negative when the slave-to-master time is longer.

The PTP Datasets Panel

The PTP Datasets Panel brings data from PTP communications to be viewed via the Web UI. There are five dataset types available:

Default Dataset

TwoStepFlag, ClockIdentity, NumberPorts, ClockClass, ClckAccuracy, OffsetScaledLogVarience, Priority1, Priority2, DomainNumber, and SlaveOnly.

Current Dataset

StepsRemoved, OffsetFromMaster, MeanPathDelay

Parent Dataset

ParentPortIdenity, ParentSts, ObservedParentOffsetScaledLogVarience, ObservedParentClockPhaseChangeRate, GrandmasterIdentity, ClockClass, Clock-Accuracy, OffsetScaledLogVarience, GrandmasterPriority1, Grand-masterPriority2.

Time Properties Dataset

CurrentUtcOffset, CurrentUtcOffsetValid, Leap59, Leap61, TimeTraceable, PtpTimescale, TimeSource

Port Dataset

PortIdentity, PortState, LogMinDelayReqInterval, PeerMeanPathDelay, LogAn-nounceInterval, AnnounceReceiptTimeout, LogSyncInterval, DelayMechanism, LogMinPdelayReqInterval, VersionNumber

Clock Description Dataset

ClockType, PhysicalLayelProtocol, PhysicalAddress, ProtocolAddress, Man-ufactureId, ProductDescription, RevisionData, UserDescription, ProfileId

The PTP Statistics Panel

This panel  provides statistics for each Ethernet port. If the PTP is set to OFF for a specific port, this screen will not display any information.

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

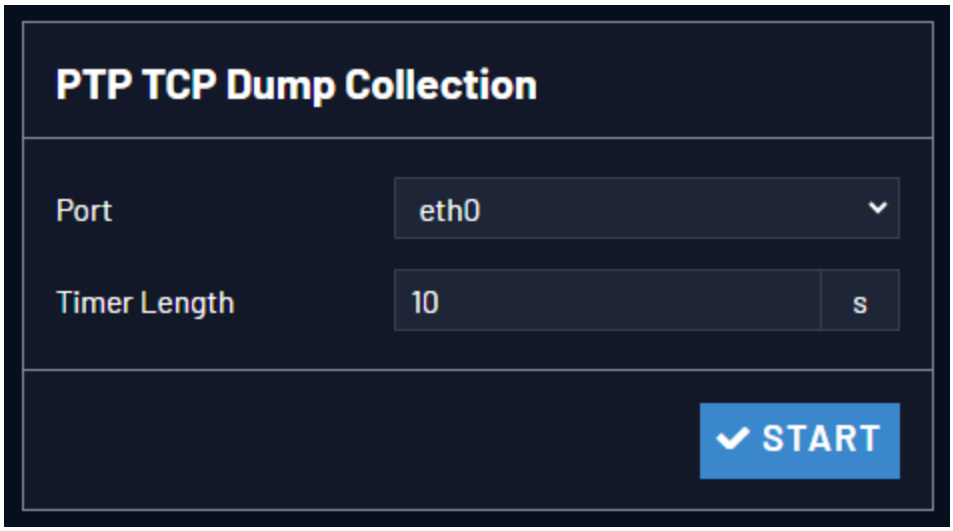
Figure 2-15: PTP Statistics Panel

Select the PTP Node to view the statistics of the communication between the Ethernet port selected and a specific PTP node.

- **State**: Current PTP state
- **Clock Type**: (Master or Slave)
- **Domain**: current settings
- **Profile**: current settings
- **PTP Node**: IP address of PTP node.
- **Address**: IP or MAC address
- **Clock Identity**: [e.g., "a0:36:9f:ff:fe:37:b9:5d"]
- **Time of Results**: [e.g., "2023-08-12 18:19:15"] Time at which stats were retrieved.
- **Results Since**: [e.g., "2021-10-18 16:05:30"] Time at which the stats collection started
- **Transmitted/Received Count**: Message count of sent/received data

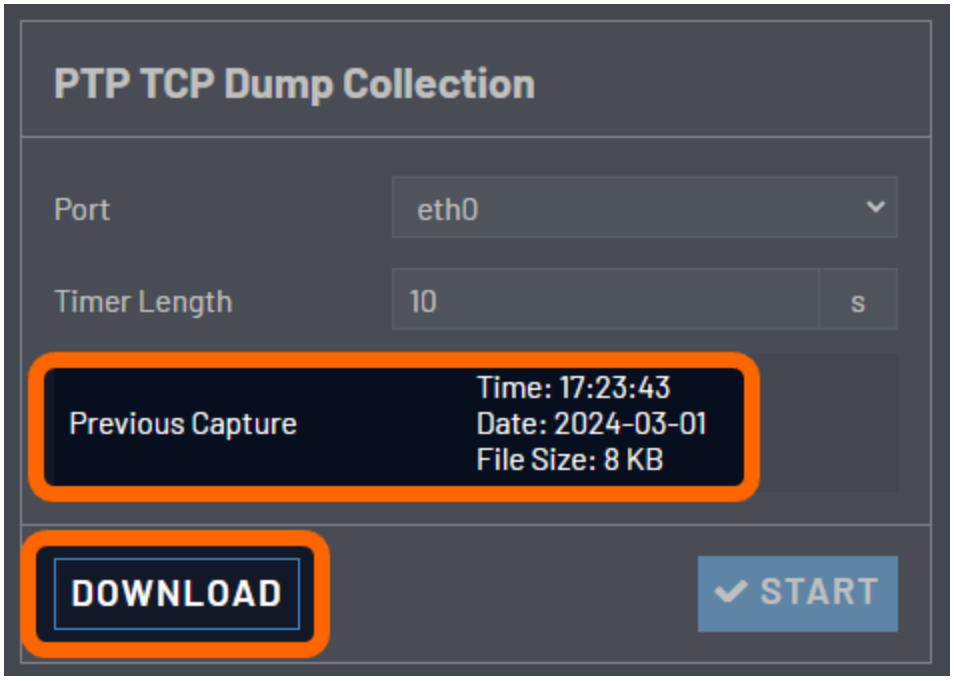
- **Average Rate**:[e.g., "0.062"] Indicates how often the selected message has been detected (in seconds; e.g., "1.0" would mean once every second).
- The **Clear Statistics** button will reset the zero count.
- The **Refresh** button will retrieve the latest results

The PTP TCP Dump Collection Panel



This feature allows you to record a PTP-specific network packet capture via `tcpdump` on a specific port for a certain amount of time. This can help with troubleshooting your PTP setup. To use the PTP TCP Dump Collection:

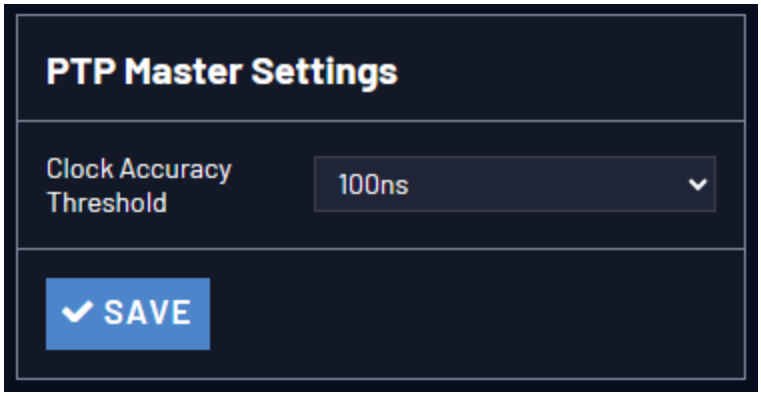
1. Select the Timer Length and Ethernet port you wish to investigate.
2. Select the Start button.
3. After the collection is completed, the latest collection information will display in the panel, and a Download button will display.



4. Select Download to obtain the PCAP file.

Note: The PTP TCP Dump panel will not display if you have removed TCP Dump from your unit. See "Network Services" on page 77 for more information about the main `tcpdump` feature.

The PTP Master Settings Panel



This feature allows you to set the grandmaster's minimum clock accuracy threshold. The setting is system-wide and is useful in events where clock accuracy oscillates above or below the default threshold of <100ns. To configure:

1. Select a value from the dropdown list.
2. Select the SAVE button.

2.8.13.2 Configure a New PTP Master or PTP Slave

To configure a PTP port:

1. Navigate to either the PTP Slaves Overview panel or the PTP Master Overview panel and select the plus icon.
2. Enter your PTP port configuration (some fields will hid or be revealed based on your selections for Profile, Mode, and other factors). For more information on your configuration options, see "The Edit PTP Settings Panel" on page 158.
3. Select Submit.
4. You will need to Enable the PTP port in the PTP Master or Slave Overview panels.
5. View your PTP Master or Slave in the PTP Overview panels. For more information on PTP verification, refer to the "PTP Monitoring" below section.

2.8.13.3 Enable/Disable PTP

To enable or disable PTP:

1. Navigate to **MANAGEMENT > NETWORK: PTP Setup**.
2. In the **PTP Masters Overview** or the **PTP Slaves Overview** panel, slide the toggle switch to ON or OFF for the desired Ethernet port.

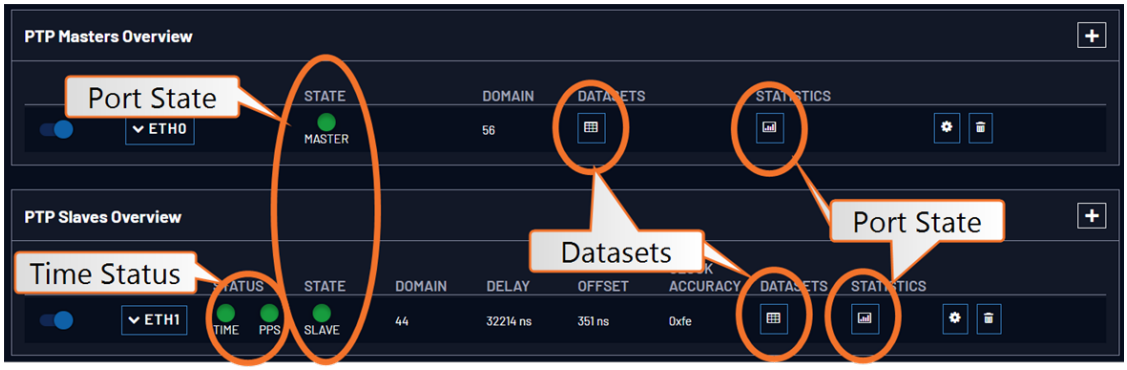
Note: You will not be able to see or Enable PTP ports if you do not have one configured. Select the plus icon in one of the PTP Overview panels to add a PTP interface.

3. Configure your settings using the Edit Settings Panel.

2.8.13.4 PTP Monitoring

To confirm that your PTP is functioning correctly, we provide a number of PTP Monitoring methods.

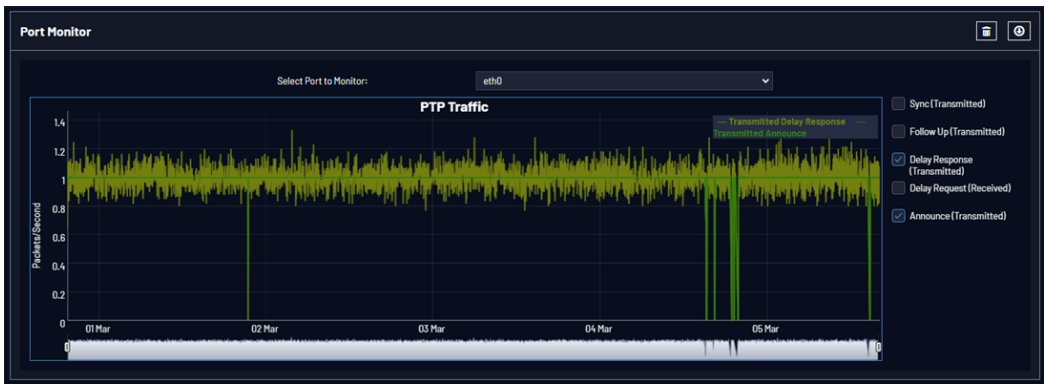
PTP Monitoring via the Web UI



After configuring and enabling your PTP port(s), the main clue to the current condition of PTP functionality is the State for either Master or Slave (found in the PTP Master and Slave Overview panels).

Another good indication of the heath and operation of your PTP setup are the PTP graphs:

» The Port Monitor graph allows you to select an Ethernet port to view the rates different types of traffic:



» The Slaves Monitor will specifically display Offset and Path Delay inform-

ation for any slaves configured on the unit:

The Datasets and Statistics buttons will also provide information about the frequency of packet exchange, and the state of timing in the nodes that the PTP port is communicating with.

You can also execute a TCP Dump collection from the Web UI to obtain a packet capture (see "The PTP Master Settings Panel" on page 165).

PTP Monitoring via SNMP

PTP monitoring is available through the SNMP MIB files (see "Accessing the SNMP Support MIB Files" on page 103).

PTP Monitoring via the REST API

You can access PTP monitoring data via the REST API. See "REST API Configuration" on page 286 for more information.

2.8.13.5 General Configuration Notes

- Ensure that the Ethernet port used for PTP is connected to the network. Navigate to **MANAGEMENT > NETWORK: Network Setup**, and verify the STATUS in the **Ports** panel.
- **For a Master Clock**: Be sure that valid time and 1PPS references are currently selected: Navigate to **MANAGEMENT > OTHER: Reference Priority**, and confirm **Reference Priority** configuration, and **Reference Status**. Note that in order to operate properly as a Master Clock, VersaSync must be synchronized to a non-PTP reference. The built-in GNSS reference provides all information needed with no user intervention. Should you, however, be using a different reference, ensure that it transmits the following information.

- 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.

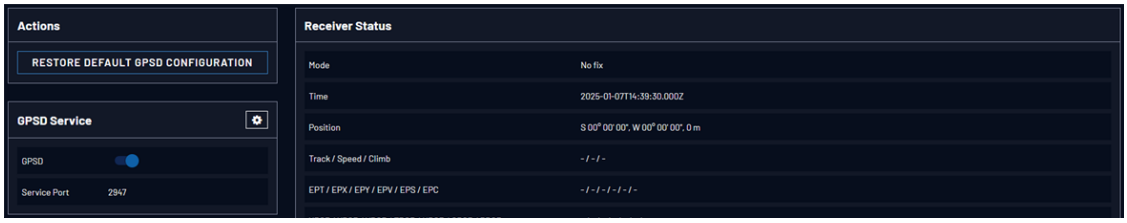
2.8.14 GPSD Setup

GPSD is a free, open-source package used worldwide to manage GNSS systems and devices. With GPSD support on a VersaSync, users are able to:

- connect to the unit over a network via TCP at the specified port using any GPSD-compatible software
- receive position and timing information from the GNSS receiver in a consistent format, and
- use the Web UI (or CLI) to configure the GPSD service and view status information.

GPSD can only be configured to track the VersaSync internal u-blox receiver.

To configure GPSD on the Web UI, navigate to **MANAGEMENT** > **NETWORK** > **GPSD Setup** to access the GPSD Setup Screen



The GPSD Setup Screen is divided into three panels:

1. The GPSD Service panel:
   - allows you to toggle the service ON or OFF (**ON** default state)
   - lists the Service Port
   - the **Gear Icon** in the GPSD Service panel allows you to change the Service Port information. If your GPSD setup changes and needs to be reconfigured within your VersaSync, this is where you can reset the service port.
2. The Actions panel provides an option to restore the **default configuration**.
3. The Receiver Status panel lists the information required by the GPSD service:
   - Mode, Time, Position, Track/Speed/Climb, Error Statistics, and Precision Statistics

- All satellites in view and the PRN, Elevation, Azimuth, Signal Strength, and Usage for each satellite.

GPSD via CLI commands

The following CLI commands are used to control the behavior of GPSD via the VersaSync CLI:

- `gpsdserviceportget` – Displays the GPSD service port
- `gpsdserviceportset` – Sets the GPSD service port

There are two GPSD utility programs already incorporated into VersaSync; `GPSpipe` and `CGPS`. Both can be used as commands within the CLI to view information currently being sent via GPSD. Both commands use `CTL + C` to stop.

CHAPTER 3

Managing Time

In this document, the notion of **Managing Time** refers not only to the concept of VersaSync's System Time, but also to reference configuration, as well as distribution of time and frequency.

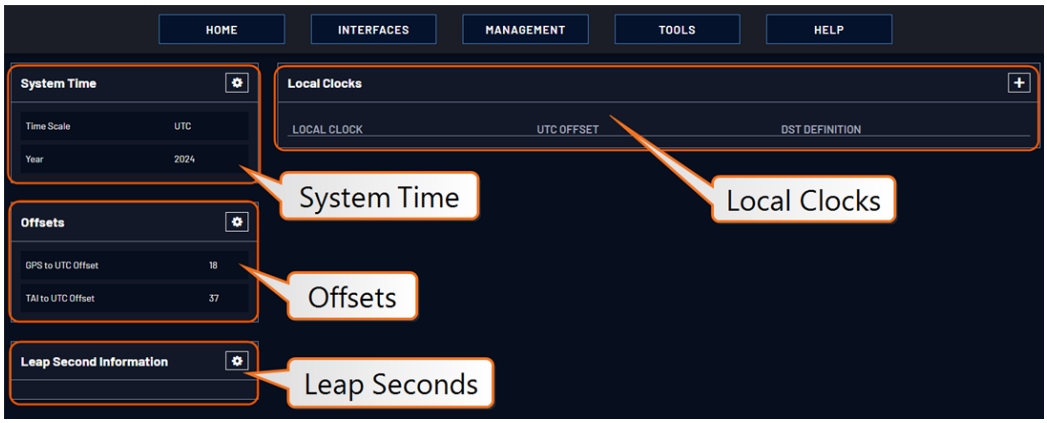
The following topics are included in this Chapter:

3.1 The Time Management Screen

The **Time Management** screen is the point of entry for all **System Time**-related settings that are user-configurable.

To access the **Time Management** screen:

1. Navigate to **MANAGEMENT > OTHER: Time Management**.
2. The **Time Management** screen opens. It is divided into 4 panels:



System Time panel

The System Time panel displays the time scale and the year, and allows access to the **Edit System Time** window via the GEAR icon in the top-right corner. This window is used to select the time scale, and to manually set a user- time, if so required.

See "System Time" on page 174.

Offsets panel

The Timescales **UTC**, **TAI**, and the **GPS**-supplied time are offset by several seconds, e.g. to accommodate leap seconds. The GPS offset may change over time, and can be managed via the GEAR icon in the top-right corner of this panel.

Leap Second Info panel

From time to time, a leap second is applied to UTC, in order to adjust UTC to the actual position of the sun. Via the **Leap Second Info** panel, leap second corrections can be applied to VersaSync's time keeping. It is also possible to enter the exact day and time when the leap second is to be applied, and to delete a leap second.

See also: "Leap Seconds" on page 181

Local Clocks panel

You can create multiple different Local Clocks, as needed. The names of all Local Clocks that have already been created are displayed in the Local Clocks panel.

See also "Local Clock(s), DST" on page 184.

3.2 System Time

The time that VersaSync maintains is referred to as the System Time. The System Time is used to supply time to all of the available time-of-day outputs (such as NTP time stamps, time stamps in the log entries, ASCII data outputs, etc.).

By default, the System Time is synchronized to VersaSync's input references (such as GNSS, IRIG, ASCII data, NTP, PTP, etc.).

If a UTC-based time is not required, however, it is also possible to manually set the System Time to a desired time/date, or to use the unit's battery backed time (Real Time Clock) as System Time (with an external 1PPS reference).

The flow chart below illustrates how VersaSync obtains the highest available and valid reference, depending on whether an external source is chosen as reference, or an internal (**User[x]**, or **Local System**).

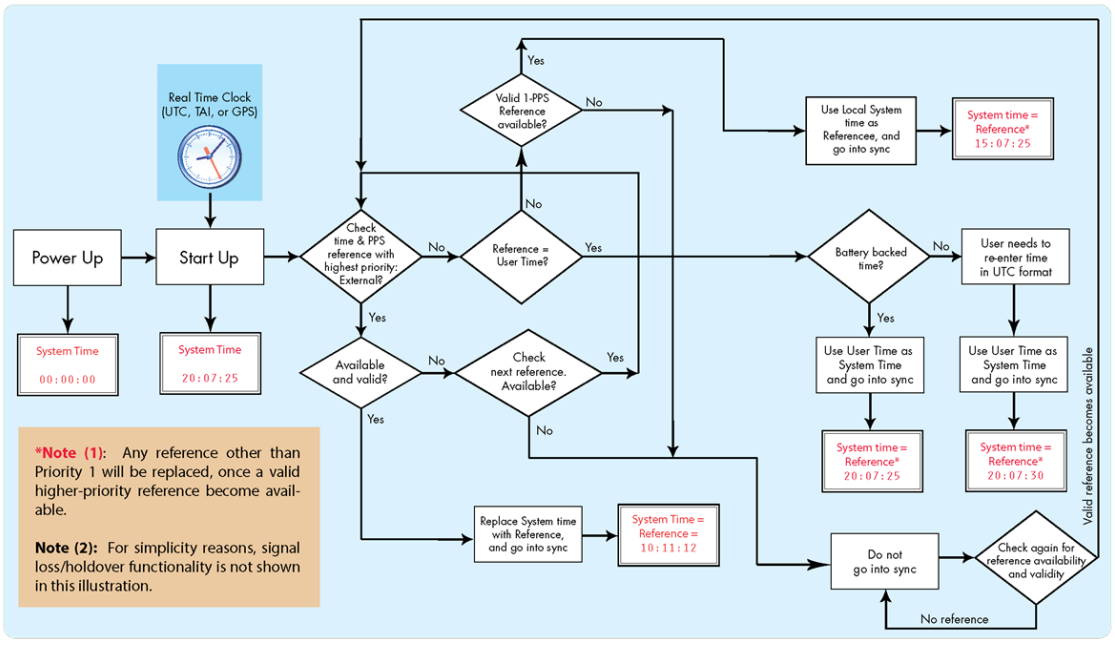


Figure 3-1: How the System Time is derived

Note: User hand-set times can only be set in UTC (not Local time).

3.2.1 System Time

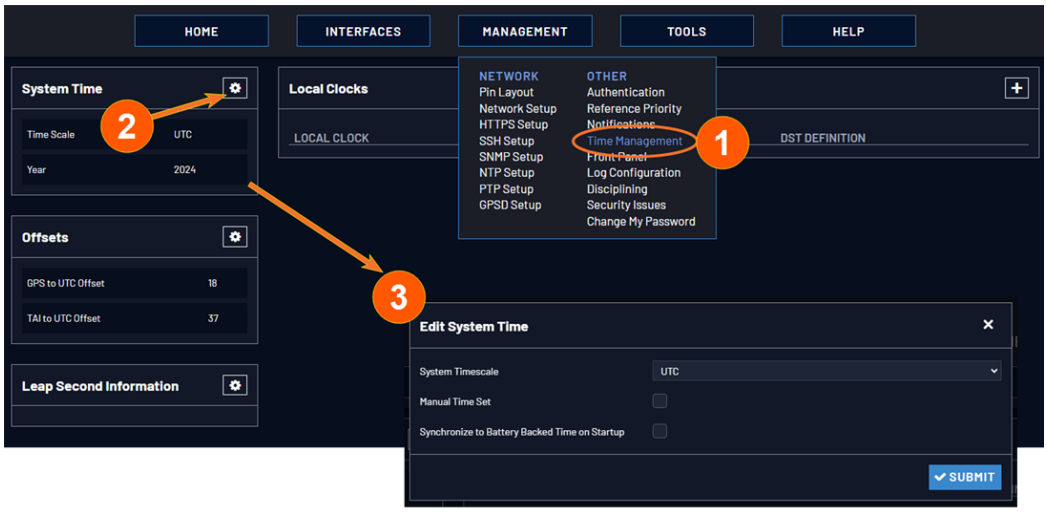
Several System Time parameters can be customized:

- The **System Timescale** can be changed.
- A **user-defined time** can be setup for e.g., for simulation purposes, or if no external reference is available.
- The **battery-backed** RTC time can be used as System Time, until an external reference become available.

3.2.1.1 Configuring the System Time

To configure the System Time:

1. Navigate to **MANAGEMENT > OTHER: Time Management**.



2. In the **System Time** panel located in the top-left corner of the **Time Management** screen, click the GEAR icon.
3. The **Edit System Time** pop-up window will display.
   - In the **System Timescale** field select a timescale from the drop-down list. The options are:
     - **UTC**: Coordinated Universal Time (Temps Universel Coordonné); your local time zone determines the difference between UTC and local time.

Note that UTC is not a time zone, but a time standard, i.e. it is not used anywhere in the world as the official local time, whereas GMT (Greenwich Mean Time) is a time zone that is used in several European and African countries as the official local time.

» **TAI**: International Atomic Time (Temps Atomique International).

The TAI time scale is based on the SI second and is not adjusted for leap seconds. As of 20-November-2025, TAI is ahead of UTC by 37 seconds. TAI is always ahead of GPS by 19 seconds.

» **GPS**: The Global Positioning System time is the timescale maintained by the GPS satellites.

Global Positioning System time is the time scale maintained by the GPS satellites. The time signal is provided by atomic clocks in the GPS ground control stations. The UTC–GPS offset as of 20-November-2025 is 18 seconds.

For more information on Timescales, see "Timescales" below.

4. If you want to override the system time with a **manually set User Time**, check the **Manual Time Set** checkbox. For information, see "Manually Setting the Time" on page 177.
5. Click **Submit** to update the System Time and close the window.

3.2.1.2 Timescales

The System Time can be configured to operate in one of several **timescales**, such as UTC, GPS and TAI *(Temps Atomique International)*. These timescales are based on international time standards, and are offset from each other by varying numbers of seconds.

When configuring VersaSync, in most cases, **UTC** will be the desired timescale to select.

Note: UTC timescale is also referred to as “ZULU” time. GPS timescale is the raw GPS time as transmitted by the GNSS satellites (in 2018 the GPS time is currently 18 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 20-November-2025 TAI time is 37 seconds ahead of UTC.

VersaSync's System timescale is configured via the **MANAGEMENT > OTHER: Time Management** screen, see "System Time" on page 174.

Input timescales

Some of the inputs may not necessarily provide time to VersaSync 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 VersaSync with "local" time, with no time jumps occurring when the reference is selected.

If an output reference is using the GPS or TAI timescale, and the System Time is set to "UTC", then the GPS Offset box in the Edit GPS Offset window must be populated with the proper timescale offset value in order for the time on the output reference to be correct. Some references (like GNSS) provide the timescale offset to the system. In the event that the input reference being used does not provide this information, it must be set in through the **Offsets** panel of the **Time Management** page.

Since the GPS and TAI offsets have a fixed relationship, only the GPS offset can be set. If only the TAI offset is known, subtract 19 from it to get the GPS offset.

Note: If the System Time is set to the UTC timescale, and all output references either use the UTC or "local" timescale, then it is not necessary to set the GPS and TAI timescale Offsets.

Caution: It is imperative to configure any input reference's timescales appropriately. Otherwise, a System Time error may occur!

Output timescales

Some of the available VersaSync outputs (such as the 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.

Other VersaSync 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).

3.2.1.3 Manually Setting the Time

For some applications, it may not be necessary to synchronize VersaSync to a UTC-based reference. Or, a GPS reference is not available yet (e.g., because the antenna is not yet installed), but the system has to be setup and tested.

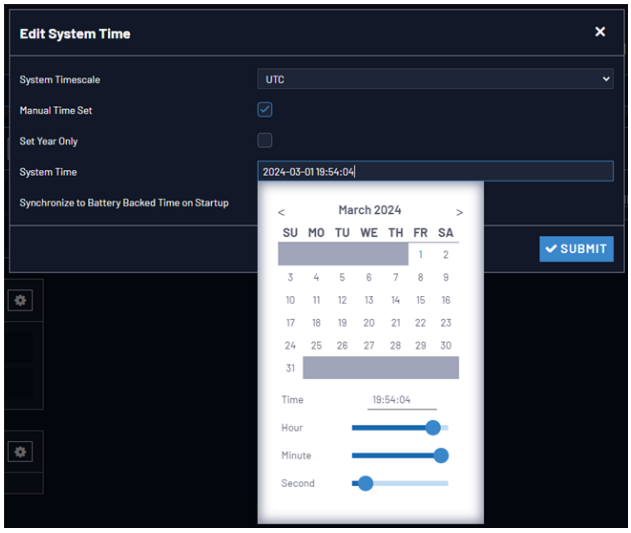
In such cases, the System Time can be hand-set, and then used as a **User [x]**-set System Time. For more information on when to use this functionality, see "The "User/User" Reference" on page 194.

Note: If synchronization to UTC is NOT required, it is advisable to set a time in the past or future, so as to avoid users inadvertently considering the distributed time to be genuine.

Caution: Note that this mode of operation is intended for special use cases e.g., autonomous systems, where legally traceable time is not required: This time will be inaccurate/not traceable, since it is not tied to any reference.

To hand-set the System Time, and configure this time to be a valid reference:

1. Navigate to **MANAGEMENT > OTHER: Time Management**.
2. In the **System Time** panel on the left, click the GEAR icon.
3. Select **Manual Time Set**. Set your time & date, as needed:
   - **System Time** [DATE; TIME]: If you do not select **Set Year Only**, this box will show the current time in the format: `Year-Month-Day Hour:Minute:Second`. To set the time manually, click anywhere in the **System Time** field. A drop-down calendar with time-setting sliders will appear:



The time in the **System Time** field will default to the current date and time. To set the time, use the sliders. The time will display between the calendar and the sliders, and also next to the chosen date in the field directly above the calendar. To close the calendar, click anywhere in the **Edit System Time** window.

NOTE: Except for testing purposes, you should not choose a date other than the current day.

- **Set Year Only**: Some legacy time formats (e.g., IRIG) do not support years. Checking this box will open a data entry field to manually set the year. Safran recommends not to utilize this feature, unless the IRIG format you are using does not provide a YEAR field.
- **Synchronize to Battery Backed Time on Startup**: See "Using Battery Backed Time on Startup" on the facing page.

4. Click Submit at the precise moment desired.
5. Navigate to **MANAGEMENT > OTHER: Reference Priority**.
6. In order for the **User** time to be a considered a valid reference, verify that the Reference Priority table includes an "Enabled" **User [x]** Time, and 1PPS reference ("**User/User**"). For more information, see "Input Reference Priorities" on page 187 and "The "User/User" Reference" on page 194.
7. Move (drag & drop) the **User** time to the top of table, and disable all other references.
8. Let Holdover expire. (Set it to a very short duration, if desired:
   i. Navigate to **MANGAGEMENT > OTHER: Disciplining**.
   ii. In the **Status** panel, click the GEAR icon.

iii. In the **Oscillator Settings** window, set the **Holdover Timeout**.)

9. Check on the **HOME** screen that **User 0** is displayed, with a **green** STATUS. Note that the **Disciplining State** will remain **yellow**, once **Holdover** has expired, since the system time is not synchronized to a reference.

Note: Contrary to the User reference discussed above, the Local System reference can be used for Time, or 1PPS (but not both). For more information, see "The "Local System" Reference" on page 193.

3.2.1.4 Using Battery Backed Time on Startup

Upon system startup, by default VersaSync will not declare synchronization until one of the external references becomes available and valid.

This functionality can be overridden by enabling the **Synchronize to Battery Backed Time on Startup** and configuring User 0 as a backup reference in the reference table, thus allowing the battery backed time to be used as System Time upon system startup. The Battery Backed Time is also referred to as the time maintained by the integrated **Real Time Clock** (**RTC**)

This will result in VersaSync providing a System Time before one of the external references becomes available and valid. This will happen automatically, i.e. without user intervention. As soon an external reference will become available and if user 0 has a lower priority than that external reference, its time will take precedence over the battery backed time: The System Clock will adjust the System Time for any time difference.

Note: The Battery Backed Time is also referred to as the time maintained by the integrated Real-Time Clock (RTC).

Use Cases

Using the Battery Backed Time on Startup is typically used in these cases:

a. If the synchronization state is to be reached as quickly as possible, even if this means the time distributed initially will most likely be less accurate than an external time reference.

b. A system is intended to operate autonomously (i.e. without any external references) and

- the hand-set time (user 0) entered manually during commissioning of the system is sufficiently accurate
- the system needs to be able to completely recover from a temporary power loss, or similar, without human intervention.

c. A system is used for simulation or testing purposes, and UTC traceability is not required.

The Accuracy of the Battery Backed Time ...

... depends on the accuracy of the hand-set time if the time is set manually in an autonomous system. In a non-autonomous system (i.e, when using external reference(s)) VersaSync's System Clock will regularly update the battery-backed time.

Another factor impacting the accuracy of the battery-backed time is how long a VersaSync unit is powered off: Any significant amount of time will cause the battery-backed RTC to drift, i.e. the battery-backed time will become increasingly inaccurate.

The battery used for the RTC is recharged during operation of the unit, and is designed to last for the lifetime of the product.

Distributing battery-backed time over NTP

When distributing a hand-set, battery backed time via NTP, please set the time relatively close to UTC, so as to prevent NTP synchronization problems when transitioning from the hand-set time to a UTC-based external input reference. See also "Input Reference Priorities" on page 187.

To use the battery-backed time as the synchronized time at start-up:

1. Navigate to **MANAGEMENT > OTHER: Time Management**.
2. In the **System Time** panel click the GEAR icon.
3. The **Edit System Time** window will display. Select the checkbox **Synchronize to Battery Backed Time on Startup**:

4. Click the **Submit** button.

3.2.2 Timescale Offset(s)

Timescale offsets account for fixed differences between timescales, in seconds. Timescale offsets may change because of leap seconds, see "Leap Seconds" below.

3.2.2.1 Configuring a Timescale Offset

To configure a timescale offset to the System Time:

1. Navigate to **MANAGEMENT > OTHER: Time Management**.
2. In the **Offsets** panel on the left, click the GEAR icon in the top-right corner.
3. The **Edit GPS Offset** window will display. Enter the desired **GPS Offset** in seconds, and click Submit.

> **Note:** Since the GPS Offset and the TAI Offset have a fixed relationship, only the GPS Offset can be set. If only the TAI offset is known, subtract 19 from it, in order to obtain the GPS offset.

Note that the data stream of GPS and several other external references includes information about a pending Leap Second, and as such automatically corrects for a Leap Second. Nevertheless, it is advisable to perform some testing in advance to ensure all system components will adjust flawlessly. For more information, see "Leap Seconds" below.

3.2.3 Leap Seconds

3.2.3.1 Reasons for a Leap Second Correction

A Leap Second is an intercalary[1] one-second adjustment that keeps broadcast standards for time of day close to mean solar time. Leap Seconds are required to synchronize time standards with civil calendars, thus keeping UTC time in sync with the earth's rotation.

Leap seconds can be introduced in UTC at the end of the months of December or June. The INTERNATIONAL EARTH ROTATION AND REFERENCE SYSTEMS SERVICE (IERS) publishes a bulletin every six months, either to announce a time step in UTC, or to confirm that there will be no time step at the next possible

[1]Intercalary: (of a day or a month) inserted in the calendar to harmonize it with the solar year, e.g., February 29 in leap years.

date. 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 time offsets. When a Leap Second occurs, VersaSync will automatically change these offsets by the proper amount, no matter which timescale is currently being used by the system.

As of 2018 the GPS to UTC Offset is 18 seconds. The last Leap Second occurred on December 31, 2016.

VersaSync can be alerted of impending Leap Seconds by any of the following methods:

- **GNSS Receiver** (if available as an input reference): The GNSS satellite system transmits information regarding a Leap Second adjustment at a specific Time and Date an arbitrary number of months in advance.
- **Input references other than GNSS**: Some of the other available input references (e.g., IRIG, ASCII, NTP) can also contain pending Leap Second notification in their data streams (see chapter below).
- **Manual user input**: VersaSync can be manually configured with the date/-time of the next pending Leap Second. On this date/time, the System Time will automatically correct for the Leap Second (unless the System Time's timescale is configured as either GPS or TAI).

3.2.3.2 Leap Second Alert Notification

VersaSync will announce a pending Leap Second adjustment by the following methods:

- ASCII Data Formats 2 and 7 (among other formats) from the **ASCII Data** option modules contain a Leap Second indicator. During the entire calendar month preceding a Leap Second adjustment, these Formats indicate that at the end of the current month a Leap Second Adjustment will be made by using the character 'L' rather than a '_ ' [space] in the data stream. Note that this does not indicate the direction of the adjustment as adding or removing seconds. These formats always assume that the Leap Second will

be added, not removed.

- **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 10b.
- **PTP Packets** provide leap indication with a 12-hour notification window.
- Some **IRIG formats** provide leap second notification indicators.

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. VersaSync 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.

3.2.3.3 Leap Second Correction Sequence

The following is the time sequence pattern in seconds that VersaSync will output at UTC midnight on the scheduled day (Note: This is NOT local time midnight; the local time at which the adjustment is made will depend on which Time Zone you are located in).

A. Sequence of seconds output when **adding a second** ("positive Leap Second"):
   - 56, 57, 58, 59, **60**, 0, 1, 2, 3 ...

B. Sequence of seconds output when **subtracting a second** ("negative Leap Second"):
   - 56, 57, **58, 0**, 1, 2, 3, 4 ...

3.2.3.4 Configuring a Leap Second

To manually correct the System Time for a leap second:

1. Navigate to **MANAGEMENT> OTHER: Time Management**. The Time Management screen will be displayed. In the lower left-hand corner, the **Leap Second Information** panel will show if a leap second if pending. This panel

will be empty, unless:

a. A leap second is pending, and VersaSync has obtained this information automatically from the GPS data stream.

b. A leap second had been configured previously by a user via the **Edit Leap Second** window.

2. To access the **Edit Leap Second** information window, click the GEAR icon in the **Leap Second Information** panel.
3. The **Edit Leap Second** window will display:
4. In the **Leap Second Offset** field enter the desired GPS Offset.
5. In the **Date and Time** field, enter the date that the desired leap second should occur.
6. Click **Submit**.

To delete a leap second correction, click the Delete button.

Note: The Delete button in the Edit Leap Second window will only be visible if a leap second has been set beforehand.

3.2.4 Local Clock(s), DST

The **Local Clock** feature allows for maintaining one or several local times. These times will reflect a time offset, thereby accounting for Time Zone, and DST (Daylight Savings Time) correction.

3.2.4.1 Adding a Local Clock

To add a Local Clock:

1. Navigate to **MANAGEMENT > OTHER: Time Management**.
2. Click the PLUS icon in the **Local Clocks** panel in the **Time Management** screen.
3. The **Local Clock** pop-up window will display.
4. Enter a **Name** for your local clock.
   - » The name must be between 1 and 64 characters long; spaces are allowed.
   - » The name can be any meaningful name that helps you know your point of reference (for example: “NewYork”, “Paris” or “EasternHQ”, 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:

> **Note:** Acceptable characters for the name include: A-Z, a-z, 0-9, (-+_) and space.

5. In the **UTC Offset** field, choose a **UTC Offset** from the drop-down list.
   - All of the **UTC Offset** drop-down selections are configured as UTC plus or minus a set number of hours.
   - Examples for the US: For **Eastern**, choose UTC–05:00; for **Central**, choose UTC-06:00; for **Mountain**, choose UTC-07:00; and for **Pacific**, choose UTC-08:00.
   - If you wish to use DST (Daylight Savings Time ["Summer Time"]) rules, click the **Use DST Rules** box. Otherwise the time for the local clock will always be standard time.
     DST options will appear in the **Local Clock** window:
6. **Set DST Rules by Region**: Check this box to apply regional DST rules. A regions drop-down menu with the following options will display:
   - **EU** (Europe): For locations complying with the European DST Rule. This rule differs from all other rules because the DST changes occur based on UTC time, not local time (all time zones in Europe change for DST at precisely the same time relative to UTC, rather than offset by local time zone).
   - **US-Canada**: For locations complying with the USA's DST Rule (as it was changed to back in 2006, where the "DST into" date is the Second Sunday of March and the "DST out" date is the first Sunday of November).
   - **Australia**.

> **Note:** If a pre-configured rule DST rule happens to be changed in the future (like the change to the US DST rule in 2006), this option allows the DST rules to be edited without the need to perform a software upgrade for a new DST rule to be defined. Select this drop-down and enter the DST parameters for the new rule.

7. **DST Start Date** and **DST End Date**: This option is provided for locations that do not follow any of the pre-configured DST rules. Click anywhere in either field to open a calendar, allowing you to enter any custom day & time rule.
8. **Offset**: In seconds. Use this field to manually define your local clock's DST offset e.g., 3600 seconds for a one hour offset.
9. **DST Reference**: When configuring a Local Clock that is synchronized to an input reference (e.g., IRIG input), VersaSync needs to know the timescale of the input time (Local Timescale, or UTC Timescale), in order to provide proper internal conversion from one Timescale to another.
   Select **Local** or **UTC**, depending on the Timescale of the Input reference this Local Clock is being used with.
   Additional Local Clocks may need to be created if multiple input Timescales are being submitted.
10. Click **Submit**. Your local clock will appear in the **Local Clocks** panel.

3.2.4.2 DST Examples

The following two examples illustrate the configuration of Daylight Savings Time (DST) for a Local Clock:

Example 1:

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

1. Navigate to **MANAGEMENT > Time Management: Local Clocks > (+): Local Clock**.
2. In the **Local Clock Name** field, assign a meaningful name to the new Local Clock.
3. From the **UTC Offset** pull down menu, select "UTC +01:00".
4. Confirm that the **Use DST Rules** checkbox is not selected.
5. Review the changes made and click the **Submit** button.

The unit will display the status of the change.

Example 2:

To create a Local Clock for a VersaSync 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. In the **MANAGEMENT > Time Management: Local Clocks > (+): Local Clock** window:

2. Navigate to **MANAGEMENT > Time Management: Local Clocks > (+): Local Clock**.

3. From the **UTC Offset** pull-down menu, select "UTC -05:00".

4. Select the **Use DST Rules** checkbox.

5. Select the **Set DST Rules by Region** checkbox.

6. From the **DST Region** drop-down list, select "US-Canada."

7. Review the changes made and click the **Submit** button.

The unit will display the status of the change.

3.2.4.3 DST and UTC, GMT

Neither UTC, nor GMT ever change to Daylight Savings Time (DST). However, some of the countries that use GMT switch to a different time zone offset during their DST period. The United Kingdom is not on GMT all year, but uses British Summer Time (BST), which is one hour ahead of GMT, during the summer months.

Additional information about regional time zones and DST can be found on the following web sites: http://www.worldtimeserver.com/, http://webexhibits.org/daylightsaving/b.html.

3.3 Managing References

3.3.1 Input Reference Priorities

VersaSync can be synchronized to different time and frequency sources that are referred to as Input References, or just References.

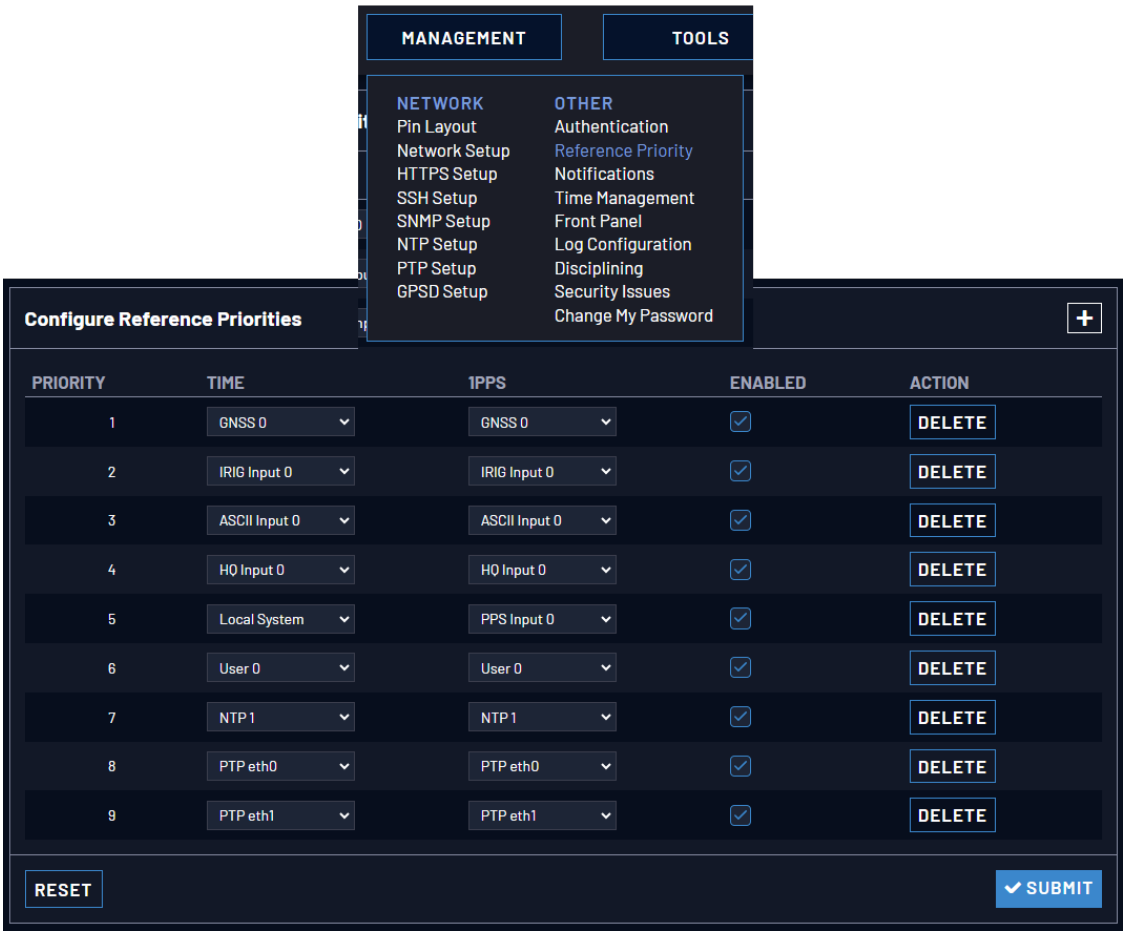
References can be a GNSS receiver, or other sources delivered into your VersaSync unit via dedicated (mostly optional) inputs. It is also possible to enter a system time manually, which VersaSync then can synchronize to.

In order for VersaSync to declare synchronization, it needs both a valid **1PPS**, and **Time** reference.

The concept of **Reference Priority** allows the ranking of multiple references for redundancy. This allows VersaSync to gracefully fall back upon a lower ranking **1PPS** or **Time** reference without transitioning into Holdover, in case a reference

becomes unavailable or invalid. The priority order you assign to your available references typically is a function of their accuracy and reliability.

Note: The References shown on your screen may look different from the illustration below, depending on your VersaSync Time and Frequency Synchronization System model and hardware configuration.



Each available type of **Time** and **1PPS** input reference is assigned a human-readable name or "title" that is used in the **Reference Priority** table, indicating the type of reference. The reference titles are listed in the following table:

Table 3-1: Reference priority titles

Title	Reference
ASCII Timecode	ASCII serial timecode input

Title	Reference
External 1PPS input	External 1PPS input
Frequency	External Frequency input
GNSS	GNSS input
PTP	PTP input
IRIG	IRIG timecode input
Local System	Built-in clock OR internal 1PPS generation
NTP	NTP input
User	Host (time is manually set by the user)
HAVEQUICK	HAVEQUICK input

The number displayed indicates the number of feature inputs of that type presently installed in the VersaSync– starting with “0” representing the first feature input. For example:

- IRIG 0 = 1st IRIG input instance
- Frequency 1 = 2nd frequency input instance
- NTP 2 = 3rd NTP input instance

The columns of the **Reference Priority** table are defined as follows:

- **Priority**—Defines the order or priority for each index (row). The range is 1 to 16, with 1 being the highest priority and 16 being the lowest priority. The highest priority reference that is available and valid is the reference that is selected.
- **Time**—The reference selected to provide the necessary “Time” reference.
- **1PPS**—The reference selected to provide the necessary “1PPS” reference.
- **Enabled**—The reference is enabled.
- **Delete**—Removes the Index (row) from the Reference Priority table.

3.3.1.1 Configuring Input Reference Priorities

VersaSync can use numerous external time sources, referred to as "references". As external time sources may be subject to different degrees of accuracy and reliability, you can determine in which order (= priority) VersaSync calls upon its external time and 1PPS references.

For additional information, see also "Input Reference Priorities" on page 187.

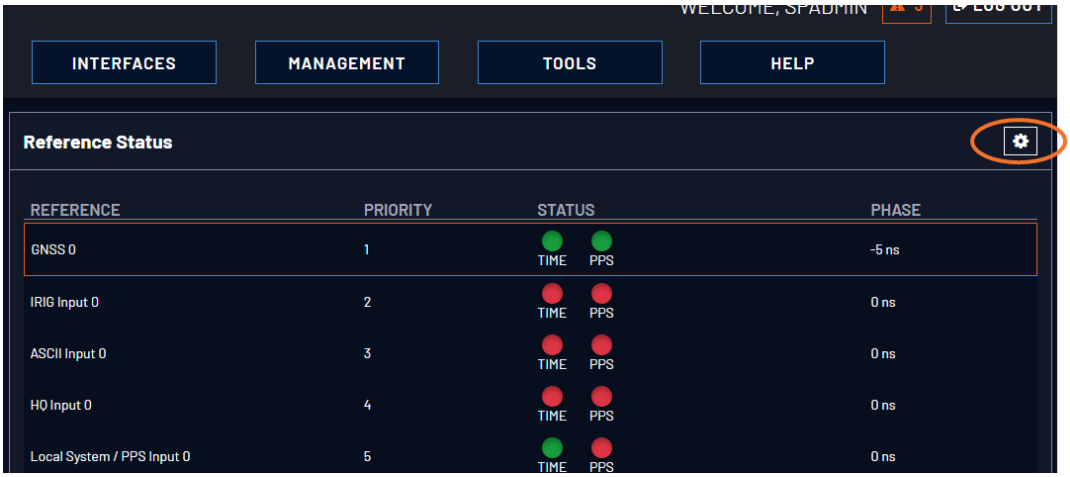
Accessing the Reference Priority Screen

To access the **Reference Priority Setup** screen:

1. Navigate to **MANAGEMENT > OTHER: Reference Priority**.

OR:

1. On the **HOME** screen, click the GEAR icon in the **Reference Status** panel:



2. The **Configure Reference Priorities** screen will display.

   The **Reference Priority** screen is divided into 3 areas:

   a. The **Actions** panel, which provides a single action:
      - Restore Factory Defaults

   b. The **Configure Reference Priorities** panel, which displays the priority of VersaSync's references in a table form.
   In this panel you can:
      - Add and configure new references
      - Delete references
      - Enable/disable references
      - Reorder the priority of VersaSync's references

   c. The **Reference Status** panel
      - The **Reference Status** panel provides a real time indicator of the status of the VersaSync's references. It is the same as the **Reference Status** panel on the **HOME** screen of the Web UI.

Adding an Entry to the Reference Status Table

To add a new entry to the **Reference Status** table:

1. Navigate to the **Configure Reference Priorities** screen via **MANAGEMENT > OTHER: Reference Priority**.
2. Click the PLUS icon in the top right-hand corner of the **Configure Reference Priorities** table.
3. The **Add Reference** window will display:

4. In the **Add Reference** window, enter:
   - **Priority Level**: Assign a priority to the new reference.
   - **Time**: Select the time reference.
   - **PPS**: Select the PPS reference.
   - **Enabled**: Check this box to enable the new reference.
5. Click **Apply** or **Submit**. (**Submit** will close the window.)

Deleting a Reference Entry

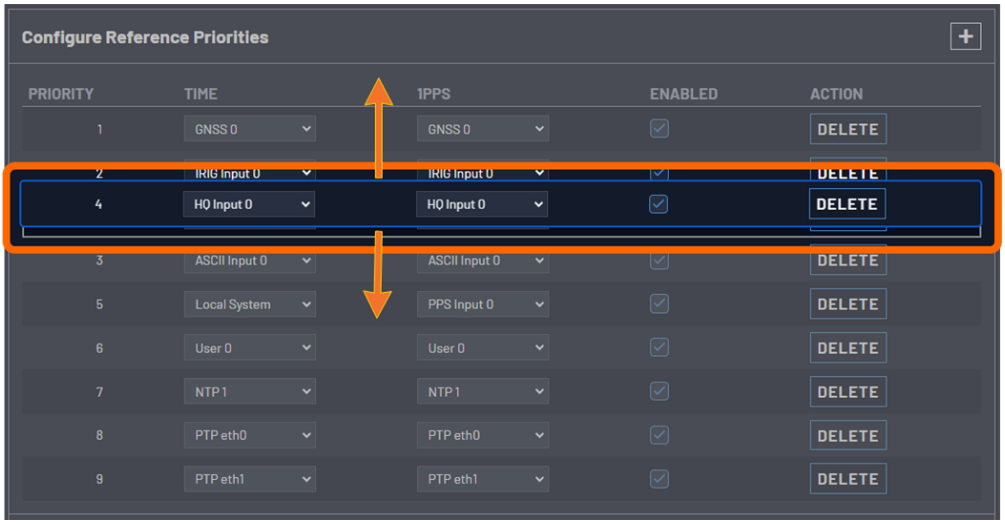
To delete an entry from the **Reference Status** table:

1. Navigate to the **Configure Reference Priorities** screen via **MANAGEMENT > OTHER: Reference Priority**.
2. In the **Configure Reference Priorities** table click the **Delete** button on the right-hand side of the entry you wish to delete.
3. In the pop-up window that opens click **OK** to confirm.

Reordering Reference Entries

To reorder the priority of a reference entry:

1. Navigate to the **Configure Reference Priorities** screen via **MANAGEMENT > OTHER: Reference Priority**.
2. Click and hold on the item whose priority you wish to reorder.
3. Drag the item up or down to the desired place.



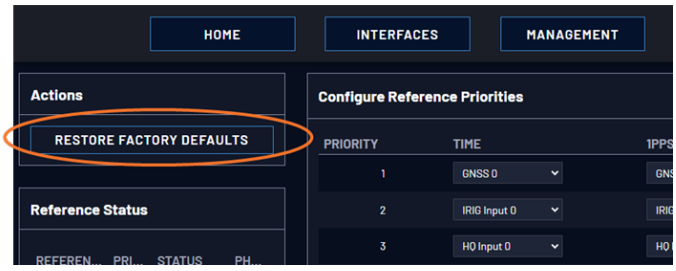
4. Click **Submit.**

> **Note:** The **Reference Status** table will always display references in order of priority. Changes made in the **Configure Reference Priorities** screen will be reflected in the table after those changes are submitted.

Resetting Reference Priorities to Factory Defaults

To reset all references in the **Reference Priority** table to their factory default priorities:

1. Navigate to the **Configure Reference Priorities** screen via **MANAGEMENT > OTHER: Reference Priority** menu.
2. In the **Actions** panel, click the **Restore Factory Defaults** button.



3.3.1.2 The "Local System" Reference

The **Local System** reference is a "Self" reference, i.e. VersaSync uses itself as an input reference for Time, or as a 1PPS reference. The **Local System** is a unique input reference in that it can be used as either the Time reference, or the 1PPS reference, but never both.

> **Note:** For VersaSync to operate as a Local System reference, you must have either a valid external Time reference, or a valid external 1PPS reference.

- When the Time reference is configured as **Local System**, VersaSync's System Time is considered a valid reference, as long as the external 1PPS input reference is valid.
- Vice versa, when the 1PPS reference is configured as **Local System**, VersaSync's built-in oscillator is considered a valid reference, as long as the external Time reference is valid.

Use case "Local System Time"

The **Local System** reference when used for Time allows VersaSync to operate using its current Time-of-Day (ToD) for Time, while synchronized to an external 1PPS reference.

While you may intentionally offset the time in this scenario, the second will be precisely aligned to the external 1PPS reference. Therefore, this use case qualifies as a legitimate, traceable time source.

Instead of an offset time, **Local System** can also be used as a backup Time reference (e.g., Priority "2"): Should the external Time reference become invalid, the **Local System** Time will become the valid backup reference, disciplined by the external 1PPS reference: VersaSync will transition to the **Local System** Time, without going into Holdover.

Use case "Local System 1PPS"

The **Local System** reference can also be used for 1PPS: This allows VersaSync to operate using an external ToD for time, while generating 1PPS from its own internal oscillator.

In this rare use case the 1PPS is NOT aligned to any standard, therefore the time may drift, and must be considered untraceable.

3.3.1.3 The "User/User" Reference

While it is normally not required, it is possible for you as the "User" to override the **System Time** (even if it is synchronized to a valid reference) with a manually set time, steered by an undisciplined oscillator, and use this manually set Time as an output reference. This concept is referred to as the **User/User** reference, because both the Time, and the 1PPS reference are not linked to any UTC-based external reference, but hand-set by you.

> **Caution:** Since the User/User reference is not traceable to a valid reference, it does not qualify as a legitimate time source. Operating VersaSync with a manually set User time bears the risk of inadvertently outputting an illegitimate System Time thought to be a valid reference time.

Use cases for the "User/User" reference

The **User/User** reference is provided for the following use cases:

a. No external references are available (yet), but you need a reference for testing or setup purposes. This may be the case e.g., while waiting for a GNSS antenna to be installed.

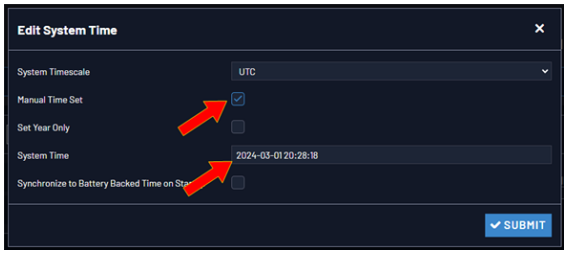
b. No external references are required e.g., if VersaSync is used solely to synchronize computers on a network, with no need for traceable UTC-based timing.

c. To utilize a backup reference as soon as possible after a power cycle or reboot of VersaSync, while waiting for the primary reference (e.g., GNSS) to become valid. To this end, in the **Edit System Time** window, the checkbox **Synchronize to Battery Backed Time on Startup** must be checked, AND the **User/User** reference is assigned a reference priority number other than "1". Note that a Time jump and/or 1PPS jump are likely to happen once the primary reference becomes valid.

Combining a **User** Time reference with a **non-User** 1PPS reference or vice versa is not a typical use case. Use the **Local System** reference instead, see "The "Local System" Reference" on the previous page.

Built-in safety barrier

In order to "validate" (= greenstatus lights) the **User/User** reference, the hand-set time must be manually submitted every time after VersaSync reboots or resets, or after the Holdover period has expired: In the **Edit System Time** window, the checkbox **Manual Time Set** must be checked. The System Time displayed in the field below will become valid the moment the Submit button is clicked.



See also below, "How long will the User/User reference be valid?": The notion of limiting the validity of the User/User reference also serves as a safety feature.

How long will the User/User reference be valid?

Since the User/User reference does not qualify as a legitimate, traceable time, it becomes invalid once VersaSync is reset, or power-cycles, or after the Holdover Time expires (whichever occurs first). It then needs to be set manually and submitted again (**Edit System Time** > **Manual Time Set**).

The only workaround for this is "Using Battery Backed Time on Startup" on page 179. This will allow VersaSync to apply the **User/User** reference after a power-cycle without manual intervention.

How to setup the User/User Reference

See "Manually Setting the Time" on page 177.

Using the "User" Reference with Other References

If the **User/User** reference is used in conjunction with other, external references (such as GNSS or IRIG), the **System Time** should be set as accurately as possible:

Otherwise, the large time correction that needs to be bridged when switching from a lost reference to a valid reference, or from a valid reference to a higher-priority reference that has become available again, will cause NTP to exit synchronization. If the difference is under 1 second, NTP will remain in sync and will "slew" (over a period of time) to the new reference time.

3.3.1.4 Reference Priorities: EXAMPLES

Example 1 – GNSS as primary reference, IRIG as backup:

In this use case, the objective is to use:

- GNSS as the primary Time, and 1PPS reference
- IRIG as the backup Time, and 1PPS reference.

Step-by-step procedure:

1. Move the reference which has “GPS 0” in the **Time** column and “GPS 0” in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.
2. Move the reference which has “GPS 0” in the **Time** column and “GPS 0” in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.
3. Move the reference which has “GPS 0” in the **Time** column and “GPS 0” in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.

Since both of these references are *default* references, no additional references need to be added to the **Reference Priority** table.

Example 2 – IRIG as primary reference, NTP input as backup

In this use case, the objective is to use:

- IRIG as the primary reference input
- Another NTP server as backup reference

Step-by-step procedure:

1. Move the reference which has “IRIG 0” in both the **Time** column and “IRIG 0” in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.
2. Move the reference which has “NTP” in the **Time** column and “NTP” in the **1PPS** column to the second place in the table, with a **Priority** value of 2. Click the **Enabled** checkbox.
3. For all other references, uncheck the **Enabled** checkbox, so that they are all disabled.

Since both of these references are *default* references, no additional references need to be added to the **Reference Priority** table.

Example 3 – NTP input as the only available input (“NTP Stratum 2 operation”)

In this use case, the objective is to have NTP provided by another NTP server as the only available reference input, i.e. the unit to be configured is operated as a Stratum 2 server. For more information, see "Configuring "NTP Stratum Synchronization"" on page 121.

Step-by-step procedure:

1. Move the reference which has “NTP” in the **Time** column and “NTP” in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.
2. For all other references, uncheck the **Enabled** checkbox, so that they are all disabled.
3. Configure the NTP Service as described under "Configuring "NTP Stratum Synchronization"" on page 121.

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 and 1PPS input when it is desired to use NTP as an input reference.

Example 4 – Time set manually by the User. Other references may or may not be available

Note: In order for a manually set time to be considered valid and used to synchronize VersaSync, a “User” needs to be created and enabled in the Reference Priority table. "The "User/User" Reference" on page 194.

In this use case, the objective is to use a hand-set time, in combination with VersaSync's oscillator as a 1PPS source as valid references.

Step-by-step procedure:

1. If necessary (see NOTE above), create a “User.”
2. Move the reference which has “User 0” in the **Time** column and “User 0” in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.
3. For all other references, uncheck the **Enabled** checkbox, so that they are all disabled.

If the objective is to use a manually set time as a *backup* to other references (such as GNSS or IRIG):

1. Move the "User/User" reference to a place in the table that has a priority lower than the references the "User/User" reference will be backing up. Make sure the **Enabled** checkbox is selected.
2. With “User/User” enabled, if no other higher priority references are enabled or available (or if the higher priority references have since been lost), you can now manually set the **System** time to the desired value (**MANAGEMENT > OTHER: Time Management > System Time > Manual Time Set**). See "System Time" on page 174 for more information. VersaSync will go into synchronization using this set time once you click the Submit button.

Note: You will need to repeat this procedure each time VersaSync is power-cycled (with no other references available), unless you enabled the feature Synchronize to Battery Backed Time on Startup.

Example 5—Time at power-up ("Local System Time") to be considered "Valid". GNSS input to serve as 1PPS reference

The objective of this use case is to allow VersaSync to use itself as a valid reference. This is referred to as “Local System” time.

In order for this to happen, VersaSync requires an external Time, or 1PPS reference. In other words, "Local System" cannot be both Time, and 1PPS. This makes "Local System" a legitimate, traceable reference.

Therefore the "Local System" does not have to be manually set ("validated") by the User after VersaSync was power cycled (as would be the case with a “User/User” reference).

Since “Local System” cannot be both **Time**, and **1PPS** input together, in this example the GNSS input will be set as the 1PPS reference (other use cases may require using different references, e.g. IRIG.)

As there is no default entry for “Local System” and “GPS”, a new entry needs to be added to the **Reference Priorities** table in order to use this combination of references.

Step-by-step procedure:

1. Add a reference to the Reference Priority by clicking the PLUS icon. Use the following settings, then click **Submit**:
   - » In the **Priority Level** text box, enter **1**. This will give this reference the highest priority.

- In the **Time** field, select “Local System”.
- In the **PPS** field, select “GPS”.
- Check the **Enabled** checkbox.

2. Confirm that the first reference in the **Reference Priority** table has “Local System” as the **Time** input and "GNSS" as the **1PPS** input.
3. After a power cycle or reboot, as soon as GNSS is declared valid, the System Time will automatically be used as-is, with no manual intervention required.

3.3.2 Reference Qualification and Validation

3.3.2.1 Reference Monitoring: Phase

The quality of input references can be assessed by comparing their phase offsets against the current system reference, and against each other. This is called **Reference Monitoring**.

Reference Monitoring helps to understand and predict system behavior, and is an interference mitigation tool. It can also be used to manually re-organize reference priorities e.g., by assigning a lower reference priority to a noisy reference or a reference with a significant phase offset, or to automatically failover to a different reference if certain quality thresholds are no longer met (see "Smart Reference Monitoring" on the next page).

VersaSync allows Reference Monitoring by comparing the phase data of references against the System Ontime Point. The phase values shown are the filtered phase differences between each input reference 1PPS, and the internal disciplined 1PPS.

The data is plotted in a graph in real-time. The plot also allows you to display historic data, zoom in on any data range or on a specific reference. A data set can be exported, or deleted.

To monitor the quality of references, navigate to **TOOLS > SYSTEM: Reference Monitor**. The Reference Monitor screen will display:

On the left side of the screen, **Status** information is displayed for the System and the References. Note that the **Reference Status** panel also displays the latest PHASE OFFSET reading (1) for active references against the System Ontime Point. The reading is updated every 30 seconds.

This Reference Phase Offset Data is plotted over time (abscissa) in the **Reference Monitor** panel in the center of the screen. Use the check boxes in the **References** panel (2) to select the reference(s) for which you want to plot the phase offset data. Use the handles (3) to zoom in on a time window.

The scale of the axis of ordinate (4) is determined by the largest amplitude of any of the references displayed in the current time window. Use the checkboxes in the **References** panel on the right to remove references from the graph, or add them to it.

Smart Reference Monitoring

The Smart Reference Monitoring uses **phase error validation** in combination with **automatic failover**:

The phase error validation calculates long-term averages and standard deviations of the phase offset between the monitored external reference and the internal system reference. The standard deviation is used to calculate two validity thresholds, a higher and a lower one (the latter acts as a hysteresis buffer, preventing the status flip/flopping if the actual phase error validation value varies closely around the outer threshold). The thresholds are not user-configurable.

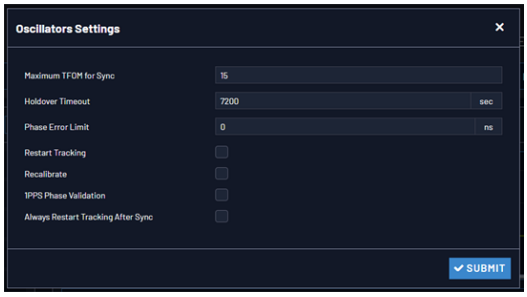
If the higher threshold value is exceeded, the **automatic failover** will cause VersaSync to fall back to its next lower reference (if available).

If no other reference is found, the unit will transition into a 1200-second coasting period. During this coasting period, the TIME and 1PPS references will continue to be considered valid, but VersaSync's oscillator will flywheel. Note that the **PPS** reference status light will turn yellow. After expiration of the 1200 seconds the unit will transition into Holdover.

Should, however, the above-mentioned higher threshold value no longer be exceeded, the unit will remain in the 1200-second flywheel mode until either (a) the lower threshold value is no longer exceeded, or (b) the 1200-second flywheel period expires. In both cases the PPS status light will turn green again.

Smart reference monitoring is OFF by default. To turn it ON:

1. Navigate to **MANAGEMENT > OTHER: Disciplining**.
2. In the **Status** panel on the left, click the GEAR icon. The **Oscillator Settings** window will open.



3. Check the box next to **1PPS Phase Validation** and click Submit.

3.3.2.2 BroadShield

What is BroadShield?

BroadShield is an optional software module for VersaSync that is capable of detecting the presence of GPS jamming or spoofing in real time.

How BroadShield Works

BroadShield monitors the GPS signal frequency band by applying proprietary error detection algorithms. If a threshold signal monitoring value level is exceeded, VersaSync will emit a Major Alarm and – depending on your system configuration – invalidate the GPS reference causing VersaSync to either transition into Holdover mode (see"Holdover Mode" on page 235), or go out of sync.

Even if you decide to turn off VersaSync's **Auto Sync Control** feature, which allows BroadShield to disable the GNSS reference, BroadShield will still add value to your overall system capability by telling you (a) if your GNSS receiver is being

spoofed, and (b) in the event of a signal loss due to jamming, *why* the signal is lost.

Also, if a normally strong GNSS signal becomes weakened, BroadShield's algorithms are capable of discerning a jamming event from natural events causing the signal to weaken.

Note: For an effective jamming detection, and – to some extent – spoofing detection, a good antenna placement with optimal sky view resulting in a high signal-to-noise ratio is essential. A strong signal is required to discern between normal signal fluctuations and a non-natural divergence of signal strength.

BroadShield Requirements

In order for BroadShield to work on your VersaSync system, the following requirements must be met:

1. The optional BroadShield software license needs to be enabled by applying the **OPT-BSH BroadShield** license key. For more information, contact your local Safran Sales Office. To determine if BroadShield has been activated on your VersaSync unit, navigate to **TOOLS: SYSTEM > Upgrade/Backup**. The center panel **System Configuration** will list the **Options** installed in your unit.

Note: After performing a clean update of the VersaSync system software, BroadShield will need to be reinstalled.

Activating the BroadShield License

If you have purchased the BroadShield license key and now want to activate it, please follow the instructions under "Applying a License File" on page 313.

To confirm that BroadShield has been activated on your VersaSync unit, navigate to **TOOLS: SYSTEM > Upgrade/Backup**. The center panel **System Configuration** will list the **Options** installed in your unit.

Enabling/Disabling the BroadShield Service

The Broadshield service can be run in two operating modes:

- **BroadShield only**: In the event jamming or spoofing is detected, VersaSync will emit a Major Alarm, however it will continue to consider the GNSS reference as valid, i.e. it will NOT go out of sync.
- **Auto Sync Control**: In the event jamming or spoofing is detected, VersaSync will emit a Major Alarm AND it will go into Holdover mode.

To configure these settings:

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

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

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

Configuring BroadShield

To configure BroadShield:

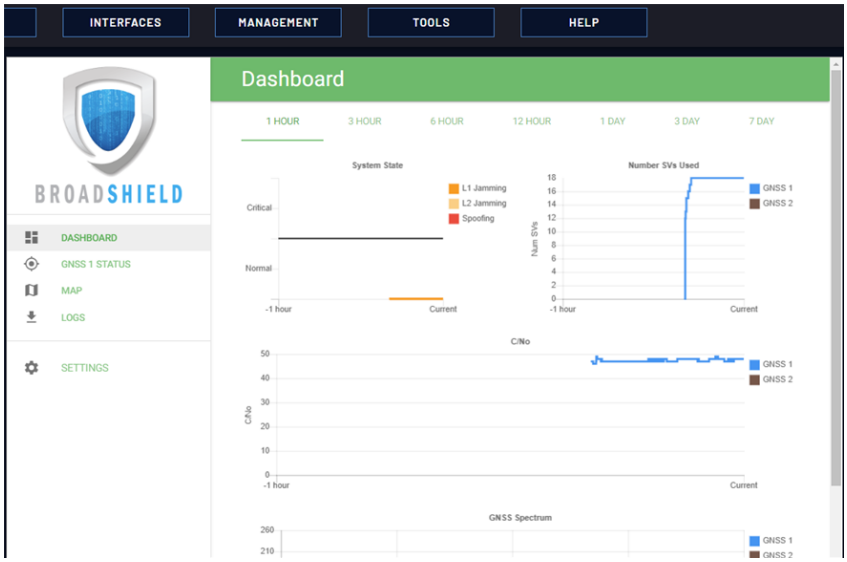
1. Navigate to **TOOLS: SYSTEM > Broadshield**. The embedded Broadshield Web UI will open. If you cannot enable Broadshield from this screen, this license is not present.
2. Click **SETTINGS** to open the following sub-menus:

BROADSIGHT

BroadSight is a service that allows collection of data from multiple BroadShield units and provides a dashboard view of the data.

Note: BroadSight for VersaSync is currently not supported.

HOME BASE



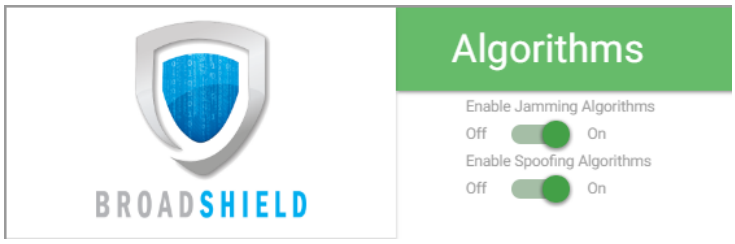
By setting the HOME BASE position you allow BroadShield to use this location as a reference position for spoofing detection: Should BroadShield detect that the geographic position reported by VersaSync's GPS receiver seems to move beyond the set **Alarm Threshold** (even though VersaSync does not move), an alarm will be triggered.

The standard use case is to make your **GNSS 1 Position** your HOME BASE:

1. Should the position fields be populated (other than the **Alarm Threshold**), click CLEAR LOCATION (this will prevent BroadShield from issuing an alarm once you SAVEd the new position.)
2. Click USE in the **GNSS 1 Position** box to apply the settings.
3. The default **Alarm Threshold** is 50 m, i.e. any detected position shift beyond a 50-m circle around the HOME BASE position will cause an alarm. You can change this setting to adjust the sensitivity.
4. Click SAVE to accept the entered values.

A less common use case may be that you want to pre-set the unit's position for later use e.g., if the VersaSync unit will be deployed in a different location: Set a position manually by entering **lat/long** (format: xx.xxxxxx degrees) and **alt**. Note, however, that this may cause a spoofing alarm, since BroadShield detects a difference between the HOME BASE position and the GNSS position.

ALGORITHMS



This menu option allows you to disaable/enable Jamming or Spoofing. **Spoofing** refers to impersonating the live- sky GNSS signal, thus "deceiving" the GNSS receiver, while **Jamming** refers to interference of the signal, i.e. making the live-sky GNSS signal unusable. Per default, both are Enabled.

ABOUT

The About menu displays Version and Build Date of the BroadShield software. Periodic updates are released with VersaSync system software updates, as they become available.

Monitoring BroadShield

You can use the BroadShield Web UI to monitor the jamming/spoofing status, or the VersaSync Web UI. In the latter case, you will be informed of a Major Alarm, as described below:

BroadShield Alarm

If BroadShield detects a jamming or spoofing event, VersaSync will emit a *BroadShield Critical, Major Alarm* (see illustration below). VersaSync will go into **Holdover** (yellow HOLD status light) and – depending on the **BroadShield Service** setting (see "Enabling/Disabling the BroadShield Service" on page 202) and your VersaSync settings – will either remain in sync (green SYNC status light), i.e. it will continue to output time and frequency signals considered valid, or it will go out of sync (red SYNC light).

You can also configure a notification alarm, see "Enabling/Disabling the BroadShield Service" on page 202.

BroadShield Web UI Monitoring

The BroadShield Web UI will also display real time signal status information, or a map status.

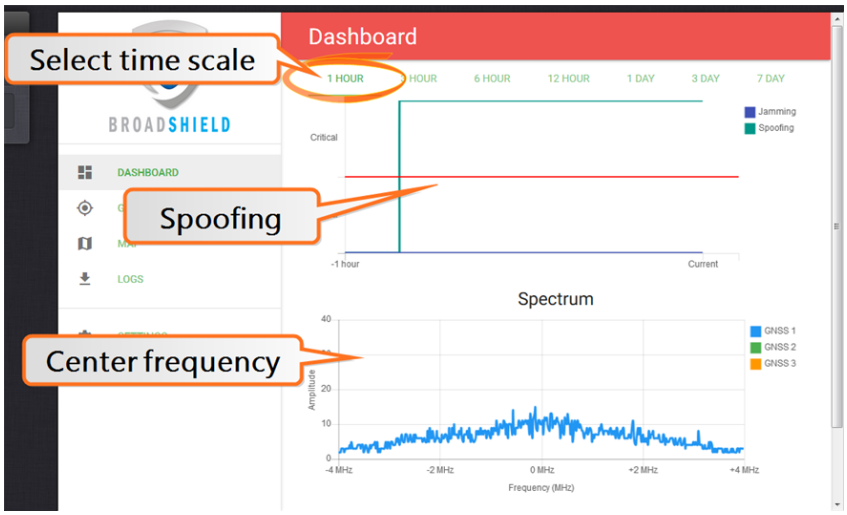
Note: If at any time you receive an error message Failed to connect to the unit, the VersaSync Web UI may have timed out (see "Web UI Timeout" on page 266). Refresh your browser page to log back in.

To open the BroadShield user interface:

1. Navigate to **TOOLS: SYSTEM > Broadshield.**
2. The embedded Broadshield Web UI will open, displaying the Dashboard and providing access to the following panels:

DASHBOARD

The Dashboard panel displays up to 7 days of history data, and a real-time amplitude frequency spectrum. The headline background color indicates the current jamming/spoofing status: red= jamming or spoofing detected; green = no alarms at this time



Top graph

The Dashboard top graph displays the past signal level over time, divided into a **Normal** and a **Critical** signal level (separated by a red line). A blue line in the **Critical** zone indicates a potential jamming incident, while a green line indicates that VersaSync may be subject to a spoofing attack.

You can change the time scale by clicking on any of the labels between 1 HOUR and 7 DAY.

Note: A VersaSync reboot will reset all history data (it can still be retrieved via LOGS.)

Bottom graph

The bottom graph labeled **Spectrum** visualizes the current signal over the GPS frequency band. Unusual amplitude spikes indicate a potential threat. If your system is equipped with more than one GNSS receivers, a green and an orange graph will indicate the signal level for additional receivers.

GNSS 1 Status

Note: The BroadShield GNSS1 reference refers to the SecureSync GNSS 0 reference.

Status information

- **GPS Time**: Time and Day as provided by VersaSync's GNSS receiver.
- **Position**: The position as determined by VersaSync's GNSS receiver.
- **Satellites Used**: The number of satellites currently received by VersaSync. This number includes all satellites currently received for all enabled constellations (see "Selecting GNSS Constellations" on page 229). Note that BroadShield uses only GPS signals for jamming/spoofing detection.
- **Average C/No**: Average signal to noise ratio. An average C/No value higher than 30 can be considered "good".

Skyplot graph

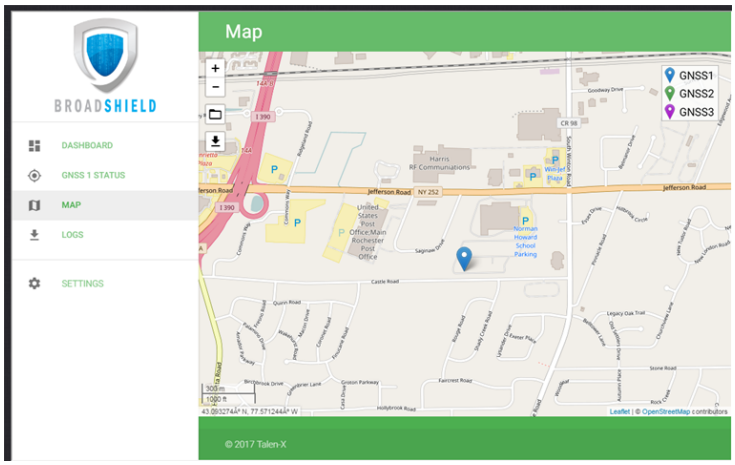
The center of the skyplot represents the antenna position. The skyplot shows all GPS satellites currently being tracked and – if enabled (under **INTERFACES: REFERENCES > GNSS Reference: GNSS 0 > Edit button > Selected Constellations**) – will also display all GLONASS satellites (numbered 65 and higher). Note, however, that GLONASS satellites will not be used by BroadShield. Galileo and Beidou satellites will not be displayed.

Note: Even though VersaSync may be configured to track multiple GNSS constellations (see "Selecting GNSS Constellations" on page 229), BroadShield only uses GPS.

Signal-to-noise bar graph

This graph visualizes the signal-to-noise ratio for up to 20 received satellites in real time. The satellites are numbered by their NMEA ID's (as in the skyplot mentioned above).

MAP



The map displays your current position, as reported by the GPS receiver. Should the displayed position differ from the actual antenna position, the GPS signal is likely spoofed.

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

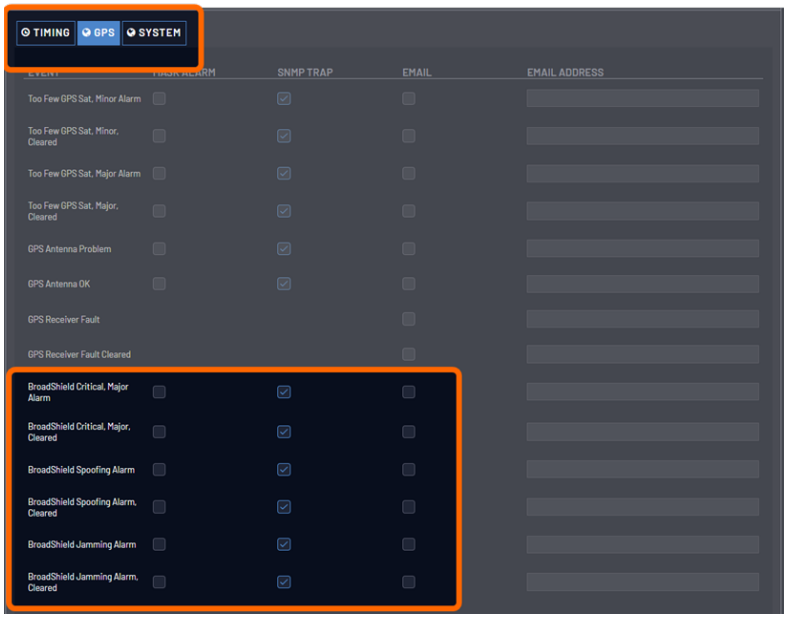
LOGS

- To clear all current logs stored on VersaSync, click **CLEAR LOGS**.
- To start a new log session, click **NEW LOG SESSION**.
- To download current logs, click **DOWNLOAD LOGS**.

Broadshield Notifications

You can setup Notifications to be sent if BroadShield detects or clears an alarm:

- Navigate to **MANAGEMENT: OTHER > Notifications**, and under the **GPS** tab, locate the two BroadShield line items. For further information on how to configure Notifications, see "Notifications" on page 249.



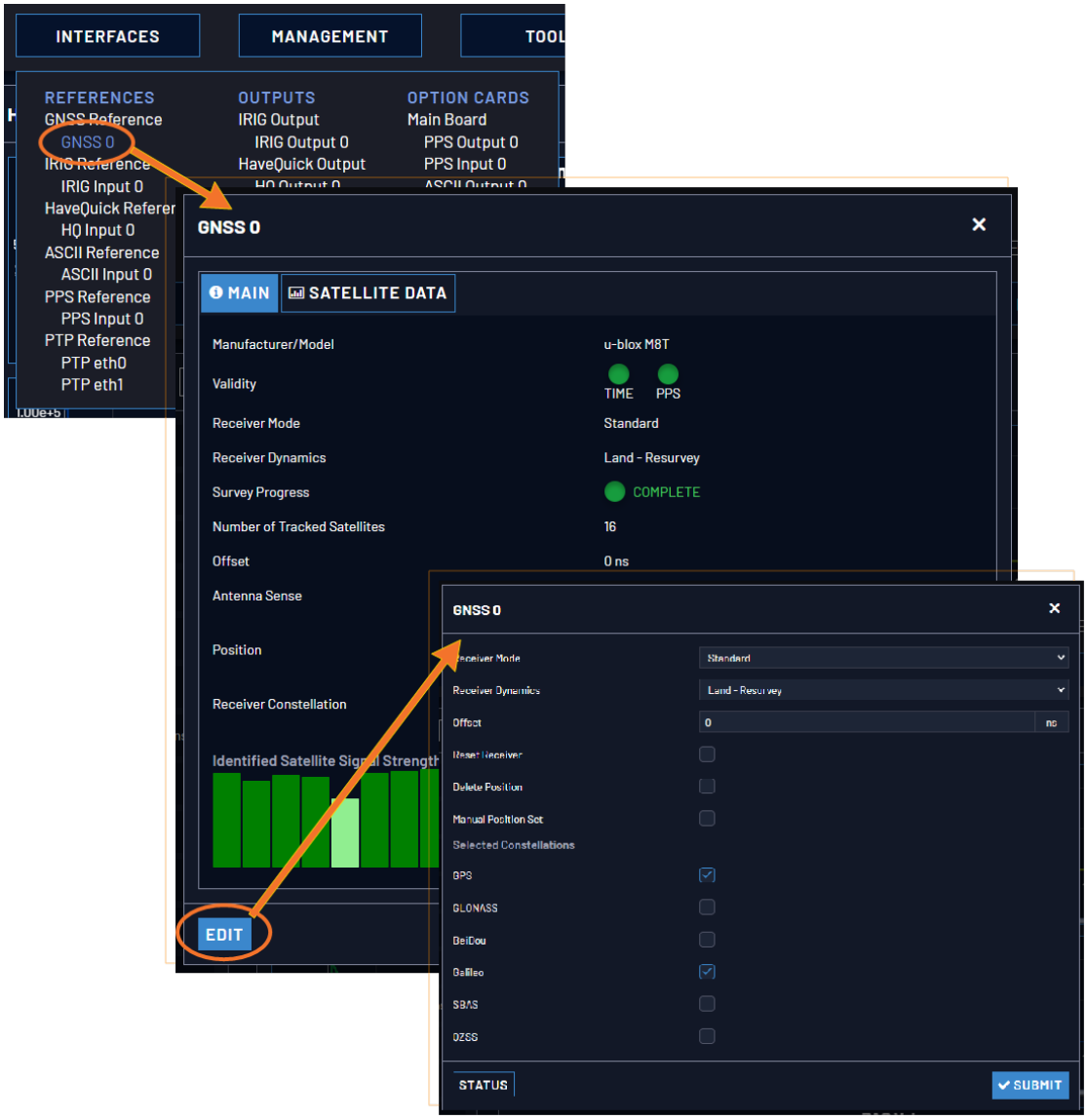
3.3.3 The GNSS Reference

With most applications, VersaSync will be setup such that it utilizes a GNSS signal as the primary (if not the only) timing reference.

VersaSync's GNSS receiver utilizes the signal provided by the GNSS antenna.

The GNSS receiver analyzes the incoming GNSS data stream and supplies the GNSS time and 1PPS (Pulse-Per-Second) signal to VersaSync's timing system. The timing system uses the data to control the System Time and discipline the oscillator.

While VersaSync's default GNSS receiver configuration will likely be adequate for most applications, it is advisable that you review the options and change settings as needed, particularly if you are experiencing poor signal reception.



To access the GNSS Receiver settings:

1. Navigate to **INTERFACES > REFERENCES: GNSS 0**.

   Note: Typically, there will be only one GNSS reference, numbered "0".

2. The **GNSS 0** status window will open. To open the configuration window, click Edit in the bottom-left corner.

OR:

1. Navigate to **INTERFACES > REFERENCES: GNSS Reference**.
2. Click on the INFO button, or the GEAR button to configure the GNSS settings, or review GNSS reference status information.

3.3.3.1 Reviewing the GNSS Reference Status

To view the current status of your GNSS reference:

1. Navigate to **INTERFACES** > **REFERENCES: GNSS Reference**.
2. Click the INFO button next to **GNSS 0**. The **GNSS 0** status window will display; it contains two tabs, explained in detail below: **Main** [= default], and **Satellite Data**.

The "Main" tab

Under the **Main** tab, the following information will display:

Note: Detailed information on the different parameters can be found in the subsequent GNSS topics.

- **Manufacturer/Model**: The manufacturer and/or model of the GNSS receiver in your VersaSync unit.
- **Validity**: Status indicator lights for **TIME** and **1PPS** signals: "**On**" (green) indicates a valid signal, "**Off**" (red) indicates that no valid signal is available. A yellow **1PPS** light indicates that the monitored 1PPS value fell below a quality threshold and the unit is in flywheel mode.

- **Receiver Mode:**
  - **Single Satellite**: Used in areas with poor GNSS reception.
  - **Standard**: Default operating mode for the GNSS receiver.
  - **Mobile**: [default] For non-stationary applications.
- **Receiver Dynamics**: (u-blox receivers only); see "Setting GNSS Receiver Dynamics" on page 219.
- **Survey Progress**: Real-time status:
  - **ACQUIRING** (x Satellites)—red
  - **SURVEYING** (x %)—yellow; remains at 1% if no satellites are in view
  - **COMPLETE**—green
- **Number of Tracked Satellites**: The number of satellites currently being tracked.
- **Offset**: As set by the user, in nanoseconds.
- **Antenna Sense**:
  - **OK** (green)
  - **Open**: Check the antenna for the presence of an open.
  - **Short**: Check the antenna for the presence of a short circuit.
- **Position**: VersaSync's geographic position by:
  - **Latitude**: In degrees, minutes, seconds
  - **Longitude**: In degrees, minutes, seconds
  - **Altitude**: In meters MSL (Mean Sea Level)
- **Receiver Constellation**: GPS/GLONASS/Galileo/BeiDou/SBAS/QZSS
- **Client A-GPS Status**: A-GPS is ENABLED and running, or DISABLED
- **Client A-GPS Data**: External A-GPS data is AVAILABLE, or UNAVAILABLE
- **Server A-GNSS Status**: The Rinex Server feature is ENABLED and running, or DISABLED
- **Server A-GNSS Data**: A-GPS data is AVAILABLE and can be downloaded by clients, or it is UNAVAILABLE
- **Identified Satellite Signal Strengths**: Bar graphs for all satellites detected. Color indicates signal strength.
  With your mouse pointer, hover over a bar graph to display tool tip information about satellite constellation, satellite number, and signal strength.

Letter Symbol	GNSS Constellation
G	GPS
R	GLONASS
E	Galileo
J	QZSS
C	BeiDou
I	IRNSS

The "Satellite Data" tab

Under the **Satellite Data** tab, there are two graphs:

- **Number of Satellites over Time**: A graphical track of how many satellites were being tracked over time.
- **SNR over Time**: A graphical track of maximum SNR, and minimum SNR.

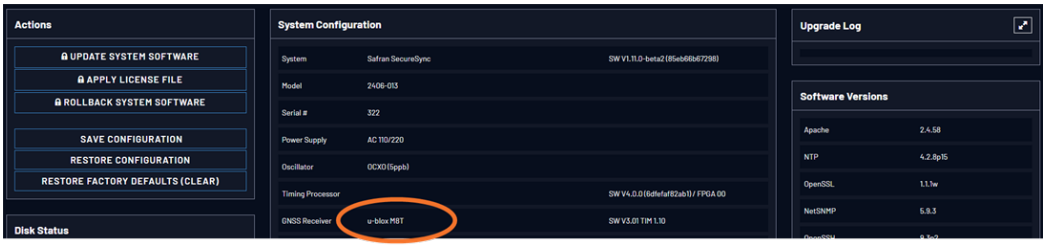
In both graphs, to see a legend of the graphical data, and time-specific status data, click inside the graph, choosing the desired point in time. If necessary, increase the time resolution by dragging the time sliders. A pop-up window will display the legend for that graph, and the status information for the selected time.

3.3.3.2 Determining Your GNSS Receiver Model

Note: All VersaSync models are currently shipped with a u-blox M8T Receiver.

To determine which GNSS receiver model is installed in a VersaSync unit:

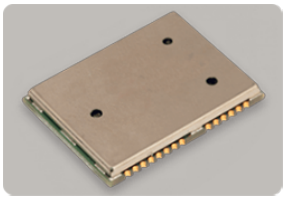
1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. In the **System Configuration** panel, locate the line item **GNSS Receiver**:



GNSS Receiver Models

Safran strives to equip VersaSync with current technology. Depending on the production date of your VersaSync unit, one of the following GNSS receiver models will be installed in your unit (if any):

u-blox® M8T



Production dates: Since 2016

Constellations: GPS, Galileo, GLONASS, BeiDou, QZSS

Other characteristics:

- **Client A-GPS** option: Yes
- **Server A-GNSS** option: Yes
- **Resurvey**: Automatic, after being moved and rebooted — can be changed, see "Setting GNSS Receiver Dynamics" on page 219.
- **Multi-GNSS** reception: Yes, within these permissible settings:

GPS	Galileo	GLONASS	Beidou
X	X	–	–
X	X	X	–
X	X	–	X

GPS	Galileo	GLONAS-S	Beido-u
X	–	X	–
X	–	–	X
–	X	X	–
–	X	–	X
–	–	X	X

Note: The augmentation systems SBAS and QZSS can be enabled only if GPS operation is configured.

3.3.3.3 Selecting a GNSS Receiver Mode

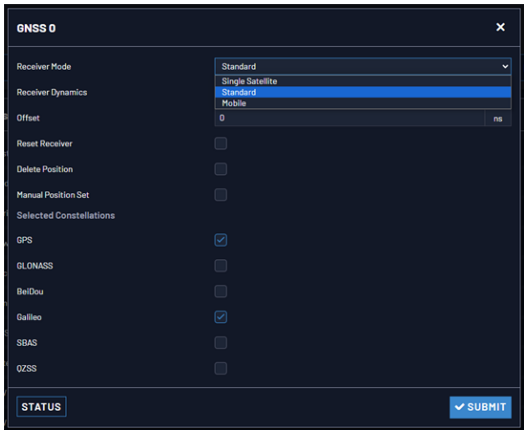
When connected to a GNSS antenna that receives a GNSS signal, VersaSync can use GNSS as an input reference. The factory default configuration allows GNSS satellites to be received/tracked with no additional user intervention required.

However, there are several user-configurable GNSS settings:

- The **Receiver Mode** function allows the GNSS receiver to operate in either a stationary mode ("**Standard**" or "**Single Satellite**" modes), or in a mobile mode environment e.g., in a vehicle, ship or aircraft.
- **Offset** [ns]: to account for antenna cable delays and other latencies
- **Receiver dynamics**: to optimize performance for land, sea or air operation
- The ability to **delete** the stored GNSS position information (latitude, longitude and antenna height).
- The option to determine when a **resurvey** is to be performed (supported only by newer GNSS receivers).
- The option to select your constellation types

To configure the GNSS Receiver Mode for your VersaSync unit:

1. Navigate to **INTERFACES > REFERENCES**: **GNSS 0**. The **GNSS 0** Status panel will open.
2. Select **Edit** in the bottom-left corner. The **GNSS 0** configuration window will open:



3. Select the desired Receiver Mode, and click **Submit**.

GNSS Receiver Modes

The receiver modes are:

- **Mobile Mode**: This is the default mode for VersaSync. In Mobile Mode, GNSS surveys (see below) will NEVER be carried out since the position status is updated in near real-time. VersaSync will go into synchronization shortly after beginning to track satellites.
- **Standard Mode**: While the Standard Mode tends to be the most accurate GNSS Receiver Mode, it can only be used for stationary applications, i.e. the VersaSync unit must not be moved. In Standard Mode the so-called **GNSS survey** will be performed as soon as at least four GNSS satellites become available and no previously carried out survey was found. Upon completion of the survey the GNSS receiver will lock-in the calculated position and will enter Standard Mode. Once the survey is completed, less than four satellites will provide a valid Time and 1PPS signal.
- **Single Satellite Mode**: This mode is designed for stationary applications which cannot track at least four GNSS satellites for at least 33 minutes continuously in a 12-hour time window so as to complete the GNSS survey. This occurs frequently in areas with limited view of the sky (e.g., "urban canyons").

  In Single Satellite Mode, the GNSS receiver will be considered a valid input reference as long as:

  - you have manually entered a valid position for your antenna location (instructions can be found under "Manually Setting the GNSS Position" on page 226 and "Determining Your Position" on page 228).
  - the GNSS receiver continues to track at least one qualified satellite.

Note: VersaSync is designed to provide the most accurate time in Standard Mode. The Single Satellite Mode should only be used if the GNSS receiver could not complete a survey.

3.3.3.4 Setting GNSS Receiver Dynamics

Receiver Dynamics further refine the reception characteristics for the individual receiver modes and determine if the receiver will automatically resurvey after a reboot.

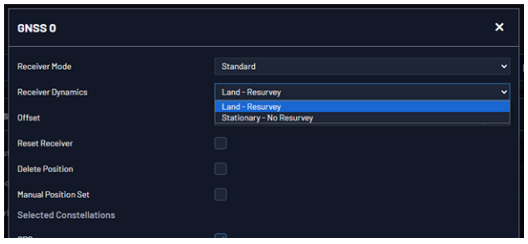
Caution: If you select a setting that does NOT resurvey, and subsequently relocate your unit (antenna) by more than 100 m, u-blox M8Treceivers will NOT detect the new position, and hence provide an incorrect time.

For more information about the **GNSS Survey**, see "Performing a GNSS Receiver Survey" on page 222.

For more information on **Receiver Modes**, see "Selecting a GNSS Receiver Mode" on page 217.

To change/review the GNSS Receiver Dynamics:

1. Navigate to **INTERFACES > REFERENCES: GNSS 0**.
2. Under the **Main** tab of the GNSS 0 status window, the line item **Receiver Dynamics** will indicate the current setting.
3. To change the setting, click Edit in the bottom-left corner. The GNSS 0 configuration window will display:



4. Select a setting and click Submit.

Available GNSS Receiver Dynamics Settings

» **Note:** This option only applies to the M8T receiver in your device, not to SAASM GPS receivers (if equipped).

Caution: If you select a setting that does NOT resurvey, and subsequently relocate your unit (antenna) by more than 100 m, the receiver will NOT detect the new position, and hence provide an incorrect time.

The following Receiver Dynamics exist:

- **Land (Resurvey/No Resurvey)**:
  When used with the Mobile Receiver Mode, the receiver is adjusted for typical dynamic land-based applications.

  When used with the Standard Receiver Mode, this setting also will automatically initiate a resurvey after VersaSync reboots, in order to account for a possible relocation.
- **Sea**: The receiver dynamics will be optimized for mobile motion patterns typical with marine applications, resulting in greater timing accuracy, and avoiding premature loss of synchronization.
- **Air**: The receiver dynamics will be optimized for acceleration forces typically experienced in civil aviation applications.
- **Stationary (No Resurvey)**: In Standard Mode, the receiver is set to a non-dynamic value for stationary applications; there will be no automatic resurvey after a reboot. Hence, should a unit be relocated, you need to delete its position, thus initiating a new survey.

The following table summarizes the different settings and their interdependencies:

Mode	Application	Survey?	(Re-)Survey – When?	Receiver Dynamics
Mobile	mobile	Never	Never	Land Air Sea

Mode	Application	Survey?	(Re-)Survey – When?	Receiver Dynamics
Standard	stationary only	Yes: needs ≥ 4 satellites for 33 minutes continuously in 12-hour window	(A) After any reboot, if the Dynamics setting is set to "Land – Resurvey". (B) If no previously carried out survey has been found after a reboot (C) When the unit detects it has been re- located (D): After "Delete Position" command was submitted	Land – Resurvey Stationary – No Resurvey
Single Satellite	stationary only	Manually set position	(A) On reboot, if no hand-set position is detected (B) After "Delete Position" command was submitted	Stationary

The following table illustrates the interdependence between Receiver Dynamics, Receiver Mode (see "Selecting a GNSS Receiver Mode" on page 217) and receiver type:

Table 3-2: Receiver dynamics, ~modes, ~ dynamics, ~ types

Receiver Mode	Receiver Dynamics			
	Land (Resurvey)	Sea	Air	Stationary (No Resurvey)
Single Satellite	irrelevant	irrelevant	irrelevant	irrelevant
Standard	✓	✗	✗	✓
Mobile (with u-blox receivers)	✓	✓	✓	✗

Notes:

» The **u-blox M8T** receiver now uses Land to indicate it will RESURVEY on reboot, and Stationary to indicate it will not resurvey after reboot.

3.3.3.5 Performing a GNSS Receiver Survey

Note: This topic only applies to stationary applications – in Mobile receiver mode NO surveys will be carried out since the position is updated continuously.

When VersaSync's integrated GNSS receiver performs a survey, it tries to determine or verify its geographic position with high accuracy. An accurate geographic position is required to calculate a precise system time from the GNSS reference.

During a GNSS survey, the position will be iteratively recalculated while gradually increasing the position accuracy. A survey can take up to 33 minutes, but typically VersaSync will synchronize earlier, i.e. offer a valid Time and 1PPS reference, once it has obtained a sufficiently accurate preliminary position.

Note: If a system has been moved, in Standard receiver mode and Land Dynamics, receivers will automatically re-survey on reboot. In Standard mode and Stationary Dynamics, the unit will survey only once, and will not re-survey on reboot.

Initiating a GNSS Survey

The standard behavior is that a power cycle or a reboot will automatically initiate a GNSS survey. To reboot your unit, navigate to **TOOLS > SYSTEM: Reboot/Halt**.

While it is crucially important to carry out a resurvey after a unit has been relocated (e.g., when commissioning a new unit), a resurvey is normally not required if a stationary unit is rebooted for other reasons. To turn off this functionality, see "Setting GNSS Receiver Dynamics" on page 219.

Verifying GNSS Survey Progress

To see if VersaSync's GNSS receiver is performing a survey and if so, verify its progress:

1. Navigate to **INTERFACES > REFERENCES: GNSS 0**.
2. The survey status (ACQUIRING, COMPLETE, or progress in percent) is displayed under the line item Survey Progress.

Note: Once a survey has been initiated, the Survey Progress may not be displayed right away until the receiver has completed its initialization process.

3.3.3.6 GNSS Receiver Offset

The **Offset** setting in the GNSS configuration window (**INTERFACES** > **GNSS 0** > "**Edit**") allows you to enter an offset to the GNSS time and 1PPS reference in order to account for antenna cable delays or other latencies (entered and displayed in nanoseconds).

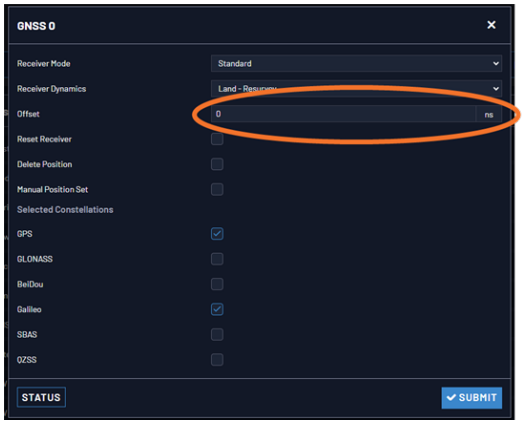
By setting the correct **Offset** value, you can offset the system's on-time point by the **Offset** value to compensate for the antenna and in-line amplifier delays. Under typical conditions, the expected cable and amplifier delays are negligible. You can calculate the delay based on the manufacture's specifications.

The offset range is ±½ seconds (i.e. ±500 ms, or ±500 000 000 ns). The default value is 0 nanoseconds, and the resolution is 1 nanosecond.

Configuring a GNSS receiver offset

To configure the GNSS receiver offset:

1. Navigate to **Interfaces > References: GNSS Reference**
2. Click on the GEAR button next to the GNSS Reference. The **GNSS 0** window will open:



3. Locate the **Offset** field, and enter the desired value.
4. Click Submit.

Calculating cable delay

The following formula can be used to calculate antenna 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 Safran **LMR-400** or equivalent coaxial cable, this formula equates to approximately 1.2 nanoseconds of delay per every foot of cable. To calculate the Offset value (cable delay), multiply the length of the entire cable run by "1.2" and then enter this value into the Offset field.

Examples of LMR-400 (or equivalent) coax cable delays:

100 feet of cable = 120 nanoseconds of cable delay

200 feet of cable = 240 nanoseconds of cable delay

300 feet of cable = 360 nanoseconds of cable delay

3.3.3.7 Resetting the GNSS Receiver

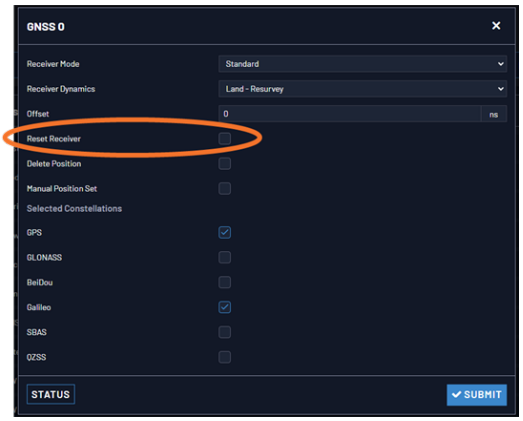
The **Reset Receiver** command causes the GNSS receiver to execute a cold start: All data will be erased from the volatile receiver memory. Only non-volatile memory is preserved.

Caution: Resetting the GNSS receiver may become necessary in the rare event of internal communication issues, and is typically ONLY required if Safran Technical Support advises you to execute this command.

Note that resetting the GNSS receiver is not the same as "Deleting the GNSS Receiver Position" on the facing page.

To reset the GNSS Receiver:

1. Navigate to **Interfaces > References: GNSS Reference**
2. Click on the GEAR button next to the GNSS Reference. The **GNSS 0** window opens:



3. Locate the **Reset Receiver** box, check it, and click Submit.

3.3.3.8 Deleting the GNSS Receiver Position

The VersaSync timing system requires the exact geographic position in order to calculate the exact system time from the GNSS signal.

The **Delete Position** command deletes the GNSS antenna position data that is stored in the non-volatile memory of the GNSS receiver.

The deletion of the position data will automatically initiate a new **GNSS self survey**, provided:

- a GNSS antenna is connected to VersaSync
- the GNSS receiver can track at least four satellites continuously
- and the GNSS receiver it is configured to operate in **Standard Mode**.

The objective of the **GNSS Survey** is to re-discover the current antenna position.

Note: A self survey will take at least 2000 seconds (33 minutes).

Relocating VersaSync

The **Delete Position** command may need to be used if a VersaSync system is physically moved, and it did not self-initiate a new survey automatically. Note that neglecting to delete the old position data and discover the new position data will cause VersaSync not to go into synchronization state.

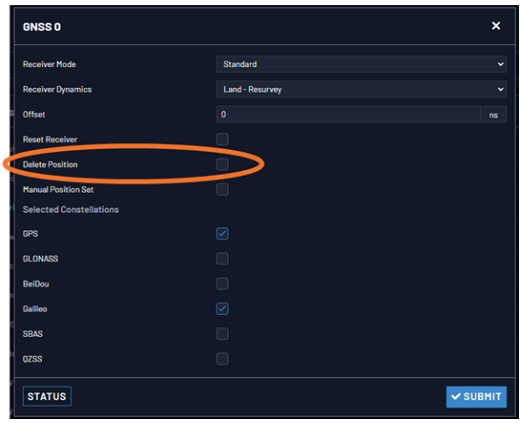
Sanitization

The **Delete Position** command is automatically applied when **sanitizing** a VersaSync unit (ensuring that no trace of position data remains on the unit). See "Sanitizing the Unit" on page 322.

Deleting the GNSS position

To delete the GNSS position:

1. Disconnect the GNSS antenna from the VersaSync unit (this is required **only when sanitizing** the unit).
2. Navigate to **Interfaces > References: GNSS Reference**.
3. Click on the GEAR button next to the GNSS Reference (typically, there is only one reference, numbered "0"). The **GNSS 0** window will open:



   Locate the **Delete Position** box, check it, and click Submit.

4. VersaSync will initiate a GNSS self survey.

Note: In Mobile Receiver Mode it is NOT possible to delete the position and start the GNSS survey. This feature is only available in Standard Mode and in Single Satellite Mode. In Single Satellite Mode a GNSS survey may take up to 24 hours.

3.3.3.9 Manually Setting the GNSS Position

Note: This topic applies only to stationary applications, i.e. to Standard mode, or Single Satellite mode.

The exact geographic position (location and elevation) of the antenna your VersaSync unit—and thus its onboard GNSS receiver—is a major factor for VersaSync to calculate an accurate System Time from the GNSS reference.

Note: The elevation (altitude) should be set in accordance with the World Geodetic System 1984 (WGS 84), not Mean Sea Level (MSL).

Normally, the onboard GNSS receiver will track and adjust the antenna position during the so-called GNSS **self survey**, which is performed during initial commissioning of a VersaSync unit, or when rebooting a unit after it had been powered down for some time ("cold start").

Depending on where your GNSS antenna is installed and thus, how good the reception is, the self survey may be adequate for most applications.

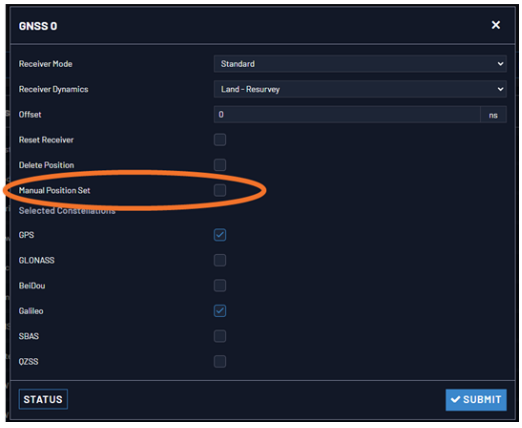
Setting a **Manual Position**, however, i.e. manually applying your current geographic position data (Latitude, Longitude, and Altitude) may be necessary if your GNSS receiver could not complete its survey due to poor reception.

In some cases, setting the position manually may also help to reduce the amount of time needed for the initial position "fix", i.e. for VersaSync to synchronize with the satellites in view.

Note that this position will also be used if **Apply A-GPS Data** is checked.

To manually set your position:

1. Determine your geographic position. For more information, see "Determining Your Position" on the next page.
2. Navigate to **INTERFACES > REFERENCES: GNSS 0**. In the **GNSS 0** status window, click **Edit** in the lower left corner. The **GNSS 0** window will open:



3. Under **Manual Position Set** accurately enter **latitude**, **longitude** (both in decimal degrees), and **altitude** (in meters [WGS 84]) of your GNSS

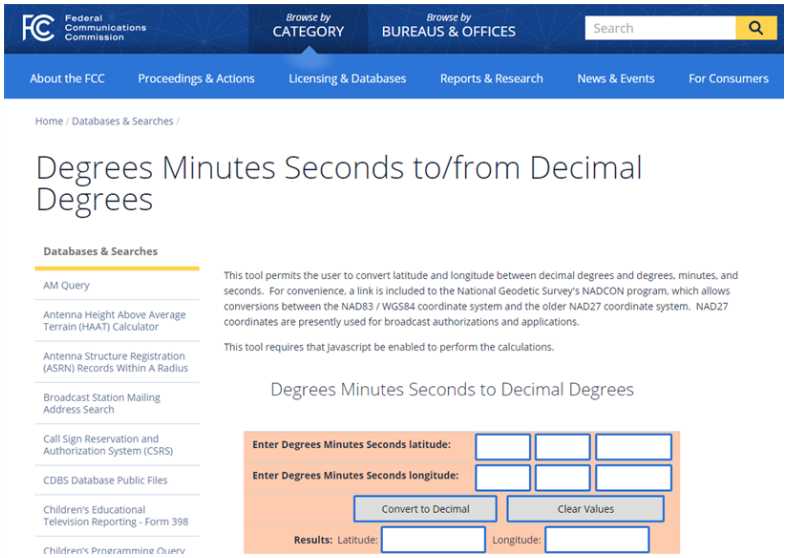
antenna, VersaSync can use this data during the satellite tracking/adjustment process, which typically leads to a quicker "fix". It is recommended to enter the position as accurately as possible.

Determining Your Position

To determine your GNSS position, using Google Maps™:

1. On your computer, open Google Maps.
2. In Google Maps, locate your building, and the location of your antenna.
3. Right-click on the location. Select **What's here?** At the bottom, you will see a card with the coordinates.
4. Take note of your **decimal** position (e.g., 43.083191, -77.589718).

> **Note:** Should you prefer to determine your position in a different way, and as a result, have your latitude & longitude data in degrees/minutes/ seconds, you need to convert this data to the decimal format e.g., by using a conversion tool, such as Earth Point www.earthpoint.us, or https://www.fcc.gov/media/radio/dms-decimal:



5. Determine your **altitude**: To find the elevation of your location, search online for a *Google Maps elevation finder* tool. Do not forget to add the height above ground for your antenna.

If a more exact altitude is desired, the use of a topographical map is recommended. Applying the WGS 84 standard will likely yield the most accurate elevation.

3.3.3.10 GNSS Constellations

VersaSync allows you to select which GNSS constellations can be tracked. For example, you can determine if you want GLONASS satellites to be tracked (besides GPS).

Selecting GNSS Constellations

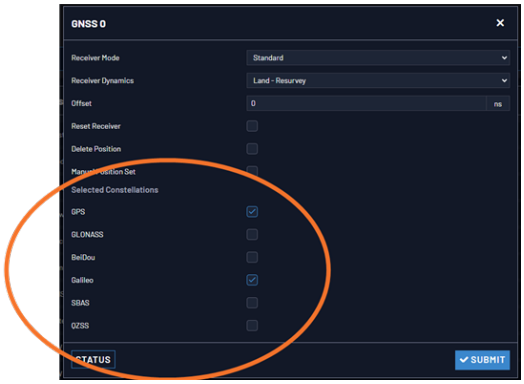
Your VersaSync is capable of tracking multiple GNSS constellations simultaneously.

To verify if satellite signals for the selected GNSS constellations are currently received, see "Determining Which GNSS Satellites Are Received" on the next page.

Configuring GNSS Constellations

To configure which GNSS constellations VersaSync's GNSS receiver shall track:

1. Navigate to **INTERFACES > REFERENCES: GNSS Reference**.
2. Click the GEAR button next to **GNSS 0**. The **GNSS 0** window will open:



3. Under **Selected Constellations**, review which constellations are currently tracked, and apply your changes. Note the following:
   - The **u-blox M8T** receiver is capable of receiving multiple GNSS constellations simultaneously; the table below shows which combinations are possible:

GPS	Galileo	GLONASS	BeiDou
X	X	-	-
X	X	X	-
X	X	-	X
X	-	X	-
X	-	-	X
-	X	X	-
-	X	-	X
-	-	X	X

Note: The augmentation system SBAS and QZSS can be enabled only if GPS operation is enabled.

Note: Should you select more than 3 + QZSS constellations, you will receive a Constellation Error once you click Submit (ConstError).

About QZSS

QZSS is enabled by default if GPS is enabled. To avoid cross-correlation issues, u-blox recommends that GPS and QZSS are always both enabled or both disabled. While it is possible to enable GPS without QZSS, the reverse is not recommended and not possible through the Web UI.

QZSS is not considered a standalone, global system, but is instead a regional system (Japan). You must be located in Japan (or using a GNSS simulator) to properly receive QZSS signals.

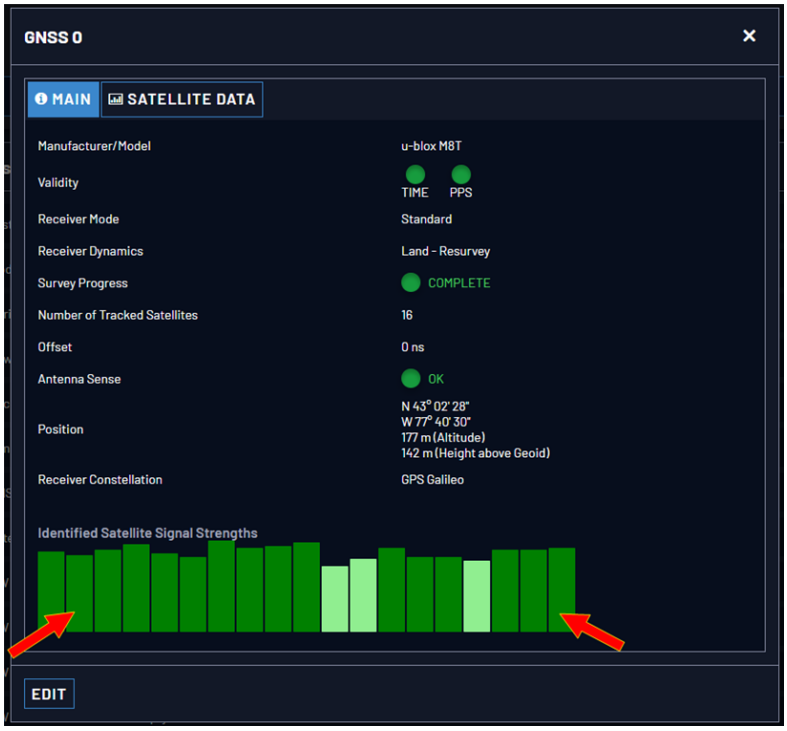
About SBAS

Satellite Based Augmentation Systems (SBAS) is an augmentation technology for GPS integrity. To use SBAS correction, you must enable GPS tracking.

Determining Which GNSS Satellites Are Received

To see which GNSS satellites your VersaSync is currently receiving:

1. Navigate to **INTERFACES > REFERENCES: GNSS 0**.
2. The **GNSS 0** status window will open:



3. Under **Identified Satellite Signal Strengths** hover with your cursor over the bars: The letter in the tooltip window displayed for each signal bar indicates which constellation the satellite belongs to:

Letter symbol	GNSS Constellation
G	GPS
R	GLONASS
E	Galileo
J	QZSS
C	BeiDou
I	IRNSS

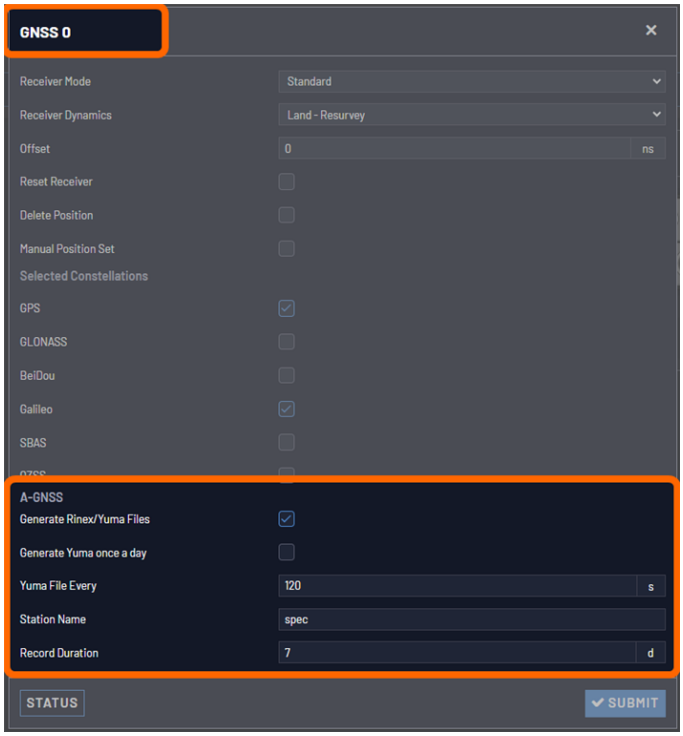
The number next to the letter indicates the satellite number. The number below indicates the signal strength (C/N_o).

3.3.3.11 AGNSS

An **A-GNSS server** allows a VersaSync unit to operate as a server, thus providing A-GNSS ephemeris and almanac data to other client devices e.g., a Safran GSG-8 series GNSS simulator.

To review or configure VersaSync AGNSS settings:

1. Navigate to **INTERFACES: REFERENCES > GNSS Reference**. The GNSS screen will be displayed.
2. In the **GNSS Reference** panel on the right, click the GEAR button next to **GNSS 0**.
3. In the **GNSS 0** window, locate the **AGNSS** panel at the bottom.



Note: The options displayed on your screen depend on your system configuration.

Generate RINEX/YUMA Files

If the option RINEX Server License (**OPT-AGP**) and a **u-blox M8T** GNSS receiver are installed on your VersaSync, it can be operated as an **A-GNSS server** by providing you the option to select not just GPS, but also Galileo, GLONASS,

and/or BeiDou, thus allowing the collection of RINEX3 navigation files and almanac files for the GPS, Galileo, GLONASS, and/or BeiDou constellations.

Based on accessible and valid GNSS data, VersaSync generates its own ephemeris and almanac data, and stores it in RINEX files and YUMA files, respectively.

Note: RINEX files (ephemeris data) must be updated no later than every 2 hours, because the ephemeris data is valid for 4 hours.

You can also determine how often, or at what time each day the YUMA almanac files will be created. Also, you can assign a 4-character **Station Name** to be used in the files generated by this unit so that their location can later be identified. Under **Record Duration**, you can determine after how many days the history files will be overwritten.

Note: YUMA files (almanac data) are valid for day.

The files can be remotely accessed via the `/home/spectracom/xfer/agnss` path on the VersaSync or via the mapped drive.

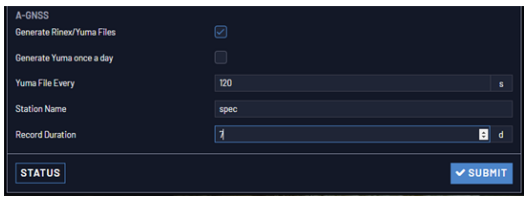
Confirming that the AGNSS RINEX Server License is installed on your unit

» Navigate to **TOOLS** > **SYSTEM: Upgrade/Backup**. In the **System Configuration** panel the option **OPT-AGP A-GPS RINEX Server** must be present.

Activating the A-GPS RINEX Server License functionality

If an A-GPS RINEX Server License is installed on your unit, you have to activate it:

1. Navigate to **INTERFACES** > **GNSS Reference**, and click the GEAR button next to **GNSS 0**.
2. In the **AGNSS** panel, check the box **Generate RINEX/YUMA Files** and populate the following options:



- **Generate YUMA once a day**:
  - If checked [default], enter the desired-time-of-day in the field **YUMA File At** [default = 12:00].
  - If unchecked, determine how often a YUMA file is generated under **YUMA File Every** [default=10 s; range = 10 s to 86400 s (1/day)].
- **Station Name**: Enter an alphanumeric 4-letter station name for the server [default: `spec`]. The names of the files generated will include the station name.
- **Record Duration**: Determine the duration for how long to keep the generated data before it gets overwritten [default: 7 days; range = between 2 and 400 days]

3. Click **Submit** to start logging ephemeris and almanac data.
4. Once you submitted the changes, verify that the setup was successful by clicking on **Status**, and confirming that the indicator lamp for **Server A-GPS Status** is green/ENABLED. The **Server A-GPS Data** indicator will be green if the RINEX server is running and the GPS receiver is valid in time and PPS.

Downloading RINEX/YUMA data

Any device that can use RINEX data, can be directed to the locations where they are stored. For example, Safran's GSG-series GNSS simulators allow for a server location to be set. With other equipment, you can also download the data to your computer, and then move the files to where they are needed.

To download the data to a client computer, point your computer's web browser to the following address:

- For hourly ephemeris data:

http:// [IP address of your unit]/home/spectracom/xfer/agnss/gps/data/hourly/ [YYYY]/ [ZZZ]/hour[ZZZ]0.15n.Z

- For daily ephemeris data:

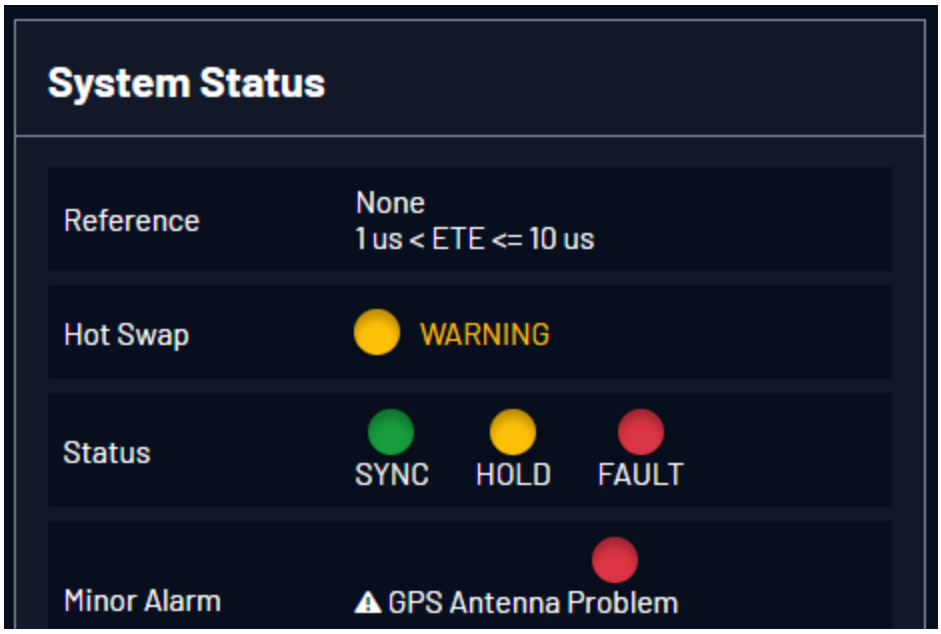
http:// [IP address of your unit]/home/spectracom/xfer/agnss/gps/data/daily/ [YYYY]/ [ZZZ]/15n/spec[ZZZ]0.15n.Z

- For almanac data:

http:// [IP address of your unit]/home/spectracom/xfer/agnss/gps/data/almanac/ [YYYY]/ [ZZZ]/[ZZZ].alm

Where: **YYYY**: Year (Example: "2017"), and **ZZZ**: Day of year (Example: "050" for 19-February)

3.3.4 Holdover Mode



When input references have been supplying input to VersaSync and input from all the references has been lost, VersaSync will not immediately declare loss of time synchronization, but first will go into Holdover mode. While the unit is in Holdover mode, the time outputs are derived from the internal 10 MHz oscillator incrementing the System Time, but the oscillator is not disciplined/steered by the external reference e.g., GNSS.

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.

While VersaSync is in Holdover, the only difference is the Holdover and associated Minor alarm are asserted. There are no changes to NTP or any of the other outputs, i.e. while in Holdover mode, NTP inside VersaSync continues to be at the same Stratum level it was at before going into Holdover mode (such as Stratum 1 when synced to GPS). Should the Holdover period expire, however, or the unit is rebooted, the NTP Stratum will go to 16, preventing any clients from being able to sync with VersaSync until GPS or another reference has been restored.

How long will the unit remain in Holdover mode?

VersaSync will remain in Holdover mode until either:

a. Any enabled and valid input reference becomes available again: If one or more references return and are declared valid before the Holdover period has expired (even momentarily, i.e. for at least one second), VersaSync exits the Holdover mode and returns to its fully synchronized state.

b. The Holdover Timeout period expires. In this case, VersaSync will declare loss of synchronization.

Note that Holdover mode does not persist through reboots or power cycles. If a reboot or power cycle occurs while VersaSync is in Holdover mode, it will power-up and remain in a "not synchronized" state until at least one valid Time and 1PPS input reference becomes available again. While in this state, NTP will be **Stratum 15** and outputs will not be usable. If the input references are restored and then lost or declared not valid again, VersaSync will then go back into Holdover mode.

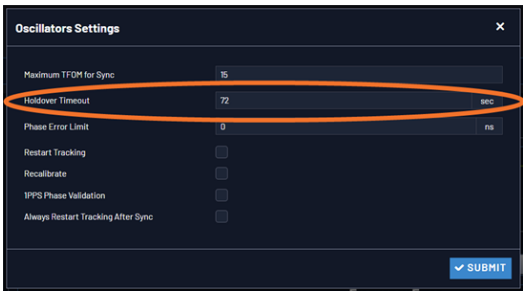
What is "Holdover Timeout"?

Holdover Timeout is the user-configurable allowable time period in which VersaSync remains in Holdover mode before it declares loss of synchronization. Holdover Timeout can be adjusted according to application-specific requirements and preferences. See below for recommendations on how long (short) the Holdover Timeout should be.

How to configure Holdover Timeout

To set the Holdover Timeout value:

» Navigate to **MANAGEMENT > OTHER: Disciplining**, and click the GEAR icon in the **Status** panel:



For more information on the TFOM value and Phase Error Limit, see "Configuring the Oscillator" on page 239.

Note: Changes made to the Holdover Timeout always take effect immediately. If VersaSync is in Holdover and the Holdover timeout is changed to a value that is less than the current time period that VersaSync has been in Holdover Mode, the unit will immediately declare loss of synchronization.

What is the recommended setting for the Holdover Timeout period?

The factory **default** Holdover period is **2 hours (7200 seconds)**. The value can be increased to up to 5 years. During this time period, VersaSync will be useable by its NTP clients (or other consumers) after GNSS reception has been lost.

The length of time is really based on the type of oscillator installed in a unit, and what the typical accuracy requirements are for the NTP clients. The longer it can run in Holdover mode before it expires, the longer it can continue being a central time source for all of its clients. But the longer VersaSync runs in Holdover, the larger the offset to true UTC time will become, because the undisciplined oscillator will drift over time:

The better the type of oscillator installed, the more stable it is while in Holdover and therefore, the less its time will drift away from true UTC time. This results in more accurate timing, over extended durations upon the loss of GPS input. For instance, a Rubidium oscillator will maintain significantly better time over a longer Holdover duration than a TCXO oscillator (TCXOs are considerably less stable than a Rb oscillator).

Oscillator Phase Drift

The chart below provides typical stability performance for the oscillator types that can be found in VersaSync units. These numbers are based on the oscillator being locked to a reference for two weeks, but then loses GPS reception for an extended period of time, while the ambient temperature remains stable.

This data can help you determine how long of a Holdover period can be tolerated, based on how much time drift may occur after GPS input is lost. The larger the time error that can be tolerated by VersaSync clients, based on the oscillator installed, the larger the Holdover timeout period can be set to.

Table 3-3: Estimated Phase Drifts

1PPS Phase Drift in Holdover (no reference available)	OCXO	OCXO (high performance)	CSAC
- 4 hours	3 µs	2.8 µs	1µs
- 24 hours	40 µs	30 µs	7 µs

1PPS Phase Drift in Holdover (no reference available)	OCXO	OCXO (high performance)	CSAC
- 7 days	1.2 ms	0.6 ms	100 µs

To find out which type of oscillator is installed in your VersaSync, navigate to **MANAGEMENT > OTHER: Disciplining**, and look for the line item **Oscillator Type** in the **Status** panel.

Typical Holdover lengths

The length of the allowed Holdover Timeout period is displayed and configured in seconds. The table below provides example conversions for typically desired Holdover periods.

Table 3-4: Typical Holdover lengths in seconds

Desired Holdover Length	Holdover Length (in seconds) to be entered
2 hours	7200 seconds (default value)
24 hours	86 400
7 days	604 800
30 days	2 419 200
1 year	29 030 400

Note: Due to Leap Seconds that are periodically inserted into the UTC and Local timescales, it is not normally recommended to exceed 30 days of Holdover without an external reference that can supply Leap Second information being applied (such as GNSS).

Configuring a Holdover value exceeding 30 days could result in a one-second time error in the UTC or Local timescales until an external reference (GNSS or IRIG input) is restored or a manually configured Leap Second is asserted by a user (leap seconds do not affect the GPS and TAI time scales).

If no external references (such as GNSS or IRIG) are available when a Leap Second is scheduled to occur, manual Leap Seconds can also be applied to the UTC or Local time base; see "Leap Seconds" on page 181.

If the Holdover Timeout has expired, do I need to reset the clock once GPS becomes available again?

No, the Holdover timer is automatically reset as soon as at least one reference has been restored/returned for at least one second. If GPS is restored and then

lost again moments later, the Holdover timer starts again with its full value. If its set to one week in this case, it then gets another week of Holdover operation before NTP goes to Stratum 16 (if GPS remained unavailable for the entire week).

Holdover mode and the User/User reference

If the only available input reference is a manually set **User** time, and VersaSync is subsequently rebooted or power cycled, time sync will be lost when VersaSync powers back-up. The time will need to be set manually again in order for VersaSync to return to its fully synchronized state. See "The "User/User" Reference" on page 194 and "Manually Setting the Time" on page 177 for more information.

3.4 Managing the Oscillator

The purpose of the built-in oscillator is to provide VersaSync with an accurate and very stable internal frequency source. This allows VersaSync to go into a holdover mode in the event that external time or frequency references are lost or become invalid. However, the oscillator can also be used as a legitimate 1PPS reference during normal operation, in conjunction with an external time reference (for more information, see "Configuring Input Reference Priorities" on page 189.)

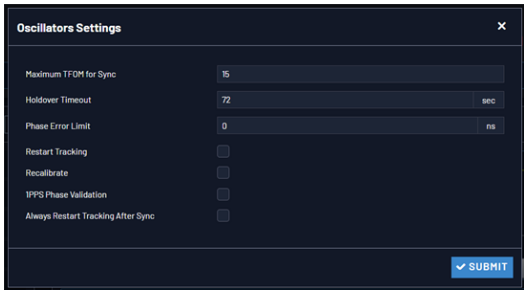
VersaSync's internal oscillator is normally disciplined to an input reference (such as GNSS, IRIG input, 1PPS input, etc.) in order to provide the highest degree of oscillator accuracy and to account for oscillator drift. While disciplining (with a 1PPS input reference input present and valid), the oscillator's 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 Oscillators Settings page provides the user with some control of the disciplining process. This page is also used to configure the length of time VersaSync is allowed to remain in the Holdover mode when all references are lost.

3.4.1 Configuring the Oscillator

VersaSync is equipped with an internal oscillator. To configure the oscillator settings:

1. Navigate to **MANAGEMENT > OTHER: Disciplining**.
2. Click the GEAR icon at the top of the **Status** panel. The **Oscillators Settings** window will display:



3. Populate the fields:
   - **Maximum TFOM for Sync**: When TFOM (Time Figure of Merit, see also "Time Figure of Merit (TFOM)" on the facing page) is greater than Max TFOM, disciplining will still be attempted against the selected reference to improve the TFOM. If the condition persists, the system will transition to holdover, and eventually out of sync. When disciplining is performed such that TFOM is no longer greater than max TFOM, the system will transition back into sync.
   - **Holdover Timeout(s)**: The default is 7200 s (= 2 hours).
     For more information on holdover timeouts, see "Typical Holdover lengths in seconds" on page 238. For additional information on holdover, see "What is "Holdover Timeout"?" on page 236.
   - **Phase Error Limit**: [Default=0 (disables this feature)]. Setting a Limit (valid for +/-) for the Phase Error between an external 1PPS reference and the System 1PPS will cause the disciplining tracking to restart automatically (after a few minutes delay) if that limit is exceeded. This will help to quickly re-align the System 1PPS with a reference.

     When using a Host Reference as a primary or backup reference, for improved performance it is recommended to set the phase error limit for NTP to a suggested value of 100000 ns (= 100 µ second). Adjust this value as needed, based on your accuracy requirements.
   - **Restart Tracking**: Check this box, and click Submit if you want to **manually** restart disciplining tracking.
     This option causes the disciplining algorithm to stop tracking the input reference and start over (as if it was just acquired). This can be useful if there is a large phase offset between reference 1PPS and system 1PPS, as it may occur when going back into sync to the external reference after a long holdover. A **Restart Tracking** will re-align the system 1PPS with the reference 1PPS very quickly, but may cause the 1PPS output to jump.
   - **Recalibrate**: In rare cases, existing calibration data may no longer be suitable to calibrate the oscillator. This function will delete the

existing calibration data, and begin a new calibration process (not applicable for low phase-noise Rubidium oscillators).

- **1PPS Phase Validation**: Turn ON Smart Reference Monitoring. See "Reference Monitoring: Phase" on page 199.
- **Always Restart Tracking After Sync**: When selected, this option will ensure that every time the unit exits holdover, the discipline tracking is restarted, to quickly align the oscillator. This may result in large timing jumps. It should be noted that this setting will only restart the tracking once when using the Phase Error Limit, unless the unit re-enters holdover.

4. Click Submit.

3.4.1.1 Time Figure of Merit (TFOM)

The TFOM reflects the **estimated error** range values between the **reference 1PPS** (such as GPS 1PPS) and the **System 1PPS** which is being aligned to the 1PPS. The estimated error is referred to as the 1PPS Phase error. TFOM values are ranges of these phase errors. The larger the phase error estimate, the larger the TFOM value will be. For example, TFOM 3 is reported when the estimated phase error is any value between 10 ns to less than 100 ns of the offset between the selected 1PPS reference and the system's 1PPS.

TFOM is VersaSync's estimation of how accurately it is synchronized with its time and 1PPS reference inputs, based on several factors, known as the **Estimated Time Error** or ETE. The larger the TFOM value, the less accurate VersaSync believes it is aligned with its 1PPS input that is used to perform disciplining. If this estimated error is too large, it could adversely affect the performance of oscillator disciplining. The available TFOM range is 1 through 15. You may refer to the following for the TFOM to ETE conversions:

Table 3-5: TFOM to ETE conversion

Reported TFOM Value	Estimated Time Error (ETE)
1	<= 1 nsec
2	1 nsec < ETE <= 10 nsec
3	10 nsec < ETE <= 100 nsec
4	100 nsec < ETE <= 1 µsec
5	1 µsec < ETE <= 10 µsec
6	10 µsec < ETE <= 100 µsec
7	100 µsec < ETE <= 1 msec

Reported TFOM Value	Estimated Time Error (ETE)
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

Example

TFOM is a value between 1 and 15. TFOM can never exceed the default MaxTFOM value of 15.

Typically the MaxTFOM requires no adjustment, but in some instances it may be advisable to decrease MaxTFOM so that TFOM can potentially exceed it: For example, by lowering the MaxTFOM to “5” it is now possible for TFOM to be always higher than the MaxTFOM value:

Assuming the MaxTFOM is set to 5 and the TFOM happens to go to a 6, i.e. TFOM is now exceeding MaxTFOM. This condition will cause a **1PPS out of specification** alarm to be asserted and the oscillator disciplining will change in order to speed-up the alignment of the system 1PPS to the selected reference (causing it to take less time getting closer into alignment with the reference):

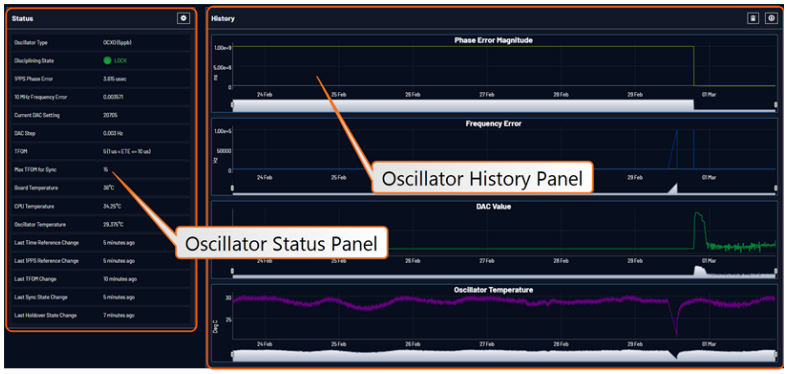
This will cause the TFOM to start to decrease faster. Once TFOM no longer exceeds MaxTFOM because the **System 1PPS** is now much closer to the **reference 1PPS**, the disciplining slows back down again as the system 1PPS continues to be brought into alignment with the selected 1PPS input.

3.4.2 Monitoring the Oscillator

The Oscillator Management screen provides current and history status information on disciplining state and accuracy.

To access the **Oscillator Management** screen:

1. Navigate to **MANAGEMENT > OTHER: Disciplining**.
2. The **Oscillator Management** screen will display. It consists of two panels:



The Oscillator Status Panel

This panel provides comprehensive information on the current status of VersaSync's timing state.

- Oscillator Type: Type of oscillator installed in the unit.
- Disciplining State: State of oscillator control and disciplining; indicates whether or not the internal oscillator is currently being disciplined (steered to an input reference). The states are: "Warm up", "Calibration", "Tracking Setup", "Lock State", "Freerun", and "Fault".
- 1PPS Phase Error: A tracking measurement [scaled time, in ns, or ms] of the internal 1PPSs' phase error with respect to the selected input reference. Long holdover periods or an input reference with excessive jitter will cause the phase error to be high. The oscillator disciplining control will gradually reduce the phase error over time. Alternatively, restarting the tracking manually (see "Restart Tracking" under "Configuring the Oscillator" on page 239), or automatically via a pre-set Phase Error Limit, will quickly reduce the phase error.
- 10 MHz Frequency Error: An internal estimated calculation (in Hertz) of the internal oscillator's frequency error, based on the phase accuracy error at the beginning and end of a frequency measurement window (the length of this window will vary depending upon the type of oscillator installed and the oscillator adjustment algorithm).
- Current DAC Setting: Current DAC value, as determined by the oscillator disciplining system. The value is converted into a voltage that is used to discipline the oscillator. A stable value over time is desirable and suggests steady oscillator performance (see also the graph in the History Panel).

- DAC Step: Step size for adjustments to the internal oscillator, as determined by the oscillator disciplining system. Larger steps = quicker, but coarser adjustments. The step size is mainly determined by the type of oscillator.
- TFOM: The Time Figure of Merit is VersaSync's estimation of how accurately the unit is synchronized with its time and 1PPS reference inputs, based on several factors, known as the Estimated Time Error or ETE. The larger the TFOM value, the less accurate VersaSync believes it is aligned with its 1PPS input that is used to perform disciplining. If this estimated error is too large, it could adversely affect the performance of oscillator disciplining. The available TFOM range is 1 through 15.
- Max TFOM for Sync: Value, as set under "Configuring the Oscillator" on page 239
- Temperature(s): Three temperatures are displayed:
  - **Oscillator** temperature, which has an effect on oscillator accuracy, and therefore can be used to interpret oscillator performance.
  - **Board** temperature (measured on the main board, sometimes also referred to as 'System temperature')
  - **CPU** temperature

Note: Oscillator temperature is plotted over time in the History panel on the right, while graphs for board and CPU temperature can be found under TOOLS > SYSTEM: System Monitor.

- Last Time Reference Change: [Timestamp: Last occurrence]
- Last 1PPS Reference Change: [Timestamp: Last occurrence]
- Last TFOM Change: [Timestamp: Last occurrence]
- Last Sync State Change: [Timestamp: Last occurrence]
- Last Holdover State Change: [Timestamp: Last occurrence]

The Oscillator History Panel

The **Oscillator History Panel** offers real-time graphical monitoring of VersaSync's internal timing. The following graphs plot key oscillator-relevant data over time::

- **Phase Error Magnitude**: See 1PPS Phase Error
- **Frequency Error**: See 10_MHz_Frequency_Error

- **Scaled DAC Value**: See DAC Step
- **Oscillator Temperature**, which has an effect on oscillator accuracy, and therefore can be used to interpret oscillator performance.

You can **zoom** in on any of the graphs by grabbing the handles at either end and pulling them inwards. The graph will focus in on the time interval you choose in real time.

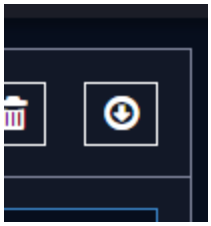
Clicking on the **Delete** icon in the top-right hand corner will erase all current oscillator log data.

Clicking on the **Download** arrow icon will download the latest oscillator log data as a `.csv` file.

3.4.3 Oscillator Logs

To export, or delete the oscillator logs:

1. Navigate to **MANAGEMENT > OTHER: Disciplining**.
2. To download the log file: In the **History** panel, click the downwards pointing ARROW icon. in the top-right corner:



3. The log file will be downloaded onto your local computer. Its name is `oscillatorStatusLog.csv`. Depending on the operating system you can open the file, or save it locally.
   To delete the log file, click the TRASH CAN icon, and confirm.

BLANK PAGE.

CHAPTER 4

System Administration

The following topics are included in this Chapter:

4.1 Issuing the HALT Command Before Removing Power

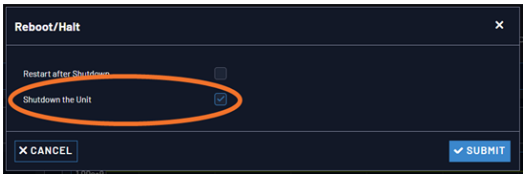
Gracefully shutting down VersaSync by using the HALT command offers the following advantages over shutting the unit down by interrupting the power supply:

- The shutdown process will be logged
- The System Clock will update the Real Time Clock with the latest System Time.
- VersaSync's file system will be synchronized, which under some circumstances will allow for faster startup next time the unit will be powered up.

Note: Wait 30 seconds after entering the HALT command before removing power.

Issuing a HALT Command via the Web UI

1. Navigate to **TOOLS > SYSTEM: Reboot/Halt**.
2. The **Reboot/Halt** window will display. Select the **Shutdown the Unit** checkbox.



3. Click **Submit**.
4. Wait 30 seconds after entering the HALT command before disconnecting power from the unit.

Issuing a HALT Command via SerialPort/Telnet/SSH:

With a serial connection to the USB port, telnet connection or SSH connection, type `halt` <Enter> to halt the unit for shutdown. For more information on VersaSync commands, see "CLI Commands" on page 335.

Note: After issuing the HALT command wait 30 seconds before you remove power.

Once you have halted your VersaSync, power must be removed (unplugged) and reapplied in order to restart the unit.

4.2 Rebooting the System

To reboot VersaSync via the Web UI:

1. Navigate to **TOOLS > SYSTEM: Reboot/Halt**.
2. Select the **Restart after Shutdown** box in the **Reboot/Halt** window.

3. VersaSync will now be rebooted and be accessible again shortly thereafter.

Rebooting via USB Port, Telnet, SSH, SNMP

With a serial connection to the USB port, telnet connection or SSH connection, type `reboot` <Enter> to reboot VersaSync.

Reboot is also is available to be performed through an `snmpset` operation. For more information on VersaSync commands, see "CLI Commands" on page 335.

4.3 Notifications

If an event occurs e.g., VersaSync transitions into Holdover, or a short is detected in the GNSS antenna, VersaSync can automatically notify users that a specific event has occurred.

In some situations, two events are generated. One event occurs in the transition to a specified state and then another event occurs when transitioning back to the original state. Examples of these are losing sync and then regaining sync, or going into Holdover mode and then going out of Holdover mode. Other situations may only consist of one event. An example of this situation is switching from one input reference to another.

Notifications of each event that may occur can be via alarms, via SNMP Traps being sent to one or more SNMP Managers, via an email being sent to a specified email recipient, or a combination of the three. The Notifications page allows a user to configure whether the occurrence of each event automatically triggers an

alarm to be generated, an SNMP trap to be sent out, an email to be sent out, or a combination of the three.

Also, this page allows the desired email recipient's address for that particular event to be specified. Each event can be configured with the desired email address that is specific to just that one event only. Note that only one email address can be specified in each Email Address field. If desired, the same email address can be used in all of the fields, or different addresses can be used for different events.

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

All available VersaSync events that can generate a notification to be sent are located under different tabs in the Notification Events panel: **Timing**, **GPS**, and **System**.

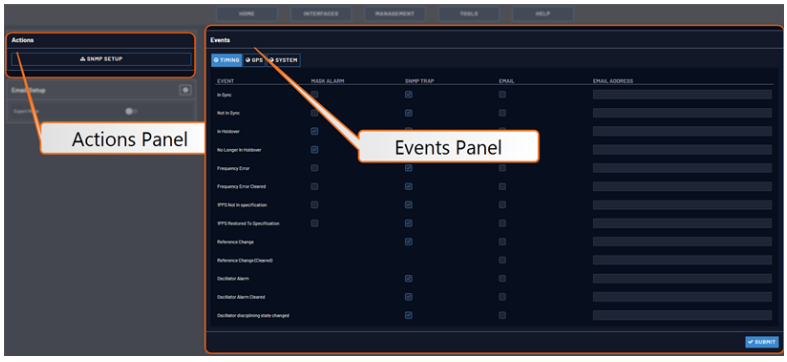
The VersaSync Events that can automatically trigger a notification are listed in the **Event** column. It is possible to:

- Mask the alarm generation for specific events (prevent the alarm)
- Enable "SNMP" (to send out an SNMP trap)
- Send an email to the address specified in the corresponding "Email Address" column.

4.3.1 Configuring Notifications

To configure Notifications:

1. Navigate to **MANAGEMENT > OTHER: Notifications**. The **Notifications** screen will display:

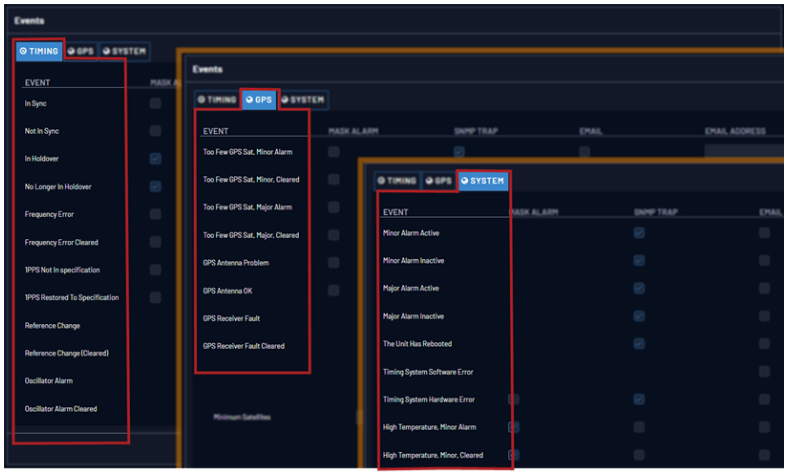


It is divided into two panels:

- The Actions panel, featuring:
  - The **SNMP Setup** button: See "SNMP" on page 99.
  - The **Email Setup** button: Configure VersaSync's interface settings for Exchange email servers and Gmail.

    For more information on this subject, see the Technical Note Email Notification Setup.
- The Events panel, offering three tabs:
  - **Timing**: Events for Sync Status and Holdover, Frequency error, Input references and the internal oscillator.
  - **GPS**: Events related to the GNSS receiver, including antenna cabling, tracking less than the minimum number of satellites and GNSS receiver faults.
  - **Systems**: Events related to the system operation, including minor and major alarms being asserted, reboot, timing system errors and option cards.

2. In the **Events** panel, choose the **Timing**, **GPS** or **System** tab. Configure your Notifications (see below), and click Submit.



The columns under each tab are:

- **Event**—This is the event that will trigger the notification. The events under each tab will vary according to context.
- **Mask Alarm**—Check here to enable an alarm mask. Enabling an alarm mask for a given notification will prevent that notification from generating an alarm condition. Other notifications for that event and logging of the event will still occur.

- **SNMP Trap**—Check here to configure the event to trigger an SNMP Trap.
- **Email**—Check here to configure the event to trigger an email notification.
- **Email Address**—Enter the address to which the email should be sent when triggered by the event.

Note: Each event can be configured with the desired email address that is specific to just that one event only. Note that only one email address can be specified in each Email Address field.

For each event choose the notification you want and an email address – if any – to which you want the notification to be sent. For more information, see "SNMP" on page 99 and "Setting Up Email Notifications" on page 255.

For each event, only the notification options available can be configured. For example, a mask alarm can be set for an In-Sync event, and a Not-in-Sync event, but not for an In-Holdover event.

4.3.2 Notification Event Types

The following types of events can be used to trigger notifications:

4.3.2.1 Timing Tab: Events

- In Sync
- Not In Sync
- In Holdover
- No Longer in Holdover
- Frequency Error
- Frequency Error Cleared
- 1PPS Not In Specification
- 1PPS Restored to Specification
- Oscillator Alarm
- Oscillator Alarm Cleared
- Oscillator Disciplining State Changed

- Reference Change (Cleared)
- Reference Change

4.3.2.2 GPS Tab: Events

- Too Few GPS Sat, Minor Alarm
- Too Few GPS Sat, Minor, Cleared
- Too Few GPS Sat, Major Alarm
- Too Few GPS Sat, Major, Cleared
- GPS Antenna Problem
- GPS Antenna OK
- GPS Receiver Fault
- GPS Receiver Fault Cleared

Under the **GPS Events** tab, you can also configure **Minor** and **Major Alarm Thresholds** for GNSS fault events; see "Configuring GPS Notification Alarm Thresholds" below.

4.3.2.3 System Tab: Events

- Minor Alarm Active
- Minor Alarm Inactive
- Major Alarm Active
- Major Alarm Inactive
- Unit Reboot
- Timing System Software Error
- Timing System Hardware Error
- High Temperature, Minor Alarm
- High Temperature, Minor, Cleared
- High Temperature, Major Alarm
- High Temperature, Major, Cleared

4.3.3 Configuring GPS Notification Alarm Thresholds

VersaSync allows you to configure Minor and Major alarm thresholds for the GNSS receiver. This is done by setting the minimum number of satellites the

receiver can track for a set time before an alarm is triggered. If both conditions are met, i.e. the reception quality falls below the set number of satellites for the set amount of time, an alarm is triggered.

The alarm notification feature described below allows you to be notified of a potential reception issue BEFORE the GNSS reference becomes invalid. This may be useful e.g., to notify system operators of a deteriorating signal reception before VersaSync loses the GNSS reference.

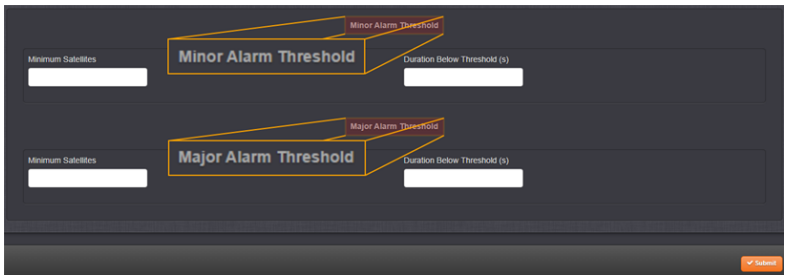
Note that VersaSync itself has a pre-defined minimum number of satellites that must be tracked in order for GNSS to be considered a valid reference. The minimum number of satellites depends e.g., on your receiver mode, the GNSS signal reception in the area where your antenna is located, and the type of receiver in your unit. In Stationary mode, and for SAASM units, the minimum number of satellites is normally 4 (four). Hence, it would be prudent to set the Minor Alarm Threshold to 8, and the Major Alarm Threshold to 6.

Note: While GPS Notification Alarms can be used in Mobile GNSS receiver mode, it is not advisable.

To determine **how many satellites** your VersaSync unit is currently receiving, navigate to **INTERFACES > REFERENCES: GNSS 0**. See also "Reviewing the GNSS Reference Status" on page 211.

To **set** the GPS Alarm Thresholds:

1. Navigate to **MANAGEMENT > OTHER: Notifications**, and choose the **GPS** tab.
2. At the bottom of the window, locate the **ALARM THRESHOLD** panel:



3. In the **Minimum Satellites** fields enter the minimum number of satellites that must be available before the alarm is triggered. The alarm will be triggered when the number of satellites available is **BELOW** this number.
4. In the **Duration Below Threshold (s)** fields, enter the time **in seconds** that the system must be below the threshold set in the **Minimum Satellites** field

before an alarm is triggered. The alarm will be triggered when this time is reached.
By default, this timeout value is set to 0 seconds: As soon as the receiver drops below the minimum number of satellites, the associated alarm is triggered. A delay of e.g., 5 seconds, however, would not trigger an alarm if the number of received satellites drops below the specified number for only 3 seconds.

You can configure this event to cause either a Minor alarm, or a Major alarm, or both.

To learn more about Minor and Major alarms, see "Minor and Major Alarms" on page 326.

Note that the GNSS receiver must initially be tracking more than the configured number of satellites in order for this alarm to be triggered (the alarm is triggered when the receiver falls below the number of **Minimum Satellites** you specified above).

4.3.4 Setting Up SNMP Notifications

SNMP Notifications are SNMP traps that occur on a change of a monitored event.

To configure SNMP notifications:

1. Navigate to **MANAGEMENT > OTHER: Notifications**.
2. In the **Actions** panel, click **SNMP Setup**.

For more information on SNMP, see "SNMP" on page 99.

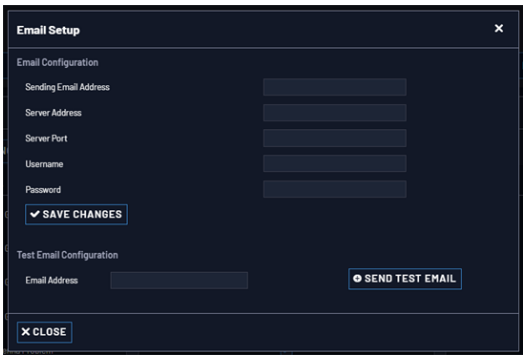
4.3.5 Setting Up Email Notifications

The **Email Setup** window provides a means to configure VersaSync with the necessary settings to interface it with Exchange email servers and Gmail.

To set up Notification Emails (Standard Mode):

1. Navigate to **MANAGEMENT> OTHER: Notifications**.
2. In the **Email Setup** panel, click on the gear icon

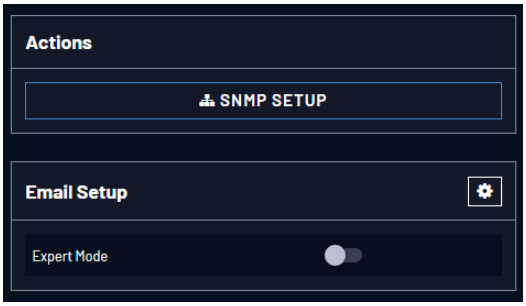
3. Enter your email information in the popup window



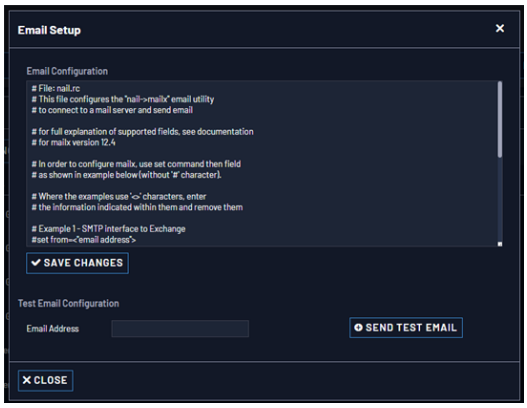
4. To test your settings:
   - In the **Test Email Address** field, enter an email address.
   - Click the **Send Test Email** button.
   - A notification that your email has been sent will appear at the top of the window.

To set up Notification Emails (Expert Mode):

1. Navigate to **MANAGEMENT> OTHER: Notifications**.
2. In the **Actions** panel of the **Notifications** screen, toggle Expert Mode to ON and click the ✉ **Email Setup** gear.



3. The **Email Setup** window will display:



The **Email Configuration** box provides two example configuration files. One is for interfacing VersaSync with an Email Exchange server; and the other is for sending emails via Gmail:

4. To configure the applicable example email configuration, delete the comments ("#") from each line and replace the "<>" with the appropriate values for your particular email server (such as the user name and password for your Email server).

Example I: SMTP interface to MS Exchange

```
set smtp=outlook.office365.com
set smtp-auth-user=john.doe@nav-timing.safrangroup.com>
set from="john.doe@nav-timing.safrangroup.com"
set smtp-auth-password=PASSWORD
set smtp-auth=login
set ssl-verify=ignore
set smtp-use-starttls
```

Example II: SMTP interface to Gmail

```
set smtp=smtp.gmail.com:587
set smtp-use-starttls
set ssl-verify=ignore
set smtp-auth-user=<user name, example user_xyz123@gmail.com>
set smtp-auth-password=<password>
set smtp-auth=login
```

5. Click the **Submit** button at the bottom of the window.
6. To test your settings:
   - In the **Test Email Address** field, enter an email address.
   - Click the **Send Test Email** button.
   - A notification that your email has been sent will appear at the top of the window.

4.4 Managing Users and Security

4.4.1 Managing User Accounts

Users need to authenticate as the login to VersaSync. The system administrator is responsible for maintaining a list of user accounts (user names, passwords etc.) via the **MANAGEMENT > OTHER: Authentication** screen of the VersaSync Web UI (HTTP/HTTPS). Note that user accounts CANNOT be created or edited via CLI commands using telnet or SSH.

4.4.1.1 Types of Accounts

There are three types of accounts:

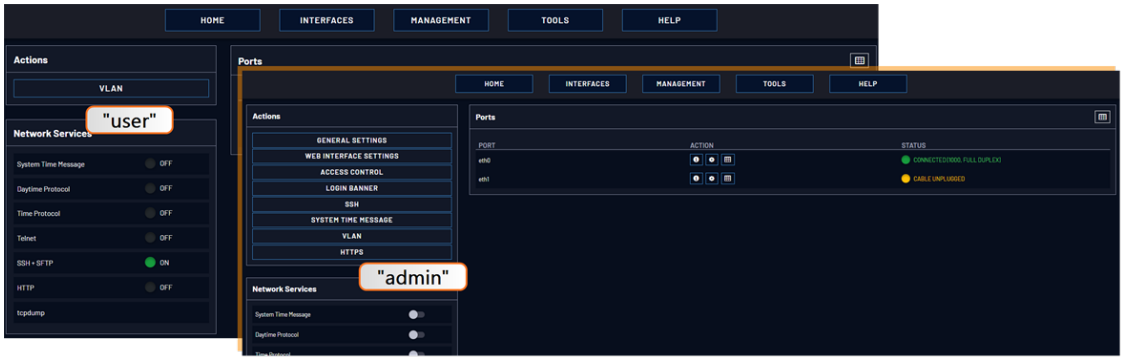
Account Type	Permissions
"user"	These accounts are intended for users only e.g., operators. These "user" accounts are read-only accounts, i.e. they do not allow any editing rights and are restricted to reviewing status-related information. The Web UI will not show (or gray-out) any editing functionality.
"admin"	Administrator accounts are intended to be used by system administrators. These accounts have writing access. You can add additional admin accounts to the pre-installed administrator account `spadmin`.
"factory"	The default factory account with the username `spfactory` is meant to provide access to Safran technical support personnel. You can delete this account, if you so prefer.

4.4.1.2 About "user" Account Permissions

As outlined above – unlike "administrator" accounts – "user" accounts are read-only accounts, i.e. they do not allow any editing rights and are restricted to reviewing status-related information. Otherwise, the privileges assigned to admin groups are exactly the same whether logging in via the Web UI, or connecting via SSH.

Account Differences, General

While most menus look the same to "admin" and "user" type accounts(except the MANAGEMENT menu, see below), the screens and panels located below the main menus will differ in such that the "user" UI will show fewer (if any) configuration options:



The status information presented, however, will be largely identical.

The most significant differences are visible in the MANAGEMENT menu, since most of the Setup menus are hidden from "user" accounts:

Account Differences, by Menu

INTERFACES Menu

"user" and "admin" accounts can view and modify all settings in these pages (can view/edit GNSS receiver, Outputs, and Option Cards).

MANAGEMENT Menu

Pin Layout: The "user" cannot see or manipulate these settings.

Network: While the toggle switches in the **Network Services** panel are displayed, "user" cannot modify any of the network-related configurations (such as telnet, FTP, SSH and HTTP/HTTPS). The switches can be moved, but an error message will be displayed shortly thereafter.

Authentication: "user" can access this page but can only change his/her own password. Users cannot create any new accounts and cannot modify any accounts.

Reference Priority: "user" can access this page and modify settings.

Notifications: "user" can access this page and modify settings.

Time Management: "user" can access this page and modify settings.

Front panel: "user" can access this page and modify settings.

Log Configuration: "user" can access this page and modify settings.

Disciplining: "user" can access this page and modify settings.

Change my password: "user" can access this page and change only their password.

TOOLS Menu

Logs: "user" can view only the listed logs

Upgrade/Backup: "user" cannot perform any updates.

Reboot/Halt: "user" cannot reboot/shutdown/halt the unit.

4.4.1.3 Rules for Usernames

- Length: Usernames can be between 3 and 32 characters long.
- Accepted characters:
  - All letters, including the first, must be lower-case.
  - Numbers, underscores and dashes are accepted.
  - Next to punctuation symbols, the following special characters are NOT accepted: ! @ # $ % ^ & * ( )

4.4.1.4 Adding/Deleting/Changing User Accounts

To access the **Users** list, and the **Password Security** panel:

1. Navigate to **MANAGEMENT > OTHER: Authentication**.
2. The **Users** panel on the right shows a list of all user accounts, including their **Username**, the **Group** to which that user account is assigned to, and any **Notes** about the user account:

VersaSync units are shipped with two default accounts:

i. The "administrator" account (`spadmin`), and

ii. The "factory" service account (`spfactory`).

Additional accounts may be added and deleted as desired. The number of accounts that can be setup is virtually unlimited.

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 VersaSync unless another admin account type is present.

Note: The `spfactory` account is for use by Safran service personnel. While the `spfactory` account can be deleted by an administrator, it should be noted that this may potentially limit remotely provided technical support.

User accounts can be created to have either limited user or full administrator rights. Each user can be assigned his own login password.

- To ADD a user account, click the PLUS icon in the top-right corner of the **Users** screen.
- To DELETE a user account, click the Delete button in that account's entry on the **Users** screen.
- To APPLY CHANGES to a user account, click the Change button next to the desired user account.

When either the Change button or the PLUS icon is clicked, the **Add or Change User** window appears:

To add a user account:

1. Enter a **Username**. (For rules, see "Rules for Usernames" on the previous page.)
2. Enter a **Password**. The password requirements are configurable, see "Managing Passwords" on the facing page. By default a password can be any combination of upper- and lower-case characters. Minimum password length = 8 characters, maximum length = 32 characters.
3. Repeat the new **Password**.
4. In the **Group** field, choose the permission group to which you want the user to belong to: user or admin. The user permission level assigns permission to access and change all settings, with the following **exceptions** that are limited to the admin accounts:
   - Changing network settings
   - Adding and deleting user accounts

- Web Interface Settings
- Upgrading VersaSync system software
- Resetting the VersaSync configuration
- Clearing log files
- Changing Disciplining Setup options
- Changing configuration options for the following protocols or features:
  - NTP
  - HTTPS, SSH
  - LDAP/RADIUS
  - SNMP (with the exception of configuring SNMP notifications).

To change a user account:

1. In the **Add or Change User** window the **Username** field will be populated.
   a. To change it, type the new name.
   b. To change the user account's password, type the new password in the **Password** field and confirm it in the **Repeat New Password** field. Note that the password requirements are configurable, see "Managing Passwords" below.
   c. To change the user account's user permission group, select the group from the drop-down menu.

For more information, see also "Managing Passwords" below.

4.4.2 Managing Passwords

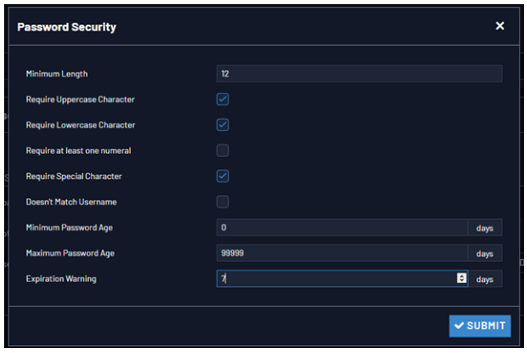
Caution: For security reasons, it is advisable to change the default credentials.

Note: Password changes cannot match any 10 previous passwords used on that specific account.

4.4.2.1 Configuring Password Policies

To configure password requirements e.g., rules for minimum password length and special characters:

1. Navigate to **MANAGEMENT > OTHER: Authentication**.
2. In the **Actions** panel, click **Security Policy**.
3. The **Password Security** window will display. Fill in the self-explanatory fields and click Submit.



4.4.2.2 The Administrator Password

The factory default administrator login password value of *admin123* can be changed from the default value to any desired value. If the current password is known, it can be changed using the VersaSync Web UI.

Caution: Once you log in to your VersaSync, you will be prompted to update your spadmin password.

Note: To follow this procedure, you must be logged in as the `spadmin` user. If you are unable to login as `spadmin`, follow the procedure outlined in "Lost Password" on the facing page.

If the password has already been changed from the default value, but the current value is no longer known, the administrator password can be reset back to the factory default value, see "Lost Password" on the facing page. Once reset, it can then be changed to a new desired value via the Web UI.

Changing the admin password

To change the admin password from a known value to another desired value:

1. Navigate to **MANAGEMENT > OTHER: Change My Password**.
2. The **Change Password** window will display.

3. In the **Old Password** field, type the current password.
4. In the **New Password** field, type the new password.

> **Note:** The new password can be from 8 to 32 characters in length.

> **Note:** Password changes cannot match any 10 previous passwords used on that specific account.

5. In the **Repeat New Password** field, retype the new password.
6. Click **Submit**.

For more information, see also "Managing User Accounts" on page 259.

4.4.2.3 Lost Password

If the current *spadmin* account password has been changed from the default value and has been forgotten or lost, you can reset the *spadmin* password back to the factory default value of *admin123*.

Resetting the *spadmin* account password does not reset any user-created account passwords. This process only resets the *spadmin* account password.

Any user with administrator rights can reset the *spadmin* password through the **MANAGEMENT > OTHER: Authentication** window.

If you do not know the password for any user with administrator rights, your only options are:

» contact customer service to request a password reset.

Changing the "spadmin" password via Web UI

To change the spadmin password:

1. Navigate to the **MANAGEMENT > OTHER: Authentication** window.
2. Locate the *spadmin* entry in the **Users** table.

3. Click the **CHANGE** button.
4. In the **Add or Change User** window:
    1. Enter a new password.

> **Note:** The new password can be from 8 to 32 characters in length.

    2. Confirm the new password.
    3. Click **Submit**.

To reset the "spadmin" account password via the serial port, or SSH:

1. Connect a PC to the USB port, and log in using an account with admin group rights (such as the *spadmin* account).
2. Type: `resetpw` <Enter>. The *spadmin* account password is now reset.

After resetting the password follow the procedure above to change the *spadmin* password in the **MANAGEMENT > OTHER: Authentication** window.

4.4.3 Web UI Timeout

For security reasons, the Web UI will automatically timeout after a set number of minutes, i.e. you will be logged out by the system, regardless of activity, and need to actively login again.

- **Minimum** timeout duration: 10 minutes
- **Maximum** timeout duration: 1440 minutes (24 hours)
- **Default** timeout duration: 60 minutes.

To change the time after which the Web UI will timeout:

1. Navigate to the **MANAGEMENT > Network Setup** screen.
2. In the **Actions** panel on the left, click on **Web Interface Settings**.
3. In the **Web Interface Settings** window, enter the desired value in minutes.

In order for a new setting to take effect, you need to log off, and then log back in again. This setting affects all users, not just the user changing the value.

Note: The Web UI does not allow simultaneous logins. Any subsequent logins will discontinue any prior instances of the Web UI.

4.4.4 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 VersaSync. 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.

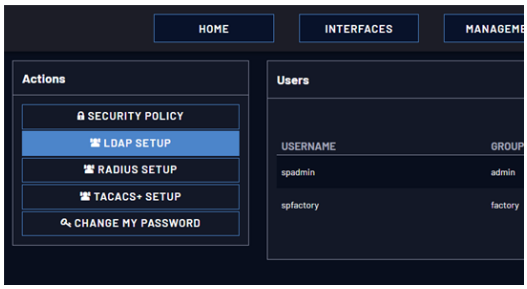
In order to use the LDAP authentication capability of VersaSync, it needs to first be configured with the appropriate settings in order to be able to communicate with the LDAP server(s) on the network.

Note: VersaSync requires commas between multiple values entered in the same field (periods not accepted).

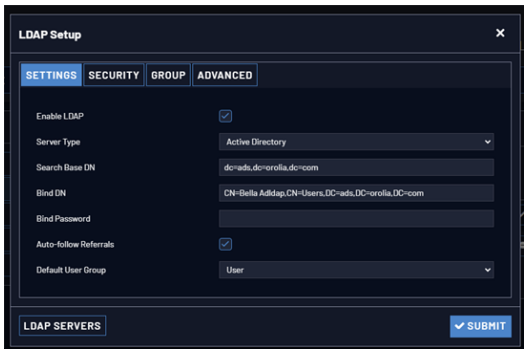
Caution: If you plan on using LDAP, configure it with diligence. If not required, Safran recommends to keep LDAP disabled.

Configuring LDAP authentication

1. Navigate to **MANAGEMENT > OTHER: Authentication**.
2. In the **Actions** panel, click the **LDAP Setup** button.



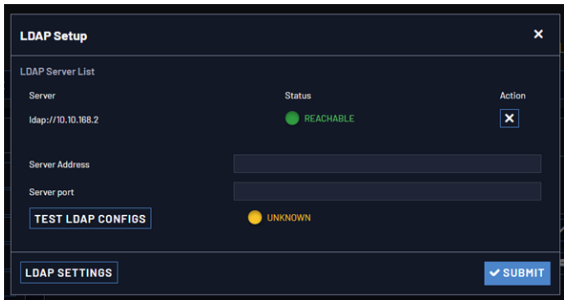
3. The **LDAP Setup** window will display.



4. Click the LDAP Servers button to add a server and identify the primary server.
5. There will be 4 tabs to allow additional LDAP configuration:
   - **Settings**: This is where you set up the general LDAP Distinguished Name and Bind settings.
   - **Security**: This is where you upload and manage the CA server certificate, CA client certificate and CA client key.
   - **Group**: This is where you enable/disable group-based authentication.
   - **Advanced**: This is where you set up your search filter(s) and login attribute.

LDAP Servers Settings

Under the **LDAP Servers** popup window, you manage the LDAP server(s) to be accessed:. It is necessary to add a server before other settings are configured.



Under the LDAP **Servers** tab, the window displays:

- **LDAP Server Status**—Attempts to ping the server and will display one of the following states:
  - **DISABLED** (yellow) —The Enabled checkbox under the Settings tab as not been selected.

    - **REACHABLE** (green)—The server is reachable.
    - **UNREACHABLE** (red)—The server is unreachable.
- **Test LDAP Configs** button -Performs an ldapsearch command with the configured servers and settings. (Note: does not test TLS Certificates).
    - **UNKNOWN** (yellow) —The LDAP Config test has not been performed yet.
    - **LDAP CONFIGURATION VALID** (green)—The ldapsearch command successfully authenticated with the server.
    - **SERVER CANNOT BE REACHED** (red)—The server cannot be reached.
    - **other message** (red)—The server could be reached, but the configuration is invalid. The error message returned by ldapsearch is displayed.
- **Server**—The hostname(s) or IP address(es) of the LDAP server(s) that have been added.
    - **Action**—After a server has been listed, it can be removed by clicking the X-button.
- **Port**: The port number of the LDAP server (default port numbers: regular LDAP = 389; secure LDAP = 636)
- **Add additional server**—Enter the hostname or IP address of the LDAP server to be queried. You may list multiple servers.

LDAP Settings

Under the **LDAP Settings** tab, set the following parameters:

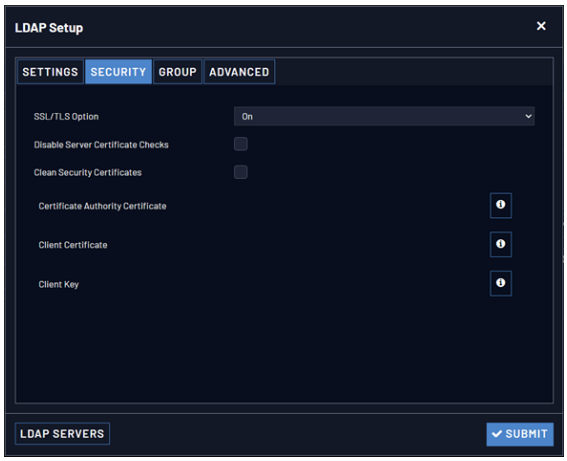
- **Server Type**: This must be the correct type—check with your LDAP server administrator if you are not sure which you are using. You have a choice of:
    - **Active Directory**: This will be used when the LDAP server is a Windows server. If you choose Active Directory, you are required to fill out the NSS Password field.
    - **Open LDAP**: This will be used when the LDAP server is a Linux/UNIX server.
- **Server Base DN**: Specifies the default base distinguished name to use for searches. This is the base name to use in the database search. Typically, this is the top-level of the directory tree structure. Your LDAP server administrator will provide this information.
- **Bind DN**: Enter the Distinguished Name used to bind to (this is an optional field if the database allows anonymous simple authentication). You are able to use any same level of the tree and everything below.

- The bind DN is the user that is permitted to search the LDAP directory within the defined search base. Most of the time, the bind DN will be permitted to search the entire directory. The role of the bind DN is to query the directory using the LDAP query filter (as specified under the **Advanced** tab) and search base for the DN for authenticating users. When the DN is returned, the DN and password are used to authenticate the user.

- **Bind Password**: Enter the password to be used to bind with the LDAP Server. Leave this field empty for anonymous simple authentication.
- Checkbox **Auto-follow Referrals**: Allow the use of LDAP referrals to be utilized in order to access locations that more likely hold a requested object.
- **Default User Group**: Select your preferred default user permissions level (Admin or User).

LDAP Security Settings

Under the LDAP **Security** tab, you can upload and install the SSL and TLS required certificates and client key. Selecting the INFO icon next to a certificate or key will open a dialog that allows you to view a currently installed certificate or key, and to upload a new item. Certificates/ keys must be in PEM or DER format.



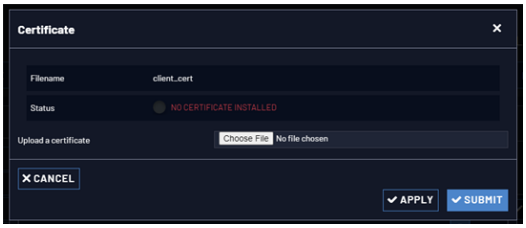
- Select an option from **SSL/TLS Option** to enable LDAP SSL/ TLS:
  - On (default) — Enables TLS encryption.
  - Off
  - Start TLS — Enables TLS encryption in compliance to FIPS 140-2.
- Select **Disable Server Certificate Checks** to disable verification of the certificate presented by the server.
- Select **Clean Security Certificates** to remove all certificates currently stored on VersaSync (e.g., to eliminate expired certificates).

- **Certificate Authority Certificate**: The Server Certificate. Required if Enable Security is checked and Disable Server Certificate Checks is unchecked.
- **Client Certificate**: Required if the LDAP server requires client authentication.
- **Client Key**: The private key that pair with the client certificate. Required if a Client Certificate is uploaded.

To upload a certificate or client key:

a. Click the INFO icon for the certificate you wish to upload.

b. In the **Certificate** window, click the **Choose File** button.



c. Locate and upload the certificate or client key file.

d. Click **Apply** to apply settings while the window remains open. Click **Submit** to apply settings and close the Certificate window.

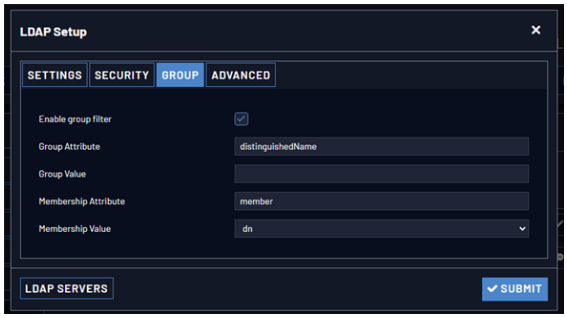
e. Verify the **Status**:

- NO CERTIFICATE INSTALLED (red): The certificate file is not found.
- *CERTIFICATE IS VALID (green: The certificate file is present and installed correctly. Additional certificate details are also displayed.
- *UNRECOGNIZED CERTIFICATE FORMAT (red): The certificate file is present and not valid. (The client key will display this message even if it has a recognized certificate format).

The SSL certificates and/or client key you upload will be installed in the `/home/spectracom/xfer/cert/` directory.

LDAP Group Settings

Under the LDAP **Group** tab, you can filter access by group.



To enable group authentication:

a. Select the **Enable group filter** checkbox.

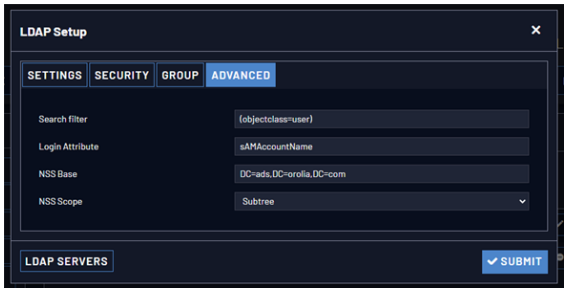
b. Enter information for:

- **Group Attribute**—Enter the group attribute. Example: `distinguishedName` for AD or `gidNumber` for OpenLDAP.
- **Group Value**—Enter the required group. Example: `ou=Group, dc=example, dc=com`.
- **Membership Attribute**— Enter the attribute of the above group that will specify a user of that group. Example: `member` or `memberUid`.
- **Membership Value**— Enter the value of the above attribute that will be stored in the group. Acceptable values are `username`, `uid`, and `dn`.

c. Click the **Submit** button.

LDAP Advanced Settings

Under the LDAP **Advanced** tab, you can set the search filter and the LDAP login attribute.



Fill in the following fields, as desired:

- **Search filter**—This is the LDAP search filter. Example: `objectclass=user`.
- **Login Attribute**— This is the LDAP login attribute. Example: `sAMAccountName`.

- **NSS base**—Enter the search base to be used for `nss_base` and `nss_shadow`. Example: `ou=People,dc=example,dc=com`
- **NSS Scope**:Enter the scope of the NSS search.

4.4.5 RADIUS Authentication

RADIUS authentication provides a means to use an external RADIUS server for authentication purposes when logging in to VersaSync. RADIUS allows the login password for user-created accounts to be stored and maintained in a central RADIUS server on the network.

This function greatly simplifies password management: Instead of having to change a password in many network appliances, it is changed on the RADIUS server only.

In order to use RADIUS authentication with VersaSync, RADIUS and the RADIUS network server first need to be configured. Currently, http/https/ssh/telnet/ftp protocols are supported, i.e. you can login to a VersaSync unit using RADIUS authentication via applications using any of these protocols.

Caution: In order to utilize RADIUS authentication, the account username on the RADIUS server must NOT be used with a local user account.

Note: VersaSync requires commas between multiple values entered in the same field (periods not accepted).

Example:

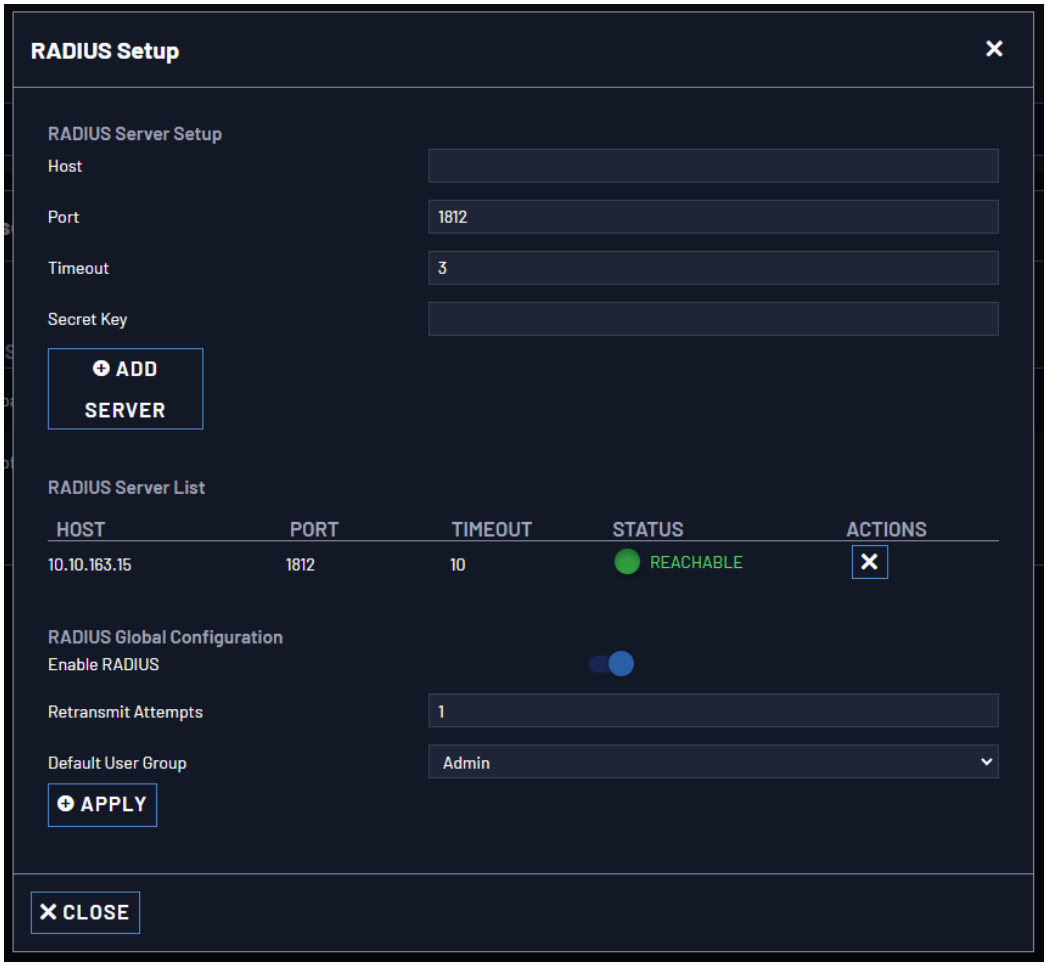
A user with the username user3 on the RADIUS server will not be able to login to a VersaSync unit, if on that unit a local user account with the username user3 exists. However, once the user deleted the local user3 account, she will be able to login with the RADIUS user3 account.

See also "TACACS+ Authentication" on page 279

4.4.5.1 Enabling/Disabling RADIUS

To enable or disable the use of RADIUS authentication on a VersaSync unit:

1. In the Web UI, navigate to **MANAGEMENT > OTHER: Authentication**.
2. In the **Actions** panel on the left, click **RADIUS**. The **RADIUS Setup** window will be displayed:

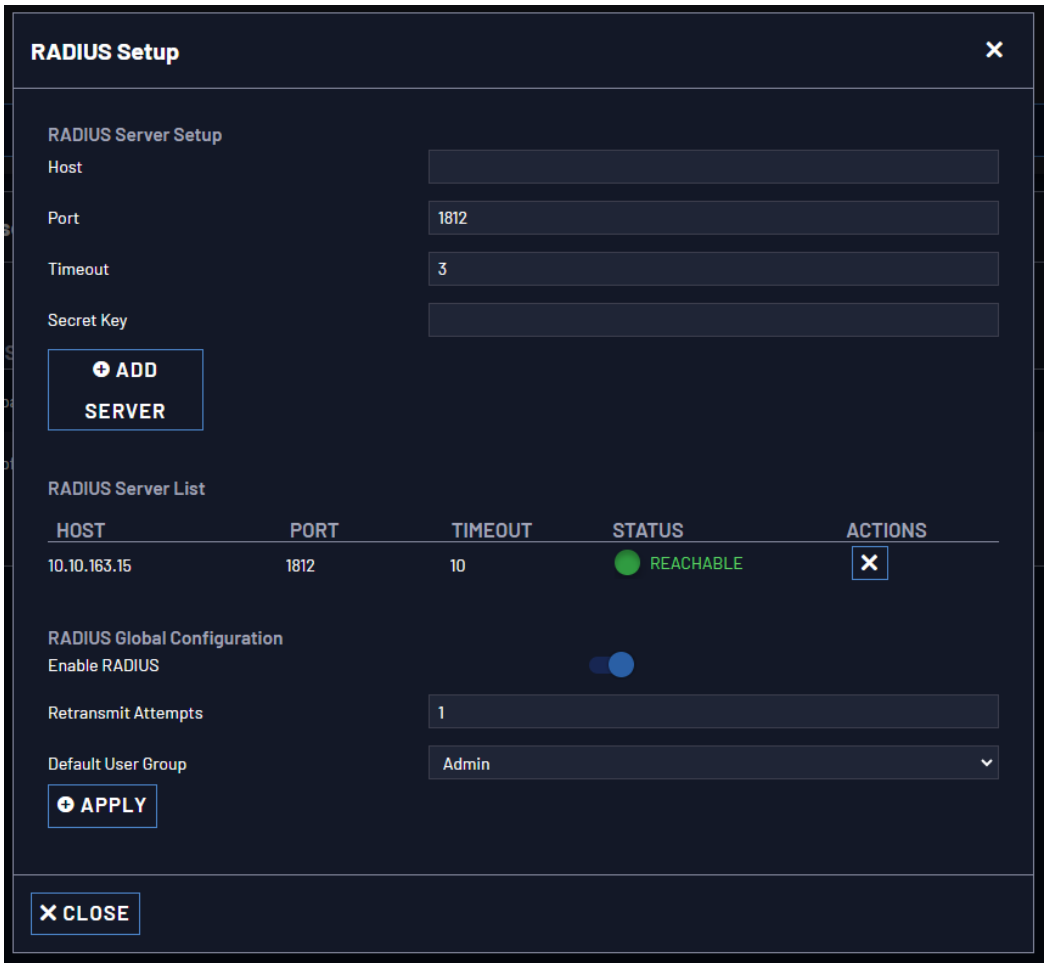


3. Click the **ON/OFF** toggle under Enable RADIUS to enable or disable the feature.
4. If you are enabling the service, in the **Retransmit Attempts** field, select the number of retries for VersaSync to communicate with the RADIUS server (default = 0).
5. Configure the **Default User Group** to select your preferred default user permissions level (Admin or User)
6. Click Submit.

4.4.5.2 Adding/Removing a RADIUS Server

To add a RADIUS authentication server, or remove a server from the list:

1. Navigate to **MANAGEMENT > OTHER: Authentication**.
2. In the **Actions** panel on the left, click **RADIUS Setup**. The **RADIUS Setup** window will be displayed:



3. Fill out the fields:
   - **Host**: The hostname or IP address of the RADIUS server
   - **Port**: Defines the RADIUS Port to use. The default RADIUS Port is 1812, but this can be changed, as required.
   - **Secret Key**: The secret key which is shared by VersaSync and the RADIUS server (the key is used to generate an MD5 hash).
   - **Timeout**: [seconds] Defines the Timeout that VersaSync will wait to communicate with the RADIUS server e.g., 10 seconds.

4. Click the **Add Server** button. A confirmation message The item has been added will be displayed if the server could be added, and the server will be added to the list, indicating its status. The server status can be:
   - DISABLED: RADIUS service is disabled.
   - UNREACHABLE: This RADIUS server cannot be reached.
   - REACHABLE: This RADIUS server can be reached.
5. To remove a RADIUS server from the list, click the **X**-button in the **Actions** column.

Note: VersaSync supports multiple RADIUS servers. The system performance, however, will be negatively affected by a large number of servers or invalid servers, respectively.

4.4.6 TACACS+ Authentication

Terminal Access Controller Access-Control System Plus (TACACS+) is a protocol that handles authentication, authorization, and accounting (AAA) services. VersaSync supports **pam_ tacplus**, allowing users to validate their username/password when logging into VersaSync via a TACACS+ server. Currently, http/https/ssh/telnet/ftp protocols are supported, i.e. you can login to a VersaSync unit using TACACS+ authentication via applications using any of these protocols.

Note: Your TACACS+ files will need to have either a `pap` or `global` user attribute. VersaSync does not authenticate `tacacs.conf` files with the default `login` user attribute.

Caution: In order to utilize TACACS+ authentication, the account username on the TACACS+ server must NOT be used with a local user account.

Example:

A user with the username user3 on the TACACS+ server will not be able to login to a VersaSync unit, if on that unit a local user account with the username user3 exists. However, once the user deleted the local user3 account, she will be able to login with the TACACS+ user3 account.

Sources of general reference information on TACACS+:

- https://en.wikipedia.org/wiki/TACACS
- http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html
- https://github.com/jeroennijhof/pam_tacplus

See also "RADIUS Authentication" on page 275

4.4.6.1 Enabling/Disabling TACACS+

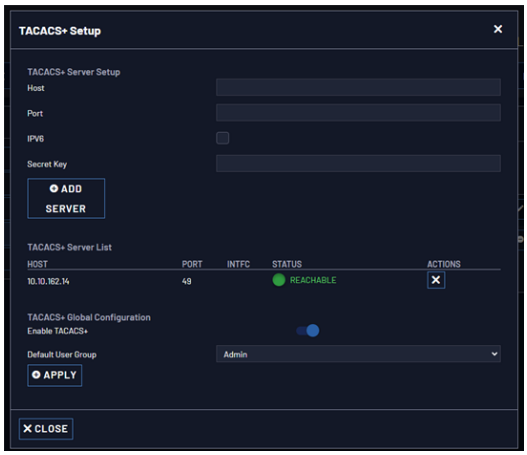
To enable or disable the use of TACACS+ authentication on a VersaSync unit:

1. In the Web UI, navigate to **MANAGEMENT > OTHER: Authentication**.
2. In the **Actions** panel on the left, click **TACACS+**. The **TACACS+ Setup** window will be displayed.
3. Configure the **Default User Group** to select your preferred default user permissions level (Admin or User)
4. Under Enable TACACS+, click the toggle to **ON** to enable TACACS+, and click the toggle to **OFF** to disable this feature.
5. Click Submit.

4.4.6.2 Adding/Removing a TACACS+ Server

To add a TACACS+ authentication server, or remove a server from the list:

1. Navigate to **MANAGEMENT > OTHER: Authentication**.
2. In the **Actions** panel on the left, click **TACACS+ Setup**. The **TACACS+ Setup** window will be displayed:



3. Fill out the fields:
   - **Host**: The hostname or IP address of the TACACS+ server
   - **Port**: Defines the TACACS+ Port to use.
   - **IPv6**: Enables IPv6 and reveals a field to select a Parent Interface.
   - **Secret Key**: The same encryption key as used on the TACACS+ server.
4. Click the **Add Server** button. A confirmation message The item has been added will be displayed if the server could be added, and the server will be added to the list. The server status can be:

- DISABLED: The TACACS+ service is disabled.
- UNREACHABLE: This TACACS+ server cannot be reached.
- REACHABLE: This TACACS+ server can be reached.

5. To remove a TACACS+ server from the list, click the **X**-button in the **Actions** column.

Note: VersaSync supports multiple TACACS+ servers. The system performance, however, will be negatively affected by a large number of servers or invalid servers, respectively.

4.4.7 Web UI Security Dashboard

The Security Dashboard Web UI page contains tabs for both security issues and security compliance.

4.4.7.1 Security Issues

The VersaSync Web UI has recommended user settings that will increase the security of the product.

- Disable HTTP functionality
- Disable Telnet functionality
- Upload an HTTPS certificate that is not self-signed, and
- Upload an HTTPS certificate with a secure algorithm

If your settings differ from the recommended ones, a security icon will appear in the upper right of the banner.

To view the security issues for your unit, log in to the Web UI and navigate to **MANAGEMENT** > **Security Dashboard** > **Security Issues**. You can also select the security issues icon in the upper right-hand corner to be directed to this page.

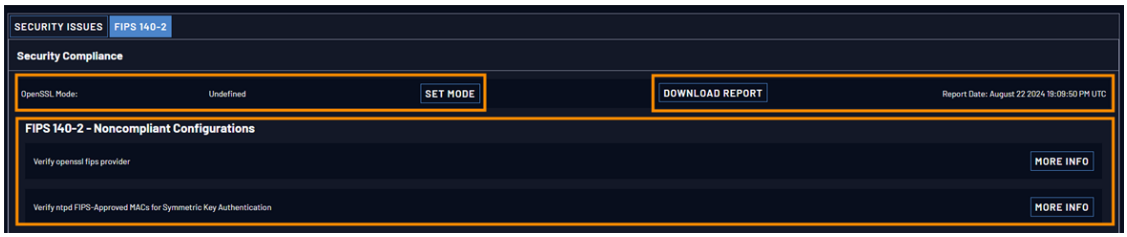
From the Security Issues tab, you can review the warnings listed for your unit, or select active warnings to be redirected to the correct field to fix the warning. You may also choose to ignore these warnings. Correcting or ignoring the warnings will both remove the warning symbol from your Web UI banner.

4.4.7.2 FIPS 140-2

The Federal Information Processing Standard (FIPS) specifies the security requirements for cryptographic modules that protect sensitive information. To achieve FIPS Compliance, services using FIPS 140-2 compliant cryptographics

must log any service that is not FIPS compliant. This information is logged and can be found by navigating to **MANAGEMENT** > **Security Dashboard**, and under the **FIPS 140-2** tab in **FIPS 140-2 - Noncompliant Configurations**.

Selecting the MORE INFO button will display more detailed information about the selected configuration including its title, name, IDRef, rationale, and description.



The FIPS 140-2 tab has three functions:

- Configure the OpenSSL Mode.
- Download the FIPS Compliance Report.
- Review a log of FIPS 140-2 Noncompliant Configurations.

OpenSSL Mode

A user with administrator privileges can change the OpenSSL mode to one of the following settings:

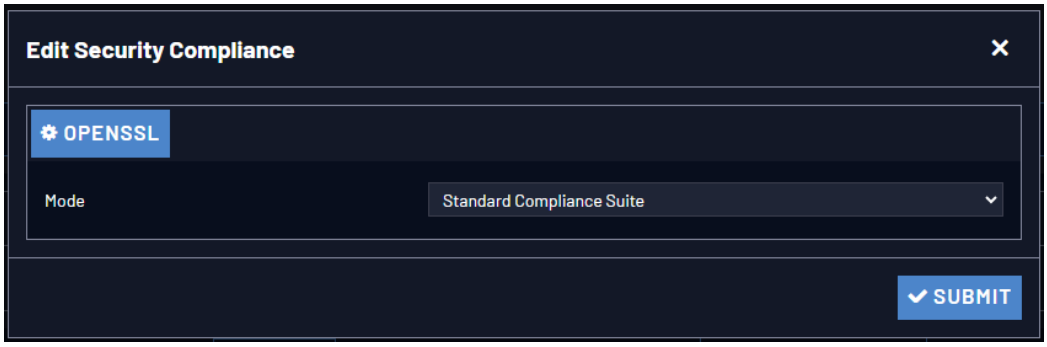
- **Legacy Enhanced:** uses non-compliant/legacy crypto module(s) (requires confirmation dialog). Enables extended functionality, including legacy algorithms that are no longer in common use while maintaining FIPS compliance.
- **Standard Compliance Suite [default]:** prefers FIPS-compliant crypto module, but allows non-compliant modules. Ensures standard compliance by activating default, base, and FIPS providers, excluding legacy algorithms.
- **Enhanced Security Core:** allows only FIPS-compliant crypto modules. Prioritizes enhanced security by activating only FIPS-certified and base providers, excluding non-FIPS compliant algorithms.

This can be done either through the Web UI or through the CLI:

Through the Web UI

To set the OpenSSL mode through the Web UI:

1. In the Web UI, navigate to **MANAGEMENT** > **Security Dashboard**, under the **FIPS 140-2** tab.
2. Select the SET MODE button, the following will display:



3. Open the dropdown menu, select the desired OpenSSL mode, and select the SUBMIT button.
4. A pop-up alert will display informing you that the change will require a system reboot. Selecting "OK" will immediately reboot the unit.

Through CLI Commands

To set the OpenSSL mode with CLI commands:

1. The command `getopenssl` will return the current compliance mode.
2. The command `setopenssl` will set the compliance mode.
   - It takes the arguments `<standard>`, `<enhanced>`, or `<legacy>` depending on the desired compliance mode.
   - `<enhanced>` and `<legacy>` will both have confirmation prompts.
   - Following a mode change, a message will appear informing you that a system reboot is necessary for the change to be applied.

Note: Switching to Enhanced Security Core mode will be disabled if an HTTPS Certificate signed with SHA1 is in use.

Enhanced Security Core Mode

Activating the "Enhanced Security Core" OpenSSL mode may cause certain Linux services to experience compatibility issues due to stricter cryptographic requirements. The table below summarizes the allowed hashing algorithms, ciphers, MACs, and HMACs under this mode:

Category	Allowed Algorithms
Message Digest	SHA1, SHA224, SHA256, SHA384, SHA512, SHA2-384, SHA2-512, SHA2-512/224, SHA2-224, SHA2-512/256, SHA3-512, SHA3-256, SHA3-224, SHA512-224, SHA512-256, SHAKE128, SHAKE256, KECCAK-KMAC128, KECCAK-KMAC256, SSL3-SHA1
Ciphers	aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc
MACs	hmac-sha2-512, hmac-sha2-256, hmac-sha2-512-etm@openssh.com, hmac-sha2-256-etm@openssh.com
HMACs	HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512

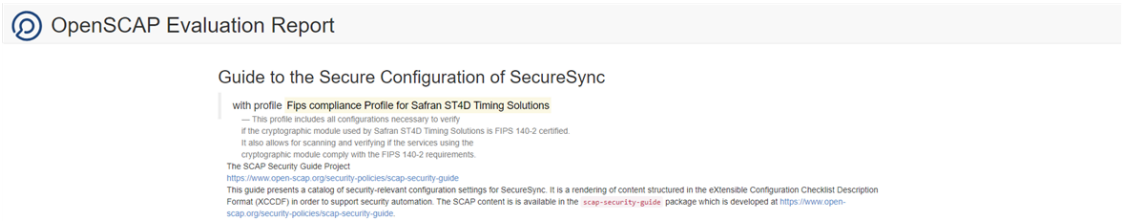
Affected Services

- **NTP:** Only the **SHA1** FIPS-approved algorithm should be used for NTP keys. Non-FIPS-approved MACs like MD5, SHA, MD4, MDC2, and RIPEMD160 in `/etc/ntp/keys/ntp.keys` will no longer function. (MDC2 will function with Legacy Enhanced mode).
- **SNMP:** Only **SNMPv3** with SHA for Auth Type and AES for Priv Type should be used (MD5/DES are not allowed). SNMPv1, v2c, community and `com2sec` configurations in `/etc/snmpd.conf` are not supported in this mode.
- **PAM:** Password hash algorithms in `/etc/pam.d/passwd` must be **SHA512** and the `ENCRYPT_METHOD` in `/etc/login.defs` must conform to the approved list (**ENCRYPT_ METHOD SHA512**). All passwords in `/etc/shadow` must be hashed using one of the allowed algorithms.
- **SSH:** The SSH service is limited to ciphers `aes256-ctr`, `aes192-ctr`, `aes128-ctr`, `aes256-gcm@openssh.com`, `aes128-gcm@openssh.com`, and MACs `hmac-sha2-512`, `hmac-sha2-256`, `hmac-sha2-512-etm@openssh.com`, `hmac-sha2-256-etm@openssh.com`.
- **Apache:** Only HTTPS with `TLSv1.2` and `TLSv1.3` is allowed. `SSLv2`, `SSLv3`, and `TLSv1.1` are not allowed.

Note: User password authentication occurs outside of the OpenSSL FIPS perimeter and can therefore support old passwords using insecure methods like MD5. It is recommended to ensure old passwords are updated to use the latest standards. If any exist, a list of accounts with MD5 passwords can be accessed by navigating to **MANAGEMENT** > **Security Dashboard** and under the **SECURITY ISSUES** tab.

FIPS Compliance Report

When the FIPS Compliance Report is generated it is logged under **TOOLS** > **Journal**. Administrators can download and view the FIPS Compliance Report by navigating to **MANAGEMENT** > **Security Dashboard**, and under the **FIPS 140-2** tab. Selecting the DOWNLOAD REPORT button will download both HTML and XML versions bundled in a zip file. The date and time the report was generated is displayed to the right of this button.



For more information on FIPS 140- 2, please refer to https://csrc.nist.gov/pubs/fips/140-2/upd2/final.

4.4.8 HTTPS Security Levels

VersaSync supports two different modes of HTTPS operation:

- The **Standard HTTPS Level** allows the use of medium strength ciphers and older TLS (Transport Layer Security) protocols,
- while the **High-Security Level** is restricted to strong ciphers and TLS version 1.2 exclusively.

While **Standard Mode** is the default setting, the **High-Security Level** is preferred (unless you require the extra compatibility), since **High Security** turns off TLSv1, which has known security vulnerabilities.

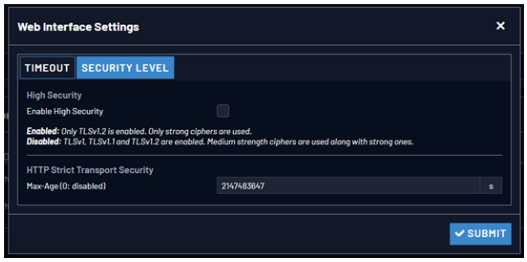
Browser Support

Note that the High Security Level requires the use of current browsers - as of July 2016, the oldest compatible clients include:
- Firefox® 27
- Chrome® 30
- Internet Explorer® 11
- Safari® 9.

(This is not an exhaustive list.)

To enable **High-Security HTTPS**:

1. Navigate to **MANAGEMENT > Network Setup**.
2. In the **Actions** Panel on the left, click on **Web Interface Settings**. The **Web Interface Settings** window will open.
3. Click on the tab **Security Level**:



4. Read the **Caution** statement and verify that you meet the requirements stated.
5. Check the box **Enable High Security**, and click Submit.
6. While it is NOT necessary to close the Web UI, and restart the browser, it is recommended to wait 90 seconds before continuing to use the Web UI, in order to allow the web server software to restart in the background.

It is also possible to disable High-Security HTTPS and TLS: Follow the procedure outlined above, but **un**check the box **Enable High Security**.

For more information on HTTPS certificates, see "HTTPS" on page 80.

4.5 Miscellanous Typical Configuration Tasks

4.5.1 REST API Configuration

REST (Representational State Transfer) API offers many benefits for customers who require additional configuration access. Any functionality that can be done manually through the Web UI can be scripted, creating machine-to-machine automation and communication.

Common tasks that would ordinarily require manual interaction with the Web UI can be scheduled and automated.

REST API is free and available on any VersaSync with Web UI communication.

You can find the latest REST API documentation related to the software version on your unit by signing in to the Web UI and navigating to **HELP > Download API Documentation**.

You can also visit rest-api-for-securesync-netclock-9400-and-versasync for the latest documentation.

4.5.2 Creating a Login Banner

A login banner is a customizable banner message displayed on the login page of the VersaSync Web UI. The login banner can be used, for example, to identify a unit.

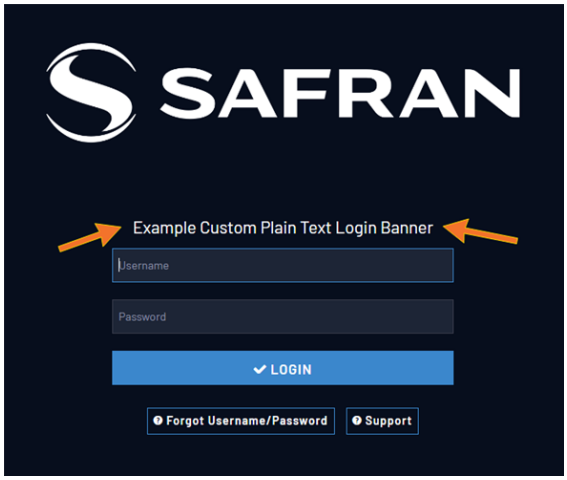


Figure 4-1: Login banner (example)

To configure a login banner:

1. Navigate to the **MANAGEMENT > Network Setup** screen.
2. In the **Actions** panel on the left, click **Login Banner**.
3. The **Network Access Banner** window will display. Check the box **Enable Custom Banner**.
4. In the **Plain Text Banner** text box, type in your custom text.

> **Note:** The Plain Text Banner is used to create a message for all interactive login interfaces (Web UI, telnet, SSH, FTP, SFTP, serial, etc.). It is not required to include HTML tags.

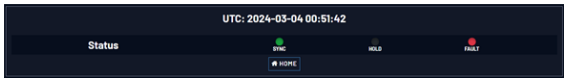
5. Optionally, you may also use the Web Interface Banner text box.

> **Note:** Enabling and using the Web Interface Banner text box will allow you to apply HTML formatting tags to your message (e.g., colors). Note that this functionality is limited to browser-based Web UI access.

6. To test your new banner, click **Apply** to see a preview at the bottom of the window. OR, click **Submit**, and log out of the Web UI, and back in so as to see the banner on the actual login page.

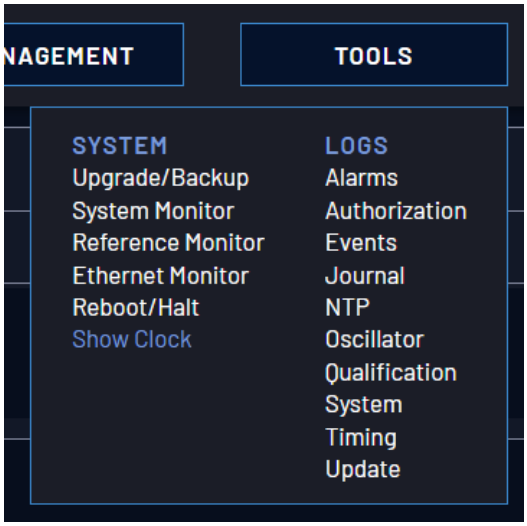
4.5.3 Show Clock

Instead of the Web UI, a large digital clock can be displayed on your computer screen. Next to the system status, the screen clock will display the UTC time, and the VersaSync System time.



To display the screen clock instead of the Web UI:

1. Navigate to **TOOLS** > **SYSTEM: Show Clock**:



2. To return to the standard Web UI, click **Home**.

4.5.4 Synchronizing Network PCs

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

4.6 Quality Management

4.6.1 System Monitoring

4.6.1.1 Status Monitoring via the Web UI

Detailed status information can be accessed via the VersaSync **Web UI**, such as:

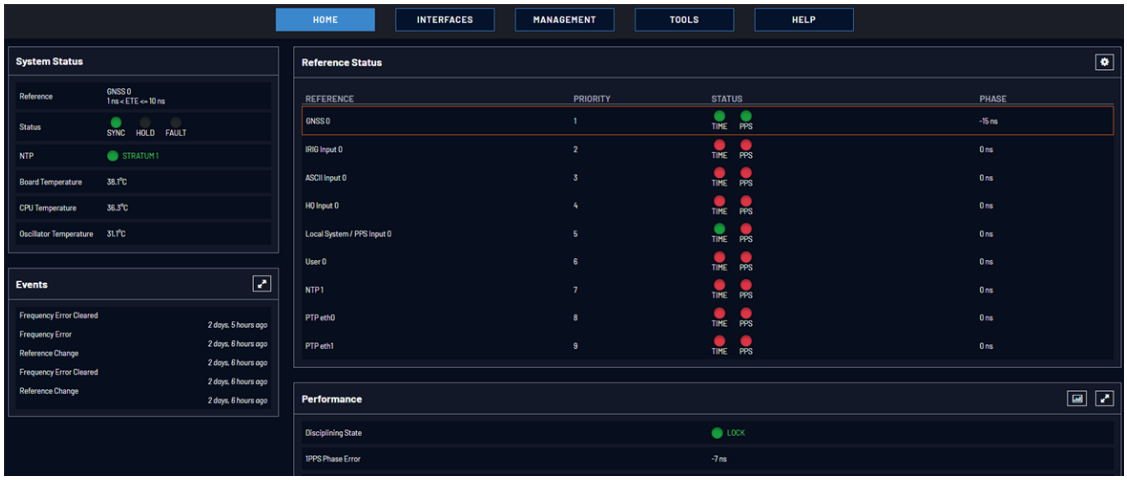
- Time synchronization status, including references
- GNSS satellites currently being tracked
- NTP sync status and current Stratum level
- Estimated time errors
- Oscillator disciplining
- Temperature monitoring

The **HOME** screen provides time server status information, while the **TOOLS** > **System Monitor** screen also displays hardware status data, e.g. temperature curves:

Status Monitoring via the HOME Screen

The **HOME** screen of the VersaSync Web UI provides a system status overview (see also "The Web UI HOME Screen" on page 23).

The **HOME** screen is divided into four panels:



System Status panel

- **Reference**—Indicates the status of the current synchronizing reference, if any.
- **Power**—Indicates whether the power is on.
- **Status**—Indicates the status of the network's timing. There are three indicators in the Status field:
  - **Sync**—Indicates whether VersaSync is synchronized to its selected input references.
    - **Green** indicates VersaSync is currently synchronized to its references.
    - **Orange** indicates VersaSync is not currently synchronized to its references.
  - **Hold**—When lit, VersaSync is in Holdover mode.
  - **Fault**—Indicates a fault in the operation of the VersaSync. See "Troubleshooting via Web UI Status Page" on page 328 for instructions for troubleshooting faults.
- **Alarm Status**—If a major or minor alarm is present, it will be displayed here.
- **NTP**—Current STRATUM status of this VersaSync unit.
- **Temperature**—The current board temperature will be displayed here.

Reference Status panel

- **REFERENCE**: Indicates the name type of each reference. These are determined by the inputs set up for the VersaSync
- **PRIORITY**: Indicates the priority of each reference. This number will be between 1 and 15. References in this panel appear in their order of priority. See "Configuring Input Reference Priorities" on page 189 for more information.
- **STATUS**: Indicates which available input reference is acting as the **Time** reference and which available input reference is acting as the **1PPS** reference.
  - **Green** indicates that the reference is present and has been declared valid.
  - **Orange** indicates the input reference is not currently present or is not currently valid.

Performance panel

- **Disciplining State**—Indicates whether or not the internal oscillator is currently being disciplined (steered to an input reference).

- **1PPS Phase Error**—An internal measurement (in nanoseconds) of the internal 1PPSs' phase error with respect to the selected input reference (if the input reference has excessive jitter, phase error will be higher)
- **10 MHz Frequency Error**—An internal estimated calculation (in Hertz) of the internal oscillator's frequency error, based on the phase accuracy error at the beginning and end of a frequency measurement window (the length of this window will vary depending upon the type of oscillator installed and the oscillator adjustment algorithm).

Events panel

The Events panel in the bottom-left corner of the **HOME** screen is a log of VersaSync's recent activity. It updates in real time.

Note: If you know the individual reference or output whose status you wish to see, you can access the Status window of that reference or output directly through the INTERFACES > REFERENCES or INTERFACES > OUTPUTS drop-down menu.

Status Monitoring via the System Monitor Screen

To display status information pertaining mainly to VersaSync's current hardware status, navigate to **TOOLS > SYSTEM > System Monitor**.

The information provided on the **System Monitor** Screen is subdivided into three panels:

System Status panel

This is identical with the HOME screen "System Status panel" on page 289.

Disk Status panel

This panel displays:

- Total: [MB]
- Used: [MB]
- Free: [MB]
- Percent: [%]

The last item refers to system storage. If you need to update the System Software, and this number is 70% or higher, it is recommended to clear logs and stats in order to free up memory space. (Navigate to **TOOLS > SYSTEM:**

Upgrade/Backup, and click the corresponding buttons in the lower left-hand corner.)

System Monitor panel

Graphs are displayed for:

- Board Temperature
- Memory Used
- CPU Used.

To delete the logged data used to generate the displayed graphs, click the TRASHCAN icon. (Note that re-populating the graphs with fresh data generated at a 1/min. rate will take several minutes.)

To download the logged data in `.csv` format, click the ARROW icon.

4.6.1.2 Ethernet Monitoring

To monitor Ethernet status and traffic:

1. Navigate to **TOOLS > SYSTEM: Ethernet Monitor**. The Ethernet monitoring screen opens:

The data displayed is linked to a specific Ethernet port e.g., ETH0. If you enable additional Ethernet ports, their throughput data will also be displayed.

In the **Traffic** pane on the right the traffic throughput in Bytes per second is displayed in two graphs. Drag the handles at the bottom of the graphs to zoom in on a particular time frame.

In the **Actions** panel on the left, you can clear or download monitoring data.

In the **Status** panel on the left, information pertaining to the given Ethernet port is displayed, including throughput statistics and error statistics. The Mode field indicates which transmission mode is being used for the given Ethernet port:

- **FULL** duplex, or
- **HALF** duplex.

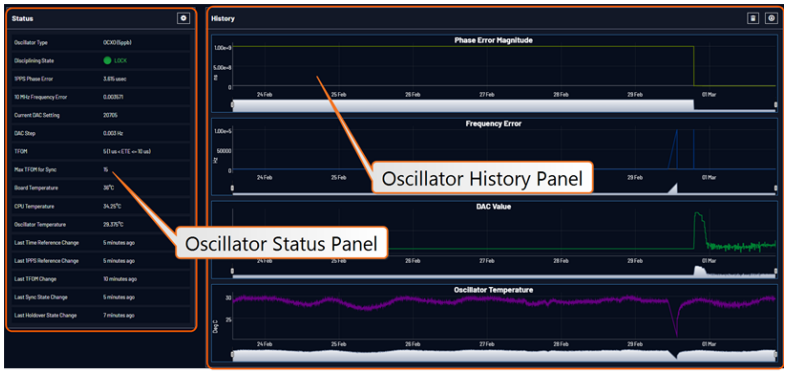
Note that the Mode is auto-negotiated by VersaSync. It can be changed only via the switch VersaSync is connected to, not by using the VersaSync Web UI.

4.6.1.3 Monitoring the Oscillator

The Oscillator Management screen provides current and history status information on disciplining state and accuracy.

To access the **Oscillator Management** screen:

1. Navigate to **MANAGEMENT > OTHER: Disciplining**.
2. The **Oscillator Management** screen will display. It consists of two panels:



The Oscillator Status Panel

This panel provides comprehensive information on the current status of VersaSync's timing state.

- Oscillator Type: Type of oscillator installed in the unit.
- Disciplining State: State of oscillator control and disciplining; indicates whether or not the internal oscillator is currently being disciplined (steered to an input reference). The states are: "Warm up", "Calibration", "Tracking Setup", "Lock State", "Freerun", and "Fault".
- 1PPS Phase Error: A tracking measurement [scaled time, in ns, or ms] of the internal 1PPSs' phase error with respect to the selected input reference. Long holdover periods or an input reference with excessive jitter will cause the phase error to be high. The oscillator disciplining control will gradually

reduce the phase error over time. Alternatively, restarting the tracking manually (see "Restart Tracking" under "Configuring the Oscillator" on page 239), or automatically via a pre-set Phase Error Limit, will quickly reduce the phase error.

- 10 MHz Frequency Error: An internal estimated calculation (in Hertz) of the internal oscillator's frequency error, based on the phase accuracy error at the beginning and end of a frequency measurement window (the length of this window will vary depending upon the type of oscillator installed and the oscillator adjustment algorithm).
- Current DAC Setting: Current DAC value, as determined by the oscillator disciplining system. The value is converted into a voltage that is used to discipline the oscillator. A stable value over time is desirable and suggests steady oscillator performance (see also the graph in the History Panel).
- DAC Step: Step size for adjustments to the internal oscillator, as determined by the oscillator disciplining system. Larger steps = quicker, but coarser adjustments. The step size is mainly determined by the type of oscillator.
- TFOM: The Time Figure of Merit is VersaSync's estimation of how accurately the unit is synchronized with its time and 1PPS reference inputs, based on several factors, known as the Estimated Time Error or ETE. The larger the TFOM value, the less accurate VersaSync believes it is aligned with its 1PPS input that is used to perform disciplining. If this estimated error is too large, it could adversely affect the performance of oscillator disciplining. The available TFOM range is 1 through 15.
- Max TFOM for Sync: Value, as set under "Configuring the Oscillator" on page 239
- Temperature(s): Three temperatures are displayed:
  - **Oscillator** temperature, which has an effect on oscillator accuracy, and therefore can be used to interpret oscillator performance.
  - **Board** temperature (measured on the main board, sometimes also referred to as 'System temperature')
  - **CPU** temperature

Note: Oscillator temperature is plotted over time in the History panel on the right, while graphs for board and CPU temperature can be found under TOOLS > SYSTEM: System Monitor.

- Last Time Reference Change: [Timestamp: Last occurrence]
- Last 1PPS Reference Change: [Timestamp: Last occurrence]
- Last TFOM Change: [Timestamp: Last occurrence]
- Last Sync State Change: [Timestamp: Last occurrence]
- Last Holdover State Change: [Timestamp: Last occurrence]

The Oscillator History Panel

The **Oscillator History Panel** offers real-time graphical monitoring of VersaSync's internal timing. The following graphs plot key oscillator-relevant data over time::

- **Phase Error Magnitude**: See 1PPS Phase Error
- **Frequency Error**: See 10_MHz_Frequency_Error
- **Scaled DAC Value**: See DAC Step
- **Oscillator Temperature**, which has an effect on oscillator accuracy, and therefore can be used to interpret oscillator performance.

You can **zoom** in on any of the graphs by grabbing the handles at either end and pulling them inwards. The graph will focus in on the time interval you choose in real time.

Clicking on the **Delete** icon in the top-right hand corner will erase all current oscillator log data.

Clicking on the **Download** arrow icon will download the latest oscillator log data as a .csv file.

4.6.1.4 NTP Status Monitoring

VersaSync's **NTP Status Summary** provides a means to monitor NTP status and performance parameters relevant to your VersaSync at a glance.

1. To access the **NTP Status Summary** panel, navigate to **MANAGEMENT > NETWORK: NTP Setup**.

2. The **NTP Status Summary** panel is at the lower left of the screen. The panel contains the following information:
   - **Selected Ref**—The reference VersaSync is currently using.
   - **Stratum**—This is the stratum level at which VersaSync is operating.
   - **Leap Indicator**—The leap indicator bits (usually 00). See "Leap Second Alert Notification" on page 182.
   - **Delay (ms)**—The measured one-way delay between VersaSync and its selected reference.
   - **Time Offset**—This is a graphical representation of the system time offset over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel containing a larger, more detailed view of the graph. See "The NTP Time Offset Performance Graph" on the facing page.
   - **Offset (ms)**—Displays the configured 1PPS offset values.
   - **Frequency Offset**—This is a graphical representation of the system frequency offset over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel containing a larger, more detailed view of the graph. See "The NTP Frequency Offset Performance Graph" on page 298.

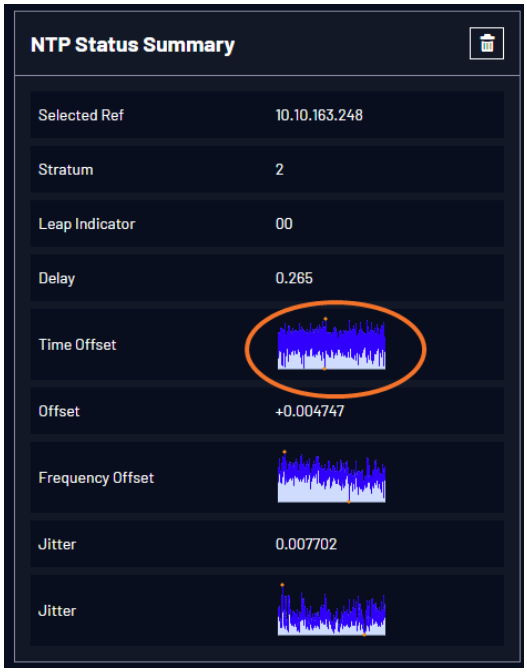
- **Jitter (ms)**—Variance (in milliseconds) occurring in the reference input time (from one poll to the next).
- **Jitter**—This is a graphical representation of the system jitter over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel containing a larger, more detailed view of the graph. See "The NTP Jitter Performance Graph" on page 300.

Note: This panel is updated every 30 seconds, or upon clicking the browser refresh button.

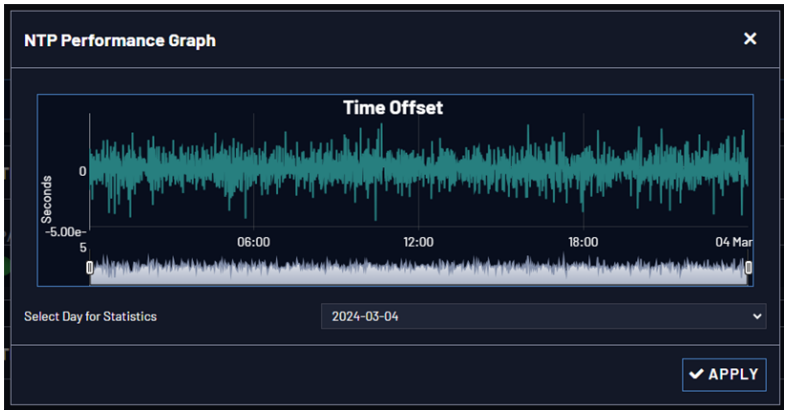
The NTP Time Offset Performance Graph

To view the NTP **Time Offset** performance graph:

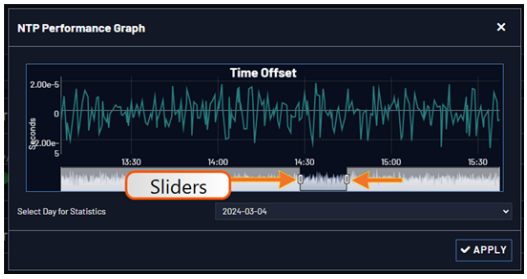
1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**.
2. In the **NTP Status Summary** panel locate the **Time Offset** graph.



3. Click the graph in the **NTP Status Summary** panel.
4. The **NTP Performance Graph** panel will appear.



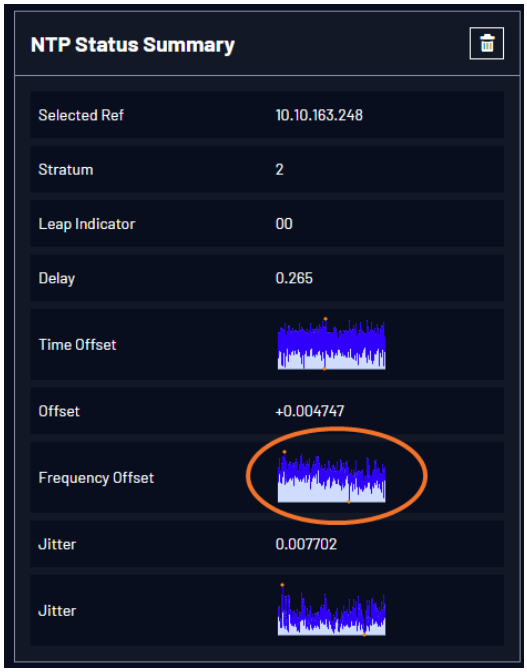
5. To select the statistics for a particular day, select a date from the drop-down list in the Select Day for Statistics field. The default date is the present date. Click **Apply**.
6. To display a higher resolution graph for a shorter time span, move one or both time sliders at the bottom of the graph inwards.



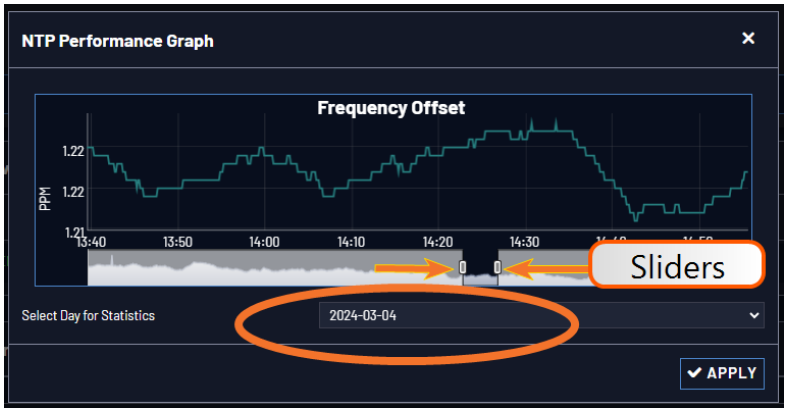
The NTP Frequency Offset Performance Graph

To view the NTP **Frequency Offset** performance graph:

1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**.
2. In the **NTP Status Summary** panel locate the **Frequency Offset** graph.



3. Click the graph in the **NTP Status Summary** panel.
4. The **NTP Performance Graph** panel will appear (the data may be displayed with a delay). The X-axis represents time, the Y-axis shows the frequency offset in parts-per-million (PPM); e.g. 290 PPM is equivalent to .0290 percent.



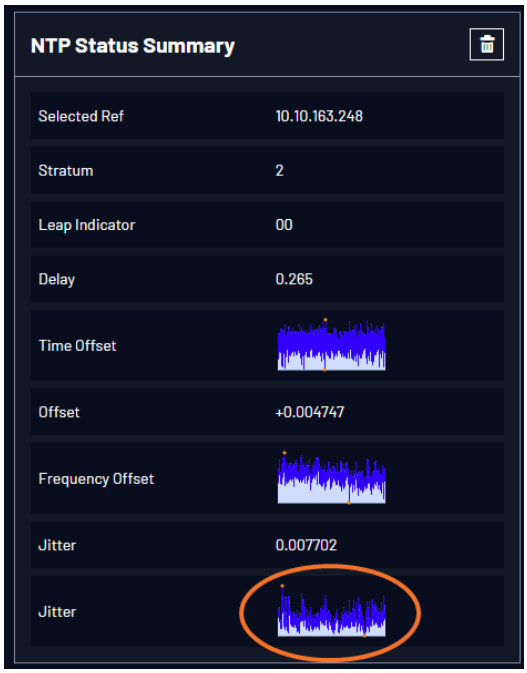
5. To select the statistics for a particular day, select a date from the drop-down list in the **Select Day for Statistics** field (highlighted in green in the illustration above). The default date is the present date. Click the **Apply** button.

» To display a higher resolution graph of a shorter time frame, move one or both of the two sliders inwards.

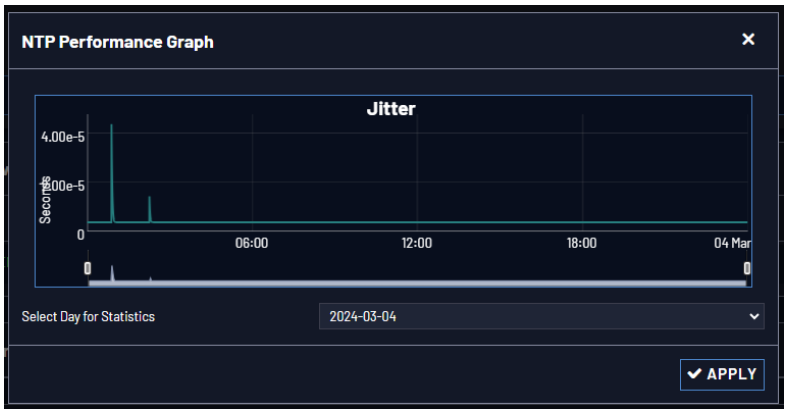
The NTP Jitter Performance Graph

To view the NTP **Jitter** performance graph:

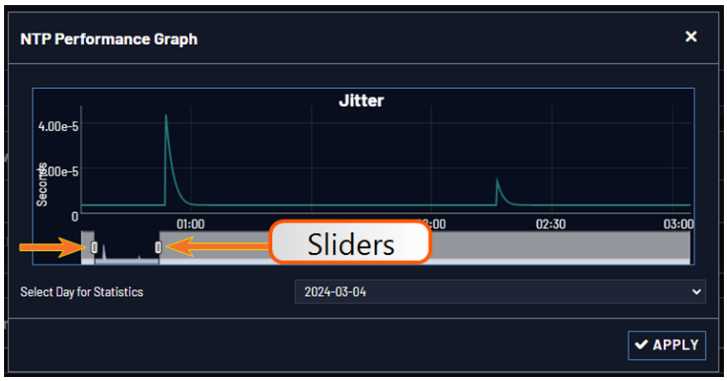
1. Navigate to **MANAGEMENT > NETWORK: NTP Setup** screen.
2. In the **NTP Status Summary** panel locate the **Jitter** graph.



3. Click the graph in the **NTP Status Summary** panel.
4. The **NTP Performance Graph** panel will appear.



5. To select the statistics for a particular day, select a date from the drop-down list in the **Select Day for Statistics** field. The default date is the present date. Click the **Apply** button.
   - » To display a higher resolution graph for a shorter time span, move one or both time sliders at the bottom of the graph inwards.



4.6.2 Logs

VersaSync maintains different types of event logs (see below) to allow for traceability, and for record keeping. Should you ever require technical support from Safran, you may be asked for a copy of your logs to facilitate remote diagnosis.

Logs stored internally are being kept automatically, while the storage of log files in a remote location has to be set up by the user.

For each type of log, four 75 KB files are maintained internally on a revolving basis, i.e. the oldest file will be overwritten, as soon as all four files have filled up with event data. The life expectancy of a log file depends on the amount of data accumulating over time: Some types of logs will fill up within days, while others can take months until they have reached their maximum storage capacity.

You can delete logs at any time, see "Clearing All Logs" on page 311.

4.6.2.1 Types of Logs

VersaSync generates log files for the following event categories:

Alarms Log

Displays log entries for the Timing System, for example:

- » **The Unit has Rebooted**: VersaSync 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**: VersaSync is synchronized to its selected Time and 1PPS reference inputs.
- **Not In Sync**: VersaSync is not synchronized to its Time and 1PPS inputs and is not currently in Holdover. NTP will indicate to the network that it is Stratum 15 and so the time server likely be ignored as a time reference.
- **Frequency Error**: The oscillator's frequency was measured and the frequency error was too large. Or, the frequency couldn't be measured because a valid input reference was not available.
- **Reference change**: VersaSync 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. VersaSync 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.

Authentication Log

Displays log entries for authentication events (e.g., unsuccessful login attempts, an incorrectly entered password, etc.) that are made to VersaSync's command line interfaces (such as telnet, SSH, FTP, etc.).

Events Log

Displays log entries related to GNSS reception status changes, Sync/Holdover state changes, SNMP traps being sent, etc. Examples include:

- **Reference Change**: VersaSync 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 VersaSync). 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**: VersaSync is synchronized to its Time and 1PPS inputs.
- **Not In Sync**: VersaSync is not synchronized to its Time and 1PPS inputs and is not currently in Holdover. NTP will indicate to the network that it is Stratum 15 and so the time server likely be ignored as a time reference.
- **Sending trap for event 1 (SNMPSAD)**: An SNMP trap was sent by the SNMP agent to the SNMP Manager. The event number in this entry indicates which SNMP trap was sent.
- **The Unit has Rebooted**: VersaSync was either rebooted or power cycled.

Journal Log

Displays log entries created for all configuration changes that have occurred (such as creating a new user account, for example).

NTP Log

The NTP log displays operational information about the NTP daemon, as well as NTP throughput statistics (e.g., packets/sec.). Examples for entries in this log include indications for when NTP was synchronized to its configured references (e.g., it became a Stratum 1 time server), as well as stratum level of the NTP references.

The NTP throughput statistics data can be utilized to calculate mean values and the standard deviation.

Example log entries include:

- **Synchronized to (IP address), stratum=1**: NTP is synchronizing to another Stratum 1 NTP server.
- **ntp exiting on signal 15**: This log entry indicates NTP is now indicating to the network that it is a Stratum 15 time server because it is not synchronized to its selected reference.
- **Time reset xxxxx s**: These entries indicate time corrections (in seconds) applied to NTP.
- **No servers reachable**: NTP cannot locate any of its configured NTP servers.
- **Synchronized to PPS(0), stratum=0**: NTP is synchronized using the PPS reference clock driver (which provides more stable NTP synchronization).

Oscillator Log

Displays log entries related to oscillator disciplining. Provides the calculated frequency error periodically while synchronizing to a reference.

GPS Qualification Log

If VersaSync 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), VersaSync 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 VersaSync 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, VersaSync 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 VersaSync is not connected to a GNSS antenna, this log will remain empty.

System Log

Displays log entries related to the Timing System events and daemon events (such as the Alarms, Monitor, Notification, or SNMP daemons starting or stopping, etc.)

Timing Log

Displays log entries related to Input reference state changes (for example, IRIG input is not considered valid), antenna cable status. Examples include:

- **GRGR = GNSS Reference[1] antenna fault**: The GNSS Antenna Problem alarm indicates the GNSS receiver has detected an over-current or undercurrent condition (an open or short exists in the GNSS antenna cable, or the GNSS antenna is not connected to VersaSync). 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.

Update Log

Displays log entries related to software updates that have been performed.

4.6.2.2 The Logs Screen

The **Logs** Screen provides access to settings that apply to all logs.

To access the Logs Screen:

1. Navigate to **MANAGEMENT** > **OTHER**: **Log Configuration.**
2. The **Logs** screen will appear, with several panels:

[1] GR = GNSS Reference

The Logs Actions panel

The **Actions** panel on the upper-left corner of the **Logs** screen allows you to perform batch actions on your logs:

- **Save and Download All Logs**—Save and download all the logs on VersaSync.
- **Clear All Logs**—Clear all the logs on VersaSync.

The Remote Log Server panel

The **Remote Log Server** panel, which is where you set up and manage logs on one or more remote locations. See also: "Setting up a Remote Log Server" on page 310.

The Logs Settings panel

The **Settings** panel allows you you change log settings for your product. These settings apply to all logs.

- **Persistence** allows the unit to retain logs permanently.
  - When Persistence is ON [default] , your logs will be retained on the disk and will always be available for troubleshooting and informational purposes.
  - When Persistence is OFF, logs will be overwritten over time by the most recent information. Logs will also be removed upon reboot of the unit.

    This setting will increase the disk lifetime by reducing the amount of permanently stored data.

The Local Logging panel

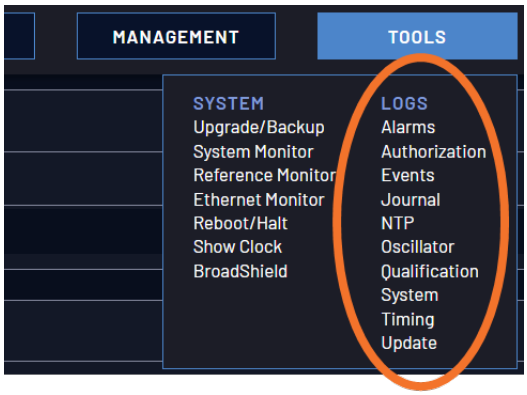
The Local Logging panel will control the local logging (logs stored directly on the unit) for each log individually.

- Each log defaults to logging locally unless the user turns off the logging for a particular log directly.
- To turn off local logging, simply switch the toggle to OFF in the Local Logging Panel. See "Types of Logs" on page 301 for information on each log type.

4.6.2.3 Displaying Individual Logs

To access individual VersaSync logs:

1. From the **TOOLS** drop-down menu, select the desired **Logs** category (for example, “Alarms”, or “Events”) from the right-hand column.

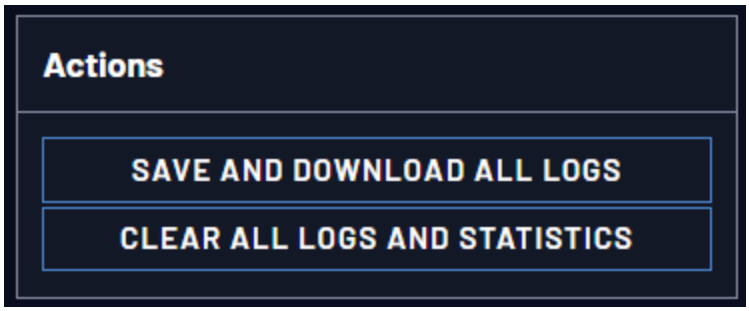


4.6.2.4 Saving and Downloading Logs

The VersaSync Web UI offers a few convenient ways to save, bundle, and download all logs in one simple step. This feature may be useful when archiving logs, for example, or for troubleshooting technical problems: Safran Technical Support/Customer Service may ask you to send them the bundled logs to remotely investigate a technical concern.

To save, bundle, and download all logs:

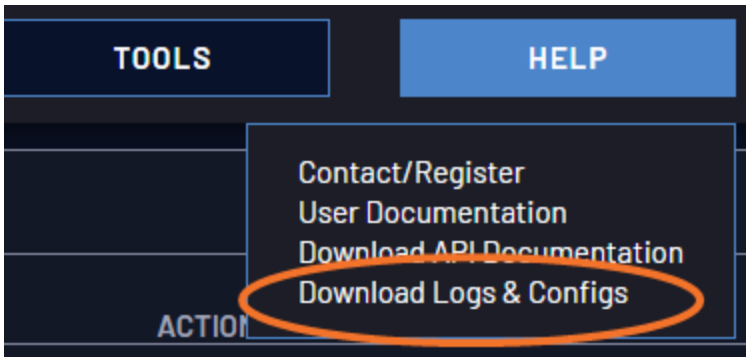
1. Navigate to **MANAGEMENT > OTHER: Log Configuration**.
2. On the left side of the screen, in the **Actions** panel, click on the **Save and Download All Logs** button.



3. Select the log bundle save locaion. The file name is logs.tar.gz
4. If so asked by Safran Technical Support, attach the bundled log files (typically together with the oscillator status log, see: "Saving and Downloading the Oscillator Log" on the facing page) to your email addressed to SafranTechnical Support.

To save, bundle, and download all logs AND current configs, there is a shortcut in the HELP menu:

1. Navigate to **HELP > Download Logs & Configs**.



2. The logs and current configuration files will be automatically downloaded.

Saving and Downloading the Oscillator Log

The oscillator status log captures oscillator performance data, such as frequency error and phase error. The data can be retrieved as a comma-separated .csv file that can be read and edited with a spreadsheet software, such as Microsoft Excel®. You may want to review and/or keep this data for your own records, or you may be asked by Safran Technical Support to download and send the oscillator status log in the event of technical problems.

To download the oscillator status log:

1. Navigate to **MANAGEMENT > OTHER: Disciplining**.
2. Click on the ARROW icon in the top-right corner of the screen. Save the .csv file to your computer.

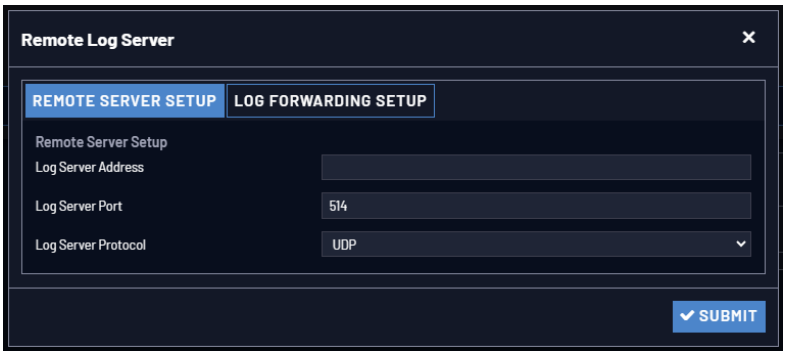
3. If so asked by Technical Support, attach the oscillator status log file (typically together with the bundled VersaSync log files, see: "Saving and Downloading Logs" on the previous page) to your email addressed to Safran Technical Support.

4.6.2.5 Setting up a Remote Log Server

Storing log files on a remote log server supports advanced logging functionality.

Adding a remote log server:

1. Navigate to **MANAGEMENT > OTHER: Log Configuration.**
2. In the **Remote Log Server** panel, click on the PLUS icon in the top-right corner of the panel. The **Add Remote Log Servers** window displays.



3. Enter the IP address or host server name (e.g., “MyDomain.com”) you want to use as a remote log server.
4. Click the **Submit** button.
5. Your remote log server will appear in the **Remote Log Server** panel.
6. This action will configure all logs to be sent to the remote server together.

Changing or deleting a remote log server:

1. Navigate to **MANAGEMENT > OTHER: Log Configuration**.
2. In the **Remote Log Server** panel locate the remote server you wish to change or delete.

3. Choose the MINUS button to delete the remote log server. Confirm by clicking OK in the message window.

—OR—

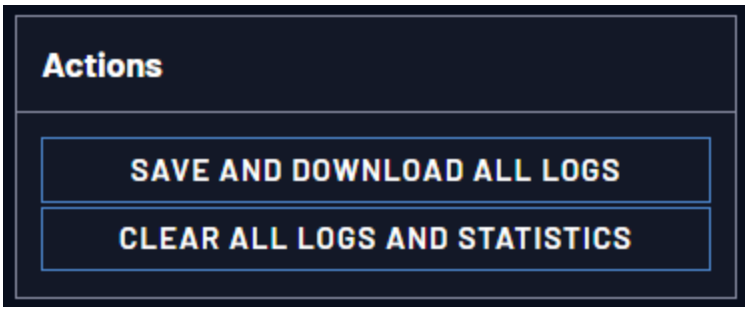
3. In the **Remote Log Server** panel, click the GEAR button to change the remote log server. Type in a new IP address or host domain server (e.g., MyDomain.com).

4.6.2.6 Clearing All Logs

All local logs in the `home/spectracom` directory will be logged. Other logs e.g., located on Syslog Servers, must be maintained by the user.

To clear all locally stored log files:

1. Navigate to **MANAGEMENT > OTHER: Log Configuration**.
2. In the **Actions** panel, click **Clear All Logs**:



3. In the grey confirmation window, click **OK**.

4.7 Updates and Licenses

4.7.1 Software Updates

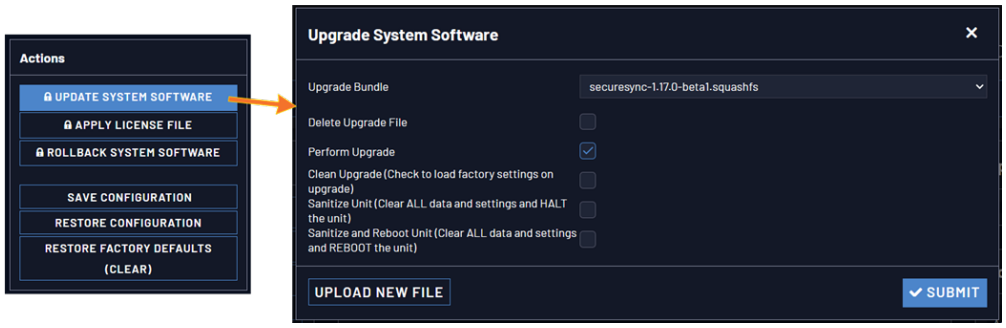
Safran periodically releases new versions of software for VersaSync. These updates[1] are offered for free and made available for download from the Safran website. If you register your product, you will be notified of software updates.

To carry out a software update:

1. In the Web UI, navigate to **Tools** > **Upgrade/Backup**.
2. Determine your System software version in the System Configuration panel: Proceed to the next step if it is lower than the software version you plan on installing.

[1]The terms update and upgrade are both used throughout Safran technical literature, as software releases may include fixes and enhancements, as well as new features.

3. Download the latest upgrade software bundle from the Safran website onto your PC.
4. Perform the actual upgrade by navigating to **TOOLS** > **Upgrade/Backup** > **Actions**: **Update System Software**. Upload the upgrade software bundle previously downloaded onto your PC (`updateXYZ.squashfs`).



   Once you have uploaded the software bundle, the following checkbox options will be presented:

   - **Delete Upgrade File**: Cancel the upgrade, and remove the uploaded software bundle from the system.
   - **Perform Upgrade**: Perform the software upgrade.
   - **Clean Upgrade**: Factory settings will be applied during the upgrade; any custom settings you may have applied previously will be over-written! This also includes the unit's static IP address (if you applied one): it will be replaced by the default DHCP address (i.e., 0.0.0.0.) Also note that the browser session will terminate: After reconfiguring the unit's IP address, you will need to login to the Web UI in a new browser session.
   - **Sanitize Unit**: Factory settings will be applied during the upgrade. In addition, logs and all other file system user data is overwritten. Roll-back to the state of the unit prior to sanitization will not be possible. Upon completion, the unit will be halted and power must be removed (unplugged) and reapplied in order to restart the unit.
   - **Sanitize and Reboot Unit**: Factory settings will be applied during the upgrade. In addition, logs and all other file system user data is over-written. Rollback to the state of the unit prior to sanitization will not be possible. Upon completion, the unit will be rebooted.

5. Click **Submit** to carry out the update. A progress bar will estimate status information:

6. Verify that the update was successful: Navigate to **Tools** > **Upgrade/Backup**, and confirm the new SW version in the **System Configuration** panel.

Note: Upgrade, license, and patch files uploaded via the Web UI can only be accessed and executed from the Web UI at /var/lib/spui. Files uploaded via the CLI can only be accessed from the CLI at home/spectracom.

Note: Should you use DHCP, a new IP address may be assigned to your unit, and you may have to point your web browser to it.

Note: In the event that the update failed, see "Troubleshooting Software Update" on page 333.

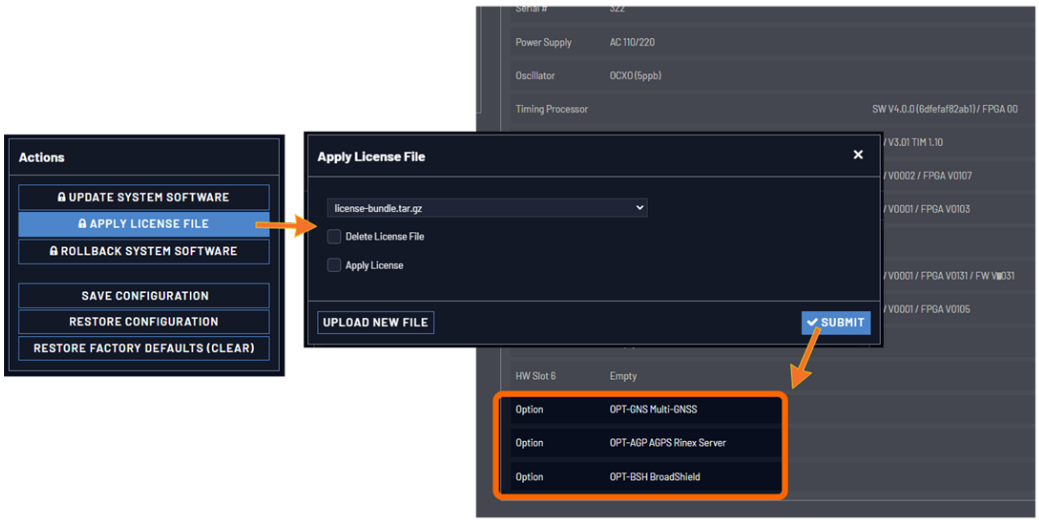
4.7.2 Applying a License File

Software options must be activated by applying a license file (OPT-xyz):

Typically, VersaSync units are shipped with the license file pre-installed, reflecting the system configuration as ordered. If, however, a feature is to be activated after delivery of the VersaSync unit, please contact your local Safran Sales Office first to have a license file generated. License files are archive files with a `tar.gz` extension. One license file may contain multiple licenses for multiple products.

To apply the license file, you need to upload it into your VersaSync unit and install it:

1. Save the license file `license.tar.gz` to a location on your PC (which needs to be connected to the same network VersaSync is.)
2. Open the VersaSync Web UI, and navigate to **Tools** > **Upgrade/Backup**:



3. In the **Actions** panel, click **Apply License File**.
4. In the **Apply License File** window, click **Upload New File**.
5. In the **Upload File** window, click **Choose File**. Using the Explorer window, navigate to the location mentioned under the first step, select the license file, and monitor the installation progress in the **Status Upgrade** window until the application has rebooted.
6. Refresh the browser window, and login to the Web UI again. Re-navigate to **Tools** > **Upgrade/Backup**, and confirm that the newly installed Option is listed in the **System Configuration** panel.

Note: Upgrade, license, and patch files uploaded via the Web UI can only be accessed and executed from the Web UI at /var/lib/spui. Files uploaded via the CLI can only be accessed from the CLI at home/spectracom.

4.8 Resetting the Unit to Factory Configuration

In certain situations, it may be desired to reset all VersaSync configurations back to the factory default configuration. The GNSS location, any VersaSync configurations and the locally stored log files can be cleared via the Web UI.

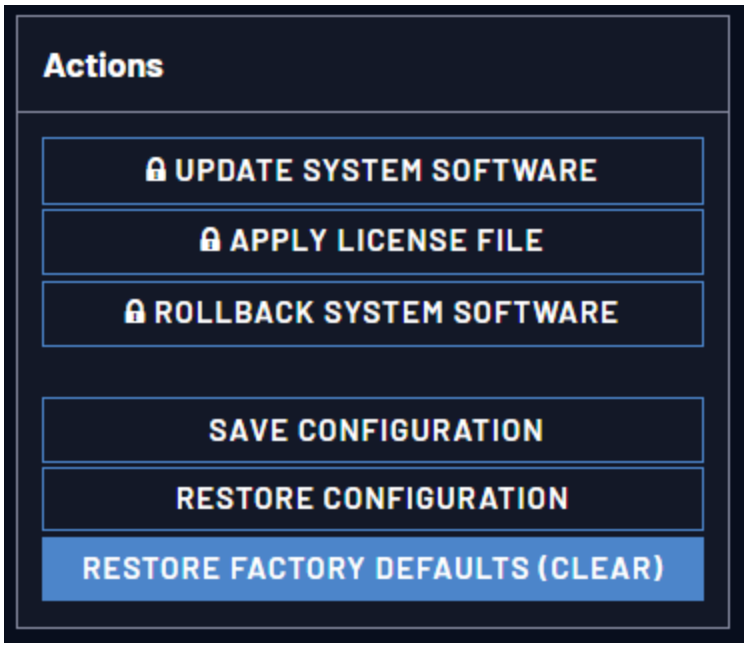
Note: Restoring configurations (reloading a saved configuration), erasing the stored GNSS location and clearing the log files are separate processes. You may restore one without restoring the others.

If VersaSync 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.

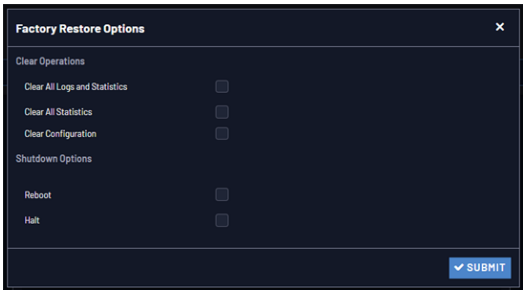
4.8.1 Resetting All Configurations to their Factory Defaults

To restore the configuration files to their factory defaults:

1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. In the **Actions** panel, click the **Restore Factory Defaults (Clear)** button.



3. In the Factory Restore Options panel, choose your options for the restore:



Clear All Logs erases all logs
Clear All Stats will clear NTP stats, PTP stats, and all database tables
Clear Configuration clears any user configuration, including network settings
Reboot restarts the unit after the clear.
Halt puts the unit in a halted stated after performing the clear.

4. Click on Submit to finalize the commands.

4.8.2 Backing-up and Restoring Configuration Files

Once VersaSync has been configured, it may be desired to back up the configuration files to a PC for off-unit storage. If necessary in the future, the original configuration of the VersaSync can then be restored into the same unit.

The capability to backup and restore configurations also adds the ability to "clone" multiple VersaSync units with similar settings. Once one VersaSync 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 VersaSync unit for duplicate configurations.

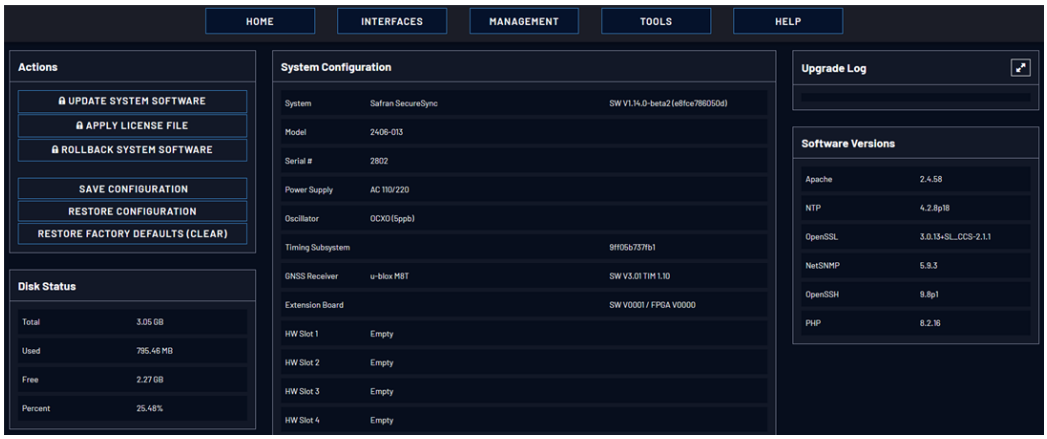
There are several configuration files that are bundled in one file for ease of handling.

Note: For security reasons, configurations relating to security of the product, such as SSH/SSL certificates, cannot be backed up to a PC.

4.8.2.1 Accessing the System Configuration Screen

The System Configuration Screen provides comprehensive information about hardware and software status. To access the **System Configuration** screen:

1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. The **System Configuration** screen will display:



The **System Configuration** screen consists of 5 panels:

The Actions panel

The **Actions** panel is used for updating the system software, managing license files, saving and restoring the configuration files, and restoring the factory defaults.

The System Configuration panel

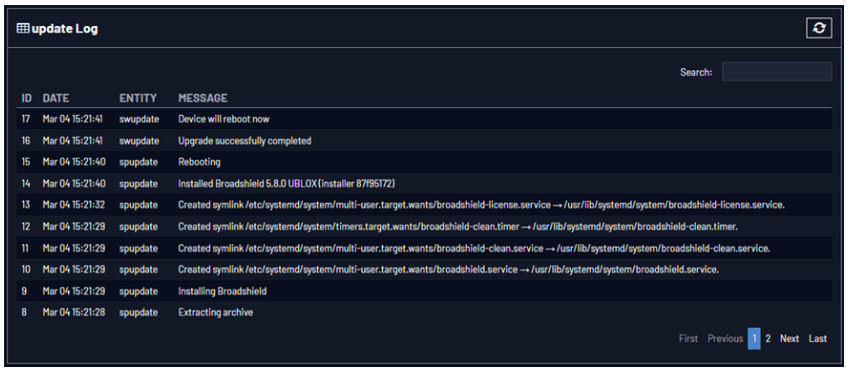
The **System Configuration** panel provides the following information:

- **System**—The model name of this unit, and the software version currently installed.
- **Model**—The model number of this unit.
- **Serial Number**—The serial number of this unit.
- **Power Supply**—The type of power supply installed in this unit. This can be AC, DC or both.
- **Oscillator**—The type of internal timing oscillator installed in this unit.
- **Timing Processor**—The timing processor in use with this unit.
- **GNSS Receiver**—The GNSS receiver in use with this unit.
- **Option**—The optional features also included on this unit.

The Upgrade Log panel

The upgrade log is a running log of system upgrades, used for historical and troubleshooting purposes. It can be expanded by clicking on the DIAGONAL

ARROWS icon in the top-right corner:



Each log entry is comprised of a unique ID, the date the entry was created, the originator of the entry, and the actual message. Refresh the log by clicking the CIRCLE ARROWS icon in the top-right corner. Go to the First, Last, or Previous entries by clicking the corresponding buttons in the bottom-right corner.

The Disk Status panel

The Disk Status panel provides information on the memory usage. This information is relevant for troubleshooting purposes, and when preparing the system for a software update.

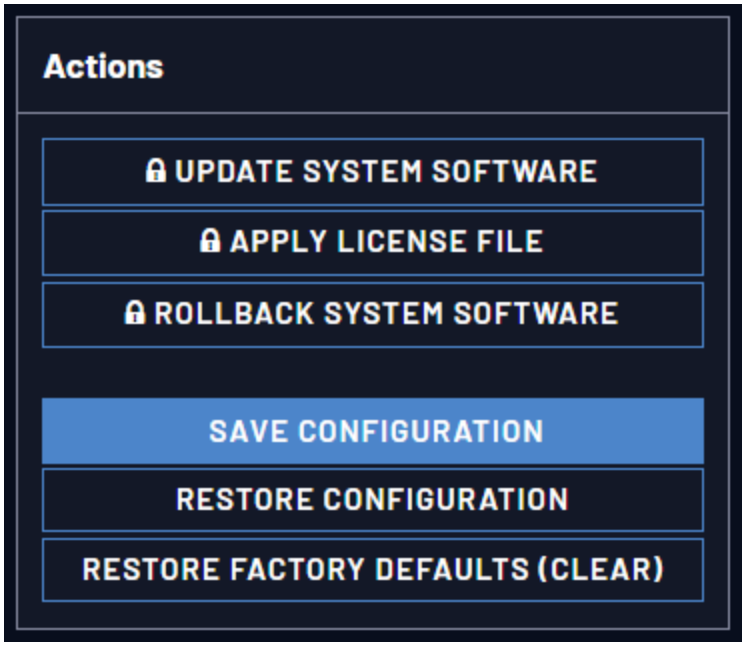
The Software Versions panel

This panel provides version information on the different SW components utilized by the system.

4.8.2.2 Saving the System Configuration Files

To save (back up) the system configuration files:

1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. In the **Actions** panel, click the **Save Configuration** button.



3. Click **OK** in the grey confirmation window that displays.
4. Save the configuration file to a directory where it will be safe. VersaSync simultaneously saves a file at `/home/spectracom/xfer/config/config.tar`.

To save, bundle, and download all logs AND current configs:

1. Navigate to **HELP > Download Logs & Configs**.
2. The logs and current configuration files will be automatically downloaded.

4.8.2.3 Uploading Configuration Files

To upload configuration files from a PC:

1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. In the **Actions** panel, click the **Upload Configuration** button.
3. Click **Choose File** in the window that displays, and navigate to the directory on your PC where the bundled file is stored.
4. Click the **Upload** button. VersaSync saves the uploaded bundled file in the `/home/spectracom/xfer/config/`directory.

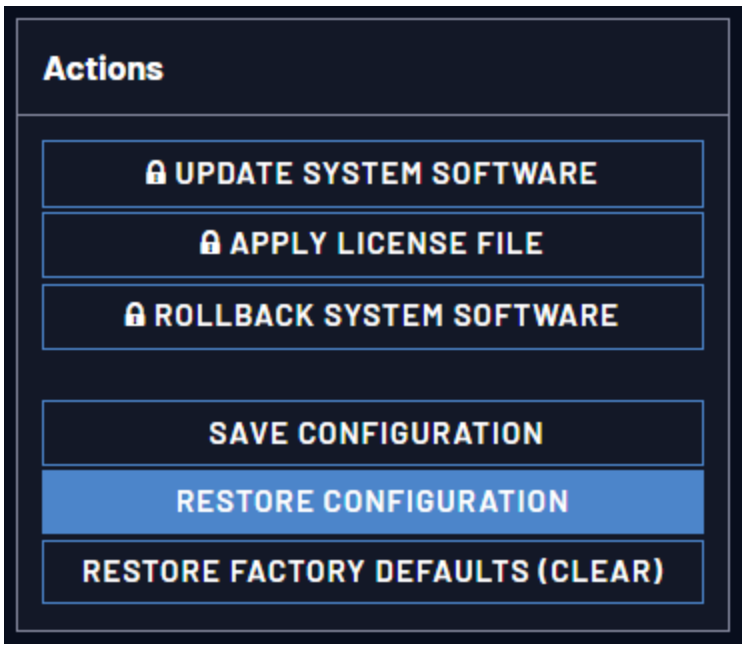
> **Note:** When uploading files remotely via long distances, or when uploading multiple files via several browser windows simultaneously, the upload process may fail to complete. In this case, cancel the upload by clicking X, and go back to Step 2.

5. To use the new configuration file for this VersaSync, click the **Restore Configuration** button, and follow the procedure described under 320.

4.8.2.4 Restoring the System Configuration

To restore the System Configuration:

1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. In the **Actions** panel, click **Restore Configuration**.



3. Click **OK** in the grey confirmation window. The system will restore the configuration using the bundled file stored at `/home/spectracom/xfer/config/VersaSync.conf`, then reboot in order to read the new configuration file. Once powered back up, VersaSync will be configured with the previously stored file.

4.8.2.5 Restoring the Factory Defaults

For instructions on how to restore the VersaSync's configuration files to their factory default settings see "Resetting All Configurations to their Factory Defaults" on page 315.

4.8.3 Default and Recommended Configurations

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

Table 4-1: Default and recommended configurations

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

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

4.8.4 Sanitizing the Unit

The concept of sanitizing a VersaSync unit refers to erasing usage data that may be stored in volatile and/or non-volatile memory, i.e. permanently eliminating any data that could be used to trace the unit's former usage. This data may include – but is not limited to – logs, configuration settings, IP addresses, passwords, GNSS geographic positioning data, option card data, and network-specific usage data.

The VersaSync has a built-in process to sanitize all usage data. This process leverages the upgrade process in order to execute the following functions:

- Performing simultaneous "clean" upgrades on both software partitions, rewriting all software to the uploaded version and erasing all user data, logs, and configurations.
- The GNSS receiver's location data is deleted via a cold reset, and is prevented from obtaining more information until electrically power cycled.
- Rewriting all eMMC data in two wipes and two confirmations and two upgrades total.
- Feedback during the process will be provided through the serial connection.
- After sanitizing all data, the unit will be brought into a HALT state.

4.8.4.1 Sanitizing Process

These are the steps to complete the data sanitizing process:

1. Disconnect all physical connection to GNSS receivers (this includes SAASM receivers and STL, if you have those configurations).
   Note: If you have a SAASM receiver installed, you will need to perform the zeroize function (reference the SAASM addendum for more information).
2. From the Safran Trusted 4D website, download the software version that you would like your unit to be set to after sanitizing.
3. Log in to the Web UI as an admin user and navigate to **TOOLS > Upgrade/Backup**. In the Actions panel, select **Update System Software**.
4. Upload the software upgrade file previously chosen to overwrite your system and select **Upload**.
5. Once the upload is successful, select **Perform Upgrade** and **Sanitize Unit**. Choose Submit and then select OK in the confirmation dialog.
6. The unit will undergo the full sanitization procedure (the entire process will take approx. 20 minutes and may take longer depending on unit

configuration). The front panel LEDs will illuminate in order from left to right scrolling and remain fully lit to simulate a progress bar. The rightmost LED will be the last to remain flashing, and this will indicate that the unit is on the final step.

7. After the unit is fully halted (no LEDs will be flashing), the process is finished and you can safely remove power. At this point, no user data or usage data exists on the unit.

Serial Feedback

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

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

4.8.4.2 Further Reading

Additional information regarding Sanitization and Volatility may be found in the Safran website. To obtain a Certificate of Volatility for VersaSync, contact Safran Trusted 4D Technical Support (see "Technical Support" on page 422).

BLANK PAGE.

APPENDIX

Appendix

The following topics are included in this Chapter:

5.1 Troubleshooting

The Web UI provide VersaSync status information that can be used to help troubleshoot failure symptoms that may occur.

5.1.1 Minor and Major Alarms

Minor Alarm

There are several conditions that can cause the Web UI status lights to indicate a Minor alarm has been asserted. These conditions include:

- **Too few GPS satellites, 1st threshold**: The GNSS receiver has been tracking less than the minimum number of satellites for too long of a duration. Refer to "Troubleshooting GNSS Reception" on page 331 for information on troubleshooting GNSS reception issues.

Major Alarm

There are several conditions that can cause the Web UI status lights to indicate a Major alarm has been asserted. These conditions include:

- **Frequency error**: Indicates a jump in the oscillator's output frequency has been detected. Contact Tech Support for additional information.
- **1PPS is not in specification**: The 1PPS input reference is either not present or is not qualified.
- **Not In Sync**: A Major alarm is asserted when the Timing System is not in sync (Input references are not available and the unit is not in Holdover). Examples of not being synced include:
  - When the Timing System has just booted-up and has not yet synced to a reference.
  - When all input references were lost and Holdover Mode has since expired.
- **Timing System Error**: A problem has occurred in the Timing System. Contact Safran technical support if the error continues.
- **Timing System Hardware Error**: An issue has been detected with the unit hardware. One possible cause is that the oscillator is not functioning properly.

5.1.2 Troubleshooting: System Configuration

One of the first tasks when troubleshooting a unit is to read out the current system configuration (you may also be asked for this when contacting Safran Technical Support.)

Select **TOOLS** > **Upgrade/Backup**: The screen displayed will provide information on:

- System configuration
- Disk status, memory status
- Software versions, and
- Recent log entries.

5.1.2.1 System Troubleshooting: Browser Support

Safran recommends using Web browsers that have been released or updated within the last year. The VersaSync Web UI does not support Internet Explorer or Edge HTML.

Using different or older browsers may lead to some incompatibility issues.

5.1.3 Troubleshooting – Unable to Open Web UI

With VersaSync connected to either a stand-alone or networked PC and with the network configuration correct, it should be possible to connect to the Web UI.

Cable connectivity issue:

- Verify one end of standard network cable is connected to VersaSync's Ethernet port and other end is connected to a hub/switch. Or a network cable is connected to VersaSync and a stand-alone PC.
- Verify network settings of VersaSync are valid for the network/PC it is connected with (IP address is on the same subnet as the other PC).

Communication issue:

- Disconnect VersaSync's network cable and ping its assigned address to ensure no response (no duplicate IP addresses on the network).
- Try accessing VersaSync from another PC on the same network.
- Network Routing/firewall issue. Try connecting directly with a PC and network cable.

5.1.4 Troubleshooting via Web UI Status Page

VersaSync's Web UI includes pages that provide current "remote" status information about VersaSync. The following table includes information that can be used as a troubleshooting guidance if status fault indications or conditions occur.

Table 5-1: Troubleshooting using the Web UI Status indications

Web UI Page location	Current Status	Indication	Troubleshooting
HOME page, System Status panel, Status row	SYNC indicator is not “lit” (not Green).HOLD indicator is “lit” (Orange).—OR—FAULT indicator is “lit” (Red). Below the System Status panel there is an Out of Sync alarm statement	VersaSync is in Holdover mode—OR—VersaSync is now out of Time Sync	All available Input References have been lost. The Reference Status table on the HOME page will show the current status of all inputs (Green is valid and Red is invalid or not present). 1. Make sure the Input Reference Priority table still has the desired reference inputs Enabled, based on the desired priority. See "Configuring Input Reference Priorities" on page 189. 2. Make sure the desired input references are still connected to the correct input port of VersaSync. 3. Verify GNSS antenna installation (if applicable). See "Troubleshooting GNSS Reception" on page 331.

Web UI Page location	Current Status	Indication	Troubleshooting
MANAGEMENT/ NTP Setup page NTP Status Summary panel Stratum row	Stratum 15	NTP is not synchronized to its available input references (VersaSync may have been in Holdover mode, but Holdover has since expired without the return of valid inputs)	Note: If VersaSync was just recently powered-up or rebooted and input references are applied, no troubleshooting may be necessary. Allow at least 10-20 minutes for the input references to be declared valid and NTP to align to the System Time (allow an additional 35-40 minutes for a new install with GNSS input). 1. Verify in the Configure Reference Priorities table that all available references enabled. See "Configuring Input Reference Priorities" on page 189. 2. Verify that the Reference Status on the HOME page shows “OK” (Green) for all available references. 3. Verify NTP is enabled and configured correctly. See "NTP Reference Configuration" on page 120.
MANAGEMENT/ NETWORK page	Cannot login or access the Web UI.	The following error message is displayed: “Forbidden You don’t have permission to access/ on this server”	This message is displayed when any value has been added to the Network Access Rules table and your PC is not listed in the table as an Allow From IP address. To restore access to the Web UI, either 1. Login from a PC that is listed as an Allow From in this table; or 2. If it is unknown what PCs have been listed in the Access table, perform an `unrestrict` command to remove all entries from the Network Access Rules table. This will allow all PCs to be able to access the Web UI.

5.1.5 Troubleshooting GNSS Reception

If VersaSync reports GPS, Holdover, and/or Time Sync Alarms caused by insufficient GNSS reception:

When a GNSS receiver is installed in VersaSync, a GNSS antenna can be connected to the rear panel antenna connector via a coax cable to allow it to track several satellites in order for GNSS to be an available input reference. Many factors can prevent the ability for the GNSS receiver to be able to track the minimum number of satellites.

With the GNSS antenna installed outdoors, with a good view of the sky (the view of the sky is not being blocked by obstructions), VersaSync 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, VersaSync may not initially be able to go into time sync. Or, if GNSS reception is subsequently lost after initially achieving time sync, VersaSync will go into the Holdover mode. If GNSS reception is not restored before the Holdover period expires (and no other input references become available) VersaSync 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 VersaSync, please refer to the **GNSS Reception Troubleshooting Guide**, available here on the Safran website.

5.1.6 Troubleshooting – 1PPS, 10 MHz Outputs

If the 1PPS and/or the 10 MHz output(s) are not present, input power may not be applied. Or VersaSync is not synchronized to its input references and Signature Control is enabled.

Web UI Page	Current Status	Indication	Troubleshooting
HOME page	Reference Status Table	One or more input references indicate “Not Valid” (red)	All available Input References have been lost. The Reference Status table on this same page will show the current status of all inputs (Green is valid and red is not valid, or not present). If Signature Control is enabled in this state, the output may be disabled. 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 VersaSync. 3. Verify GNSS antenna installation (if applicable).
Navigate to INTERFACES/OUTPUTS/ PPS Output page	Select the PPS Output screen.	Signature Control will show "Output Always Enabled", "Output Enabled in Holdover", "Output Disabled in Holdover" or "Output Always Disabled".	1. With "Output Always Enabled" selected, the selected output will be present no matter the current synchronization state.2. Any other configured value will cause the applicable output to be halted if VersaSync is not fully synchronized with its input references.

Table 5-2: Troubleshooting 1PPS and/or 10 MHz outputs not being present

5.1.7 Troubleshooting – Network PCs Cannot Sync

In order for clients on the network to be able to sync to VersaSync, several requirements must be met:

1. The PC(s) must be routable to VersaSync. Make sure you can access VersaSync Web UI from a PC that is not syncing. If the PC cannot access the Web UI, a network issue likely exists. Verify the network configuration.

2. The network clients have to be configured to synchronize to VersaSync's address. For additional information on syncing Windows PC's, see https://safran-navigation-timing.com/document/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 VersaSync, the issue is likely not with VersaSync itself. The only VersaSync configurations that can prevent certain PCs from syncing to the time server are the NTP Access table and MD5 authentication. See "Configuring NTP Symmetric Keys" on page 136. A network or PC issue likely exists. A firewall may be blocking Port 123 (NTP traffic), for example.
4. NTP in VersaSync must be “in sync” and at a higher Stratum level than Stratum 15 (such as Stratum 1 or 2, for example). This requires VersaSync to be either synced to its input references or in Holdover mode. Verify the current NTP stratum level and the sync status.

5.1.8 Troubleshooting Software Update

When experiencing slow data transmission rates, or other network issues, it may be possible that a system software update will be aborted due to a web server timeout during the transfer.

In such an event, the **Upload New File** window will disappear, and the **Upgrade System Software** window will be displayed again instead.

- Should this happen repeatedly, you can transfer the update file using a file transfer protocol such as scp, sftp or ftp, if security is not a concern. The update can then be initiated from the Web UI or Command Line.
- Disk Status: In the event of an aborted update process, under **Tools** > **Upgrade/Backup** > **Disk Status**, check **Percent Used**: If the number is greater than 70%, free up disk space, before starting another attempt to update the System Software.

Rollback System Software

In the event of a malfunctioning of a newly uploaded System software, it is possible to rollback to the previously installed system software, a copy of which is maintained by default:

1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. In the **Actions** panel on the left, click *** Rollback System ***. Follow the instructions on the screen.

Caution: The Rollback option is designed for system recovery and some features and functionality may be lost after rolling back.

5.2 Command-Line Interface

A terminal emulation program is used to emulate a video terminal, so as to access VersaSync's CLI (Command-Line Interface) remotely via a serial cable. This may be required if no other means of remotely accessing VersaSync are available, for example if Ethernet ports are used otherwise or have been disabled (e.g., for security reasons).

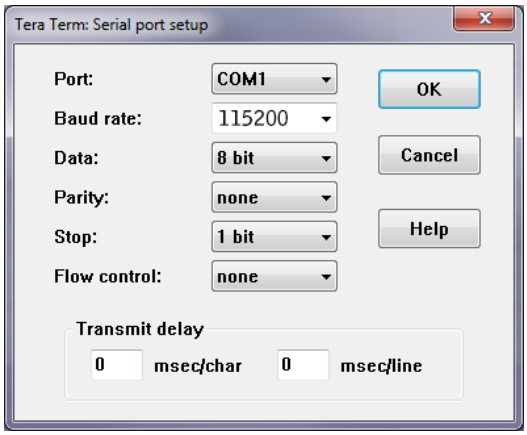
5.2.1 Setting up a Terminal Emulator

If no other means are available to access VersaSync, a terminal emulation program can be used to carry out certain configuration changes by accessing VersaSync's CLI (command- line interface) via a serial port connection. An application example for this scenario is to enable a network port so that the VersaSync Web UI can be used. While it is also possible to retrieve selected logs, a terminal emulator does not replace the VersaSync Web UI.

Orolia does not distribute or support its own terminal emulator, and newer Microsoft operating systems no longer include HyperTerminal. However, there are several third-party open-source programs available, such as **TeraTerm®** or **PuTTY®**. The example below illustrates the use of TeraTerm. The setup procedure is similar when using other terminal emulation programs.

Procedure:

1. Connect the personal computer to the USB interface.
2. Configure your terminal emulation program, using the following settings:
   - **Port**: COM1
   - **Bits per second**: 115200
   - **Data bits**: 8
   - **Parity**: None
   - **Stop bits**: 1
   - **Flow control**: None



3. Depending on which network protocol you are using (SSH, Telnet), you will need to enter authentication upon establishment of the connection either in a separate authentication window, or the Terminal window: The default user name is `spadmin`, and the password `admin123`.
4. Using the Terminal window, you can now submit commands.

5.2.2 CLI Commands

VersaSync features a suite of command-line interface (CLI) commands that can be used to configure parameters and retrieve status information or log files via a remote connection, using the `telnet` or `ssh` (if enabled) protocol.

This section includes a list of some of the supported commands.

Notes:

a. The command "`helpcli`" will provide a list of all available commands and their syntax (**Note**: Typing "`help`" will output bash shell help only and will not provide useful information).

b. You can scroll up or scroll down through the output by using the Page Up/Page down keys, or the arrow keys.

c. Type "`q`" (lower-case) to quit.

d. Pressing the up/down keys scrolls through previously typed commands.

e. Commands need to be typed in all lower-case letters.

f. Where `eth0` and `eth1` are the base network ports.

g. User accounts with "user" group permissions can perform "`get`" commands but cannot perform any "`set`" commands or change/reset passwords. Only user accounts with "admin" group permissions can perform "`set`" commands or change/reset password. Refer to "Adding/Deleting/Changing User Accounts" on page 261 for user account setup information. The Privileges column describes each command's required user level.

Command	Description	Privileges
agnss server	Display AGNSS status ie. enabled or disabled	
agnss server disable	Disable AGNSS server	
agnss server enable	Enable AGNSS server	
agnss server gen	Display almanac generation configuration. <daily <HH:MM>|interval> Use with arguments to set the almanac generation configuration to either daily with 24hr gen time each day or an interval in s between 10 and 86400	
agnss server station	Display AGNSS station <station> Use with arguments to set AGNSS station to a 4-letter station name.	
agnss server record	Display the time in days the records are kept. <days> Use with argument to set the time the records are kept between 2 and 400 days.	

Command	Description	Privileges
agnss server all	Display all AGNSS information; combines status, time age and list commands.	
agnss server status	<ephemeris|almanac> Display Ephemeris or Almanac data status.	
agnss server time	<ephemeris|almanac> Display time in seconds until next data set is ready.	
agnss server age	<ephemeris|almanac> Display data age in seconds.	
agnss server rnx	<GPS|GLO|GAL|BEI> Display list of constellations's satellites found in today's RINEX file.	
clean	Restores VersaSync configuration, logs, and stats to factory defaults and reboots	admin
cleanhalt	Restores VersaSync configuration to factory defaults and halts	admin
clearcfg	Restores configuration to factory defaults and reboots	admin
clearlogs	Clears all logs	admin
clearstats	Clears all statistical data (NTP, and oscillator/disciplining)	admin
dateget	Displays current date (for example, 15 APR 2015)	admin or user
dateset	Used to set the current date	admin
defcert	Used to create a new Safran self-signed SSL certificate for HTTPS in case of expiration of the original certificate	admin
dhcp4get	Displays whether DHCP is enabled	admin or user
dhcp4set	Used to enable or disable DHCP	admin
dhcp6get	Displays whether DHCPv6 is enabled	admin or user
dhcp6set	Used to enable or disable DHCPv6	admin
dns4cfg	Display the configured IPv4 primary and secondary DNS addresses	admin or user
dns4get	Displays the configured DNS servers	admin or user
dns4set	Used to configure the DNS servers	admin

Command	Description	Privileges
dnssecget	Displays current DNSSEC configuration status	admin
dnssecset	Mananges DNSSEC validation settings	admin
dnssecremovekey	Removes a custom root key	admin
dnsseclistkeys	Lists all available custom root keys in the system	admin
doyget	Used to obtain the current Day of Year	admin or user
doyset	Used to set the current Day of Year	admin
drill	DNS(SEC) debug tool that displays information about the DNS.	admin or user
getopenssl	Returns the current FIPS compliance mode	admin
gettemp	Displays the temperature of the oscillator, board, or CPU	admin or user
gpsdop	Displays GNSS receiver positional accuracy estimates	admin or user
gpsdserviceportget	Displays the GPSD service port	admin or user
gpsdserviceportset	Sets the GPSD service port	admin
gpsinfo	Applicable to SAASM-equipped VersaSync units only	admin or user
gpsloc	Displays GNSS latitude, longitude and antenna height	admin or user
gpsmdl	Displays the GNSS Manufacturer and Model	admin or user
gpsreset	Resets the GNSS Position stored in the unit.	admin
gpssat	Displays GNSS satellites tracked and maximum signal strength being received	admin or user
gw4cfg	Display the configured IPv4 gateway	admin or user
gw4get	Displays the default IPv4 gateway	admin or user
gw4set	Used to configure the IPv4 gateway addresses	admin
gw6cfg	Display the configured IPv6 gateway.	admin or user

Command	Description	Privileges
gw6get	Displays the default IPv6 gateway address	admin or user
gw6set	Used to configure the IPv6 gateway address	admin
halt	Used to Halt the system for shutdown	admin
helpcli	Provides list of available commands and syntax	admin or user
hostget	Displays the system hostname.	admin or user
hostset	<hostname> Sets the system Hostname. Note that changing the system hostname may require NTP Autokey keys/certificates to be regenerated.	admin
hotstart	Initiate a hot start operation on the SAASM GPS receiver	admin
ip4cfg	Display the IPv4 static configuration.	admin or user
ip4get	Displays IPv4 Ethernet port settings information (IP address net mask and gateway)	admin or user
ip4set	Used to set IPv4 Ethernet port settings information (IP address net mask and gateway)	admin
ip6add	Used to add IPv6 Ethernet port settings information (IP address net mask and gateway)	admin
ip6cfg	Display the IPv6 static configuration	admin or user
ip6del	Used to delete IPv6 IP address	admin
ip6get	Used to obtain the IPv6 IP address	admin or user
iptables-install	Must be used in conjunction with "sudo". Make the IPV4 packet filter rules persistent.	
iptables-recover	Must be used in conjunction with "sudo". Restore the default IPV4 packet filter rules.	
ip6tables	Must be used in conjunction with "sudo". Set up, maintain, and inspect the tables of IPV6 packet filter rules in the Linux kernel.	

Command	Description	Privileges
ip6tables-install	Must be used in conjunction with "sudo". Make the IPV6 packet filter rules persistent.	
ip6tables-recover	Must be used in conjunction with "sudo". Restore the default IPV6 packet filter rules.	
licenses	Displays configured licenses installed (if any)	admin or user
list	Outputs a list of commands	admin or user
loadconf	Restore a saved configuration and reboot	admin
localget	Used to obtain the local clock applied to the front panel	admin or user
locallist	Used to display local clocks	admin or user
localset	<clock name> Set the name of the local clock that is applied to the front panel.	admin
manifest	See a list of all files	admin or user
model	Displays the Serial Number of the unit	admin or user
net	Displays network status	admin or user
netnum	Displays the number of general-purpose network interfaces	admin or user
net4	Displays IPv4 network status	admin or user
net6	Displays IPv6 network status	admin or user
options	Displays configured options installed (if any)	admin or user
oscget	Displays the installed system oscillator	admin or user
portget	Display whether network port is enabled (for example, "portget ETH2")	admin or user

Command	Description	Privileges
portset	Enable or disable a network port: "portset x on" where "x" is the port number (for example, "ETH2") "portset X off"	admin
portstate	Display the current state for a network port	admin or user
ppsctrl	Enable/disable individual 1PPS output signals	admin
priorset	Sets the priority of an entry in the reference priority table	admin
ptpcfgload	Copies specified file to PTP config location.	admin
ptpifaceset	Enable or disable PTP on a specified interface.	admin
ptpifacesetcfg	Set the configuration of a specified interface from a file.	admin
rbxostatus check	For mRO-50 rubidium oscillators, returns INVALID if standby power has been lost and the oscillator state has been compromised.	admin
rbxostatus reset	For mRO-50 rubidium oscillators, resets INVALID flag to VALID.	admin
reboot	Used to warm-boot the unit without having to dis-connect or reconnect power	admin
reftable	Displays reference priority table	admin or user
renew4	Used with DHCP to renew the assigned IPv4 address	admin
renew6	Used with DHCPv6 to renew the assigned IPv6 address	admin
resetpw	Resets the administrator account (spadmin) password back to the default value "admin123"	admin
restrict	Reapplies all configured access control restrictions to VersaSync	admin
rollback	Rollback the system software to the backup.	
routes4	Displays the current IPv4 routing table(s)	admin or user
routes6	Displays the current IPv6 routing table(s)	admin or user
rt4add	Adds an IPv4 static route	admin

Command	Description	Privileges
rt4del	Deletes an IPv4 static route	admin
rt4get	Displays the configured IPv4 static routes	admin or user
rt6add	Adds an IPv6 static route	admin
rt6del	Deletes an IPv6 static route	admin
rt6get	Displays the configured IPv6 static routes	admin or user
saveconf	Generate archive of current configuration	admin
savelog	Generate archive of all log files	admin or user
scaleget	Displays configured system timescale	admin or user
scaleset	Used to configure the system timescale	admin
sendnmeaudp	Used to configure, enable and disable the NMEA over UDP feature (see "System Time Message" on page 110 for more information)	admin
sendtrap	Triggers one type of a possible set of alarms.	admin
sendtrap all	Sends one instance of all alarms	
services	Displays the state of services (enabled/disabled)	admin or user
servget	Displays the state of individual services	admin or user
servset	Enable or disable specific services	admin
setopenssl	<standard | enhanced | legacy> Sets the FIPS compliance mode	admin
speedget	<iface> Display the speed, the duplex, and the negotiation mode of the specified network interface.	admin or user
speedset	<iface> <speed> <duplex> <autoneg> Set the speed, the duplex, and the negotiation mode of the specified network interface.	admin
stateset	Enable or disable an entry in the reference priority table. index = 0...15. state = 0 (disable), 1 (enable)	admin

Command	Description	Privileges
status	Displays information about the oscillator disciplining	admin or user
swupgrade	Performs system upgrade using the update bundle provided	
syncstate	Display timing system synchronization state	admin or user
tfomget	Displays current estimated system time error (TFOM – Time Figure of Merit)	admin or user
timeget	Displays current system time (time is displayed in the configured timescale – See `scaleget` command to retrieve the configured timescale)	admin or user
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	admin
unrestrict	Used for clearing access control restrictions to VersaSync	admin
version	Displays the installed main VersaSync and timing system software versions	admin or user
vlanadd	Add a VLAN connection	admin
vlandel	Delete a VLAN connection	admin
yearget	Displays the current year	admin or user
yearset	Used to set the current year	admin
zeroize	Applicable to SAASM-equipped VersaSync units only	admin

5.3 Time Code Data Formats

This section describes the different time code data format selections available for use with VersaSync option cards that accept ASCII data streams as inputs or outputs via their RS-485 and RS-232 interfaces.

Supported are formats like NMEA, BBC, Spectracom, GSSIP, and Endrun.

5.3.1 NMEA GGA Message

The GGA Format provides essential fix data which includes 3D location and accuracy data.

Example message:

$GPGGA,123519.00,4807.038,N,01131.000,E,1,08,0.9,545.4,M,-164.0,M,,,,*47

Note: Not all fields below are available on all products in all applications.

NOTE: The GGA format does not support precision timing and 1PPS functionality; the Web UI may permit the selection of **Message** or **PPS Pin** as **PPS Source**, but the NMEA GGA Message will not use either. If this data is required for your application, use the ZDA Message format instead (see "NMEA ZDA Message" on page 351).

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 (geoid)
-164.0,M	Height of geoid (mean sea level) above WGS84 ellipsoid

(empty field)	(Field not provided in this setup)
*47	Checksum data, always begins with *

Note: Enabling more NMEA messages increases the minimum baud rate required. A minimum rate of 9600 baud is suggested when enabling more messages.

5.3.2 NMEA GLL Message

The Format GLL Data message provides position fix, time of position fix, and status information.

Example message:

$GPGLL,3953.88008971,N,10506.75318910,W,034138.00,A,D*7A

Where:

$GPGLL	Message ID
3953.88008971	Latitude in dd mm,mmmm format (0-7 decimal places)
N	Direction of latitude N: North S: South
10506.75318910	Longitude in ddd mm,mmmm format (0-7 decimal places)
W	Direction of longitude E: East W: West
034138.00	UTC of position in hhmmss.ss format
A	Status indicator: A: Data valid V: Data not valid This value is set to V (Data not valid) for all Mode Indicator values except A (Autonomous) and D (Differential)

D	Mode indicator: A: Autonomous mode D: Differential mode E: Estimated (dead reckoning) mode M: Manual Input mode S: Simulator mode N: Data not valid
*7A	The checksum data, always begins with *

Note: Enabling more NMEA messages increases the minimum baud rate required. A minimum rate of 9600 baud is suggested when enabling more messages.

5.3.3 NMEA GSA Message

The Format GSA Data message provides GNSS DOP and Active Satellites information.

Example message:

$GNGSA,A,3,21,5,29,25,12,10,26,2,,,,,1.2,0.7,1.0*27

Where:

GSA	Message ID
A	Mode 1: M = Manual A = Automatic
3	Mode 2: Fix type: 1 = not available 2 = 2D 3 = 3D
21	PRN number: 01 to 32 for GPS 33 to 64 for SBAS 64+ for GLONASS

5	PRN number
29	PRN number
25	PRN number
12	PRN number
10	PRN number
26	PRN number
2	PRN number
(empty field)	(Field not provided in this setup)
(empty field)	(Field not provided in this setup)
(empty field)	(Field not provided in this setup)
(empty field)	(Field not provided in this setup)
1.2	PDOP: 0.5 to 99.9
0.7	HDOP: 0.5 to 99.9
1.0	VDOP: 0.5 to 99.9
*27	The checksum data, always begins with *

Note: Enabling more NMEA messages increases the minimum baud rate required. A minimum rate of 9600 baud is suggested when enabling more messages.

5.3.4 NMEA GSV Message

The Format GSV Data message identifies the number of SV's in view, the PRN numbers, elevations, azimuths, and SNR values.

Example message:

$GPGSV,5,1,19,4,17,69,46,5,18,303,44,6,36,200,50,7,63,135,48*4B
$GPGSV,5,2,19,9,54,66,48,11,52,257,48,13,6,248,43,16,12,44,40*74
$GPGSV,5,3,19,20,46,301,50,29,8,322,44,30,41,183,50,70,55,58,0*43
$GPGSV,5,4,19,71,56,308,48,72,13,280,39,73,22,146,43,79,18,26,43*41
$GPGSV,5,5,19,80,42,83,49,85,11,206,44,86,40,255,49*75

Note: A GSV message is split across several and all GSV messages are outputted each reporting cycle (every second). The table below examines the first line from the above example message.

Where:

Field	Example	Meaning
0	GSV	Message ID
1	5	Total number of messages of this type in this cycle
2	1	Message Number
3	19	Total number of SVs visible
4	4	SV PRN number
5	17	Elevation, in degrees, 90° maximum
6	69	Azimuth, degrees from True North, 000° through 359°
7	46	SNR, 00 through 99 dB (null when not tracking)
8	5	(Information about second SV, same format as field 4)
9	18	(Information about second SV, same format as field 5)
10	303	(Information about second SV, same format as field 6)
11	44	(Information about second SV, same format as field 7)
12	6	(Information about third SV, same format as field 4)
13	36	(Information about third SV, same format as field 5)
14	200	(Information about third SV, same format as field 6)
15	50	(Information about third SV, same format as field 7)
16	7	(Information about fourth SV, same format as field 4)
17	63	(Information about fourth SV, same format as field 5)
18	135	(Information about fourth SV, same format as field 6)
19	48	(Information about fourth SV, same format as field 7)
20	*4B	The checksum data, always begins with *

Note:
$GPGSV indicates GPS and SBAS satellites. If the PRN is greater than 32, this indicates an SBAS PRN, 87 should be added to the GSV PRN number to determine the SBAS PRN number.
$GLGSV indicates GLONASS satellites. 64 should be subtracted from the GSV PRN number to determine the GLONASS PRN number.
$GBGSV indicates BeiDou satellites. 100 should be subtracted from the GSV PRN number to determine the BeiDou PRN number.
$GAGSV indicates Galileo satellites.
$GQGSV indicates QZSS satellites.

Note: Enabling more NMEA messages increases the minimum baud rate required. A minimum rate of 9600 baud is suggested when enabling more messages.

5.3.5 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,,9.02,230394,,,A*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
(empty field)	(Field not provided in this setup)

9.02	Speed over the ground in knots
230394	Date - 23rd of March 1994
(empty field)	(Field not provided in this setup)
(empty field)	(Field not provided in this setup)
A	Mode Indicator: A=Autonomous, D=Differential, E=Estimated, F=Float RTK, M=Manual input, N=No fix, P=Precise, R=Real time kinematic, S=Simulator
*6A	Checksum data, always begins with *

Note: Enabling more NMEA messages increases the minimum baud rate required. A minimum rate of 9600 baud is suggested when enabling more messages.

5.3.6 NMEA VTG Message

The Format ZDA Data message provides track made good and speed over ground information.

Example message:

$GPVTG,140.88,T,,M,8.04,N,14.89,K,D*05

Where:

VTG	Message ID
140.88	Track made good (degrees true)
T	T: track made good is relative to true north
(empty field)	(Field not provided in this setup)
M	M: track made good is relative to magnetic north
8.04	Speed, in knots
N	N: speed is measured in knots
14.89	Speed over ground in kilometers/hour (kph)
K	K: speed over ground is measured in kph

D	Mode indicator: A: Autonomous mode D: Differential mode E: Estimated (dead reckoning) mode M: Manual Input mode S: Simulator mode N: Data not valid
*05	The checksum data, always begins with *

Note: Enabling more NMEA messages increases the minimum baud rate required. A minimum rate of 9600 baud is suggested when enabling more messages.

5.3.7 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

Note: Enabling more NMEA messages increases the minimum baud rate required. A minimum rate of 9600 baud is suggested when enabling more messages.

5.3.8 ASCII Output Settings

These settings may only be used if your hardware contains the legacy IMU VectorNav 300, and your Multi I/O connector pinout is set to INS Out.

5.3.8.1 VNYPR

Output Type: Yaw, Pitch, Roll

Register ID: 8

Async Header: YPR

Access: Read Only

Comment: Attitude solution as yaw, pitch, and roll in degrees. The yaw, pitch, and roll is given as a 3,2,1 Euler angle rotation sequence describing the orientation of the sensor with respect to the inertial North East Down (NED) frame.

Size (Bytes): 12

Example Response: $VNRRG, 8, +006.271,+000.031, -002.000*66

Table 5-3: VNYPR Settings

Offset	Name	Format	Unit	Description
0	Yaw	float	deg	Yaw angle.
4	Pitch	float	deg	Pitch angle.
8	Roll	float	deg	Roll angle.

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System subsystem. Once configured the data in this register will be sent out with the $VNYPR header.

5.3.8.2 VNQTN

Output Type: Attitude Quarternion

Register ID: 9

Async Header: QTN

Access: Read Only

Comment: Attitude solution as a quaternion.

Size (Bytes): 16

Example Response: $VNRRG, 9, - 0.017386, - 0.000303, +0.055490, +0.998308*4F

Table 5-4: VNQTN Settings

Offset	Name	Format	Unit	Description
0	Quat[0]	float	-	Calculated attitude as quaternion.
4	Quat[1]	float	-	Calculated attitude as quaternion.
8	Quat[2]	float	-	Calculated attitude as quaternion.
12	Quat[3]	float	-	Calculated attitude as quaternion. Scalar component.

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System sub-system. Once configured the data in this register will be sent out with the $VNQTN header.

5.3.8.3 VNQMR

Output Type: Quaternion, Magnetic, Acceleration and Angular Rates

Register ID: 15

Async Header: QMR

Access: Read Only

Comment: Attitude solution, magnetic, acceleration, and compensated angular rates.

Size (Bytes): 52

Example Response: $VNRRG, 15, -0.017057, -0.000767, +0.056534, +0.998255, +1.0670, -0.2568, +3.0696, -00.019, +00.320, -09.802, -0.002801, -0.001186, -0.001582*65

Table 5-5: VNQMR

Offset	Name	Format	Unit	Description
0	Quat[0]	float	–	Calculated attitude as quaternion.
4	Quat[1]	float	–	Calculated attitude as quaternion.
8	Quat[2]	float	–	Calculated attitude as quaternion.
12	Quat[3]	float	–	Calculated attitude as quaternion. Scalar component.
16	MagX	float	Gauss	Compensated magnetometer measurement in x-axis.
20	MagY	float	Gauss	Compensated magnetometer measurement in y-axis.
24	MagZ	float	Gauss	Compensated magnetometer measurement in z-axis.
28	AccelX	float	m/s^2	Compensated accelerometer measurement in x-axis.
32	AccelY	float	m/s^2	Compensated accelerometer measurement in y-axis.
36	AccelZ	float	m/s^2	Compensated accelerometer measurement in z-axis.
40	GyroX	float	rad/s	Compensated angular rate in x-axis.
44	GyroY	float	rad/s	Compensated angular rate in y-axis.
48	GyroZ	float	rad/s	Compensated angular rate in z-axis.

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System subsystem. Once configured the data in this register will be sent out with the $VNQMR header.

5.3.8.4 VNMAG

Output Type: Magnetic Measurements

Register ID: 17

Async Header: MAG

Access: Read Only

Comment: Magnetometer measurements.

Size (Bytes): 12

Example Response: $VNRRG,17, +1.0647, -0.2498, +3.0628*66

Table 5-6: VNMAG Settings

Offset	Name	Format	Unit	Description
0	MagX	float	Gauss	Compensated magnetometer measurement in x-axis.
4	MagY	float	Gauss	Compensated magnetometer measurement in y-axis.
8	MagZ	float	Gauss	Compensated magnetometer measurement in z-axis.

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System sub-system. Once configured the data in this register will be sent out with the $VNMAG header.

5.3.8.5 VNACC

Output Type: Acceleration Measurements

Register ID: 18

Async Header: ACC

Access: Read Only

Comment: Acceleration measurements.

Size (Bytes): 12

Example Response: $VNRRG,18, +00.013, +00.354, -09.801*65

Table 5-7: VNACC Settings

Offset	Name	Format	Unit	Description
0	AccelX	float	m/s^2	Compensated accelerometer measurement in x-axis.
4	AccelY	float	m/s^2	Compensated accelerometer measurement in y-axis.
8	AccelZ	float	m/s^2	Compensated accelerometer measurement in z-axis.

> **Note:** You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System sub-system. Once configured the data in this register will be sent out with the $VNACC header.

5.3.8.6 VNGYR

Output Type: Angular Rate Measurements

Register ID: 19

Async Header: GYR

Access: Read Only

Comment: Compensated angular rates.

Size (Bytes): 12

Example Response: $VNRRG, 19, +0.002112, -0.000362, -0.000876*6C

Table 5-8: VNGYR Settings

Offset	Name	Format	Unit	Description
0	GyroX	float	rad/s	Compensated angular rate in x-axis.
4	GyroY	float	rad/s	Compensated angular rate in y-axis.
8	GyroZ	float	rad/s	Compensated angular rate in z-axis.

> **Note:** You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System sub-system. Once configured the data in this register will be sent out with the $VNGYR header.

5.3.8.7 VNMAR

Output Type: Magnetic, Acceleration and Angular Rates

Register ID: 20

Async Header: MAR

Access: Read Only

Comment: Magnetic, acceleration, and compensated angular rates.

Size (Bytes): 36

Example Response: $VNRRG,20, +1.0684, -0.2578, +3.0649, -00.005, +00.341, -09.780, -0.000963, +0.000840, -0.000466*64

Table 5-9: VNMAR Settings

Offset	Name	Format	Unit	Description
0	MagX	float	Gauss	Compensated magnetometer measurement in x-axis.
4	MagY	float	Gauss	Compensated magnetometer measurement in y-axis.
8	MagZ	float	Gauss	Compensated magnetometer measurement in z-axis.
12	AccelX	float	m/s^2	Compensated accelerometer measurement in x-axis.
16	AccelY	float	m/s^2	Compensated accelerometer measurement in y-axis.
20	AccelZ	float	m/s^2	Compensated accelerometer measurement in z-axis.
24	GyroX	float	rad/s	Compensated angular rate in x-axis.
28	GyroY	float	rad/s	Compensated angular rate in y-axis.
32	GyroZ	float	rad/s	Compensated angular rate in z-axis.

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System sub-system. Once configured the data in this register will be sent out with the $VNMAR header.

5.3.8.8 VNYMR

Output Type: Yaw, Pitch, Roll, Magnetic, Acceleration, and Angular Rates

Register ID: 27

Async Header: YMR

Access: Read Only

Comment: Attitude solution, magnetic, acceleration, and compensated angular rates.

Size (Bytes): 48

Example Response: $VNRRG,27, +006.380, +000.023, - 001.953, +1.0640, -0.2531, +3.0614, +00.005, +00.344, -09.758, -0.001222, -0.000450, -0.001218*4F

Table 5-10: VNYMR Settings

Offset	Name	Format	Unit	Description
0	Yaw	float	deg	Calculated attitude heading angle in degrees.
4	Pitch	float	deg	Calculated attitude pitch angle in degrees.
8	Roll	float	deg	Calculated attitude roll angle in degrees.
12	MagX	float	Gauss	Compensated magnetometer measurement in x-axis.
16	MagY	float	Gauss	Compensated magnetometer measurement in y-axis.
20	MagZ	float	Gauss	Compensated magnetometer measurement in z-axis.
24	AccelX	float	m/s^2	Compensated accelerometer measurement in x-axis.
28	AccelY	float	m/s^2	Compensated accelerometer measurement in y-axis.
32	AccelZ	float	m/s^2	Compensated accelerometer measurement in z-axis.
36	GyroX	float	rad/s	Compensated angular rate in x-axis.
40	GyroY	float	rad/s	Compensated angular rate in y-axis.
44	GyroZ	float	rad/s	Compensated angular rate in z-axis.

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System sub-system. Once configured the data in this register will be sent out with the $VNYMR header.

5.3.8.9 VNYBA

Output Type: Yaw, Pitch, Roll, Body True Acceleration, and Angular Rates

Async Header: YBA

Table 5-11: VNYBA Settings

Offset	Name	Format	Unit	Description
0	Yaw	float	deg	Yaw angle.
4	Pitch	float	deg	Pitch angle.
8	Roll	float	deg	Roll angle.
12	AccelX	float	m/s^2	True acceleration. (X-axis)
16	AccelY	float	m/s^2	True acceleration. (Y-axis)
20	AccelZ	float	m/s^2	True acceleration. (Z-axis)
24	AngularRateX	float	rad/s	Angular rate. (X-axis)
28	AngularRateY	float	rad/s	Angular rate. (Y-axis)
32	AngularRateZ	float	rad/s	Angular rate. (Z-axis)

5.3.8.10 VNYIA

Output Type: Yaw, Pitch, Roll, Inertial True Acceleration, and Angular Rates

Async Header: YIA

Table 5-12: VNYIA Settings

Offset	Name	Format	Unit	Description
0	Yaw	float	deg	Yaw angle.
4	Pitch	float	deg	Pitch angle.
8	Roll	float	deg	Roll angle.
12	AccelX	float	m/s^2	Inertial true acceleration. (X-axis)
16	AccelY	float	m/s^2	Inertial true acceleration. (Y-axis)
20	AccelZ	float	m/s^2	Inertial true acceleration. (Z-axis)
24	AngularRateX	float	rad/s	Angular rate. (X-axis)

Offset	Name	Format	Unit	Description
28	AngularRateY	float	rad/s	Angular rate. (Y-axis)
32	AngularRateZ	float	rad/s	Angular rate. (Z-axis)

5.3.8.11 VNIMU

Output Type: IMU Measurements

Register ID: 54

Async Header: IMU

Access: Read Only

Comment: Provides the calibrated IMU measurements including barometric pressure.

Size (Bytes): 44

Example Read Response: $VNRRG,54, -02.0841, +00.6045, +02.8911, +00.381, -00.154, -09.657, -00.005683, +00.000262, +00.001475, +21.6, +00099.761*5B

Table 5-13: VNIMU Settings

Offset	Name	Format	Unit	Description
0	MagX	float	Gauss	Uncompensated Magnetic X-axis.
4	MagY	float	Gauss	Uncompensated Magnetic Y-axis.
8	MagZ	float	Gauss	Uncompensated Magnetic Z-axis.
12	AccelX	float	m/s^2	Uncompensated Acceleration X-axis.
16	AccelY	float	m/s^2	Uncompensated Acceleration Y-axis.
20	AccelZ	float	m/s^2	Uncompensated Acceleration Z-axis.
24	GyroX	float	rad/s	Uncompensated Angular rate X-axis.
28	GyroY	float	rad/s	Uncompensated Angular rate Y-axis.
32	GyroZ	float	rad/s	Uncompensated Angular rate Z-axis.
36	Temp	float	C	IMU Temperature.
40	Pressure	float	kPa	Barometric pressure.

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System sub-system. Once configured the data in this register will be sent out with the $VNIMU header.

5.3.8.12 VNGPS

Output Type: GPS Solution - LLA

Register ID: 58

Async Header: GPS

Access: Read Only

Size (Bytes): 72

Example Read Response: $VNRRG, 58, 333733.000159, 1694,3,05, +32.95622080, -096.71415970, +00169.457, -000.850, -000.580, -002.860, +005.573, +003.644, +009.760, +003.320, 2.00E-08*0E

Table 5-14: VNGPS Settings

Offset	Name	Format	Unit	Description
0	Time	double	sec	GPS time of week in seconds.
8	Week	unit16	week	GPS week.
10	GpsFix	uint8	–	GPS fix type. See table below.
11	NumSats	uint8	–	Number of GPS satellites used in solution.
12	–	–	–	--- 4 PADDING BYTES ---
16	Latitude	double	deg	Latitude in degrees.
24	Longitude	double	deg	Longitude in degrees.
32	Altitude	double	m	Altitude above ellipsoid. (WGS84)
40	NedVelX	float	m/s	Velocity measurement in north direction.
44	NedVelY	float	m/s	Velocity measurement in east direction.
48	NedVelZ	float	m/s	Velocity measurement in down direction.
52	NorthAcc	float	m	North position accuracy estimate. (North)

Offset	Name	Format	Unit	Description
56	EastAcc	float	m	East position accuracy estimate. (East)
60	VertAcc	float	m	Vertical position accuracy estimate. (Down)
64	SpeedAcc	float	m/s	Speed accuracy estimate.
68	TimeAcc	float	sec	Time accuracy estimate.

Table 5-15: GPS Fix

Value	Description
0	No fix
1	Time only
2	2D
3	3D

This register provides the GPS PVT (position, velocity, & time) solution from GPS receiver A. This is the GPS receiver that is used by the INS (Inertial Navigation System) Kalman filter for position and velocity inputs.

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System subsystem. Once configured the data in this register will be sent out with the $VNGPS header.

5.3.8.13 VNGPE

Output Type: GPS Solution - ECEF

Register ID: 59

Async Header: GPE

Access: Read Only

Comment: Available at 5Hz only.

Size (Bytes): 72

Example Read Response: $VNRRG, 59, 333752.800322, 1694, 3, 06, -0626351.600, -5320522.490, +3449975.910, - 000.810, -002.970, +000.850, +010.170, +010.170, +010.170, +002.740, 1.80E-08*35

Table 5-16: VNGPE Settings

Offset	Name	Format	Unit	Description
0	Tow	double	sec	GPS time of week.
8	Week	unit16	week	Current GPS week.
10	GpsFix	uint8	–	GPS fix type. See table below.
11	NumSats	uint8	–	Number of GPS satellites used in solution.
12	–	–	–	--- 4 PADDING BYTES ---
16	PositionX	double	m	ECEF X coordinate.
24	PositionY	double	m	ECEF Y coordinate.
32	PositionZ	double	m	ECEF Z coordinate.
40	VelocityX	float	m/s	ECEF X velocity.
44	VelocityY	float	m/s	ECEF Y velocity.
48	VelocityZ	float	m/s	ECEF Z velocity.
52	PosAccX	float	m	ECEF X position accuracy estimate.
56	PosAccY	float	m	ECEF Y position accuracy estimate.
60	PosAccZ	float	m	ECEF Z position accuracy estimate.
64	SpeedAcc	float	m/s	Speed accuracy estimate.
68	TimeAcc	float	sec	Time accuracy estimate.

Table 5-17: GPS Fix

Value	Description
0	No fix
1	Time only
2	2D
3	3D

This register provides the GPS PVT (position, velocity, & time) solution from GPS receiver A. This is the GPS receiver that is used by the INS (Inertial Navigation System) Kalman filter for position and velocity inputs.

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System subsystem. Once configured the data in this register will be sent out with the $VNGPE header.

5.3.8.14 VNINS

Output Type: INS Solution – LLA

Register ID: 63

Async Header: INS

Access: Read Only

Size (Bytes): 72

Example Read Response:$VNRRG, 63, 333811.902862, 1694, 0004, +009.500, -004.754, -000.225, +32.95602815, -096.71424297, +00171.195, -000.840, -000.396, -000.109, 07.8, 01.6, 0.23*5F

Table 5-18: VNINS Settings

Offset	Name	Format	Unit	Description
0	Time	double	sec	GPS time of week in seconds
8	Week	uint16	week	GPS week.
10	Status	uint16	–	Status flags for INS filter. Hexadecimal format. See table below.
12	Yaw	float	deg	Yaw angle relative to true north.
16	Pitch	float	deg	Pitch angle relative to horizon.
20	Roll	float	deg	Roll angle relative to horizon.
24	Latitude	double	deg	INS solution position in geodetic latitude.
32	Longitude	double	deg	INS solution position in geodetic longitude.
40	Altitude	double	m	Height above ellipsoid. (WGS84)

Offset	Name	Format	Unit	Description
48	NedVelX	float	m/s	INS solution velocity in NED frame. (North)
52	NedVelY	float	m/s	INS solution velocity in NED frame. (East)
56	NedVelZ	float	m/s	INS solution velocity in NED frame. (Down)
60	AttUncertainty	float	deg	Uncertainty in attitude estimate.
64	PosUncertainty	float	m	Uncertainty in position estimate.
68	VelUncertainty	float	m/s	Uncertainty in velocity estimate.

Table 5-19: INS Status

Name	Bit	Format	Description
Mode	0	2 bits	Indicates the current mode of the INS filter. 0 = Not tracking. GPS Compass is initializing. Output heading is based on magnetometer measurements. 1 = Aligning. INS Filter is dynamically aligning. For a stationary startup: GPS Compass has initialized and INS Filter is aligning from the magnetic heading to the GPS Compass heading. For a dynamic startup: INS Filter has initialized and is dynamically aligning to True North heading. In operation, if the INS Filter drops from INS Mode 2 back down to 1, the attitude undertainty has increased above 2 degrees. 2 = Tracking. The INS Filter is tracking and operating within specification. 3 = Loss of GPS. A GPS outage has lasted more than 45 seconds. The INS Filter will no longer update the position and velocity outputs, but the attitude remains valid.
GpsFix	2	1 bits	Indicates whether the GPS has a proper fix.
Error	3	4 bits	Sensor measurement error code. See table below. 0 = No errors detected.
Reserved	7	1 bit	Reserved for internal use. May toggle state during runtime and should be ignored.
GpsHeadingIns	8	1 bit	In stationary operation, if set the INS Filter has fully aligned to the GPS Compass solution. In dynamic operation, the GPS Compass solution is currently aiding the INS Filter heading solution.
GpsCompass	9	1 bit	Indicates if the GPS compass is operational and reporting a heading solution.
Reserved	10	8 bits	Reserved for internal use. These bits will toggle state and should be ignored.

Table 5-20: Error Bitfield

Name	Bit Offset	Format	Description
Reserved	0	1 bit	Reserved for future use and not currently used.
IMU Error	1	1 bit	High if IMU communication error is detected.
Mag/Pres Error	2	1 bit	High if Magnetometer or Pressure sensor error is detected.
GPS Error	3	1 bit	High if GPS communication error is detected.

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System subsystem. Once configured the data in this register will be sent out with the $VNINS header.

5.3.8.15 VNINE

Output Type: INS Solution – ECEF

Register ID: 64

Async Header: INE

Access: Read Only

Size (Bytes): 72

Example Read Response: $VNRRG, 64, 333837.222917, 1694,0004, +009.315, -004.767, -000.193, -0626356.433, -5320530.947, +3449961.679, -000.224, -000.476, -000.564, 07.7, 01.5, 0.22*65

Table 5-21: VNINE Settings

Offset	Name	Format	Unit	Description
0	Time	double	sec	GPS time of week in seconds
8	Week	uint16	week	GPS week.
10	Status	uint16	–	Status flags for INS filter. Hexadecimal format. See table below.
12	Yaw	float	deg	Yaw angle relative to true north.

Offset	Name	Format	Unit	Description
16	Pitch	float	deg	Pitch angle relative to horizon.
20	Roll	float	deg	Roll angle relative to horizon.
24	PositionX	double	m	INS solution position in ECEF. (X-axis)
32	PositionY	double	m	INS solution position in ECEF. (Y-axis)
40	PositionZ	double	m	INS solution position in ECEF. (Z-axis)
48	VelocityX	float	m/s	INS solution velocity in ECEF frame. (X-axis)
52	VelocityY	float	m/s	INS solution velocity in ECEF frame. (Y-axis)
56	VelocityZ	float	m/s	INS solution velocity in ECEF frame. (Z-axis)
60	AttUncertainty	float	deg	Expected uncertainty in estimated attitude.
64	PosUncertainty	float	m	Expected uncertainty in estimated position.
68	VelUncertainty	float	m/s	Expected uncertainty in estimated velocity.

Table 5-22: INS Status

Name	Bit	Format	Description
Mode	0	2 bits	Indicates the current mode of the INS filter. 0 = Not tracking. GPS Compass is initializing. Output heading is based on magnetometer measurements. 1 = Aligning. INS Filter is dynamically aligning. For a stationary startup: GPS Compass has initialized and INS Filter is aligning from the magnetic heading to the GPS Compass heading. For a dynamic startup: INS Filter has initialized and is dynamically aligning to True North heading. In operation, if the INS Filter drops from INS Mode 2 back down to 1, the attitude uncertainty has increased above 2 degrees. 2 = Tracking. The INS Filter is tracking and operating within specification. 3 = Loss of GPS. A GPS outage has lasted more than 45 seconds. The INS Filter will no longer update the position and velocity outputs, but the attitude remains valid.
GpsFix	2	1 bits	Indicates whether the GPS has a proper fix.
Error	3	4 bits	Sensor measurement error code. See table below. 0 = No errors detected.
Reserved	7	1 bit	Reserved for internal use. May toggle state during runtime and should be ignored.

Name	Bit	Format	Description
GpsHeadingIns	8	1 bit	In stationary operation, if set the INS Filter has fully aligned to the GPS Compass solution. In dynamic operation, the GPS Compass solution is currently aiding the INS Filter heading solution.
GpsCompass	9	1 bit	Indicates if the GPS compass is operational and reporting a heading solution.
Reserved	10	8 bits	Reserved for internal use. These bits will toggle state and should be ignored.

Table 5-23: Error Bitfield

Name	Bit Offset	Format	Description
Reserved	0	1 bit	Reserved for future use and not currently used.
IMU Error	1	1 bit	High if IMU communication error is detected.
Mag/Pres Error	2	1 bit	High if Magnetometer or Pressure sensor error is detected.
GPS Error	3	1 bit	High if GPS communication error is detected.

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System subsystem. Once configured the data in this register will be sent out with the $VNINE header.

5.3.8.16 VNISL

Output Type: INS State - LLA

Register ID: 72

Async Header: ISL

Access: Read Only

Size (Bytes): 72

Example Read Response: $VNRRG, 72, +170.420, +001.398, +001.806, +00.000295, - 00.000911, - 00.000905, +32.95680804, - 096.71414860, +00179.592, +000.181, -000.073, -000.050, +00.209, -00.322, -10.040*52

Table 5-24: VNISL Settings

Offset	Name	Format	Unit	Description
0	Yaw	float	deg	Yaw angle relative to true north.
4	Pitch	float	deg	Pitch angle relative to horizon.
8	Roll	float	deg	Roll angle relative to horizon.
12	Latitude	double	deg	Estimated position in geodetic latitude.
20	Longitude	double	deg	Estimated position in geodetic longitude.
28	Altitude	double	m	Estimated height above ellipsoid. (WGS84)
36	VelocityX	float	m/s	Estimated velocity in NED frame. (North)
40	VelocityY	float	m/s	Estimated velocity in NED frame. (East)
44	VelocityZ	float	m/s	Estimated velocity in NED frame. (Down)
48	AccelX	float	m/s^2	Estimated acceleration in body frame. (X-axis)
52	AccelY	float	m/s^2	Estimated acceleration in body frame. (Y-axis)
56	AccelZ	float	m/s^2	Estimated acceleration in body frame. (Z-axis)
60	AngularRateX	float	rad/s	Estimated angular rate in body frame. (X-axis)
64	AngularRateY	float	rad/s	Estimated angular rate in body frame. (Y-axis)
68	AngularRateZ	float	rad/s	Estimated angular rate in body frame. (Z-axis)

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System sub-system. Once configured the data in this register will be sent out with the $VNISL header.

5.3.8.17 VNISE

Output Type: INS State - ECEF

Register ID: 73

Async Header: ISE

Access: Read Only

Size (Bytes): 72

Example Read Response: $VNRRG, 73, +170.558, +001.267, +001.762, +00.001502, - 00.000403, +00.000394, - 626343.88590823, - 5320499.92650050, +3450022.606, +000.001, -000.010, +000.094, +00.255, -00.308, -10.060*50

Example Async Message: $VNISE, +170.558, +001.267, +001.762, +00.001502, -00.000403, +00.000394, - 626343.88590823, - 5320499.92650050, +3450022.606, +000.001, -000.010, +000.094, +00.255, -00.308, -10.060*XX

Table 5-25: VNISE Settings

Offset	Name	Format	Unit	Description
0	Yaw	float	deg	Yaw angle relative to true north.
4	Pitch	float	deg	Pitch angle relative to horizon.
8	Roll	float	deg	Roll angle relative to horizon.
12	PositionX	double	m	Estimated position in ECEF. (X-axis)
20	PositionY	double	m	Estimated position in ECEF. (Y-axis)
28	PositionZ	double	m	Estimated position in ECEF. (Z-axis)
36	VelocityX	float	m/s	Estimated velocity in ECEF frame. (X-axis)
40	VelocityY	float	m/s	Estimated velocity in ECEF frame. (Y-axis)
44	VelocityZ	float	m/s	Estimated velocity in ECEF frame. (Z-axis)
48	AccelX	float	m/s^2	Estimated acceleration in body frame. (X-axis)
52	AccelY	float	m/s^2	Estimated acceleration in body frame. (Y-axis)
56	AccelZ	float	m/s^2	Estimated acceleration in body frame. (Z-axis)
60	AngularRateX	float	rad/s	Estimated angular rate in body frame. (X-axis)
64	AngularRateY	float	rad/s	Estimated angular rate in body frame. (Y-axis)
68	AngularRateZ	float	rad/s	Estimated angular rate in body frame. (Z-axis)

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System sub-system. Once configured the data in this register will be sent out with the $VNISE header.

5.3.8.18 VNDTV

Output Type: Delta Theta and Delta Velocity

Register ID: 80

Async Header: DTV

Access: Read

Comment: This register contains the output values of the onboard coning and sculling algorithm.

Size (Bytes): 28

Example Read Response: $VNRRG, 80, +0.665016, -000.119, -000.409, -000.025, +000.011, -000.084, -006.702*6A

Table 5-26: VNDTV Settings

Offset	Name	Format	Unit	Description
0	DeltaTime	float	sec	Delta time for the integration interval.
8	DeltaThetaX	float	deg	Delta rotation vector component in the x-axis.
10	DeltaThetaY	float	deg	Delta rotation vector component in the y-axis.
12	DeltaThetaZ	float	deg	Delta rotation vector component in the z-axis.
16	DeltaVelocityX	float	m/s	Delta velocity vector component in the x-axis.
20	DeltaVelocityY	float	m/s	Delta velocity vector component in the y-axis.
24	DeltaVelocityZ	float	m/s	Delta velocity vector component in the z-axis.

The Delta Theta and Delta Velocity register contains the computed outputs from the onboard coning and sculling algorithm. The coning and sculling integrations are performed at the IMU sample rate (nominally at 400Hz) and reset when the register data is output. If polling this register, the values will represent the delta time, angles, and velocity since the register was last polled. If the Delta

Theta/Velocity data is selected for asynchronous output via the Async Data Output Type register (Register 6, type 30), the integrals will be reset each time the data is asynchronously output at the configured rate.

The delta time output contains the length of the time interval over which the deltas were calculated. This can be used to check the interval time or to compute nonlinear “average” rates and accelerations from the integrated values.

The delta theta is output as a principal rotation vector, defined as the product of the unit vector of the principal rotation axis and the principal rotation angle in degrees. For small rotations, a typical use case for delta angles, the principal rotation vector elements may be treated individually as rotations in degrees about the individual sensor axes (in any Euler rotation sequence) with little error.

The delta velocity output provides the integration of the acceleration in the chosen frame, taking into account the coupling effects of any simultaneous rotation experienced.

The coning and sculling algorithm can be configured to operate in multiple frames and with a variety of compensations applied. See the Delta Theta and Delta Velocity Configuration Register in the IMU subsystem for further details

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System subsystem. Once configured the data in this register will be sent out with the $VNDTV header.

5.3.8.19 VNG2S

Output Type: GPS2 Solution - LLA

Register ID: 103

Async Header: G2S

Access: Read Only

Comment: The calculated navigation solution of the Ant B receiver, expressed in the LLA/NED frames. Updates at the GPS rate (5Hz default).

Size (Bytes): 72

Example Read Response: $VNRRG, 103, 505020.999614, 1941, 3, 13, +32.89195540, -096.70376740, +00165.491, +000.000, -000.008, -000.025, +001.320, +001.303, +003.259, +000.098, 2.00E-09*35

Table 5-27: VNG2S Settings

Offset	Name	Format	Unit	Description
0	Time	double	sec	GPS time of week in seconds.
8	Week	uint16	week	GPS week.
10	GpsFix	uint8	–	GPS fix type. See table below.
11	NumSats	uint8	–	Number of GPS satellites used in solution.
12	–	–	–	--- 4 PADDING BYTES ---
16	Latitude	double	deg	Latitude in degrees.
24	Longitude	double	deg	Longitude in degrees.
32	Altitude	double	m	Altitude above ellipsoid. (WGS84)
40	NedVelX	float	m/s	Velocity measurement in north direction.
44	NedVelY	float	m/s	Velocity measurement in east direction.
48	NedVelZ	float	m/s	Velocity measurement in down direction.
52	NorthAcc	float	m	North position accuracy estimate. (North)
56	EastAcc	float	m	East position accuracy estimate. (East)
60	VertAcc	float	m	Vertical position accuracy estimate. (Down)
64	SpeedAcc	float	m/s	Speed accuracy estimate.
68	TimeAcc	float	sec	Time accuracy estimate.

Table 5-28: GPS Fix

Value	Description
0	No fix
1	Time only
2	2D
3	3D

> **Note:** You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System sub-system. Once configured, the data in this register will be sent out with the $VNG2S header.

5.3.8.20 VNG2E

Output Type: GPS2 Solution - ECEF

Register ID: 103

Async Header: G2E

Access: Read Only

Comment: The calculated navigation solution of the Ant B receiver, expressed in the ECEF frame. Updates at the GPS rate (5Hz default).

Size (Bytes): 72

Example Read Response: $VNRRG, 104, 505024.199617, 1941, 3, 13, -0625837.176, -5324476.241, +3443992.903, -000.001, -000.020, +000.007, +001.311, +001.298, +003.198, +000.098, 2.00E-09*03

Table 5-29: VNG2E Settings

Offset	Name	Format	Unit	Description
0	Time	double	sec	GPS time of week.
8	Week	uint16	week	Current GPS week.
10	GpsFix	uint8	–	GPS fix type. See table below.
11	NumSats	uint8	–	Number of GPS satellites used in solution.
12	–	–	–	--- 4 PADDING BYTES ---
16	PositionX	double	m	ECEF X coordinate.
24	PositionY	double	m	ECEF Y coordinate.
32	PositionZ	double	m	ECEF Z coordinate.
40	VelocityX	float	m/s	ECEF X velocity.
44	VelocityY	float	m/s	ECEF Y velocity.

Offset	Name	Format	Unit	Description
48	VelocityZ	float	m/s	ECEF Z velocity.
52	PosAccX	float	m	ECEF X position accuracy estimate.
56	PosAccY	float	m	ECEF Y position accuracy estimate.
60	PosAccZ	float	m	ECEF Z position accuracy estimate.
64	SpeedAcc	float	m/s	Speed accuracy estimate.
68	TimeAcc	float	sec	Time accuracy estimate.

Table 5-30: GPS Fix

Value	Description
0	No fix
1	Time only
2	2D
3	3D

Note: You can configure the device to output this register at a fixed rate using the Async Data Output Type Register in the System sub-system. Once configured, the data in this register will be sent out with the $VNG2E header.

5.3.9 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:

?	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

5.3.10 Spectracom Format 1

Format 1 converts the received day of year data (001-366) to a date consisting of day of week, month, and day of the month. Format 1 also contains a time synchronization status character, year, and time reflecting time zone offset and DST correction when enabled.

Available Formats 1 and 1S are very similar to each other. Most external systems utilizing Data Format 1 will look for a single-digit day of the month for day 1 through day 9, with a space in front of each digit (^1, ^2, ^3 ... 10, 11...), whereas other systems need to see a two digit day of the month for all days 1 through 9 with a leading 0 instead of a space (01, 02, 03... 10, 11...).

- If your device requires the two digit day of the month for days 1 through 9 (i.e. 01, 02 etc.), select Format 1.
- If your device requires the single digit day of the month for days 1 through 9 (i.e. ^1, ^2, etc.), select Format 1S instead. Refer to "Spectracom Format 1S" on the next page 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:

?	When the receiver is unable to track any satellites and the time synchronization lamp is red.
*	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

Example:

FRI 20APR01 12:45:36

The example data stream provides the following information:

Sync Status	The clock is not time synchronized to GNSS. Time is derived from the battery backed clock or set manually
Date	Friday, April 23, 2015
Time	12:45:36

5.3.11 Spectracom Format 1S

Format 1S (Space) is very similar to Format 1, with the exception of a space being the first character of Days 1 through 9 of each month (instead of the leading “0” which is present in Format 1).

Most external systems utilizing Data Format 1 will look for a single digit day of the month for day 1 through day 9, with a space in front of each digit (^1, ^2, ^3 ... 10, 11...) whereas other systems need to see a two digit day of the month for all days 1 through 9 with a leading 0 instead of a space (01, 02, 03... 10, 11...).

» If your device requires the single digit day of the month for days 1 through 9 (i.e. 1, 2, etc.), select Format 1S.

» If your device requires the two digit day of the month for days 1 through 9 (i.e. 01, 02, etc.), select Format 1 instead. Refer to "Spectracom Format 1" on page 377 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:

?	When the receiver is unable to track any satellites and the time synchronization lamp is red.
*	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

Example:

FRI 20APR15 12:45:36

The example data stream provides the following information:

Sync Status	The clock is not time synchronized to GNSS. Time is derived from the battery backed clock or set manually.
Date	Friday April, 23, 2015
Time	12:45:36

5.3.12 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:

?	When the receiver is unable to track any satellites and the time synchronization lamp is red.
*	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The quality indicator (Q) provides an inaccuracy estimate of the output data stream. When the receiver is unable to track any GNSS satellites, a timer is started. "Quality indicators" below lists the quality indicators and the corresponding error estimates based upon the GNSS receiver 1PPS stability, and the time elapsed tracking no satellites. The Tracking Zero Satellites timer and the quality indicator reset when the receiver reacquires a satellite.

Quality	Time (hours)	TXCO Error (milliseconds)	OCXO Error (milliseconds)	Rubidium Error (microseconds)
Space	Lock	<1	<0.01	<0.3
A	<10	<10	<0.72	<1.8
B	<100	<100	<7.2	<18
C	<500	<500	<36	<90
D	>500	>500	>36	>90

Table 5-31: Quality indicators

The leap second indicator (L) is defined as:

(Space)	When a leap second correction is not scheduled for the end of the month.
L	When a leap second correction is scheduled for the end of the month.

The Daylight Saving Time indicator (D) is defined as:

S	During periods of Standard time for the selected DST schedule.
I	During the 24-hour period preceding the change into DST.
D	During periods of Daylight Saving Time for the selected DST schedule.
O	During the 24-hour period preceding the change out of DST.

Example:

?A15 271 12:45:36.123 S

The example data stream provides the following information:

Sync Status	The clock has lost GNSS time sync. The inaccuracy code of “A” indicates the expected time error is <10 milliseconds.
Date	Day 271 of year 2015.
Time	12:45:36 UTC time, Standard time is in effect.

5.3.13 Spectracom Format 3

Format 3 provides a format identifier, time synchronization status character, year, month, day, time with time zone and DST corrections, time difference from UTC, Standard time/DST indicator, leap second indicator and on-time marker. The Format 3 data structure is shown below:

Example message:

FFFFI^YYYYMMDD^HHMMSS±HHMMD L # CR LF

Where:

FFFF	Format Identifier (0003)
I	Time Sync Status (Space, ?, *)
^	Space separator
YYYY	Year (1999, 2000, 2001, etc.)
MM	Month Number (01-12)
DD	Day of the Month (01-31)

HH	Hours (00-23)
MM	Minutes (00-59)
SS	Seconds (00-60)
±	Positive or Negative UTC offset (+,-) Time Difference from UTC
HHMM	UTC Time Difference Hours Minutes (00:00-23:00)
D	Daylight Saving Time Indicator (S,I,D,O)
L	Leap Second Indicator (space, L)
#	On time point
CR	Carriage Return
LF	Line Feed

The time synchronization status character (`I`) is defined as described below:

?	When the receiver is unable to track any satellites and the time synchronization lamp is red.
*	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The time difference from UTC, ±HHMM, is selected when the Serial Com or Remote port is configured. A time difference of -0500 represents Eastern Time. UTC is represented by +0000.

The Daylight Saving Time indicator (`D`) is defined as:

S	During periods of Standard time for the selected DST schedule.
I	During the 24-hour period preceding the change into DST.
D	During periods of Daylight Saving Time for the selected DST schedule.
O	During the 24-hour period preceding the change out of DST.

The leap second indicator (`L`) is defined as:

(Space)	When a leap second correction is not scheduled for the end of the month.
L	When a leap second correction is scheduled for the end of the month.

Example:

0003 20150415 124536-0500D #

The example data stream provides the following information:

Data Format	3
Sync Status	Day 271 of year 2015.
Date	April 15, 2015.
Time	12:45:36 EDT (Eastern Daylight Time). The time difference is 5 hours behind UTC.
Leap Second	No leap second is scheduled for this month.

5.3.14 Spectracom Format 4

Format 4 provides a format indicator, time synchronization status character, modified Julian date, time reflecting UTC with 0.1 millisecond resolution and a leap second indicator. Format 4 data structure is shown below:

Example:

FFFFIMJDXX^HHMMSS.SSSS^L CR LF

Where:

FFFF	Format Identifier (0004)
I	Time Sync Status (Space, ?, *)
MJDXX	Modified Julian Date
^	Space separator
HH	Hours (00-23 UTC time)
MM	Minutes (00-59)
SS.SSSS	Seconds (00.0000-60.0000)
L	Leap Second Indicator (space, L)
CR	Carriage Return
LF	Line Feed

The start bit of the first character marks the on-time point of the data stream.

The time synchronization status character (`I`) is defined as described below:

?	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.

5.3.15 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:

?	When the receiver is unable to track any satellites and the time synchronization lamp is red.
*	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The leap second indicator (L) is defined as:

(Space)	When a leap second correction is not scheduled for the end of the month.
L	When a leap second correction is scheduled for the end of the month.

The Daylight Saving Time indicator (D) is defined as:

S	During periods of Standard time for the selected DST schedule.
I	During the 24-hour period preceding the change into DST.
D	During periods of Daylight Saving Time for the selected DST schedule.
O	During the 24-hour period preceding the change out of DST.

Example:

? 15 271 12:45:36.123 S

The example data stream provides the following information:

Sync Status	The clock has lost GNSS time sync.
Date	Day 271 of year 2015.
Time	12:45:36 UTC time, Standard time is in effect.

5.3.16 Spectracom Format 8

Format 8 includes a time synchronization status character, the four digit year, day of year, time reflecting Time Zone Offset and DST corrections when enabled. Format 8 also includes the DST/Standard Time indicator, and the Time Zone Offset value. Format 8 data structure is shown below:

Example:

CR LF I ^ ^YYYY^ DDD ^ HH:MM:SS ^ D+XX CR LF
or
CR LF I ^ ^YYYY^ DDD ^ HH:MM:SS ^ D-XX CR LF

Where:

CR	Carriage Return
LF	Line Feed
I	Time Sync Status (space, ?, *)
YYYY	Four digit year indication
^	Space separator
DDD	Day of Year (001-366)
HH	Hours (00-23)
:	Colon separator
MM	Minutes (00-59)
SS	Seconds (00-60)

D	Daylight Saving Time indicator (S,I,D,O)
XX	Time Zone Switch Setting (±00...12)

The leading edge of the first character (CR) marks the on-time point of the data stream. Time sync status character (I) is described below:

(Space)	When VersaSync is synchronized to UTC source.
*	When VersaSync time is set manually.
?	When VersaSync 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.

5.3.17 Spectracom Format 9

Format 9 provides Day-of-Year and Time information.

Example message:

<SOH>DDD:HH:MM:SSQ<CR><LF>

Where:

SOH	Start of header (ASCII Character 1)
DDD	Day of Year (001-366)
:	Colon Separator
HH	Hours (00-23)
MM	Minutes (00-59)
SS	Seconds (00-59) (00-60 for leap second)
Q	Time Sync Status [as INPUT] space = SYNC '.' = SYNC '*'=NOT IN SYNC '#' = NOT IN SYNC "?" = NOT IN SYNC

Q	Time Sync Status [as OUTPUT] space = Time error is less than time quality flag 1's threshold (TFOM < or = 3) “.” = Time error has exceeded time quality flag 1's threshold (TFOM = 4) “*” = Time error has exceeded time quality flag 2's threshold (TFOM = 5) “#” = Time error has exceeded time quality flag 3's threshold (TFOM = 6) “?” = Time error has exceeded time quality flag 4's threshold OR a reference source is unavailable (TFOM >=7)
CR	Carriage Return (ASCII Character 13)
LF	Line Feed (ASCII Character 10)

The leading edge of the first character (CR) marks the on-time point of the data stream.

5.3.17.1 Format 9S

Format 9S is a variation of ASCII Format 9 that uses Sysplex compatible fields indicating sychronization status:

FL_SYNC_SYS_REF_NONE ('X')	Never been in sync
FL_SYNC_SYS_REF_YES (' ')	In sync with a reference
FL_SYNC_SYS_REF_LOST ('F')	Out of sync, lost reference

5.3.18 Spectracom Epsilon Formats

5.3.18.1 Spectracom Epsilon TOD 1

This message corresponds to the TOD 1 format provided by EPSILON 2S/3S Series products on RS232/422 ports.

The structure of this format is as follows:

» <space>DD/MM/YYYY<space>HH:MM:SST(CR)(LF)

Length=23 bytes

Where:

<space>	separator
DD	2-digit Day of month
</>	separator

MM	2-digit Month
</>	separator
YYYY	4-digit Year
<space>	separator
HH	2-digit Hour
:	separator
MM	2-digit Minutes
:	separator
SS	2-digit Seconds
T	1-digit Timescale ('N' None, 'G' GPS, 'U' UTC, 'A' TAI, 'L' Local, 'M' Manual)
(CR)	Carriage Return (ASCII Character 13 0x0D)
(LF)	Line Feed (ASCII Character 10 0x0A)

5.3.18.2 Spectracom Epsilon TOD 3

This message corresponds to the TOD 3 format provided by EPSILON 2S/3S Series products on RS232/422 ports.

The structure of this format is as follows:

» <space>DOY/YYYY<space>HH:MM:SS<space>T(CR)(LF)

Length=22 bytes

Where:

<space>	separator
DOY	3-digit Day of year
</>	separator
YYYY	4-digit Year
</>	separator
YYYY	4-digit Year
<space>	separator
HH	2-digit Hour
:	separator

MM	2-digit Minutes
:	separator
SS	2-digit Seconds
T	1-digit Timescale ('N' None, 'G' GPS, 'U' UTC, 'A' TAI, 'L' Local, 'M' Manual)
(CR)	Carriage Return (ASCII Character 13 0x0D)
(LF)	Line Feed (ASCII Character 10 0x0A)

5.3.18.3 Spectracom Epsilon TOD D1

This message corresponds to the TOD 3 format provided by EPSILON 2S/3S Series products on RS232/422 ports.

If the day is less than 10, the structure of this format is as follows:

» <space>D/MM/YYYY<space>HH:MM:SST(CR)(LF)(CR)

Length=23 bytes

Where:

<space>	separator
D	1-digit Day of month
</>	separator
MM	2-digit Month
</>	separator
YYYY	4-digit Year
<space>	separator
HH	2-digit Hour
:	separator
MM	2-digit Minutes
:	separator
SS	2-digit Seconds
T	1-digit Timescale ('N' None, 'G' GPS, 'U' UTC, 'A' TAI, 'L' Local, 'M' Manual)
(CR)	Carriage Return (ASCII Character 13 0x0D)
(LF)	Line Feed (ASCII Character 10 0x0A)

(CR)	Carriage Return (ASCII Character 13 0x0D)

If the day is greater than 10, the structure of this format is as follows:

» DD/MM/YYYY<space>HH:MM:SST(CR)(LF)(CR)

Length=23 bytes

Where:

DD	2-digit Day of month
</>	separator
MM	2-digit Month
</>	separator
YYYY	4-digit Year
<space>	separator
HH	2-digit Hour
:	separator
MM	2-digit Minutes
:	separator
SS	2-digit Seconds
T	1-digit Timescale ('N' None, 'G' GPS, 'U' UTC, 'A' TAI, 'L' Local, 'M' Manual)
(CR)	Carriage Return (ASCII Character 13 0x0D)
(LF)	Line Feed (ASCII Character 10 0x0A)
(CR)	Carriage Return (ASCII Character 13 0x0D)

5.3.19 BBC Message Formats

5.3.19.1 Format BBC-01

This format is based on string ASCII characters, and is sent once per second. It provides year, month, day, day of week, day of month, hours, minutes, and seconds.

Number of characters: 24 (including CRLF and '.')

Example message:

T:ye:mo:da:dw:ho:mi:sc

Where:

T	Indicates the synchronous moment for the time setting.
ye	Year (00-99)
mo	Month (01-12)
da	Day of month (01-31)
dw	Day of week (01=Monday to 7=Sunday)
ho	Hours (00-23)
mi	Minutes (00-59)
sc	Seconds (00-59)

5.3.19.2 Format BBC-02

This is a hexadecimal frame/message sent twice per second. The message should be sent such that the final "99" occurs at 0 msec and 500 msec.

Number of bytes: 26

Format:

START		Year		Month	Day	Hour	Min	Sec.
AA	AA	07	DA	06	16	13	59	01

Millisecond		Time Zone		Daylight	Leap-second Sign	Leap-second Month	Leap-second Zone	GPS Week	
02	BA	80	00	00	00	00	00	1A	2A

GPS Second			GPS to UTC Offset	Check-sum	END	
09	3A	7E	12	FE	99	99

Where:

Leap Second Sign:

- 01=Positive
- FF=Negative
- 00=No leap second

Leap Second Month:

- 00=None scheduled
- 03=March
- 06=June
- 09=September
- 0C=December

Leap Second Zone:

- 0=Out of zone
- 1=Within zone
- Zone is 15 minutes before to 15 minutes after a leap second.

GPS Week:

- Up to FFFF

GPS Second:

- Second of week 000000 up to 093A7F (604799 decimal)

GPS to UTC offset:

- 2's complement binary signed integer, seconds

Checksum:

- Sum of all bytes up to and including the checksum (sum includes the AAAA start identifier but excludes the 9999 end identifier)

5.3.19.3 Format BBC-03 PSTN

The third format is a string ASCII characters and is sent on a received character.

The message should be advanced by an appropriate number such that the stop bit of each <CR> occurs at the start of the next second. For example, at 300 baud, 8 data bits, 1 stop bit, and no parity, each byte takes 10/300 s=33 ms, so the <CR> byte should be advanced by 33 ms in order for the <CR>'s stop bit to line up with the start of the next second.

Time information is available in UTC format or UK TOD format.

't' command

Input format: t<CR>

Output format:

Current Second	Second + 1	Second + 2	Second + 3
<CR>	HHMMSS<CR>	HHMMSS<CR>	HHMMSS<CR>

Number of characters: 7 (including CR)

Each HHMMSS filed refers to the time at the start of the next second. The data transmitted by VersaSync is timed so that the stop bit of each <CR> ends at the start of the next second.

'd' command

VersaSync transmits the date on request.

Input format: d<CR>

Output format: YYMMDD<CR>

Number of output characters: 7 (including CR)

's' command

VersaSync transmits the status information on request.

Input format: s<CR>

Output Format: status

Number of output characters: 1

Where returned, values for status are:

- G = System Good
- D = Failure of VersaSync internal diagnostics
- T = VersaSync does not have correct time

‘l’ command

The loopback command will cause VersaSyncto echo the next character received back to the caller. This may be used by a caller’s equipment to calculate the round trip delay across the PSTN connection in order to apply a correction to the received time data.

Input format: l<CR>

Output format: (Next character received)

‘hu’ command

The hang up command will cause VersaSync to drop the line immediately and terminate the call.

Input format: hu<CR>

5.3.19.4 Format BBC-04

This format is a string of ASCII characters and is sent once per second.

Number of characters: 18 (including CRLF)

Example message:

T:ho:mi:sc:dw:da:mo:ye:lp:cs<CR><LF>

Where:

T	Indicates the synchronous moment for the time setting.
ho	Hours (00-23)
mi	Minutes (00-59)
sc	Seconds (00-59)
dw	Day of week (01=Monday to 7=Sunday)

da	Day of month (01-31)
mo	Month (01-12)
ye	Year (00-99)
lp	0 (for 60s, no leap) or 1 (for 61s, leap)
cs	Checksum. This is calculated from the start of the message, including start identifier and excluding CRLF. It is created by adding all the 1s. If the sum is even, 0 is returned. If the sum is odd, 1 is returned. This is mathematically the same as sequentially running an XOR on each bit of each byte.

Standard Serial configuration is:

- RS-232 format
- 115200 baud
- 8 data bits
- 1 stop bit
- No parity

5.3.19.5 Format BBC-05 (NMEA RMC Message)

The NMEA Message Format RMC, (Recommended Minimum) provides fix information, speed over ground and Magnetic Variance information. Note that this RMC Message is not 100% identical to the official NMEA RMC MESSAGE (that corresponds to the 3.01 NMEA 0183 standard and is another time code format supported by VersaSync.)

The BBC RMC message (BBC-05) corresponds to Version 2 of the NMEA 0183 standard, following the description below:

Example message:

$GPRMC,123519,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A

Where:

RMC	Recommended Minimum sentence C

123519	Fix taken at 12:35:19 UTC
A	Status: A=active or V=Void.
4807.038,N	Latitude 48 deg 07.038′ N
01131.000,E	Longitude 11 deg 31.000′ E
22.4	Speed over the ground in knots
84.4	Track angle in degrees True
230394	Date—23rd of March 1994
003.1,W	Magnetic Variation
*6A	The checksum data, always begins with *

5.3.20 GSSIP Message Format

The GSSIP[1] format includes 3 ICD-GPS-153C messages which are used to support emulation of a SAASM GPS used in a SINCGARS interface. The messages are the Buffer Box (253), Time Transfer (5101), and the Current Status (5040).

The ICD-GPS-153C protocol defines the format of these messages. The Current Status and Time Transfer are sent once per second (1Hz). The Buffer Box is sent once every 6 seconds (1/6 Hz).

The purpose of these three messages is to emulate a SINCGARS interface connection to a SAASM GPS. VersaSync 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 VersaSync and receive time and 1PPS as if communicating with and ICD-GPS-153C compatible SAASM GPS.

These commands are emulated only and contain only time information; position and velocity information is zeroed out. No controlled data is included in the messages, hence no SAASM GPS receiver is required.

The ASCII Output supports two configurations for supporting SINCGARS:

[1]GSSIP = GPS STANDARD SERIAL INTERFACE PROTOCOL

A configuration of Time Transfer as Message Format1 and Current Status as Format2 causes the SINCGARS protocol to be emulated and the machine state to be initializated.

- **Format1**: Time Transfer (5101)
- **Format2**: Current Status (5040)
- **Format3**: Buffer Box (253)

A configuration of Current Status as Message Format1 and Time Transfer as Format2 results in broadcasting of the messages Current Status (1Hz), Time Transfer (1Hz), and Buffer Box (1/6Hz) at their default rates.

- **Format1**: Current Status (5040)
- **Format2**: Time Transfer (5101)
- **Format3**: Buffer Box (253)

5.3.21 EndRun Formats

The following formats provide compatibility with **EndRun** technology.

5.3.21.1 EndRun Time Format

Example message:

T YYYY DDD HH:MM:SS zZZ m<CR><LF>

Where:

T	Time Figure of Merit character (TFOM), limited to the range 6 to 9: 9 indicates error >±10 milliseconds, or unsynchronized condition 8 indicates error <±10 milliseconds 7 indicates error <±1 millisecond 6 indicates error <±100 microseconds
YYYY	Year
DDD	Day of Year (001-366)
HH	Hour of the day (00-23)
:	Colon Separator

MM	Minutes of the hour
SS	Seconds (00-59), (00-60 for leap second)
z	The sign of the offset to UTC, + implies time is ahead of UTC
ZZ	The magnitude of the offset to UTC in units of half-hours. If ZZ = 0, then z = +
m	Time mode character, is one of: G = GPS L = Local U = UTC T = TAI
CR	Carriage Return
LF	Line Feed

5.3.21.2 EndRunX (Extended) Time Format

The **EndRunX** format is identical to the **EndRun** format, with the addition of two fields: the current leap second settings and the future leap second settings.

The following example message string is sent once each second:

T YYYY DDD HH:MM:SS zZZ m CC FF<CR><LF>

Where:

T	Time Figure of Merit character (TFOM), limited to the range 6 to 9: 9 indicates error >±10 milliseconds, or unsynchronized condition 8 indicates error <±10 milliseconds 7 indicates error <±1 millisecond 6 indicates error <±100 microseconds
YYYY	Year
DDD	Day of Year (001-366)
HH	Hour of the day (00-23)
:	Colon Separator
MM	Minutes of the hour

SS	Seconds (00-59), (00-60 for leap second)
z	The sign of the offset to UTC, + implies time is ahead of UTC
ZZ	The magnitude of the offset to UTC in units of half-hours. If ZZ = 0, then z = +
m	Time mode character, is one of: G = GPS L = Local U = UTC T = TAI
CC	The current leap seconds
FF	The future leap seconds, which will show a leap second pending 24 hours in advance
CR	Carriage Return
LF	Line Feed

5.3.22 Event Broadcast Time Code Formats

The following ASCII-based time code formats are available:

5.3.22.1 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

5.3.22.2 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

5.4 IRIG Standards and Specifications

5.4.1 About the IRIG Output Resolution

The IRIG output signals are generated from VersaSync's System Time, which can be synced to one or more external input references (such as GPS, IRIG, PTP, etc). The accuracy of the System time to true UTC time is dependent upon what the selected external reference is (with GPS typically being the most accurate reference for the system to sync with).

IRIG AM synchronization of a device to its IRIG source is typically measured in the tens of microseconds, while synchronization using a IRIG DCLS signal can typically provide around 100 nanoseconds or so (plus the cable delays between VersaSync and the other device, as well as the processing delays of the other system itself).

IRIG AM functionality is available through an option card.

Note that all IRIG outputs has its own available 'offset' capability, which is configurable via VersaSync's Web UI, to help account for cabling and processing delays of the device each output is connected with.

5.4.2 IRIG Carrier Frequencies

Each IRIG code specifies a carrier frequency that is modulated to encode date and time, as well as control bits to time-stamp events. Initially, IRIG applications were primarily military and government associated. Today, IRIG is commonly used to synchronize voice loggers, recall recorders, and sequential event loggers found in emergency dispatch centers and power utilities.

Table 5-32: Available IRIG output signals

Format	Encoding	Modulation	Carrier	Coded Expressions	Bit rate	Time Frame Interval
IRIG-A						
IRIG-A	A000	DCLS	N/A	BCD_{TOY}, CF and SBS	1000 pps	0.1 sec
IRIG-A	A001	DCLS	N/A	BCD_{TOY}, CF	1000 pps	0.1 sec
IRIG-A	A002	DCLS	N/A	BCD_{TOY}	1000 pps	0.1 sec
IRIG-A	A003	DCLS	N/A	BCD_{TOY}, SBS	1000 pps	0.1 sec
IRIG-A	A004	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, CF and SBS	1000 pps	0.1 sec
IRIG-A	A005	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and CF	1000 pps	0.1 sec
IRIG-A	A006	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}	1000 pps	0.1 sec

Format	Encoding	Modulation	Carrier	Coded Expressions	Bit rate	Time Frame Interval
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						
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

Format	Encoding	Modulation	Carrier	Coded Expressions	Bit rate	Time Frame Interval
IRIG-B	B122	AM	1 kHz	BCD_{TOY}	100 pps	1 sec
IRIG-B	B123	AM	1 kHz	BCD_{TOY}, SBS	100 pps	1 sec
IRIG-B	B124	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}, CF and SBS	100 pps	1 sec
IRIG-B	B125	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}, and CF	100 pps	1 sec
IRIG-B	B126	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}	100 pps	1 sec
IRIG-B	B127	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}, and SBS	100 pps	1 sec
IRIG-E						
IRIG-E	E000	DCLS	N/A	BCD_{TOY}, CF and SBS	10 pps	1 sec
IRIG-E	E001	DCLS	N/A	BCD_{TOY}, CF	10 pps	1 sec
IRIG-E	E002	DCLS	N/A	BCD_{TOY}	10 pps	1 sec
IRIG-E	E003	DCLS	N/A	BCD_{TOY}, SBS	10 pps	1 sec
IRIG-E	E004	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, CF and SBS	10 pps	1 sec
IRIG-E	E005	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and CF	10 pps	1 sec
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

Format	Encoding	Modulation	Carrier	Coded Expressions	Bit rate	Time Frame Interval
IRIG-E	E117	AM	100 Hz	BCD_{TOY}, BCD_{YEAR}, and SBS	10 pps	1 sec
IRIG-E	E120	AM	100 Hz	BCD_{TOY}, CF and SBS	10 pps	1 sec
IRIG-E	E121	AM	1kHz	BCD_{TOY}, CF	10 pps	10 sec
IRIG-E	E122	AM	1kHz	BCD_{TOY}	10 pps	10 sec
IRIG-E	E123	AM	1kHz	BCD_{TOY}, SBS	10 pps	10 sec
IRIG-E	E124	AM	1kHz	BCD_{TOY}, BCD_{YEAR}, CF and SBS	10 pps	10 sec
IRIG-E	E125	AM	1kHz	BCD_{TOY}, BCD_{YEAR}, and CF	10 pps	10 sec
IRIG-E	E126	AM	1kHz	BCD_{TOY}, BCD_{YEAR}	10 pps	10 sec
IRIG-E	E127	AM	1kHz	BCD_{TOY}, BCD_{YEAR}, and SBS	10 pps	10 sec
IRIG-G						
IRIG-G	G001	DCLS	N/A	BCD_{TOY}, CF	10000 pps	10 msec
IRIG-G	G002	DCLS	N/A	BCD_{TOY}	10000 pps	10 msec
IRIG-G	G005	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and CF	10000 pps	10 msec
IRIG-G	G006	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}	10000 pps	10 msec
IRIG-G	G141	AM	100 kHz	BCD_{TOY}, CF	10000 pps	10 msec
IRIG-G	G142	AM	100 kHz	BCD_{TOY}	10000 pps	10 msec
IRIG-G	G145	AM	100 kHz	BCD_{TOY}, BCD_{YEAR}, and CF	10000 pps	10 msec
IRIG-G	G146	AM	100 kHz	BCD_{TOY}, BCD_{YEAR}	10000 pps	10 msec
NASA-36						
NASA-36	N/A	AM	1msec	UNKNOWN	100 pps	1 sec

Format	Encoding	Modulation	Carrier	Coded Expressions	Bit rate	Time Frame Interval
NASA-36	N/A	DCLS	10 msec	UNKNOWN	100 pps	1 sec

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.

VersaSync can provide various IRIG code in amplitude modulated (AM) or pulse width coded (TTL) formats, depending on your unit configuration and additional options. A signature control feature may be enabled for any IRIG output. Signature control removes the modulation code when a Time Sync Alarm is asserted.

5.4.3 IRIG B Output

The IRIG B Time Code description follows.

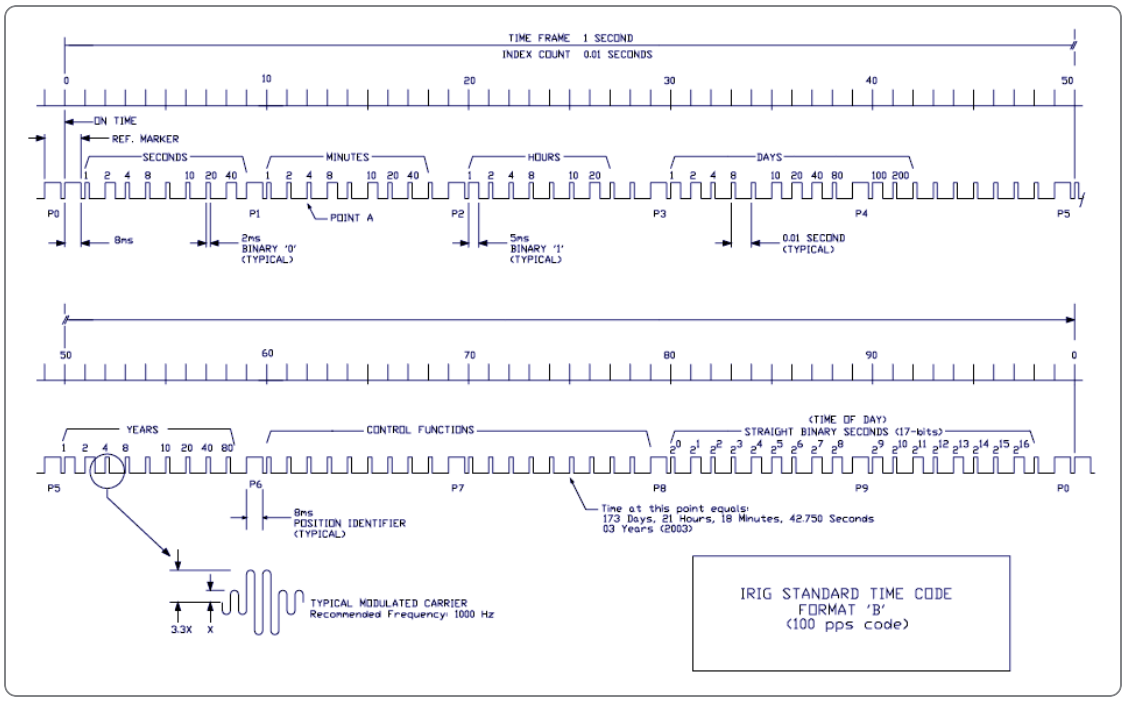


Figure 5-1: IRIG B time code description

The IRIG B code contains the Binary Coded Decimal (BCD) time of year, Control Function (CF) field and the Straight Binary Seconds time of day. The following figure illustrates the IRIG B data structure. The BCD time of year provides the day of the year, 1-366, and the time of day including seconds. The hour of the day is expressed in 24 hour format. The SBS time is the number of seconds elapsed since midnight. The Control Function field contains year information and a time synchronization status bit.

1. Time frame: 1.0 seconds.
2. Code digit weighting:
    A. Binary Coded Decimal time-of-year.
    - » Code word - 30 binary digits.
    - » Seconds, minutes hours, and days.
    - » Recycles yearly.

    B. Straight Binary Seconds time-of-day.

- Code word - 17 binary digits.
- Seconds only, recycles daily.

3. Code word structure:
   - **BCD**: Word seconds digits begin at index count 1. Binary coded elements occur between position identifier elements P0 and P5 (7 for seconds, 7 for minutes, 6 for hours, and 10 for days) until the code word is complete. An index marker occurs between decimal digits in each group to provide separation for visual resolution. Least significant digit occurs first.
   - **CF**: IRIG formats reserve a set of elements known as Control Functions (CF) for the encoding of various control, identification, or other special purpose functions. IRIG B has 27 Control Functions located between elements 50 and 78. The VersaSync uses the Control Functions to encode year information and time synchronization status.

The table below lists the **Control Function Field** and the function of each element.

- Element 55 is the time synchronization status bit. Element 55 is a Binary 1 when the unit is in sync, and a Binary 0 when it is not.
- 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: 1kHz when modulated.

Table 5-33: IRIG B control function field

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

C.F. Element #	Digit #	Function
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

5.4.4 IRIG E Output

The **IRIG E** code contains the Binary Coded Decimal (BCD) time of year and Control Functions. The figure IRIG E Time Code Description illustrates the IRIG E data structure. The BCD time of year provides the day of year, 1-366, and time of day to tens of seconds. The hour of the day is expressed in 24 hour format. The Control Function field includes a time synchronization status bit, year information and SBS time of day.

- **Time frame**: 10 seconds.
- **Code Digit Weighting**:
  - Binary Coded Decimal time of year.
  - Code world - 26 binary digits.
  - Tens of seconds, minutes, hours, and days.
  - Recycles yearly.

- **Code Word Structure**: BCD word tens of seconds digits begin at index count 6. Binary coded elements occur between position identifier elements

P0 and P5 (3 for seconds, 7 for minutes, 6 for hours, and 10 for days) until the code word is complete. An index marker occurs between decimal digits in each group to provide separation for visual resolution. Least significant digit occurs first.

- **Control Functions**: IRIG formats reserve a set of elements known as Control Functions (CF) for the encoding of various control, identification, or other special purpose functions. IRIG E has 45 Control Functions located between elements 50 and 98. The VersaSync 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.

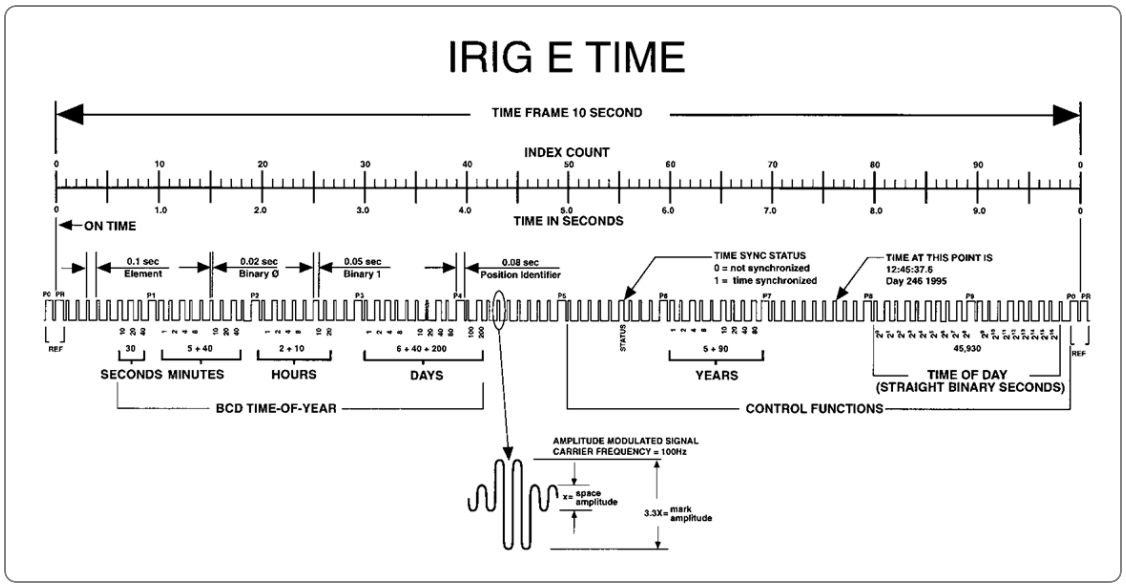


Figure 5-2: IRIG E time code description

Additional information

The beginning of each 10 second time frame is identified by two consecutive 80 ms elements (P_0 and P_R). The leading edge of the second 80 ms element (P_R) is the "on time" reference point for the succeeding time code. 1PPS position identifiers P_0, P_1 ... P_9 (80 ms duration) occur 0.1 s before 1PPS "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 for combination of control function elements can be pro-

grammed to read a binary "one" during any specified number of time frames. Each control element is identified on the Control Function Field Table.

Table 5-34: IRIG E control function field

BIT No.	CF ELEMENT No.	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

BIT No.	CF ELEMENT No.	FUNCTION
75	24	SPACE
76	25	SPACE
77	26	SPACE
78	27	SPACE
79	PID P8	POSITION IDENTIFIER
80	28	SBS 20
81	29	SBS 21
82	30	SBS 22
83	31	SBS 23
84	32	SBS 24
85	33	SBS 25
86	34	SBS 26
87	35	SBS 27
88	36	SBS 28
89	PID P9	POSITION IDENTIFIER
90	37	SBS 29
91	38	SBS 210
92	39	SBS 211
93	40	SBS 212
94	41	SBS 213
95	42	SBS 214
96	43	SBS 215
97	44	SBS 216
98	45	SPACE
99	PID P0	POSITION IDENTIFIER

5.4.5 IRIG Output Accuracy Specifications

The IRIG outputs deliver signals with the following 1PPS accuracy:

IRIC DCLS

Signal Category	Measured Accuracy
IRIG A	30 ns
IRIG B	30 ns
IRIG G	30 ns
IRIG NASA	30 ns
IRIG E	30 ns

IRIG AM

Signal Category	Measured Accuracy
IRIG A	200 ns
IRIG B	800 ns
IRIG G	200 ns
IRIG NASA	800 ns
IRIG E	1.5 µs

5.5 IRIG AM Option Card

These instructions apply to the VersaSync model 1228-2xx4 AM-IRIG Option Card. This card supports IRIG AM formats A, B, G, E, and NASA-36; it also includes up to 2 IRIG AM inputs or 4 IRIG AM outputs. Your VersaSync IRIG AM Option Card comes pre-installed at the factory, and only requires basic configuration of your unit before use.

5.5.1 Pinout for IRIG AM

There are four dedicated channels for the IRIG AM Option Card: 3 outputs and 1 input. To use these channels for the purpose of IRIG AM, you will need to set the pinout on the multi I/O connector using the Web UI. There are four configurable

IRIG AM channels: pins 11 & 12, 13 & 14, 15 & 16, and 17 & 18 (see the chart on the following page for specifics on all pinout configuration options).

- Pins 11 & 12 – IRIG AM Output or Input
- Pins 13 & 14 – IRIG AM Output or Input
- Pins 15 & 16 – IRIG AM Output
- Pins 17 & 18 – IRIG AM Output

To update the pin layout and configure the IRIG AM channels:

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

Choose IRIG-AM for the Type Filter, under Signal select either **IRIG_OUT | IRIG-AM** or **IRIG_IN | IRIG-AM**, and select the pin set numbers for the pin pair you wish to configure. Click Submit.

The Layout panel should display your new settings.

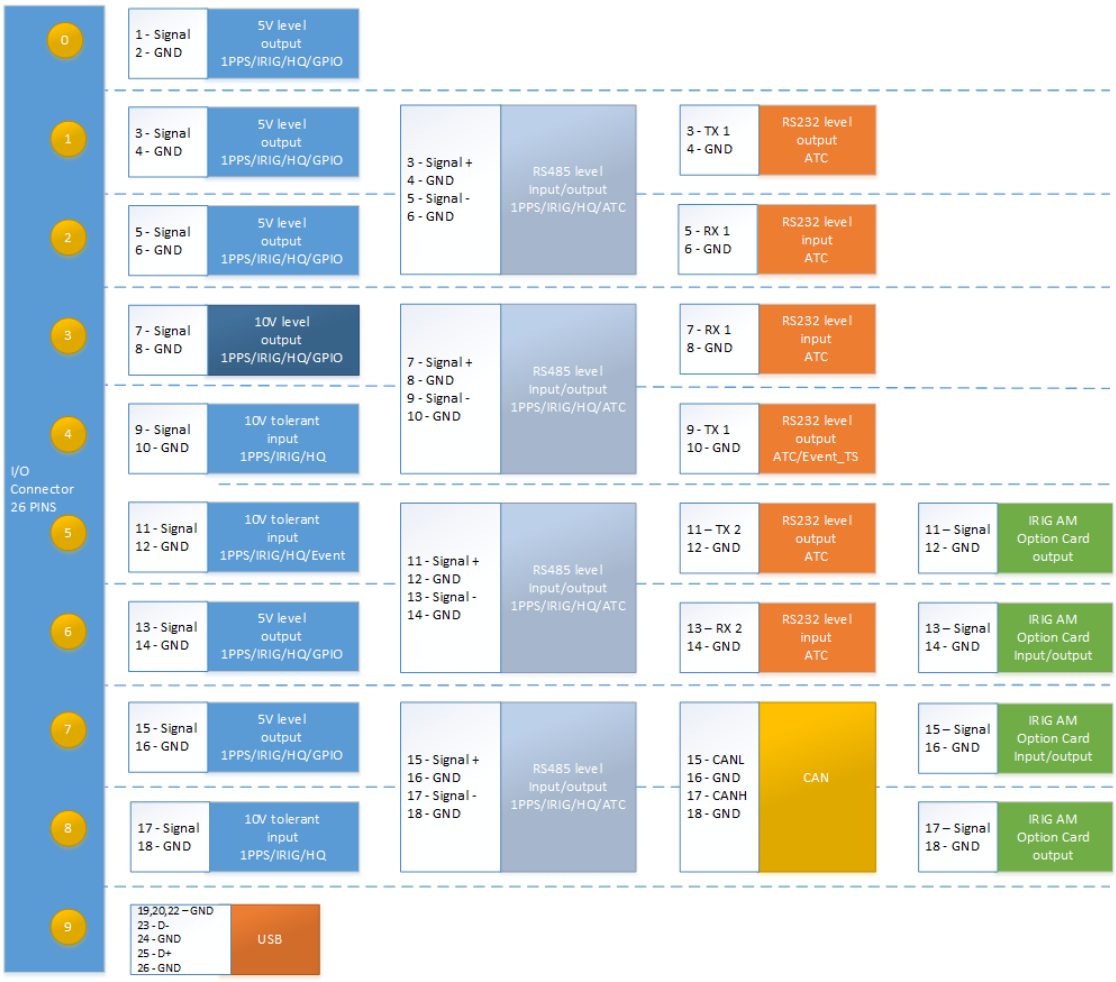
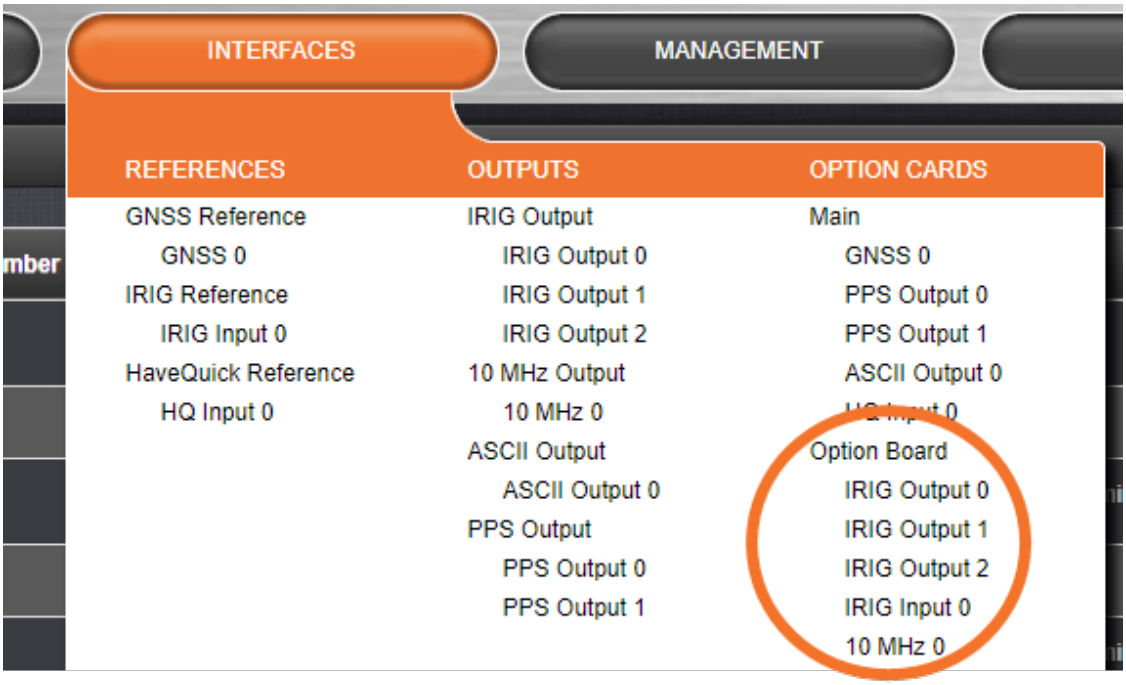


Figure 5-3: VersaSync Pinout (IRIG AM Option Card in Green)

5.5.2 IRIG AM Settings

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



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

The 10 MHz Output (**10 MHz 0**) controls move from the Main board to the Option Board on units with the IRIG-AM board installed. This does not affect the configuration or performance of the output(s).

IRIG AM Output settings

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

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

Modulation: [IRIG AM Only]

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

Note on Format and Frequency: only the following format and frequency combinations are software supported:

- IRIG A: 10 KHz
- IRIG B: 1 KHz
- IRIG G: 100 KHz
- NASA 36: 1 KHz
- IRIG E: 1 KHz

Amplitude: Must be between 0 and 255.

Coded Expression: [(0) BCD TOY, CF, BS, (1) BCD TOY, CF, (2) BCD TOY, (3) BCD TOY, BS, (4) BCD TOY/Year, CF, BS, (5) BCD TOY/Year, CF, (6) BCD TOY/Year, (7) BCD TOY/Year, BS], where:

- BCD = Binary Coded Decimal
- TOY = Time of Year
- CF = Control Function
- BS = Binary Seconds

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

Control Function Conformance: [Fields conform to RCC 200-04, IEEE C37.118-2005, Spectracom format, Spectracom FAA format, or Spectracom IEEE C37.188-2005]

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

IRIG AM Input settings

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

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

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

Coded Expression: [(0) BCD TOY, CF, BS, (1) BCD TOY, CF, (2) BCD TOY, (3) BCD TOY, BS, (4) BCD TOY/Year, CF, BS, (5) BCD TOY/Year, CF, (6) BCD TOY/Year, (7) BCD TOY/Year, BS], where:

- BCD = Binary Coded Decimal
- TOY = Time of Year

- CF = Control Function
- BS = Binary Seconds

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

Control Function Conformance: [Fields conform to RCC 200-04, IEEE C37.118-2005, Spectracom format, Spectracom FAA format, or Spectracom IEEE C37.188-2005]

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

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

5.6 Subnet Mask Values

Table 5-35: Subnet mask values

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

5.7 Maintenance

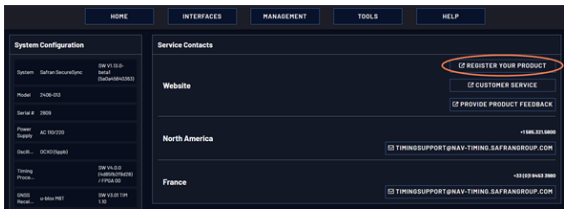
Safran recommends regularly cleaning the inlet air vents of your VersaSync unit to ensure long term functionality.

VersaSync has a small internal recharging lithium coin cell battery to support the Real Time Clock. If the unit is left unpowered for any amount of time up to 4 months, it is recommended to plug in and power the unit continuously for 7 days. This fully charges the battery and prevents potential damage from being left unpowered for long periods of time.

5.8 Product Registration

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

Upon initial start of the VersaSync Web UI, you will be prompted to register your new product. It is also possible to register at a later time via the HELP menu item, or directly on the **Safran Trusted 4D website:** https://register.safran-navigation-timing.com/



5.9 Technical Support

To request technical support for your VersaSync unit, please go to the "Timing Support" page of the Safran Trusted 4D website, where you can not only submit a support request, but also find additional technical documentation.

Phone support is available during regular office hours under the telephone numbers listed below.

To speed up the diagnosis of your VersaSync, please send us:

- the current **product configuration**, and
- the **events log**.

To save, bundle, and download all logs AND current configs:

1. Navigate to **HELP > Download Logs & Configs**.
2. The logs and current configuration files will be automatically downloaded.

Thank you for your cooperation.

5.9.1 Product Feedback

Product feedback may be provided by logging into the Web UI, navigating to **HELP** > **Contact/Register**, and selecting the PROVIDE PRODUCT FEEDBACK button. This is also possible directly on the Safran Trusted 4D website: https://safran-navigation-timing.com/product-feedback/

5.9.2 Regional Contact

Safran Trusted 4D operates globally and has offices in several locations around the world. Our main offices are listed below:

Country	Location	Phone
France	Les Ulis, Cedex	+33 (0)1 6453 3980
Spain	Granada	+34 958 285 024
USA	Rochester, NY	+1.585.321.5800

Table 5-36: Safran contact information

Additional regional contact information can be found on the Contact page of the Safran Trusted 4D website.

5.10 Return Shipments

Please contact Safran Technical Support before returning any equipment to Safran. Technical Support must provide you with a Return Material Authorization Number (RMA#) prior to shipment.

When contacting Technical Support, please be prepared to provide your equipment serial number(s) and a description of the failure symptoms or issues you would like resolved.

Freight to Safran is to be prepaid by the customer.

Note: Should there be a need to return equipment to Safran, it must be shipped in its original packing material. Save all packaging material for this purpose.

5.11 List of Tables

5.12 List of Images

5.13 Document Revision History

Rev	Description	Date
1	First-generation VersaSync User Manual.	August 2016
2	Errata. Document maintenance.	
3	Errata. Document maintenance.	

Rev	Description	Date
4	ZeroConf topic added. Errata. Document maintenance	July 2017
5	Errata implementation: Power consumption specifications. Replaced long-term stability specifications stated in Chapter3. under Holdover to short term stability.	Sept. 2017
6	Updated for latest software. Errata. Document maintenance.	August 2018
7	Updated for static IP default. Added reverse polarity warning. New grounding info. Updated power cable drawing. Document maintenance.	August 2019
8	Corrected oscillator holdover performance values. Added new front panel images to reflect latest design.	August 2020
9	Refreshed mechanical chassis drawings. Corrected Ethernet cable drawing. Updated PTP information and instruction. Corrected to reflect latest software features and capabilities.	October 2021
9.1	Added two PTP profiles	December 2021
10	Added information on new Sanitizing data procedure, rollback and downgrade information, and HSTS and Security Issues Web UI page descriptions. Added mRO-50 oscillator information. Errata updates.	May 2022
10.1	Added NMEA over UDP link. Updated NMEA RMC message to include speed over ground. Corrected LDAPs description. Added Authentication user permissions. Error corrections.	February 2023
11	Added new PTP page information. Updated product images and back panel Web UI images. Switched to Safran Trusted 4D branding.	November 2023
12	Updated all Web UI images to reflect new design; added , AGNSS feature, and PTP graphs.	March 2024
12.1	Added new NTP symmetic key types, added speedget and speedset commands, edited location of files uploaded via the Web UI.	May 2024

Rev	Description	Date
13	Added new information about FIPS compliance and new Security Dashboard page. Added new NMEA messages. Added information on 1204-58 to the WROX option card page. Edited CLI commands page for clarity and accuracy. Added information about new product feedback button in Web UI.	October 2024
13.1	Added information on effects of enabling OpenSSL Enhanced Security Core Mode.	October 2024
14	Added information about NTP Anycast and Anycast via Expert Mode. Added information about new Web UI SNMP MIB file download button, HTTPS certificate request requirements, and BroadShield installation. Corrected minor errors.	January 2025
15	Document maintenance, minor error corrections.	May 2025
15.1	Added information on new PTP Master Settings panel, corrected specifications, and other minor fixes.	August 2025
16	Added information on new DNNSEC configuration feature, configurable FIPS compliance settings, reboot after sanitization feature, and TOD1D ASCII data message format. Updated I/O pin configuration page with new unit models. Other minor fixes.	November 2025
16.1	Minor fixes.	November 2025

INDEX

O

P

R

S

T

U

V

W

Y