ELECTRONICS & DEFENSE

SecureSync

2400 MODEL



User Manual

Document Part No.: 2400-5000-0050

Revision: 11.1

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 1

1.1 Getting Started 2

1.2 SecureSync Introduction 2

1.2.1 SecureSync's Inputs and Outputs 3

1.3 SecureSync Front Panel 3

1.3.1 Status LEDs 4

1.3.1.1 Blinking Intervals 5

1.3.1.2 LED Lighting Patterns 5

1.3.1.3 Legend, individual LEDs 5

1.3.2 Front Panel Keypad, and Display 6

1.3.2.1 Using the Keypad 7

1.3.2.2 Using the Front Panel Display 7

1.4 Unit Rear Panel 13

1.5 Option Cards 15

1.5.1 Option Cards Overview 17

1.5.2 Option Card Identification 21

1.5.2.1 Option Card Identification by ID/Part Number 21

1.5.3 Option Card Connectors 24

1.6 Specifications 25

1.6.1 Input Power 25

1.6.2 GNSS Receiver 25

1.6.3 10 MHz Output 26

1.6.3.1 10 MHz Output — Oscillator Phase Noise (dBc/Hz) 27

1.6.4 Multi I/O 28

1.6.5 DCLS Output 30

1.6.5.1 1PPS Output 30

1.6.6 10/100/1000 Ethernet Port (RJ45) 31

1.6.7 10/100/1000 Ethernet Port (SFP) 31

1.6.8 RS-232 Serial Port (Rear Panel) 32

1.6.9 USB Serial Port (Front Panel) 32

1.6.10 Cables 32
1.6.11 Protocols Supported 33
1.6.12 Mechanical and Environmental Specifications 34
1.7 The SecureSync Web UI 35
1.7.1 The Web UI HOME Screen 36
1.7.2 The INTERFACES Menu 37
1.7.3 The Configuration MANAGEMENT Menu 38
1.7.4 The TOOLS Menu 38
1.8 Regulatory Compliance 39

CHAPTER 2
SETUP 41
2.1 Installation Overview 42
2.1.1 Main Installation Steps 42
2.2 Unpacking and Inventory 43
2.3 Required Tools and Parts 44
2.3.1 Required GNSS Antenna Components 44
2.4 SAFETY 45
2.5 Mounting the Unit 48
2.5.1 Rack Mounting (Ears) 49
2.6 Connecting the GNSS Input 50
2.7 Connecting Network Cables 51
2.8 Connecting Inputs and Outputs 52
2.9 Connecting Supply Power 52
2.9.1 Using AC Input Power 53
2.9.2 Using DC Input Power 53
2.9.3 Hot Swap Power Supply 56
2.9.3.1 Hot Swap Installation 57
2.9.3.2 Hot Swap Monitoring 57
2.10 Powering Up the Unit 61
2.11 Zero Configuration Setup 62
2.11.1 Using Zeroconf 63
2.12 Setting up an IP Address 63
2.12.1 Dynamic vs. Static IP Address 65

2.12.2 Assigning a Static IP Address 65
2.12.2.1 Setting Up an IP Address via the Front Panel 66
2.12.2.2 Setting Up a Static IP Address via a DHCP Network 68
2.12.2.3 Setting Up an IP Address via the Serial Port 69
2.12.2.4 Setting up a Static IP Address via Ethernet Cable 70
2.12.3 Subnet Mask Values 70
2.13 Accessing the Web UI 71
2.14 Configure Network Settings 73
2.14.1 HSTS Setup 74
2.14.2 General Network Settings 75
2.14.3 Network Ports 75
2.14.4 Network Services 77
2.14.5 Static Routes 78
2.14.6 Access Rules 79
2.14.7 HTTPS 80
2.14.7.1 Accessing the HTTPS Setup Window 80
2.14.7.2 About HTTPS 81
2.14.7.3 Supported Certificate Formats 82
2.14.7.4 Creating an HTTPS Certificate Request 83
2.14.7.5 Adding HTTPS Subject Alternative Names 86
2.14.7.6 Requesting an HTTPS Certificate 87
2.14.7.7 Uploading an X.509 PEM Certificate Text 89
2.14.7.8 Uploading an HTTPS Certificate File 90
2.14.8 SSH 91
2.14.9 SNMP 99
2.14.9.1 SNMP V1/V2c 104
2.14.9.2 SNMP V3 106
2.14.9.3 SNMP Traps 107
2.14.10 VLAN Support 110
2.14.11 System Time Message 110
2.14.11.1 System Time Message Format 111
2.14.12 DNSSEC 112
2.15 Configure NTP 113
2.15.1 Checklist NTP Configuration 114
2.15.2 The NTP Setup Screen 114
2.15.3 Dis-/Enabling NTP 117

2.15.4 Viewing NTP Clients 117
2.15.5 Restoring the Default NTP Configuration 118
2.15.6 NTP Output Timescale 119
2.15.7 NTP Reference Configuration 120
2.15.7.1 The NTP Stratum Model 121
2.15.7.2 Configuring "NTP Stratum 1" Operation 121
2.15.7.3 Configuring "NTP Stratum Synchronization" 122
2.15.8 NTP Servers and Peers 123
2.15.8.1 The NTP Servers and NTP Peers Panels 124
2.15.8.2 NTP Servers: Adding, Configuring, Removing 125
2.15.8.3 NTP Peers: Adding, Configuring, Removing 128
2.15.9 NTP Authentication 130
2.15.9.1 NTP Autokey 130
2.15.9.2 NTP: Symmetric Keys (MD5) 136
2.15.10 NTP Access Restrictions 139
2.15.11 Enabling/Disabling NTP Broadcasting 140
2.15.12 NTP over Anycast 141
2.15.12.1 Configuring NTP over Anycast (General Settings) 142
2.15.12.2 Configuring NTP over Anycast (OSPF IPv4) 143
2.15.12.3 Configuring NTP over Anycast (OSPF IPv6) 144
2.15.12.4 Configuring NTP over Anycast (BGP) 145
2.15.12.5 Configuring Anycast via NTP Expert Mode 147
2.15.12.6 Testing NTP over Anycast 151
2.15.13 Host Disciplining 151
2.15.14 NTP Expert Mode 151
2.15.15 Safran Technical Support for NTP 154
2.16 Configuring PTP 155
2.16.1 The PTP Screen 156
2.16.1.1 The PTP Masters Overview Panel 156
2.16.1.2 The PTP Slaves Overview Panel 158
2.16.1.3 The Edit PTP Settings Panel 160
2.16.1.4 The PTP Datasets Panel 163
2.16.1.5 The PTP Statistics Panel 163
2.16.1.6 The PTP TCP Dump Collection Panel 165
2.16.1.7 The PTP Master Settings Panel 166
2.16.2 Configure a New PTP Master or PTP Slave 167
2.16.3 Enable/Disable PTP 167
2.16.4 PTP Monitoring 167

2.16.5 General Configuration Notes 169
2.17 GPSD Setup 170
2.18 Configurable Connectors 171
2.18.1 BNC DCLS OUT 171
2.18.2 DB15 Multi I/O 172
2.18.3 Assigning Signals 174
2.18.4 Network Ports 176
2.19 Configuring Input References 176
2.19.1 How to Configure an Input Reference 176
2.19.2 Configure a 1PPS Input 178
2.19.3 Configure an ASCII Input 178
2.19.4 Configure a HaveQuick Input 181
2.19.5 Configuring an IRIG Input 182
2.20 Configuring Outputs 184
2.20.1 How to Configure an Output 184
2.20.2 Configuring a 1PPS Output 185
2.20.3 Configuring the 10 MHz Output 186
2.20.4 Configure an ASCII Output 186
2.20.5 Configuring a GPIO Output 189
2.20.6 Configuring a HaveQuick Output 190
2.20.7 Configuring an IRIG Output 192
2.20.8 The Outputs Screen 195
2.20.9 The 1PPS and 10 MHz Outputs 195
2.21 The Option Cards Screen 196
2.22 Signature Control 198

CHAPTER 3
Managing Time 201
3.1 The Time Management Screen 202
3.2 System Time 203
3.2.1 System Time 204
3.2.1.1 Configuring the System Time 204
3.2.1.2 Timescales 205
3.2.1.3 Manually Setting the Time 207
3.2.1.4 Using Battery Backed Time on Startup 209

3.2.2 Timescale Offset(s) 211
3.2.2.1 Configuring a Timescale Offset 211
3.2.3 Leap Seconds 211
3.2.3.1 Reasons for a Leap Second Correction 211
3.2.3.2 Leap Second Alert Notification 212
3.2.3.3 Leap Second Correction Sequence 213
3.2.3.4 Configuring a Leap Second 213
3.2.4 Local Clock(s), DST 214
3.2.4.1 Adding a Local Clock 214
3.2.4.2 DST Examples 216
3.2.4.3 DST and UTC, GMT 217
3.3 Managing References 217
3.3.1 Input Reference Priorities 217
3.3.1.1 Configuring Input Reference Priorities 219
3.3.1.2 The "Local System" Reference 223
3.3.1.3 The "User/User" Reference 224
3.3.1.4 Reference Priorities: EXAMPLES 225
3.3.2 Reference Qualification and Validation 229
3.3.2.1 Reference Monitoring: Phase 229
3.3.2.2 BroadShield 231
3.3.3 The GNSS Reference 239
3.3.3.1 Reviewing the GNSS Reference Status 241
3.3.3.2 Determining Your GNSS Receiver Model 245
3.3.3.3 Selecting a GNSS Receiver Mode 247
3.3.3.4 Setting GNSS Receiver Dynamics 250
3.3.3.5 Performing a GNSS Receiver Survey 252
3.3.3.6 GNSS Receiver Offset 252
3.3.3.7 Resetting the GNSS Receiver 254
3.3.3.8 Deleting the GNSS Receiver Position 255
3.3.3.9 Manually Setting the GNSS Position 256
3.3.3.10 GNSS Constellations 259
3.3.3.11 AGNSS 261
3.4 Holdover Mode 265
3.5 Managing the Oscillator 269
3.5.1 Oscillator Types 269
3.5.2 Configuring the Oscillator 271
3.5.2.1 Time Figure of Merit (TFOM) 272
3.5.3 Monitoring the Oscillator 273

3.5.4 Oscillator Logs 276

CHAPTER 4

System Administration 277

4.1 Powering Up/Shutting Down 278

4.1.1 Powering Up the Unit 278

4.1.2 Shutting Down the Unit 278

4.1.3 Issuing the HALT Command Before Removing Power 279

4.1.4 Rebooting the System 280

4.2 Notifications 281

4.2.1 Configuring Notifications 282

4.2.2 Notification Event Types 284

4.2.2.1 Timing Tab: Events 284

4.2.2.2 GPS Tab: Events 284

4.2.2.3 System Tab: Events 285

4.2.3 Configuring GPS Notification Alarm Thresholds 285

4.2.4 Setting Up SNMP Notifications 287

4.2.5 Setting Up Email Notifications 287

4.3 Managing Users and Security 290

4.3.1 Managing User Accounts 290

4.3.1.1 Types of Accounts 290

4.3.1.2 About "user" Account Permissions 290

4.3.1.3 Rules for Usernames 292

4.3.1.4 Adding/Deleting/Changing User Accounts 292

4.3.2 Managing Passwords 294

4.3.2.1 Configuring Password Policies 295

4.3.2.2 The Administrator Password 295

4.3.2.3 Lost Password 296

4.3.3 Web UI Timeout 298

4.3.4 LDAP Authentication 299

4.3.5 RADIUS Authentication 306

4.3.5.1 Enabling/Disabling RADIUS 306

4.3.5.2 Adding/Removing a RADIUS Server 307

4.3.6 TACACS+ Authentication 310

4.3.6.1 Enabling/Disabling TACACS+ 310

4.3.6.2 Adding/Removing a TACACS+ Server 311

4.3.7 Web UI Security Dashboard 312
4.3.7.1 Security Issues 312
4.3.7.2 FIPS 140-2 312
4.3.8 HTTPS Security Levels 316
4.4 Miscellanous Typical Configuration Tasks 317
4.4.1 REST API Configuration 317
4.4.2 Configuring the Front Panel 318
4.4.2.1 To change the time display on the front panel: 318
4.4.2.2 To lock or unlock the front panel: 318
4.4.3 12 or 24 Hour Time 319
4.4.3.1 Set 12- or 24-hour time: 319
4.4.3.2 Viewing 12-Hour or 24-Hour Time 319
4.4.4 Creating a Login Banner 319
4.4.5 Show Clock 321
4.4.6 Product Registration 321
4.4.7 Synchronizing Network PCs 322
4.5 Quality Management 322
4.5.1 System Monitoring 322
4.5.1.1 Status Monitoring via Front Panel 322
4.5.1.2 Status Monitoring via the Web UI 323
4.5.1.3 Status Monitoring of Input References 327
4.5.1.4 Reference Monitoring: Phase 328
4.5.1.5 Ethernet Monitoring 330
4.5.1.6 Outputs Status Monitoring 331
4.5.1.7 Monitoring the Oscillator 335
4.5.1.8 Monitoring the Status of Option Cards 338
4.5.1.9 NTP Status Monitoring 339
4.5.1.10 Temperature Management 345
4.5.2 Logs 348
4.5.2.1 Types of Logs 349
4.5.2.2 The Logs Screen 353
4.5.2.3 Displaying Individual Logs 355
4.5.2.4 Saving and Downloading Logs 355
4.5.2.5 Setting up a Remote Log Server 357
4.5.2.6 Clearing All Logs 358
4.6 Updates and Licenses 359
4.6.1 Software Updates 359
4.6.2 Applying a License File 361

4.7 Backing-up and Restoring Configuration Files 362
4.7.1 Accessing the System Configuration Screen 362
4.7.2 Saving the System Configuration Files 364
4.7.3 Uploading Configuration Files 365
4.7.4 Restoring the System Configuration 366
4.7.5 Restoring the Factory Defaults 366
4.7.6 Resetting the Unit to Factory Configuration 367
4.7.6.1 Resetting All Configurations to their Factory Defaults 367
4.7.7 Default and Recommended Configurations 368
4.7.8 Sanitizing the Unit 369
4.7.8.1 Sanitizing Process 370
4.7.8.2 Further Reading 371

APPENDIX

Appendix 373
5.1 Troubleshooting 374
5.1.1 Minor and Major Alarms 374
5.1.2 Troubleshooting: System Configuration 375
5.1.2.1 System Troubleshooting: Browser Support 376
5.1.3 Troubleshooting – Unable to Open Web UI 376
5.1.4 Troubleshooting via Web UI Status Page 376
5.1.5 Troubleshooting GNSS Reception 379
5.1.6 Troubleshooting – Outputs 379
5.1.7 Troubleshooting the Serial Port 380
5.1.8 Troubleshooting the Cooling Fan(s) 381
5.1.9 Troubleshooting – Network PCs Cannot Sync 382
5.1.10 Troubleshooting Software Update 383
5.2 Option Cards 383
5.2.1 Accessing Option Cards Settings via the Web UI 384
5.2.1.1 Web UI Navigation: Option Cards 384
5.2.1.2 Viewing Input/Output Configuration Settings 385
5.2.1.3 Configuring Option Card Inputs/Outputs 386
5.2.1.4 Viewing an Input/Output Signal State 387
5.2.1.5 Verifying the Validity of an Input Signal 388
5.2.2 Option Card Field Installation Instructions 390
5.2.2.1 Field Installation: Introduction 390

5.2.2.2 Outline of the Installation Procedure 390
5.2.2.3 Safety 391
5.2.2.4 [1]: Unpacking 391
5.2.2.5 [2]: Saving Reference Priority Configuration 392
5.2.2.6 [3]: Determining the Installation Procedure 393
5.2.2.7 [4]: Slot 1 & 2 Installation 396
5.2.2.8 [5]: Bottom Slot Installation 398
5.2.2.9 [6]: Top Slot Installation, Bottom Slot Empty 399
5.2.2.10 [7]: Top Slot Installation, Bottom Slot Occupied 401
5.2.2.11 [8]: WROX Card Installation 403
5.2.2.12 [9]: Frequency Output Cards: Wiring 405
5.2.2.13 [10]: Alarm Relay Card, Cable Installation 406
5.2.2.14 [11]: NENA Card, Cable Installation 407
5.2.2.15 [12]: Verifying HW Detection and SW Update 408
5.2.2.16 [13]: Restoring Reference Priority Configuration 409
5.2.3 Time and Frequency Option Cards 410
5.2.3.1 1PPS Out [1204-18, -19, -21, -2B] 410
5.2.3.2 1PPS In/Out [1204-28, -2A] 415
5.2.3.3 1PPS In/Out, 10 MHz In [1204-01, -03] 420
5.2.3.4 Frequency Out [1204-08, -1C, -26] 427
5.2.3.5 Programmable Frequency Out [1204-13, -2F, -30] 430
5.2.3.6 Programmable Square Wave Out [1204-17] 435
5.2.3.7 Simulcast (CTCSS/Data Clock) [1204-14] 438
5.2.4 Telecom Option Cards 447
5.2.4.1 T1/E1 Out [1204-09, -0A, -4C, -53] 447
5.2.5 Time Code Option Cards 454
5.2.5.1 IRIG Out [1204-15, -1E, -22] 455
5.2.5.2 IRIG In/Out [1204-05, -27] 461
5.2.5.3 STANAG Out [1204-11, -25] 476
5.2.5.4 STANAG In [1204-1D, -24] 484
5.2.5.5 HAVE QUICK Out [1204-10, -1B] 491
5.2.5.6 HAVE QUICK In/Out [1204-29] 497
5.2.5.7 ASCII Time Code In/Out [1204-02, -04] 503
5.2.6 Network Interface Option Cards 514
5.2.6.1 NTP and Networking [4A, 49] 515
5.2.6.2 White Rabbit Option Cards (WROX) [1204-58, -59] 519
5.2.6.3 PTP Grandmaster [1204-32] 534
5.2.7 Miscellaneous Option Cards 551
5.2.7.1 STL Option Module [1204-3E] 552

5.2.7.2 Alarm Relay Out [1204-0F] 560
5.2.7.3 Revertive Selector Card [1204-2E] 565
5.2.7.4 Event Broadcast [1204-23] 567
5.2.7.5 NavIC [1204-5E and 1204-5F] 575
5.3 Command-Line Interface 575
5.3.1 Setting up a Terminal Emulator 575
5.3.2 CLI Commands 577
5.4 Time Code Data Formats 585
5.4.1 NMEA GGA Message 585
5.4.2 NMEA RMC Message 587
5.4.3 NMEA ZDA Message 587
5.4.4 NMEA VTG Message 588
5.4.5 NMEA GSV Message 589
5.4.6 NMEA GLL Message 591
5.4.7 NMEA GSA Message 592
5.4.8 Spectracom Format 0 593
5.4.9 Spectracom Format 1 595
5.4.10 Spectracom Format 1S 596
5.4.11 Spectracom Format 2 598
5.4.12 Spectracom Format 3 600
5.4.13 Spectracom Format 4 602
5.4.14 Spectracom Format 7 603
5.4.15 Spectracom Format 8 605
5.4.16 Spectracom Format 9 606
5.4.16.1 Format 9S 607
5.4.17 Spectracom Epsilon Formats 607
5.4.17.1 Spectracom Epsilon TOD 1 607
5.4.17.2 Spectracom Epsilon TOD 3 608
5.4.17.3 Spectracom Epsilon TOD D1 609
5.4.18 BBC Message Formats 611
5.4.18.1 Format BBC-01 611
5.4.18.2 Format BBC-02 611
5.4.18.3 Format BBC-03 PSTN 613
5.4.18.4 Format BBC-04 614
5.4.18.5 Format BBC-05 (NMEA RMC Message) 615
5.4.19 GSSIP Message Format 616

5.4.20 EndRun Formats 617
5.4.20.1 EndRun Time Format 617
5.4.20.2 EndRunX (Extended) Time Format 618
5.5 IRIG Standards and Specifications 619
5.5.1 About the IRIG Output Resolution 619
5.5.2 IRIG Carrier Frequencies 620
5.5.3 IRIG B Output 625
5.5.3.1 FAA IRIG B Code Description 628
5.5.4 IRIG E Output 632
5.5.5 IRIG Output Accuracy Specifications 636
5.6 Strain Relief Ancillary Kit 637
5.6.1 Product Description 638
5.6.2 Installation 638
5.6.2.1 Install rear-mounting brackets 639
5.6.2.2 Install the L-bracket 640
5.6.2.3 Install a grounding cable 641
5.6.2.4 Install the cross bar 643
5.7 Maintenance 644
5.8 Technical Support 645
5.8.1 Product Feedback 645
5.8.2 Regional Contact 645
5.9 Return Shipments 646
5.10 List of Tables 646
5.11 List of Images 648
5.12 Document Revision History 651

INDEX

CHAPTER 1

Product Description

The Chapter presents an overview of the SecureSync 2400 Time and Frequency Synchronization System, its capabilities, main technical features and specifications.

The following topics are included in this Chapter:

1.1 Getting Started 2
1.2 SecureSync Introduction 2
1.3 SecureSync Front Panel 3
1.4 Unit Rear Panel 13
1.5 Option Cards 15
1.6 Specifications 25
1.7 The SecureSync Web UI 35
1.8 Regulatory Compliance 39

1.1 Getting Started



Welcome to the SecureSync User Reference Guide.

Where to start:

- **First-time users**: "SecureSync Introduction" below.
- Users with **some knowledge** of Time and Frequency Servers: "Installation Overview" on page 42.
- If your unit is up and running and you want to **change a setting**: "Managing Time" on page 201, or "System Administration" on page 277.

1.2 SecureSync Introduction

SecureSync 2400 Time and Frequency Synchronization System® is the latest-version, security-hardened 1-rack unit network appliance designed to meet rigorous network security standards and best practices. It ensures accurate timing through multiple references, tamper-proof management, and extensive logging. Robust network protocols are used to allow for easy but secure configuration. Features can be enabled or disabled based on your network policies. Installation is aided by DHCP (IPv4), AUTOCONF (IPv6), and a front-panel keypad and OLED display.

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

SecureSync combines Safran's precision master clock technology and secure network-centric approach with a compact modular hardware design to bring you a

powerful time and frequency reference system at the lowest cost of ownership. Military and commercial applications alike will benefit from its extreme reliability, security, and flexibility for synchronizing critical operations.

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

You can choose from a variety of configurable option cards, each with an assortment of input/output timing signal types and quantity, including additional 1PPS, 10 MHz, timecode (IRIG, ASCII, HAVE QUICK), other frequencies (5MHz, 2.048 MHz, 1.544 MHz, 1MHz), Precision Timing Protocol (PTP) input/output, multi-Gigabit Ethernet (10/100/1000Base-T), telecom T1/E1 data rates and multi-network NTP, allowing SecureSync to be customized for your exact requirements.

A variety of internal oscillators is available, depending on your requirements for holdover capability and phase noise.

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

1.2.1 SecureSync's Inputs and Outputs

SecureSync provides multiple outputs for use in networked devices and other synchronized devices. A 10 MHz frequency reference provides a precise, disciplined signal for control systems and transmitters. A 1-Pulse-Per-Second (1PPS) output acts as a precise metronome, counting off seconds of System Time in the selected timescale (such as UTC, TAI or GPS); this BNC connector can also be configured to produce IRIG, HaveQuick, or GPO signals. A multi-I/O 15 pin connector provides default IRIG, ATC, and HaveQuick Inputs, as well as IRIG, IRIG AM, HaveQuick, and ATC Outputs. These options can all be configured to suit your application (see "Configurable Connectors" on page 171).

SecureSync's outputs are driven by its inputs – most notably, Global Navigation Satellite System (GNSS), or IRIG signal generators and other available input references. GNSS-equipped SecureSyncs can track up to 72 GNSS satellites simultaneously and synchronize to the satellite's atomic clocks. This enables SecureSync-equipped computer networks to synchronize anywhere on the planet.

1.3 SecureSync Front Panel

The front panel of a SecureSync unit consists of:

- an LED **time display**
- seven illuminated status LED **menu buttons**
- a front panel control **keypad**
- an OLED **information display** menu
- micro-B USB **serial console**
- intake for temperature-controlled cooling **fans**

The OLED information display is configurable using the front panel controls. The micro USB serial interface and the front panel controls provide a means to configure the unit's network settings and perform other functions without requiring access to the Web UI.

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

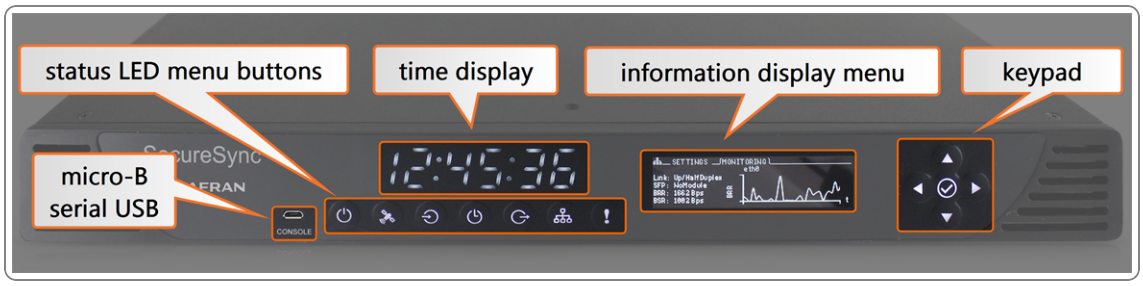


Figure 1-1: SecureSync front panel layout

1.3.1 Status LEDs

SecureSync's front panel status LEDs provide a real-time status overview: Seven (7) LEDs indicate the unit's current operating state.

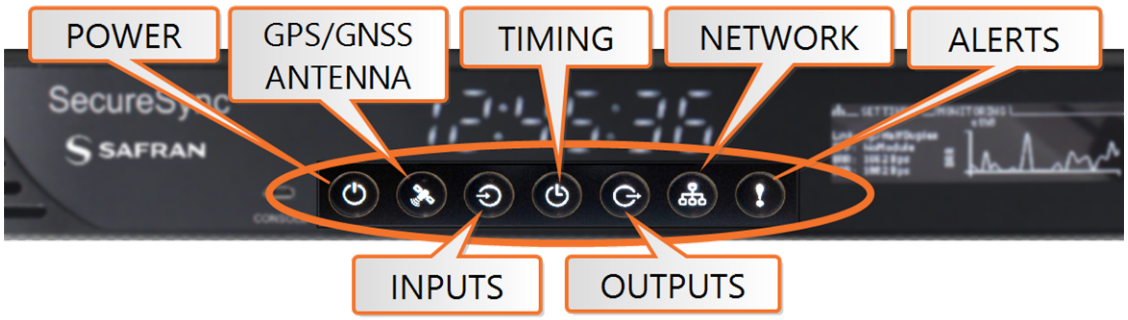


Figure 1-2: Front panel LEDs

1.3.1.1 Blinking Intervals

The status LEDs can communicate four different operating states:

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

1.3.1.2 LED Lighting Patterns

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

Table 1-1: Common light patterns

							
Start-up	ON	OFF	OFF	OFF	OFF	OFF	OFF
Software upgrade/re-boot	HEARTBEAT PATTERN IN ORDER, BECOMING SOLID LEFT TO RIGHT TO REPRESENT PROGRESS						

1.3.1.3 Legend, individual LEDs

Table 1-2: Legend for Status LEDs

Icon	Light	Meaning
	OFF	No power
	ON	Powered
	OFF	No GNSS reception (0 satellites)
	HEARTBEAT	GNSS acquisition in process (≥1 satellite(s), or 1PPS OK, or Time OK
	FAST	Antenna short circuit
	ON	GNSS is available as reference (1PPS and Time OK)

Icon	Light	Meaning
	OFF	No valid references
	FAST	Using non-primary reference
	ON	Using primary reference
	OFF	Unit is in Holdover (valid)
	ON	In Sync (valid)
	FAST	Not In Sync (Holdover period exceeded, or oscillator damaged)
	OFF	No output signal(s) detected/all outputs are disabled
	ON	At least one enabled output
	OFF	Both ETH0 and ETH1 invalid
	ON	At least one Ethernet connection valid
	OFF	Unit OK
	FAST	At least one active alarm, see Web UI

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.

Responding to Alarms

If you are in front of your units, the fastest way to determine the origin of alarms is to press the button that is flashing; this will automatically bring up the menu of the category with a difficulty. See "Front Panel Keypad, and Display" below for more information.

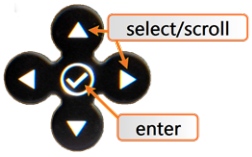
1.3.2 Front Panel Keypad, and Display

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

The front panel keypad, information display menu, and status LED menu buttons can be used to configure basic network settings and obtain status information. For more complex functionality, users should refer to the Web UI or Command Line Interface (CLI).

For instruction on changing the front panel time display or locking front panel access, see "Configuring the Front Panel" on page 318.

1.3.2.1 Using the Keypad



The functions of the five keys are:

- ◀▶▲ ▼ **arrow keys**: Navigate to a menu option (will be highlighted); move the focus on the screen; switch between submenus
- ▲ ▼ **arrow keys**: Scroll through parameter values in edit displays; move the focus on the screen
- ✓ **ENTER** key: Select a menu option, or confirm a selection when editing
- **menu buttons**: Press these buttons to navigate to each of the seven main menus.

1.3.2.2 Using the Front Panel Display

There are seven main menu screens on the SecureSync front information display.

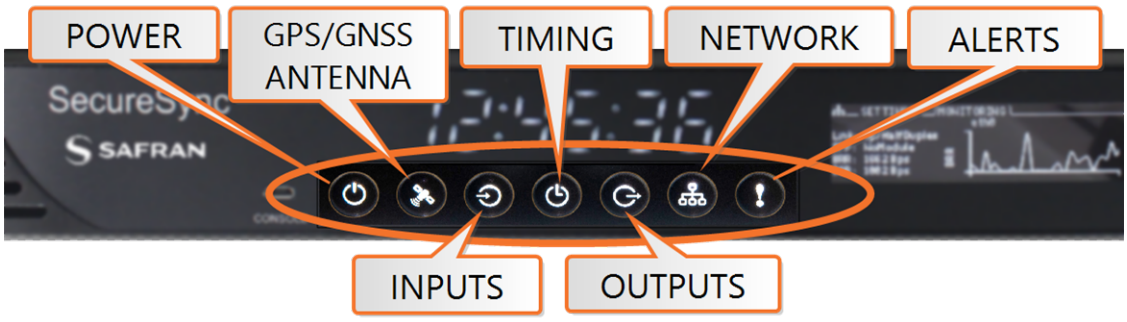


Figure 1-3: Status LED menu buttons

1. Your front panel screen will timeout and darken after two minutes of inactivity. If your screen is dark, press any menu or keypad button to wake.
2. Press a menu button to enter that menu on the front panel display.
3. After entering a menu, the cursor will automatically begin on the submenu selection that you last visited.
4. Use the left and right buttons to switch between submenus if necessary.

5. To enter into a submenu body, press the down button. You will only be able to highlight fields that can be changed.
6. If the field has arrows on either side of your selection, use the directional arrow keys; OR:
7. If the line is highlighted, press the ENTER button to change a value, and use the directional keys to obtain the desired setting.
8. Once your editing is done, press the ENTER button.
9. Press ENTER again to confirm your choice in the confirmation menu that will appear on the right side of the screen.

Front Panel Display: Menu Tree

The illustration below shows how the menu is organized, and which functions can be accessed via the front panel (i.e. without using the Web UI):

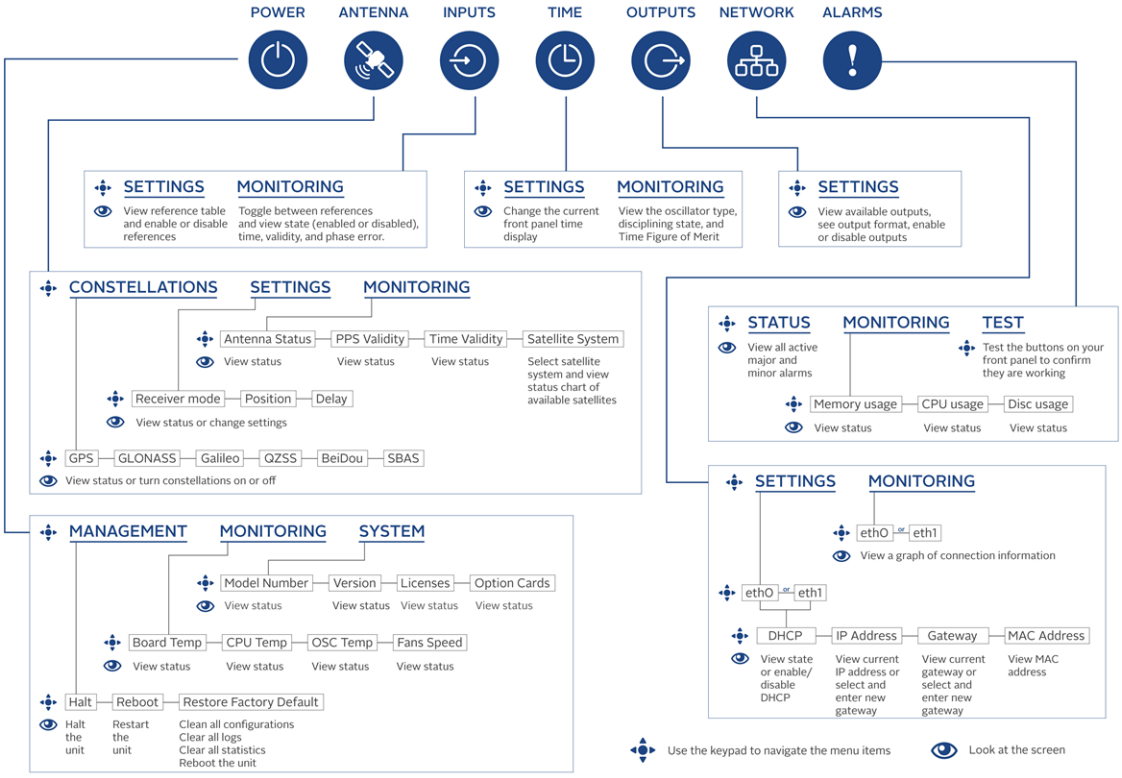


Figure 1-4: Front panel menu tree

The main menu options and their functions are as follows:

Power Menu:

- Management



  - halt the unit (see "Issuing the HALT Command Before Removing Power" on page 279)
  - reboot the unit (see "Rebooting the System" on page 280)
  - restore the factory defaults (see "Resetting the Unit to Factory Configuration" on page 367)
- Monitoring



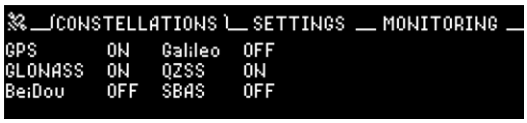
  - view the temperature status: Board Temp, CPU Temp, and OSC (oscillator) Temp
  - view the Fan(s) Speed
- System



  - view model number
  - view serial number
  - view software version
  - view licenses
  - view a rolling ribbon of option cards installed
- Hot Swap
  - this sub menu will only be available if you have a Hot Swap Power Supply configuration. See "Hot Swap Power Supply" on page 56 for more information.

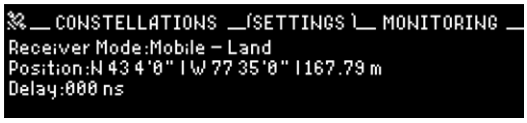
GNSS Antenna Menu:

- Constellations



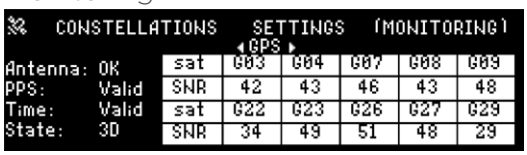
  - view the status for GPS, GLONASS, BeiDou, Galileo, QNSS, and SBAS
  - turn reception OFF or ON to any satellite system by selecting the status

- Settings



  - view or change receiver position mode
  - view or set position
  - view or change delay

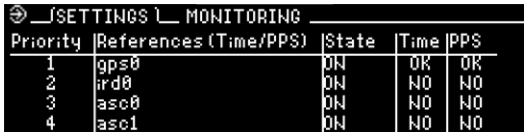
- Monitoring



  - view the following information:
    - antenna status
    - PPS validity
    - time validity
    - state
  - view for each satellite system:
    - chart of all visible satellites

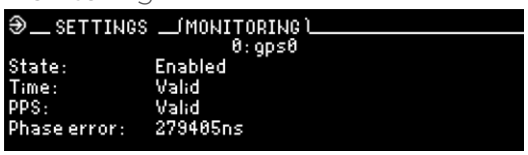
Inputs Menu:

- Settings



- view reference table
- enable or disable references (see "Configuring Input Reference Priorities" on page 219

- Monitoring



- view each input reference
- view reference state, time, validity, and phase error

Time Menu:

- Settings:



change the current time display

- Monitoring:



view the oscillator type, disciplining state, and TFOM value

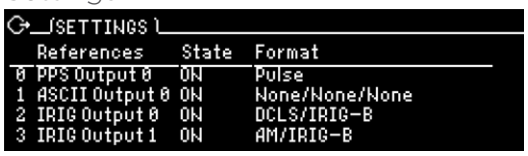
- Date:



view the Day Month Year.

Outputs Menu:

- Settings



- view list of outputs available
- see outputs format
- enable or disable outputs (see "Signature Control" on page 198)

Network Menu:

- Settings: Scroll to each ETH connection to view information or perform actions (see "Setting Up an IP Address via the Front Panel" on page 66):



  - enable or disable DHCP
  - view or set IP address
  - view or change gateway
  - view MAC address
- Monitoring: View a graph for each ETH connection (highlight eth0 or eth1 and toggle left and right)

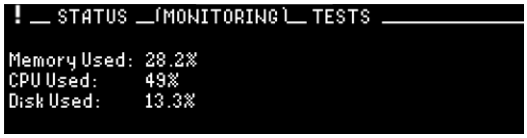


Alerts Menu:

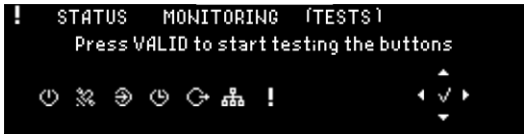
- Status



  - show current major or minor alarms and descriptions
- Monitoring



  - monitor memory usage
  - monitor CPU usage
  - monitor disk usage
- Test



» confirm that the buttons on your front panel are working (highlight **Press VALID to start testing buttons** and push the ✓ **ENTER** key).

1.4 Unit Rear Panel



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

- » GPS/GNSS **antenna connector** (SMA)
- » **10 MHz output** (BNC female connector)
- » **Multi I/O** (sub HD15 connector)
- » **1PPS out**, configurable DCLS Output (BNC female connector)
- » **ETH0** 1GB Ethernet (RJ45 connector)
- » **ETH1** Ethernet (SFP connector)
- » **Serial console** (RJ45 connector)
- » Two or six slots for **option cards**
- » **AC power** input connection

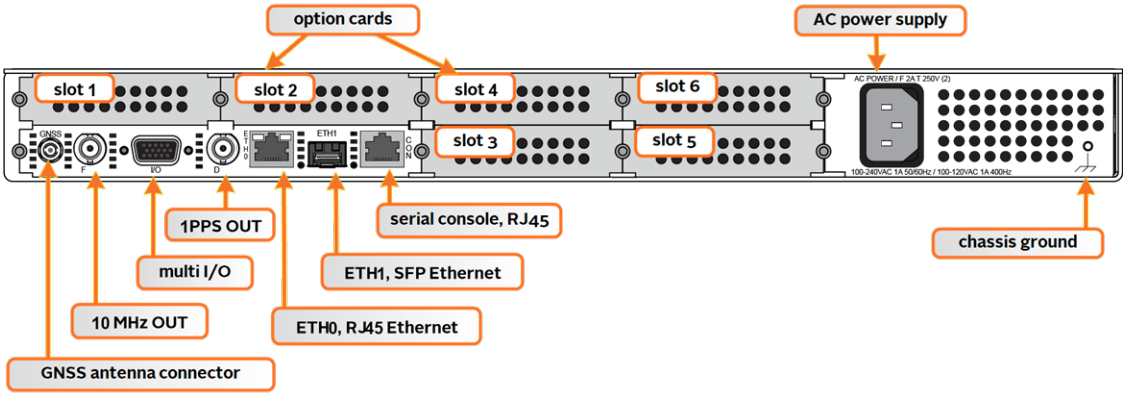


Figure 1-5: Standard rear panel

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

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

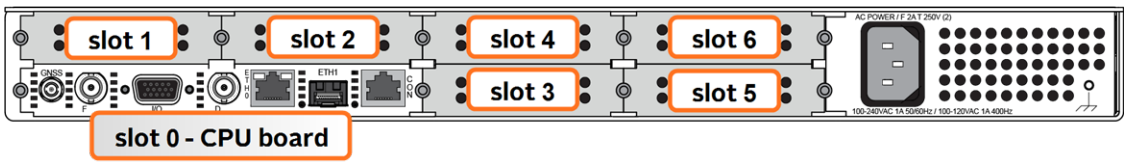
Table 1-3: Ethernet status indicator lights

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

- The rear **Serial Console** accepts commands to locally configure the unit via CLI.
- The **AC Power** connector is the input for the AC power (does not include an ON/OFF switch).
- The chassis ground on the rear panel is a supplementary ground. SecureSync is grounded through the power connector.

Typically, **option cards** will be installed at the factory. Should you purchase an extra option card at a later point, you will need to undergo field installation (for technically proficient service personnel only). Your local Sales Office will gladly assist you with the optimal option cards selection for your application.

1.5 Option Cards



Option Cards are circuit boards that can be installed into a SecureSync unit in order to **add input and output functionality**. Installation is normally done in the factory when the unit is built. Many cards, however, can be retrofitted in the field by qualified customer personnel (see "Option Card Field Installation Instructions" on page 390).

SecureSync has the capacity to hold either two or six option cards, depending on whether or not an **extension board** is installed in your unit. If you are not sure whether or not you have an extension board, identify the part number of your unit:

- In the Web UI, navigate to **TOOLS** > **Upgrade/Backup**. In the System Configuration panel, your product number is listed under Model. OR;
- On the front panel display, press the POWER button, and navigate over to the System submenu. Your part number is listed under Model Number.

If your product number begins with the numbers 2402, then your unit does not contain an extension board and has a two-option card capacity. If your product number begins with the numbers 2406, then your unit contains an extension board, and can house up to six option cards. For more information, contact your Safran sales personnel.

Caution: NEVER install an option card from the back of the unit, ALWAYS from the top. It is therefore necessary to remove the top cover of the main chassis (housing).

Input and outputs can be categorized by:

- **Communication direction**:
  - Input
  - Output
- **Signal type**:
  - Frequency: 1/5/10/[programmable] MHz
  - Wave form (square, sinus)

    - 1PPS
    - TTS
    - CTCSS
- **Signal protocol**:
    - ASCII time code
    - IRIG
    - STANAG
    - Have Quick
    - E1/T1 data
    - Telecom timing, etc.
    - Ethernet (NTP, PTP)
    - Time code I/O
    - Alarm out, etc.
- **Functionality**:
    - Networking card (incl. NTP, PTP)
    - Time code I/O
    - Alarm output
    - Special functionality e.g., revertive selector, bidirectional communication
- **Connector type**:
    - BNC
    - DB-9/25
    - Terminal block
    - RJ-12/45
    - SFP
    - ST fiber optic

To **visually identify** an option card installed in your unit, or to **obtain an overview** which option cards are available for SecureSync, see "Option Cards Overview" on the facing page.

To obtain **detailed information** on a specific option card, using its ID number, see "Option Card Identification" on page 21.

To locate **option card topics** in this manual by their heading or functionality, see "Option Cards" on page 383. This Chapter also includes information on **field installation** and Web UI functionality.

To visually **identify a connector** type, see "Option Card Connectors" on page 24.

1.5.1 Option Cards Overview

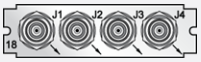
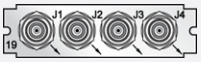
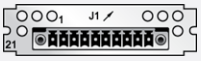
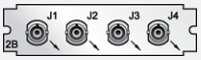
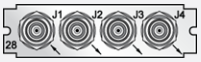
The table below lists all SecureSync option cards available at the time of publication of this document, **sorted by their function**.

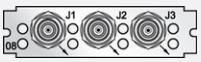
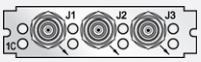
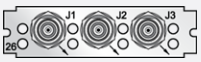
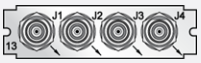
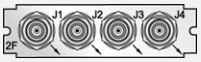
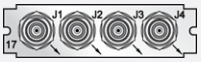
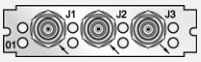
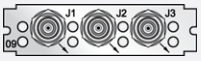
The table column (see table below) **Web UI Name** refers to the names under which the cards installed in a SecureSync unit are listed in the **INTERFACES > OPTION CARDS** drop-down menu.

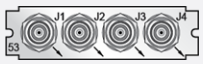
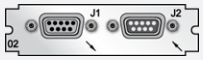
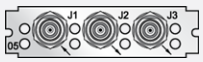
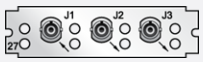
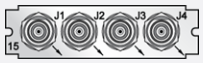
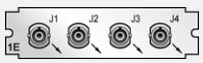
Detailed specifications and configuration assistance for every card can be found in the APPENDIX. To quickly access the APPENDIX topic for your option card(s), you may use the hyperlinks in table "Option cards listed by their ID number" on page 21.

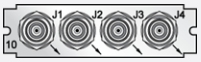
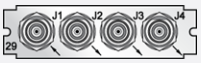
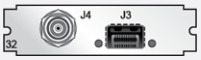
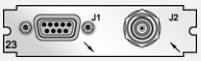
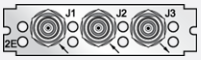
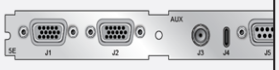
Note: * Every option card has a unique 2-digit ID number located on its cover plate, and in the center column of the table below. The complete Safran Part Number for option cards is 1204-xx (e.g., 1204-18).

Table 1-4: Option cards identification

Function	Web UI Name	Illustration	ID*	Inputs	Outputs	Conn.'s
Time and Frequency Cards						
Quad 1PPS out (TTL)	1PPS Out BNC		18	0	1PPS, TTL (4x)	BNC (4x)
Quad 1PPS out (10 V)	1PPS Out 10V		19	0	1PPS, 10 V (4x)	BNC (4x)
Quad 1PPS out (RS-485)	1PPS Out, RS-485		21	0	1PPS, RS-485 (4x)	Terminal block, 10-pin
Quad 1PPS out (fiber optic)	1PPS Out, Fiber		2B	0	1PPS, F/O (4x)	ST Fiber optic (4x)
1in/3out 1PPS (TTL [BNC])	1PPS/Frequency RS-485		28	1PPS (1x)	1PPS (3x)	BNC (4x)
1in/2out 1PPS/freq (fiber optic)	1PPS In/Out, Fiber		2A	1PPS (1x)	1PPS (2)	ST Fiber optic (3x)

Function	Web UI Name	Illustration	ID*	Inputs	Outputs	Conn.'s
5MHz out	5MHz Out		08	0	5MHz (3x)	BNC (3x)
10 MHz out	10 MHz Out		1C	0	10 MHz (3x)	BNC (3x)
1MHz out	1MHz Out		26	0	1MHz (3x)	BNC (3x)
Progr. frequ. out (Sine Wave)	Prog Freq Out, Sine		13	0	progr. clock, sine (4x)	BNC (4x)
Progr. frequ out (TTL)	Prog Freq Out, TTL		2F	0	progr. clock, TTL/sq. (4x)	BNC (4x)
Prog frequ out (RS-485)	Prog Freq Out, RS-485		30	0	progr. clock, RS-485 (4x)	Ter-minal block, 10-pin
Square Wave out	Square Wave Out, BNC		17	0	square wave, TTL (4x)	BNC (4x)
1PPS in/out + frequ. in	1PPS/Fre-quency BNC		01	Var. frequ. + 1PPS	1PPS (TTL)	BNC (3x)
1PPS in/out + frequ. in	1PPS/Fre-quency RS-485		03	10 MHz + 1PPS	1PPS	Ter-minal block, 10-pin
CTCSS, Data Syn-c/Clock	Simulcast		14	0	data clock, CTCSS frequ., 1PPS, 1 alarm (3x)	RJ-12 & DB-9
Telecom Timing Cards						
E1/T1 data, 75 Ω	E1/T1 Out BNC		09	0	1.544/2.0-48 MHz (1x) unbal. E1/T1 (2x)	BNC (3x)
E1/T1 data, 100/120 Ω	E1/T1 Out Ter-minal		0A	0	1.544/2.0-48 MHz (1x) unbal. E1/T1 (2x)	Ter-minal block, 10-pin

Function	Web UI Name	Illustration	ID*	Inputs	Outputs	Conn.'s
E1/T1 data, 75 Ω	E1/T1 Out BNC		53	0	unbal. E1/T1 (4x)	BNC (4x)
E1/T1 data, 100/120 Ω	E1/T1 Out Ter-minal		4C	0	unbal. E1/T1 (4x)	Ter-minal block, 10-pin
Time Code Cards						
ASCII Time Code RS-232	ASCII Time-code RS-232		02	1	RS-232 (1x)	DB-9 (2x)
ASCII Time Code RS-485	ASCII Time-code RS-485		04	1	1	Ter-minal block, 10-pin
IRIG BNC	IRIG In/Out BNC		05	1	2	BNC (3x)
IRIG Fiber Optic	IRIG In/Out, Fiber		27	1	2	ST Fiber optic (3x)
IRIG out, BNC	IRIG Out BNC		15	0	4	BNC (4x)
IRIG out, fiber optic	IRIG Out, Fiber		1E	0	4	ST Fiber optic (4x)
IRIG out, RS-485	IRIG Out, RS-485		22	0	4	Ter-minal block, 10-pin
STANAG input	STANAG In		1D	2x	1x	DB-25 (1x)
STANAG in, isol.	STANAG In, Isolated		24	2x	1x	DB-25 (1x)
STANAG out	STANAG Out		11	0	2x STANAG, 1x 1PPS	DB-25 (1x)
STANAG out, isol.	STANAG Out, Isolated		25	0	2x STANAG, 1x 1PPS	DB-25 (1x)

Function	Web UI Name	Illustration	ID*	Inputs	Outputs	Conn.'s
HAVE QUICK out BNC	HAVE QUICK Out, BNC		10	0	4 (TTL)	BNC (4x)
HAVE QUICK out RS-485	HAVE QUICK Out, RS-485		1B	0	4	Ter-minal block, 10-pin
HAVE QUICK	HAVE QUICK		29	1	3	BNC (4x)
Networking Cards						
1Gb PTP: Master only	Gb PTP		32	0	1PPS (1x BNC), SFP (1x)	BNC (1x), SFP (1x)
Quad 1 Gb NTP Server	Quad 1 Gb		4A	0	4	SFP ports
Dual 1 Gb NTP Serv-er	Dual 1 Gb		49	0	2	SFP ports
Communication and Specialty Cards						
STL (Satel-lite Time and Loca-tion)	STL		3E	Satellite, Eth. (Main-tenance)	0	SMA, RJ45
Event in, Broadcast out	Event Broad-cast		23	BNC: Event trigger	DB-9: Event broadcast	DB-9 + BNC (1x each)
Revertive Selector ("Fail-over")	n/a		2E	Frequ. or 1 PPS: (2x)	Frequ. or 1PPS(1x)	BNC (3x)
Alarm Relay Out	Relay Output		0F	0	Relay Out (3x)	Ter-minal block, 10-pin
NavIC	Proprietary GNSS Receiv-er		5E	-	-	-
NavIC	Proprietary GNSS Receiv-er		5F	-	-	-

1.5.2 Option Card Identification

Here are a few ways to identify the option card(s) installed in your SecureSync unit:

a. Using the Web UI, navigate to the **INTERFACES > OPTION CARDS** drop-down menu, and compare the list displayed in your UI with the table "Option cards identification" on page 17.

b. If you have physical access to your SecureSync unit, inspect its rear panel, and compare the 2-digit **ID number** printed in the lower left-hand corner on each option card with the table below.

1.5.2.1 Option Card Identification by ID/Part Number

If you are looking for information specific to a particular option card, the table below can help you find this information in this User Manual.

Note: * Every option card has a 2-digit identification (ID) number that can be found in the corner of its cover plate, and in the table below. The ID number is comprised of the two center digits of your option card's Safran Part Number: 1204-0180-0600.

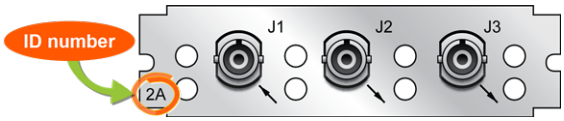


Figure 1-6: Option Card ID number

The table lists all option cards available at the publication date of this documentation, **sorted by their ID number**. Locate the option card **ID number** on its cover plate, and follow the corresponding hyperlink in the right-hand column.

Table 1-5: Option cards listed by their ID number

Card ID*	Card Name	Name in UI	See ...
01	1PPS/freq input (TTL levels) module	1PPS/Frequency BNC	"1PPS In/Out, 10 MHz In [1204-01, -03]" on page 420
02	ASCII Time Code module (RS-232)	ASCII Timecode RS-232	"ASCII Time Code In/Out [1204-02, -04]" on page 503
03	1PPS/freq input (RS-485 levels) module	1PPS/Frequency RS-485	"1PPS In/Out, 10 MHz In [1204-01, -03]" on page 420
04	ASCII Time Code module (RS-485)	ASCII Timecode RS-485	"ASCII Time Code In/Out [1204-02, -04]" on page 503

Card ID*	Card Name	Name in UI	See ...
05	IRIG module, BNC (1 input, 2 outputs)	IRIG In/Out BNC	"IRIG In/Out [1204-05, -27]" on page 461
08	5 MHz output module (3 outputs)	5 MHz Out	"Frequency Out [1204-08, -1C, -26]" on page 427
09	T1-1.544 (75 Ω) or E1-2.048 (75 Ω) module	E1/T1 Out BNC	"T1/E1 Out [1204-09, -0A, -4C, -53]" on page 447
0A	T1-1.544 (100 Ω) or E1-2.048 (120 Ω) module	E1/T1 Out Terminal	"T1/E1 Out [1204-09, -0A, -4C, -53]" on page 447
0F	Alarm module	Relay Output	"Alarm Relay Out [1204-0F]" on page 560
10	HaveQuick output module (TTL)	HAVE QUICK Out, BNC	"HAVE QUICK Out [1204-10, -1B]" on page 491
11	STANAG output module	STANAG Out	"STANAG Out [1204-11, -25]" on page 476
13	Programmable Frequency Output module (Sine Wave)	Prog Freq Out, Sine	"Programmable Frequency Out [1204-13, -2F, -30]" on page 430
14	CTCSS, Data Sync/Clock module ("Simulcast")	Simulcast	"Simulcast (CTCSS/Data Clock) [1204-14]" on page 438
15	IRIG module, BNC (4 outputs)	IRIG Out BNC	"IRIG Out [1204-15, -1E, -22]" on page 455
17	Square Wave (TTL) output module	Sq Wv Out, BNC	"Programmable Square Wave Out [1204-17]" on page 435
18	Quad 1 PPS output module (TTL)	1PPS Out BNC	"1PPS Out [1204-18, -19, -21, -2B]" on page 410
19	Quad 1 PPS output module (10 V)	1PPS Out 10V	"1PPS Out [1204-18, -19, -21, -2B]" on page 410
1B	HaveQuick output module (RS-485)	HAVE QUICK Out, RS-485	"HAVE QUICK Out [1204-10, -1B]" on page 491
1C	10 MHz output module (3 outputs)	10 MHz Out	"Frequency Out [1204-08, -1C, -26]" on page 427
1D	STANAG input module	STANAG In	"STANAG In [1204-1D, -24]" on page 484
1E	IRIG module, Fiber Optic (4 outputs)	IRIG Out, Fiber	"IRIG Out [1204-15, -1E, -22]" on page 455
21	Quad 1 PPS output module (RS-485 [terminal block])	1PPS Out, RS-485	"1PPS Out [1204-18, -19, -21, -2B]" on page 410
22	IRIG module, RS-485 (4 outputs)	IRIG Out, RS-485	"IRIG Out [1204-15, -1E, -22]" on page 455

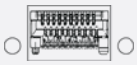
Card ID*	Card Name	Name in UI	See ...
23	Event Broadcast module	Event Broadcast	"Event Broadcast [1204-23]" on page 567
24	STANAG isolated input module	STANAG In, Isolated	"STANAG In [1204-1D, -24]" on page 484
25	STANAG isolated output module	STANAG Out, Isolated	"STANAG Out [1204-11, -25]" on page 476
26	1 MHz output module (3 outputs)	1MHz Out	"Frequency Out [1204-08, -1C, -26]" on page 427
27	IRIG module, Fiber Optic (1 input, 2 outputs)	IRIG In/Out, Fiber	"IRIG In/Out [1204-05, -27]" on page 461
28	1-in/3-out 1 PPS module (TTL [BNC])	1PPS/Frequency RS-485	"1PPS In/Out [1204-28, -2A]" on page 415
29	1-in/3-out HaveQuick module (TTL [BNC])	HAVE QUICK	"HAVE QUICK In/Out [1204-29]" on page 497
2A	1-in/3-out 1 PPS module (Fiber Optic)	1PPS In/Out, Fiber	"1PPS In/Out [1204-28, -2A]" on page 415
2B	Quad 1 PPS output module (Fiber Optic)	1PPS Out, Fiber	"1PPS Out [1204-18, -19, -21, -2B]" on page 410
2E	Revertive Selector module ("Failover")	n/a	"Revertive Selector Card [1204-2E]" on page 565
2F	Programmable Frequency Output module (TTL)	Prog Freq Out, TTL	"Programmable Frequency Out [1204-13, -2F, -30]" on page 430
30	Programmable Frequency Output module (RS-485)	Prog Freq Out, RS-485	"Programmable Frequency Out [1204-13, -2F, -30]" on page 430
32	1Gb PTP module	Gb PTP	"PTP Grandmaster [1204-32]" on page 534
3E	STL input module	STL	"STL Option Module [1204-3E]" on page 552
49	Dual 1 Gb NTP Server	Dual 1GBE	"NTP and Networking [4A, 49]" on page 515
4A	Quad 1 Gb NTP Server	Quad 1GBE	"NTP and Networking [4A, 49]" on page 515
4C	Differential Terminal Block 4 Port E1/T1 module	E1/T1 Out Quad Terminal	"T1/E1 Out [1204-09, -0A, -4C, -53]" on page 447
53	Single-ended BNC 4 port E1/T1 module	E1/T1 Out Quad BNC	"T1/E1 Out [1204-09, -0A, -4C, -53]" on page 447
5E	NavIC	Proprietary GNSS Receiver	"NavIC [1204-5E and 1204-5F]" on page 575

Card ID*	Card Name	Name in UI	See ...
5F	NavIC	Proprietary GNSS Receiver	"NavIC [1204-5E and 1204-5F]" on page 575

1.5.3 Option Card Connectors

The table below lists the connector types used in SecureSync option cards.

Table 1-6: Option card connectors

Connector	Illustration	Electr. Signals	Timing signals
BNC		Differential TTL xV, sine wave, programm. square wave, AM sine wave, DCLS	1PPS, frequency, IRIG, HAVE QUICK, PTP
ST Fiber Optic		DCLS	IRIG, 1PPS
Terminal Block [**Recommended mating connector:** Phoenix Contact, part no. 182 7787]		RS-485	1PPS, frequency, ASCII time code, IRIG, HAVEQUICK, Alarm, T1/E1
DB-9		RS-232, RS-485	ASCII time code, GPS NMEA, data clocks, CTCSS frequency, 1PPS, Alarm signal
DB-25		Differential TTL xV, RS-485	STANAG
RJ-12		RS-485	data clock, CTCSS frequency, 1PPS, Alarm
RJ-45		Gb-Ethernet	PTP timing signal
SFP		Ethernet	NTP timing signal, PTP timing signal
SMA		RF, differential TTL xV, sine wave, programm. square wave, AM sine wave, DCLS	1PPS, frequency

1.6 Specifications

The specifications listed below apply to the SecureSync standard model, i.e. not including any option cards, and are based on “normal” operation, with SecureSync synchronized to valid Time and 1PPS input references (in the case of GNSS input, this is with the GNSS receiver operating in Stationary mode).

Specifications for the available option cards are provided in their corresponding topics; see "Option Cards Overview" on page 17.

1.6.1 Input Power

AC power source:

- 100 to 240 V_{AC}, ±10 %, 50/60 Hz

DC power source (option):

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

Maximum power draw:

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

Backup Battery: SecureSync has an internal battery to support the Real Time Clock. The battery is a small recharging lithium coin cell that is not customer-replaceable. This battery will keep approximate time and date in a shutdown state over ~135 days before requiring recharge. After full drain, the battery will require ~5 days to fully recharge. Minimum battery life is ~30+ years. For information on battery maintenance, see "Maintenance" on page 644

Hot Swap Power Supply: Some SecureSync models have hot-swappable power supplies and can ensure power redundancy in case of failure. Each power sled has the same specifications as the standard AC or DC specifications (see above). For information on safe operation, see "Hot Swap Power Supply" on page 56.

1.6.2 GNSS Receiver

Model: u-blox M8T

Compatible signals:

- GPS L1 C/A Code transmissions at 1575.42 MHz
- GLONASS L1 0F transmissions centered at 1602.0 MHz
- Galileo E1 B/C transmissions at 1575.42 MHz
- BeiDou B1 transmissions centered at 1561.098 MHz
- QZSS L1-SAIF transmissions at 1575.42 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 SecureSync, 16 dB gain minimum

Antenna connector: SMA (SMA to N-type conversion cable included in anxillary kit)

1.6.3 10 MHz Output

- **Signal**: 10 MHz sine wave
- **Signal Level**: +13 dBm ±2dB into 50 Ω
- **Harmonics**: -30 dBc minimum
- **Spurious**: -70 dBc minimum; -60 dBc minimum (Rb)
- **Connector**: BNC female
- **Signature Control**: This configurable feature removes the output signal whenever a major alarm condition or loss of time synchronization condition is present. The output will be restored once the fault condition is corrected.
- Accuracy rating depends on the oscillator selected during the ordering process.

Table 1-7: 10 MHz output — oscillator types and accuracies

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

Oscillator Type	Accuracy
OCXO	$1x10^{-12}$ typical 24-hour average locked to GPS
	$1x10^{-9}$ per day typical aging unlocked
TCXO	$1x10^{-12}$ typical 24-hour average locked to GPS
	$1x10^{-8}$ per day typical aging unlocked

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

See also "Configuring the Oscillator" on page 271.

Table 1-8: 10 MHz output — oscillator stability

Oscillator Type	Medium-Term Stability (without GPS after 2 weeks of GPS lock)	Short-Term Stability (Allan variance)			Temperature Stability (p-p)
		1 sec.	10 sec.	100 sec.	
Low-phase noise Rubidium	$5x10^{-11}$/month ($3x10^{-11}$/month typical)	$1x10^{-11}$	$1x10^{-11}$	$5x10^{-12}$	$1x10^{-10}$
Rubidium	$5x10^{-11}$/month ($3x10^{-11}$/month typical)	$1x10^{-11}$	$9x10^{-12}$	$4x10^{-12}$	$1x10^{-10}$
Low-phase noise OCXO	$2x10^{-10}$/day	$1x10^{-11}$	$9x10^{-12}$	$8x10^{-12}$	$1x10^{-9}$
OCXO	$5x10^{-10}$/day	$1x10^{-11}$	$9x10^{-12}$	$9x10^{-12}$	$5x10^{-9}$
TCXO	$1x10^{-8}$/day	$2.5x10^{-9}$	$1x10^{-9}$	$5x10^{-10}$	$1x10^{-6}$

1.6.3.1 10 MHz Output — Oscillator Phase Noise (dBc/Hz)

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

1.6.4 Multi I/O

The Multi I/O HD15-pin connector can be configured to provide different output and input types. For more information, see "Configurable Connectors" on page 171.

Connector: 15 pin D-Sub (HD15) female

Available signals:

- DCLS IN:
  - Input level 1.5 V (min), impedance 50 Ω
- DCLS OUT:
  - Output level 5 V (peak), impedance 50 Ω
- IRIG AM OUT:
  - Output impedance - 50 Ω
  - Output level: 10 V (peak to peak max, user configurable)
- RS232:
  - Output level: ± 5.0 V, impedance 300 Ω
  - Input level: -15 to 15 V (max), threshold 0.6 V min to 2.4 V max, impedance 3 kΩ min
- RS485 (2):
  - Output level: ± 1.5 V, impedance 54 Ω
  - Input level: -7 to 12 V (max), sensitivity - ± 200 mV, impedance 12 kΩ min

Available Output Types: 1PPS, ASCII Time Code, IRIG (DCLS), IRIG (AM), HAVEQUICK, GPO

Available Input ("Reference") Types: 1PPS, ASCII Time Code, HAVEQUICK, IRIG (DCLS)

Pinout:

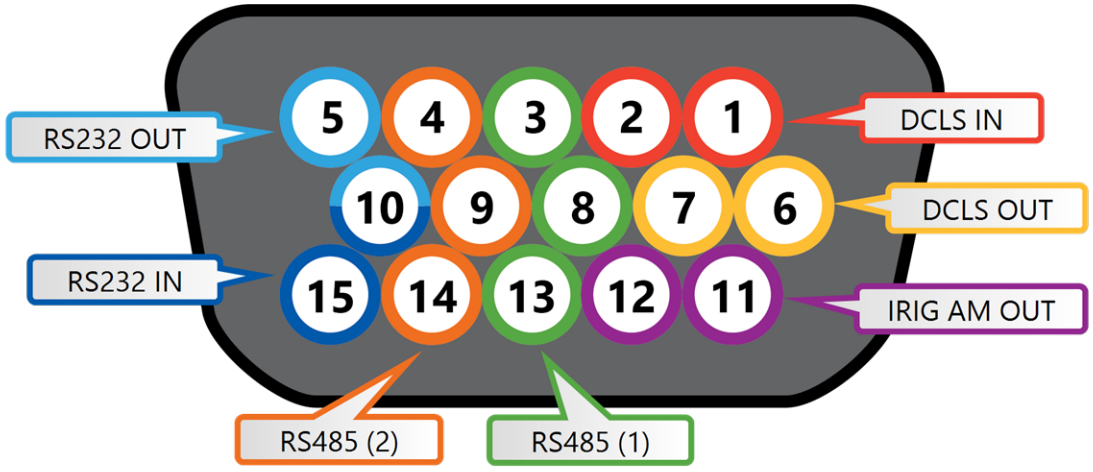


Figure 1-7: Multi I/O connector, viewed in mating direction on rear of unit

Table 1-9: Multi I/O connector signal pinout

Pin	Signal
1	DCLS IN
2	GND
3	(First signal) RS485 A, non-inverting
4	(Second signal) RS485 A, non-inverting
5	RS232 TX OUT
6	DCLS OUT
7	GND
8	GND
9	GND
10	GND
11	IRIG AM OUT
12	GND
13	(First signal) RS485 B, inverting
14	(Second signal) RS485 B, inverting
15	RS232 RX IN

Table 1-10: Multi I/O signal defaults

Pins	Channel	Default Signal
6 & 7	DCLS OUT	IRIG OUT
1 & 2	DCLS IN	IRIG IN
15 & 10	RS232 IN	ATC IN
5 & 10	RS232 OUT	ATC OUT
3, 8, 13	RS485 (1)	HAVEQUICK OUT
4, 9, 14	RS485 (2)	HAVEQUICK IN
11 & 12	IRIG AM OUT	IRIG OUT (AM ONLY)

1.6.5 DCLS Output

The rear panel DCLS OUT BNC female connector defaults to a 1PPS Output (see below), but can be configured to produce different output signals: IRIG Output, HaveQuick Output, and GPIO Output. For more information, see "Configurable Connectors" on page 171.

1.6.5.1 1PPS Output

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

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

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

Pulse width range: 20 ns to 900 ms

Rise time: <10 ns

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

Connector: BNC female

Table 1-11: 1PPS output accuracies

Oscillator Type	Accuracy to UTC (1 sigma locked to GPS)	Holdover (constant temp. after 2 weeks of GPS lock)	
		After 4 hours	After 24 hours
Low-phase noise Rubidium	±15 ns	0.2 µs	1µs
Rubidium	±15 ns	0.2 µs	1µs

Oscillator Type	Accuracy to UTC (1 sigma locked to GPS)	Holdover (constant temp. after 2 weeks of GPS lock)	
		After 4 hours	After 24 hours
Low-phase noise OCXO	±15 ns	0.5 µs	10 µs
OCXO	±25 ns	1µs	25 µs
TCXO	±50 ns	12 µs	450 µs

1.6.6 10/100/1000 Ethernet Port (RJ45)

ETH0

Function: 10/100/1000 Base-T, auto-sensing LAN connection for NTP/SNTP and remote management and configuration, monitoring, diagnostics and upgrade

Connector: RJ45, Network IEEE 802.3

1.6.7 10/100/1000 Ethernet Port (SFP)

ETH1

Function: 10/100/1000 (speed depends on connection) Base-T, auto-sensing LAN connection for NTP/SNTP and remote management and configuration, monitoring, diagnostics and upgrade

Connector: Ethernet via SFP

- 6COM 6C-SFP-T
- Avago ABCU-5740RZ
- Avago ABCU-5741ARZ
- Avago AFBR-5710LZ (available from Safran as **SFP-FIBER-MM**)
- Bel SFP-1GBT-05
- Bel SFP-1GBT-06 GBIC 1000BASE-T
- Finisar FCLF8522P2BTL (available from Safran as **SFP-COPPER**)
- Finisar FTLF1318P3BTL (available from Safran as **SFP-FIBER-SM**)
- Molex 1837021004 (available from Safran as **SFP-COPPER**)
- Molex 1837022037

An SFP module found to NOT be supported: Arista SFP-1G-T

1.6.8 RS-232 Serial Port (Rear Panel)

Function: Accepts commands to locally configure the IP network parameters via CLI for initial unit configuration.

Connector: RJ45

Character structure: ASCII, 115200 baud, 1 start, 8 data, 1 stop, no parity

1.6.9 USB Serial Port (Front Panel)

Function: Accepts commands to locally configure the IP network parameters via CLI for initial unit configuration.

Connector: micro-B USB (requires installed driver; if your driver does not automatically install, visit: https://www.ftdichip.com/Drivers/VCP.htm)

Character structure: ASCII, 115200 baud, 1 start, 8 data, 1 stop, no parity

1.6.10 Cables

CA08R-D500-0001

This breakout cable option is available for purchase for the multi-I/O (15-pin) connector on the front panel.

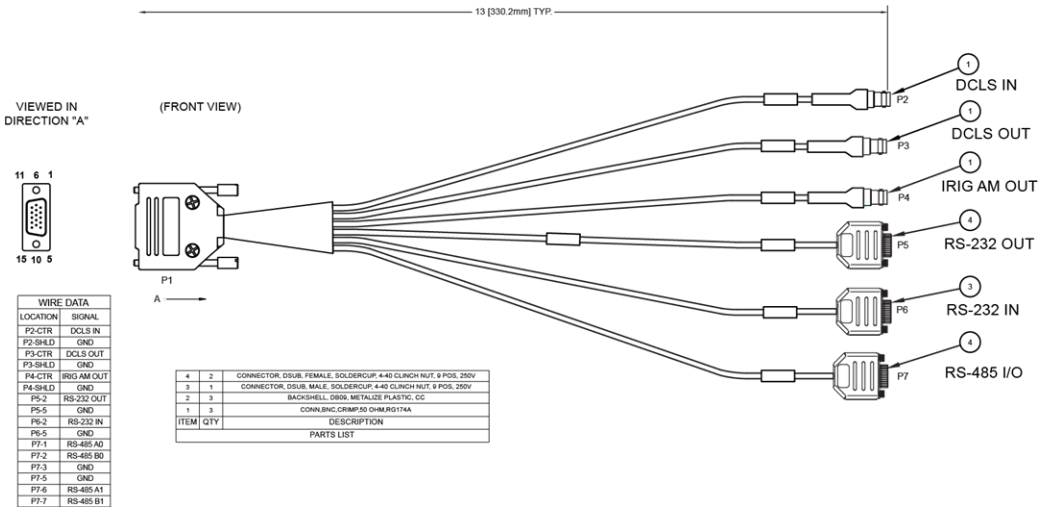


Figure 1-8: CA08R-D500-0001 drawing

CA08R-0000-0010

The CA08R-0000-0010 NENA breakout cable connects to the multi-I/O (15-pin) connector and a 1204-0F option card and provides an IRIG AM output, an RS-485 input/output, and an RS-232 input/output.

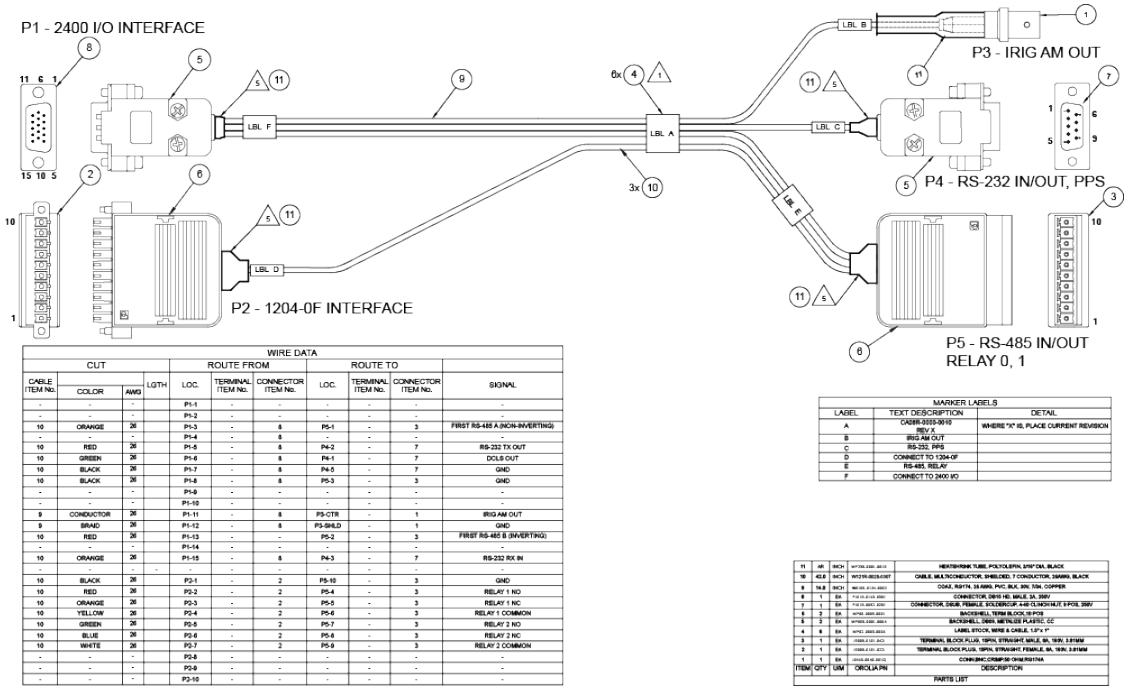


Figure 1-9: CA08R-0000-0010 drawing

The 2400-0000-0715 Strain Relief Anc Kit (optional) provides cable management, strain relief, and grounding for the SecureSync. For more information see "Strain Relief Ancillary Kit" on page 637.

1.6.11 Protocols Supported

NTP: NTP Version 4. Provides MD5, Stratum 1 through 15 (RFC 5905).

PTP: IEEE 1588 :2019 (PTP v2.1)

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

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

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

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

SNMP: Supports v1, v2c, and v3

Telnet/SSH: For limited remote configuration

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

Authentication: LDAP v2 and v3, RADIUS, MD5 Passwords, TACAS+.

1.6.12 Mechanical and Environmental Specifications

Dimensions:

- Designed for EIA 19" rack mount:
- Housing w/o connectors and brackets:
  - 17.1" W x 1.74" H [1U] x 15.17" D actual
  - (434 mm W x 44 mm H x 385 mm D)

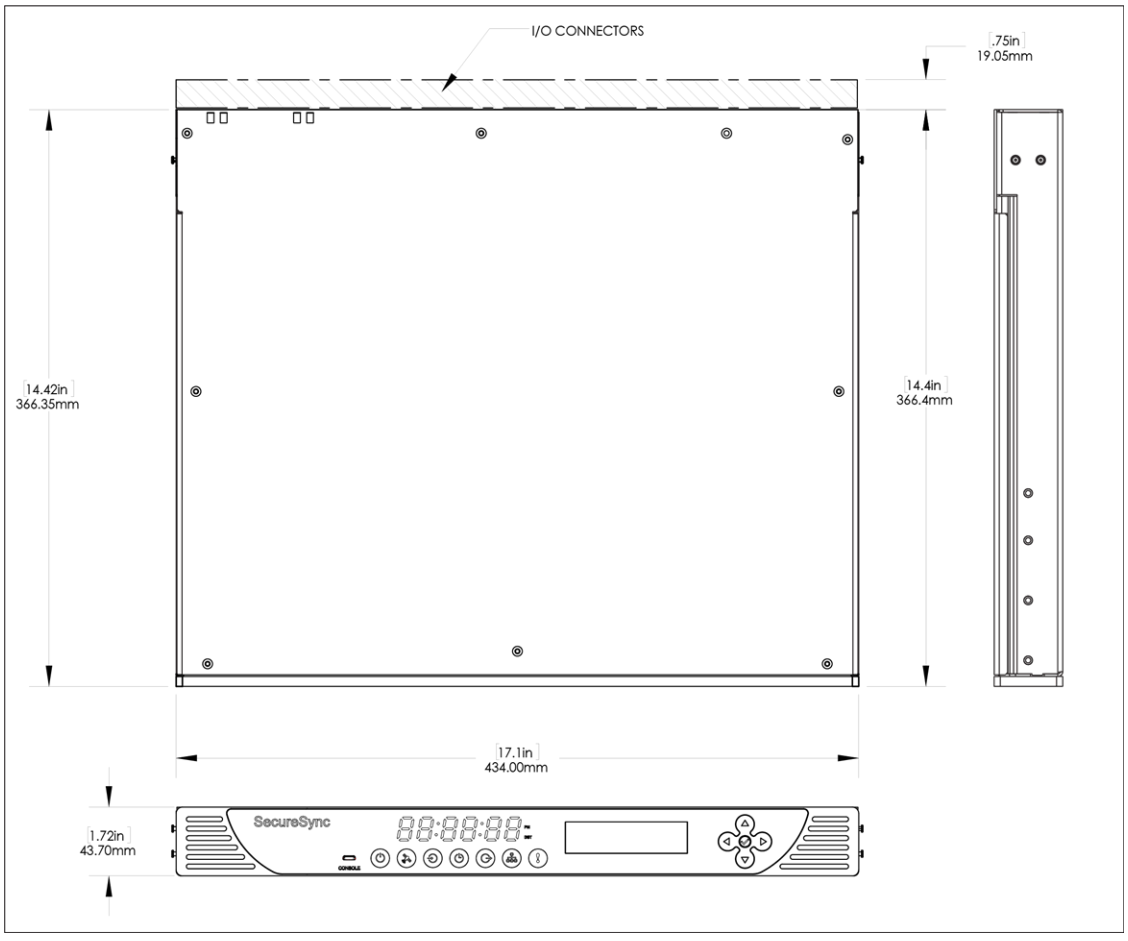


Figure 1-10: Mechanical dimensions

Weight: 6.0 lbs (2.72 kg) for base unit with AC power supply

Temperature:

- **Operating:**–20°C to +65°C (55°C with Rubidium oscillator option)
- **Storage:** –40°C to +85°C

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

Altitude:

- **Operating:** 100-240 V_{AC}: up to 13120 ft (3999 m)
- **Storage range:** up to 45000 ft (13716 m)

Shock and Vibration (Operating and Storage):

- **Shock:** 516.8 15g, 11 ms halfsine
- **Vibration:** 514.8C-2 cat 4 and 514.8D-11, cat 21 1.1 g rms vertical and 0.8 g rms longitudinal

MIL-STD-810G: 500.6, 501.6, 502.6, 503.6, 507.6

MIL-STD-810H: 514.8, 516.8

1.7 The SecureSync Web UI

SecureSync has an integrated web user interface (referred to as "Web UI" throughout this documentation) that can be accessed from a computer over a network connection, using a standard web browser. The Web UI is the most complete way to configure the unit, and for status monitoring during everyday operation.



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 575.



Note: Should it ever be necessary, you can restore SecureSync's configuration to the factory settings at any time. See "Resetting the Unit to Factory Configuration" on page 367.

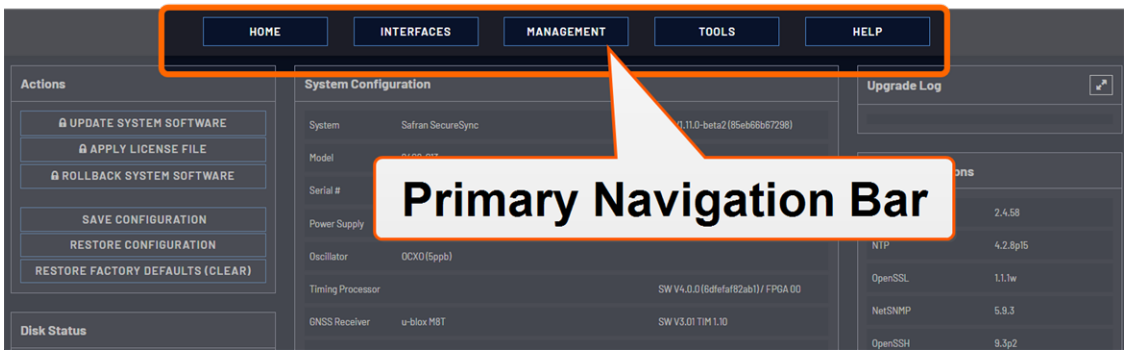
1.7.1 The Web UI HOME Screen

> **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 SecureSync 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:

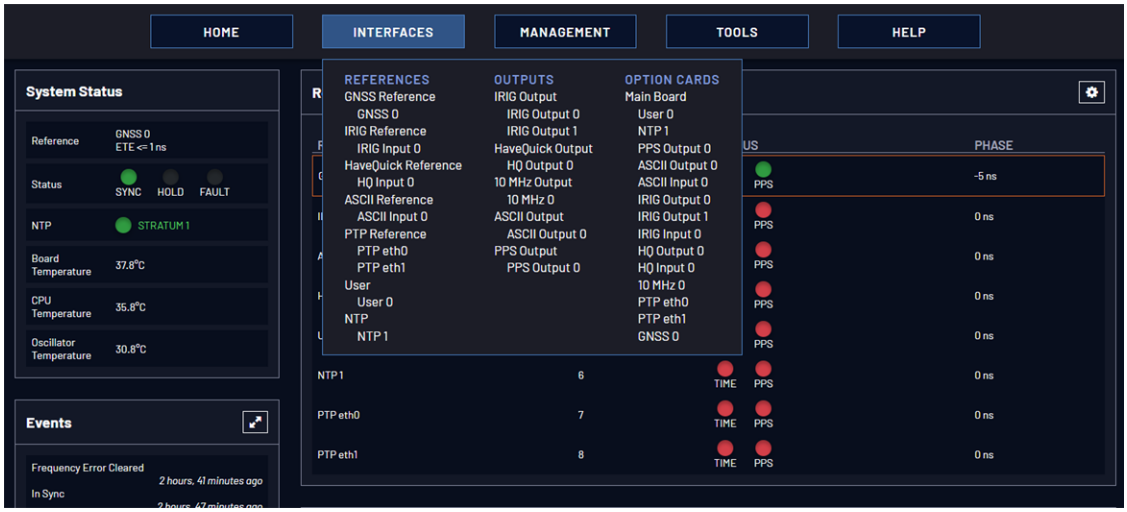
- **HOME**: Return to the HOME screen (see above)
- **INTERFACES**: Access the configuration pages for ...
  - ... references (e.g., GNSS, NTP)
  - ... outputs (e.g. 10 MHz, PPS, NTP) and
  - ... installed input/output option cards.
- **MANAGEMENT**: Access the NETWORK setup screens, and OTHER setup 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.

1.7.2 The INTERFACES Menu

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

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



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.

> **Note:** Many of the interfaces can be accessed through different menu items e.g., an optional output will be available under the OPTION CARDS menu and the OUTPUTS menu.

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

1.7.3 The Configuration MANAGEMENT Menu

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

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

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

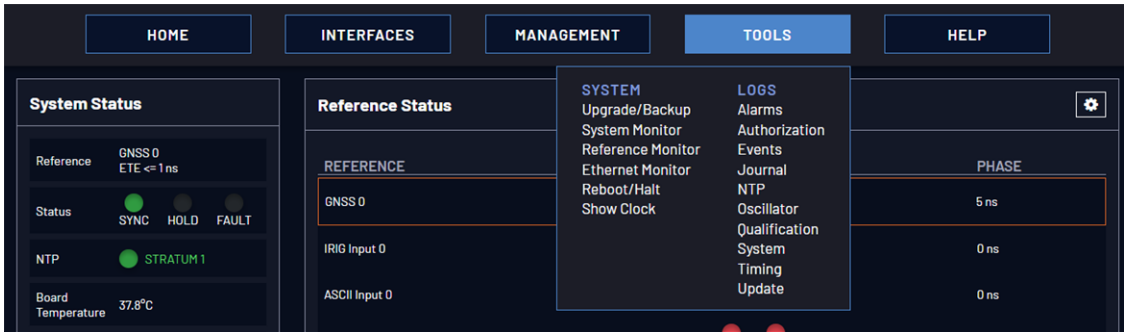
Under **OTHER**, you can access non-network related screens:

- **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 SecureSync's events. A notification can be a combination of a mask alarm and/or SNMP Trap and/or email.
- **Time Management**: Manage the Local Clock, UTC Offset, DST Definition and Leap Second information.
- **Log Configuration**: Manage the system logs.
- **Disciplining**: Manage oscillator disciplining.
- **Change My Password**: Configure the admin password.

1.7.4 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



1.8 Regulatory Compliance

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

FCC

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

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

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

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

Safety

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

- IEC 62368-1:2014 (Second Edition)
- EN 62368-1:2014 +A11:2017
- UL 62368-1:2014

- CAN/CSA-C22.2 NO. 62368-1-14
- IEC62368-1(2014) + Japanese deviation (or J62368-1(2020))

EMC Compliance

This product has been tested and meets the following standards:

- EN 55032:AC:2015
- FCC CFR 47 PART 15 SubPart B: 2016
- CAN/CSA-CISPR 22-10/ ICES-003 Issue 6: Class A
- AS/NZS CISPR 32:2015/ AMDI1.2019
- EN 55035:2017: Class A
- CISPR32(2015:2nd) + Japanese deviation (or J55032(H29))
- EN61000-3-2:2014, EN61000-3-3:2013, EN61000-4-2:2009, EN61000-4-3:2006: +A1:2008 + A2:2010, EN61000-4-4:2012, EN61000-4-5:2006, EN61000-4-6:2009, EN61000-4-8:2010, EN61000-4-11:2004 EN 301 489-1 V2.0.1 (2016-11) and EN 301 489-19 V1.2.1 (2002-11)

Radio Spectrum Efficiency:

- EN 303 413 V1.1.1

European Directives

This product has been tested and complies with the following:

- 2014/30/EU Electromagnetic Compatibility (EMC)
- 2014/35 EU Low Voltage (LVD)
- 2011/65/EU with Amendment 2015/863/EU on the Restriction of Hazardous Substance (RoHS3)
- 2014/53/EU Radio Equipment Directive (RED)

Environmental Compliance

- WEEE (Waste Electrical and Electronic Equipment)
- REACH (Registration, Evaluation, Authorization and Restriction of Chemicals)

CHAPTER 2

SETUP

The following topics are included in this Chapter:

2.1 Installation Overview 42
2.2 Unpacking and Inventory 43
2.3 Required Tools and Parts 44
2.4 SAFETY 45
2.5 Mounting the Unit 48
2.6 Connecting the GNSS Input 50
2.7 Connecting Network Cables 51
2.8 Connecting Inputs and Outputs 52
2.9 Connecting Supply Power 52
2.10 Powering Up the Unit 61
2.11 Zero Configuration Setup 62
2.12 Setting up an IP Address 63
2.13 Accessing the Web UI 71
2.14 Configure Network Settings 73
2.15 Configure NTP 113
2.16 Configuring PTP 155
2.17 GPSD Setup 170
2.18 Configurable Connectors 171
2.19 Configuring Input References 176
2.20 Configuring Outputs 184
2.21 The Option Cards Screen 196
2.22 Signature Control 198

2.1 Installation Overview

This section provides an outline of the steps that need to be performed prior to putting SecureSync into service. This includes:

- 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.

The following factors determine which steps need to be taken:

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

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

c. How you would like to setup basic network configuration parameters:
   - Using the unit's front panel keypad and information display
   - Using a PC connected to SecureSync via serial cable
   - Using a PC connected to SecureSync via network cable.

     You can connect your PC to SecureSync either...
     - ...directly by means of a dedicated Ethernet cable, or
     - ...indirectly, using your existing Ethernet network (using a network hub).

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

2.1.1 Main Installation Steps

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

1. Read the Safety instructions: "SAFETY" on page 45.
2. Unpack the unit, and take inventory: "Unpacking and Inventory" on the facing page.
3. Obtain required tools and parts: "Required Tools and Parts" on page 44.
4. Mount the unit: ."Mounting the Unit" on page 48.

5. Connect Input References such as your GNSS antenna, and network cable (s): "Connecting the GNSS Input" on page 50, and "Connecting Network Cables" on page 51.
6. Connect your power supply/-ies: "Connecting Supply Power" on page 52.
7. Power up the unit: "Powering Up the Unit" on page 278.
8. Setup basic network connectivity....
    i. ...via front panel keypad and information display: "Setting Up an IP Address via the Front Panel" on page 66
    ii. ...or via serial port, using a PC with a CLI: "Setting Up an IP Address via the Serial Port" on page 69
    iii. ...or via Ethernet, using a PC with a web browser, and the SecureSync Web UI: "Accessing the Web UI" on page 71.
9. Register your product: "Product Registration" on page 321.

2.2 Unpacking and Inventory



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

Unpack the equipment and inspect it for damage. If any equipment has been damaged in transit, or you experience any problems during installation and configuration of your Safran product, please contact Safran (see "Technical Support" on page 645).



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

The following items are included with your shipment:

- SecureSync unit
- QuickStart Guide (printed version)
- Ancillary items (except for rack mounting items, the contents of this kit may vary based on equipment configuration and/or regional requirements)

- Purchased optional equipment (note that option cards listed on the purchase order will be pre-installed in the unit). See "Option Card Identification" on page 21 and "Option Cards Overview" on page 17.

2.3 Required Tools and Parts

Depending on your application and system configuration, the following tools and parts may be required:

- Phillips screwdrivers to install the rack-mount ears, and to mount the unit in a 19"-rack
- Ethernet cables (see "Connecting Network Cables" on page 51).

2.3.1 Required GNSS Antenna Components

Should you plan on using a GNSS reference with your SecureSync, you will also need the following items (sold separately):

- Antenna cable with SMA connector, or conversion cable

> **Note:** The SMA-to-N-type conversion cable included in the ancillary kit is approved for pull weight of up to 60 lbs. If you are using a heavier cable, you will need to apply appropriate strain relief.

- GNSS antenna with mounting bracket
- GNSS antenna surge suppressor (recommended)
- GNSS antenna inline amplifier (optional for short cable lengths)

For antenna installation guidelines, see the separate documentation shipped with the antenna components.

2.4 SAFETY

Safety: Symbols Used

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

Symbol	Signal word	Definition
	DANGER!	Potentially dangerous situation which may lead to personal injury or death! Follow the instructions closely.
	CAUTION!	Caution, risk of electric shock.
	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.
	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.

SAFETY: Before You Begin Installation

This product has been designed and built in accordance with state-of-the-art standards and the recognized safety rules. Nevertheless, its use may constitute a risk to the operator or installation/maintenance personnel, if the product is 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 the 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 Safran Technical Support if this equipment needs to be serviced. Do not open the equipment, unless instructed to do so by Safran Service personnel. Follow Safran Safety instructions and observe all local electrical regulatory requirements.

DANGER! – IF THE EQUIPMENT MUST BE OPENED:
Never remove the cover or blank option card plates while power is applied to this unit. The unit may contain more than one power source. Disconnect AC and DC power supply cords before removing the cover to avoid electrical shock.



DANGER! — GROUNDING:
This equipment must be EARTH GROUNDED.
This product is grounded through the power supply. There is an additional, supplementary chassis ground on the rear panel.
Never defeat the ground connector or operate the equipment in the absence of a suitably installed earth ground connection. Contact the appropriate electrical authority or an electrician if you are unsure that suitable earth grounding is available.



DANGER! This unit might have more than one power supply connection. All connections must be removed to de-energize the unit



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

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 Safran.
- Always follow the instructions set out in this User Manual, or in other Safran documentation for this product.
- Observe generally applicable legal and other local mandatory regulations.

SAFETY: Other Tips

- Keep these instructions at hand, near the place of use.
- Keep your workplace tidy.
- Apply technical common sense: If you suspect that it is unsafe to use the product, do the following:

- Disconnect the supply voltage from the unit.
- Clearly mark the equipment to prevent its further operation.

2.5 Mounting the Unit

SecureSync units can be operated on a desktop or in a rack in a **horizontal**, **right-side-up** position. The location needs to be well-ventilated, clean and accessible.

Caution: For safety reasons the SecureSync unit is intended to be operated in a HORIZONTAL POSITION, RIGHT-SIDE-UP.

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

Rack mounting requirements:

- The maximum **ambient operating temperature** must be observed. See "Mechanical and Environmental Specifications" on page 34 for the operating temperature range specified for the type of oscillator installed in your SecureSync unit.
- If the SecureSync unit is to be installed in a closed rack, or a rack with large amounts of other equipment, a **rack cooling fan** or fans should be part of the rack mount installation.
- Installation of the unit in a rack should be such that the amount of **air flow** required for safe operation of the equipment is not compromised.
- Follow the mounting directions described below to **prevent uneven mechanical loading**, possibly resulting in a hazardous condition.
- **Do not overload power supply circuits**. Use only supply circuits with adequate overload protection. For power requirements, see "Input Power" on page 25.
- Reliable **grounding** of rack-mounted equipment must be maintained. Particular attention must be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips).

2.5.1 Rack Mounting (Ears)

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

- 2 each 2400-1000-0714 equipment rack mount ears
- 6 each HM20R-04R7-0010 M4 flat head Phillips screws

The 2400-0000-0715 Strain Relief Ancillary Kit (optional) contains additional mounting items available for purchase:

- 2 each 2400-1000-0797 rear brackets
- 10 each HM20R-04R7-0010 M4 flat head Phillips screws

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

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

To rack mount the SecureSync unit:

1. Attach the 2400-1000-0714 **rack mount ears** to the sides of the SecureSync with the ears facing outward, aligned with the front edge of the SecureSync front panel. (See image below). To secure, use the #2 Phillips screwdriver, and 3 each of the HM20R-04R7-0010 M4 flat head Phillips screws per side.

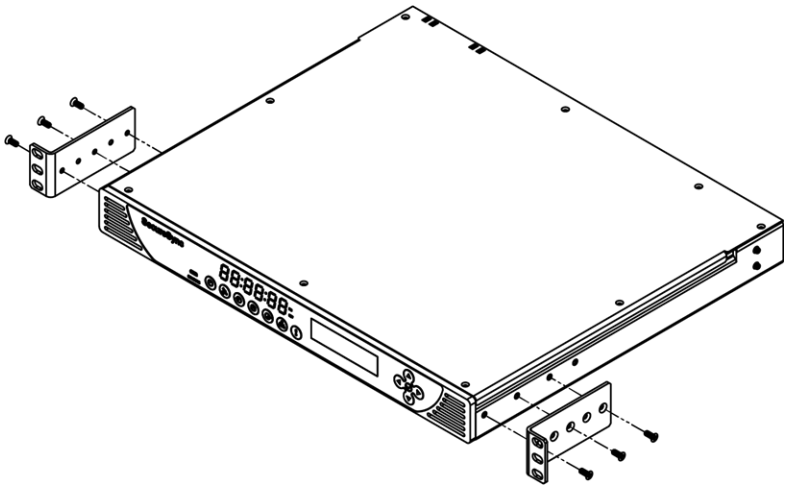


Figure 2-1: Rack mount installation

2. Secure the rack mount brackets to the rack using the #10-32 rack mount screws and #2 Phillips head screwdriver, 2 each per side of the rack.
3. If you purchased additional **rear rack mounts**, you will align the holes with the available pegs near the rear of the unit and slide the rail forward into place.

   Secure the mount with the screw hole closest to the front of the chassis using 1 each of the supplied HM20R-04R7-0010 screws per side.

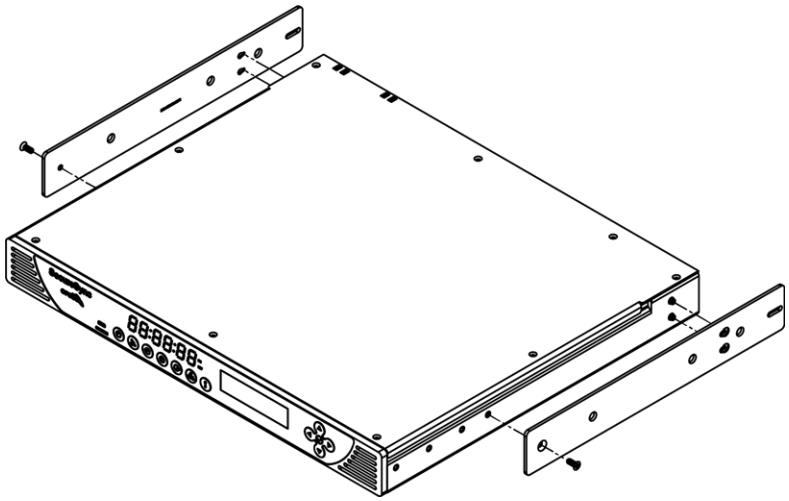


Figure 2-2: Rear rack mount installation

2.6 Connecting the GNSS Input

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

1. Install a GNSS antenna, surge suppressor, antenna cabling, and GNSS preamplifier (if required). Refer to the documentation included with your GNSS antenna for information regarding GNSS antenna installation.

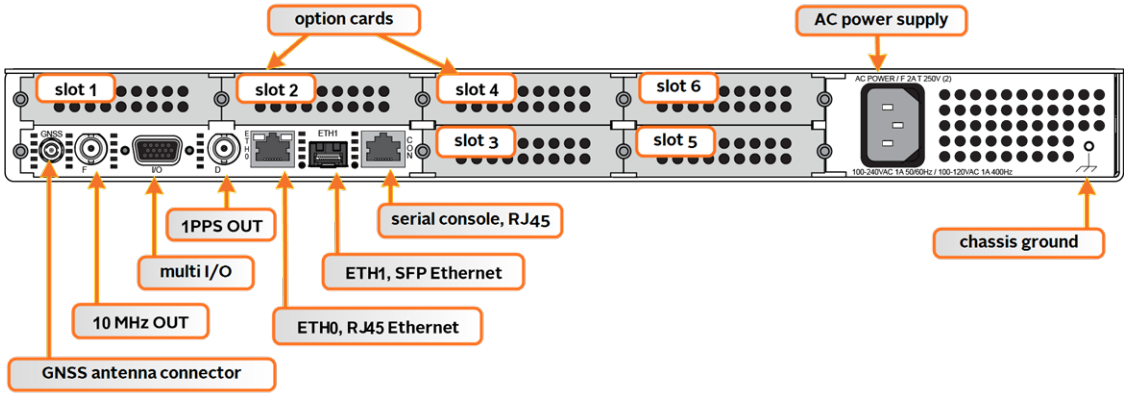
> **Note:** The SMA-to-N-type conversion cable included in the ancillary kit is approved for pull weight of up to 60 lbs. If you are using a heavier cable, you will need to apply appropriate strain relief.

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

2. Connect the GNSS cable to the rear panel antenna input jack.

Initial synchronization with GNSS input may take up to 12 minutes (approximately) when used in the default stationary GNSS operating mode. If using GNSS, verify that GNSS is the synchronization source by navigating to **MANAGEMENT > OTHER: Reference Priority**: Confirm that GNSS is **Enabled**, and its **Status** for TIME and 1PPS is valid (green).

2.7 Connecting Network Cables



SecureSync includes two BASE 10/100/1000 Ethernet ports (ETH0- RJ45, and ETH1- SFP) for full NTP functionality, as well as a comprehensive web-based user interface ("Web UI") for configuration, monitoring and diagnostic support.

Before connecting the network cable(s), you need to decide which port(s) you want to use for which purpose (e.g., ETH0 for configuration only, etc.), and how you want to configure basic network connectivity e.g., the IP address:

a. Configure SecureSync via the unit's front panel: See "Setting Up an IP Address via the Front Panel" on page 66.

b. Configure SecureSync by means of a PC connected to an existing network.

   » When connecting to a hub, router, or network computer, use a **straight-through wired, shielded CAT 5, Cat 5E or CAT 6 cable with RJ45 connectors (Eth0) or SFP connectors (Eth1)**. Connect one end to the Ethernet port on the SecureSync rear panel, and the opposite end of the cable to a network hub or switch.

c. Configure SecureSync by connecting a stand-alone computer directly via a dedicated network cable (standard-wired, or crossover cable):

» When connecting directly to a stand-alone PC, use a network cable. Connect the cable to the NIC card of the computer.
Since no DHCP server is available in this configuration both SecureSync, and the PC must be configured with static IP addresses that are on the same subnet (10.1.100.1 and 10.1.100.2 with a subnet mask value of 255.255.255.0 on both devices, for example). For more information on configuring static IP addresses, see "Assigning a Static IP Address" on page 65.

On Eth0: Once the unit is up and running, verify that the green link light on the Ethernet port is illuminated. The amber "Activity" link light may periodically illuminate when network traffic is present.

2.8 Connecting Inputs and Outputs

SecureSync can synchronize not only to an external GNSS reference signal, but also to other optional external references such as IRIG, HAVE QUICK and ASCII inputs (in addition to network based references such as NTP and/or PTP).

At the same time, SecureSync can output timing and frequency signals for the consumption by other devices via the same formats as listed above.

EXAMPLE:

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

To use e.g., an external IRIG reference, connect the IRIG time source to the BNC connector "J1" on the optional IRIG Input/Output module. For additional information on optional connectivity, such as pinout tables, signal levels and other specifications, see "Option Cards" on page 383.

Note that some option cards offer both input and output functionality, while others offer only one or the other.

2.9 Connecting Supply Power

Depending on the equipment configuration at time of purchase, SecureSync may be powered from different sources.

Table 2-2: SecureSync 2400 Power Supply via Part Number

Part number	Connections	Power Supply
240x-**0**xx	1	AC (fixed)
240x-**3**xx	1	12 V DC (fixed)
240x-**4**xx	1	24 V DC (fixed)
240x-**6**xx	1-2 (Hot Swap)	AC, DC (12 V or 24 V), in any combination

Before connecting power to the unit, be sure that you have read all safety information detailed in section "SAFETY" on page 45.

2.9.1 Using AC Input Power

Connect the AC power cord supplied in the SecureSync ancillary kit to the AC input on the rear panel and the AC power source outlet.

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

2.9.2 Using DC Input Power

Note: DC power is an option chosen at time of purchase. The rear panel DC input port connector is only installed if the DC input option is available. Different DC power input options are available (12 V_{DC} with a voltage range of 12 to 17 V at 10 A maximum or 24/48 V_{DC} input with a voltage range of 21 to 60 V at 5.5 A maximum). Review the DC power requirement chosen, prior to connecting DC power.

DANGER! GROUNDING: SecureSync is NOT earth grounded through the 12 V_{DC} (2-Pin) power connector. Before connecting the unit to a DC power source, connect to earth ground with a grounding ring via the grounding post.

DANGER! GROUNDING: SecureSync is earth grounded through the 24/48 V $_{DC}$ 3-Pin power connector. Ensure that the unit is connected to a DC power source that is connected to earth ground via the grounding pin C of the SecureSync DC power plug supplied in the ancillary kit.

A DC power connector to attach DC power to SecureSync is included in the ancillary kit provided with the equipment. A cable of 6 feet or less, using 16AWG wire, with adequate insulation for the DC voltage source should be used with this connector. The cable clamp provided with the DC power plug for strain relief of the DC power input cable should be used when DC power is connected to SecureSync.

DC power- +12 V and +24/48 V identification

To eliminate confusion, the two different voltages for DC power use different connectors. The DC connectors are identical between the fixed or hot-swappable versions.

The +12 V $_{DC}$ power supply uses a **2-pin** connector and has a 12 V label, either above the input or on the body of the power supply module (for Hot Swap models). The connector is keyed to prevent incorrect insertion.

The +24/48 V $_{DC}$ power supply uses a **3-pin** connector and has a 24/48 V label, either above the input or on the body of the power supply sled (for Hot Swap models). This connector is also keyed to prevent incorrect insertion.

DC power connectors

SecureSync units can be ordered in a DC version that includes the following DC receptacle on the back panel: **DC Receptacle , 2-pin, chassis mount:** Amphenol 97-3102A-10SL-4P(946); (Safran P/N J240R-0021-000G) or **DC Receptacle , 3-pin, chassis mount:** Amphenol 97-3102A-10SL-3P(946) (Safran P/N J240R-0032-012F):



Figure 2-3: DC Plug, 2-Pin and DC Plug, 3-Pin

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

- **Mating 12 V_{DC} Connector**, circular, 2-pin, solder socket, 16AWG,13A,300V: Amphenol P/N 97-3106A10SL-4S(946); (Safran P/N P240R-0021-000G)
- OR, **Mating 24/48 V_{DC} Connector**, circular, 3-pin, solder socket, 16AWG,13A,300V: Amphenol P/N DL3106A10SL-3S; (Safran part no. P240R-0032-002F):



Figure 2-4: DC Connector, 2-Pin and DC Connector, 3-Pin

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



Figure 2-5: Cable Clamp, DC Power

Pinout description, DC connectors

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

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

Pin C goes to the Earth ground of the DC source (on +24/48 V units ONLY).

The **grounding post** provides an earth ground for the +12 V power supply (using a customer-supplied grounding ring)

AC/DC Converter

A +24/48 V_{DC} power supply can optionally be used as an AC input: Safran offers a kit containing an AC/DC converter with assembled DC connector: The part number for this adapter kit is **PS06R-2Z1M-DT01**.



Figure 2-6: DC to AC Converter

2.9.3 Hot Swap Power Supply

DANGER! Remove the connected power source BEFORE attempting to remove a power sled for replacement.

Caution: Only use Safran-approved replacement parts. Incorrect parts may cause damage to the product.

The hot swap power supply (HSPS) option consists of two bays with redundant power systems. The sleds in the unit can be a mix of AC and DC power supplies. When both power supplies are active, the electrical draw is shared between the two bays. If one power supply is damaged or removed, the other bay will automatically take the entire power load without any additional configuration.

2.9.3.1 Hot Swap Installation

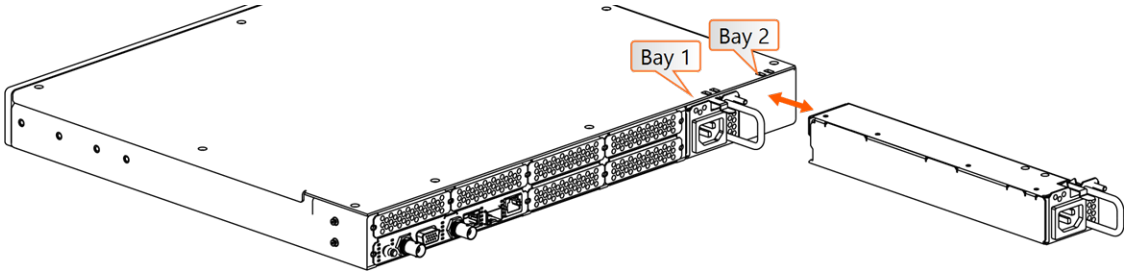


Figure 2-7: Hot Swap Power Supply installation (rear view)

To remove a power supply, first unplug the power input to be removed. (If you are working with a 12 V_{DC} (2-Pin) sled, you will need to remove the ground connection from the post after disconnecting power). Then, press the lever fully down and pull on the handle.

To install a power supply, first insert the sled until the latch clicks and the rear panel of the supply is aligned with the rear panel of the SecureSync. (Be sure to connect power AFTER the sled is fully inserted, and not before). Then, plug in the power input. (If you are working with a **12 V_{DC} (2-Pin)** sled, you will also connect a grounding ring to the external post before connecting power).

2.9.3.2 Hot Swap Monitoring

After installing power supplies, functionality can be confirmed through the Web UI, CLI, front panel, or via SNMP.

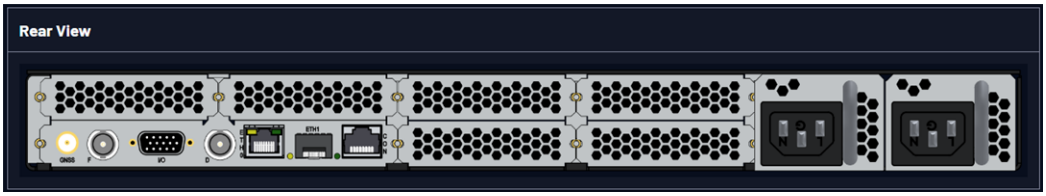
Web UI Hot Swap Monitoring

You can view the status of the power supplies through the Web UI: navigate to **MANAGEMENT** > **OTHER** > **Hot Swap**:

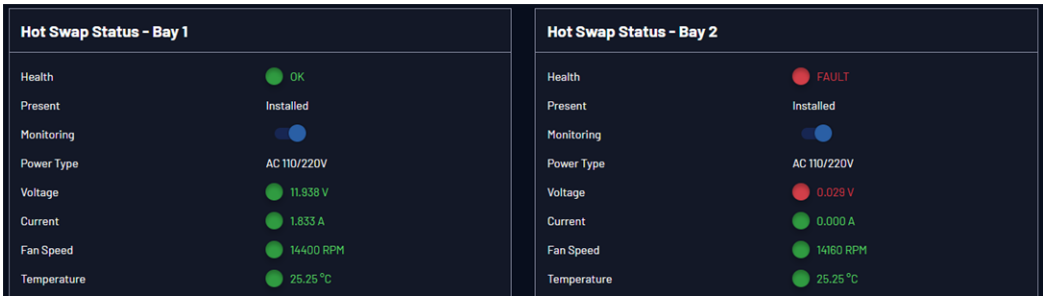
- The **Hot Swap Overall Status** light at the top right of this page indicates whether the unit has at least one active, valid power supply.
  - **Green** indicates all detected power supplies are valid
  - The status will show **yellow** if one power supply is not valid.
  - **Red** if there is no single HSPS module working properly (urgent need for replacement).
  - **Grey** if the monitoring on both sleds has been disabled.

  In this panel, you can also download (or clear) a file of the most recent monitoring information for both bays.

- The **Rear View** panel of the Hot Swap page will display a rendering of the rear panel. You can hover over a power supply to confirm the bay number, and power specifications.



- The **Hot Swap Status** panels for Bay 1 and Bay 2 each provide information and charts related to monitoring the power supplies of the unit, and contain the following elements:



  - **Health**: OK, Warning, Fault, or Monitoring Disabled
  - **Present**: Installed or Not Installed
  - **Monitoring**: ON/OFF. Monitoring of Hot Swap Power Supply statuses can be disabled to reduce logging and health status updates. This setting disables alarming in the case of power supply failure or issue (it is still possible to view statistics for the bay if monitoring is disabled).

> **Note:** It is recommended to disable monitoring on a bay if you choose to remove a power supply long term or keep one inserted that you know is faulty. Disabling monitoring on a faulty supply or empty bay will cause the overall status to display as Okay (provided there is one fully functional power supply installed).

  - **Power Type**: AC 110/220 V, DC 12/24 V, or DC 24/48 V
  - **Voltage** (V)
  - **Current** (A)
  - **Fan Speed** (RPM)

- **Temperature** (C°)
- **Voltage graph**
- **Current graph**
- **Fan Speed graph**
- **Temperature graph**

CLI Hot Swap Monitoring

Functionality and status of the Hot Swap Power Supplies can also be obtained by using the CLI command `HS_GetStatus`.

This command will return the overall Hot Swap status and total current, as well as the status and details for each of the bays (health status, present, power type, fan speed, temp, voltage, current, percentage).

Front Panel Hot Swap Monitoring

If your unit is configured with hot swappable power supplies, an additional menu will be visible on the front panel OLED information menu.

- Press the **Power** Menu button (you will need to pres twice if the first press was waking up the display on the front panel).
- Press the right button to highlight the Hot Swap sub-menu:



- Press the down button to toggle between specific information for Bay 1 and Bay 2:



  In the case of faulty power supplies, the front panel will flash on the important parameter(s) to indicate the need for attention (in the image above, the issue on Bay 2 is with the fan speed and voltage).

- You can also disable monitoring on a specific bay by pressing the ✓ **ENTER** key while the bay is highlighted. Bays with disabled monitoring will be noted on the front panel:



Note: Disabling monitoring on a single bay will remove it from consideration in the Overall Hot Swap Status and remove alarming for the bay.

SNMP/Notifications Hot Swap Monitoring

If your unit is configured with hot swappable power supplies, additional options will be visible in the Web UI under **MANAGEMENT** > **Notifications** in the System tab:



You can configure these notifications to be send via SNMP: "Setting Up SNMP Notifications" on page 287.

Hot Swap Power Supply Alarms

There are two Hot Swap specific alarms:

The **Hot Swap, Major Alarm** will cause the status to appear red in the Web UI and is triggered if one of the power supplies falls within the following thresholds:

- Voltage (< 11V) or (> 13V)
- Current (> 9A)
- Fan Speed (< 10,000 RPM) or (> 18,000 RPM)

The **Hot Swap, Minor Alarm** will cause the status to appear yellow in the Web UI and is triggered if one of the power supplies falls within the following thresholds:

- Temperature AC sled (<-25 °C) or (> 85°C)
- Temperature DC sled (<-40 °C) or (> 85°C)
- Unknown Sled Type installed

Note: An alarm can also be triggered if one of the power supplies is only partially inserted into the unit, and not inserted enough for the latch to click, or if you disconnect, but do not remove, a power supply.
It is also possible that the hot swap power supply may shift during shipping or setup enough to trigger this alarm. In this case, remove the power supply and attempt to reinsert it.

2.10 Powering Up the Unit

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

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

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



Figure 2-8: SecureSync front panel

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

For additional information, see "Status LEDs" on page 4 and "Status Monitoring via Front Panel" on page 322.

2.11 Zero Configuration Setup

As an alternative to conventional network configuration, SecureSync 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 SecureSync's ETH connector is connected to a network, you can directly access the SecureSync 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
- in circumstances when your unit is not connected directly to a PC
- when you wish to access the Web UI of your SecureSync without using the CLI commands or serial connection
- anytime the IP address of a unit is not known (for instance, if you have "lost" your unit on a network).

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 (this is the default setting).
- The PC you will use to communicate with your unit is connected to the same network as your SecureSync.
- 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.

2.11.1 Using Zeroconf

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

1. Obtain the last 6 digits of the **MAC** address: e.g., "`0E 51 7B`". The MAC address can be found:
   - » On the front panel display under the Network menu
   - » On the serial number label on the side on the unit
   - » Through the CLI using the `ifconfig` command.
2. Connect the SecureSync to a router on your LAN via ETH0 or ETH1 connector.
3. Connect the power supply to the SecureSync unit.
4. On a connected computer, open your web browser and in the URL field type the following:

   securesync-[xxxxxx].local/

   where the [xxxxxx] of the hostname are the last six digits of the MAC address.

   (If your browser doesn't recognize the information as an address, it may be necessary to add the prefix `http://` or `https://`)

   You should now connected to the unit Web UI and can login using the factory default credentials:

   Username: **spadmin**

   Password: **admin123**

Once you logged into the SecureSync 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 71 for more information.

2.12 Setting up an IP Address

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

using an address assigned by a DHCP server.

There are several ways to setup an **IP address**, described below:

- via the front panel keypad and information display
- remotely ...
  - ... via serial cable
  - ... via dedicated network cable
  - ... via a DHCP network.

Before you continue ...

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

- **Available static IP address**
  - This is the unique address assigned to the SecureSync unit by the network administrator. Make sure the chosen address is outside of the DHCP range of your DHCP server.



Note: The default static IP addresses of the SecureSync unit are:
192.168.1.1 for eth0
192.168.1.2 for eth1

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



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

2.12.1 Dynamic vs. Static IP Address

On a DHCP network (Dynamic Host Configuration Protocol), SecureSync's IP address will be assigned automatically once it is connected to the DHCP server. This negotiated address and other network information are displayed on the unit front panel when the unit boots up.

If you plan on allowing your SecureSync to use this negotiated DHCP Address on a permanent basis, you can skip the following topics about setting up an IP address, and instead proceed to "Accessing the Web UI" on page 71, in order to complete the SecureSync configuration process.

Please note:

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

SecureSync network settings default to static IP addresses. The Ethernet ports come pre-configured with IP addresses as follows:

Eth0 - 192.168.1.1

Eth1 - 192.168.1.2

Default subnet mask: 255.255.255.0

2.12.2 Assigning a Static IP Address

Safran recommends assigning a static IP address to SecureSync, even if the unit is connected to a DHCP server.

This can be accomplished in several ways:

a. Via the **keypad and information display** on the front panel of the unit, see "Setting Up an IP Address via the Front Panel" on the next page

b. By connecting the SecureSync to an existing **DHCP network**, temporarily using the assigned DHCP address, see "Setting Up a Static IP Address via a DHCP Network" on page 68.

c. By connecting a Personal Computer to SecureSync via a **serial cable**, see "Setting Up an IP Address via the Serial Port" on page 69.

d. By connecting a Personal Computer directly to SecureSync via a dedicated **Ethernet cable**, see "Setting up a Static IP Address via Ethernet Cable" on page 70.

2.12.2.1 Setting Up an IP Address via the Front Panel

Assigning an IP address to SecureSync, using the front panel keypad and information display is a preferred way to provide network access to the unit, thus enabling you thereafter to complete the setup process via the Web UI.

Note: The following instructions apply to IPv4. To configure static addresses in IPv6, you will need to use either the CLI or the front panel.

Keypad Operation

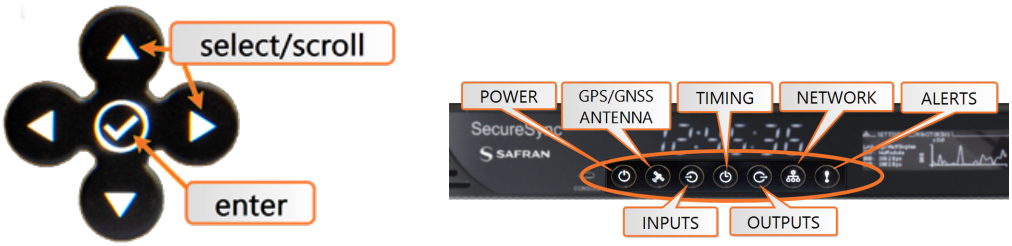


Figure 2-9: Front panel keypad and menu buttons

The functions of the keys are:

- ◀▶▲ ▼ **arrow keys**: Navigate to a menu option (will be highlighted); move the focus on the screen; switch between submenus
- ▲ ▼ **arrow keys**: Scroll through parameter values in edit displays; move the focus on the screen
- ✓ **ENTER** key: Select a menu option, or confirm a selection when editing
- **menu buttons**: Press these buttons to navigate to each of the seven main menus.

Detailed information on the front panel display menus can be found at "Front Panel Keypad, and Display" on page 6

IP configuration, step-by-step instructions:

A. **Disable DHCP:**

1. Press the **Network.Menu Button**. Ensure that you are on the Settings submenu.



2. Using the arrow key, press down once and press L/R to select the Ethernet interface for which DHCP is to be disabled, such as `eth0`.



3. Press down to highlight the current DHCP state [`ON` or `OFF`], and press ENTER to change the setting.



4. Use the arrow keys to select OFF, and press the ENTER key twice (once to enter the setting, and once to confirm when the confirmation menu appears to the right).



B. Enter **IP Address** and **Subnet Mask**:

1. Select the `IPv4 Address` row, press ENTER to allow changes, and use the up and down arrows to change `000.000.000.000/00` to the value of the static IP address and subnet mask/network bits to be assigned (for a list of subnet mask values refer to the table "Subnet mask values" on page 70).



2. Press the ✓ ENTER key once to enter the setting, then again to confirm the new setting in the confirmation menu.

C. Enter the **Gateway Address** (if required)

1. Highlight the gateway row. Press the ✓ key once to enter the setting.
2. The display will change, allowing you to input an address at `000.000.000.000`. Enter the gateway address here. The address entered must correspond to the same network IP address assigned to SecureSync.

The remainder of the configuration settings can be performed via the Web UI (accessed via an external workstation with a web browser such as Firefox® or Chrome®). For more information, see "The Web UI HOME Screen" on page 36.

2.12.2.2 Setting Up a Static IP Address via a DHCP Network

SecureSync network settings default to static IP addresses. The Ethernet ports come pre-configured with IP addresses as follows:

Eth0 - 192.168.1.1

Eth1 - 192.168.1.2

Default subnet mask: 255.255.255.0

To setup a permanent static IP address, after connecting SecureSync to a DHCP network:

1. Enter the IP address shown on the front panel information display of your SecureSync unit into the address field of your browser (on a computer connected to the SecureSync network). If the network supports DNS, the hostname may also be entered instead (the default hostname is `productname-macaddress`. See "Zero Configuration Setup " on page 62to identify your MAC address). The start screen of the SecureSync Web UI will be displayed.
2. Log into the Web UI as an administrator. The factory-default user name and password are:

   Username: `spadmin`

   Password: `admin123`
3. Disable DHCP 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 yet.
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 the next page.

5. Verify on the front panel information display that the settings have been accepted by SecureSync.
6. Enter the static IP address into the address field of the browser, and again log into the Web UI in order to continue with the configuration; see: "The Web UI HOME Screen" on page 36.

2.12.2.3 Setting Up an IP Address via the Serial Port

SecureSync's **rear** panel serial port connector is a standard RJ45 female connector. Communication with the serial port can be performed using a PC with a terminal emulator program (such as PuTTY or TeraTerm) using a pinned straight-thru standard RJ45M to DB9M serial cable.

SecureSync's **front** panel serial port connector is a standard micro-B USB female connector.

The serial ports can be used to make configuration changes (such as the network settings), retrieve operational data (e.g., GNSS receiver information) and log files, or to perform operations such as resetting the admin password.

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

To configure an IP address via the serial port:

1. Connect a serial cable to a PC running PuTTY, Tera Term, or HyperTerminal, and to your SecureSync. For detailed information on the serial port connection, see "Setting up a Terminal Emulator" on page 575
2. Login to SecureSync with a user account that has “admin” group rights, such as the default `spadmin` account (the default password is `admin123`).
3. Disable DHCP, type: `dhcp4set X off` <Enter>, where `X` is the Ethernet port you wish to configure (Eth0, Eth1).

   Note: For a list of CLI commands, type `helpcli`, or see "CLI Commands" on page 577.

4. Configure the IP address and subnet mask, type:
   - `ip4set x y.y.y.y z.z.z.z` <Enter>
     (where `x` is the desired interface (eth0, eth1), “`y.y.y.y`” is the desired

IP address for SecureSync, and "`z.z.z.z`" is the full subnet mask for the network (For a list of subnet mask values, see "Subnet Mask Values" below.)

5. Configure the gateway by typing `gw4set x y.y.y.y` <Enter> (where `x` indicates the interface routing table to add the default gateway (eth0, eth1), and "`y.y.y.y`" is the default gateway address).
6. Remove the serial cable, connect SecureSync to the network, and access the Web UI, using the newly configured IP address. (For assistance, see "Accessing the Web UI" on the facing page).

The remainder of the configuration settings will be performed via the Web UI (accessed via an external workstation with a web browser such as Firefox® or Chrome®).

2.12.2.4 Setting up a Static IP Address via Ethernet Cable

This procedure will allow you to configure SecureSync using the Web UI directly via the Ethernet port, if you cannot or do not wish to use a DHCP network.

1. First, **disable DHCP** using the front panel keypad and information display: see "Setting Up an IP Address via the Front Panel" on page 66.
2. Change the workstation IP address to be on the same network as SecureSync.
3. Connect workstation and SecureSync with an Ethernet cable.

The remainder of the configuration settings will be performed via the Web UI (accessed via an external workstation with a web browser such as Firefox® or Chrome®). For more information, see "The Web UI HOME Screen" on page 36.

2.12.3 Subnet Mask Values

Table 2-3: 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

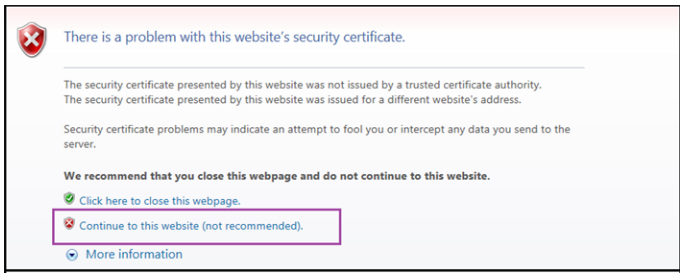
Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		

2.13 Accessing the Web UI

SecureSync's web user interface ("Web UI") is the recommended means to interact with the unit, since it provides access to nearly all configurable settings, and to obtain comprehensive status information without having to use the Command Line Interpreter (CLI).

You can access the Web UI either by using the automatically assigned DHCP IP address, or by using a manually set static IP address (see "Assigning a Static IP Address" on page 65):

1. On a computer connected to the SecureSync network, start a web browser, and enter the IP address shown on the SecureSync front panel.
2. When first connecting to the Web UI, a warning about security certificates may be displayed:



Select **Continue...**.

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

> **Note:** HTTPS only: Depending on your browser, the certificate/security pop-up window may continue to be displayed each time you open the Web UI until you saved the certificate in your browser.

> **Note:** Static IP address only: To prevent the security pop-up window from opening each time, a new SSL Certificate needs to be created using the assigned IP address of SecureSync during the certificate generation. See "HTTPS" on page 80 for more information on creating a new SSL certificate.

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

   Username: `spadmin`

   Password: `admin123`

   > **Caution:** For security reasons, it is advisable to change the default credentials, see: "Managing Passwords" on page 294.

4. Upon initial login, you will be asked to register your product. Safran recommends to register SecureSync, so as to receive software updates and services notices. See also "Product Registration" on page 321.

Number of login attempts

The number of failed login attempts for ssh is hard-set to (4) four. This value is not configurable.

The number of failed login attempts for the Web UI (HTTP/HTTPS) is hard-set to (5) five failed login attempts, with a 60 second lock. These two values are not configurable.

To continue with the configuration, see e.g., "The Web UI HOME Screen" on page 36.

To learn more about setting up different types of user accounts, see "Managing User Accounts" on page 290.

2.14 Configure Network Settings

Before configuring the network settings, you need to setup access to SecureSync web user interface ("Web UI"). This can be done by assigning a static IP address, or using a DHCP address. For more information, see "Setting up an IP Address" on page 63.

Once you have assigned the IP address, login to the Web UI. For more information, see "Accessing the Web UI" on page 71.

To configure network settings, or monitor your network, navigate to SecureSync'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 SecureSync to a network. See "General Network Settings" on page 75.
- **Web Interface Settings**:
  - Web interface **timeout**: Determines how long a user can stay logged on. For more information, see "Web UI Timeout" on page 298.
  - Web **Security Level**: High security will not allow browsers to use TLS below v1.3 (to prevent known security vulnerabilities).

- **Access Control**: Allows the configuration of access restrictions from assigned networks/nodes.
- **Login Banner**: Allows the administrator to configure a custom banner message to be displayed on the SecureSync Web UI login page 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 110.
- **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 112.

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 SecureSync's network ports via three buttons:

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

2.14.1 HSTS Setup

HTTP Strict Transport Security (HSTS) support is available for SecureSync.

To configure HSTS, navigate to **MANAGEMENT** > **Network Setup**. In the Actions Panel, select **Web Interface Settings**.

Select the Security Level tab to configure HSTS. The default is set to 31536000s. Max Age: 2147483647s. Disabled: 0.

For more information on HSTS requirements, refer to https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security.

2.14.2 General Network Settings

To expedite network setup, SecureSync 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.

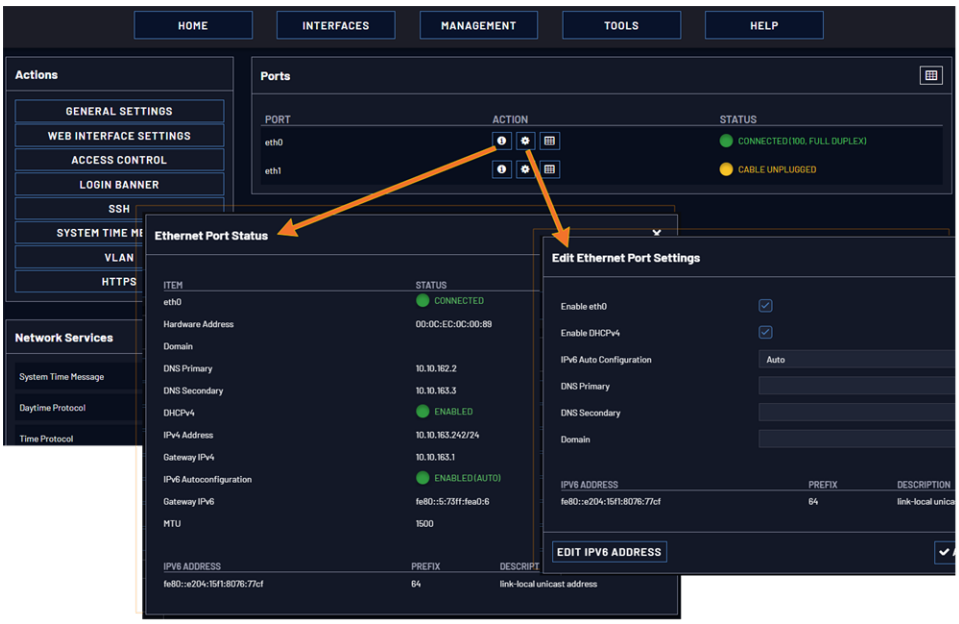
2.14.3 Network Ports

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.
     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 70 for a list of subnet mask values.
   - **IPv4 Gateway**: The gateway (default router) address is needed if communication to the SecureSync is made outside of the local network. By default, the gateway is disabled.

- **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].
- **Edit IPv6 Address**: Click on this button to configure a static IPv6 address.

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

2.14.4 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
- **tcpdump**: A LINUX program that can be used to monitor network traffic by inspecting tcp packets. Default = ON.
  If not needed, or wanted (out of concern for potential security risks), **tcpdump** can be disabled permanently: Once toggled to OFF, and after executing a page reload, **tcpdump** will be deleted from the system: The toggle switch will be removed, and the function cannot be enabled again (even after a software upgrade) 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 166).



Note: A listing of recommended and default network settings can be found under "Default and Recommended Configurations" on page 368.

2.14.5 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 70.
     - **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.

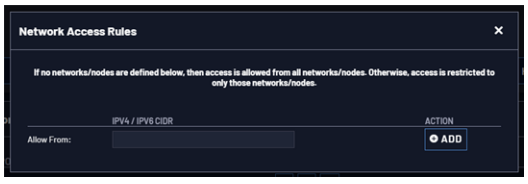
2.14.6 Access Rules

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 70 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.

2.14.7 HTTPS

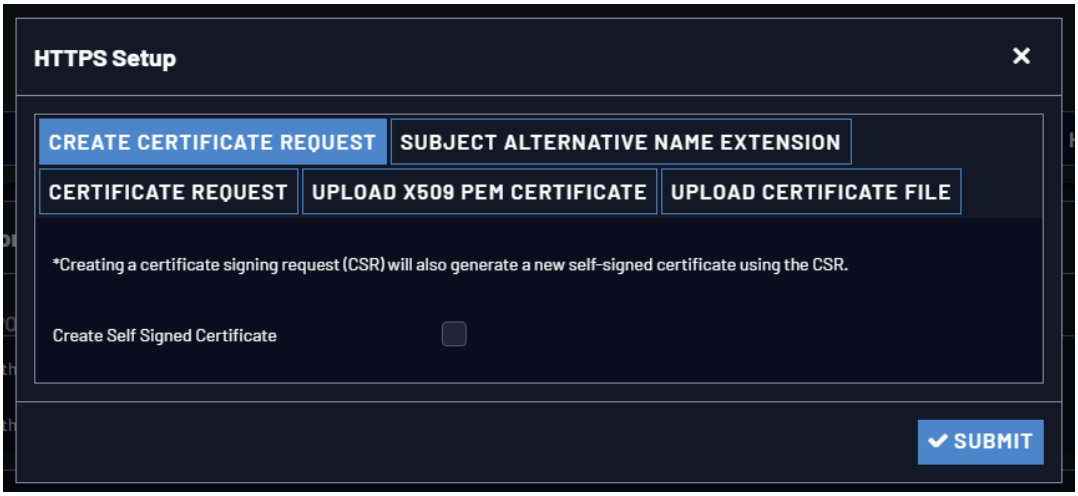
HTTPS stands for HyperText Transfer Protocol over SSL (Secure Socket Layer). This TCP/IP protocol is used to transfer and display data securely by adding an encryption layer to protect the integrity and privacy of data traffic. Certificates issued by trusted authorities are used for sender/recipient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

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

Note that SecureSync supports two different modes of HTTPS operation: The **Standard HTTPS Level** (default), and a **High-Security Level**. For more information, see "HTTPS Security Levels" on page 316.

2.14.7.1 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 SecureSync.
- **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.

2.14.7.2 About HTTPS

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

SecureSync 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.

2.14.7.3 Supported Certificate Formats

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

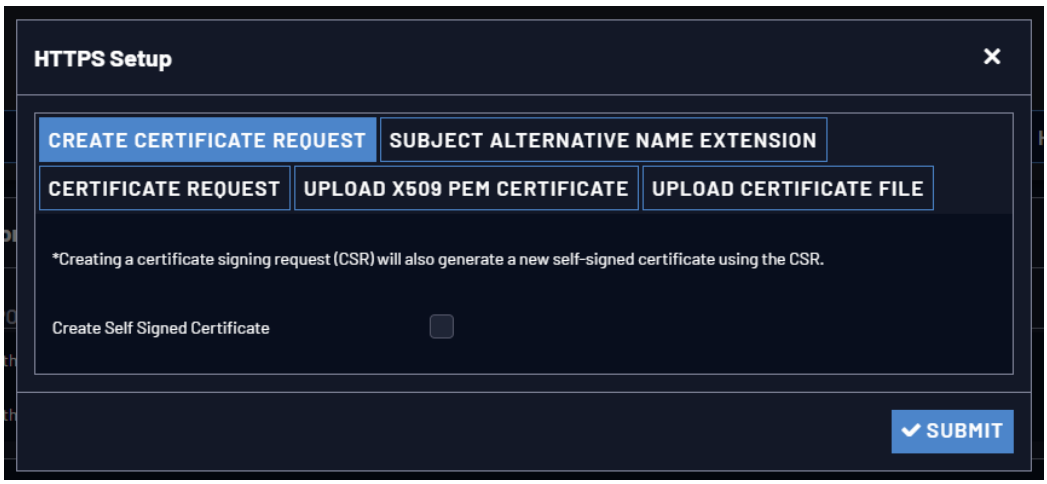
You can create a unique X.509 self-signed Certificate, an RSA private key and X.509 certificate request using the Web UI. RSA private keys are supported because they are the most widely accepted. At this time, DSA keys are not supported.

2.14.7.4 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 SecureSync 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 312.

   - **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.

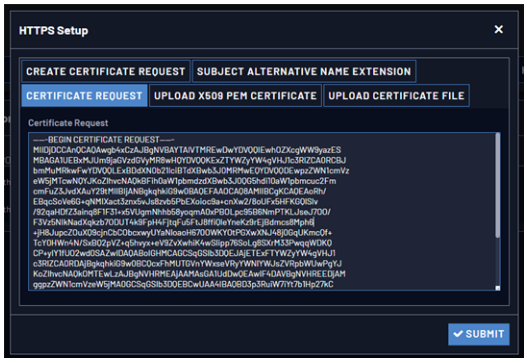
When using a self-signed Certificate, choose values based on your company's security policy.

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 SecureSync 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.

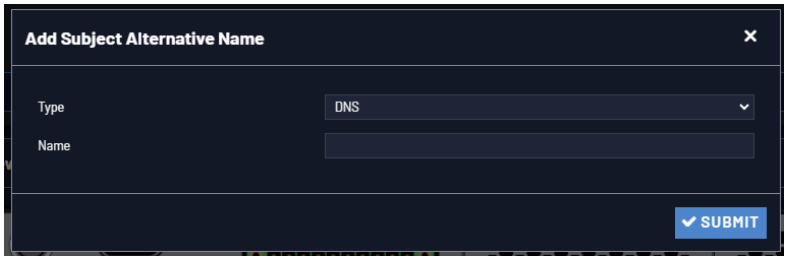
2.14.7.5 Adding HTTPS Subject Alternative Names

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.



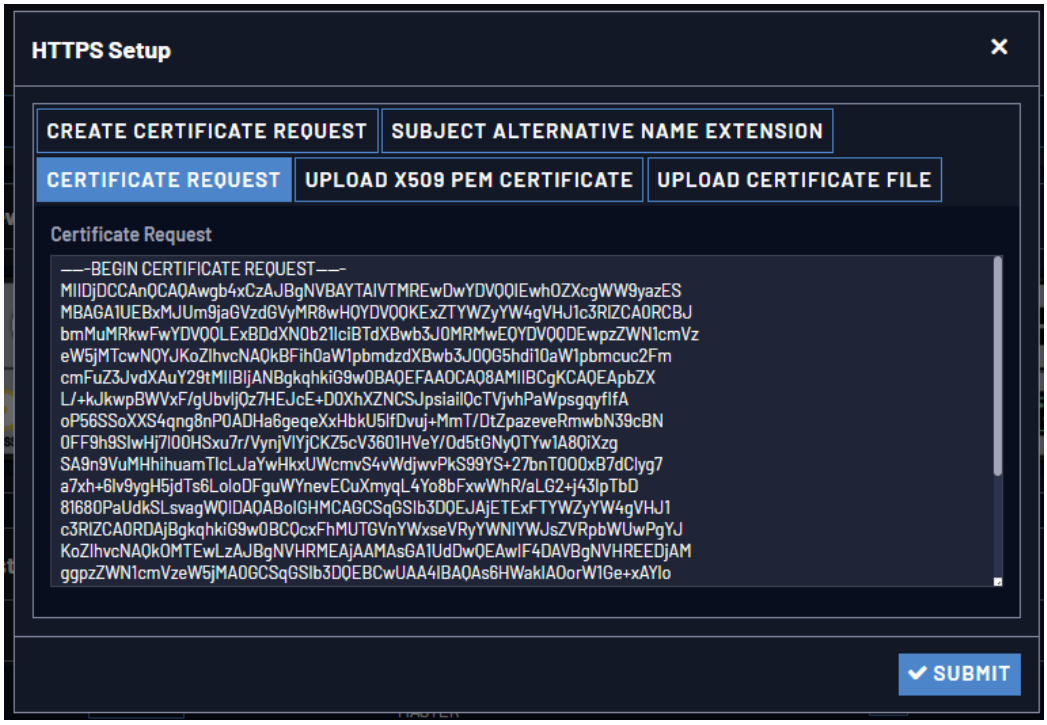
3. Fill in the available fields:
   - **Type** [DNS, IP, email, URI, RID, dirName]
   - **Name**
   - for Directory Subject Alternative Names (**dirName**), check the Directory Name box, and additional optional fields will be available:
     - Two Letter Country Code: must match ISO-3166-1 value.
     - 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.

2.14.7.6 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 SecureSync 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.

2.14.7.7 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.

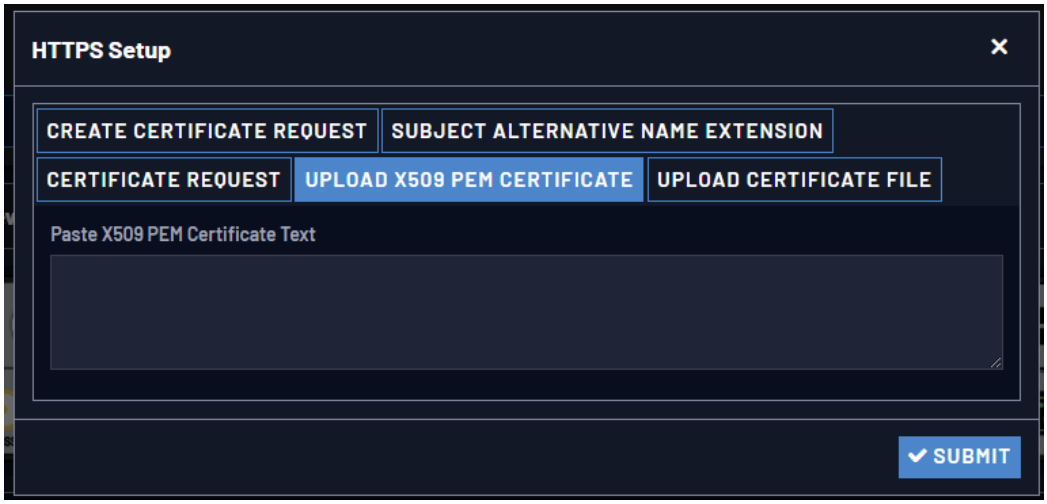
Certificate Chain

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 SecureSync:

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 SecureSync.

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

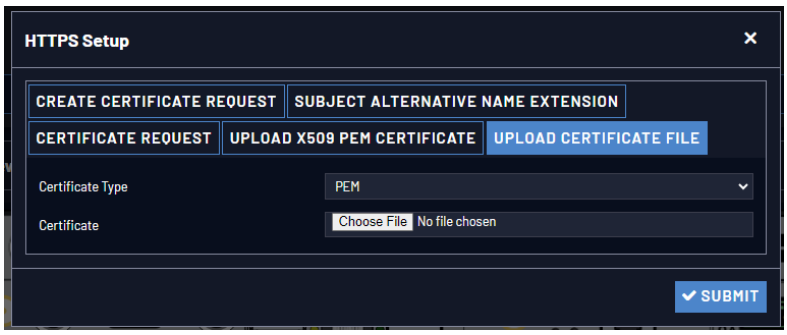
2.14.7.8 Uploading an HTTPS Certificate File

Once the HTTPS Certificate has been issued by your Certificate Authority, you have to upload the Certificate file to SecureSync, 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 SecureSync:

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:** SecureSync 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.

2.14.8 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 SecureSync are:

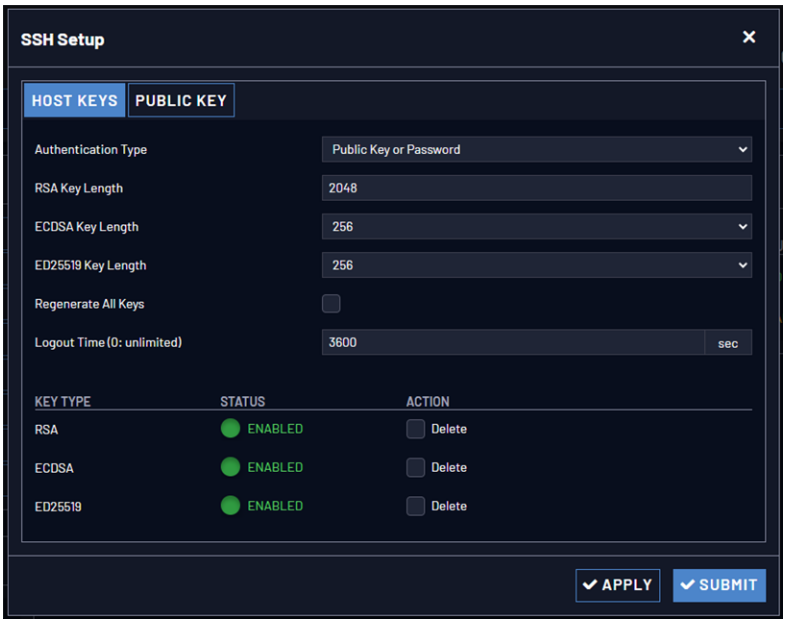
- **SSH**: Secure Shell
- **SCP**: Secure Copy
- **SFTP**: Secure File Transfer Protocol

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

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

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.

SecureSync units have their initial host keys created at the factory. RSA host key sizes can vary between 768 and 4096 bits. The recommended key size is 1024. Though many key sizes are supported, it is recommended that users select key sizes that are powers of 2 or divisible by 2. The most popular sizes are 768, 1024, and 2048. Large key sizes 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 SecureSync 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 SecureSync regenerates the keys. The Host keys are generated in the background. Creating RSA and DSA keys, each with 1024 bits length, typically takes about 30 seconds. Keys are created in the order of RSA, DSA, ECDSA, ED25519. SecureSync 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 SecureSync. This public key must match the private key found in the users account and be accessible to the SSH, SCP, or SFTP client program. The user must then enter the Passphrase after authentication of the keys to provide the second factor for 2-factor authentication.

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

Public Keys: Viewing, Editing, Loading

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

If 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 SecureSync. 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

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

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

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

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

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

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

Perform an SCP file transfer 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).

2.14.9 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).

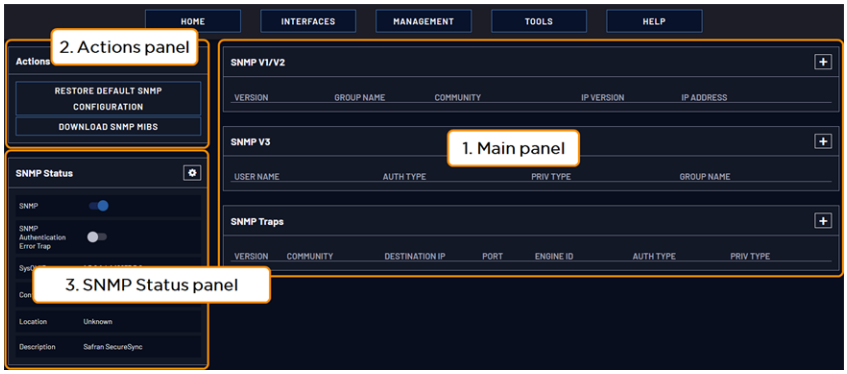
SecureSync's SNMP functionality supports SNMP versions V1, V2c and V3 (with SNMP Version 3 being a secure SNMP protocol).

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 106.

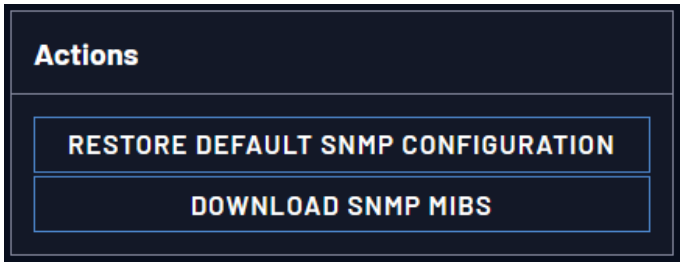
- **SNMP Traps**: This panel allows you to define different SNMP Managers that SNMP traps can be sent to over the network. This allows for SNMP Managers in different geographical areas to receive the same SNMP traps that Managers in other areas also receive. Clicking the PLUS icon in the top-right corner opens the SNMP Traps Settings Screen. See also "SNMP Traps" on page 107 and "Setting Up SNMP Notifications" on page 287.

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 SecureSync 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.

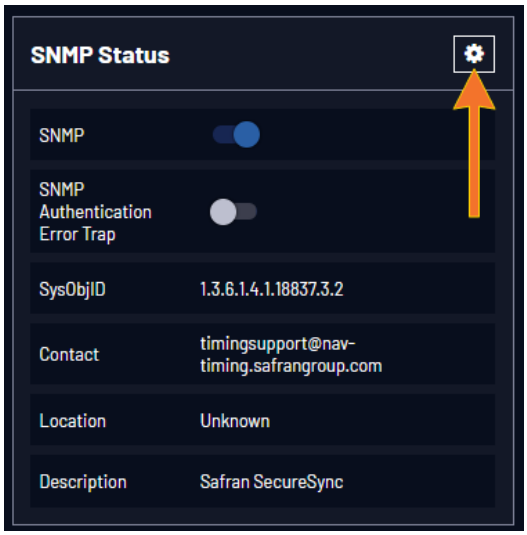


3. Confirm that you want to restore the default settings in the pop-up message.

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 SecureSync 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 SecureSync, using an FTP client such as FileZilla or any other shareware/freeware FTP program.

Note: Current SecureSync 2400 Time and Frequency Synchronization System software requires SFTP to ensure increased security.

To obtain the MIB files from SecureSync 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 SecureSync 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 SecureSync and it provides traps to notify the user when it starts, restarts, or shuts down. These MIB files may also be compiled into your SNMP manager, if they are not already present.

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.

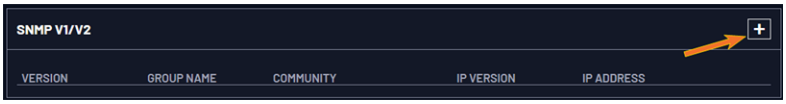
Note: By default, TimingSupport@nav-timing.safrangroup.com is the address in the sysContact field of the SNMP Status panel of the SNMP Setup page.

2.14.9.1 SNMP V1/V2c

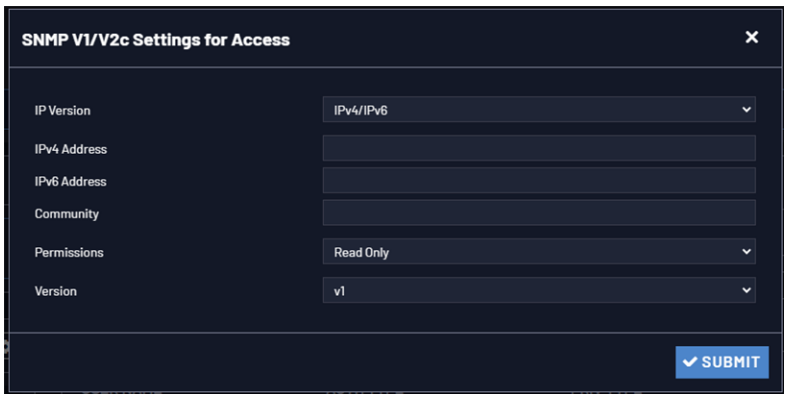
SNMP V1 is the first version of the SNMP protocol, as defined in the IETF (Internet Engineering Task Force) RFCs (Request for Comments) number 1155 and 1157. SNMP V2c is the revised protocol, but it also uses the V1 community based administration model.

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, SecureSync uses the system default address.
   - SNMP **Community** names should be between 4 and 32 characters in length.
   - **Permissions** may be Read Only or Read/Write.
   - The **Version** field provides a choice of V1 or V2c.
5. Click **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.

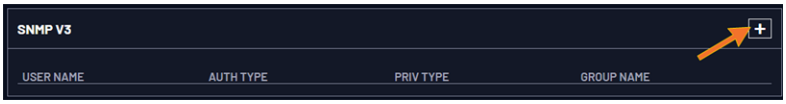
4. To edit the settings, enter the new details you want to edit and click **Submit**. OR: To delete the entry, click **Delete**.

2.14.9.2 SNMP V3

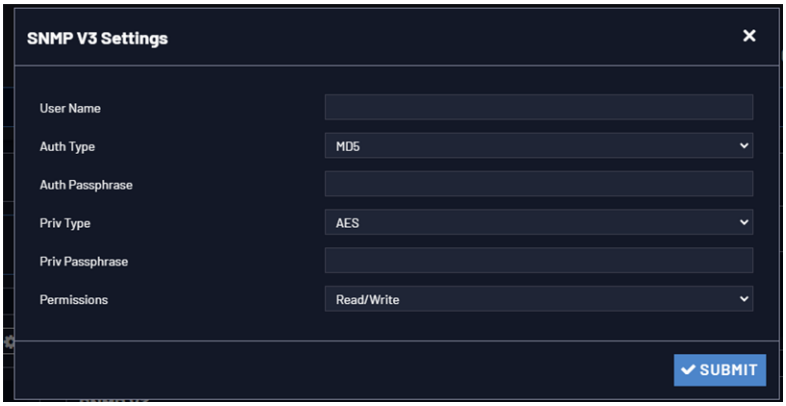
SNMP V3 utilizes a user-based security model which, among other things, offer enhanced security over SNMP V1 and V2.

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 SecureSync and on the management station.
- The **Auth Type** field provides a choice between MD5 and SHA.
- The **Auth Password** must be between 8 and 32 characters in length.
- The **Priv Type** field provides a choice between AES, 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.

2.14.9.3 SNMP Traps

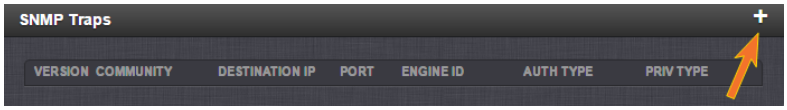
SNMP traps allow for automatic event notification, and as such are one way to remotely monitor SecureSync's status.

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 SecureSync data object that is related to the specific trap that was sent. For example, when a Holdover trap is sent because SecureSync either entered or exited the Holdover mode, the trap varbind will indicate that SecureSync is either currently in Holdover mode or not currently in Holdover mode.

For testing purposes, a command line interface command is provided. This command, `sendtrap`, allows one, several, or all of the traps defined in the SecureSync MIB to be generated. Refer to "CLI Commands" on page 577 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.



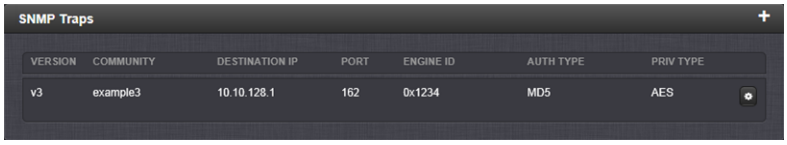
3. The **SNMP Traps Settings** window will display:



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]
- 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 SecureSync, please refer to the SecureSync MIB files. See "Accessing the SNMP Support MIB Files" on page 103.

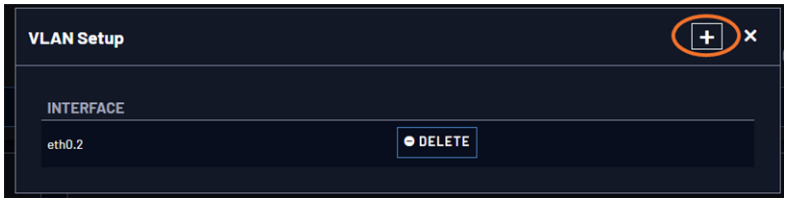
[1] If your SNMP manager is not providing an Engine ID, you can generate one yourself according to protocols within RFC 3411 and apply it to your network manager and trap configuration.

2.14.10 VLAN Support

VLAN support in SecureSync 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-eth1], 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].

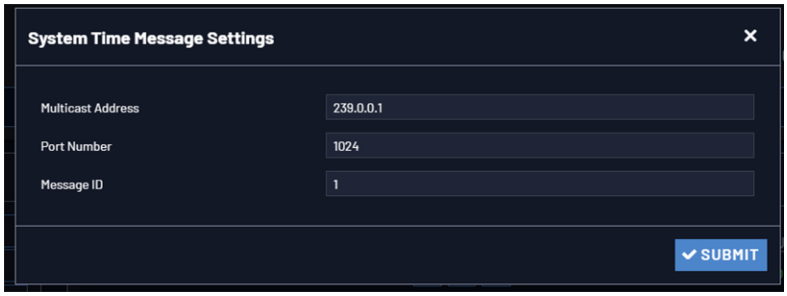
2.14.11 System Time Message

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

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

1. Navigate to **MANAGEMENT** > **Network Setup > Actions** panel, and select **System Time Message**. The **Settings** window will open.

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



2.14.11.1 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 2-4: 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 2-5: System Time Message field descriptions

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

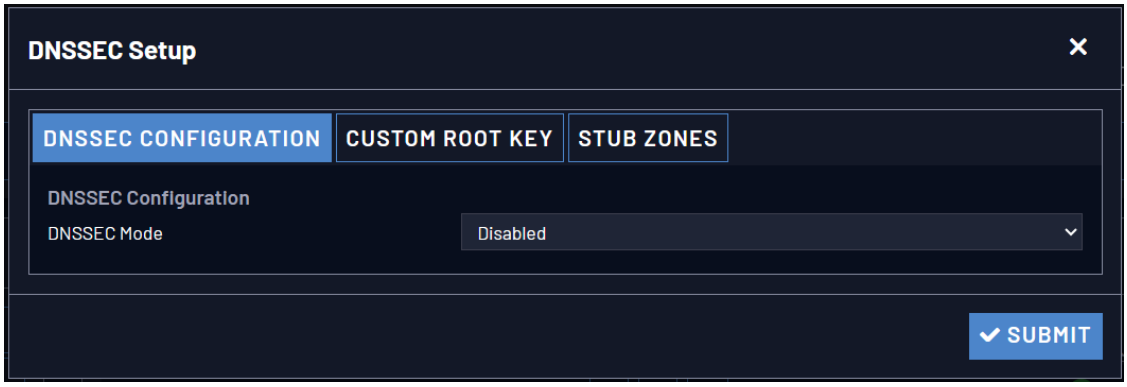
It is also possible to use the System Time Message to send NMEA over UDP. For more information about this functionality, see the NMEA over UDP App Note.

2.14.12 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 SecureSync 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.

2.15 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 MD5 authentication 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, SecureSync will "listen" for NTP request messages from NTP clients on the network. When an NTP request packet is received, SecureSync will send an NTP response time packet to the requesting client. Under typical conditions, SecureSync can service 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.

2.15.1 Checklist NTP Configuration

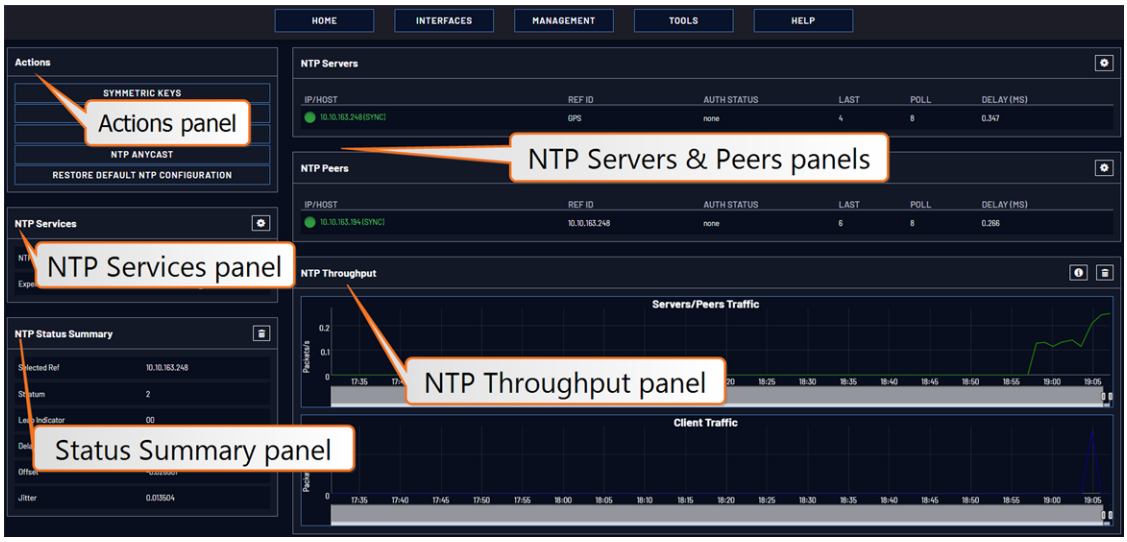
The following is a list of configuration settings you may want to consider as you setup your NTP Service. (Not all items may apply to your application, or there may be other considerations not included in this list.)

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.

2.15.2 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 SecureSync 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 SecureSync 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 123.

The NTP Throughput panel

... shows two graphs depicting the rate of NTP traffic from Clients and Servers/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 SecureSync 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 SecureSync's NTP settings to the factory default. Any settings you have created previously will be lost. See "Restoring the Default NTP Configuration" on page 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" on the facing page.



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 SecureSync Web UI. [Default =OFF] See "NTP Expert Mode" on page 151.



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 339.

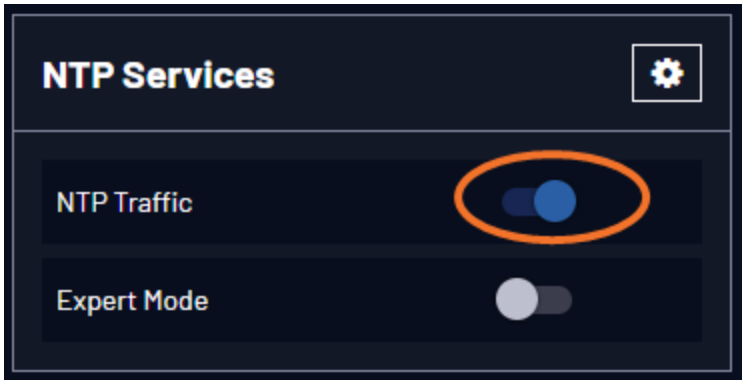
2.15.3 Dis-/Enabling NTP

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

You can, however, also disable or enable the SecureSync NTP Service manually.

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.



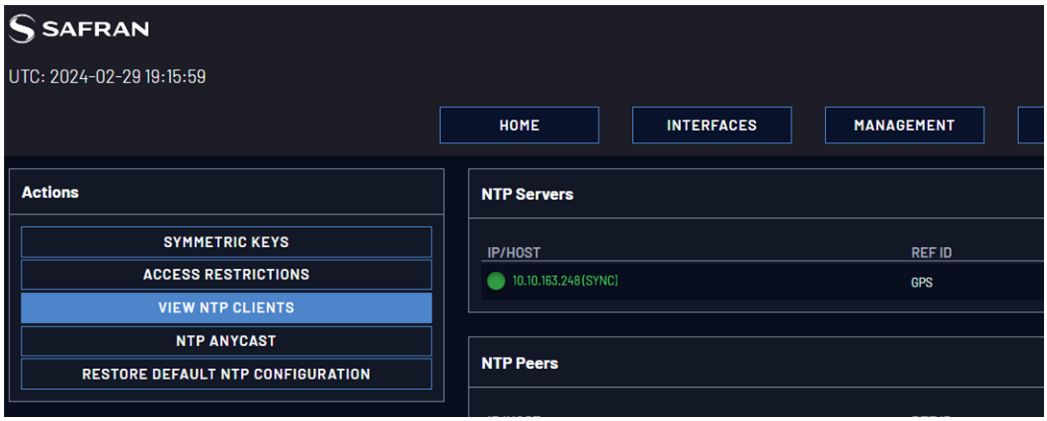
3. A notification window will confirm the status change.
4. In the **NTP Services** panel, set the ON/OFF toggle switch to ON again.

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

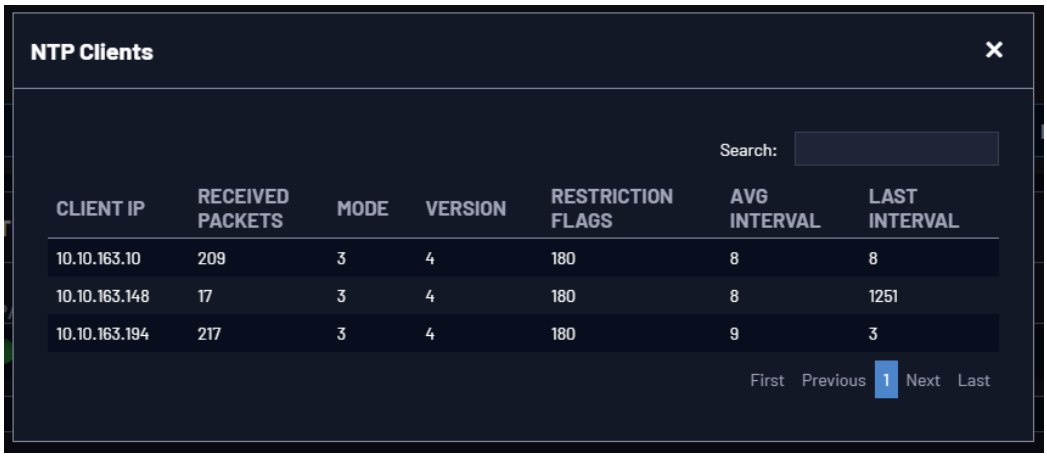
2.15.4 Viewing NTP Clients

To view the NTP clients being served by SecureSync:

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



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



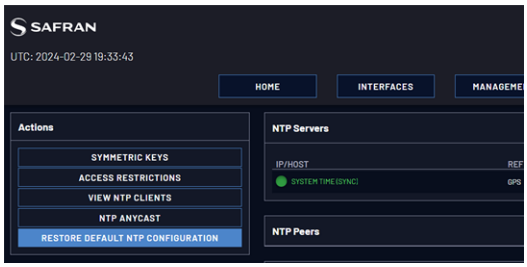
- You can search any of the fields for specific information in the Search field at the top of the window.
- A limit of 10 entries will appear on the screen at any one time. If you have more than 10 clients, you can move through the table using the **First**, **Previous**, **Next** and **Last** navigation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

2.15.5 Restoring the Default NTP Configuration

The SecureSync 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 SecureSync 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**.

2.15.6 NTP Output Timescale

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

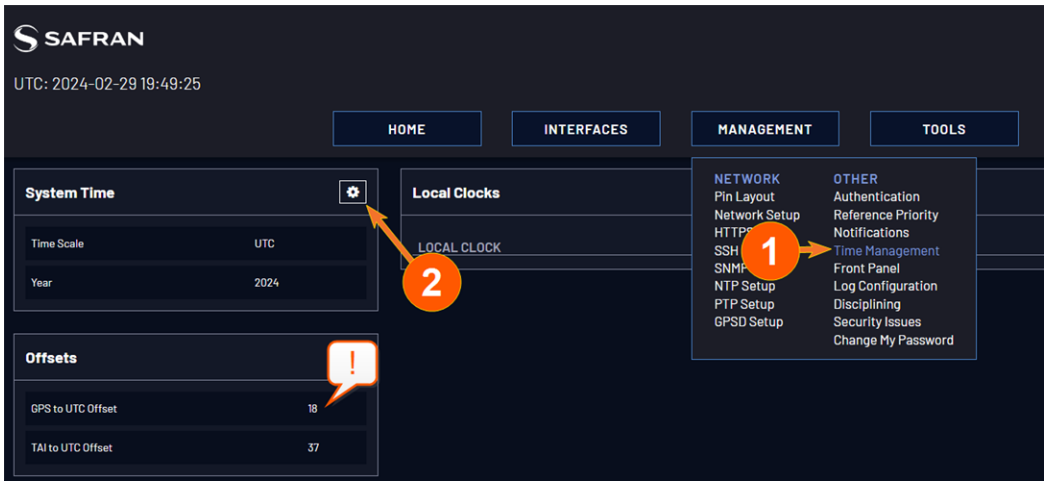
Note that the **System Time** affects not only NTP output, but also all other aspects of time management e.g., time distributed via channels other than NTP, logging, and time displayed in the Web UI.

If SecureSync is operated as a Stratum 2 server, i.e. as a client to a Stratum 1 server (see "Configuring "NTP Stratum Synchronization"" on page 122), the other server will override SecureSync'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 SecureSync 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 SecureSync 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.

2.15.7 NTP Reference Configuration

SecureSync'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 SecureSync'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 SecureSync will be the Stratum 1 (or primary) server. This is the most common configuration.

2.15.7.1 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 SecureSync 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 SecureSync unit as a time reference.

2.15.7.2 Configuring "NTP Stratum 1" Operation

When the Timing System references of your SecureSync 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 SecureSync operates as a **Stratum 1** NTP server.

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

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.

2.15.7.3 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 SecureSync you are configuring a **Stratum 2** server, since the other server is Stratum 1.

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

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 SecureSync'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.

2.15.8 NTP Servers and Peers

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

If SecureSync 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, SecureSync 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, SecureSync will then drop to a **Stratum 2** time server (with System Time being derived from the NTP time packets being received from the other NTP Peers.

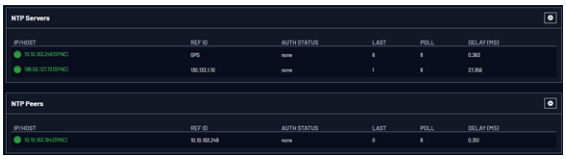
Holdover

If SecureSync 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), SecureSync 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 SecureSync as an NTP time reference.

For more information about Holdover, see "Holdover Mode" on page 265.

2.15.8.1 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 SecureSync 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

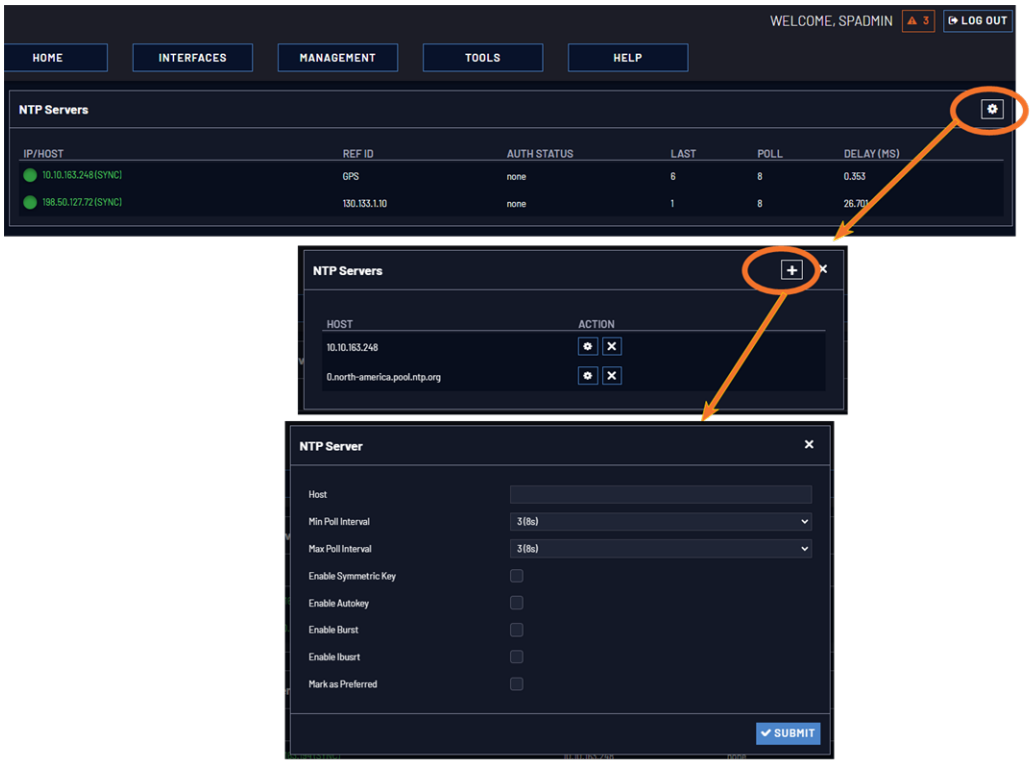
- **ATC**: ASCII time code reference
- **USER**: User provided time
- **LOCL**: Local reference (synced to itself)
- **INIT**: NTP on server/peer is initializing
- **STEP**: NTP on server/peer is performing initial synchronization step and restarting

- **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 SecureSync is polling this NTP reference for its time.
- **DELAY (ms)**: The measured one-way delay between SecureSync and its selected reference.

2.15.8.2 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 219.

   » 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 SecureSync and the NTP Peer or NTP Server. If the Symmetric Key-ID/Key string pair method is selected the Key-ID must be first defined on the Symmetric Key page.
   - **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.

2.15.8.3 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.

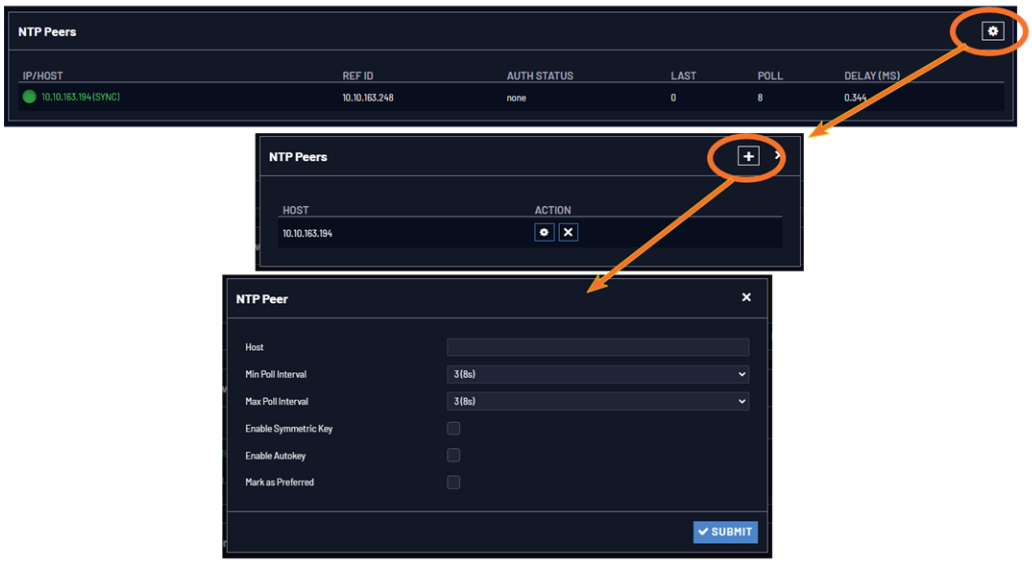
> **Note:** Should the list be empty, no servers have been added yet. In the event that added peers are not displayed, they could not be resolved. Verify the IP address

» 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.

   - **Mark as Preferred**: Check this box to prefer this NTP Peer over other NTP Peers ("NTP Peer Preference"). This will result in SecureSync 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 SecureSync will not prevent you from doing so.

5. Click Submit, or press Enter.

2.15.9 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.

2.15.9.1 NTP Autokey

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

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

NTP Autokey: IFF Autokey Support

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

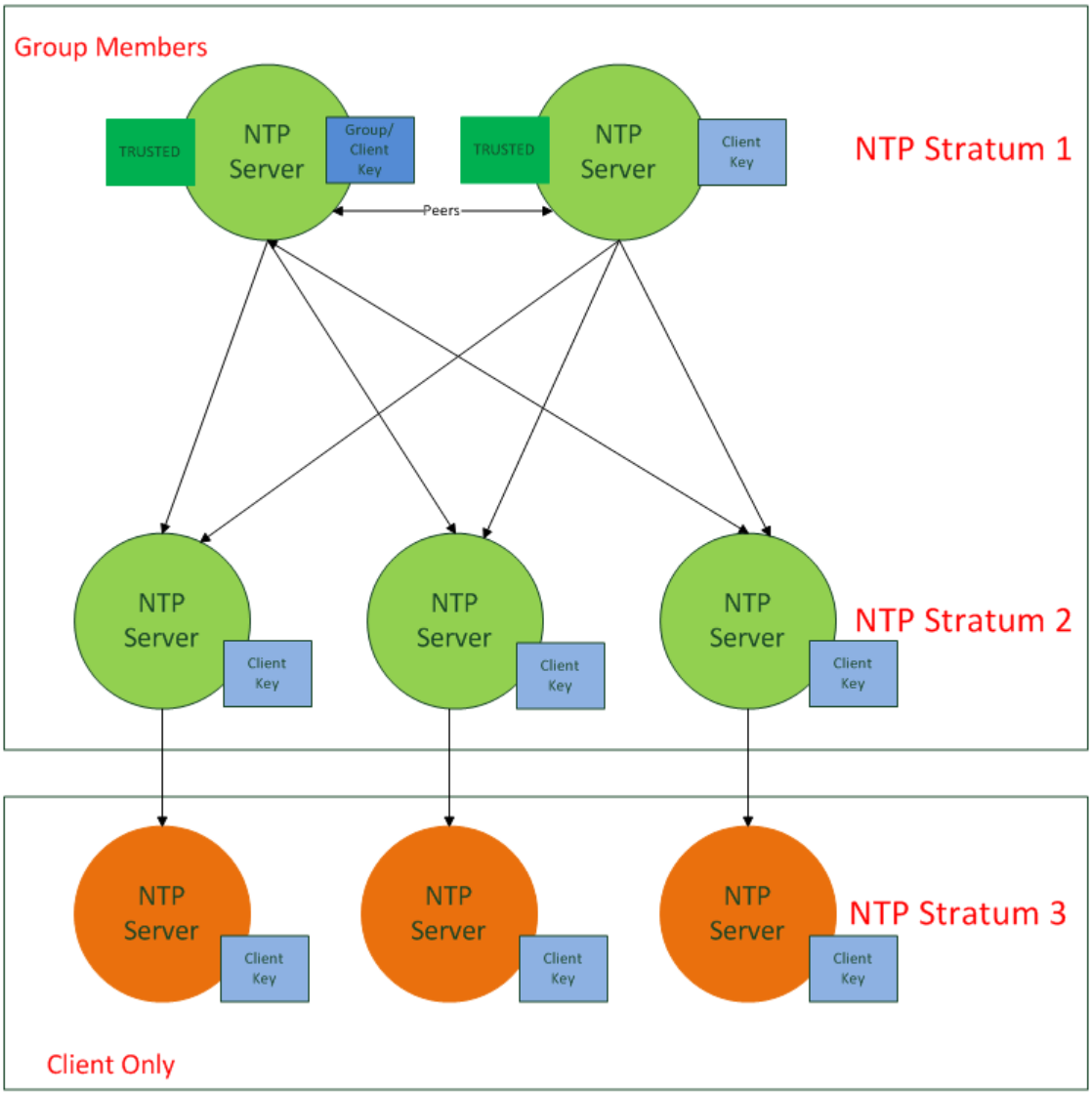


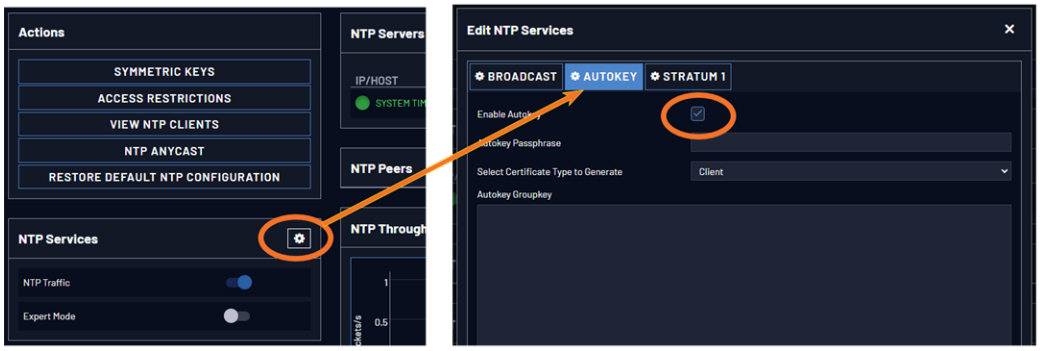
Figure 2-10: IFF Autokey configuration example

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 117.

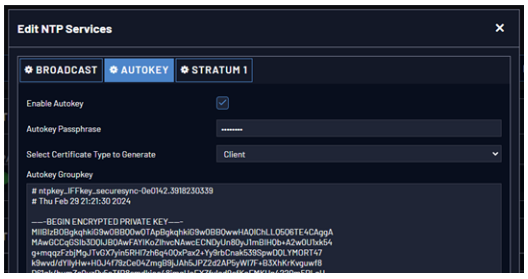
To configure NTP Autokey:

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

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 SecureSync 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 75.
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.

2.15.9.2 NTP: Symmetric Keys (MD5)

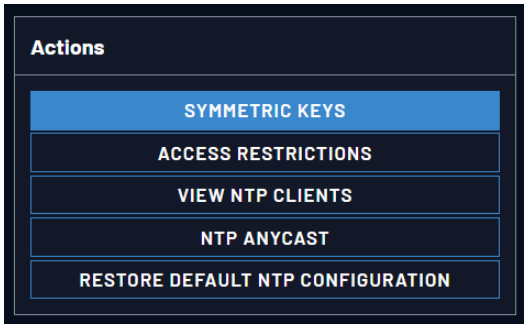
Symmetric Keys are an encryption means that can be used with NTP for authentication purposes.

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

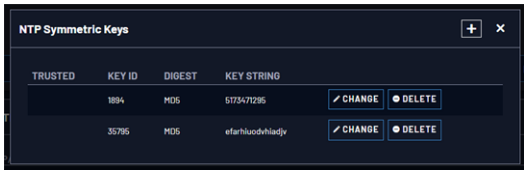
Configuring NTP Symmetric Keys

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 SecureSync 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.

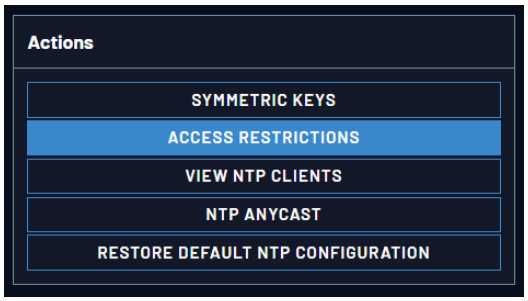
You may define the trusted Symmetric Keys that must be entered on both SecureSync, and any network client with which SecureSync is to communicate. Only those keys for which the "Trusted" box has been checked will appear in the dropdown menus on the **NTP References** screen.

2.15.10 NTP Access Restrictions

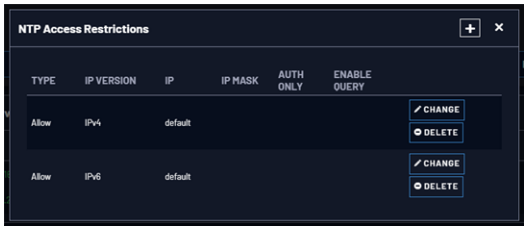
Next to encrypted authentication by means of Symmetric Keys, NTP supports a list-based means of access restriction, the use of which is also recommended to prevent fraudulent or inadvertent manipulation of a time server.

To configure NTP Access Restrictions:

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

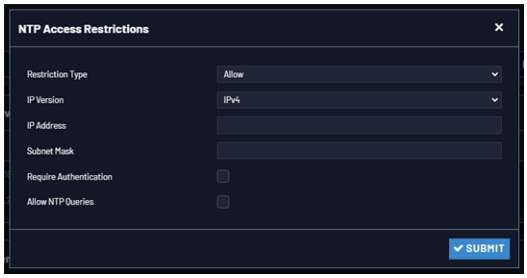


3. The **NTP Access Restrictions** Status window will display:



- 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 SecureSync, but the rest of the network will have access to SecureSync. If you select "allow", the configured portion of the network will have NTP access to SecureSync, but the rest of the network will not have access to SecureSync. By default, SecureSync 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. SecureSync to accept only authenticated requests (MD5) from this user or network segment.
     - **Allow NTP Queries** (checkbox)—Check this box if you want to allow external NTP queries into SecureSync services.
5. Click the **Submit** button.

2.15.11 Enabling/Disabling NTP Broadcasting

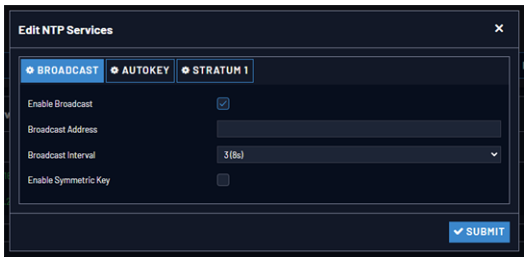
The NTP Broadcast mode is intended for one or a few servers and many clients. SecureSync allows the NTP service to be configured to broadcast the NTP time only to the network's broadcast address at scheduled intervals.

NTP Broadcasting is used to limit the NTP service to only certain clients on the network. NTP Broadcasting also reduces the amount of network traffic, but is therefore less accurate since there is no compensation for cable delays, or other delays between NTP Server and Client.

Note that NTP Broadcasting is rarely used and typically limited to special applications.

To enable NTP Broadcasting:

1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**.
2. On the **NTP Services** panel, click the GEAR icon.
3. The **Edit NTP Services** window will display. Check the **Broadcast** box.



4. Select a **Broadcast Interval**. When NTP Broadcasting is selected, in addition to still responding to NTP time requests sent from network appliances, SecureSync will also send unsolicited NTP time packets to the local broadcast address at the Broadcast Interval specified by you.
5. To utilize **MD5 Authentication**, select a **Symmetric Key** (see "Configuring NTP Symmetric Keys" on page 136.)
6. Click Submit, or press Enter.

To disable NTP broadcasting, simply uncheck the **Broadcast** box and click **Submit**.

2.15.12 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 SecureSync, is a combination of the two concepts, allowing SecureSync to:

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

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

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

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

OSPF Protocol EXAMPLE:

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

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

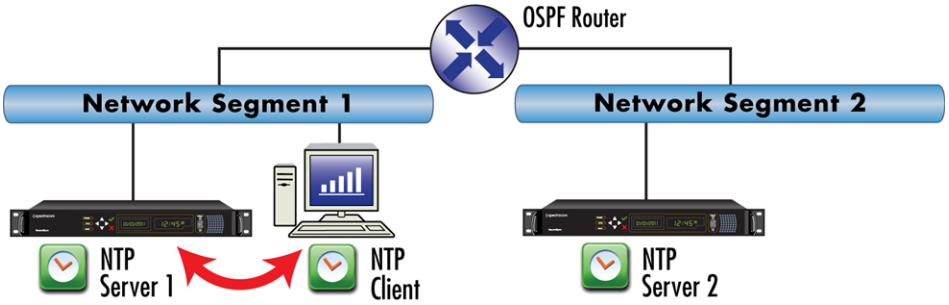


Figure 2-11: All NTP Servers are synchronized

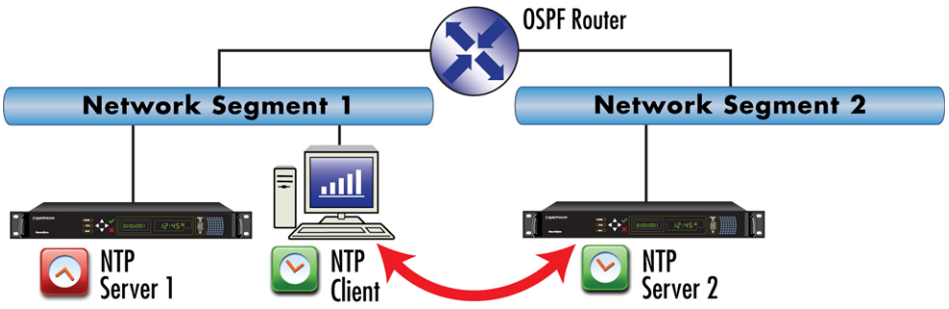


Figure 2-12: NTP Server 1 is out of sync

2.15.12.1 Configuring NTP over Anycast (General Settings)

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

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

4. In the **NTP Anycast** window, select the **General** tab.
5. On the **General** tab, select the **IP Version** you will be running Anycast service for. The options are IPv4, IPv6, or both.
6. Configure the **Anycast Address** to be used.
7. Select the port to associate the Anycast service with (depending on the option card configuration of your unit, there may be only ETH0 available). If you desire IPv6 functionality, you must also select the IPv6 port address since there may be multiple IPv6 addresses on a single port.
8. 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, SecureSync 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.

2.15.12.2 Configuring NTP over Anycast (OSPF IPv4)

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

1. Confirm that your existing network infrastructure is Anycast capable, and uses OSPF Version 2 (IPv4). Determine the OSPF area.
2. In the SecureSync Web UI, navigate to **MANAGEMENT** > **Network** > **NTP Setup**.

3. In the **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 SecureSync's accuracy "tolerance window": A small window will cause SecureSync to deliver a more accurate time window, but also will cause it to quickly withdraw from the Anycast server pool, i.e. declare itself an invalid reference. (For more information about TFOM, see "Configuring the Oscillator" on page 271.)
    Navigate to **Management** > **Disciplining**, and click the GEAR icon in the top-right corner of the **Status** panel.
14. Set the value **Maximum TFOM for Sync** to 4 (this will make SecureSync to go out of sync if the phase error is greater than 1µs).
15. Set the value for **Holdover Timeout** to 10 s, to allow SecureSync to exit holdover quickly.
16. Leave the **Phase Error Limit** at 0, and do not check any of the checkboxes (or, for more information, see "Configuring the Oscillator" on page 271).

2.15.12.3 Configuring NTP over Anycast (OSPF IPv6)

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

1. Confirm that your existing network infrastructure is Anycast capable, and uses OSPF Version 3 (IPv6). Determine the OSPF area.
2. In the SecureSync Web UI, navigate to **MANAGEMENT** > **Network** > **NTP Setup**.

3. In the **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 SecureSync's accuracy "tolerance window": A small window will cause SecureSync to deliver a more accurate time window, but also will cause it to quickly withdraw from the Anycast server pool, i.e. declare itself an invalid reference. (For more information about TFOM, see "Configuring the Oscillator" on page 271.)
    Navigate to **Management** > **Disciplining**, and click the GEAR icon in the top-right corner of the **Status** panel.
14. Set the value **Maximum TFOM for Sync** to 4 (this will make SecureSync to go out of sync if the phase error is greater than 1µs).
15. Set the value for **Holdover Timeout** to 10 s, to allow SecureSync to exit holdover quickly.
16. Leave the **Phase Error Limit** at 0, and do not check any of the checkboxes (or, for more information, see "Configuring the Oscillator" on page 271).

2.15.12.4 Configuring NTP over Anycast (BGP)

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

1. Confirm that your existing network infrastructure is Anycast capable, and uses BGP. Determine the network specifics, such as your Autonomous

System (AS) number, Neighbor's address and Neighbor's AS number.

2. In the SecureSync Web UI, navigate to **MANAGEMENT > Network > NTP Setup.**
3. In the **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 SecureSync's accuracy "tolerance window": A small window will cause SecureSync to deliver a more accurate time window, but also will cause it to quickly withdraw from the Anycast server pool, i.e. declare itself an invalid reference. (For more information about TFOM, see "Configuring the Oscillator" on page 271.)
    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 SecureSync 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 SecureSync 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 271).

2.15.12.5 Configuring Anycast via NTP Expert Mode

Advanced Anycast configuration is possible via the **NTP Expert Mode** (see also "NTP Expert Mode" on page 151), 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.



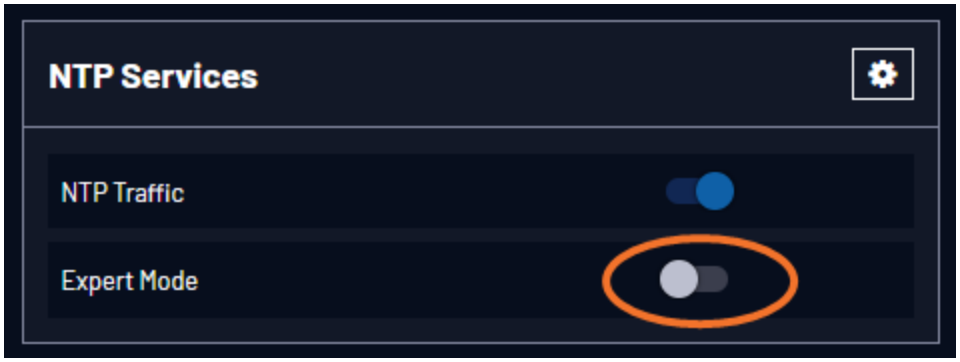
Note: Interfaces intended for Anycast use should be connected and fully configured for IPv4 or IPv6 communication.



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 SecureSync.

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
!
```

2.15.12.6 Testing NTP over Anycast

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

2.15.13 Host Disciplining

Host Disciplining allows an NTP input reference to discipline SecureSync's oscillator. This may be utilized e.g., with SecureSync units that do not have a GPS receiver because they are operated as Stratum 2 servers.

In general, units that do not have a GNSS reference will look to the time references as they are ordered in the Reference Priority to obtain their time references. If NTP is enabled and valid, it will discipline the unit's system time when it is the highest valid reference.

2.15.14 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, SecureSync 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 SecureSync Web UI. However, it may be desired in certain circumstances to edit this file directly, instead of using the web-based setup screens. When Expert Mode is enabled, the user has direct access to the `NTP.conf` file.

Caution: 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 SecureSync 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.

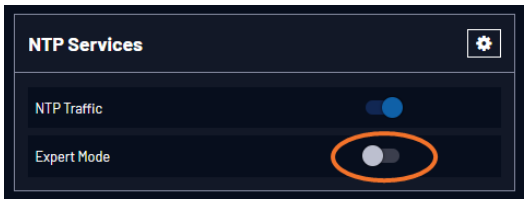
Factory default `NTP.conf` file:

```
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. SecureSync 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.

2.15.15 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.

2.16 Configuring PTP



Note: These instructions refer to the PTP available directly through your unit via ETH0 and ETH1.

If you have a 1204-32 Grandmaster PTP option card installed, you will need to follow separate instructions to configure that PTP functionality. See "PTP Grandmaster [1204-32]" on page 534

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

SecureSync 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 SecureSync 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**: SecureSync has PTP time stamp functionality which is set to use the PTP timescale.

2.16.1 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:

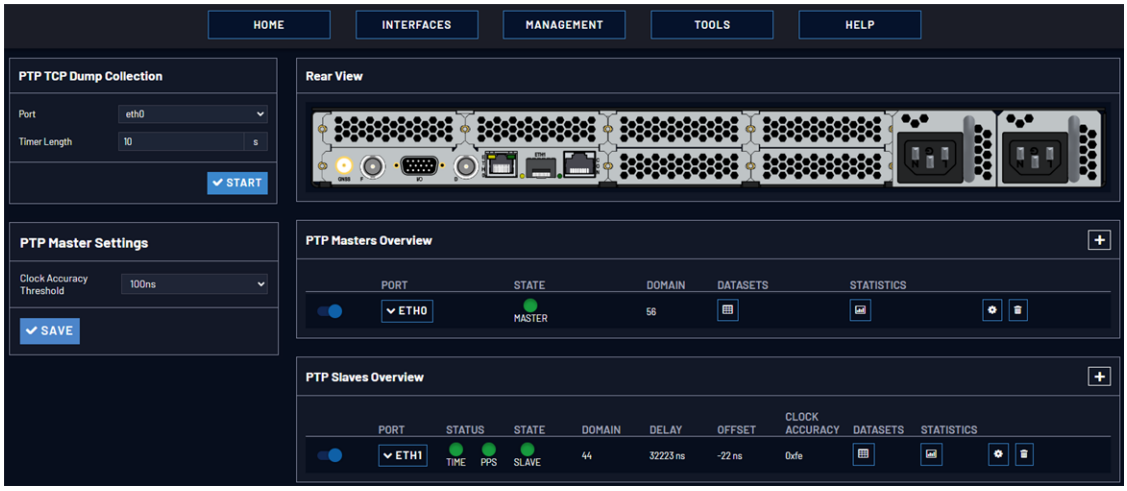


Figure 2-13: PTP setup screen

You will see the PTP Masters Panel, the PTP Slaves Panel, the PTP Master Settings Panel, the PTP TCP Dump Collection Panel, and a Rear Panel image of the product.

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.

2.16.1.1 The PTP Masters Overview Panel

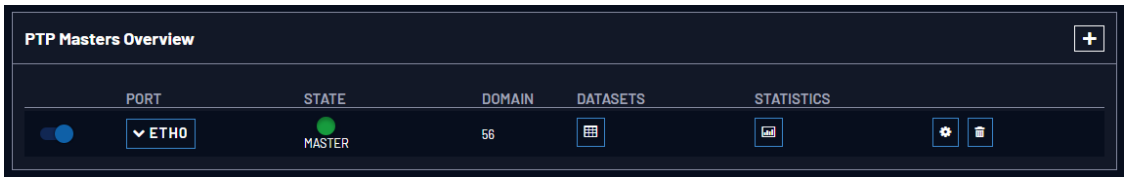


Figure 2-14: PTP Masters Overview Panel

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 167

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:

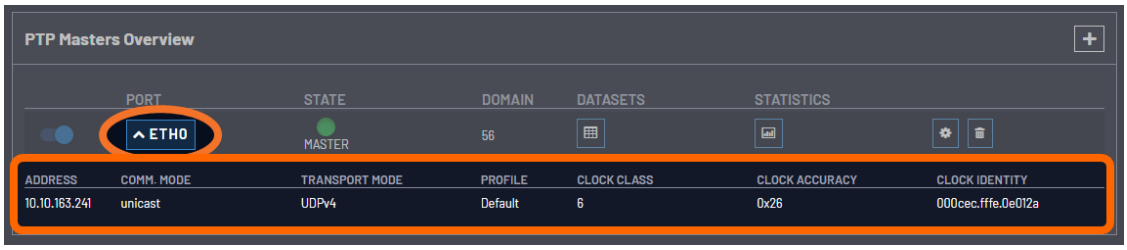


Figure 2-15: PTP Master Overview Drop Down

- 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 163).

The **Statistics button** displays the Statistics popup window (see "The PTP Statistics Panel" on page 163).

The **Settings button** brings up the popup window to edit settings (see "The Edit PTP Settings Panel" on page 160).

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..

2.16.1.2 The PTP Slaves Overview Panel

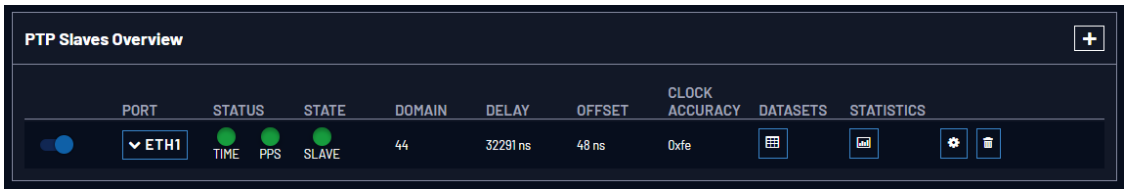


Figure 2-16: PTP Slaves Overview Panel

> 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 167

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:

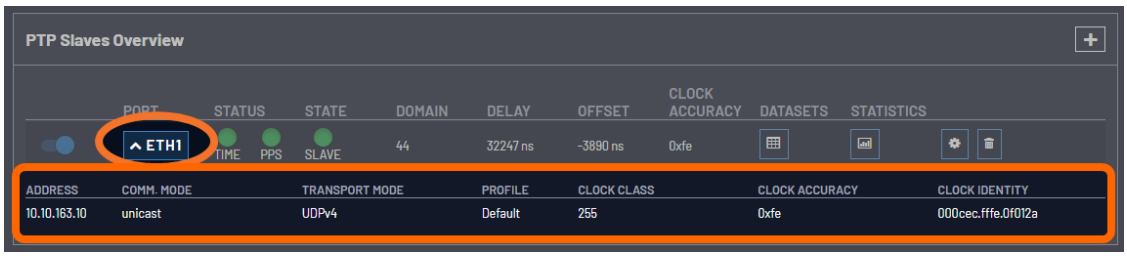


Figure 2-17: PTP Slaves Overview Drop Down

- 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 163).

The **Statistics button**  displays the Statistics popup window (see "The PTP Statistics Panel" on page 163).

The **Settings button**  brings up the popup window to edit settings (see "The Edit PTP Settings Panel" on the next page).

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.

2.16.1.3 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.

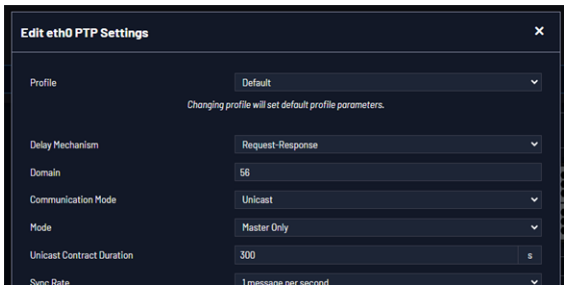


Figure 2-18: Edit PTP Settings panel

- **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.

2.16.1.4 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, ClockAccuracy, OffsetScaledLogVarience, GrandmasterPriority1, GrandmasterPriority2.

Time Properties Dataset

CurrentUtcOffset, CurrentUtcOffsetValid, Leap59, Leap61, TimeTraceable, PtpTimescale, TimeSource

Port Dataset

PortIdentity, PortState, LogMinDelayReqInterval, PeerMeanPathDelay, LogAnnounceInterval, AnnounceReceiptTimeout, LogSyncInterval, DelayMechanism, LogMinPdelayReqInterval, VersionNumber

Clock Description Dataset

ClockType, PhysicalLayelProtocol, PhysicalAddress, ProtocolAddress, ManufactureId, ProductDescription, RevisionData, UserDescription, ProfileId

2.16.1.5 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 SecureSync, i.e. in a Unicast environment, SecureSync may only detect traffic that is addressed to it, based on switch configuration.

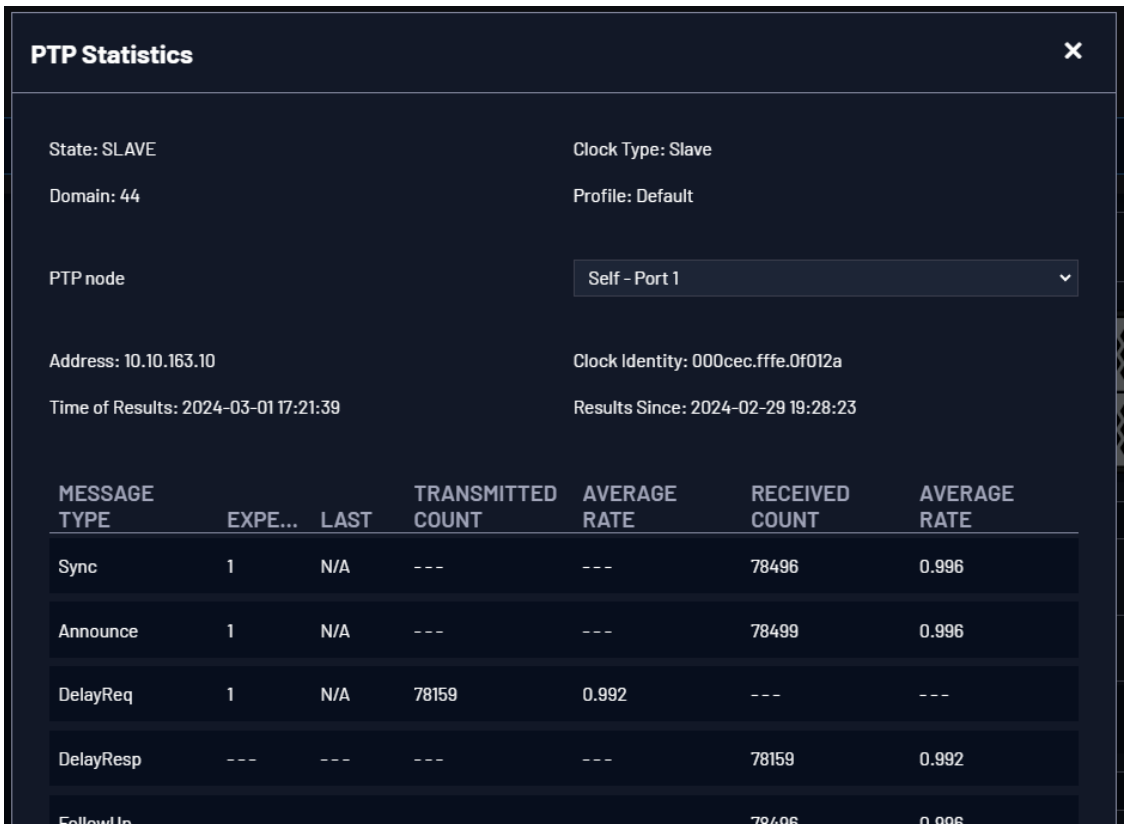


Figure 2-19: PTP Statistics Panel

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.

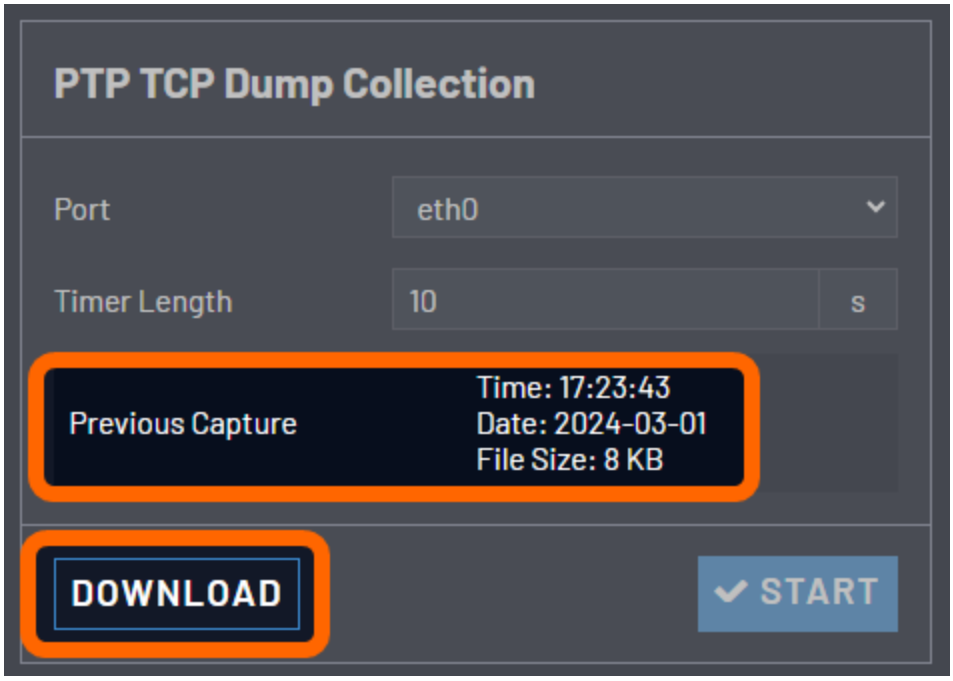
- **Results Since**: [e.g., "2021-10-18 16:05:30"] Time at which the stats collection started
- **Transmitted/Received Count**: Message count of sent/received data
- **Average Rate**:[e.g., "0.062"] Indicates how often the selected message has been detected (in seconds; e.g., "1.0" would mean once every second).
- The **Clear Statistics** button will reset the zero count.
- The **Refresh** button will retrieve the latest results

2.16.1.6 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:

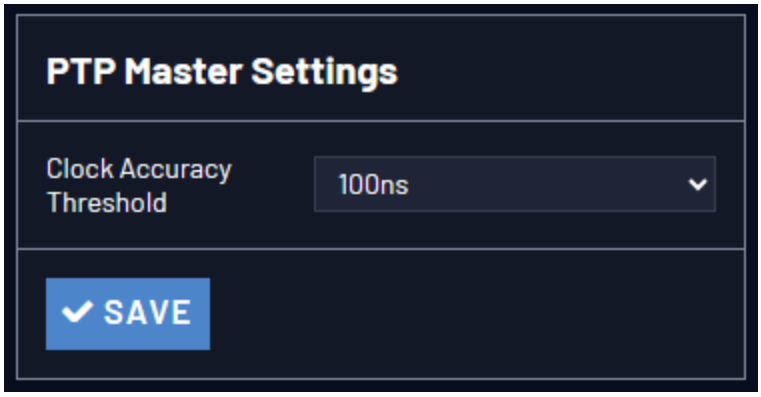
1. Select the Timer Length and Ethernet port you wish to investigate.
2. Select the Start button.
3. After the collection is completed, the latest collection information will display in the panel, and a Download button will display.



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.

2.16.1.7 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.

2.16.2 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 160.
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.

2.16.3 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.



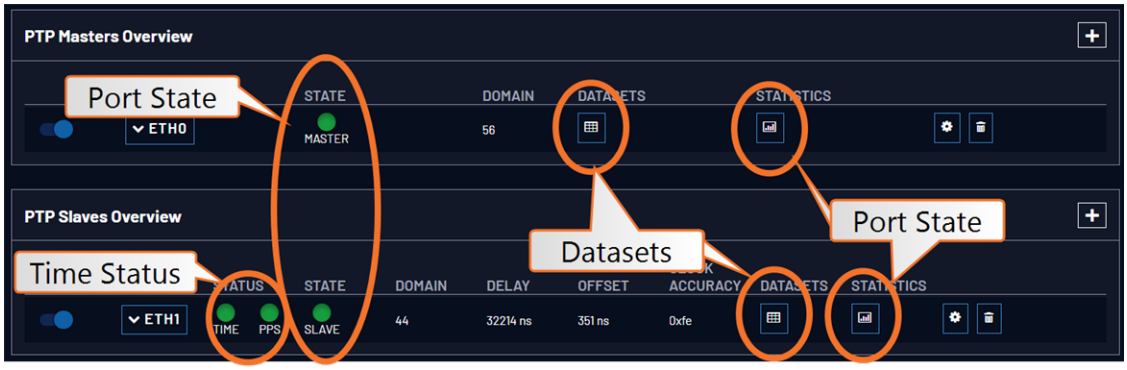
Note: You will not be able to see or Enable PTP ports if you do not have one configured. Select the plus icon in one of the PTP Overview panels to add a PTP interface.

3. Configure your settings using the Edit Settings Panel.

2.16.4 PTP Monitoring

To confirm that your PTP is functioning correctly, we provide a number of PTP Monitoring methods.

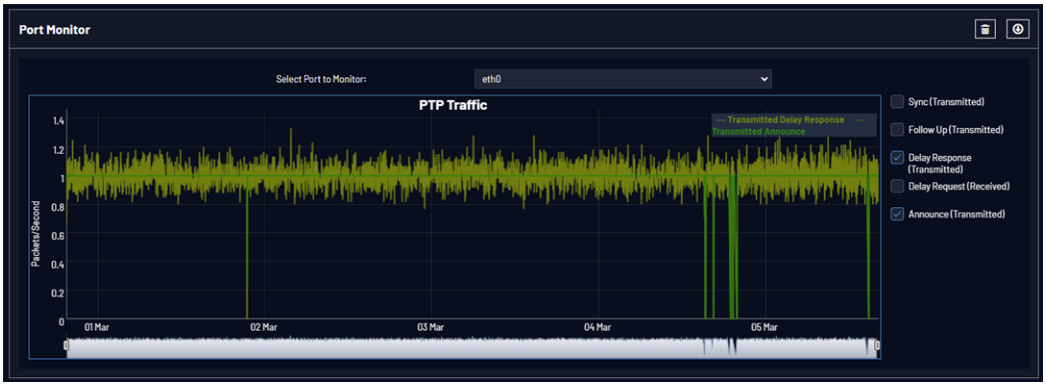
PTP Monitoring via the Web UI



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 166).

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 317 for more information.

2.16.5 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, SecureSync 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.

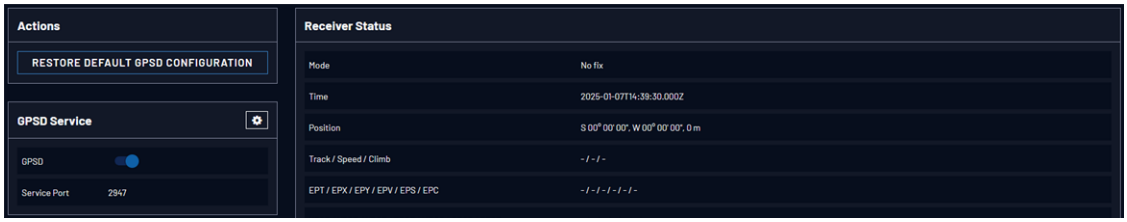
2.17 GPSD Setup

GPSD is a free, open-source package used worldwide to manage GNSS systems and devices. With GPSD support on a SecureSync, 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 SecureSync 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 SecureSync, 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.

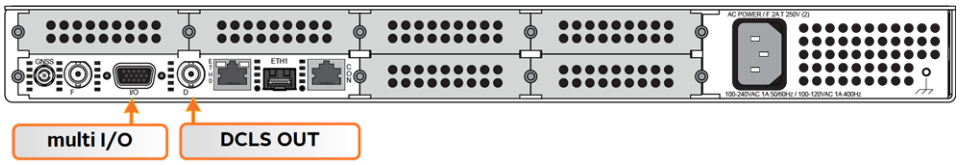
GPSD via CLI commands

The following CLI commands are used to control the behavior of GPSD via the SecureSync CLI:

- `gpsdserviceportget` – Displays the GPSD service port
- `gpsdserviceportset` – Sets the GPSD service port

There are two GPSD utility programs already incorporated into SecureSync; `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.

2.18 Configurable Connectors



This Section covers the two software-configurable connectors on the CPU board (rear panel): the **BNC DCLS OUT** connector and the **HD15 multi I/O** connector.

When you configure an input our output via the DCLS OUT connector or the I/O connector, you will need to adjust both the pin configuration ("Assigning Signals" on page 174) and (for some types) the settings for that input or output via the Web UI ("Configuring Input References" on page 176 and "Configuring Outputs" on page 184).

You can find the settings for signals currently configured through these two connectors under **INTERFACES** > **OPTION CARDS** > **Main**. The CPU board with the standard-issue connectors is referred to as "Option Card 0" in the Web UI.

2.18.1 BNC DCLS OUT

The DCLS Out connector can be configured with the following options. See "Assigning Signals" on page 174 for detailed instructions.

Table 2-6: DCLS Output Options

	Location	Available Signal Types	Web UI Selection
DCLS OUT	BNC Connector (rear Panel)	**1PPS Output (default)**	PPS_OUT | DCLS_TTL
		IRIG Output	IRIG_OUT | DCLS_TTL
		HaveQuick Output	HQ_OUT | DCLS_TTL
		GPIO Output	GPIO_OUT | DCLS_TTL

2.18.2 DB15 Multi I/O

Note on the table below: Both RS485 connectors have optional termination on their inputs. To select this feature, choose the Web UI feature as listed below that also includes **With Termination** in the listing.

Table 2-7: Multi I/O Input and Output Options

	Pin Location	Available Signal Types	Web UI Selection
DCLS OUT	Pin 6 (signal) Pin 7 (ground)	1PPS Output	PPS_OUT | DCLS_TTL
		IRIG Output (Default)	IRIG_OUT | DCLS_TTL
		HaveQuick Output	HQ_OUT | DCLS_TTL
		GPIO Output	GPIO_OUT | DCLS_ TTL
DCLS IN	Pin 1 (signal) Pin 2 (ground)	1PPS Input	PPS_IN | DCLS_TTL
		IRIG Input (Default)	IRIG_IN | DCLS_TTL
		HaveQuick Input	HQ_IN | DCLS_TTL
RS232 IN	Pin 15 (signal) Pin 10 (ground)	**ASCII Time Code Input (Default)**	ATC_IN | RS232
RS232 OUT	Pin 5 (signal) Pin 10 (ground)	**ASCII Time Code Output (Default)**	ATC_OUT | RS232

	Pin Location	Available Signal Types	Web UI Selection
RS485 (#1)	Pin 3 (signal) Pin 13 (signal) Pin 8 (ground)	1PPS Output	PPS_OUT | RS485
		IRIG Output	IRIG_OUT | RS485
		HaveQuick Output (Default)	HQ_OUT | RS485
		ASCII Time Code Output	ATC_OUT | RS485
		1PPS Input	PPS_IN | RS485
		IRIG Input	IRIG_IN | RS485
		HaveQuick Input	HQ_IN | RS485
		ASCII Time Code Input	ATC_IN | RS485
RS485 (#2)	Pin 4 (signal) Pin 14 (signal) Pin 9 (ground)	1PPS Output	PPS_OUT | RS485
		IRIG Output	IRIG_OUT | RS485
		HaveQuick Output	HQ_OUT | RS485
		ASCII Time Code Output	ATC_OUT | RS485
		1PPS Input	PPS_IN | RS485
		IRIG Input	IRIG_IN | RS485
		HaveQuick Input (Default)	HQ_IN | RS485
		ASCII Time Code Input	ATC_IN | RS485
IRIG AM Out-put	Pin 11 (signal) Pin 12 (ground)	**IRIG AM Output (Default, non-configurable)**	

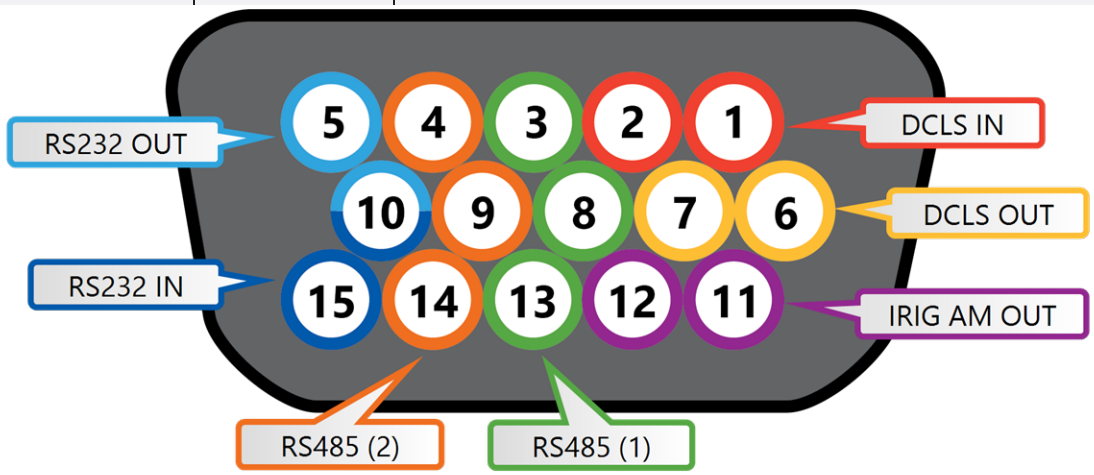


Figure 2-20: Multi I/O 15-pin connector, in mating direction from front

Pin	Signal
1	DCLS IN
2	GND
3	(First signal) RS485 A, non-inverting
4	(Second signal) RS485 A, non-inverting
5	RS232 TX OUT
6	DCLS OUT
7	GND
8	GND
9	GND
10	GND
11	IRIG AM OUT
12	GND
13	(First signal) RS485 B, inverting
14	(Second signal) RS485 B, inverting
15	RS232 RX IN

2.18.3 Assigning Signals

Changing the signals on either the rear panel BNC DCLS connector, or on the Multi I/O 15-pin connector requires access to the Web UI.

Note: Applying changes to the pin configuration will reset the reference priority table. See also "Configuring Input Reference Priorities" on page 219.

Configuring a new Input or Output

1. In the SecureSync Web UI, navigate to **MANAGEMENT > NETWORK: Pin Layout**. The **Pin Layout** screen will be displayed.
2. View your current pin layout settings in the Layout panel. The pins are grouped together by their channels (see the "Multi I/O 15-pin connector, in mating direction from front" on the previous page). One pin in each channel will update the settings for the entire channel.

3. To change a signal, you can **Delete** it, but you may also simply assign the new signal as described below, thus overwriting the existing Input or Output.
4. Add a pin configuration by clicking the PLUS icon in the top-right corner. The **Add Pin** popup window will display.
5. Start with the **Type Filter** drop-down menu (second line in the window) and select a signal type.
6. From the **Signal** drop-down menu, select a signal.
7. From the **Pins** drop-down menu in line 3, select the pin set you wish to configure.
8. Click **Submit**.
9. In the **Actions** panel, click **Apply Changes** after all your configuration is done. This button will finalize your changes and force a server reboot (some timing sources may be affected by this change).

Restoring the Default I/O Configuration

SecureSync 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.

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**.

Saving your unique Pin Layout

Before you perform a clean upgrade or restore your unit's default settings, you can choose to download your current pin layout settings.

(Note: The Save Layout option applies only to the pin configuration for the DCLS BNC connector and the 15-pin I/O connector. To save your entire configuration including these settings, see "Backing-up and Restoring Configuration Files" on page 362.)

1. To save the current layout, navigate to the **MANAGEMENT** > **NETWORK** > **Pin Layout** screen.
2. In the **Actions** panel, click the **Save Layout** button to download a file containing your current settings.
3. Save this file in a location of your choosing and perform any necessary actions.
4. To restore your former layout, click the **Upload Layout** button in the Pin Layout screen.
5. Choose the name and location of the file saved when using the Save Layout function. Click the Upload button.

2.18.4 Network Ports

The Network Ports can be configured under **MANAGEMENT > Network Setup**. For more information, see "Configure Network Settings" on page 73.

2.19 Configuring Input References

Depending on the type of input reference, some of its settings may be user-editable. To access these settings for a given input reference, choose one of the two methods described below.

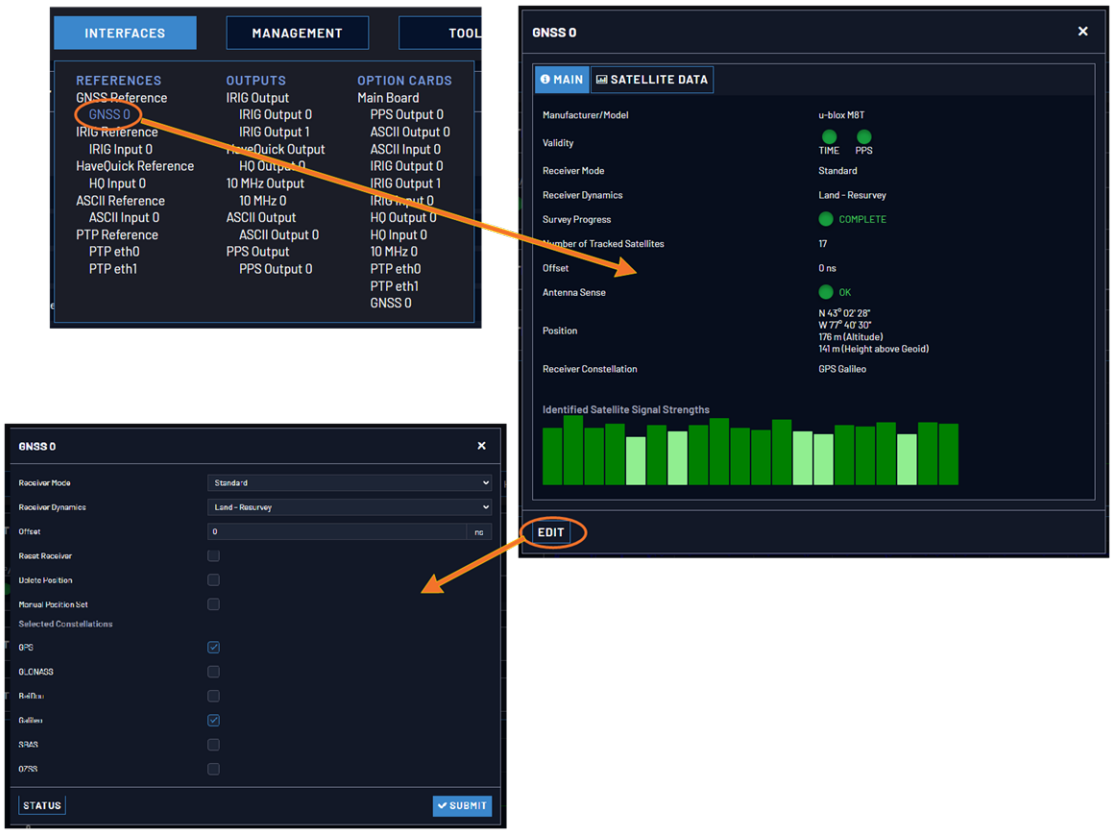
(To disable references or change the priority that your timing system will be guided by those references, visit "Configuring Input Reference Priorities" on page 219).

Note: The illustrations shown below are examples. The windows displayed in your Web UI may look differently.

2.19.1 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 217.

The following configuration instructions apply to optional inputs on the basic unit model. For specifics on inputs made available through option cards, see the section "Option Cards" on page 383.

2.19.2 Configure a 1PPS Input

A 1PPS Input can be set up through the Multi-I/O connector (see "Configurable Connectors" on page 171).

To configure the settings of the **PPS Input** (also referred to as 'Reference'), go to its Edit window..

The Web UI list entries for these cards are:

- 1PPS In/Out
- 1PPS In/Out, Fiber

The connector number for the input is: J1



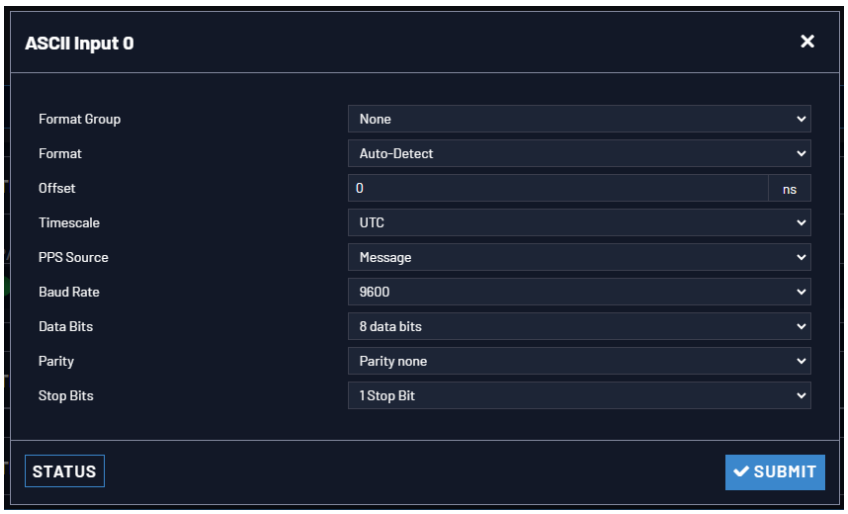
The Edit window allows the configuration of the following settings:

- **Edge**: The operator can select either the rising or the falling edge as the input time reference (defines the on-time point of the signal).
- **Offset**: It is possible to add an offset to the input signal (to account for cable delays), with a resolution of 5ns and a positive or negative value of 500 ms maximum.

2.19.3 Configure an ASCII Input

An ASCII Input is available by default configuration through the Multi-I/O connector (see "Configurable Connectors" on page 171).

To configure the **ASCII Input** (also referred to as 'Reference'), go to its **Edit** window.



The Input Edit window allows the configuration of the following settings:

- **Format Group**: Determines the time code message format category (see also "Time Code Data Formats" on page 585.) Choices are:
  - Auto
  - Spectracom
  - NMEA
  - ICD-153
  - EndRun
- **Format**: Once a **Format Group** has been selected, one or more **Format** fields may appear, allowing you to select one or more time code **Formats**. For detailed specifications and limitations on the supported time code formats, see "Time Code Data Formats" on page 585.

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

- **Offset**: Provides the ability to account for ASCII input cable delays or other latencies in the ASCII input. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is –500 to +500 ms.
- **Timescale**: Used to select the time base for the incoming ASCII time code data. The entered Timescale is used by the system to convert the time in the incoming ASCII data stream to UTC time for use by the System Time. The available choices are:

- **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
- **TAI**: Temps Atomique International
- **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of 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 202 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.
  The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to "Local", select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. See for more information on Local Clocks.



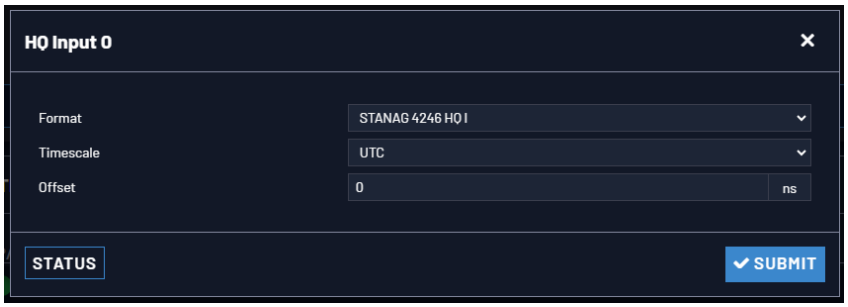
Note: The Timescale of the ASCII input (as configured in the ASCII time source) must be set correctly, especially if other input references are enabled. Failure to configure the Timescale of the ASCII input correctly could result in time jumps occurring in the System Time when input reference changes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

2.19.4 Configure a HaveQuick Input

A HaveQuick Input is available by default configuration through the Multi-I/O connector (see "Configurable Connectors" on page 171).

To configure the settings of the **HAVE QUICK Input** (also referred to as 'Reference'), go to its Edit window.



The Edit window allows the configuration of the following settings:

- **Format**: Used to configure the formatting of the available HAVE QUICK inputs and outputs. The available formats are as follows:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 STM
  - STANAG 4430 Ext HQ
  - STANAG 4430 Ext HQ Ed1
  - 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)
  - Offset: Provides the ability to account for HAVE QUICK cable delays or other latencies in the HAVE QUICK outputs. The Offset values are

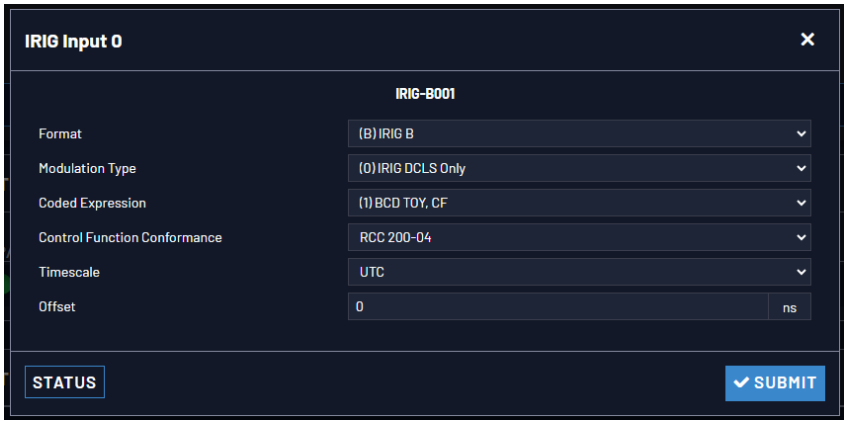
entered in nanoseconds (ns). The available Offset range is –500 to +500 ms.

2.19.5 Configuring an IRIG Input

An IRIG Input is available by default configuration through the Multi-I/O connector (see "Configurable Connectors" on page 171).

Unless you have an IRIG option card, IRIG AM is not available as an input at this time.

To configure the IRIG Input (also referred to as 'Reference'), navigate to its Edit window.



The Edit window allows the configuration of the following settings:

- **Format**: Sets the formatting of the IRIG input signal, as defined by the IRIG generator time source. The available choices are:
  - IRIG A
  - IRIG B
  - IRIG G
  - NASA-36
- **Modulation Type**: Configures the type of input signal modulation. The choices are:
  - IRIG DCLS—A TTL (Phase) modulated signal.
- **Frequency**: The IRIG modulation frequency. This is determined by the configuration of Format and Modulation Type. See "IRIG Carrier Frequencies" on page 620 for details.

- **Coded Expression**—Defines the data structure of the IRIG signal, where:
  - BCD = Binary Coded Decimal
  - TOY = Time of Year
  - CF = Control Field
  - SBS = Straight Binary Seconds
  - The available options will vary according to the configurations of Format and Modulation Type.
- **Control Function Field**: IRIG signals have an optional section in the data stream that can be used to include additional information (such as the present year, for example). This field allows the Control Field section of the IRIG output to be defined. The available configurations are:
  - Fields conform to **RCC 200-04**: IRIG spec 200-04 specified a location for year value, if included in this field.
  - Fields conform to **IEEC 37.118-2005** (IEEE 1344): Control Field contains year, leap second and daylight savings time information.
  - Fields conform to **Spectracom Format**: Year is included in Control Field but not in the same location as RCC-2004 output (year is offset by one position).
  - Fields conform to **Spectracom FAA Format**: A unique IRIG output Control Field that contains satellite lock status and time error flags.
  - Fields conform to **NASA Formats**: Variants of IRIG B
  - Fields confirm to **Spectracom IEEE C37.118-2005**: Has been extended to support one-month leap second notification

  The available options will vary according to the configurations of Format and Modulation Type.



Note: If the Format value is changed, the Control Field and Coded Expression change to the default values for the given Format value. The user can only change the Control Field field and Coded Expression field to allowed values for the Format field.

It is recommended that the SecureSync administrator/operator only use this if they do not know what the IRIG Input Format is, and they wish to identify the signal type, or to determine if a signal is present.

- **Local Clock**: The incoming IRIG input time information may be provided as local time, but System Time may be configured as UTC time, so internal

computations need to be performed. With the Timescale field set to "Local", select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display.

» **Offset**: Provides the ability to account for IRIG cable delays or other latencies in the IRIG input. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.

2.20 Configuring Outputs

Depending on the type of output interface, some of its settings may be user-editable. To access these settings for a given output, choose one of the two methods described below.

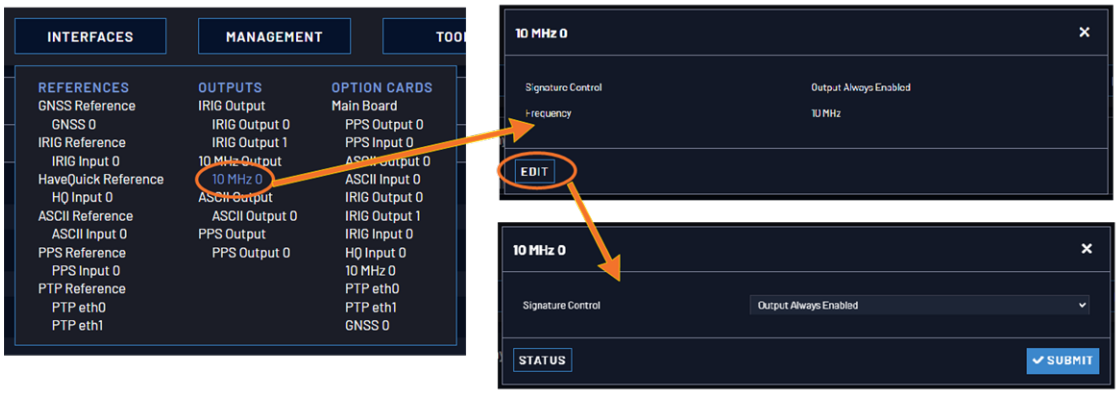
For information on disabling and enabling outputs, see "Signature Control" on page 198

Note: The illustrations shown below are examples. The windows displayed in your Web UI may look differently.

2.20.1 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 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.

The following configuration instructions apply to optional outputs on the basic unit model. For specifics on outputs made available through option cards, see the section "Option Cards" on page 383.

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.

2.20.2 Configuring a 1PPS Output

A 1PPS Output is available by default configuration through the BNC connector, and can also be output through the Multi-I/O connector (see "Configurable Connectors" on page 171).

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 198.
- **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.

2.20.3 Configuring the 10 MHz Output

A 10 MHz Output is available on the rear panel of the SecureSync 2400 Time and Frequency Synchronization System.

To configure the 10 MHz 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 **10 MHz** output that you want to edit.
3. The **10 MHz** edit window will display. Choose a value from the **Signature Control** field drop-down list to determine what SecureSync shall do with the output signal in the event its input reference is lost. For more information, see "Signature Control" on page 198.



4. Click Submit.

2.20.4 Configure an ASCII Output

An ASCII Output is available by default and configuration through the Multi-I/O connector (see "Configurable Connectors" on page 171).

To configure the **ASCII Output**, go to its Edit window.



The Output Edit window allows the configuration of the following settings:

- **Format Group** – configures the message format type. Choices are:
  - None (no message will be output)
  - Spectracom
  - NMEA
  - BBC
  - ICD-153
  - EndRun

  Once selected, the **Format Group** may offer a choice of **Formats**. For more information on supported **Formats**, see "Time Code Data Formats" on page 585.
  - **Format 1**: Selects either the first of up to five, 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.”
  - **Format 4**: Selects the fourth consecutive format message to be outputted. Select “None” if only one output format is desired. “None” will be the only choice available if Format 3 is “None.”
  - **Format 5**: Selects the fifth consecutive format message to be outputted. Select “None” if only one output format is desired. “None” will be the only choice available if Format 4 is “None.”
- **Signature Control**: Signature Control controls when the selected ASCII data output format will be present; see "Signature Control" on page 198.

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

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

- **Time Scale**: Used to select the time base for the incoming data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International
  - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of 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 202 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. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. See for more information on Local Clocks.

- **Baud Rate**: Determines the speed at which the output port will operate.
- **Data Bits**: Defines the number of Data Bits for the output port.
- **Parity**: Configures the parity checking of the output port.
- **Stop Bits**: Defines the number of Stop Bits for the output.

To *view* the current settings of the **ASCII Input** (also referred to as 'Reference'), go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

2.20.5 Configuring a GPIO Output

A GPIO Output is available through the BNC and/or Multi-I/O connector on the rear panel (see "Configurable Connectors" on page 171).

Note: The fields viewable will depend on the selection for the Output Mode.

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.

- **Output Mode**:
  - Direct Output Value: Output will be low or high, determined by the Output Value section below.
  - Square Wave: Output will generate a programmable square wave determined by the configuration.
- **Output Enabled**: Check this box to enable or disable the output. If Enabled, additional configurable parameters will be displayed.
- **Output Value**: Determines the output level (Low or High).
- **Signature Control**: Controls when the output will be present. See also: "Signature Control" on page 198.

- **Edge**: Used to determine if the on-time point of the output is the **Rising** or **Falling** edge of the signal.
- **Offset**: Accounts for cable delays and other latencies [nanoseconds].
- **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.
- **Period Correction**: Period correction allows for the generation of more precise frequencies at the expense of additional period jitter. Over a length of time, the true square wave period comes to:
  - Period + [(numerator/denominator) * 5 ns]
- **Pulse Width**: Pulse width of the output [nanoseconds].
- **On-Time Point Pulse Width**: The on-time point pulse width is the pulse width of the first square wave pulse aligned to the 1PPS On-Time Point. This is only active when the alignment count is non-zero [nanoseconds].
- **Alignment Count (s)**: The alignment counter determines how often (in seconds) the square wave will be aligned back to the 1PPS. Setting zero will disable PPS alignment beyond the initial alignment.
- **Time Alignment**: (Enabled/Disabled) The time alignment enable changes the function of the alignment counter to align the square wave whenever the current time's seconds value is a multiple of the alignment count. For example: If time alignment is enabled and alignment count is set to 15 seconds, the square wave will be aligned to the 1PPS when the seconds value on the time display equals 00, 15, 30, 45.
- **Re-Initialize**: Re-initializes square wave generation and aligns to 1PPS.

2.20.6 Configuring a HaveQuick Output

A HaveQuick Output is available by default configuration through the Multi-I/O connector and can be optionally configured through the BNC connector on the rear panel (see "Configurable Connectors" on page 171).

To configure the settings of a **HAVE QUICK Output**, go to its Edit window.



The Edit window allows the configuration of the following settings:

- **Signature Control**: Signature Control is used to control when the HAVE QUICK modulation is present, see "Signature Control" on page 198.
- **Format**: Used to configure the formatting of the available HAVE QUICK inputs and outputs. The available formats are as follows:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 STM (Standard Time Message)
  - STANAG 4430 Ext HQ (Extended HAVE QUICK)
  - STANAG 4430 Ext HQ Ed1
  - 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: This option will appear under the name of the local clock you have set up. Refer to "The Time Management Screen" on page 202 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

  The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to for more information on Local Clocks.
- **Offset**: Provides the ability to account for HAVE QUICK cable delays or other latencies in the HAVE QUICK outputs. The Offset values are entered in nanoseconds (ns). The available Offset range is –500 to +500 ms.

2.20.7 Configuring an IRIG Output

IRIG DCLS Output is available through the Multi I/O connector in the default settings (pins 6 & 7), and can also be configured on the DCLS OUT BNC connector on the rear panel, as well as through the multi I/O connector on either of the two RS485 channels (pins 3, 13, and 8, and pins 4, 14, and 9). See "Configurable Connectors" on page 171 for more information. None of these listed channels allow IRIG AM outputs.

IRIG AM Output is available in the default configuration through the IRIG AM Output channel (pins 11 & 12) o(n the Multi I/O connector Additional outputs of IRIG AM would require an option card..

In the default configuration:

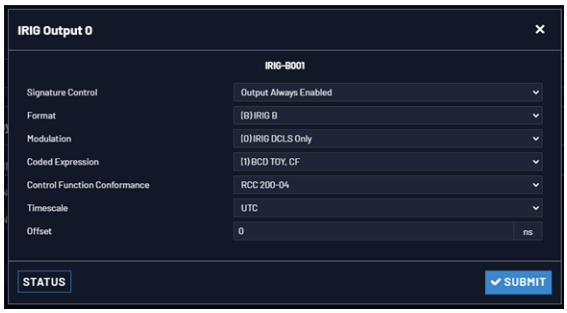
- **IRIG Output 0** represents IRIG DCLS output (pins 6 & 7). This channel can only be DCLS.
- **IRIG Output 1** represents the IRIG AM output (pins 11 & 12). This setting can only be configured to AM.

The numbering of outputs and inputs can change during pin layout changes (and when option cards are added).

Possible settings will be limited by the interface you are configuring.

To configure the settings of one of the two **IRIG Outputs**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

Note: The choices available will change based on the type of IRIG you have chosen to configure.



The Edit window allows the configuration of the following settings:

- **Signature Control**: Is used to control when the IRIG modulation will be present. This function allows the modulation to stop under certain conditions; see also "Signature Control" on page 198.

- **Format**: Used to configure the desired IRIG output formatting. The available choices are:
  - IRIG A
  - IRIG B
  - IRIG G
  - IRIG E
  - NASA-36
- **Modulation**: Changes the type of output signal modulation. The available choices are:
  - IRIG DCLS—A TTL-modulated output.
  - IRIG AM-–An amplitude modulated output. The amplitude of the output is determined by the value entered in the Amplitude field.
  - Frequency—The IRIG modulation frequency. This is determined by the configuration of Format and Modulation Type. See also "IRIG Carrier Frequencies" on page 620.
- **Coded Expression**: Defines the data structure of the IRIG signal, where:
  - BCD = Binary Coded Decimal
  - TOY = Time of Year
  - CF = Control Field
  - SBS = Straight Binary Seconds
  - The available options will vary according to the values of Format and Modulation Type.
- **Control Function Field**: IRIG signals have an optional section in the data stream that can be used to include additional information (such as the present year, for example). This field allows the Control Field section of the IRIG output to be defined. The available configurations are:
  - Fields conform to **RCC 200-04**: IRIG spec 200-04 specified a location for year value, if included in this field.
  - Fields conform to **IEEC 37.118-2005** (IEEE 1344): Control Field contains year, leap second and daylight savings time information.
  - Fields conform to **Spectracom Format**: Year is included in Control Field but not in the same location as RCC-2004 output (year is offset by one position).
  - Fields conform to **Spectracom FAA Format**: A unique IRIG output Control Field that contains satellite lock status and time error flags.

- Fields conform to **NASA Formats**: Variants of IRIG B
- Fields confirm to **Spectracom IEEE C37.118-2005**: Has been extended to support one-month leap second notification

The available options will vary according to the configurations of Format and Modulation Type.

- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**—Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**—Temps Atomique International
  - **GPS**—The raw GPS time as transmitted by the GNSS satellites (as of 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. See "Local Clock(s), DST" on page 214 for more information. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.
- **Amplitude**: The peak-to-peak output voltage level into a 600 Ω load is adjusted by entering a digital control value in this field. The level adjustment has no effect on TTL outputs, only on AM formats. The value of 128 will cause the Mark amplitude to be about $5V_{p-p}$ into high impedance. A value of 200 results in an output amplitude of about $9V_{p-p}$ into high impedance.



Note: These are nominal values only. Actual values will vary from unit to unit. To adjust the level precisely, connect an oscilloscope to the output connector when adjusting.

- **Offset**: Provides the ability to account for IRIG cable delays or other latencies in the IRIG input. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.

For IRIG frequency and output specifications, see "IRIG Standards and Specifications" on page 619.

2.20.8 The Outputs Screen

SecureSync outputs deliver a time or frequency signal to a device that consumes this signal.

To access the **Outputs** screen in the Web UI:

1. Navigate to **INTERFACES** and click on **OUTPUTS** (white on orange).
2. The **Outputs** screen will display.

   While **System Status** and logged **Events** are displayed on the left, the **Outputs** panel on the right lists all the outputs detected.

   - If you have only one output of any type, SecureSync will number that output 0. Additional outputs will be numbered 1 or above.
   - If you click the INFO button next to an output, a Status window will open.
   - If you click the GEAR button next to an output, the Configuration window will open.

2.20.9 The 1PPS and 10 MHz Outputs

The SecureSync includes one 1PPS output and one 10 MHz output. To configure these outputs, navigate to:

- INTERFACES > OUTPUTS

and select the **1PPS Output** or **10 MHz Output** you would like to see, or configure.

SecureSync's 1PPS output is generated from the oscillator's 10 MHz output and is aligned to the on-time point. The on-time point of the 1PPS output can be configured to be either the rising or falling edge of the 1PPS signal (by default, the rising edge is the on-time point).

There is a fixed phase relationship between the 1PPS and the 10 MHz outputs, as described below:

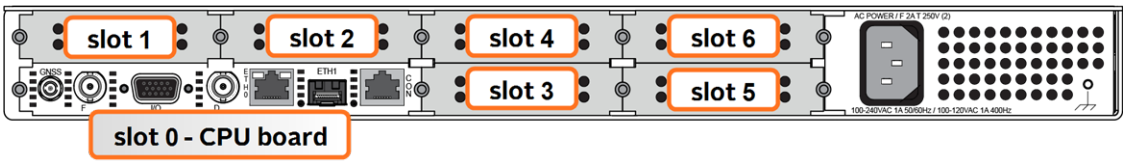
- SecureSync equipped with **TCXO/OCXO/Low-Phase-Noise Rubidium oscillator**: With oscillator disciplining active (one or more 1PPS references available and valid) and after the on-time point has been initially slewed into alignment with the selected reference, there will always be exactly 10 million counts of the oscillator between each 1PPS output, even while in the Holdover mode (= input references are currently unavailable) and even after input references have become available again.
- SecureSync equipped with **Rubidium (Rb) oscillator**: With oscillator disciplining active (one or more 1PPS references available and valid), after the on-time point has been slewed into alignment with the selected reference, with the exception of 1PPS input reference changes occurring, there will

always be exactly 10 million oscillator counts between each PPS output pulse.
With the Rubidium oscillator installed, when a 1PPS input reference change occurs (such as switching from IRIG input to GNSS input, or switching from a reference being valid to no reference being present or valid—known as the **Holdover** mode), the oscillator counts between two 1PPS outputs may momentarily not be exactly 10 million counts. Once the reference transition has occurred, however, the counts between each PPS output pulse will return to exactly 10 million counts.

Like other types of SecureSync's signal outputs, a 1PPS output can be configured in several ways:

- **Signature Control** allows you to determine under which conditions an output signal shall be present, i.e. what SecureSync will do about a given output when an external reference is lost. See also "Signature Control" on page 198.
- The **on-time point** of the 1PPS signal: rising or falling edge
- The **pulse width**
- An **offset** can be entered to account for cable delays or other latencies.

2.21 The Option Cards Screen



This menu lists all the interfaces on the unit, including the option cards installed on your SecureSync, and an image depicting your unit's rear panel.

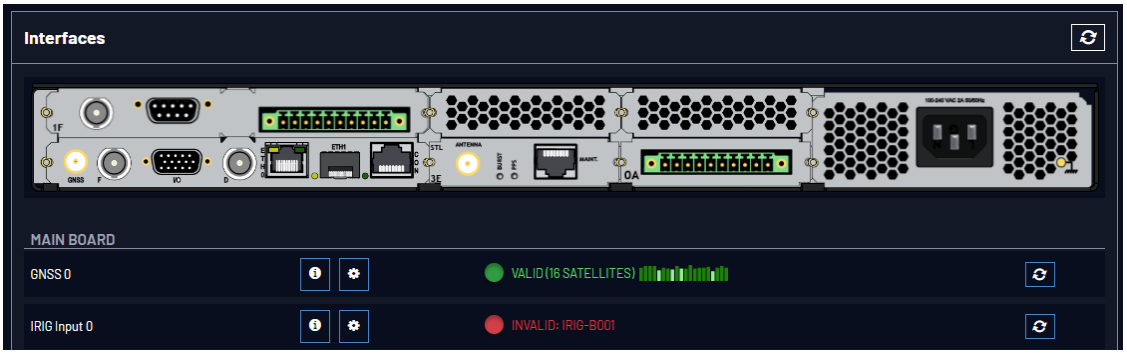
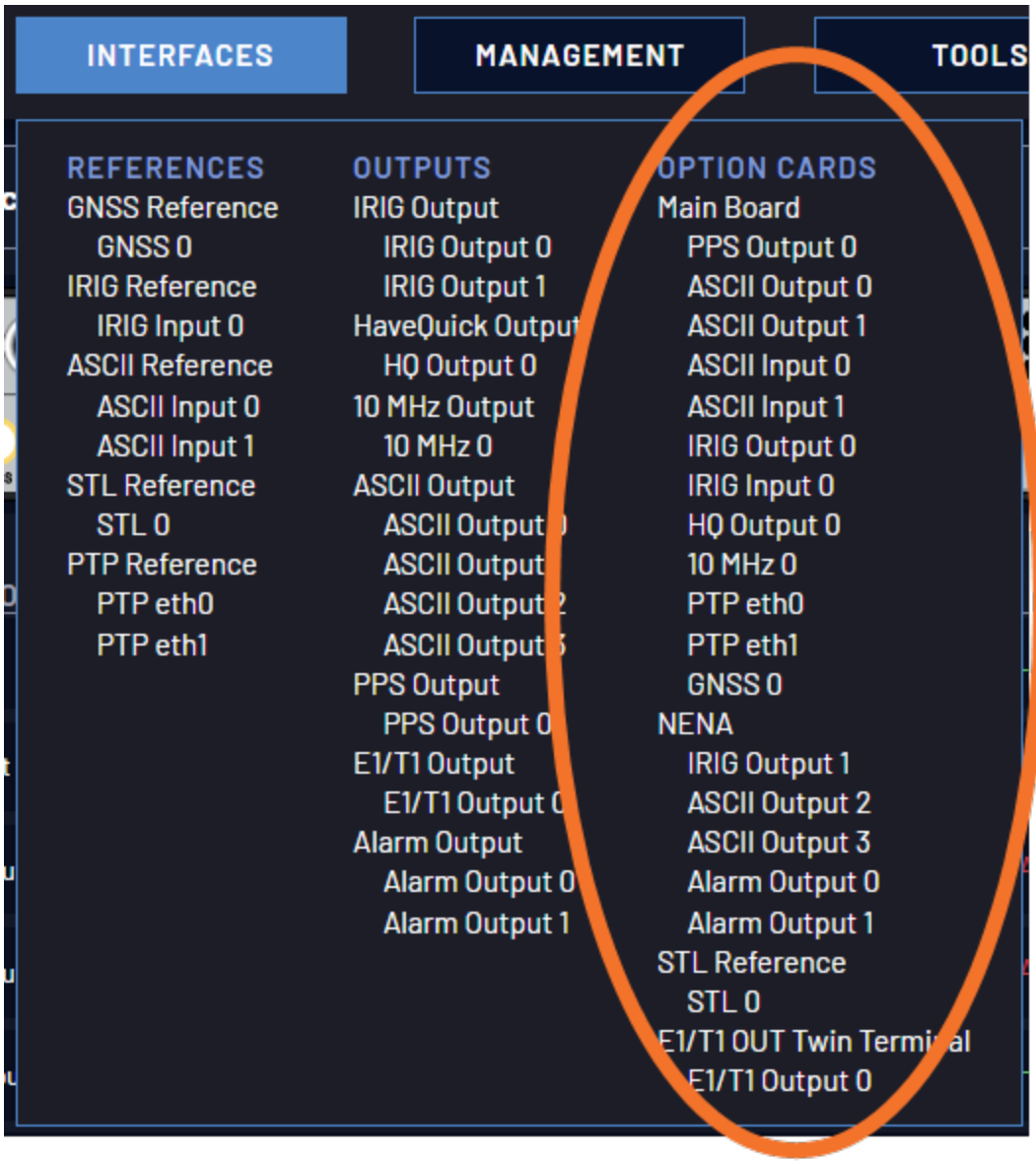


Figure 2-21: Option Card Rear Panel Image

The rear panel connectors included with a standard SecureSync are all listed in this menu under "Main" and "Option Card 0".

To navigate to the Option Card Menu in the Web UI, navigate to **INTERFACES** > and click on the white-on-orange menu header, OPTION CARDS.



In the **Interfaces** Panel, all of the factory interfaces are listed under Option Card 0, and each installed option card is shown with every available interface.

To edit the settings on an interface, click on the GEAR icon.



See "Option Cards" on page 383 for more information on option card settings, and individual option card functionality.

2.22 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 SecureSync'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 SecureSync in holdover mode, but not in free run.

The available options are:

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

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

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

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

Table 2-8: 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.

Changing Signature Control via the Front Panel

The SecureSync front panel allows you to change the signature control between two states: Output Always Enabled and Output Always Disabled. For more options and control over the Signature Control setting, you must use the Web UI (see above).

On the unit front panel:

1. Press the Outputs button.
2. Select the output you wish to configure.
3. Use the arrow keys to select ON (enabled) or OFF (disabled). Press the enter key.
4. In the confirmation menu on the right hand side of the screen, press the enter key again.

BLANK PAGE.

CHAPTER 3

Managing Time

In this document, the notion of **Managing Time** refers not only to the concept of SecureSync's System Time, but also to reference configuration, as well as distribution of time and frequency.

The following topics are included in this Chapter:

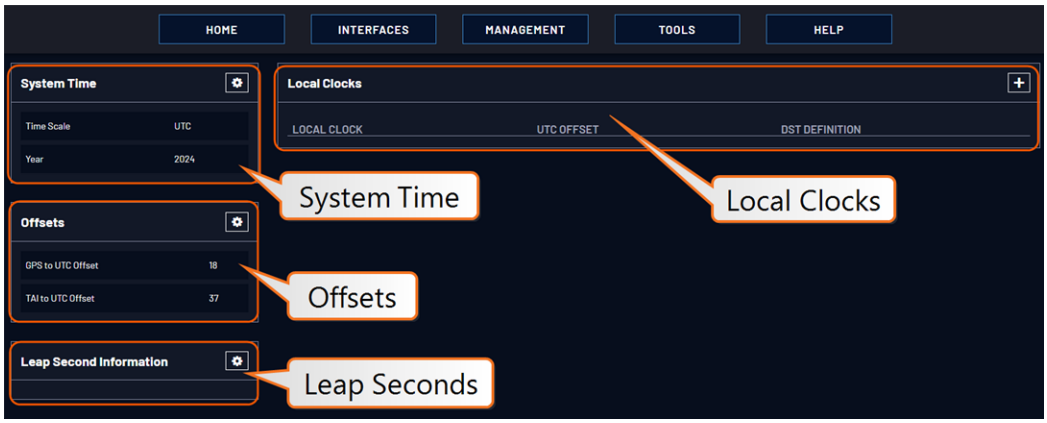
3.1 The Time Management Screen 202
3.2 System Time 203
3.3 Managing References 217
3.4 Holdover Mode 265
3.5 Managing the Oscillator 269

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 204.

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 SecureSync's time keeping. It is also possible to enter the exact day and time when the leap second is to be applied, and to delete a leap second.

See also: "Leap Seconds" on page 211

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 214.

3.2 System Time

The time that SecureSync 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 SecureSync'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 SecureSync 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**).

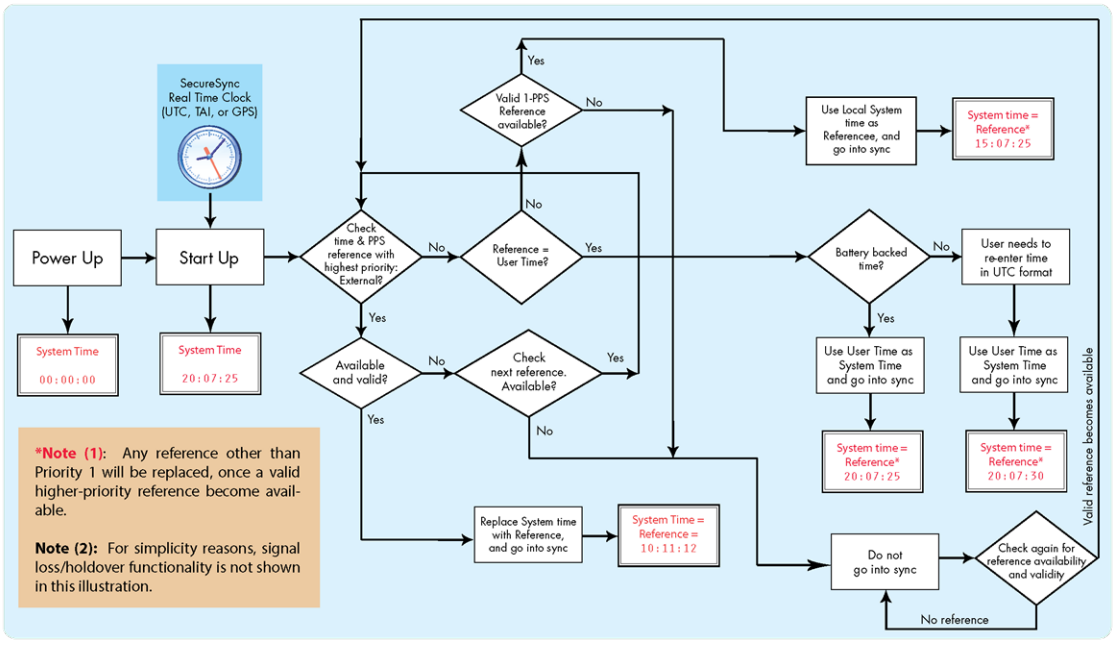


Figure 3-1: How the System Time is derived

Note: User hand-set times can only be set in UTC (not Local time).

3.2.1 System Time

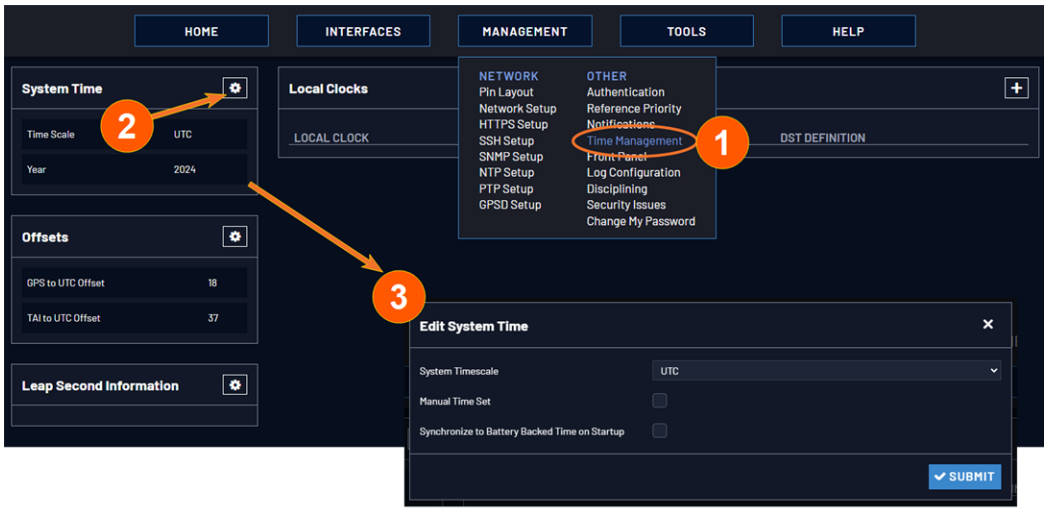
Several System Time parameters can be customized:

- 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 207.
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 SecureSync, 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.

SecureSync's System timescale is configured via the **MANAGEMENT > OTHER: Time Management** screen, see "System Time" on page 204.

Input timescales

Some of the inputs may not necessarily provide time to SecureSync in the same timescale selected in the System Time's timescale field. These inputs have internal conversions that allow the timescale for the inputs to also be independently defined, so that they don't have to be provided in the same timescale. For example, the System timescale can be configured as "UTC", but the IRIG input data stream can provide SecureSync with "local" time, with no time jumps occurring when the reference is selected.

If an output reference is using the GPS or TAI timescale, and the System Time is set to "UTC", then the GPS Offset box in the Edit GPS Offset window must be populated with the proper timescale offset value in order for the time on the output reference to be correct. Some references (like GNSS) provide the timescale offset to the system. In the event that the input reference being used does not provide this information, it must be set in through the **Offsets** panel of the **Time Management** page.

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 SecureSync 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 SecureSync outputs will be provided in the same timescale that is selected in the System timescale field. The NTP output for network synchronization and the time stamps included in all log entries will be in the same timescale as the configured System timescale. For example, if "GPS" is selected as the System timescale, the log entries and the time distributed to the network will all be in GPS time (time broadcasted directly from the GNSS constellation).

3.2.1.3 Manually Setting the Time

For some applications, it may not be necessary to synchronize SecureSync 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 224.

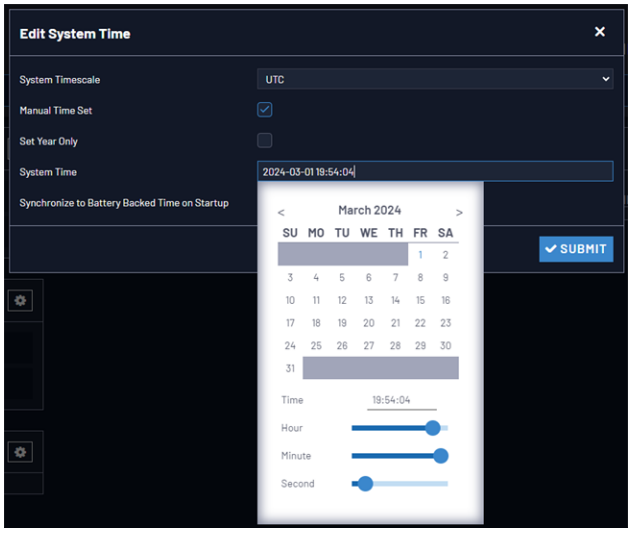


Note: If synchronization to UTC is NOT required, it is advisable to set a time in the past or future, so as to avoid users inadvertently considering the distributed time to be genuine.

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 217 and "The "User/User" Reference" on page 224.
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 223.

3.2.1.4 Using Battery Backed Time on Startup

Upon system startup, by default SecureSync 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 SecureSync 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)) SecureSync's System Clock will regularly update the battery-backed time.

Another factor impacting the accuracy of the battery-backed time is how long a SecureSync unit is powered off: Any significant amount of time will cause the battery-backed RTC to drift, i.e. the battery-backed time will become increasingly inaccurate.

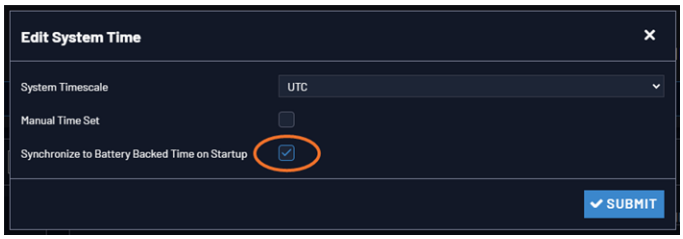
The battery used for the RTC is designed to last for the lifetime of the product.

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 217.

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, SecureSync 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.

SecureSync can be alerted of impending Leap Seconds by any of the following methods:

- **GNSS Receiver** (if available as an input reference): The GNSS satellite system transmits information regarding a Leap Second adjustment at a specific Time and Date an arbitrary number of months in advance.
- **Input references other than GNSS**: Some of the other available input references (e.g., IRIG, ASCII, NTP) can also contain pending Leap Second notification in their data streams (see chapter below).
- **Manual user input**: SecureSync can be manually configured with the date/-time of the next pending Leap Second. On this date/time, the System Time will automatically correct for the Leap Second (unless the System Time's timescale is configured as either GPS or TAI).

3.2.3.2 Leap Second Alert Notification

SecureSync 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. SecureSync will make the correction at the right time. However, because computers and other systems may not utilize the time every second, the Leap Second correction may be delayed until the next scheduled interval, unless the software properly handles the advance notice of a pending Leap Second and applies the correction at the right time.

3.2.3.3 Leap Second Correction Sequence

The following is the time sequence pattern in seconds that SecureSync will output at UTC midnight on the scheduled day (Note: This is NOT local time midnight; the local time at which the adjustment is made will depend on which Time Zone you are located in).

A. Sequence of seconds output when **adding a second** ("positive Leap Second"):
   - 56, 57, 58, 59, **60**, 0, 1, 2, 3 ...

B. Sequence of seconds output when **subtracting a second** ("negative Leap Second"):
   - 56, 57, **58, 0**, 1, 2, 3, 4 ...

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 SecureSync 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), SecureSync 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 SecureSync installed in the Eastern Time Zone of the US, and desiring the Local Clock to automatically adjust for DST (using the post 2006 DST rules for the US).

1. 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

SecureSync can be synchronized to different time and frequency sources that are referred to as Input References, or just References.

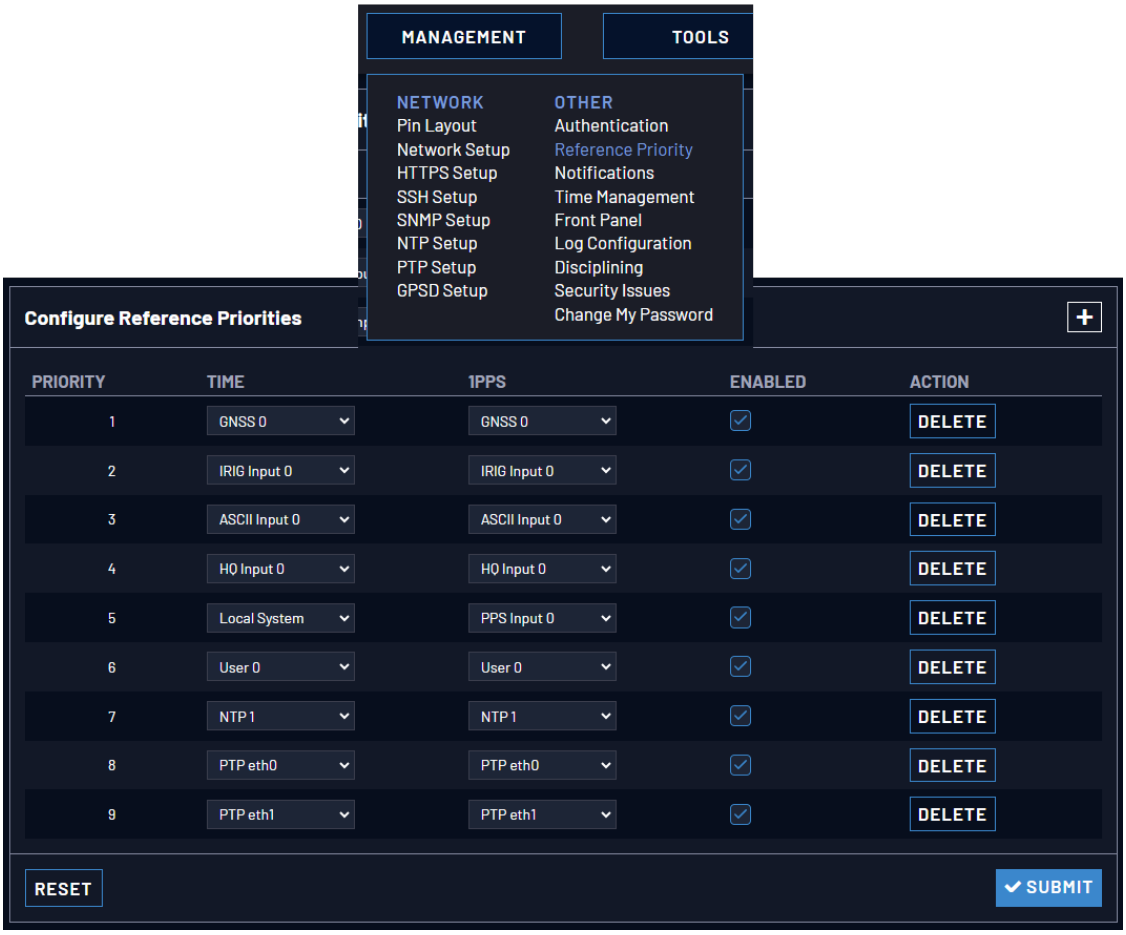
References can be a GNSS receiver, or other sources delivered into your SecureSync unit via dedicated (mostly optional) inputs. It is also possible to enter a system time manually, which SecureSync then can synchronize to.

In order for SecureSync 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 SecureSync 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 SecureSync 2400 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 SecureSync– starting with “0” representing the first feature input. For example:

- IRIG 0 = 1st IRIG input instance
- Frequency 1 = 2nd frequency input instance
- NTP 2 = 3rd NTP input instance

The columns of the **Reference Priority** table are defined as follows:

- **Priority**—Defines the order or priority for each index (row). The range is 1 to 16, with 1 being the highest priority and 16 being the lowest priority. The highest priority reference that is available and valid is the reference that is selected.
- **Time**—The reference selected to provide the necessary “Time” reference.
- **1PPS**—The reference selected to provide the necessary “1PPS” reference.
- **Enabled**—The reference is enabled.
- **Delete**—Removes the Index (row) from the Reference Priority table.

3.3.1.1 Configuring Input Reference Priorities

SecureSync can use numerous external time sources, referred to as "references". As external time sources may be subject to different degrees of accuracy and reliability, you can determine in which order (= priority) SecureSync calls upon its external time and 1PPS references.

For additional information, see also "Input Reference Priorities" on page 217.

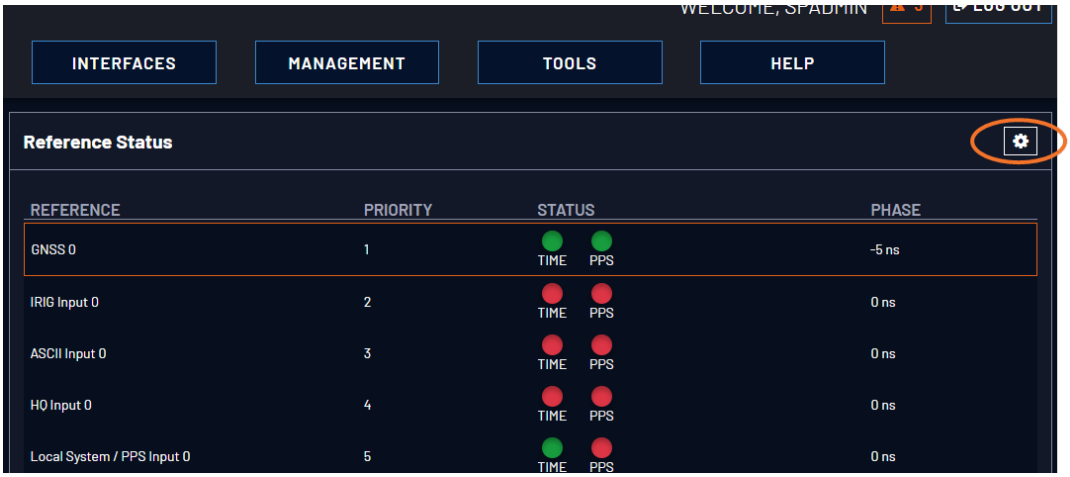
Accessing the Reference Priority Screen

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 SecureSync's references in a table form.
   In this panel you can:

      - Add and configure new references
      - Delete references
      - Enable/disable references

        Note: It is also possible to disable and enable References via the front panel display. Navigate to **Inputs Menu** > **Settings** and select the reference you would like to enable or disable using the ENTER key. You will then be able to edit the STATE to either on or off. To confirm you choice, press the ENTER key Press ENTER again in the confirmation menu.

      - Reorder the priority of SecureSync's references

   c. The **Reference Status** panel

» The **Reference Status** panel provides a real time indicator of the status of the SecureSync's references. It is the same as the **Reference Status** panel on the **HOME** screen of the Web UI.

Adding an Entry to the Reference Status Table

To add a new entry to the **Reference Status** table:

1. Navigate to the **Configure Reference Priorities** screen 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:

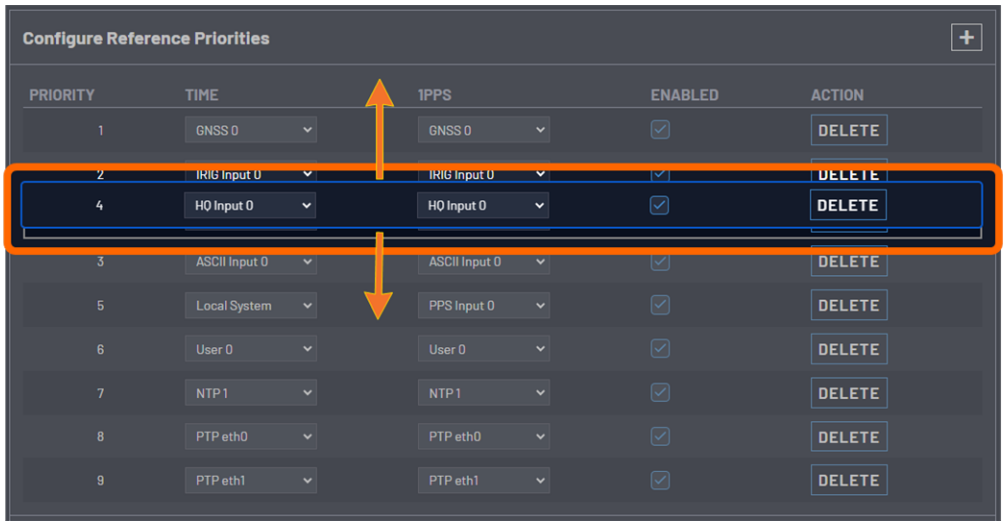
1. Navigate to the **Configure Reference Priorities** screen via **MANAGEMENT > OTHER: Reference Priority**.
2. In the **Configure Reference Priorities** table click the **Delete** button on the right-hand side of the entry you wish to delete.
3. In the pop-up window that opens click **OK** to confirm.

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.



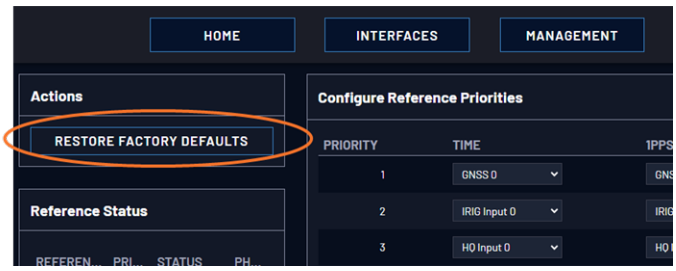
4. Click **Submit.**

> **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. SecureSync 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 SecureSync 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**, SecureSync'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**, SecureSync'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 SecureSync 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: SecureSync 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 SecureSync 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 SecureSync 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.

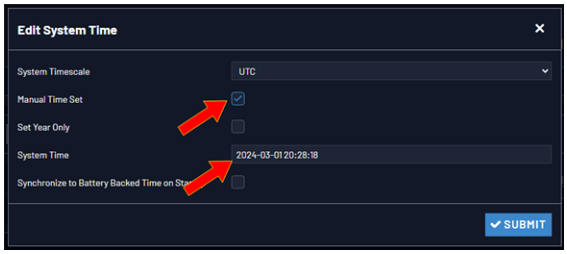
b. No external references are required e.g., if SecureSync is used solely to synchronize computers on a network, with no need for traceable UTC-based timing.

c. To utilize a backup reference as soon as possible after a power cycle or reboot of SecureSync, 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 SecureSync 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 SecureSync 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 209. This will allow SecureSync 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 207.

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 122.

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 122.



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 SecureSync, a “User” needs to be created and enabled in the Reference Priority table. "The "User/User" Reference" on page 224.

In this use case, the objective is to use a hand-set time, in combination with SecureSync'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 204 for more information. SecureSync will go into synchronization using this set time once you click the Submit button.

Note: You will need to repeat this procedure each time SecureSync 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 SecureSync to use itself as a valid reference. This is referred to as “Local System” time.

In order for this to happen, SecureSync 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 SecureSync 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).

SecureSync allows Reference Monitoring by comparing the phase data of references against the System Ontime Point. The phase values shown are the filtered phase differences between each input reference 1PPS, and the internal disciplined 1PPS.

The data is plotted in a graph in real-time. The plot also allows you to display historic data, zoom in on any data range or on a specific reference. A data set can be exported, or deleted.

To monitor the quality of references, 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.

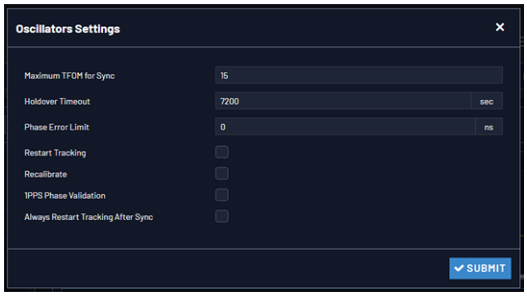
If the higher threshold value is exceeded, the **automatic failover** will cause SecureSync to fall back to its next lower reference (if available).

If no other reference is found, the unit will transition into a 1200-second coasting period. During this coasting period, the TIME and 1PPS references will continue to be considered valid, but SecureSync's oscillator will flywheel. Note that the **PPS** reference status light will turn yellow. After expiration of the 1200 seconds the unit will transition into Holdover.

Should, however, the above-mentioned higher threshold value no longer be exceeded, the unit will remain in the 1200-second flywheel mode until either (a) the lower threshold value is no longer exceeded, or (b) the 1200-second flywheel period expires. In both cases the PPS status light will turn green again.

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 SecureSync 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, SecureSync will emit a Major Alarm and – depending on your system configuration – invalidate the GPS reference causing SecureSync to either transition into Holdover mode (see"Holdover Mode" on page 265), or go out of sync.

Even if you decide to turn off SecureSync'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 SecureSync 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 SecureSync 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 SecureSync 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 361.

To confirm that BroadShield has been activated on your SecureSync unit, navigate to **TOOLS: SYSTEM > Upgrade/Backup**. The center panel **System Configuration** will list the **Options** installed in your unit.

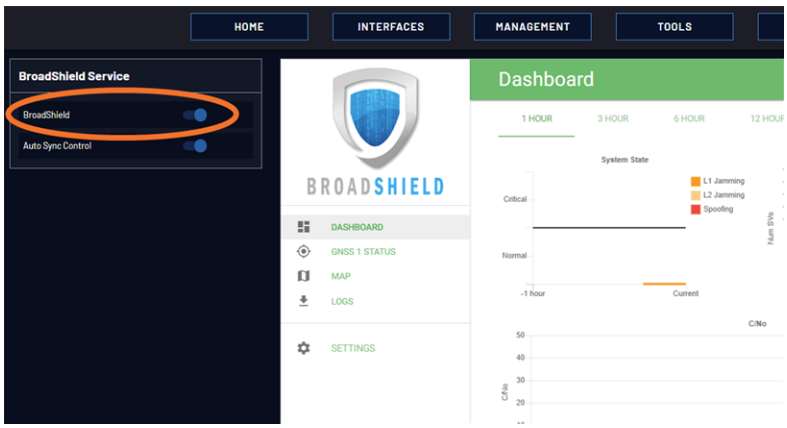
Enabling/Disabling the BroadShield Service

The Broadshield service can be run in two operating modes:

- **BroadShield only**: In the event jamming or spoofing is detected, SecureSync will emit a Major Alarm, however it will continue to consider the GNSS reference as valid, i.e. it will NOT go out of sync.
- **Auto Sync Control**: In the event jamming or spoofing is detected, SecureSync will emit a Major Alarm AND it will go into Holdover mode.

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:

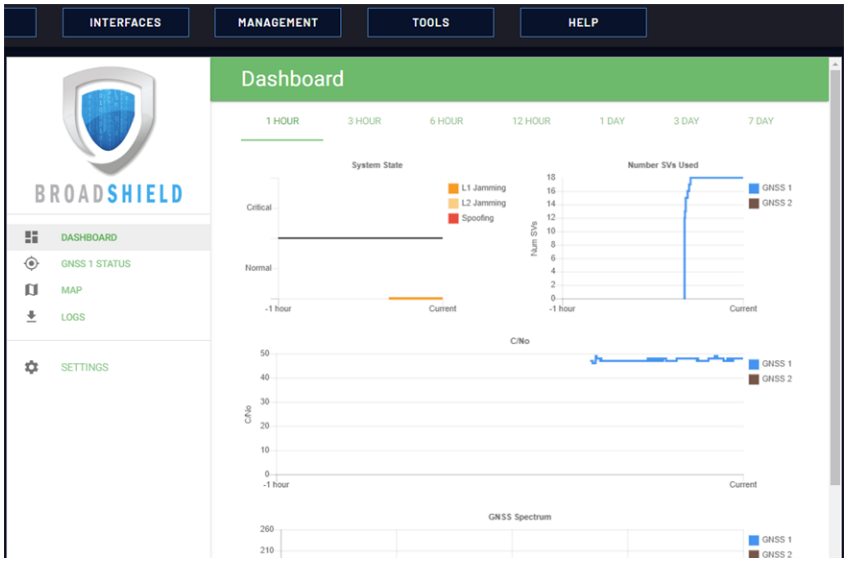
1. Navigate to **TOOLS: SYSTEM > Broadshield**. The embedded Broadshield Web UI will open. If you cannot enable Broadshield from this screen, this license is not present.
2. Click **SETTINGS** to open the following sub-menus:

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 SecureSync is currently not supported.

HOME BASE



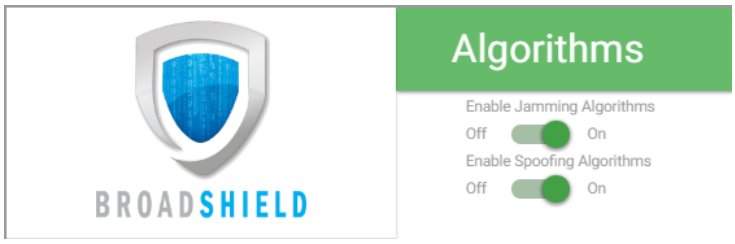
By setting the HOME BASE position you allow BroadShield to use this location as a reference position for spoofing detection: Should BroadShield detect that the geographic position reported by SecureSync's GPS receiver seems to move beyond the set **Alarm Threshold** (even though SecureSync does not move),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

The standard use case is to make your **GNSS 1 Position** your HOME BASE:

1. Should the position fields be populated (other than the **Alarm Threshold**), click CLEAR LOCATION (this will prevent BroadShield from issuing an alarm once you SAVEd the new position.)
2. Click USE in the **GNSS 1 Position** box to apply the settings.
3. The default **Alarm Threshold** is 50 m, i.e. any detected position shift beyond a 50-m circle around the HOME BASE position will cause an alarm. You can change this setting to adjust the sensitivity.
4. Click SAVE to accept the entered values.

A less common use case may be that you want to pre-set the unit's position for later use e.g., if the SecureSync unit will be deployed in a different location: Set a position manually by entering **lat/long** (format: xx.xxxxxx degrees) and **alt**. Note, however, that this may cause a spoofing alarm, since BroadShield detects a difference between the HOME BASE position and the GNSS position.

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 SecureSync system software updates, as they become available.

Monitoring BroadShield

You can use the BroadShield Web UI to monitor the jamming/spoofing status, or the SecureSync Web UI. In the latter case, you will be informed of a Major Alarm, as described below:

BroadShield Alarm

If BroadShield detects a jamming or spoofing event, SecureSync will emit a *BroadShield Critical, Major Alarm* (see illustration below). SecureSync will go into **Holdover** (yellow HOLD status light) and – depending on the **BroadShield Service** setting (see "Enabling/Disabling the BroadShield Service" on page 232) and your SecureSync settings – will either remain in sync (green SYNC status light), i.e. it will continue to output time and frequency signals considered valid, or it will go out of sync (red SYNC light).

You can also configure a notification alarm, see "Enabling/Disabling the BroadShield Service" on page 232.

BroadShield Web UI Monitoring

The BroadShield Web UI will also display real time signal status information, or a map status.

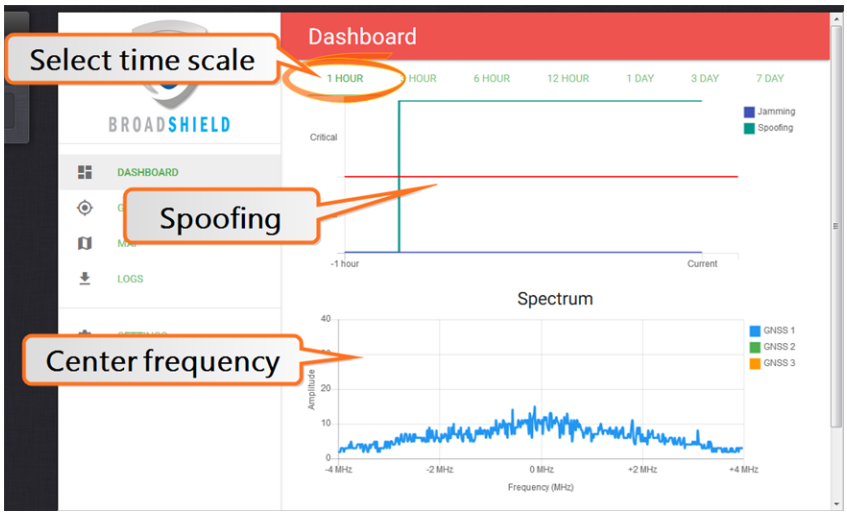
Note: If at any time you receive an error message Failed to connect to the unit, the SecureSync Web UI may have timed out (see "Web UI Timeout" on page 298). Refresh your browser page to log back in.

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 SecureSync 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 SecureSync 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 SecureSync's GNSS receiver.
- **Position**: The position as determined by SecureSync's GNSS receiver.
- **Satellites Used**: The number of satellites currently received by SecureSync. This number includes all satellites currently received for all enabled constellations (see "Selecting GNSS Constellations" on page 259). 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

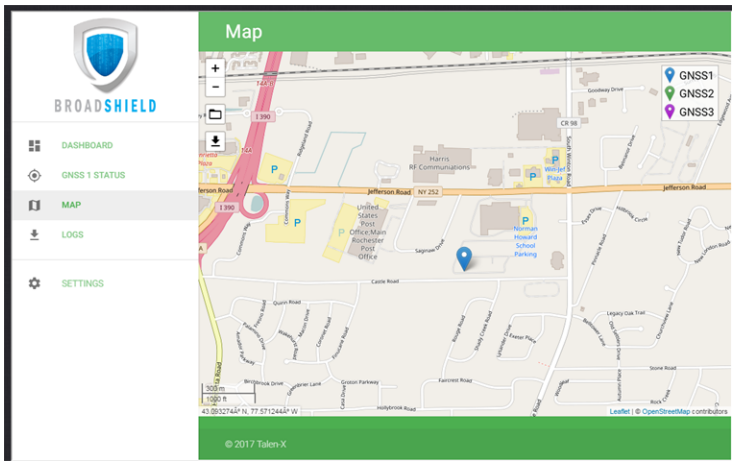
The center of the skyplot represents the antenna position. The skyplot shows all GPS satellites currently being tracked and – if enabled (under **INTERFACES: REFERENCES > GNSS Reference: GNSS 0 > Edit button > Selected Constellations**) – will also display all GLONASS satellites (numbered 65 and higher). Note, however, that GLONASS satellites will not be used by BroadShield. Galileo and Beidou satellites will not be displayed.

Note: Even though SecureSync may be configured to track multiple GNSS constellations (see "Selecting GNSS Constellations" on page 259), 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 SecureSync unit is connected to the Internet.

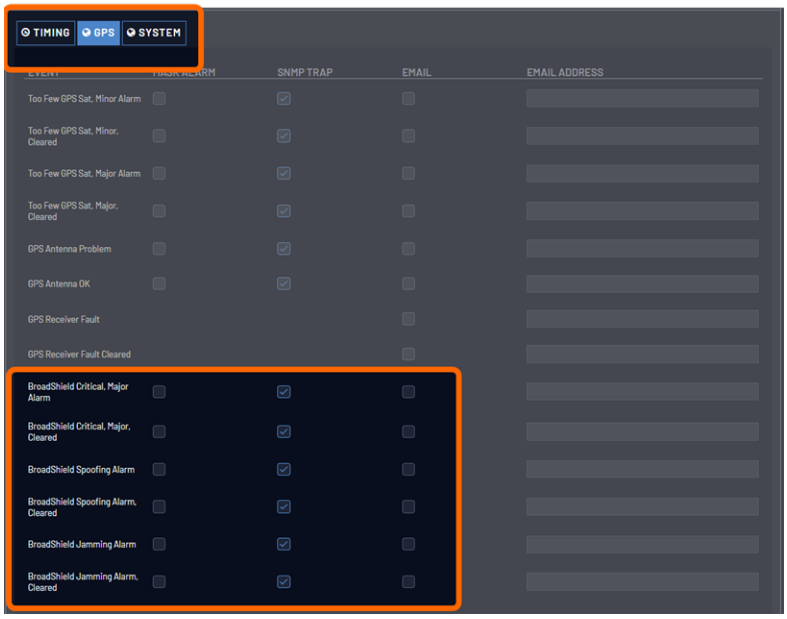
LOGS

- To clear all current logs stored on SecureSync, 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 281.



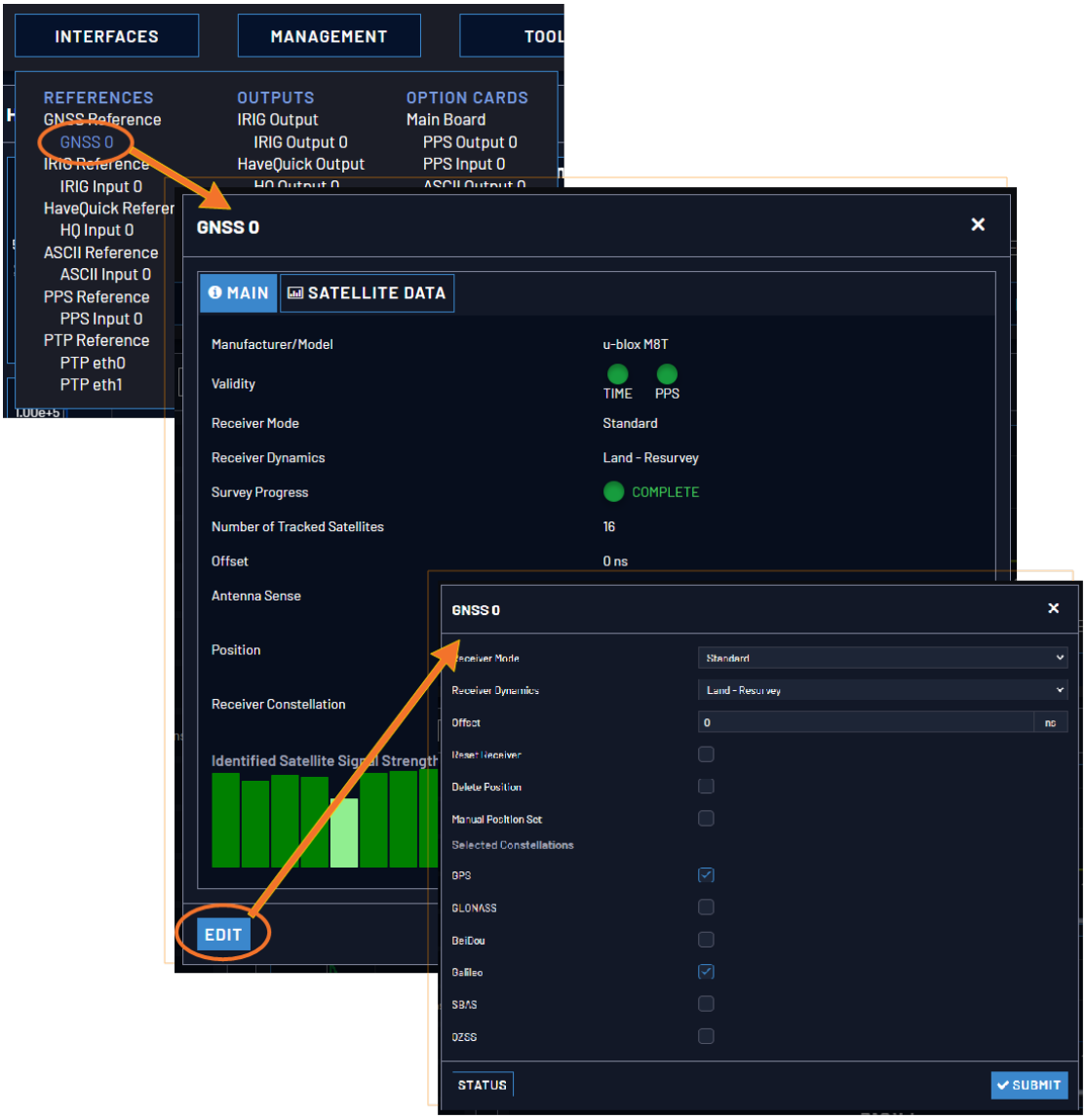
3.3.3 The GNSS Reference

With most applications, SecureSync will be setup such that it utilizes a GNSS signal as the primary (if not the only) timing reference.

SecureSync'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 SecureSync's timing system. The timing system uses the data to control the System Time and discipline the oscillator.

While SecureSync'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 SecureSync unit.
- **Validity**: Status indicator lights for **TIME** and **1PPS** signals: "**On**" (green) indicates a valid signal, "**Off**" (red) indicates that no valid signal is available. 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**: For non-stationary applications.
- **Receiver Dynamics**: (u-blox receivers only); see "Setting GNSS Receiver Dynamics" on page 250.
- **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**: SecureSync'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.



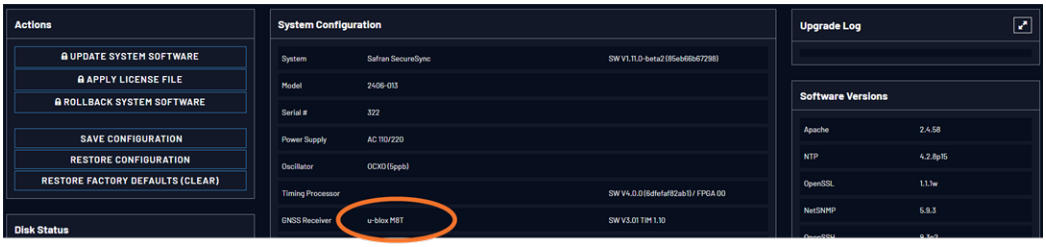
In both graphs, to see a legend of the graphical data, and time-specific status data, click inside the graph, choosing the desired point in time. If necessary, increase the time resolution by dragging the time sliders. A pop-up window will display the legend for that graph, and the status information for the selected time.

3.3.3.2 Determining Your GNSS Receiver Model

Note: All SecureSync models are currently shipped with a u-blox M8T Receiver.

To determine which GNSS receiver model is installed in a SecureSync unit:

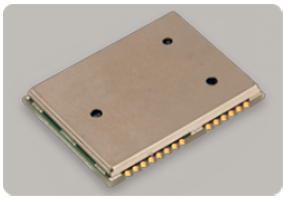
1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. In the **System Configuration** panel, locate the line item **GNSS Receiver**:



GNSS Receiver Models

Safran strives to equip SecureSync with current technology. Depending on the production date of your SecureSync 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 250.
- **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

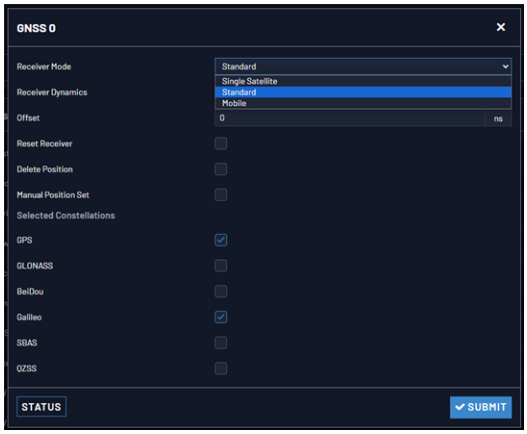
When connected to a GNSS antenna that receives a GNSS signal, SecureSync can use GNSS as an input reference. The factory default configuration allows GNSS satellites to be received/tracked with no additional user intervention required.

However, there are 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 SecureSync 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:

Standard GNSS Receiver Mode

The default GNSS receiver mode is the **Standard Mode**: It is the most accurate, and hence the preferred GNSS receiver mode.

The Standard Mode can be used only for stationary applications, i.e. the SecureSync unit will not be moved. Also, it must be able to track initially at last four satellites in order to complete the survey. (Once the survey is completed, less than four satellites will provide a valid Time and 1PPS.)

In the Standard Mode the **GNSS survey** will initially be performed, once at least four GNSS satellites become available. The GNSS survey is used to determine the exact position and time; it takes 2000 seconds (33 minutes) to complete a survey. During the survey, the GNSS receiver must continue to track at least four satellites, otherwise the GNSS survey will not complete.

Upon completion of the GNSS survey the GNSS receiver will lock-in the calculated GNSS position and will enter **Standard Mode**. Once in **Standard Mode**, the GNSS survey will only be performed again if:

- the unit is halted or rebooted (see "Performing a GNSS Receiver Survey" on page 252).
- the equipment will be relocated to another location and the receiver detects this (applies to most Trimble receivers)
- you manually delete the GNSS position, see "Deleting the GNSS Receiver Position" on page 255.

In the event that SecureSync cannot complete a GNSS survey within 24 hours (e.g., the survey progress does not go beyond 99%), see "Single Satellite GNSS Receiver Mode" below.

Single Satellite GNSS Receiver Mode

The **Single Satellite Mode** is designed for use cases in which it is not possible for the GNSS receiver to 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, i.e. obtain a 3-D fix. In such cases, SecureSync cannot operate in **Standard Mode**. 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:

a. the receiver was able to complete a survey during a time window with good satellite reception, OR you have manually entered a valid position for your antenna location (instructions can be found under "Manually Setting the GNSS Position" on page 256 and "Determining Your Position" on page 258.)

b. the GNSS receiver continues to track at least one qualified satellite.

Note that SecureSync is designed to provide the most accurate time in **Standard Mode**, hence the Single Satellite Mode should only be used if the GNSS receiver could not complete a survey. Note also that Single Satellite Mode can only be used if the SecureSync unit remains stationary at all times.

Mobile GNSS Receiver Mode

In **Mobile Mode** no surveys will be carried out since the position status is updated in near real-time. SecureSync will go into synchronization shortly after beginning to track satellites.

The **Mobile Mode** should only be selected if your SecureSync unit will NOT remain stationary at all times, i.e. instead of being operated in a building, it is installed in a mobile platform (such as a vehicle, ship, plane, etc.).



Note: With SecureSync's GNSS receiver configured in Mobile Mode, the specified accuracies of SecureSync will be degraded to less than three times that of Standard Mode. Standard Mode accuracy of the receiver is less than 50 ns to GPS/UTC (1 sigma), hence Mobile Mode is less accurate than 150 ns to GPS/UTC time (1 sigma).

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.

Note: This option only applies to u-blox M8T receivers (RES-SMT-GG and SAASM GPS do NOT support this.)

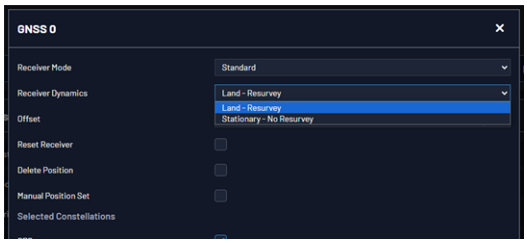
Caution: If you select a setting that does NOT resurvey, and subsequently relocate your unit (antenna) by more than 100 m, u-blox M8Treceivers will NOT detect the new position, and hence provide an incorrect time.

For more information about the **GNSS Survey**, see "Performing a GNSS Receiver Survey" on page 252.

For more information on **Receiver Modes**, see "Selecting a GNSS Receiver Mode" on page 247.

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

The following Receiver Dynamics settings are available:

- **Land (Resurvey)**: [default]
  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 SecureSync 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. Should a unit be relocated, you need to delete its position, thus initiating a new survey.

The following table illustrates the interdependence between Receiver Dynamics, Receiver Mode (see "Selecting a GNSS Receiver Mode" on page 247) 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 SecureSync'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 SecureSync 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.

Verifying GNSS Survey Progress

To see if SecureSync'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).

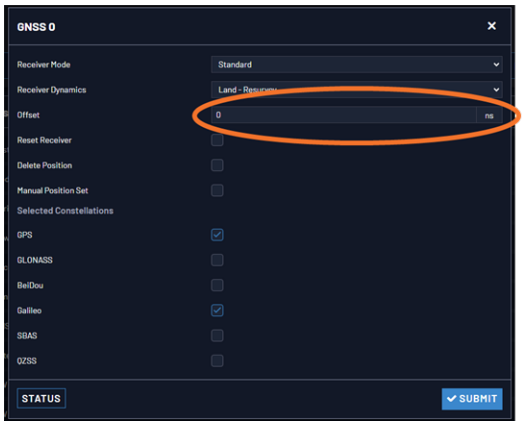
By setting the correct **Offset** value, you can offset the system's on-time point by the **Offset** value to compensate for the antenna and in-line amplifier delays. Under typical conditions, the expected cable and amplifier delays are negligible. You can calculate the delay based on the manufacture's 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

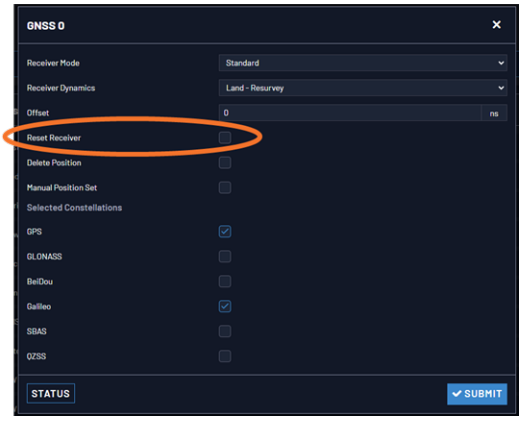
The **Reset Receiver** command causes the GNSS receiver to execute a cold start: All data will be erased from the volatile receiver memory. Only non-volatile memory is preserved.

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 SecureSync 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 SecureSync
- 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 SecureSync

The **Delete Position** command may need to be used if a SecureSync 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 SecureSync not to go into synchronization state.

Sanitization

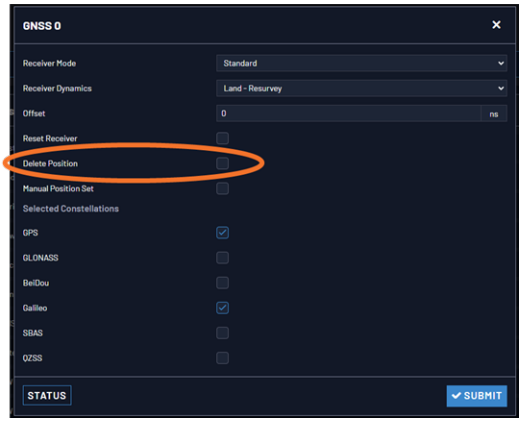
The **Delete Position** command is automatically applied when **sanitizing** a SecureSync unit (ensuring that no trace of position data remains on the unit). See

"Sanitizing the Unit" on page 369.

Deleting the GNSS position

To delete the GNSS position:

1. Disconnect the GNSS antenna from the SecureSync 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. SecureSync 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 SecureSync unit—and thus its onboard GNSS receiver—is a major factor for SecureSync 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 SecureSync 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.

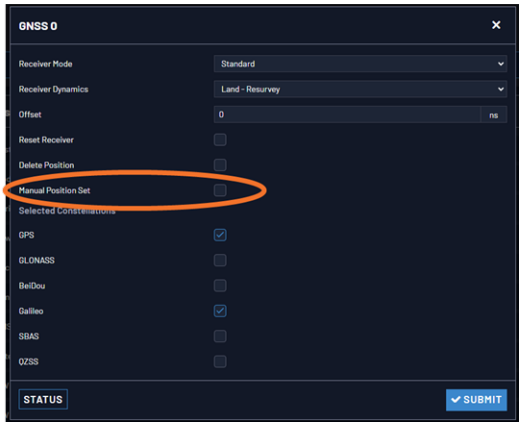
Setting a **Manual Position**, however, i.e. manually applying your current geographic position data (Latitude, Longitude, and Altitude) may be necessary if your GNSS receiver could not complete its survey due to poor reception.

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 SecureSync 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:



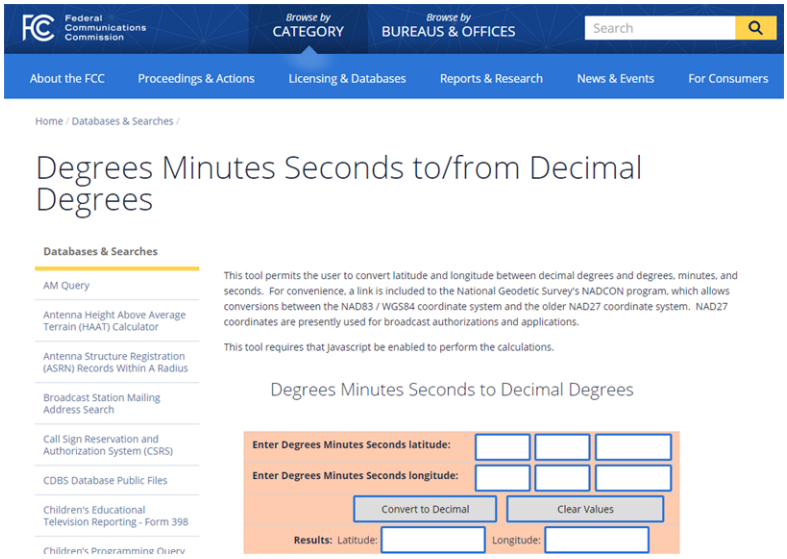
3. Under **Manual Position Set** accurately enter **latitude**, **longitude** (both in decimal degrees), and **altitude** (in meters [WGS 84]) of your GNSS antenna, SecureSync can use this data during the satellite tracking/adjustment process, which typically leads to a quicker "fix". It is recommended to enter the position as accurately as possible.

Determining Your Position

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

SecureSync 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

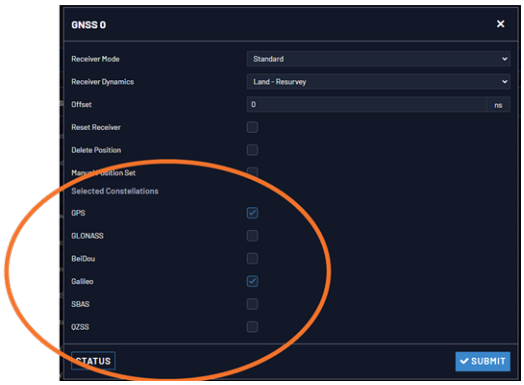
our SecureSync is capable of tracking multiple GNSS constellations simultaneously.

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 SecureSync'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	–

GPS	Galileo	GLONASS	BeiDou
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.

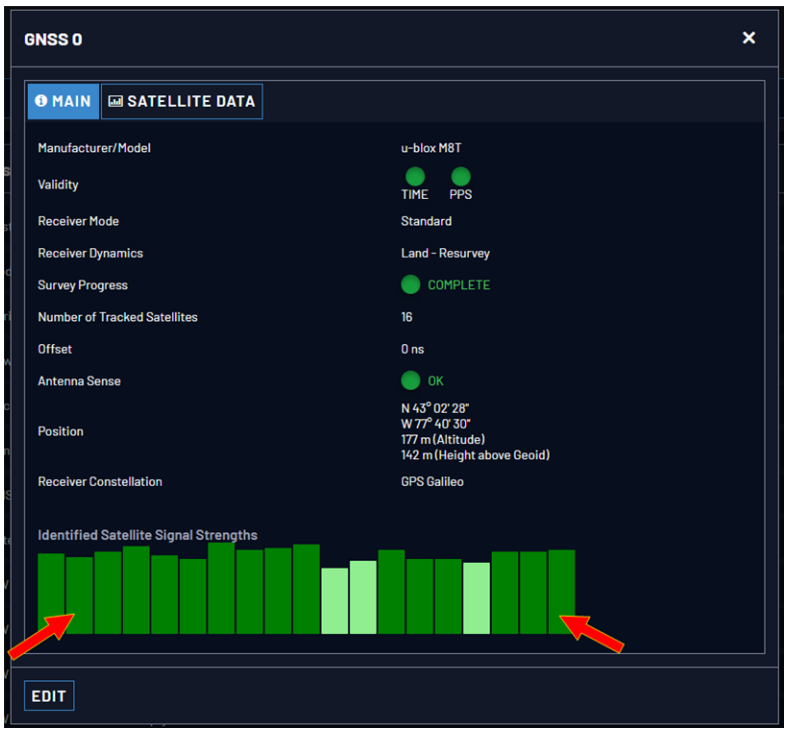
About SBAS

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 SecureSync 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

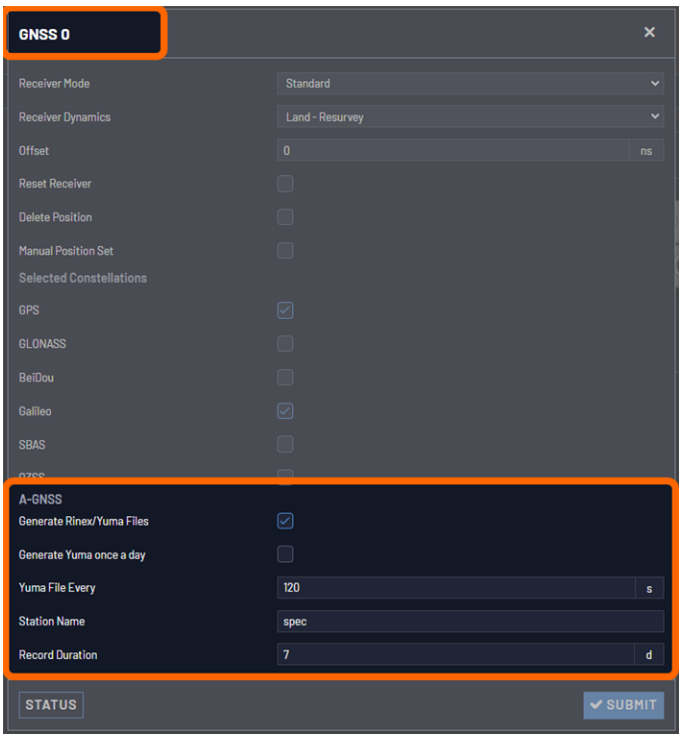
The number next to the letter indicates the satellite number. The number below indicates the signal strength (C/N_o).

3.3.3.11 AGNSS

An **A-GNSS server** allows a SecureSync 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 SecureSync 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 SecureSync, 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, SecureSync 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 SecureSync or via the mapped drive.

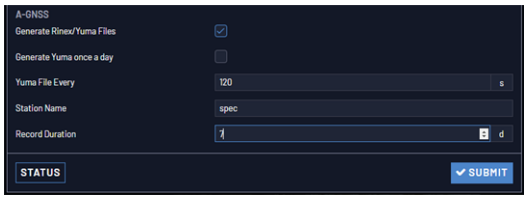
Confirming that the AGNSS RINEX Server License is installed on your unit

» 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:

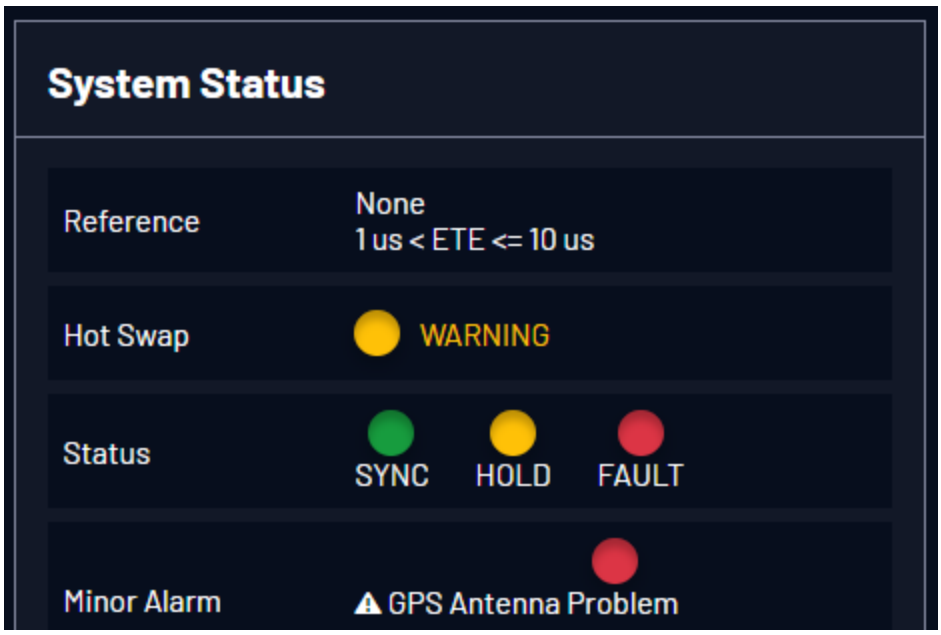
http:// [IP address of your unit]/home/spectracom/xfer/agnss/gps/data/daily/ [YYYY]/ [ZZZ]/15n/spec[ZZZ]0.15n.Z

- 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)

3.4 Holdover Mode



When input references have been supplying input to SecureSync and input from all the references has been lost, SecureSync will not immediately declare loss of time synchronization, but first will go into Holdover mode. While the unit is in Holdover mode, the time outputs are derived from 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 SecureSync 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 SecureSync 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 SecureSync until GPS or another reference has been restored.

How long will the unit remain in Holdover mode?

SecureSync will remain in Holdover mode until either:

a. Any enabled and valid input reference becomes available again: If one or more references return and are declared valid before the Holdover period has expired (even momentarily, i.e. for at least one second), SecureSync exits the Holdover mode and returns to its fully synchronized state.

b. The Holdover Timeout period expires. In this case, SecureSync 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 SecureSync is in Holdover mode, it will power-up and remain in a "not synchronized" state until at least one valid Time and 1PPS input reference becomes available again. While in this state, NTP will be **Stratum 15** and outputs will not be usable. If the input references are restored and then lost or declared not valid again, SecureSync will then go back into Holdover mode.

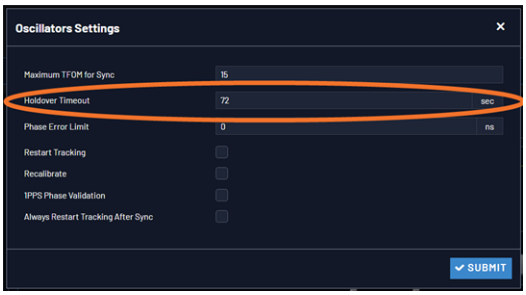
What is "Holdover Timeout"?

Holdover Timeout is the user-configurable allowable time period in which SecureSync remains in Holdover mode before it declares loss of synchronization. Holdover Timeout can be adjusted according to 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 271.

Note: Changes made to the Holdover Timeout always take effect immediately. If SecureSync is in Holdover and the Holdover timeout is changed to a value that is less than the current time period that SecureSync has been 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, SecureSync 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 SecureSync 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 SecureSync 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 SecureSync 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)	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium
After 4 hours	12 µs	1µs	0.5 µs	0.2 µs	0.2 µs

1PPS Phase Drift in Holdover (no reference available)	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium
After 24 hours	450 µs	25 µs	10 µs	1µs	1µs

To find out which type of oscillator is installed in your SecureSync, 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 211.

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 SecureSync is subsequently rebooted or power cycled, time sync will be lost when SecureSync powers back-up. The time will need to be set manually again in order for SecureSync to return to its fully synchronized state. See "The "User/User" Reference" on page 224 and "Manually Setting the Time" on page 207 for more information.

3.5 Managing the Oscillator

The purpose of the built-in oscillator is to provide SecureSync with an accurate and very stable internal frequency source. This allows SecureSync to go into a holdover mode in the event that external time or frequency references are lost or become invalid. However, the oscillator can also be used as a legitimate 1PPS reference during normal operation, in conjunction with an external time reference (for more information, see "Configuring Input Reference Priorities" on page 219.)

SecureSync's internal oscillator is normally disciplined to an input reference (such as GNSS, IRIG input, 1PPS input, etc.) in order to provide the highest degree of oscillator accuracy and to account for oscillator drift. While disciplining (with a 1PPS input reference input present and valid), the oscillator's output frequency is monitored and based on the measured frequency, the oscillator is steered to maintain a very accurate 10 MHz output. If no valid 1PPS input references are present (or input references are present but not considered valid), the oscillator will be in Freerun mode instead.

The Oscillators Settings page provides the user with some control of the disciplining process. This page is also used to configure the length of time SecureSync is allowed to remain in the Holdover mode when all references are lost.

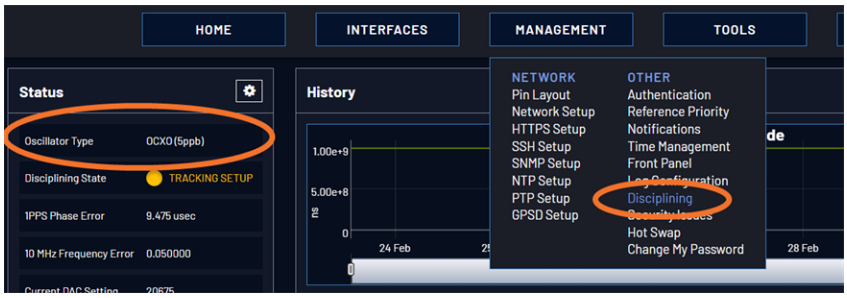
3.5.1 Oscillator Types

SecureSync units are available with different types of internal oscillators:

- **TCXO** (Temperature-Compensated Crystal Oscillator)
- one of two different types of **OCXO** (Oven-Controlled Crystal Oscillator) oscillators, or
- one of two different types of **Rb** (Rubidium) oscillators.

The two different types of OCXO oscillators are a precision OCXO oscillator and a high-precision (low phase noise) OCXO oscillator. The two different types of Rubidium oscillators are a precision Rubidium oscillator and a low-phase noise Rubidium oscillator. All of these internal oscillators are self-calibrating and can be disciplined to a 1PPS input reference for maximum accuracy.

To determine which oscillator is installed in your SecureSync unit, navigate to **MANAGEMENT > OTHER: Disciplining**. The first entry in the **Status** panel on the left indicates the type of oscillator:



Because of its high degree of stability, the Rubidium oscillator provides the greatest ability to extend the hold-over period when input references are not present. Extending the hold-over period allows the unit to provide very accurate and useable time stamps and a 10 MHz output for a longer period of time once time synchronization has been lost.

Note: Oscillators are installed at the factory, in accordance with order specifications; an oscillator cannot be swapped/retrofitted later in the product life cycle (with the exception of repairs).

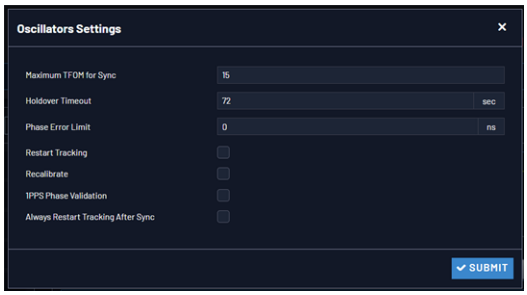
The Rubidium oscillator is atomic in nature but requires no MSDS (Material Safety Data Sheet).

Note: External Oscillator: It is possible for an external oscillator to be locked to SecureSync's 10 MHz output via an external PLL, with the lock state of the external PLL monitored by SecureSync. Contact Safran for more information.

3.5.2 Configuring the Oscillator

SecureSync 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 next 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 268. For additional information on holdover, see "What is "Holdover Timeout"?" on page 266.
   - **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 328.
- **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.

3.5.2.1 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 SecureSync's estimation of how accurately it is synchronized with its time and 1PPS reference inputs, based on several factors, known as the **Estimated Time Error** or ETE. The larger the TFOM value, the less accurate SecureSync believes it is aligned with its 1PPS input that is used to perform disciplining. If this estimated error is too large, it could adversely affect the performance of oscillator disciplining. The available TFOM range is 1 through 15. You may refer to the following for the TFOM to ETE conversions:

Table 3-5: TFOM to ETE conversion

Reported TFOM Value	Estimated Time Error (ETE)
1	<= 1 nsec
2	1 nsec < ETE <= 10 nsec

Reported TFOM Value	Estimated Time Error (ETE)
3	10 nsec < ETE <= 100 nsec
4	100 nsec < ETE <= 1 µsec
5	1 µsec < ETE <= 10 µsec
6	10 µsec < ETE <= 100 µsec
7	100 µsec < ETE <= 1 msec
8	1 msec < ETE <= 10 msec
9	10 msec < ETE <= 100 msec
10	100 msec < ETE <= 1 sec
11	1 sec < ETE <= 10 sec
12	10 sec < ETE <= 100 sec
13	100 sec < ETE <= 1000 sec
14	1000 sec < ETE <= 10000 sec
15	ETE > 10000 sec

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):

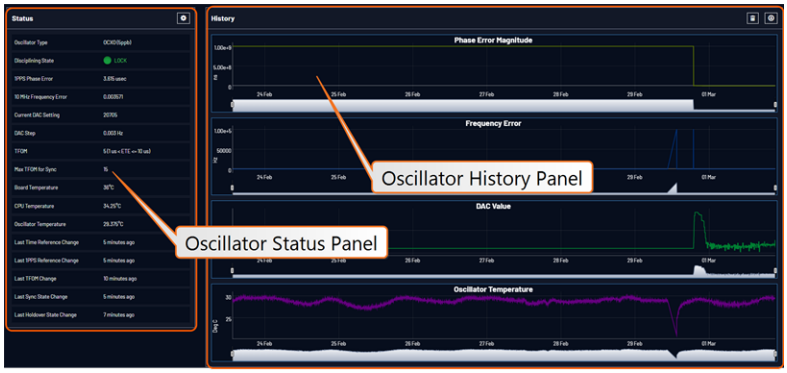
This will cause the TFOM to start to decrease faster. Once TFOM no longer exceeds MaxTFOM because the **System 1PPS** is now much closer to the **reference 1PPS**, the disciplining slows back down again as the system 1PPS continues to be brought into alignment with the selected 1PPS input.

3.5.3 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 SecureSync'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 271), or automatically via a pre-set Phase Error Limit, will quickly reduce the phase error.
- 10 MHz Frequency Error: An internal estimated calculation (in Hertz) of the internal oscillator's frequency error, based on the phase accuracy error at the beginning and end of a frequency measurement window (the length of this window will vary depending upon the type of oscillator installed and the oscillator adjustment algorithm).
- Current DAC Setting: Current DAC value, as determined by the oscillator disciplining system. The value is converted into a voltage that is used to discipline the oscillator. A stable value over time is desirable and suggests steady oscillator performance (see also the graph in the History Panel).

- DAC Step: Step size for adjustments to the internal oscillator, as determined by the oscillator disciplining system. Larger steps = quicker, but coarser adjustments. The step size is mainly determined by the type of oscillator.
- TFOM: The Time Figure of Merit is SecureSync's estimation of how accurately the unit is synchronized with its time and 1PPS reference inputs, based on several factors, known as the Estimated Time Error or ETE. The larger the TFOM value, the less accurate SecureSync believes it is aligned with its 1PPS input that is used to perform disciplining. If this estimated error is too large, it could adversely affect the performance of oscillator disciplining. The available TFOM range is 1 through 15.
- Max TFOM for Sync: Value, as set under "Configuring the Oscillator" on page 271
- 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 SecureSync'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.

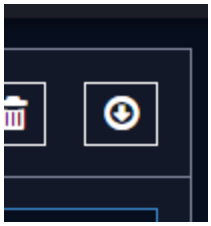
Clicking on the **Delete** icon in the top-right hand corner will erase all current oscillator log data.

Clicking on the **Download** arrow icon will download the latest oscillator log data as a `.csv` file.

3.5.4 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.

CHAPTER 4

System Administration

The following topics are included in this Chapter:

4.1 Powering Up/Shutting Down 278
4.2 Notifications 281
4.3 Managing Users and Security 290
4.4 Miscellanous Typical Configuration Tasks 317
4.5 Quality Management 322
4.6 Updates and Licenses 359
4.7 Backing-up and Restoring Configuration Files 362

4.1 Powering Up/Shutting Down

4.1.1 Powering Up the Unit

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

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

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



Figure 4-1: SecureSync front panel

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

For additional information, see "Status LEDs" on page 4 and "Status Monitoring via Front Panel" on page 322.

4.1.2 Shutting Down the Unit

To shut down the unit gracefully, it is recommended to employ the Halt command.

To learn more, see "Issuing the HALT Command Before Removing Power" on the facing page.

4.1.3 Issuing the HALT Command Before Removing Power

Gracefully shutting down SecureSync 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.
- SecureSync's file system will be synchronized, which under some circumstances will allow for faster startup next time the unit will be powered up.

The HALT command may be issued to the SecureSync via:

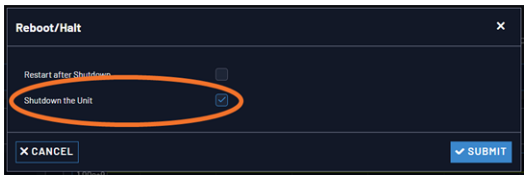
- the **Web UI**
- the front panel **keypad**
- the front panel **serial port.**

> **Note:** Wait 30 seconds after entering the HALT command before removing power.

Once the HALT process has been initiated, the front panel display will show **halting** and the time display will stop incrementing.

Issuing a HALT Command via the Web UI

1. Navigate to **TOOLS > SYSTEM: Reboot/Halt**.
2. The **Reboot/Halt** window will display. Select the **Shutdown the Unit** checkbox.



3. Click **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 front panel USB or rear panel serial port, telnet connection or SSH connection, type `halt` <Enter> to halt the unit for shutdown.

For more information on SecureSync commands, see "CLI Commands" on page 577.

Note: After issuing the HALT command wait 30 seconds before you remove power.

Issuing a HALT Command via the Front Panel:

1. Press the POWER menu button to switch the front panel display to the Power Menu. Verify that you are under the Management sub menu (use the left and right arrow keys if necessary).
2. Press DOWN until **Halt** is highlighted. Press the ENTER button in the center of the keyapd once to activate the halt, and then press it again to confirm your choice in the confirmation menu to the right.

Once you have halted your SecureSync, power must be removed (unplugged) and reapplied in order to restart the unit.

4.1.4 Rebooting the System

To reboot SecureSync via the Web UI:

1. Navigate to **TOOLS > SYSTEM: Reboot/Halt**.
2. Select the **Restart after Shutdown** box in the **Reboot/Halt** window.



3. SecureSync will now be rebooted and be accessible again shortly thereafter.

Rebooting via LCD/Keypad, Serial Port, Telnet, SSH, SNMP

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

Reboot is also is available to be performed through an `snmpset` operation. For more information on SecureSync commands, see "CLI Commands" on page 577.

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

Rebooting via the front panel

1. Press the POWER menu button to switch the front panel display to the Power Menu. Verify that you are under the Management sub menu (use the left and right arrow keys if necessary).
2. Press DOWN until **Reboot** is highlighted. Press the ENTER button in the center of the keypad once to activate the halt, and then press it again to confirm your choice in the confirmation menu to the right.

During reboot, the front panel display will read **Rebooting** and the time display will stop incrementing.

4.2 Notifications

If an event occurs e.g., SecureSync transitions into Holdover, or a short is detected in the GNSS antenna, SecureSync 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 SecureSync events that can generate a notification to be sent are located under different tabs in the Notification Events panel: **Timing**, **GPS**, and **System**.

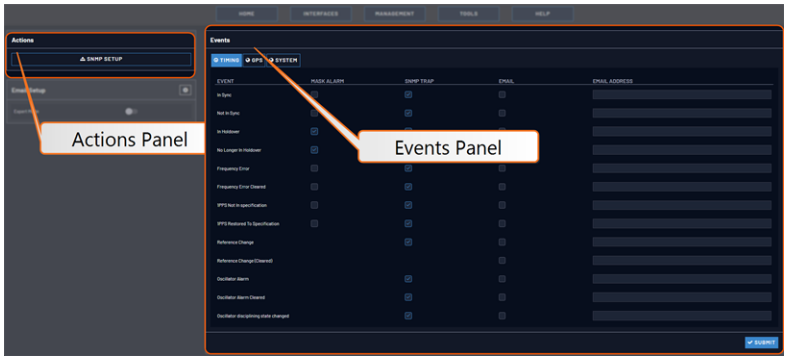
The SecureSync Events that can automatically trigger a notification are listed in the **Event** column. It is possible to:

- 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.

4.2.1 Configuring Notifications

To configure Notifications:

1. Navigate to **MANAGEMENT > OTHER: Notifications**. The **Notifications** screen will display:



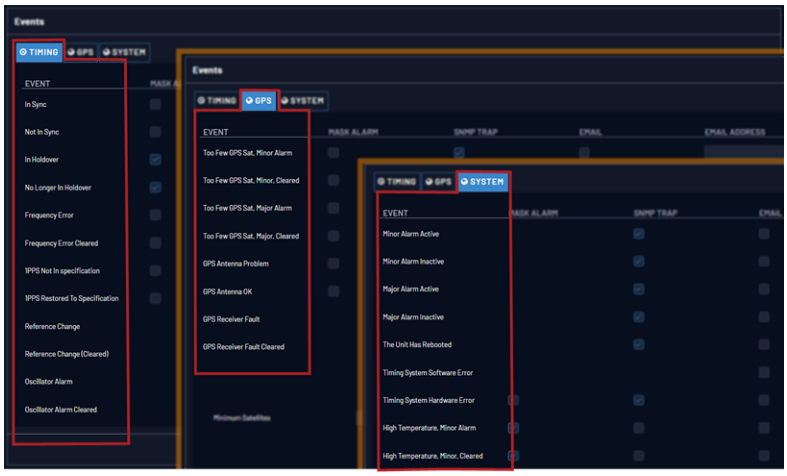
It is divided into two panels:

- The Actions panel, featuring:
  - The **SNMP Setup** button: See "SNMP" on page 99.
  - The **Email Setup** button: Configure SecureSync'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 287.

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.

4.2.2 Notification Event Types

The following types of events can be used to trigger notifications:

4.2.2.1 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

4.2.2.2 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.

4.2.2.3 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
- Fan Fault, Major Alarm
- Fan Fault, Major, Cleared

4.2.3 Configuring GPS Notification Alarm Thresholds

SecureSync 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 SecureSync loses the GNSS reference.

Note that SecureSync 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

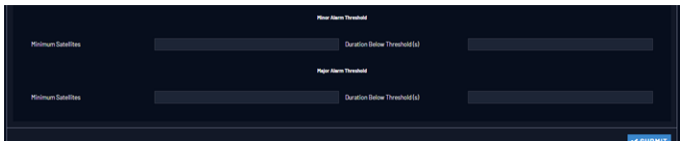
your unit. In Stationary mode, and for SAASM units, the minimum number of satellites is normally 4 (four). Hence, it would be prudent to set the Minor Alarm Threshold to 8, and the Major Alarm Threshold to 6.

Note: While GPS Notification Alarms can be used in Mobile GNSS receiver mode, it is not advisable.

To determine which **GNSS receiver mode** your SecureSync is using and **how many satellites** your SecureSync unit is currently receiving, navigate to **INTERFACES > REFERENCES: GNSS 0**. See also "Reviewing the GNSS Reference Status" on page 241.

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 374.

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).

4.2.4 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**.



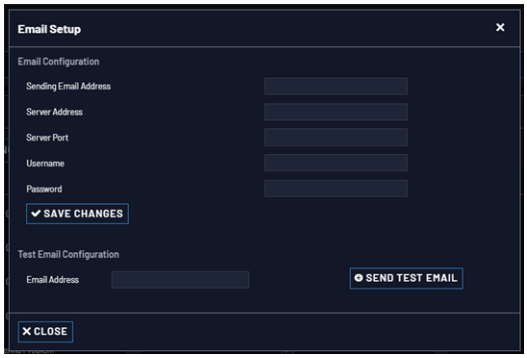
For more information on SNMP, see "SNMP" on page 99.

4.2.5 Setting Up Email Notifications

The **Email Setup** window provides a means to configure SecureSync 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



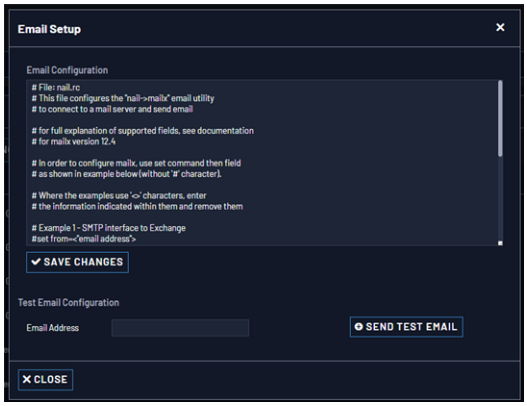
4. To test your settings:
   - In the **Test Email Address** field, enter an email address.
   - Click the **Send Test Email** button.
   - A notification that your email has been sent will appear at the top of the window.

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 SecureSync with an Email Exchange server; and the other is for sending emails via Gmail:

4. To configure the applicable example email configuration, delete the comments ("#") from each line and replace the "<>" with the appropriate values for your particular email server (such as the user name and password for your Email server).

Example 1: 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.

4.3 Managing Users and Security

4.3.1 Managing User Accounts

Users need to authenticate as the login to SecureSync. The system administrator is responsible for maintaining a list of user accounts (user names, passwords etc.) via the **MANAGEMENT > OTHER: Authentication** screen of the SecureSync Web UI (HTTP/HTTPS). Note that user accounts CANNOT be created or edited via CLI commands using telnet or SSH.

4.3.1.1 Types of Accounts

There are three types of accounts:

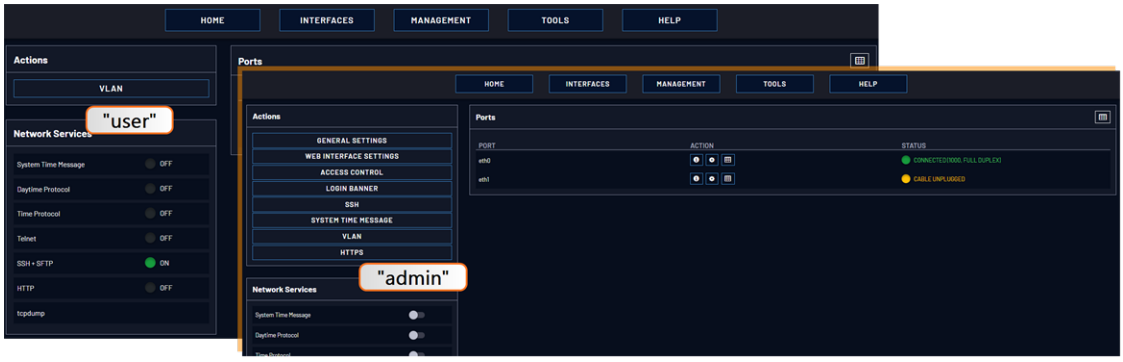
Account Type	Permissions
"user"	These accounts are intended for users only e.g., operators. These "user" accounts are read-only accounts, i.e. they do not allow any editing rights and are restricted to reviewing status-related information. The Web UI will not show (or gray-out) any editing functionality.
"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.

4.3.1.2 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

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.

4.3.1.3 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: ! @ # $ % ^ & * ( )

4.3.1.4 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:



SecureSync 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 SecureSync 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 next 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 SecureSync system software
- Resetting the SecureSync configuration
- Clearing log files
- Changing Disciplining Setup options
- Changing configuration options for the following protocols or features:
  - NTP
  - HTTPS, SSH
  - LDAP/RADIUS
  - SNMP (with the exception of configuring SNMP notifications).

To change 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.

4.3.2 Managing Passwords

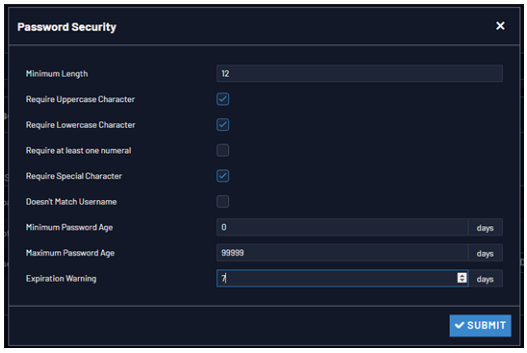
Caution: For security reasons, it is advisable to change the default credentials.

Note: Password changes cannot match any 10 previous passwords used on that specific account.

4.3.2.1 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.



4.3.2.2 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 SecureSync Web UI.

Caution: Once you log in to your SecureSync, you will be prompted to update your spadmin password.

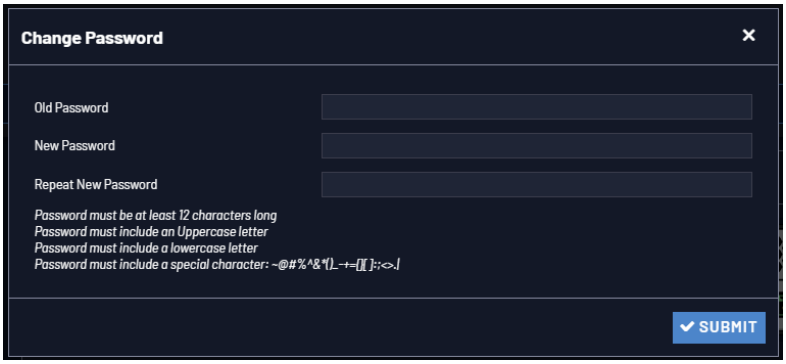
Note: To follow this procedure, you must be logged in as the `spadmin` user. If you are unable to login as `spadmin`, follow the procedure outlined in "Lost Password" on the next page.

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 next 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 290.

4.3.2.3 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.

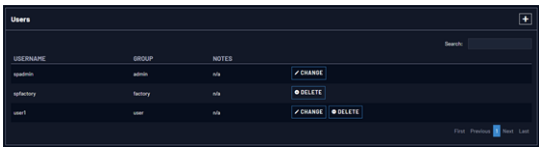
If you do not know the password for any user with administrator rights, your only options are:

- restore the factory defaults via the front panel (press the power button and select **Restore factory defaults**), or:
- 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 front panel USB or rear panel seial console 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.

4.3.3 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.

4.3.4 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 SecureSync. LDAP allows the login password for user-created accounts to be stored and maintained in a central LDAP or server on the network. This function greatly simplifies password management. Instead of having to change the password in many network appliances when a password needs to be changed, if a user password is changed in the LDAP server, it automatically changes the login password for all of the appliances that are using the LDAP server to authenticate a user login.

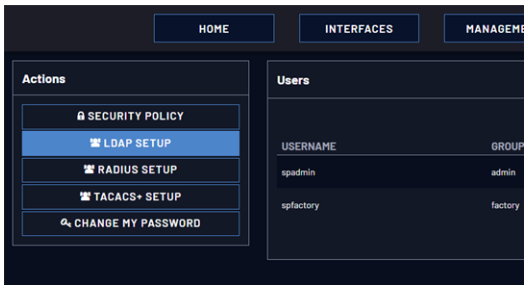
In order to use the LDAP authentication capability of SecureSync, it needs to first be configured with the appropriate settings in order to be able to communicate with the LDAP server(s) on the network.

Note: SecureSync requires commas between multiple values entered in the same field (periods not accepted).

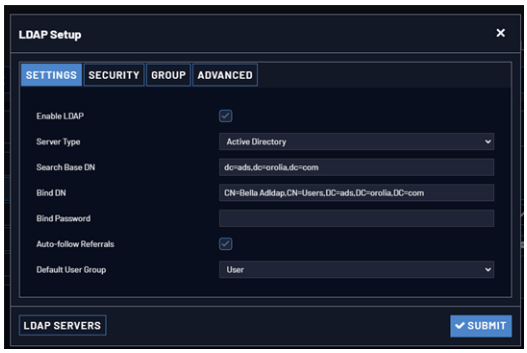
Caution: If you plan on using LDAP, configure it with diligence. If not required, Safran recommends to keep LDAP disabled.

Configuring LDAP authentication

1. Navigate to **MANAGEMENT > OTHER: Authentication**.
2. In the **Actions** panel, click the **LDAP Setup** button.



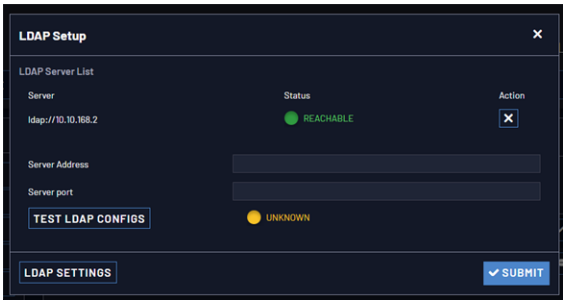
3. The **LDAP Setup** window will display.



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:

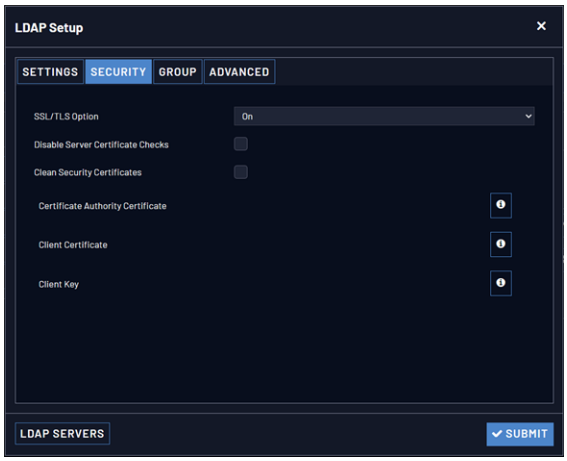
- **Server Type**: This must be the correct type—check with your LDAP server administrator if you are not sure which you are using. You have a choice of:
  - **Active Directory**: This will be used when the LDAP server is a Windows server. If you choose Active Directory, you are required to fill out 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.



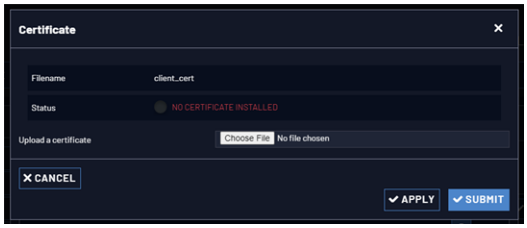
- Select an option from **SSL/TLS Option** to enable LDAP SSL/ TLS:
  - On (default) — Enables TLS encryption.
  - Off
  - Start TLS — Enables TLS encryption in compliance to FIPS 140-2.
- Select **Disable Server Certificate Checks** to disable verification of the certificate presented by the server.
- Select **Clean Security Certificates** to remove all certificates currently stored on SecureSync (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.

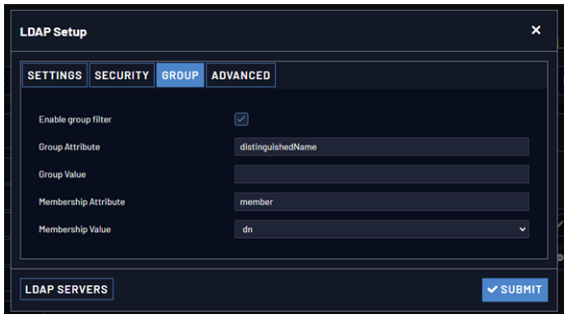
e. Verify the **Status**:

- 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.

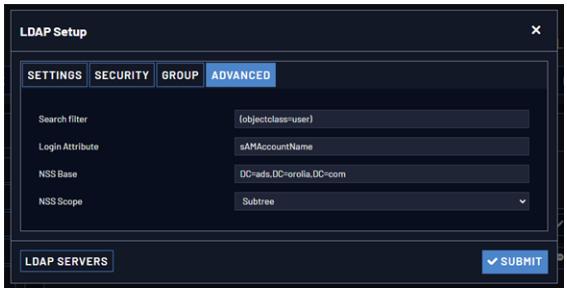
b. Enter information for:

- **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.

4.3.5 RADIUS Authentication

RADIUS authentication provides a means to use an external RADIUS server for authentication purposes when logging in to SecureSync. 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 SecureSync, 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 SecureSync 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: SecureSync requires commas between multiple values entered in the same field (periods not accepted).

Example:

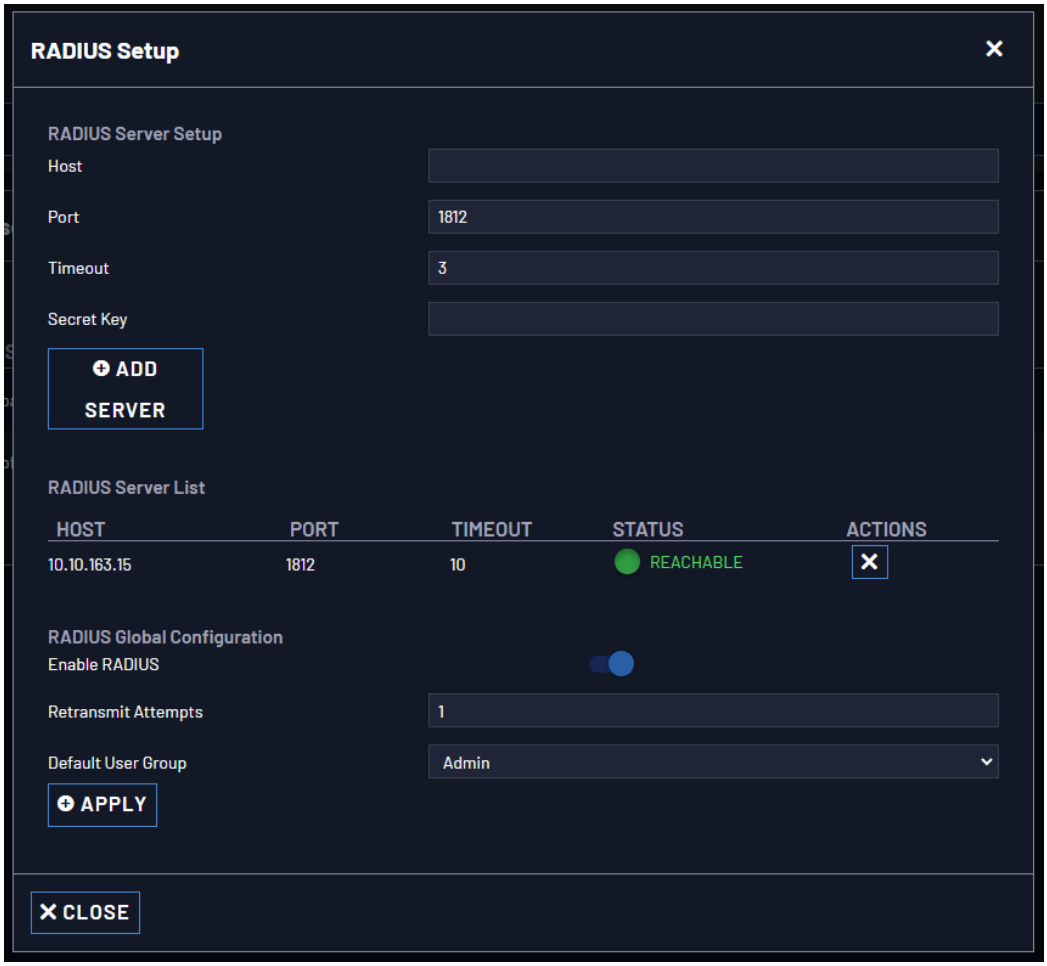
A user with the username user3 on the RADIUS server will not be able to login to a SecureSync unit, if on that unit a local user account with the username user3 exists. However, once the user deleted the local user3 account, she will be able to login with the RADIUS user3 account.

See also "TACACS+ Authentication" on page 310

4.3.5.1 Enabling/Disabling RADIUS

To enable or disable the use of RADIUS authentication on a SecureSync 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:

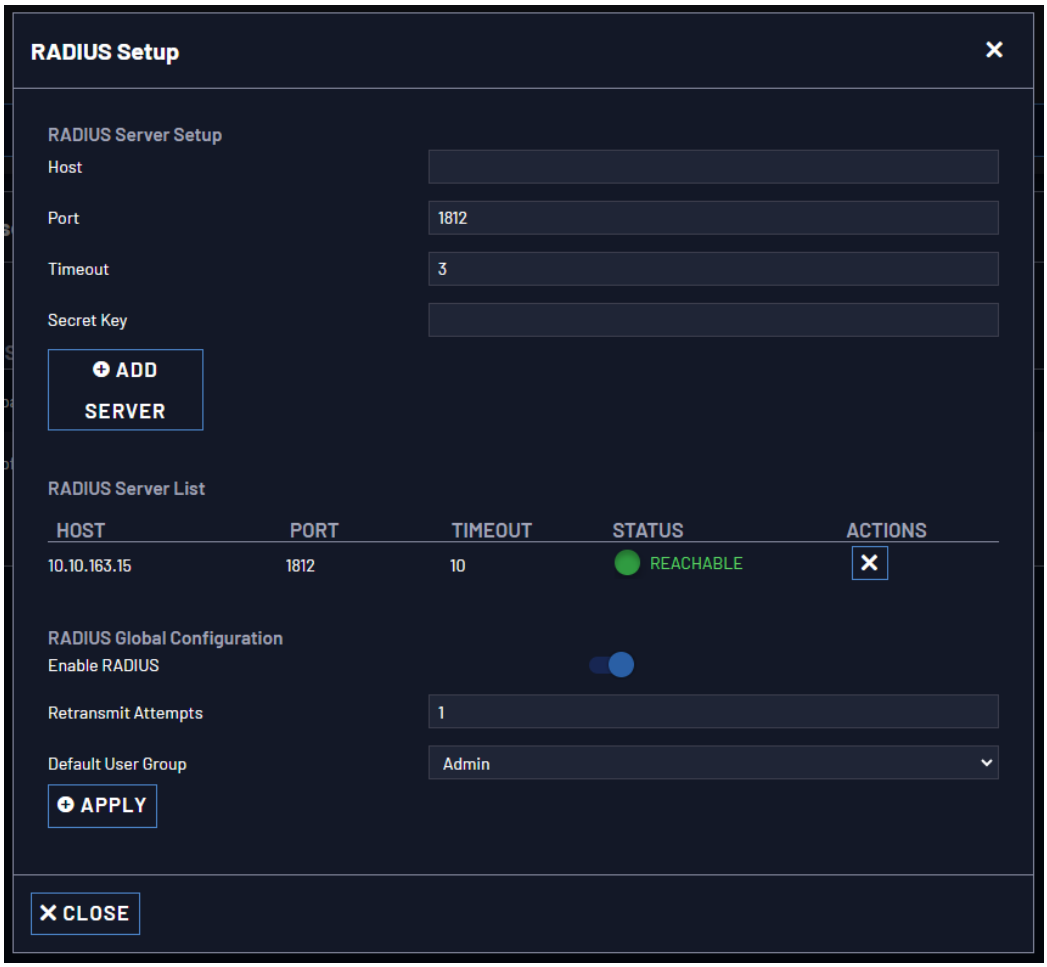


3. Click the **ON/OFF** toggle under Enable RADIUS to enable or disable the feature.
4. If you are enabling the service, in the **Retransmit Attempts** field, select the number of retries for SecureSync to communicate with the RADIUS server (default = 0).
5. Configure the **Default User Group** to select your preferred default user permissions level (Admin or User)
6. Click Submit.

4.3.5.2 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 SecureSync and the RADIUS server (the key is used to generate an MD5 hash).
   - **Timeout**: [seconds] Defines the Timeout that SecureSync will wait to communicate with the RADIUS server e.g., 10 seconds.

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: SecureSync supports multiple RADIUS servers. The system performance, however, will be negatively affected by a large number of servers or invalid servers, respectively.

4.3.6 TACACS+ Authentication

Terminal Access Controller Access-Control System Plus (TACACS+) is a protocol that handles authentication, authorization, and accounting (AAA) services. SecureSync supports **pam_tacplus**, allowing users to validate their username/password when logging into SecureSync via a TACACS+ server. Currently, http/https/ssh/telnet/ftp protocols are supported, i.e. you can login to a SecureSync 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. SecureSync 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 SecureSync 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 306

4.3.6.1 Enabling/Disabling TACACS+

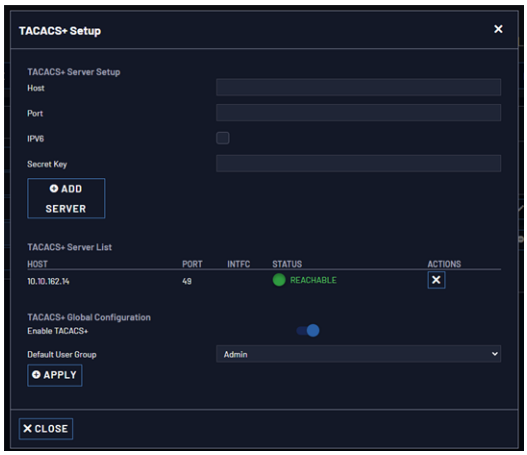
To enable or disable the use of TACACS+ authentication on a SecureSync unit:

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.

4.3.6.2 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: SecureSync supports multiple TACACS+ servers. The system performance, however, will be negatively affected by a large number of servers or invalid servers, respectively.

4.3.7 Web UI Security Dashboard

The Security Dashboard Web UI page contains tabs for both security issues and security compliance.

4.3.7.1 Security Issues

The SecureSync 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.

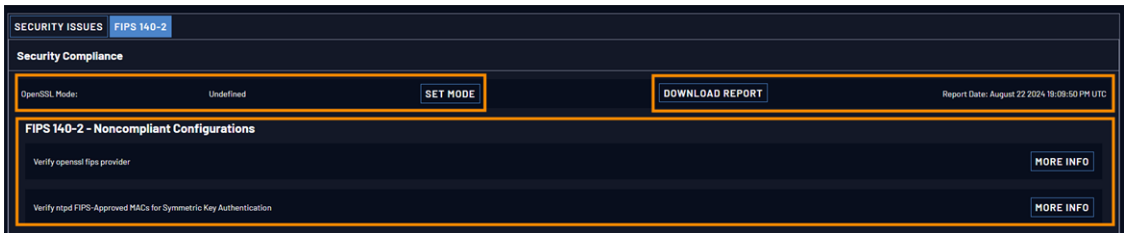
From the Security Issues tab, you can review the warnings listed for your unit, or select active warnings to be redirected to the correct field to fix the warning. You may also choose to ignore these warnings. Correcting or ignoring the warnings will both remove the warning symbol from your Web UI banner.

4.3.7.2 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:

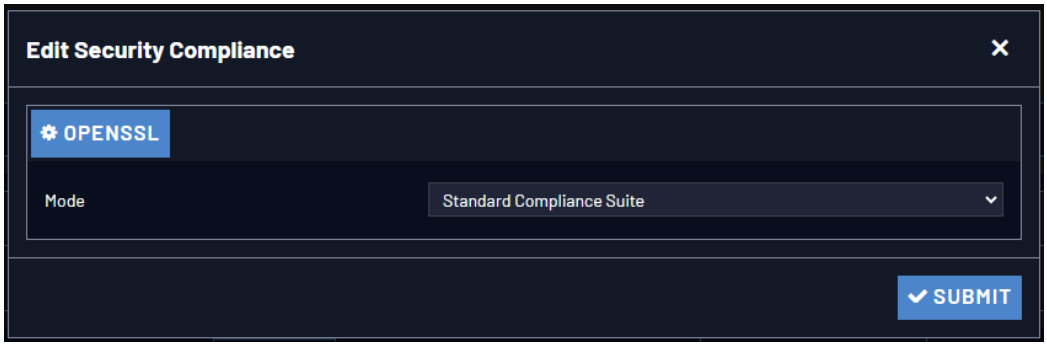
- **Legacy Enhanced:** uses non-compliant/legacy crypto module(s) (requires confirmation dialog). Enables extended functionality, including legacy algorithms that are no longer in common use while maintaining FIPS compliance.
- **Standard Compliance Suite [default]:** prefers FIPS-compliant crypto module, 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

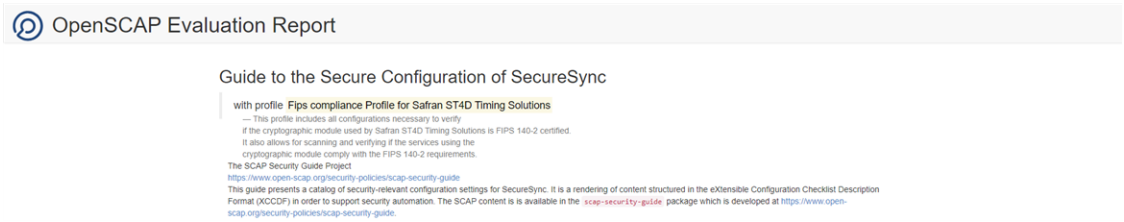
- **NTP:** Only the **SHA1** FIPS-approved algorithm should be used for NTP keys. Non-FIPS-approved MACs like MD5, SHA, MD4, MDC2, and RIPEMD160 in `/etc/ntp/keys/ntp.keys` will no longer function. (MDC2 will function with Legacy Enhanced mode).
- **SNMP:** Only **SNMPv3** with SHA for Auth Type and 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.

4.3.8 HTTPS Security Levels

SecureSync 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.

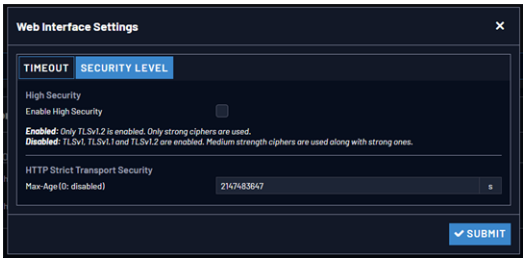
Browser Support

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.

4.4 Miscellanous Typical Configuration Tasks

4.4.1 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 SecureSync 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.

4.4.2 Configuring the Front Panel

The front panel of the SecureSync 2400 Time and Frequency Synchronization System can be configured to display your local time and can be locked to prevent unwanted access.

4.4.2.1 To change the time display on the front panel:

1. Log on to the Web UI

2. Navigate to MANAGEMENT > Front Panel.

3. Select your general region, and the specific time zone. The listed time regions and zones are based on the zones found here.

4. Click Submit

Changing this time display does not affect any internal clocks or create a local clock within the system.

4.4.2.2 To lock or unlock the front panel:

1. Log on to the Web UI

2. Navigate to MANAGEMENT > Front Panel.

3. Check the box next to Lock Front Panel to lock. To unlock, verify that the box is unchecked.

4. Click Submit

The front panel information display will lock at the last viewed screen. A small padlock icon will appear in the upper right hand corner of the display, and will flash brighter if any buttons are pressed on the front panel.

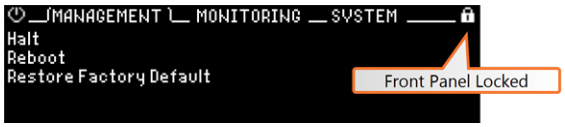


Figure 4-2: Locked Front Panel Display

The front panel will remain locked until it is unlocked through the Web UI or via CLI commands.

To lock or unlock the front panel via the CLI, use the `fp_lock` and `fp_unlock` commands (admin access is required).

4.4.3 12 or 24 Hour Time

The 12/24 hour time feature allows the product to display time on a 12- or 24-hour (military) timescale. This time will display on the front panel

4.4.3.1 Set 12- or 24-hour time:

In the Web UI:

Navigate to **Management** > **Front Panel**. In the Front Panel window under Clock Format, select either 12-Hour or 24-Hour time in the drop-down menu. Then select Submit.

In the CLI:

The command `displaymodeset <12|24>` will configure the front panel display time to either 12 or 24-hour time, depending on the included argument. You can also use `displaymodeget` to identify the display mode currently in use.

The `displaymodeset` command requires admin-level permissions.

Via the Front Panel:

Press any button to wake the front panel if it is in energy-saving mode. Then, press the Time button .

Navigate to Timing > Settings > Time Display Mode, and select 12- or 24-hour time as desired. Select the confirmation button ✓ to confirm your choice.

4.4.3.2 Viewing 12-Hour or 24-Hour Time

24-hour time is the default configuration. Identical time is displayed throughout the product. On units with a PM indication light on the front panel, the light will remain off at all times.

12-hour time will change the appearance of the front panel display time. When the time is past noon, the PM indicator light will illuminate.

4.4.4 Creating a Login Banner

A login banner is a customizable banner message displayed on the login page of the SecureSync Web UI. The login banner can be used, for example, to identify a unit.

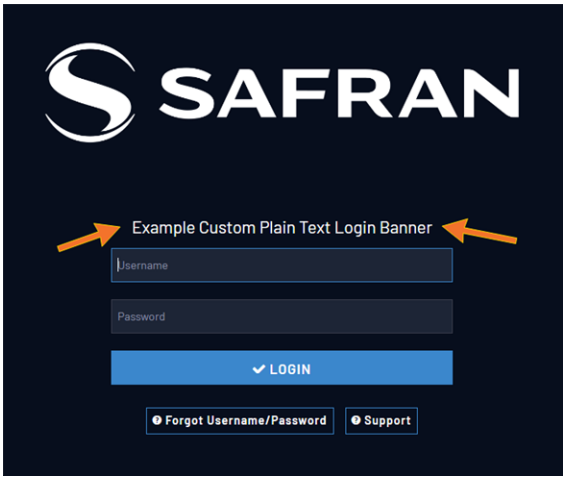


Figure 4-3: Login banner (example)

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.

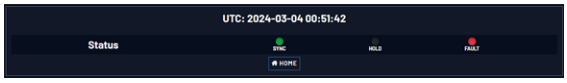
5. Optionally, you may also use the Web Interface Banner text box.

> **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.

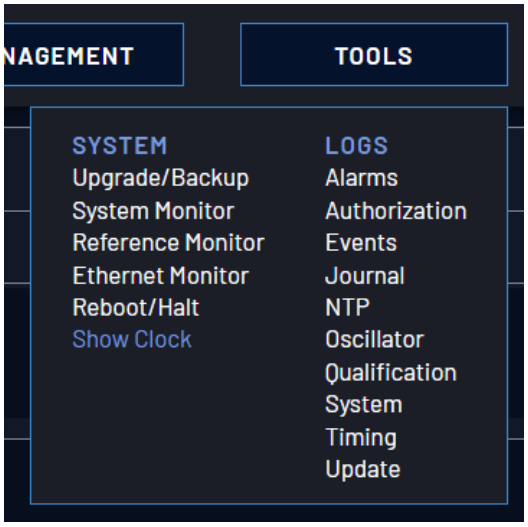
4.4.5 Show Clock

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 SecureSync System time.



To display the screen clock instead of the Web UI:

1. Navigate to **TOOLS** > **SYSTEM: Show Clock**:

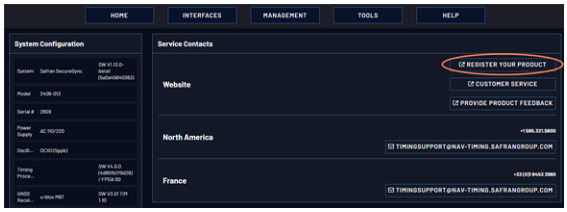


2. To return to the standard Web UI, click **Home**.

4.4.6 Product Registration

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

Upon initial start of the SecureSync Web UI, 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/



4.4.7 Synchronizing Network PCs

Frequently, network PCs have to be synchronized to SecureSync via the Ethernet port, using NTP (Network Time Protocol). A detailed description on how to synchronize Windows PCs can be found online in the 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.

4.5 Quality Management

4.5.1 System Monitoring

4.5.1.1 Status Monitoring via Front Panel

When you have physical access to the SecureSync front panel, you can obtain a system status overview. To see specifics on how to operate the front panel, see "Front Panel Keypad, and Display" on page 6



Figure 4-4: Front panel layout

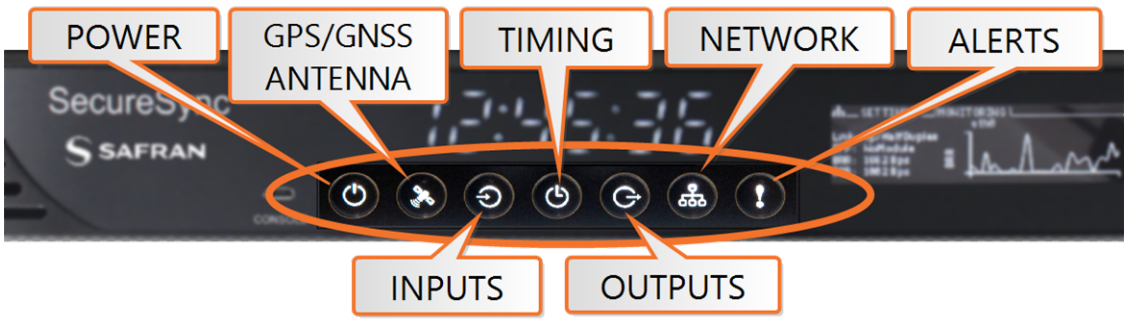


Figure 4-5: Status LED menu buttons

The GNSS Menu provides monitoring of the tracked constellations under the MONITORING submenu. Toggle between constellations to see a chart of each tracked satellite.

The INPUTS Menu provides monitoring of the references and the order of their priority under the MONITORING submenu.

The TIMING Menu provides a description of the current oscillator state in the MONITORING submenu.

The NETWORK Menu provides a graph of the network traffic in the MONITORING submenu. Toggle between **eth0** and **eth1** to view the traffic data for each port.

The ALARMS Menu provides valuable information about any current alerts and alarms.

- the STATUS submenu will list active alarms. Toggle between minor alarms and major alarms to see each list.
- the MONITORING submenu lists the temperature status, the memory, CPU, and disk used thus far within the unit. Select each of these values to see a graph relating to the measurement.

4.5.1.2 Status Monitoring via the Web UI

status information can be accessed via the SecureSync **Web UI**, such as:

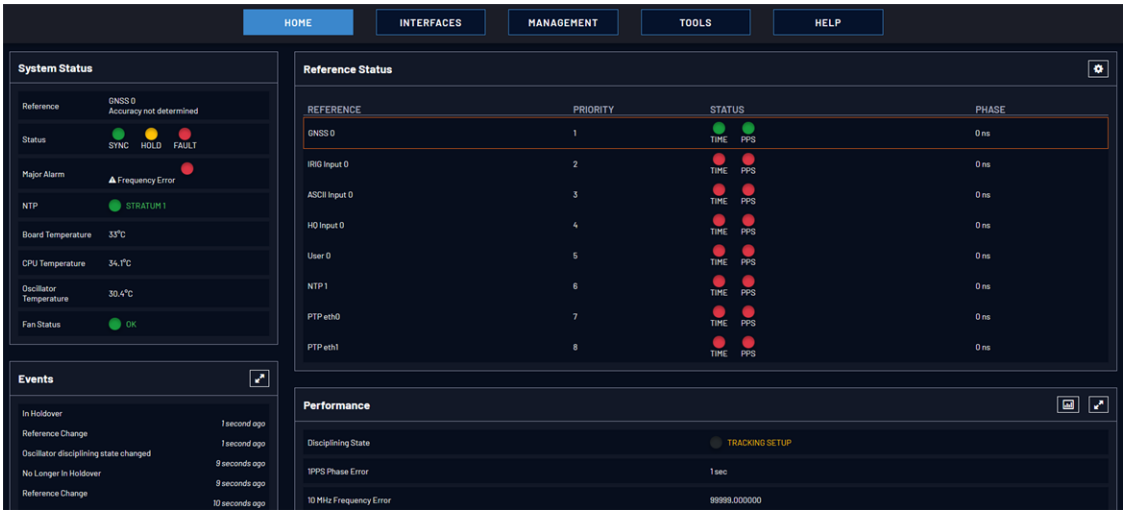
- Time synchronization status, including references
- GNSS satellites currently being tracked
- NTP sync status and current Stratum level
- Estimated time errors
- Oscillator disciplining
- Temperature monitoring
- Fan status

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 SecureSync Web UI provides a system status overview (see also "The Web UI HOME Screen" on page 36).

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 SecureSync is synchronized to its selected input references.
    - **Green** indicates SecureSync is currently synchronized to its references.
    - **Orange** indicates SecureSync is not currently synchronized to its references.
  - **Hold**—When lit, SecureSync is in Holdover mode.
  - **Fault**—Indicates a fault in the operation of the SecureSync. See "Troubleshooting via Web UI Status Page" on page 376 for instructions for troubleshooting faults.
- **Alarm Status**—If a major or minor alarm is present, it will be displayed here.
- **NTP**—Current STRATUM status of this SecureSync unit.
- **Temperature**—The current board temperature will be displayed here.
- **Fan Status**—Indicates the status of this SecureSync unit's cooling fan(s).



Note: The fan status for SecureSync units with one cooling fan will always display as FAULT.

Reference Status panel

- **REFERENCE**: Indicates the name type of each reference. These are determined by the inputs set up for the SecureSync
- **PRIORITY**: Indicates the priority of each reference. This number will be between 1 and 15. References in this panel appear in their order of priority. See "Configuring Input Reference Priorities" on page 219 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 SecureSync's recent activity. It updates in real time.

Note: If you know the individual reference or output whose status you wish to see, you can access the Status window of that reference or output directly through the INTERFACES > REFERENCES or INTERFACES > OUTPUTS drop-down menu.

Status Monitoring via the System Monitor Screen

To display status information pertaining mainly to SecureSync's current hardware status, navigate to **TOOLS > SYSTEM > System Monitor**.

The information provided on the **System Monitor** Screen is subdivided into three panels:

System Status panel

This is identical with the HOME screen "System Status panel" on page 324.

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.

4.5.1.3 Status Monitoring of Input References

SecureSync's input references can be monitored in real time through the **INTERFACES** menus. The menus will populate dynamically, depending on which references are available.

- To display **all** references, navigate to **INTERFACES > REFERENCES**.
- To display all references of a **given type**, click on the entry for that reference type (*not* indented e.g., **GNSS Reference**).
- To display **one particular** reference, click on its entry (indented e.g., **GNSS 0**).

The Reference window will show the validity status for the chosen reference(s):



To display more status information for a particular input reference, click the corresponding INFO button:

The reference window being displayed will show additional status information and option-card specific settings. The type of input reference, and the option card model determine which status information and option card settings will be displayed.



To change settings, click the **Edit** button in the bottom left corner.

4.5.1.4 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 facing page).

SecureSync allows Reference Monitoring by comparing the phase data of references against the System Ontime Point. The phase values shown are the filtered phase differences between each input reference 1PPS, and the internal disciplined 1PPS.

The data is plotted in a graph in real-time. The plot also allows you to display historic data, zoom in on any data range or on a specific reference. A data set can be exported, or deleted.

To monitor the quality of references, 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.

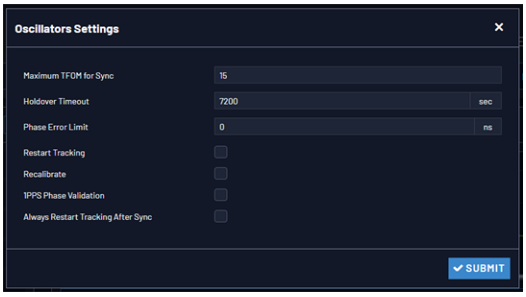
If the higher threshold value is exceeded, the **automatic failover** will cause SecureSync to fall back to its next lower reference (if available).

If no other reference is found, the unit will transition into a 1200-second coasting period. During this coasting period, the TIME and 1PPS references will continue to be considered valid, but SecureSync's oscillator will flywheel. Note that the **PPS** reference status light will turn yellow. After expiration of the 1200 seconds the unit will transition into Holdover.

Should, however, the above-mentioned higher threshold value no longer be exceeded, the unit will remain in the 1200-second flywheel mode until either (a) the lower threshold value is no longer exceeded, or (b) the 1200-second flywheel period expires. In both cases the PPS status light will turn green again.

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.

4.5.1.5 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:

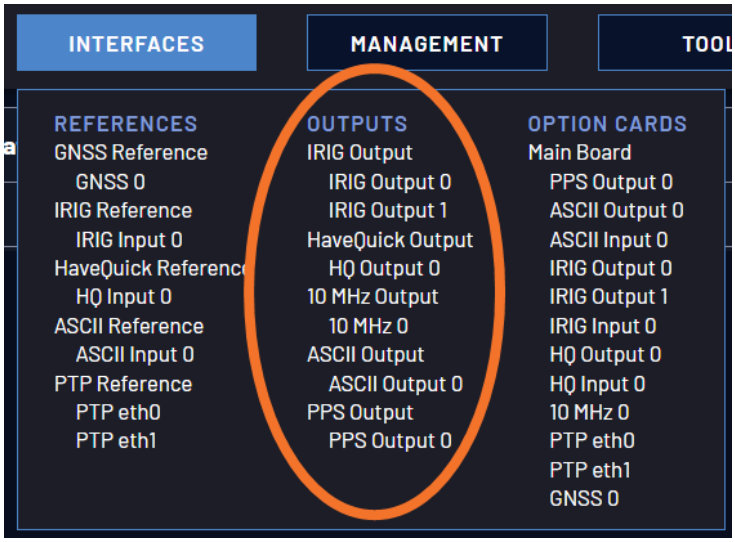
- **FULL** duplex, or
- **HALF** duplex.

Note that the Mode is auto-negotiated by SecureSync. It can be changed only via the switch SecureSync is connected to, not by using the SecureSync Web UI.

4.5.1.6 Outputs Status Monitoring

Per standard configuration, SecureSync is equipped with one 1PPS and one 10 MHz output. Additional outputs can be added by means of output option cards.

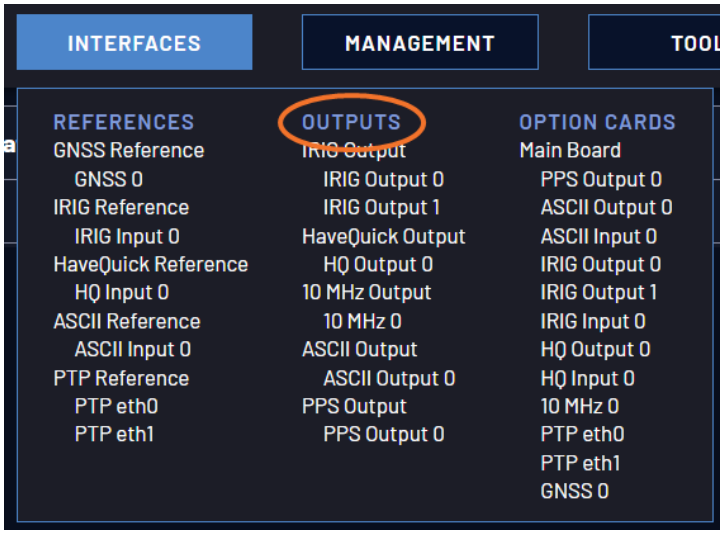
Outputs can be monitored in real time via the **INTERFACES** drop-down menu. The menu will populate dynamically, depending on which outputs are installed.



Monitoring the status of all outputs

To display a list of all the outputs installed in a SecureSync unit:

1. Select **INTERFACES** and click **OUTPUTS** in the menu heading.



2. The **Outputs** panel will list all the outputs installed, sorted by category.

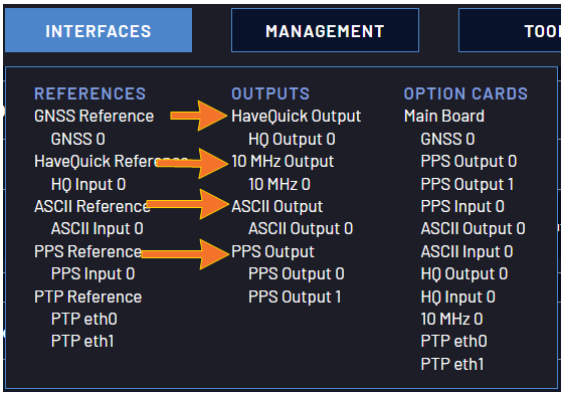


- To display more detailed information about a particular output, click the corresponding INFO button.
- To edit the settings of an output, click the GEAR button (see also "Configuring Outputs" on page 184.)
- To refresh the information displayed, click the REFRESH button (circling arrows icon on the right side of the screen).
- On the rear panel illustration, click on an output connector to highlight its list entry.

Monitoring all outputs of a specific type

To monitor all the outputs of a particular category (PPS, for example) simultaneously:

1. Navigate to **INTERFACES > OUTPUTS**, and click the desired output category (*not* recessed e.g., **PPS Output**):



2. The Status window will display a list of all outputs of the selected category:



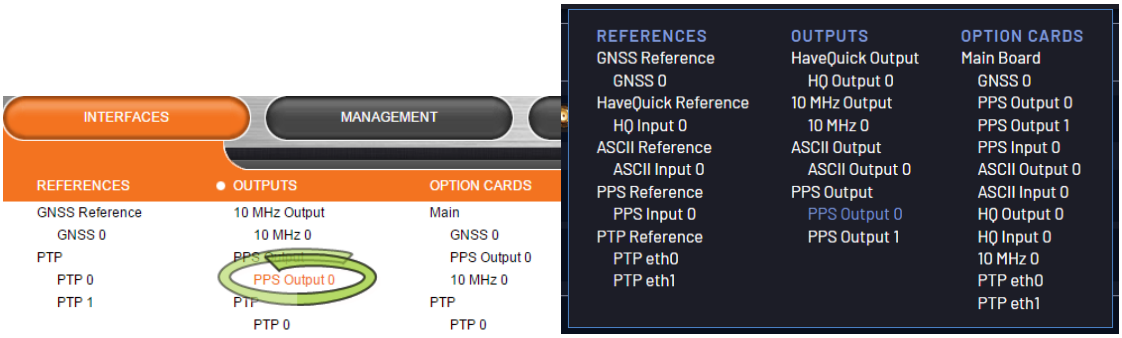
   - To display more detailed information about a particular output, click the corresponding INFO button.
   - To edit the settings of a given output, click the GEAR button (see also "Configuring Outputs" on page 184.)
   - To refresh the information displayed, click the REFRESH button (circling arrows icon).
   - In the illustration of the rear panel, click on a connector to highlight the corresponding list entry.

Displaying the settings of a specific output

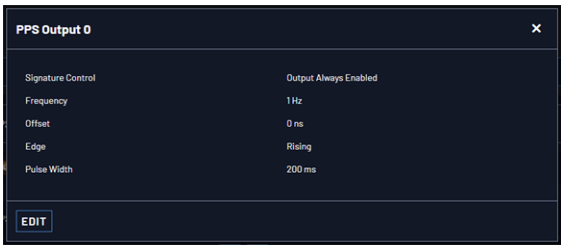
The outputs installed in your SecureSync unit have specific settings that can be reviewed, and—to some extent—edited.

To display the settings of an output:

1. Navigate to **INTERFACES > OUTPUTS**, and click on the desired output (recessed e.g., **PPS Output 0**):



2. The corresponding Status window will display:



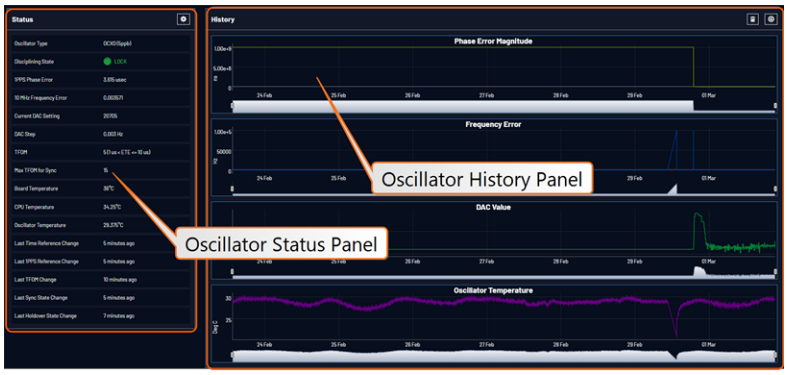
Click the **Edit** button in the bottom-left corner to configure settings that are user-editable. See also "Configuring Outputs" on page 184.

4.5.1.7 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 SecureSync'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 271), or automatically via a pre-set Phase Error Limit, will quickly reduce the phase error.
- 10 MHz Frequency Error: An internal estimated calculation (in Hertz) of the internal oscillator's frequency error, based on the phase accuracy error at the beginning and end of a frequency measurement window (the length of this window will vary depending upon the type of oscillator installed and the oscillator adjustment algorithm).
- Current DAC Setting: Current DAC value, as determined by the oscillator disciplining system. The value is converted into a voltage that is used to discipline the oscillator. A stable value over time is desirable and suggests steady oscillator performance (see also the graph in the History Panel).
- DAC Step: Step size for adjustments to the internal oscillator, as determined by the oscillator disciplining system. Larger steps = quicker, but coarser adjustments. The step size is mainly determined by the type of oscillator.
- TFOM: The Time Figure of Merit is SecureSync's estimation of how accurately the unit is synchronized with its time and 1PPS reference inputs, based on several factors, known as the Estimated Time Error or ETE. The larger the TFOM value, the less accurate SecureSync believes it is aligned with its 1PPS input that is used to perform disciplining. If this estimated error is too large, it could adversely affect the performance of oscillator disciplining. The available TFOM range is 1 through 15.
- Max TFOM for Sync: Value, as set under "Configuring the Oscillator" on page 271

- 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 SecureSync'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.

4.5.1.8 Monitoring the Status of Option Cards

SecureSync's installed option cards can be monitored in real time through the **INTERFACES > OPTION CARDS** drop-down menu. The menu will populate dynamically, depending on which option cards are installed.



Monitoring ALL Option Cards

To monitor all option cards, or a specific option card installed in your SecureSync:

1. Navigate to **INTERFACES**, and click on **OPTION CARDS**:



2. The resulting screen will display all installed option cards, and their current status.



You can drill down on any of the listed input references and outputs by clicking the INFO button (for status information), or the GEAR button (to edit settings).

The Main Board of the unit and any inputs or outputs that are currently configured on that board, also appear in this list.

Monitoring a SPECIFIC Option Card

To monitor the status of a selected option card:

1. Navigate to **INTERFACES > OPTION CARDS**, and click on a specific option card, or one of its indented input references, or outputs drop-down menu.



2. A window will display for the specific option you chose.

   Via the GEAR button, INFO button, or Edit button you can access and edit more detailed settings.

4.5.1.9 NTP Status Monitoring

SecureSync's **NTP Status Summary** provides a means to monitor NTP status and performance parameters relevant to your SecureSync at a glance.

1. To access the **NTP Status Summary** panel, navigate to **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 SecureSync is currently using.
   - **Stratum**—This is the stratum level at which SecureSync is operating.
   - **Leap Indicator**—The leap indicator bits (usually 00). See "Leap Second Alert Notification" on page 212.
   - **Delay (ms)**—The measured one-way delay between SecureSync and its selected reference.
   - **Time Offset**—This is a graphical representation of the system time offset over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel containing a larger, more detailed view of the graph. See "The NTP Time Offset Performance Graph" on the facing page.
   - **Offset (ms)**—Displays the configured 1PPS offset values.
   - **Frequency Offset**—This is a graphical representation of the system frequency offset over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel containing a larger, more detailed view of the graph. See "The NTP Frequency Offset Performance Graph" on page 342.

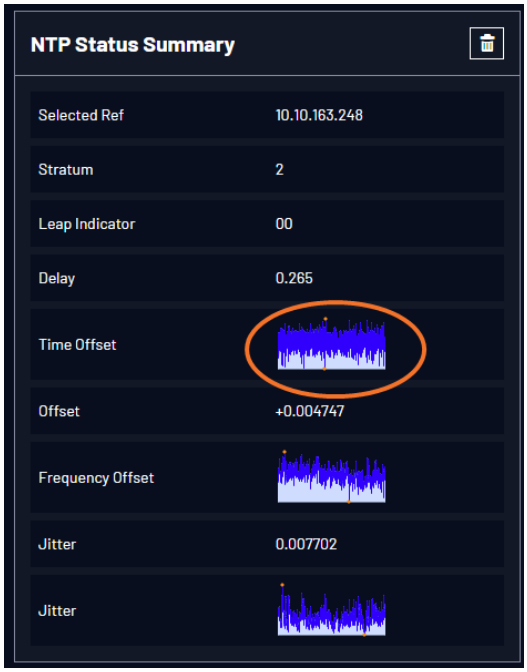
- **Jitter (ms)**—Variance (in milliseconds) occurring in the reference input time (from one poll to the next).
- **Jitter**—This is a graphical representation of the system jitter over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel containing a larger, more detailed view of the graph. See "The NTP Jitter Performance Graph" on page 344.

Note: This panel is updated every 30 seconds, or upon clicking the browser refresh button.

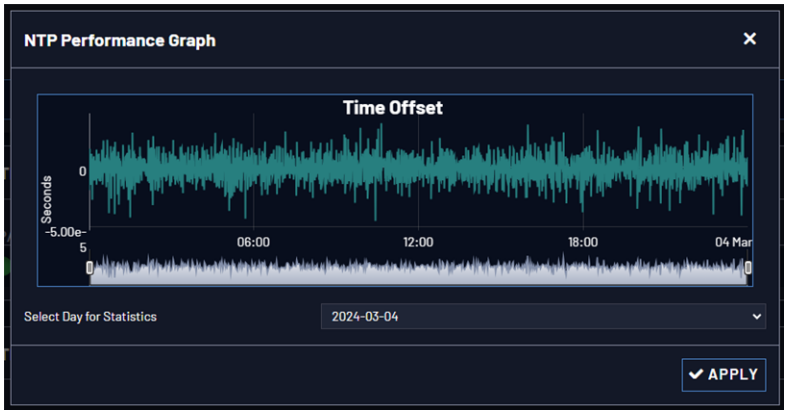
The NTP Time Offset Performance Graph

To view the NTP **Time Offset** performance graph:

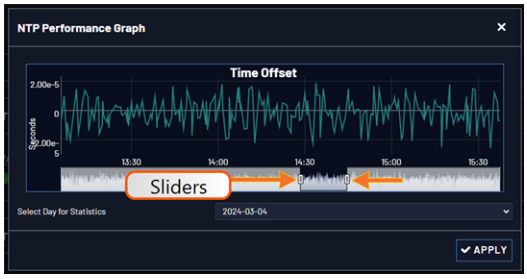
1. Navigate to **MANAGEMENT > NETWORK: NTP Setup**.
2. In the **NTP Status Summary** panel locate the **Time Offset** graph.



3. Click the graph in the **NTP Status Summary** panel.
4. The **NTP Performance Graph** panel will appear.



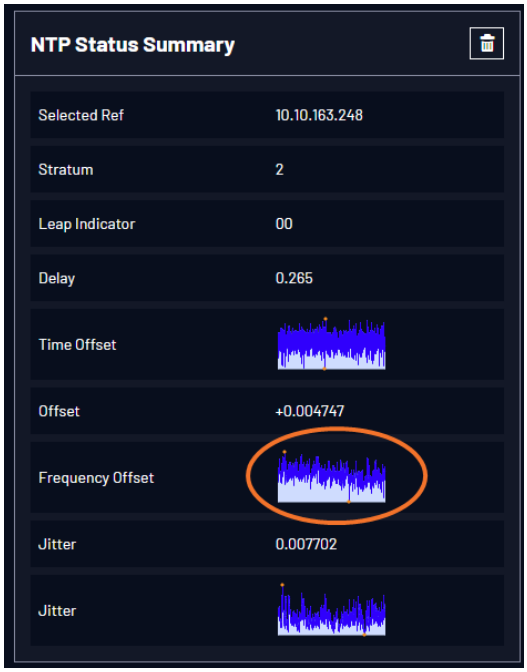
5. To select the statistics for a particular day, select a date from the drop-down list in the Select Day for Statistics field. The default date is the present date. Click **Apply**.
6. To display a higher resolution graph for a shorter time span, move one or both time sliders at the bottom of the graph inwards.



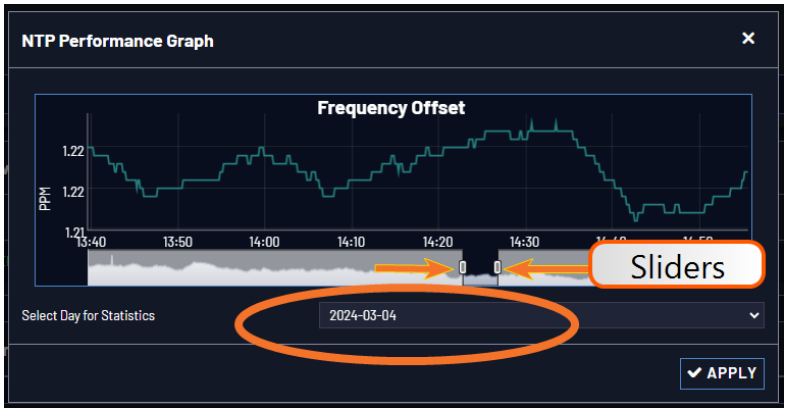
The NTP Frequency Offset Performance Graph

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.



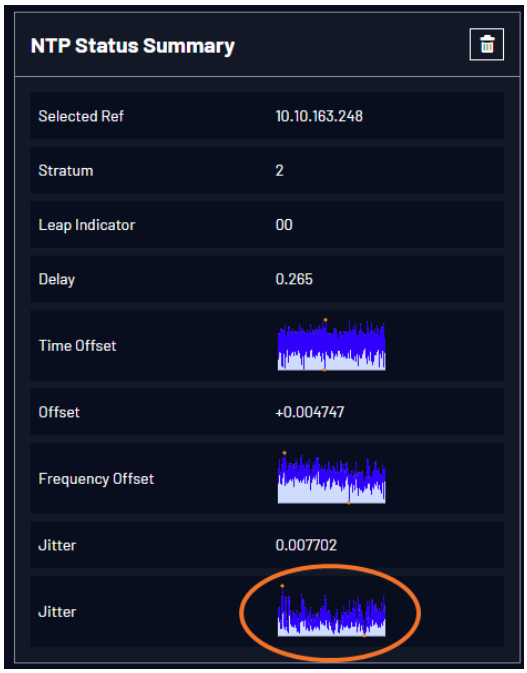
5. To select the statistics for a particular day, select a date from the drop-down list in the **Select Day for Statistics** field (highlighted in green in the illustration above). The default date is the present date. Click the **Apply** button.

» To display a higher resolution graph of a shorter time frame, move one or both of the two sliders inwards.

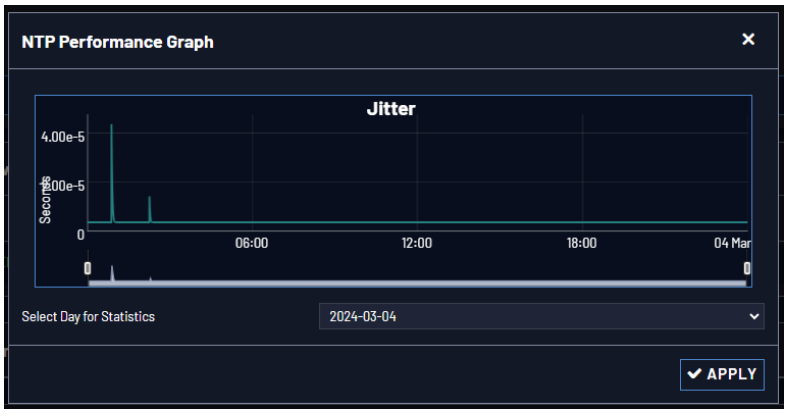
The NTP Jitter Performance Graph

To view the NTP **Jitter** performance graph:

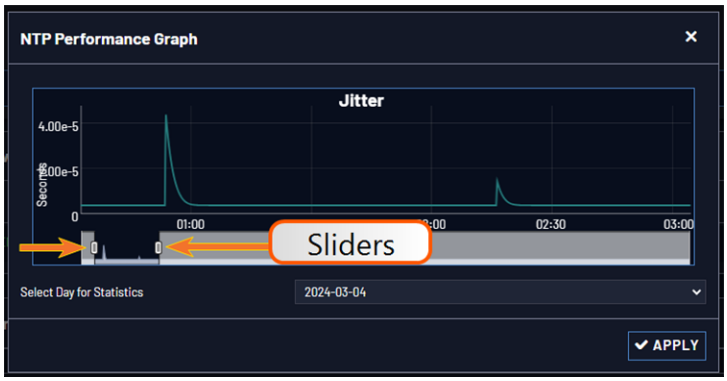
1. Navigate to **MANAGEMENT > NETWORK: NTP Setup** screen.
2. In the **NTP Status Summary** panel locate the **Jitter** graph.



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.



4.5.1.10 Temperature Management

SecureSync is equipped with one cooling fan, located behind the right-hand side of the front panel, and several hardware temperature sensors, including:

- » the **board** temperature near the CPU
- » the **CPU** temperature
- » the air temperature near the **oscillator**.

Temperature readings are performed once per minute. The temperature data is logged, and can be visualized via graphs integrated into the Web UI.

Note: Depending on your unit, there may be one or two cooling fans.

Temperature Monitoring

You can monitor the unit's measured temperatures actively by inspecting the temperature graphs in the Web UI, or passively by setting up automatic alarm messages.

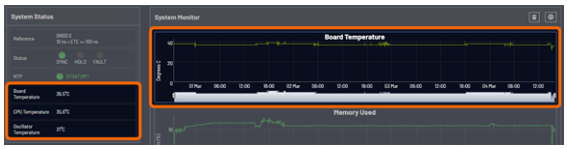
Alarm notifications can be generated via SNMP Traps and Emails, as well as log messages in the Alarm and Event Logs. The alarms may optionally be masked.

Also, it is possible to implement a delay by setting the number of times the 1/minute readings need to exceed a temperature threshold before an alarm is triggered.

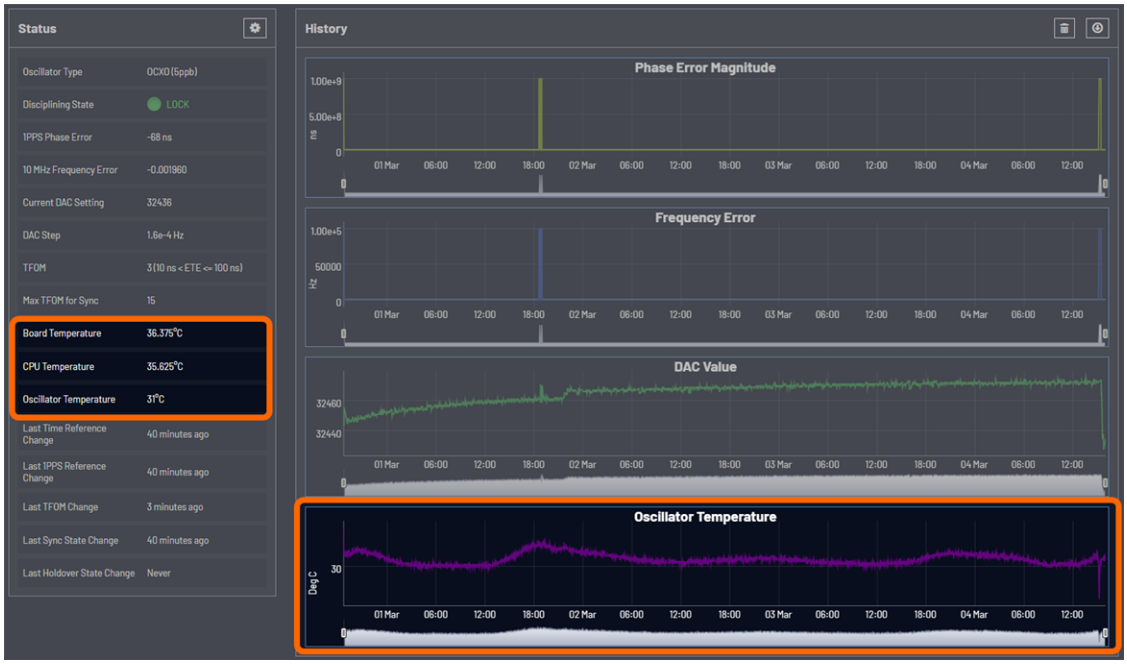
Monitoring CPU and Board Temperature

Current readings for Oscillator/Board/CPU Temperature are displayed in the **System Status** panel, which can be accessed via the **HOME** screen, or via **TOOLS > System Monitor**.

Board Temperature graphs are displayed under **TOOLS > System Monitor**:



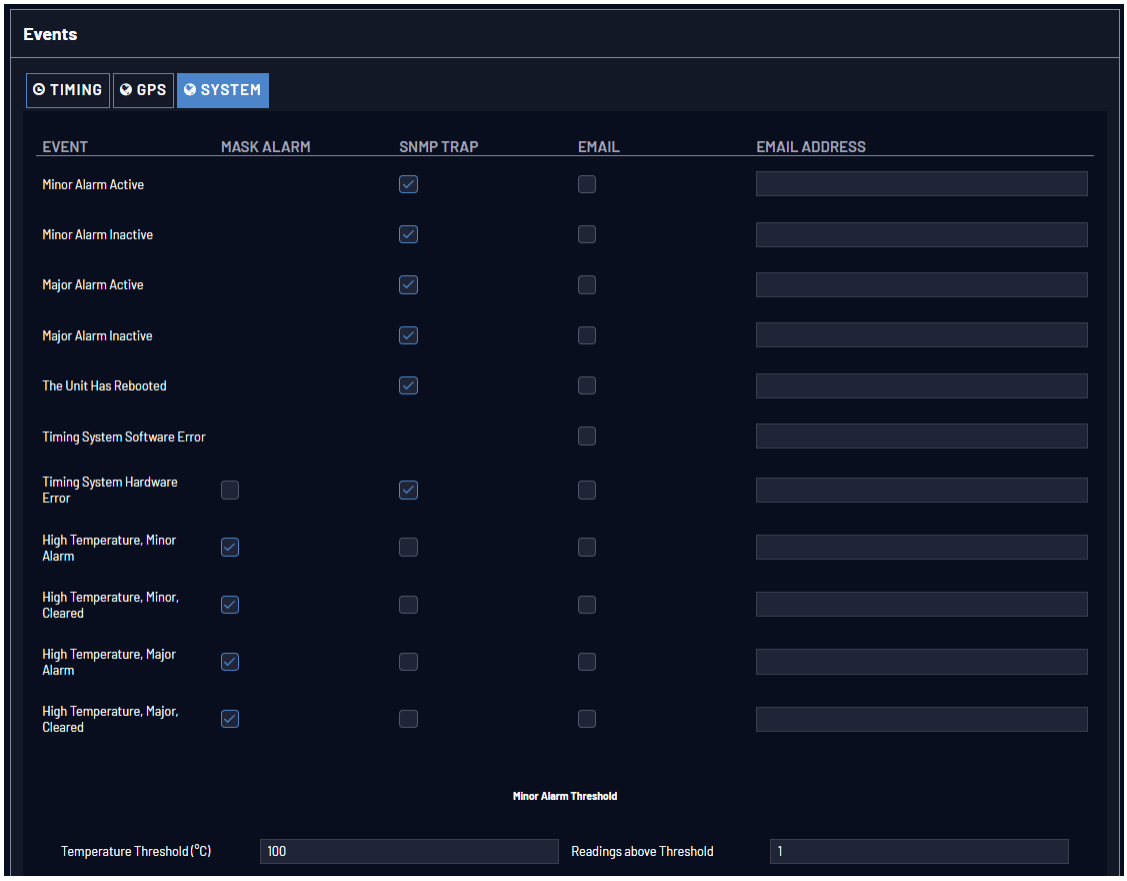
The graph for the Oscillator Temperature is displayed under **MANAGEMENT > OTHER: Disciplining**:



Temperature readings are subject to environmental conditions and hardware configuration e.g., oscillator type. Under normal operating conditions, all temperatures should remain fairly constant. Drastic changes may indicate e.g., a problem with the fan. Note that the oscillator temperature will have a direct impact on its accuracy, i.e. there is a strong correlation between disciplining performance and oscillator temperature.

Setting Temperature Monitoring Alarms

Navigate to **MANAGEMENT > OTHER: Notifications**. In the **Events** panel, select the **System** tab:



Under the **System** tab, you can set Notifications for Minor and Major Alarms/Clearances. The temperature readouts used for the Alarms are generated by the **CPU temperature sensor**.

Also, you can set the temperature threshold value for Minor/Major alarms, and define a retry value by determining how many readings (1/min.) the temperature must exceed the threshold value before an alarm/clearance is triggered.

The default temperature threshold value for both Minor, and Major Alarms is 100°C. With simultaneous alarm triggerings, the Major Alarm will override the Minor Alarm, i.e. you will be notified only about the Major Alarm. If you want to be notified early about a rise in temperature, a recommended setting for the Minor Alarm temperature would be 90°C. Please note that it is not advisable to set the Major Alarm temperature to a value higher than 100°C.

Downloading Temperature Data

It is possible to download the temperature data e.g., to plot your own temperature graphs, or because Safran Technical Support inquires about this data for diagnostic purposes in the event of technical problems.

» To download the logged data used to generate the displayed graphs, navigate to any panel that displays one or more graphs (see above), and click on the **Arrow** icon in the top-right corner.

A file named `systemMonitorLog.csv` file will be generated in your designated download folder.

Deleting Temperature Data

Temperature graphs (and other graphs as well) will display up to approximately 10000 readings, which are generated at a 1/min. rate, i.e. the data displayed covers about 7 days. Thereafter, the oldest data gets overwritten.

» To delete the logged data used to generate the displayed graphs, click the TRASH CAN icon in the top-right corner of the panel.

Note that re-populating the graphs with fresh data will take several minutes.

Temperature Readout via CLI

Temperature data can be read out via the CLI using the **i2cget** command:

EXAMPLE:

i2cget -y 0 0x4d <register>

i2cget returns temperature in Celsius in hex format. No additional conversion required.

Further reading

See also: "Troubleshooting the Cooling Fan(s)" on page 381.

4.5.2 Logs

SecureSync maintains different types of event logs (see below) to allow for traceability, and for record keeping. Should you ever require technical support from 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 .

4.5.2.1 Types of Logs

SecureSync generates log files for the following event categories:

Alarms Log

Displays log entries for the Timing System, for example:

- **The Unit has Rebooted**: SecureSync was either rebooted or power cycled.
- **In Holdover**: Input references were available, but all input references have since been lost. If the references are not restored before the Holdover period expires, time sync will be lost.
- **No longer in Holdover**: Input references were lost at one point (or declared not valid), but have since been restored OR the Input references were not restored before the Holdover period expired (Time Sync alarm is asserted).
- **In Sync**: SecureSync is synchronized to its selected Time and 1PPS reference inputs.
- **Not In Sync**: SecureSync is not synchronized to its Time and 1PPS inputs and is not currently in Holdover. NTP will indicate to the network that it is Stratum 15 and so the time server likely be ignored as a time reference.
- **Frequency Error**: The oscillator's frequency was measured and the frequency error was too large. Or, the frequency couldn't be measured because a valid input reference was not available.
- **Reference change**: SecureSync has selected a different Time and 1PPS input reference for synchronization. Either the previously selected input reference was declared not valid (or was lost), so a lower priority reference (as defined by the Reference Priority Setup table) is now selected for synchronization OR a valid reference with higher priority than the previous reference is now selected for synchronization.

EXAMPLE:

GNSS is the highest priority reference with IRIG input being a lower priority. SecureSync is synced to GNSS and so GNSS is the selected reference. The GNSS antenna is disconnected and IRIG becomes the selected reference. The Reference change entry is added to this log.

Authentication Log

Displays log entries for authentication events (e.g., unsuccessful login attempts, an incorrectly entered password, etc.) that are made to SecureSync's command line interfaces (such as 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**: SecureSync has switched from one input reference to another (for example, IRIG was the selected input being used, but now GNSS is the selected reference).
- **GPS Antenna Problem**: The GPS Antenna Problem alarm indicates the GNSS receiver has detected an over-current or undercurrent condition (an open or short exists in the GNSS antenna cable, or the GNSS antenna is not connected to SecureSync). The receiver will attempt to continue the normal acquisition and tracking process regardless of the antenna status. The current draw measurements that will indicate an antenna problem are:
  - Under-current indication < 8 mA
  - Over-current indication > 80 mA



Note: This alarm condition will also be present if a GNSS antenna splitter that does not contain a load to simulate an antenna being present is being used.

- **GPS Antenna OK**: The antenna coax cable was just connected or an open or short in the antenna cable was being detected but is no longer being detected.
- **Frequency Error**: The oscillator's frequency was measured and the frequency error was too large. Or, the frequency couldn't be measured because a valid input reference was not available.
- **Frequency Error cleared**: The Frequency Error alarm was asserted but was then cleared.
- **In Holdover**: Input references were available, but all input references have since been lost. If the references are not restored before the Holdover period expires, time sync will be lost.
- **No longer in Holdover**: Input references were lost at one point (or declared not valid), but have since been restored OR the Input references were not restored before the Holdover period expired (Time Sync alarm is asserted).
- **In Sync**: SecureSync is synchronized to its Time and 1PPS inputs.
- **Not In Sync**: SecureSync is not synchronized to its Time and 1PPS inputs and is not currently in Holdover. NTP will indicate to the network that it is Stratum 15 and so the time server likely be ignored as a time reference.

- **Sending trap for event 1 (SNMPSAD)**: An SNMP trap was sent by the SNMP agent to the SNMP Manager. The event number in this entry indicates which SNMP trap was sent.
- **The Unit has Rebooted**: SecureSync was either rebooted or power cycled.
- **Fan Status**: A fault is detected in theSecureSynccooling fans.

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 SecureSync is connected to a GNSS antenna and is tracking satellites, this log contains a running hourly count of the number of GNSS satellites tracked each hour. This history data can be used to determine if a GNSS reception problem

exists and whether this is a continuous or intermittent reception issue.

GNSS reception may be displayed as cyclic in nature. A cyclic 12 hour pattern of decreased GNSS reception typically indicates that the GNSS antenna has an obstructed view of the horizon. The GNSS satellites are in a 12-hour orbit, so if part of the sky is blocked by large obstructions, at the same time every day (at approximately 12 hour intervals), the GNSS reception may be reduced or may vanish altogether. If this occurs, the antenna should be relocated to afford it an unobstructed view of the sky.

Every hour (displayed in the log as UTC time), SecureSync counts the total number of satellites that were tracked during that hour. The GNSS qualification log shows the number of satellites that were tracked followed by the number of seconds that the particular number of satellites were tracked during the hour (3600 seconds indicates a full hour). The number to the left of the "=" sign indicates the number of satellites tracked and the number to the right of the "=" sign indicates the number of seconds (out of a total of 3600 seconds in an hour) that the unit was tracking that number of satellites. For example, "0=3600" indicates the unit was tracking 0 satellites for the entire hour, while "0=2700 1=900" indicates the unit was tracking one satellite for 900 seconds, but for the remaining portion of the hour it was tracking zero satellites.

Every hourly entry in the log also contains a quality value, represented by "Q= xxxx" (where x can be any number from 0000 through 3600). The Qualification log records how many satellites were tracked over a given hour. If for every second of the hour a tracked satellite was in view, the Quality value will equal 3600. For every second SecureSync tracked less than the minimum number of satellites, the value will be less than 3600. The minimum requirement is one satellite at all times after the unit has completed the GNSS survey and indicates "Stationary". A minimum of four satellites are required in order for the GNSS survey to be initially completed.

If all entries in the qualification log are displayed as "0=3600", a constant GNSS reception problem exists, so the cause of the reception issue is continuous. If the unit occasionally shows 0=3600 but at other times shows that 1 through 12 have numbers of other than "0000", the reception is intermittent, so the cause of the reception issue is intermittent. If the Quality value normally equals 3600 but drops to lower than 3600 about every 12 hours, the issue is likely caused by the GNSS antenna having an obstructed view of the sky.

Example GPS Qualification Log Entry:

6 = 151 7 = 1894 8 = 480 9 = 534 10 = 433 12 = 108 Q = 3600

In this example, SecureSync tracked no less that 6 satellites for the entire hour. Out of the entire hour, it was tracking 6 satellites for a cumulative total of 151 seconds (not necessarily in a row). For the duration of the hour, it was tracking, 7, 8, 9, 10 and 12 satellites for a period of time. Because it was tracking at least at least one satellite for the entire hour, this Quality value is Q=3600.

Note: If SecureSync is not connected to a GNSS antenna, this log will remain empty.

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 SecureSync). The receiver will attempt to continue the normal acquisition and tracking process regardless of the antenna status.
- **GR antenna ok**: The antenna coax cable was connected at this time or an open or short in the antenna cabling was occurring but is no longer being detected.

Update Log

Displays log entries related to software updates that have been performed.

4.5.2.2 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.**

[1] GR = GNSS Reference

2. The **Logs** screen will appear, with several panels:



The Logs Actions panel

The **Actions** panel on the upper-left corner of the **Logs** screen allows you to perform batch actions on your logs:

- **Save and Download All Logs**—Save and download all the logs on SecureSync.
- **Clear All Logs**—Clear all the logs on SecureSync.

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 357

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

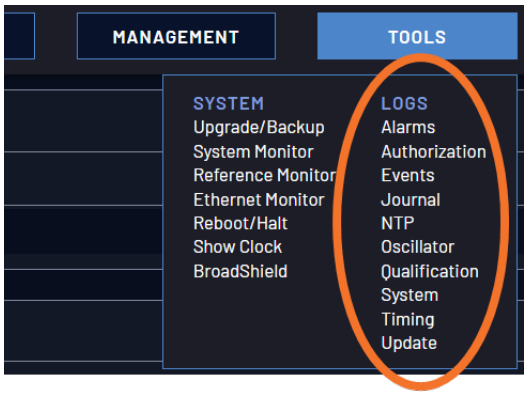
The Local Logging panel will control the local logging (logs stored directly on the unit) for each log individually.

- 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 349 for information on each log type.

4.5.2.3 Displaying Individual Logs

To access individual SecureSync logs:

1. From the **TOOLS** drop-down menu, select the desired **Logs** category (for example, “Alarms”, or “Events”) from the right-hand column.



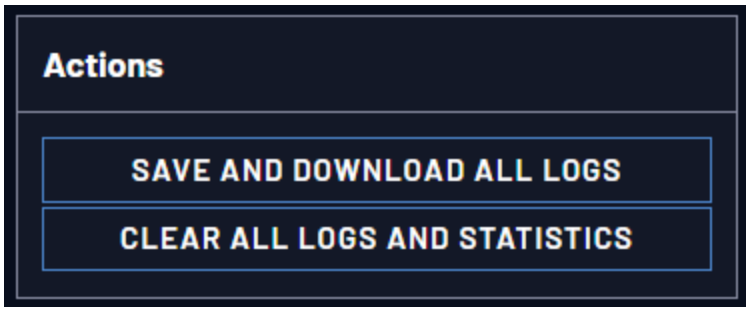
4.5.2.4 Saving and Downloading Logs

The SecureSync 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**.

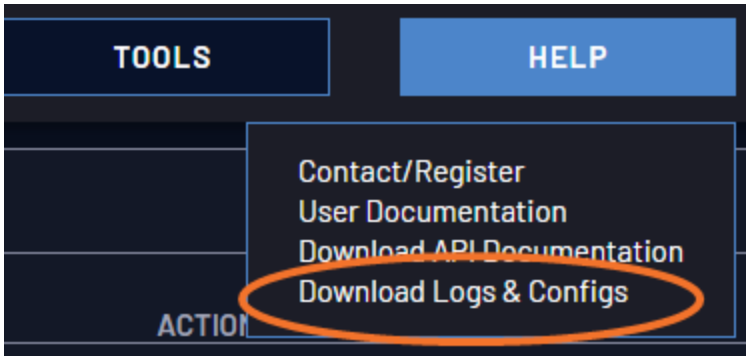
2. On the left side of the screen, in the **Actions** panel, click on the **Save and Download All Logs** button.



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" below) 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.



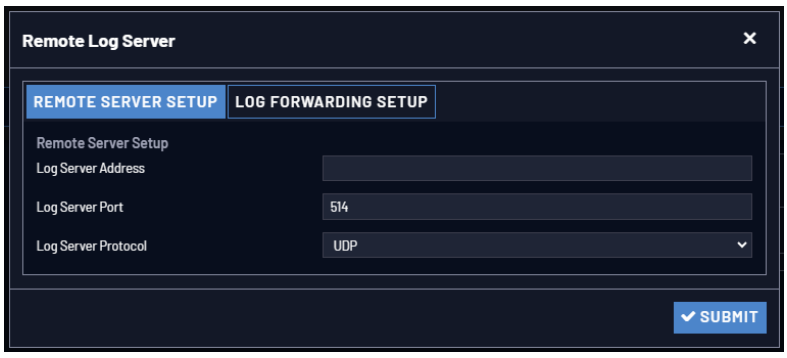
3. If so asked by Technical Support, attach the oscillator status log file (typically together with the bundled SecureSync log files, see: "Saving and Downloading Logs" on page 355) to your email addressed to Safran Technical Support.

4.5.2.5 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 Servers** panel, click on the PLUS icon in the top-right corner of the panel. The **Remote Log Server**window displays.



3. In the **Remote Server Setup** tab, enter the IP address or host server name (e.g., “MyDomain.com”) you want to use as a remote log server under Log Server Address.
4. Fill out your desired Log Server Port.
5. Select your Log Server Protocol [UDP, TCP].

6. In the **Log Forwarding Setup** tab, click the checkbox of each type of Log File to be used by your remote log server. You can also select the Facility and Severity of the message.
7. Click the **Submit** button.
8. Your remote log server will appear in the **Remote Log Server** panel.

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 **X** button to delete the remote log server. Confirm by clicking OK in the message window.

—OR—

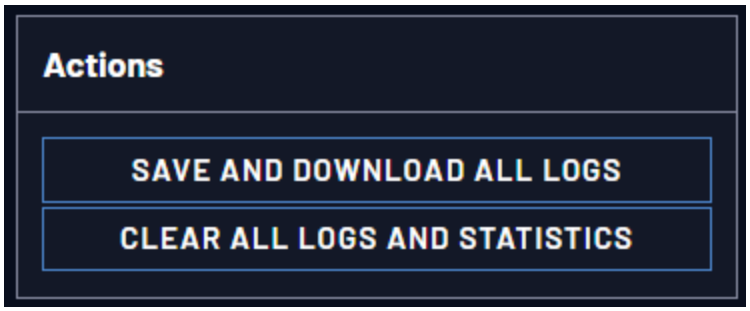
3. In the **Remote Log Server** panel, click the GEAR button to edit the remote log server. Type in a new IP address, for instance, or select new logs to be configured.

4.5.2.6 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**.

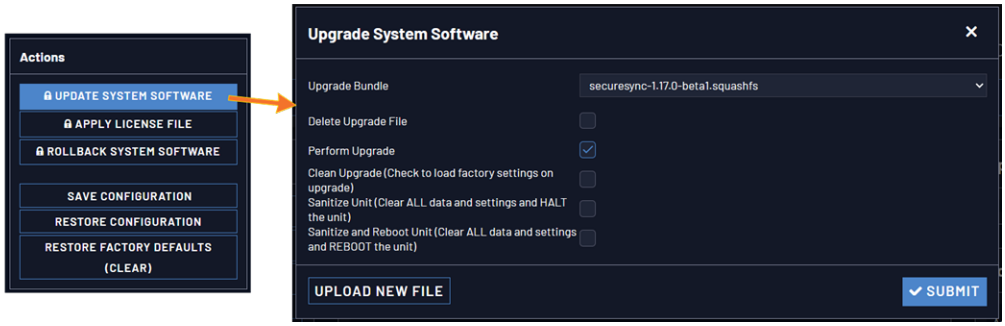
4.6 Updates and Licenses

4.6.1 Software Updates

Safran periodically releases new versions of software for SecureSync. 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.
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:

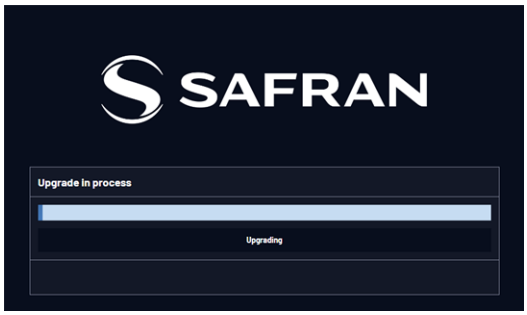
- **Delete Upgrade File**: Cancel the upgrade, and remove the uploaded software bundle from the system.
- **Perform Upgrade**: Perform the software upgrade.
- **Clean Upgrade**: Factory settings will be applied during the upgrade; any custom settings you may have applied previously will be over-written! 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

[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.

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. Rollback 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 overwritten. 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 383.

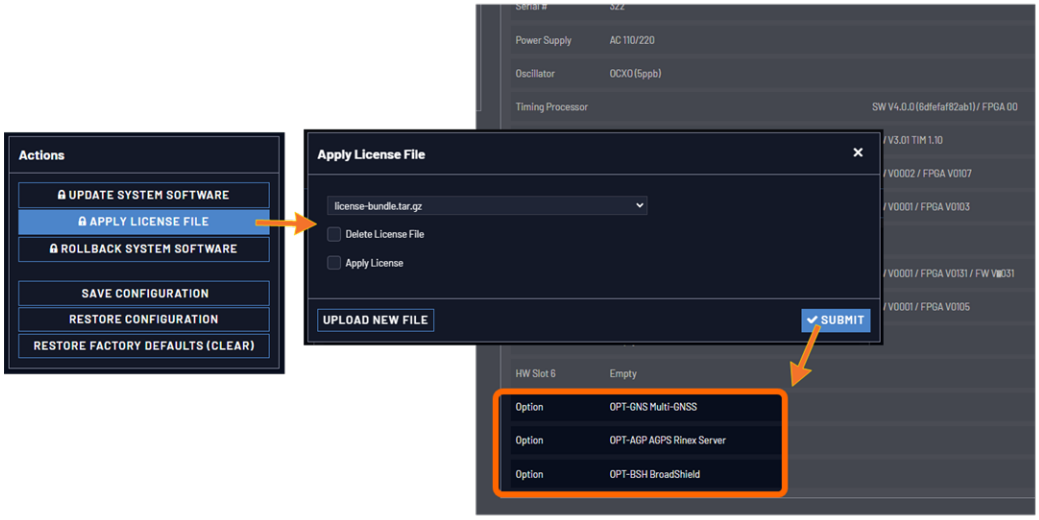
4.6.2 Applying a License File

Software options must be activated by applying a license file (OPT-xyz):

Typically, SecureSync 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 SecureSync 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 SecureSync unit and install it:

1. Save the license file `license.tar.gz` to a location on your PC (which needs to be connected to the same network SecureSync is.)
2. Open the SecureSync Web UI, and navigate to **Tools** > **Upgrade/Backup**:



3. In the **Actions** panel, click **Apply License File**.
4. In the **Apply License File** window, click **Upload New File**.
5. In the **Upload File** window, click **Choose File**. Using the Explorer window, navigate to the location mentioned under the first step, select the license file, and monitor the installation progress in the **Status Upgrade** window until the application has rebooted.
6. Refresh the browser window, and login to the Web UI again. Re-navigate to **Tools** > **Upgrade/Backup**, and confirm that the newly installed Option is listed in the **System Configuration** panel.



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.

4.7 Backing-up and Restoring Configuration Files

Once SecureSync has been configured, it may be desired to back up the configuration files to a PC for off-unit storage. If necessary in the future, the original configuration of the SecureSync can then be restored into the same unit.

The capability to backup and restore configurations also adds the ability to "clone" multiple SecureSync units with similar settings. Once one SecureSync unit has been configured as desired, configurations that are not specific to each unit (such as NTP settings, log configs, etc.) can be backed up and loaded onto another SecureSync unit for duplicate configurations.

There are several configuration files that are bundled in one file for ease of handling.

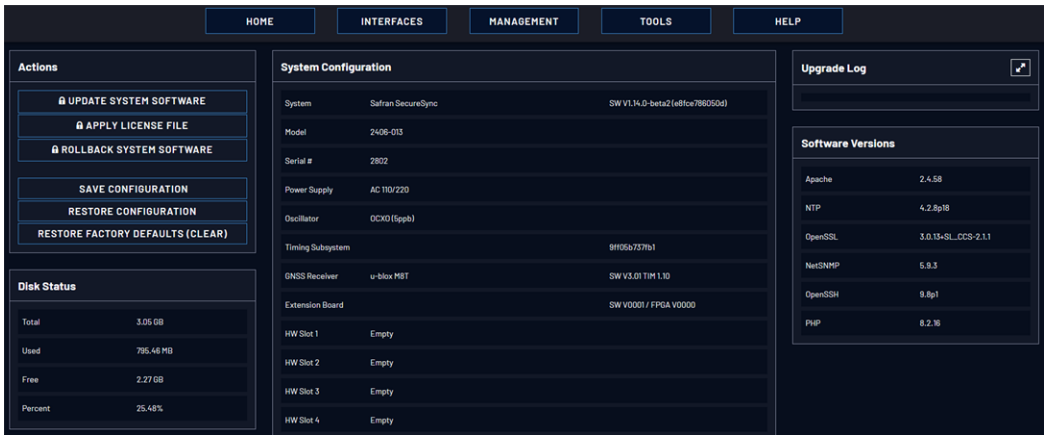


Note: For security reasons, configurations relating to security of the product, such as SSH/SSL certificates, cannot be backed up to a PC.

4.7.1 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.

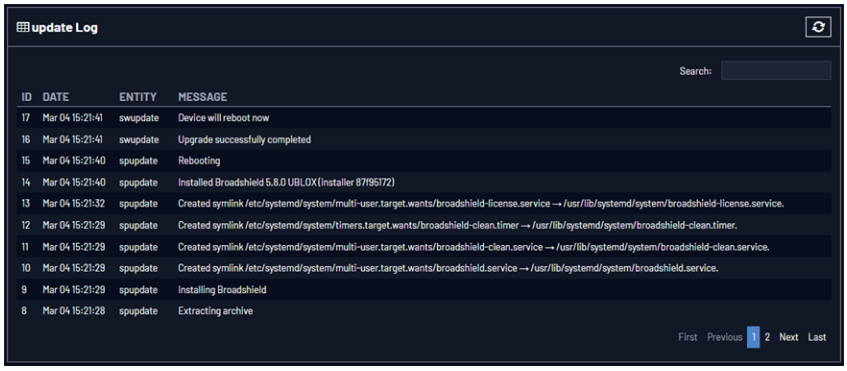
The System Configuration panel

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.
- **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.
- **HW Slots 1–6**—The Option Cards installed in 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.

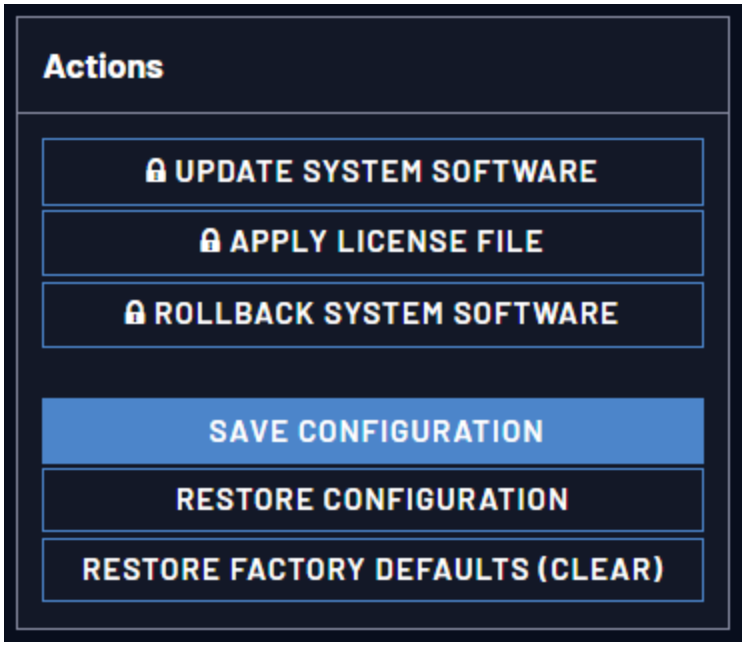
The Software Versions panel

This panel provides version information on the different SW components utilized by the system.

4.7.2 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. SecureSync 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.

4.7.3 Uploading Configuration Files

To upload configuration files from a PC:

1. Navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. In the **Actions** panel, click the **Upload Configuration** button.
3. Click **Choose File** in the window that displays, and navigate to the directory on your PC where the bundled file is stored.
4. Click the **Upload** button. SecureSync saves the uploaded bundled file in the `/home/spectracom/xfer/config/`directory.

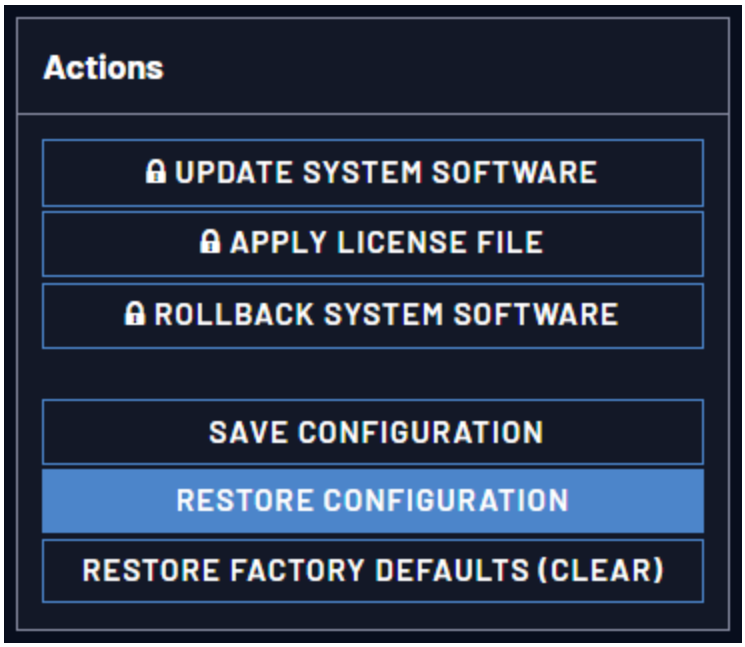
> **Note:** When uploading files remotely via long distances, or when uploading multiple files via several browser windows simultaneously, the upload process may fail to complete. In this case, cancel the upload by clicking X, and go back to Step 2.

5. To use the new configuration file for this SecureSync, click the **Restore Configuration** button, and follow the procedure described under 366.

4.7.4 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/SecureSync.conf`, then reboot in order to read the new configuration file. Once powered back up, SecureSync will be configured with the previously stored file.

4.7.5 Restoring the Factory Defaults

For instructions on how to restore the SecureSync's configuration files to their factory default settings see "Resetting All Configurations to their Factory

Defaults" on the facing page.

4.7.6 Resetting the Unit to Factory Configuration

In certain situations, it may be desired to reset all SecureSync configurations back to the factory default configuration. The GNSS location, any SecureSync configurations and the locally stored log files can be cleared via the Web UI.

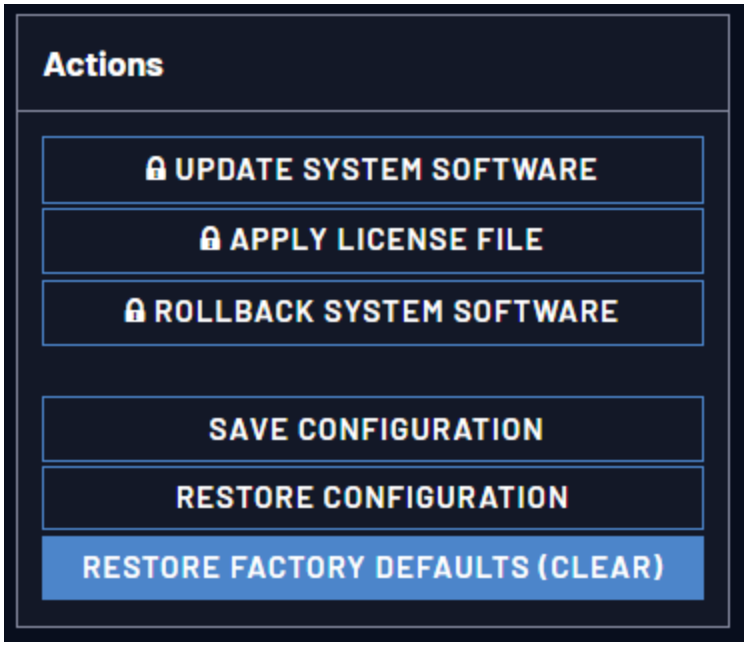
Note: Restoring configurations (reloading a saved configuration), erasing the stored GNSS location and clearing the log files are separate processes. You may restore one without restoring the others.

If SecureSync was assigned a static IP address before cleaning the configurations, it will be reset to DHCP after the clean has been performed. If no DHCP server is available after the clean operation, the static IP address will need to be manually reconfigured.

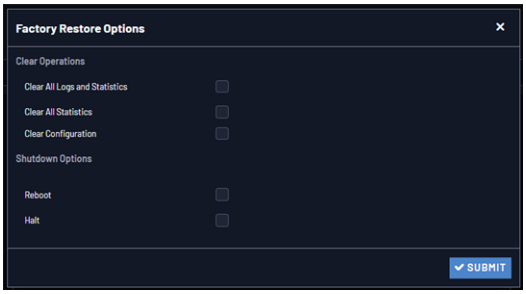
4.7.6.1 Resetting All Configurations to their Factory Defaults

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.

4.7.7 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			
Serial Port	Available	Available	n/a

Feature	Default Setting	Recommended Setting	Where to Configure
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.

4.7.8 Sanitizing the Unit

The concept of sanitizing a SecureSync 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 SecureSync 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 (referred to as a WIPE 1-4 on the front panel) 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.



Note: Option cards do not have memory which needs to be cleared; their configuration is stored on your machine and is cleared by the sanitization procedure outlined below. The one exception to this rule is the WROX cards (-58 and -59); in order to clear all memory and configurations, issue `wrz_config -F && reboot` command in the WROX CLI.

4.7.8.1 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 on the rear panel 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`

4.7.8.2 Further Reading

Additional information regarding Sanitization and Volatility may be found in the Safran website. To obtain a Certificate of Volatility for SecureSync, contact Safran Trusted 4D Technical Support (see "Technical Support" on page 645).

BLANK PAGE.

APPENDIX

Appendix

The following topics are included in this Chapter:

5.1 Troubleshooting 374
5.2 Option Cards 383
5.3 Command-Line Interface 575
5.4 Time Code Data Formats 585
5.5 IRIG Standards and Specifications 619
5.6 Strain Relief Ancillary Kit 637
5.7 Maintenance 644
5.8 Technical Support 645
5.9 Return Shipments 646
5.10 List of Tables 646
5.11 List of Images 648
5.12 Document Revision History 651

5.1 Troubleshooting

The Web UI provide SecureSync status information that can be used to help troubleshoot failure symptoms that may occur.

5.1.1 Minor and Major Alarms

Alarms and alerts are designed to warn of issues such as GNSS access, timing errors, and system functionality. Alarms can appear on the Web UI, displayed on the front panel, and through system communication (via SSH, SNMP, etc.).

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:

- **Hot Swap Power Supply**: At least one power supply is in a warning state. This could be due to temperature, voltage, fan speed, or current readings. Refer to "Hot Swap Power Supply" on page 56.
- **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 379 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.

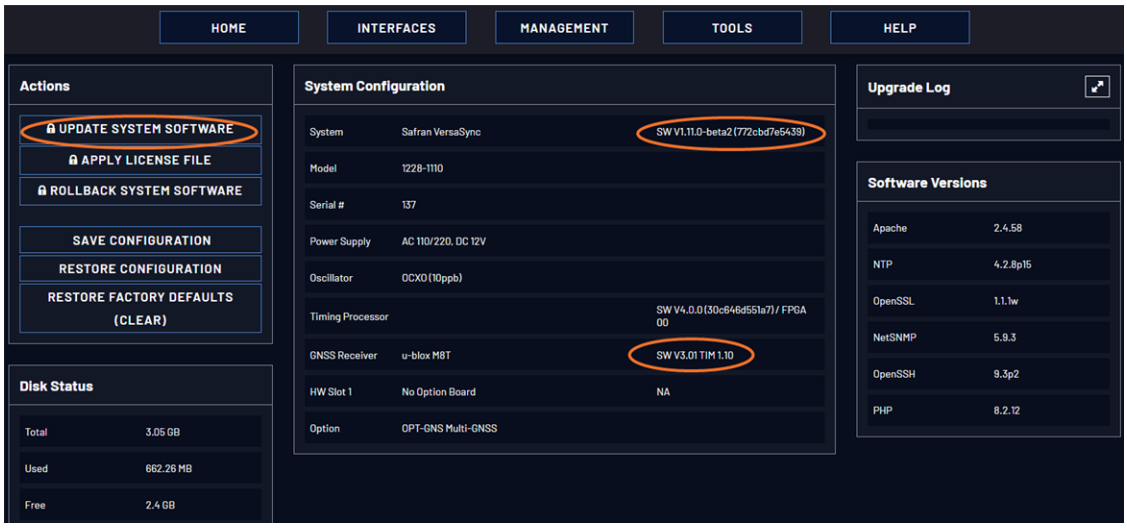
- **Timing System Error**: A problem has occurred in the Timing System. Contact Safran technical support if the error continues.
- **Timing System Hardware Error**: An issue has been detected with the unit hardware. One possible cause is that the oscillator is not functioning properly.
- **Hot Swap Power Supply**: At least one power supply is faulty, either due to functionality, or because it has been removed or disconnected. Refer to "Hot Swap Power Supply" on page 56 .

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 SecureSync 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 SecureSync connected to either a stand-alone or networked PC and with the network configuration correct, it should be possible to connect to the Web UI.

Verify	Current Status	Indication	Troubleshooting
LEDs on network connector	Green "Good link" is not solid green	SecureSync ICMP test is failing. SecureSync is not connected to PC via Ethernet connection	1) Verify one end of standard network cable is connected to SecureSync's Ethernet port and other end is connected to a hub/switch. Or a network cable is connected to SecureSync and a stand-alone PC. 2) Verify network settings of SecureSync are valid for the network/PC it is connected with (IP address is on the same subnet as the other PC).
	Green "Good Link" is solid green on both SecureSync and other end of network cable.	SecureSync ICMP test is passing. SecureSync is connected to PC via Ethernet connection	1) Disconnect SecureSync's network cable and ping its assigned address to ensure no response (no duplicate IP addresses on the network). 2) Try accessing SecureSync from another PC on the same network. 3) Network Routing/firewall issue. Try connecting directly with a PC and network cable.

Table 5-1: Troubleshooting network connection issues

5.1.4 Troubleshooting via Web UI Status Page

SecureSync's Web UI includes pages that provide current "remote" status information about SecureSync. The following table includes information that can be used as a troubleshooting guidance if status fault indications or conditions occur.

Table 5-2: 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	SecureSync is in Holdover mode—OR—SecureSync is now out of Time Sync	All available Input References have been lost. The Reference Status table on the HOME page will show the current status of all inputs (Green is valid and Red is invalid or not present). 1. Make sure the Input Reference Priority table still has the desired reference inputs Enabled, based on the desired priority. See "Configuring Input Reference Priorities" on page 219. 2. Make sure the desired input references are still connected to the correct input port of SecureSync. 3. Verify GNSS antenna installation (if applicable). See "Troubleshooting GNSS Reception" on page 379.

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 (SecureSync may have been in Holdover mode, but Holdover has since expired without the return of valid inputs)	Note: If SecureSync was just recently powered-up or rebooted and input references are applied, no troubleshooting may be necessary. Allow at least 10-20 minutes for the input references to be declared valid and NTP to align to the System Time (allow an additional 35-40 minutes for a new install with GNSS input). 1. Verify in the Configure Reference Priorities table that all available references enabled. See "Configuring Input Reference Priorities" on page 219. 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 SecureSync reports GPS, Holdover, and/or Time Sync Alarms caused by insufficient GNSS reception:

When a GNSS receiver is installed in SecureSync, a GNSS antenna can be connected to the rear panel antenna connector via a coax cable to allow it to track several satellites in order for GNSS to be an available input reference. Many factors can prevent the ability for the GNSS receiver to be able to track the minimum number of satellites.

With the GNSS antenna installed outdoors, with a good view of the sky (the view of the sky is not being blocked by obstructions), SecureSync will typically track between 5-10 satellites (the maximum possible is 12 satellites). If the antenna's view of the sky is hindered, or if there is a problem with the GNSS antenna installation, the GNSS receiver may only be able to a few satellites or may not be able to track any satellites at all.

When GNSS is a configured time or 1PPS input reference, if the GNSS receiver is unable to continuously track at least four satellites (until the initial GNSS survey has been completed) or at least one satellite thereafter, the GNSS signal will not be considered valid. If no other inputs are enabled and available, SecureSync may not initially be able to go into time sync. Or, if GNSS reception is subsequently lost after initially achieving time sync, SecureSync will go into the Holdover mode. If GNSS reception is not restored before the Holdover period expires (and no other input references become available) SecureSync will go out of sync. The GNSS reception issue needs to be troubleshot in order to regain time sync.

For additional information on troubleshooting GNSS reception issues with SecureSync, please refer to the **GNSS Reception Troubleshooting Guide**, available here on the Safran website.

5.1.6 Troubleshooting – Outputs

If the 1PPS from the DCLS OUT BNC connector and/or the 15-pin multi-I/O connector outputs are not present, input power may not be applied. Or SecureSync is not synchronized to its input references and Signature Control is enabled.

Table 5-3: Troubleshooting outputs not being present

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 SecureSync. 3. Verify GNSS antenna installation (if applicable).
Navigate to INTERFACES/OUTPUTS page	Select the Outputs 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 SecureSync is not fully synchronized with its input references.

5.1.7 Troubleshooting the Serial Port

The front panel or rear panel serial port can be used for SecureSync configuration or to obtain select data. The serial port is a standard DB9 female port. Communication with this port is via a standard DB9 F to DB9M serial cable (minimum pinout is pin 2 to 2, pin 3 to 3 and pin 5 to 5) connected to a PC running a terminal emulator program such as Tera Term or Microsoft HyperTerminal. The port set-

tings of the terminal emulator should be configured as 115200, N, 8, 1 (flow control setting does not matter).

If the terminal emulator program does not display any data when the keyboard <Enter> key is pressed, either SecureSync is not powered up or there is a problem with the connection between SecureSync and the PC.

Using a multimeter, ring out the pins from one end of the serial cable to the other. Verify the cable is pinned as a straight-thru serial cable (pin 2 to 2, pin 3 to 3 and pin 5 to 5) and not as a null-modem or other pin-out configuration.

Disconnect the serial cable from SecureSync. Then, jumper (using a wire, paperclip or car key, etc.) pins 2 and 3 of the serial cable together while pressing any character on the PC's keyboard. The character typed should be displayed on the monitor. If the typed character is not displayed, there is a problem with either the serial cable or with the serial COM port of the PC.

Refer to "Setting up a Terminal Emulator" on page 575 for more information on using a terminal emulator software to communicate with SecureSync via serial port.

5.1.8 Troubleshooting the Cooling Fan(s)

The cooling fan (located on the front panel, to the right of the LED time display) is a temperature controlled cooling fan. Temperature sensor(s) determine when the cooling fan needs to turn on and off. It is normal operation for the cooling fan to not operate the entire time SecureSyncis running. The cooling fan may be turned off for long periods at a time, depending on the ambient and internal temperatures.



Note: Depending on your unit, there may be one or two cooling fans.

On the**HOME**screen of the Web UI, the**Fan Status**indicator in the**System Status**panel indicates the current operational status of the cooling fans.

In the CLI (Command Line Interface), inputting the`fanstatus`command will output the current operational status of the cooling fans and fan speeds.

Note: The fan status forSecureSyncunits with one cooling fan will always display as FAULT.

To verify the cooling fan is still operational, power cycle SecureSync unit .

Note: If the internal temperature in the unit is below 30 degrees Celsius, the fan may not turn on as part of the power-up sequence. In this case, it is recommended to let the unit “warm up” for approximately 30 minutes, in order to allow the unit to get to the appropriate temperature.

See also: "Temperature Management" on page 345

5.1.9 Troubleshooting – Network PCs Cannot Sync

In order for clients on the network to be able to sync to SecureSync, several requirements must be met:

1. The PC(s) must be routable to SecureSync. Make sure you can access SecureSync Web UI from a PC that is not syncing. If the PC cannot access the Web UI, a network issue likely exists. Verify the network configuration.
2. The network clients have to be configured to synchronize to SecureSync's address. For additional information on syncing Windows PC's, 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 SecureSync, the issue is likely not with SecureSync itself. The only SecureSync configurations that can prevent certain PCs from syncing to the time server are the NTP Access table and MD5 authentication. 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 SecureSync must be “in sync” and at a higher Stratum level than Stratum 15 (such as Stratum 1 or 2, for example). This requires SecureSync

to be either synced to its input references or in Holdover mode. Verify the current NTP stratum level and the sync status.

5.1.10 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 Option Cards

This Chapter lists all option cards currently available, their features, specifications, and how to configure them via the Web UI.

5.2.1 Accessing Option Cards Settings via the Web UI

The topics below describe Web UI functionality that is common to all Option Cards.

5.2.1.1 Web UI Navigation: Option Cards

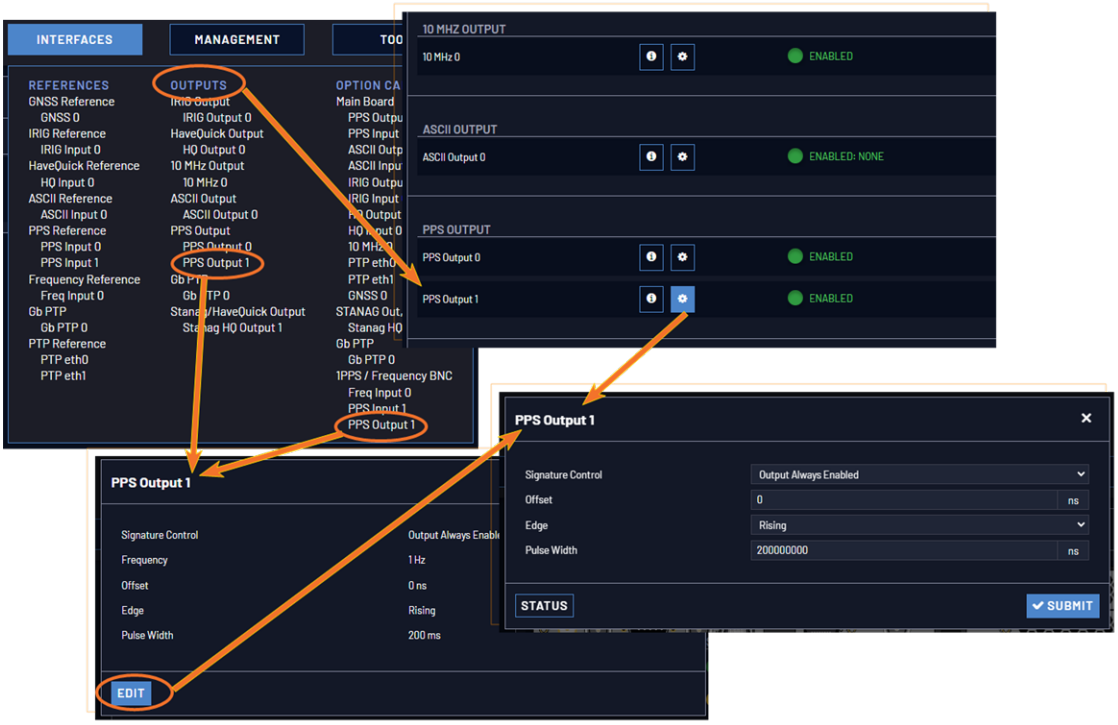


Figure 5-1: Option card navigation

To view or edit option card settings in the SecureSync Web UI (see also image above):

Status Summary panel

» Under **INTERFACES > OPTION CARDS**, clicking the superordinate list entry will open the Status Summary panel, which provides a status overview, as well as access to the Status window and the Edit window.

Status window

» Under **INTERFACES > OPTION CARDS**, clicking subordinate (indented) entries will open the Status window, providing detailed option card status information.

Edit window

» To edit option card settings, either click the **Edit** button in the lower-left corner of the Status window, or click the GEAR button in the Status Summary panel: The Edit window will open.

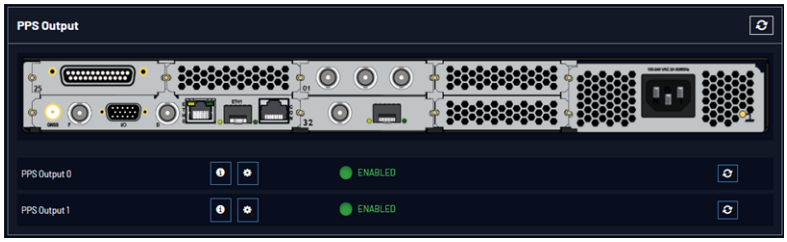
5.2.1.2 Viewing Input/Output Configuration Settings

The configurable settings of any SecureSync input or output interface can be viewed in its **Status** window. The **Status** window can be accessed in several ways; the procedure below describes the standard way:

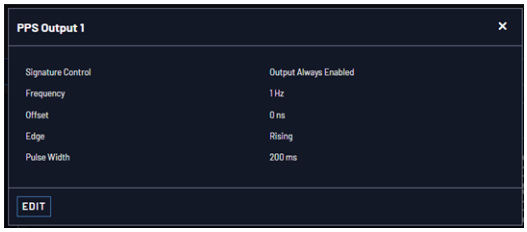
1. Identify the name of the option card, (e.g., **PPS OUT, 4-BNC**) and the name of the input or output you want to configure (e.g., **PPS Output 1**).

> **Note:** If you have only one input or output of any type, SecureSync will number that input or output 0. Additional inputs or outputs will be numbered 1 or above.

2. Navigate to **INTERFACES > OPTION CARDS**, and click the list entry of the option card identified above. The option card's Status Summary panel opens:



3. Click on the INFO button next to the input or output whose settings you wish to review. The **Status** window will open:



4. If you want to change any of the settings shown in the Status window, click the **Edit** button in the bottom-left corner. The **Edit** window will open:



5. Information about the configurable settings can be found in the corresponding option card section, see "Option cards listed by their ID number" on page 21.

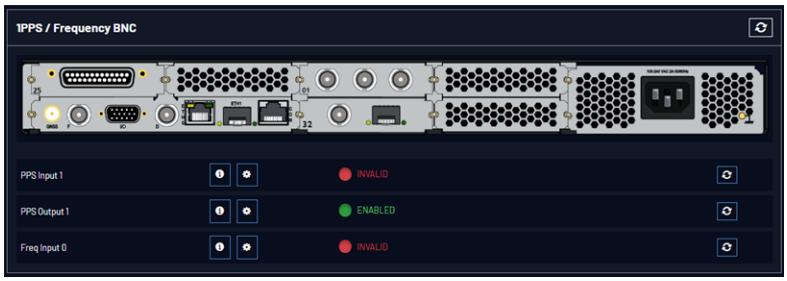
5.2.1.3 Configuring Option Card Inputs/Outputs

The configurable settings of any SecureSync input or output interface are accessible through the **Edit** window of the option card to which the input or output belongs. The **Edit** window can be accessed in several ways; the procedure below describes the standard way:

1. Identify the name of the card, (e.g., **PPS OUT, 4-BNC**), and verify the name of the input or output you want to configure (e.g., **PPS Output 1**).

> **Note:** If you have only one input or output of any type, SecureSync will number that input or output 0. Additional inputs or outputs will be numbered 1 or above.

2. Navigate to the **INTERFACES > OPTION CARDS** drop-down menu, and click the list entry of the option card identified above. The option card's Status Summary panel opens:



3. Click on the GEAR button next to the input or output you wish to configure (as verified in Step 1 of this procedure). The **Edit** window of the input or output opens:



4. Information about the configurable settings can be found in the corresponding option card section, see "Option cards listed by their ID number" on page 21.

5.2.1.4 Viewing an Input/Output Signal State

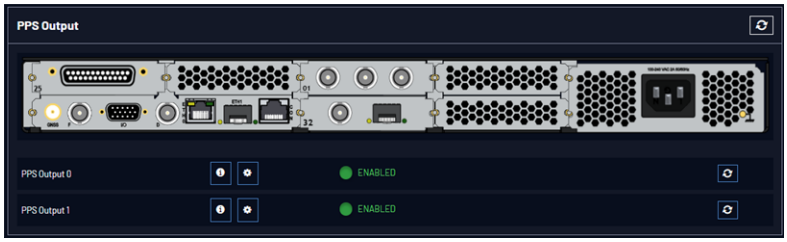
To view if an input or output is currently enabled or disabled, go to the option card's Status Summary panel:

1. Identify the name of the option card, (e.g., **PPS OUT, 4-BNC**), and the name of the input or output you want to configure (e.g., **PPS Output 1**).

> **Note:** If you have only one input or output of any type, SecureSync will number that input or output 0. Additional inputs or outputs will be numbered 1 or above.

2. Navigate to the **INTERFACES > OPTION CARDS** drop-down menu, and click the list entry of the option card identified above. The option card's

Status Summary panel opens:



All the inputs and/or outputs of this option card are listed in the Status Summary panel.

In accordance with the Signature Control setting, and the Lock Status, the current signal state for an output is indicated as:

- **ENABLED** (green); or
- **DISABLED** (orange)

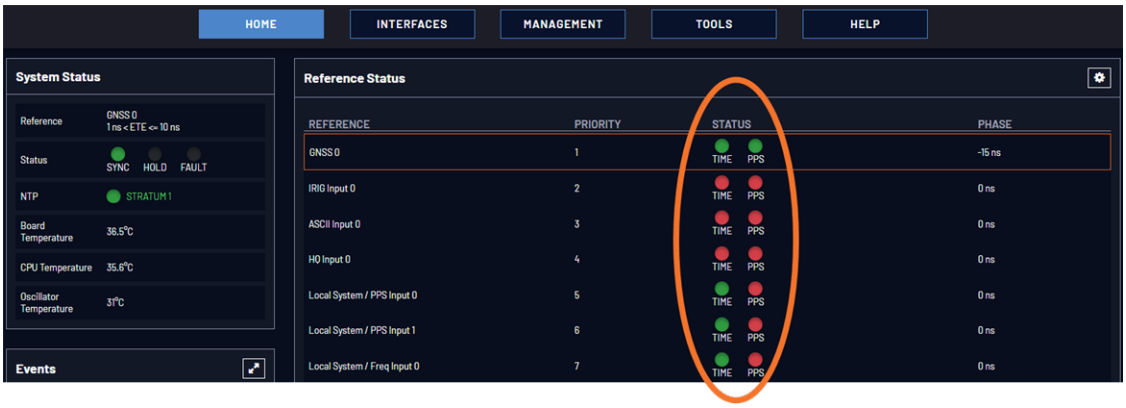
The current state of an input signal is indicated as:

- **VALID** (in green); or
- **INVALID** (in red)

The Status Summary panel will be refreshed automatically every 30 seconds. Click the **Refresh** button (circling arrows) on the right to refresh the status instantaneously. A slight refreshment delay is normal (the duration depends on the configuration of your system.)

5.2.1.5 Verifying the Validity of an Input Signal

The **HOME** page of the SecureSync Web UI provides quick access to the status of all inputs via its **Reference Status** panel.



If an INPUT is not present, or not valid, and qualified, the **1PPS Validity** and **Time Validity** fields will be "**Not Valid**" (orange).

If an INPUT is present, and the signal is considered valid, and qualified, the two indicators will then turn "Valid" (Green).

5.2.2 Option Card Field Installation Instructions

Typically, SecureSync units are shipped with custom-ordered option cards pre-installed at the factory. In the event that an option card is purchased at a later time, you need to install it yourself, following the instructions below.

5.2.2.1 Field Installation: Introduction

SecureSync time and frequency synchronization system offers customizability and expandability via the addition of a range of modular option cards. Up to 6 option cards (depending on your unit specifications) can be accommodated to offer not only synchronization to a variety of input references, but also numerous types of output signals, supporting an extensive number of traditional and contemporary timing protocols including:

- digital and analog timing and frequency signals (1PPS, 1MHz/5MHz/10 MHz)
- timecodes (IRIG, STANAG, ASCII)
- high accuracy and precision network timing (NTP, PTP)
- telecom timing (T1/E1), and more.



Note: The installation procedure varies, depending on the type of option card and the installation location to be installed.

5.2.2.2 Outline of the Installation Procedure

The general steps necessary for installing SecureSync option cards are as follows:

1. If adding or removing option cards that provide a reference, optionally backup your SecureSync configuration (refer to "[2]: Saving Reference Priority Configuration" on page 392, if applicable to your scenario or environment.)
2. Safely **power down** the SecureSync unit and remove the top cover of the main chassis (housing).



DANGER! SecureSync does not have an ON/OFF switch. It is necessary to unplug the machine to remove power!

Caution: NEVER install an option card from the rear of the unit, ALWAYS from the top, after removing the chassis cover.

3. Select one of the unused Slots as installation location for the new card. The chosen Slot **determine**s the installation procedure (see "[3]: Determining the Installation Procedure" on page 393).
4. **Prepare** slot (if required), and plug card into the slot.
5. **Connect** any required cables and secure option card into place.
6. Replace chassis cover, **power on** unit.
7. Log in to the SecureSync web interface; **verify** the installed card is identified.
8. **Restore**SecureSync configuration (if it had been backed up before, see above).

5.2.2.3 Safety

Before beginning any type of option card installation, please carefully read the safety statements and precautions under "SAFETY" on page 45.

5.2.2.4 [1]: Unpacking

On receipt of materials, unpack and inspect the contents and accessories (retain all original packaging for use in return shipments, if necessary).

The following items are included with the **ancillary kit** for the field installation of option card(s). Some of the parts listed below will not be required for the installation (depending upon option card model, and installation location).

Table 5-4: Parts list, Ancillary Kit [1204-0000-0700]

Item	Quant.	Part Number
50-pin ribbon cable	1	CA20R-R200-0R21
Washer, flat, alum., #4, .062 thick	2	H032R-0440-0002
Screw, M3-.5, 18-8SS, 4 mm, thread lock	5	HM11R-03R5-0004
Standoff, M3 x 18 mm, hex, M-F, 18-8 stainless steel	2	HM50R-03R5-0118
Standoff, M3 x 12 mm, hex, M-F, 18-8 stainless steel	1	HM50R-03R5-0112
Cable tie	2	MP00000

In addition to the parts supplied with your option card ancillary kit, you will need a #1 Phillips head screwdriver, and may need a cable tie clipper and 6mm nut driver.

5.2.2.5 [2]: Saving Reference Priority Configuration

Note: This step is optional.

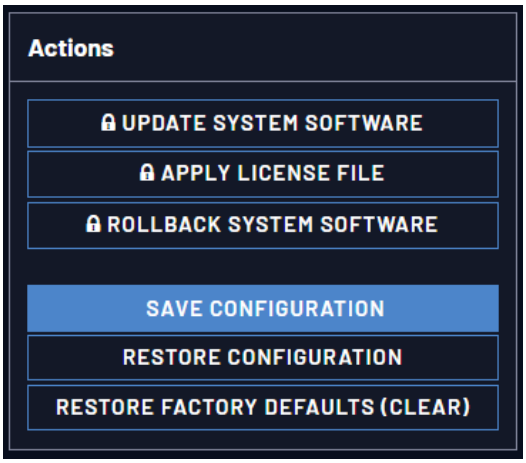
When adding or removing option cards with reference inputs such as IRIG Input, ASCII Timecode Input, etc., any user-defined Reference Priority configuration will be reset back to the factory default. This means that you will need to re-configure the Reference Priority table at the end of the installation procedure.

To avoid this manual re-configuration, you can save your configuration: For instructions, see "Saving the System Configuration Files" on page 364.

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.

Note: The Reference Priority configuration must be saved BEFORE beginning the hardware installation.

After completion of the hardware installation, the Reference Priority configuration needs to be restored; see STEP [12].

5.2.2.6 [3]: Determining the Installation Procedure

The installation procedure for option cards varies, depending on:

i. option card model
ii. installation slot chosen by you, and
iii. for upper slots only: if the bottom slot is used or not.

Determining the correct installation procedure

a. Identify the last two digits of the **part number** of your option card (see label on bag).

b. Inspect the back of the SecureSync housing, and select an **empty slot** for the new card. If the card is to be installed in one of the upper slots (4, or 6), take note if the corresponding lower slot (3 or 5) is occupied.

   Slots 1 and 2 always have an occupied slot below them.

   Units must be equipped with an Extension Board to fill option card slots 3, 4, 5, and 6.

> **Note:** To identify if the unit is equipped with an Extension Board, safely power down the SecureSync unit and remove the top cover of the main chassis (housing).

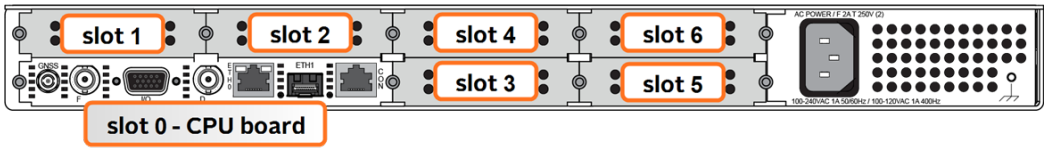


Figure 5-2: Unit rear view

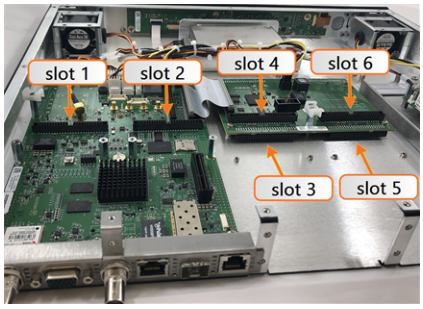


Figure 5-3: Unit internal view (from rear)

c. Identify your installation steps via the table below.

   i. Find your **part number** in the left-hand column. Some cards require special installation steps or specific locations.

   ii. Choose your **Installation Location** (as determined above).

   iii. If using slots 4 or 6, select either the **Bottom Slot** row "empty" or "populated"

iv. Note or highlight the **PROCEDURE STEPS [x]** for your installation scenario and follow the procedure step by step.

Table 5-5: Installation steps

Part No. Option Card	Card Function	Installation Location	Bottom Slot	PROCEDURE STEPS [x]
1204-08 1204-26 1204-1C	Frequency output	Slot 1 or 2		1, 2, 3, 4, 9, 12, 13
		Slot 3 or 5		1, 2, 3, 5, 9, 12, 13
		Slot 4 or 6	empty	1, 2, 3, 6, 9, 12, 13
			populated	1, 2, 3, 7, 9, 12, 13
1204-0F	Alarm relay	Slot 1 or 2		1, 2, 3, 4, 10, 12, 13
		Slot 3 or 5		1, 2, 3, 5, 10, 12, 13
		Slot 4 or 6	empty	1, 2, 3, 6, 10, 12, 13
			populated	1, 2, 3, 7, 10, 12, 13
1204-1F	NENA-Compliant	Slots 1 & 2		1, 2, 3, 4, 11, 12, 13
1204-49 1204-4A	Gb Ethernet and NTP Networking	Slot 1 or 2		1, 2, 3, 4, 12, 13
1204-58 1204-59	White Rabbit Option Cards (WROX)	Slots 3 & 4 or 5 & 6		1, 2, 3, 8, 12, 13
All other Part No.'s	(miscellaneous)	Slot 1 or 2		1, 2, 3, 4, 12, 13
		Slot 3 or 5		1, 2, 3, 5, 12, 13
		Slot 4 or 6	empty	1, 2, 3, 6, 12, 13
			populated	1, 2, 3, 7, 12, 13

Note: All installation situations include steps 1 (unpacking), 2 (save reference configuration), 3 (determine installation procedure), 12 (verifying hardware detection and software upgrade) and 13 (restoring configurations)

Steps 4 through 11 of this installation procedure should only be performed if your installation location or card requires it.

5.2.2.7 [4]: Slot 1 & 2 Installation

Option cards installed in Slot 1 or Slot 2 sit on top of and are screwed into pre-installed standoffs and plug in to the unit through the included ribbon cable.

Instructions for installing an option card into one of the slots above the CPU board (**1** or **2**):

a. Safely power down the SecureSync unit and remove the top cover of the main chassis (housing). Save the screws.

b. DANGER! SecureSync does not have an ON/OFF switch. You must unplug the machine to remove power!

Caution: NEVER install an option card from the rear of the unit, ALWAYS from the top, after removing the chassis cover.

c. Unscrew and remove the blank option card plate from the back of the unit (or the existing option card). Save the screws.

d. Insert option card into the slot, lining up the screw holes on the card with the standoffs..

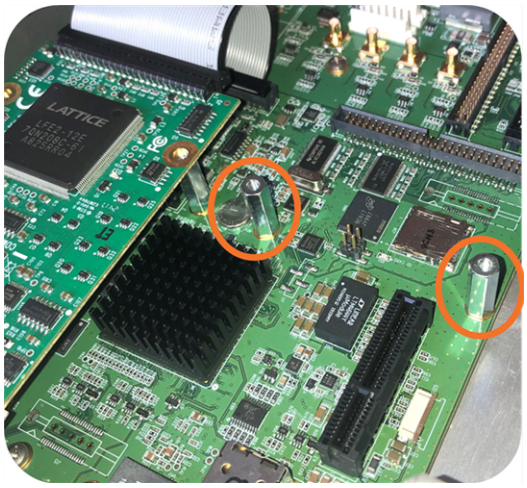
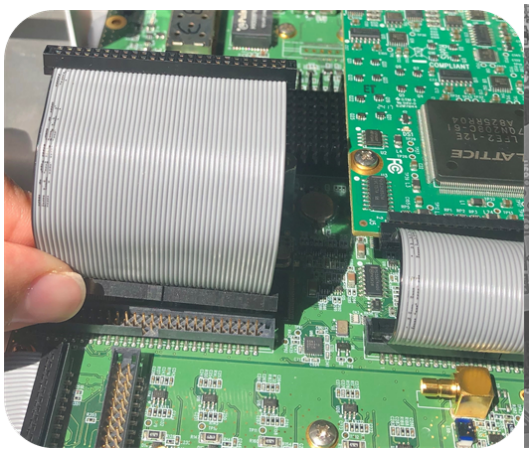
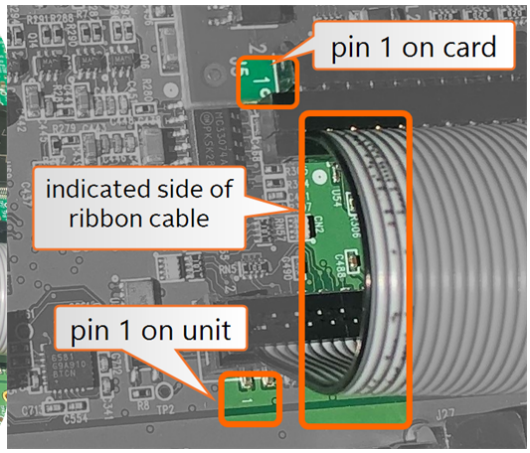


Figure 5-4: Standoffs location

e. Using the supplied M3 screws, screw the board, and the option card plate into the chassis, applying a torque of 0.9 Nm/8 in-lbs.

f. Take the supplied 50-pin ribbon cable and carefully press it into the connector on the mainboard (lining up the indicated end of the cable with PIN 1 on the mainboard), then into the connector on the option card (see Figure below).





> **Caution:** Ensure that the ribbon cable is aligned and fastened properly to all pins on the connector of the card, before powering the unit up, to avoid damage to the equipment.

5.2.2.8 [5]: Bottom Slot Installation

Instructions for installing an option card into one of the bottom slots (**3**, or **5**):

a. Safely power down the unit and remove the top cover of the main chassis (housing). Save the screws.

> **DANGER!** SecureSync does not have an ON/OFF switch. It is necessary to unplug the machine to remove power!

> **Caution:** NEVER install an option card from the rear of the unit, ALWAYS from the top, after removing the chassis cover.

b. Remove the blank option card plate, or the existing option card in the slot. Save the screws.

   If a card is populating the slot above the bottom slot your option card is to be installed into, remove it temporarily (also remove and save the screws and standoffs for reuse, washers may be discarded).

c. Insert the card into the bottom slot by carefully pressing its connector into the extension board connector (see Figure below), and by lining up the screw holes on the card with the screw holes on the chassis.

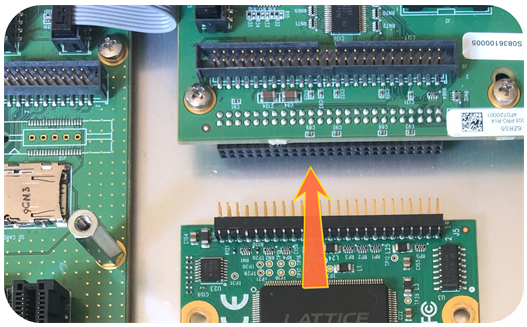


Figure 5-5: Connector installation

d. Using the supplied M3 screws, screw the board, and the option card plate into the chassis, applying a torque of 0.9 Nm/8 in-lbs.

   If you are reinstalling an option card above this one, you should instead follow the instructions for "[7]: Top Slot Installation, Bottom Slot Occupied" on page 401 (you will be using standoffs in this situation).

> **Caution:** Align and secure screw holes to chassis to avoid equipment damage.

5.2.2.9 [6]: Top Slot Installation, Bottom Slot Empty

Instructions for installing an option card into an upper slot (**4**, or **6**) of the SecureSync unit, with no card populating the bottom slot:

a. Safely power down your SecureSync unit and remove the top cover of the main chassis (housing). Save the screws.

> **DANGER!** SecureSync does not have an ON/OFF switch. It is necessary to unplug the machine to remove power!

> **Caution:** NEVER install an option card from the rear of the unit, ALWAYS from the top, after removing the chassis cover.

b. Remove blank option card plate, or existing option card. Save the screws.

c. Place one of the supplied washers over each of the two chassis screw holes (see Figure below), then screw the 18 mm standoffs (the longer standoffs) into the chassis (see Figure below), applying a torque of 0.9 Nm/8 in-lbs.

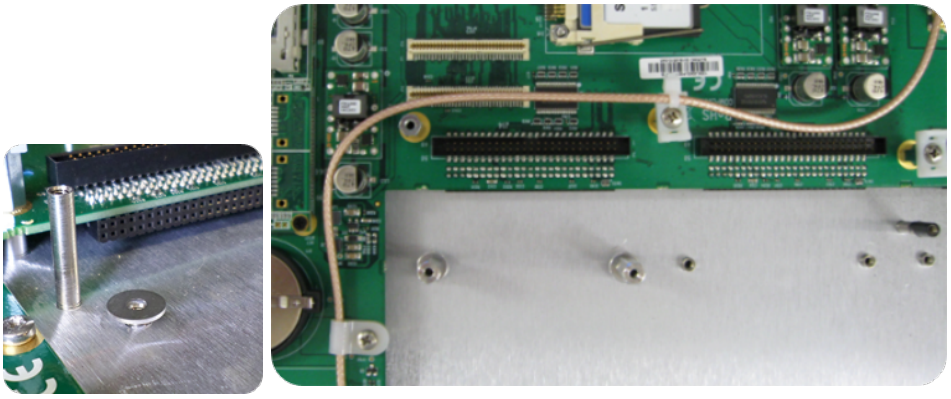


Figure 5-6: Washers & standoffs secured to chassis screw holes

d. Insert option card into the slot, lining up the screw holes on the card with the standoffs.

e. Using the supplied M3 screws, screw the board into the standoffs, and the option card plate into the chassis, applying a torque of 0.9 Nm/8 in-lbs.

f. Take the supplied 50-pin ribbon cable and carefully press it into the connector on the mainboard (lining up the indicated end of the cable with PIN 1 on the mainboard), then into the connector on the option card (see Figure below).

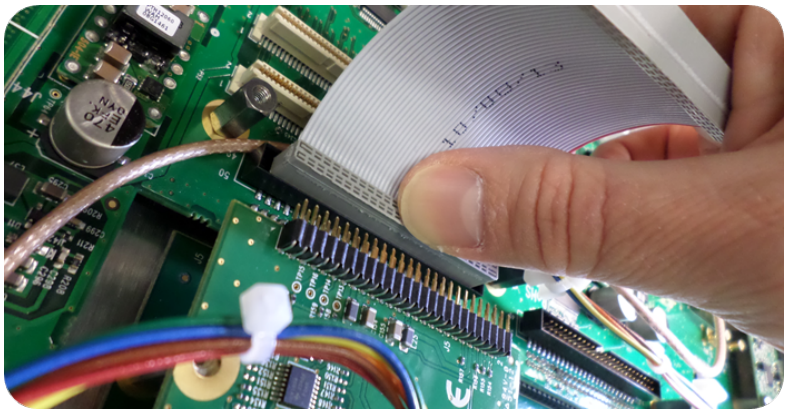


Figure 5-7: Ribbon cable installation

> **Caution:** Ensure that the ribbon cable is aligned and fastened properly to all pins on the connector of the card. Otherwise, damage to the equipment may occur during power-up.

5.2.2.10 [7]: Top Slot Installation, Bottom Slot Occupied

Instructions for installing an option card into an upper slot (**4**, or **6**), above a populated bottom slot:

a. Safely power down the SecureSync unit, and remove the top cover of the main chassis (housing). Save the screws.

b.

> **DANGER!** SecureSync does not have an ON/OFF switch. It is necessary to unplug the machine to remove power!

> **Caution:** NEVER install an option card from the rear of the unit, ALWAYS from the top, after removing the chassis cover.

c. Remove the blank option card plate, or the existing option card. Save the screws.

d. Remove screws securing the card already populating the bottom slot. Save the screws.

e. Screw the 18-mm standoffs into the option card populating the bottom slot (see Figure below) , applying a torque of 0.9 Nm/8 in-lbs.

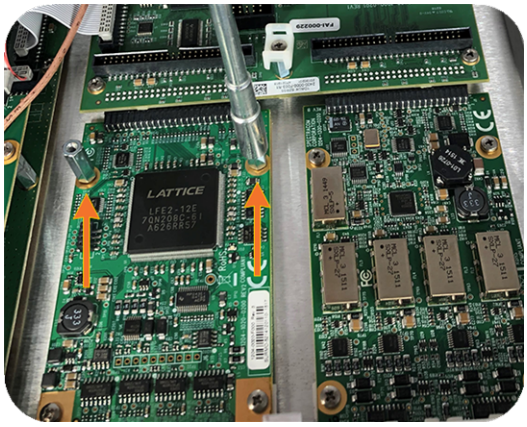


Figure 5-8: Bottom card with standoffs installed

f. Insert option card into the slot above the existing card, lining up the screw holes with the standoffs.

g. Using the supplied M3 screws, screw the board into the standoffs, and the option plate into the chassis, applying a torque of 0.9 Nm/8 in-lbs.

h. Take the supplied 50-pin ribbon cable and carefully press it into the connector on the extension board (lining up the ribbon cable with PIN 1 on the board with PIN 1 on the card), then into the connector on the option card (see Figure below).

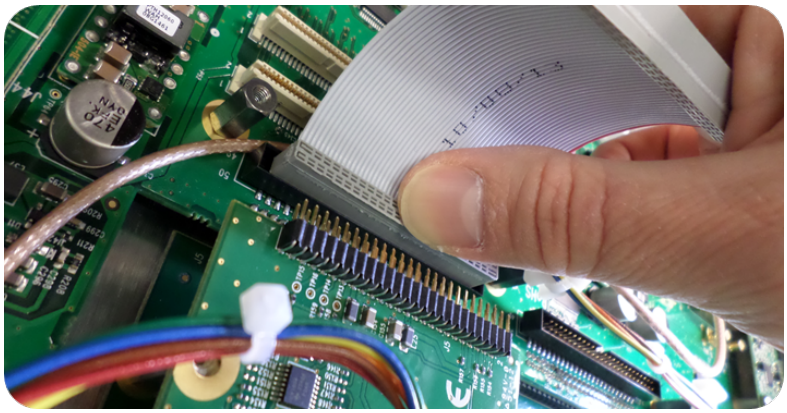


Figure 5-9: Ribbon cable installation

> **Caution:** Ensure that the ribbon cable is aligned and fastened properly to all pins on the connector of the card. Otherwise, damage to equipment may result during power up.

5.2.2.11 [8]: WROX Card Installation

This card requires an open bottom slot and an open top slot. Instructions for installing a WROX card (PN 1204-58 and 1204-59) into slots **3 & 4** or **5 & 6**:

a. Safely power down the unit and remove the top cover of the main chassis. Save the screws.

> **DANGER!** SecureSync does not have an ON/OFF switch. It is necessary to unplug the machine to remove power!

> **Caution:** NEVER install an option card from the rear of the unit, ALWAYS from the top, after removing the chassis cover.

b. Remove the blank option card plates, or the existing option card(s) in the slots. Save the screws.

c. Feed the coax cable straight through the slot to avoid interference with card insertion.

d. Insert the card into the slot by carefully pressing its connector into the extension board connector (see Figure below), and by lining up the screw holes on the card with the screw holes on the chassis. Align and secure screw holes to chassis to avoid equipment damage.

> **Caution:** WROX cards are larger and require caution during installation. Unintended contact with the chassis and standoffs may cause equipment damage.

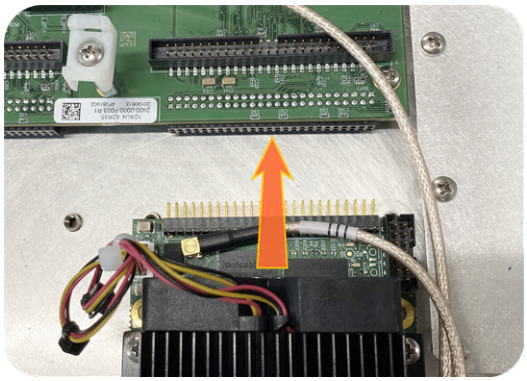


Figure 5-10: Connector installation

e. Using the supplied M3 screws, screw the board, and the option card plate into the chassis, applying a torque of 0.9 Nm/8 in-lbs.

f. Install the coax cable onto the main PCB, connecting it to the first available open connector, from **J4** to **J7**. See Figure below:

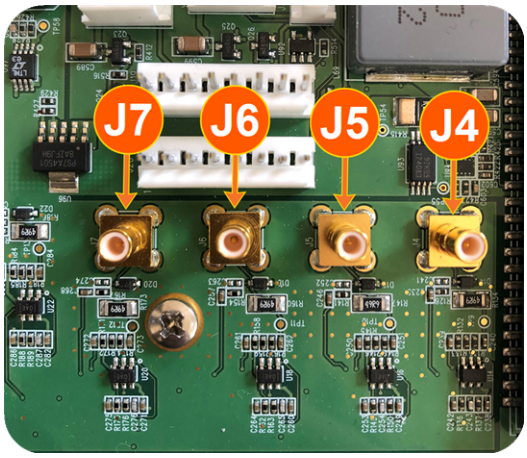


Figure 5-11: J Connectors (10MHz Outputs)

g. Using the supplied cable ties, secure the coax cable from the option card to the white nylon cable tie holders fastened to the mainboard.

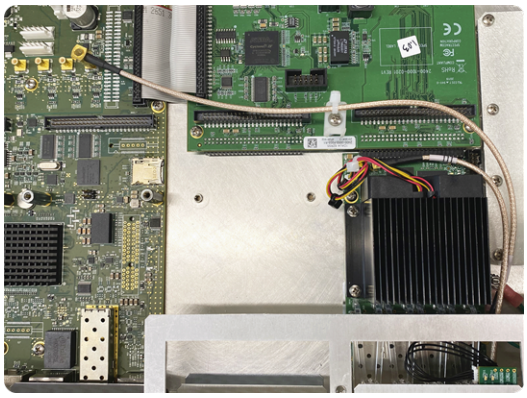


Figure 5-12: Completed installation

WROX requires a different upgrade procedure than other option cards. More information can be found in the main user manual: https://safran-navigation-timing.com/manuals/2400/Content/NC_and_SS/2400/OCs/WROX/WROC.htm.

5.2.2.12 [9]: Frequency Output Cards: Wiring

Additional installation instructions for the following option card models:

- Frequency Output cards:
  - 1MHz (PN 1204-26)
  - 5MHz (PN 1204-08)
  - 10 MHz (PN 1204-1C)

For the cable installation, follow the steps detailed below:

a. Install the coax cable(s) onto the main PCB, connecting them to the first available open connectors, from J4 to J7. See figure below:

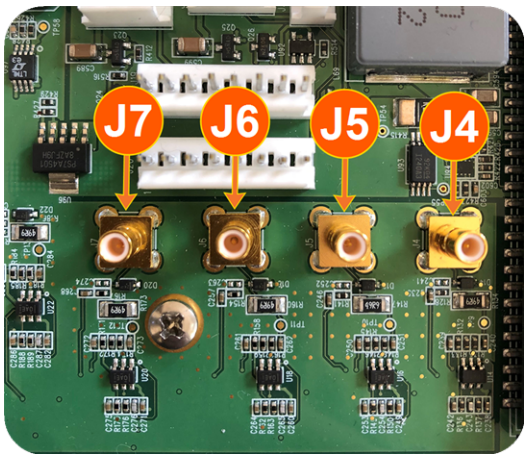


Figure 5-13: J Connectors (10MHz Outputs)

b. Using the supplied cable ties, secure the coax cable from the option card to the white nylon cable tie holders fastened to the mainboard.

5.2.2.13 [10]: Alarm Relay Card, Cable Installation

Additional steps for the installation of the Alarm Relay Output card (PN 1204-0F).

a. Connect the supplied cable, part number 8195-0000-5000, to the main-board connector J19. If your connector has 8 pins, use pins 3 - 8 as shown in the figure below.

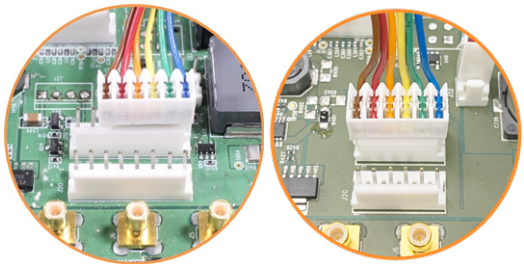


Figure 5-14: [Left] J19 Connector with 8 pins, [Right] J19 Connector with 6 pins, seen from rear of unit.

b. Using the supplied cable ties, secure the cable, part number 8195-0000-5000, from the option card to the white nylon cable tie holders fastened to the mainboard (see figure below). Use the fastener closest to your installation location.

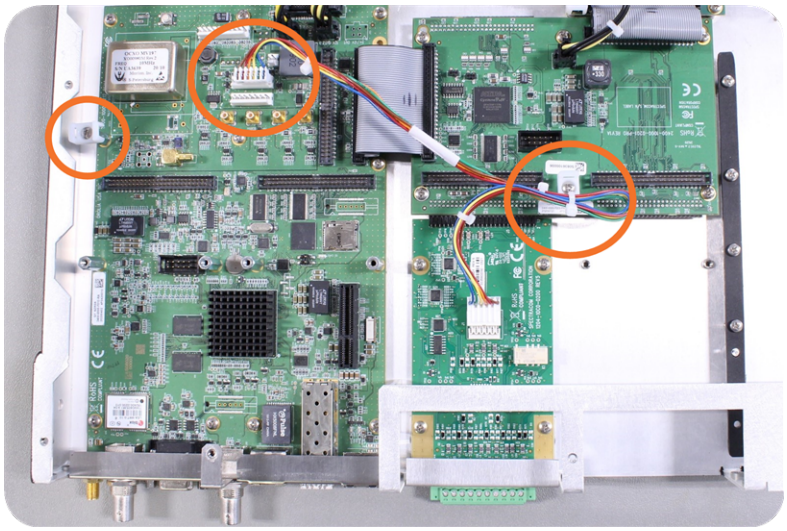


Figure 5-15: Cable routing

5.2.2.14 [11]: NENA Card, Cable Installation

Additional steps for the installation of the NENA card (PN 1204-1F).

Note: The double-wide NENA card can only be installed in slots 1 & 2 on the SecureSync 2400.

a. After installation in slots 1 and 2, connect the supplied cable, part number 8195-0000-5000, to the mainboard connector J19. If your connector has 8 pins, use pins 3 - 8 as shown in the figure below.

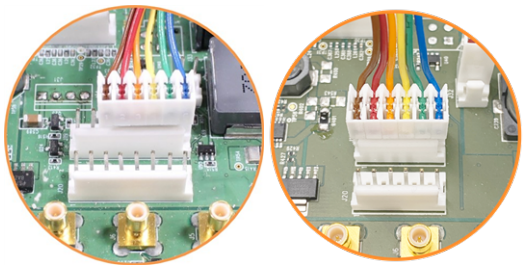


Figure 5-16: [Left] J19 Connector with 8 pins, [Right] J19 Connector with 6 pins, seen from rear of unit.

b. Using the supplied cable ties, secure the cable, part number 8195-0000-5000, from the option card to the white nylon cable tie holder fastened to the mainboard (see figure below).

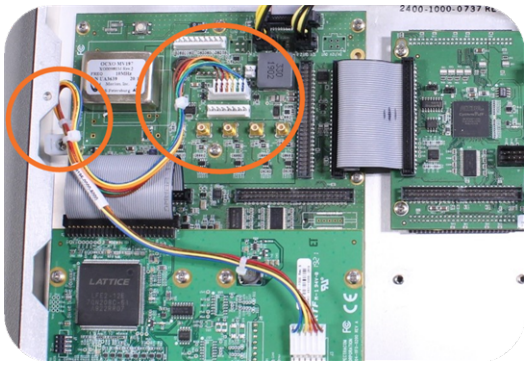


Figure 5-17: Cable routing

5.2.2.15 [12]: Verifying HW Detection and SW Update

Complete the Option Card installation procedure by verifying that SecureSync detected the card, and by updating the system software:

a. Re-install the top cover of the unit chassis (housing), using the saved screws.

> **Caution:** Ensure that screw holes on the card are properly lined up and secured to the chassis before powering the unit up, otherwise damage to the equipment may result.

b. Power on the unit.

c. Verify the successful installation by ensuring the card has been detected:

Open a web browser, log in to the SecureSync Web UI, and navigate to **INTERFACES > OPTION CARDS**: The new card will be displayed in the list.

» If the card **does not** appear to be properly identified, proceed with the Software update as described below, and then navigate to **INTERFACES > OPTION CARDS** again to confirm the card has been detected.

» If the card has been detected properly, proceed with the Software update as described below to ensure SecureSync and the newly installed card are using the same, latest available version.

Updating the System Software

Even if the newly installed option card has been detected, and even if the latest System Software version is installed on your SecureSync unit, it is recommended to (re-)install the software to ensure both SecureSync, and the option card are using the latest software:

» Follow the System Software update procedure, as outlined in the main SecureSync User Manual under "Software Updates" on page 359.

NEXT: Restore your reference priority configuration, as described in the following topic, and configure other option card-specific settings, as described in the main User Manual.

5.2.2.16 [13]: Restoring Reference Priority Configuration

If you saved your Reference Priority configuration under STEP [2], you can now restore it:

» For instructions, see "Restoring the System Configuration" on page 366.

Card-specific configuration instructions may be found in the Option Cards Guide, see "Option Card Identification" on page 21 to locate your card.

5.2.3 Time and Frequency Option Cards

This section contains technical information and Web UI procedures relevant to SecureSync option cards designed to deliver time and frequency signals.

5.2.3.1 1PPS Out [1204-18, -19, -21, -2B]

1PPS Output Modules (TTL, 10V, RS-485)

The 1PPS output module provides four additional 1PPS outputs on BNC connectors or terminal block for the SecureSync platform.

Model 1204-18 1PPS Output (TTL): Specifications

- **Outputs:** (4) 1PPS output
- **Signal Type and Connector:** TTL (BNC)
- **Output Load Impedance:** 50 Ω
- **Rise Time to 90% of Level:** <10 ns
- **Programmable Pulse Width:** 100 ns to 900 ms with 20 ns resolution
- **Absolute Phase Error:** ±50 ns (1σ)
- **Programmable Phase Shift:** ±5ns to 500 ms with 5ns resolution
- **Maximum Number of Cards:** 6
- **Ordering Information:** 1204-18 1PPS TTL output module, BNC connector

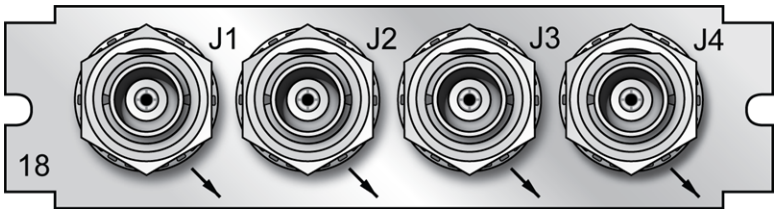


Figure 5-18: Model 1204-18 option card rear plate

Model 1204-19 1PPS Output (10 V): Specifications

- **Outputs: (**4) 1PPS output
- **Signal Type and Connector:** 10 V (BNC)
- **Output Load Impedance:** 50 Ω
- **Rise Time to 90% of Level:** <30 ns
- **Programmable Pulse Width:** 100 ns to 900 ms with 20 ns resolution
- **Absolute Phase Error:** ±50 ns (1σ)
- **Programmable Phase Shift:** ±5ns to 500 ms with 5ns resolution
- **Maximum Number of Cards:** 6
- **Ordering Information:** 1204-19 1PPS 10 V output module, BNC connector

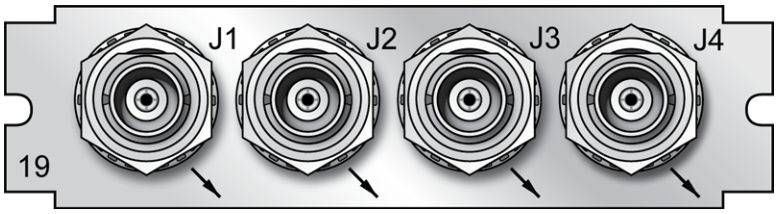


Figure 5-19: Model 1204-19 option card rear plate

Model 1204-21 1PPS Output (RS-485): Specifications

- **Inputs/Outputs:** (4) 1PPS output
- **Signal Type and Connector:** RS-485 (terminal block)
- **Output Load Impedance:** 120 Ω
- **Rise Time to 90% of Level:** <30 ns
- **Programmable Pulse Width:** 100 ns to 900 ms with 20 ns resolution
- **Absolute Phase Error:** ±50 ns (1σ)
- **Programmable Phase Shift:** ±5ns to 500 ms with 5ns resolution
- **Maximum Number of Cards:**6
- **Ordering Information:** 1204-21 1PPS RS-485 output module, terminal block

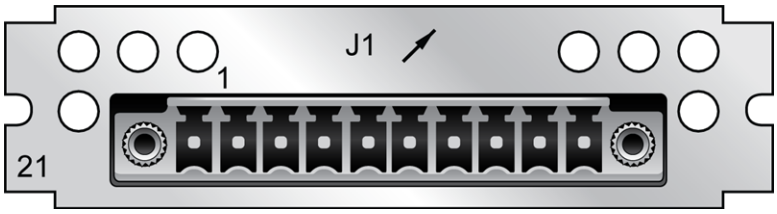


Figure 5-20: Model 1204-21 option card rear plate

Model 1204-21 terminal block pin assignments

Pin No.	Function
1	1PPS Output 1 +
2	1PPS Output 1 -
3	GND
4	1PPS Output 2 +
5	1PPS Output 2 -
6	1PPS Output 3 +
7	1PPS Output 3 -
8	GND
9	1PPS Output 4 +
10	1PPS Output 4 -

Model 1204-2B 1PPS Output (Fiber Optical): Specifications

- **Inputs/Outputs:** (4) 1PPS output
- **Operating Wavelength:** 820/850 nm
- **Optical Power:** -15 dBm average into 50/125 fiber
- **Fiber Optic Compatibility:** 50/125 µm, 62.5/125 µm multi-mode cable
- **Optical Connector:** ST
- **Programmable Pulse Width:** 100 ns to 900 ms with 20 ns resolution
- **Absolute Phase Error:** ±50 ns (1σ)
- **Programmable Phase Shift:** ±5ns to 500 ms with 5ns resolution

- **Maximum Number of Cards:** 6
- **Ordering Information:** 1204-12B 1PPS Fiber Optic output module, ST connector

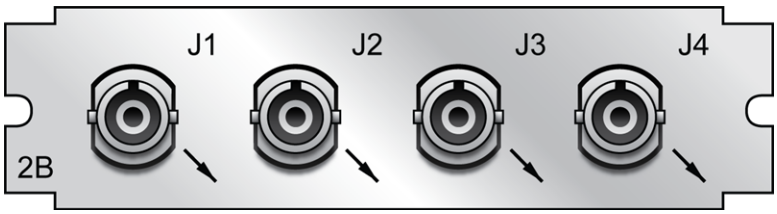


Figure 5-21: Model 1204-2B option card rear plate

1PPS Output: Edit Window

To configure the settings of a **1PPS Output**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entries for these option cards are:

- 1PPS OUT, 4-BNC
- 1PPS OUT, 10 V
- 1PPS OUT, RS-485
- 1PPS OUT, Fiber



The Edit window allows the configuration of the following settings:

- **Signature Control:** Used to control when the 1PPS output signal will be present. See "Signature Control" on page 198.
- **Offset:** Used to account for 1PPS cable delays or other latencies in the 1PPS output. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.
- **Edge:** The operator can select if the output signal is a positive (reference on the rising edge) or a negative (reference on the falling edge) pulse.

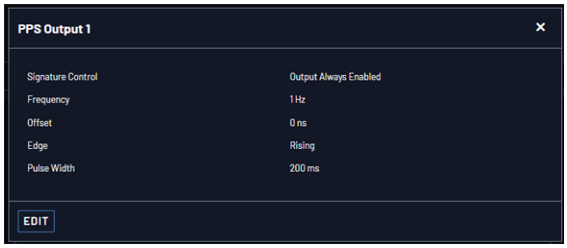
- **Pulse Width:** Configures the Pulse Width of the 1PPS output. The Pulse Width is entered and displayed in nanoseconds (ns). The default Pulse Width is 200 milliseconds.

1PPS Output: Status Window

To view the current settings of a **1PPS Output**, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entries for these option cards are:

- 1PPS OUT, 4-BNC
- 1PPS OUT, 10V
- 1PPS OUT, RS-485
- 1PPS OUT, Fiber



The Status window displays the following settings:

- **Signature Control:** Displays the current configuration of Signature Control; see "Signature Control" on page 198.
- **Frequency:** Indicates the configured frequency of the 1PPS output signal.
- **Offset:** Displays the configured Offset (to account for cable delays or other latencies).
- **Edge:** Shows if the on-time point of the 1PPS output is the rising or falling edge of the pulse.
- **Pulse Width:** Displays the configured Pulse Width of the 1PPS output. The Pulse Width is displayed in nanoseconds (ns). The default Pulse Width is 200 milliseconds.

5.2.3.2 1PPS In/Out [1204-28, -2A]

These 1PPS input/output cards provide one 1PPS input, and three or two additional 1PPS outputs on BNC or ST connectors for the SecureSync platform.

Model 1204-28 1PPS Input/Output: Specifications

- **Inputs/Outputs**: (1) 1PPS input/(3) 1PPS output
- **Signal Type and Connector**: TTL (BNC)
- **Input Impedance**: 50 Ω
- **Output Load Impedance**: 50 Ω
- **Rise Time to 90% of Level**: <10 ns
- **Programmable Pulse Width**: 100 ns to 900 ms with 20 ns resolution
- **Absolute Phase Error**: ±50 ns (1σ)
- **Programmable Phase Shift**: ±5ns to 500 ms with 5ns resolution
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-28: 1PPS 1-input/3-output, BNC connectors

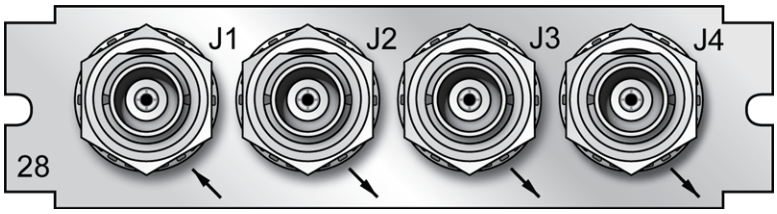


Figure 5-22: Model 1204-28 option card rear plate

Model 1204-2A 1PPS Input/Output: Specifications

- **Inputs/Outputs**: (1) 1PPS input/(2) 1PPS output
- Operating Wavelength: 820/850 nm
- **Optical Input Minimum Sensitivity**: -25 dBm @ 820 nanometers
- **Optical Output Power**: -15 dBm average into 50/125 fiber
- **Fiber Optic Compatibility**: 50/125 µm, 62.5/125 µm multi-mode cable
- **Optical Connector**: ST
- **Output Programmable Pulse Width**: 100 ns to 900 ms with 20 ns resolution

- **Output Absolute Phase Error**: ±50 ns (1σ)
- **Output Programmable Phase Shift**: ±5ns to 500 ms with 5ns resolution
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-2A: 1PPS 1-in/2-output, ST connectors

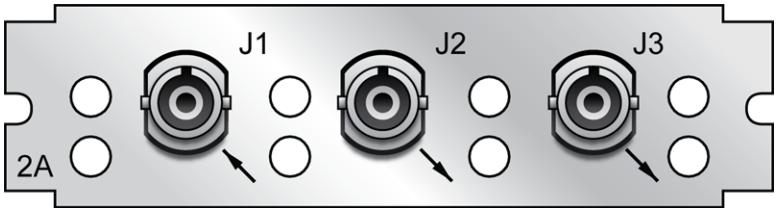


Figure 5-23: Model 1204-2A option card rear plate

1PPS Input or Output: Viewing Signal State

To quickly view if the 1PPS inputs and outputs of this option card are currently enabled or disabled, go to the option card's **Status Summary** panel. For instructions, see: "Viewing an Input/Output Signal State" on page 387.

1PPS Output: Edit Window

To configure the settings of a **1PPS output**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entries for these cards are:

- 1PPS In/Out
- 1PPS In/Out, Fiber

The connector numbers are:

- J2, J3, J4 (model -28)
- J2, J3 (model -2A)

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



The fields available are:

- **Signature Control**: Used to control when the 1PPS output signal will be present. See: "Signature Control" on page 198.
- **Offset**: Used to account for 1PPS cable delays or other latencies in the 1PPS output. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.
- **Edge**: The operator can select if the output signal is a positive (reference on the rising edge) or a negative (reference on the falling edge) pulse.
- **Pulse Width**: Configures the Pulse Width of the 1PPS output. The Pulse Width is entered and displayed in nanoseconds (ns). The default Pulse Width is 200 milliseconds.

1PPS Output: Status Window

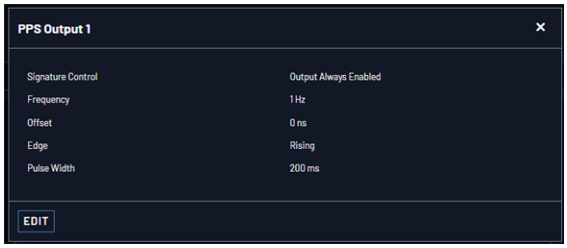
To view the current settings of a **1PPS output**, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entries for these cards are:

- 1PPS In/Out
- 1PPS In/Out, Fiber

The connector numbers are:

- J2, J3, J4 (model -28)
- J2, J3 (model -2A)



The fields displayed are:

- **Signature Control**: Displays the current configuration of Signature Control. See "Signature Control" on page 198.
- **Frequency**: Indicates the configured frequency of the 1PPS output signal.
- **Offset**: Displays the configured Offset (to account for cable delays or other latencies).
- **Edge**: Shows if the on-time point of the 1PPS output is the rising or falling edge of the pulse.
- **Pulse Width**: Displays the configured Pulse Width of the 1PPS output. The Pulse Width is displayed in nanoseconds (ns). The default Pulse Width is 200 milliseconds.

1PPS Input: Edit Window

To configure the settings of the **PPS Input** (also referred to as 'Reference'), go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entries for these cards are:

- 1PPS In/Out
- 1PPS In/Out, Fiber

The connector number for the input is: J1



The Edit window allows the configuration of the following settings:

- **Edge**: The operator can select either the rising or the falling edge as the input time reference (defines the on-time point of the signal).
- **Offset**: It is possible to add an offset to the input signal (to account for cable delays), with a resolution of 5ns and a positive or negative value of 500 ms maximum.

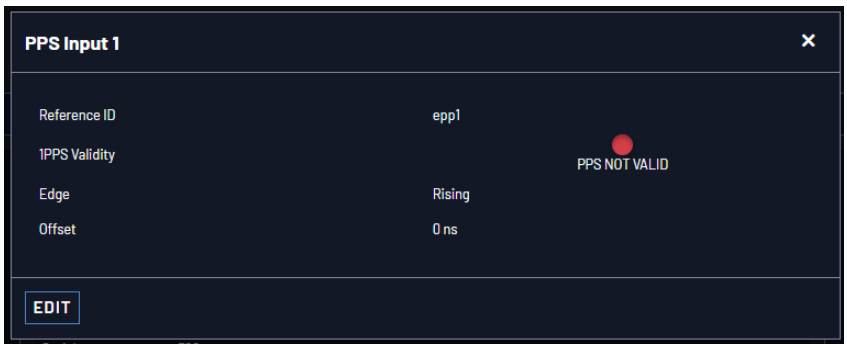
1PPS Input: Status Window

To view the current settings of the **PPS Input** (also referred to as 'Reference'), go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entries for these cards are:

- 1PPS In/Out
- 1PPS In/Out, Fiber

The connector number for the input is: J1



The Status window displays the following settings:

- **Reference ID**: Name used to represent this 1PPS input reference in the Reference Priority table. See also: "Configuring Input Reference Priorities" on page 219.
- **1PPS Validity**: Indicates "OK" (green) if the 1PPS input signal is present and valid. Indicates "Not Valid" (orange) if the 1PPS input signal is either not present or is not considered valid.
- **Edge**: Displays the selected Edge (rising of falling) of the 1PPS input that defines the on-time point.
- **Offset**: Displays the configured 1PPS offset values.

The 1PPS Input signal is analyzed and an absence of the signal triggers a "Not Valid" indication.

5.2.3.3 1PPS In/Out, 10 MHz In [1204-01, -03]

Model 1204-01, 1PPS/Freq Input (TTL): General Specifications

- **Inputs/Outputs**: One Frequency Input (=J1), one 1PPS Input (=J2), one 1PPS Output
- **Signal Type And Connector**: TTL/Sine (BNC into 50 Ω)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-01: 1PPS/Freq input (TTL levels) module

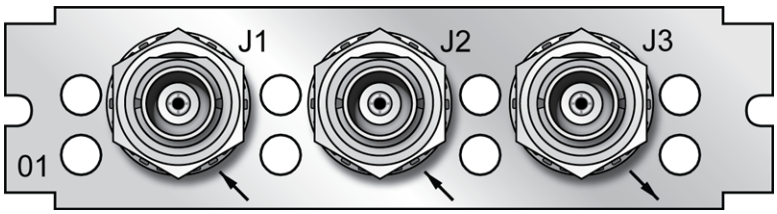


Figure 5-24: Model 1204-01 option card rear plate

Model 1204-03, 1PPS/Freq Input (RS-485): General Specifications

- **Inputs/Outputs**: (1) 1PPS Input, (1) Freq Input (1) 1PPS Output. All input and output signals are RS-485 compatible.
- **Signal Type And Connector**: Balanced RS-485 (3.8 mm terminal block)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-03: 1PPS/Freq input (RS-485 levels) module

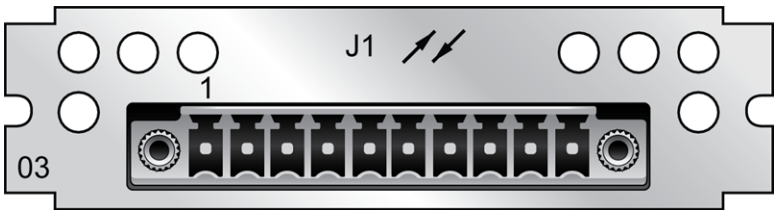


Figure 5-25: Model 1204-03 option card rear plate

Table 5-6: Model 1204-03 1PPS/Freq Input: Connector pin assignment

Pin No.	Signal	Function
1	GND	Ground
2	FREQIN_RS485+	RS-485 Frequency Input +
3	FREQIN_RS485-	RS-485 Frequency Input –
4	GND	Ground
5	PPSIN_RS485+	RS-485 1PPS Input +
6	PPSIN_RS485-	RS-485 1PPS Input –
7	GND	Ground
8	PPSOUT_RS485+	RS-485 1PPS Output +
9	PPSOUT_RS485-	RS-485 1PPS Output –
10	GND	Ground

Models 1204-01,-03: Input/Output Specifications

FREQ Input Specifications

- **Signal Type And Connector**: Sine wave (BNC)
- **Detected Level**: +13 dBm to -6dBm
- **Frequency Setting**: 1KHz...10 MHz in 1Hz steps

1PPS Input Specifications

- **Input Impedance**: 50 Ω
- **Minimum Pulse Width detected**: 100 ns
- **Input Signal Jitter**: <±500 ns t o achieve oscillator lock, <±50 ns to achieve system performance
- **Programmable Phase Shift**: ±5ns to 500 ms with 5ns resolution

1PPS Output Specifications

- **Signal Type And Connector**: TTL level (BNC)
- **Output Load Impedance**: 50 Ω

- **Rise Time to 90% of Level**: <10 ns
- **Programmable Pulse Width**: 100 ns to 900 ms with 20 ns resolution
- **Absolute Phase Error**: ±50 ns (1σ)
- **Programmable Phase Shift**: ±5ns to 500 ms with 5ns resolution

1PPS Input and Output: Viewing Signal State

To quickly view if the PPS inputs and outputs of this option card are currently enabled or disabled, go to the option card's Status Summary panel. For instructions, see: "Viewing an Input/Output Signal State" on page 387.

1PPS Input: Edit Window

To configure the settings for the **1PPS Input** (also referred to as 'Reference'), go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entries for these cards are: **1PPS/Frequency BNC** and **1PPS/Frequency RS-485**. The connector number is: J2 (Model 1204-03: RS-485 connector: Pins 5 and 6)



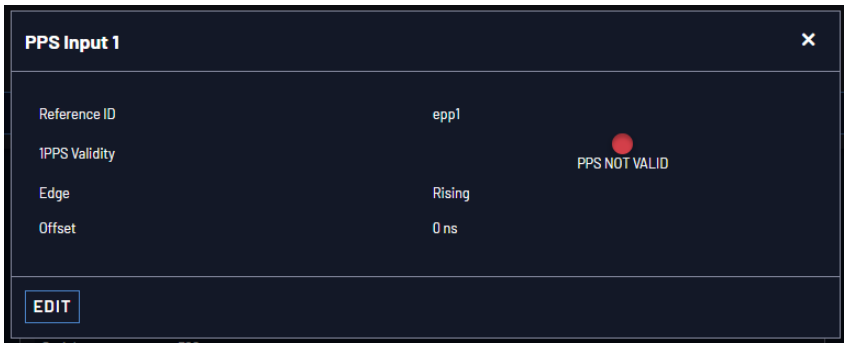
The Edit window allows the configuration of the following settings:

- **Edge**: The operator can select either the rising or the falling edge as the input time reference (defines the on-time point of the signal).
- **Offset**: It is possible to add an offset to the input signal (to account for cable delays), with a resolution of 5ns and a positive or negative value of 500 ms maximum.

1PPS Input: Status Window

To view the current settings of the **PPS Input** (also referred to as 'Reference'), go to its Status window. For instructions, see: "Verifying the Validity of an Input Signal" on page 388.

The Web UI list entries for these cards are: 1PPS/Frequency BNC and 1PPS/Frequency RS-485. The connector number is: J2 (Model 1204-03: RS-485 connector: Pins 5 and 6)



The Status window displays the following settings:

- **Reference ID**: Name used to represent this 1PPS input reference in the Reference Priority table; see "Configuring Input Reference Priorities" on page 219 for more information on reference priority configuration.
- **1PPS Validity**: Indicates “OK” (green) if the 1PPS input signal is present and valid. Indicates “Not Valid” (orange) if the 1PPS input signal is either not present or is not considered valid.
- **Edge**: Displays the selected Edge (rising of falling) of the 1PPS input that defines the on-time point.
- **Offset**: Displays the configured 1PPS offset values.

The 1PPS Input signal is analyzed and an absence of the signal triggers a “Not Valid” indication.

Frequency Input: Edit Window

To configure the settings for the **Frequency Input** (also referred to as ‘Reference’), go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entries for these cards are: 1PPS/Frequency BNC and 1PPS/Frequency RS-485. The connector number is: J1 (BNC card); J1 (RS-485 card).



The Edit window allows the configuration of the following settings:

- **Reference Mode**: Used to control how the reference mode operates in determining its validity. Values are:
  - **Primary Reference**—Allows the frequency reference to be valid based solely on its own presence.
  - **Secondary Reference**—Requires another valid reference to synchronize the system before the frequency reference can be determined to be valid. This is used when the frequency reference is intended to operate as a backup reference to a different primary reference source.
- **Frequency**: Used to configure the frequency (in Hertz) of the input signal. The available Frequency range is 1KHz...10 MHz in 1Hz steps.

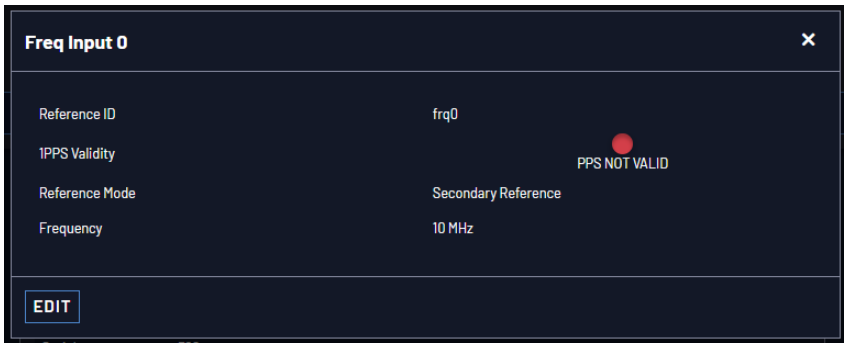
The input frequency is measured versus internal frequency and compared to the setup value. If the discrepancy is larger than 1kHz, the input is disqualified and not considered valid. The frequency reference does not inherently provide an on-time point, so it relies on the current on-time point of the system prior to its taking over for synchronization.

Frequency Input: Status Window

To view the current settings of the **Frequency Input** (also referred to as 'Reference'), go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entries for these cards are: 1PPS/Frequency BNC and 1PPS/Frequency RS-485.

The connector number is: J1 (BNC card); J1 (RS-485 card).



The Status window displays the following settings:

- **Reference ID**: Name used to represent this 1PPS input reference in the Reference Priority table; see "Configuring Input Reference Priorities" on page 219 for more information on reference priorities.
- **1PPS Validity**: Indicates “OK” (green) if the 1PPS input signal is present and valid. Indicates “Not Valid” (orange) if the 1PPS input signal is either not present or is not considered valid.
- **Reference Mode**: Displays how the reference mode operates in determining its validity.
- **Frequency**: Displays (in Hertz) the configured frequency of the input frequency signal.

The 1PPS Input signal is analyzed and an absence of the signal triggers a “Not Valid” indication.



1PPS Output: Edit Window

To configure the settings of the **1PPS output**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entries for these cards are: 1PPS/Frequency BNC and 1PPS/Frequency RS-485.

The connector number is: J3 (BNC card); J1 (RS-485 card).



The Edit window allows the configuration of the following settings:

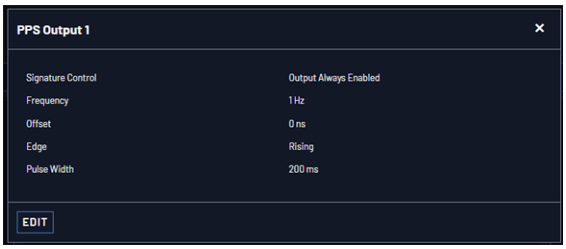
- **Signature Control**: Used to control when the 1PPS output signal will be present. See "Signature Control" on page 198 for more information.
- **Offset**: Used to account for 1PPS cable delays or other latencies in the 1PPS output. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.
- **Edge**: The operator can select if the output signal is a positive (reference on the rising edge) or a negative (reference on the falling edge) pulse.
- **Pulse Width**: Configures the Pulse Width of the 1PPS output. The Pulse Width is entered and displayed in nanoseconds (ns). The default Pulse Width is 200 milliseconds.

PPS Output: Status Window

To view the current settings of the **1PPS output**, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entries for these cards are: 1PPS/Frequency BNC and 1PPS/Frequency RS-485.

The connector number is: J3 (BNC card); J1 (RS-485 card).



The Status window displays the following settings:

- **Signature Control**: Displays the current configuration of Signature Control. See also: "Signature Control" on page 198.
- **Frequency**: Indicates the configured frequency of the 1PPS output signal.

- **Offset**: Displays the configured Offset (to account for cable delays or other latencies).
- **Edge**: Shows if the on-time point of the 1PPS output is the rising or falling edge of the pulse.
- **Pulse Width**: Displays the configured Pulse Width of the 1PPS output. The Pulse Width is displayed in nanoseconds (ns). The default Pulse Width is 200 milliseconds.

5.2.3.4 Frequency Out [1204-08, -1C, -26]

The Frequency Out option cards provide three sine wave outputs that are phase-locked to the disciplined oscillator to supply highly precise waveforms with minimal distortion.

Frequency Out [1204-08, -1C, -26]: Specifications

- **Outputs**: (3) 1MHz, (3) 5MHz, or (3) 10 MHz Outputs
- **Signal Type and Connector**:
  - (10 MHz) +13 dBm into 50 Ω, BNC, or TNC (-38)
  - (5MHz) +10 dBm into 50 Ω, BNC, or TNC (-38)
  - (1MHz) +10 dBm into 50 Ω, BNC, or TNC (-38)
- **1MHz or 5MHz Phase Noise** (with OCXO or low phase noise Rubidium oscillator):
  - -115 dBc/Hz @ 10 Hz
  - -130 dBc/Hz @ 100 Hz
  - -140 dBc/Hz @ 1kHz
- **1MHz or 5MHz Phase noise** (with Rubidium oscillator):
  - -85 dBc/Hz @ 10 Hz
  - -110 dBc/Hz @ 100 Hz
  - -130 dBC/Hz @ 1kHz
- **10 MHz Phase Noise** (with TCXO oscillator):

- -110 dBc/Hz @ 100 Hz
- -135 dBc/Hz @ 1kHz
- -140 dBc/Hz @ 10 kHz

- **10 MHz Phase Noise** (with OCXO oscillator) [Numbers in brackets represent Low Phase Noise OCXO option]:
  - -95 [-100] dBc/Hz @ 1Hz
  - -123 [-128] dBc/Hz @ 10 Hz
  - -140 [-148] dBc/Hz @ 100 Hz
  - -145 [-153] dBc/Hz @ 1kHz
  - -150 [-155] dBc/Hz @ 10 kHz
- **Harmonics**: -40 dBc minimum
- **Spurious**:
  - -60 dBc minimum (1MHz)
  - -50 dBc minimum (5MHz)
  - -70 dBc minimum (10 MHz)
- **Accuracy**: See "10 MHz Output" on page 26
- **Maximum Number of Cards**:
  - (4)
- **Ordering Information**:
  - 1204-1C: 10 MHz output (3X) Module
  - 1204-08: 5MHz output (3X) Module
  - 1204-26: 1MHz output (3X) Module

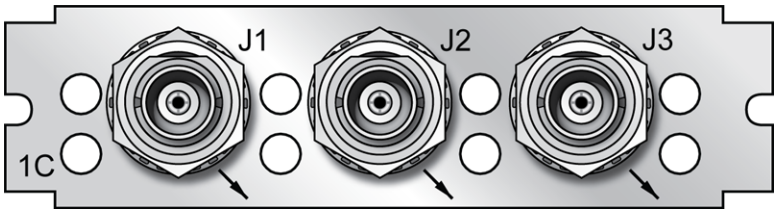


Figure 5-26: Model 1204-1C option card rear plate

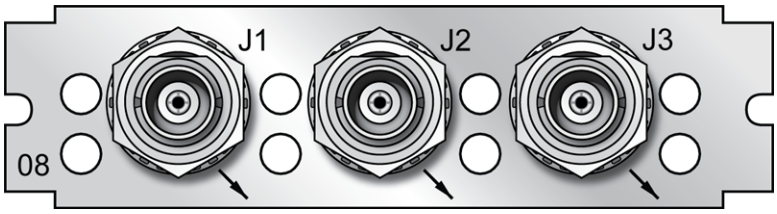


Figure 5-27: Model 1204-08 option card rear plate

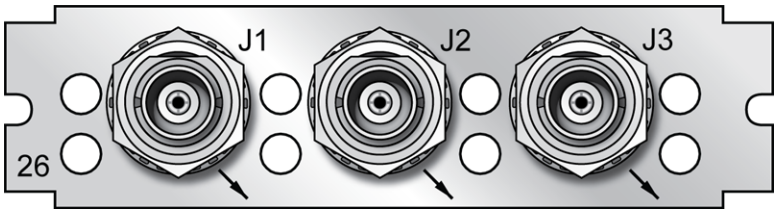


Figure 5-28: Model 1204-26 option card rear plate

The Frequency Out option cards each have 3 outputs, distributing a 1MHz signal, 5MHz or 10 MHz signal (depending on the card model). All 3 outputs are configured as a single output and will appear as such in the SecureSync Web UI, numbered sequentially by card instance, starting with 0 (except the 10 MHz option card, which starts with no.1 because of the built-in 10 MHz output.)

Frequency Output: Edit Window

To configure the settings of a **Frequency Output**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The list entry for this card is named: 1/5/10 MHz BNC (or: TNC)

The connector numbers are: J1...J3.



The Edit window allows the configuration of the following settings:

- **Signature Control**: Controls when the output will be present; see "Signature Control" on page 198.

Frequency Output: Status Window

To view the settings of a **Frequency output**, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entry for this card is named: 1/5/10 MHz BNC (or: TNC).

The connector numbers are: J1...J3.



The Status window displays the following settings:

- **Signature Control**: Controls when the output will be present. See also: "Signature Control" on page 198.
- **Frequency**: The frequency of the output: 1MHz, 5MHz or 10 MHz, depending on the card model.

For more information on monitoring installed option cards, see: "Monitoring the Status of Option Cards" on page 338.

5.2.3.5 Programmable Frequency Out [1204-13, -2F, -30]

Programmable Frequency Output option modules provide output square waves at programmable pulse rates, or sine waves at programmable frequencies. The output frequency, which is adjustable via the SecureSync Web UI, is locked to the SecureSync system-disciplined oscillator.

These option cards can be used for a variety of applications requiring programmable frequency outputs. The RS-485 model of this card can be operated as an N.8 frequency synthesizer.

Depending on your card model number, the outputs are available in different formats:

- RS-485 on a pluggable terminal block
- TTL square wave on BNC, or
- Sine wave on BNC

Each output can be phase-offset between 0-360° in 0.1°-increments.

Programmable Frequency Card 1204-13 (Sine Wave, BNC): Specifications

- **Outputs**: (4) independently programmable sine wave outputs
- **Signal Type**: +13 dBm
- **Wave Form**: sine
- **Connector**: BNC
- **Output Load Impedance**: 50 Ω
- **Output Pulse/Frequency Rates**: 1Hz to 25 MHz in 0.1-Hz increments
- **Accuracy**: Function of input synchronization source (GPS, IRIG, 1 PPS, etc.)
- **Synchronization**: Output frequency locked to SecureSync disciplined 10 MHz
- **Jitter**, cycle-to-cycle: n/a
- **Phase Noise**:
  - -120 dBc/Hz @ 1kHz offset
  - -130 dBc/Hz @ 10-kHz offset
  - -140 dBc/Hz @ 100-kHz offset
- Harmonics: <-30 dBc
- **Spurious**: <-60 dBc
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-13, Programmable Frequency Card, sine wave, BNC

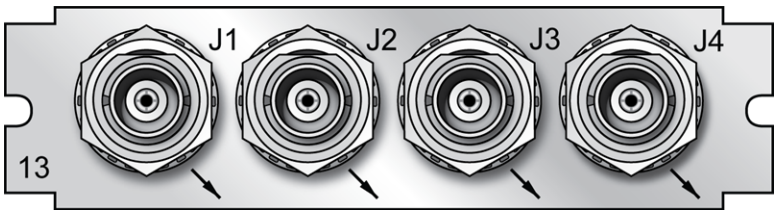


Figure 5-29: Model 1204-13 option card rear plate

Programmable Frequency Card 1204-2F (TTL, BNC): Specifications

- **Outputs**: (4) independently programmable square wave outputs
- **Signal Type**: TTL (BNC)
- **Wave Form**: square
- **Connector**: BNC
- **Output Load Impedance**: 50 Ω
- **Output Pulse/Frequency Rates**: 1PPS to 25 MPPS in 0.1-PPS increments
- **Accuracy**: Function of input synchronization source (GPS, IRIG, 1 PPS, etc.)
- **Synchronization**: Output frequency locked to SecureSync disciplined 10 MHz
- **Jitter**, cycle-to-cycle: <10 ns
- **Phase Noise**: n/a
- **Harmonics**: n/a
- **Spurious**: n/a
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204—2F, Programmable Frequency Card, TTL, BNC

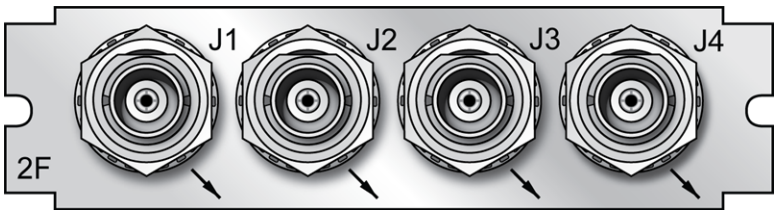


Figure 5-30: Model 1204-2F option card rear plate

Progr. Frequ. Card 1204-30 (TTL, RS-485): Specifications

- **Outputs**: (4) independently programmable square wave outputs
- **Signal Type**: RS-485
- **Wave Form**: square
- **Connector**: Terminal block
- **Output Load Impedance**: n/a

- **Output Pulse/Frequency Rates**: 1PPS to 25 MPPS in 0.1-PPS increments
- **Accuracy**: Function of input synchronization source (GPS, IRIG, 1 PPS, etc.)
- **Synchronization**: Output frequency locked to SecureSync disciplined 10 MHz
- **Jitter**, cycle-to-cycle: <10 ns
- **Phase Noise**: n/a
- **Harmonics**: n/a
- **Spurious**: n/a
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204—30, Programmable Frequency Card, TTL, RS-485

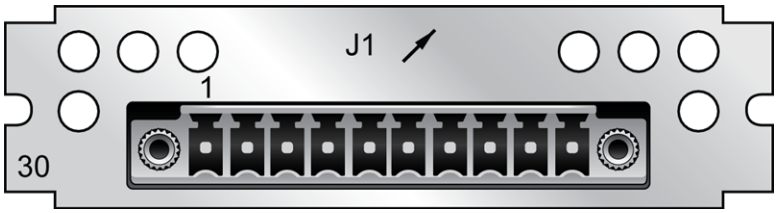


Figure 5-31: Model 1204-30 option card rear plate

Table 5-7: Model 1204-30 terminal block pin assignments

Pin No.	Function
1	Frequ. Output 1 +
2	Frequ. Output 1 –
3	GND
4	Frequ. Output 2 +
5	Frequ. Output 2 –
6	Frequ. Output 3 +
7	Frequ. Output 3 –
8	GND
9	Frequ. Output 4 +
10	Frequ. Output 4 –

Programmable Frequency Output: Edit Window

To configure a **Programmable Frequency Output**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entry for this card is: Prog Freq Out, Sine [or: TTL, or: RS-485, respectively].

The connector numbers are: J1...J4 [J1 for the RS-485 model].



The Edit window allows the configuration of the following settings:

- **Signature Control**: Controls when the output will be present. See also: "Signature Control" on page 198.
- **Frequency**: Enter the desired output frequency. The ranges are as follows:
  - Sine wave output frequency (model no. 1204-13): 1 to 25,000,000 Hz
  - Pulse rate output in Hertz (model no.'s 1204-2F/-30): 1 to 25,000,000 PPS
- **Phase**: Adjust the phase by entering a phase offset (0.1 to 360°), if required.

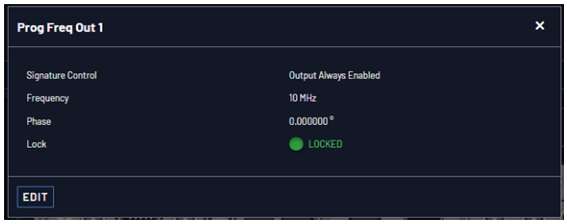
> **Note:** The phase offset will lose its reference at a SecureSync reboot, and hence the value will be reset to 0 (ZERO).
>
> The reference will also be lost if you enter a new output frequency for a port – however in this case, the value will not be reset to 0, but instead remain unchanged. In both cases you will need to re-enter the required phase offset value.

Programmable Frequency Output: Status Window

To view the settings of a **Programmable Frequency Output**, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entry for this card is named: Prog Freq Out, Sine [or: TTL, or: RS-485, respectively].

The connector numbers are: J1...J4 [J1 for the RS-485 model].



The Status window displays the following settings:

- **Signature Control**: Controls when the output will be present. See also: "Signature Control" on page 198.
- **Frequency**: Indicates the configured frequency.
- **Phase**: Displays the configured phase offset (e.g., to account for delays caused by different cable lengths, or other latencies).
- **Lock**: Shows, if the output frequency is locked to the SecureSync system-disciplined oscillator.

Note: Even if an output frequency status is LOCKED, it will not be available at the output port, if the Signature Control for that port has been DISABLED.

5.2.3.6 Programmable Square Wave Out [1204-17]

The Model 1204-17 Square Wave output Option Card provides four programmable square wave outputs for the SecureSync platform.

- **Inputs/Outputs**: (4) Programmable square wave outputs
- **Signal Type and Connector**: TTL (BNC)
- **Accuracy**: ±50 ns (1σ)
- **Output Load Impedance**: 50 Ω
- **Rise Time to 90% of Level**: <10 ns

- **Programmable Period**: 100 ns to 2,000,000,000 ns in 5ns steps, or to 1,800,000,000 µs in 1µs steps
- **Programmable Pulse Width**: 20 ns to 900 ms with 5 ns resolution
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-17: Square Wave Out

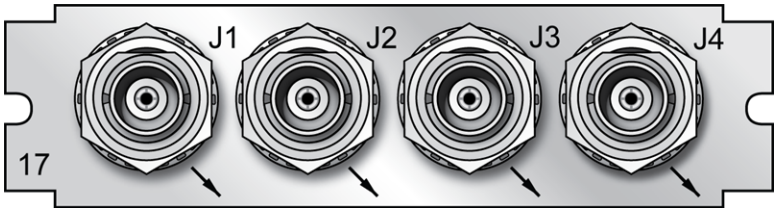


Figure 5-32: Model 1204-17 option card rear plate

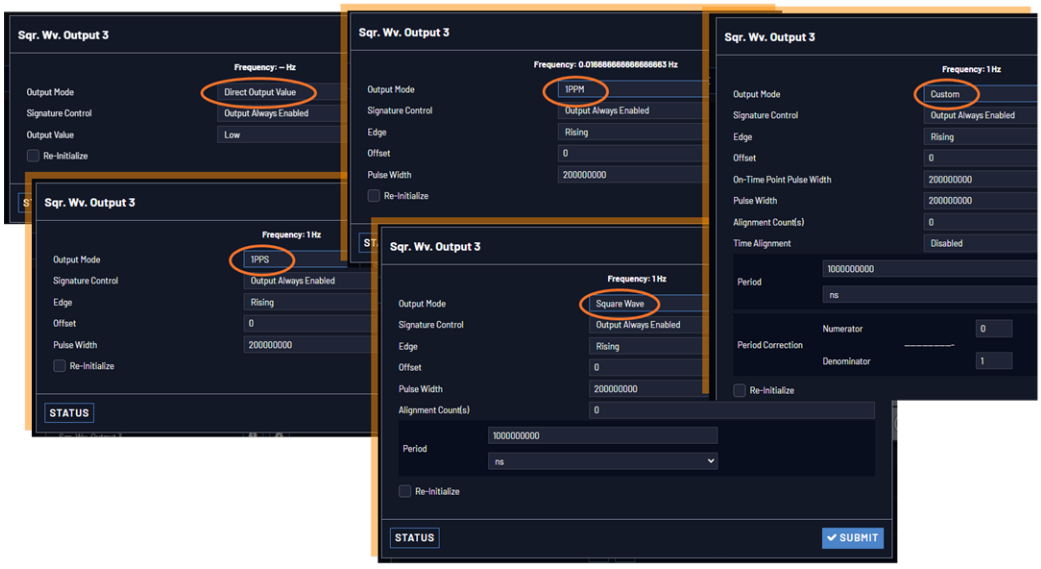
Configuring a Square Wave Output

To configure one of the **Square Wave Outputs**:

1. Navigate **INTERFACES >OUTPUTS: Square Wave Output**. The panel on the right side of the screen displays all **Sqr. Wv. Outputs** and their statuses. All outputs are numbered by signal type (e.g., 'pulse'), hence the numbering may not start with 0.
   - To determine which output number is allocated to which connector (J1–J4), hover your mouse pointer over the **back panel image**.
   - Click on the INFO button next to one of the outputs to open a detailed **Status** panel (the displayed settings are described below.)



2. Click on the GEAR button to open the **Edit** window.



The **Edit** window allows the configuration of the following settings:

> **Note:** The fields viewable are contextually determined according to the Output Mode.

- **Output Mode**:
  - Direct Output Value
  - 1PPS
  - 1PPM
  - 5MPPS/1PPS
  - Square Wave
  - Custom
- **Output Value**: Determines the output level (Low or High).
- **Re-Initialize**: Re-initializes square wave generation and aligns to 1PPS.
- **Signature Control**: Controls when the output will be present. See also: "Signature Control" on page 198.

- **Edge**: Used to determine if the on-time point of the output is the **Rising** or **Falling** edge of the signal.
- **Offset**: Accounts for cable delays and other latencies [nanoseconds].
- **On-Time Point Pulse Width**: The on-time point pulse width is the pulse width of the first square wave pulse aligned to the 1PPS On-Time Point. This is only active when the alignment count is non-zero [nanoseconds].
- **Pulse Width**: Pulse width of the output [nanoseconds].
- **Alignment Count(s)**: The alignment counter determines how often (in seconds) the square wave will be aligned back to the 1PPS. Setting zero will disable PPS alignment beyond the initial alignment.
- **Time Alignment**: (Enabled/Disabled) The time alignment enable changes the function of the alignment counter to align the square wave whenever the current time's seconds value is a multiple of the alignment count. For example: If time alignment is enabled and alignment count is set to 15 seconds, the square wave will be aligned to the 1PPS when the seconds value on the time display equals 00, 15, 30, 45. The current Time Alignment range is from 0 to 3600 seconds.
- **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.
- **Period Correction**: Period correction allows for the generation of more precise frequencies at the expense of additional period jitter. Over a length of time, the true square wave period comes to:
  - Period + [(numerator/denominator) * 5 ns]

5.2.3.7 Simulcast (CTCSS/Data Clock) [1204-14]

The Simulcast CTCSS/Data Sync/Data Clock Option Card provides CTCSS, data clock, and alarm outputs through relays for the SecureSync platform through one DB-9 and one RJ-12 connector. The maximum number of cards installed is six (6).

a. **Connector**: DB-9
   - **Outputs**:
     - (3) RS-485 Outputs (Data Clocks, CTCSS frequencies, 1PPS)
     - (1) Alarm
   - **Voltage**:
     - Alarms: GND normally, high impedance when Alarm

b. **Connector**: RJ-12
   - **Outputs**:
     - (1) RS-485 Outputs (Data Clocks, CTCSS frequencies, 1PPS)
     - (2) Alarm
   - **Voltage**:
     - Alarms: 5V pulled up through 10 kΩ normally, GND when Alarm

- **Note:** By factory default, all CTCSS outputs are DISABLED.

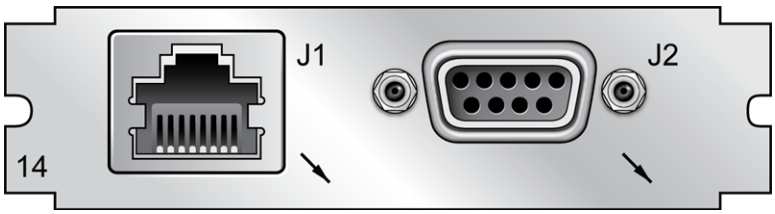


Figure 5-33: Model 1204-14 option card rear plate

Pin Assignment: DB-9 Connector

Outputs: Alarm0, CTC0 Out, CTC1 Out, CTC2 Out (with only one Simulcast option card installed)

Note: Alarm Output 0 through Alarm Output 3 are reserved by SecureSync. In the Web UI, numbering for alarm outputs for this option card will begin at Alarm 4, which is available on the DB-9 output, while Alarms 5 and 6 are assigned to the RJ-12 connector.

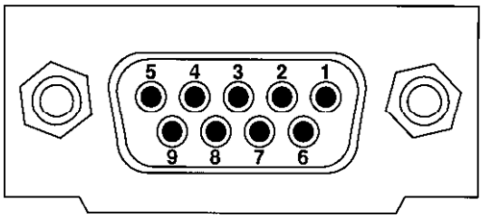


Figure 5-34: DB-9 connector pin-out

Table 5-8: DB-9 pin-out

PIN	NOTES	SIGNAL	819x Mapping	819x Option17 Mapping
1	RS-485 + Terminal	Output 0+	+9.6 kHz	+CTCSS #1
2	RS-485 + Terminal	Output 1+	+18 kHz	+18 kHz
3	RS-485 + Terminal	Output 2+	+1 PPS	+CTCSS #2
4	Ground = Normal OPEN = ALARM	Major Alarm	Major Alarm	Major Alarm
5	Cable Shield	Ground	Ground	Ground
6	RS-485 – Terminal	Output 0 –	–9.6 kHz	– CTCSS #1
7	RS-485 – Terminal	Output 1 –	–18 kHz	– 18 kHz
8	RS-485 – Terminal	Output 2 –	–1PPS	– CTCSS #2
9	Cable Shield	GROUND	GROUND	GROUND

Pin Assignment: RJ-12 Connector

Outputs: Alarm1, Alarm2, CTC3 Out, (with only one Simulcast option card installed)

Note: Alarm Output 0 through Alarm Output 3 are reserved by SecureSync. In the Web UI, numbering for alarm outputs for this option card will begin at Alarm 4, which is available on the DB-9 output, while Alarms 5 and 6 are assigned to the RJ-12 connector.

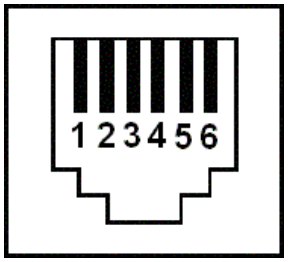


Figure 5-35: RJ-12 connector pin-out

Table 5-9: RJ-12 pin assignments

PIN	NOTES	SIGNAL	938x SP360 Mapping
1	Cable Shield	GROUND	GROUND
2	5V = NORMAL GROUND = ALARM	MAJOR ALARM RELAY	MAJOR ALARM RELAY
3	RS-485 + Terminal	Output 3+	+ 1PPS
4	RS-485 - Terminal	Output 3-	- 1PPS
5	5V = NORMAL GROUND = ALARM	MINOR ALARM RELAY	MINOR ALARM RELAY
6	Cable Shield	GROUND	GROUND

CTCSS and Alarm Outputs: Viewing Signal States

To quickly view the current signal state of the 1204-14 **Simulcast outputs**, in the Web UI navigate to the option card's Status Summary panel. For instructions, see: "Viewing an Input/Output Signal State" on page 387.



All outputs are listed, displaying their current output states. For a listing of the states, see "CTCSS Outputs: Edit Window" below, and "Alarm Outputs: Edit Window" on page 444.

To view the settings of *one* of the **Alarm Outputs** or **CTCSS Outputs**, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entry for this card is named: **Simulcast**.

Note: Alarm Output 0 through Alarm Output 3 are reserved by SecureSync. Numbering for alarm outputs from the option card will begin at Alarm 4, which is available on the DB-9 output, while Alarms 5 and 6 are assigned to the RJ-12 connector.

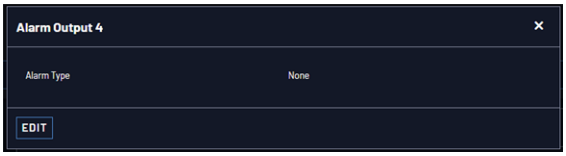
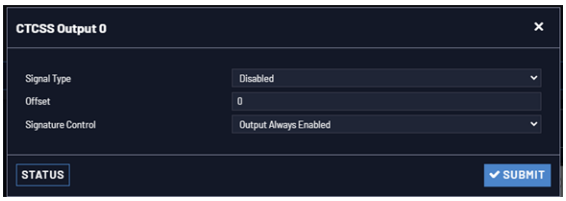


Figure 5-36: Simulcast Alarm Output Status window

CTCSS Outputs: Edit Window

To configure a **CTCSS output**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entry for this card is named: **Simulcast**.



The Edit window allows the configuration of the following settings:

- **Signal Type**: Allows selection of the desired signal type. Available options include:
  - Disabled
  - CTCSS 1/3 Tones
  - CTCSS 1/10 Tones
  - Data Clocks
  - 1PPS
- **Signal Output**:
  - CTCSS 1/3 Tones (see also: "CTCSS exact (1/3 Hz) tones" on page 445)
  - CTCSS 1/10 Tones (see also: "CTCSS exact (1/10 Hz) tones" on page 446)
  - Data Clocks (see also: "Data Clock Signals" on page 446)
  - 1PPS (see also: "1PPS Duty Cycle" on page 446)
- **Offset**: Value in nanoseconds that can be used to adjust for cable delays or latencies.
- **Signature Control**: Controls when the output will be present. For more information, see "Signature Control" on page 198.

819x Option 17 Mapping

To replicate settings used in Series 819x devices, use the following information to configure option card no. 1204-14 for compatible CTCSS operation:

- **DB-9 Output Index 0**: Set to desired CTCSS 1/10 or CTCSS 1/3 tone
- **DB-9 Output Index 1**: Set to 18 kHz Data Clock
- **DB-9 Output Index 2**: Set to desired CTCSS 1/10 or CTCSS 1/3 tone.

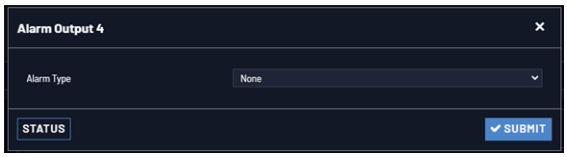
Alarm Outputs: Edit Window

To configure one of the **ALARM Outputs**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entry for this card is named: **Simulcast**.

Note: Alarm Output 0 through Alarm Output 3 are reserved by SecureSync. Numbering for alarm outputs from the option card will begin at Alarm 4, which is available on the DB-9 output, while Alarms 5 and 6 are assigned to the RJ-12 connector.

Note: You can configure the alarm type (None, Minor, or Major) for both the DB-9 and RJ-12 connectors. For additional information on alarm types, see "Minor and Major Alarms" on page 374.



The Edit window allows the configuration of the following settings:

- **Alarm Type**:
  - None—Will not output for an alarm
  - Minor—Will output on a minor alarm
  - Major—Will output on a major alarm.

CTCSS Encoding Tables, Signal Data

Table 5-10: CTCSS exact (1/3 Hz) tones

Code	Tone Freq.	Code	Tone Freq.	Code	Tone Freq.
		1A	103.666	6A	173.666
		1B	107.333	6B	180.000
XZ	67.000	2Z	111.000	7Z	186.333
WZ	69.333	2A	115.000	7A	193.000
XA	72.000	2B	119.000	M1	203.666
WA	74.333	3Z	123.000	8Z	206.666
XB	77.000	3A	127.333	M2	210.666
WB	79.666	3B	132.000	M3	218.333
YZ	82.666	4Z	136.666	M4	225.666
YA	85.333	4A	141.333	9Z	229.000
YB	88.666	4B	146.333	M5	233.666
ZZ	91.666	5Z	151.333	M6	242.000
ZA	95.000	5A	156.666	M7	250.333
ZB	97.333	5B	162.333	0Z	254.000
1Z	100.000	6Z	168.000		

Table 5-11: CTCSS exact (1/10 Hz) tones

Code	Tone Freq.	Code	Tone Freq.	Code	Tone Freq.
XZ	67.0	1B	107.2	6A	173.8
WZ	69.3	2Z	110.9	6B	179.9
XA	71.9	2A	114.8	7Z	186.2
WA	74.4	2B	118.8	7A	192.8
XB	77.0	3Z	123.0	M1	203.5
WB	79.7	3A	127.3	8Z	206.5
YZ	82.5	3B	131.8	M2	210.7
YA	85.4	4Z	136.5	M3	218.1
YB	88.5	4A	141.3	M4	225.7
ZZ	91.5	4B	146.2	9Z	229.1
ZA	94.8	5Z	151.4	M5	233.6
ZB	97.4	5A	156.7	M6	241.8
1Z	100.0	5B	162.2	M7	250.3
1A	103.5	6Z	167.9	0Z	254.1

Table 5-12: Data Clock Signals

Output	Duty Cycle
9.6 kHz, 18.0 kHz, 64.0 kHz	50% ±2%
17 2/3 Hz	888 µs pulse width
26 2/3 Hz	25% low, 75% high
33 1/3 Hz	208 µs pulse width

Table 5-13: 1PPS Duty Cycle

Output	Duty Cycle
1PPS	20% ±5%

5.2.4 Telecom Option Cards

This section contains technical information and Web UI procedures relevant to SecureSync option cards commonly used in the telecommunications industry.

5.2.4.1 T1/E1 Out [1204-09, -0A, -4C, -53]

The 1204-09 and 1204-0A E1/T1 option card provide 1.544 MHz or 2.048 MHz and E1 or T1 data outputs for the SecureSync platform. The 1204-4C and 1204-53 E1/T1 option cards each provide (4) E1 or T1 data outputs (but do not include a clock output).

SecureSync meets G.812 Type I when installed with a Rubidium option, and G.811 when installed with a Rubidium option and synchronized with GNSS.



Note: Rubidium oscillators are recommended for the E1/T1 option cards.

Model 1204-09 E1/T1 (75 Ω): Specifications

- **Outputs**:
  - (1) 1.544/2.048 MHz Output
  - (2) Unbalanced E1/T1 Outputs
- **T1 mode**:
  - 1.544 MHz (square wave) frequency output
  - (2) 1.544 Mb/sec data rate outputs:
    - Outputs are DS1 framed all ones
    - Supports Super Frame (SF or D4) and Extended Super Frame (ESF)
    - SSM support

- **E1 mode**:
  - 2.048 MHz (square wave) frequency output
  - (2) 2.048 Mb/sec data rate outputs:
    - Outputs are E1 frame all ones
    - Supports CRC4 and CAS Multiframe
    - SSM support
- **Connector and Signal Type**: BNC
  - 1.544/2.048 MHz TTL into 50 Ω
  - T1 according to GR-499-CORE (75 Ω)
  - E1 according to ITU-T G703 (75 Ω)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-09: T1/E1 (75 Ω) module

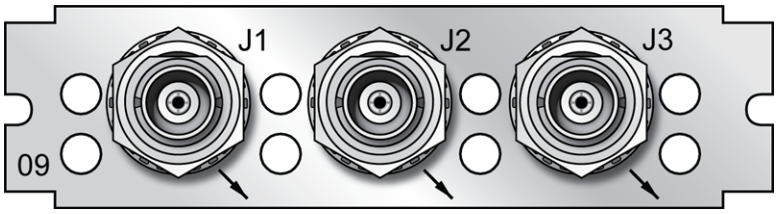


Figure 5-37: Model 1204-09 option card rear plate

Model 1204-0A E1/T1 (100/120 Ω): Specifications

- **Outputs**:
  - (1) 1.544/2.048 MHz RS-485 Outputs
  - (2) Balanced E1/T1Outputs
- **T1 mode**:
  - 1.544 MHz (square wave) frequency output
  - (2) 1.544 Mb/sec data rate outputs:
    - Outputs are DS1 framed all ones
    - Supports Super Frame (SF or D4) and Extended Super Frame

(ESF)
    - SSM support
- **E1 mode**:
    - 2.048 MHz (square wave) frequency output
    - (2) 2.048 Mb/sec data rate outputs:
        - Outputs are E1 frame all ones
        - Supports CRC4 and CAS Multiframe
        - SSM support
- **Connector and Signal Type**: Terminal block
    - 1.544/2.048 MHz RS-485
    - T1 according to GR-499-CORE (100 Ω)
    - E1 according to ITU-T G703 (120 Ω)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-0A: T1/E1 (100/120 Ω) module

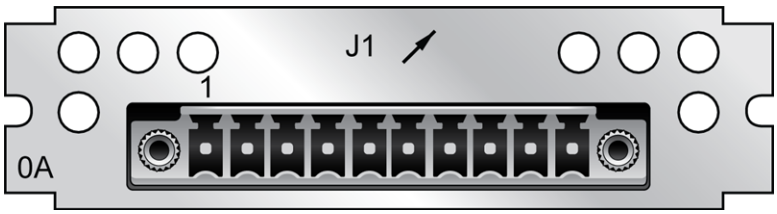


Figure 5-38: Model 1204-0A option card rear plate

Table 5-14: 1204-0A option card pin assignments

Pin Assignments			
Pin No.	Signal	Function	Description
1	GND	Ground	Ground
2	1.544MHz/2.048MHz	RS-485 A Terminal	Square wave
3	1.544MHz/2.048MHz	RS-485 B Terminal	Square wave
4	GND	Ground	Ground

Pin Assignments			
Pin No.	Signal	Function	Description
5	T1/E1 output A1	GR-499/G.703	Tip
6	T1/E1 output B1	GR-499/G.703	Ring
7	GND	Ground	Ground
8	T1/E1 output A2	GR-499/G.703	Tip
9	T1/E1 output B2	GR-499/G.703	Ring
10	GND	Ground	Ground

Model 1204-53 E1/T1 (75 Ω): Specifications

- **Outputs**:
  - (4) Unbalanced E1 or T1 Outputs
- **T1 mode**:
  - (4) 1.544 Mb/sec data rate outputs:
    - Outputs are DS1 framed all ones
    - Supports Super Frame (SF or D4) and Extended Super Frame (ESF)
    - SSM support
- **E1 mode**:
  - (4) 2.048 Mb/sec data rate outputs:
    - Outputs are E1 frame all ones
    - Supports CRC4 and CAS Multiframe
    - SSM support
- **Connector and Signal Type**: BNC
  - T1 according to GR-499-CORE (75 Ω)
  - E1 according to ITU-T G703 (75 Ω)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-53: T1/E1 (75 Ω) module

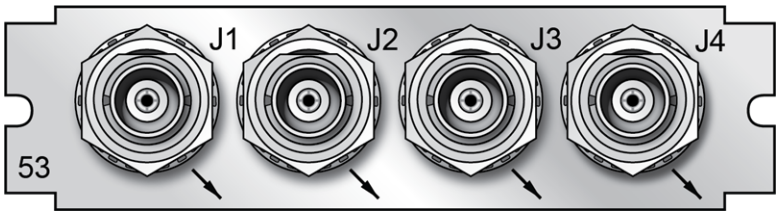


Figure 5-39: Model 1204-53 option card rear plate

Model 1204-4C E1/T1 (100/120 Ω): Specifications

- **Outputs**:
  - (4) Balanced E1 or T1 Outputs
- **T1 mode**:
  - (4) 1.544 Mb/sec data rate outputs:
    - Outputs are DS1 framed all ones
    - Supports Super Frame (SF or D4) and Extended Super Frame (ESF)
    - SSM support
- **E1 mode**:
  - (4) 2.048 Mb/sec data rate outputs:
    - Outputs are E1 frame all ones
    - Supports CRC4 and CAS Multiframe
    - SSM support
- **Connector and Signal Type**: Terminal block
  - T1 according to GR-499-CORE (100 Ω)
  - E1 according to ITU-T G703 (120 Ω)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-4C: T1/E1 (100/120 Ω) module

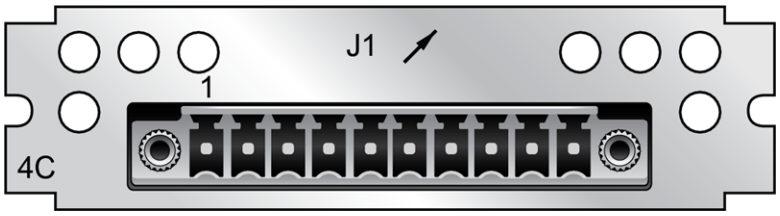


Figure 5-40: Model 1204-4C option card rear plate

Table 5-15: 1204-4C option card pin assignments

Pin Assignments			
Pin No.	Signal	Function	Description
1	GND	Ground	Ground
2	T1/E1 output A1	GR-499/G.703	Tip
3	T1/E1 output B1	GR-499/G.703	Ring
4	T1/E1 output A2	GR-499/G.703	Tip
5	T1/E1 output B2	GR-499/G.703	Ring
6	T1/E1 output A3	GR-499/G.703	Tip
7	T1/E1 output B3	GR-499/G.703	Ring
8	T1/E1 output A4	GR-499/G.703	Tip
9	T1/E1 output B4	GR-499/G.703	Ring
10	GND	Ground	Ground

E1/T1 Output: Edit Window

To configure an E1/T1 **data output** (1.544/2.048 MHz clock on J1 BNC connector and unbalanced E1/T1 outputs on J2 to J3 BNC connectors, or all terminal block J1 outputs), navigate to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

In the Web UI this card is listed under: **E1/T1 Out BNC** and **E1/T1 OUT Terminal**.



The Edit window allows the configuration of the following settings (visible fields will change depending on selections in this window):

- **Signature Control**: Controls when the output will be present. For more information, see "Signature Control" on page 198.
- **Mode**: This option selects T1, E1, or disabled mode. For T1 mode, the clock output (on the -09 and -0A cards) will be 1.544 MHz, and for E1 the clock output will be 2.048 MHz.
- **SSM Enabled**: Enables or disables Sync Status Messaging (SSM). T1 SSM is not valid with D4/Superframe or AIS framing. E1 SSM is not valid with AIS framing.
- **E1 Encode**: HDB3 only.
- **E1 Framing**: This option selects the framing standard (CRC-4, No CRC-4, or AIS).
- **T1 Framing**: This option selects the framing standard (D4/Superframe, Extended Superframe [CRC-6/no CR C-6], or AIS).
- **T1 Encoding**: This option selects the encoding method (B8ZS or AMI).
- **T1SSM Value**: This option selects the SSM quality level transmitted when SSM is enabled.
- **E1 SSM Value**: This option selects the SSM quality level transmitted when SSM is enabled.

E1/T1 Output: Status Window

To view the configuration settings of the **E1 OUT** or **T1 OUT** output, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entries for these cards are: **E1/T1 Out BNC** and **E1/T1 OUT Terminal**.



The E1/T1 Output 0 Status Screen will vary according to whether the output signal mode is E1 or T1.

The Status windows display the following settings:

- **Signature Control**: Controls when the output will be present; see "Signature Control" on page 198.
- **Mode**: This option selects T1, E1, or disabled mode. For T1 mode, the clock output (on the -09 and -0A cards) will be 1.544 MHz, and for E1 the clock output will be 2.048 MHz.
- **SSM Enabled**: Enables or disables Sync Status Messaging (SSM). T1 SSM is not valid with D4/Superframe or AIS framing. E1 SSM is not valid with AIS framing.
- **E1 Encoding**: HDB3 only.
- **E1 Framing**: This option selects the framing standard (CRC-4, No CRC-4, or AIS).
- **T1 Framing**: This option selects the framing standard (D4/Superframe, Extended Superframe [CRC-6/no CR C-6], or AIS).
- **T1 Encoding**: This option selects the encoding method (B8ZS or AMI).
- **T1 SSM Value**: This option selects the SSM quality level transmitted when SSM is enabled.
- **E1 SSM Value**: This option selects the SSM quality level transmitted when SSM is enabled.

5.2.5 Time Code Option Cards

This section contains technical information and SecureSync Web UI procedures for option cards designed to deliver timing data in time code formats, e.g. IRIG, HAVE QUICK, or STANAG.

5.2.5.1 IRIG Out [1204-15, -1E, -22]

These IRIG Output option cards provide SecureSync with four IRIG outputs. Available with BNC connectors, Fiber Optic ST connectors, or RS-485 terminal block.

IRIG Out (BNC): Specifications

- **Inputs/Outputs**: (4) IRIG Outputs
- **Output Signal**: IRIG A, B, E, G, or NASA-36, amplitude modulated sine wave (AM), 0.5V to 6V_{p-p} into 50 Ω; or pulse-width-coded (DCLS).User-selectable.
- **AM Carrier**: IRIG B 1000 Hz, IRIG A and G 100 or 100
- **AM Signal Level**: 500 mV to 10 V_{p-p} [high Z]; (modulated 2:1 to 6:1).
- **DCLS Signal Level**: >10 kΩ TTL
- **Connector**: AM and DCLS: BNC female
- **Accuracy**: see "IRIG Output Accuracy Specifications" on page 636
- **Number of Cards**: Up to 6
- **Ordering Information**: 1204-15, IRIG module, BNC Connector

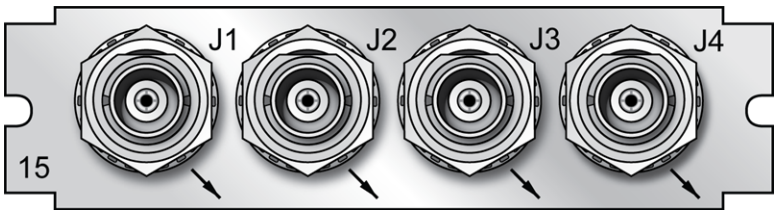


Figure 5-41: Model 1204-15 option card rear plate

IRIG Out (Fiber Optic): Specifications

- **Inputs/Outputs**: (4) IRIG Outputs
- **Signal**: IRIG A, B, E, G or NASA-36
- **Operating Wavelength**: 820/850 nm
- **Optical Power**: -15 dBm average into 50/125 fiber
- **Fiber Optic Compatibility**: 50/125 µm, 62.5/125 µm multi-mode cable
- **Optical Connector**: ST

- **Signal Type**: DC Level Shift (unmodulated)
- **Accuracy**: see "IRIG Output Accuracy Specifications" on page 636
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-1E Four IRIG Output Module, Fiber Optic

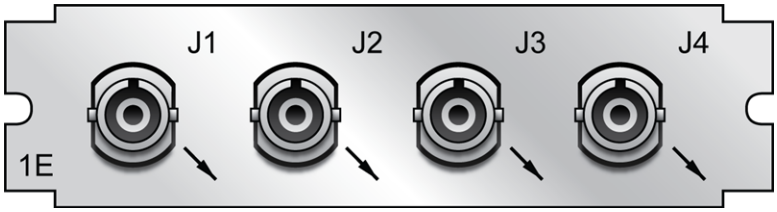


Figure 5-42: Model 1204-1E option card rear plate

IRIG Out (RS-485): Specifications

- **Inputs/Outputs**: (4) IRIG Outputs
- **Signal**: IRIG A, B, E, G or NASA-36
- **Signal Type and Connector**: RS-485 levels (terminal block)
- **Output Load Impedance**: 120 Ω
- **Accuracy**: see "IRIG Output Accuracy Specifications" on page 636
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-22 Four IRIG Output Module, RS-485

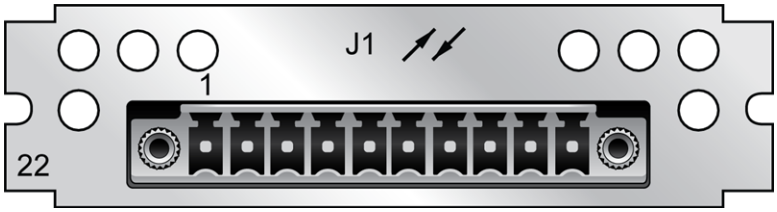


Figure 5-43: Model 1204-22 option card rear plate

Pin Assignments

J1 Pin No.	Function
1	IRIG Output 1 +

J1 Pin No.	Function
2	IRIG Output 1 –
3	GND
4	IRIG Output 2 +
5	IRIG Output 2 –
6	IRIG Output 3 +
7	IRIG Output 3 –
8	GND
9	IRIG Output 4 +
10	IRIG Output 4 –

Table 5-16: 1204-22 terminal block pin-out

IRIG Output: Viewing Signal State

To quickly view if an IRIG output is enabled or disabled, go to the option card's Status Summary panel. For instructions, see: "Viewing an Input/Output Signal State" on page 387.

IRIG Output: Edit Window

To configure an **IRIG Output**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entries for these option cards are: **IRIG Out BNC, IRIG Out Fiber, IRIG Out RS-485**.



The Edit window allows the configuration of the following settings:

- **Signature Control**: Used to control when the IRIG modulation will be present. This function allows the modulation to stop under certain conditions; see also "Signature Control" on page 198.
- **Format**: Used to configure the desired IRIG output formatting. The available choices are:
  - IRIG A
  - IRIG B
  - IRIG G
  - IRIG E
  - NASA-36
- **Modulation**: Changes the type of output signal modulation. The available choices are:
  - IRIG DCLS: TTL-modulated output
  - IRIG AM: Amplitude-modulated output. The amplitude of the output is determined by the value entered in the **Amplitude** field.
- **Frequency**: The IRIG modulation frequency. This is determined by the configuration of Format and Modulation Type. See "IRIG Carrier Frequencies" on page 620 for details.
- **Coded Expression**: Defines the data structure of the IRIG signal, where:
  - BCD = Binary Coded Decimal
  - TOY = Time of Year
  - CF = Control Field
  - SBS = Straight Binary Seconds



Note: The available options will vary according to the values of Format and Modulation Type.

- **Control Function Field**: IRIG signals have an optional section in the data stream that can be used to include additional information (such as the present year, for example). This field allows the Control Field section of the IRIG output to be defined. The available configurations are:

- Fields conform to **RCC 200-04**: IRIG spec 200-04 specified a location for year value, if included in this field.
- Fields conform to **IEEC 37.118-2005** (IEEE 1344): Control Field contains year, leap second and daylight savings time information.
- Fields conform to **Spectracom Format**: Year is included in Control Field but not in the same location as RCC-2004 output (year is offset by one position).
- Fields conform to **Spectracom FAA Format**: A unique IRIG output Control Field that contains satellite lock status and time error flags.
- Fields conform to **NASA Formats**: Variants of IRIG B
- Fields confirm to **Spectracom IEEE C37.118-2005**: Has been extended to support one-month leap second notification



Note: The available options will vary according to the configurations of Format and Modulation Type.

- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International
  - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of 20-November-2025, this is 18 seconds ahead of UTC)
  - A **local clock** set up through the Time Management Page: This option will appear under the name of the local clock you have set up. See for more information. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.
- **Amplitude**: The peak-to-peak output voltage level into a 600 Ω load is adjusted by entering a digital control value in this field. The level adjustment has no effect on TTL outputs, only on AM formats. The value of 128 will cause the Mark amplitude to be about $5V_{p-p}$ into high impedance. A

value of 200 results in an output amplitude of about 9V_{p-p} into high impedance.

Note: These are nominal values only. Actual values will vary from unit to unit. To adjust the level precisely, connect an oscilloscope to the output connector when adjusting.

» **Offset**: Provides the ability to account for IRIG cable delays or other latencies in the IRIG input. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.

For IRIG frequency and output specifications, see "IRIG Standards and Specifications" on page 619.

For information on IRIG output resolution, see "About the IRIG Output Resolution" on page 619.

IRIG Output: Status Window

To view the specifications of an **IRIG Output**, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entries for these option cards are: **IRIG Out BNC, IRIG Out Fiber, IRIG Out RS-485**.



Descriptions of the settings shown in the Status window can be found "IRIG Output: Edit Window" on page 457. For IRIG frequency and output specifications, see "IRIG Standards and Specifications" on page 619.

5.2.5.2 IRIG In/Out [1204-05, -27]

The IRIG Input/Output option card provides SecureSync with one IRIG input and two IRIG outputs. The IRIG input can be used as the primary SecureSync time and 1PPS reference input for synchronization. Or, it can also be used in conjunction with other primary references (such as GNSS and NTP) to synchronize SecureSync. Available with BNC or Fiber Optic ST connectors.

IRIG In/Out, BNC [1204-05]: Input Specifications

- **Input Signal**: IRIG A, B, G or NASA-36;
  amplitude modulated sine wave (AM) OR pulse-width-coded (DCLS); user-selectable, with automatic switching of load on input
- **AM Carrier**: IRIG B 1000 Hz, IRIG A 10 kHz and G 100 kHz
- **AM Signal Level**: 500 mV to 10 V_{p-p} (modulated 2:1 to 6:1); 50 Ω load
- **DCLS Signal Level**: TTL; 0.8V max., 2.3V min fail.; >10 kΩ load
- **Connector**: AM and DCLS: BNC female
- **Accuracy**: n/a
- **Number of Cards**: Up to 6
- **Ordering Information**: 1204-05, IRIG module, BNC Connector

IRIG In/Out, BNC [1204-05]: Output Specifications

- **Output Signal**: IRIG A, B, G, E, or NASA-36, amplitude modulated sine wave (AM), 0.5V to 6V_{p-p} into 50 Ω; or pulse-width-coded (DCLS). User-selectable.
- **AM Carrier**: IRIG B 1000 Hz, IRIG A 10 kHz, and G 100 kHz
- **AM Signal Level**: 500 mV to 10 V_{p-p} [high Z]; (modulated 2:1 to 6:1).
- **DCLS Signal Level**: 50 Ω TTL
- **Connector**: AM and DCLS: BNC female
- **Accuracy**: see "IRIG Output Accuracy Specifications" on page 636
- **Number of Cards**: Up to 6
- **Ordering Information**: 1204-05, IRIG module, BNC Connector

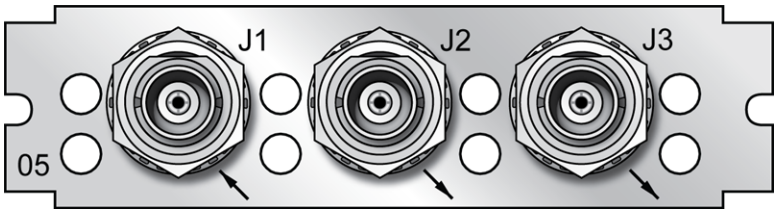


Figure 5-44: Model 1204-05 option card rear plate

IRIG In/Out, Fiber Opt. [1204-27]: Input Specifications

- **Signal**: IRIG A, B, G or NASA-36, (DCLS only, unmodulated)
- **Operating Wavelength**: 820/850 nm
- **Optical Minimum Sensitivity**: -25 dBm @ 820 nm
- **Fiber Optic Compatibility**: 50/125 µm, 62.5/125 µm multi-mode cable
- **Optical Connector**: ST
- **Accuracy**: n/a
- **Number of Cards**: Up to 6
- **Ordering Information**: 1204-27, IRIG module, Fiber Optic ST Connector

IRIG In/Out, Fiber Opt. [1204-27]: Output Specifications

- **Signal**: IRIG A, B, E, G or NASA-36, (DCLS only, unmodulated)
- **Operating Wavelength**: 820/850 nm
- **Optical Power**: -15 dBm average into 50/125 fiber
- **Fiber Optic Compatibility**: 50/125 µm, 62.5/125 µm multi-mode cable
- **Optical Connector**: ST
- **Accuracy**: see "IRIG Output Accuracy Specifications" on page 636
- **Number of Cards**: Up to 6
- **Ordering Information**: 1204-27, IRIG module, Fiber Optic ST Connector

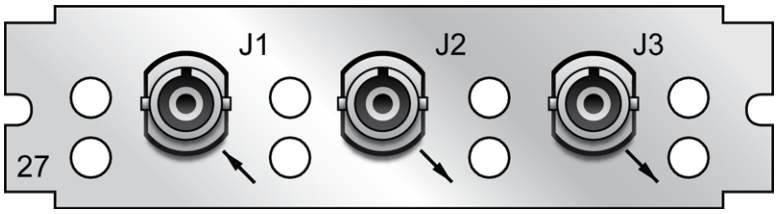


Figure 5-45: Model 1204-27 option card rear plate

Supported IRIG Formats

The IRIG option cards models 1204-05 and -27 support IRIG input and output formats A, B, and G (DCLS). IRIG-E is also available as an output, and the 1204-05 card supports A, B, E, G, and AM formats (see the following tables). Additionally, the cards support inputs with frequency/resolution values of no carrier/index count interval, 1kHz/1ms, 10 kHz/0.1 ms, and 100 kHz/10 ms, as well as IRIG input coded expressions of the fields BCD_{TOY}, CF, SBS, and BCD_{YEAR}.

The IRIG inputs support the following coded expression combinations for BCD_{TOY}, CF, SBS, and BCD_{YEAR} fields:

- 0 – BCD_{TOY}, CF, SBS
- 1 – BCD_{TOY}, CF
- 2 – BCD_{TOY}
- 3 – BCD_{TOY}, SBS
- 4 – BCD_{TOY}, BCD_{YEAR}, CF, SBS
- 5 – BCD_{TOY}, BCD_{YEAR}, CF
- 6 - BCD_{TOY}, BCD_{YEAR}
- 7 - BCD_{TOY}, BCD_{YEAR}, SBS

The cards support synchronization with the following DCLS IRIG input formats:

Provided DCLS IRIG Code Format	Code Description
A-DCLS	
A000	IRIG A, DCLS, BCD_{TOY}, CF, SBS
A001	IRIG A, DCLS, BCD_{TOY}, CF

Provided DCLS IRIG Code Format	Code Description
A002	IRIG A, DCLS, BCD_{TOY}
A003	IRIG A, DCLS, BCD_{TOY}, SBS
A004	IRIG A, DCLS, BCD_{TOY}, BCD_{YEAR}, CF, SBS
A005	IRIG A, DCLS, BCD_{TOY}, BCD_{YEAR}, CF
A006	IRIG A, DCLS, BCD_{TOY}, BCD_{YEAR}
A007	IRIG A, DCLS, BCD_{TOY}, BCD_{YEAR}, SBS
B-DCLS	
B000	IRIG B, DCLS, BCD_{TOY}, CF, SBS
B001	IRIG B, DCLS, BCD_{TOY}, CF
B002	IRIG B, DCLS, BCD_{TOY}
B003	IRIG B, DCLS, BCD_{TOY}, SBS
B004	IRIG B, DCLS, BCD_{TOY}, BCD_{YEAR}, CF, SBS
B005	IRIG B, DCLS, BCD_{TOY}, BCD_{YEAR}, CF
B006	IRIG B, DCLS, BCD_{TOY}, BCD_{YEAR}
B007	IRIG B, DCLS, BCD_{TOY}, BCD_{YEAR}, SBS
E-DCLS **(output only)**	
E000	IRIG E, DCLS, BCD_{TOY}, CF, SBS
E001	IRIG E, DCLS, BCD_{TOY}, CF
E002	IRIG E, DCLS, BCD_{TOY}
E003	IRIG E, DCLS, BCD_{TOY}, SBS
E004	IRIG E, DCLS, BCD_{TOY}, BCD_{YEAR}, CF, SBS
E005	IRIG E, DCLS, BCD_{TOY}, BCD_{YEAR}, CF
E006	IRIG E, DCLS, BCD_{TOY}, BCD_{YEAR}
E007	IRIG E, DCLS, BCD_{TOY}, BCD_{YEAR}, SBS
G-DCLS	
G001	IRIG G, DCLS, BCD_{TOY}, CF
G002	IRIG G, DCLS, BCD_{TOY}

Provided DCLS IRIG Code Format	Code Description
G005	IRIG G, DCLS, BCD_{TOY}, BCD_{YEAR}, CF
G006	IRIG G, DCLS, BCD_{TOY}, BCD_{YEAR}
NASA-36	
NASA-36	NASA-36, DCLS, 10 msec

Table 5-17: Accepted IRIG reference formats

The 1204-05 card also supports the following analog IRIG inputs.

Provided AM IRIG Code Format	Code Description
A-AM	
A130	IRIG A, AM, 10kHz, BCD_{TOY}, CF, SBS
A131	IRIG A, AM, 10kHz, BCD_{TOY}, CF
A132	IRIG A, AM, 10kHz, BCD_{TOY}
A133	IRIG A, AM, 10kHz, BCD_{TOY}, SBS
A134	IRIG A, AM, 10kHz, BCD_{TOY}, BCD_{YEAR}, CF, SBS
A135	IRIG A, AM, 10kHz, BCD_{TOY}, BCD_{YEAR}, CF
A136	IRIG A, AM, 10kHz, BCD_{TOY}, BCD_{YEAR}
A137	IRIG A, AM, 10kHz, BCD_{TOY}, BCD_{YEAR}, SBS
B-AM	
B120	IRIG B, AM, 1kHz, BCD_{TOY}, CF, SBS
B121	IRIG B, AM, 1kHz, BCD_{TOY}, CF
B122	IRIG B, AM, 1kHz, BCD_{TOY}
B123	IRIG B, AM, 1kHz, BCD_{TOY}, SBS
B124	IRIG B, AM, 1kHz, BCD_{TOY}, BCD_{YEAR}, CF, SBS
B125	IRIG B, AM, 1kHz, BCD_{TOY}, BCD_{YEAR}, CF
B126	IRIG B, AM, 1kHz, BCD_{TOY}, BCD_{YEAR}
B127	IRIG B, AM, 1kHz, BCD_{TOY}, BCD_{YEAR}, SBS
E-AM **(output only)**	

Provided AM IRIG Code Format	Code Description
E110	IRIG E, AM, 100 Hz, BCD_{TOY}, CF, SBS
E111	IRIG E, AM, 100 Hz, BCD_{TOY}, CF
E112	IRIG E, AM, 100 Hz, BCD_{TOY}
E113	IRIG E, AM, 100 Hz, BCD_{TOY}, SBS
E114	IRIG E, AM, 100 Hz, BCD_{TOY}, BCD_{YEAR}, CF, SBS
E115	IRIG E, AM, 100 Hz, BCD_{TOY}, BCD_{YEAR}, CF
E116	IRIG E, AM, 100 Hz, BCD_{TOY}, BCD_{YEAR}
E117	IRIG E, AM, 100 Hz, BCD_{TOY}, BCD_{YEAR}, SBS
E120	IRIG E, AM, 100 Hz, BCD_{TOY}, CF, SBS
E121	IRIG E, AM, 1 kHz, BCD_{TOY}, CF
E122	IRIG E, AM, 1 kHz, BCD_{TOY}
E123	IRIG E, AM, 1 kHz, BCD_{TOY}, SBS
E124	IRIG E, AM, 1 kHz, BCD_{TOY}, BCD_{YEAR}, CF, SBS
E125	IRIG E, AM, 1 kHz, BCD_{TOY}, BCD_{YEAR}, CF
E126	IRIG E, AM, 1 kHz, BCD_{TOY}, BCD_{YEAR}
E127	IRIG E, AM, 1 kHz, BCD_{TOY}, BCD_{YEAR}, SBS
G-AM	
G141	IRIG G, AM, 100kHz, BCD_{TOY}, CF
G142	IRIG G, AM, 100kHz, BCD_{TOY}
G145	IRIG G, AM, 100kHz, BCD_{TOY}, BCD_{YEAR}, CF
G146	IRIG G, AM, 100kHz, BCD_{TOY}, BCD_{YEAR}
NASA-36	
NASA-36	NASA-36, AM, 1 msec

Table 5-18: Additional IRIG reference formats for 1204-05

IRIG Output: Signal State

To quickly view if an **IRIG output** is enabled, or disabled, navigate to the option card's Status Summary panel. For instructions, see: "Viewing an Input/Output

Signal State" on page 387.

IRIG Input: Edit Window

To configure the IRIG Input (also referred to as 'Reference'), navigate to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entries for these cards are: **IRIG In/Out BNC** and **IRIG In/Out Fiber**.

The connector number is: J1.



The Edit window allows the configuration of the following settings:

- **Format**: Sets the formatting of the IRIG input signal, as defined by the IRIG generator time source. The available choices are:
  - IRIG A
  - IRIG B
  - IRIG G
  - NASA-36
- **Modulation Type**: Configures the type of input signal modulation. The choices are:
  - IRIG DCLS—A TTL (Phase) modulated signal.
  - IRIG AM—An amplitude modulated signal.
- **Frequency**: The IRIG modulation frequency. This is determined by the configuration of Format and Modulation Type. See "IRIG Carrier Frequencies" on page 620 for details.

- **Coded Expression**—Defines the data structure of the IRIG signal, where:
  - BCD = Binary Coded Decimal
  - TOY = Time of Year
  - CF = Control Field
  - SBS = Straight Binary Seconds
  - The available options will vary according to the configurations of Format and Modulation Type.
- **Control Function Field**: IRIG signals have an optional section in the data stream that can be used to include additional information (such as the present year, for example). This field allows the Control Field section of the IRIG output to be defined. The available configurations are:
  - Fields conform to **RCC 200-04**: IRIG spec 200-04 specified a location for year value, if included in this field.
  - Fields conform to **IEEC 37.118-2005** (IEEE 1344): Control Field contains year, leap second and daylight savings time information.
  - Fields conform to **Spectracom Format**: Year is included in Control Field but not in the same location as RCC-2004 output (year is offset by one position).
  - Fields conform to **Spectracom FAA Format**: A unique IRIG output Control Field that contains satellite lock status and time error flags.
  - Fields conform to **NASA Formats**: Variants of IRIG B
  - Fields confirm to **Spectracom IEEE C37.118-2005**: Has been extended to support one-month leap second notification

  The available options will vary according to the configurations of Format and Modulation Type.



Note: If the Format value is changed, the Control Field and Coded Expression change to the default values for the given Format value. The user can only change the Control Field field and Coded Expression field to allowed values for the Format field.

It is recommended that the SecureSync administrator/operator only use this if they do not know what the IRIG Input Format is, and they wish to identify the signal type, or to determine if a signal is present.

- **Local Clock**: The incoming IRIG input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to "Local", select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display.
- **Offset**: Provides the ability to account for IRIG cable delays or other latencies in the IRIG input. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.

Configuring the IRIG Input Year

The IRIG time source may be able to provide SecureSync with the current year information via the IRIG input data stream. As the year value is not a required field in the IRIG data stream, (and if the year value is present, it may not always be in the same location of the Control Field), if the year value is contained in the control field section of the IRIG data stream, the control field "layout" needs to be defined in SecureSync (as determined by the Coded Expressions and Control Field values). If the year value is not present in the IRIG input signal, the year value will need to be manually set in SecureSync when using IRIG input as the only input Time reference.



Note: By default, the "year" fields in the IRIG message are ignored and a user-defined value is used.



Note: By default, the "year" fields in the IRIG message are ignored and a user-defined value is used. Make sure the year is set correctly when the SecureSync is installed. If the year is not set correctly before NTP achieves time synchronization, it will use the value entered. The unit will also default to the year entered if it is powered down during the rollover of the year. If the SecureSync was not switched on during the rollover, this value must be updated.

Note: When the IRIG Input year is updated, NTP must be restarted from the Web UI NTP page (or the SecureSync unit rebooted) for the New Year value to take effect.

The current year value can be manually entered from the MANAGEMENT/OTHER/Time Management page. The year value only needs to be manually entered once, as it will automatically increment to the next year each New Year's day. See "System Time" on page 204 for instructions on how to set the current year manually.

Verifying IRIG Input Signal Validity

See: "Verifying the Validity of an Input Signal" on page 388.

IRIG Input: Status Window

To view the current settings of the **IRIG Input** (also referred to as 'Reference'), go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entries for these cards are: **IRIG In/Out BNC** and **IRIG In/Out Fiber**. The connector number is: J1.



The Status window displays the following settings:

- **Reference ID**: If you have only one IRIG card installed, SecureSync will number that card 0 and it will be identified as irg0. Additional cards will be numbered irg1 or above.
- **Validity**: If the IRIG input is not present, or is not considered valid and qualified, the "1PPS Validity" and "Time Validity" fields will be considered "Not Valid" (Orange).



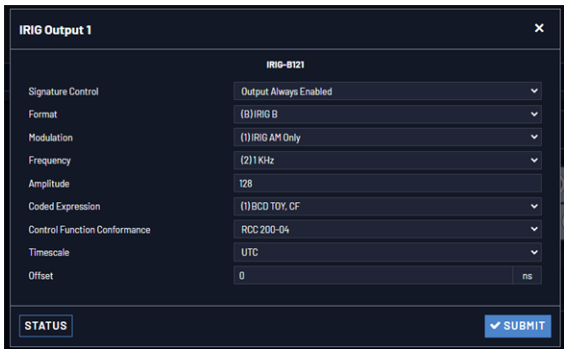
- Once the IRIG input has been supplied and the signal is considered valid and qualified, the two indicators will then turn “Valid” (Green).
- **Format**: Identifies the formatting of the IRIG input signal, as defined by the IRIG generator time source. The possible values are:
  - IRIG A
  - IRIG B
  - IRIG G
  - NASA-36
- **Modulation Type**: Identifies the type of input signal modulation. The possible values are:
  - IRIG DCLS—A TTL (Phase) modulated signal.
  - IRIG AM—An amplitude modulated signal.
  - Frequency—The IRIG modulation frequency. This is determined by the configuration of Format and Modulation Type. See also: "IRIG Carrier Frequencies" on page 620.
- **Coded Expression**: Defines the data structure of the IRIG signal, where:
  - BCD = Binary Coded Decimal
  - TOY = Time of Year
  - CF = Control Field
  - SBS = Straight Binary Seconds
- **Message**: The IRIG message.

IRIG Output: Edit Window

To configure the settings of one of the two **IRIG Outputs**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entries for these cards are: **IRIG In/Out BNC** and **IRIG In/Out Fiber**.

The connector numbers are: J2 and J3.



The Edit window allows the configuration of the following settings:

- **Signature Control**: Is used to control when the IRIG modulation will be present. This function allows the modulation to stop under certain conditions; see also "Signature Control" on page 198.
- **Format**: Used to configure the desired IRIG output formatting. The available choices are:
  - IRIG A
  - IRIG B
  - IRIG G
  - IRIG E
  - NASA-36
- **Modulation**: Changes the type of output signal modulation. The available choices are:
  - IRIG DCLS—A TTL-modulated output.
  - IRIG AM-–An amplitude modulated output. The amplitude of the output is determined by the value entered in the Amplitude field.
  - Frequency—The IRIG modulation frequency. This is determined by the configuration of Format and Modulation Type. See also "IRIG Carrier Frequencies" on page 620.
- **Coded Expression**: Defines the data structure of the IRIG signal, where:
  - BCD = Binary Coded Decimal
  - TOY = Time of Year
  - CF = Control Field

- SBS = Straight Binary Seconds
- The available options will vary according to the values of Format and Modulation Type.

- **Control Function Field**: IRIG signals have an optional section in the data stream that can be used to include additional information (such as the present year, for example). This field allows the Control Field section of the IRIG output to be defined. The available configurations are:
  - Fields conform to **RCC 200-04**: IRIG spec 200-04 specified a location for year value, if included in this field.
  - Fields conform to **IEEC 37.118-2005** (IEEE 1344): Control Field contains year, leap second and daylight savings time information.
  - Fields conform to **Spectracom Format**: Year is included in Control Field but not in the same location as RCC-2004 output (year is offset by one position).
  - Fields conform to **Spectracom FAA Format**: A unique IRIG output Control Field that contains satellite lock status and time error flags.
  - Fields conform to **NASA Formats**: Variants of IRIG B
  - Fields confirm to **Spectracom IEEE C37.118-2005**: Has been extended to support one-month leap second notification

  The available options will vary according to the configurations of Format and Modulation Type.
- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**—Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**—Temps Atomique International
  - **GPS**—The raw GPS time as transmitted by the GNSS satellites (as of 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. See "Local Clock(s), DST" on page 214 for more information. Local

timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

» **Amplitude**: The peak-to-peak output voltage level into a 600 Ω load is adjusted by entering a digital control value in this field. The level adjustment has no effect on TTL outputs, only on AM formats. The value of 128 will cause the Mark amplitude to be about $5V_{p-p}$ into high impedance. A value of 200 results in an output amplitude of about $9V_{p-p}$ into high impedance.

Note: These are nominal values only. Actual values will vary from unit to unit. To adjust the level precisely, connect an oscilloscope to the output connector when adjusting.

» **Offset**: Provides the ability to account for IRIG cable delays or other latencies in the IRIG input. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.

For IRIG frequency and output specifications, see "IRIG Standards and Specifications" on page 619.

IRIG Output: Status Window

To view the current settings of one of the **IRIG Outputs**, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entries for these cards are: **IRIG In/Out BNC** and **IRIG In/Out Fiber**. The connector numbers are: J2 and J3.



The Status window displays the following settings:

- **Signature Control**: is used to control when the IRIG modulation will be present. This function allows the modulation to stop under certain conditions; see also "Signature Control" on page 198.
- **Format**: Used to configure the desired IRIG output formatting. The possible values are:
  - IRIG A
  - IRIG B
  - IRIG G
  - IRIG E
  - NASA-36
- **Modulation**: Changes the type of output signal modulation. The possible values are:
  - IRIG DCLS—A TTL-modulated output.
  - IRIG AM-–An amplitude modulated output. The amplitude of the output is determined by the value entered in the Amplitude field.
  - Frequency—The IRIG modulation frequency. This is determined by the configuration of Format and Modulation Type. See also: "IRIG Carrier Frequencies" on page 620.
- **Coded Expression**: Defines the data structure of the IRIG signal, where:
  - BCD = Binary Coded Decimal
  - TOY = Time of Year
  - CF = Control Field
  - SBS = Straight Binary Seconds
  - The possible values will vary according to the values of Format and Modulation Type
- **Message**: The IRIG message of the output.

For IRIG frequency and output specifications, see "IRIG Standards and Specifications" on page 619.

5.2.5.3 STANAG Out [1204-11, -25]

The STANAG Output option card models 1204-11 and 1204-25 provide (2) configurable STANAG outputs and (1) 1PPS output for the SecureSync platform.

STANAG Out [1204-11, -25]: Specifications

- **Outputs**: (2) STANAG Outputs, (1) 1PPS Output
- **Signal Type and Connector**: 5V or 10 V or RS-485 level (user selectable) for STANAG and 1PPS output. DB-25 connector.
- **Formats Supported**:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 STM (Standard Time Message)
  - STANAG 4430 Ext HQ (Extended HAVE QUICK)
  - STANAG 4430 Ext HQ Ed1
  - ICD-GPS-060A BCD
  - ICD-GPS-060A HQ
  - DOD-STD-1399 BCD
- **Programmable Pulse Width** (1PPS Output): 100 ns to 500 ms with 20 ns resolution
- **Accuracy**: ±50 ns (1σ)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-11 (for non-isolated board); 1204-25 (for isolated board)

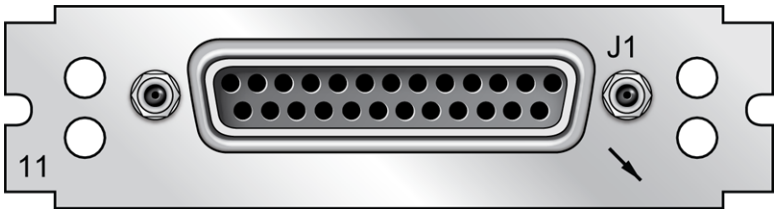


Figure 5-46: Model 1204-11 option card rear plate

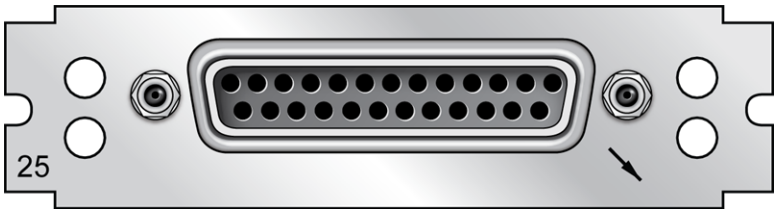


Figure 5-47: Model 1204-25 option card rear plate

Pin Assignments

Pin No.	Signal	Function	Pin No.	Signal	Function
1	GND	Ground	14	TOD1-	TOD1 RS-485- Out
2	TOD1+	TOD1 RS-485+ Out	15	NC	-
3	NC	-	16	NC	-
4	TOD2+	TOD2 RS-485+ Out	17	TOD2-	TOD2 RS-485- Out
5	NC	-	18	NC	-
6	GND	Ground	19	NC	5 MHz Out (1204-11 Only)
7	GND	Ground	20	NC	-
8	NC	-	21	1PPS-	1PPS RS-485- Out
9	1PPS+	1PPS RS-485+ Out	22	NC	-
10	TFD	Time Fault Discrete	23	GND	Ground
11	TOD1	TOD1 TTL Out	24	1PPS	1PPS TTL Out
12	GND	Ground	25	GND	Ground
13	TOD2	TOD2 TTL Out			

Table 5-19: Models 1204-11, -25: DB-25 pin-out

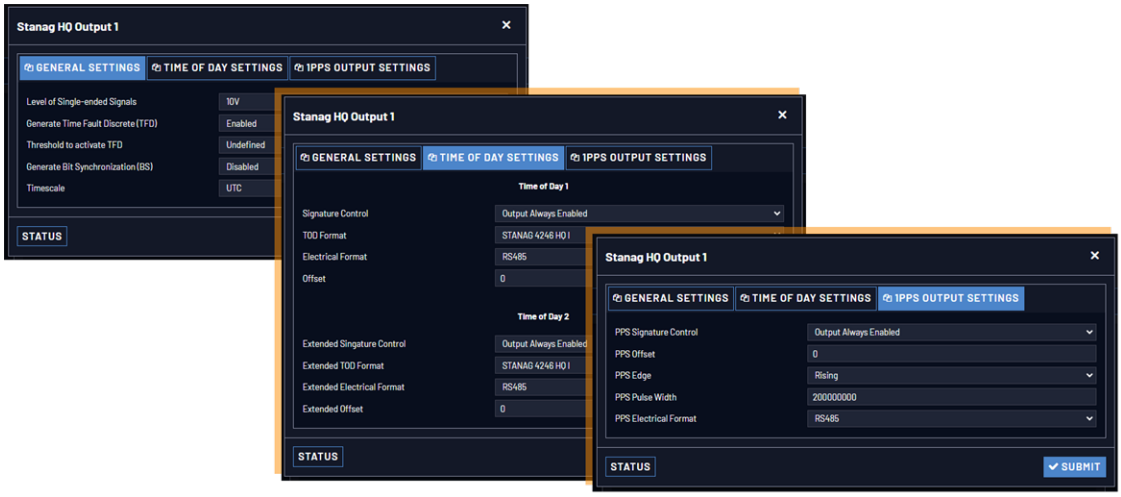
STANAG Output: Edit Window

To configure a **STANAG output**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entries for these cards are: **STANAG Out** and **STANAG Out, Isolated**.

The outputs are named: **Stanag HQ Output [number]**.

> **Note:** SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



The Edit window allows the configuration of the following settings:

Under **General Settings**:

- **Level of Single-ended Signals**: 10 V or 5V can be selected for the TOD 1 and 1PPS Output.
- **Generate Time Fault Discrete (TFD)**:
  - Enabled: The TFD signal uses the “Threshold to activate” value to provide the level of TFD.
  - Disabled: The TFD signal is always valid.
- **Threshold to activate TFD**: If the TFD is activated, the user can select the TFOM value threshold. Below this value, the TFD is high, otherwise the TFD is low.
- **Generate Bit Synchronization (BS)**:
  - **Enabled**: The second STANAG signal (TOD 2) is used to send the BS (Bit Stream) signal used with STANAG 4430-STM. When BS is active, the configuration of TOD 2 is superseded and only used for BS.

- **Disabled**: The second STANAG signal (TOD 2) can be used to send an independent TOD.

- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**—Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**—Temps Atomique International
  - **GPS**—The raw GPS time as transmitted by the GNSS satellites (as of 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 202 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the **Timescale** field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to for more information on Local Clocks.

Configurable settings for each **Time of Day** are:

- **Signature Control**: Used to control when the signal will be present. This function allows the modulation to stop under certain conditions, see also "Signature Control" on page 198.
- **TOD Format**: The user-selectable format to be used. Available formats include:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 STM
  - STANAG 4430 Ext HQ

- STANAG 4430 Ext HQ Ed1
- ICD-GPS-060A BCD
- ICD-GPS-060A HQ
- DOD-STD-1399 BCD

- **Electrical Format**: Selects signaling on either RS-485 or TTL (supporting up to 10 V levels) signal lines.
- **Time Scale**: Used to set the desired time scale (UTC, TAI, GPS, or Local). See above.
- **Offset (ns)**: Provides the ability to account for STANAG Line (TOD1 and TOD2 independently) cable delays or other latencies in the STANAG output. Available Offset range is –500 to +500 ms in 5ns steps.

Configurable settings under **1PPS Output** are:

- **PPS Signature Control**: Used to control when the signal will be present. This function allows the modulation to stop under certain conditions, see also "Signature Control" on page 198.
- **PPS Offset (ns)**: Used to account for 1PPS cable delays or other latencies in the 1PPS output. Available Offset range is –500 to +500 ms in 5ns steps.
- **PPS Edge**: The operator can select if the output signal is a rising or falling edge pulse.
- **PPS Pulse Width**: Configures the Pulse Width of the 1PPS output. The Pulse Width is entered and displayed in nanoseconds (the default Pulse Width is 200 ms).
- **PPS Electrical Format**: Selects signaling on either RS-485 or TTL (supporting up to 10 V levels) signal lines.

STANAG Output: Status Window

To view the current settings of a **STANAG Output**, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entries for these cards are: **STANAG Out** and **STANAG Out, Isolated**.

The outputs are named: **Stanag HQ Output [number]**.



The Status window displays the following settings:

Under **General Status**:

- **Level of Single-ended Signals**: 10 V or 5V will be indicated for the TOD 1 and 1PPS Output.
- **Generate Time Fault Discrete (TFD)**:
  - **Enabled**: The TFD signal uses the "Threshold to activate" value to provide the level of TFD.
  - **Disabled**: The TFD signal is always valid.

- **Threshold to activate TFD**: If the TFD is activated, indicates the TFOM value threshold. Below this value, the TFD is high, otherwise the TFD is low.
- **Generate Bit Synchronization (BS)**:
  - **Enabled**: The second STANAG signal (TOD 2) is used to send the BS (Bit Stream) signal used with STANAG 4430-STM. When BS is active, the configuration of TOD 2 is superseded and only used for BS.
  - **Disabled**: The second STANAG signal (TOD 2) can be used to send an independent TOD.
- **Timescale**: Indicates the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**—Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**—Temps Atomique International
  - **GPS**—The raw GPS time as transmitted by the GNSS satellites (as of 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 202 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to for more information on Local Clocks.

For each **Time of Day** the following settings are displayed:

- **Signature Control**: Indicates when the signal is present. This function allows the modulation to stop under certain conditions, see "Signature Control" on page 198.
- **TOD Format**: The user-selectable format being used. Available formats include:

- STANAG 4246 HQ I
- STANAG 4246 HQ II
- STANAG 4372 HQ IIA
- STANAG 4430 STM
- STANAG 4430 Ext HQ
- STANAG 4430 Ext HQ Ed1
- ICD-GPS-060A BCD
- ICD-GPS-060A HQ
- DOD-STD-1399 BCD

- **Electrical Format**: Selects signaling on either RS-485 or TTL (supporting up to 10 V levels) signal lines.
- **Time Scale**: Used to set the desired time scale (UTC, TAI, GPS, or Local). See above.
- **Offset (ns)**: Provides the ability to account for STANAG Line (TOD1 and TOD2 independently) cable delays or other latencies in the STANAG output. Available Offset range is –500 to +500 ms in 5ns steps.
- **STANAG TFOM**: The Time Figure of Merit for the output.

Under **1PPS Output**, the following settings are displayed:

- **PPS Signature Control**: Indicates whether the signal will be present. This function allows the modulation to stop under certain conditions, see "Signature Control" on page 198.
- **PPS Offset (ns)**: Used to account for 1PPS cable delays or other latencies in the 1PPS output. Available Offset range is –500 to +500 ms in 5ns steps.
- **PPS Edge**: Indicates whether the output signal is a rising or falling edge pulse.
- **PPS Pulse Width**: Indicates the Pulse Width of the 1PPS output. The Pulse Width is entered and displayed in nanoseconds (the default Pulse Width is 200 ms).
- **PPS Electrical Format**: Indicates signaling on either RS-485 or TTL (supporting up to 10 V levels) signal lines.

5.2.5.4 STANAG In [1204-1D, -24]

The STANAG Input option cards 1204-1D and 1204-24 STANAG provide (2) configurable STANAG inputs and (1) 1PPS input for the SecureSync platform.

STANAG In [1204-1D, -24]: Specifications

- **Inputs**: (2) STANAG Inputs, (1) 1PPS Input
- **Signal Type and Connector**: TTL or RS-485 level (user selectable) for STANAG and 1PPS input. DB25.
- **Formats Supported**:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 STM (Standard Time Message)
  - STANAG 4430 Ext HQ (Extended HAVE QUICK)
  - STANAG 4430 Ext HQ Ed1
  - ICD-GPS-060A BCD
  - ICD-GPS-060A HQ
  - DOD-STD-1399 BCD
- **Accuracy**: 100 ns
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-1D (for non-isolated board); 1204-24 (for isolated board)

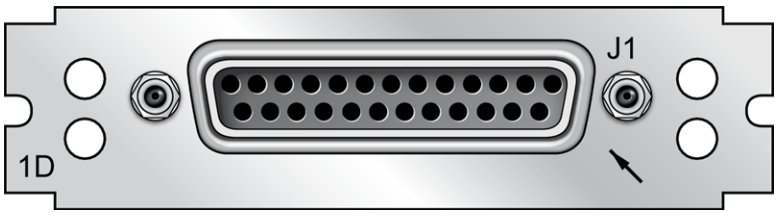


Figure 5-48: Model 1204-1D option card rear plate

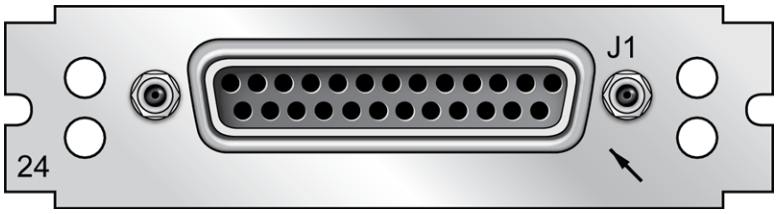


Figure 5-49: Model 1204-24 option card rear plate

Pin Assignments

Pin No.	Signal	Function	Pin No.	Signal	Function
1	GND	Ground	14	TOD1-	TOD1 RS-485- Input
2	TOD1+	TOD1 RS-485+ Input	15	NC	-
3	NC	-	16	NC	-
4	TOD2+	TOD2 RS-485+ Input	17	TOD2-	TOD2 RS-485- Input
5	NC	-	18	NC	-
6	GND	Ground	19	NC	-
7	GND	Ground	20	NC	-
8	NC	-	21	1PPS-	1PPS RS-485- Input
9	1PPS+	1PPS RS-485+ Input	22	NC	-
10	TFD	Time Fault Discrete	23	GND	Ground
11	TOD1	TOD1 TTL Input	24	1PPS	1PPS TTL Input
12	GND	Ground	25	GND	Ground
13	TOD2	TOD2 TTL Input			

Table 5-20: 1204-1D, 1204-24 option cards: DB-25 pin-outs

STANAG Input: Edit Window

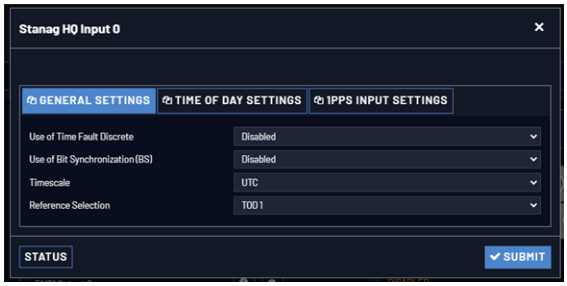
To configure a **STANAG Input** (also referred to as 'Reference'), go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entries for this card are: **STANAG In** and **STANAG In, Isolated**.

The inputs are named: **Stanag HQ Input [number]**.

The configurable settings are grouped under the following three tabs:

General Settings tab

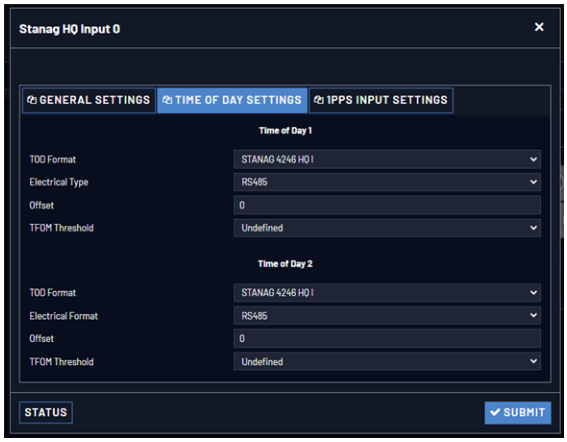


- **Use of Time Fault Discrete**: There are two options:
  - **Enabled**: The TFD input signal is used to validate the STANAG input.
  - **Disabled** (default): The TFD input signal is ignored.
- **Use of Bit Synchronization (BS)**: There are two options:
  - **Enabled**: The second STANAG input (TOD 2) is used to receive the BS (Bit Stream) signal used with STANAG 4430-STM. When BS is active, the configuration of TOD2 is superseded and only used for BS.
  - **Disabled**: The second STANAG input (TOD 2) can be used to receive an independent TOD.
- **Timescale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International
  - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of 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 202 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to for more information on Local Clocks.

- **Reference Selection**: Selects TOD 1 or TOD 2 (configured below) which TOD signal is used for synchronization.

Time of Day Settings tab



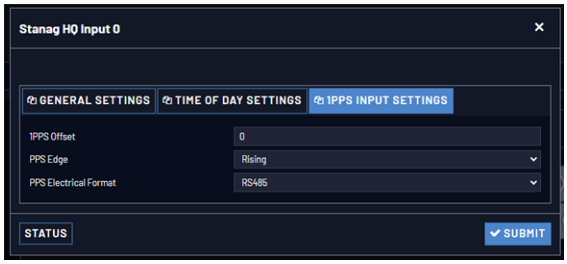
For **Time of Day 1** and **Time of Day 2** (STANAG content supports two ToD streams).

- **ToD Format**: The user-selectable format to be used. Available formats include:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 STM
  - STANAG 4430 Ext HQ
  - STANAG 4430 Ext HQ Ed1
  - ICD-GPS-060A BCD

- ICD-GPS-060A HQ
- DOD-STD-1399 BCD

- **Electrical Type**: Selects synchronization to either RS-485 or TTL (supporting up to 10 V levels) signal lines.
- **Offset**: Provides the ability to account for STANAG Line (TOD1 and TOD2 independently) cable delays or other latencies in the STANAG input. Available Offset range is –500 to +500 ms in 5ns steps.
- **TFOM Threshold**: Under the STANAG protocol, the TFOM (Time Figure of Merit) threshold value can be utilized as a means to validate timing data based on the TFOM. For more information on TFOM, see "Configuring the Oscillator" on page 271.

1PPS Input Settings tab



- **1PPS Offset**: Used to account for 1PPS cable delays or other latencies in the 1PPS input. Available Offset range is –500 to +500 ms in 5ns steps
- **PPS Edge**: The operator can select if the output signal is a rising or falling edge pulse.
- **PPS Electrical Format**: Selects synchronization to either RS-485 or TTL (supporting up to 10 V levels) signal lines.

STANAG Input: Status Window

To view the current settings of a **STANAG Input** (also referred to as 'Reference'), go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entries for this card are: **STANAG In** and **STANAG In, Isolated**.

The inputs are named: **Stanag HQ Input [number]**.



The Status window displays the following settings:

Under General Status:

- **Reference ID**: This is the identifier given to the input by SecureSync.
- **Validity**: Indicates the validity of the Time input and the PPS input. If the input signal is valid the indicator will be green. If the signal is not valid, the indicator will be orange.
- **Use of Time Fault Discrete**: There are two options:
  - **Enabled**: The TFD input signal is used to validate the STANAG input.
  - **Disabled** (default): The TFD input signal is ignored.

- **Time Fault Discrete State**: If this is valid, the indicator will be green. If it is not valid, the indicator will be orange.
- **Use of Bit Synchronization (BS)**: There are two options:
  - **Enabled**: The second STANAG input (TOD 2) is used to receive the BS (Bit Stream) signal used with STANAG 4430-STM. When BS is active, the configuration of TOD2 is superseded and only used for BS.
  - **Disabled**: The second STANAG input (TOD 2) can be used to receive an independent TOD.
- **Reference Selection**: Indicates which TOD signal is used for synchronization. This will be either TOD 1 or TOD 2.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to for more information on Local Clocks.

Under Time of Day Inputs:

- **TOD Format**: The user-selectable format being used. Available formats include:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 STM
  - STANAG 4430 Ext HQ
  - STANAG 4430 Ext HQ Ed1
  - ICD-GPS-060A BCD
  - ICD-GPS-060A HQ
  - DOD-STD-1399 BCD
- **Electrical Type**: Either RS-485 or TTL (supporting up to 10 V levels) signal lines.

- **Time Scale**: Used to select the time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time

    TAI: Temps Atomique International

    GPS: The raw GPS time as transmitted by the GNSS satellites (as of 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 214. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.
- **Offset**: Provides the ability to account for STANAG Line (TOD1 and TOD2 independently) cable delays or other latencies in the STANAG input. Available Offset range is –500 to +500 ms in 5ns steps.
- **Stanag TFOM**: The Time Figure of Merit for the input.

Under 1PPS Input:

- **1PPS Offset**: Used to account for 1PPS cable delays or other latencies in the 1PPS input. The available Offset range is –500 to +500 ms in 5ns steps.
- **PPS Edge**: Indicates whether the output signal is a rising or falling edge pulse.
- **PPS Electrical Format**: Indicates whether the signal is synchronized to RS-485 or TTL (supporting up to 10 V levels) signal lines.

5.2.5.5 HAVE QUICK Out [1204-10, -1B]

The HAVE QUICK option cards provide (4) HAVE QUICK outputs for the SecureSync platform.

HAVE QUICK Out, BNC [1204-10]: Specifications

- **Outputs**: (4) HAVE QUICK
- **Signal Type and Connector**: TTL levels (BNC)

- **Formats Supported**:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 STM (Standard Time Message)
  - STANAG 4430 Ext HQ (Extended HAVE QUICK)
  - STANAG 4430 Ext HQ Ed1
  - ICD-GPS-060A BCD
  - ICD-GPS-060A HQ
  - DOD-STD-1399 BCD
- **Output Load Impedance**: 10 kΩ
- **Start of Signal**: <10 µs after 1PPS output
- **Programmable Phase Shift**: ±20ns to 500 ms with 20ns resolution
- **Accuracy**: ±50 ns (1σ)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-10 HAVE QUICK outputs, BNC

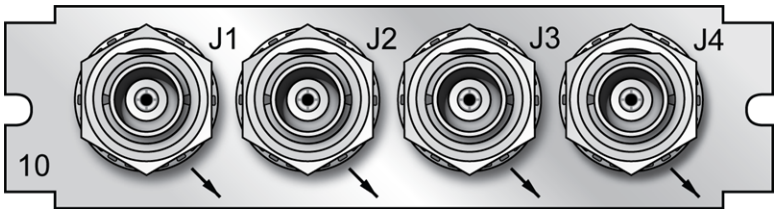


Figure 5-50: Model 1204-10 option card rear plate

HAVE QUICK Out, RS-485 [1204-1B]: Specifications

- **Outputs**: (4) HAVE QUICK outputs
- **Signal Type and Connector**: RS-485 levels (terminal block)
- **Formats Supported**:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II

- STANAG 4372 HQ IIA
- STANAG 4430 STM (Standard Time Message)
- STANAG 4430 Ext HQ (Extended HAVE QUICK)
- STANAG 4430 Ext HQ Ed1
- ICD-GPS-060A BCD
- ICD-GPS-060A HQ
- DOD-STD-1399 BCD

- **Output Load Impedance**: 120 Ω
- **Start of Signal**: <10 µs after 1PPS output
- **Programmable Phase Shift**: ±5ns to 500 ms with 5ns resolution
- **Accuracy**: ±50 ns (1σ)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-1B HAVE QUICK outputs, RS-485

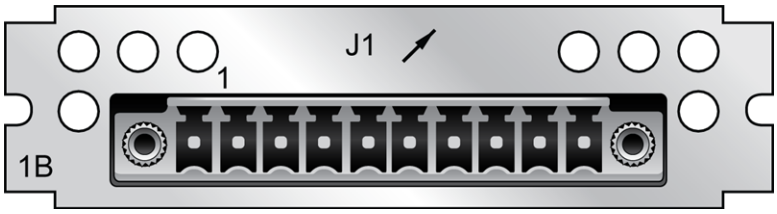


Figure 5-51: Model 1204-1B option card rear plate

Pin Assignments

Pin No.	Function
1	HAVE QUICK Output 1 +
2	HAVE QUICK Output 1 -
3	GND
4	HAVE QUICK Output 2 +
5	HAVE QUICK Output 2 -
6	HAVE QUICK Output 3 +

Pin No.	Function
7	HAVE QUICK Output 3 -
8	GND
9	HAVE QUICK Output 4 +
10	HAVE QUICK Output 4 -

Table 5-21: 1204-1B terminal block pin-out

HAVE QUICK Output: Viewing Signal State

To quickly view if a **HAVE QUICK Output** is enabled or disabled, go to the option card's Status Summary panel. For instructions, see: "Viewing an Input/Output Signal State" on page 387.

HAVE QUICK Output: Edit Window

To configure a **HAVE QUICK Output**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entries for this card are: **HAVE QUICK out, BNC** and **HAVE QUICK Out, RS-485**.

The outputs are named: **HQ Output [number]**.



The Edit window allows the configuration of the following settings:

- **Signature Control**: Signature Control is used to control when the HAVE QUICK modulation is present; see also "Signature Control" on page 198.
- **Format**: Used to configure the formatting of the available HAVE QUICK inputs and outputs. The available formats are as follows:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA

- STANAG 4430 STM (Standard Time Message)
- STANAG 4430 Ext HQ (Extended HAVE QUICK)
- STANAG 4430 Ext HQ Ed1
- 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: This option will appear under the name of the local clock you have set up. Refer to "The Time Management Screen" on page 202 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. See also .

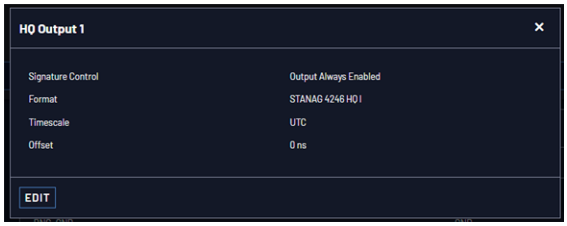
- **Offset**: Provides the ability to account for HAVE QUICK cable delays or other latencies in the HAVE QUICK outputs. The Offset values are entered in nanoseconds (ns). The available Offset range is –500 to +500 ms.

HAVE QUICK Output: Status Window

To view the current settings of a **HAVE QUICK Output**, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entries for this card are: **HAVE QUICK out, BNC** and **HAVE QUICK Out, RS-485**.

The outputs are named: **HQ Output [number]**.



The Status window displays the following settings:

- **Signature Control**: Signature Control is used to control when the HAVE QUICK modulation is present, see "Signature Control" on page 198.
- **Format**: Used to configure the formatting of the available HAVE QUICK inputs and outputs. The available formats are as follows:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 STM (Standard Time Message)
  - STANAG 4430 Ext HQ (Extended HAVE QUICK)
  - STANAG 4430 Ext HQ Ed1
  - 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: This option will appear under the name of the local clock you have set up. Refer to "The Time Management Screen" on page 202 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to for more information on Local Clocks.

- **Offset**: Provides the ability to account for HAVE QUICK cable delays or other latencies in the HAVE QUICK outputs. The Offset values are entered in nanoseconds (ns). The available Offset range is –500 to +500 ms.

5.2.5.6 HAVE QUICK In/Out [1204-29]

The HAVE QUICK input/output option card 1204-29 provides SecureSync with (1) HAVE QUICK input and (3) HAVE QUICK outputs.

HAVE QUICK In/Out [1204-29]: Specifications

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

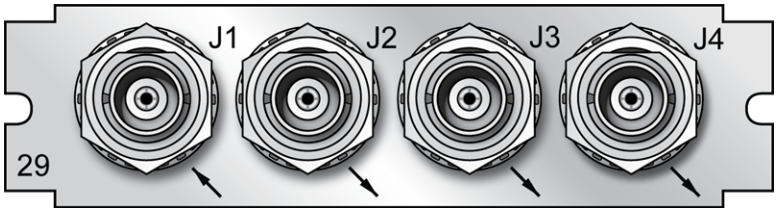


Figure 5-52: Model 1204-29 option card rear plate

HAVE QUICK Output: Viewing Signal State

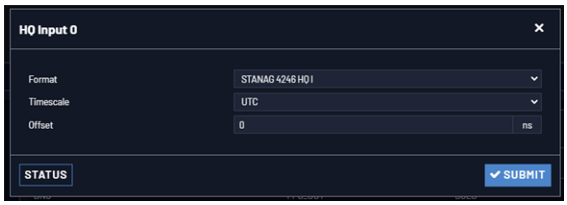
To quickly view if a **HAVE QUICK Output** is enabled or disabled, go to the option card's Status Summary panel. For instructions, see: "Viewing an Input/Output Signal State" on page 387.

HAVE QUICK Input: Edit Window

To configure the settings of the **HAVE QUICK Input** (also referred to as 'Reference'), go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entry for this card is: **HAVE QUICK In/Out**.

The input is named: **HQ Input [number]**.



The Edit window allows the configuration of the following settings:

- **Format**: Used to configure the formatting of the available HAVE QUICK inputs and outputs. The available formats are as follows:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 STM (Standard Time Message)
  - STANAG 4430 Ext HQ (Extended HAVE QUICK)
  - STANAG 4430 Ext HQ Ed1
  - 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)
  - Offset: Provides the ability to account for HAVE QUICK cable delays or other latencies in the HAVE QUICK outputs. The Offset values are entered in nanoseconds (ns). The available Offset range is –500 to +500 ms.

HAVE QUICK Input: Status Window

To view the current settings of the **HAVE QUICK Input** (also referred to as 'Reference'), go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entry for this card is: **HAVE QUICK In/Out**.

The input is named: **HQ Input [number]**.



The Status window displays the following settings:

- **Reference ID**: Indicates the letters used in the Input Reference Priority table for this particular input reference.
- **Validity**: [TIME, PPS] Indicates the validity of the Time input and the PPS input. If the input signal is valid the indicator will be green. If the signal is not valid, the indicator will be orange.

- **Format**: Used to configure the formatting of the available HAVE QUICK inputs and outputs. The available formats are as follows:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 STM (Standard Time Message)
  - STANAG 4430 Ext HQ (Extended HAVE QUICK)
  - STANAG 4430 Ext HQ Ed1
  - 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).
- **Offset**: Provides the ability to account for HAVE QUICK cable delays or other latencies in the HAVE QUICK outputs. The Offset values are entered in nanoseconds (ns). The available Offset range is –500 to +500 ms.
- **TFOM**: The Time Figure of Merit for the input.

HAVE QUICK Output: Edit Window

To configure the settings of a **HAVE QUICK Output**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entry for this card is: **HAVE QUICK In/Out**.

Outputs are named: **HQ Output [number]**.



The Edit window allows the configuration of the following settings:

- **Signature Control**: Signature Control is used to control when the HAVE QUICK modulation is present, see "Signature Control" on page 198.
- **Format**: Used to configure the formatting of the available HAVE QUICK inputs and outputs. The available formats are as follows:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 STM (Standard Time Message)
  - STANAG 4430 Ext HQ (Extended HAVE QUICK)
  - STANAG 4430 Ext HQ Ed1
  - 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: This option will appear under the name of the local clock you have set up. Refer to "The Time Management Screen" on page 202 for more information

on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to for more information on Local Clocks.

- **Offset**: Provides the ability to account for HAVE QUICK cable delays or other latencies in the HAVE QUICK outputs. The Offset values are entered in nanoseconds (ns). The available Offset range is –500 to +500 ms.

HAVE QUICK Output: Status Window

To view the current settings of a **HAVE QUICK Output**, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entry for this card is: **HAVE QUICK In/Out**.

Outputs are named: **HQ Output [number]**.



The Status window displays the following settings:

- **Signature Control**: Signature Control is used to control when the HAVE QUICK modulation is present, see "Signature Control" on page 198.
- **Format**: Used to configure the formatting of the available HAVE QUICK inputs and outputs. The available formats are as follows:
  - STANAG 4246 HQ I
  - STANAG 4246 HQ II
  - STANAG 4372 HQ IIA
  - STANAG 4430 STM (Standard Time Message)

- STANAG 4430 Ext HQ (Extended HAVE QUICK)
- STANAG 4430 Ext HQ Ed1
- 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: This option will appear under the name of the local clock you have set up. Refer to "The Time Management Screen" on page 202 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to for more information on Local Clocks.

- **Offset**: Provides the ability to account for HAVE QUICK cable delays or other latencies in the HAVE QUICK outputs. The Offset values are entered in nanoseconds (ns). The available Offset range is –500 to +500 ms.

5.2.5.7 ASCII Time Code In/Out [1204-02, -04]

The ASCII Time Code Option Card, **Model 1204-02 (RS-232)** provides:

- one male DB-9 RS-232 input connector (J2),
- and one female DB-9 RS-232 output connector (J1)

The ASCII Time Code Option Card, **Model 1204-04 (RS-485)** consists of one RS-485 input, and one RS-485 output, integrated in a shared terminal block connector.

The interfaces accept Asynchronous Serial signals including date and time information. The input and output Data Formats are selected among predefined formats.

ASCII input

The ASCII input provides a serial data interface between an ASCII time generator (e.g., another SecureSync unit), serving as an input reference for Time and 1PPS in order to synchronize SecureSync (in conjunction with, or in lieu of, other available inputs, such as GNSS and/or IRIG).

ASCII output

The ASCII output provides SecureSync with the ability to output one, two or three back-to-back ASCII time code data streams that can be provided to peripheral devices which accept an ASCII RS-232 input data stream for either their external time synchronization or for data processing. See "Time Code Data Formats" on page 585 for a description of all supported time code formats.

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

When SecureSync is configured to output only one format message (the second and third formats configured as “None”), the one configured message will be available on the output port as either a broadcast message or only upon a request character being received. SecureSync has the ability to output one or two additional data stream messages immediately following the first message. In this configuration, only the first message determines the on-time point for the entire output string. The on-time points for the second and third messages that are provided at the same time as the first message are discarded. This unique capability allows SecureSync to be able to simultaneously provide multiple pieces of data from different selected format messages.

An example of selecting multiple formats is selecting “NMEA GGA” as the first format, “NMEA RMC” as the second format and “NMEA ZDA” as the third format. Depending on the setting of the “Mode” field (which determines if the data

streams are available every second or upon a request character being received), at the next second or the receipt of the next request character, the output port will provide the GGA message followed immediately by the corresponding RMC message for that same second, followed immediately by the corresponding ZDA message for that same second. The first GGA message will provide the on-time point for the entire output data stream.

ASCII Time Code, RS-232 [1204-02]: Specifications

- **Inputs/Outputs**: (1) Input, (1) Output
- **Signal Type and Connector**:
  - **Connector J1** — (RS-232 Output) RS-232 DB-9 F
  - **Connector J2** -- (RS-232 Input) RS-232 DB-9 M
- **Accuracy**: ±100...1000 µs (format dependent)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-02: ASCII Time Code Module (RS-232)

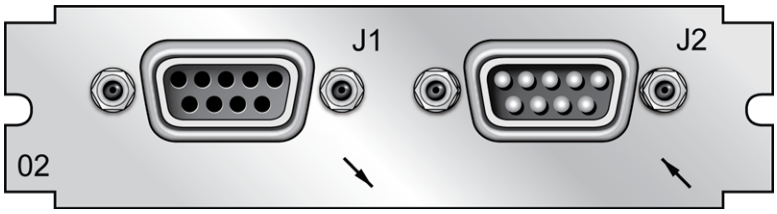


Figure 5-53: Model 1204-02 option card rear plate

Pin Assignments: OUTPUT connector J1

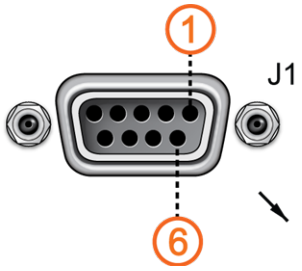


Figure 5-54: OUTPUT connector J1

Table 5-22: Pin-out, OUTPUT connector "J1"

Pin Number	Signal	Function	Notes
Top row of 5 pins			
1	PPS_OUT	1PPS output	TTL level on 50 Ω
2	SERIAL_OUT_TX	RS-232 Transmit data	Data output (ToD messages)
3	SERIAL_IN_RX	RS-232 Receive data	Data input into unit; use this to transmit commands to the unit)
4	NC	No connection	
5	GND	Ground	
Bottom row of 4 pins			
6	NC	No connection	
7	NC	No connection	
8	NC	No connection	
9	NC	No connection	

Pin Assignments: INPUT connector J2

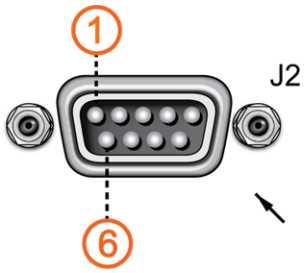


Figure 5-55: INPUT connector J2

Table 5-23: Pin-out, INPUT connector "J2"

Pin Number	Signal	Function	Notes
Top row of 5 pins			
1	PPS_IN	1PPS input	
2	SERIAL_IN_RX	RS-232 Receive data	Data input into unit; ToD message
3	NC	No Connection	
4	NC	No connection	
5	GND	Ground	
Bottom row of 4 pins			
6	NC	No connection	
7	NC	No connection	
8	NC	No connection	
9	NC	No connection	

ASCII Time Code, RS-485 [1204-04]: Specifications

- **Inputs/Outputs**: (1) Input, (1) Output
- **Signal Type and Connector**: (1) RS-485 terminal block for both Input and Output
- **Accuracy**: ±100...1000 µs (format dependent)
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-04 ASCII Time Code Module (RS-485)

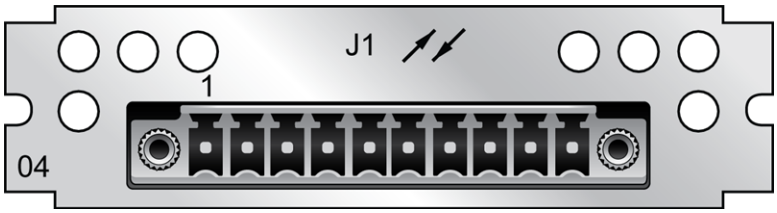


Figure 5-56: Model 1204-04 option card rear plate

Pin Assignments

Table 5-24: Pin-out, RS-485 terminal block connector J1

Pin No.	Signal	Function
1 (left)	SERIALTX_RS485+	+ RS-485 data output
2	SERIALTX_RS485-	- RS-485 data output
3	GND	Ground
4	PPS_OUT_RS485+	+ 1PPS output
5	PPS_OUT_RS485-	- 1PPS output
6	SERIALRX_RS485+	+ RS-485 data input
7	SERIALRX_RS485-	- RS-485 data input
8	GND	Ground
9	PPS_IN_RS485+	+ 1PPS input
10 (right)	PPS_IN _RS485-	- 1PPS input

ASCII Time Code Input: Edit Window

To configure the **ASCII Input** (also referred to as 'Reference'), go to its **Edit** window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entries for this card are: **ASCII TIMECODE RS-232** and **ASCII TIMECODE RS-485**.



The Input Edit window allows the configuration of the following settings:

- **Format Group**: Determines the time code message format category (see also "Time Code Data Formats" on page 585.) Choices are:
  - Auto
  - Spectracom
  - NMEA
  - ICD-153
  - EndRun
- **Format**: Once a **Format Group** has been selected, one or more **Format** fields may appear, allowing you to select one or more time code **Formats**. For detailed specifications and limitations on the supported time code formats, see "Time Code Data Formats" on page 585.



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

- **Offset**: Provides the ability to account for ASCII input cable delays or other latencies in the ASCII input. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is –500 to +500 ms.
- **Timescale**: Used to select the time base for the incoming ASCII time code data. The entered Timescale is used by the system to convert the time in the incoming ASCII data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International
  - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of 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 202 for more information on how to configure and read the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to "Local", select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. See 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.

ASCII Time Code Output: Edit Window

To configure the **ASCII Output**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entries for this card are: **ASCII TIMECODE RS-232** and **ASCII TIMECODE RS-485**.



The Output Edit window allows the configuration of the following settings:

- **Format Group** – configures the message format type. Choices are:
  - None (no message will be output)
  - Spectracom
  - NMEA
  - BBC
  - ICD-153
  - EndRun

  Once selected, the **Format Group** may offer a choice of **Formats**. For more information on supported **Formats**, see "Time Code Data Formats" on page 585.
  - **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 198.
- **Output Mode**: This field determines when the output data will be provided. The available Mode selections are as follows:

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

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

- **Time Scale**: Used to select the time base for the incoming data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:
  - **UTC**: Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
  - **TAI**: Temps Atomique International
  - **GPS**: The raw GPS time as transmitted by the GNSS satellites (as of 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 202 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.

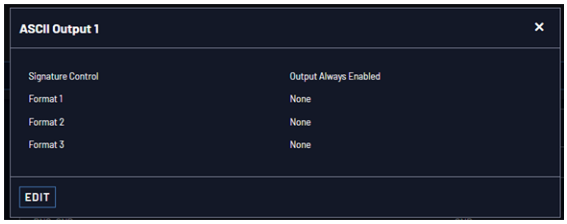
The incoming input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. See for more information on Local Clocks.

- **Baud Rate**: Determines the speed at which the output port will operate.
- **Data Bits**: Defines the number of Data Bits for the output port.
- **Parity**: Configures the parity checking of the output port.
- **Stop Bits**: Defines the number of Stop Bits for the output.

ASCII Time Code Output: Status Window

To view the current settings of the **ASCII Output**, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entries for this card are: **ASCII TIMECODE RS-232** and **ASCII TIMECODE RS-485**.



The Status window displays the following settings:

- **Signature Control**: Indicates whether Signature Control is enabled (Signature Control determines when the ASCII data stream will be enabled to be present). See also: "Signature Control" on page 198.
- **Format 1**: Indicates the configured format of the ASCII time code input data stream.
- **Format 2**: Indicates the configured format of the second consecutive ASCII time code input data stream.
- **Format 3**: Indicates the configured format of the third consecutive ASCII time code input data stream.

ASCII Time Code Input: Status Window

To *view* the current settings of the **ASCII Input** (also referred to as 'Reference'), go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entries for this card are: **ASCII TIMECODE RS-232** and **ASCII TIMECODE RS-485**.



The Status window displays the following settings:

- **Reference ID**: Indicates the letters used in the Input Reference Priority table for this particular input reference.
  - **Validity**: Indicates whether the ASCII input data is present and considered valid for Time and 1PPS references.
    - A **green** light indicates a valid reference.
    - An **orange** light indicates the reference is not considered valid.
- **Leap Flag**: Displays whether the incoming data stream is indicating that a pending leap second is to be added to the UTC timescale at the end of the month. See "Leap Seconds" on page 211.
- **Format**: Indicates the configured format of the ASCII time code input data stream.

5.2.6 Network Interface Option Cards

This section contains technical information and SecureSync Web UI procedures pertaining to option cards designed as Ethernet network interfaces using, e.g. the PTP format.

5.2.6.1 NTP and Networking [4A, 49]

The NTP and Networking cards have interfaces that allow the user to communicate outside of the normal channels that the SecureSync provides.

The 4A card, for instance, provides (4) 1 Gb NTP Server Outputs that can operate independently of the unit network.

The Ethernet ports provided on the NTP and Networking cards are designed for machine-to-machine network communication providing NTP functions. There is no management interface access through these cards. Settings are available for these Ethernet ports through the Web UI (login is available through the usual means).

Quad 1 Gb NTP Server [-4A]: Specifications

- **Inputs/Outputs**: (4) Gigabit Ethernet
- **Connectors**: SFP Ports (4x)
- **Management**: Enabled or Disabled (NTP server only)
- **Maximum Number of Cards**: 2
- **Ordering Information**: 1204-4A: Quad Gigabit Ethernet

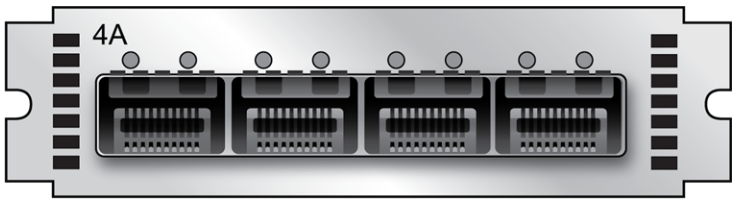


Figure 5-57: 1204-4A option card rear plate

Dual 1 Gb NTP Server [-49]: Specifications

- **Inputs/Outputs**: (2) Gigabit Ethernet
- **Connectors**: SFP Ports (2x)
- **Management**: Enabled or Disabled (NTP server only)
- **Maximum Number of Cards**: 2
- **Ordering Information**: 1204-49: Dual Gigabit Ethernet

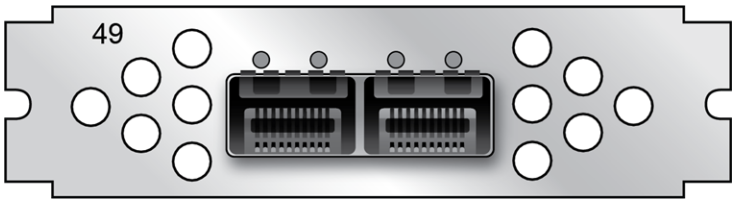


Figure 5-58: 1204-49 option card rear plate

Hardware

Cards in this category have SFP interface(s) that accept any number of brands chosen by the user.

Safran has successfully tested the following SFP models with the Gb Networking cards:

- Bel SFP-1GBT-05
- Finisar FCLF8522P2BTL
- Molex 1837022037
- Avago AFBR-5710LZ (available from Safran as **SFP-FIBER-MM**)
- Finisar FTLF1318P3BTL (available from Safran as **SFP-FIBER-SM**)

The following SFP models are NOT approved for use with cards of this type (found to be incompatible in testing):

- Arista SFP-1G-T

Networking

To configure the network information on this set of cards, navigate to MANAGEMENT > Network Setup.

In the Actions Panel, select Configure xxxx 1GBE (Slot x).

In the xxxx 1GBE (Slot x) Network Status window, each of your Ethernet ports will be listed, along with their status.



To view the network information for each port, click on the information icon.

To edit the network information, click on the gear icon.

xxxx 1GBE (Slot x) Edit Interface Settings: eth* Window

Add your network information in the following fields to edit or add network information to an Ethernet port. (Some selections will reveal or hide additional fields).

General Status tab:

- Enable Interface [checkbox]
- Auto-connect [checkbox]
- MTU (0=auto)

IPv4 Status tab

- Enable DHCP [checkbox]
- Address
- Subnet Mask
- Gateway
- Ignore Auto DNS? [checkbox]
- Ignore Auto Routes? [checkbox]
- Primary DNS
- Secondary DNS

IPv6 Status tab

- Enable DHCP [checkbox]
- Address
- Subnet prefix
- Gateway
- Ignore Auto DNS? [checkbox]
- Ignore Auto Routes? [checkbox]
- Primary DNS
- Secondary DNS

NTP

To configure NTP on this set of option cards, navigate to MANAGEMENT > NTP Setup.

In the Actions panel, select the Configure xxxx 1GBE (Slot x) button.

In the xxxx 1GBE (Slot x) NTP Status window are four tabs:

In the **General Status** tab:

- Enable or disable NTP
- Enter Symmetric Keys
- Enter Access Restrictions

In the **Ref-Clocks** tab:

- The phc0 of your host unit will be listed (the time reference provided to the card)

In the **Servers** tab:

- View a list of configured servers and click Edit Servers to add or edit them.
- In the NTP Servers window, click on the plus sign to add additional servers by entering information into the following fields:
  - Host
  - Min Poll Interval
  - Max Poll Interval
  - Symmetric Key
  - Enable Burst [checkbox]

- Enable Iburst [checkbox]
- Mark ad Preferred [checkbox]

In the **Peers** tab:

- View a list of configured peers and click Edit Peers to add or edit them.
- In the NTP Peers window, click on the plus sign to add additional servers by entering information into the following fields:
  - Host
  - Min Poll Interval
  - Max Poll Interval
  - Symmetric Key
  - Enable Burst [checkbox]
  - Enable Iburst [checkbox]
  - Mark ad Preferred [checkbox]



5.2.6.2 White Rabbit Option Cards (WROX) [1204-58, -59]

The White Rabbit Option 1204-58 and -59 cards provide (4) x Output interfaces to the SecureSync 2400. All four SFP ports can serve as a PTP, NTP, or WR master, or a PTP or WR slave, to distribute time through high-speed networks.

The WROX card management functionality operates independently of the SecureSync 2400 and is conducted through CLI commands via the console or through SSH.

WROX 10 Gb [-59]: Specifications

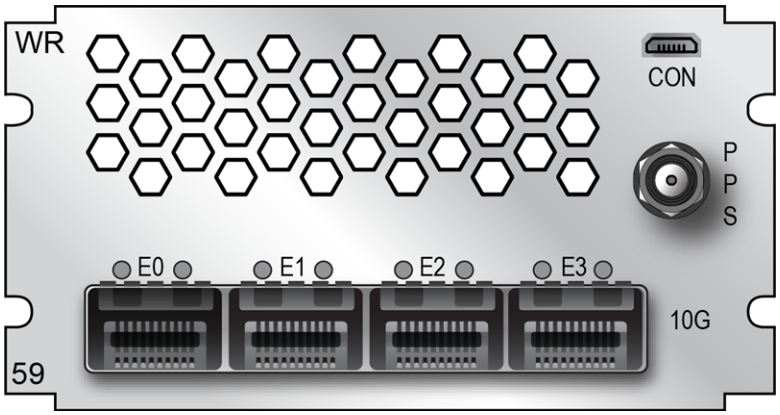


Figure 5-59: 1204-59 option card rear plate

Interfaces:	(4) 10 Gb Ethernet	(1) PPS OUT	Serial Console
Connectors:	(4) SFP+ (Eth0-Eth3)	SMA (3.3 V)	micro-USB
Notes:	Layer 2 and Layer 3 protocol capable. SSH communication.	less than 5ns rise time	management port

- **Management**: Serial Console management port. Following initial network setup, management on Eth0-Eth3 via SSH.
- **Maximum Number of Cards**: 2
- **Unit Restriction**: SecureSync 2400 six-slot capable base unit (2406-xyz). This option card is not backward-compatible and should only be installed in a SecureSync 2400 (NOT a SecureSync 1200).
- **Slot Restriction**: Double-high slot occupation, limited to slots 3 & 4 and/or slots 5 & 6.
- **Ordering Information**: 1204-59: WROX 10 Gb

Supported SFPs

The following 10 Gb SFP+s have been tested with the **-59 card**:

- Avago AFBR-710SMZ, Unidirectional fiber, PTP, 10 G, 400 m, MM
- Coherent FTLX8574D3BCL, Unidirectional fiber, PTP, 10 G, 300 m, MM, available from Safran as SFP-PLUS-FIBER-MM

- Fiberstore SFP-10G-BX #36351, Bidirectional fiber, WR & PTP, 10 G, 10 km, SM
- Fiberstore SFP-10G-BX #36353, Bidirectional fiber, WR & PTP, 10 G, 10 km, SM

WROX 1 Gb [-58]: Specifications

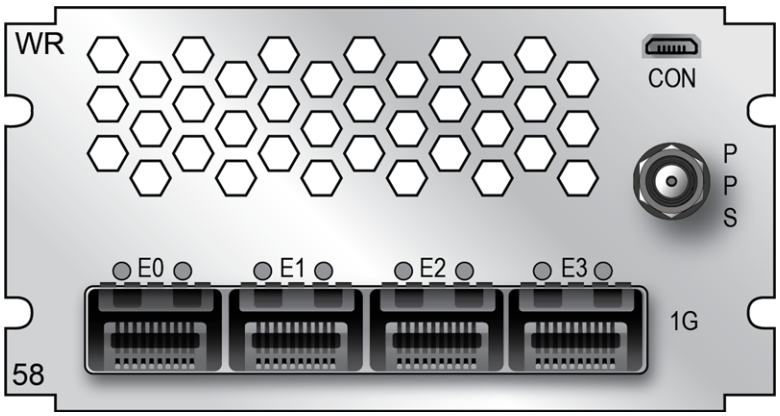


Figure 5-60: 1204-58 option card rear plate

Interfaces:	(4) 1 Gb Ethernet	(1) PPS OUT	Serial Console
Connectors:	(4) SFP (Eth0-Eth3)	SMA (3.3 V)	micro-USB
Notes:	Layer 2 and Layer 3 protocol capable. SSH communication.	less than 5ns rise time	management port

- **Management**: Serial Console management port. Following initial network setup, management on Eth0-Eth3 via SSH.
- **Maximum Number of Cards**: 2
- **Unit Restriction**: SecureSync 2400 six-slot capable base unit (2406-xyz). This option card is not backward-compatible and should only be installed in a SecureSync 2400 (NOT a SecureSync 1200).
- **Slot Restriction**: Double-high slot occupation, limited to slots 3 & 4 and/or slots 5 & 6.
- **Ordering Information**: 1204-58: WROX 1 Gb

Supported SFPs

The following 1 Gb SFPs have been tested with the **-58 card**:

- Avago AFBR-5710LZ, Unidirectional fiber, PTP, 1 G, 550 m, MM (available from Safran as SFP-FIBER-MM)
- Axcen AXGD-3454-0531, Bidirectional fiber, WR & PTP, 1 G, 10 km, SF
- Axcen AXGD-1254-0531, Bidirectional fiber, WR & PTP, 1 G, 10 km, SF
- Finisar FCLF8522P2BTL, Copper, PTP, 1 G, ≥100 m, RJ45 (available from Safran as SFP-COPPER)
- Molex 183702-2037, Unidirectional fiber, PTP, 1 G, 550 m, MM

Included in this Shipment

(1) WROX card (either 1204-58 or 1204-59), pre-installed if ordered with SecureSync 2400 unit

(4) SFP modules, pre-installed if ordered

(1) Micro-USB to USB cable for Console communication

Setup

Information on the hardware connections and network configuration of your SecureSync 2400 can be found in the main user manual: safran-navigation-timing.com/manuals/2400.

The setup of your WROX card uses a different software and method. **Initial communication** with a WROX card must be done through the micro-USB port on the card itself:

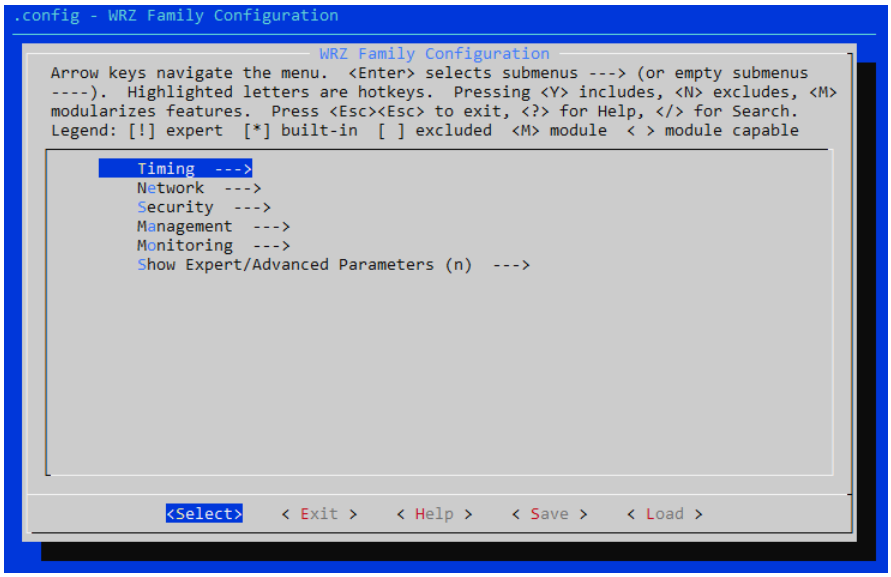
1. Connect the provided micro-USB to USB cable to the faceplate of the WROX card and the USB connector to a computer using a terminal emulator (115200 baud rate). Also connect (at least) one Ethernet port to a network.
2. Log in to the unit using the **default credentials**:

   ```
   Username: root

   Password: root
   ```

   You will be prompted to change your default password. (If you choose to update your password, this must be done through the CLI, as the WROX card does not yet have a user interface).

3. Issue the CLI command **wrz_config** to bring up a list of common actions necessary for configuration of this card:

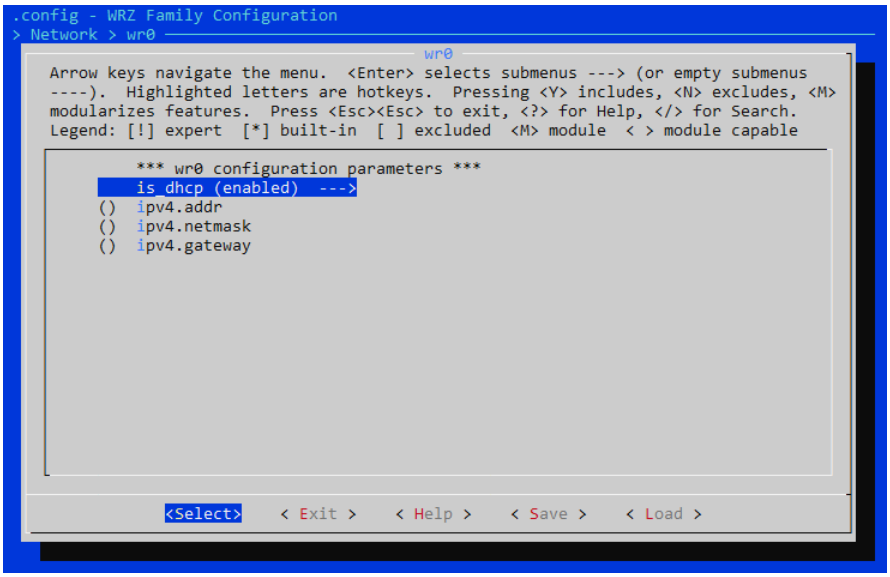


> **Note:** The `wrz_config` command is a robust tool originated from our WR-ZEN and WR-Z16 products. Not all functions of the wrz_config tool currently apply to the WROX card.

4. To **enable DHCP**, or to **assign a static address** for a specific Ethernet port, use the wrz_config tool.

> **Note:** Eth3 has DHCP enabled by default; Eth0-Eth2 have DHCP disabled.

Within wrz_config, navigate to **Network > [selected interface]**. From this page, you can enable DHCP for Eth0-Eth2, or configure a static IP:



5. To apply any configuration changes to the WROX card, you must **reboot** the unit.
   - » Exit the wrz_config tool using the on-screen prompts
   - » Issue the `reboot` command

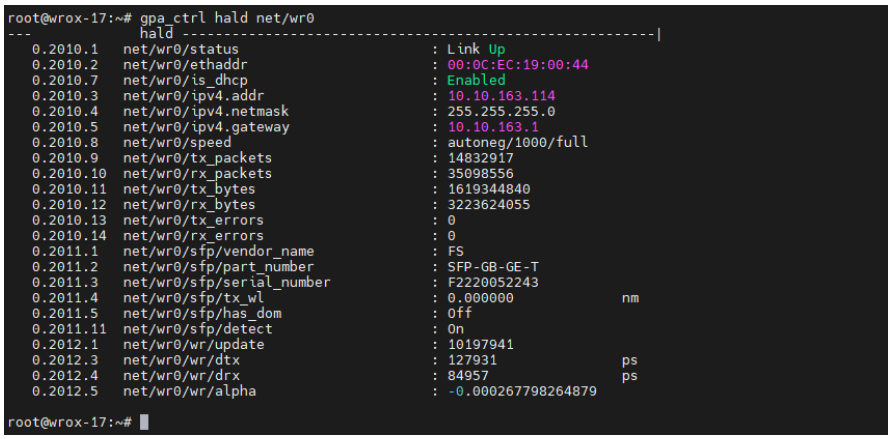
   The reboot in this context will only reboot your WROX card, not the SecureSync 2400.

   The card will flash red on all LEDs to indicate a reboot is taking place.

6. Once your card is fully rebooted, log in again. You can **identify the IP addresses** of your WROX Ethernet ports by exiting the wrz_config tool and issuing the `ip a` command.

   Note: The Eth0-Eth3 ports are listed as wr0-wr3 within the WROX card CLI commands.

   (The `gpa_ctrl` command is a robust tool that can also be used to identify the IP address of your ports. This tool can also identify the MAC address of each port for use with Layer 2 protocol. To do so, issue the `gpa_ctrl hald net/[interface]` command, using wr0-wr3 as your selected interface.



SSH Management

Once you have identified the IP address of an Ethernet port, you may choose how to interact with your unit to perform the rest of your setup and communication. You can continue using the management port, or you can also SSH into any of the Ethernet ports using the IP address.

Common CLI commands

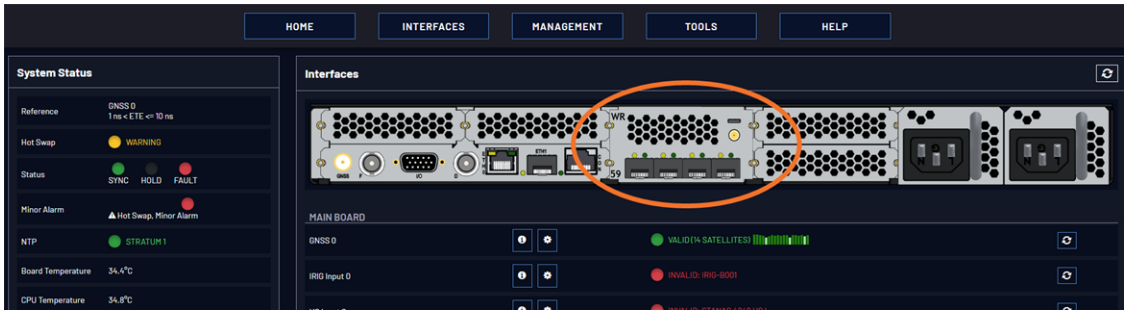
- **wrz_config**: a tool used to perform most setup functionality for the WROX
  - **wrz_config -f** can be used to perform a factory reset
- **wrz_flashfw**: tool used to flash uploaded firmware.
- **wrz_ip_rule**: management of user-defined rule configuration.
- **wrz_ip_route**: management of user-defined route configuration.
- **wrz_logdump**: tool that creates a log file for analysis by the support team.
- **wrz_set_sysctl**: set kernel attributes related to IPv4 ARP messages.
- **gpa_ctrl**: a tool used to identify metrics. Use the command without arguments to list all the parameters of the WRZ-OS. Specify some arguments to modify usage: `gpa_ctrl [OPTIONS] [<module_name> [<path> [<write_val>]]]`
- **ip a**: identify the networking information for your Ethernet ports
- **ip rule**: rule management

- **ip route**: routing management
- **reboot**: reboot the WROX card (necessary to implement all configuration changes).

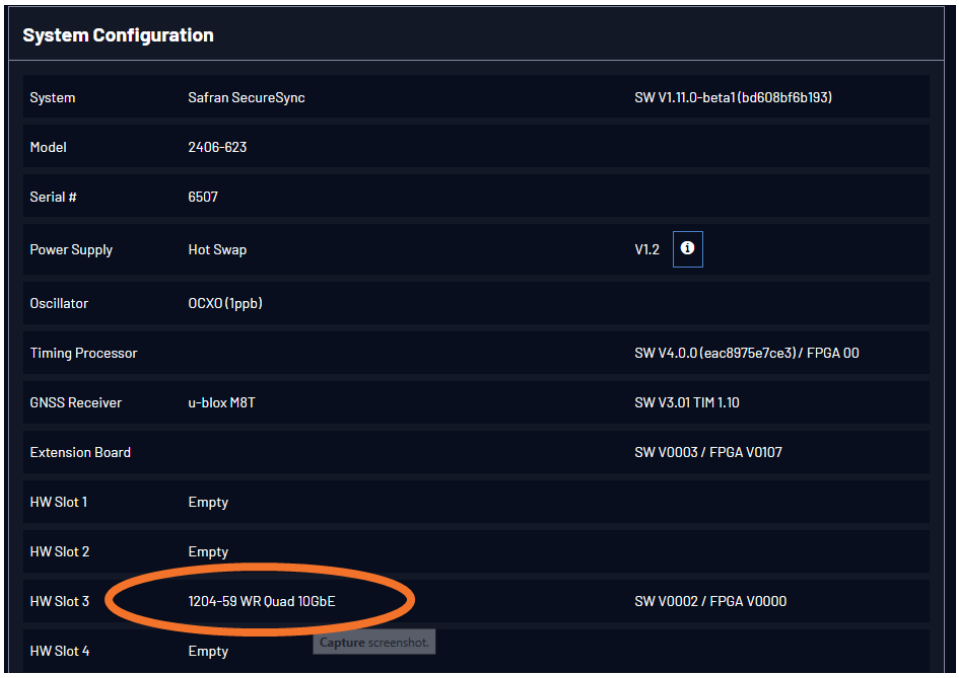
WROX Card in a SecureSync 2400

The SecureSync 2400 does not currently directly manage the WROX cards, but it is possible to confirm that your SecureSync 2400 registers the cards via the Web UI.

Navigate to Interfaces > Option Cards to see an image of the WROX card on your unit:



The WROX cards will also appear in the Tools > SYSTEM > Upgrade Backup system configuration list:



However, you cannot access a menu for configuration or to view the status of the WROX cards via the SecureSync 2400 Web UI at this time.

Finally, if your unit has Slave functionality configured, the SecureSync 2400 will identify WROX card references in the Input/References menus, as below:



Configuration Management

In order to configure PTP, NTP, or WR on one of your Ethernet interfaces on a WROX card, you will need to configure a **preset** timing profile.

Master-only units will use GM or Custom profiles, and cards that are also configured as Slaves in WR or PTP will use the BC (Boundary Clock) presets

To set your timing profile and allow the WROX card to function as desired:

1. Enter the `wrz_config` command, and navigate to Timing > General.
2. Make your selection from the following list of presets:
   - **BC: wr0 | WR** will configure your Eth0 as a White Rabbit slave and Eth1-Eth3 as WR masters.
   - **GM: ext GNSS | WR** will configure your Eth0-Eth3 ports as White Rabbit masters.
   - **GM: ext GNSS | PTP** will configure your Eth0-Eth3 ports as PTP masters.
   - **BC: wr0->wr1 | WR** will configure your Eth0 as a White Rabbit slave, Eth1 as the next White Rabbit source if Eth0 fails, and Eth2-Eth3 as WR masters.
   - **BC: wr0 | PTP** will configure your Eth0 as a White Rabbit slave and Eth1-Eth3 as PTP masters.
   - **BC: wr0->wr1 | PTP** will configure your Eth0 as a White Rabbit slave, Eth1 as the next White Rabbit source if Eth0 fails, and Eth2-Eth3 as PTP masters.
   - **BC: wr0->wr1 (PTP) | PTP** will configure your Eth0 as a PTP slave, Eth1 as the next PTP source if Eth0 fails, and Eth2-Eth3 as PTP masters.
   - **Custom**: Preset used to create and save custom configurations different from defined presets.
   - **BC: wr0 (PTP) | PTP** will configure your Eth0 as a PTP slave and Eth1-Eth3 as PTP masters.
   - **GM: ext GNSS | NTP** will configure your Eth0-Eth3 ports to NTP.
3. You may then adjust the protocol-specific settings for PTP, WR, and NTP (see next sections).
4. Once your preset it configured, the changes will NOT take effect until you issue the `reboot` command. Exit the wrz_config tool; you will be prompted

to save your configuration changes; then, issue reboot. (If you have several configuration changes to make, it is okay to wait until they have all been set to reboot your unit).

PTP

Specifications

Configuration: PTP Master or Slave; available on (4) x Ethernet ports (Eth0-Eth3).

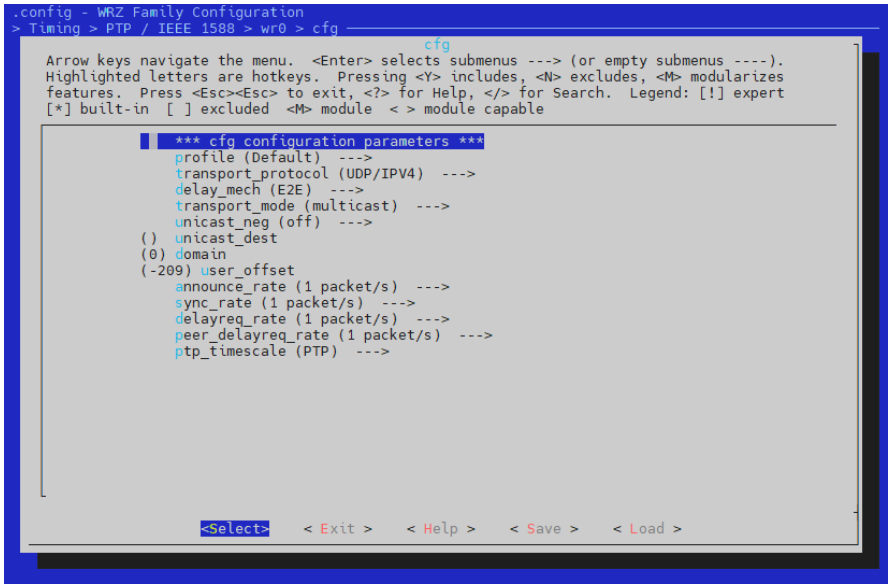
Profiles: Default, Custom, 61850-9-3 Power Profile, C37.238-2017 Power Profile, G.8265.1 Telecom Profile.

PTP Setup

PTP configuration on the WROX cards is conducted through the `wrz_config` CLI tool.

1. Enter the `wrz_config` command, and navigate to Timing > PTP / IEEE 1588.
2. Select the interface you wish to configure (wr0-wr3 as corresponds to Eth0-Eth3 on the WROX card faceplate). Choose cfg and then make your selection from the following list of desired parameters:
   - profile
   - transport_protocol
   - delay_mech
   - transport_mode
   - unicast_neg
   - unicast_dest
   - domain
   - user_offset
   - announce_rate
   - sync_rate
   - delayreq_rate

- peer_delayreq_rate
- ptp_timescale



3. Once your PTP commands are configured, they will NOT take effect until you issue the `reboot` command. Exit the wrz_config tool; you will be prompted to save your configuration changes; then, issue reboot.

NTP

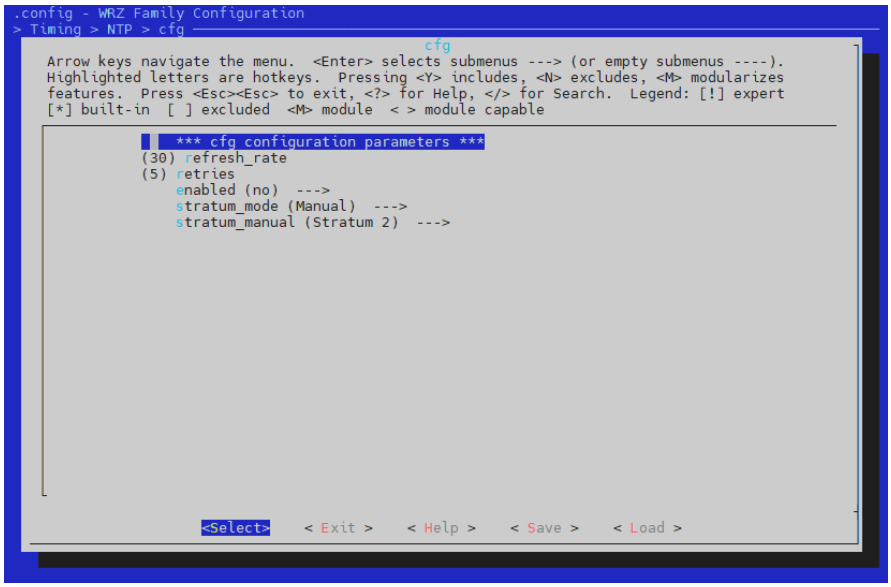
Specifications

Configuration: NTP Master-only; available on (4) x Ethernet ports (Eth0-Eth3).

NTP Configuration

A small amount of NTP configuration on the WROX card is conducted through the `wrz_config` CLI tool.

1. Enter the `wrz_config` command, and navigate to Timing > NTP > cfg.
2. From here, you can edit the available NTP settings.



3. Once your NTP commands are configured, they will NOT take effect until you issue the `reboot` command. Exit the wrz_config tool; you will be prompted to save your configuration changes; then, issue reboot.

The NTP service, chrony, is directly modifiable by editing the configuration file to access the full feature set (symmetric keys, access restrictions, etc.) included with the linux package. Doing this is considered enabling expert mode where not all NTP chrony configurations have been tested and validated on the WROX cards.

To edit the NTP config file:

1. Modify the config file through the CLI by either editing the existing conf file for chrony, found at `/etc/chrony/chrony.conf`, or uploading your own file.
2. The ntp daemon will then need to be reloaded to apply the configuration changes. You can do this by restarting the tmgrd service:

   ```
   gpa_ctrl tmgrd cfg/update_config 1
   ```

3. This method will not persist between reboots unless you also modify or upload the ntp Chrony file at `/media/data/usr/local/etc/chrony/chrony.conf`

White Rabbit Protocol (WR)

Specifications

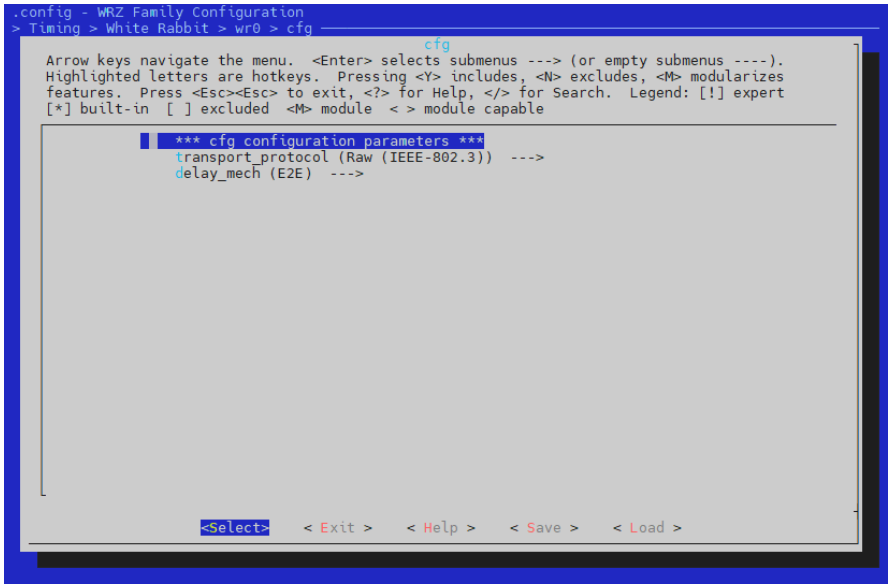
Configuration: WR Master or Slave; available on (4) x Ethernet ports (Eth0-Eth3).

> **Note:** 10G White Rabbit is in beta with limited functionality available.

WR Setup

WR configuration on the WROX cards is conducted through the `wrz_config` CLI tool.

1. Enter the `wrz_config` command, navigate to Timing > General and select the `GM: ext GNSS | WR` preset, and then navigate to Timing > White Rabbit.
2. Select the interface you wish to configure (wr0-wr3 as corresponds to Eth0-Eth3 on the WROX card faceplate). Choose cfg and then make your selections from the list of desired parameters.

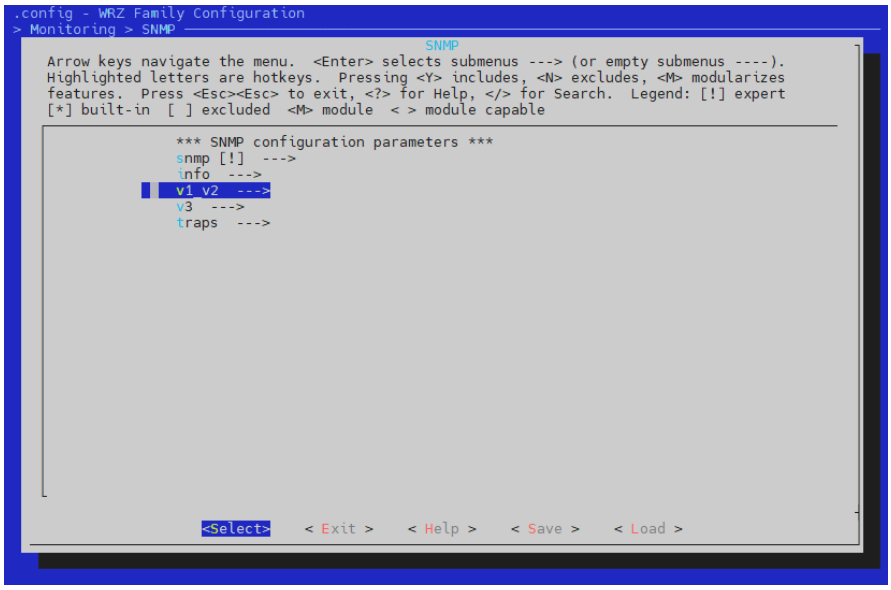


3. Once your WR commands are configured, they will NOT take effect until you issue the `reboot` command. Exit the wrz_config tool; you will be prompted to save your configuration changes; then, issue reboot.

SNMP

SNMP functionality is configured through the `wrz_config` CLI command.

1. Run the `wrz_config` command. Navigate to Show Expert/Advanced Parameters and select (y).
2. Navigate to Monitoring > SNMP > snmp [!]. Select show_experts, and select (y).
3. Still within the `wrz_config` tool, navigate to Monitoring > SNMP, and configure your v1/v2, v3, or traps settings to your specifications.



4. Select Exit unit you are prompted to save your configuration changes; once you have exited the `wrz_config` tool, you must `reboot` your WROX card for the changes to take effect.

Upgrades

In order to upgrade your WROX card, you must first obtain an upgrade file from Safran. Then,

1. Using SCP/SFTP, send the tarball to the device root folder.
2. Execute `wrz_flashfw <firmware_tarball>`
3. When prompted, issue the `reboot` command to reboot the card.

5.2.6.3 PTP Grandmaster [1204-32]

> **Note:** These instructions refer only to the PTP available directly through an installed 1204-32 Grandmaster PTP option card.
>
> The on-unit PTP has different specifications. See "Configuring PTP" on page 155 for more information.

Precision Time Protocol (PTP) is a protocol that can be used to synchronize computers on an Ethernet network. The Precision Time Protocol (PTP) option module supports PTP Version 2, as specified in the IEEE 1588-2008 standard (PTP Version 1 is not supported), via one (1) Ethernet port.

The PTP option module implements a PTP Ordinary Clock that can be configured to run as a Master Clock only. It transmits PTP packets via the Ethernet port, with information about the current time and synchronization reference selected by the SecureSync device.

PTP Grandmaster [-32]: Specifications

- **Inputs/Outputs**: (1) Configurable as Input or Output
- **Signal Type and Connector**: Ethernet via SFP, and 1PPS Output via BNC
- **Management**: Web UI
- **Resolution**: 8ns (±4ns) packet time stamping resolution
- **Accuracy**: 30 ns accuracy (3σ) Master to Slave, via crossover cable
- **Network Speeds**: 100 Mb/s, or 1Gb/s, depending on SFP module used
- **PTP Version** supported: PTP 2 (IEEE 1588-2008)
- **PTP Profiles** supported: Default, Telecom, Enterprise
- **Transmission modes**: Unicast [default], Multicast
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-32: PTP/Precision Timing Protocol Option Module

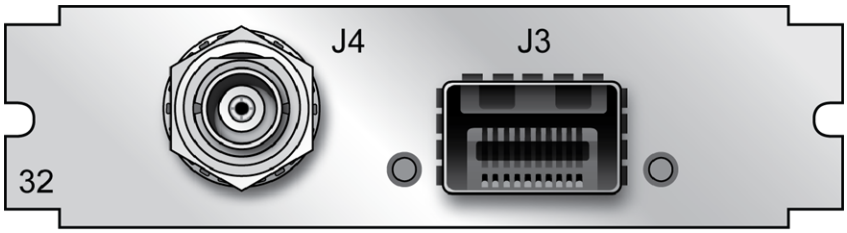


Figure 5-61: Model 1204-32 option card rear plate

Supported SFPs

Arista SFP-1G-T

Avago AFBR-5710LZ

Avago AFBR-57M5APZ

Bel Fuse SFP-1GBT-05

CISCO MGBSX1

CISCO GLC-T

Finisair FTLF1318P3BTL

Finisair FTRJ8519P1BNL

Finisair FTLF8519P3BNL

Finisar FCLF8522P2BTL (available from Safran as **SFP-COPPER**)

Omitron 7206-0

Optorate S.1312.10.D

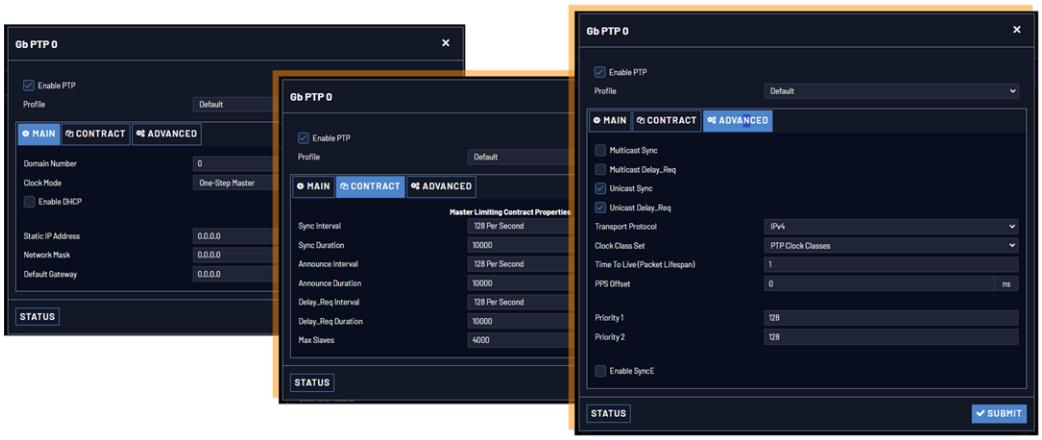
Proline SFP-TX-CDW

PTP Grandmaster [-32]: Edit Window

1. To configure this option card, go to its **Edit** window. For instructions, see "Configuring Option Card Inputs/Outputs" on page 386.

> **Note:** If you have only one input or output of any type, SecureSync will number that input or output 0. Additional inputs or outputs will be numbered 1 or above.

2. The **Gb PTP Edit window** will display. It includes the **top panel**, and offers access to three different **tabs**, described below:



Top panel settings

- **Enable PTP**: Enables/Disables PTP. Check the box to enable PTP. Uncheck it to disable PTP.
- **Profile**: offers a choice of:
  - Default (incl. Enterprise)
  - Telecom

Bottom panel: tabs

- **Main**: These settings pertain to network connectivity.
- **Contract**: These settings pertain to the unicast contract.
- **Advanced**: These setting pertain to time Sync information.

Main tab settings

- **Domain Number**: Sets the current PTP Domain Number, as defined in IEEE Std 1588-2008 Section 7.1
- **Clock Mode**: PTP has two ways to transmit the initial T1 timestamp of the Sync packet transmission from the Master to the Slave:

- **One-Step** Master: The Sync packet is timestamped, then the timestamp is inserted into the Sync packet in real-time, as it is transmitted.
- **Two-Step Master**: The Sync packet is timestamped, but the timestamp value in the Sync packet is ignored. The actual T1 value is transmitted in a "Follow-Up" packet after the Sync packet.



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

- **Enable DHCP**: This is a checkbox to enable or disable the delivery of IP addresses from a DHCP Server. The default setting is enabled (the box is checked).
- **Static IP Address**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this IP address. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].
- **Network Mask**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this Network Mask. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].
- **Default Gateway**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this Default Gateway. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].

Contract tab settings



Note: The settings under this tab only apply to Unicast mode.

[Default settings in parenthesis]

- **Min Sync Interval**: The minimum value of Sync interval granted by the Master Clock. In packets per second. [128 Per Second]

- **Max Sync Duration**: The maximum value of Sync interval granted by the Master Clock. In seconds. [10000]
- **Min Announce Interval**: The minimum value of the Announce interval granted by the Master Clock. In packets per second. [128 Per Second
- **Max Announce Duration**: The maximum value of the Announce interval granted by the Master Clock. In seconds. [10000]
- **Min Delay_Req Interval**: In packets per second. [128 Per Second]
- **Max Delay_Req Duration**: In seconds. [10000]
- **Max Slaves**: The maximum number of slaves the card will serve. [4000]

Advanced tab settings

About... PTP Transmission Modes

The PTP Card is able to transmit the PTP packets in three transmission modes:

• **Multicast Mode**: PTP packets are transmitted to all PTP Clocks by means of Multicast IP addresses dedicated to the PTP protocol (224.0.1.129, 224.0.0.107). PTP packets received by the PTP Clocks are then filtered from the Domain Number, the Port Identity (Clock Identity + Port Number) of the transmitter, the packet identifier (Sequenced). When the Master Clock is set in Multicast mode, this module will deny the requests from the Slaves Clocks to run in Unicast mode. When the Master Clock is set in Unicast mode, it doesn't transmit any PTP messages until a Slave has been granted to run in Unicast mode.

• **Unicast Mode**: This mode is enabled by default. This is a Point-to-Point transmission mode between two PTP Clocks by means of the unique IP address assigned to each PTP Clock.

N O T E: The Unicast mode is only implemented for the following PTP packets:

Announce, **Sync** and **Follow-Up**, **Delay_Req** and **Delay_Resp**.

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

_____

• **Minicast/Hybrid Mode**: The Minicast/Hybrid mode is a method to minimize the PTP packets payload on the network, where: The transmissions initiated by the Master (Announce, Sync/Follow-Up) run in Multicast mode.

The transmissions initiated by the Slaves (Delay_Req/Delay_Resp) run in Unicast mode.

- **Multicast Sync**: Activating this option will cause the PTP Master to broadcast Sync and Announce messages to the Multicast address (as long as it is the Best Master on the network). Deactivating this option will remove the messages. When the PTP module is set in multicast mode, this will deny the requests from the Slaves Clocks to running in unicast mode.
  - Checking this box will cause two additional fields to display that will allow you to configure the:
    - Multicast Sync Rate
    - Multicast Announce Rate
- **Multicast Delay_Req**: Activating this option will cause the PTP Master to respond to multicast Delay Requests (as long as it is the Best Master on the network). Deactivating this option will prevent the Master from responding to these.
- **Unicast Sync**: The PTP Master will always respond to attempts from Unicast slaves to communicate with it, provided the Slaves use the proper Unicast Auto-Negotiation process. This setting is always enabled.
- **Unicast Delay_Req**: The PTP Master will always respond to attempts from Unicast slaves to communicate with it, provided the Slaves use the proper Unicast Auto-Negotiation process. This setting is always enabled.
- **Transport Protocol**: Selects the transport protocol used for PTP packets.

- **Clock Class Set**: Parameter broadcast in a PTP profile, indicating the quality of the attached reference; PTP [default], ARB, ITU [Telecom[1]]. See also "ESMC Signal Control" below.
- **Time To Live (Packet Lifespan)**: Sets the TTL field for PTP packets except for Peer-to-Peer packets for which TTL is forced to 1 as specified in IEEE Std 1588-2008 Annex D.3.
- **1PPS Offset**: The 1PPS signal of this option card can be offset from the main System 1PPS. This offset will be applied to all timestamps created by this card. It can be set in 8ns increments. Range is -500 ms to +500 ms.
- **Priority 1**: See IEEE 1588-2008, Section 8.10.1, 8.10.2.
- **Priority 2**: See IEEE 1588-2008, Section 8.10.1, 8.10.2.
- **Enable SyncE**: If checked, allows access to the synchronous Ethernet settings. There will always be an ESMC message broadcast if Enable SyncE is checked.



Note: For full functionality, SyncE requires Fiber Optic SFP modules. Standard RJ45/ 1000BASE-T modules are generally not compatible with SyncE.

  - **Enable ESMC**: [checkbox]
    - **ESMC Signal Control**: Determines which SSM to use in the ESMC message. One of two messages will be broadcast: either the message selected in the SSM Code dropdown or the QL_DNU code. The user may set one of the following broadcasting options:
      - **Output Always Enabled**: Always broadcasts the selected SSM code, even when SecureSync is not synchronized to its references.

[1]The Telecom profile uses different clock class values than the default profile. It uses clock classes in the range from 80 to 110, and these values map to the SSM Quality level that is broadcast in the ESMC message, as defined in Section 6.7.3.1 of G8265.1. If the user enables Sync-E, and broadcasting of the ESMC message, the parameter that controls which SSM quality level is broadcast when the unit is in sync is user-accessible. This will appear both in the ESMC message, and in the Clock Class (if the “Clock Class Set” is set to ITU). It is also possible to control whether the ESMC message chosen degrades to QL-DNU when out of sync.

- **Output Enabled in Holdover**: The output uses the selected SSM code unless SecureSync is not synchronized to its references (the output is present while in the Holdover mode). While SecureSync is not synchronized, QL-DNU SSM code will be broadcast.
- **Output Disabled in Holdover**: The output uses the selected SSM code unless the SecureSync references are considered not qualified and invalid (the output is not present while in the Holdover mode). While references are invalid, QL-DNU SSM code will be broadcast.
- **Output Always Disabled**: The output is not present, even if any SecureSync references are present and considered qualified. QL-DNU SSM code is broadcast.

- **SSM Code**: The Sync Status Messaging (SSM) code to be used. Choice of code is made through the drop-down list.

> **Note:** Note: Some parameters define a PTP packet's throughput. They use the "log2seconds", defined as follows.

  - Positive Value: n => 2n seconds between two successive PTP packets
  - Negative Value: -n => 2(-n) = (1/2n) => 2n PTP packets per second

PTP Grandmaster [-32]: Status Window

To view the status of a PTP interface, go to its Status window. For instructions, see "Viewing Input/Output Configuration Settings" on page 385.



The **GB PTP** Status window contains two tabs: Main and Advanced.

Main tab: Status information

- **Ethernet Status**: Whether the module is connected to a network through Ethernet.
  - **Green**=Connected. The speed of the connection is indicated.
  - **Orange**=Not connected.
- **Port State**: Reports the current state of the PTP State Machine:
  - **Disabled**: PTP Ethernet port is Disabled. See PTP Setup/Network page, PTP Network Settings options.
  - **Initializing**: Ethernet link is unplugged/PTP Module is in power-up state. A Master Clock doesn't leave this state while it can't get the current time and synchronization references from the SecureSync to synchronize with it.
  - **Listening**: PTP module is looking for a Master Clock.
  - **Master**: PTP Master has become the active Master Clock on the network.
  - **Passive**: PTP Module has become a Passive Master Clock. (There is another Master Clock on the network with better quality or higher priority). This Master will wait until the Best Master Clock Algorithm determines it should become the best Master Clock, and then it will transition to the Master Clock state.
  - **Uncalibrated**: PTP Slave has selected a Master Clock on the network attempts to synchronize with it using sync packets.
- **Number of Unicast Slaves**: Number of PTP Slaves that have been granted by the PTP Master to run in unicast mode (maximum = 4000 unicast contracts)
- **Profile**: Whether the profile is the default or Telecom.
- **Domain Number**: The current PTP Domain Number.
- **Clock Mode**: See "Main tab settings" on page 536.
- **Current IP Address**: The IP address currently being used by the PTP interface.
- **MAC Address**: The MAC address currently being used by the PTP interface.

Advanced tab: Status information

Time Properties:

- **UTC Offset**: The Master's current offset between UTC time and TAI time. Units: seconds.
- **UTC Offset Valid**: Indicates whether or not the Master's UTC Offset is valid.
- **Leap Second**: The Leap second correction as set on the **Time Management** page.
- **Time Traceable**: Indicates whether the Master's time is traceable (Enabled) to a primary reference or not (Disabled).
- **Frequency Traceable**: Indicates whether the Master's Frequency is traceable (Enabled) to a primary reference or not (Disabled).
- **PTP Time Scale**: Indicates the timescale that the Master is using to broadcast its time. TAI is the default PTP timescale.
- **Time source**: The Time Source that the Master is using. Refer to IEEE Standard 1588-2008, Section 7.6.2.6.

Clock Quality:

- **Clock Accuracy**: A number describing the accuracy of the oscillator in the Master relative to its UTC reference (see IEEE Standard 1588-2008, Section 7.6.2.5).
- **Offset Scaled Variance**: A constant value based on the variance of the oscillator installed in the SecureSync unit.
- **Clock Class**: A number describing the state of the time and 1pps references of the PTP Clock.
  See table below for Clock Class definitions (see also: IEEE Standard 1588-2008, Section 7.6.2.4, Table 5).

Table 5-25: Clock class definitions

PTP Time Scale	Arbitrary Time Scale	Clock Class Definition
6	13	Time and 1pps references are synchronized with the host references and PTP clock shall not be a slave to another clock in the domain.
7	14	Time and 1pps references are in holdover state, within specifications and PTP clock shall not be a slave to another clock in the domain.

PTP Time Scale	Arbitrary Time Scale	Clock Class Definition
52	58	Time and 1pps references are in holdover state, not within specifications, and PTP clock shall not be a slave to another clock in the domain. Then, applied to Master Clocks who have just powered on and have not yet achieved a suitable TFOM value.
187	193	Time and 1pps references are in holdover state, not within specifications, and PTP clock may be a slave to another clock in the domain.
255	255	Class assigned to "Slave-Only" clocks.
248	248	"Unknown" class.

Ethernet Status

- **Current IP Address**: The IP address currently being used by the PTP interface.

> **Note:** If the PTP Module is set up for DHCP but fails to obtain an IP address, it will use the Static IP instead. To reacquire a DHCP address, reset the module via the Main tab in the PTP settings window.

- **Current Network Mask**: The Network Mask currently being used by the PTP interface.
- **Current Gateway**: The Gateway address currently being used by the PTP interface.

Port Status

- **Port State**: Reports the current state of the PTP State Machine:
  - **Disabled**: PTP Ethernet port is Disabled. See PTP Setup/Network page, PTP Network Settings options.
  - **Initializing**: Ethernet link is unplugged/PTP Module is in power-up state. A Master Clock doesn't leave this state while it can't get the current time and synchronization references from SecureSync to synchronize with it.
  - **Listening**: PTP module is looking for a Master Clock.

- **Master**: PTP Master has become the active Master Clock on the network.
- **Passive**: PTP Module has become a Passive Master Clock. (There is another Master Clock on the network with better quality or higher priority). This Master will wait until the Best Master Clock Algorithm determines it should become the best Master Clock, and then it will transition to the Master Clock state.
- **Uncalibrated**: PTP Slave has selected a Master Clock on the network attempts to synchronize with it using sync packets.
- **One Step Mode**: Determines the number of steps in the PTP protocol. Will be one of the following:
  - **Disabled**: Two-Step Mode is enabled
  - **Enabled**: One-Step Mode is enabled
    [Default=Disabled]



Note: One-Step Mode is not supported with the Peer-to-Peer Delay Mechanism.

The current implementation of One-Step Mode involves a software oriented timestamping. The Two-Step Mode imlements a hardware oriented timestamping, insensitive to software execution time variations. The Two-Step Mode is recommended, as it increases the PTP Clock's accuracy

- **Delay Mechanism**: Will be one of the following:
  - **E2E**: End-to-End Delay Mechanism
  - **P2P**: Peer-to-Peer Mechanism
  - **Disabled**: No Delay Mechanism
    Default setting: **E2E**

> **Note:** Peer-to-Peer Delay Mechanism is only applicable on networks equipped with Transparent Clocks (switches/routers IEEE 1588 compatible). Peer-to-Peer Delay Mechanism is not supported in Unicast transmission mode.

- **PPS Offset**: See "Advanced tab settings" on page 538.

Module Information

- **Software Version**: Version number of embedded software
- **Hardware Version:** Version number

Configuration — General Steps

- Ensure that SecureSync's PTP port is connected to the network (check the Link Status in the **PTP Status/Network** page).
- Ensure the PTP port speed is 100 Mb/s (see: **PTP Status** page > **Advanced** tab > **Port Speed**).
- Be sure that valid time and 1PPS references are currently selected (go to **MANAGEMENT/OTHER/Time Management**).

In order to operate properly as a Master Clock, SecureSync must be synchronized to a non-PTP reference. Confirm that the chosen reference transmits the following information (as reported by the Time Properties on the **PTP Status** page, under the **Advanced** tab):

- The proper TAI or UTC time (including the current year)
- The current TAI to UTC offset (required even if the reference's time is in TAI)
- Pending leap second information at least a day in advance.

If the reference does not transmit this information, it must be provided by the user in order for the Master Clock to function properly.

The built-in GNSS reference provides all information needed with no user intervention.

Configuration — PTP-Specific Steps

Confirm that:

- The PTP Port Activity is enabled (check the **Port Status** on the **PTP Status** page under the **Advanced** tab). If not, enable it from the **Port Activity** of the **PTP Setup/Network** page).
- The clock is set to be a Master-Only clock (check the **Clock Mode** on the **PTP Setup/Clock** page).
- A valid IP address is currently being used (check the **Ethernet Settings** on the **PTP Setup/Network** page).

When the PTP Module is set to be a Master Clock, the module will immediately attempt to become the active Master Clock on the network (**PTP Port State** = **Master**). If it does, it will start to transmit PTP packets (even if SecureSync is not yet synchronized).

There are several reasons why the PTP Module may not become the active Master Clock, or may not be broadcasting the correct time, even if it is set to be a Master Clock:

a. If using any reference other than self for 1PPS, SecureSync will not become an active Master Clock until the **Time Figure of Merit (TFOM)** value of the system is less than 15. After first going into sync after power-up, it may take a minute or two for the Time Figure of Merit (TFOM) value to fall to an acceptable level. The current Time Figure of Merit (TFOM) value is available in the Time Properties panel under the **Advanced** tab on the **Status** page.

b. PTP uses the TAI timescale to transfer time. Many timing references communicate time in the UTC timescale. UTC is offset from TAI by a small amount which changes every time a leap second occurs. The TAI to UTC Offset is part of the PTP Specification and must be provided to a Master Clock. If no active reference can provide that information, the offset must be provided by the Host. The TAI to UTC Offset can be set from the **MANAGEMENT/OTHER/Time Management** page (while setting the GPS to UTC Offset).

c. The PTP protocol also provides for the transfer of Leap Second information. If the active time reference does not provide Leap Second information, it must be added by the user through the **MANAGEMENT/OTHER/Time Management** page. If this is not done, the PTP network will have the incorrect UTC time after a leap second event.

d. If there are multiple multicast Master Clocks on the network, the PTP Module uses the Best Master Clock (BMC) algorithm specified in the PTP Specification to decide whether or not to become the active Master Clock. The BMC algorithm selects the Best Master Clock on the network from the following criteria:

   i. The BMC algorithm first selects the clock having the higher Priority1 parameter (a lowest value means a higher priority).

   ii. If the BMC cannot be determined from the previous parameter, the BMC algorithm selects the clock having the higher Clock Quality (Clock Class, Clock Accuracy, Clock Variance).

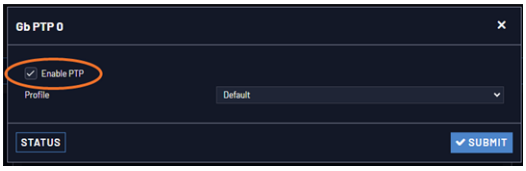
   iii. If the BMC cannot be determined from the previous parameters, the BMC algorithm selects the clock having the higher Priority2 parameter.

The Master Clock selected by the BMC algorithm as the Best Master Clock will transition into the Master state to become the active Master Clock on the network. It will then start to transmit Sync packets to the Slave Clocks. The other Master Clocks will transition into the Passive state.

Enabling PTP

To enable PTP:

1. Navigate to the Top panel of the GB PTP Edit window.
2. Check the **Enable PTP** box.

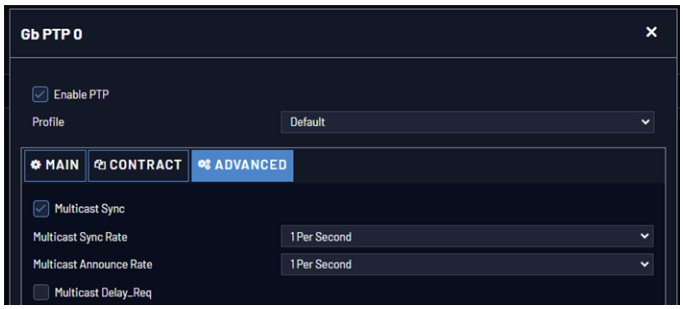


Configuring Multicast Mode

To enter Multicast mode, perform the following steps:

1. In the **GB PTP** Edit window, navigate to the **Advanced** tab.
2. Select the **Multicast Sync** checkbox.
3. Select the **Multicast Sync Rate** from the drop-down list.

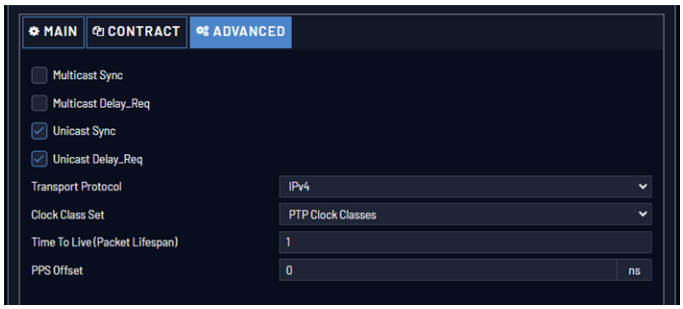
4. Select the **Multicast Announce Rate** from the drop-down list.



Configuring Unicast Mode

To enter the Unicast mode, perform the following steps:

1. In the GB PTP **Edit** window, navigate to the **Advanced** tab.
2. Confirm that **Unicast Sync** is checked. The 1204-32 PTP module should always respond to unicast negotiations.



Configuring Minicast/Hybrid Mode

To enter the Minicast/Hybrid mode, perform the following steps:

1. In the GB PTP Edit window, navigate to the **Advanced** tab.
2. Select the **Multicast Sync** checkbox.
3. Select the **Multicast Sync Rate** from the drop-down list.
4. Select the **Multicast Announce Rate** from the drop-down list.
5. Confirm that **Unicast Sync** is checked. The 1204-32 PTP module should always respond to unicast negotiations.

Configuring PTP on the Network

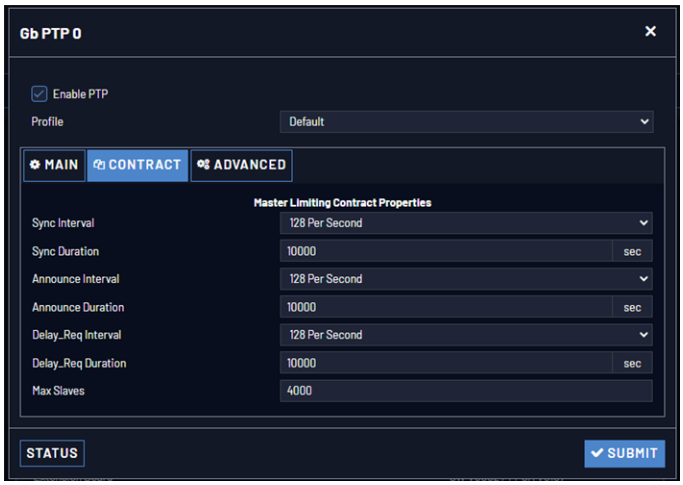
To configure PTP on the network:

1. In the GB PTP **Edit** window, navigate to the **Main** tab.
2. Under the **Main** tab of the **GB PTP** Edit window, make the following settings:
   - **Domain Number**: Sets the current PTP Domain Number, as defined in IEEE Std 1588-2008 Section 7.1
   - **Clock Mode**: See under "Main tab settings" on page 536.
   - **Enable DHCP**: This is a checkbox to enable or disable the delivery of IP addresses from a DHCP Server. The default setting is enabled (the box is checked).
   - **Static IP Address**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this IP address. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].
   - **Network Mask**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this Network Mask. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].
   - **Default Gateway**: When a DHCP server is not requested or is requested but not available, the PTP Module will use this Default Gateway. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].

Tip: VLAN encapsulation is not officially supported on the 1204-32 card and may cause error.

Configuring PTP Contracts

1. Navigate to the **Contract** tab of the **GB PTP** Edit window.



2. Under the **Contract** tab of the GB PTP Edit window, make the following settings:
   - **Min Sync Interval**: The minimum value of Sync interval granted by the Master Clock. In packets per second.
   - **Max Sync Duration**: The maximum value of Sync interval granted by the Master Clock. In seconds.
   - **Min Announce Interval**: The minimum value of the Announce interval granted by the Master Clock. In packets per second.
   - **Max Announce Duration**: The maximum value of the Announce interval granted by the Master Clock. In seconds.
   - **Min Delay_Req Interval**: In packets per second.
   - **Max Delay_Req Duration**: In seconds.
   - **Max Slaves**: The maximum number of slaves to be served. The 1204-32 module can serve up to 4000 slaves (unicast contracts).

5.2.7 Miscellaneous Option Cards

This section contains technical information and SecureSync Web UI procedures pertaining to option cards that do not fall into other categories, e.g. cards that serve as signal relays.

5.2.7.1 STL Option Module [1204-3E]

The Satelles **Satellite Time and Location** (STL) signal is broadcast on Iridium satellites and offers a spoofing-resilient encrypted signal that is 1000x stronger than GNSS-based timing signals. Hence, it is difficult to jam, and it can be received indoors.

STL is a subscription-based service. Please contact Safran for details.

A SecureSync equipped with the STL 1204-3E option card can be operated with or without GPS, depending on your application, i.e. STL can be utilized as a backup, or as the only external timing source.

Note: Devices are shipped with the STL subscription deactivated. It is necessary to contact customer service to activate the subscription: stlsubscription@nav-timing.safrangroup.com US: +1 585 321 5800; France: +33 (0)1 64 53 3980.

For subscription renewal information, see "Renewing Your STL Subscription" on page 558

Hardware Installation

1. If your STL option card was purchased together with a SecureSync unit, the card will be pre-installed in the unit. Proceed to Step 3.
2. If you purchased your STL option card separately, you will need to install the card into the SecureSyncunit. For instructions, see the hard copy of the **Option Card Installation Guide** that shipped with the unit, or see the **Field Installation** instructions in the user manual.

   Note: The -3E card can be installed in any free card slot.

3. Install the SecureSync unit in its assigned location e.g., in a server rack.
4. Install the supplied STL satellite antenna: The antenna is designed for indoor use. The ideal location for the antenna is near the ceiling of the room in which your SecureSync unit is located, or near an outside wall. In general, a higher location is preferable over a lower location. Do not cover the antenna with electronic equipment or other metal objects.

Note: The supplied antenna cable is 2.4 m (96") long. Longer cables are available upon request. The antenna does not require a separate power supply.

5. Connect the antenna cable to the SecureSync unit via the SMA connector on the option card -3E rear plate. The SecureSync can be in a powered off or a powered on state during antenna installation.

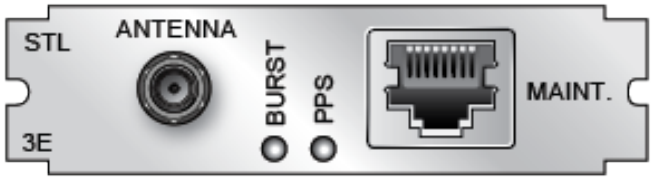


Figure 5-62: Model 1204-3E option card rear plate

» If the unit is ON, verify that the BURST lamp is blinking.

» If the unit is OFF, turn it on, and wait until the BURST lamp is blinking.

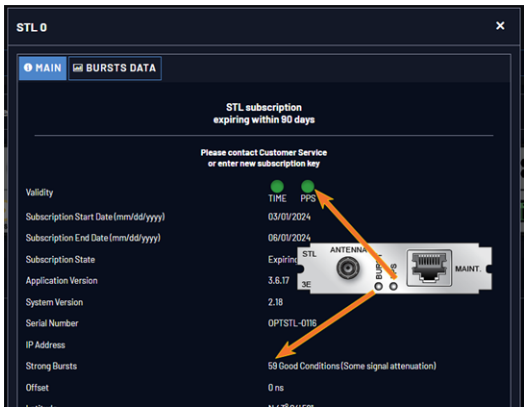
If the BURST lamp is not blinking **after the subscription has been activated**, the STL receiver is not receiving an STL signal. Check the antenna cable and its connections, and the antenna location. Move the antenna to another location (higher or closer to an outside wall).

Rear Plate LEDs:

BURST: Indicates the incoming STL burst rate. A high burst rate (desired) is indicated by the LED flashing quickly.

PPS: Indicates that the STL receiver is sending out a PPS signal to SecureSync. One (1) pulse per second means that the receiver is locked. NOTE: It can take approximately 10 minutes or longer until the receiver is locked. This depends on the burst rate (see "Burst Rate" on page 558.)

Both LEDs have equivalent indicators in the Web UI **STL 0** status window:



6. Proceed with the SW configuration of the STL settings, as described below.

> **Note:** The RJ-45 MAINT. connector will not be needed for the STL configuration. Use this connector only if so requested by Safran Service personnel.

Configuring STL Settings

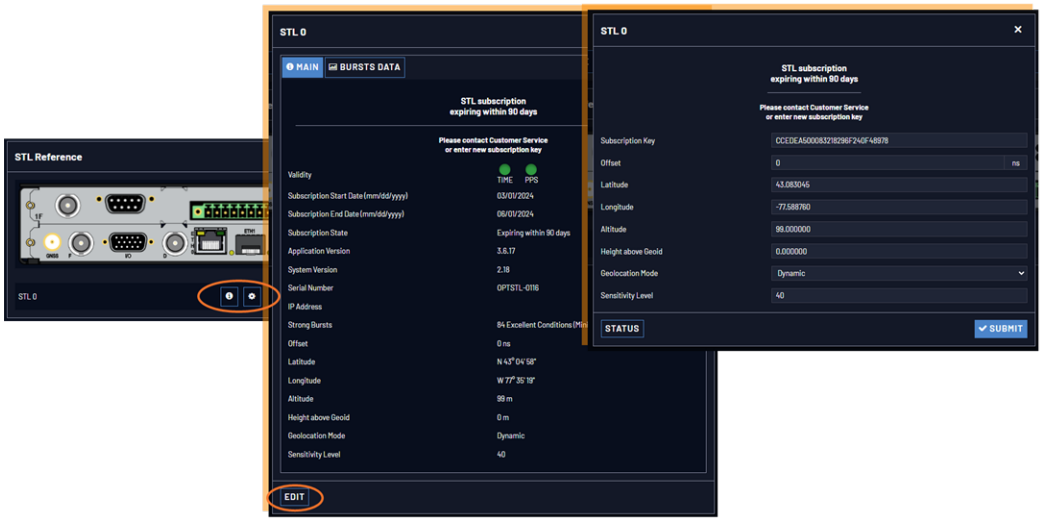
> **Note:** If you do not yet have a subscription key, you will need to obtain one before continuing with installation. Please contact Safran customer service:
> stlsubscription@nav-timing.safrangroup.com
> US: +1 585 321 5800; France: +33 (0)1 64 53 3980

> **Note:** During the initial installation of a unit equipped with an STL card, the exact geographic position needs to be entered into the Web UI (see below). Should the unit be relocated at a later point in time, the position must be changed accordingly.

The STL option card 1204-3E is configured via the SecureSync Web UI. See "The SecureSync Web UI" on page 35 for basic SecureSync setup and initial login information.

To configure STL settings:

1. Log into the Web UI, and navigate to **INTERFACES > OPTION CARDS: STL 0**. The **STL 0** status window will be displayed.
2. In the **STL 0** status window, click on the **Edit** button to open the **STL 0** setup window.



In the **STL 0** setup window, you can configure the following parameters:

- **Subscription Key**: [required] Enter the key obtained from customer service in order to activate STL access.
- **Latitude, Longitude, Altitude**: [decimal degrees, meters] Actual geographic position of SecureSync's STL antenna. For help determining your actual position, see "Determining Your Position" on page 258.
- **Geolocation Mode**: **Static Known Position/Static Unknown Position** [default]/**Pseudo Static/Dynamic**: This parameter refers to how the STL receiver handles position estimation. The default setting is recommended for most applications.
- **Sensitivity Level**: [default = 40] This value determines the sensitivity of the STL receiver towards the STL signal bursts transmitted by the satellites. The lower the number, the more responsive the receiver will be to acknowledge the bursts. The default value is optimized for an indoor antenna. A higher value can be used for outdoor antenna installations (not typical). A value lower than (40) is not recommended.

3. Assign the **STL 0** reference a reference priority by navigating to **MANAGEMENT > OTHER: Reference Priority**.
4. In the Configure Reference Priorities panel, click the **+** icon in the upper right corner. The **Add Reference** window will open.
5. Select a **Priority Level**:
   a. If STL is to be used as a backup to GPS: Select a **Priority Level** of **2**.
   b. If STL is the only reference: Select a **Priority Level** of **1**.

   For **Time** and **PPS**, select **STL 0**. Click Submit.
6. Verify your settings in the **Reference Priority** table, and ensure that the new reference is **Enabled**.

Reviewing the STL Status

Validity Status

To check or monitor the validity of the STL reference:

1. Navigate to **INTERFACES > REFERENCES**.
2. In the **References** status panel, under **STL 0**, check the status indicator light:



Detailed Status

To obtain detailed STL status information:

1. Navigate to **INTERFACES > REFERENCES: STL 0**. The **STL 0** status panel will be displayed.
2. In the **STL 0** status panel, click the INFO button. The **STL 0** status window

will open:



Besides STL system data, the window also displays STL validity and the subscription status. For a description of the other parameters, see "Configuring STL Settings" on page 554.

Subscription status reminder banner: Lists your current subscription state.

Validity – **TIME**: Should always be green; if red, the -3E card is not installed correctly, or there is a defect; – **PPS**: If green, indicates the STL receiver is sending a PPS signal to SecureSync.

Subscription Start Date, End Date: Day the STL subscription began and will end.

Application Version, System Version: Receiver software versions.

Serial Number: Receiver serial number.

IP address [button]: Maintenance port – opens a separate browser window indicating the IP address of the Maintenance port (if a cable is plugged into the MAINT. port). **NOTE**: This functionality is only required if Safran Trusted 4D Service personnel request access to the STL receiver directly.

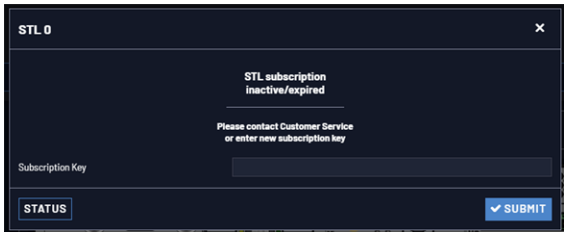
Strong Burst: Indicates color-coded burst rate. For more information see "Burst Rate" on the next page.

Latitude, Longitude, Altitude: Position data, as entered under "Configuring STL Settings" on page 554.

Geolocation Mode: Position estimation setting, as entered under "Configuring STL Settings" on page 554.

Sensitivity Level: STL receiver sensitivity setting, as entered under "Configuring STL Settings" on page 554.

Renewing Your STL Subscription



Contact customer service to obtain a new subscription key: US: +1 585 321 5800; France: +33 (0)1 64 53 3980.

In the Web UI, navigate to **INTERFACES > OPTION CARDS: STL0 > EDIT** to access to STL edit panel. Enter your new subscription key.and click submit.

If your location information is different from your End User Agreement, please contact customer service.

Confirm that your start date, end date, and subscription state have updated in the STL reference panel.

Burst Rate

Satellites transmit the STL time and location data in bursts. The number of bursts per minute that the receiver detects is the burst rate, but only **strong bursts** have a quality high enough to be usable. Note that the burst rate changes over time due to the movement of the satellites and other factors.

The current strong burst rate is shown in the **STL 0** status window (described above) and offers a good indication on the reception quality. Typically, a number of received strong bursts per minute is greater than 60, the location has sufficient STL service for the receiver to converge and provide a timing solution.

Strong Bursts	Conditions	Typically experienced ...	Receiver lock status	Troubleshooting
80+	Excellent, minimal signal attenuation	... outdoors	Short time to convergence	No action required
35-55	Good, some signal attenuation	... indoors near windows	Short time to convergence	No action required
15-30	Moderate, strong signal attenuation	... indoors far from windows	Longer time to convergence	Wait a couple of minutes for better satellite geometry; relocate antenna
5-15	Marginal, major signal attenuation	... deep indoors	Significantly longer time to convergence	Wait several minutes for better satellite geometry; relocate antenna
0	Poor, severe signal attenuation	... very deep indoors	No convergence	Verify that STL service is enabled in your area; wait several minuts for better satellite geometry; relocate antenna

Note: The values shown above are only guidelines: Due to the dynamic nature of satellite signal characteristics over time, a specific burst threshold value does not guarantee a good receiver performance.

Specifications

The specifications of the STL Option Module 1204-3E are:

- **Inputs**: One STL antenna input, one Ethernet maintenance input
- **Antenna input connector**: SMA
- **Maintenance connector**: RJ45
- **Frequency band**: 1626 MHz
- **Timing synchronization accuracy to UTC**: ±500 ns (specified); ±200 ns (typical)
- **Coverage**: Global

- **Time-to-first-fix (Timing)**: Several seconds (the PPS pulse will become available once the positioning fix has been obtained)
- **Jamming resilience**: Signal is 30 to 40 dB stronger than GPS signal
- **Spoofing resilience**: Encrypted signal
- **Maximum number of cards**: 1
- **Ordering information**:
  - STL module: 1204-3E
  - STL subscription (1 year): STL-SS-1Y

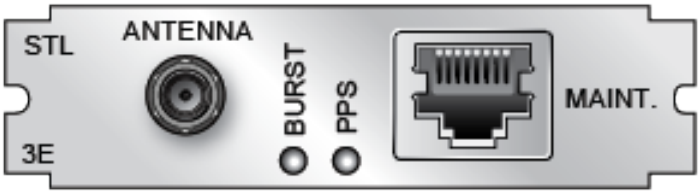


Figure 5-63: Model 1204-3E option card rear plate

5.2.7.2 Alarm Relay Out [1204-0F]

The Model 1204-0F Alarm Relay Option Card provides three (3) configurable relay outputs for the SecureSync platform.

Alarm Relay Out [1204-0F]: Specifications

- **Inputs/Outputs**: (3) three contact relay connections (NC, common, NO)
- **Signal Type and Connector**: Terminal block
- **Contacts** switch under max. load of 30 VDC, 2A
- **Contacts** rated to switch: 220 VDC
- Nominal **Switch Capacity**: 30 V, 2A
- Maximum **switch voltage**: 220 VDC
- Maximum **switch power**: 60 W
- Maximum **switch current**: 2A
- **Breakdown voltage**: 1000 VDC between contacts

- **Switch time**: 4ms, max.
- **Maximum Number of Cards**: 1
- **Ordering Information**: 1204-0F: Relay Outputs Module

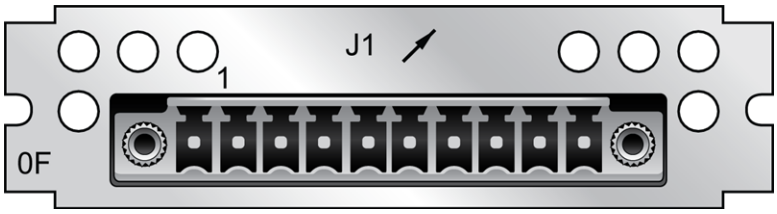


Figure 5-64: Model 1204-0F option card rear plate

Terminal block pin-out, alarm relay out

PIN	SIGNAL
1	GND
2	Relay 0 NO
3	Relay 0 NC
4	Relay 0 COMMON
5	Relay 1 NO
6	Relay 1 NC
7	Relay 1 COMMON
8	Relay 2 NO
9	Relay 2 NC
10	Relay 2 COMMON

Operation of the Alarm Relay Card

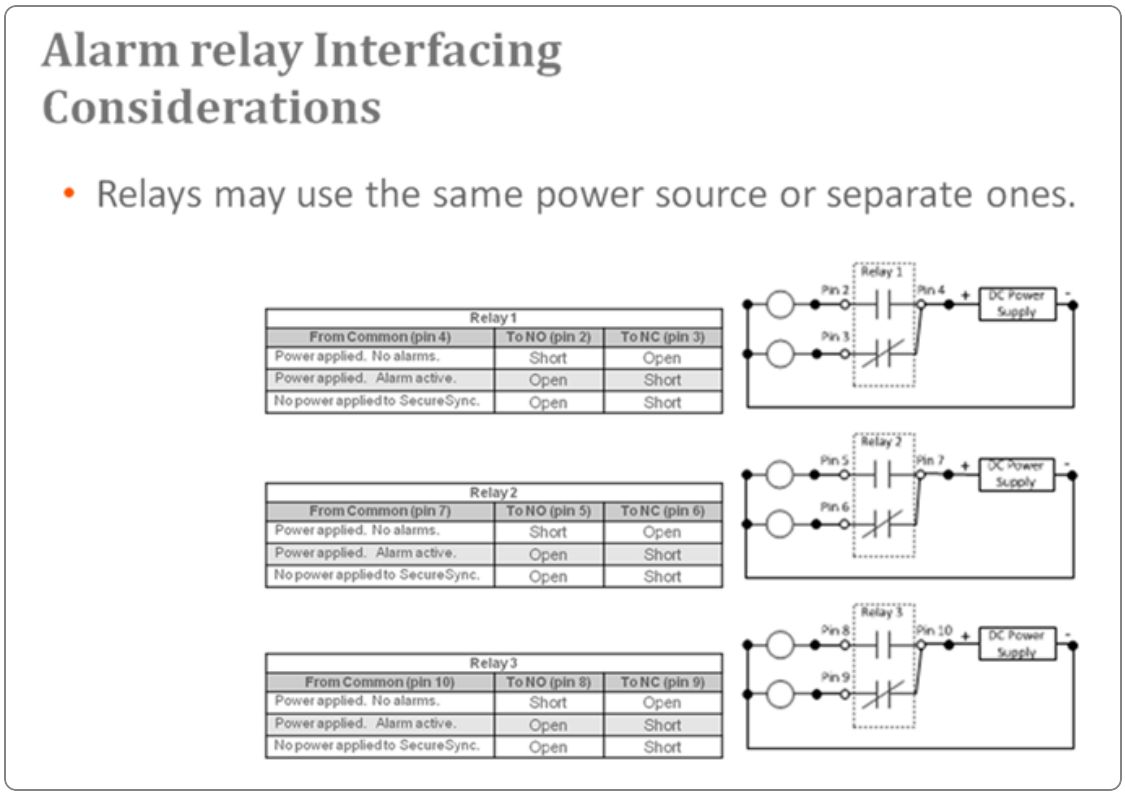


Figure 5-65: Contact closure relay pinouts

1. All relay contacts are labeled as in their de-energized state (power removed or alarm asserted).
2. The "normal" state of the relays (no alarms asserted) is relays energized.
3. The applicable relay(s) (Minor or Major, as configured in the browser) is /are de-energized when a Minor or Major alarm is asserted.
4. Both the Minor and Major alarms are active (relays de-energized and in their alarm state) when input power is removed from SecureSync.
5. For information on how to configure the relays as either a Minor alarm relay or a Major alarm relay, see "Alarm Relay Output: Edit Window" on page 564.

Each of the three available relays on this option card can be configured to be either a Minor or a Major alarm relay. The three relays are dry contact closures that can either open or complete a circuit, depending on whether the relay is

energized/de-energized and whether the custom alarm circuit is connected to the NO or NC contacts.

To use this option card to provide an audible indication of a Minor or Major alarm being asserted, SecureSync does not pass or generate an audible tone. It is just the switch that allows the tone to be generated. Or for a visible alarm indication, the three relays can allow DC voltage to be routed to the light, when an alarm is asserted.

The best way to think of each of the alarm relays is that they are simply a light switch on the wall. When the switch is off (relay is in one position) the light/buzzer is off. But if you toggle the switch (relay) to the other position (either a Minor or Major alarm is alarm is asserted), the light/buzzer comes on. When a Minor or Major Alarm is asserted, the applicable relay(s) switches states. This can then allow a custom circuit to be able to sound an alarm or to illuminate a light, as desired.

The nominal switch capacity is 30V, 2A (maximums: voltage = 220 VDC, power = 60W, current = 2A). So you can connect any desired audible//visible device or component to this relay that can operate within this rating (Safran doesn't make any specific recommendations on what visible or audible alarms to use in conjunction with this Option Card). Further below is a diagram of ways that a light or buzzer can be connected to any of the three relays on this Option Card.

Note that any necessary wiring, the light/buzzer and the power source (labeled in the diagram above as “DC Power Supply”) for the light/buzzer is supplied by the customer. “Relay 1”, “Relay 2” and “Relay 3” represent the three available relays. The three tables on the left provide the pin-outs for each of the relay contact closures.

Alarm Relay Output: Viewing Signal State

To quickly view the signal state of all three alarm outputs, see: "Viewing an Input/Output Signal State" on page 387.



Each alarm output will be in one of these 3 states:

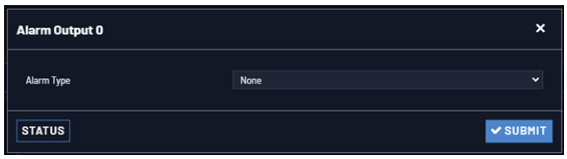
- NEVER OUTPUTS
- OUTPUTS ON MINOR ALARM
- OUTPUTS ON MAJOR ALARM

Alarm Relay Output: Edit Window

To configure the Alarm Relay Output, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entry for this card is: **Relay Output**. The name of the output is: **Alarm Output [number].**

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



The Edit window allows the configuration of the following settings:

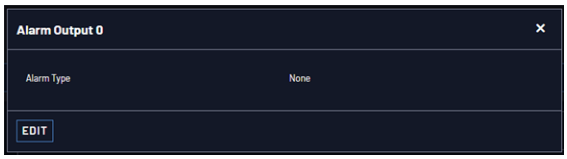
- **Alarm Type**:
  - **None**: Will not output for an alarm.
  - **Minor**: Will output on a minor alarm.
  - **Major**: Will output on a major alarm.

Alarm Relay Output: Status Window

To view the current settings of an Alarm Relay Output, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entry for this card is: **Relay Output**. The name of the output is: **Alarm Output [number]**.

Note: SecureSync starts numbering I/O ports with 0 (only 1PPS and 10 MHz outputs start at 1, because of the built-in outputs).



The Status window displays the following settings:

- **Alarm Type**:
  - **None**: Will not output for an alarm.
  - **Minor**: Will output on a minor alarm.
  - **Major**: Will output on a major alarm.

5.2.7.3 Revertive Selector Card [1204-2E]

The Revertive Selector Option Card provides automatic failover capability, using one option card slot for a single output signal.

Operating Principle

The output follows the selected input. Signals can be 1PPS, 10 MHz, 5MHz or 1MHz.

Input “A” is selected if present and valid. If input “A” disappears, or if power to host SecureSync is interrupted, input “B” is presented at output “OUT”.

As soon as input “A” becomes valid again, the output switches back to use “A” as source.

At power-up or module reset, there is a timed delay before input “A” is presented. This allows reference at input “A” to stabilize before being used.

Model 1204-2E Specifications

- **Inputs/Outputs**:
  - (2) Inputs – Unselected input terminated with 50 Ω
  - (1) Output
- **Connectors**: 3 BNC

- **Signal Type**: User selected (jumper switch):
  - >1MHz
  - 1MHz to 100 Hz
  - 1PPS
- **Signal Level**:
  - Sine Wave, 0.5 V to 30 V_{p-p}
  - TTL (50 Ω)
- **Default Power-on Switch State**:
  Initially, **input "B"**; until a valid signal on input "A" is detected, causing the switch state to change to **"A"**.
- **Maximum Number of Cards**: 6
- **Ordering Information**: 1204-2E: Revertive Selector Option Module

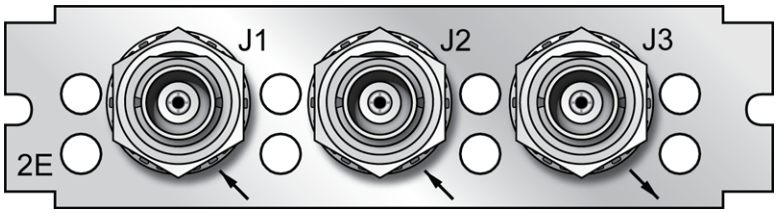


Figure 5-66: Model 1204-2E option card rear plate

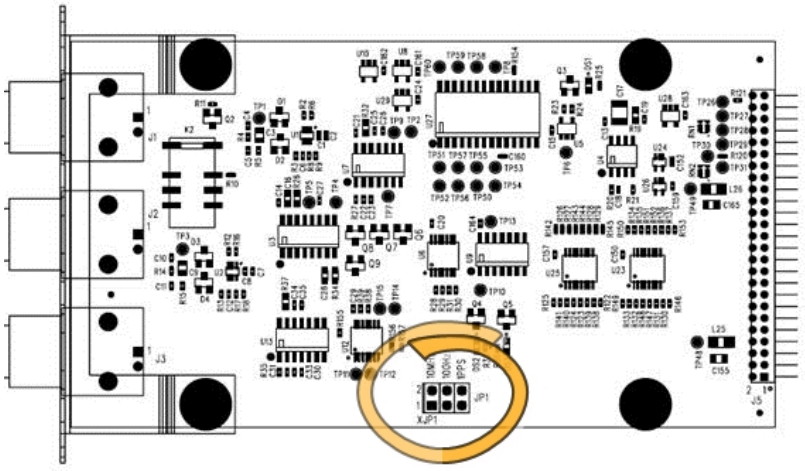


Figure 5-67: Location of jumper switches

5.2.7.4 Event Broadcast [1204-23]

The Event Broadcast Module (RS-232) provides a BNC connection for an Event Trigger Input and a RS-232 connector for an ASCII message output.

When the defined signal edge is detected on the **Event Input** BNC Connector, an ASCII message is created containing the current time.

ASCII messages are stored in a **Message Buffer**. The message buffer can store 512 entries before overflowing. Messages may be lost if the buffer overflows.

Messages can be output in one of two ways:

- If the **Mode** is set to Broadcast, messages in the **Message Buffer** will be output immediately through the RS-232 Output port. If another event is captured while a message is being sent, it will be queued in the buffer until the first message completes, then the next message will be sent.
- If the **Mode** is set to Request, messages in the **Message Buffer** are only sent when the Request Character is received.

The output format used is selected among a small group of formats with the capability to output data at 5ns resolution. Event Broadcast Output formats are detailed in "Event Broadcast Time Code Formats" on page 573.

Event Broadcast [1204-23]: Specifications

- **Inputs/Outputs**: (1) Event Trigger Input, (1) Event Broadcast Output
- **Signal Type and Connector**:
  - Connector J1 – (RS-232 Output) RS-232 DB9F
  - Connector J2 – (Event Input) TTL BNC
- **Event Resolution**: 5ns
- **Minimum Time Between Events**: 20 ns
- **Message Buffer Size**: 512 messages
- **Ordering Information**: 1204-23: Event Broadcast

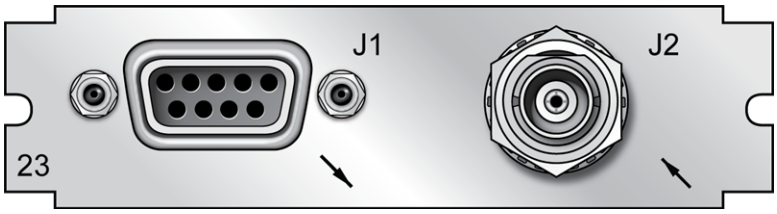


Figure 5-68: Model 1204-23 option card rear plate

Output Port: Pin Assignments

Table 5-26: Output connector DB-9: pin-out

Pin Number	Signal Name	Function
Top row of 5 pins		
1	NC	No Connection
2	SERIAL_OUT_TX	RS-232 Transmit data
3	SERIAL_OUT_RX	RS-232 Receive data
4	NC	No connection
5	GND	Ground
Bottom row of 4 pins		
6	NC	No connection
7	NC	No connection
8	NC	No connection
9	NC	No connection

Viewing the State of Event Broadcast and Event Input

To view the Status of Event Broadcast and Event Input, see "Viewing an Input/Output Signal State" on page 387.

Event Broadcast Output: Edit Window

To configure the **Event Broadcast Output**, go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entry for this card is: **Event Broadcast**.



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 198.
- **Format**: Selects the format of the message to be outputted. Refer to "Event Broadcast Time Code Formats" on page 573 for a description of all of the available formats.
  The Event Broadcast card only supports two formats (Event Broadcast Format 0 and Event Broadcast Format 1), and only supports the output of one message per event. If format is set to “None”, no messages will be queued in the Message Buffer.
- **Output Mode**: This field determines when the output data will be provided. Available Mode selections are as follows:
  - **Broadcast**—Event Messages are automatically broadcast when they are created by an event. If a new event happens while an older message is being broadcast, the new message will be queued in a “First-in, First-out” manner. When the message has finished, the next message out of the queue will be broadcast.
  - **Request**—Event Messages are only broadcast in response to a Request Character. New messages will be queued in a “First-in, First-out” manner.
- **Request character**: This field defines the character that SecureSync needs to receive in order for a message to be provided when in “Request” mode. This field will only appear if the Output Mode is set as “Request Broadcast.”

- **Timescale**—Used to select the time base for the incoming ASCII time code data. The entered Timescale is used by the system to convert the time in the incoming ASCII data stream to UTC time for use by the System Time. The available choices are:
- **UTC**—Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
- **TAI**—Temps Atomique International
- **GPS**—The raw GPS time as transmitted by the GNSS satellites (as of 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 202 for more information on configuring and reading the System Clock. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.



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

- **Baud Rate**: Determines the speed that the output port will operate at.
- **Data Bits**: Defines the number of Data Bits for the output port.
- **Parity**: Configures the parity checking of the output port.
- **Stop Bits**: Defines the number of Stop Bits for the output.

Event Broadcast Output: Status Window

To view the current settings of the **Event Broadcast Output**, go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entry for this card is: **Event Broadcast**.



The Status window displays the following settings:

- **Signature Control**: Signature Control controls when messages will be broadcast in response to events on the Event Input (J2) port when events are enabled and the card is in “broadcast” mode. (Events are still queued even if they are not broadcast, and are transmitted once the signature control conditions permit.) For more information on Signature Control, see "Signature Control" on page 198.
- **Format**: The format of the message to be output. Refer to "Event Broadcast Time Code Formats" on page 573 for a description of all of the available formats.
  The Event Broadcast card only supports two formats (Event Broadcast Format 0 and Event Broadcast Format 1), and only supports the output of one message per event. If format is set to “None”, no messages will be queued in the Message Buffer.
- **Output Mode**: When the output data will be provided. Available Mode selections are as follows:
  - **Broadcast**—Event Messages are automatically broadcast when they are created by an event. If a new event happens while an older message is being broadcast, the new message will be queued in a “First-in, First-out” manner. When the message has finished, the next message out of the queue will be broadcast.
  - **Request**—Event Messages are only broadcast in response to a Request Character. New messages will be queued in a “First-in, First-out” manner.
- **Timescale**: The time base for the incoming time code data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time. The available choices are:

- UTC—Coordinated Universal Time ("temps universel coordonné"), also referred to as ZULU time
- TAI—Temps Atomique International
- GPS—The raw GPS time as transmitted by the GNSS satellites (as of 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 202 for more information on configuring and reading the System Time. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.



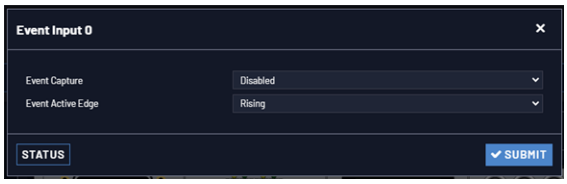
Note: The Timescale of the input (as configured in the time source) must be set correctly, especially if other input references are enabled. Failure to configure the Timescale of the ASCII input correctly could result in time jumps occurring in the System Time when input reference changes occur. These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

- **Request character**: This field defines the character that SecureSync needs to receive in order for a message to be provided when in “Request” mode. This field will only appear if the Output Mode is set as “Request Broadcast.”
- **Baud Rate**: The speed that the output port will operate at.
- **Data Bits**: The number of Data Bits for the output port.
- **Parity**: The parity checking of the output port.
- **Stop Bits**: The number of Stop Bits for the output.

Event Broadcast Input: Edit Window

To configure the **Event Broadcast Input** (also referred to as ‘**Reference**’), go to its Edit window. For instructions, see: "Configuring Option Card Inputs/Outputs" on page 386.

The Web UI list entry for this card is: **Event Broadcast**.



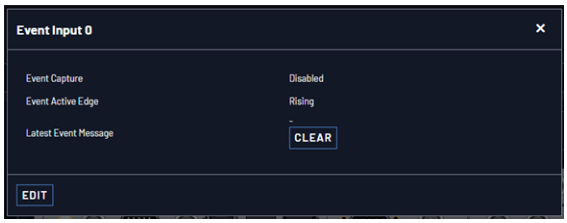
The Status window displays the following settings:

- **Event Capture**: Enables the processing of events on the Event Input port J2. When set to “Disabled”, no event messages will be queued. When set to “Enabled”, event messages will be triggered (if a valid Format is selected).
- **Event Active Edge**: Selects the signal edge used for triggering events on Event Input port J2.

Event Broadcast Input: Status Window

To view the current settings of the **Event Broadcast Input**, (also referred to as ‘**Reference**’), go to its Status window. For instructions, see: "Viewing Input/Output Configuration Settings" on page 385.

The Web UI list entry for this card is: **Event Broadcast**.



The Status window displays the following settings:

- **Event Capture**: The processing of events on the Event Input port J2. When set to “Disabled”, no event messages will be queued. When set to “Enabled”, event messages will be triggered (if a valid Format is selected).
- **Event Active Edge**: The signal edge used for triggering events on Event Input port J2.
- **Latest Event Message**: The last message sent. This can be cleared with the Clear button.

Event Broadcast Time Code Formats

The following ASCII-based time code formats are available:

Event Broadcast Format 0

Example message:

SSSSSSSSSS.XXXXXXXXX<CR><LF>

Where:

SSSSSSSSSS	10-digit Seconds Time (references from January 1st, 1970)
.	Decimal Point Separator
XXXXXXXXX	9-digit Sub-Seconds Time (5 ns resolution)
CR	Carriage Return
LF	Line Feed

Event Broadcast Format 1

Example message

YYYY DDD HH:MM:SS.XXXXXXXXX<CR><LF>

Where:

YYYY	Year
	Space Separator
DDD	Day of Year (001-366)
	Space Separator
HH	Hour of the Day (00-23)
:	Colon Separator
MM	Minutes of the Hour (00-59)
:	Colon Separator
SS	Seconds (00-59), (00-60 for leap second)
.	Period Separator
XXXXXXXXX	9-digit Sub-Seconds Time (5 ns resolution)

CR	Carriage Return
LF	Line Feed

5.2.7.5 NavIC [1204-5E and 1204-5F]

For more information on use of the NavIC 1204-5E and 1204-5F options cards, please contact Safran "Technical Support" on page 645.

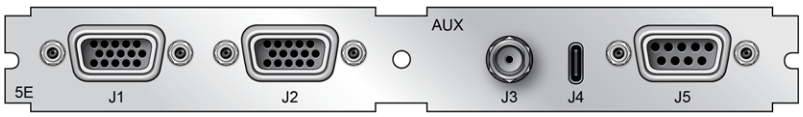


Figure 5-69: Model 1204-5E option card rear plate

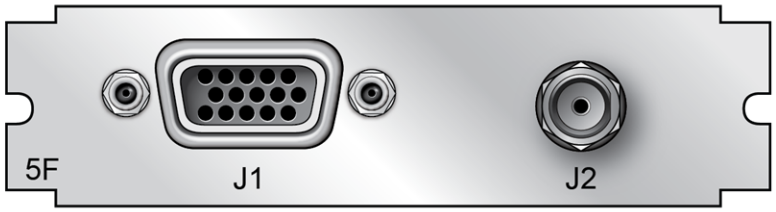


Figure 5-70: Model 1204-5F option card rear plate

5.3 Command-Line Interface

A terminal emulation program is used to emulate a video terminal, so as to access SecureSync's CLI (Command-Line Interface) remotely via a serial cable. This may be required if no other means of remotely accessing SecureSync are available, for example if Ethernet ports are used otherwise or have been disabled (e.g., for security reasons).

5.3.1 Setting up a Terminal Emulator

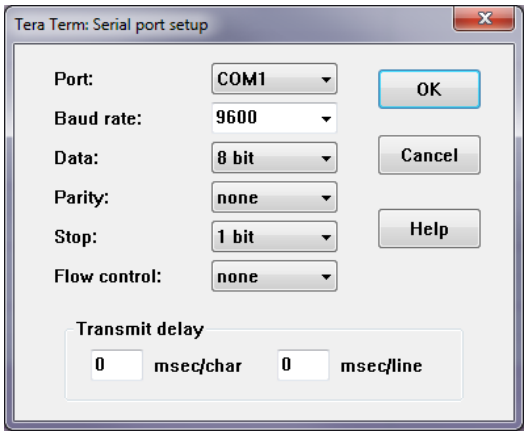
If no other means are available to access SecureSync, a terminal emulation program can be used to carry out certain configuration changes by accessing SecureSync's CLI (command-line interface) via a serial port connection. An

application example for this scenario is to enable a network port so that the SecureSync Web UI can be used. While it is also possible to retrieve selected logs, a terminal emulator does not replace the SecureSync Web UI.

Safran 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**: COM(#)
   - **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.

5.3.2 CLI Commands

SecureSync features a suite of command-line interface (CLI) commands that can be used to configure parameters and retrieve status information or log files via a remote connection, using the `telnet` or `ssh` (if enabled) protocol.

This section includes a list of some of the supported commands.

Notes:

a. The command "`helpcli`" will provide a list of all available commands and their syntax (**Note**: Typing "`help`" will output bash shell help only and will not provide useful information).

b. You can scroll up or scroll down through the output by using the Page Up/Page down keys, or the arrow keys.

c. Type "`q`" (lower-case) to quit.

d. Pressing the up/down keys scrolls through previously typed commands.

e. Commands need to be typed in all lower-case letters.

f. Where `eth0` 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 292 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	

Command	Description	Privileges
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.	
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 list	<GPS|GLO|GAL|BEI> Display list of active satellites for a single, given constellation.	
agnss server rnx	<GPS|GLO|GAL|BEI> Display list of constellations's satellites found in today's RINEX file.	
clean	Restores SecureSync configuration, logs, and stats to factory defaults and reboots	admin
cleanhalt	Restores SecureSync 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

Command	Description	Privileges
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
displaymodeget	Retrieves the display mode setting (either 12-hour or 24-hour time)	admin or user
displaymodeset	Sets the system display mode to either 12-hour time or 24-hour time	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
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
fanstatus	Displays fan status and individual fan speed	admin or user
fp_lock	Lock the front panel (admin access required)	admin
fp_unlock	Unlock the front panel (admin access required)	admin
getopenssl	Returns the current FIPS compliance mode	admin

Command	Description	Privileges
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 SecureSync 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
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

Command	Description	Privileges
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
hs_getstatus	Used to obtain the status of the Hot Swap Power Supplies	admin or user
ip4cfg	Display the IPv4 static configuration.	admin or user
ip4get	Displays IPv4 Ethernet port information (IP address net mask and gateway)	admin or user
ip4set	Used to set IPv4 Ethernet port information (IP address net mask and gateway)	admin
ip6add	Used to add IPv6 Ethernet port 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.	
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

Command	Description	Privileges
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
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

Command	Description	Privileges
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
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 SecureSync	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
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

Command	Description	Privileges
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
status	Displays information about the oscillator disciplining	admin or user
stlgetinfo	Provides STL data	
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

Command	Description	Privileges
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 SecureSync	admin
version	Displays the installed main SecureSync 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 SecureSync units only	admin

5.4 Time Code Data Formats

This section describes the different time code data format selections available for use with SecureSync option cards that accept ASCII data streams as inputs or outputs via their RS-485 and RS-232 interfaces.

Supported are formats like NMEA, BBC, Spectracom, GSSIP, and Endrun.

5.4.1 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 the facing page).

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.

5.4.2 NMEA RMC Message

NMEA Message Format RMC, (Recommended Minimum) provides fix information, speed over ground and Magnetic Variance information.

Example message:

$GPRMC,123519.00,A,4807.038,N,01131.000,E,,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.

5.4.3 NMEA ZDA Message

The Format ZDA Data message provides Date and Time information.

Example message:

$GPZDA,HHMMSS.00,DD,MM,YYYY,XX,YY*CC

Where:

HHMMSS.00	HrMinSec(UTC)
DD,MM,YYYY	Day, Month, Year
XX	Local zone hours -13...13
YY	Local zone minutes 0...59
*CC	Checksum

Note: Enabling more NMEA messages increases the minimum baud rate required. A minimum rate of 9600 baud is suggested when enabling more messages.

5.4.4 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.

5.4.5 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.

5.4.6 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.

5.4.7 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.

5.4.8 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

5.4.9 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

5.4.10 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 595 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

5.4.11 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" on the next page lists the quality indicators and the corresponding error estimates based upon the GNSS receiver 1PPS stability, and the time elapsed tracking no satellites. The Tracking Zero Satellites timer and the quality indicator reset when the receiver reacquires a satellite.

Quality	Time (hours)	TXCO Error (milliseconds)	OCXO Error (milliseconds)	Rubidium Error (microseconds)
Space	Lock	<1	<0.01	<0.3
A	<10	<10	<0.72	<1.8
B	<100	<100	<7.2	<18
C	<500	<500	<36	<90

Quality	Time (hours)	TXCO Error (milliseconds)	OCXO Error (milliseconds)	Rubidium Error (microseconds)
D	>500	>500	>36	>90

Table 5-27: 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.

5.4.12 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.

5.4.13 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.

5.4.14 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.

5.4.15 Spectracom Format 8

Format 8 includes a time synchronization status character, the four digit year, day of year, time reflecting Time Zone Offset and DST corrections when enabled. Format 8 also includes the DST/Standard Time indicator, and the Time Zone Offset value. Format 8 data structure is shown below:

Example:

CR LF I ^ ^YYYY^ DDD ^ HH:MM:SS ^ D+XX CR LF
or
CR LF I ^ ^YYYY^ DDD ^ HH:MM:SS ^ D-XX CR LF

Where:

CR	Carriage Return
LF	Line Feed

I	Time Sync Status (space, ?, *)
YYYY	Four digit year indication
^	Space separator
DDD	Day of Year (001-366)
HH	Hours (00-23)
:	Colon separator
MM	Minutes (00-59)
SS	Seconds (00-60)
D	Daylight Saving Time indicator (S,I,D,O)
XX	Time Zone Switch Setting (±00...12)

The leading edge of the first character (CR) marks the on-time point of the data stream. Time sync status character (I) is described below:

(Space)	When SecureSync is synchronized to UTC source.
*	When SecureSync time is set manually.
?	When SecureSync has not achieved or has lost synchronization to UTC source.

The time and date can be set to either local time or UTC time, depending upon the configuration of the output port.

5.4.16 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.

5.4.16.1 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

5.4.17 Spectracom Epsilon Formats

5.4.17.1 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)

5.4.17.2 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)

5.4.17.3 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)

5.4.18 BBC Message Formats

5.4.18.1 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)

5.4.18.2 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)

5.4.18.3 Format BBC-03 PSTN

The third format is a string ASCII characters and is sent on a received character.

The message should be advanced by an appropriate number such that the stop bit of each <CR> occurs at the start of the next second. For example, at 300 baud, 8 data bits, 1 stop bit, and no parity, each byte takes 10/300 s=33 ms, so the <CR> byte should be advanced by 33 ms in order for the <CR>'s stop bit to line up with the start of the next second.

Time information is available in UTC format or UK TOD format.

't' command

Input format: t<CR>

Output format:

Current Second	Second + 1	Second + 2	Second + 3
<CR>	HHMMSS<CR>	HHMMSS<CR>	HHMMSS<CR>

Number of characters: 7 (including CR)

Each HHMMSS filed refers to the time at the start of the next second. The data transmitted by SecureSync is timed so that the stop bit of each <CR> ends at the start of the next second.

'd' command

SecureSync transmits the date on request.

Input format: d<CR>

Output format: YYMMDD<CR>

Number of output characters: 7 (including CR)

‘s’ command

SecureSync transmits the status information on request.

Input format: `s<CR>`

Output Format: `status`

Number of output characters: 1

Where returned, values for `status` are:

- `G` = System Good
- `D` = Failure of SecureSync internal diagnostics
- `T` = SecureSync does not have correct time

‘l’ command

The loopback command will cause SecureSyncto echo the next character received back to the caller. This may be used by a caller’s equipment to calculate the round trip delay across the PSTN connection in order to apply a correction to the received time data.

Input format: `l<CR>`

Output format: (Next character received)

‘hu’ command

The hang up command will cause SecureSync to drop the line immediately and terminate the call.

Input format: `hu<CR>`

5.4.18.4 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

5.4.18.5 Format BBC-05 (NMEA RMC Message)

The NMEA Message Format RMC, (Recommended Minimum) provides fix information, speed over ground and Magnetic Variance information. Note that this RMC Message is not 100% identical to the official NMEA RMC MESSAGE (that corresponds to the 3.01 NMEA 0183 standard and is another time code format supported by SecureSync.)

The BBC RMC message (BBC-05) corresponds to Version 2 of the NMEA 0183 standard, following the description below:

Example message:

$GPRMC,123519,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A

Where:

RMC	Recommended Minimum sentence C
123519	Fix taken at 12:35:19 UTC
A	Status: A=active or V=Void.
4807.038,N	Latitude 48 deg 07.038′ N
01131.000,E	Longitude 11 deg 31.000′ E
22.4	Speed over the ground in knots
84.4	Track angle in degrees True
230394	Date—23rd of March 1994
003.1,W	Magnetic Variation
*6A	The checksum data, always begins with *

5.4.19 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. SecureSync generates these messages emulating the Time and 1PPS transfer behavior of the SINCGARS interface. An external device compatible with the SINCGARS interface can attach to an ASCII Output from SecureSync and receive time and 1PPS as if communicating with and ICD-GPS-153C compatible SAASM GPS.

[1]GSSIP = GPS STANDARD SERIAL INTERFACE PROTOCOL

These commands are emulated only and contain only time information; position and velocity information is zeroed out. No controlled data is included in the messages, hence no SAASM GPS receiver is required.

The ASCII Output supports two configurations for supporting SINCGARS:

A configuration of Time Transfer as Message Format1 and Current Status as Format2 causes the SINCGARS protocol to be emulated and the machine state to be initializated.

- **Format1**: Time Transfer (5101)
- **Format2**: Current Status (5040)
- **Format3**: Buffer Box (253)

A configuration of Current Status as Message Format1 and Time Transfer as Format2 results in broadcasting of the messages Current Status (1Hz), Time Transfer (1Hz), and Buffer Box (1/6Hz) at their default rates.

- **Format1**: Current Status (5040)
- **Format2**: Time Transfer (5101)
- **Format3**: Buffer Box (253)

5.4.20 EndRun Formats

The following formats provide compatibility with **EndRun** technology.

5.4.20.1 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

5.4.20.2 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

5.5 IRIG Standards and Specifications

5.5.1 About the IRIG Output Resolution

The IRIG output signals are generated from SecureSync'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 SecureSync 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 SecureSync's Web UI, to help account for cabling and processing delays of the device each output is connected with.

5.5.2 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 5-28: 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

Format	Encoding	Modulation	Carrier	Coded Expressions	Bit rate	Time Frame Interval
IRIG-A	A006	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}	1000 pps	0.1 sec
IRIG-A	A007	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and SBS	1000 pps	0.1 sec
IRIG-A	A130	AM	10 kHz	BCD_{TOY}, CF and SBS	1000 pps	0.1 sec
IRIG-A	A131	AM	10 kHz	BCD_{TOY}, CF	1000 pps	0.1 sec
IRIG-A	A132	AM	10 kHz	BCD_{TOY}	1000 pps	0.1 sec
IRIG-A	A133	AM	10 kHz	BCD_{TOY}, SBS	1000 pps	0.1 sec
IRIG-A	A134	AM	10 kHz	BCD_{TOY}, BCD_{YEAR}, CF and SBS	1000 pps	0.1 sec
IRIG-A	A135	AM	10 kHz	BCD_{TOY}, BCD_{YEAR}, and CF	1000 pps	0.1 sec
IRIG-A	A136	AM	10 kHz	BCD_{TOY}, BCD_{YEAR}	1000 pps	0.1 sec
IRIG-A	A137	AM	10 kHz	BCD_{TOY}, BCD_{YEAR}, and SBS	1000 pps	0.1 sec
IRIG-B						
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

Format	Encoding	Modulation	Carrier	Coded Expressions	Bit rate	Time Frame Interval
IRIG-B	B121	AM	1 kHz	BCD_{TOY}, CF	100 pps	1 sec
IRIG-B	B122	AM	1 kHz	BCD_{TOY}	100 pps	1 sec
IRIG-B	B123	AM	1 kHz	BCD_{TOY}, SBS	100 pps	1 sec
IRIG-B	B124	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}, CF and SBS	100 pps	1 sec
IRIG-B	B125	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}, and CF	100 pps	1 sec
IRIG-B	B126	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}	100 pps	1 sec
IRIG-B	B127	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}, and SBS	100 pps	1 sec
IRIG-E						
IRIG-E	E000	DCLS	N/A	BCD_{TOY}, CF and SBS	10 pps	1 sec
IRIG-E	E001	DCLS	N/A	BCD_{TOY}, CF	10 pps	1 sec
IRIG-E	E002	DCLS	N/A	BCD_{TOY}	10 pps	1 sec
IRIG-E	E003	DCLS	N/A	BCD_{TOY}, SBS	10 pps	1 sec
IRIG-E	E004	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, CF and SBS	10 pps	1 sec
IRIG-E	E005	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and CF	10 pps	1 sec
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

Format	Encoding	Modulation	Carrier	Coded Expressions	Bit rate	Time Frame Interval
IRIG-E	E116	AM	100 Hz	BCD_{TOY}, BCD_{YEAR}	10 pps	1 sec
IRIG-E	E117	AM	100 Hz	BCD_{TOY}, BCD_{YEAR}, and SBS	10 pps	1 sec
IRIG-E	E120	AM	100 Hz	BCD_{TOY}, CF and SBS	10 pps	1 sec
IRIG-E	E121	AM	1kHz	BCD_{TOY}, CF	10 pps	10 sec
IRIG-E	E122	AM	1kHz	BCD_{TOY}	10 pps	10 sec
IRIG-E	E123	AM	1kHz	BCD_{TOY}, SBS	10 pps	10 sec
IRIG-E	E124	AM	1kHz	BCD_{TOY}, BCD_{YEAR}, CF and SBS	10 pps	10 sec
IRIG-E	E125	AM	1kHz	BCD_{TOY}, BCD_{YEAR}, and CF	10 pps	10 sec
IRIG-E	E126	AM	1kHz	BCD_{TOY}, BCD_{YEAR}	10 pps	10 sec
IRIG-E	E127	AM	1kHz	BCD_{TOY}, BCD_{YEAR}, and SBS	10 pps	10 sec
IRIG-G						
IRIG-G	G001	DCLS	N/A	BCD_{TOY}, CF	10000 pps	10 msec
IRIG-G	G002	DCLS	N/A	BCD_{TOY}	10000 pps	10 msec
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
IRIG-H						

Format	Encoding	Modulation	Carrier	Coded Expressions	Bit rate	Time Frame Interval
IRIG-H	H002	DCLS	N/A	BCD_{TOY}	1 pps	1 sec
IRIG-H	H122	AM	1KHz	BCD_{TOY}	1 pps	1 sec
NASA-36						
NASA-36	N/A	AM	1msec	UNKNOWN	100 pps	1 sec
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.

SecureSync 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.

5.5.3 IRIG B Output

The IRIG B Time Code description follows.

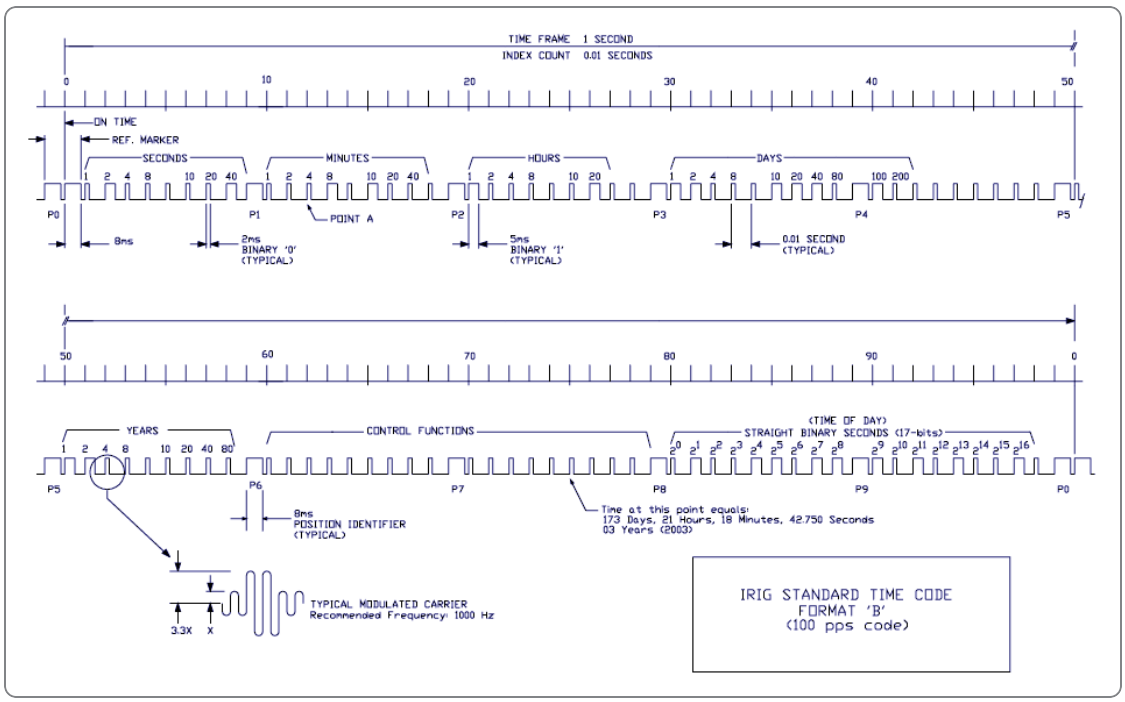


Figure 5-71: IRIG B time code description

The IRIG B code contains the Binary Coded Decimal (BCD) time of year, Control Function (CF) field and the Straight Binary Seconds time of day. The following figure illustrates the IRIG B data structure. The BCD time of year provides the day of the year, 1-366, and the time of day including seconds. The hour of the day is expressed in 24 hour format. The SBS time is the number of seconds elapsed since midnight. The Control Function field contains year information and a time synchronization status bit.

1. Time frame: 1.0 seconds.
2. Code digit weighting:
    A. Binary Coded Decimal time-of-year.

- Code word - 30 binary digits.
- Seconds, minutes hours, and days.
- Recycles yearly.

B. Straight Binary Seconds time-of-day.

- Code word - 17 binary digits.
- Seconds only, recycles daily.

3. Code word structure:
   - **BCD**: Word seconds digits begin at index count 1. Binary coded elements occur between position identifier elements P0 and P5 (7 for seconds, 7 for minutes, 6 for hours, and 10 for days) until the code word is complete. An index marker occurs between decimal digits in each group to provide separation for visual resolution. Least significant digit occurs first.
   - **CF**: IRIG formats reserve a set of elements known as Control Functions (CF) for the encoding of various control, identification, or other special purpose functions. IRIG B has 27 Control Functions located between elements 50 and 78. The SecureSync uses the Control Functions to encode year information and time synchronization status.

The table below lists the **Control Function Field** and the function of each element.

- Element 55 is the time synchronization status bit. Element 55 is a Binary 1 when the 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 5-29: 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

C.F. Element #	Digit #	Function
65	15	Years Tens Y10
66	16	Years Tens Y20
67	17	Years Tens Y40
68	18	Years Tens Y80
69	PID P7	Position Identifier
70	19	Space
71	20	Space
72	21	Space
73	22	Space
74	23	Space
75	24	Space
76	25	Space
77	26	Space
78	27	Space

5.5.3.1 FAA IRIG B Code Description

SecureSync can be configured to provide IRIG timing, reflecting UTC or local time, with or without daylight saving time corrections. Below is a detailed description of the **FAA modified IRIG B code**. The FAA modified the IRIG B code by including satellite lock status and time error flags in the Control Function Field. The error flags provide an inaccuracy estimate based on the time elapsed since loss of GPS lock. In addition, the Straight Binary Seconds (SBS) data was removed from the data stream. The SBS time is the number of seconds elapsed since midnight.

FAA IRIG B OUTPUT

The FAA IRIG B code contains the Binary Coded Decimal (BCD) time of year and a Control Function (CF) field containing satellite lock status and time error flags. With the exception of the position identifiers, all remaining code elements are set to a binary 0. Figure A-1 illustrates the FAA IRIG B data structure. The BCD time

of year provides the day of the year, 001-366, and the time of day including seconds. The hour of the day is expressed in 24-hour format.

FAA IRIG B General Description

1. Time frame: 1.0 seconds
2. Pulse rates:
   A. Element rate: 100 per second
   B. Position identifier rate: 10 per second
   C. Reference marker rate: 1 per second
3. Element identification: The "on time" reference point for all elements is the pulse leading edge.
   A. Index marker (Binary 0 or uncoded element): 2 millisecond duration
   B. Code digit (Binary 1): 5 millisecond duration
   C. Position identifier: 8 millisecond duration
   D. 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.
4. Resolution: 10 milliseconds
5. 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 FAA IRIG B code uses five of the Control Function elements to encode satellite lock status and time error flags. For a description of the status and error flag implementation, refer to the table and the paragraphs below.

Element 53 (530 ms) is the time sync status bit. Element 53 is a Binary 1 when the receiver locked to GPS, and a Binary 0 when the receiver is not locked to GPS.

Element 55 (550 ms) is the ±1.0 millisecond error flag. Element 55 is set to Binary 1 when the expected time error is within +/- 1.0 millisecond, and a Binary 0 during all other conditions of operation.

Element 56 (560 ms) is the ±5.0 millisecond error flag. Element 56 is set to Binary 1 when the expected time error is within +/- 5.0 milliseconds. and a Binary 0 during all other conditions of operation.

Element 57 (570 ms) is the ±50 millisecond error flag. Element 57 is set to Binary 1 when the expected time error is within +/- 50 milliseconds, and a Binary 0 during all other conditions of operation.

Element 58 (580 ms) is the ±500 millisecond error flag. Element 58 is set to Binary 1 when the expected time error is within ±500 milliseconds, and a Binary 0 during all other conditions of operation.

Table 5-30: FAA Time Error Indicators

Time Since Loss of Lock	Status/Error	Lock Indicator	±1ms	±5ms	±50 ms	±500 ms
N/A	Locked Error < 2µs	1	0	0	0	0
< 00:16:40	Unlocked Error < 1ms	0	1	0	0	0
00:16:41 to 01:23:39	Unlocked Error < 5ms	0	0	1	0	0
01:23:40 to 13:53:19	Unlocked Error < 50 ms	0	0	0	1	0
13:53:20 to 5 days 18:53:19	Unlocked Error < 500 ms	0	0	0	0	1
>5 days 18:53:20	Unlocked Error Unknown	0	0	0	0	0
N/A	Power On	0	0	0	0	0

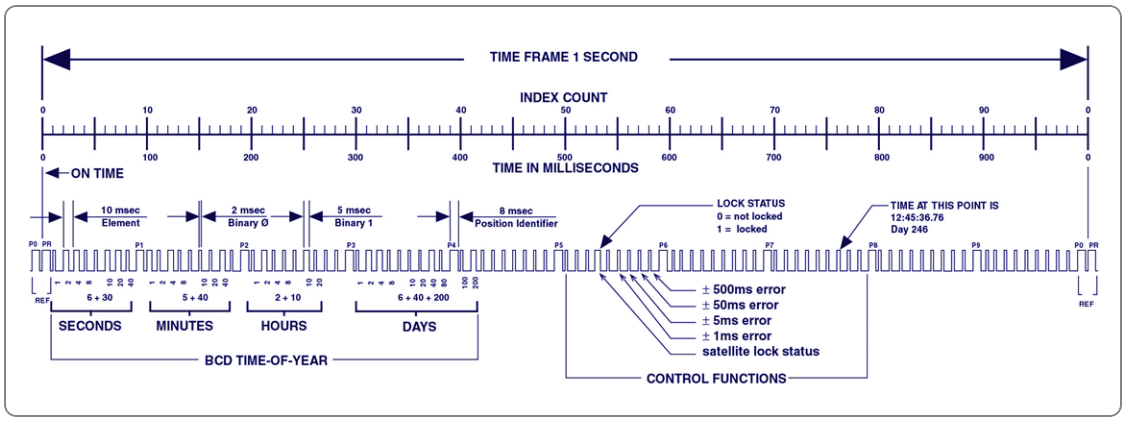


Figure 5-72: FAA modified IRIG B

Notes

The beginning of each 1.0 second time frame is identified by two consecutive 8.0 ms elements (P_0 and P_8). The leading edge of the second 8.0 ms element (P_R) is the "on time" reference point for the succeeding time code. 10 pps position identifiers P_0, P_1, ... P_8 (8.0 ms duration) occur 10 ms before 10 pps "on time" and refer to the leading edge of the succeeding element.

The time code word and the control functions presented during the time frame are pulse-width coded. The binary "zero" and index markers have a duration of 2.0 ms, and the binary "one" has a duration of 5.0 ms. The leading edge is the 100 pps "on time" reference point for all elements.

The binary coded decimal (BCD) time-of-year code word consists of 30 digits beginning at index count 1. The binary coded subword elements occur between position identifiers P_0 and P_5 (7 for seconds; 7 for minutes; 6 for hours; 10 for days) until the code word is complete. An index marker occurs between the decimal digits in each subword to provide separation for visual resolution. The least significant digit occurs first. The BCD code recycles yearly.

Twenty-seven control functions occur between position identifiers P_5 and P_8. FAA uses this field to communicate satellite lock status and time error and indicators. The first flag element is at 530 ms which indicates satellite lock. The ±1ms error flag occurs at 550 ms. The ±5ms error flag occurs at 560 ms. The ±50 ms error flag occurs at 570 ms. The ±500 ms error flag occurs at 580 ms.

The straight binary (SB) time-of-day code word normally found between position identifiers P_8 and P_0 is eliminated for FAA IRIG B. All elements between position identifiers P_8 and P_0 are set to Binary 0.

5.5.4 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 SecureSync uses the Control Function field to encode year data, time synchronization status, and SBS time data. Table B-2 lists the Control Function Field and each element's function.

Element 55 is the time synchronization status bit. Element 55 is a Binary 1 when the front panel time synchronization lamp is green, and a Binary 0 when the lamp is red.

Year information consists of the last two digits of the current year (i.e. 98, 99, etc.). Elements 60 through 63 contain the binary equivalent of year units. Elements 65 through 68 contain the binary equivalent of tens of years. In keeping with IRIG formats, the least significant bit occurs first.

Elements 80 through 97 are encoded with the Straight Binary Seconds (SBS) time data. The SBS time data is incremented in 10-second steps and recycles every 24 hours.

- Pulse rates:
  - Element rate: 10 per second.
  - Position identifier rate: 1 per second.
  - Reference marker rate: 1 per 10 seconds.
- Element identification: The "on time" reference point for all elements is the pulse leading edge.
- Index marker (Binary 0 or uncoded element): 20 millisecond duration.
- Code digit (Binary 1): 50 millisecond duration.
- Position identifier: 80 millisecond duration.
- Reference marker: 80 millisecond duration, 1 per 10 seconds. The reference marker appears as two consecutive position identifiers. The second position identifier or reference marker is the on-time point for the succeeding code word.

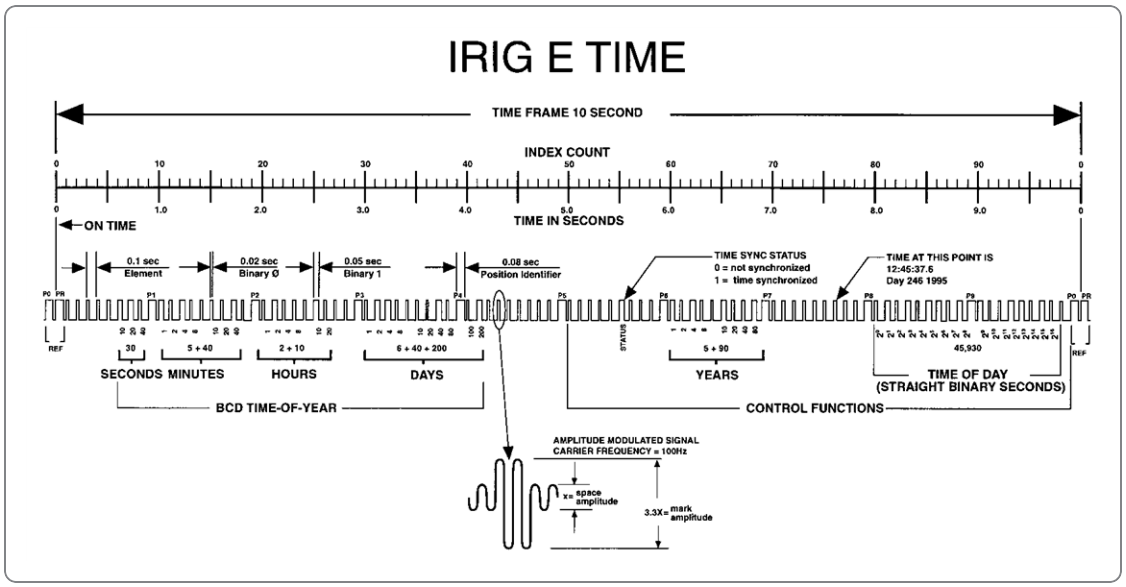


Figure 5-73: IRIG E time code description

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 5-31: 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

5.5.5 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

5.6 Strain Relief Ancillary Kit

The Strain Relief Anc Kit is designed to provide cable management, strain relief, and grounding, for the SecureSync 2400 model. It features a rear bracket set and an additional L-shaped bracket with an added hole pattern which allows configurable orientation and strain relief for the antenna mount, and attachment of ground. A connective cross bar provides additional strain relief of other cabling.

5.6.1 Product Description

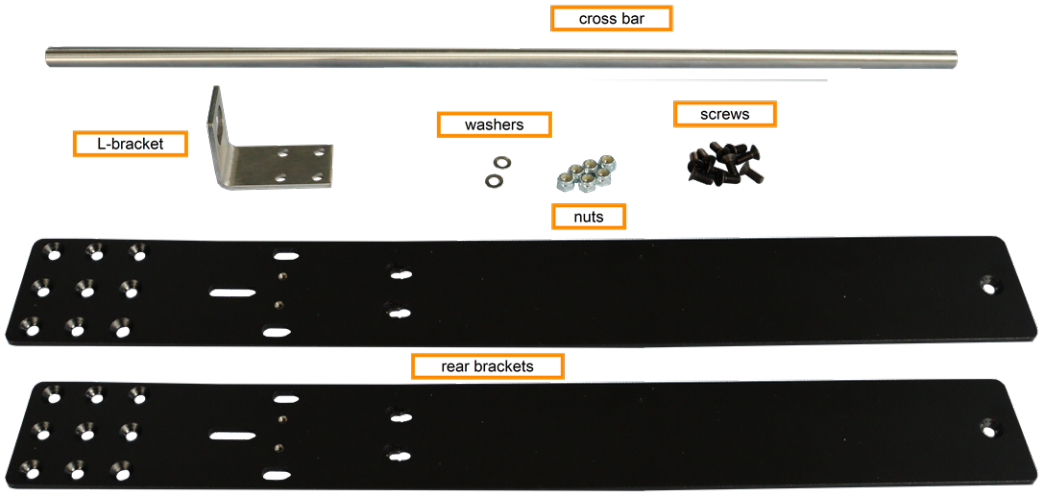


Figure 5-74: All parts included in the Strain Relief Anc Kit

The Strain Relief Anc Kit (part number 2400-0000-0715) includes the following materials:

- (2) Rear bracket (2400-1000-0795)
- L Bracket (2400-1000-0797)
- Cross Bar (2400-1000-0798)
- (10) M4 x 10MM Screws (HM20R-04R7-0010)
- (6) M4 x 4MM Nuts (HM72R-04R7-0003)
- (2) M4 Washers (HM30R-0400-0001)
- Installation Guide (this document)

5.6.2 Installation

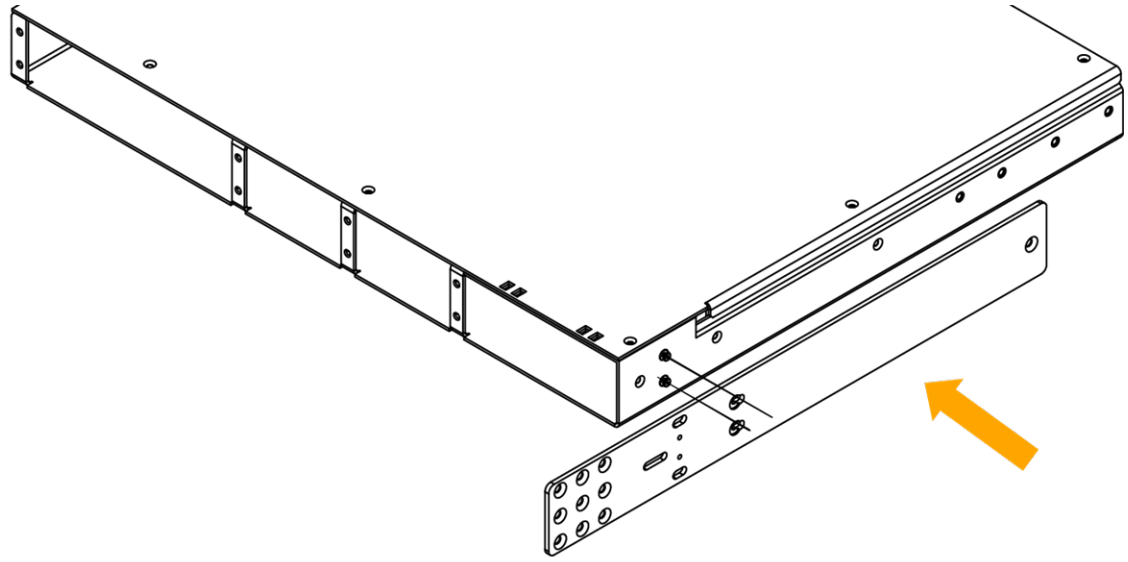
The Strain Relief Anc Kit is designed to allow for user customization to suit different rack mounting, cable management, and grounding needs. Not all installation procedures listed within this document and not all hardware included will be needed for every installation.

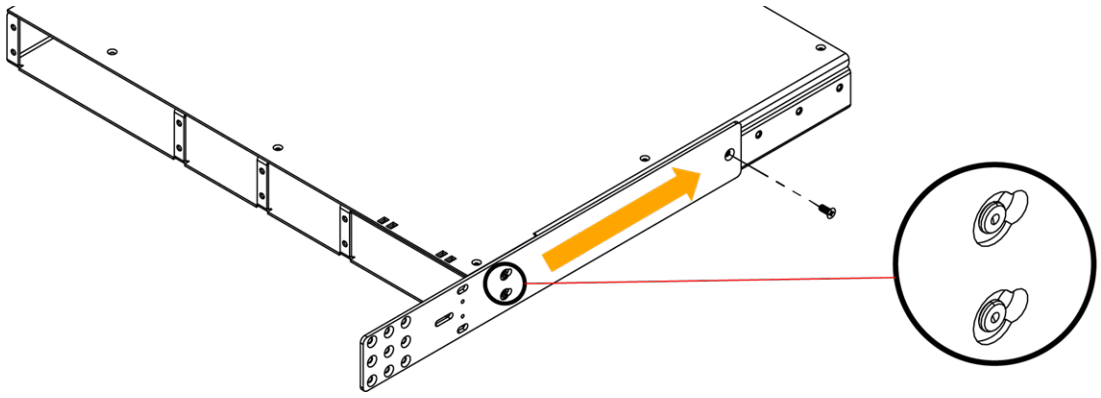
First, install the rear mounting brackets. Next, the L-bracket and cross bar both connect to available holes on the rear brackets.

5.6.2.1 Install rear-mounting brackets

The two rear bracket sections (2400-1000-0795) are identical and are installed on each side of the SecureSync 2400.

Align the rear mount bracket with the SecureSync unit as shown below. Insert the pegs into the fastening slot and slide the bracket toward the front panel (see images below).



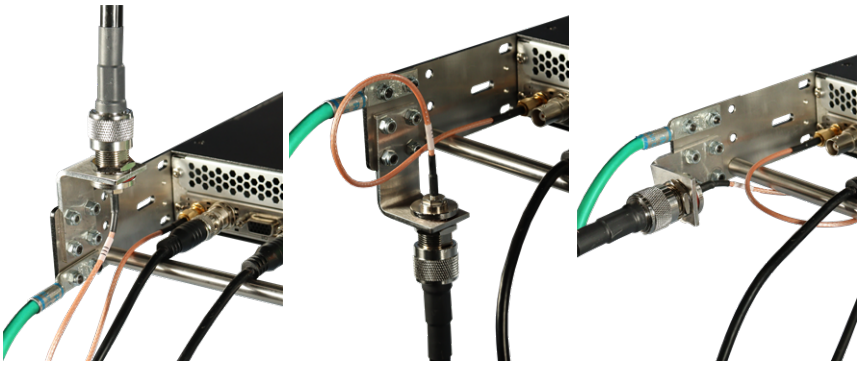


Install (1) screw on each bracket to secure.

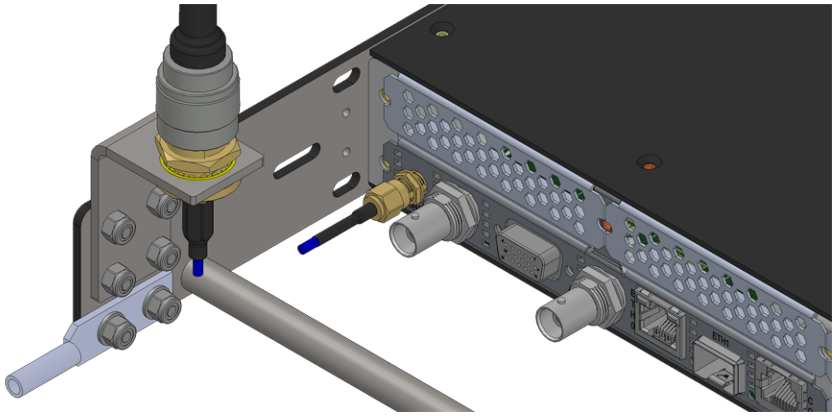
5.6.2.2 Install the L-bracket

The single L-shaped bracket (2400-1000-0797) is designed to provide cable strain relief for the SMA to N-type adapter cable (included with the SecureSync 2400 in ancillary kit 2400-0000-0701). It can also house connection for a grounding cable, such as a customer-supplied LCD6-14A-L ground terminal.

To install the L-bracket, first choose an installation orientation. Depending on the unit's rack location, as well as the location and direction of the antenna cable, the connector can be installed to face upward, outwards, or downwards, on four of the nine available holes in the rear mounting bracket. See installation orientation examples in the following images:

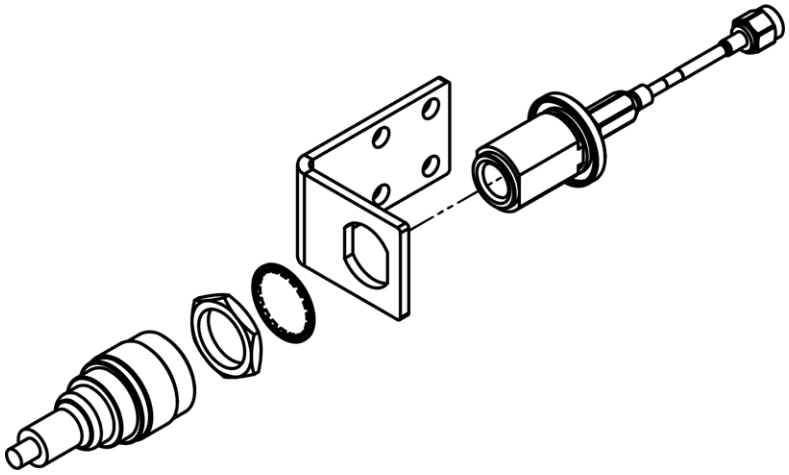


The bracket will be installed on the rear mounting bracket that is closest to the GNSS connector. Using four HM20R-04R7-0010 screws and four HM72R-04R7-0003 nuts, secure the L-bracket to the rear mount bracket:



To provide cable strain relief for the SMA-to-N-type GNSS cable:

1. Remove the nut and washer from N-type end of cable.
2. Slide N-type end of cable through L-bracket, add washer and nut, and tighten to torque.

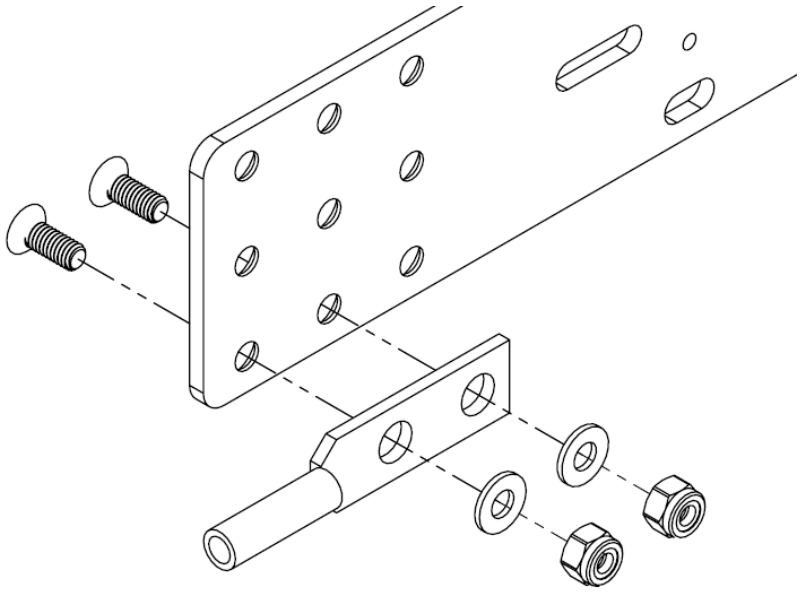


3. Secure the SMA plug end of the cable to the GNSS connector to torque.

5.6.2.3 Install a grounding cable

To secure a customer-supplied grounding cable to one of the rear mount brackets, choose an orientation and secure the ground terminal piece using two

HM20R-04R7-0010 screws, two HM72R-04R7-0003 nuts, and two HM30R-0400-0001 washers, occupying your chosen two holes in the rear bracket (see image below):



5.6.2.4 Install the cross bar

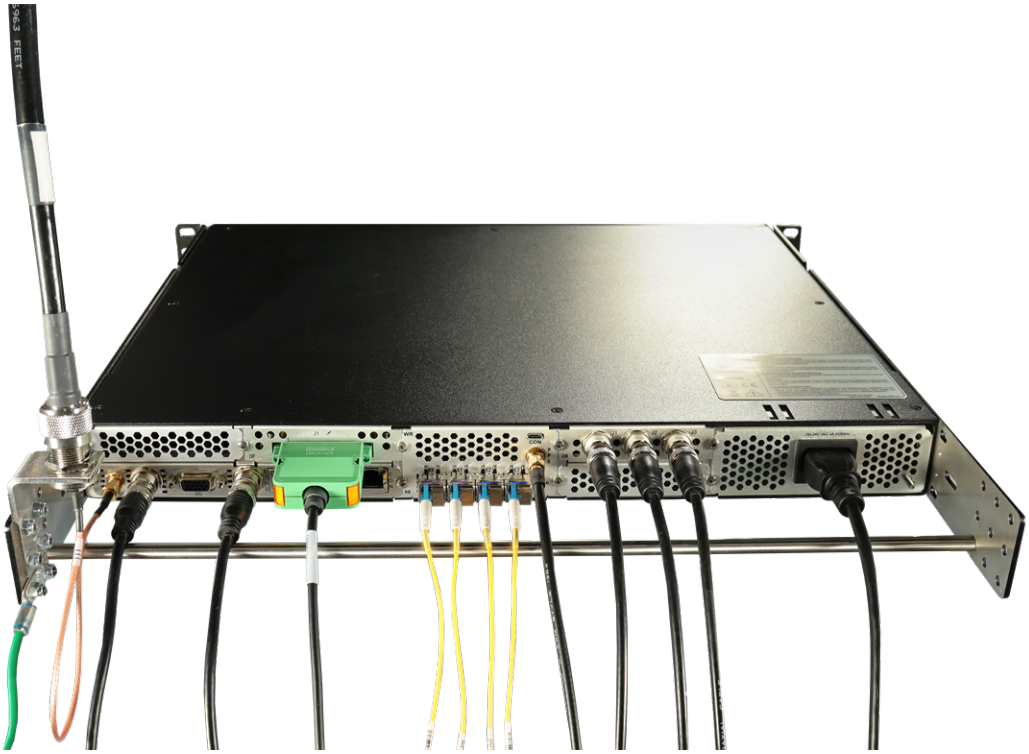


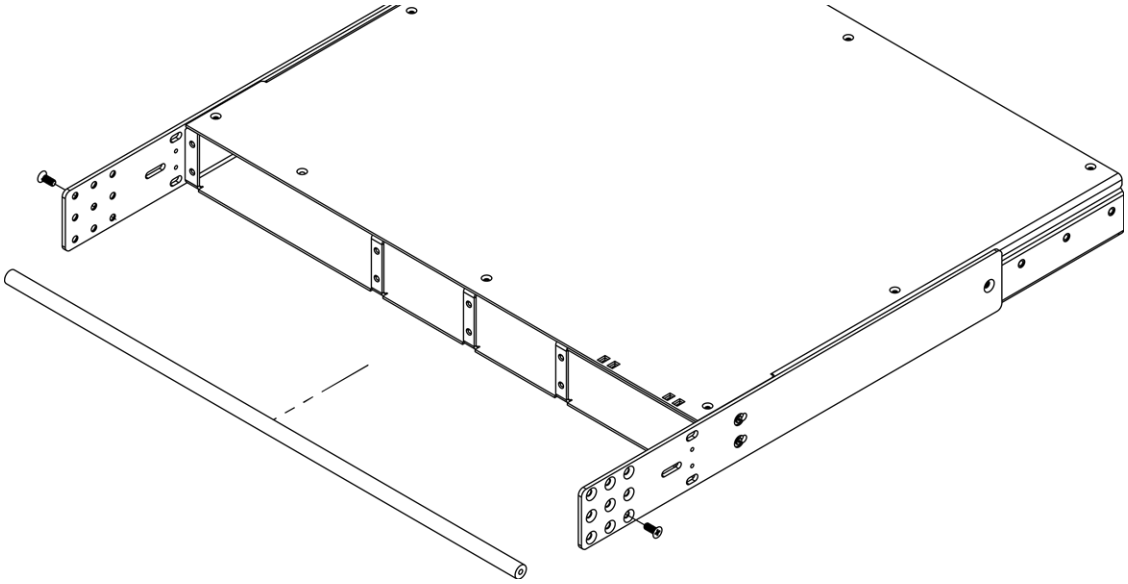
Figure 5-75: SecureSync with cross bar installed

The cross bar (2400-1000-0798) is especially useful to customers with multiple option cards to organize and reduce strain on cables extending from the unit; this is additionally true in installation environments without cable organization within mounting racks.

Note: The cross bar provided in this kit is not compatible with easy removal of hot-swap power supplies. Customers with hot swap power may select to omit using the cross bar or expect to uninstall the cross bar in order to remove or insert hot swap power sleds.

The cross bar is installed between the two rear-mounting backets and is affixed using a single HM20R-04R7-0010 screw on both ends (see image below).

Depending on your chosen location of the other parts of the kit, the bar can be installed in any of the nine sets of holes in the rear mount brackets.



Note: DC power supplies may interfere with locations of the cross bar closest to the unit.

5.7 Maintenance

Safran recommends regularly cleaning the inlet air vents of your SecureSync unit to ensure long term functionality.

SecureSync 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 Technical Support

To request technical support for your SecureSync unit, please go to the "Timing Support" page of the Safran website, where you can not only submit a support request, but also find additional technical documentation.

Phone support is available during regular office hours under the telephone numbers listed below.

To speed up the diagnosis of your SecureSync, please send us:

- the current **product configuration** (see "Option Card Identification" on page 21 to find out which option cards are installed in your unit), and
- the **events log** "Saving and Downloading Logs" on page 355).

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.

5.8.1 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/

5.8.2 Regional Contact

Safran operates globally and has offices in several locations around the world. Our main offices are listed below:

Country	Location	Phone
France	Les Ulis	+33 (0)1 6453 3980
Spain	Granada	+34 958 285 024
USA	West Henrietta, NY	+1.585.321.5800

Table 5-32: Safran contact information

Additional regional contact information can be found on the Contact page of the Safran Trusted 4D website.

5.9 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.

5.10 List of Tables

Table 1-1: Common light patterns 5
Table 1-2: Legend for Status LEDs 5
Table 1-3: Ethernet status indicator lights 14
Table 1-4: Option cards identification 17
Table 1-5: Option cards listed by their ID number 21
Table 1-6: Option card connectors 24
Table 1-7: 10 MHz output — oscillator types and accuracies 26
Table 1-8: 10 MHz output — oscillator stability 27
Table 1-9: Multi I/O connector signal pinout 29
Table 1-10: Multi I/O signal defaults 30
Table 1-11: 1PPS output accuracies 30
Table 2-1: Safety symbols used in this document, or on the product 45
Table 2-2: SecureSync 2400 Power Supply via Part Number 53

Table 2-3: Subnet mask values 70
Table 2-4: System Time Message format 111
Table 2-5: System Time Message field descriptions 111
Table 2-6: DCLS Output Options 172
Table 2-7: Multi I/O Input and Output Options 172
Table 2-8: Signature control output-presence states 199
Table 3-1: Reference priority titles 218
Table 3-2: Receiver dynamics, ~modes, ~ dynamics, ~ types 251
Table 3-3: Estimated Phase Drifts 267
Table 3-4: Typical Holdover lengths in seconds 268
Table 3-5: TFOM to ETE conversion 272
Table 4-1: Default and recommended configurations 368
Table 5-1: Troubleshooting network connection issues 376
Table 5-2: Troubleshooting using the Web UI Status indications 377
Table 5-3: Troubleshooting outputs not being present 380
Table 5-4: Parts list, Ancillary Kit [1204-0000-0700] 392
Table 5-5: Installation steps 395
Table 5-6: Model 1204-03 1PPS/Freq Input: Connector pin assignment 421
Table 5-7: Model 1204-30 terminal block pin assignments 433
Table 5-8: DB-9 pin-out 440
Table 5-9: RJ-12 pin assignments 441
Table 5-10: CTCSS exact (1/3 Hz) tones 445
Table 5-11: CTCSS exact (1/10 Hz) tones 446
Table 5-12: Data Clock Signals 446
Table 5-13: 1PPS Duty Cycle 446
Table 5-14: 1204-0A option card pin assignments 449
Table 5-15: 1204-4C option card pin assignments 452
Table 5-16: 1204-22 terminal block pin-out 457
Table 5-17: Accepted IRIG reference formats 465
Table 5-18: Additional IRIG reference formats for 1204-05 466
Table 5-19: Models 1204-11, -25: DB-25 pin-out 477
Table 5-20: 1204-1D, 1204-24 option cards: DB-25 pin-outs 485
Table 5-21: 1204-1B terminal block pin-out 494
Table 5-22: Pin-out, OUTPUT connector "J1" 506
Table 5-23: Pin-out, INPUT connector "J2" 507
Table 5-24: Pin-out, RS-485 terminal block connector J1 508
Table 5-25: Clock class definitions 543
Table 5-26: Output connector DB-9: pin-out 568
Table 5-27: Quality indicators 600
Table 5-28: Available IRIG output signals 620
Table 5-29: IRIG B control function field 627

Table 5-30: FAA Time Error Indicators 630
Table 5-31: IRIG E control function field 635
Table 5-32: Safran contact information 646

5.11 List of Images

Figure 1-1: SecureSync front panel layout 4
Figure 1-2: Front panel LEDs 4
Figure 1-3: Status LED menu buttons 7
Figure 1-4: Front panel menu tree 8
Figure 1-5: Standard rear panel 13
Figure 1-6: Option Card ID number 21
Figure 1-7: Multi I/O connector, viewed in mating direction on rear of unit 29
Figure 1-8: CA08R-D500-0001 drawing 32
Figure 1-9: CA08R-0000-0010 drawing 33
Figure 1-10: Mechanical dimensions 34
Figure 2-1: Rack mount installation 49
Figure 2-2: Rear rack mount installation 50
Figure 2-3: DC Plug, 2-Pin and DC Plug, 3-Pin 54
Figure 2-4: DC Connector, 2-Pin and DC Connector, 3-Pin 55
Figure 2-5: Cable Clamp, DC Power 55
Figure 2-6: DC to AC Converter 56
Figure 2-7: Hot Swap Power Supply installation (rear view) 57
Figure 2-8: SecureSync front panel 61
Figure 2-9: Front panel keypad and menu buttons 66
Figure 2-10: IFF Autokey configuration example 132
Figure 2-11: All NTP Servers are synchronized 142
Figure 2-12: NTP Server 1 is out of sync 142
Figure 2-13: PTP setup screen 156
Figure 2-14: PTP Masters Overview Panel 156
Figure 2-15: PTP Master Overview Drop Down 157
Figure 2-16: PTP Slaves Overview Panel 158
Figure 2-17: PTP Slaves Overview Drop Down 158
Figure 2-18: Edit PTP Settings panel 160
Figure 2-19: PTP Statistics Panel 164
Figure 2-20: Multi I/O 15-pin connector, in mating direction from front 173
Figure 2-21: Option Card Rear Panel Image 196
Figure 3-1: How the System Time is derived 203

Figure 4-1: SecureSync front panel 278
Figure 4-2: Locked Front Panel Display 318
Figure 4-3: Login banner (example) 320
Figure 4-4: Front panel layout 322
Figure 4-5: Status LED menu buttons 322
Figure 5-1: Option card navigation 384
Figure 5-2: Unit rear view 394
Figure 5-3: Unit internal view (from rear) 394
Figure 5-4: Standoffs location 397
Figure 5-5: Connector installation 399
Figure 5-6: Washers & standoffs secured to chassis screw holes 400
Figure 5-7: Ribbon cable installation 401
Figure 5-8: Bottom card with standoffs installed 402
Figure 5-9: Ribbon cable installation 403
Figure 5-10: Connector installation 404
Figure 5-11: J Connectors (10MHz Outputs) 405
Figure 5-12: Completed installation 405
Figure 5-13: J Connectors (10MHz Outputs) 406
Figure 5-14: [Left] J19 Connector with 8 pins, [Right] J19 Connector with 6 pins, seen from rear of unit. 407
Figure 5-15: Cable routing 407
Figure 5-16: [Left] J19 Connector with 8 pins, [Right] J19 Connector with 6 pins, seen from rear of unit. 408
Figure 5-17: Cable routing 408
Figure 5-18: Model 1204-18 option card rear plate 410
Figure 5-19: Model 1204-19 option card rear plate 411
Figure 5-20: Model 1204-21 option card rear plate 412
Figure 5-21: Model 1204-2B option card rear plate 413
Figure 5-22: Model 1204-28 option card rear plate 415
Figure 5-23: Model 1204-2A option card rear plate 416
Figure 5-24: Model 1204-01 option card rear plate 420
Figure 5-25: Model 1204-03 option card rear plate 420
Figure 5-26: Model 1204-1C option card rear plate 428
Figure 5-27: Model 1204-08 option card rear plate 429
Figure 5-28: Model 1204-26 option card rear plate 429
Figure 5-29: Model 1204-13 option card rear plate 431
Figure 5-30: Model 1204-2F option card rear plate 432
Figure 5-31: Model 1204-30 option card rear plate 433
Figure 5-32: Model 1204-17 option card rear plate 436
Figure 5-33: Model 1204-14 option card rear plate 439
Figure 5-34: DB-9 connector pin-out 440
Figure 5-35: RJ-12 connector pin-out 441

Figure 5-36: Simulcast Alarm Output Status window 442
Figure 5-37: Model 1204-09 option card rear plate 448
Figure 5-38: Model 1204-0A option card rear plate 449
Figure 5-39: Model 1204-53 option card rear plate 451
Figure 5-40: Model 1204-4C option card rear plate 452
Figure 5-41: Model 1204-15 option card rear plate 455
Figure 5-42: Model 1204-1E option card rear plate 456
Figure 5-43: Model 1204-22 option card rear plate 456
Figure 5-44: Model 1204-05 option card rear plate 462
Figure 5-45: Model 1204-27 option card rear plate 463
Figure 5-46: Model 1204-11 option card rear plate 476
Figure 5-47: Model 1204-25 option card rear plate 477
Figure 5-48: Model 1204-1D option card rear plate 484
Figure 5-49: Model 1204-24 option card rear plate 485
Figure 5-50: Model 1204-10 option card rear plate 492
Figure 5-51: Model 1204-1B option card rear plate 493
Figure 5-52: Model 1204-29 option card rear plate 498
Figure 5-53: Model 1204-02 option card rear plate 505
Figure 5-54: OUTPUT connector J1 505
Figure 5-55: INPUT connector J2 506
Figure 5-56: Model 1204-04 option card rear plate 507
Figure 5-57: 1204-4A option card rear plate 515
Figure 5-58: 1204-49 option card rear plate 516
Figure 5-59: 1204-59 option card rear plate 520
Figure 5-60: 1204-58 option card rear plate 521
Figure 5-61: Model 1204-32 option card rear plate 535
Figure 5-62: Model 1204-3E option card rear plate 553
Figure 5-63: Model 1204-3E option card rear plate 560
Figure 5-64: Model 1204-0F option card rear plate 561
Figure 5-65: Contact closure relay pinouts 562
Figure 5-66: Model 1204-2E option card rear plate 566
Figure 5-67: Location of jumper switches 566
Figure 5-68: Model 1204-23 option card rear plate 568
Figure 5-69: Model 1204-5E option card rear plate 575
Figure 5-70: Model 1204-5F option card rear plate 575
Figure 5-71: IRIG B time code description 625
Figure 5-72: FAA modified IRIG B 631
Figure 5-73: IRIG E time code description 634
Figure 5-74: All parts included in the Strain Relief Anc Kit 638
Figure 5-75: SecureSync with cross bar installed 643

5.12 Document Revision History

Rev	Description	Date
1	First generation SecureSync 2400 product manual	September 2019
1	2400-5000-0050p release for special configuration	December 2019
2	Updated option card availability, added security pages for LDAP, RADIUS, and TACACS+. New oscillator availability and Hot Swap Power Supply added. Corrected CLI Commands page. Newest generation hardware images added. Numerous editorial and document maintenance changes.	February 2021
3	Edits to reflect latest software updates. Refreshed PTP information and instruction. Updated option cards lists. Corrected various website links.	November 2021
4	Added CA08R-D500-0001 drawing. Added additional PTP profiles.	December 2021
5	Added information on new Sanitizing data procedure, rollback and downgrade feature information. Added information on DC power (fixed and hot swap) and HSTS and Security Issues Web UI page descriptions.. Added hot swap monitoring information.	October 2022
5.1	Updated Shock and vibration specifications. Corrected missing Sanitization procedure. Corrected LDAPs description. Added Authentication user permissions. Error corrections.	February 2023
5.2	Corrected oscillator specifications, corrected minor errors. Switch to Safran Trusted 4D branding.	August 2023
5.3	Fixed font render errors in specifications.	September 2023
6.0	Added new PTP page information. Updated product images. Switched to Safran Trusted 4D branding.	November 2023
7.0	Updated all Web UI images to reflect new design; added 12-hour time, AGNSS, and PTP graphs.	March 2024
7.1	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
8	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
8.1	Added information on effects of enabling OpenSSL Enhanced Security Core Mode.	October 2024
9	Added new information about NTP 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
9.1	WROX cards information modifications.	March 2025
10	Added new information on cooling fan Web UI status indicator, fan troubleshooting, and fan status CLI command.	May 2025
10.1	Added information on new PTP Master Settings panel, added cable strain relief anc kit information, and other minor fixes.	August 2025
11	Added information on new DNNSEC configuration feature, configurable FIPS compliance settings, reboot after sanitization feature, TOD1D ASCII data message format, and NavIC option cards. Added drawing of NENA breakout cable. Other minor fixes.	November 2025
11.1	Minor fixes.	November 2025

INDEX

#

10 MHz 195
15 pin 28

A

Access control 74
A-GPS 263
Alarm threshold, GPS Notification Alarm 285
Ancillary kit 43, 49
Anycast
  Configuring 142-144
  NTP over ... 141
Anycast, Advanced Configuration via NTP Expert Mode 147
Authentication 290
Authorized keys file 96

B

Battery 210
Battery Backed Time 209
BBC Message Formats 611
BGP (Border Gateway Protocol) 145
Border Gateway Protocol (BGP) 145
Browser support 376

C

Cable delay 253
Certificate, HTTPS 89
CLI 577
Command-line interpreter 575
Connector, DC power 54
contact, Safran Trusted 4D 645
Cookies 71

D

Daylight Savings Time 215
DC connector 54
DC power connector 54
default IP address 64
Desktop operation 48
disk status
  memory status 375
DST 215
Duplex, FULL, HALF 331

E

EMC compliance 40

Emissions
Electro-magnetic compliance 40
EndRun Formats 617
Engine Id 109
Ephemeris 578
EST API 317
Estimated Time Error 272
ETE 272
Ethernet
configuration 73
Expert Mode, Anycast 147
extension board 15

F

FCC compliance 39
Frequency band
Signal type 231
Front panel
information display 3, 6
keypad 3, 6
layout 4
status LEDs 4
time display 3

G

GNSS
Connecting 50
GNSS receiver modes 248
GNSS reference, about 247
GPSD 170
GSSIP Message Format 616

H

HALT command 279
HD15 28
Holdover 6, 30, 107, 123, 144-146, 195, 198, 208, 217, 223-224, 231, 265, 269, 271, 275, 281-282, 284, 324, 330, 337, 349, 374, 377, 379-380, 382, 541
Host disciplining 151
Host keys, SSH 93
HTTPS 80

I

IPv4 76
IRIG
output accuracy 636
Standards 619
IRIG Carrier Frequencies 620
IRIG output resolution 460

K

Keys, host 94

L

LDAP 299
Leap second 170, 183, 193, 211, 459, 468, 514, 546, 574, 598, 600, 602-603, 607, 612, 618
license file
applying 361
Local clock 214
Local System Input Reference 223
Log entries 375

Logging into the Web UI 72
Login banner 74
Login Web UI 72

M

Main Screen of Web UI 36
Manual time, setting (User) 205
memory status
  disk status 375
MIB files 103
Mobile GNSS receiver mode 249
Mobile mode dynamics 250
Moving, unit 255

N

Netmask 76
Network port, enabling 76
Network services 77
Network setup 73
NMEA 585, 587-589, 591-592
Non-volatile memory 369
Notifications 281
NTP 113, 141
  autokey 130
  Expert Mode 116, 151
  Peers 123-124, 128
  Servers 123-125
  Setup screen 114
  stratum 120
  Symmetric Keys 136
  time stamp 119
  timescale 119
NTP Peer Preference 129

O

Offset 185
Offset, GNSS receiver 252
On-time point 185
Option card 21
  identification 21
Option card installation 390
Oscillator
  accuracies 26
Oscillator configuration 271
OSPF IPv4 143
OSPF IPv6 144

P

Phase 229, 328
Phase error limit 271
Phase Offset 230, 329
Phase validity monitoring 230, 329
PLL, external 270
Port, network, enabling 76
Power
  connecting 52
  connector, DC, AC 13
  consumption 25
  DC connector, pin-out 52
PPS status light is yellow 231, 330
Preferred NTP Peer 129
Preferred NTP Server 128
Primary Navigation menu 36
Private keys, SSH 95
PTP
  one-step mode 545

two-step mode 545
Public keys, SSH 96

R

Rack mounting 49
RADIUS 306
Real Time Clock 209
Rear panel 13
Recalibrate oscillator 272
Reference Priorities
Configuring 219
Reference Priority, examples 225
Registration, product 321
Regulatory compliance 39
Relocating, GNSS receiver 255
Resetting GNSS receiver position 255
RINEX Server 263
Rinex/Yuma files 262
Route, static, add 78
Routes, static 74

S

Safety
instructions
symbols 45
Symbols 45
Sanitization 255
Sanitization, sanitizing 369
SCP 98
Screen clock 321
Self survey 255
Self survey, GNSS position 255-256
Self survey, GNSS receiver 255
SFTP 98
Shipment, return 646
Show Clock 321
Signal type
Frequency band 175, 183, 436, 443, 469
Signature control 198
Single satellite GNSS receiver mode 249
Smart reference monitoring 230, 329
SNMP 99
SNMP traps 100
software version
version number, software 375
Specifications 25, 420
Spectracom Format 593
SSH 91
SSH clients 99
SSH timeout 99
Standard GNSS receiver mode 248
Standards compliance 39
start
getting started 2
Static Route, add 78
Static Routes 74
STL 552
Subnet mask values 70
subnet mask; default 65, 68
Subnet, default 76
Summer Time 215
Survey, GNSS 248, 252, 255
Symmetric keys 115

Synchronizing Windows computers 322
System on-time point 185
System Time 123, 205

T

TACACS+ Authentication 310
Technical support 645
Temperature 275, 337
  operating, range 25
Terminal emulator 575
TFOM 271
Timeout 73
Timeout, Web UI, automatic 298
Troubleshooting 375

U

Unicast 113
Update, software 359
Upgrade, software 359
User time, manually setting 205
Usernames, rules 292

V

VLAN 110
Volatile memory 369

W

Web Interface Settings 298
Web UI, opening 71

Y

Yellow PPS status light 231, 330
Yellow status light 231, 330

Z

Zero Configuration Setup 62
zeroconf 62