SEL-2488

Satellite-Synchronized Network Clock

Instruction Manual

20241003

SCHWEITZER ENGINEERING LABORATORIES

Part Number: PM2488-01

Table of Contents

Section 13: Hostname Resolution

Section 14: Event Reporting System

Section 15: Alarm Contact

Section 16: Syslog Reporting

Section 17: Simple Network Management Protocol (SNMP)

Section 18: Usage Policy

Section 19: Date/Time

Section 20: Global Settings

Appendix A: Firmware and Manual Versions

Appendix B: Precision Time Protocol Field Upgrade Instructions

Appendix C: Link Budget Analysis

Appendix D: Syslog

Appendix E: IRIG-B

Appendix F: X.509

Appendix G: Configuring Windows Network Parameters

Appendix H: Lightweight Directory Access Protocol

Appendix I: Cybersecurity Features

This page intentionally left blank

List of Tables

List of Figures

Preface

Safety Information

Dangers, Warnings, and Cautions

This manual uses three kinds of hazard statements, defined as follows:

⚠DANGER
Indicates an imminently hazardous situation that, if not avoided, **will** result in death or serious injury.

⚠WARNING
Indicates a potentially hazardous situation that, if not avoided, **could** result in death or serious injury.

⚠CAUTION
Indicates a potentially hazardous situation that, if not avoided, **may** result in minor or moderate injury or equipment damage.

Safety Symbols

The following symbols are often marked on SEL products.

	**⚠CAUTION** Refer to accompanying documents.	**⚠ATTENTION** Se reporter à la documentation.
	Earth (ground)	Terre
	Protective earth (ground)	Terre de protection
	Direct current	Courant continu
	Alternating current	Courant alternatif
	Both direct and alternating current	Courant continu et alternatif
	Instruction manual	Manuel d'instructions

Safety Marks

The following statements apply to this device.

General Safety Marks

⚠CAUTION There is danger of explosion if the battery is incorrectly replaced. Replace only with Panasonic BR2330A or equivalent recommended by manufacturer. See Owner's Manual for safety instructions. The battery used in this device may present a fire or chemical burn hazard if mistreated. Do not recharge, disassemble, heat above 100°C or incinerate. Dispose of used batteries according to the manufacturer's instructions. Keep battery out of reach of children.	**⚠ATTENTION** Une pile remplacée incorrectement pose des risques d'explosion. Remplacez seulement avec un Panasonic BR2330A ou un produit équivalent recommandé par le fabricant. Voir le guide d'utilisateur pour les instructions de sécurité. La pile utilisée dans cet appareil peut présenter un risque d'incendie ou de brûlure chimique si vous en faites mauvais usage. Ne pas recharger, démonter, chauffer à plus de 100°C ou incinérer. Éliminez les vieilles piles suivant les instructions du fabricant. Gardez la pile hors de la portée des enfants.
⚠CAUTION To ensure proper safety and operation, the equipment ratings, installation instructions, and operating instructions must be checked before commissioning or maintenance of the equipment. The integrity of any protective conductor connection must be checked before carrying out any other actions. It is the responsibility of the user to ensure that the equipment is installed, operated, and used for its intended function in the manner specified in this manual. If misused, any safety protection provided by the equipment may be impaired.	**⚠ATTENTION** Pour assurer la sécurité et le bon fonctionnement, il faut vérifier les classements d'équipement ainsi que les instructions d'installation et d'opération avant la mise en service ou l'entretien de l'équipement. Il faut vérifier l'intégrité de toute connexion de conducteur de protection avant de réaliser d'autres actions. L'utilisateur est responsable d'assurer l'installation, l'opération et l'utilisation de l'équipement pour la fonction prévue et de la manière indiquée dans ce manuel. Une mauvaise utilisation pourrait diminuer toute protection de sécurité fournie par l'équipement.
The SEL-2488 battery is the only field-serviceable part (see *Battery Change Instructions* in the instruction manual). For all other repairs, return the faulty or failed unit to the factory for repair or replacement.	La batterie SEL-2488 est la seule pièce réparable sur site (voir la section *Battery Change Instructions* dans le manuel d'instructions). Pour toutes les autres réparations, renvoyez l'unité défectueuse à l'usine pour la réparer ou la remplacer.
For use in Pollution Degree 2 environment.	Pour l'utilisation dans un environnement de Degré de Pollution 2.
Overvoltage Category: II	Catégorie de surtension : II
Insulation Class: I	Classe d'isolation : I
Ambient air temperature shall not exceed 40°C (104°F) in locations where touch temperature safety is required.	La température ambiante de l'air ne doit pas dépasser 40°C (104°F) dans des endroits où la température des surfaces doit être suffisamment basse pour les toucher en toute sécurité.
Ambient air temperature shall not exceed 85°C (185°F).	La température ambiant de l'air ne doit pas dépasser 85°C (185°F).
For use in a Nema Type 1 enclosure or greater.	Pour utilisation dans un boîtier de Type 1.
IP Rating: IP3X	Indice de protection: IP3X

Other Safety Marks (Sheet 1 of 2)

⚠DANGER Disconnect or de-energize all external connections before opening this device. Contact with hazardous voltages and currents inside this device can cause electrical shock resulting in injury or death.	**⚠DANGER** Débrancher tous les raccordements externes avant d'ouvrir cet appareil. Tout contact avec des tensions ou courants internes à l'appareil peut causer un choc électrique pouvant entraîner des blessures ou la mort.
⚠DANGER Contact with instrument terminals can cause electrical shock that can result in injury or death.	**⚠DANGER** Tout contact avec les bornes de l'appareil peut causer un choc électrique pouvant entraîner des blessures ou la mort.
⚠DANGER Safety insulation is not provided between output contact terminals. If hazardous live voltage is attached to one terminal, all contact output terminals must be treated as hazardous live. Failing to do so can cause electrical shock that can result in injury or death.	**⚠DANGER** L'isolation de sécurité n'est pas fournie entre les bornes de contact de sortie. Si une tension sous tension dangereuse est attachée à une borne, toutes les bornes de sortie de contact doivent être traitées comme sous tension dangereuse. Le nonrespect de cette consigne peut provoquer un choc électrique pouvant entraîner des blessures ou la mort.

Other Safety Marks (Sheet 2 of 2)

⚠WARNING Always use an overcurrent protection device such as a circuit breaker or fuse. The contact output must operate on the load side of the overcurrent protection device. The type and size of the overcurrent protection device must be appropriate for the connected load and wiring.	**⚠AVERTISSEMENT** Utiliser toujours un dispositif de protection contre les surintensités tel qu'un disjoncteur ou un fusible. La sortie doit fonctionner du côté de la charge du dispositif de protection contre les surintensités. Le type et la taille du dispositif de protection contre les surintensités doivent être adaptés à la charge et au câblage connectés.
⚠WARNING Earth connection is essential before making telecommunication network connections. Earth ground connections should not be removed when the equipment is energized.	**⚠AVERTISSEMENT** Une connexion à la terre est essentielle avant de faire des connexions au réseau de télécommunications. Il ne faut pas enlever les connexions de mise à la terre pendant que l'équipement est sous tension.
⚠WARNING Use of this equipment in a manner other than specified in this manual can impair operator safety safeguards provided by this equipment.	**⚠AVERTISSEMENT** L'utilisation de cet appareil suivant des procédures différentes de celles indiquées dans ce manuel peut désarmer les dispositifs de protection d'opérateur normalement actifs sur cet équipement.
⚠WARNING Have only qualified personnel service this equipment. If you are not qualified to service this equipment, you can injure yourself or others, or cause equipment damage.	**⚠AVERTISSEMENT** Seules des personnes qualifiées peuvent travailler sur cet appareil. Si vous n'êtes pas qualifiés pour ce travail, vous pourriez vous blesser avec d'autres personnes ou endommager l'équipement.
⚠WARNING Do not perform any procedures or adjustments that this instruction manual does not describe.	**⚠AVERTISSEMENT** Ne pas appliquer une procédure ou un ajustement qui n'est pas décrit explicitement dans ce manuel d'instruction.
⚠WARNING Incorporated components, such as LEDs and transceivers, are not user serviceable. Return units to SEL for repair or replacement.	**⚠AVERTISSEMENT** Les composants internes tels que les leds (diodes électroluminescentes) et émetteurs-récepteurs ne peuvent pas être entretenus par l'usager. Retourner les unités à SEL pour réparation ou remplacement.
⚠CAUTION Equipment components are sensitive to electrostatic discharge (ESD). Undetectable permanent damage can result if you do not use proper ESD procedures. Ground yourself, your work surface, and this equipment before removing any cover from this equipment. If your facility is not equipped to work with these components, contact SEL about returning this device and related SEL equipment for service.	**⚠ATTENTION** Les composants de cet équipement sont sensibles aux décharges électrostatiques (DES). Des dommages permanents non-décelables peuvent résulter de l'absence de précautions contre les DES. Raccordez-vous correctement à la terre, ainsi que la surface de travail et l'appareil avant d'en retirer un panneau. Si vous n'êtes pas équipés pour travailler avec ce type de composants, contacter SEL afin de retourner l'appareil pour un service en usine.
⚠CAUTION Insufficiently rated insulation can deteriorate under abnormal operating conditions and cause equipment damage. For external circuits, use wiring of sufficiently rated insulation that will not break down under abnormal operating conditions.	**⚠ATTENTION** Un niveau d'isolation insuffisant peut entraîner une détérioration sous des conditions anormales et causer des dommages à l'équipement. Pour les circuits externes, utiliser des conducteurs avec une isolation suffi-sante de façon à éviter les claquages durant les conditions anormales d'opération.
⚠CAUTION In order to avoid losing system logs on a factory-default reset, configure the SEL-2488 to forward syslog messages.	**⚠ATTENTION** Pour éviter de perdre les enregistrements du système sur un redémarrage défini par défaut, configurer le SEL-2488 pour envoyer les messages de l'enregistreur du système ("syslog").
⚠CAUTION Class 1 LASER Product. This product uses visible or invisible LASERs based on model option. Looking into optical connections, fiber ends, or bulkhead connections can result in hazardous radiation exposure.	**⚠ATTENTION** Produit LASER de Classe 1. Ce produit utilise des LASERS visibles ou invisibles dépendant des options du modèle. Regarder vers les connecteurs optiques, les extrémités des fibres ou les connecteurs de cloison peut entraîner une exposition à des rayonnements dangereux.

General Safety Notes

- The SEL-2488 is designed for restricted access locations. Access should be limited to qualified service personnel.
- The SEL-2488 should neither be installed nor operated in a condition this manual does not specify.
- Installation of transient voltage surge suppressors external to the International Technology Equipment (ITE) to reduce overvoltages or to bypass surge current shall be installed per article 285 of ANSI/NFPA 70.

Cleaning Instructions

- The device should be de-energized (by removing the power connection to both the power and alarm connection) before cleaning.
- The case can be wiped down with a damp cloth. Solvent-based cleaners should not be used on plastic parts or labels.

Battery Change Instructions

The battery in the SEL-2488 maintains power to the real-time clock so that it retains the time through power cycles. The battery is rated to last more than 10 years, but if you need to change the battery, use the following steps:

Step 1. Disconnect power from the SEL-2488.

Step 2. Remove all communication and alarm contact cabling and remove the unit from its mounting.

Step 3. Ground yourself, your workstation, and the SEL-2488 to the same ground.

Step 4. Remove the screws on the top lid of the chassis, and then remove the top lid itself. The battery is located in the top left corner of the main board (when viewing from the rear).

Step 5. Replace the battery with a Panasonic BR2330A or equivalent recommended by the manufacturer.

Step 6. Reassemble the device and return it to service.

Step 7. Dispose of the battery to a qualified recycle facility or a facility that supports a hazardous waste disposal program suitable for batteries.

Examples

This instruction manual uses several example illustrations and instructions to explain how to effectively operate the SEL-2488. These examples are for demonstration purposes only; the firmware identification information or settings values these examples include may not necessarily match those in your SEL-2488.

Trademarks

Trademarks appearing in this manual are shown in the following table.

ACSELERATOR QuickSet®	SEL ICON®
Job Done® example	SkyView®

Copyrighted Software

The software included in this product may contain copyrighted software licensed under terms that give you the opportunity to receive source code. You may obtain the applicable source code from SEL by sending a request to:

Legal Department
GPL Compliance
Schweitzer Engineering Laboratories, Inc.
One Schweitzer Drive
Pullman, WA 99163

Please include your return address, product number, and firmware revision.

Technical Support

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.338.3838
Fax: +1.509.332.7990
Internet: selinc.com/support
Email: info@selinc.com

This page intentionally left blank

Section 1
Clock Overview and Specifications

The SEL-2488 Satellite-Synchronized Network Clock receives Global Navigation Satellite System (GNSS) time signals and distributes precise time via multiple output protocols, including IRIG-B, Precision Time Protocol (PTP) and Network Time Protocol (NTP). The advanced capabilities of the SEL-2488 make it well suited for demanding applications like synchrophasors, and for substations with multiple time synchronization requirements.

Front-Panel Overview

Figure 1.1 Front-Panel View

Lamp Test

When pressed, the **LAMP TEST** button illuminates front-panel LED indicators and the LCD screen.

Device Status LEDs

The **ENABLED** indicator is green when the unit has passed self-tests and is operational. This indicator is unlit during startup. The **ALARM** indicator is unlit unless the unit asserts an alarm. A one-second blink indicates a minor alarm, while solid red indicates a major alarm. The **PWR A**/**PWR B** indicators will be green if that power supply is installed and healthy. If the unit detects a fault on a power supply, its indicator turns red. For units with redundant power supplies, loss of power in one supply causes that supply's LED to turn red. If a power supply is not installed, the corresponding indicator will be unlit. Device status LEDs are described in more detail in *Getting Started* and *Section 15: Alarm Contact*.

Port Activity LEDs

Each of the four rear-panel Ethernet ports has a pair of corresponding LED indicators on the front panel. The amber LED for port speed is positioned above the green LED for link activity. Refer to *Section 4: Ethernet Network Interfaces* for more information.

LCD Screen

The SEL-2488 is equipped with an LCD screen that provides information such as time, accuracy, satellite constellations, latitude/longitude/altitude, front Ethernet port (**ETH F**) Internet Protocol (IP) address, and major event messages. Pressing the **Up** and **Down** arrow pushbuttons next to the LCD screen navigates through the messages. You can also press and hold these buttons simultaneously to set display contrast. During clock startup, the LCD screen displays a sequence of status messages. These capabilities are described in *Section 22: LCD Screen*.

Time Status Indicators

The front panel of the clock displays several indicators of clock time input and output status. These indicators include the satellite lock status, time quality indication, antenna status, PTP/NTP status and activity, and OUT 1 status for timer contact. For more information on time status indicators, see *Section 3: Time Synchronization*, *Section 7: Precision Time Protocol (PTP)*, *Section 8: Network Time Protocol (NTP)*, and *Section 9: Timer Contact*.

Local Management Port (ETH F)

Use the front-panel Ethernet port for commissioning and management. For more detail, see *Section 4: Ethernet Network Interfaces*.

Rear-Panel Overview

Figure 1.2 Rear-Panel View Including Optional Frequency Outputs

Alarm and Timer Contact

The rear panel provides one Form C output mechanical alarm contact and one Form A solid-state timer contact. The timer contact is designed for testing external systems needing precise timing to trigger the start of an event. The functions of these contacts are described in *Section 9: Timer Contact* and *Section 15: Alarm Contact*.

Pinhole Reset

The rear panel includes a pinhole reset with two functions. The first function re-enables **ETH F** functionality. See *Section 4: Ethernet Network Interfaces* for details. The second function resets the device to factory defaults. See *Section 23: Device Reset* for more information.

BNC Time Outputs

The SEL-2488 comes standard with eight BNC time output ports, **T01**–**T08**. You can configure all eight of these outputs individually for demodulated IRIG-B, PPS, or kPPS formats. You can configure cable delay compensation for each of these outputs.

You can configure ports **T01**–**T04** for modulated IRIG-B.

See *Section 6: Time-Code Outputs* for more details.

SMA Frequency Outputs

With the purchase of the frequency outputs hardware option, the SEL-2488 comes with six SMA frequency outputs. One output (**F1**) is a frequency-disciplined, TTL-compatible 10 MHz square-wave frequency output and the remaining five (**F2**–**F6**) are frequency-disciplined 10 MHz sine-wave frequency outputs.

See *Section 26: Frequency Outputs* for more details.

Ethernet Ports

The four rear-panel Ethernet ports support 10/100 Mbps. Ports are orderable as 10/100BASE-T copper, 100BASE-FX, or 100BASE-LX in pairs. See *Section 4: Ethernet Network Interfaces* for more specifics.

DB-9 Port

COM 1 on the rear panel is a DB-9 female port. Pin 4 and Pin 6 transmit demodulated IRIG-B, PPS, or kPPS outputs. Cable delay compensation can be configured for this port. *Table 1.1* shows the pinout for the port. See *Section 6: Time-Code Outputs* for more details.

Table 1.1 DB-9 Port Pinout

Pin	Description
1	N/C
2	N/A
3	–9 Vdc
4	+IRIG-B
5	GND
6	–IRIG-B
7	+9 Vdc
8	N/C
9	N/C

TNC Antenna Input

An antenna cable, preferably an SEL-C961 LMR-400 cable, connects to the TNC antenna input. An SEL Surge Protector Kit (915900139) should also be used for lightning protection. SEL recommends using the SEL-9524B GPS/GLONASS GNSS Antenna. See *Getting Started* for complete antenna installation instructions.

IRIG-B Input

The SEL-2488 has an isolated IRIG-B input port (BNC). The functionality will be enabled in a future firmware release.

Redundant, Hot-Swappable Power Supplies

The SEL-2488 comes standard with one power supply. A second, optional power supply is available for powering with redundant sources. The second power supply can be connected to a separate power source. See *Getting Started* for more information on power supplies.

Grounding Lug

A grounding lug is located at the far right side of the clock rear panel. See *Getting Started* for grounding instructions.

HTTPS Device Webpage

Commission and manage the SEL-2488 through the device webpage. The Captive Port feature on the SEL-2488 provides a DHCP server and limited DNS resolver on the front Ethernet port for an easy initial connection to the clock. Secure access is controlled through X.509 certificates, user-based accounts, and Lightweight Directory Access Protocol (LDAP) authentication. The SEL device webpage includes a dashboard display of satellite signals for both GPS and GLONASS satellites. Bar charts indicate signal strengths, and SkyView displays present satellite azimuth and elevation information. This is useful for troubleshooting potential signal and antenna installation issues. *Figure 1.3* shows the dashboard display.

Figure 1.3 SEL-2488 Device Webpage With Dashboard Display

Getting Started

This section outlines the steps to install and commission the SEL-2488 with the appropriate accessories. These include the antenna and mounting, surge protection, power supplies, and appropriate cabling. For more details about the available accessories for the SEL-2488, see the *SEL Satellite-Synchronized Clocks Accessory Guide* available at the SEL-2488 product page at selinc.com/products/2488/.

Clock Installation and Grounding

The SEL-2488 is designed to mount in a standard 19-inch rack and is rated for indoor use. For optimal ambient heat dissipation, SEL recommends 1U of open spacing above and below the SEL-2488. Once the clock is mounted and before initial startup, make sure that the clock is properly grounded to the common building or substation ground system.

Unit Placement and Maintenance Physical Location

To satisfy safety requirements, the unit shall be installed in a suitable fire/electrical/mechanical enclosure. To protect against electrical shock hazards, the enclosure shall prevent access to the rear-panel power supply and I/O terminals during normal operation. For installations requiring additional

personnel protection against electrical energy hazard, apply the 915900656 Euro connector cover kit for the SEL-2488, double-insulated wiring, and/or approved wiring loom.

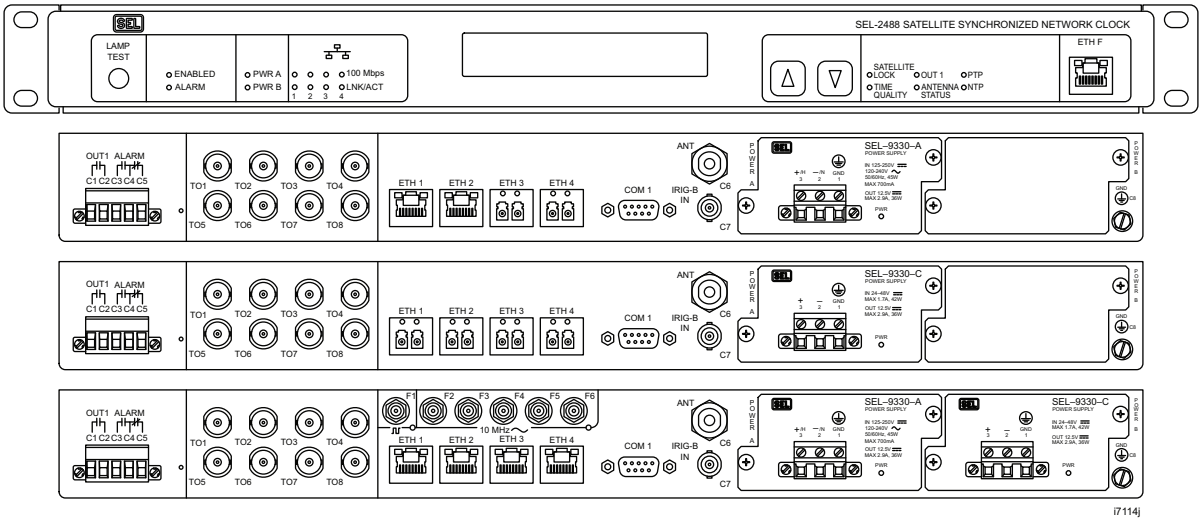


Figure 1.4 Front-and Rear-Panel Diagrams

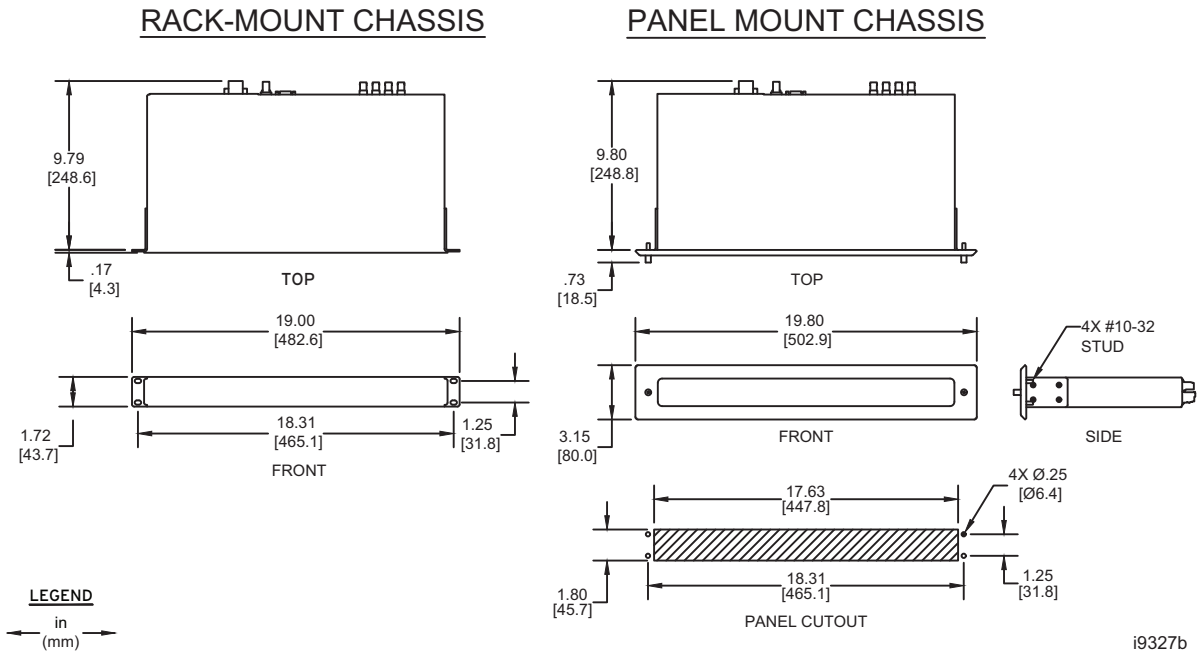


Figure 1.5 Dimensions for Rack- and Panel-Mount Models

Antenna and Mounting

The SEL-2488 requires the SEL-9524B GPS/GLONASS GNSS Antenna to achieve lock with satellite signal verification enabled. The SEL-2488 can achieve lock with a standard GPS antenna when satellite signal verification is disabled. For more information see *Satellite Signal Verification on page 3.1*.

The SEL-9524B GPS/GLONASS GNSS Antenna must be installed in accordance with national electrical codes. An unobstructed 360-degree view of the sky is required for reliable operation.

The antenna is housed in waterproof packaging designed to withstand exposure to the elements. It is equipped with a TNC female connector.

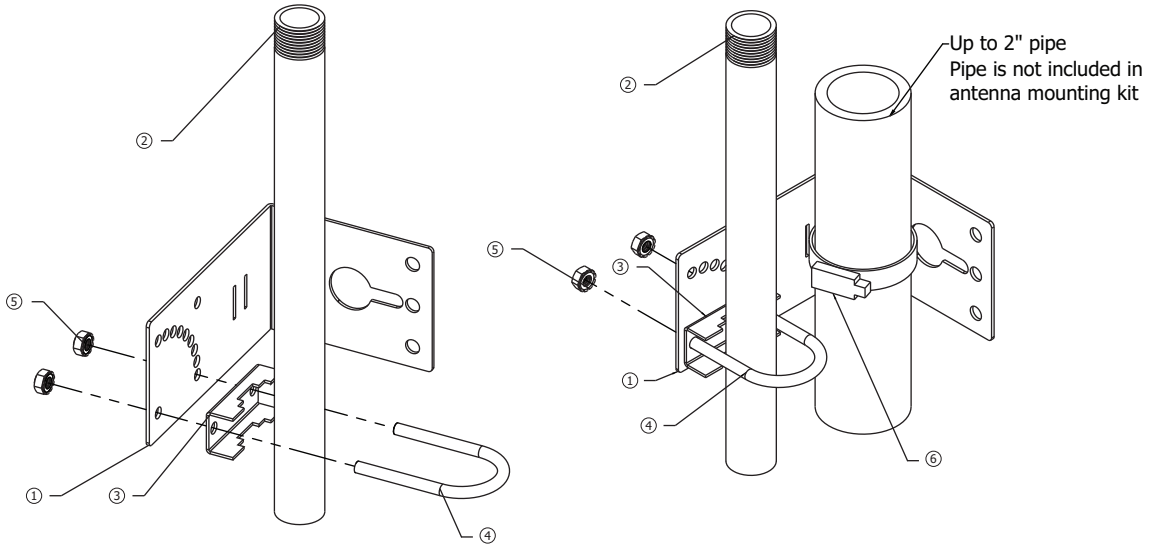
Figure 1.6 SEL-9524B GPS/GLONASS GNSS Antenna

The pipe-mount collar is designed to attach to a 1-inch outside diameter tube with 1 in.-14 straight thread. SEL offers a tube as a part of the Antenna Pipe Mounting Kit (915900043).

Position the antenna so that the top of the antenna points skyward. The antenna should be located low and close to the control house roof (above maximum snow accumulation and away from roof maintenance activities). From a surge perspective, mounting the antenna on an equipment building roof or cabinet is safest because the potential rise on the outside of either of these structures would be more or less equal to the potential on the inside.

When mounting multiple, co-located GNSS antennas, it is best practice to position the antennas as far apart as possible to prevent common mode disruptions such as lightning strikes, intermittent obstructions, or other environmental disturbances. However, when space is constrained, a minimum separation of 1 meter (~3 feet) between GNSS antennas is recommended. When located in close proximity, antennas should be mounted at the same height with an unobstructed view of the sky.

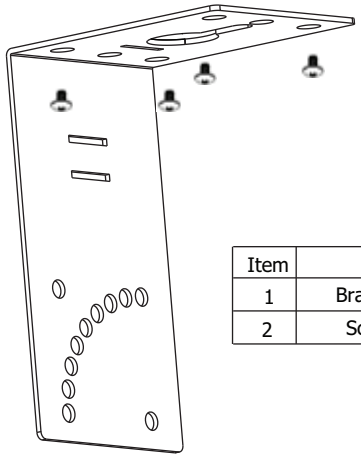
SEL offers mounting equipment as part of the Precise Timing product line. For the SEL-2488, most substation antenna installations will use a mast mount or pipe mount. SEL offers an Antenna Pipe Mounting Kit (915900043) that supports mounting to a wall or an existing pipe.



Item	Description	QTY.
1	Bracket, Antenna Mount	1
2	Mast, Pole Mount	1
3	Bracket, Stepped, U-Bolt Mount	1
4	U-Bolt, 1.75", SS	1
5	Nut, 1/4-20, 18-8 SS	2
6	Clamp, Worm-Drive, Pipe, 3.125-6"	1

Figure 1.7 Antenna Pipe Mounting Kit

SEL also offers an Antenna Surface Mounting Kit (915900044) for mounting the antenna directly to an external cabinet.



Item	Description	QTY.
1	Bracket, Antenna Mount	1
2	Screw, 10-32 x 5/16	4

Figure 1.8 Antenna Surface Mounting Kit

Surge Protection

This section outlines best practices for protecting the SEL-2488 from surge events. The surge protector protects the clock from a high-energy event. SEL offers the Gas Tube Coaxial Surge Protector and Mounting Kit (915900139).

Figure 1.9 Gas Tube Coaxial Surge Protector and Mounting Kit

The higher the GNSS antenna is mounted on a support structure, the greater the probability of equipment damage resulting from a lightning strike or other high-energy event. In all surge protector applications, mount the surge protector at the building or enclosure entrance, and ground the surge protector body as shown in *Figure 1.10*. Ground the surge protector body to the building grounding system to avoid damage to the clock because of ground-rise-potential.

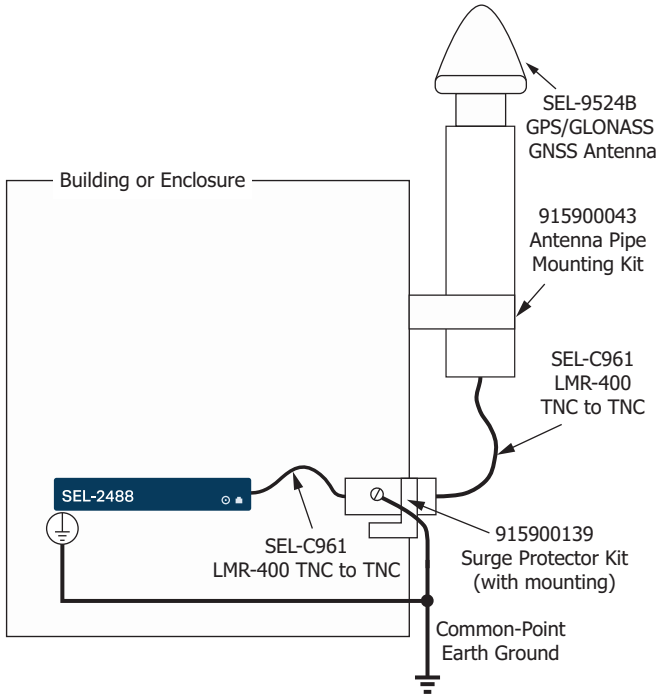


Figure 1.10 Typical Surge Protector Installation

Antenna Cabling

The SEL-9524, the Gas Tube Coaxial Surge Protector, and the SEL-2488 are all equipped with TNC female connectors. The SEL-2488 supports a maximum cable length of 152 meters (500 feet) for LMR-400 (SEL-C961) antenna

cables. Users can choose RG-8X (SEL-C965) cables if long distances are not required. See *Appendix C: Link Budget Analysis* for more detailed information on calculating cable losses based on your cable selections.

Clock Installation

After the antenna system is installed, and before applying power, make sure the clock is mounted and properly grounded. Connect the coaxial cable from the surge protector to the **ANT** port on the back of the clock. Make all desired connections, including BNC (time code), Ethernet, and contact outputs.

Power Supplies

SEL offers two choices for power supplies. The SEL-9330-A is a 125–250 Vac/Vdc supply and the SEL-9330-C is a 24–48 Vdc supply. SEL also offers an 8-ft ac line cord (915900377) to power the SEL-9330-A power supply via a standard wall outlet. For installations requiring additional personnel protection against electrical energy hazard, apply the 915900656 Euro connector cover kit for the SEL-2488.

Figure 1.11 SEL-9330-A 125–250 Vac/Vdc

Figure 1.12 8 ft AC Line Cord for SEL-9930-A Power Supply (915900377)

Figure 1.13 SEL-9330-C 24–48 Vdc

You can install a second power supply to provide redundancy. Connect each power supply to a separate power source. If one source is interrupted, the other source continues to keep the SEL-2488 operational. The power supply has an estimated mean time between failures (MTBF) of 3000 years. The power supplies are hot-swappable, and users can mix and match with both the SEL-9330-A and SEL-9330-C versions. Power supply inputs are isolated from ground and have reverse polarity protection.

Table 1.2 SEL-9330 Power Supply Connections

Pin	Description
1	GND
2	–/N
3	+/H

Connecting to the Device

The SEL-2488 includes an HTTPS web server for configuration and management functions. The recommended browsers are Microsoft Edge, Mozilla Firefox, or Google Chrome.

For the initial connection to the SEL-2488, the following will be required:

- A computer with a wired Ethernet port
- One RJ45 Ethernet cable

Physical Network

Connect the SEL-2488 to your computer, as shown in *Figure 1.14*. Using a standard RJ45 Ethernet cable, connect the Ethernet port of your computer to the front Ethernet port (ETH F) of the device. If your computer is configured as a DHCP client, the SEL-2488 Captive Port service configures a computer to communicate with the SEL-2488.

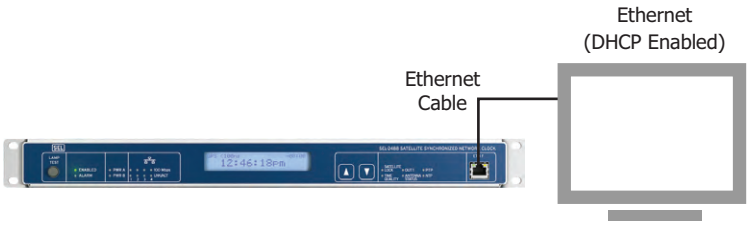


Figure 1.14 Commissioning Network

The default URL for the web server via the ETH F port is https://192.168.1.2. Initially, the management interface can only be reached through the front Ethernet port. After commissioning (setting up a user account), additional management interfaces can be configured. See *Section 4: Ethernet Network Interfaces* for information on enabling an additional IP interface.

See *Section 4: Ethernet Network Interfaces* for more information about the Captive Port feature. If the computer is configured to use static IP addresses, see *Appendix G: Configuring Windows Network Parameters* for assistance in configuring a computer's network parameters.

Commissioning

A new unit will have the front Ethernet port, ETH F, enabled and the Captive Port feature turned on. This will make setup of the computer's network parameters simple, and in many cases, will require no setup at all.

Configure the computer's network connection as described in *Physical Network*. Connect a DHCP-enabled computer to ETH F on the SEL-2488. Wait for the connection to be configured. This can take as many as ten seconds.

Step 1. Open a web browser. In the address bar, enter **https://192.168.1.2**. This will open the **Device Commissioning** page.

NOTE: You may receive a certificate error from your browser. The message is dependent on the browser you are using. This error appears because the default certificate is a self-signed certificate and is not signed by a trusted Certificate Authority (CA). You will need to create a certificate exception to access the device login page. Your browser will provide instructions for doing this. For information on creating an X.509 certificate to eliminate this error, please see Section 12: X.509 Certificate Management.

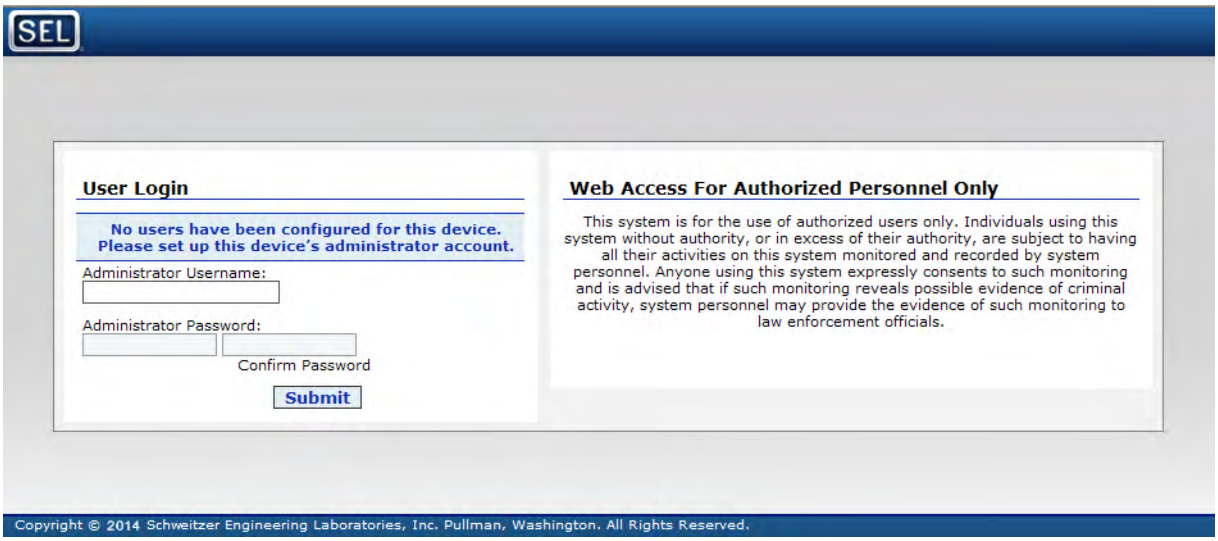


Figure 1.15 Device Commissioning Page

NOTE: The commissioning page only appears during initial setup of a new unit or after a factory-default reset. After the device has been commissioned the initial page will be the login page.

NOTE: In the event that an administrator forgets his or her password, the device can be reset to its factory-default settings. For more information, see Lost Password/ Pinhole Reset on page 23.2.

Step 2. Enter the account information for the first administrative user. This requires both a username and a password. You must type the password a second time (in the **Confirm Password** box) to confirm that it is entered correctly.

Step 3. Select the **Submit** button to complete commissioning. When the page reloads, log in as the administrative user to set up accounts and configure the system. After you successfully log in, the SEL-2488 will redirect you to the dashboard page.

Front Panel

The front panel of the SEL-2488 is equipped with the following LEDs related to device hardware: the **PWR A** and **PWR B** LEDs, which indicate whether the power supplies are operating properly; and the **ANTENNA STATUS** LED, which indicates whether the antenna is installed and functional.

Table 1.3 Device Hardware LEDs

Label	Color	Description
PWR A, PWR B	Green	Power supply is installed and working properly.
	Red	Power supply has failed or is not energized. This will only display when the other power supply is installed and energized.
	Off	Power supply is not installed.
ANTENNA STATUS	Green	Antenna is connected and functional.
	Red	Clock detected an antenna open or short failure condition.
	Off	GNSS is disabled via settings.

Initial Startup Sequence

The LCD screen displays the initialization sequence shown in *Figure 1.16* on startup when the SEL-2488 is connected to its antenna.

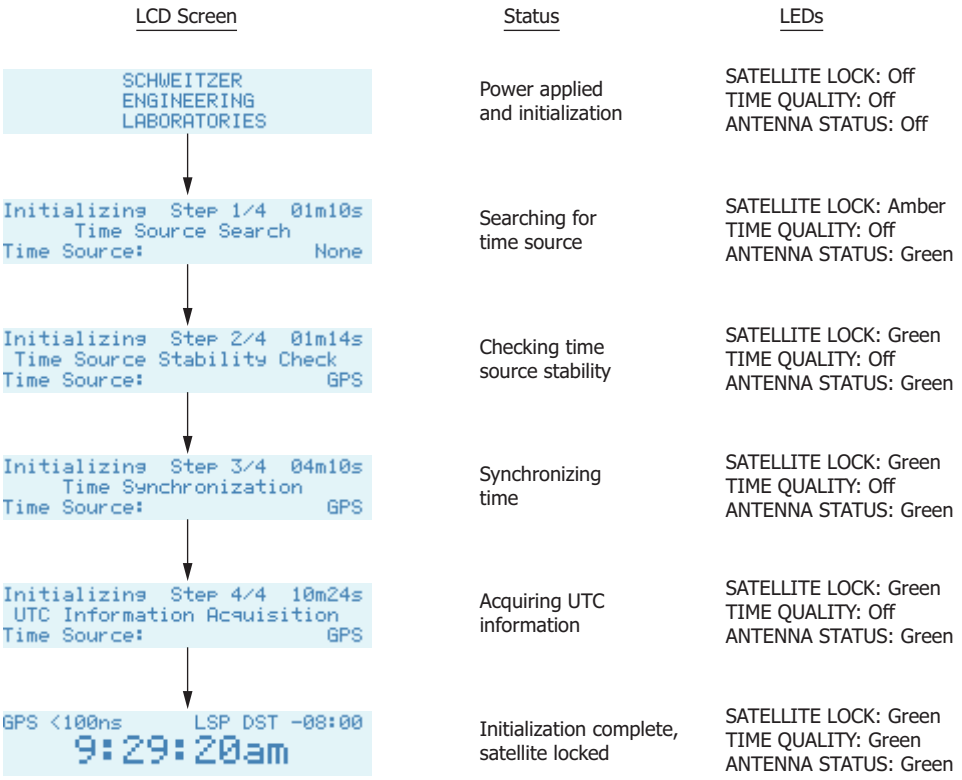


Figure 1.16 Initial Startup Sequence

Dashboard

The top of the dashboard contains a replication of the front-panel LEDs described in *Front Panel on page 1.12*. The LEDs seen on the dashboard will behave in the same manner as those on the front panel.

The **Diagnostics** status widget of the web dashboard shows diagnostic information related to the device hardware.

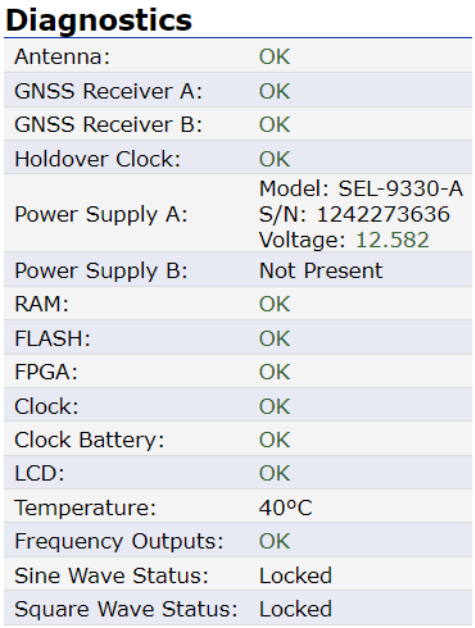


Figure 1.17 Device Hardware Diagnostics

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for events associated with hardware installation. The SEL-2488 replaces message variables in {} with values it logs. For detailed information on alerts and notifications, see *Section 14: Event Reporting System*.

Table 1.4 Hardware Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
Device commissioned by {0} at {user_ip}	Notice	None	–
Device initialization completed	Notice	Minor	Chassis
Failure: Power Supply A	Alert	Major	–
Failure: Power Supply B	Alert	Major	–
OK: Power Supply A	Error	Minor	–
OK: Power Supply B	Error	Minor	–
The Part Number for the device has changed from {0} to {1}	Critical	Major	Chassis

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

Events with an alarm category of Minor and alarm class of "–" will always trigger the alarm contact. Events classified as None will not trigger the alarm contact. Events classified as Major will latch the alarm contact.

Specifications

Compliance

Designed and manufactured under an ISO 9001 certified quality management system

United States and Canada
FCC 47 CFR Pt 15B, Class A
Industry Canada ICES-001 (A) / NMB-001 (A)
UL Listed to U.S. and Canadian safety standards (File 220228; NRAQ/NRAQ7)

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area may be likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Any changes or modifications not expressly approved by the manufacturer can void the user's authority to operate the equipment.

European Union
CE Mark
RoHS Compliant

United Kingdom
UKCA Mark
RoHS Compliant

Australia and New Zealand
RCM Mark

General

Receiver

Satellite Tracking:	GPS L1, C/A Code (1575.42 MHz), GLONASS L1 (1602 MHz), track as many as 16 satellites for each constellation

Acquisition Times

Warm Start:	240 s (with saved almanac data)
Cold Start:	240 s + UTC compensation time (as many as 12.5 minutes)

Clock Accuracy (to UTC)

1 PPS:	±40 ns average, ±100 ns peak
Demodulated IRIG-B:	±40 ns average, ±100 ns peak
Modulated IRIG-B:	±1 µs peak
PTP Time-Stamp Accuracy:	±100 ns peak
NTP Time-Stamp Accuracy (Typical):	<100 µs

Typical client synchronization accuracy to the SEL-2488 NTP server on a LAN is 0.5–2 ms. Actual accuracy depends on network conditions.

Frequency Outputs:	<1E-10 measured over 100 s <1E-12 measured over 24 hr

Holdover Timing Accuracy After 24 Hours (Typical)

TCXO:	36 µs, constant temperature 315 µs, ±1°C
OCXO:	5 µs
DOCXO:	2.5 µs

Note: Holdover accuracy values assume the device has been in operation for 24 hours or longer prior to holdover.

Holdover Frequency Accuracy After 24 Hours (Typical):

OCXO:	1E-10 Hz/Hz
DOCXO:	5E-11 Hz/Hz

Antenna Requirements

5 V, <80 mA
≥32 dB preamp

Electrical Output Drive Levels

Demodulated IRIG-B/PPS BNC Ports (T01–T08):	5 Vdc (TTL), 250 mA max
Modulated IRIG-B BNC Ports (T01–T04):	6.2 Vpp nominal
DB-9 Port IRIG-B Output (COM1 Pin 4/Pin 6):	5 Vdc (TTL), 5 mA

Note: Cabling on the DB-9 port shall be no longer than 3 m.

Square-Wave Frequency SMA Port (F1):	10 MHz, 5 Vdc (TTL), 100 mA max

Note: Cable lengths >2 m requires use of LMR-240 or better quality cabling.

Sine-Wave Frequency SMA Ports (F2–F6):	10 MHz, +13 dBm nominal, ±2 dB into 50 Ω
Subharmonics:	<–40 dBc
Spurious:	<–70 dBc

Operating Environment

Pollution Degree:	2
Overvoltage Category:	II
Insulation Class:	I

Dimensions

1U Rack Mount

Height:	43.7 mm (1.72 in)
Depth:	248.6 mm (9.79 in)
Width:	482.5 mm (19.0 in)

1U Panel Mount:

Height:	80.0 mm (3.15 in)
Depth:	248.8 mm (9.80 in)
Width:	502.9 mm (19.80 in)

Weight

2.8 kg (6.2 lb)

Warranty

10 years

Network Management

HTTPS Web User Interface
ACSELERATOR QuickSet SEL-5030 Software
Settings Import/Export

User-Based Accounts

Maximum Local Accounts:	256
User Roles:	Administrator, Engineer, User Manager, Monitor
Password Length:	1–72 characters
Password Set:	All printable ASCII characters

Note: If complex passwords are enabled, the password must have at least 8 characters with at least one digit, uppercase, lowercase, and special character.

Syslog

Storage for 60,000 local syslog messages

Support for three remote syslog destinations

Simple Network Management Protocol (SNMP)

Monitors diagnostics through SNMP v2c and v3 read operations

Sends notifications using SNMP v2c traps

Support for as many as three trap servers

Network Time Protocol (NTP)

Implements NTPv4 Server, Broadcast, and Multicast formats

Precision Time Protocol (PTP)

Implements the following IEEE 1588-2008 profiles:

Default UDP (Annex D and J)
Default 802.3 (Annex F and J)
IEEE C37.238-2011
IEEE C37.238-2017
IEC/IEEE 61850-9-3:2016

Parallel Redundancy Protocol (PRP)

Implements IEC 62439-3:2016

Supports as many as two Doubly Attached Node implementing PRP (DANP) interfaces for separate PRP networks using the following physical Ethernet port combinations:
ETH 1 and ETH 2
ETH 3 and ETH 4

Supports PTP as a Doubly Attached Clock (DAC) on ports where PRP is enabled.

Active-Backup Port Bonding

Implements Active-Backup port bonding (also known Failover) using the following physical Ethernet port combinations:
ETH 1 and ETH 2
ETH 3 and ETH 4

Communications Ports

Ethernet Ports

Ports:	4 rear, 1 front
Data Rate:	10 or 100 Mbps
Front Connector:	RJ45 Female
Rear Connectors:	RJ45 Female or LC Fiber (single-mode or multimode)
Standard:	IEEE 802.3

Fiber-Optic Ports

Multimode Option (to 2 km)

Maximum TX Power:	–14 dBm
Minimum TX Power:	–20 dBm
RX Sensitivity:	–31 dBm
System Gain:	11 dB
Source:	LED
Wavelength:	1310 nm
Connector Type:	LC (IEC 61754-20)

Single-Mode Option (to 15 km)

Maximum TX Power:	–8 dBm
Minimum TX Power:	–15 dBm
RX Sensitivity:	–28 dBm
System Gain:	13 dB
Source:	Laser
Wavelength:	1310 nm
Connector Type:	LC (IEC 61754-20)

Alarm Output

Pilot Duty Rating (Per UL 508):	B300, R300
Power Supply Burden:	<0.5 W max
Rated Operational Voltage:	24–250 Vdc
Contact Protection:	270 Vdc, MOV protected
Continuous Carry:	2 A
Pickup Time:	≤8 ms typical
Dropout Time:	≤8 ms typical

Timer Contact

Power Supply Burden:	<0.5 W max
Rated Operational Voltage:	12–250 Vdc
Contact Protection:	330 Vdc (250 Vac), MOV protected
Continuous Carry:	100 mA
Off Resistance:	5 MΩ
Minimum Voltage:	12 Vdc
Timing Accuracy (Closing):	±1 µs (applies only to dc voltages)

Terminal Connections

Warning: When using stranded wire, use crimp ferrules to safely capture all wire strands before assembling and attaching the plug or ground wire.

Power Supply Compression Screw Terminals

Part Number:	Use SEL P/N 420-0219 (provided)
Tightening Torque:	0.5–0.6 Nm (4–5 in-lb)
Insulation Ratings:	300 V, 90°C (194°F), minimum
Wire Material:	Copper
Size:	12–18 AWG (4.00–0.75 mm^2)

Alarm and Timing Contact Compression Screw Terminal

Part Number:	Use SEL P/N 420-0071 (provided)
Tightening Torque:	0.5–0.6 Nm (4–5 in-lb)
Insulation Ratings:	300 V, 90°C (194°F), minimum
Wire Material:	Copper
Size:	16–22 AWG (1.50–0.34 mm^2)

Ground Screw

Part Number:	#6 crimp ring terminal is recommended
Tightening Torque:	0.90–1.36 Nm (8–12 in-lb)
Insulation Ratings:	300 V, 90°C (194°F), minimum
Wire Material:	Copper
Size:	12–18 AWG (4.00–0.75 mm^2)
Length:	<3.0 m (<9.8 ft)

Power Supply

125–250 Volt Power Supply (SEL-9330-A)

Rated Supply Voltage:	125–250 Vdc 120–240 Vac, 50/60 Hz
Input Voltage Range:	88–300 Vdc or 85–264 Vac
Burden:	AC: <75 VA, 700 mA DC: <45 W
Input Voltage Interruptions:	50 ms @ 125 Vac/Vdc 100 ms @ 250 Vac/Vdc
Peak Inrush:	8 A
Internal Fuse Rating:	2.5 A, 250 Vdc/300 Vac time-lag T, 250 Vac/1500 A break rating

Note: Fuses are not user-serviceable.

24–48 Volt Power Supply (SEL-9330-C)

Rated Supply Voltage:	24–48 Vdc (polarized)
Input Voltage Range:	19.2–60.0 Vdc
Burden:	<42W, 1.7 A
Input Voltage Interruptions:	50 ms @ 48 Vdc 10 ms @ 24 Vdc
Peak Inrush:	18 A
Internal Fuse Rating:	4.0 A, 150 Vdc time-lag T, 250 Vac/1500 A break rating

Note: Fuses are not user-serviceable.

Recommended External Overcurrent Protection

Breaker Type:	Standard
Breaker Rating:	15 A at 250 Vdc
Current Breaking Capacity:	10 kA
Grounded Neutral Systems:	Device in series with the HOT or energized conductor
DC and Isolated Systems:	Device in series with both conductors

Environmental

Temperature

Operating: –40° to +85°C (–40° to +185°F)

Note: UL Ambient +40°C (+104°F).
See *Safety Information* for additional details.

Non-Operating (Storage): –40° to +85°C (–40° to +185°F)

Relative Humidity

5% to 95% noncondensing

Altitude

2000 m

Type Tests

Communication Product Testing

Communications for Substation Equipment:	IEEE 1613-2009 Class 2
Communications Networks and Systems for Power Utility Automation—Pt 3: General Requirements:	IEC 61850-3:2013

Electromagnetic Compatibility General

Measuring Relays and Protection Equipment:	IEC 60255-26:2013

Electromagnetic Compatibility Emissions

IEC 60255-25:2000
IEC 60255-26:2013
CISPR 11:2009 + A1:2010
CISPR 22:2008
Canada ICES-001 (A) / NMB-001 (A)
47 CFR Part 15.107 and 109
Severity Level: Class A

Electromagnetic Compatibility Immunity

Conducted RF Immunity:	IEC 60255-26:2013 IEC 61000-4-6:2014 Severity Level: 10 Vrms
Radiated RF Immunity:	IEC 60255-26:2013 IEC 61850-3:2013 IEC 61000-4-3:2005 + A1:2008 + A2:2010 Severity Level: 10 V/m IEEE C37.90.2-2004 IEEE 1613-2009 Severity Level: 20 V/m
Electrostatic Discharge Immunity:	IEC 60255-26:2013 IEC 61850-3:2013 IEC 61000-4-2:2008 Severity Level: ±2, 4, 6, 8 kV contact; ±2, 4, 8, 15 kV air IEEE 1613-2009 IEEE C37.90.3-2001 Severity Level: ±2, 4, 8 kV contact; ±4, 8, 15 kV air
IEEE Surge Withstand Capability:	IEC 60255-22-1:2007 Severity Level: ±2.5 kV peak common mode, ±1.0 kV peak differential mode IEEE C37.90.1-2005 IEEE 1613-2023 IEEE C37.90.1-2012 + ERTA:2–13 Severity Level: ±2.5 kV, 1 MHz oscillatory; ±4 kV, 5.0 kHz fast transient
IEC Fast Transient/Burst Immunity:	IEC 60255-26:2013 IEC 61850-3:2013 IEC 61000-4-4:2011 Severity Level: ±4 kV, 5 kHz; ±2 kV, 5 kHz on communications ports
IEC SDOW Immunity:	IEC 60255-26:2013 IEC 61850-3:2013 IEC 61000-4-18:2006 + A1:2010 Severity Level: ±2.5 kV; ±1.0 kV on communications ports
IEC Surge Immunity:	IEC 60255-26:2013 IEC 61850-3:2013 IEC 61000-4-5:2005 Severity Level: ±0.5 kV, 1 kV line-to-line, ±0.5 kV, 2 kV line-to-earth; ±0.5 kV, 1 kV, 2 kV line-to-earth on communications ports
Conducted Common-Mode Immunity:	IEC 61850-3:2013 IEC 61000-4-16:2016 Severity Level: 300 Vac for 60 s; 30 Vac for 1 s
Power Frequency Magnetic Field Immunity:	IEC 61000-4-8:2009 Severity Level: 1000 A/m for 3 s, 100 A/m for 1 min
Pulse Magnetic Field Immunity:	IEC 61000-4-9:2001 Severity Level: 1000 A/m
Damped Oscillatory Magnetic Field Immunity:	IEC 61000-4-10:2001 Severity Level: 100 A/m (at 1 kHz and 1 MHz)
Voltage Dips and Interruptions Immunity:	IEC 60255-26:2013 IEC 61850-3:2013 IEC 61000-4-11:2004 + A1:2017 IEC 61000-4-17:2002 + A1:2001 + A2:2008 IEC 61000-4-29:2000

Environmental

Cold:	IEC 60068-2-1:2007 Severity Level: 16 hours at –40°C
Damp Heat, Cyclic:	IEC 60068-2-30:2005 Severity Level: 25° to 55°C, 6 cycles, relative humidity (RH): 95%
Dry Heat:	IEC 60068-2-2:2007 Severity Level: 16 hours at +85°C
Change of Temperature:	IEC 60068-2-14:2009 Severity Level: 20°C and 60% RH to 90°C and 16% RH to –45°C and 36% RH
Damp Heat Steady State:	IEC 60068-2-78:2001 Severity Level: 40°C, RH: 93%, 10 days

Free Fall:	IEEE 1613-2009 Severity Level: 100 mm
Vibration:	IEC 60255-21-1:1988 Severity Level: Class 2 Endurance Class 2 Response
Shock & Bump:	IEC 60255-21-2:1998 Severity Level: Class 1 Shock Withstand Class 1 Bump Class 2 Shock Response
Seismic:	IEC 60255-21-3:1993 Severity Level: Class 2 (Quake Response)

Safety

Measuring Relays and Protection Equipment:	IEC 60255-27:2013
Protection IP Code:	IEC 60529:1989 + A1:1999 + A2:2013 IP Code: IP3X for category 2 equipment
Insulation Coordination:	IEC 60255-27:2013 IEEE C37.90-2005 Dielectric (HiPot) Severity Level: Power Supply: ±3.6 kVdc Alarm Contact: ±3.6 kVdc IRIG-B Input: ±2.25 kVdc Ethernet Ports: ±2.25 kVdc Timer Contact: ±3.6 kVdc Impulse Severity Level: 5 J; ±5 kV, 1.2/50 µs
Electrical Equipment for Measurement, Control, and Laboratory Use:	IEC 61010-1:2010/AMD1:2016/COR:2019 UL 61010-1:2019, C22.2 No. 61010-1:12/A1:18 IEC 61010-2-201:2017 UL 61010-2-201:2018, C22.2 No. 61010-2-201:18

Section 2
Applications

Overview

The primary application for the SEL-2488 Satellite-Synchronized Network Clock is to receive Global Navigation Satellite System (GNSS) time signals and distribute precise time via demodulated IRIG-B, Precision Time Protocol (PTP), and Network Time Protocol (NTP).

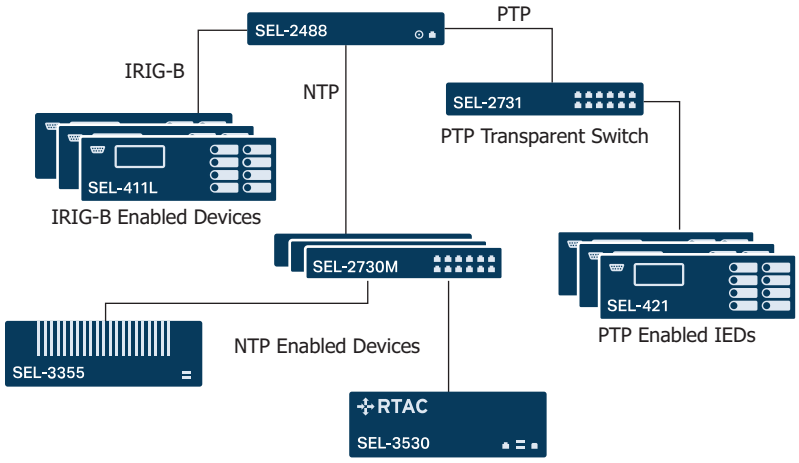


Figure 2.1 SEL-2488 Applications

Demodulated IRIG-B provides time output to within ±100 ns peak accuracy to UTC for synchronizing relays, phasor measurement units, and other intelligent electronic devices (IEDs). The SEL-2488 preserves IRIG-B accuracy by providing cable delay compensation for antenna cables and output cables on a per-port basis.

The SEL-2488 also supports PTP (IEEE 1588-2008) output with the purchase of the PTP firmware option or PTP field upgrade. As with demodulated IRIG-B, PTP can provide time output to within ±100 ns peak accuracy to UTC. To achieve sub-microsecond accuracies, all devices synchronizing with PTP must support IEEE 1588 with hardware time-stamping, and the network must be properly designed. The SEL-2488 supports Default (Annex J), Power System (IEEE C37.238-2011/2017), and Power Utility Automation (IEC/IEEE 61850-9-3:2016) profiles for PTP and can serve PTP to four independent networks.

The SEL-2488 supports NTP Server mode to distribute time to devices on the substation local-area network (LAN). Such devices include servers, computers, and other devices that set their time through NTP or the Simple Network Time Protocol (SNTP). The SEL-2488 can serve NTP to four independent networks. The SEL-2488 acts as a Stratum 1 time server with typical 0.5–2 ms client synchronization accuracy on a LAN.

Job Done Examples

Example 1

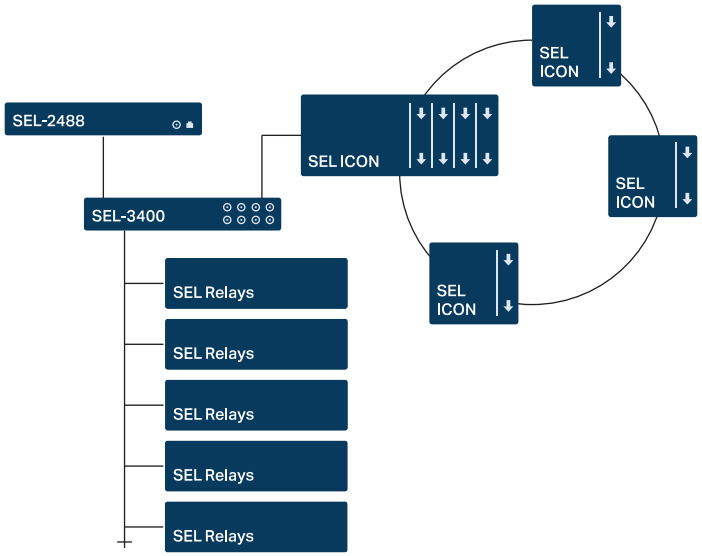


Figure 2.2 SEL-2488 Working in Conjunction With SEL ICON and SEL-3400 to Provide Redundant IRIG-B Sources to SEL Relays

The SEL-2488 provides unsurpassed IRIG-B time synchronization accuracy traceable to UTC from GNSS signals. However, external events such as snow build-up, physical damage to the GNSS antenna, or other environmental effects can prevent the reception of the GNSS signals. You can mitigate the effects of these external events on your system by combining the SEL-2488 with an SEL-3400 IRIG-B Distribution Module. The SEL-3400 has two IRIG-B inputs, which it continuously compares. The source with the best time quality will be selected as the primary source. For example, you can connect one input of the SEL-3400 to the SEL-2488 and the other input to the IRIG-B output of an SEL Integrated Communications Optical Network (ICON) node. This provides a GNSS time source both from a local antenna and from the SEL ICON ring, providing a robust solution for maintaining IRIG-B signals to your SEL relays.

Example 2

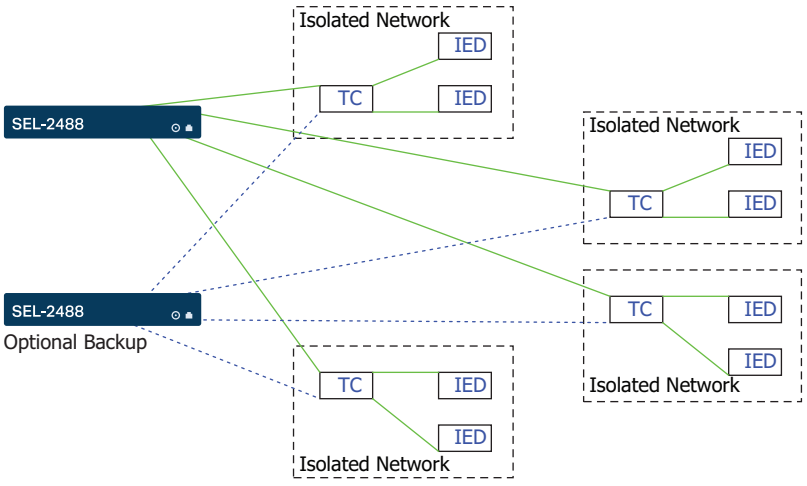


Figure 2.3 SEL-2488 Providing PTP/NTP Time to Isolated Networks

Installations can have separate networks inside a facility; for example, a protection network, an automation network, and an administration network. Most clocks only have one Ethernet interface, requiring multiple clocks to support the separate networks in this scenario. The SEL-2488 has four independent Ethernet interfaces, and can provide time to four separate networks. Each interface on the SEL-2488 is independent of one another, and the PTP master and NTP server options are set for each interface. This allows the same clock to provide accurate time to each of the networks without joining the networks or compromising design requirements.

See *Section 7: Precision Time Protocol (PTP)* and *Section 8: Network Time Protocol (NTP)* for information on configuring each of the time protocols.

Example 3

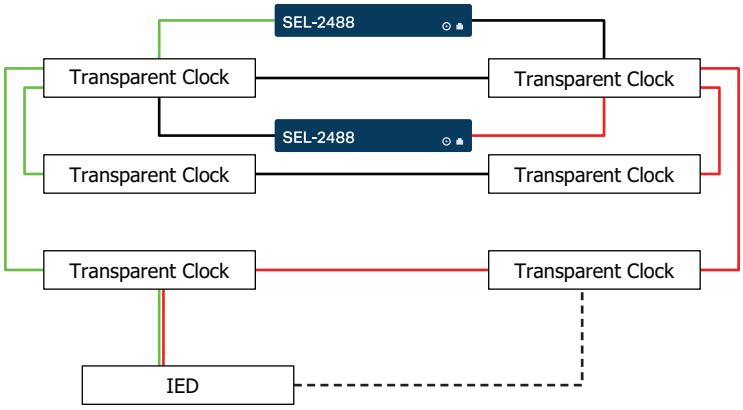


Figure 2.4 SEL-2488 Overcomes Single Point of Failure With Multiple Connections to a Redundant Ethernet Network Topology

The SEL-2488 with four independent Ethernet interfaces can connect to multiple transparent clocks on the network. This removes the single point of connection failure that many clocks with a single connection can experience. Either of the transparent clocks to which the SEL-2488 connects can fail, but the network will still provide PTP time to the IED. Addition of a second SEL-2488 provides protection in the event of the failure of the first SEL-2488. In the sample topology shown in *Figure 2.4*, the IED will continue to receive PTP time with a failure of the SEL-2488 or one of the main transparent clocks. If the IED supports multiple network backbone connections, as indicated, only failure of the IED itself will cause the IED to lose PTP time.

Example 4

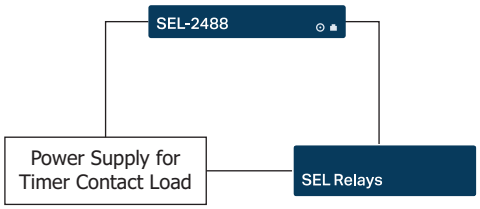


Figure 2.5 SEL-2488 Providing High-Precision Pulse Contact Output

For devices that do not support external time synchronization, you can use a periodic pulse to a contact input on the device to align time stamps within the device. The SEL-2488 includes a clock-controlled Form A high-speed solid-state contact output. You can set this output to provide a single contact closure or a repeating contact closure of configurable closure duration and closure period.

See *Section 9: Timer Contact* for information on connecting and configuring the pulse contact output.

Example 5

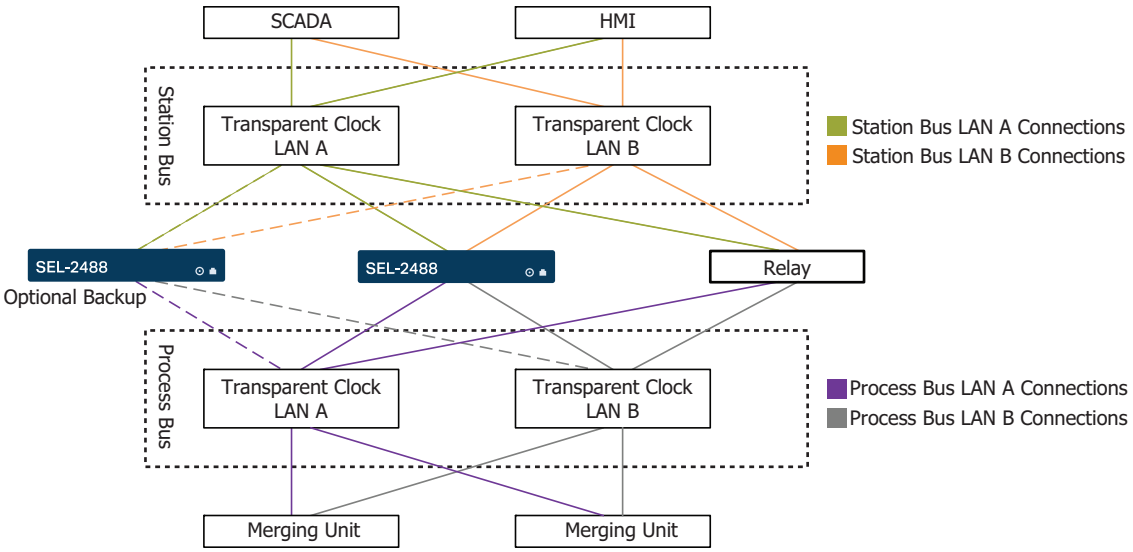


Figure 2.6 SEL-2488 Providing PTP/NTP Across Separate Station Bus and Process Bus PRP Networks

The SEL-2488 supports two independent PRP interfaces that use the four rear-panel physical Ethernet ports. You can combine **ETH 1** and **ETH 2** for one PRP interface and **ETH 3** and **ETH 4** for another, separate PRP interface. With the PTP option, the SEL-2488 will act as a PTP Doubly Attached Clock (DAC) on ports where PRP is enabled. When you use a single SEL-2488 in an IEC 61850 substation automation system (SAS), it can provide accurate PTP and NTP time to each of the separate PRP networks for Station Bus and Process Bus, as shown in *Figure 2.6*. The addition of a second SEL-2488 provides a robust and resilient network topology, removing single points of failure.

For information on configuring each of the protocols, see *Section 7: Precision Time Protocol (PTP)*, *Section 8: Network Time Protocol (NTP)*, and *Section 24: Parallel Redundancy Protocol (PRP)*.

Example 6

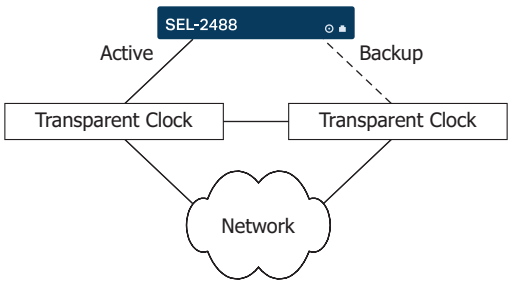


Figure 2.7 SEL-2488 Providing Ethernet Failover with Active-Backup Port Bonding

The SEL-2488 supports as many as two independent active-backup bonded interfaces that use the four rear-panel physical Ethernet ports. Active-backup port bonding logically combines two physical Ethernet ports into a single network interface with only one port active while the other serves as a failover backup. You can combine **ETH 1** and **ETH 2** for one bonded interface and **ETH 3** and **ETH 4** for another, separate bonded interface. When enabled, you can

directly connect the two physical Ethernet ports of the bonded interface to separate locations within the same LAN to provide Ethernet failover for PTP, NTP, management, and reporting.

For information on configuring each of the protocols, see *Section 7: Precision Time Protocol (PTP)*, *Section 8: Network Time Protocol (NTP)*, and *Section 25: Active-Backup Port Bonding*.

Example 7

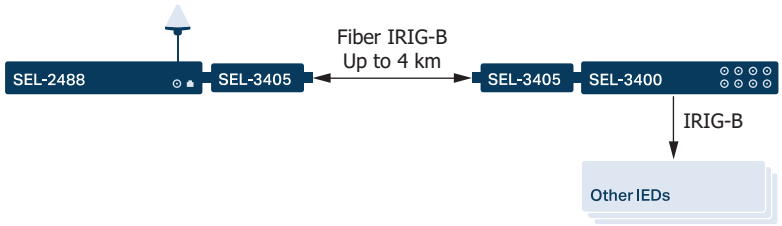


Figure 2.8 SEL-2488 Providing High-Accuracy IRIG-B via Fiber-Optic Cable With the SEL-3405

For installations that require extensive IRIG-B distribution, you can use the SEL-2488 DB-9 port with the SEL-2812 Fiber-Optic Transceivers With IRIG-B or the SEL-3405 High-Accuracy IRIG-B Fiber-Optic Transceivers to send IRIG-B over long distances via a fiber-optic cable.

You can connect the transceiver to the SEL-2488 by using the SEL-C942 cable and the SEL-9321 power supply, and, when using the SEL-3405 specifically, use the SEL-3400 with the SEL-C940 cable on the other end to provide further high-accuracy IRIG-B distribution to a large number of your SEL relays, as shown in *Figure 2.8*.

For information on configuring the DB-9 (**COM1**) port, see *Section 6: Time-Code Outputs*.

Example 8

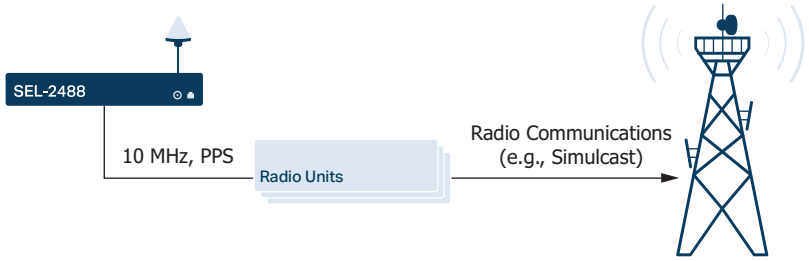


Figure 2.9 SEL-2488 Providing Time Synchronization to a Land Mobile Radio (LMR) System

With the purchase of the frequency outputs hardware option, the SEL-2488 provides six 10 MHz SMA output ports. Using both 10 MHz and PPS outputs, the SEL-2488 ensures reliable time synchronization for Land Mobile Radio (LMR) systems, such as simulcast radio systems used in 911 emergency response.

For information on the frequency outputs hardware option, see *Section 26: Frequency Outputs*.

This page intentionally left blank

Section 3
Time Synchronization

Overview

The SEL-2488 uses Global Navigation Satellite System (GNSS) signals to synchronize its internal clock and time outputs to Coordinated Universal Time (UTC). As of August 2014, the only globally operational GNSS systems were GPS (U.S.) and GLONASS (Russian).

The SEL-2488 primarily uses GPS signals for synchronization to UTC; however, it has the capability to use GLONASS signals through its satellite signal verification (SSV) feature. This feature gives the SEL-2488 the ability to compare GNSS sources and provide alerts when it detects anomalies between signals.

Operation

Visible Versus Used

The SEL-2488, when initially synchronizing and during normal operation, classifies satellites into two categories: Used and Visible. Used references the satellites included in the processing algorithms that determine accurate time. Visible indicates satellites the receiver can detect. Satellites must be in the Visible category before the SEL-2488 can use them, but lack of adequate signal level or other requirements may prevent some visible satellites from being included in the Used group.

Almanac and Ephemeris

To provide highly accurate time synchronized to UTC, the SEL-2488 relies on current GNSS Almanac and Ephemeris data. The SEL-2488 receives this information continuously as part of the signals the satellites transmit, but it requires approximately 12.5 minutes of continuous signal reception to receive the full package. The SEL-2488 maintains this information so that it can initialize and start providing time on the next startup sequence without having to wait the full period to receive all of the information. If the unit has been without power for a period or if its antenna location changed, the device deems the local information to be out of date and waits for the download of the most recent information to complete initialization. This can take as many as 30 minutes.

Satellite Signal Verification

Satellite signal verification is a process by which the SEL-2488 compares GNSS information it receives from GPS and GLONASS sources and uses this information to identify anomalies in the received signals.

Satellite Lock Requirements

The timing accuracy of GNSS receivers can vary based on the information that GNSS provides. To achieve precise timing synchronization on the order of tens of nanoseconds, it is important for the GNSS receiver to see enough GNSS satellites (dispersed throughout the sky) to accurately determine its

position. This allows the proper offset to be applied so the receiver can accurately synchronize its time. Certain factors, including distance between the used satellites, can affect the positioning measurements, and therefore the timing accuracy of the receiver.

The SEL-2488 will not lock unless it can qualify that the GNSS signal is accurate. Assuming a favorable satellite geometry, the SEL-2488 requires at minimum 4 satellites to lock. These satellites must be in the Used category with a signal level of 30 dB-Hz or greater per active constellation. This means it will always require four GPS constellation satellites in a Used status and, if SSV is enabled, it will require an additional four GLONASS satellites in a Used status. The SEL-2488 is designed to briefly operate using its internal oscillator to ride through short satellite anomalies. This allows the clock to maintain high accuracy, even when satellite conditions are not ideal.

Time Qualification

When the GNSS receivers have the most recent almanac and ephemeris information and have completed locking to the satellite signals, the SEL-2488 performs a time qualification on the GNSS signals. Once time qualification is complete, the time outputs enable and start sending time signals, and the front-panel LCD starts displaying time.

Holdover

If the SEL-2488 loses its primary reference (GNSS), it goes into holdover mode and continues to provide time outputs based on its internal reference oscillator. This holdover mode is available after the clock has synchronized to a GNSS source for a period and has not experienced a power interruption since that synchronization. The clock exits holdover operation after the GNSS source becomes available and is requalified.

There are two variations of the clock with different internal reference oscillators. The standard version includes a temperature-compensated crystal oscillator (TCXO), with options for an oven-controlled crystal oscillator (OCXO) or a double-oven-controlled crystal oscillator (DOCXO). The three oscillators differ in the amount of time drift the oscillator will exhibit when in holdover operation.

Antenna Diagnostics

The SEL-2488 antenna port is powered with a +5 Vdc source to supply power to the GNSS antenna and signal splitters. The power flow through the antenna port is monitored as part of the clock diagnostics. These diagnostics are enabled when Enable GNSS Time Source is selected in the settings.

The antenna port is operating normally if it is supplying the appropriate amount of power for a GNSS antenna and the connected antenna splitters.

An Antenna Short event is triggered if there is excessive power flow. This can occur if there is an antenna or cable short or if there are too many signal splitters attached to the antenna port.

An Antenna Open/Absent event is triggered when there is very little or no power flow out of the port. This could be a result of a disconnected cable or an antenna issue.

Settings

Upon application of power, the SEL-2488, when properly installed and connected to an antenna system, will complete the initialization process and synchronize the clock to UTC. This section discusses the settings that

customize and affect the operation of time synchronization. Access these settings via the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **Time Management > GNSS Settings** menu option.

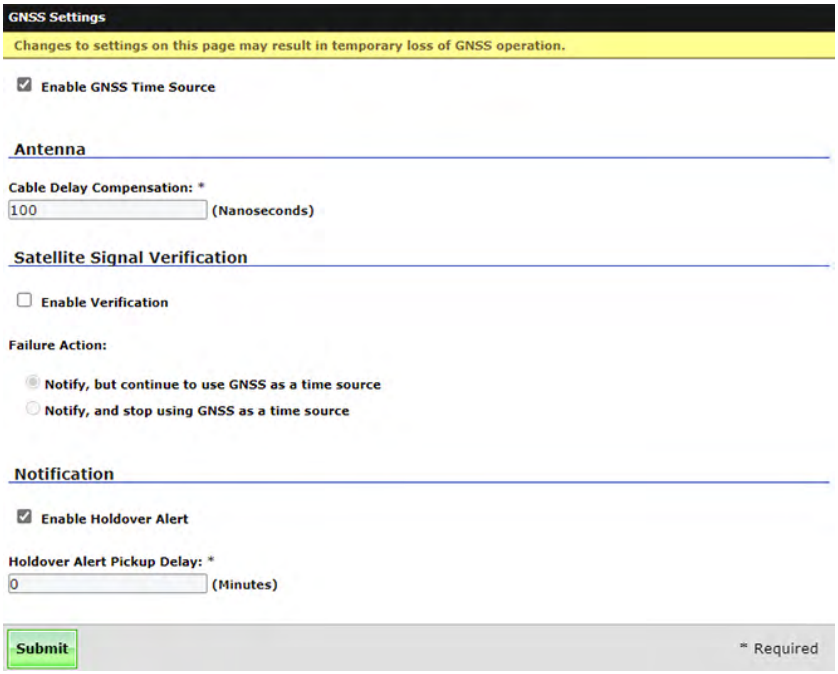


Figure 3.1 GNSS Settings Page

Use the GNSS settings (*Figure 3.1* and *Table 3.1*) to customize settings for the GNSS receiver. Through use of these settings, you can enable or disable the receiver and compensate for antenna cable delay.

Table 3.1 GNSS Settings (Sheet 1 of 2)

Setting Name	Values	Default	Description
Enable GNSS Time Source	Checked, Unchecked	Checked	Enables or disables the use of GNSS as a time source. When unchecked, GNSS sources are not used for time synchronization. If the clock previously was locked to a GNSS source, it goes into holdover and continues providing time outputs. If the clock has not synchronized, it does not go into holdover or provide time outputs.
Cable Delay Compensation	0–2500 ns	100	This value is used to compensate for the signal delays resulting from antenna cable type and length. Entered in nanoseconds of delay. LMR-400: 3.92 ns/meter (1.19 ns/foot) RG-8X: 3.87 ns/meter (1.18 ns/foot)
(SSV[a]) Enable Verification	Checked, Unchecked	Unchecked	Provides a layer of protection against GNSS vulnerabilities when enabled. While this setting is checked, the system monitors the GNSS signals for any potential problems. If it detects a potential problem, the system acts according to the (SSV) Failure Action setting.
(SSV) Failure Action	Notify, but continue to use GNSS as a time source Notify, and stop using GNSS as a time source	Notify, but continue to use GNSS as a time source	Determines the device action when SSV detects a potential problem.

Table 3.1 GNSS Settings (Sheet 2 of 2)

Setting Name	Values	Default	Description
Enable Holdover Alert	Checked, Unchecked	Checked	Determines whether the system generates a major event when the device is in holdover.
Holdover Alert Pickup Delay	0–120 minutes	0	Pickup delay for holdover alert notifications. Notifications will occur when the device has been in holdover for Holdover Alert Pickup Delay minutes.

[a] For the SSV to be operational, you must use the SEL-9524B GPS/GLONASS GNSS Antenna.

Cable Delay Compensation

Propagation delay because of the antenna system cables can be compensated for in the SEL-2488 by using the Cable Delay Compensation setting. The clock uses this setting to offset the received time information and synchronize to UTC with greater accuracy.

Satellite Signal Verification

NOTE: If you enable the satellite signal verification feature, the clock will not lock unless you use the specified GPS/GLONASS GNSS antenna and the clock verifies both constellations.

The SEL-2488 can receive signals from two satellite constellations to validate GNSS time signals, providing a layer of protection from GPS spoofing attacks. To enable SSV, you must enable the verification setting in the web interface and use the SEL-9524B GPS/GLONASS GNSS Antenna. *Table 3.2* shows what constellations are in use according to the Satellite Signal Verification Setting.

Table 3.2 SEL-2488 Constellations Used

SEL-2488 GNSS Setting	GNSS Used
Satellite Signal Verification (SSV)—Disabled (default)	GPS
Satellite Signal Verification (SSV)—Enabled	GPS and GLONASS

GLONASS signal information will display on the dashboard and front panel regardless of the SSV setting. The SEL-2488 will use GLONASS signals for verification only when SSV is enabled.

When satellite signal verification is enabled and the SEL-2488 is locked, the Failure Action setting determines what steps to take when the system detects an anomaly. Once the setting is enabled, the default action for the SEL-2488 is **Notify, but continue to use GNSS as a time source**. This action creates an event when satellite signals can no longer be verified. In this mode, the clock continues to use available GNSS signals for timekeeping regardless of satellite errors. When you select **Notify, and stop using GNSS as a time source**, the clock goes immediately into holdover, creates a syslog event, and does not use GNSS for timekeeping until after proper verification of time from that source.

The SEL-2488 can connect to a GPS-only antenna system and synchronize time. When using a GPS-only antenna system, the satellite signal verification option must be disabled for the clock to achieve satellite lock and provide time.

Holdover Alert Notification

The Enable Holdover Alert setting determines if the system generates an event when the SEL-2488 experiences a loss of GNSS and enters holdover operation. The Holdover Alert Pickup Delay setting determines how long the SEL-2488 must continuously remain in holdover operation before generating an event.

Front Panel

The **ANTENNA STATUS**, **SATELLITE LOCK**, and **TIME QUALITY** LEDs are related to time synchronization and are found on the front panel to the right of the LCD.

Figure 3.2 Time Synchronization Front-Panel LEDs

Table 3.3 Front-Panel Indicators

LED Indicators	Normal Operation	Error Condition	GNSS Disabled
ANTENNA STATUS	Green	Red: antenna missing or cable shorted	Off
SATELLITE LOCK	Green: GNSS enabled, satellite lock achieved for all required constellations	Amber: GNSS enabled, satellite lock not achieved for all required constellations	Off
TIME QUALITY	Green: time quality < 1 µs Flashing Green: time quality < 1 ms Red: time quality ≥ 1 ms Off: time quality not determined since startup	NA	NA

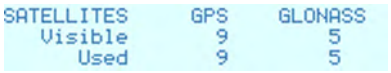


Figure 3.3 LCD–Satellite Status

Figure 3.4 LCD–Position

Table 3.4 Satellite Status LCD

LCD Indicators	Normal Operation	GNSS Disabled
Satellite Status	Number of in-use and visible satellites by constellation.	Off
Position	Latitude, Longitude, and Altitude of Antenna position. All zeros if position not determined.	Off

Dashboard

Satellite Status

The web dashboard contains a satellite status bar graph and SkyView (**Satellite Status** status widget). The satellite status displays the present GPS and GLONASS satellite numbers, signal strengths, and whether satellites are visible or used by the SEL-2488. The SkyView graph and satellite status display the same information, but SkyView indicates the relative location in the sky for each satellite. The status updates automatically every 10 seconds. These graphs help troubleshoot signal acquisition issues during installation. A minimum of four satellites being used at a level of 30 dB-Hz or greater per active constellation is necessary for the SEL-2488 to initially lock. Once there is a lock, the SEL-2488 only requires three Used satellites per constellation to maintain lock and time synchronization.

The bar graph and SkyView represent used satellites in full color and visible satellites in the same color but transparent (opaque). The Used/Visible status, signal level, azimuth, and elevation update at each screen refresh. See *Visible Versus Used* for a description of the terms "Used" and "Visible."

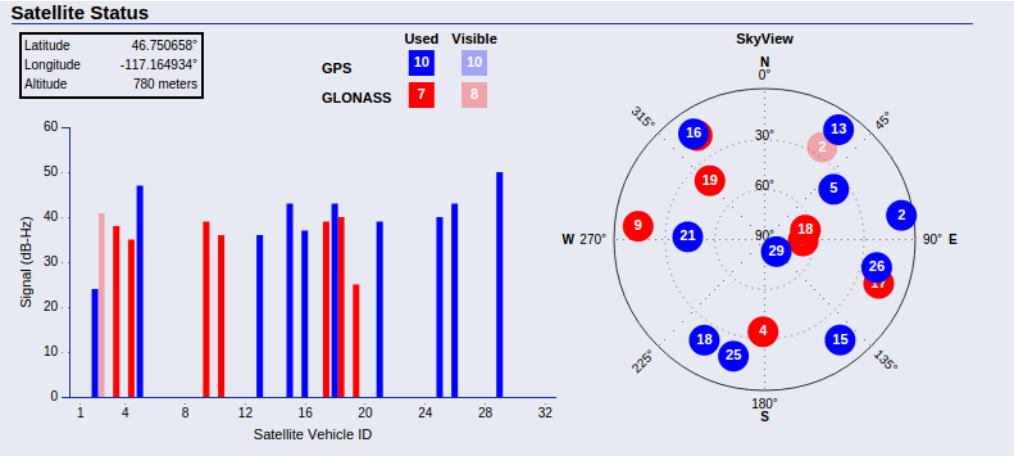


Figure 3.5 Dashboard Satellite Status Status Widget

To view the **Satellite Status** status widget, you must use a recommended web browser; see *Connecting to the Device on page 1.10*.

The **Satellite Status** status widget displays additional information regarding each satellite. Access this information by hovering your mouse pointer over a satellite in either the bar graph or SkyView, as shown in *Figure 3.6* and *Figure 3.7*. The dashboard provides the following information:

- Satellite constellation
- Satellite ID
- Signal level
- Elevation, relative to the horizon
- Azimuth, relative to true north

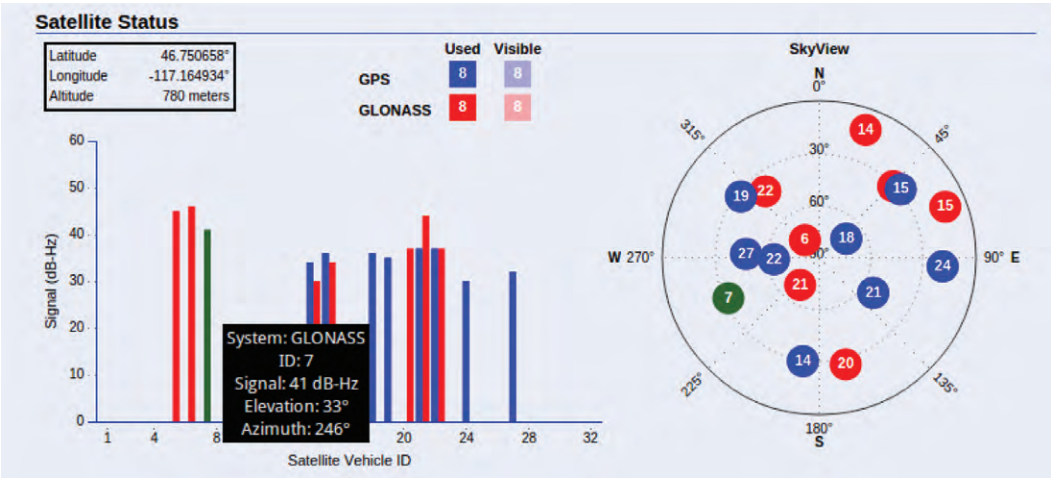


Figure 3.6 Satellite Information on Bar Graph

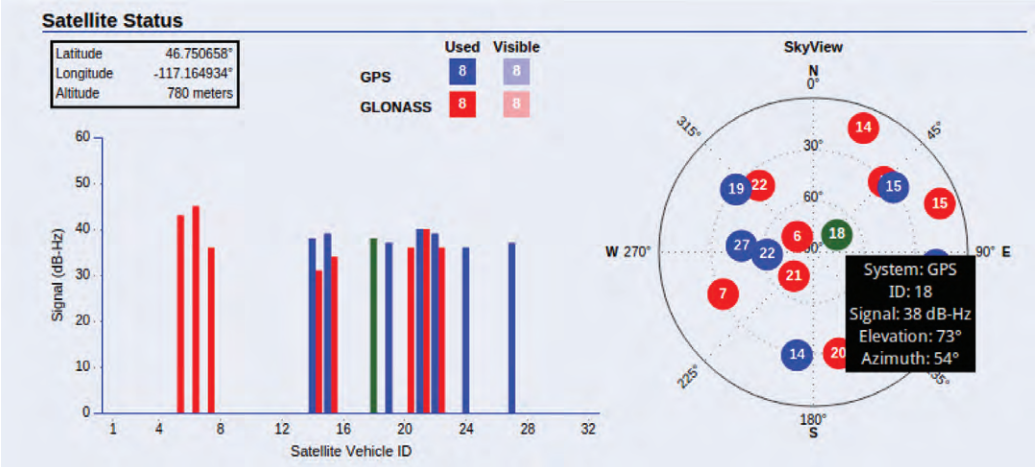


Figure 3.7 Satellite Information on SkyView

Front-Panel Replication

The **Satellite Lock**, **Time Quality**, and **Antenna** LEDs on the dashboard replicate the front-panel indicators of the same name. See *Front Panel* for operational indications.

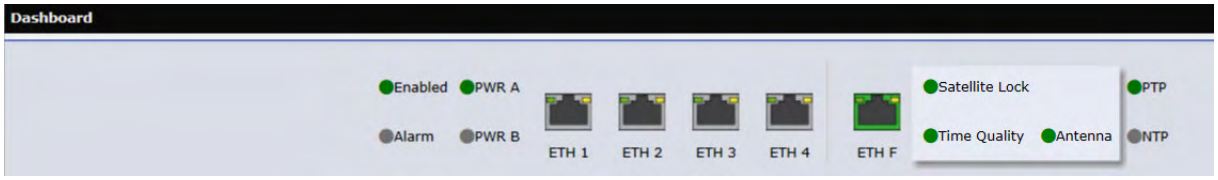


Figure 3.8 Time Synchronization Dashboard LEDs

Time Input Status

When GNSS Time Source is enabled and the SEL-2488 is locked, **GPS** displays in the **Available Sources** section. After qualification of the GNSS input and a determination of its accuracy, **GPS** will display as the **(Selected)** source (*Figure 3.9*).

When GNSS Time Source is disabled or the SEL-2488 is not receiving GNSS signals, **GPS** will not display in the **Available Sources** section of the **Time Input** status widget.

If the clock is in Holdover operation, **Holdover** will display as the **(Selected)** source at the top of **Available Sources**.

Until the SEL-2488 has initially synchronized to a source, the Available Sources displays **None**. When you set the SEL-2488 through Manual Date/Time mode, **Manual** displays under **Available Sources**.

There are times when the (Selected) source may show poorer time quality than another source. This can happen when the SEL-2488 is in the process of qualifying a new time source.

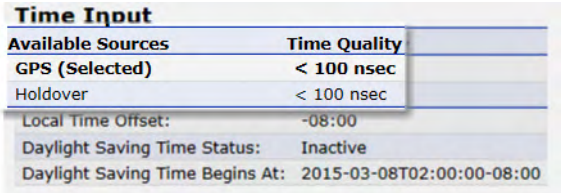


Figure 3.9 Time Input Status Widget: Available Sources

Time Offset and Daylight Saving information is not available until GNSS time is qualified.

The **Time Input** status widget also provides **Local Time Offset**, **Daylight Saving Status** (Off, Active, Inactive) and indicates when the next transition will happen (if Daylight Saving is enabled) and **Leap Second Pending** status (when known).

Diagnostics Status

The **Diagnostics** status widget provides the present operational status of the antenna system, GNSS receivers, and the holdover clock.

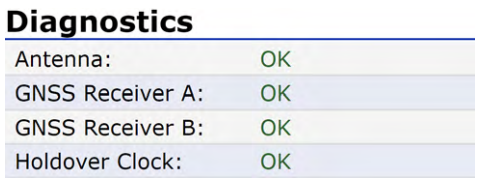


Figure 3.10 Diagnostics Status Widget: Time Synchronization

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for the events associated with time synchronization. The SEL-2488 replaces message variables in {} with values it logs.

Table 3.5 Time Synchronization Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
1µs ≤ Time Quality < 1ms.	Notice	Minor	Time Synchronization
Failure: Antenna open/absent	Alert	Major	–
Failure: Antenna short	Alert	Major	–
Failure: GNSS Receiver A	Alert	Major	–
Failure: GNSS Receiver B	Alert	Major	–
Failure: Holdover Clock	Alert	Major	–
GNSS Notification Settings: Changed by {username} at {user_ip}.	Notice	Minor	Configuration
GNSS Settings: Changed by {username} at {user_ip}.	Notice	Minor	Configuration
GNSS signal verification failed.	Error	Minor	System Integrity
GNSS signal verification is not operational.	Warning	Minor	System Integrity
GNSS signal verification is operational.	Warning	Minor	System Integrity
GNSS signal verification successful.	Error	Minor	System Integrity
Holdover Alert.	Critical	Major	–
OK: Antenna connection	Error	Minor	–
Time Quality ≥ 1ms.	Notice	Minor	Time Synchronization
Time Quality < 1µs.	Notice	Minor	Time Synchronization
Time source has changed to {0}.	Warning	Minor	Time Synchronization

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Events with an alarm category of Minor and alarm class of "–" will always trigger the alarm contact. Events classified as Major will latch the alarm contact.

This page intentionally left blank

Section 4
Ethernet Network Interfaces

Overview

The SEL-2488 Ethernet network interfaces make possible many of the features on the device. They provide the connectivity to allow device management, Precision Time Protocol (PTP) and Network Time Protocol (NTP) operation, remote status and event reporting, and access to centralized user authentication solutions.

The SEL-2488 has four network interfaces for normal network connections and one interface on the front designed for local management of the device. All of the interfaces are independent of each other and do not pass (bridge or route) network traffic among the interfaces.

The interfaces operate in Ethernet Layer 2 mode when the interface is enabled in the configuration. At least one interface must be configured to Layer 3 with an Internet Protocol (IP) address assigned to the interface and Hypertext Transfer Protocol Secure (HTTPS) service enabled for management of the device. By default this is the front Ethernet interface (ETH F); however, it can be assigned to other interfaces.

By enabling each interface and assigning an IP address to each, you can configure all interfaces for Layer 2 and Layer 3 operation. IP services (HTTPS, NTP, SNMP, and Captive Port) are individually enabled by interface and service may only be available on specific interfaces. Captive Port, for example, is only available on the **ETH F** interface, and NTP and PTP are not available on this interface. An IP address must be set on an interface before IP services can be enabled and active.

Although Precision Time Protocol (PTP) is a network service, it is controlled through the PTP Settings page and not the IP Configuration page.

The interfaces provide a gratuitous ARP request when you enable an Ethernet port, connect a cable, or change IP settings to an enabled interface. The device will send out the gratuitous ARP request at the time of a port change and sends a second request two seconds later.

Interface Status Indicators

Each physical Ethernet interface port contains two status LEDs collocated with the port. The green LED indicates connection and activity, and the yellow LED indicates speed and collision.

The green LED reflects the following conditions:

- ON (solid): Link present, no port activity (transmit/receive)
- Blinking: Link present, port activity (transmit/receive)
- OFF: Link absent or interface disabled

The yellow LED reflects the following conditions:

- ON (Solid): 100 Mbps link
- Blinking: Data collision
- OFF: 10 Mbps link

ETH F Interface Reset

The SEL-2488 provides a physical mechanism to enable the **ETH F** interface and services (HTTPS, Captive Port) on that interface. This mechanism becomes necessary in situations when configuration disables this interface and the clock is inaccessible from the other interfaces.

Perform the following steps while the clock is operating to reset the **ETH F** interface.

Step 1. Locate the pinhole reset access hole next to the alarm contact connector.

Step 2. Insert a pin or paper clip into the hole and gently depress the reset button for at least five seconds.

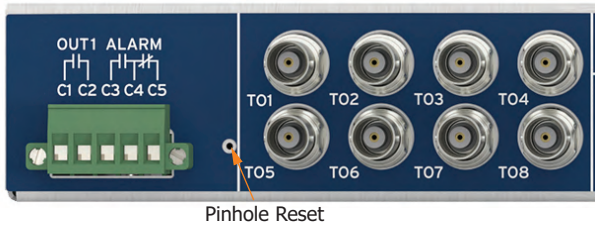


Figure 4.1 Location of Pinhole Reset

Do not do this when turning on the clock, or the clock will be reset to factory-default conditions.

Once reset, the **ETH F** interface will have both the HTTPS and Captive Port services enabled. The **ETH F** IP address will display on one of the LCD screens.

Captive Port

Captive Port is a service that combines a subset of Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) applications to assist with automatic network configuration of devices connected to a port. A network device (typically a computer) with the DHCP client enabled will, when connected to the interface with Captive Port enabled, receive an IP address, a default gateway, and a limited DNS resolver. This will resolve all DNS requests to the address the Captive Port configuration designates. However, in some web browsers, such DNS requests to arbitrary

site names (selinc.com, for example) in combination with a self-signed security certificate, may result in a browser error message that can be difficult to resolve. To avoid this, it is best to directly use the IP address of the device whenever possible.

To use the Captive Port feature for managing the clock, connect a DHCP client-enabled desktop or laptop computer to the SEL-2488 ETH F port. Captive Port is enabled on the SEL-2488 ETH F port by default. Wait a few minutes for the service to complete its configuration, and then open a recommended web browser; see *Connecting to the Device on page 1.10*. Enter a site name (selinc.com, for example) or the ETH F IP address (displayed on one of the LCD screens) into the address bar. The browser automatically redirects to the commissioning page (noncommissioned device) or to the login page (commissioned device).

Figure 4.2 LCD ETH F Information Screen

Captive Port on the SEL-2488 is intended to supply an IP address to one device directly connected to the ETH F port. It is not meant to supply IP addresses to a network of devices. If the ETH F port is connected to a network, the Captive Port option should be disabled.

Captive Port assigns IP addresses to the DHCP client according to the IP address configuration of the ETH F interface. A change of IP address on the ETH F interface causes Captive Port reconfiguration and results in it assigning addresses based on the new settings. The client must request a new DHCP lease to continue working. It is typically easiest to disconnect and reconnect the cable from ETH F to accomplish this.

HTTPS

HTTPS is the service that allows the Internet browser client to connect to the device to manage configuration settings. This service is enabled independently on each port. To prevent loss of management access to the device, at least one interface must remain enabled, it must have an IP address, and HTTPS must be enabled on that interface.

NTP Server

NTP Server is enabled on a per-interface basis. It is only available on the four rear interfaces, not on the management interface (ETH F). The service requires an IP address to operate, so the interface must be configured with an IP address and enabled to allow NTP Server for that interface. This enables basic NTP client-server operation. Additional NTP operation modes, Broadcast and Multicast, can be enabled on the Network Time Protocol settings page and are discussed in *Section 8: Network Time Protocol (NTP)*.

SNMP

SNMP read access to the SEL-2488 is enabled on a per-interface basis. It is available on the four rear interfaces and the management interface (ETH F). The service requires an IP address to operate, so the interface must be configured with an IP address and SNMP enabled. This action determines which interfaces will allow SNMP requests to the device. In addition, to set up the connection methods, SNMP read profiles must be created on the Simple Network Management Protocol settings page.

Settings

This section discusses the settings that customize and affect the operation of the Ethernet network interfaces. Use the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **Network Management > IP configuration** menu option to configure SEL-2488 network interfaces.

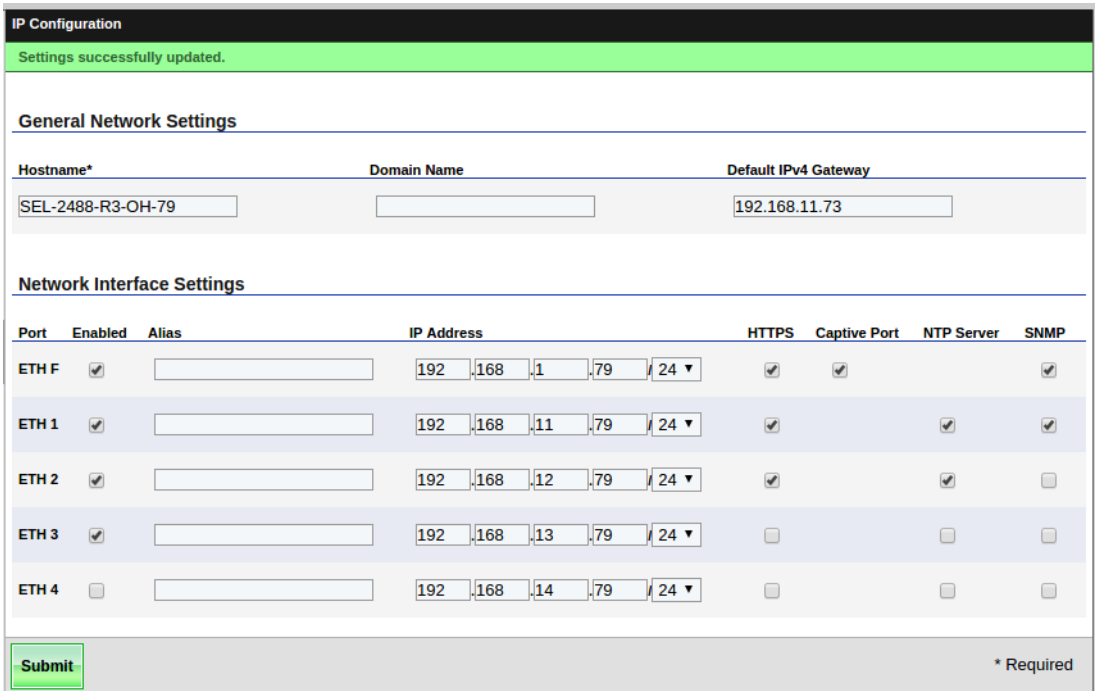


Figure 4.3 IP Configuration Page

CAUTION

With the release of firmware version R102, the SEL-2488 will verify that device interface IP addresses do not fall within the same network address range.

If your device is using firmware version R101 or earlier, and has IP addresses for different ports that fall within the same network address range, an upgrade to R102 will cause the settings import to fail and all device settings will revert to the factory-default values.

The SEL-2488 network interface settings must adhere to the following.

IP Addresses:

- All IP addresses defined on the device are IPv4 addresses.
- All IP addresses must be in the range 1.0.0.0–223.255.255.254.
- Interface IP addresses cannot be the network or broadcast address (first or last address in the address range the mask defines).

- Interface IP addresses must be unique. Two or more interfaces cannot have the same IP address.
- Interface IP address cannot be the same as the default gateway.
- Interface IP addresses cannot have the same network address (first address in the address range the mask defines).
- Interface IP address cannot be the same as a remote syslog server or SNMP trap server address.
- A port alias is required if an IP address is entered.
- Layer 3 services can only be enabled on ports with an IP address. It is possible to select services on ports without an IP address, but the selection will not remain after submission.
- ETH F requires an IP address even when the port is disabled. This is to support the front management port reset option.

Host and Domain Name:

- Hostname must be at least a single character and cannot be longer than 63 characters.
- Hostname can only contain characters a–z, A–Z, 0–9, the underscore "_", and the hyphen "-".
- Domain names can only contain characters a–z, A–Z, 0–9, the underscore "_", the period ".", and the hyphen "-".
- The hyphen cannot be the first or last character.
- Domain names can contain a period, but not as the first or last character.
- The hostname cannot contain a period.
- Domain names are a group of labels separated by periods.
- Each domain label must be at least one character and cannot be longer than 63 characters.
- The domain name can be blank.
- The combined length of the hostname and domain name cannot exceed 253 characters.

Table 4.1 General Network Settings

Setting Name	Values	Default	Description
Hostname	1–63 characters	SEL<SERIAL#>	The unique name identifying the device on the network
Domain Name	0–253 characters		The domain name of which the device is a member
Default IPv4 Gateway	Unicast IP address		The IP address of the device used to transfer packets to another network

The Network Interface Settings groups in the following listing have two sections, one for the ETH F interface and one for the ETH 1–4 interfaces, because of different default values and available settings.

Table 4.2 ETH F Network Interface Settings

Setting Name	Values	Default	Description
Enabled	Checked, Unchecked	Checked	Enables or disables the interface
Alias	1–32 characters	Default F	Associates a name with the network interface
IP Address	Unicast IP address	192.168.1.2/24	Establishes the IP address of the interface. The device uses classless inter-domain routing (CIDR) notation to assign the subnet mask.
HTTPS	Checked, Unchecked	Checked	Enables or disables HTTPS on the interface
Captive Port	Checked, Unchecked	Checked	Enables or disables Captive Port on the interface
SNMP	Checked, Unchecked	Unchecked	Enables or disables SNMP read through the interface

Table 4.3 ETH 1–4 Network Interface Settings

Setting Name	Values	Default	Description
Enabled	Checked, Unchecked	Unchecked	Enables or disables the interface
Alias	1–32 characters		Associates a name with the network interface
IP Address	Unicast IP address		Determines the IP address of the interface. The device uses classless inter-domain routing (CIDR) notation to assign the subnet mask.
HTTPS	Checked, Unchecked	Unchecked	Enables or disables HTTPS on the interface
NTP Server	Checked, Unchecked	Unchecked	Enables or disables NTP Server on the interface
SNMP	Checked, Unchecked	Unchecked	Enables or disables SNMP read through the interface

IP Configuration With PRP/Port Bonding Enabled

When PRP and/or active-backup port bonding is enabled, the combined physical Ethernet ports are listed as a single IP configuration as shown in *Figure 4.5*. See *Section 24: Parallel Redundancy Protocol (PRP)* and *Section 25: Active-Backup Port Bonding* for details.

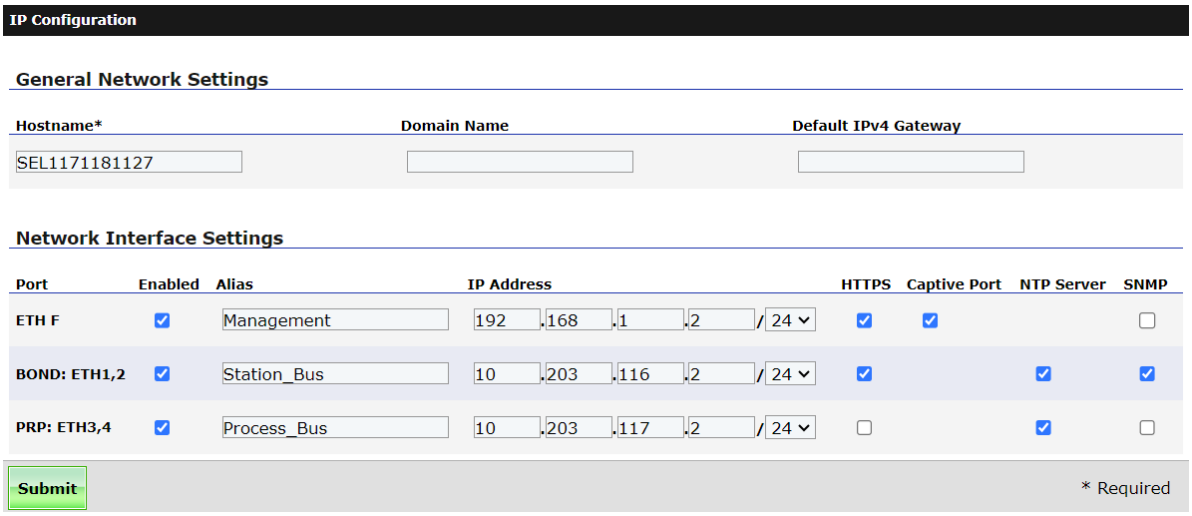


Figure 4.4 IP Configuration Page: One PRP Interface and One Active-Backup Bonded Interface Enabled

Front Panel

Interface LEDs

The **ETH F** interface is located on the front panel, and its LEDs are incorporated into that interface. **ETH 1–4** are located on the back panel and have status LEDs incorporated into those interfaces (copper or fiber). There are LEDs on the front panel that mimic the status of the interface LEDs.

Table 4.4 Interface Status Indicators

LED Indicators	On	Blinking	Off
ETH F: Green	Link present—no activity	Link present—transmit/receive activity	Interface disabled or no link
ETH F: Yellow	100 Mbps communication	Data collision	10 Mbps communication
ETH 1–4: Link/ACT (Green)	Link present—no activity	Link present—transmit/receive activity	Interface disabled or no link
ETH 1–4: 100 Mbps (Yellow)	100 Mbps communication	Data collision	10 Mbps communication

Figure 4.5 Ethernet Front-Panel Interface LEDs

LCD

Table 4.5 LCD Ethernet Interface Screen

Indicator	Interface Enabled	Interface Disabled
ETH F Interface Information	`ETH F` <CIDR IP address of ETHF Interface> Ex. `192.168.1.2/24` If Captive Port is enabled, the third line shows `DHCP (Captive Portal)`	`ETH F` `Disabled`

Figure 4.6 LCD ETH F Information Screen

Dashboard

The web dashboard contains a graphical indication of the status of the Ethernet interfaces on the device. The color of the interface icon defines whether the port is enabled, disabled, or enabled but lacking a connection to an Ethernet device. The icon has small indicator boxes that reflect the status lights on the physical interface ports. See *Table 4.4* for definition of the indicators.

When the icon contains green fill, as shown in *Figure 4.7*, the interface is enabled and has a connection to an Ethernet device.

Figure 4.7 Ethernet Dashboard Indicators: Enabled and Connected

When the icon contains light gray fill, as shown in *Figure 4.8*, the interface is enabled but does not have a connection to an Ethernet device.

Figure 4.8 Ethernet Dashboard Indicators: Enabled and Not Connected

When the icon contains dark gray fill, as shown in *Figure 4.9*, the interface is disabled.

Figure 4.9 Ethernet Dashboard Indicators: Disabled

Additional information regarding the interface is displayed in a table below the Ethernet indicator icons. The information includes the physical Ethernet port, alias, media type, the operational speed and duplex, port bonding status, MAC address, IP address and mask in CIDR format, and the services/ protocols presently enabled on the interface.

Port	Alias	Media Type	Speed/Duplex	Port Bonding	MAC Address	IP Address	Services/Protocols
ETH 1	Station_Bus	10/100BASE-T	100Mbps Full Duplex	BOND: ETH1,2 (Active)	00:30:a7:14:5a:06	10.203.116.2/24	HTTPS, NTP Server, SNMP
ETH 2	Station_Bus	10/100BASE-T	100Mbps Full Duplex	BOND: ETH1,2 (Backup)	00:30:a7:14:5a:06	10.203.116.2/24	HTTPS, NTP Server, SNMP
ETH 3	Process_Bus	100BASE-FX	100Mbps Full Duplex	PRP: ETH3,4 (LAN A)	00:30:a7:14:5a:08	10.203.117.2/24	NTP Server, PTP
ETH 4	Process_Bus	100BASE-FX	100Mbps Full Duplex	PRP: ETH3,4 (LAN B)	00:30:a7:14:5a:08	10.203.117.2/24	NTP Server, PTP
ETH F	Management	10/100BASE-T	100Mbps Full Duplex	Not Bondable	00:30:a7:14:5a:0a	192.168.1.2/24	Captive Port, HTTPS

Figure 4.10 Ethernet Dashboard Indicators: Additional Information

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for events associated with Ethernet network interfaces. The SEL-2488 replaces message variables in {} with values it logs.

Table 4.6 Ethernet Network Interfaces Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
`Captive Port: disabled by {username} at {user_ip}`	Notice	Minor	Configuration
`Captive Port: enabled by {username} at {user_ip}`	Notice	Minor	Configuration
`Front management port reset initiated through pinhole button`	Alert	Minor	Chassis
`Network Interface {0}: changed by {username} at {user_ip}`	Notice	Minor	Configuration
`Network Settings: changed by {username} at {user_ip}`	Notice	Minor	Configuration
`Port {0} changed link state to down`	Notice	Minor	Link
`Port {0} changed link state to up`	Notice	Minor	Link

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

This page intentionally left blank

Section 5
Static Routes

Overview

The SEL-2488 supports the assignment of static routing as an enhancement to the Ethernet Network Interfaces. Ethernet traffic has two possible destination options. One is local, or Layer 2 communication, where packets use media access control (MAC) IDs to move from the source to the destination and do not travel to other networks. The second destination option is routed, or Layer 3 communication, in which the packets leave one local network and route to another local network. This communication is based on Internet Protocol (IP) addresses.

Routing Explained

Just as a car going from one city to another has to take correct roads and perhaps travel through one city and then take a different road to get to the next, Ethernet traffic destined for other networks must take the correct route through various networks to reach the destination network. Routing is the process of determining how to navigate through networks. It makes use of routing tables that provide information to Ethernet traffic. Routing basically defines which device on the local network forwards traffic for a specific remote destination. That device will have its own routing table that defines where it should send the traffic for the next intersection on the way to its destination.

Traffic traveling to a remote destination will always take the highest priority route to that destination. Network devices using the Ethernet standard define a default route (typically called the default gateway) to which all traffic not destined for the local network will travel for routing to the destination. The default route is always the lowest priority route and serves as a catch-all for any traffic without a higher priority (more specific) route.

The SEL-2488 supports default route functionality and the capability to define more specific routes, known as static routes.

Static routes allow traffic for a specific device or network to be directed to a local device other than the default gateway. Perhaps the destination local network is unreachable from the default route, or use of the alternative route causes the traffic to travel less used networks and reach the destination faster. Applications for such routing may include special routes for management traffic or NTP request/responses or remote event reporting. Static routes you define on the SEL-2488 apply only to traffic the SEL-2488 generates.

In the SEL-2488, static routes are entered in the format of destination network (Remote Network) and the local IP address (Gateway). Some examples are as follows:

NOTE: Static routes will not work if the gateway IP is unreachable from the local network; traffic will route to the default gateway instead.

Remote Network	Gateway
192.168.15.0/24	192.168.1.1
172.16.0.0/16	192.168.1.5
192.168.2.125/32	192.168.1.9 (single device)

Settings

This section discusses the settings that customize and affect operation of the static routes. Use the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **Network Management > Static Routes** menu option to configure the SEL-2488 static routes.

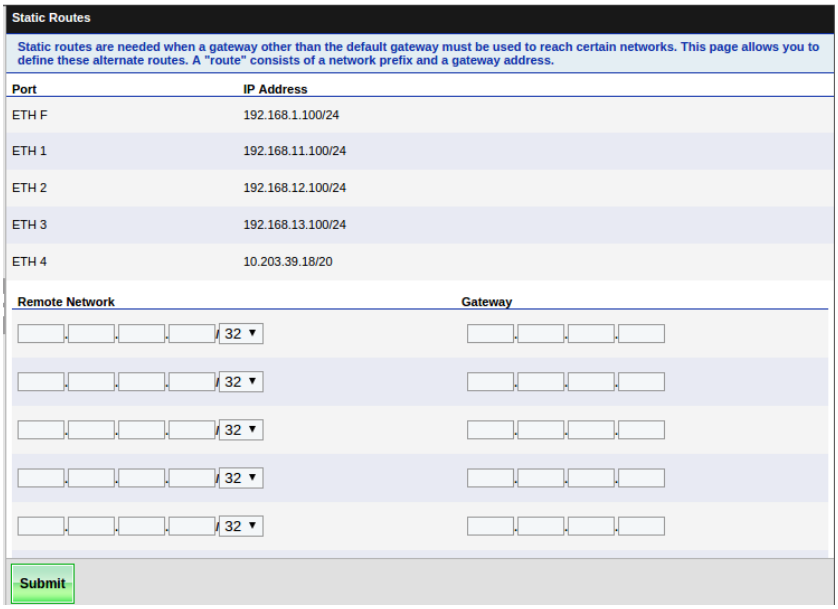


Figure 5.1 Static Routes Settings Page

NOTE: The presence of an interface does not indicate that the interface is enabled, only that there is an IP address assigned.

The **Static Routes** settings page is divided into two sections. The top section is an information block that describes interfaces that presently have an IP address set for the interface. This information displays to assist you in determining the gateway address for the static route. The gateway address must be within the range of one of the defined IP addresses in this section and the interface must be enabled for the static route to work. Look to the **IP Configuration** settings page to determine if the interface is enabled.

Use the lower section of the **Static Routes** settings page to define static routes. The SEL-2488 supports as many as 20 optional static route definitions.

Table 5.1 Static Route Settings

Setting Name	Values	Default	Description
Remote Network	Unicast Network address	n/a	Network address corresponding to the remote network, consisting of an IP address and its subnet mask
Gateway	Unicast IP address	n/a	IP address for the device (not SEL-2488 address) to which the SEL-2488 sends packets destined for the remote network

The Remote Network setting converts the IP address you enter to the network address (first IP address of range) based on the IP address and subnet mask you enter when you submit the form.

For example, 192.168.23.161/25 will convert to 192.168.23.128/25.

To clear a static route you have entered, delete the remote network and gateway IP values for the route before submitting changes. You do not need to clear the subnet mask value (the drop list after the /). Clearing a static route from the middle of the list causes the remainder of the list to move up and the empty route row to move to the bottom when you submit the form.

Static Routes Settings With PRP/ Port Bonding Enabled

When PRP and/or active-backup port bonding is enabled, the combined physical Ethernet ports are listed as a single static routes configuration as shown in *Figure 5.2*. See *Section 24: Parallel Redundancy Protocol (PRP)* and *Section 25: Active-Backup Port Bonding* for details.

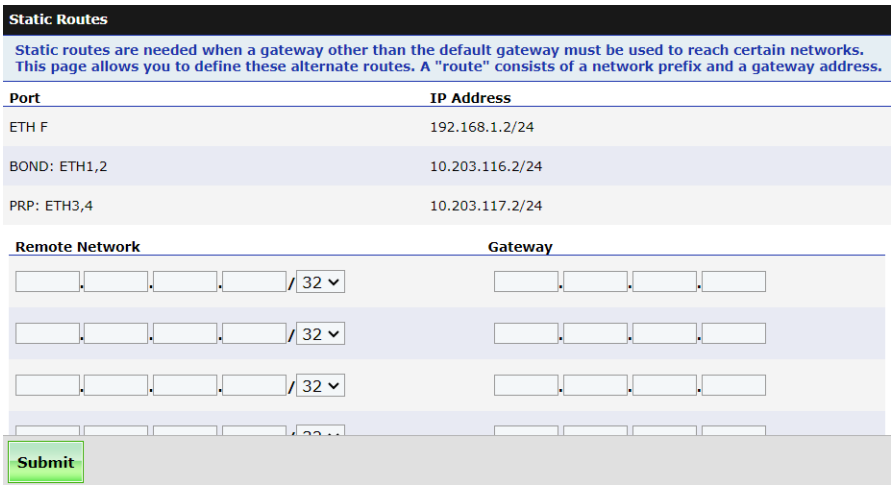


Figure 5.2 Static Routes Settings Page: One PRP Interface and One Active-Backup Bonded Interface Enabled

Front Panel

The front panel does not display any static route information.

Dashboard

The dashboard does not display any static route information.

Alerts/Notifications

The SEL-2488 provides the following alert or notification when the user changes static route settings. The SEL-2488 replaces message variables in {} with values it logs.

Table 5.2 Static Routes Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
`Static Route Settings: changed by {username} at {user_ip}`	Notice	Minor	Configuration

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Section 6
Time-Code Outputs

Overview

The SEL-2488 comes standard with eight Bayonet Neill–Concelman (BNC) outputs and a single DB-9 output. Each of these ports can independently output demodulated IRIG-B, kilo pulses per second (kPPS), and pulses per second (PPS). Ports **TO1** through **TO4** can output modulated IRIG-B signals. The SEL-2488 has sufficient drive capacity to provide time-code signals to many products simultaneously.

Operation

The SEL-2488 continuously transmits selected signals from each port once it determines initial time source selection, qualification, and accuracy. On startup, to prevent transmission of inaccurate information from the time-code output ports, the clock will not enable these ports until it selects a time source and determines its accuracy. Depending on the source and the interval since the clock last synchronized to the source, this process may take as long as 15 minutes. IRIG-BXX4 signaling transmits the present clock reported time quality as part of the message.

When no other source is present, you can set the SEL-2488 in the Manual Date/Time mode. This meets the criterion for a selected source that enables the time-code output ports. In this case, IRIG-BXX4 signaling reports a time quality of 0 (locked to a UTC traceable source) for demonstration purposes. See *Section 19: Date/Time* for details.

The SEL-2488 also delivers time-code output signaling through Pin 4 and Pin 6 of the DB-9 (**COM 1**) connector.

Holdover

If the SEL-2488 loses its primary reference (GNSS), it goes into holdover mode and continues to provide time outputs based on its internal reference oscillator. While in holdover mode, the time quality (TQ) and continuous time quality (CTQ) data points in the IRIG-BXX4 signaling reflect the present holdover accuracy.

Signal Output Formats

IRIG-B002	Transmit demodulated IRIG-B002 in local time or Coordinated Universal Time (UTC). Format does *not* send year or control bits.
IRIG-B004	Transmit demodulated IRIG-B004 format in local time or UTC. Control bits comply with the IEEE C37.118.1-2011 standard (reverse compatible with IRIG-B000 and IEEE C37.118-2005).
IRIG-B122	Transmit modulated IRIG-B122 in local time or UTC. Format does *not* send year or control bits.

IRIG-B124	Transmit modulated IRIG-B124 format in local time or UTC. Control bits comply with the IEEE C37.118.1-2011 standard (reverse compatible with IRIG-B120 and IEEE C37.118-2005).
kPPS	Transmit 1,000 pulses per second.
PPS	Transmit 1 pulse per second.

The SEL-2488 transmits IRIG-B signaling in two formats: standard (XX2) and extended (XX4). The extended format transmits the control bits according to the IEEE C37.118.1-2011 definition, which is backward-compatible to extended format (XX0) and IEEE C37.118-2005. The SEL-2488 can generate even or odd parity for the extended IRIG-B format in BXX4 signaling. Parity is not selectable per port, but is a global configuration for the time-code outputs. All ports sending the extended format(s) use the same parity calculation.

In addition to demodulated IRIG-B, kPPS, or PPS, for Ports **T01** through **T04**, you can optionally select modulated IRIG-B signaling. Configuration of IRIG-B format, time reference, and parity are common for all ports configured to use modulated IRIG-B signaling. The modulated output is a standard IRIG-B12X amplitude-modulated signal. The accuracy of this signal is ±1 µs peak, and the nominal output level is 6.2 Vpp. Maximum cable length is 152 m (500 ft).

The SEL-2488 can represent time in the IRIG-B message either in local time or UTC. You can select either local time or UTC by port for demodulated IRIG-B. For modulated IRIG-B, this is a common setting across all ports. Local time is based on the present local time offset and daylight-saving time settings on the clock. Local/UTC reference selection has no impact on the kPPS/PPS signaling formats.

For details on the information contained in the specific IRIG-B formats, see *Appendix E: IRIG-B*.

Output Drive Capacity

Output drive capacity depends on loading of the output. The input impedance of devices connected to the output determine that load. High-impedance input devices, typically ≥1 kilohm input impedance, do not load the output as much as low-impedance devices, so you can connect more high-impedance devices to one output. We introduce here a few design considerations toward providing a robust connection solution.

We recommend limiting the connections on one output to either all high-impedance or all low-impedance devices.

NOTE: Do not apply a 50 Ω termination when five or more low-impedance devices are on a chain. The cumulative effect of the low-impedance devices will provide the terminating effect.

The end of the device chain must be terminated to 50 ohms (see note to left for exception). This balances the supply line to the devices, provides the maximum energy transfer from the output to the devices, and limits the interference generated by reflections of signals from the devices. In some cases, the devices may be internally terminated. When this is the case, do not use external termination and set only one (the end) device to terminate the supply line.

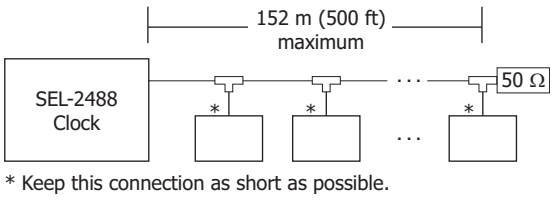


Figure 6.1 Multiple Device Connections

NOTE: Equipment that is not in close proximity may, during normal operation or an energy event, exhibit a phenomenon known as ground potential rise where each chassis is at a different potential. Be cautious when using coaxial cables because they can become unintentional conductors for the differential energy. The farther devices are apart, the greater the chance for this phenomenon.

The cabling used from the output to the devices should be a 50 Ω impedance coaxial cable. Using cable with a different impedance will cause additional line loss and interference, reducing the number of devices that you can connect or the allowable length of the supply cable. The SEL standard cable used for the time-code output is the RG-58 cable. If you use this cable, the length can be as long as 152 m (500 ft) between the output and the end device. Using cables with lower loss per foot (e.g., an RG-8X cable) extends this distance.

Table 6.1 shows typical drive capabilities per demodulated BNC output for the SEL-2488 to other SEL equipment. The demodulated BNC outputs provide a standard IRIG-B00X DC level-shift signal. The drive capability of each output is 250 mA at a nominal level of 5.0 V. Typically, this works out to 10 low-impedance devices or 20 high-impedance devices per output.

NOTE: Avoid mixing low-impedance and high-impedance devices on the same output.

Table 6.1 Output Drive Capacity

Product	Input Impedance	Units Per SEL-2488 Output
SEL-100 Series	Very Low	2 parallel, 20 series/parallel[a]
SEL-200 Series	Very Low	2 parallel, 20 series/parallel[a]
SEL-300 Series	Low	10[b]
SEL-400 Series	High[c]	20[d]
SEL-500 Series	Low	10[b]
SEL-651R	High[c]	20[d]
SEL-700 Series	High[c]	20[d]
SEL-2020, SEL-2030, SEL-2032	Low	10[b]
SEL-2240	High[c]	20[d]
SEL-2411	High[c]	20[d]
SEL-2414	High[c]	20[d]
SEL-2431	Low	10[b]
SEL-2440	High[c]	20[d]
SEL-2523, SEL-2533	High[c]	20[d]
SEL-2810MT, SEL-2812MT	High[c]	20[d]
SEL-3031	Low	10[b]
SEL-3350 Series	High[c]	20[d]
SEL-3530	High[c]	20[d]
SEL-3610, SEL-3620, SEL-3622	High[c]	20[d]
SEL-3400	High[c]	20[d]
SEL-3401 manufactured before Sept. 2011	Low	10[b]
SEL-3401 manufactured Sept. 2011 or later	High[c]	20[d]

[a] Do not add external terminating resistor.
[b] Install 50 Ω termination resistor on farthest device for four or fewer devices.
[c] High impedance is typically equal to or greater than 1 kilohms.
[d] Install 50 Ω termination resistor on farthest device.

The SEL-100 and SEL-200 series devices are a special case because they have extremely low input impedance. Because of this, it is recommended to only connect two of these devices in parallel, as shown in *Figure 6.1*. However, it is standard practice to connect these devices in a series of parallel connections

consisting of two relays, where the –IRIG input of the first relay is connected to the +IRIG input of the second relay, with as many as ten paired series connected in parallel.

Cable Delay Compensation

Compensating for the type and length of cable connected between the time output and the IEDs helps maintain a very tight timing accuracy to all local devices. To preserve accuracy, the SEL-2488 provides time-delay compensation for output cables on a per-port basis. *Figure 6.2* shows an example of a clock with two output ports configured with different cable lengths. One output port is configured for a 30 ns delay (simulating 6 meters of RG-58), while another is configured for a 180 ns delay (simulating 36 meters of RG-58).

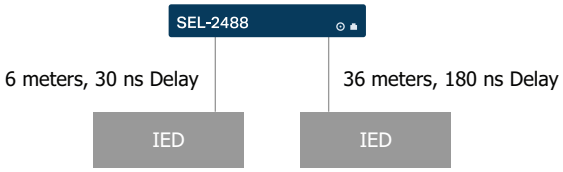


Figure 6.2 SEL-2488 Cable Delay Compensation Example

Typical cable delay is as follows:

- RG-58: 5 ns/meter (1.52 ns/foot)—Recommended cable
- RG-8X: 3.87 ns/meter (1.18 ns/foot)

When designing for cable delay compensation and using a time output connected to multiple IEDs, consider grouping IEDs by location to minimize the cable lengths between devices. Calculate and apply cable delay based on the average distance between the nearest and farthest IEDs in the group.

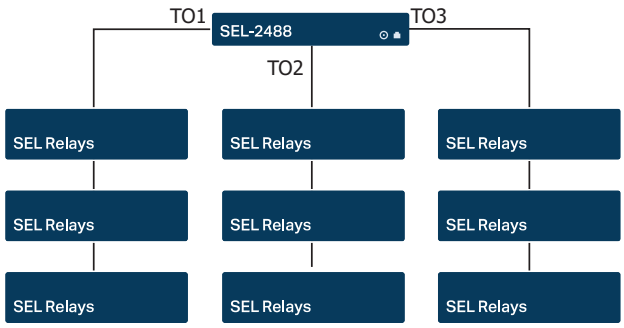


Figure 6.3 SEL-2488 Grouping for Use of Cable Delay Compensation

Settings

The **Time Code Outputs** page allows setting of time outputs TO1 through TO8 and COM1 (see *Figure 6.4*).

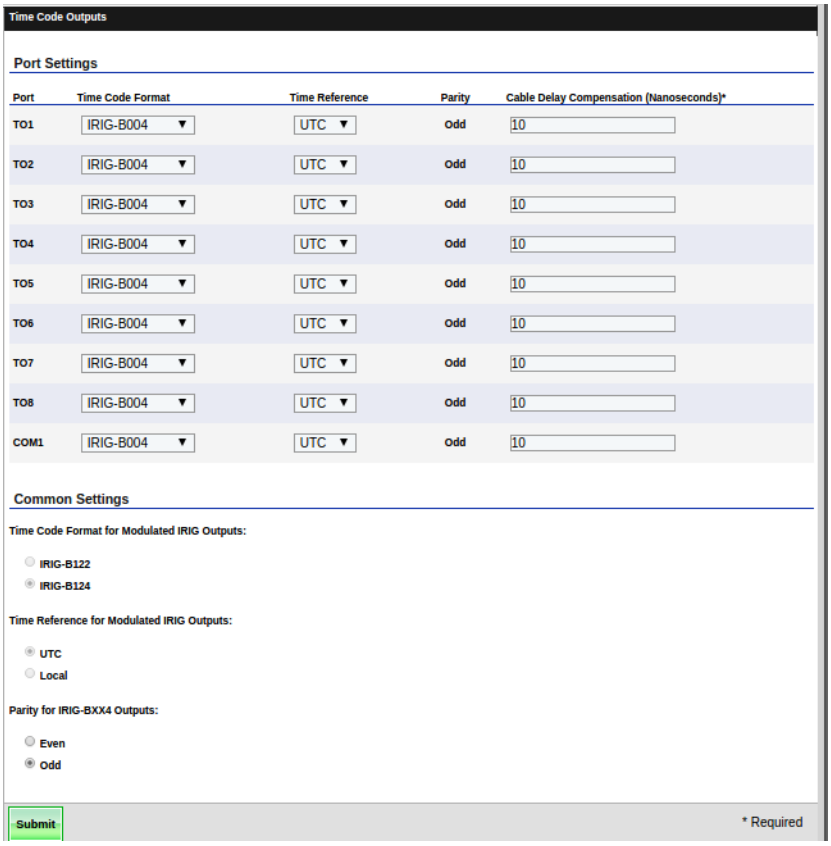


Figure 6.4 Time-Code Outputs Settings Page

Table 6.2 Time-Code Output Common Settings

Setting	Values	Default	Description
Time Code Format for Modulated IRIG-B Outputs:	IRIG-B122, IRIG-B124	IRIG-B124	Selects the format of the modulated IRIG-B signal for the ports using modulated IRIG-B output.
Time Reference for Modulated IRIG-B Outputs:	UTC, Local	UTC	Selects Local or UTC time for the modulated IRIG-B messages.
Parity for IRIG-BXX4 Outputs:	Even, Odd	Odd	Sets the parity of the IRIG-B frame.

Table 6.3 Time-Code Output Port Settings (Sheet 1 of 2)

Settings (Per Port)	Values	Default	Description
Time Code Format (Ports TO1–TO4)	IRIG-B002, IRIG-B004, Modulated IRIG-B, PPS, KPPS	IRIG-B004[a]	Sets TO1–TO4 to the specified signal format.
Time Code Format (Ports TO5–TO8, COM1)	IRIG-B002, IRIG-B004, PPS, KPPS	IRIG-B004[a]	Sets TO5–TO8 and COM1 to the specified signal format.
Time Reference	Local, UTC	UTC	Selects local time or UTC for the IRIG-B message. When **Modulated IRIG Output** is selected, tracks Common Settings Time reference. Has no effect on PPS or kPPS signals.

Table 6.3 Time-Code Output Port Settings (Sheet 2 of 2)

Settings (Per Port)	Values	Default	Description
Parity	Even, Odd, -	Odd	Not directly settable on port, tracks to common Parity for IRIG-BXX4 Outputs setting when **IRIG-B004** or **Modulated with IRIG-B124** format selected. Otherwise, set to "-".
Cable Delay Compensation	0–2500 ns	10	Compensates for signal delays introduced by cable type and length, adjustable for demodulated, kPPS, or PPS formats. When modulated time format is selected for a port, this setting for that port is forced to 0 and is not adjustable. Entered in nanoseconds of delay: RG-58: 5 ns/meter (1.52 ns/foot) RG-8X: 3.87 ns/meter (1.18 ns/foot)

[a] With the frequency outputs hardware option installed, the time outputs TO1–TO8 and COM1 will default to the PPS signal format.

Table 6.3 lists all the settings in the time-code output settings. All time outputs allow configuration of the ports as IRIG-B002, IRIG-B004, kPPS, and PPS. Ports TO1 through TO4 can individually be configured for modulated IRIG-B output. Common settings control the modulated time configuration. You can only choose one time-code format and time reference for all ports configured for modulated time.

Front Panel

The front panel does not display any time-code output information.

Dashboard

The **Time Output** section provides a quick reference showing the present state of all device time outputs. The OUT1 output refers to the status of the timer contact, which is addressed in further detail in *Section 9: Timer Contact*.

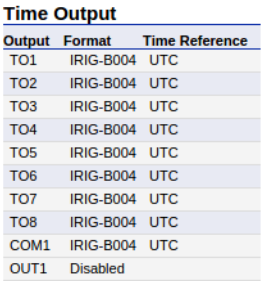


Figure 6.5 Time Output Dashboard Status Widget

Alerts/Notifications

The SEL-2488 provides the following alert or notification for the event associated with time-code outputs. The SEL-2488 replaces message variables in {} with values it logs.

Table 6.4 Time-Code Outputs Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
Time Code Output Settings: Changed by {username} at {user_ip}	Notice	Minor	Configuration

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

This page intentionally left blank

Section 7
Precision Time Protocol (PTP)

Overview

The SEL-2488 includes Precision Time Protocol (PTP) master functionality as an ordering option. PTP is an industry standard protocol (IEEE 1588-2008) for sub-microsecond time synchronization of Ethernet-based devices.

Definitions

PTP Domain—A PTP domain is a logical grouping of clocks that are synchronized to each other.

PTP Master Clock—A PTP master clock is a clock capable of providing a source of time to which other clocks on that path synchronize. The SEL-2488 is a master clock.

PTP Grandmaster Clock—A PTP grandmaster clock is the clock that is the ultimate time source for the PTP domain. The devices on the PTP domain can select the SEL-2488 as the grandmaster clock.

PTP Slave Clock—A PTP slave clock is a clock capable of synchronizing to a PTP master clock. The SEL-2488 cannot be a PTP slave clock.

PTP Doubly Attached Clock (DAC)—A PTP ordinary clock with a PRP interface that uses two (i.e., double) separate PTP enabled ports.

Operation

The SEL-2488 continuously transmits PTP messages from enabled Ethernet interfaces once it determines initial time source selection, qualification, and accuracy. On startup, to prevent transmission of inaccurate information over PTP, the clock will not enable PTP on these interfaces until it selects a time source and determines its accuracy. Depending on the source and the interval since the clock last synchronized to the source, this process may take as long as 15 minutes.

PTP transmits the present clock reported time quality as part of the protocol. When no other source is present, you can set the SEL-2488 in the Manual Date/Time mode. This meets the criterion for a selected source and enables PTP output on selected interfaces. In this case, PTP Announce messages will simulate a Clock Class of 6 and a Clock Accuracy <100 ns for demonstration purposes, with the Time Source field indicating the “HAND_SET” enumeration value. See *Section 19: Date/Time* for details.

Holdover

If the SEL-2488 loses its primary reference (GNSS), it goes into holdover mode and continues to provide time outputs based on its internal reference oscillator. While in holdover mode, the Clock Class and Clock Accuracy PTP status indicators reflect the present holdover accuracy.

PTP V1 vs V2

PTP V2 (IEEE 1588-2008) messages are a significant departure from V1 (IEEE 1588-2002) and is not backward compatible. The SEL-2488 only supports PTP V2 messages.

Accuracy

The SEL-2488 uses hardware time-stamping to achieve sub-microsecond time accuracy in the PTP event messages. There are two methods for time-stamping messages: hardware and software. Hardware time-stamping provides greater accuracy than software time-stamping.

Best Master Clock Algorithm (BMCA)

The Best Master Clock Algorithm (BMCA) is the process by which PTP clocks determine the master and subsequently the grandmaster clock of the domain. The algorithm evaluates priority values, clock class, clock accuracy, clock identity, and other data values in announce messages to determine the grandmaster clock to which all others will synchronize in the PTP domain. IEEE 1588-2008 describes BMCA in greater detail.

PTP Network Design

A well-designed PTP network can provide redundancy and greater coverage that is not available with other timing solutions. Furthermore, with the addition of redundant network paths when utilizing PRP, a robust and resilient network solution can be deployed. Please contact an SEL Customer Service Representative for additional information on PTP network design and best practices.

Settings

NOTE: If the PTP settings are not visible on the web interface of your clock, you will need to purchase the PTP firmware option. See Appendix B: Precision Time Protocol Field Upgrade Instructions for details.

This section discusses the settings that customize the PTP operation. Use the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **Time Management > Precision Time Protocol (PTP)** menu option to configure PTP on an SEL-2488.

Precision Time Protocol (PTP)

Settings

Port	Enable PTP	Profile	Domain	Priority 1	Priority 2	Path Delay Mechanism	Announce Interval	Announce Timeout	Sync Interval	Delay Interval	VLAN Enabled	VLAN ID	802.1Q Priority	Grandmaster ID
ETH 1	☑	IEEE C37.238-2011	0	128	128	P2P	1	2	1	1	☐	-	-	5
ETH 2	☑	Default (UDP)	0	128	128	P2P	1	2	1	1	☐	-	-	-
ETH 3	☐	IEEE C37.238-2017	0	128	128	P2P	1	3	1	1	☐	-	-	5
ETH 4	☐	IEC 61850-9-3:2016	0	128	128	P2P	1	3	1	1	☐	-	-	-

Figure 7.1 PTP Settings Page

Table 7.1 PTP Settings (Sheet 1 of 2)

Setting Name	Values	Default	Description
Enable PTP	Checked/Unchecked	Unchecked	Enables or disables PTP operation for the selected interface.
Profile	Default (UDP), Default (802.3), IEEE C37.238-2011, IEEE C37.238-2017, IEC 61850-9-3:2016	IEEE C37.238-2011	Selects the PTP Profile for the interface. Each profile configures and locks settings based on requirements of the associated standard. The Default profiles use requirements of IEEE 1588-2008 Annex J with UDP (Annex D) Layer 3 or 802.3 (Annex F) Layer 2 transport mechanisms to distribute time. The IEEE C37.238-2011/2017 and IEC 61850-9-3:2016 profiles use the standards of the same name.
Domain	0–255	0	Sets the PTP clock domain for the interface. This is a logical grouping of clocks in a network system. The IEC 61850-9-3:2016 profile allows for a range of 0–255, with a recommended default of 93. The IEEE C37.238-2017 profile allows for a range of 0–127 and 254, with a recommended default of 254. All other profiles allow for a range of 0–127, with a default of 0.
Priority 1	0–255	128	Sets the Priority 1 value for the interface, which is the highest priority value used in the BMCA. Fixed at 128 for the IEEE C37.238-2011 profile.
Priority 2	0–255	128	Sets the Priority 2 value for the interface, which is the penultimate tie breaker value in the BMCA. Fixed at 128 for the IEEE C37.238-2011 profile.
Path Delay Mechanism	E2E, P2P	P2P	Sets the Path Delay Mechanism for the interface. This is used to determine the delay between master and slave clocks. End-to-end (E2E) uses the delay request-response mechanism and peer-to-peer (P2P) uses the peer delay mechanism. Fixed at P2P for the IEEE C37.238-2011/2017 and IEC 61850-9-3:2016 profiles.
Announce Interval	1, 2, 4, 8, 16 seconds	1	Sets how often the interface will send Announce messages while in the Master port state. Fixed at 1 for the IEEE C37.238-2011/2017 and IEC 61850-9-3:2016 profiles.
Announce Timeout	2, 3, 4, 5, 6, 7, 8, 9, 10	2	Sets the number of Announce Intervals that must pass without receipt of an Announce message before the interface changes state from passive to master and begins sending Announce messages. Fixed at 2 for the IEEE C37.238-2011 profile and 3 for the IEEE C37.238-2017 and IEC 61850-9-3:2016 profiles.
Sync Interval	0.5, 1, 2 seconds	1	Sets how often the interface sends Sync messages when in the Master port state. Fixed at 1 for the IEEE C37.238-2011/2017 and IEC 61850-9-3:2016 profiles.
Delay Interval	1, 2, 4, 8, 16, 32 seconds	1	Sets the minimum average interval the interface allows for the reception of Delay_Req/Pdelay_Req messages. Increasing this value lowers network traffic but may make path delay calculations less accurate. Fixed at 1 for IEEE C37.238-2011/2017 and IEC 61850-9-3:2016 profiles.
VLAN Enable	Checked/Unchecked	Unchecked	Enables or disables VLAN tagging of PTP messages for the interface when using the IEEE C37.238-2011/2017 and IEC 61850-9-3:2016 profiles.
VLAN ID	0–4094	0	Sets the VLAN ID of VLAN tagged PTP messages for the interface. For editing, VLAN Enable must be checked.

Table 7.1 PTP Settings (Sheet 2 of 2)

Setting Name	Values	Default	Description
802.1Q Priority	0–7	4	Sets the 802.1Q Priority of VLAN tagged PTP messages for the interface. For editing, VLAN Enable must be checked.
Grandmaster ID	0–65535	5	Sets the Grandmaster ID field within the IEEE C37.238 TLV, which is included with Announce messages when using the IEEE C37.238-2011/2017 profiles. IEEE C37.238-2011 allows for a range of 3–254. IEEE C37.238-2017 allows for a range of 0–65535, with 0 indicating the value is unused.

Profile

The Profile setting in the SEL-2488 defines the mode of operation. PTP can operate either with Layer 2 (802.3) or User Datagram Protocol (UDP) communications protocols. Default (802.3) selects Layer 2, and Default (UDP) selects Layer 3 communication. Selecting either Default profile makes other PTP settings such as Priority, Path Delay Mechanism, etc. available for customization.

IEEE C37.238-2011/2017 define the Power System profiles and IEC/IEEE 61850-9-3:2016 defines the Power Utility Automation profile. These profiles are used for power system and industrial automation applications. Each requires Layer 2 communications and lock most of the remaining PTP settings to a single preset value defined in the associated standard.

Path Delay Mechanism

The Path Delay Mechanism determines the manner in which path delay is calculated to provide an accurate offset at the slave clock. The delay request-response mechanism is the end-to-end (E2E) calculation of the path delay. The peer delay mechanism is the peer-to-peer (P2P) calculation method by which each PTP device determines the delay to its peer and updates PTP Sync messages with its calculated delay. The IEEE C37.238-2011/2017 and IEC/IEEE 61850-9-3:2016 profiles require the use of the P2P path delay calculation method.

PTP Settings With PRP/Port Bonding Enabled

When PRP and/or active-backup port bonding is enabled, the combined physical Ethernet ports are listed as a single PTP configuration as shown in *Figure 7.2*. See *Section 24: Parallel Redundancy Protocol (PRP)* and *Section 25: Active-Backup Port Bonding* for details.

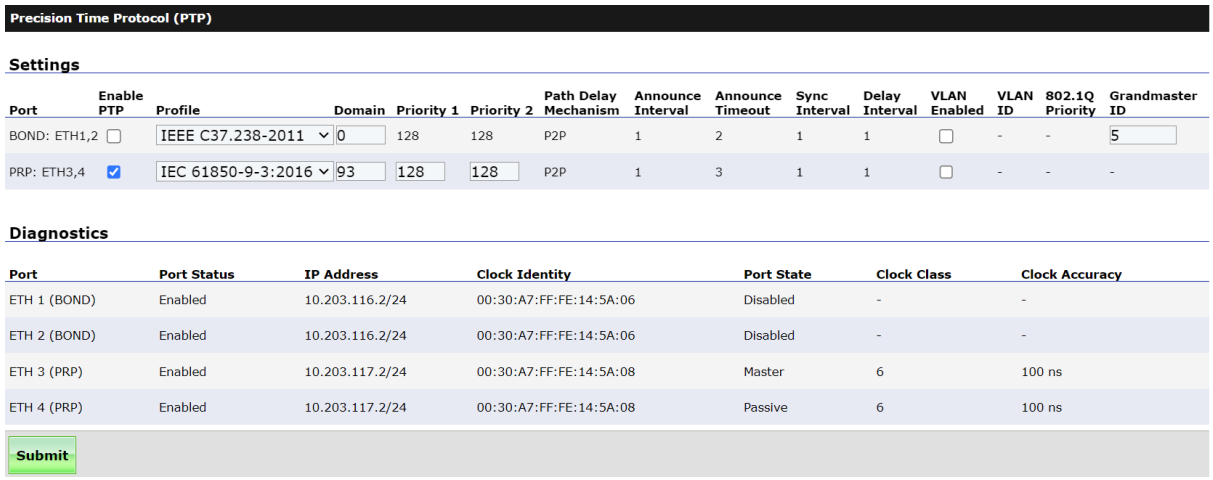


Figure 7.2 PTP Settings Page: One PRP Interface and One Active-Backup Bonded Interface Enabled

When PRP and/or active-backup port bonding is enabled, both of the physical Ethernet ports of the combined interface use the Ethernet MAC address of the lower port number (i.e., ETH 1 for ETH 1 and ETH 2; ETH 3 for ETH 3 and ETH 4). The PTP Clock Identity of a port uses the physical Ethernet port MAC address and adjusts accordingly. However with PTP enabled, each physical Ethernet port retains a PTP Port Number that matches the physical interface (e.g., ETH 1 retains a PTP Port Number of 1, ETH 2 retains 2, etc.). Alternatively, with active-backup port bonding enabled, both of the physical Ethernet ports of the combined interface use the PTP Port Number of the lower port number (i.e., 1 for ETH 1 and ETH 2; 3 for ETH 3 and ETH 4).

Precision Time Protocol

Port	Clock Identity	Port State
ETH 1 (BOND)	00:30:A7:FF:FE:14:5A:06	Disabled
ETH 2 (BOND)	00:30:A7:FF:FE:14:5A:06	Disabled
ETH 3 (PRP)	00:30:A7:FF:FE:14:5A:08	Master
ETH 4 (PRP)	00:30:A7:FF:FE:14:5A:08	Passive

Figure 7.3 Precision Time Protocol Status Widget: One PRP Interface and One Active-Backup Bonded Interface Enabled

PTP Diagnostics

The clock web management interface includes a table detailing basic per-interface diagnostic information regarding the PTP master clock operation in the PTP Settings section. Information such as Clock Identity, Class, and Accuracy is available along with other status indicators.

Diagnostics

Port	Port Status	IP Address	Clock Identity	Port State	Clock Class	Clock Accuracy
ETH 1	Enabled		00:30:A7:FF:FE:0B:E0:01	Master	6	100 ns
ETH 2	Enabled	192.168.12.104/24	00:30:A7:FF:FE:0B:E0:02	Master	6	100 ns
ETH 3	Enabled		00:30:A7:FF:FE:0B:E0:03	Disabled	-	-
ETH 4	Enabled		00:30:A7:FF:FE:0B:E0:04	Disabled	-	-

Figure 7.4 PTP Diagnostics

Port indicates the physical Ethernet port number. When PRP is enabled, the port will have an additional **(PRP)** label.

Port Status reflects the present status of the Ethernet interface. If the Ethernet interface is assigned an Internet Protocol (IP) address, the address is reflected in the IP Address column. See *Section 4: Ethernet Network Interfaces* for additional information on changing these values.

Clock Identity is a fixed value that uniquely identifies a PTP clock. The SEL-2488 assigns each interface an individual Clock Identity.

Port State reflects the current status of the PTP clock for that interface. Options are Disabled, Initializing, Listening, Master, and Passive.

Clock Class reflects the time traceability. A “6” indicates synchronization to a primary reference source and not another clock in the domain. A “7” indicates the clock has lost synchronization to a primary reference source and is operating in holdover mode. A “52” indicates the clock is not synchronized to any primary reference source. For the IEEE C37.238-2017 and IEC/IEEE 61850-9-3:2016 profiles, the Clock Class traceability descriptions

are modified. A “6” retains the original meaning, a “7” indicates holdover with ≤250 ns Clock Accuracy, a “52” indicates holdover with ≤1 µs Clock Accuracy, and a “187” indicates holdover with >1 µs Clock Accuracy.

Clock Accuracy indicates the present accuracy of the PTP clock with reference to UTC.

Front Panel

Table 7.2 PTP LED Status

LED State	Description
Off	PTP disabled on all interfaces
Amber	PTP enabled on any interface and the corresponding network interface not enabled or PTP enabled for UDP communication on any interface and corresponding network interface does not have an IP address configured
Green	At least one Ethernet interface has the PTP service and no remaining interfaces are in a misconfigured (amber) condition

Figure 7.5 PTP Front-Panel LED

Dashboard

The **Precision Time Protocol** section provides a quick reference showing the present status of precision time outputs.

Precision Time Protocol

Port	Clock Identity	Port State
ETH 1 (BOND)	00:30:A7:FF:FE:14:5A:06	Disabled
ETH 2 (BOND)	00:30:A7:FF:FE:14:5A:06	Disabled
ETH 3 (PRP)	00:30:A7:FF:FE:14:5A:08	Master
ETH 4 (PRP)	00:30:A7:FF:FE:14:5A:08	Passive

Figure 7.6 Precision Time Protocol Status

The dashboard replication of the **PTP** LED follows the light patterns defined in *Table 7.2*.

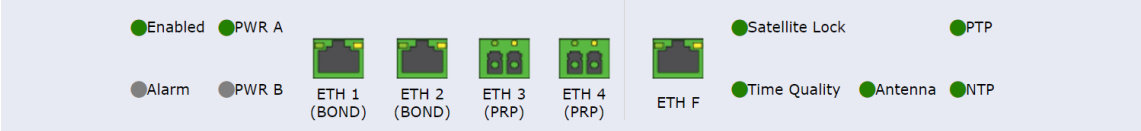
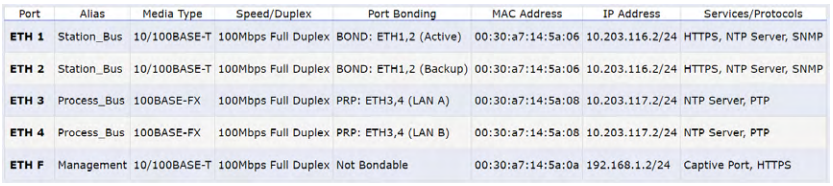


Figure 7.7 PTP LED Status Display on Dashboard

As discussed in *Dashboard on page 4.7*, the table below the Ethernet dashboard indicators will list if PTP is enabled.



Port	Alias	Media Type	Speed/Duplex	Port Bonding	MAC Address	IP Address	Services/Protocols
ETH 1	Station_Bus	10/100BASE-T	100Mbps Full Duplex	BOND: ETH1,2 (Active)	00:30:a7:14:5a:06	10.203.116.2/24	HTTPS, NTP Server, SNMP
ETH 2	Station_Bus	10/100BASE-T	100Mbps Full Duplex	BOND: ETH1,2 (Backup)	00:30:a7:14:5a:06	10.203.116.2/24	HTTPS, NTP Server, SNMP
ETH 3	Process_Bus	100BASE-FX	100Mbps Full Duplex	PRP: ETH3,4 (LAN A)	00:30:a7:14:5a:08	10.203.117.2/24	NTP Server, PTP
ETH 4	Process_Bus	100BASE-FX	100Mbps Full Duplex	PRP: ETH3,4 (LAN B)	00:30:a7:14:5a:08	10.203.117.2/24	NTP Server, PTP
ETH F	Management	10/100BASE-T	100Mbps Full Duplex	Not Bondable	00:30:a7:14:5a:0a	192.168.1.2/24	Captive Port, HTTPS

Figure 7.8 Additional Diagnostic Information for Ethernet Interfaces

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for events associated with PTP. The SEL-2488 replaces message variables in {} with values it logs.

Table 7.3 PTP Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
`Port {0} changes PTP state to Master.`	Notice	None	–
`Port {0} changes PTP state to Passive.`	Notice	None	–
`PTP Settings: changed by {username} at {user_ip}.`	Notice	Minor	Configuration
`PTP Settings Misconfigured. Either PTP is enabled on an interface that is disabled, or PTP is enabled using Default (UDP) on a port that has no IP address`	Notice	Minor	Configuration
`PTP Settings Misconfiguration Repaired`	Notice	Minor	Configuration

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Events classified as None will not trigger the alarm contact.

This page intentionally left blank

Section 8
Network Time Protocol (NTP)

Overview

The SEL-2488 includes Network Time Protocol server functionality. Network Time Protocol (NTP) is an industry standard protocol for time synchronization of Ethernet-based devices. The SEL-2488 supports the following NTP modes of providing time to clients from the server:

- Client-server
- Broadcast
- Multicast

Definitions

Primary NTP Server—An NTP server that gets its time directly from a Coordinated Universal Time (UTC) reference source. Global Navigation Satellite System (GNSS) receivers are recognized as a UTC reference for NTP purposes. The SEL-2488 is an example of a primary NTP server.

Secondary NTP Server—An NTP server that obtains its time from another NTP server (primary or secondary) and serves time to other NTP devices.

NTP Client—A device that requests time from the NTP server.

Stratum—The measurement that defines the number of steps the NTP server is removed from the Coordinated Universal Time (UTC) reference source. NTP servers that are directly connected to a reference source such as the Global Positioning System (GPS) are called primary servers and have a stratum of one (1). A secondary NTP server increments the received stratum by one (1) when publishing its NTP messages; therefore, a secondary NTP server connected to a primary NTP server reports its stratum as two (2). Servers with stratum values greater than 15 are not recognized as valid sources.

NTP Client-Server Mode—A mode in which the client sends a request message to the server and the server responds with a message to the client that includes the time, stratum, and time stamps that allow the client to determine path delays.

NTP Broadcast Mode—A mode in which the server sends out a structured NTP message and the clients use this information as a type of discovery service to determine available NTP servers on the local subnet. Broadcast messages typically are limited to a local subnet and are not routed to other networks. Clients listen for the messages, send several quick client-server requests to determine the path delay, apply this delay to the broadcast

messages, and establish the correct adjusted client time. Clients will listen for all available servers, then determine the best three to use for ongoing time synchronization.

NTP Multicast Mode—A mode similar to the Broadcast mode, but instead of transmitting to a subnet broadcast address, the server transmits a structured NTP message to a multicast Internet Protocol (IP) address to which clients are programmed to listen. There is a time-to-live (TTL) component to the message that determines the number of hops a message can have before the NTP client ignores the message. NTP deviates from normal IP routing in that all enabled interfaces, rather than just the interface with the correct packet delivery route (as defined by route rules), send the multicast message.

Operation

The SEL-2488 is a Stratum 1 NTP server because it is referenced to UTC via Global Navigation Satellite System (GNSS). It provides client synchronization accuracy of 0.5–2 ms (typical) depending on network architecture. The implementation of NTP in the SEL-2488 is based on Internet Engineering Task Force (IETF) RFC-5905 NTP v4. The SEL-2488 transmits NTP on any of the four main network interfaces in Client-Server, Broadcast, and Multicast modes. It does not provide the service on the ETH F port.

NTP is an IP-based protocol that requires Layer 3 Ethernet services (IP address, default gateway, and optional static routes) to be configured and enabled. To enable basic client-server mode on the SEL-2488, enable the service on an interface that has Layer 3 Ethernet services enabled. This sets up the service and allows the device to respond to client requests that the interface receives. See *Section 4: Ethernet Network Interfaces* for information on configuring Ethernet services.

You can enable the NTP Broadcast option on individual interfaces and control the broadcast message interval on a per-interface basis. The basic client-server service for the interface must be enabled before the SEL-2488 can transmit broadcast messages.

You can enable the NTP Multicast option on individual interfaces. The multicast address and multicast message interval are common to all enabled interfaces. NTP sends the multicast packet out all interfaces where both the basic client-server and multicast service are enabled. NTP transmits the present clock reported time quality as part of the protocol. When no other source is present, you can set the SEL-2488 in the Manual Date/Time mode. In this case, NTP will reflect a Stratum 1 primary server for demonstration purposes, with the reference ID field indicating "LOCL". See *Section 19: Date/Time* for details.

Holdover

If the SEL-2488 loses its primary reference (GNSS), it goes into holdover mode and continues to provide time outputs based on its internal reference oscillator. While in holdover mode, NTP messages will reflect the present holdover accuracy.

Settings

This section discusses the settings that customize and affect operation of the Network Time Protocol. Use the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **Network Management > IP Configuration and Time Management > NTP Settings** menu option to configure the SEL-2488 NTP services.

NTP settings include a common group of settings for multicast operation and interface-based settings for enablement and broadcast options. The common settings configure the destination address for NTP multicast packets and the interval of transmission for the multicast message.

NTP Server Service

You must enable the NTP Server service on an interface to allow the SEL-2488 to respond to client requests and before the advanced broadcast and multicast modes can transmit packets. As stated previously, you must first enable the interface and set the IP address for the interface in the **IP Configuration** page before you can enable the NTP service. The NTP Server setting will be disabled if no configured IP address exists on the interface.

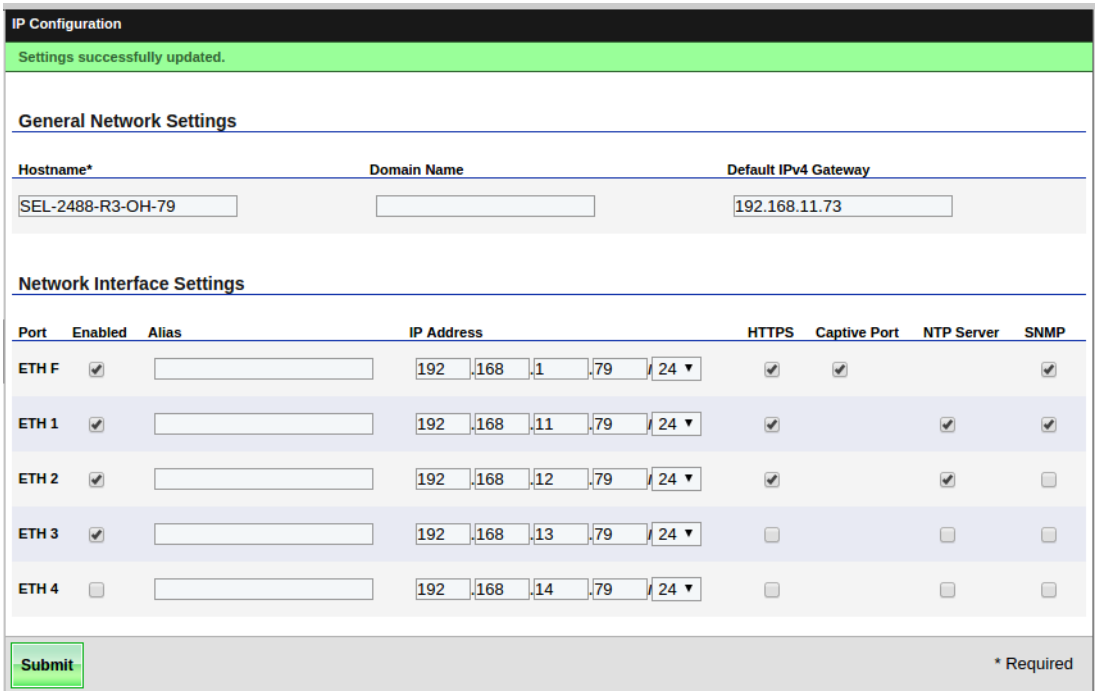


Figure 8.1 IP Configuration Page: NTP Aspect

Table 8.1 ETH 1–4 Network Interface Settings

Setting Name	Values	Default	Description
NTP Server	Checked, Unchecked	Unchecked	Enables or disables operation for the selected interface.

NTP Server Settings

NOTE: If the NTP Server service is enabled and the interface is disabled, the clock will neither respond to NTP requests nor transmit broadcast or multicast packets on that interface.

After you configure the IP address for the interface, you can configure the NTP settings for multicast and broadcast in the **Network Time Protocol (NTP)** page, as shown in *Figure 8.2*.

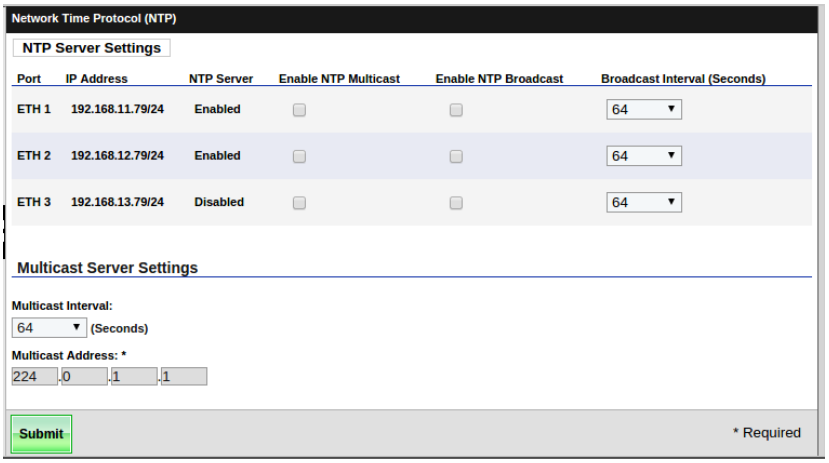


Figure 8.2 NTP Settings Page

You can set each enabled interface individually to transmit NTP broadcast or multicast messages. In addition, on each interface you can set the interval of transmission for NTP broadcast messages when that option is enabled for the interface.

Table 8.2 NTP Multicast/Broadcast Settings

Setting Name	Values	Default	Description
Enable NTP Multicast	Checked, Unchecked	Unchecked	Enables or disables the use of NTP as a time server sending multicast time messages through interface
Enable NTP Broadcast	Checked, Unchecked	Unchecked	Enables or disables the use of NTP as a time server broadcasting time packets to a local network subnet, defined by an interface IP address
Broadcast Interval	16–131072 seconds	64	Sets the interval between the broadcast messages on the interface

Multicast Server Settings

To edit the common multicast settings, you must enable multicast for one of the interfaces.

The multicast address must be in the range of 224.0.0.0/8 or 224.0.0.0 through 239.255.255.255. Many multicast addresses, such as this, are reserved for specific functions, so it is always a good idea to coordinate changes to this address from the default with groups responsible for the network. The address assigned by default is the reserved address for Network Time Protocol.

The multicast interval adjusts the frequency of NTP multicast packet transmission.

Table 8.3 Multicast Server Settings

Setting Name	Values	Default	Description
Multicast Interval	16–131072 seconds	64	Sets the interval when the NTP server sends time to the corresponding multicast address
Multicast Address	Multicast IP addresses	224.0.1.1	Sets the NTP server multicast IP address

NTP Settings With PRP/Port Bonding Enabled

When PRP and/or active-backup port bonding is enabled, the combined physical Ethernet ports are listed as a single NTP configuration as shown in *Figure 8.3*. See *Section 24: Parallel Redundancy Protocol (PRP)* and *Section 25: Active-Backup Port Bonding* for details.

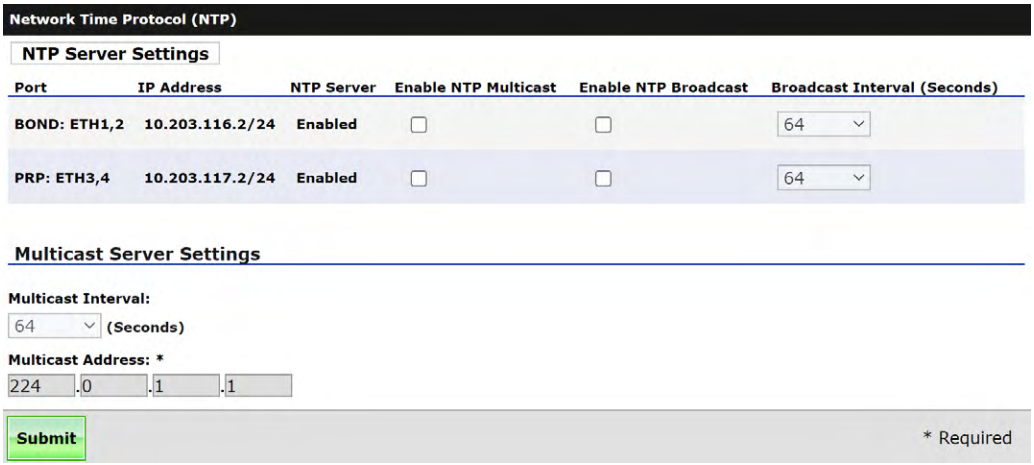


Figure 8.3 NTP Settings Page: One PRP Interface and One Active-Backup Bonded Interface Enabled

Front Panel

The **NTP** LED on the front panel turns on (illuminates green) when at least one Ethernet interface has the NTP service and interface enabled.

Figure 8.4 NTP Front-Panel LED

Dashboard

The dashboard replicates the **NTP** LED status as displayed on the front panel.

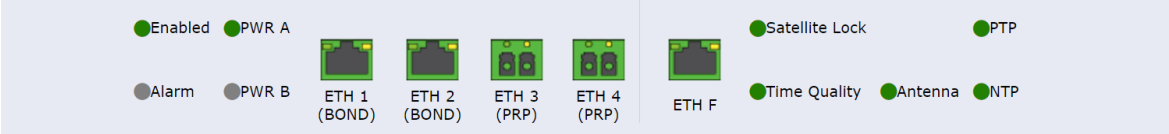


Figure 8.5 NTP Dashboard LED

As discussed in *Dashboard on page 4.7*, the table below the Ethernet dashboard indicators will list if NTP is enabled.

Port	Alias	Media Type	Speed/Duplex	Port Bonding	MAC Address	IP Address	Services/Protocols
ETH 1	Station_Bus	10/100BASE-T	100Mbps Full Duplex	BOND: ETH1,2 (Active)	00:30:a7:14:5a:06	10.203.116.2/24	HTTPS, NTP Server, SNMP
ETH 2	Station_Bus	10/100BASE-T	100Mbps Full Duplex	BOND: ETH1,2 (Backup)	00:30:a7:14:5a:06	10.203.116.2/24	HTTPS, NTP Server, SNMP
ETH 3	Process_Bus	100BASE-FX	100Mbps Full Duplex	PRP: ETH3,4 (LAN A)	00:30:a7:14:5a:08	10.203.117.2/24	NTP Server, PTP
ETH 4	Process_Bus	100BASE-FX	100Mbps Full Duplex	PRP: ETH3,4 (LAN B)	00:30:a7:14:5a:08	10.203.117.2/24	NTP Server, PTP
ETH F	Management	10/100BASE-T	100Mbps Full Duplex	Not Bondable	00:30:a7:14:5a:0a	192.168.1.2/24	Captive Port, HTTPS

Figure 8.6 Additional Diagnostics Information for Ethernet Interfaces

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for events associated with NTP. The SEL-2488 replaces message variables in {} with values it logs.

Table 8.4 NTP Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
`NTP Server: Disabled on port {0}, {1} by {username} at {user_ip}.`	Notice	Minor	Configuration
`NTP Server: Enabled on port {0}, {1} by {username} at {user_ip}.`	Notice	Minor	Configuration
`NTP Server Settings: Changed by {username} at {user_ip}.`	Notice	Minor	Configuration[a]

[a] Caused by Broadcast, Multicast, or Intervals settings changes.

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Section 9
Timer Contact

Overview

The SEL-2488 includes a clock-controlled, Form A, high-speed, solid-state contact output. You can set this output for a single contact closure or a repeating contact closure of configurable duration and period.

Definitions

According to standard classification, we define a Form A contact as one that is normally open (NO) when the contact is in a de-energized state. The contact closes when energized.

Pulse duration is the time that the contact is in the energized (closed) state.

Pulse period is the time from the start of the energized state of one activation to the start of the energized state of the next activation. This only applies to repeating pulse configurations.

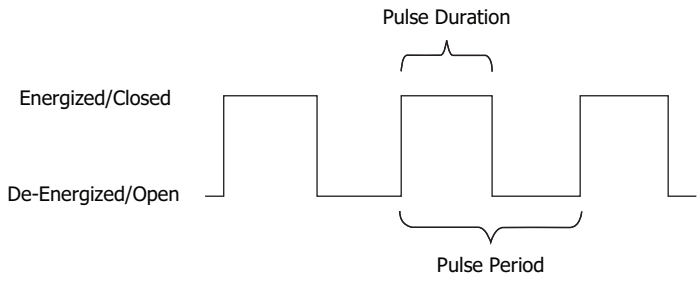


Figure 9.1 Pulse Duration and Period for Form A Contact

Operation

The timer contact requires an external power source to provide an output pulse to an end device.

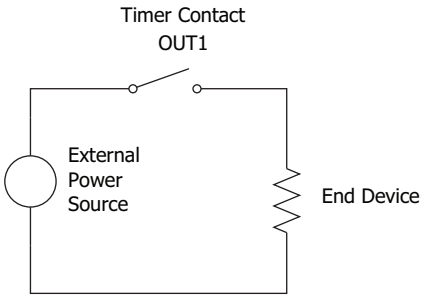


Figure 9.2 Timer Contact Connection Diagram

NOTE: The timer contact (OUT1) requires a minimum external power source potential of 12 volts for correct contact operation.

The **Timer Contact** settings page has several configuration options that control the contact operation. There is a master enable control (Enable Timer Contact) that allows you to enable and configure the timer contact operation. Disabling the timer contact via settings while a contact operation is in progress can interrupt the operation without changing the duration, period, or start modes. When you re-enable the control, the same repeating operation will resume.

Pulse Repeat Mode defines whether the contact only operates once or if the operation repeats on the schedule defined in the Pulse Period setting. Single Pulse generates one contact closure for the pulse duration when the start time (local) defined by Pulse Start Mode is reached. Repeating Pulses generates a contact closure for the Pulse Duration at the occurrence of Pulse Period. You can only change Pulse Period when you set the Pulse Repeat Mode to Repeating Pulses.

NOTE: To resubmit the same settings, for example, to resubmit a single pulse, clear **Enable Timer Contact** and submit, then check **Enable Timer Contact** and submit again.

Pulse Start Mode defines when the contact operation starts. You can set it to start immediately (**Now**) or at a date/time in the future or past (**Scheduled**). The range of the start date/time is 2000-01-01 00:00:00.0 through 2035-12-31 23:59:59.9. The Now starting point is the time when you apply the setting to the device. You can change the Start Date and Time fields when you select **Scheduled**.

Repeating Pulse Timing

Repeating contact timing provides a method to generate a custom repeating pulse sequence. For example, 1 ppm (pulse per minute) or 1 pph (pulse per hour).

The start of pulse timing for all timer contact operations is based on the original start date/time of the initial contact closure. This information is the reference that all future contact closures for that sequence will follow. Once you have established the reference point, the SEL-2488 changes to a period-based trigger for the start of pulse timing. Changes to the local time (DST, leap second, etc.) will have no effect on the repeating pulse. Therefore, after a DST or leap-second event, the start of pulse may appear to have changed relative to the local time the SEL-2488 presents.

Settings

This section discusses the settings that customize and affect operation of the timer contact. Configure the SEL-2488 Timer Contact via the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **System > Contact I/O** settings menu option and selecting the **Timer Contact** tab.

Figure 9.3 shows a view of the timer contact settings.

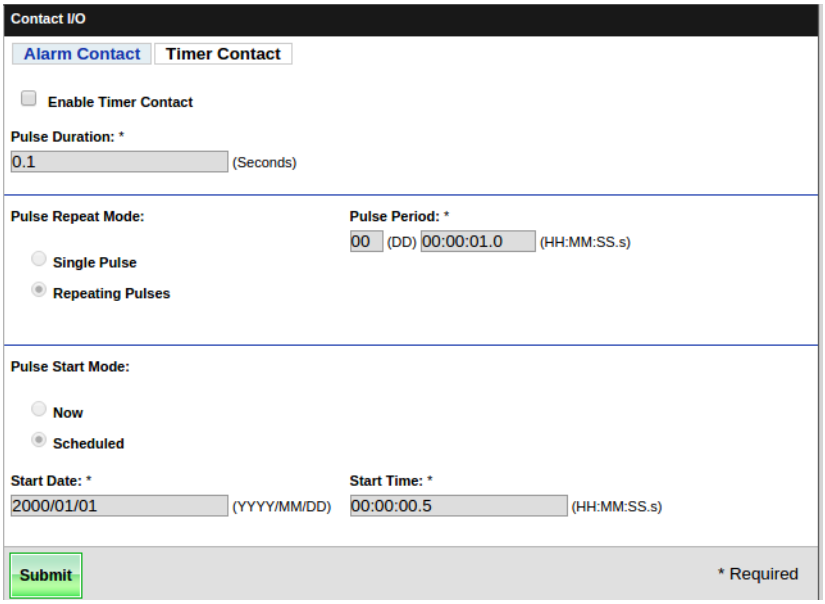


Figure 9.3 Timer Contact Settings Tab

The setting ranges, options, and default values are shown in *Table 9.1*.

Table 9.1 Timer Contact Settings

Setting Name	Values	Default	Description
Enable Timer Contact	Checked, Unchecked	Unchecked	Enables or disables the timer contact for use
Pulse Duration	0.01–3600 seconds	0.5	Sets the time during which the contact remains closed when activated
Pulse Repeat Mode	Single Pulse, Repeating Pulses	Single Pulse	Sets whether the contact keeps repeating the operation or occurs only once
Pulse Period	00–99 (DD), 0.1–23:59:59.9 (HH:MM:SS.s)	00 (DD) 00:00:01.0 (HH:MM:SS.s)	Sets the interval between pulses
Pulse Start Mode	Now, Scheduled	Now	Sets the time when the contact will start to pulse
Start Date	01/01/2000–12/31/2035	01/01/2000	Sets the start date to start the pulse operation
Start Time	00:00:00.0–23:59:59.9	00:00:00.0	Sets the start time to start the pulse operation

Front Panel

The **OUT1** LED on the front panel turns on (illuminates green) when the timer contact is in an energized (closed) state.

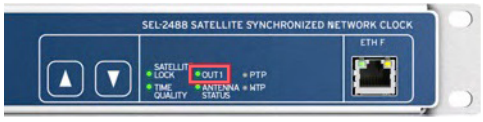


Figure 9.4 OUT1 LED

Dashboard

The **Time Output** section of the dashboard provides a quick reference regarding the status of the timer contact. Output OUT1 displays ENABLED when it is enabled and DISABLED when the timer contact is disabled.

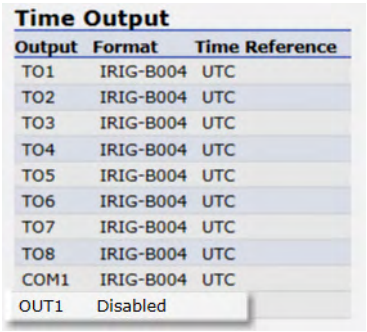


Figure 9.5 Time Output Dashboard Status Widget—OUT1

Alerts/Notifications

The SEL-2488 provides the following alert or notification for the event associated with the timer contact. The SEL-2488 replaces message variables in {} with values it logs.

Table 9.2 Timer Contact Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
Timer Contact Settings: Changed by {username} at {user_ip}	Notice	Minor	Configuration

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Section 10

Local User Management

Overview

Local accounts are the engineering access accounts that reside on SEL products. SEL has historically used global accounts such as Level 1 (ACC) and Level 2 (2AC) access levels and a password associated with each to control access to SEL devices. With global accounts, every user has the same login credentials (username and password), which weakens the security of the system. To strengthen authentication, authorization, and accountability, this SEL product uses a user-based account structure.

Logging in With SEL User-Based Accounts

Upon connection to the SEL-2488, a user will see the device usage policy and a login prompt. The login prompt includes fields for entering a username and the password associated with that username. To log in, the user must enter a valid username and the appropriate password. Usernames are case insensitive and unique to each individual with authority to access the device. Users who enter valid usernames and matching passwords will have access to the device.

If the SEL-2488 determines a username or password to be invalid, then it rejects the access attempt and provides an alert to the user. This alert will inform the user that the login credentials were incorrect. After three failed login attempts within one minute, the SEL-2488 will disallow access attempts with the locked username for 30 seconds. Additionally, this device will pulse the alarm contact for one second to provide an alert to the control center that a failed login attempt has occurred. These security features are designed to prevent and slow down password-guessing attacks. Login failure can happen for three reasons: the username was invalid, the password was incorrect, or the user's account is disabled. Please check the spelling of the username and password if an access attempt fails. If you are certain that you entered the username and password correctly, please contact your system administrator to verify that your account has not been disabled.

Benefits of User-Based Accounts

User-based accounts allow for a stronger security posture than global accounts. One of the drawbacks of global accounts is that revocation of an individual's privileges can result in either everyone who uses that account being temporarily without access or an unauthorized individual having secret

knowledge that the individual can use or sell for malicious purposes. User-based accounts correct this problem with the ability to disable or remove an individual account without affecting access for anyone else.

Similarly, when password changes are necessary, either because of a compromised system, routine maintenance, or regulatory requirements, users will not need to remember several new and different global passwords. They will only need to remember their own personal password changes. This increases security by reducing the need to write passwords down and by reducing the chance that an unauthorized individual might obtain an active password.

Three key parts of strong access control are authentication, authorization, and accountability. Authentication is the process of verifying user identity. This is very difficult to do reliably with global accounts because of the nature of shared passwords. User-based accounts allow for the reliable authentication of individual users of a system. This creates more trust that those who access the system really are whom they claim.

Authorization is the process of granting privileges to users of a system. You can perform authorization with global accounts when the accounts are organized into access roles, such as with ACC and 2AC. However, unless you have a large number of roles (and, therefore, a large number of shared passwords), it is difficult to assign privileges granularly to global accounts. You can use user-based accounts to assign specific privileges to users of a system.

Accountability is the idea that individual users can be held responsible for their actions on a system. The lack of authentication with global accounts creates too much opportunity to cast doubt on the activities of a user, making accountability difficult to enforce. The ability to clearly authenticate a user to the individual level allows the assignment of all actions to specific users. Accountability is very important to event tracking and forensic investigations.

Administration of User-Based Accounts

This product comes unconfigured from the factory. This means that there are no user accounts installed. To access the product, you must create an initial account through the **Commissioning** page. This account has authorization to add, remove, enable, and disable system users. Only the individual who creates this account should have knowledge of this account password.

It is possible to create other accounts that can manage users. Only those users with a need to manage user accounts should be a member of the User Manager or Administrator group.

The SEL-2488 stores user accounts in nonvolatile memory. This allows the device to maintain account status through power cycles and other unexpected events.

The SEL-2488 has user-based access control to improve authentication, authorization, and accountability. Individuals responsible for configuring, monitoring, or maintaining the device can have their own unique user accounts. User-based access controls are organized to answer “Who did what and when?” and allow flexibility for detailed auditing. This structure eases the burden of password management for operators by only requiring users to remember their own personal passwords. This eliminates the need for each operator to remember a new password every time an employee leaves or no longer needs access.

Roles

Device permissions are organized into roles, and access is granted through role-based access controls (RBACs). The device has four roles: Administrator, Engineer, User Manager, and Monitor. User account privileges are based on the group (i.e., role) in which the user is a member. The following list provides a brief overview of each role:

- Administrator: Users have full access to the device.
- Engineer: Users have access to most device settings and information, but cannot access user account management.
- User Manager: Users have access to user account management. Access to other settings is restricted.
- Monitor: Users have read-only access to device settings.

Passphrases

Passphrases provide a user the ability to create strong and easy-to-remember passwords that protect access to a system. A strong passphrase includes many different characters from many different character sets. Longer passphrases provide greater security than shorter passphrases. SEL user-based accounts support complex passphrases that must include at least one character from each of the following character sets:

- Uppercase letters
- Lowercase letters
- Digits
- Special characters

Additionally, complex passphrases must be at least eight characters in length. Spaces are allowed in passphrases. Sample passphrases include the following:

- Strong: W3b$ter!
- Stronger (and easier to remember): A phras3 is 3v3n Str0ng3r!

Users with User Management access (Administrator, User Manager) can set or change passphrases for any user of the system. Users without administrative access can only change their own passphrases. For protection of your account, the SEL-2488 never displays, transmits, or stores a passphrase in plaintext.

Settings

This section discusses the settings that customize and affect the local user accounts on the device. Configure the SEL-2488 local user accounts via the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **Accounts > Local Users** menu option.

The User Management section contains three pages: **List Users**, **Add New User**, and **Change Your Password**. If the logged-in user lacks user management access, only the **Change Your Password** page will be visible.

Access to **Local Users** pages is restricted to accounts with Administrator or User Manager role assignment. The lone exception is the **Change Your Password** page, which is available to all local user accounts.

Entry into this section results in display of the **List Users** page. This page shows the list of users that have been created on the device and status regarding the user accounts. You can edit or delete existing accounts by selecting the edit or delete buttons associated with the account.

List Users

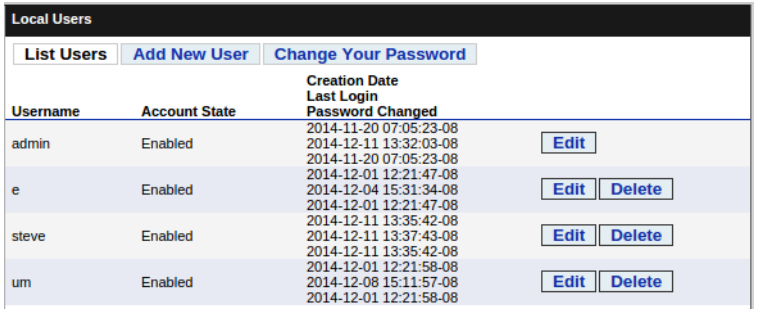


Figure 10.1 List Users Management Tab

The SEL-2488 requires that at least one Administrator-level account be available and enabled at all times. If there is only one Administrator-level account on the device, there will be no associated **Delete** button on the record. While you can disable the account you used for logging into the device (you will be immediately logged off the device after you submit the setting), you cannot delete the account you used to log in.

Edit User

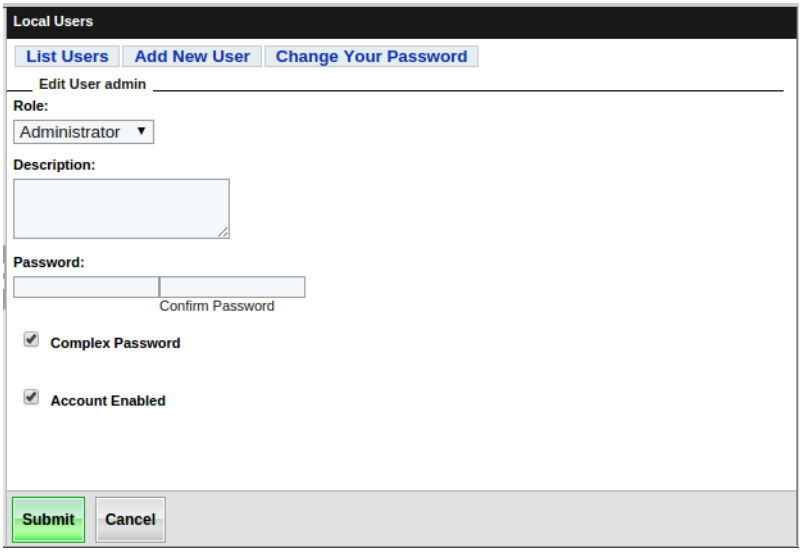


Figure 10.2 Edit User Page

The **Edit User** page is similar to the **Add New User** page, except that the user is already defined and this definition cannot be changed. The remainder of the settings follow the same guidelines as those in *Table 10.1*.

Delete User

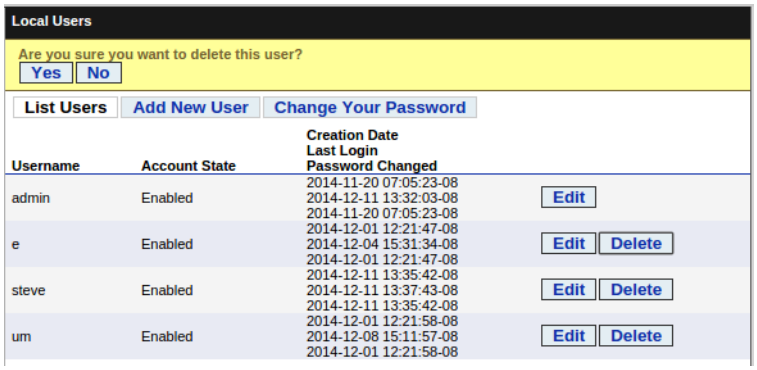


Figure 10.3 Delete User Dialog

Pressing the **Delete** button associated with a user account causes the display of a dialog box (*Figure 10.3*) that confirms deletion of the user.

Add New User

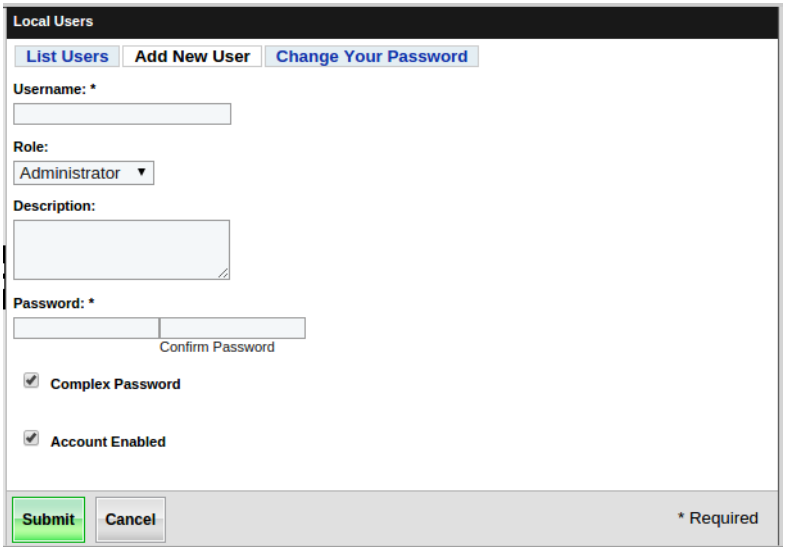


Figure 10.4 Add New User Tab

Change Password

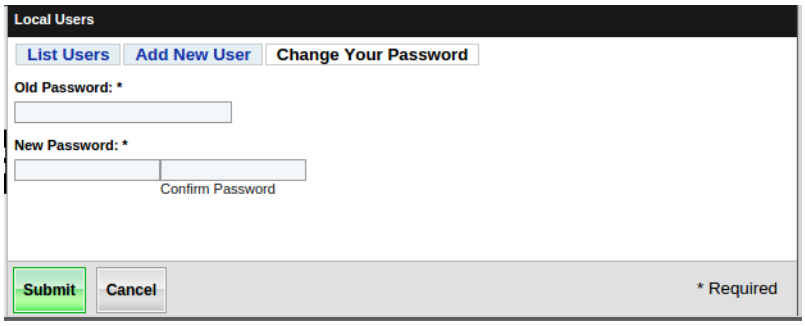


Figure 10.5 Change Your Password Tab

The **Change Your Password** page allows the user to change the password on the local user account that is accessing the SEL-2488. You cannot use this page to change passwords on centrally managed Lightweight Directory

Access Protocol (LDAP) accounts. Password rules for complexity apply to the new password if the **Complex Password** check box is selected for the account.

This page is the only page in the **Local Users** menu option that is available to all users. Should a user without User Management privileges select the **Local Users** menu option, the page in *Figure 10.6* displays. Select **Change Your Password** to start the process.

Figure 10.6 Local User Page for Non-Privileged Account

Table 10.1 User Manager Settings

Setting Name	Values	Default	Description
Username	Printable ASCII characters (as many as 63 characters)		Name that user will use to access device. Name is not case sensitive and will be displayed as lowercase.
Role	Administrator, Engineer, User, Manager, Monitor	Administrator	Permission that will be granted to user (see *Roles on page 10.3*).
Description	UTF-8 characters (as many as 4096 characters)		Description of account.
Password/Confirm Password	Printable ASCII characters (as many as 72 characters)		Password for user account. Must be entered in both **Password** and **Confirm Password** fields.
Complex Password	Checked/Unchecked	Checked	Enforces use of complex password rules (see *Pass-phrases on page 10.3*).
Account Enabled	Checked/Unchecked	Checked	Enables or disables the user account.

The **Password** and **Confirm Password** fields are data entry points only; these fields do not display the present password. When you enter values in each of these fields, the field represents the characters you enter as bullet placeholders that disappear when you submit the form.

Front Panel

The front panel does not display any local user management information.

Dashboard Indications

While the dashboard provides no indications regarding the role of the current user, the webpage does display the logged-in user on the right side of the title bar.

Figure 10.7 Username on Dashboard

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for events associated with user management. The SEL-2488 replaces message variables in { } with values it logs.

Table 10.2 Local User Management Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
Login to {interface}: failed from {user_ip}	Notice	Minor	Authentication
Login to {interface}: successful by {username} at {user_ip}	Notice	Minor	Authentication
Logout {interface}: {username} at {user_ip}	Notice	Minor	Authentication
User {0}: attributes changed by {username} at {user_ip}	Notice	Minor	Configuration
User {0}: created by {username} at {user_ip}	Warning	Minor	Configuration
User {0}: deleted by {username} at {user_ip}	Warning	Minor	Configuration
User {0}: disabled by {username} at {user_ip}	Notice	Minor	Configuration
User {0}: enabled by {username} at {user_ip}	Notice	Minor	Configuration
User {0}: password set by {username} at {user_ip}	Warning	Minor	Configuration
User account {0} locked out due to consecutive failed login attempts	Warning	Minor	Authentication
User account {0} timeout	Warning	Minor	Authentication

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

This page intentionally left blank

Section 11

Centralized User Management With LDAP

Overview

Many information technology departments use Lightweight Directory Access Protocol (LDAP) to manage user authorization and device access on their corporate networks.

The SEL LDAP client within the SEL-2488 provides a mechanism for centralized user management. With LDAP, users are managed on a central server. When a user without a local user account requests device access, the SEL-2488 consults the central directory to verify that the user has authorization to access the SEL-2488 (see *Figure 11.1*).

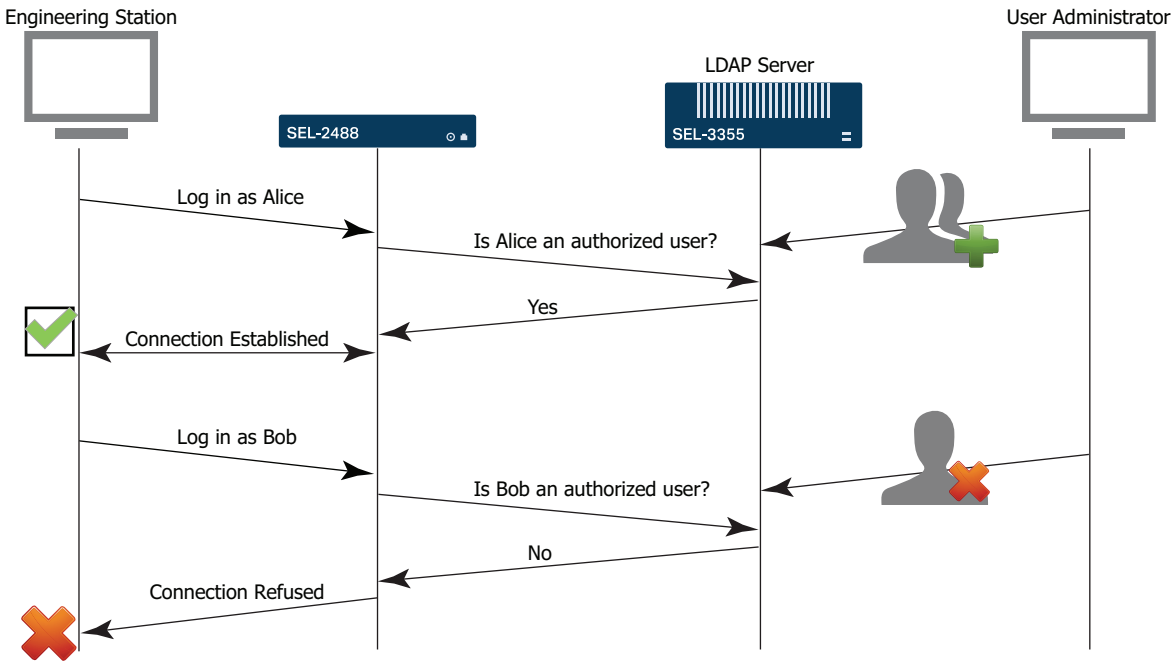


Figure 11.1 LDAP Login Process

The SEL LDAP client allows the SEL-2488 to bind with existing centralized account directories, such as the Microsoft Active Directory directory service, for user authentication and authorization. The LDAP client implementation from SEL uses the StartTLS method to secure LDAP data from the device to the centralized account server. See *Figure 11.2* for information about the LDAP interaction between the SEL LDAP client and the centralized server.

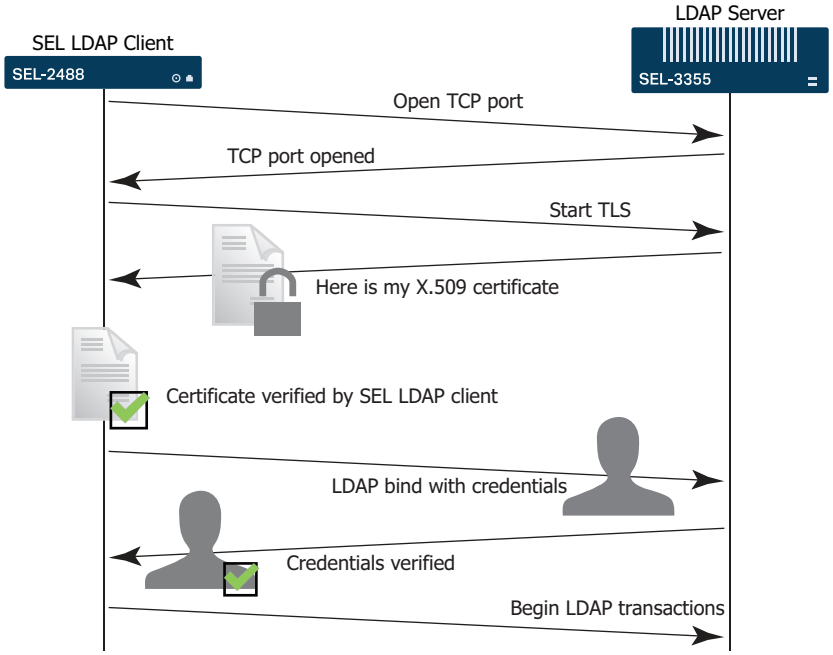


Figure 11.2 LDAP Transaction

Supported LDAP Servers

Testing has verified that the SEL LDAP client binds with the following LDAP servers in supported configurations:

- Active Directory Domain Services on Windows Server 2008 Server Standard/Enterprise
- CentOS Directory Server 8.1 on CentOS 5.5–5.6

NOTE: This SEL LDAP client is incompatible with LDAP deployments that permit commas in usernames.

SEL does not guarantee compatibility of the SEL LDAP client with all possible LDAP server architectures and implementations. Commissioning and configuration of an LDAP server typically requires advanced knowledge of certificate authority hierarchies and centralized user group configurations. It is important that LDAP administrators within an organization be involved during design and implementation to ensure compatibility of device settings with the specific trust management infrastructure of the organization.

Settings

This section discusses the settings that customize and affect the operation of the SEL LDAP client. Use the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **Accounts > LDAP** menu option to configure the SEL-2488 LDAP client operation.

Prior to LDAP client configuration on the device, you must configure Hosts and X.509 settings with the appropriate LDAP information.

Hosts

The ability of the device to contact the LDAP server for an organization depends upon the device first having the server name and Internet Protocol (IP) address. See *Section 13: Hostname Resolution* to set up server name-to-IP address associations.

X.509

LDAP requires X.509 authentication before it can create binds (authenticated connections) between the server and client. This ensures that attackers cannot masquerade as the authentication server to gain unauthorized access. The device requires local storage of the root certificate of the certificate chain for the LDAP server. LDAP administrators for the organization can provide this certificate. See *Section 12: X.509 Certificate Management* for installation of X.509 certificates.

Configuration Summary

Figure 11.3 details the present configuration of the SEL LDAP client.

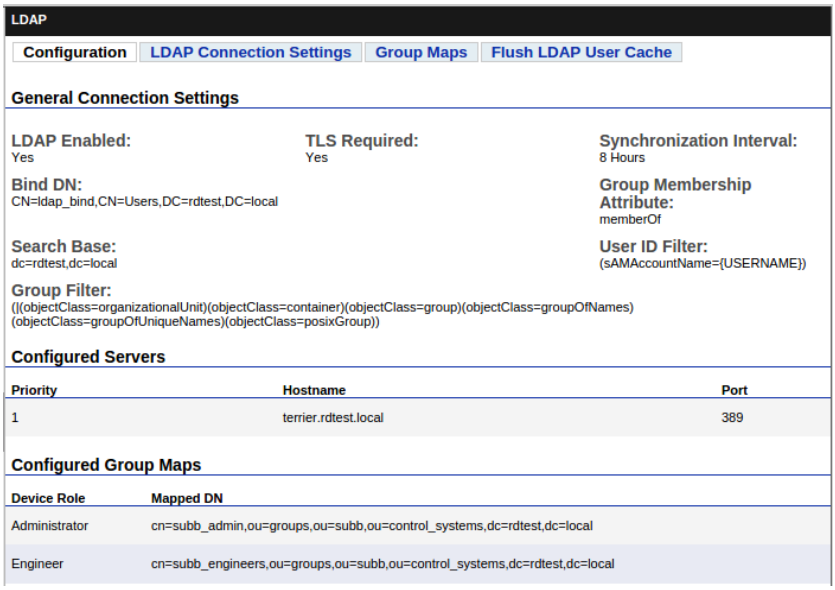


Figure 11.3 LDAP Configuration Summary Tab

LDAP Connection Settings

Figure 11.4 shows the LDAP Connection Settings form and all options for communicating with LDAP servers for the organization. To simplify configuration for LDAP administrators, *Appendix H: Lightweight Directory Access Protocol* contains a form with the information necessary to populate all LDAP client fields.

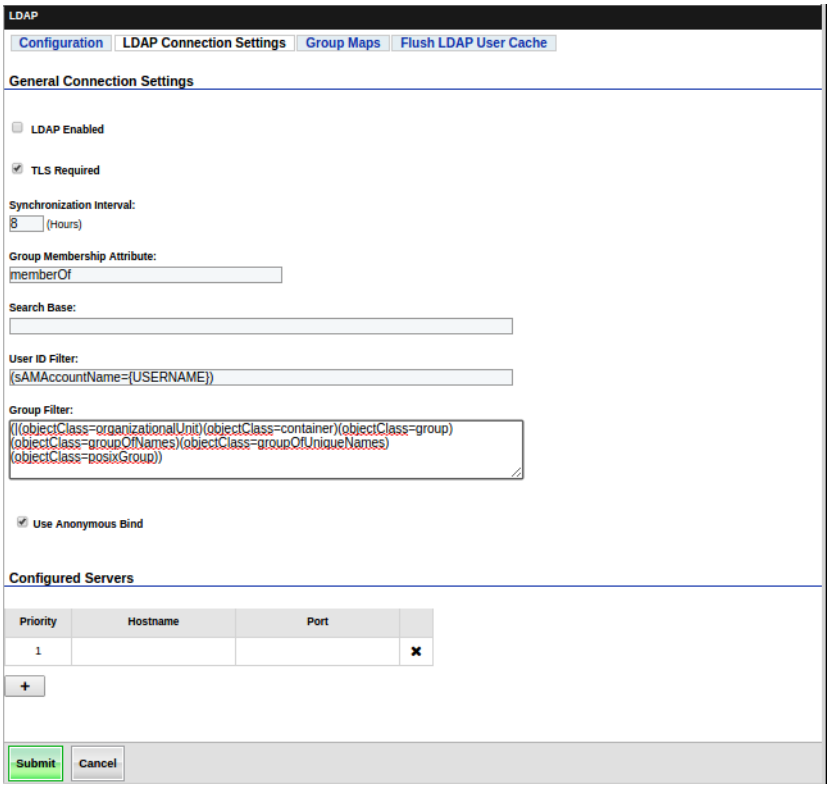


Figure 11.4 LDAP Connection Settings Tab

Table 11.1 LDAP Connection Settings (Sheet 1 of 2)

Setting Name	Values	Default	Description
LDAP Enabled	Checked, Unchecked	Unchecked	Administratively enables or disables the LDAP client.
TLS Required	Checked, Unchecked	Checked	Determines whether a transport layer security (TLS) session protects the connection to the LDAP server.
Synchronization Interval	1–24 hours	8	Specifies the number of hours to locally cache user credentials from the LDAP server. A value of 0 forces resynchronization each login.
Group Member-ship Attribute	0–32 characters	memberOf	The LDAP attribute name for attributes, on an LDAP entry, which have values of distinguished names (DNs) mapping to parent groups of the entry.
Search Base	0–4096 characters		The DN from where LDAP searches begin. Example: dc=rdtest,dc=local
User ID Filter	0–4096 characters	(sAMAccountName={USERNAME})	An LDAP filter the SEL-2488 uses to map a user login name to the LDAP directory DN for that user. The login name for the user replaces the {USERNAME} place holder.
Group Filter	0–4096 characters	(|(objectClass=organizationalUnit) (objectClass=container) (objectClass=group) (objectClass=groupOfNames) (objectClass=groupOfUniqueNames) (objectClass=posixGroup))	An LDAP filter the SEL-2488 uses to search for groups.

Table 11.1 LDAP Connection Settings (Sheet 2 of 2)

Setting Name	Values	Default	Description
Use Anonymous Bind	Checked, Unchecked	Checked	Enabling this setting causes the SEL-2488 to use Anonymous Bind to access the LDAP directory. When this setting is unchecked, the SEL-2488 uses the Bind service account and password.
Bind DN	0–4096 characters		The DN of a service account with authorization to search the LDAP directory.
Bind Password/ Confirm Password	0–128 characters		The service account password for the BIND_DN account.
Hostname	1–255		The hostname of the LDAP server. This name must match the entry in Hostname Resolution.
Port	1–65535	389	The port of the LDAP process on the LDAP server.

Check the **LDAP Enabled** setting to ensure that centrally managed accounts are available to the SEL-2488 for logins. When LDAP is enabled, if the credentials the user enters are not in the locally configured accounts on the SEL-2488, it uses LDAP to consult the enterprise directory in an attempt to authenticate the user. If LDAP authentication is successful, the directory service supplies user attributes that indicate the privilege level of the user upon login to this device.

The **TLS Required** setting determines whether a TLS session protects the connection to the LDAP server. Using TLS requires that the LDAP server receive a suitable X.509 server certificate and that the SEL-2488 import a suitable Certificate Authority (CA) or server certificate.

Use the **Synchronization Interval** setting to reduce overhead associated with pulling account information from an LDAP server. The device caches the credentials and privileges of centralized users locally for a configured time. Set the synchronization interval from 0 to 24 hours. If the synchronization interval value is 0, then the device resynchronizes on every login. The synchronization interval expedites the login process. The SEL-2488 continues to verify the authenticity of users against the central directory even if their privilege information is cached locally.

The SEL-2488 uses **Group Membership Attribute**, **Search Base**, **User ID Filter**, and **Group Filter** settings to construct queries to the LDAP server for the purpose of locating a user and verifying credentials for that user. Be careful to enter the exact form and content of these items as you receive them from the LDAP administrator. It is best to use the form in *Appendix H: Lightweight Directory Access Protocol* to collect this information.

Consider **Search Base** to be the root directory from which to begin the user search. Form this by listing all components of the search base, each component separated by a comma, from the most specific component to the broadest component. In *Figure 11.4*, the search base configuration is “dc=rdtest,dc=local.” In this search base, dc refers to the domain component. We later combine the domain components with “.” to create the search domain. In this case, the search domain is rdtest.local. We can interpret this search base to mean “search the directory residing on an LDAP server in the rdtest.local domain.”

NOTE: The broader your search base, the more user/groups may be able to access the device. Broader search bases can take significantly more time to search than search bases that use more specific organizational units or groups.

One other common component of LDAP queries is CN, which stands for "common name." This is a name that refers to a specific object that may or may not be unique. Examples of CNs are groups and usernames.

The User ID and Group Member attributes are the LDAP labels that identify usernames and groups for system users. Incorrect entry of these causes an inability of the device to determine which LDAP fields to search for usernames or privileges. Configure the User ID similar to **(sAMAccountName={USERNAME})** or **(uid={USERNAME})**. In these examples, "sAMAccountName" or "uid" is the name of the attribute on the directory server that identifies the ownership of a user account. The {USERNAME} portion of the User ID is the variable that holds the username of the person attempting to log in to the device. For example, if the User ID were configured as **(sAMAccountName={USERNAME})**, and a person with the username **jsmith** were to attempt to log in to the device, the device would search the LDAP directory for an entry with an sAMAccountName attribute that contained a value of "jsmith". This field is extendable, so it can search for entries matching multiple criteria. For example, the search field **(&(sAMAccountName={USERNAME}) (memberOf=cn=activeusers, dc=your,dc=domain))** would only allow access to users who have valid usernames and who are members of the activeusers group of your domain.

The **Use Anonymous Bind** setting determines how the SEL LDAP client accesses the LDAP server. The LDAP client supports both authenticated and anonymous binds to the LDAP servers. Authenticated binds use a service account to access the LDAP server. In the event of service account revocation or password expiration, the LDAP client will be unable to access the LDAP server, and centralized users will be unable to access the device. Anonymous binds forgo the use of service accounts. Learn from the LDAP administrator which method the organization prefers.

To use service accounts for authenticated binds, clear **Use Anonymous Bind**. Enter the service account username in the **Bind DN** field, and enter the service account password in the **Bind DN Password** fields.

The **Bind Password** and **Confirm Password** fields are data entry points only; they do not display the present password. Upon your entry of values in these fields, the SEL-2488 represents each value with bullet placeholders that disappear when you submit the form.

LDAP Servers

The **Configured Servers** section (see *Figure 11.5*) lists the LDAP servers that the SEL LDAP client uses to authenticate logins.

Identify LDAP servers by their hostname and port numbers. Unless the LDAP administrator specifies a different port number, use Port 389. Use the form in *Appendix H: Lightweight Directory Access Protocol* to obtain information from the LDAP administrators. Enter the hostname and port number of the primary LDAP server. The hostname must match the hostname entry in Hostname Resolution and the Common Name entry in the LDAP server X.509 certificate.

To improve availability in the event the primary LDAP server becomes inaccessible, the SEL LDAP client supports access to a secondary LDAP server. To add a secondary LDAP server, select the plus (+) sign below the Configured Servers table. This adds a new row to the table. Enter the hostname and port of the secondary LDAP server, confirm that the hostname has a matching entry in Hostname Resolution, and submit your changes.

To remove an LDAP server entry, select the “X” associated with the row and submit the change.

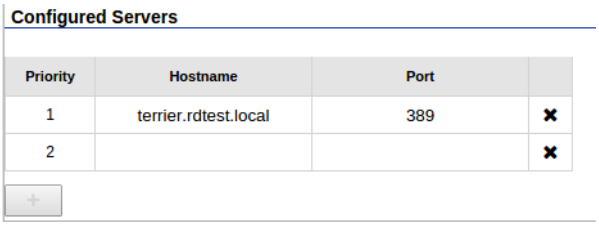


Figure 11.5 Adding an LDAP Server

Group Maps

The device has specific device roles that can be mapped to LDAP group memberships on the **Group Maps** tab. The view shown in *Figure 11.6* has a single group defined for administrators.

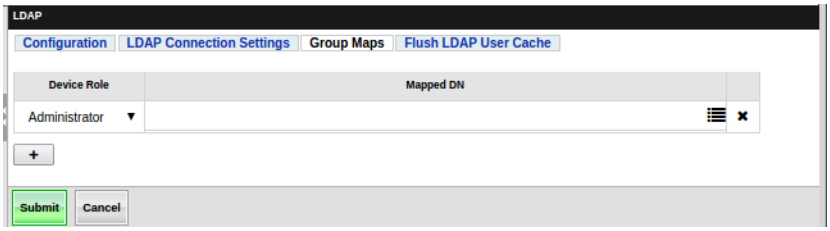


Figure 11.6 LDAP Group Maps Tab

Table 11.2 LDAP Client Settings

Setting Name	Values	Default	Description
Device Role	Administrator, Engineer, User Manager, Monitor	Administrator	Local device role
Mapped DN	0–4096 characters		LDAP group to be mapped to the local device role

The **Device Role** is a selection from the previous list in *Table 11.2*. This setting defaults to Administrator for an empty row.

You can either enter the **Mapped DN** field directly or, preferably, select it from the list box on the right side of the row. Selecting from the list confirms that the LDAP server can be reached, credentials are established, and the entry has no typos or missing commas, etc. Submit your changes.

Select the plus sign (+) at the end of the table to configure a new group mapping in a new row of the table. *Figure 11.7* shows the opening of a new table row.

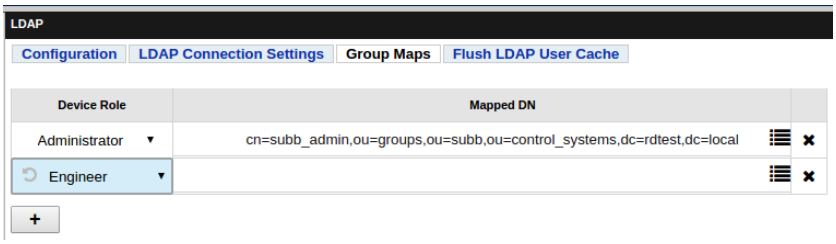


Figure 11.7 LDAP Adding a New Role

To expand the tree of groups for a row of the table, select the list icon at the right end of the **Mapped DN** field in the table. Select the icon again to close the tree of groups. *Figure 11.8* shows the tree of possible groups that appears after you select the list icon.

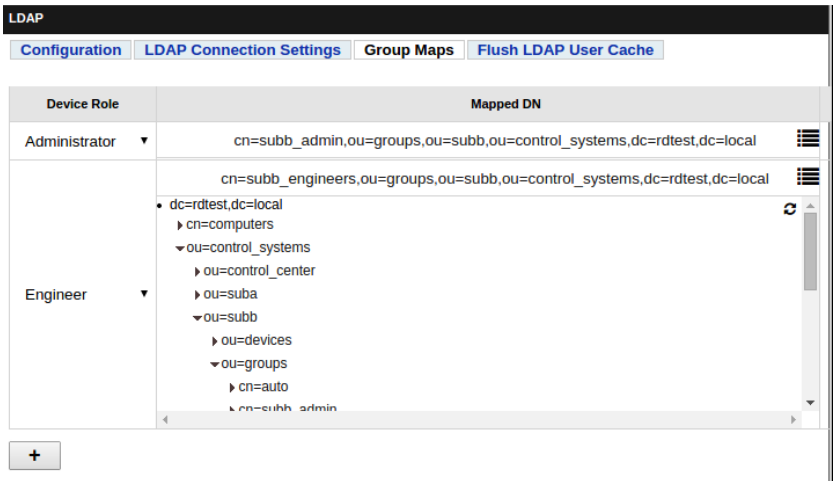


Figure 11.8 LDAP Selecting a Group From the Tree Display

If you cannot locate an appropriate group, the LDAP administrator may need to create new groups and assign members appropriate for those mappings. Use the form in *Appendix H: Lightweight Directory Access Protocol* and work with the LDAP administrator to determine group mappings.

To remove a group map entry, select the "X" associated with the row and submit changes.

Flush LDAP User Cache

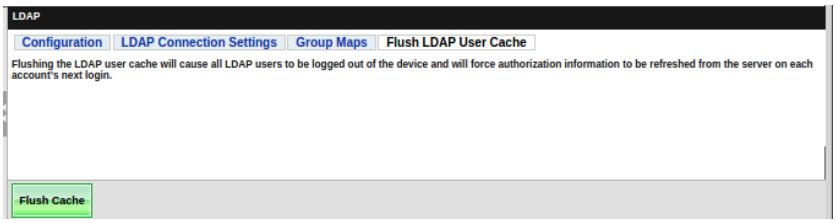


Figure 11.9 Flush LDAP User Cache Tab

The last tab on the LDAP page is **Flush LDAP User Cache**. Selecting the **Flush Cache** button flushes the LDAP user cache, which causes all active LDAP users to be logged out of the device and forces the server to refresh authentication information the next time each account logs in.

Front Panel

The front panel does not display any LDAP client information.

Dashboard

The dashboard does not provide any LDAP client information.

Alert/Notifications

The SEL-2488 provides the following alerts or notifications for events associated with the LDAP client. The SEL-2488 replaces message variables in {} with the values it logs.

Table 11.3 LDAP Client Alerts and Notifications (Sheet 1 of 2)

Message	Event Threshold	Alarm Category	Alarm Class
LDAP: {0}:{1} does not respond	Error	None	–
LDAP: An error occurred during authentication or authorization on server {0}:{1}	Error	None	–
LDAP: An error occurred during Bind DN authentication on server {0}:{1}	Error	None	–
LDAP: An error occurred when searching for a DN on the server {0}:{1}	Error	None	–
LDAP: An error occurred when searching for the user's DN on the server {0}:{1}	Error	None	–
LDAP: Bind DN authentication failed on server {0}:{1}	Error	None	–
LDAP Bind DN changed by {username} at {user_ip}	Warning	Minor	Configuration
LDAP Bind DN Password changed by {username} at {user_ip}	Warning	Minor	Configuration
LDAP disabled by {username} at {user_ip}	Warning	Minor	Configuration
LDAP enabled by {username} at {user_ip}	Warning	Minor	Configuration
LDAP Group Filter changed by {username} at {user_ip}	Warning	Minor	Configuration
LDAP: Group Filter search on server {0}:{1} returned no groups	Warning	None	–
LDAP: Group Filter syntax invalid for server {0}:{1}	Error	None	–
LDAP group mapping {0} changed to {1} by {username} at {user_ip}	Warning	Minor	Configuration
LDAP group mapping {0} mapping created by {username} at {user_ip}	Warning	Minor	Configuration
LDAP group mapping {0} mapping deleted by {username} at {user_ip}	Warning	Minor	Configuration
LDAP Group Membership Attribute changed by {username} at {user_ip}	Warning	Minor	Configuration
LDAP: LDAP version used by server {0}:{1} is not supported	Error	None	–
LDAP: No Group Mappings set for server {0}:{1}	Warning	None	–
LDAP: One or more of the user-configured DNs for server {0}:{1} contains syntax errors.	Error	None	–
LDAP Search Base changed by {username} at {user_ip}	Warning	Minor	Configuration
LDAP: Search base entry not found on server {0}:{1}	Error	None	–
LDAP server {0}:{1} created by {username} at {user_ip}	Warning	Minor	Configuration
LDAP server {0}:{1} deleted by {username} at {user_ip}	Warning	Minor	Configuration

Table 11.3 LDAP Client Alerts and Notifications (Sheet 2 of 2)

Message	Event Threshold	Alarm Category	Alarm Class
LDAP server {0}:{1} hostname changed to {2} by {username} at {user_ip}	Warning	Minor	Configuration
LDAP server {0}:{1} port changed to {2} by {username} at {user_ip}	Warning	Minor	Configuration
LDAP: Server {0}:{1} returned a DN that was longer than 4096 bytes. That DN was ignored.	Error	None	–
LDAP settings changed by {username} at {user_ip}	Warning	Minor	Configuration
LDAP Synchronization Interval changed by {username} at {user_ip}	Warning	Minor	Configuration
LDAP: The certificate presented by {0}:{1} is expired	Error	None	–
LDAP: The certificate presented by {0}:{1} is invalid	Error	None	–
LDAP: The hostname of the certificate presented by {0}:{1} does not match	Error	None	–
LDAP: The issuing authority of the certificate presented by {0}:{1} is untrusted	Error	None	–
LDAP TLS disabled by {username} at {user_ip}	Warning	Minor	Configuration
LDAP TLS enabled by {username} at {user_ip}	Warning	Minor	Configuration
LDAP: Unable to connect to server at {0}:{1}	Error	None	–
LDAP: Unable to start TLS session with {0}:{1}	Error	None	–
LDAP User ID Filter changed by {username} at {user_ip}	Warning	Minor	Configuration
LDAP: User ID Filter syntax invalid for server {0}:{1}	Error	None	–

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Events classified as None will not trigger the alarm contact.

Section 12
X.509 Certificate Management

Overview

Hypertext Transfer Protocol Secure (HTTPS [SSL/TLS]) connections require authentication to confirm that the user is communicating with the correct server. X.509 certificates provide this authentication. By default, the SEL-2488 has a self-signed X.509 certificate that can cause the client web browser to issue a security alert. This security alert requires a security exception before authentication can continue.

The SEL-2488 requires one X.509 certificate that is used for HTTPS communication between the client web browser and the web server running on the device. The device automatically generates a unique initial self-signed certificate whenever there is a factory-default reset. This initial certificate can be replaced with organization-generated X.509 server certificates that are signed by the organization or other trusted Certificate Authority (CA). Replacing the default certificate with a CA-signed certificate the browser trusts will remove the security warning.

Certificates have valid start and end dates. After the certificate end date, the browser provides a warning that the certificate has expired.

Certificates have a public key and a private key. Both are necessary before the device trusts the certificate and allows device communication with the server. All devices connecting to the SEL-2488 Web Management pages receive the public key. Only the owner of each device has the private key specific to that device. In the case of a compromised private key or one distributed to other than authorized personnel, replace all certificates corresponding to that private key.

Other X.509 certificates that can be installed on the SEL-2488 are "Root" certificates CAs publish. These certificates allow the SEL-2488 to authenticate other devices it may be communicating with, such as Lightweight Directory Access Protocol (LDAP) servers.

Settings contains directions for working with certificates on the SEL-2488.

For additional details on X.509 certificates, see *Appendix F: X.509*.

Settings

This section discusses the operations you can perform on X.509 certificates within the SEL-2488. Configure X.509 certificates on the SEL-2488 via the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **Security > X.509 Certificates** menu option.

List Certificates

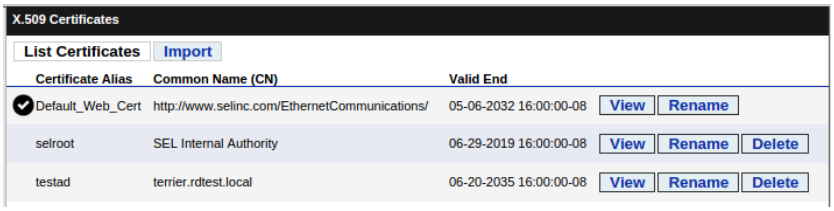


Figure 12.1 X.509 List Certificates Tab

The **List Certificates** tab provides a list of certificates presently installed on the SEL-2488 and provides options for managing the installed certificates.

View Certificate

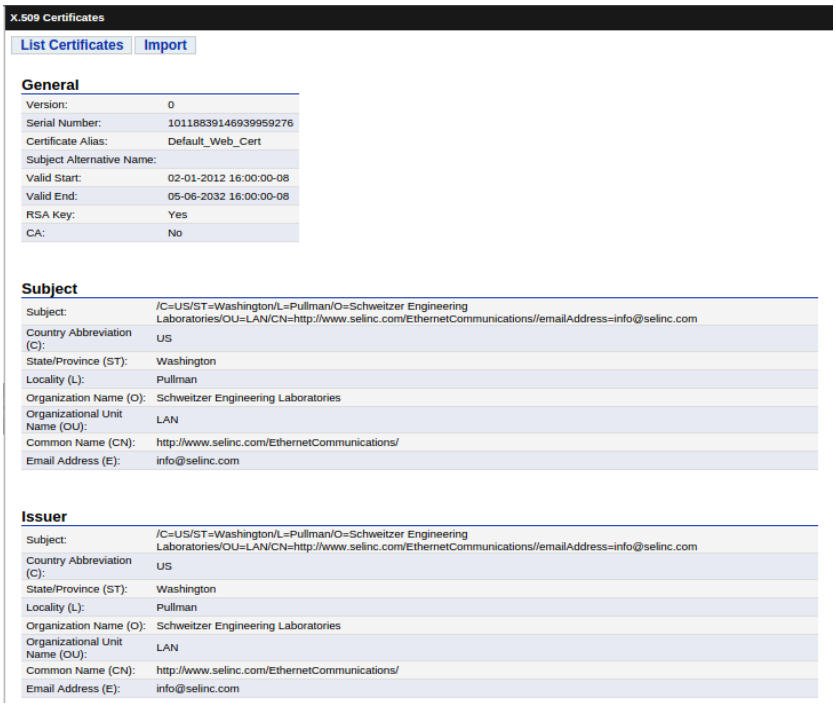


Figure 12.2 X.509 View Certificate Page

Selecting the **View** button displays the details of the certificate. You cannot modify any values.

Rename Certificate

Figure 12.3 X.509 Rename Certificate Page

Selecting the **Rename** button allows you to change the certificate alias. The certificate alias is a label the SEL-2488 uses for tracking purposes and has no effect on the function of the certificate. This option allows you to change the label you applied to a certificate during the Import Certificate process.

Delete Certificate

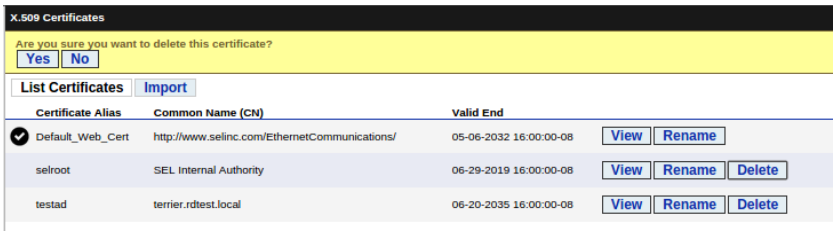


Figure 12.4 X.509 Delete Certificate Dialog

Selecting the **Delete** button associated with a certificate displays a dialog box to confirm the deletion of the certificate.

Activate Certificate

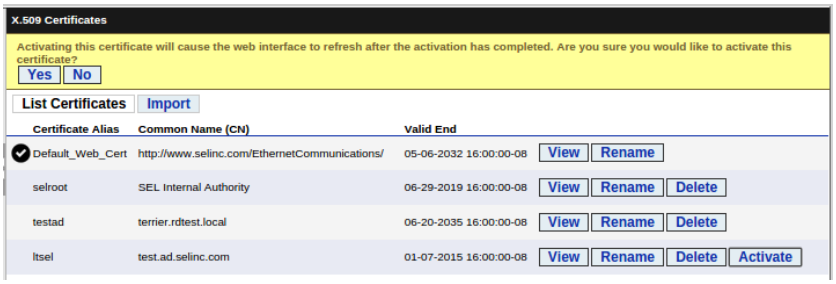


Figure 12.5 X.509 Activate Certificate Dialog

If you import an alternate server certificate into the SEL-2488, possibly one signed by the organization's CA, it can become the certificate for the SEL-2488. Pressing the **Activate** button on the new certificate displays a dialog box to confirm the change of certificates and notifies you that the web interface will refresh (the system will log you out). Some imported certificates may not be allowed to activate if they are missing required fields or are not formatted correctly.

A check mark in the black circle to the left of the alias identifies the active web certificate. You cannot delete the active certificate.

Import Certificate

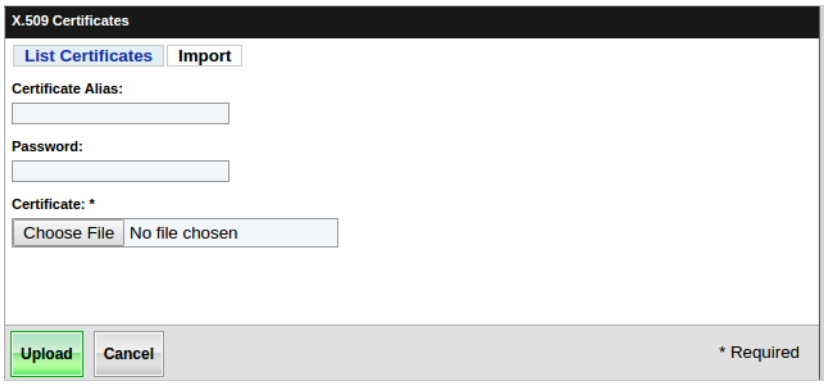


Figure 12.6 X.509 Import Certificate Tab

The **Import** tab allows new certificates to be added to the SEL-2488. These can be root certificates you use with LDAP or CA-backed web server certificates. You can also use this option to generate a certificate alias for the SEL-2488 to use in tracking the certificate. This alias does not affect the certificate.

If the certificate you are importing has a password, enter the password on this screen.

Select the **Choose File** button to open a dialog box that allows you to navigate to a certificate location and select the certificate you want to import.

Front Panel

The front panel does not display any X.509 certificate management information.

Dashboard

The dashboard does not display any X.509 certificate management information.

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for the events associated with X.509 certificate management. The SEL-2488 replaces message variables in {} with values it logs.

Table 12.1 X.509 Certificate Management Alerts and Notifications (Sheet 1 of 2)

Message	Event Threshold	Alarm Category	Alarm Class
Web Server Certificate: changed from {0} to {1} by {username} at {user_ip}	Warning	Minor	Configuration
X.509 certificate {0} Alias: certificate changed to {1} by {username} at {user_ip}	Notice	Minor	Configuration
X.509 certificate {0}: certificate import completed successfully	Notice	Minor	Configuration
X.509 certificate {0} deleted by {username} at {user_ip}	Notice	Minor	Configuration
X.509 certificate {0} has expired; communications requiring X.509 based authentication may have stopped	Error	Minor	Configuration
X.509 certificate {0} set as default web certificate by {username} at {user_ip}	Notice	Minor	Configuration
X.509 certificate {0} will expire in {1} days; communications requiring X.509 based authentication may be affected when it expires	Warning	Minor	Configuration

Table 12.1 X.509 Certificate Management Alerts and Notifications (Sheet 2 of 2)

Message	Event Threshold	Alarm Category	Alarm Class
X.509 certificate {0} will expire in {1} days; communications requiring X.509 based authentication may be affected when it expires	Notice	Minor	Configuration
X.509 certificate {0} will expire in {1} days; communications requiring X.509 based authentication may be affected when it expires	Informational	None	–
X.509 certificate import failed	Warning	Minor	Configuration
X.509 certificate import started by {username} at {user_ip}	Notice	Minor	Configuration

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Events classified as None will not trigger the alarm contact.

This page intentionally left blank

Section 13
Hostname Resolution

Overview

SEL-2488 hostname resolution provides an interface for manually configuring the Ethernet network name resolution functionality used to associate hostnames with Internet Protocol (IP) addresses.

Ethernet traffic uses a system of IP addresses to identify and communicate with other devices across the networks. IP addresses, while very convenient for interaction among network devices, are not easy for humans to remember.

Name resolution allows labels, such as www.selinc.com, to represent IP addresses. A network device can resolve the labels to IP addresses and establish communication with target devices. Another feature of name resolution is that the target device IP address can change while the label remains the same. In personal computers and other network devices, the Domain Name Service (DNS) resolver performs this association. At present, the SEL-2488 does not incorporate this service but instead provides hostname resolution through the use of a manually edited lookup table on the device.

IP addresses can change, so X.509 certificates use labels instead of addresses to identify target devices. The Lightweight Directory Access Protocol (LDAP) option in the SEL-2488 requires X.509 certificates published by certificate authorities to verify the identity of the LDAP server with which it will communicate to verify user access credentials and permissions.

To use this functionality in conjunction with X.509 certificates, you must enter the server labels in the certificate as records in the Hosts menu option along with the IP address of the server to which the label belongs. The label in the certificate common name field is the server that the certificate represents; enter this label in the Hostname field exactly as the certificate shows. For more information on certificates and certificate management, see *Section 12: X.509 Certificate Management*.

Settings

This section discusses the settings that customize and affect operation of hostname resolution. Use the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **Network Management > Hosts** menu option to configure SEL-2488 hostname resolution.

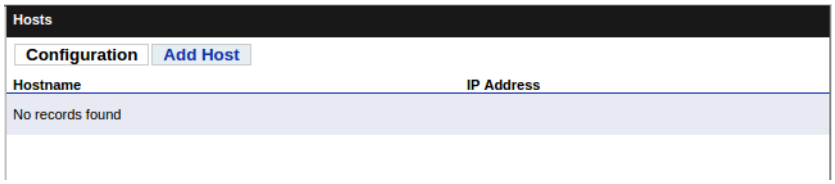


Figure 13.1 Host Configuration Tab

Figure 13.2 Add Host Tab

Hostname resolution allows for the definition of 64 hostname to IP address entries. The hostname must be unique across all entries, but multiple hostnames can resolve to the same IP address. An entry must contain both a valid hostname and IP address.

Table 13.1 Host Settings

Setting Name	Values	Default	Description
Hostname	See hostname notes below		The unique name identifying a remote device on the network
IP Address	Unicast IP Address (See notes below)		The IP address of the remote device on the network

A hostname for the purpose of hostname resolution is a label or group of labels representing a unique identifier for the remote entity.

- A hostname must have at least one label
- Each label must be at least one character and cannot exceed 63 characters
- Labels can only contain characters a–z, A–Z, 0–9, and the hyphen "-"
- The hyphen cannot be the first or last character of a label
- Labels are separated by periods
- A hostname can contain a period, but not as the first or last character
- The overall length of the hostname (all labels and periods) cannot exceed 254 characters

SEL-2488 hostname resolution IP address settings must adhere to the following:

- All IP addresses defined on a device are IPv4 addresses
- All IP addresses must be in the range 1.0.0.0–223.255.255.255

Front Panel

The front panel does not display any hostname resolution information.

Dashboard

The dashboard does not display any hostname resolution information.

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for the events associated with hostname resolution. The SEL-2488 replaces message variables in {} with values it logs.

Table 13.2 Hostname Resolution Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
`Host Settings: Added host {0} with IP address {1} by {username} at {user_ip}.`	Notice	Minor	Configuration
`Host Settings: Changed hostname {0} with IP address {1} to {2} with IP address {3} by {username} at {user_ip}.`	Notice	Minor	Configuration
`Host Settings: Removed host {0} with IP address {1} by {username} at {user_ip}.`	Notice	Minor	Configuration

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

This page intentionally left blank

Section 14
Event Reporting System

Overview

The SEL-2488 event reporting system is a centralized mechanism that monitors for alerts or notifications other systems generate on the device and reports these events through the various notification subsystems. This is not to be confused with a Sequence of Events report that other products produce.

The event reporting system provides notification through the local syslog report, and also through the following interfaces based on event severity and device configuration:

- Simple network management protocol (SNMP) notification
- Remote syslog
- Alarm contact (including **ALARM** LED)
- Front-panel display LCD
- Web interface notification

A discussion of web interface notification appears in following text. All other notification interfaces have separate sections defining how and when notifications generate.

Major vs. Minor Events

Syslog reporting includes a severity classification system ranging from Emergency to Informational. SEL-2488 local syslog events, remote syslog events, and SNMP notifications are tied to these classifications. All other event reporting interfaces use a two-level method (Major or Minor) of classifying event severity.

A correlation exists between event severities and major versus minor events. Event severities of Emergency, Alert, and Critical correspond to a major event, while Error, Warning, Notice, and Informational correspond to a minor event.

Major Events

Major events are either an indication that the device has a failed component such as a Global Navigation Satellite System (GNSS) receiver, or that the device experienced a significant change in status, such as a part number change. Major events provide notification through the following interfaces.

- Local syslog event generated
- Remote syslog event generated (if configured)
- SNMP notification generated (if trap server configured)

- Alarm contact latched in alarm condition
- **ALARM** LED turns on
- Front-panel LCD displays error message and backlight remains lit
- Web interface presents notification and notification remains active

Many major events require operator acknowledgment before the event reporting interface clears the notification. If the condition causing the event is not resolved prior to event acknowledgment, the event notification will reappear after acknowledgment.

Self-Healing Major Events

Self-healing major events are significant events that clear automatically after the condition that created the issue is resolved. An example of this is an open antenna condition. If the antenna is disconnected, a major alarm condition with event reporting and alarm contact latching occurs. If, however, the antenna is reconnected and no other error occurs, the event clears the latched alarm contact and reports that the event condition no longer exists. At this time, the SEL-2488 has four self-healing major events:

- Antenna open/short condition
- Holdover operation (loss of satellite signal)
- Loss of power supply (or power to power supply) in redundant power supply configuration
- Change of part number (clears when original part number is restored following an unacknowledged notification)

Minor Events

Minor events are less significant events reflecting items such as settings changes or momentary operational condition changes such as a temporary loss of link on an Ethernet connection. Minor events pulse the alarm contact but do not latch the contact as in major events. Not all reporting interfaces reflect minor events. Front-panel LCD and web interface notifications do not report minor events.

Web Interface Notification

The SEL-2488 has an event notification system that displays on the web interface for the device. This notification system is in the form of a banner at the top of the webpage (see *Figure 14.1*). The notification only displays for events that are classified as Major events and shows a text message for the event in progress. The notification remains on the webpage until event acknowledgment. Self-healing events clear without acknowledgment.

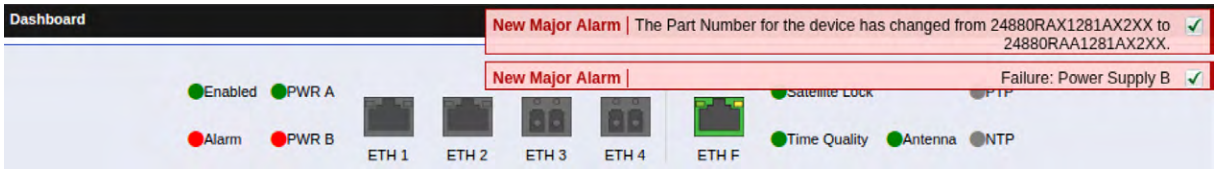


Figure 14.1 Event Notification Dialog

Clearing Major Events (Alarms)

The web interface notification allows you to acknowledge a major event and clear a major event alarm. The notification presents a check box on the right side of the banner that, when selected, acknowledges the event and clears the banner for that event. If there are multiple major events in progress, each event must be acknowledged individually.

This acknowledgment also clears the major events reflected on the front panel and the alarm contact. If there are multiple major events in progress, acknowledgment of all events must occur to clear the front panel and alarm contact.

Settings

Section 15: Alarm Contact, *Section 16: Syslog Reporting*, and *Section 17: Simple Network Management Protocol (SNMP)* discuss settings controls that affect event notifications. There is no separate setting section for the event reporting system.

Front Panel

Major events display the message text from the syslog entry in a scrolling mode on the LCD screen. Only the most recent unacknowledged event displays on the LCD.

The **ALARM** LED tracks the alarm contact operation.

Dashboard

The web interface notification banner displays the message text from the syslog entry.

Alert/Notifications

The SEL-2488 provides the following alerts or notifications for events associated with the event reporting system. The SEL-2488 replaces message variables in {} with values it logs.

Table 14.1 Event Reporting System Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
The {0} event queue left the overflow condition. Approximately {1} events were lost.	Notice	None	–
The {0} event queue overflowed	Error	None	–

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

Events classified as None will not trigger the alarm contact.

Section 15
Alarm Contact

Overview

The SEL-2488 alarm contact is part of the event reporting system that notifies users of an event through the operation of a mechanical Form C contact. This contact contains both normally open (NO) and normally closed (NC) contacts. NO and NC refer to the state of the contact when it is in a de-energized state. The SEL-2488 energizes the Form C alarm contact during typical operating conditions, so a normally open contact will be closed and a normally closed contact will be open. Triggering of an alarm event de-energizes the contact, resulting in the NO contact returning to the open state and the NC contact returning to the closed state. By providing a Form C alarm contact, the SEL-2488 will work in either open- or closed-loop monitoring systems.

The alarm contact has two levels of alarm severity: Major and Minor. The mode of operation defines these two levels. A major alarm will de-energize the contact output and latch in that mode until there is acknowledgment of the alarm, whereas a minor alarm will de-energize the contact output for one second and then re-energize the contact. See *Section 14: Event Reporting System* for additional details on major and minor events.

Table 15.1 shows the Form C contact pinout.

Table 15.1 Alarm Contact Pinout

Pin	Description
C3	Normally open
C4	Common
C5	Normally closed

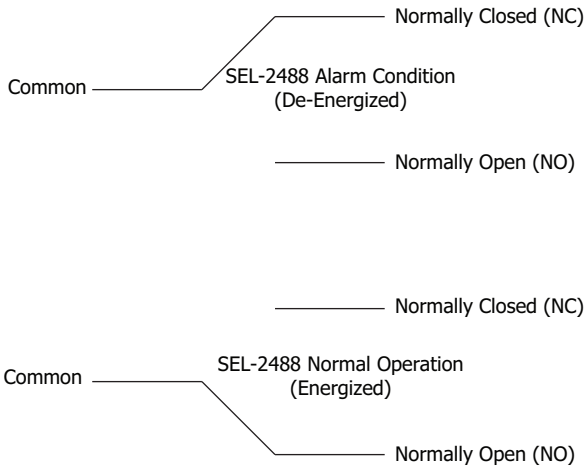


Figure 15.1 SEL-2488 Alarm Contact Status

Major alarm events cannot be prevented from operating the alarm contact. Most minor alarm events, however, can be enabled or disabled based on a defined set of categories. These categories and their associated event types are defined as follows:

- Authentication—events associated with authenticating with the SEL-2488, such as login and logout.
- Chassis—events associated with the hardware. Examples include adding or removing a redundant power supply.
- Configuration—events associated with changing settings on the device.
- Link—events associated with Ethernet interface link status changes.
- System Integrity—events associated with validation of satellite date/time.
- Time Synchronization—events associated with time quality.

Settings

This section discusses the settings that customize and affect alarm contact operation. Use the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **System > Contact I/O** menu option to configure the SEL-2488 alarm contact.

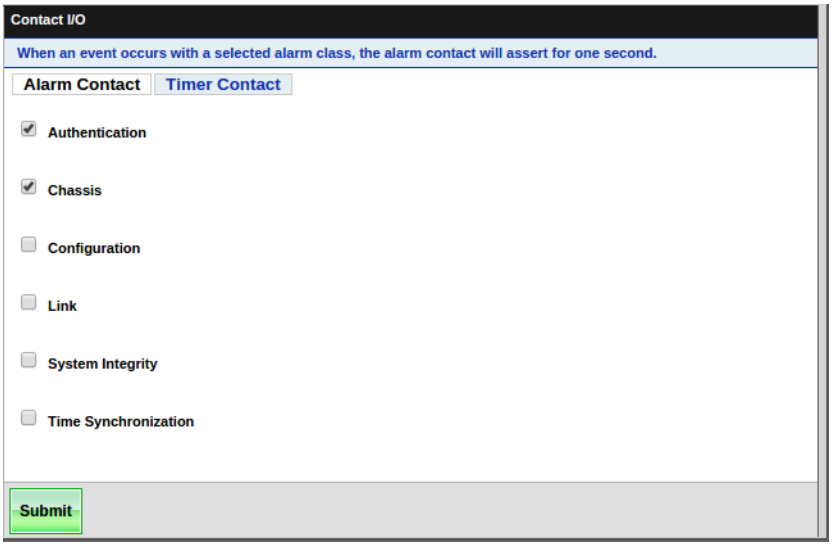


Figure 15.2 Alarm Contact Settings Tab

Table 15.2 General Alarm Settings (Sheet 1 of 2)

Setting Name	Values	Default	Description
Authentication	Checked, Unchecked	Checked	Enables or disables notification of minor authentication events on the alarm contact
Chassis	Checked, Unchecked	Checked	Enables or disables notification of minor chassis events on the alarm contact
Configuration	Checked, Unchecked	Unchecked	Enables or disables notification of minor configuration events on the alarm contact

Table 15.2 General Alarm Settings (Sheet 2 of 2)

Setting Name	Values	Default	Description
Link	Checked, Unchecked	Unchecked	Enables or disables notification of minor link events on the alarm contact
System Integrity	Checked, Unchecked	Unchecked	Enables or disables notification of minor system integrity events on the alarm contact
Time Synchronization	Checked, Unchecked	Unchecked	Enables or disables notification of minor time synchronization events on the alarm contact

Front Panel

The ALARM LED on the front panel illuminates (red) when the device is in an alarm condition (alarm contact de-energized).

Figure 15.3 Front-Panel Alarm LED

Dashboard

The **Alarm** LED on the dashboard replicates the front-panel alarm indicator and illuminates (red) when the device is in an alarm condition (alarm contact de-energized).

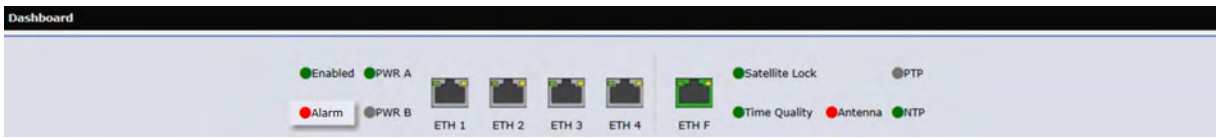


Figure 15.4 Alarm Dashboard LED

Alerts/Notifications

The SEL-2488 provides the following alert or notification for the event associated with the alarm contact. The SEL-2488 replaces message variables in {} with values it logs.

Table 15.3 Alarm Contact Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
`Alarm Contact: configuration changed by {username} at {user_ip}`	Notice	Minor	Configuration

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Section 16
Syslog Reporting

Overview

SEL-2488 syslog reporting is part of the event reporting system that notifies through two mechanisms, a local syslog report and formatted network message traffic.

Threshold Setting

The Syslog Protocol contains a field called Severity with predefined values representing increasing or decreasing levels of event severity. The values the SEL-2488 uses appear in the following list in order from highest to lowest priority:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational

The SEL-2488 allows lower-priority messages to be filtered out based on a threshold setting. Setting this threshold to a higher priority filters out all messages with a priority less than the one you have selected and causes the SEL-2488 to send only messages with the priority you have selected or higher. This filtering is at the time of the event, so changing the threshold only affects future messages, not preexisting ones. A higher threshold reduces the number of events the SEL-2488 sends to the remote syslog destinations. This can result in traffic loads being reduced, but it can also cause the loss of key event notifications.

You can set the threshold independently for each of the remote syslog destinations through the syslog setting interface discussed in *Settings*.

Local Syslog Reporting

The SEL-2488 uses a format that contains the same information syslog messages provide as a local reporting method for the clock. The **Reports > Syslog Report** menu option presents this on the web interface.

The device stores information from every event locally. The report maintains as many as 60,000 events, removing the oldest events first.

The report contains seven columns. Five are populated with information from the event (Timestamp, Tag, Severity, Facility, and Message), and the remaining two (Acknowledged, ID) are part of the report display.

The records, by default, display newest first in descending ID order. The ID field is a tracking of the sequence in which the **Local Syslog Reporting** display receives the event. You can sort the data in the report window by all columns except for **Message**.

Acknowledged	ID	Timestamp	Tag	Severity	Facility	Message
☐	2158	2015-09-29 15:23:06.582712-07	Login	Notice	SECURITY	Login to web: successful by a at 192.168.2.99
☐	2157	2015-09-29 13:00:07.194172-07	Login	Warning	SECURITY	User account a timeout
☐	2156	2015-09-29 13:29:38.686869-07	PTP	Notice	SYSTEM	Port ETH 4 changed PTP state to Master
☐	2155	2015-09-29 13:29:38.61733-07	PTP	Notice	SYSTEM	Port ETH 2 changed PTP state to Master
☐	2154	2015-09-29 13:29:38.638884-07	PTP	Notice	SYSTEM	Port ETH 1 changed PTP state to Master
☐	2153	2015-09-29 13:29:38.646768-07	PTP	Notice	SYSTEM	Port ETH 3 changed PTP state to Master
☐	2152	2015-09-29 13:29:37.61215-07	TimeSync	Notice	CLOCK	Time Quality < 1µs.
☐	2151	2015-09-29 13:29:33.609253-07	TimeSync	Warning	CLOCK	Time source has changed to Manual.
☐	2150	2015-09-29 13:29:32.075309-07	TimeSync	Notice	USER	Time set manually by a at 192.168.2.99.
☐	2149	2015-09-29 13:29:15.722062-07	Login	Notice	SECURITY	Login to web: successful by a at 192.168.2.99
☐	2148	2015-09-29 13:29:09.617184-07	Power	Notice	SYSTEM	Device initialization completed
☐	2147	2015-09-29 13:29:08.706335-07	LinkUpDown	Notice	SYSTEM	Port ETH 1 changed link state to up
☐	2146	2015-09-29 13:28:54.490175-07	SystemIntegrity	Warning	CLOCK	GNSS signal verification is not operational.
☐	2145	2015-09-29 13:28:25.816085-07	Power	Error	USER	Device rebooted by a at 192.168.2.99
☐	2144	2015-09-29 13:28:11.791784-07	Login	Notice	SECURITY	Login to web: successful by a at 192.168.2.99
☐	2143	2015-09-30 12:05:03.366237-07	PTP	Notice	SYSTEM	Port ETH 3 changed PTP state to Master

Figure 16.1 Syslog Report

Local Syslog Report Fields

The **Acknowledged** check box allows the operator to flag reviewed events. Acknowledging an entry does not remove the event. It is not possible to reverse the acknowledgment of an event. *Acknowledge Events* discusses use of the **Acknowledged** column.

The **Timestamp** column represents the time the event occurred on the device, using the present device time. The format for this is {date} {time}{offset from UTC}. The date format is YYYY-MM-DD, and time is in a 24-hour format, with six decimal digits of second precision (hh:mm:ss.zzzzzz). Time always displays in local time based on the Local Time Offset setting and Daylight-Saving Time offset (when applicable). The local time stamp in the syslog report reflects changes to the local time or daylight-saving offset. The last component of the time stamp is the offset field, which represents the number of hours and minutes the local time is offset from UTC. A positive offset indicates that local time is ahead of UTC and that the offset component will

need to be subtracted from the local time stamp to obtain UTC. Conversely, negative offsets will be added. To display UTC with zero offset, navigate to the **Date/Time** menu option, set the local time offset to 00:00, and select **No Daylight Saving Time observed** in the Daylight Saving Time Mode.

Tag represents the name of the process that generated the event. Tag names ending in "Config" typically represent settings changes made to the device through the web interface.

NOTE: Events indicate occurrence of reportable conditions, while the **Severity** field provides a level of concern for each event. The event may be a positive notification such as achievement of satellite lock or a negative notification such as an antenna failure.

Severity represents the level of concern the event represents. *Threshold Setting* includes the list of severity levels available on the device and their order of precedence. These levels are representative of the values in the Syslog protocol (RFC3164). You cannot adjust the severity levels for the events.

Facility, a classification from the Syslog Protocol, provides a method of classifying the subsystem that triggered the event.

Message details the action that generated the event. See *Figure 16.1* for examples of these messages.

Appendix D: Syslog contains a full list of all local syslog report messages.

Acknowledge Events

After reviewing event records, you should acknowledge them to aid tracking of new event records. There are two methods for acknowledging records (neither option is reversible when finished). The first method is to select the **Acknowledge** check boxes for each desired record, and then select the **Acknowledge Selected** button at the top of the page. The black check marks will turn to green. With this method, you must acknowledge items you select each page before moving to the next page.

The other method is to select the **Acknowledge All** button, which acknowledges all unacknowledged records on all pages.

Acknowledging records generates a new event record indicating acknowledgment of one or more events.

Download Events

This option allows you to download locally stored event records on the device to a comma-separated-values (CSV) formatted file. Selecting **Download** starts the download of the file **syslog_download.csv**. If there is a large number of event records, download time may be significant.

If you open the CSV file directly from Microsoft Excel, the Message column may not display properly. This is because of the automatic default formatting set by Excel. To properly view and import the SEL-2488 syslog CSV file by using Excel, follow these steps:

Step 1. Open a blank worksheet in Excel.

Step 2. On the **Data** tab, in the **Get External Data** group, select **From Text**.

Step 3. Browse to the SEL-2488 syslog CSV file and select it, and then select **Import**.

Step 4. In the first step of the Text Import Wizard, configure the settings as follows:

a. Select **Delimited** as the original data type

b. In the **File Origin** drop-down list, select 65001 : Unicode (UTF-8)

c. Select the **My data has headers** check box

Select **Next** to continue.

Step 5. In the second step of the Text Import Wizard, select the **Comma** check box and clear the **Tab** check box for the delimiters, and then select **Finish**.

Step 6. Choose the location where you want to put the syslog data in your spreadsheet, and select **OK**.

Your SEL-2488 syslog CSV file should now import and display with the **Message** field formatted correctly.

Page Navigation

Local syslog reporting displays records in a series of pages. The **Records Per Page** option at the bottom of the page allows you to choose how many records to display on each page (25, 50, 100, or 200).

Remote Syslog Reporting

The SEL-2488 formats and transmits event messages according to the Syslog protocol defined in RFC-3164 with the enhancement that the SEL-2488 time stamps include the local time offset to UTC. The SEL-2488 can transmit the event messages to three different remote syslog destinations.

While the implementation allows specification of the remote server Internet Protocol (IP) address, the port number is fixed to the default port for the Syslog Protocol (514) and cannot be changed.

As previously stated, you can set threshold levels individually for each remote syslog.

Settings

This section discusses the settings that customize and affect operation of syslog reporting. Use the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **Network Management > Syslog Settings** menu option to configure SEL-2488 syslog reporting.

The user configures the remote syslog reporting option through the **Syslog Settings** page.

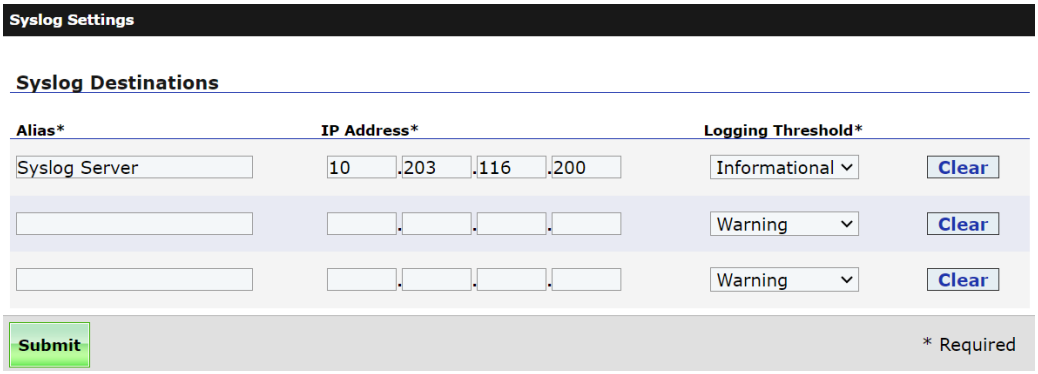


Figure 16.2 Syslog Settings Page

A unique alias is necessary for each record for which there is a populated IP address in the **Syslog Destinations** area.

Table 16.1 Syslog Destination Settings

Setting Name	Values	Default	Description
Alias	1–32 characters		Alias for the remote Syslog server. If supplied, the alias must be unique among the Syslog servers.
IP Address	Unicast IP Address		The IP address of the syslog destination.
Logging Threshold	Alert Critical Error Warning Notice Informational	Warning	The minimum severity level that an event must have before the SEL-2488 can forward it to this destination.

The SEL-2488 **Syslog Destinations** IP addresses must adhere to the following:

- All IP addresses defined on the device are IPv4 addresses
- Destination IP addresses must be unique; two or more destinations cannot have the same IP address
- Destination IP address cannot be the same as any device Ethernet interface IP address

Front Panel

The front panel does not display any syslog reporting information.

Dashboard

The dashboard does not display any syslog reporting information.

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for the events associated with syslog reporting. The SEL-2488 replaces message variables in {} with values it logs.

Table 16.2 Syslog Reporting Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
Local Syslog Event Queue contains <= 65% unacknowledged events.	Notice	None	–
Local Syslog Event Queue contains <= 80% unacknowledged events.	Notice	None	–
Local Syslog Event Queue contains >= 75% unacknowledged events.	Warning	None	–
Local Syslog Event Queue contains >= 90% unacknowledged events.	Critical	None	–
Syslog Destination {0}: created by {username} at {user_ip}	Notice	Minor	Configuration
Syslog Destination {0}: deleted by {username} at {user_ip}	Warning	Minor	Configuration
Syslog Destination {0} Settings: modified by {username} at {user_ip}	Warning	Minor	Configuration
Syslog events acknowledged by {username} at {user_ip}	Notice	None	–

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Events classified as None will not trigger the alarm contact.

Section 17

Simple Network Management Protocol (SNMP)

Overview

The SEL-2488 provides Simple Network Management Protocol (SNMP) read request and notification (trap) support. Through SNMP read requests, you can access SEL-2488 diagnostic and status information from your SNMP client or Network Management System (NMS). You can configure the SEL-2488 to send SNMP notifications to a central location, which provides event monitoring and correlation across the network infrastructure. The SEL-2488 will respond to read requests using SNMP v2c or v3 protocols and uses the SNMP v2c protocol to send trap messages to a trap server.

SNMP Read

You can access the current status information that is available on the SEL-2488 web dashboard through the SNMP read operations from your client. The SEL-2488 allows SNMPGET, SNMPGETNEXT, and SNMPWALK requests using SNMP v2c and v3 protocols. The status information is presented as value responses to OIDs (identifiers used for SNMP operations). Most of the information is grouped using the same grouping found on the web dashboard.

SEL provides customized Management Information Base (MIB) modules to install on your SNMP client to assist with finding the information and decoding the responses. The SEL-2488 utilizes the SNMP standard IF-MIB to provide details (name, speed, media type, and status) regarding the Ethernet ports. These MIBs are available for download directly from the SEL-2488. The following is a list of the MIBs supporting the information inquiry:

- IF-MIB
- SEL-2488-DASHBOARD-MIB
- SEL-2488-DEVICE-INFORMATION-MIB
- SEL-2488-DEVICE-DIAGNOSTICS-MIB
- SEL-2488-PORT-STATUS-MIB
- SEL-2488-PTP-DIAGNOSTICS-MIB
- SEL-2488-SATELLITE-STATUS-MIB

- SEL-2488-SYSTEM-STATISTICS-MIB
- SEL-2488-TIME-INPUT-MIB
- SEL-2488-TIME-OUTPUT-MIB

Settings

This section discusses the settings that customize and affect the operation of SNMP on the SEL-2488. Use the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **Network Management > SNMP** menu option to configure SNMP.

The SNMP Settings section contains three tabs: Configuration, Profile Settings, and Trap Server Settings.

Configuration

The **Configuration** tab displays the current SNMP profiles and trap servers configured for the SEL-2488. The SNMP profile defines the v2c or v3 SNMP profile used with SNMP read requests and the v2c profiles available for use with SNMP trap messages. The SNMP Profiles table shows the specific details—Alias and Community for v2c; Username, Authentication, and Encryption modes for v3—assigned to each profile (see *Profile Settings* for further details). An SNMP trap server is a device that is configured to receive the trap notification message and send alerts or reports based on the SNMP trap message received from the SEL-2488. The Trap Servers table provides a list of all configured SNMP trap servers for the SEL-2488.

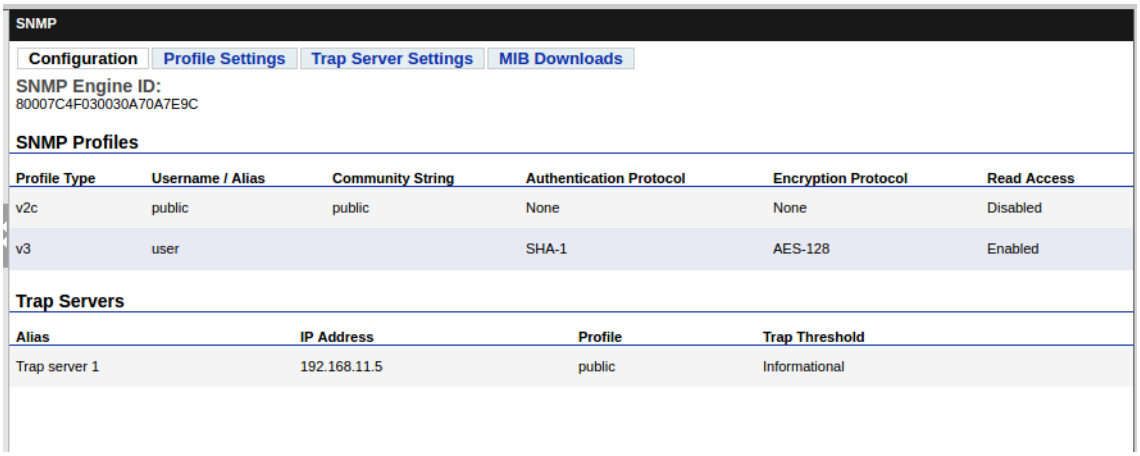


Figure 17.1 SNMP Configuration Tab

Passphrases

Passphrases provide a user the ability to create strong and easy-to-remember passwords that protect access to a system. A strong passphrase includes many different characters from many different character sets. Longer passphrases provide greater security than shorter passphrases. SNMP v3 accounts support complex passphrases that must include at least one character from each of the following character sets:

- Uppercase letters
- Lowercase letters
- Digits
- Special characters

Additionally, passphrases must be at least eight characters in length. Spaces are allowed in passphrases. Sample passphrases include the following:

- Strong: W3b$ter!
- Stronger (and easier to remember): A phras3 is 3v3n Str0ng3r!

Profile Settings

The **Profile Settings** tab allows you to configure either a v2c or v3 profile. Depending on the profile selected, you will be required to enter an Alias or Username and optionally mark the profile to allow read access. The Alias is a unique user-defined name for the v2c profile, and when configuring a v2c profile, you will also be required to enter a Community String. If configuring a v3 profile, you will have the option to select authentication and encryption modes and provide passwords for those selections.

SNMP profiles fulfill the following two requirements:

- Define the connection method for accessing the SEL-2488 to read diagnostic and status information.
- Provide the connection details for sending notifications to a remote SNMP trap server.

Either a v2c or v3 profile is required for read access to be used to access the SEL-2488. SNMP v2c profiles use a nonsecure common community string to allow access, whereas v3 profiles use specific usernames and have the option for secure message authentication and encryption. Use of v3 profiles with authentication and encryption enabled where possible is highly recommended to preserve the security of the communications with the device.

An SNMP v2c profile is required before you can configure an SNMP trap server for the SEL-2488. The Trap Community string can be used in the SNMP trap message for authentication purposes. If your SNMP trap server uses a community string, ensure that the Trap Community string for the profile matches the SNMP Community string for your SNMP trap server.

Figure 17.2 shows an example of the SEL-2488 configured with two SNMP profiles.

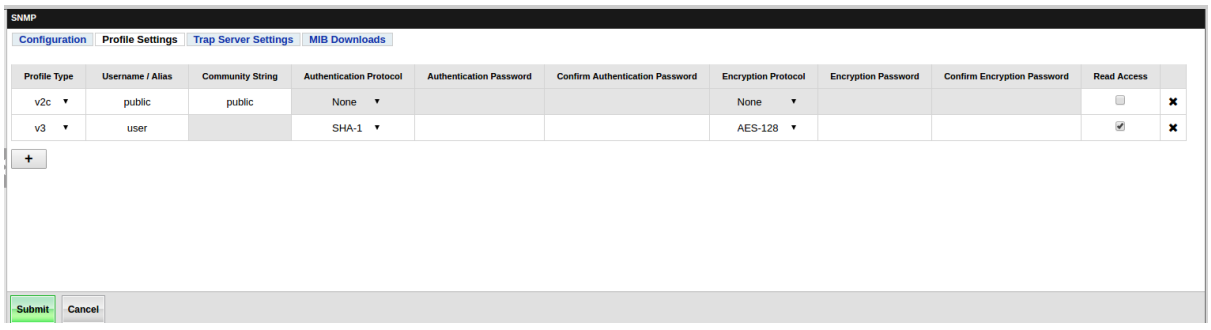


Figure 17.2 SNMP Profile Settings Tab

To add additional SNMP profiles to the SEL-2488, select the plus (+) button below the table. In the new table row, select and enter the appropriate profile details and select **Submit**. The SEL-2488 supports as many as eight user-defined SNMP profiles. To remove an SNMP profile, select the **X** button on the right side of the profile that you want to delete and select **Submit**. If a profile is currently in use for a trap server, you must remove the trap server association for the profile before you can delete it.

Table 17.1 SNMP Profile Settings

Setting Name	Values	Default	Description
Profile Type	v2c, v3	v2c	Selects the type of profile that will be added. Enables appropriate additional settings for the profile.
Username/Alias	1–32 characters	N/A	SNMP v2c alias or v3 username. The number of characters in a v3 username may be limited because of character selection.
Community String	1–128 characters	N/A	The community string used to authenticate SNMP v2c sessions.
Authentication Protocol	None, SHA-1, MD5	None	The v3 authentication protocol used to authenticate SNMP v3 sessions.
Authentication Password/ Confirm Authentication Password	8–128 ASCII characters	N/A	The v3 authentication password must include at least one uppercase and one lowercase letter, one number, and one special character. See *Passphrases* for more information.
Encryption Protocol[a]	None, AES-128	N/A[b]	The v3 encryption protocol to be used to encrypt the message traffic. An authentication protocol must be selected to allow selection of an encryption protocol.
Encryption Password/ Confirm Encryption Password	8–128 ASCII characters	N/A	The v3 encryption password must include at least one uppercase and one lowercase character, one number, and one special character. The encryption password must be different than the authentication password. See *Passphrases* for more information.
SNMP Read Enable	Checked, Unchecked	Unchecked	Allows the profile to be used for SNMP read access to the SEL-2488.

[a] If Encryption Protocol is enabled, both the Authentication and Encryption passwords must be entered if either is changed or if the Authentication Protocol is changed to a value other than None.
[b] The Encryption Protocol setting is not available if Authentication Protocol = None (which is the default value). To configure Encryption Protocol, Authentication Protocol must first be set to SHA-1 or MD5.

The **Password** and **Confirm Password** fields are data entry points only; these fields do not display the present password. When you enter values in each of these fields, the field represents the characters you enter as bullet placeholders that disappear when you submit the form.

Trap Server Settings

The **Trap Server Settings** tab displays the SNMP trap servers that are currently configured to receive SNMP traps and provides the interface from which you can add a trap server. An SNMP profile is necessary prior to configuring a trap server. The device supports as many as three trap servers.

SNMP trap messages are sent based on the syslog event messaging system of the device. SNMP traps will contain the same data as the syslog messages received on the SEL-2488. The Trap Server setting allows you to set the threshold to determine what messages you will receive. The SNMP trap threshold values for the SEL-2488 are the following, in order from highest to lowest priority:

- Alert
- Critical
- Error
- Warning
- Notice
- Informational

The SEL-2488 allows lower-priority SNMP trap messages to be filtered out based on the threshold setting. The SEL-2488 will only send trap messages with a priority at or above the threshold setting you select. This filtering occurs at the time of the event; changing the threshold setting only affects

future messages and not pre-existing ones. A higher threshold reduces the number of trap messages the SEL-2488 sends to the trap server destinations. This can result in reduced traffic loads, but may also prevent key event notifications from being sent.

Perform the following steps to add a trap server:

Step 1. On the **SNMP Settings** page, navigate to the **Trap Server Settings** tab (shown in *Figure 17.3*). A dialog at the top of this screen reminds the user to select v2c profiles.

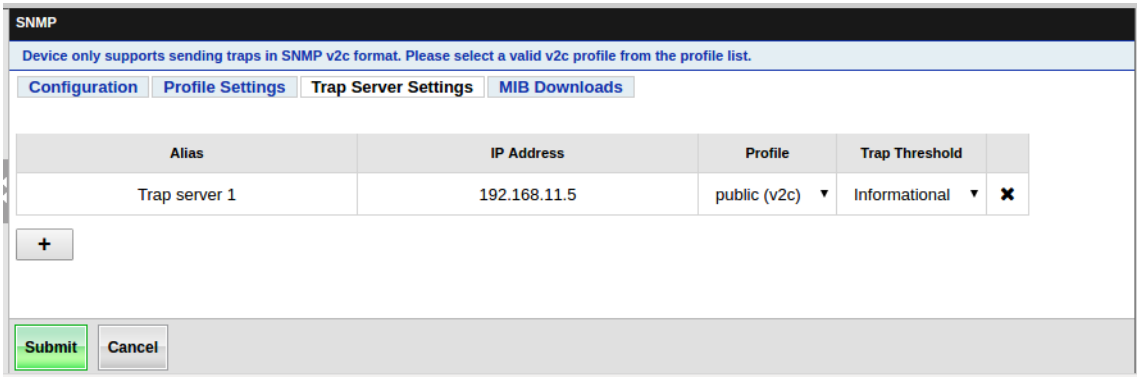


Figure 17.3 SNMP Trap Server Settings Tab

Step 2. Enter the **Alias** and **IP Address** of the trap server to which you want to send SNMP traps.

Step 3. In the **Profile** drop-down list, select your desired SNMP v2c profile.

Step 4. In the **Trap Threshold** drop-down list, select the severity threshold to filter which trap messages are sent to the trap server.

Step 5. Select **Submit** to add the SNMP trap server.

Table 17.2 SNMP Trap Server Settings

Setting Name	Values	Default	Description
Alias	1–128 characters	N/A	A user-configurable name associated with the SNMP trap server.
IP Address	Host IP address	N/A	The IP address of the SNMP trap server.
Profile	A list of SNMP v2c trap profiles	N/A	The SNMP v2c profile whose identity you will use to send traps.
Trap Threshold	See *Trap Server Settings*	Informational	The device will send SNMP traps to the configured trap server when an event occurs within the selected trap category.

To add additional SNMP trap servers, select the plus (+) button below the table. In the new table row, enter the SNMP trap server Alias, IP Address, Profile, and Trap Threshold. To remove an SNMP trap server, select the **X** button on the right side of the trap server that you want to delete, and select **Submit**.

If the user changes an existing v2c profile to a v3 profile, the SEL-2488 will allow the change. However, if there are trap servers associated with that profile, the user will see an alert banner, as shown in *Figure 17.4*.

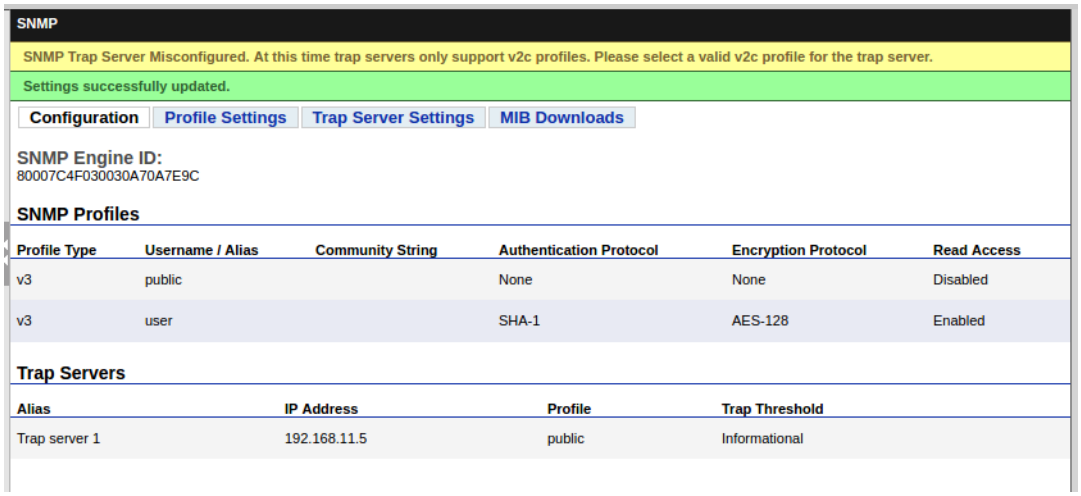


Figure 17.4 SNMP Trap Server Misconfiguration Alert Banner

The user must navigate to the **Trap Server Settings** page and either remove the trap server with the v3 profile or change it to a valid v2c profile (see *Figure 17.5*).

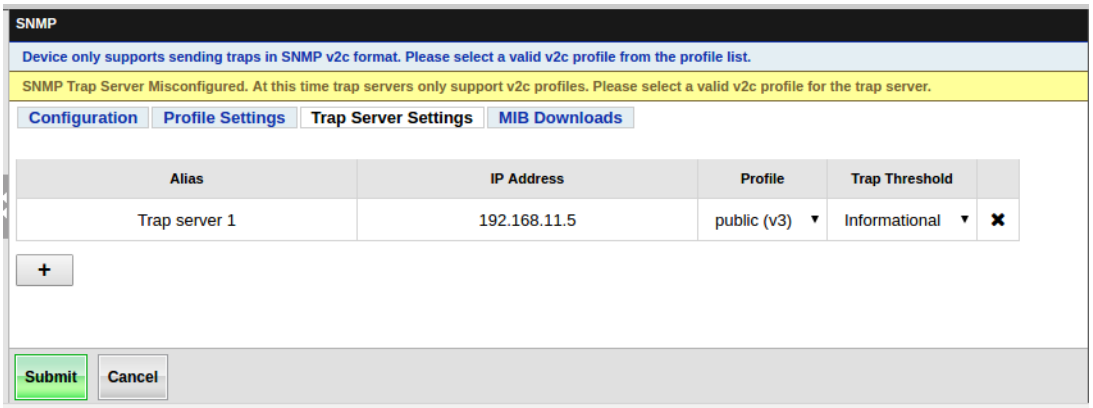


Figure 17.5 SNMP Trap Server Settings Tab Misconfiguration Notification

SNMP Management Information Base

SNMP MIB modules contain definitions and other information about the SNMP implementation on the SEL-2488. The SEL-2488 uses the following MIBs:

- IANAifType-MIB
- IF-MIB
- INET-ADDRESS-MIB
- SEL-2488-DASHBOARD-MIB
- SEL-2488-DEVICE-INFORMATION-MIB
- SEL-2488-DEVICE-DIAGNOSTICS-MIB
- SEL-2488-PORT-STATUS-MIB
- SEL-2488-PTP-DIAGNOSTICS-MIB
- SEL-2488-SATELLITE-STATUS-MIB
- SEL-2488-SYSLOG-X-MIB
- SEL-2488-SYSTEM-STATISTICS-MIB

- SEL-2488-TC-MIB
- SEL-2488-TIME-INPUT-MIB
- SEL-2488-TIME-OUTPUT-MIB
- SEL-DEFINITIONS-MIB
- SEL-PRODUCTS-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMPv2-MIB
- SNMPv2-SMI-MIB
- SNMPv2-TC-MIB
- SYSLOG-MSG-MIB
- SYSLOG-TC-MIB

You can download the SEL-2488 MIBs directly from the SEL-2488.

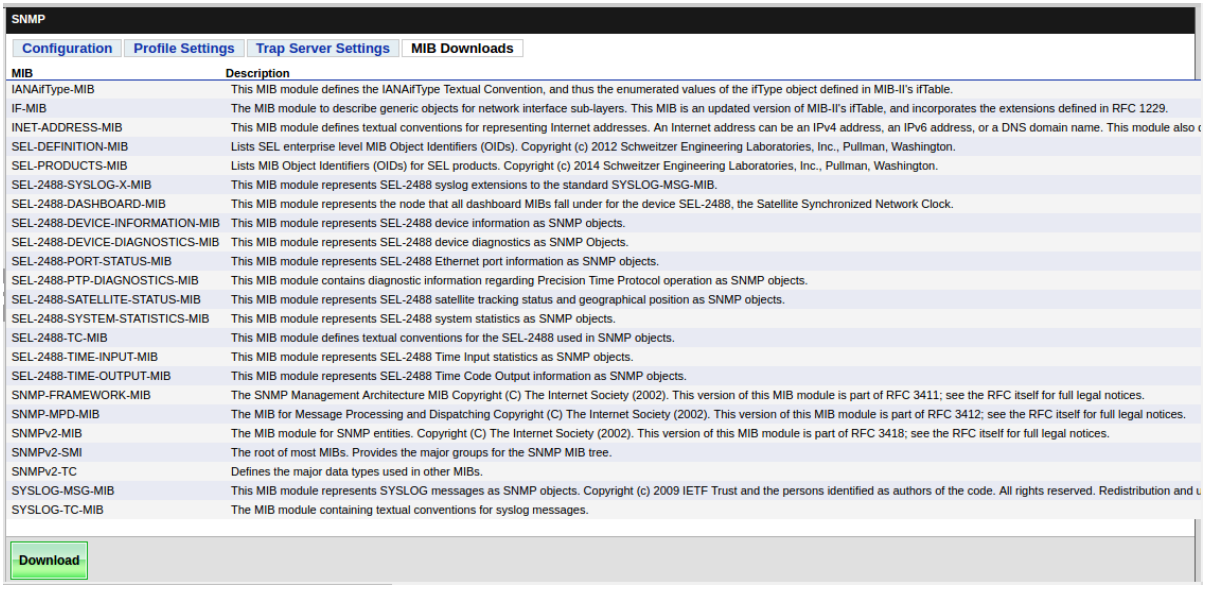


Figure 17.6 SNMP MIB Downloads Tab

The **MIB Downloads** page lists all of the MIBs in use on the SEL-2488 and a brief description of their function.

To download the MIBs from the SEL-2488 (as a .zip file), navigate to the **MIB Downloads** page and select **Download**.

Settings Import Warning—SNMP v3 Profiles

The SEL-2488 allows settings information to be exported and imported back onto the original unit or onto a different unit. This allows configurations to be archived and standardized across multiple units. The SNMP v3 profiles use passwords for the authentication and encryption of v3 messages as part of the protocol. These passwords are encrypted using details specific to the unit when the passwords are set. Importing the settings configuration file back onto the same unit does not cause any issue with these passwords. However, when importing the same file onto a different unit, the stored passwords will not work with the new unit.

To notify the user of the v3 profile issue, the SEL-2488 will trigger a major alarm condition after a settings import if the stored information was created on a different unit. The user will need to re-enter the passwords for the v3 profiles on the SNMP profile page to clear the major alarm condition.

With the release of R105, the DES Encryption Protocol is no longer available. Devices that were using this protocol upon a firmware upgrade will trigger a major alarm condition and require the user to reconfigure the profile. Importing settings that use DES will similarly trigger a major alarm condition and require user interaction.

Front Panel

The front panel does not display any SNMP information.

Dashboard

As described in *Dashboard on page 4.7*, the table below the Ethernet dashboard indicators shows additional information, including whether SNMP read is enabled.

Port	Alias	Media Type	Speed/Duplex	Port Bonding	MAC Address	IP Address	Services/Protocols
ETH 1	Station_Bus	10/100BASE-T	100Mbps Full Duplex	BOND: ETH1,2 (Active)	00:30:a7:14:5a:06	10.203.116.2/24	HTTPS, NTP Server, SNMP
ETH 2	Station_Bus	10/100BASE-T	100Mbps Full Duplex	BOND: ETH1,2 (Backup)	00:30:a7:14:5a:06	10.203.116.2/24	HTTPS, NTP Server, SNMP
ETH 3	Process_Bus	100BASE-FX	100Mbps Full Duplex	PRP: ETH3,4 (LAN A)	00:30:a7:14:5a:08	10.203.117.2/24	NTP Server, PTP
ETH 4	Process_Bus	100BASE-FX	100Mbps Full Duplex	PRP: ETH3,4 (LAN B)	00:30:a7:14:5a:08	10.203.117.2/24	NTP Server, PTP
ETH F	Management	10/100BASE-T	100Mbps Full Duplex	Not Bondable	00:30:a7:14:5a:0a	192.168.1.2/24	Captive Port, HTTPS

Figure 17.7 Ethernet Dashboard Indicators: Additional Information

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications when the user changes SNMP settings. The SEL-2488 replaces message variables in {} with values it logs.

Table 17.3 SNMP Alerts and Notifications (Sheet 1 of 2)

Message	Event Threshold	Alarm Category	Alarm Class
SNMP Trap destination {0} added by {username} at {user_ip}.	Notice	Minor	Configuration
SNMP Trap destination {0} modified by {username} at {user_ip}.	Notice	Minor	Configuration
SNMP Trap destination {0} removed by {username} at {user_ip}.	Notice	Minor	Configuration
SNMP Trap Server Misconfiguration. Trap server will only operate with v2c profiles.	Notice	Minor	Configuration
SNMP Trap Server Misconfiguration Repaired.	Notice	Minor	Configuration

Table 17.3 SNMP Alerts and Notifications (Sheet 2 of 2)

Message	Event Threshold	Alarm Category	Alarm Class
SNMP v2c profile {0} added by {username} at {user_ip}.	Notice	Minor	Configuration
SNMP v2c profile {0} modified by {username} at {user_ip}.	Notice	Minor	Configuration
SNMP v2c profile {0} removed by {username} at {user_ip}.	Notice	Minor	Configuration
SNMP v3 profile {0} added by {username} at {user_ip}	Notice	Minor	Configuration
SNMP v3 profile {0} modified by {username} at {user_ip}	Notice	Minor	Configuration
SNMP v3 profile {0} removed by {username} at {user_ip}	Notice	Minor	Configuration

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

This page intentionally left blank

Section 18
Usage Policy

Overview

The device presents a usage policy to all users accessing the login or commissioning pages. This is a system message that can be changed by the organization. It is designed to notify users regarding what constitutes appropriate use of this device, what actions are necessary to ensure the device is not used inappropriately, and what actions will be taken if abuse is discovered. The device comes with the following default usage policy:

> This system is for the use of authorized users only. Individuals using this system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such activity to law enforcement officials.

Settings

This section discusses the process and restrictions for changing the usage policy. Configure the SEL-2488 Usage Policy via the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **System > Usage Policy** menu option.

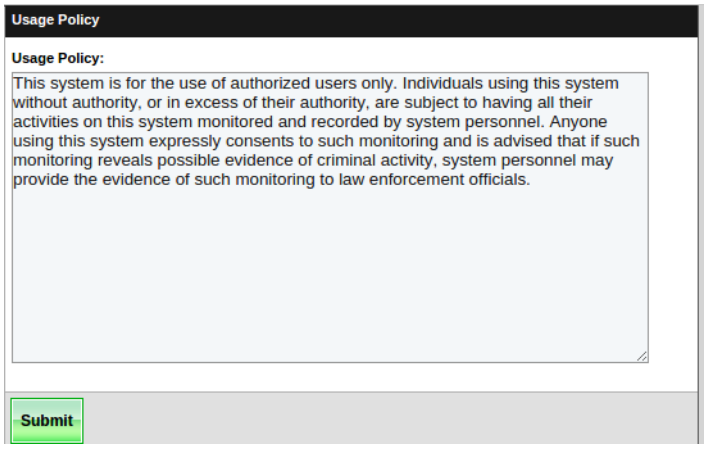


Figure 18.1 Usage Policy Settings Page

The usage policy is configurable to as many as 4095 characters, and it supports all characters in the UTF-8 character set.

Front Panel

The front panel does not display any usage policy information.

Dashboard

The dashboard does not display any usage policy information.

Alerts/Notifications

The SEL-2488 provides the following alert or notification for the event associated with the usage policy. The SEL-2488 replaces message variables in {} with values it logs.

Table 18.1 Usage Policy Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
Usage Policy: changed by {username} at {user_ip}	Notice	Minor	Configuration

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Section 19
Date/Time

Overview

The SEL-2488 allows you to set the local time zone, adjust for daylight-saving time, and manually set the clock through the **Date/Time** page.

Local Time

Use local time settings to define a local time offset from Coordinated Universal Time (UTC). This can include offsets resulting from the time zone setting and daylight-saving time.

Settings

This section discusses the settings that are used to configure local time. Use the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **System > Date > Time** menu option under the **Local Time** tab to configure the SEL-2488 Local Time Settings.

To display local time, set the **Local Time Zone Offset from UTC** and **Daylight Saving Time Mode**.

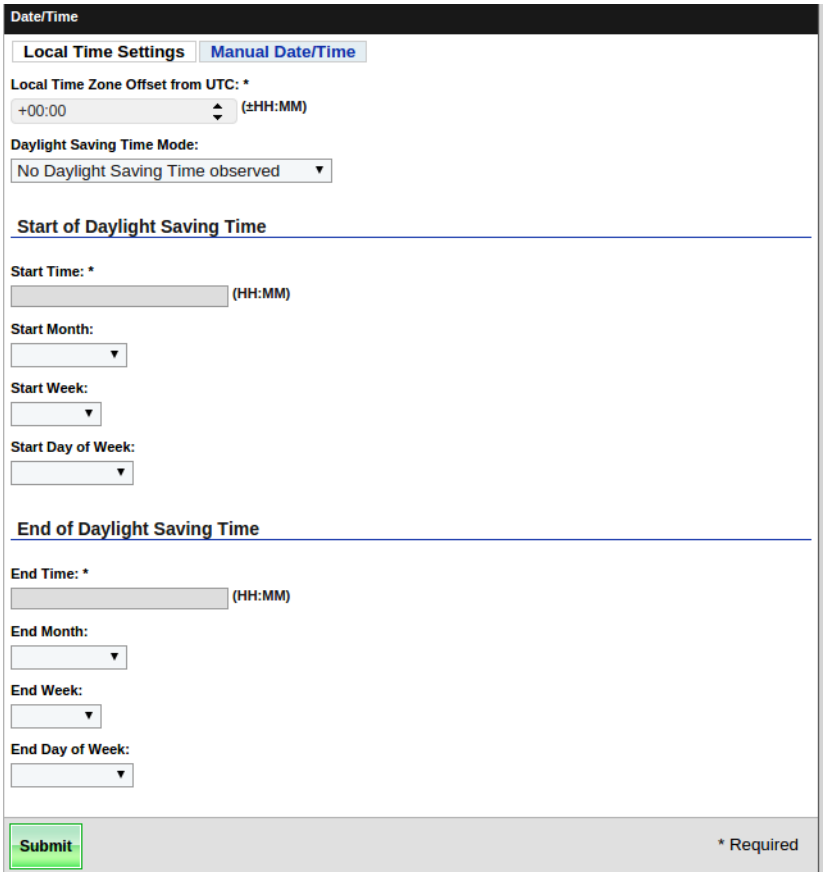


Figure 19.1 Local Time Settings Tab

NOTE: Time changes resulting from DST take effect at the given time in local time in the United States. In the European Union, DST changes are made at the given time in UTC.

The **Start of Daylight Saving Time** and **End of Daylight Saving Time** settings are only configurable if **Daylight Saving Time Mode** is set to **Custom DST**. Otherwise, these settings display the automatic daylight-saving start/end dates for the selected mode. See *Table 19.1* for more information on local time settings.

Table 19.1 Local Time Settings

Setting Name	Values	Default	Description
Local Time Offset from UTC	–13:00 to +13:00	–08:00	Sets local time offset from UTC. Can be set in 30-minute increments.
Daylight Saving Time Mode	No DST, United States, European Union, Custom DST	United States	Sets the DST settings profile for local time.
Start Time	00:00–24:00	02:00	Sets the start time when DST begins.
Start Month	January–December	March	Sets the month when DST begins.
Start Week	First, Second, Third, Fourth, Last	Second	Sets which week of the month DST begins.
Start Day of Week	Sunday–Saturday	Sunday	Sets the day of the week when DST begins.
End Time	00:00–24:00	02:00	Sets the time when DST ends.
End Month	January–December	November	Sets the month when DST ends.
End Week	First, Second, Third, Fourth, Last	First	Sets which week of the month DST ends.
End Day of Week	Sunday–Saturday	Sunday	Sets the day of the week when DST ends.

Front Panel

The front-panel LCD screen displays the time offset from UTC as well as DST and leap second information in the top right portion of the display. During daylight-saving time, the display shows DST. To inform you of a pending DST event, the LCD screen displays a blinking DST indicator during the 24 hours prior to the event. Similarly, the screen displays LSP (leap second pending) for 24 hours prior to a leap-second event.

Figure 19.2 LCD Screen–Local Time Settings

Dashboard

The **Time Input** section of the dashboard shows the local time offset, daylight-saving status, and the time of the next DST event. It will also add an additional line when there is a pending leap-second event indicating the time of the event.

Figure 19.3 Time Input Status Widget–Local Time

Manual Date/Time

Use Manual Date/Time mode for demonstration purposes when a Global Navigation Satellite System (GNSS) source is not available. In this mode, the clock simulates a GNSS connection and transmits the configured Manual Date/Time on all enabled time outputs. For IRIG-B interfaces, the clock sets time quality to 0 (locked to a UTC traceable source). For Precision Time Protocol (PTP) interfaces, the clock will simulate that the time is accurate to <100 ns. Network Time Protocol (NTP) will reflect a Stratum 1 primary server.

The SEL-2488 can only enter Manual Date/Time mode if it has not yet locked to a primary reference (GNSS). If the SEL-2488 starts receiving time through a GNSS source when it is in Manual Date/Time mode, that source will override the Manual Date/Time mode. Additionally, the Manual Date/Time mode will not remain active through the removal and restoration of device power or through a device restart.

Settings

This section discusses the settings necessary for configuring manual date and time. Use the settings interface (in a web browser) through the **System > Date/Time** menu option and navigate to the **Manual Date/Time** tab.

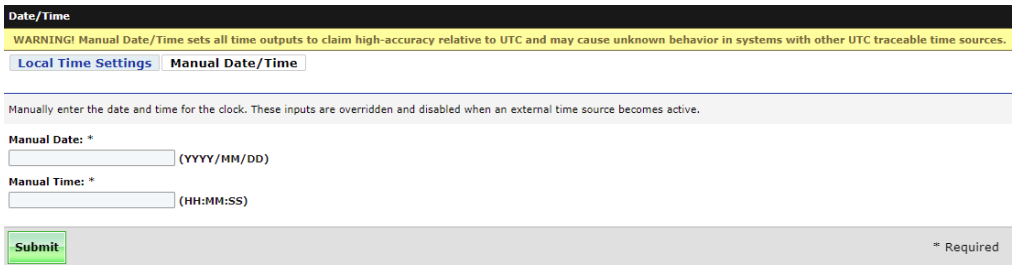


Figure 19.4 Manual Date/Time Settings Tab

Table 19.2 Manual Date/Time Settings

Setting Name	Values	Default	Description
Manual Date	YYYY/MM/DD 2000/01/01–2035/12/31	N/A	Manually sets the date. The date will proceed forward from the date you enter.
Manual Time	HH:MM:SS 00:00:00–23:59:59	N/A	Manually sets the time. Time will proceed forward from this entered time, which must be in 24-hour format.

If the clock is synchronized to a GNSS source, it will not allow you to manually override the time without first disabling the GNSS time source. The following instructions explain how to set the Manual Date/Time for a clock that presently receives time from a GNSS source:

Step 1. Disable the GNSS time source. Navigate to the **GNSS Settings** page on the web interface, clear the **Enable GNSS Time Source** check box, and select **Submit**.

Step 2. Restart or remove and restore power to the device.

Step 3. Log in to the device and go to the **Date/Time** settings page under the **System** settings panel.

Step 4. Navigate to the **Manual Date/Time** tab.

Step 5. Enter the **Manual Date** and **Manual Time** in the format shown next to the settings fields.

Step 6. Select the **Submit** button.

After you have completed the previous steps, the device enters Manual Date/Time mode. In this mode, all time outputs generate time codes corresponding to the manually configured date and time. The front-panel display shows the corresponding date and time.

Once the clock is in Manual Date/Time mode, you can change the date and time freely without restarting the clock.

To exit Manual Date/Time mode, navigate to the **GNSS Settings** page on the web interface, select the **Enable GNSS Time Source** check box, and select **Submit**.

Front Panel

When the SEL-2488 is in Manual Date/Time mode, the **TIME QUALITY** LED is solid green on the device front panel. Because GNSS is disabled, the **SATELLITE LOCK** LED and the **ANTENNA STATUS** LED are turned off.

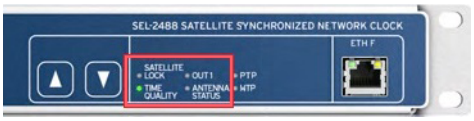


Figure 19.5 Front-Panel LEDs—Manual Date/Time Mode

The time source portion of the LCD screen indicates that the device is in Manual Date/Time with a time quality of <100 ns.

Figure 19.6 LCD Screen—Manual Date/Time Mode

Dashboard

To operate the clock in Manual Date/Time mode, you must disable GNSS. Because GNSS is disabled, the **Satellite Status** section of the dashboard will display no data. The dashboard reflects the status of the front-panel LEDs, with the **Time Quality** LED in green and the **Satellite Lock** and **Antenna** LEDs off.

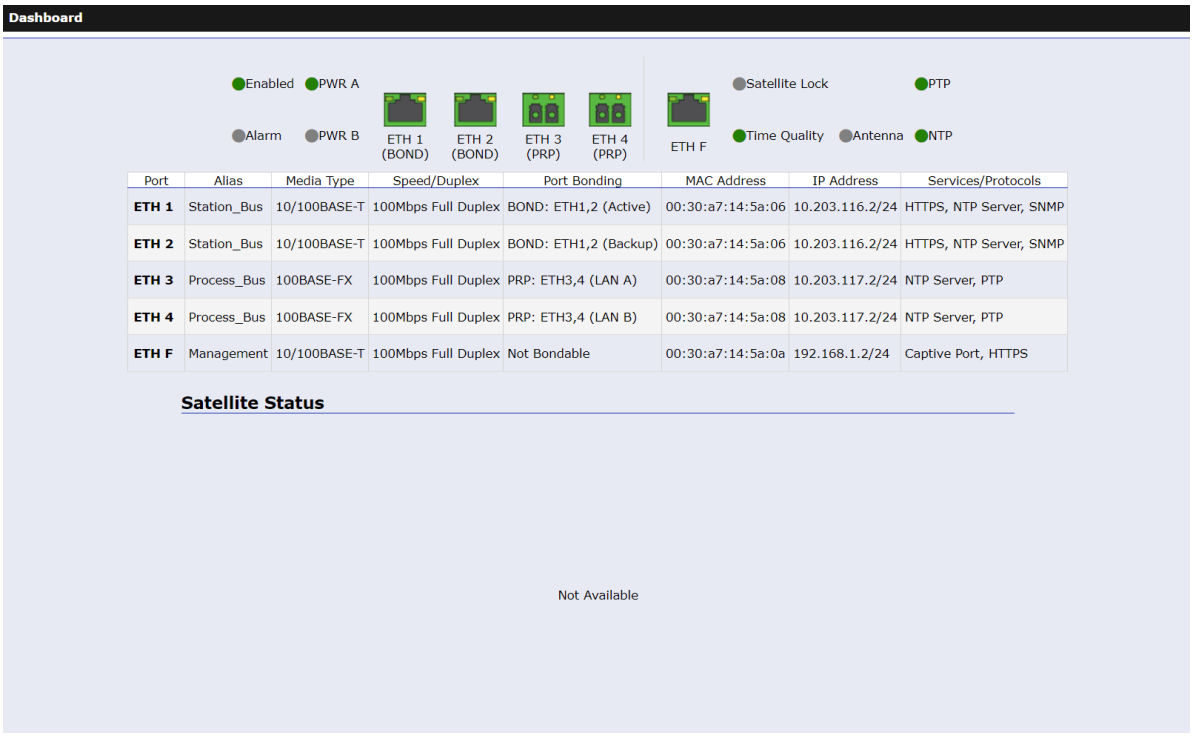


Figure 19.7 Dashboard—Satellite Status When in Manual Date/Time Mode

When the device is in Manual Date/Time mode, the **Time Input** section of the dashboard lists Manual as the source.

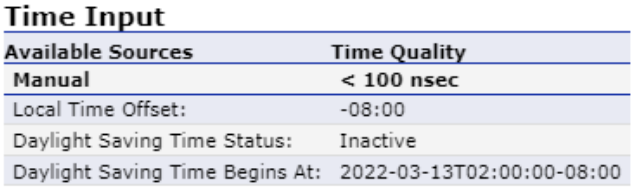


Figure 19.8 Time Input Status Widget—Manual Date/Time Mode

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for the events associated with date and time. The SEL-2488 replaces message variables in {} with values it logs.

Table 19.3 Date/Time Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
Daylight Saving Time adjustment pending.	Notice	None	–
Daylight Saving Time began.	Informational	None	–
Daylight Saving Time ended.	Informational	None	–
Leap Second adjustment pending.	Notice	None	–
Leap Second deleted.	Informational	None	–
Leap Second inserted.	Informational	None	–
Local Time Settings: Changed by {username} at {user_ip}.	Notice	Minor	Configuration
Time set manually by {username} at {user_ip}.	Notice	Minor	Time Synchronization

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Events classified as None will not trigger the alarm contact.

Section 20
Global Settings

Overview

Use the Global settings to customize the settings for the web interface and system contact information.

Settings

This section discusses the available settings you perform via the **Global Settings** page. Configure SEL-2488 Global settings via the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **System > Global Settings** menu option.

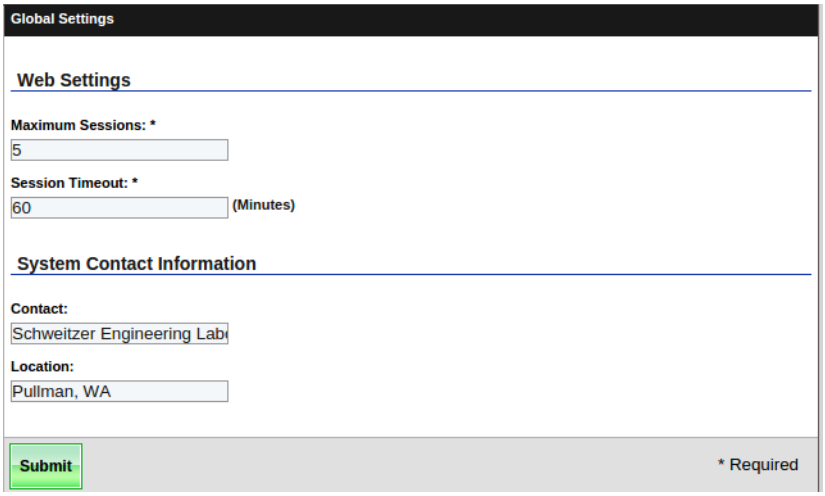


Figure 20.1 Global Settings Page

Web Settings

Use Web Settings to modify settings related to the web management interface of the device. *Table 20.1* lists web settings.

Table 20.1 Web Settings

Setting Name	Values	Default	Description
Maximum Sessions	1–20	5	Maximum number of concurrent web user sessions
Session Timeout	1–60 minutes	5	Time a user session is inactive before the device terminates the session

System Contact Information

The system contact information settings provide fields for entering a system contact and system location.

Table 20.2 System Contact Information Settings

Setting Name	Values	Default	Description
Contact	0–128 characters	Schweitzer Engineering Laboratories, Inc. (509) 332-1890	Contact information for the device
Location	0–28 characters	Pullman, WA	Location of the device

Front Panel

The front panel does not display any Global settings information.

Dashboard

System contact information settings appear in the Device Information portion of the dashboard display.

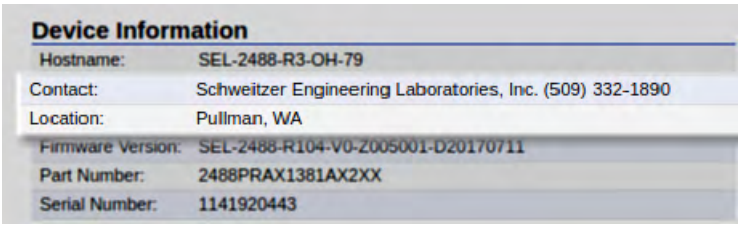


Figure 20.2 Device Information Status Widget—System Contact

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for the events associated with the Global settings. The SEL-2488 replaces message variables in {} with values it logs.

Table 20.3 Global Settings Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
`System Contact Information: changed by {username} at {user_ip}`	Notice	Minor	Configuration
`Web Server Settings: changed by {username} at {user_ip}`	Warning	Minor	Configuration

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Section 21
File Management

Overview

File management provides an interface from which you can import and export settings, as well as perform firmware upgrades and download diagnostics reports. Exporting system settings is useful for providing device configuration backups for disaster recovery, as well as for creating a template configuration that you can use in commissioning large numbers of devices. For example, if all devices share the same configuration, with the exception of a few device-specific settings such as hostname and Internet Protocol (IP) address, you only need to create the configuration once and then export it as a template. Then, once you import the configuration file into a new device, you only need to make minor changes before the device is fully configured.

Export Settings

The settings export functionality is useful for creating a copy of the device configuration as a device backup. You can use this copy for disaster recovery purposes in the event of lost device configuration. Export settings in either encrypted or unencrypted XML formats. The encrypted format provides greater security; the unencrypted option may be more convenient because it allows offline editing.

Perform the following steps to export a settings file.

Step 1. Log in to the device by using an account with the Administrator role.

Step 2. Browse to the **File Management** page. The device defaults to the **Export Settings** tab, as shown in *Figure 21.1*.

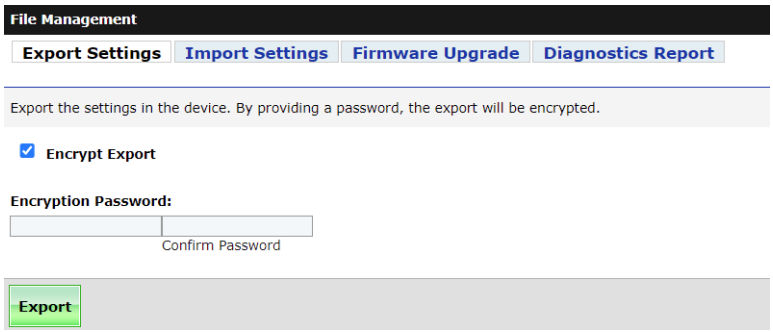


Figure 21.1 Export Settings Tab

Step 3. Choose whether to export the settings in encrypted or unencrypted XML format. To export settings in an encrypted format, leave the **Encrypt Export** check box selected and enter an encryption password for use in encrypting the settings file. You must use a password to perform an import of the encrypted settings file, so be sure you store the password in a secure location. To export in unencrypted format, clear the **Encrypt Export** check box.

NOTE: Store settings files in a secure location, because they contain sensitive information.

Step 4. Select the **Export** button.

Step 5. The settings export initializes and displays the export progress for each module. The device displays the following message when the export is complete.

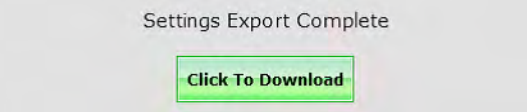


Figure 21.2 Settings Export Complete

Step 6. Select the **Click to Download** button. The device downloads the settings to your local computer.

Import Settings

The **Import Settings** tab provides an interface through which you can import settings from either an encrypted or unencrypted settings file. Perform the following steps to import a settings file:

Step 1. Log in to the device by using an account with the Administrator role.

Step 2. Browse to the **File Management** page and select the **Import Settings** tab, as shown in *Figure 21.3*.

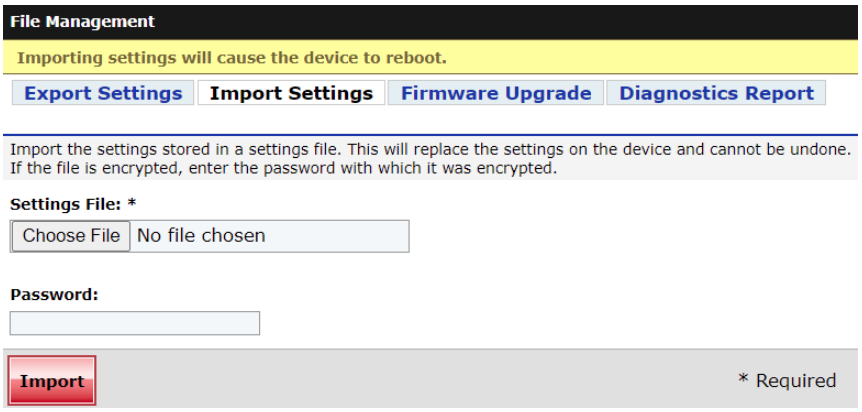


Figure 21.3 Import Settings Tab

CAUTION
With the release of firmware version R102, the SEL-2488 will now verify that the device interface IP addresses do not fall within the same network address range.

If your device is using firmware version R101 or earlier, and has IP addresses for different ports that fall within the same network address range, an upgrade to R102 will cause the settings import to fail and all device settings will revert to the factory-default values.

NOTE: With the release of firmware version R103, the SEL-2488 will trigger a major alarm condition after the settings import process if the configuration file contains SNMP v3 profiles with passwords and it was created on a different SEL-2488. See Settings Import Warning—SNMP v3 Profiles on page 17.7 for additional details.

Before commencing the settings import, SEL advises that you have the current SNMP v3 profile passwords available. You will be required to re-enter them after the import completes to clear the major alarm.

NOTE: Importing settings replaces the present settings and restarts the device.

Step 3. Select the **Choose File** button and browse to the location of the settings file you want to import. Select the file and select **Open**.

Step 4. If the file was encrypted during the export process, enter the encryption password into the **Password** field. If the file was not encrypted during the export process, leave the **Password** field blank.

Step 5. Select the **Import** button.

Once the device successfully imports settings, the following message displays:

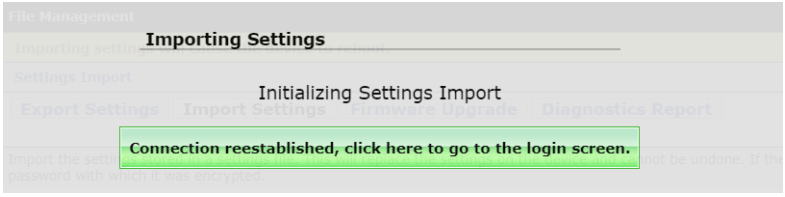


Figure 21.4 Successful Import Message

If there is a problem with the imported file, the following message displays:

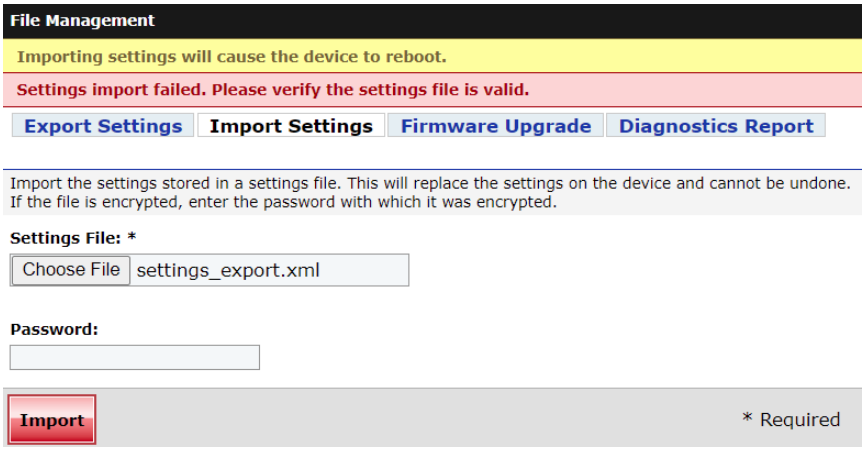


Figure 21.5 Unsuccessful Import Message

Firmware Upgrade Instructions

CAUTION
Firmware downgrades that are allowed may result in the SEL-2488 reverting to factory-default settings after the downgrade completes. SEL advises manually documenting device settings prior to a downgrade, as exported settings from a newer firmware version may not be compatible with older versions.

SEL occasionally offers firmware upgrades to improve the performance of the device. The SEL-2488 stores firmware in nonvolatile memory. These instructions provide a step-by-step procedure for upgrading the device firmware by uploading a file from a personal computer to the device via the web interface. The SEL-2488 logs all firmware upgrades and transfers all existing settings to newer firmware.

You can upgrade the SEL-2488 with the PTP option in the same manner you would use to perform a firmware upgrade. For instructions on adding the PTP option to your SEL-2488, see *Appendix B: Precision Time Protocol Field Upgrade Instructions*.

To perform a firmware upgrade, you need the appropriate firmware upgrade file and access to an administrative account on the device.

Firmware Files

The SEL-2488 firmware upgrade files have a tar.gz file extension. An example firmware filename is **install_2488_R100.tar.gz**.

The firmware packages are cryptographically signed so that the device can recognize official SEL firmware. The device will not process any files it uploads for which it cannot verify SEL as the file creator.

Upgrade Instructions

Perform the following steps to upgrade the SEL-2488 firmware:

Step 1. Log in to the device by using an account with the Administrator role.

Step 2. Browse to the **File Management** page and select the **Firmware Upgrade** tab, which displays the version of the presently running firmware and allows you to choose the upgrade file to upload to the unit (see *Figure 21.6*).

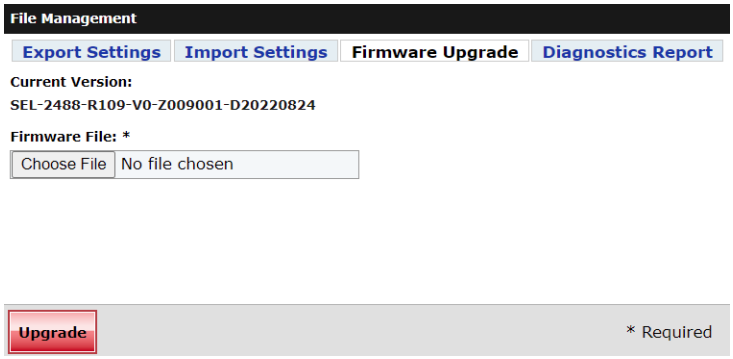


Figure 21.6 Firmware Upgrade Tab

Step 3. Select **Choose File** and navigate to the location where the upgrade file is stored. Select the file and select **Open**.

Step 4. Select the **Upgrade** button to upload and install the new firmware. The device displays `Upgrading Firmware` and periodically updates the progress of the upgrade operation. Completion of a firmware upgrade takes about 10 minutes.

Front Panel

The front-panel LCD screen displays the firmware version on the firmware version screen, as shown in *Figure 21.7*.

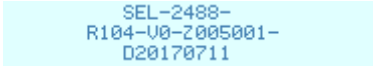


Figure 21.7 Firmware Version Screen

Dashboard

The dashboard displays the current firmware version in the **Device Information** section, as shown in *Figure 21.8*.

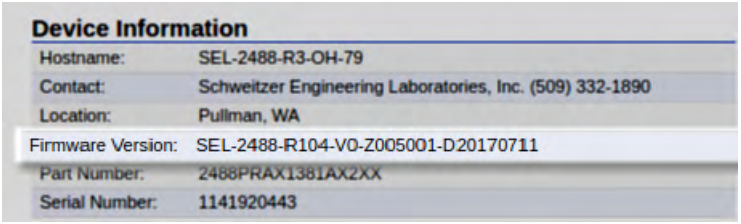


Figure 21.8 Device Information Status Widget—Firmware Version

Diagnostics Report

A diagnostics report provides system status, diagnostics, and crash logs to SEL for analysis. Diagnostic reports are encrypted to protect sensitive information.

Step 1. Log in to the device by using an account with the Administrator role.

Step 2. Browse to the **File Management** page and select the **Diagnostics Report** tab, as shown in *Figure 21.9*.

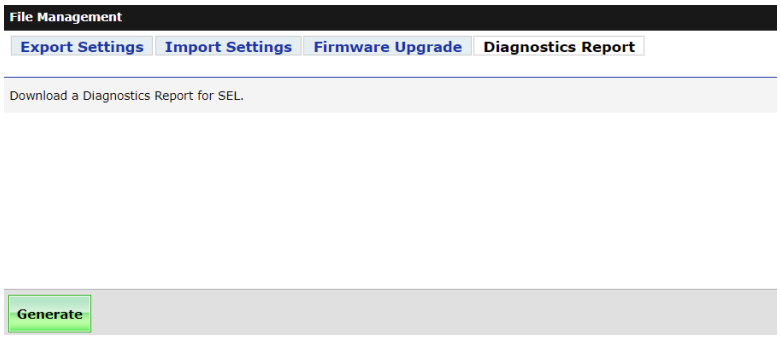


Figure 21.9 Diagnostics Report Tab

Step 3. Select the **Generate** button. The page displays `Generating Diagnostics Report` for less than a minute while the Diagnostics Report initializes.

Step 4. Select the **Click to Download** button (see *Figure 21.10*) to download the hostname_diagnostics.log file that you can share with your SEL representative.

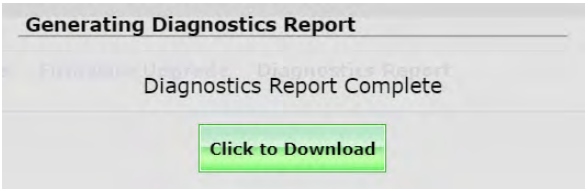


Figure 21.10 Diagnostics Report Complete

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for the events associated with file management. The SEL-2488 replaces message variables in { } with values it logs.

Table 21.1 File Management Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
Configuration file export started by {username} at {user_ip}	Notice	Minor	Configuration
Configuration file export successful	Notice	Minor	Configuration
Configuration file export failed	Warning	Minor	Configuration
Configuration file import started by {username} at {user_ip}	Notice	Minor	Configuration
Configuration file import successful	Notice	Minor	Configuration
Configuration file import failed	Warning	Minor	Configuration
Firmware update from {0} to {1} succeeded	Warning	Minor	Configuration
Firmware update to new version initiated by {username} at {user_ip}	Notice	Minor	Configuration
The firmware update from {0} to new version failed with an error of "{1}". Please contact Schweitzer Engineering Laboratories, Inc. for assistance	Critical	Major	–
The firmware version downgrade is not compatible with the current firmware	Error	Minor	Configuration
Uploaded firmware update package is corrupted; unable to either decrypt the firmware update package or validate the signature on the firmware update package	Error	Minor	Configuration
Diagnostic Report generated by {username} at {user_ip}	Notice	Minor	–

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Events classified as Major will latch the alarm contact.

Section 22
LCD Screen

Overview

The front-panel liquid crystal display (LCD) screen displays time, time source and accuracy, device information, location, satellite status information, and major event messages. You can scroll through the screens by pressing the **Up** and **Down** buttons.

Settings

This section discusses the settings that customize and affect the operation of the LCD screen. Use the settings interface (in a web browser or ACSELERATOR QuickSet SEL-5030 Software) through the **System > Front Panel** menu option to configure the SEL-2488 LCD screen.

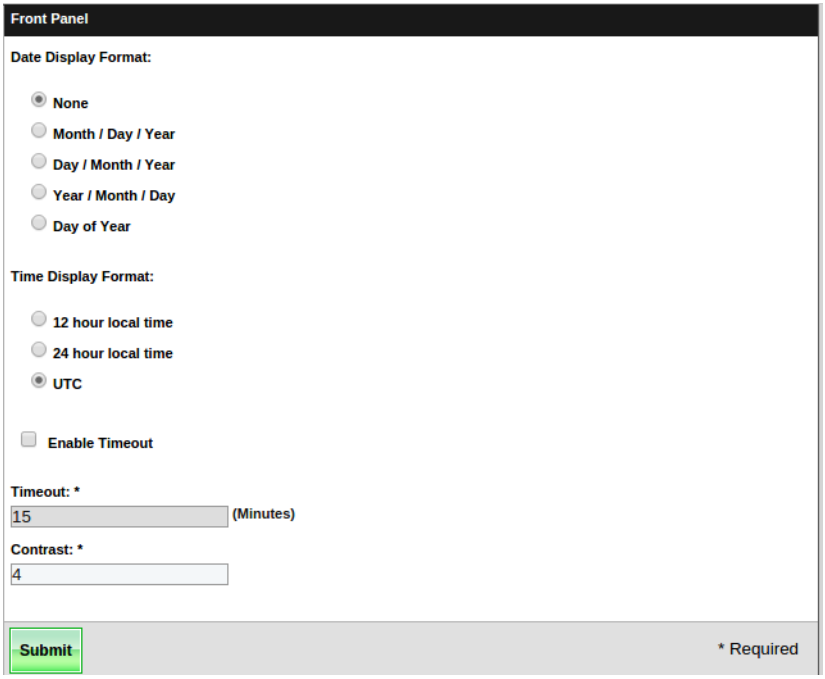


Figure 22.1 Front-Panel Settings Page

Table 22.1 Front-Panel Settings

Setting Name	Values	Default	Description
Date Display Format	None Month/Day/Year Day/Month/Year Day of Year	None	Determines whether the date is displayed and what format it is in.
Time Display Format	12-hour local time 24-hour local time UTC	12-hour local time	Displays the time on the front panel in 12/24 hour format. UTC is Coordinated Universal Time displayed in 24-hour format.
Enable Timeout	Checked, Unchecked	Checked	Enables or disables front-panel display timeout as a result of inactivity. If no front-panel activity occurs for a set duration, the backlight automatically turns off and the display returns to the Time Screen (see *Figure 22.2*).
Timeout	1–30 minutes	15	Sets the duration after which the front-panel timeout occurs.
Contrast	1–8	4	Sets the contrast of the front-panel LCD.

Front-Panel Contrast Adjustment

You can also adjust LCD screen contrast via the front panel by pressing and holding the **Up** and **Down** arrows simultaneously for five seconds. Then press the **Up** and **Down** arrows to set the contrast to values one through eight, with one being the lowest contrast and eight being the highest contrast.

Front Panel

Primary Screens

The SEL-2488 has five primary LCD screens that you can access by using the front-panel **Up** and **Down** arrows. Descriptions of the five screens follow.

Time

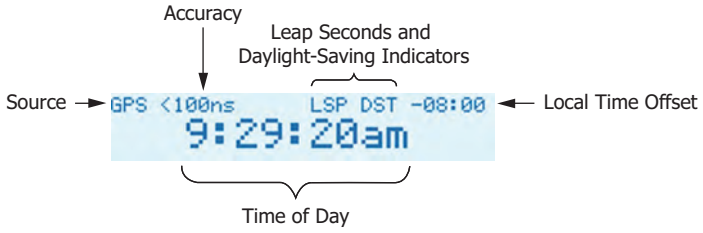


Figure 22.2 Time Screen LCD

The default display is the Time Screen (*Figure 22.2*). By default, the time display shows the local time in 12-hour format.

The upper left-hand corner of this screen shows which source the SEL-2488 is using. Available sources are GPS, Holdover, Manual, and None. After the device achieves satellite lock, it displays `GPS` as the source. In the event it loses satellite lock, the device displays `Holdover`. If you disable GNSS and have the device in Manual Date/Time mode, the device displays `Manual`.

To the right of the source, the device displays the accuracy of the clock relative to UTC.

The Time Screen displays `DST` during daylight-saving time and flashes `DST` in the 24 hours prior to a DST event. It displays `LSP` when a leap second is pending, beginning 24 hours before the leap second takes place.

In the top right corner, the device displays the local time offset from UTC.

Firmware Version

Pressing the **Down** arrow once makes the device display the firmware version (see *Figure 22.3*). This screen provides easy access to information identifying the firmware version running on the clock.

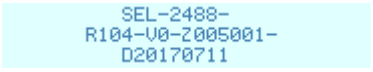


Figure 22.3 Firmware Version LCD Screen

Location

The next screen in the sequence displays antenna location information (see *Figure 22.4*). When locked to GPS satellites, the SEL-2488 displays the present GPS location of the device. If not locked, this screen displays the last known location of the device. This screen is only visible when GNSS is enabled.

Figure 22.4 Location LCD Screen

Serial and Part Number

The following screen in the sequence displays the current device serial number and part number for the SEL-2488 (see *Figure 22.5*). This provides a convenient way to verify the device part number and serial number from the front panel.

Figure 22.5 Serial and Part Number LCD Screen

ETH F Information

Figure 22.6 shows the subsequent screen, which displays information about the present configuration of the front Ethernet port. The top line shows whether **ETH F** is enabled. The second line shows the Internet Protocol (IP) address of the management interface. The last line shows whether Captive Portal is enabled.

Figure 22.6 ETH F LCD Information Screen

Satellite Information

Figure 22.7 displays the number of all visible and used satellites the SEL-2488 is tracking. The SEL-2488 can track GPS and GLONASS satellite constellations simultaneously.

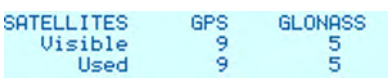


Figure 22.7 Front-Panel Satellite Information LCD Screen

Startup Sequence

Upon application of power to the device, the front-panel LCD keeps you informed about the initialization process as it looks to qualify a time source. The process involves four steps: time source search, time source stability check, time synchronization, and UTC information acquisition.

Major Event Screens

When a major event occurs, the clock notifies the user via the LCD screen. The notifications are designed to alert you to the presence of any unexpected issues and to help you troubleshoot problems. During a major event, the LCD screen remains backlit until you acknowledge or clear the event and its associated alarm.

Figure 22.8 Example Major Event LCD Sample Screen

Dashboard

The dashboard does not display any information related to the LCD screen.

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for events associated with the front-panel LCD screen. The SEL-2488 replaces message variables in {} with values it logs.

Table 22.2 LCD Screen Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
Front Panel Contrast: Changed by user at Front Panel.	Notice	None	Configuration
Front Panel Settings: Changed by {username} at {user_ip}.	Notice	None	Configuration

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

Events classified as None will not trigger the alarm contact.

Section 23
Device Reset

Overview

The SEL-2488 has two options for resetting/rebooting the device. You can choose to perform a basic device reboot or a factory-default reset.

Device Reboot

The device reboot function performs a warm restart on the device, similar to the **<Ctrl+Alt+Del>** function on a computer. The SEL-2488 restarts its time acquisition process after the device reboots.

Use the **System > Device Reset** menu option through the web interface to perform device reboots.

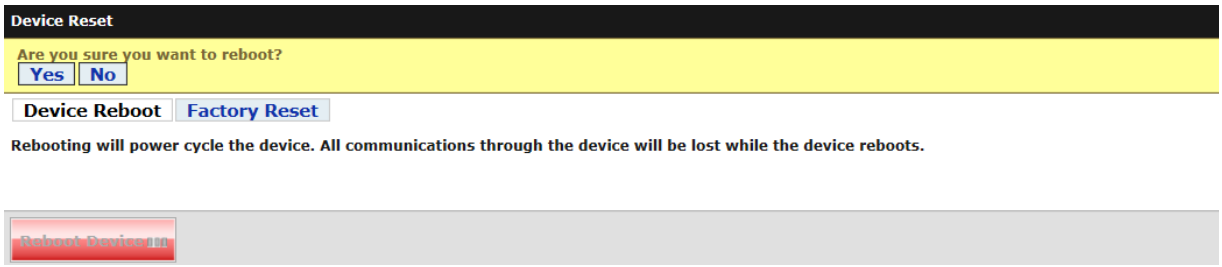


Figure 23.1 Device Reboot Tab

Factory-Default Reset

A factory-default reset restores the unit to its factory configuration. Performing a factory-default reset decommissions the SEL-2488. The factory-reset function erases the log files in the device and returns device settings back to factory-default values. You can use the same **Device Reset** menu option as for a device reboot to perform a factory-default reset.

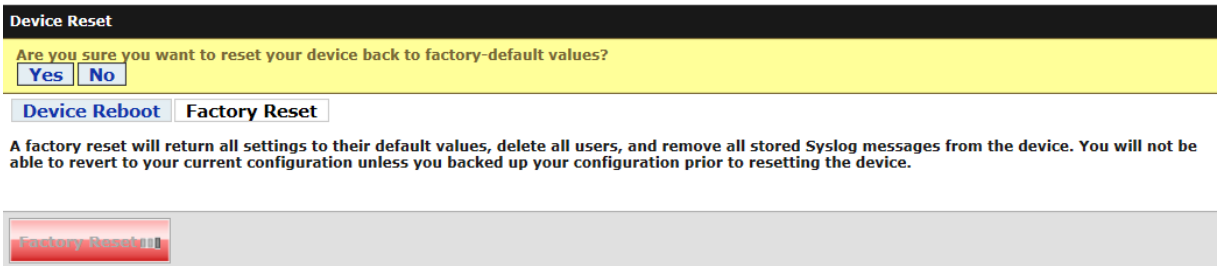


Figure 23.2 Factory-Default Reset Tab

Lost Password/ Pinhole Reset

If the login credentials for all accounts with the Administrator or User Manager role are lost, you must perform a factory-default reset of the device by using the pinhole reset option.

To manually perform a factory-default reset, disconnect power to the SEL-2488. Insert a tool such as a straightened paper clip into the pinhole reset located between the alarm contact and the BNC connectors on the rear panel, and press the recessed reset button. Keeping the button depressed, apply power. After five seconds, release the reset button.

Wait for the green **ENABLED** LED on the front panel to illuminate, indicating that the SEL-2488 has reset to factory-default settings and is ready. **ETH F** will be enabled, the Captive Port feature will be on, and the Internet Protocol (IP) address for the unit will be 192.168.1.2. After you perform a factory-default reset, you must recommission the device before it can be used. Refer to *Getting Started on page 1.4* for details on commissioning the device.

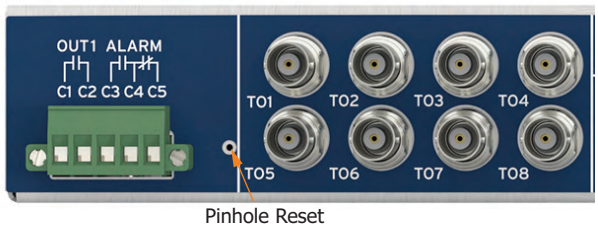


Figure 23.3 Location of Pinhole Reset

Hardware Watchdog Reset

If the device detects a stalled process, it restarts that process and provides notification, via the event reporting system, that the hardware watchdog performed a device reset.

Settings

There are no settings related to resetting the device. After a factory-default reset, all settings within the SEL-2488 change to their default values.

Front Panel

During a device restart/reset, the front panel temporarily turns off and then back on along with the rest of the clock. The clock then goes through its typical initialization sequence.

Dashboard

During a device reboot, the web interface notifies you of the progress of the reboot. Once the reboot is complete and the connection is reestablished, the device prompts you to select the link to return to the login screen.

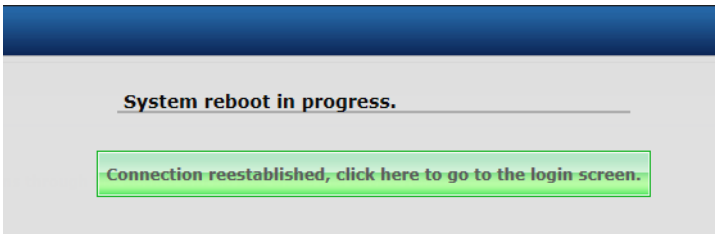


Figure 23.4 System Reboot Screen

A factory-default reset restores the unit to its factory configuration, which disables all rear Ethernet ports, generates a new unique default self-signed X.509 certificate, and resets ETH F to 192.168.1.2 with the Captive Port feature enabled. These changes will likely not allow for the web session to automatically reconnect, therefore it is recommended to manually navigate to https://192.168.1.2 using ETH F.

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for the events associated with resetting the device. The SEL-2488 replaces message variables in {} with values it logs.

Table 23.1 Device Reset Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
Device factory reset initiated by {username} at {user_ip}	Notice	None	–
Device factory reset initiated through pinhole button	Notice	Minor	Chassis
Device rebooted by {username} at {user_ip}	Error	Minor	Chassis
Device reset because of hardware watchdog	Critical	Minor	Chassis

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Events classified as None will not trigger the alarm contact.

Section 24

Parallel Redundancy Protocol (PRP)

Overview

PRP is an industry standard protocol (IEC 62439-3:2016) for duplicating Ethernet traffic across two separate LAN topologies to provide redundancy. The SEL-2488 supports PRP functionality for two separately configurable PRP interfaces. You can directly connect the PRP interface to each LAN of a PRP network and provide redundancy for PTP, NTP, management, and reporting.

Operation

The SEL-2488 offers as many as two independent PRP interfaces that use the four rear-panel physical Ethernet ports. You can combine **ETH 1** and **ETH 2** for one PRP interface and **ETH 3** and **ETH 4** for another, separate PRP interface. When enabled, both of the physical Ethernet ports use the Ethernet MAC address of the lower port number (i.e., **ETH 1** for **ETH 1** and **ETH 2**; **ETH 3** for **ETH 3** and **ETH 4**).

A PRP network consists of two separate LANs named **LAN A** and **LAN B**, which operate in parallel. When PRP is enabled, the SEL-2488 will consider connections to the lower port number of a PRP interface (**ETH 1** or **ETH 3**) to be **LAN A**, and the higher number port (**ETH 2** or **ETH 4**) to be **LAN B**. The PRP link status events will reflect this terminology.

A Singly Attached Node (SAN) is a device that is not capable of PRP functionality and is connected to a single LAN of a PRP network (**LAN A** or **LAN B**). When PRP is enabled, the SEL-2488 PRP interface can communicate with both DANP and SAN devices simultaneously when connected to both LANs of a PRP network.

The configuration of PRP on the SEL-2488 consists of two parts. The first is the basic PRP configuration found on the **Network Management > Port Bonding** page. The second is the network configuration and services found on the **Network Management > IP Configuration** page.

The user enables PRP and adjusts (if required) protocol-specific values for supervision frames and frame waiting periods on the **Port Bonding** page. The default protocol-specific values will work with most installations. The user should change these values only to match configuration requirements for the overall PRP network.

When PRP is enabled, the SEL-2488 removes the individual configuration interfaces for the two physical Ethernet ports on the **IP Configuration** page and replaces them with a single PRP interface. A user can then enable the PRP interface to configure the IP address and control web, NTP, and SNMP

services. Disabling PRP restores the individual physical Ethernet port interfaces and removes the PRP interface. In addition, the **PTP**, **NTP**, and **Static Routes** pages will reflect the changes in the available interfaces.

Configuration Warning—Disruptive Event

Configuring PRP on the SEL-2488 is a *disruptive event*. When enabling PRP, the existing configurations for the physical Ethernet interfaces are removed and the new configuration for the combined PRP interface sets all configurations to default values and disables them. If the user is configuring the clock by using a connection to a rear-panel physical Ethernet port and attempts to enable a PRP interface that uses the same port, they will lose the connection to the clock.

The recommended practice is to configure PRP from a computer directly connected to the front-panel Ethernet management port (ETH F). This maintains an operational interface during PRP configuration as required by IP configuration rules.

Settings

To enabled PRP, use the settings interface in a web browser through the **Network Management > Port Bonding** menu option and select PRP as the Bonding Mode. In ACSELERATOR QuickSet SEL-5030 Software, use the **Network Management > PRP** menu option to enable PRP.

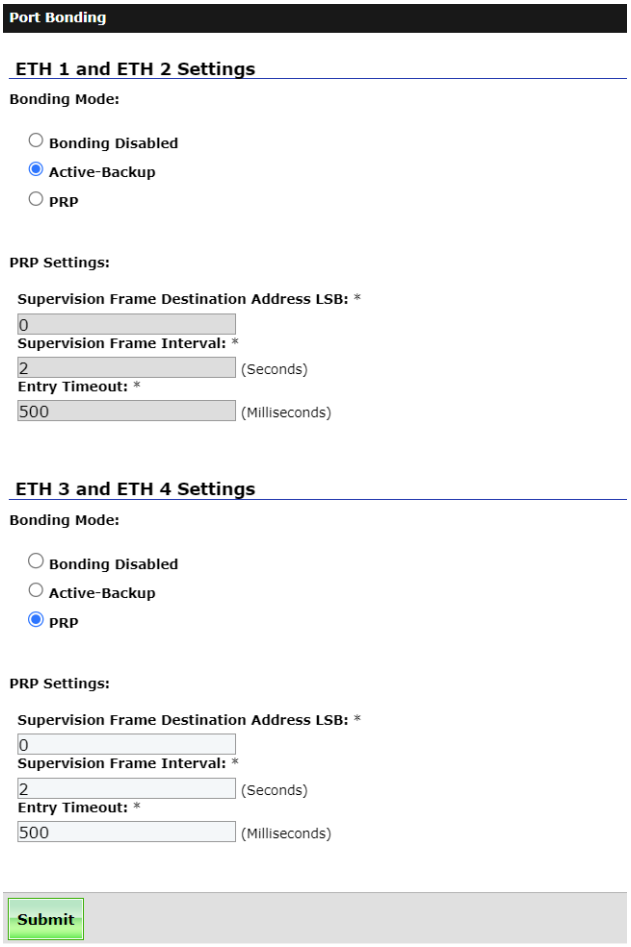


Figure 24.1 Port Bonding Settings Page

When you select the PRP radio button in **Network Management > Port Bonding**, the PRP specific settings become editable and you can configure them.

Table 24.1 PRP Specific Settings

Settings Name	Values	Default	Description
Bonding Mode	Bonding Disabled, Active-Backup, PRP	Bonding Disabled	Selects the Bonding Mode for physical Ethernet ports ETH 1 and ETH 2 or ETH 3 and ETH 4. With Active-Backup mode (also called Failover), only one port is active at a time. With PRP mode, both ports are active simultaneously per IEC 62439-3:2016.
Supervision Frame Destination Address LSB	0–255	0	The least significant byte (LSB) of the multicast destination MAC address for the PRP Supervision frames, i.e., XX in 01-15-4E-00-01-XX.
Supervision Frame Interval	1–10 seconds	2	The transmit interval for the PRP Supervision frames.
Entry Timeout	100–10000 ms	500	The duration the device will wait for a corresponding duplicate to arrive of a received PRP Ethernet frame before forgetting the frame entry from the internal duplicate matching table.

Once PRP is enabled, the PRP interface IP address and network services are managed through the **Network Management > IP Configuration** menu option. The **IP Configuration** page reflects a PRP interface after enabling PRP. In addition, this removes the individual physical Ethernet interfaces from the page. To complete the PRP configuration, navigate to the **IP**

Configuration page, assign the IP address, and enable the interface and services required on the PRP interface. See *Section 4: Ethernet Network Interfaces* for information on configuring Ethernet services.

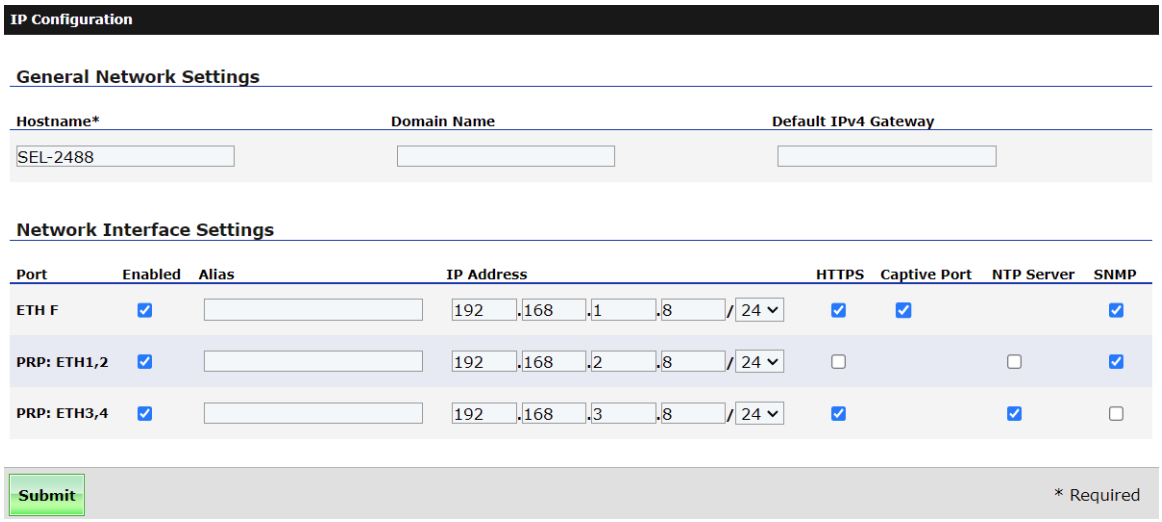


Figure 24.2 IP Configuration Page: Both PRP Interfaces Enabled

Similarly, the **Static Routes** (*Figure 24.3*), **PTP** (*Figure 24.4*), and **NTP** (*Figure 24.6*) settings pages will reflect the changes in the available interfaces as shown. See *Section 5: Static Routes*, *Section 7: Precision Time Protocol (PTP)*, and *Section 8: Network Time Protocol (NTP)* for more information on the settings for each within these pages.

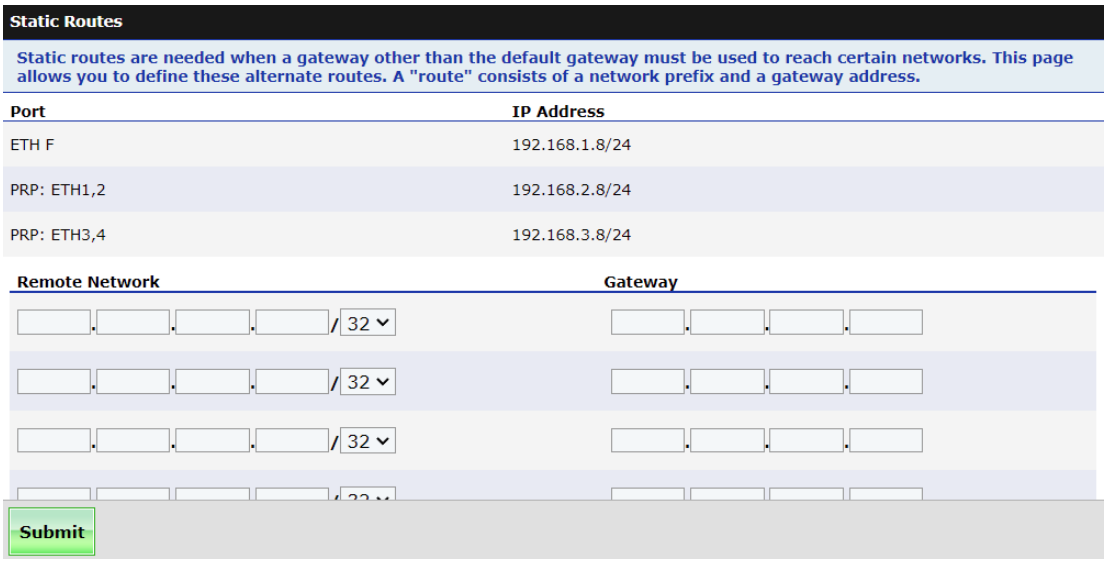


Figure 24.3 Static Routes Settings Page: Both PRP Interfaces Enabled

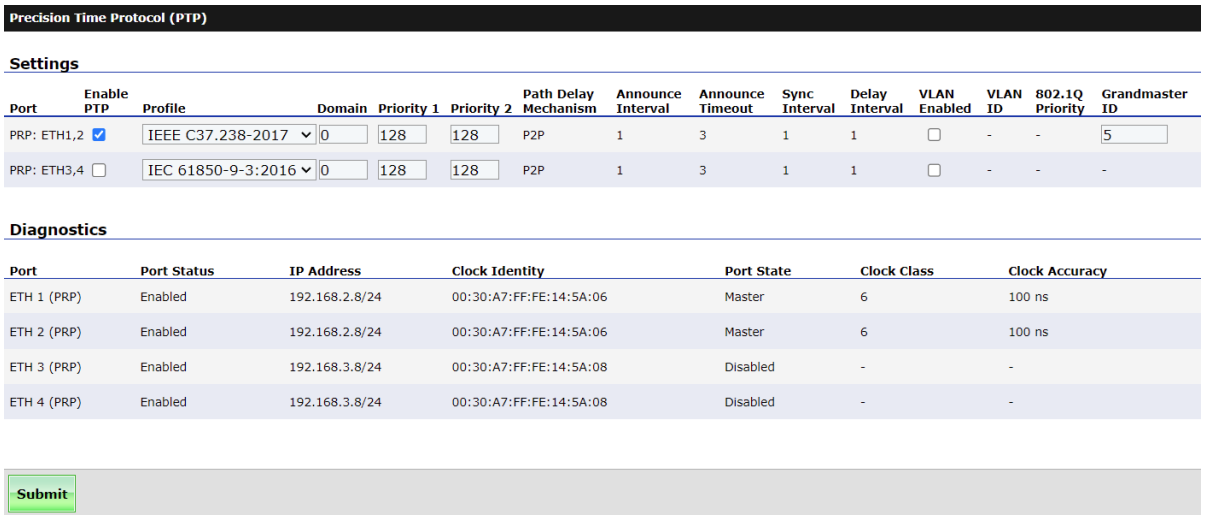


Figure 24.4 PTP Settings Page: Both PRP Interfaces Enabled

The PTP status widget displays ports with PRP enabled with the additional label (**PRP**) next to the port identifier, as shown in *Figure 24.5*.

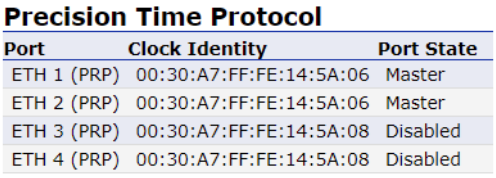


Figure 24.5 Precision Time Protocol Status Widget: Both PRP Interfaces Enabled

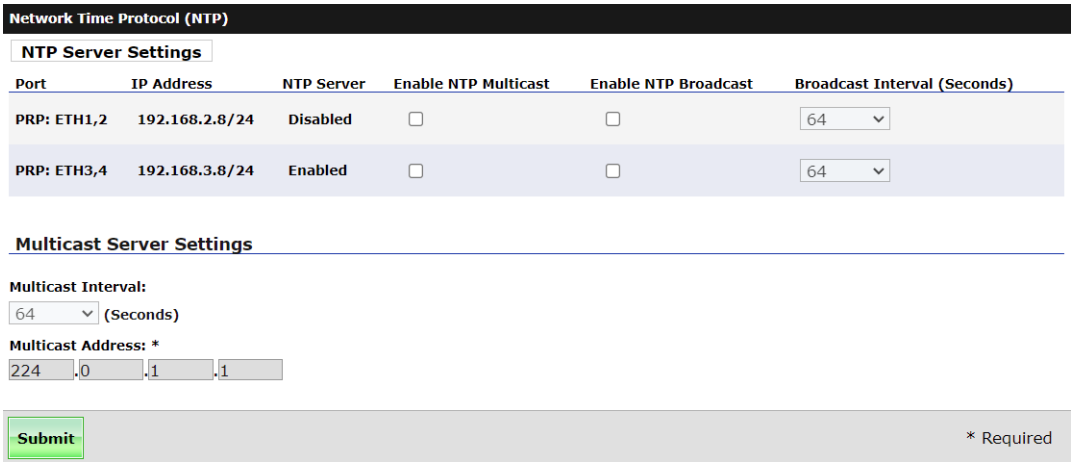


Figure 24.6 NTP Settings Page: Both PRP Interfaces Enabled

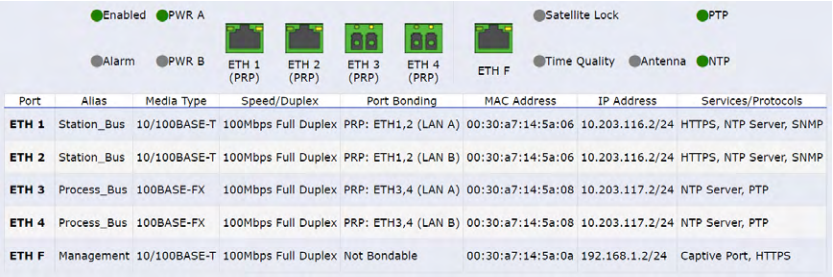
Front Panel

The front panel does not display any PRP information.

Dashboard

The Ethernet dashboard indicators reflect the status of PRP on the device. When PRP is enabled, the label below the icon includes the text **(PRP)** as shown in *Figure 24.7*. This display provides a quick visual indicator of the health of the connections to the PRP network.

Within the table shown below the Ethernet dashboard indicators is a Port Bonding column that displays PRP configuration information when PRP is enabled.



Port	Alias	Media Type	Speed/Duplex	Port Bonding	MAC Address	IP Address	Services/Protocols
ETH 1	Station_Bus	10/100BASE-T	100Mbps Full Duplex	PRP: ETH1,2 (LAN A)	00:30:a7:14:5a:06	10.203.116.2/24	HTTPS, NTP Server, SNMP
ETH 2	Station_Bus	10/100BASE-T	100Mbps Full Duplex	PRP: ETH1,2 (LAN B)	00:30:a7:14:5a:06	10.203.116.2/24	HTTPS, NTP Server, SNMP
ETH 3	Process_Bus	100BASE-FX	100Mbps Full Duplex	PRP: ETH3,4 (LAN A)	00:30:a7:14:5a:08	10.203.117.2/24	NTP Server, PTP
ETH 4	Process_Bus	100BASE-FX	100Mbps Full Duplex	PRP: ETH3,4 (LAN B)	00:30:a7:14:5a:08	10.203.117.2/24	NTP Server, PTP
ETH F	Management	10/100BASE-T	100Mbps Full Duplex	Not Bondable	00:30:a7:14:5a:0a	192.168.1.2/24	Captive Port, HTTPS

Figure 24.7 Ethernet Dashboard Indicators: Both PRP Interfaces Enabled

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for events associated with PRP. The SEL-2488 replaces message variables in { } with values it logs.

Table 24.2 PRP Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
`LAN A of {prp_interface} is down`	Warning	Minor	Link
`LAN B of {prp_interface} is down`	Warning	Minor	Link
`LAN A of {prp_interface} is restored`	Notice	Minor	Link
`LAN B of {prp_interface} is restored`	Notice	Minor	Link
`PRP Settings: changed by {username} at {user_ip}`	Notice	Minor	Configuration

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Section 25
Active-Backup Port Bonding

Overview

Active-backup port bonding is a method for combining two physical Ethernet ports into a single network interface with only one port active while the other serves as a failover backup. The SEL-2488 supports two independent active-backup bonded interfaces. You can directly connect the two physical Ethernet ports of the bonded interface to separate locations within the same LAN to provide Ethernet failover for PTP, NTP, management, and reporting.

Operation

The SEL-2488 offers as many as two independent active-backup bonded interfaces that use the four rear-panel physical Ethernet ports. You can combine ETH 1 and ETH 2 for one bonded interface and ETH 3 and ETH 4 for another, separate bonded interface. When enabled, both of the physical Ethernet ports use the Ethernet MAC address of the lower port number (i.e., ETH 1 for ETH 1 and ETH 2; ETH 3 for ETH 3 and ETH 4).

Active-backup port bonding logically combines two physical Ethernet ports into a single network interface with only one port active while the other serves as a failover backup. Failover from the active port to the backup port occurs only if the active port fails resulting in a link down event. When a failover occurs, the backup port becomes the new active port and issues one or more gratuitous ARPs, allowing external networked devices to learn the new physical port location of the IP/MAC address of the bonded interface within the network. The user can determine which port of the bonded interface is currently active and which one is the backup via the Port Bonding column within the table below the Ethernet indicator icons on the dashboard.

Active-backup port bonding provides fault tolerance for the two direct Ethernet connections of the bonded interface. For network redundancy beyond the immediate Ethernet connections, other redundancy protocols such as the Spanning Tree Protocol (STP) can be externally applied between network switching devices.

The configuration of active-backup port bonding on the SEL-2488 consists of two parts. The first is the basic configuration found on the **Network Management > Port Bonding** page. The second is the network configuration and services found on the **Network Management > IP Configuration** page.

When active-backup port bonding is enabled, the SEL-2488 removes the individual configuration interfaces for the two physical Ethernet ports on the **IP Configuration** page and replaces them with a single bonded interface. A user can then enable the bonded interface to configure the IP address and

control web, NTP, and SNMP services. Disabling active-backup port bonding restores the individual physical Ethernet port interfaces and removes the bonded interface. In addition, the **PTP**, **NTP**, and **Static Routes** pages will reflect the changes in the available interfaces.

Configuration Warning-Disruptive Event

Configuring active-backup port bonding on the SEL-2488 is a disruptive event. When you enable active-backup port bonding, the existing configurations for the physical Ethernet interfaces are removed and the new configuration for the combined active-backup port bonded interface sets all configurations to default values and disables them. If the user is configuring the clock by using a connection to a rear-panel physical Ethernet port and attempts to enable an active-backup port bonded interface that uses the same port, they will lose the connection to the clock.

The recommended practice is to configure active-backup port bonding from a computer directly connected to the front-panel Ethernet management port (**ETH F**). This maintains an operational interface during active-backup port bonding configuration as required by IP configuration rules.

Settings

To enable active-backup port bonding, use the settings interface in a web browser through the **Network Management > Port Bonding** menu option and select Active-Backup as the Bonding Mode. In ACSELERATOR QuickSet SEL-5030 Software, use the **Network Management > Active Backup** menu option to enable active-backup port bonding.

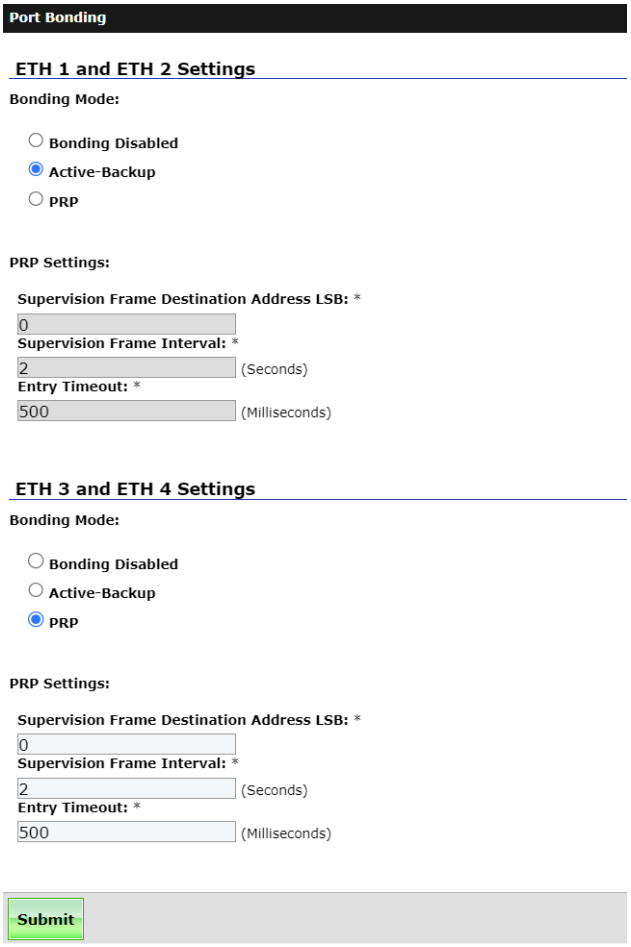


Figure 25.1 Port Bonding Settings Page

Table 25.1 Active-Backup Port Bonding Settings

Settings Name	Values	Default	Description
Bonding Mode	Bonding Disabled, Active-Backup, PRP	Bonding Disabled	Selects the bonding mode for physical Ethernet ports **ETH 1** and **ETH 2** or **ETH 3** and **ETH 4**. In Active-Backup mode (also called Failover), only one port is active at a time. In PRP mode, both ports are active simultaneously per IEC 62439-3:2016.

The IP Configuration page reflects a bonded interface after enabling active-backup port bonding. In addition, this removes the individual physical Ethernet interfaces from the page. To complete the active-backup port bonding configuration, navigate to the IP Configuration page, assign the IP address, and enable the interface and services required on the bonded interface. See *Section 4: Ethernet Network Interfaces* for information on configuring Ethernet services.

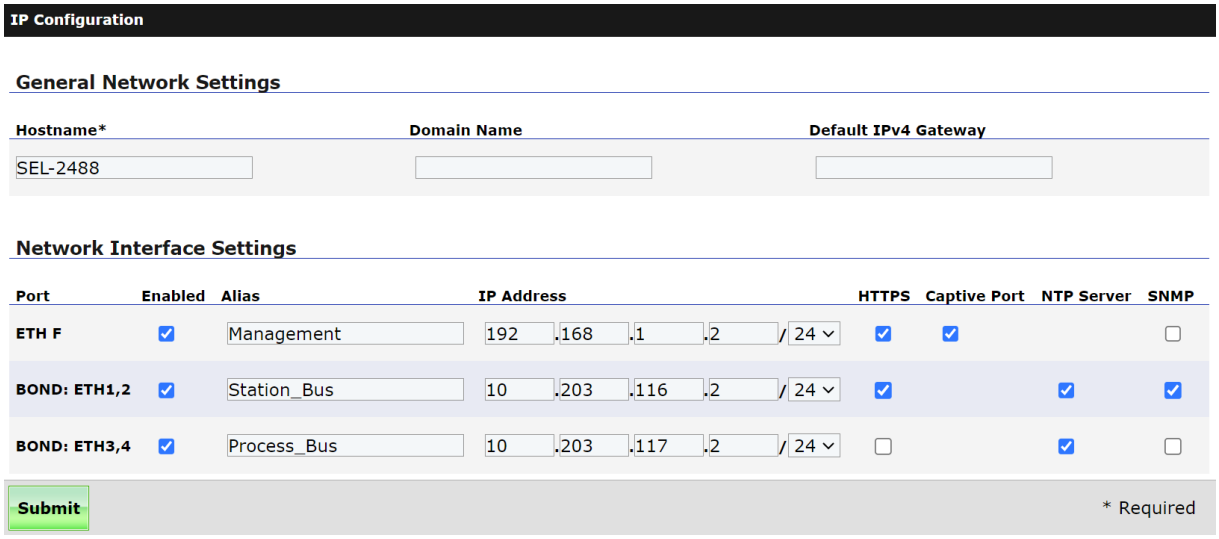


Figure 25.2 IP Configuration: Both Active-Backup Port Bonded Interfaces Enabled

Similarly, the **Static Routes** (*Figure 25.3*), **PTP** (*Figure 25.4*), and **NTP** (*Figure 25.6*) settings pages reflect the changes in the available interfaces. See *Section 5: Static Routes*, *Section 7: Precision Time Protocol (PTP)*, and *Section 8: Network Time Protocol (NTP)* for more information on the settings for each within these pages.

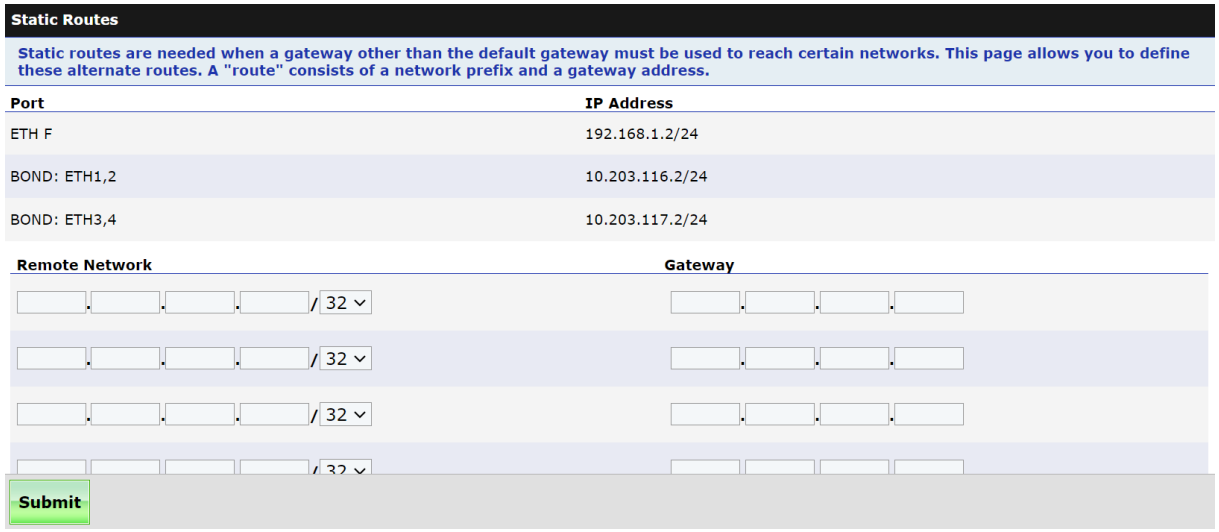


Figure 25.3 Static Routes Settings Page: Both Active-Backup Port Bonded Interfaces Enabled

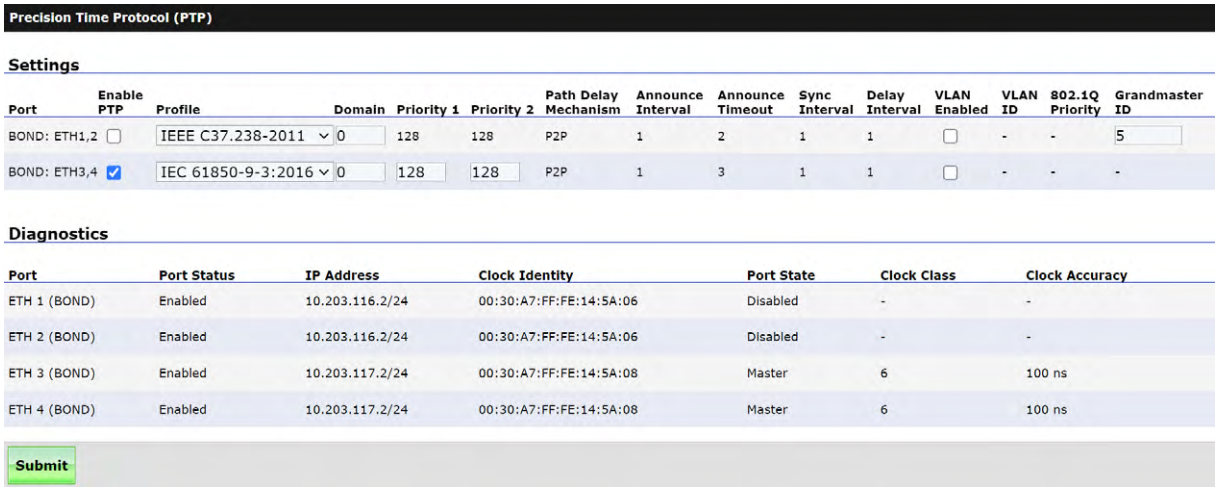


Figure 25.4 PTP Settings Page: Both Active-Backup Port Bonded Interfaces Enabled

The PTP status widget displays ports with active-backup port bonding enabled with the additional label (**BOND**) next to the port identifier, as shown in *Figure 25.5*.

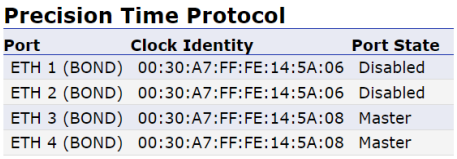


Figure 25.5 Precision Time Protocol Status Widget: Both Active-Backup Port Bonded Interfaces Enabled

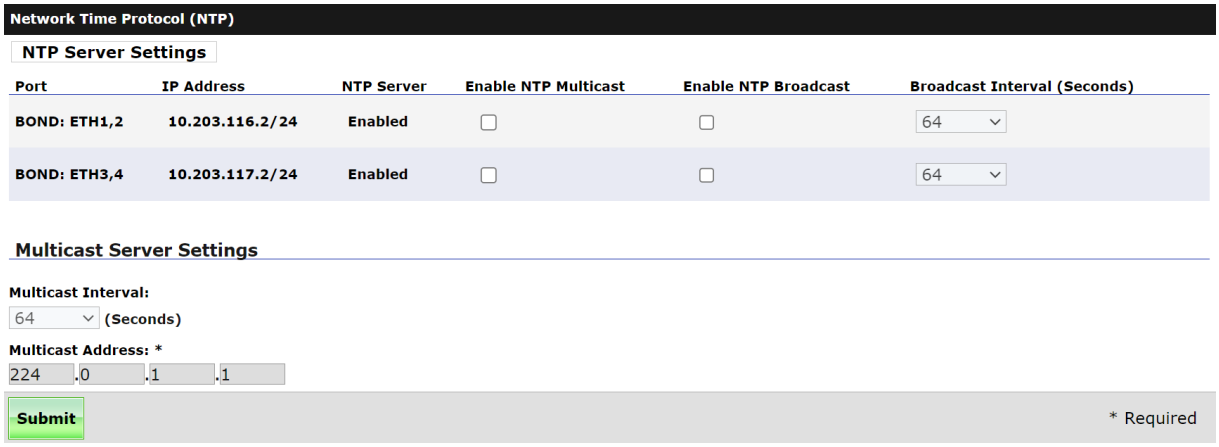


Figure 25.6 NTP Settings Page: Both Active-Backup Port Bonded Interfaces Enabled

Front Panel

The front panel does not display any active-backup port bonding information.

Dashboard

The Ethernet dashboard indicators reflect the status of the individual physical Ethernet ports of the active-backup bonded interface. When active-backup port bonding is enabled, the label below the icon includes the text (**BOND**) as shown in *Figure 25.7*. This display provides a quick visual indicator of the health of the connections to the network through the bonded interface.

As discussed in *Dashboard on page 4.7*, the table below the Ethernet dashboard indicators includes the Port Bonding column which shows if active-backup port bonding is enabled, and whether a participating port is active, backup, or down.

Port	Alias	Media Type	Speed/Duplex	Port Bonding	MAC Address	IP Address	Services/Protocols
ETH 1	Station_Bus	10/100BASE-T	100Mbps Full Duplex	BOND: ETH1,2 (Active)	00:30:a7:14:5a:06	10.203.116.2/24	HTTPS, NTP Server, SNMP
ETH 2	Station_Bus	10/100BASE-T	100Mbps Full Duplex	BOND: ETH1,2 (Backup)	00:30:a7:14:5a:06	10.203.116.2/24	HTTPS, NTP Server, SNMP
ETH 3	Process_Bus	100BASE-FX	100Mbps Full Duplex	BOND: ETH3,4 (Active)	00:30:a7:14:5a:08	10.203.117.2/24	NTP Server, PTP
ETH 4	Process_Bus	100BASE-FX	100Mbps Full Duplex	BOND: ETH3,4 (Backup)	00:30:a7:14:5a:08	10.203.117.2/24	NTP Server, PTP
ETH F	Management	10/100BASE-T	100Mbps Full Duplex	Not Bondable	00:30:a7:14:5a:0a	192.168.1.2/24	Captive Port, HTTPS

Figure 25.7 Ethernet Dashboard Indicators: Both Active-Backup Port Bonded Interfaces Enabled

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for events associated with active-backup port bonding. The SEL-2488 replaces message variables in {} with values it logs.

Table 25.2 Active-Backup Port Bonding Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
`The Active port for {bond_interface} is {0}`	Warning	Minor	Link
`Both ports of {bond_interface} are down`	Warning	Minor	Link
`Port Bonding Settings: changed by {username} at {user_ip}`	Notice	Minor	Configuration

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Section 26
Frequency Outputs

Overview

With the purchase of the frequency outputs hardware option, the SEL-2488 comes with six SMA frequency outputs. One output (**F1**) is a frequency-disciplined, TTL-compatible 10 MHz square-wave frequency output and the remaining five (**F2**–**F6**) are frequency-disciplined 10 MHz sine-wave frequency outputs.

Operation

The SEL-2488 enables the SMA frequency output ports once it determines initial time-source selection, qualification, and accuracy. On startup, to prevent transmission of inaccurate frequency, the frequency outputs are disabled until the clock selects a time source and determines the clock's accuracy. Typically, this takes about 5 minutes; however, depending on the source and the interval since the clock last synchronized to the source, this process may take as long as 20 minutes.

When no other source is present, you can set the SEL-2488 in the Manual Date/Time mode. This meets the criterion for a selected source that enables the SMA frequency output ports for demonstration purposes. See *Section 19: Date/Time* for details.

Many installations that require a 10 MHz frequency output signal also typically require a PPS output signal. To simplify the setup procedure for such installations, the time outputs **TO1**–**TO8** and **COM1** default to the PPS signal format when the frequency outputs hardware option is installed within the SEL-2488.

The cabling used for the SMA frequency output ports to end devices should be a 50 Ω impedance coaxial cable. Using a cable with a different impedance causes additional line loss and interference. The maximum possible cable length supported by each frequency output depend on the end device's minimum input peak-to-peak voltage and quality of the cabling used. Take special care in analyzing the installation to confirm proper signal levels over the desired cable lengths. However, to ensure proper shielding of the square-wave frequency output signal, the square-wave frequency output must use LMR-240 or better quality cabling for lengths greater than 2 meters. SEL recommends limiting the connections of each SMA frequency output port to a single end device unless an appropriate 50 Ω RF splitter is used.

Frequency Disciplining

The SEL-2488 disciplines the 10 MHz square-wave output signal (**F1**) separately from the five identical 10 MHz sine-wave output signals (**F2**–**F6**) to the selected time source. When a frequency output signal is being properly

disciplined, it is in a locked state. If a frequency output signal is unable to be disciplined, it is in an unlocked state. When a frequency output signal remains unlocked for at least 10 minutes, the clock restarts the disciplining process for all frequency output signals.

Holdover

If the SEL-2488 loses its primary reference time source, it goes into holdover mode and continues to provide time outputs based on its internal reference oscillator. While in holdover mode, the frequency outputs continue to provide a 10 MHz signal within the present holdover accuracy.

Status LEDs

Figure 26.1 Frequency Output SMA Ports and LED Indicators

Accompanying the six SMA frequency output ports are two LED indicators, as shown in *Figure 26.1*. As previously stated, the 10 MHz square-wave output signal (F1) is generated separately from the five identical 10 MHz sine-wave output signals (F2–F6). Therefore, the square-wave output has a single status LED located below the F1 label, while the five sine-wave outputs share a single status LED located below the F6 label. *Table 26.1* lists the states of both LED indicators, which operate in the same way.

Table 26.1 Frequency Output Signal LED Status

LED State	Description
Off	The frequency output signal is disabled.
Green	The frequency output signal is disciplining to the time source and is in a locked state.
Blinking Green	The frequency output signal is in holdover.
Red	The frequency output signal is unable to be disciplined by the time source and is in an unlocked state.

Front Panel

The front panel does not display any frequency output information.

Dashboard

The **Diagnostics** status widget provides the present operational status of the frequency outputs hardware module, as well as the disciplining state of the sine-wave and square-wave outputs, as shown in *Figure 26.2*.

Frequency Outputs:	OK
Sine Wave Status:	Locked
Square Wave Status:	Locked

Figure 26.2 Diagnostics Status Widget: Frequency Outputs Locked

If the SEL-2488 remains continuously unlocked after 30 minutes or a hardware failure is detected, the clock generates a major event and indicates a failure for the frequency output hardware module, as shown in *Figure 26.3*.

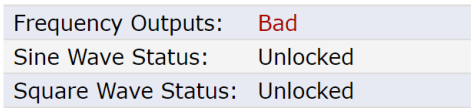


Figure 26.3 Diagnostics Status Widget: Frequency Outputs Failure

When the SEL-2488 does not have the frequency outputs hardware option installed, the clock indicates the status of the frequency outputs hardware module as Not Present, as shown in *Figure 26.4*.

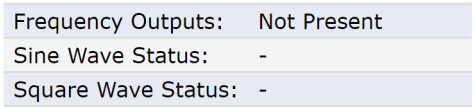


Figure 26.4 Diagnostics Status Widget: Frequency Outputs Not Present

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for events associated with the frequency outputs. The SEL-2488 replaces message variables in {} with values it logs.

Table 26.2 Frequency Outputs Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
`Failure: Frequency Outputs`	Alert	Major	–

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact. Events classified as Major will latch the alarm contact.

This page intentionally left blank

Section 27

Diagnostics and Troubleshooting

Troubleshooting

Inspection Procedure

If you suspect a problem with your SEL-2488, complete the following procedure before making any adjustments to the device. After you finish your inspection, refer to *Table 27.1*.

Step 1. Record a description of any problem you encountered.

Step 2. Measure and record the power supply voltage at the power input terminals.

Step 3. Record the states of the LED indicators.

Step 4. Record front-panel LCD messages and information.

Step 5. Record present environmental conditions and any unexpected conditions.

Step 6. If the web interface is accessible, record the part number, serial number, and firmware version from the **Device Information** table in the device dashboard.

Step 7. Examine the **System Statistics** and **Diagnostics** tables on the SEL-2488 web interface dashboard and record any unusual values.

Step 8. Export device syslog report and device settings.

Troubleshooting Procedure

Table 27.1 lists common issues and indicators with the SEL-2488. Use this table to help identify and resolve common issues.

Table 27.1 Troubleshooting Procedure (Sheet 1 of 6)

Issue/Indicator	Possible Causes	Solution
Device will not start or device is not powered on and front-panel **PWR A** and **PWR B** indicators are both dark.	Input power is not present or power supply is not fully seated.	Remove power source. Verify power cabling and connections. Remove power supply(s) and reseat. Reconnect power source.
The front-panel **PWR A** or **PWR B** indicator is red.	Power supply is properly seated but input power is not present.	Remove power source. Verify power cabling and connections. Remove indicated power supply and reseat. Reconnect power source.
	Failed power supply.	Test with known good power supply if available. Replace power supply.
The front-panel **PWR A** or **PWR B** indicator is dark when configured with a redundant power supply.	Input power is present but power supply is not properly seated.	Remove power source. Verify power cabling and connections. Remove indicated power supply and reseat. Reconnect power source.
Front-panel **ENABLE** LED is dark after startup.	Device has experienced a diagnostics failure that prevents it from operating.	Perform *Inspection Procedure*. Contact Schweitzer Engineering Laboratories, Inc. for further support.

Table 27.1 Troubleshooting Procedure (Sheet 2 of 6)

Issue/Indicator	Possible Causes	Solution
ETH F amber LED blinking.	Network communication collision detected.	Configure attached network devices for full-duplex communications.
ETH F amber LED indicator is dark after making connection or slow network speeds are experienced.	Attached network device is configured for 10BASE-T.	Set connection settings for the attached network device to 100BASE-T or Auto Sense.
ETH F green LED indicator is off after making connection.	Attached network device interface is disabled.	Enable attached network device's interface.
	Fiber cable RX/TX lines are crossed.	Verify fiber connections are properly seated and correctly connected.
	SEL-2488 interface is disabled.	Enable interface on the SEL-2488. See *Section 4: Ethernet Network Interfaces*.
The satellite clock will not lock.	Antenna or cable is not properly connected or is defective.	View the **ANTENNA STATUS** LED on the front panel. If **ANTENNA STATUS** is red, then an antenna or cable issue is present and must be repaired or there is no antenna connected to the device.
	Antenna does not have a sufficient view of the sky.	View the web dashboard or the front panel. If the clock shows no visible satellites, then there may be an issue with the antenna or cable. The clock must track four or more satellites with a dB-Hz level ≥ 30 for each constellation to obtain lock. Reposition the antenna so that it has a better view of the sky. The antenna needs to have a clear and unobstructed view of the sky in all directions. See *Section 3: Time Synchronization* for more information.
	Satellite Signal Verification (SSV) is turned on and an incorrect antenna is in use.	Satellite Signal Verification requires a dual-constellation antenna. If the **SATELLITE LOCK** LED is amber, you may be using an incorrect antenna. Either turn satellite signal verification off or order the SEL-9524B GPS/GLONASS GNSS Antenna. If a single constellation antenna is used and SSV is configured to **Notify, and stop using GNSS as a time source**, the clock cannot verify sources and will not lock.
TIME QUALITY LED is blinking.	SEL-2488 has lost lock and time quality is >1 µs but <1 ms.	View *The satellite clock will not lock* troubleshooting steps.
TIME QUALITY LED is red.	SEL-2488 has lost lock and time quality is ≥1 ms.	View *The satellite clock will not lock* troubleshooting steps.
Clock will not maintain lock, or it randomly goes into holdover during normal operation.	Antenna does not have a sufficient view of the sky to maintain lock.	The clock must track four or more satellites with a dB-Hz level ≥30 for each constellation to obtain lock. Once lock is obtained, the clock requires three satellites to be tracked and used from each constellation to maintain lock. Use the SEL-2488 SkyView located on the web interface dashboard to identify satellite blockages and proper installation. Reposition the antenna so that it has a better view of the sky. The antenna must have a clear and unobstructed view of the sky in all directions.
Dashboard reports low satellite signal strength.	Antenna does not have a sufficient view of the sky to maintain signal levels.	Reposition the antenna so that it has a better view of the sky. The antenna must have a clear and unobstructed view of the sky in all directions.
	Antenna cable is damaged.	Check cable connections for proper seal and damage. Replace damaged cable.
	Improper cable used or cable length too long.	Verify correct cables are used and cable connections and length are valid. See *Appendix C: Link Budget Analysis*.
	Antenna signal levels are weak because of extended cable length or improper cable type.	Use the link budget calculator to verify cable. See *Appendix C: Link Budget Analysis* for more information.

Table 27.1 Troubleshooting Procedure (Sheet 3 of 6)

Issue/Indicator	Possible Causes	Solution
The satellite clock will not output time on startup.	Satellite clock is not locked or time is not qualified yet.	Monitor the front-panel LCD for startup progress. The startup process may take as long as 15 minutes. Once the process is complete, the **TIME QUALITY** LED turns solid green and the SEL-2488 will then transmit time. If the **SATELLITE LOCK** LED is not green or the startup process displayed on the LCD does not complete, then view satellite lock troubleshooting steps.
IED will not synchronize time with the clock through IRIG-B.	Cable is disconnected, bad, or not terminated.	Verify the cable is properly seated and terminated if termination is needed. See *Section 3: Time Synchronization* for more information.
	IRIG-B cable is connected to the incorrect port.	Verify cable connections.
	IRIG-B impedance mismatch.	Verify that low-impedance devices are on a separate output. See *Section 6: Time-Code Outputs* for IRIG-B impedance considerations.
	Exceeded output port drive capability.	Verify that the number of devices attached to the time output port meets acceptable drive capability based on *Section 6: Time-Code Outputs*.
	Incorrect time-code format is being used.	Verify that the SEL-2488 time output port is configured for the desired format. See *Section 6: Time-Code Outputs* for more details.
	IRIG-B time quality is below acceptable threshold.	Verify time quality on web interface dashboard. Verify clock is locked to GNSS.
The SEL-2488 is not setting the year for the IED when IRIG-B is in use.	Incorrect time-code format is being used.	Configure the time-code format for the desired output port to IRIG-B004. See *Section 6: Time-Code Outputs* for more details.
	IRIG-B cable is connected to the incorrect port.	Verify cable connections.
IED will not synchronize using modulated IRIG.	Incorrect time-code format is being used.	Configure the time-code format for the desired output port to **Modulated IRIG**. See *Section 6: Time-Code Outputs* for more details.
IED will not synchronize time with the clock through NTP.	Ethernet port is not enabled.	Verify the Ethernet port specified for NTP is enabled on the SEL-2488. See *Section 4: Ethernet Network Interfaces*.
	NTP is not enabled for Ethernet port.	Enable NTP server on desired Ethernet port. See IP Configuration in *Settings on page 4.4*.
	Client is configured for manycast.	Change client setting to match the SEL-2488 server settings (multicast, unicast, or broadcast).
	Client is configured for broadcast or multicast and the server does not have these features enabled.	Enable broadcast or multicast for the NTP server. See *Section 8: Network Time Protocol (NTP)* for more information.
	Clock is not locked to satellites or Manual Date/Time mode is not configured.	Verify that clock is locked to satellites, is in holdover, or configured for Manual Date/Time mode.
IED will not synchronize time with the clock through PTP.	SEL-2488 is not the current PTP Grandmaster.	See Precision Time Protocol (PTP) diagnostics page in *Section 7: Precision Time Protocol (PTP)*.
	Incorrect profile/Network layer mismatch.	Set correct PTP profile for the required port. See *Section 7: Precision Time Protocol (PTP)* for more information.
	Clock domain mismatch.	Set correct grandmaster clock domain. See *Section 7: Precision Time Protocol (PTP)* for more information.
	Ethernet port is not enabled.	Verify the Ethernet port specified for PTP is enabled on the SEL-2488. See *Section 4: Ethernet Network Interfaces*.

Table 27.1 Troubleshooting Procedure (Sheet 4 of 6)

Issue/Indicator	Possible Causes	Solution
	PTP is not enabled for Ethernet port.	Enable PTP on desired Ethernet port. See PTP settings in *Section 7: Precision Time Protocol (PTP).*
PTP LED is amber.	PTP is configured for Default UDP (Layer 3) communication profile, but no IP address is configured for the port or Ethernet port is not enabled.	Verify that the Ethernet port specified for PTP is enabled and an IP address has been configured for the port. See *Section 4: Ethernet Network Interfaces* for more information.
	PTP is configured for a profile using Layer 2 communications, but the Ethernet port is not enabled.	Verify that the Ethernet port specified for PTP is enabled on the SEL-2488. See *Section 4: Ethernet Network Interfaces* for more information.
Timer contact is not providing a pulse.	No source is connected to the timer contact.	Connect a power source to the timer contact to provide pulses. See *Section 9: Timer Contact* for more information.
	Timer contact is not enabled.	Enable timer contact in the Timer Contact settings page. See *Section 9: Timer Contact* for more information.
	Timer contact pulse start is configured for a future date/time.	Verify that the correct pulse start mode has been configured for the timer contact. See *Section 9: Timer Contact* for more information.
	Timer contact is configured for a single pulse.	Verify that the correct pulse repeat mode has been configured for the timer contact. See *Section 9: Timer Contact* for more information.
The login page is inaccessible from **ETH F**.	The **ETH F** network interface on the SEL-2488 is not enabled.	Insert a small tool such as a paper clip into the pinhole reset located between the alarm contact and the BNC connectors on the rear panel of the device, and depress the reset button for five seconds. This will enable the interface and turn on the Captive Port feature, with which you should be able to use **ETH F** to connect to the management interface. See *Section 23: Device Reset*.
	DHCP is disabled on SEL-2488 **ETH F** but the management computer is not configured with a static IP address.	Verify the physical and logical connection between the management computer and the SEL-2488. Verify using the front-panel LCD that DHCP is disabled on **ETH F**. Configure the IP address for the network adapter of the management computer to the same network as the SEL-2488. See *Appendix G: Configuring Windows Network Parameters* for more information.
	DHCP is enabled on SEL-2488 **ETH F** but the management computer is configured with a static IP address.	Verify the physical and logical connection between the management computer and the SEL-2488. Verify using the front-panel LCD that DHCP is enabled on **ETH F**. Configure the network adapter for the management computer to obtain an IP address automatically. See *Appendix G: Configuring Windows Network Parameters* for more information.
A user cannot log in.	The user's account is missing or disabled.	Log in to the SEL-2488 as an Administrator or User Manager and verify the details for the subject account on the Local Users page. See *Section 10: Local User Management*.
	The user's password is incorrect.	Check that **<Caps Lock>** is not active on the computer logging in. If necessary, reset the user's account from the Local Users page. See *Section 10: Local User Management*.
No remote syslog messages received from the SEL-2488.	No syslog servers defined.	Navigate to the **Syslog Settings** page and ensure that the proper syslog IP address is configured. See *Section 16: Syslog Reporting* for more information.
	The syslog logging threshold is unexpectedly high.	Navigate to the **Syslog Settings** page and ensure that Logging Threshold settings are entered there. See *Section 16: Syslog Reporting* for more information.
	The syslog server is not reachable from the network containing the SEL-2488.	Ensure that the syslog server IP address is valid and reachable.

Table 27.1 Troubleshooting Procedure (Sheet 5 of 6)

Issue/Indicator	Possible Causes	Solution
	The SEL-2488 network gateway is not configured.	If the syslog server is on another network, ensure that a network gateway is configured and available to route the syslog traffic. See *Section 16: Syslog Reporting* for more information.
Not receiving all expected remote syslog messages.	The remote syslog logging threshold is unexpectedly high.	Navigate to the Syslog Settings page and ensure that Logging Threshold settings are properly entered for syslog destinations. See *Section 16: Syslog Reporting* for more information.
Not receiving all expected local syslog messages.	The local syslog logging threshold is unexpectedly high.	Navigate to the Syslog Settings page and ensure that Logging Threshold settings are properly entered for local logging. See *Section 16: Syslog Reporting* for more information.
IED reported time quality is bad.	Clock is in holdover mode.	Verify time quality on web interface dashboard. Verify clock is not locked to GNSS. View *The satellite clock will not lock* troubleshooting steps.
No remote SNMP notification received from the SEL-2488.	No SNMP trap servers defined.	Navigate to the SNMP Settings page and ensure that the proper SNMP trap server IP address is configured. See *Section 17: Simple Network Management Protocol (SNMP)* for more information.
	The SNMP trap threshold is unexpectedly high.	Navigate to the SNMP Settings page and ensure that Trap Threshold settings are properly configured. See *Section 17: Simple Network Management Protocol (SNMP)* for more information.
	The SNMP profile trap community string is incorrect.	Navigate to the SNMP settings page and ensure that the proper Trap Community string is entered in the Profile Settings tab. See *Section 17: Simple Network Management Protocol (SNMP)* for more information.
	The SNMP trap server is not reachable from the network containing the SEL-2488.	Ensure that the SNMP trap server IP address is valid and reachable.
	The SEL-2488 network gateway is not configured.	If the SNMP trap server is on another network, ensure that a network gateway is configured and available to route the SNMP traffic. See *Section 17: Simple Network Management Protocol (SNMP)* for more information.
SNMP information is not properly displayed.	The required MIBs are not loaded for the SNMP server.	Load the MIB files downloaded directly from the SEL-2488 (see *SNMP Management Information Base on page 17.6* for a full list of the files).
Not receiving all expected SNMP notifications.	The SNMP trap threshold is unexpectedly high.	Navigate to the SNMP Settings page and ensure that Trap Threshold settings are properly entered for SNMP Trap Server destinations. See *Section 17: Simple Network Management Protocol (SNMP)* for more information.
Cannot access SNMP diagnostics on SEL-2488 from SNMP Client.	SNMP is not enabled on the interface.	Navigate to the **IP Configuration** page and ensure SNMP is enabled for the interface through which the client is trying to connect.
	The SNMP Client is on a remote network.	Navigate to the **IP Configuration** page and ensure the default route is set on the SEL-2488 and that the client is attempting to access SNMP through the address that corresponds with the default route.
	The SNMP profile is either not set or incorrect.	Navigate to the **SNMP Configuration** page and confirm that the profile the client is using is entered and enabled for SNMP to read. Confirm that the password(s) [v3] or Community String [v2c] is correct by re-entering it on the SEL-2488 or the client.
Cannot change values on the SEL-2488 from the SNMP Client.	The SEL-2488 does not support SNMPSET (write) functionality.	Configure the SEL-2488 through the web management interface or ACSELERATOR QuickSet SEL-5030 Software.

Table 27.1 Troubleshooting Procedure (Sheet 6 of 6)

Issue/Indicator	Possible Causes	Solution
SNMP Major Alarm after settings import on SEL-2488.	The settings file was created on a different SEL-2488 and contains SNMP v3 profiles with passwords.	Navigate to the SNMP profile settings page and re-enter the v3 profile passwords to clear the alarm. Alternatively, if the current passwords are not known, either removing the profile or entering temporary passwords will clear the alarm.
Clock will not communicate through both PRP LANs.	PRP not enabled or configured.	Enable PRP on the clock, configure PRP interface IP address and services. See *Section 24: Parallel Redundancy Protocol (PRP)*.
Clock will not communicate on one of the PRP LANs.	PRP not enabled or configured.	Enable PRP on the clock, configure PRP interface IP address and services. See *Section 24: Parallel Redundancy Protocol (PRP)*.
	Clock not connected to both PRP LANs.	Confirm that the correct physical Ethernet ports are connected to PRP LAN A and LAN B. Confirm via the web dashboard or front-panel LEDs that both physical Ethernet ports with PRP enabled are showing link indication. See *Section 4: Ethernet Network Interfaces*.
PRP Interface is not shown on **IP Configuration** page.	PRP is disabled.	Enable PRP on the clock and configure the PRP interface IP address and services. See *Section 24: Parallel Redundancy Protocol (PRP)*.
Active-backup bonded interface is not shown on **IP Configuration** page.	Active-backup port bonding is disabled	Enable active-backup port bonding on the clock and configure the bonded interface IP address and services. See *Section 25: Active-Backup Port Bonding*.
ETH 1 and ETH 2 or ETH 3 and ETH 4 interfaces are not shown on **IP Configuration** page.	PRP or active-backup port bonding is enabled.	Disable PRP or active-backup port bonding on for the relevant physical Ethernet ports and reconfigure interfaces on **IP Configuration** page.
The LED for the square-wave frequency output (F1) or the sine-wave frequency outputs (F2–F6) is red.	The relevant frequency output signal is unable to discipline to the selected time source.	The SEL-2488 automatically restarts the disciplining process if a frequency output signal remains continuously unlocked after 10 minutes.

Alerts/Notifications

The SEL-2488 provides the following alerts or notifications for events associated with diagnostics and troubleshooting. The SEL-2488 replaces message variables in {} with values it logs.

Table 27.2 Diagnostics and Troubleshooting Alerts and Notifications

Message	Event Threshold	Alarm Category	Alarm Class
`Failure: Flash`	Alert	Major	–
`Failure: FPGA`	Alert	Major	–
`Failure: RAM`	Alert	Major	–
`Failure: Internal Clock`	Critical	Major	–
`Failure: LCD`	Error	Minor	–
`Failure: Internal Clock Battery`	Warning	Minor	–
`Failure: Internal Clock Battery absent`	Warning	Minor	–
`OK: Internal Clock Battery`	Warning	Minor	–

All events generate local syslog messages. Events generate remote syslog messages or SNMP notifications when the event severity meets or exceeds the event threshold configured for reporting.

When the specific Alarm Class is enabled on the **Alarm Contact** settings page, minor events associated with that alarm class will trigger the alarm contact. When the class is disabled, the same events will not trigger the alarm contact.

Events with an alarm category of Minor and alarm class of "–" will always trigger the alarm contact. Events classified as Major will latch the alarm contact.

Technical Support

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.338.3838
Fax: +1.509.332.7990
Internet: selinc.com/support
Email: info@selinc.com

This page intentionally left blank

Appendix A
Firmware and Manual Versions

Firmware

Determining the Firmware Version

The Firmware Identification (FID) number is shown on the SEL-2488 front-panel LCD (press the **Up** or **Down** buttons to scroll through displays until it appears) and on the web dashboard in the **Device Information** section (as shown in *Figure 21.8*).

The firmware version will be either a standard release or a point release. A standard release adds new functionality to the firmware beyond the specifications of the existing version. A point release is reserved for modifying firmware functionality to conform to the specifications of the existing version.

A standard release is identified by a change in the R-number of the device FID number.

Existing firmware:

FID=SEL-2488-**R100**-V0-Z001001-Dxxxxxxxx

Standard release firmware:

FID=SEL-2488-**R101**-V0-Z001001-Dxxxxxxxx

A point release is identified by a change in the V-number of the device FID number.

Existing firmware:

FID=SEL-2488-R100-**V0**-Z001001-Dxxxxxxxx

Point release firmware:

FID=SEL-2488-R100-**V1**-Z001001-Dxxxxxxxx

The date code is after the D. For example, the following is firmware version number R100, release date June 20, 2014.

FID=SEL-2488-R100-V0-Z001001-**D20140620**

Revision History

Table A.1 lists the firmware versions, revision descriptions, and corresponding instruction manual date codes. The most recent firmware version is listed first.

Starting with revisions published after March 1, 2022, changes that address security vulnerabilities are marked with "[Cybersecurity]". Other improvements to cybersecurity functionality that should be evaluated for potential cybersecurity importance are marked with "[Cybersecurity Enhancement]".

Table A.1 Firmware Revision History (Sheet 1 of 6)

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-2488-R111-V0-Z010001-D20241003	➤ Added support for 10 MHz frequency outputs and DOCXO holdover hardware options. ➤ Disallowed downgrade prior to R111 to prevent backward compatibility issues with updated hardware.	20241003

Table A.1 Firmware Revision History (Sheet 2 of 6)

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-2488-R110-V0-Z010001-D20240124	➤ [Cybersecurity Enhancement] Modified the default self-signed X.509 certificate behavior to generate a new unique certificate when factory-default reset. ➤ [Cybersecurity Enhancement] Updated OpenSSL to ensure continuity of support. ➤ Added support for active-backup port bonding. ➤ Modified the PTP behavior to reduce transition time between passive and master states. ➤ Modified the PTP behavior for advertising the currentUTCOffsetValid field while in holdover for improved interoperability. ➤ Modified the table below the Ethernet dashboard indicators to display permanently and include more information. ➤ Modified the device hostname and domain name behavior to allow the underscore "_" character. ➤ Reduced the processing time of large syslog event logs. ➤ Resolved an issue where unnecessary PRP syslog events were generated during a reboot or settings changes. ➤ Resolved an issue where the estimated time error because of temperature changes during holdover could be underestimated. ➤ Resolved an issue where cleared static routes were not removed from the device until a device reboot. ➤ Resolved an issue where a high number of concurrent web user sessions could result in users no longer able to log in. ➤ Resolved an issue where a firmware upgrade may fail because of insufficient available device memory, requiring a reboot prior to further attempts.	20240124
SEL-2488-R109-V1-Z009001-D20231222	Includes all the functions of SEL-2488-R109-V0-Z009001-D20220824 with the following addition: ➤ Resolved an issue where Ethernet ports on some devices become unresponsive at an ambient temperature above 65°C.	20231222
SEL-2488-R109-V0-Z009001-D20220824	➤ Added support for a second Doubly Attached Node implementing PRP (DANP) interface that uses physical Ethernet ports **ETH 3** and **ETH 4**. ➤ Added support for PTP as a Doubly Attached Clock (DAC) on ports where PRP is enabled. ➤ Added the PTP port number SNMP entry to the SEL-2488-PTP-DIAGNOSTICS-MIB. ➤ Added a diagnostics report, which will generate a report to help SEL diagnose field issues. ➤ Modified the LAN down event for PRP from a Severity of Critical and Alarm Category of Major to a Severity of Warning and Alarm Category of Minor. ➤ Modified the Manual Date/Time mode to simulate a PTP Clock Accuracy of <100 ns. Previously, the device simulated a PTP Clock Accuracy of <25 ns. ➤ Addressed an issue where transmitted NTP messages had a Leap Indicator value of "unknown" for a few seconds during leap second events.	20220824

Table A.1 Firmware Revision History (Sheet 3 of 6)

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
	➤ Addressed an issue where major alarms would persist on startup for several minutes, despite the alarm condition no longer being present. ➤ [Cybersecurity] Addressed an issue where an authenticated user uploading a malicious X.509 certificate could temporarily cause degraded performance to the X.509 Certificate Import, Settings Import/Export, and Firmware Upgrade features on the web user interface (CVE-2022-0778).	
SEL-2488-R108-V1-Z008001-D20231222	Includes all the functions of SEL-2488-R108-V0-Z008001-D20220401 with the following addition: ➤ Resolved an issue where Ethernet ports on some devices become unresponsive at an ambient temperature above 65°C.	20231222
SEL-2488-R108-V0-Z008001-D20220401	➤ Disallowed downgrade prior to R108 to prevent backward compatibility issues with updated hardware.	20220401
SEL-2488-R107-V0-Z008001-D20211101	➤ Added PTP profile support for the updated Power System profile (IEEE C37.238-2017). ➤ Modified the behavior of the Manual Date/Time mode to simulate a time quality of <25 ns on all time outputs. Previously, the device simulated a time quality of 1 µs. ➤ Modified the behavior of the Alternate Time Offset Indicator (ATOI) TLV, which is appended to all transmitted PTP Announce messages, to indicate leap second events 13 seconds prior to occurrence in accordance with IEEE C37.238-2017. Previously, the ATOI TLV data would only be adjusted during a leap second event. ➤ Addressed an issue that could affect the PTP path delay calculation accuracy when using the peer delay mechanism (P2P) with other PTP devices, which send Pdelay_Req messages with a non-zero value in the Correction Field. Previously, the SEL-2488 did not copy the Correction Field of valid received Pdelay_Req messages into the Correction Field of the corresponding transmitted response message. ➤ Addressed an issue where the Diagnostics section of the web dashboard would not show negative temperature values. ➤ Addressed an issue in R106-V0 where the Time Input section of the web dashboard would incorrectly add one second to the displayed date/time of an upcoming leap second insertion. ➤ Addressed an issue in R106-V0 with the IEC/IEEE 61850-9-3:2016 PTP profile where, when coming out of holdover, the PTP Clock Class may jump above 6 or remain above 6 for several minutes with an advertised PTP Clock Accuracy at a contradicting lower value.	20211101
SEL-2488-R106-V0-Z007001-D20210614	➤ Added PTP profile support for the Power Utility Automation profile (IEC/IEEE 61850-9-3:2016). ➤ Adjusted the default Grandmaster ID setting from “blank” (which results in a “0” value) to “5” for the PTP Power Profile (IEEE C37.238-2011). All “blank” values will be set to “5” after upgrading to R106. ➤ Addressed an issue in R105-V0 where the NTP server functionality did not advertise leap second pending 24 hours prior to the event. ➤ Addressed an issue in R105-V0 where some devices estimated time error at an accelerated degradation rate while in holdover.	20210614

Table A.1 Firmware Revision History (Sheet 4 of 6)

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
	➤ Addressed an issue in R105-V0 where some SNMP OIDs in the IF-MIB presented information differently compared with previous firmware releases. ➤ Addressed X.509 certificate processing vulnerabilities allowing denial of service on the web interface (CVE-2021-3449, 23840).	
SEL-2488-R105-V0-Z006001-D20210223	➤ Updated the operating system to prevent potential security vulnerabilities. ➤ Addressed a security vulnerability allowing denial of service to the web interface (TCP SACK CVE-2019-11477, 11478, and 11479). ➤ Addressed a security vulnerability allowing control of a compromised user's web session through cross-site scripting (jQuery CVE-2020-11022 and 11023). ➤ Removed support for encryption protocols no longer considered secure. These include TLS versions 1.0 and 1.1 used in older web browsers and support for DES Encryption Protocol option in SNMP v3.	20210223
SEL-2488-R104-V1-Z005001-D20181031	Includes all the functions of SEL-2488-R104-V0-Z005001-D20170711 with the following addition: ➤ Addressed an issue caused by an interaction between the device firmware and the flash hardware.	20181031
SEL-2488-R104-V0-Z005001-D20170711	➤ Implement PRP functionality on the SEL-2488. ➤ Addressed issue where ping messages were responding on incorrect interfaces. ➤ Addressed issue where ARP messages were responding through incorrect interfaces. ➤ Applied current patches to kernel to address vulnerabilities: CVE-2016-5195 (Dirty Cow), CVE-2016-6480, CVE-2016-3070, CVE-2016-4470, CVE-2016-2847, CVE-2016-3134, CVE-2016-0774, CVE-2013-4312, CVE-2016-0728, CVE-2015-7550, CVE-2015-8543, and CVE-2014-8160. ➤ Applied current patches to GLIBC to address vulnerabilities: CVE-2015-1781, CVE-2014-8121, CVE-2014-9761, CVE-2015-8776, CVE-2015-8777, CVE-2015-8778, CVE-2015-8779, CVE-2016-3075, and CVE-2013-2207. ➤ Applied patches to PAM to address current vulnerabilities: CVE-2013-7041, CVE-2014-2583, and CVE-2015-3238. ➤ Disallowed downgrade below R104 to prevent backward compatibility issues with updated hardware.	20170711
SEL-2488-R103-V1-Z004001-D20181031	Includes all the functions of SEL-2488-R103-V0-Z004001-D20161207 with the following addition: ➤ Addressed an issue caused by an interaction between the device firmware and the flash hardware.	20181031
SEL-2488-R103-V0-Z004001-D20161207	➤ Added the ability to pull diagnostic information through SNMP read support. ➤ Applied current patches to lighttpd to address the following vulnerabilities: CVE-2011-4362, CVE-2013-4508, CVE-2013-4559, CVE-2013-4560, CVE-2014-2323, and CVE-2014-2324. ➤ Applied current patches to OpenSSL to address CVE-2013-2566. ➤ Removed support for SHA-1 from TLS/SSL.	20161207

Table A.1 Firmware Revision History (Sheet 5 of 6)

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
	➤ Updated web interface to prevent click-jacking attacks. ➤ Updated time input diagnostic to indicate Manual Time when the clock is operating in manual time. ➤ Enhanced manual time operation to deliver simulated 1 µs accuracy for PTP time quality. ➤ Updated web interface copyright date. ➤ Applied current patches to OpenSSL to address the following vulnerabilities: CVE-2015-7575, CVE-2016-0702, CVE-2016-0705, CVE-2016-0797, CVE-2016-0798, CVE-2016-0799, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2108-1, CVE-2016-2108-2, CVE-2016-2109, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, and CVE-2016-6306. ➤ Applied current patches to NTPD to address the following vulnerabilities: CVE-2014-9297, CVE-2014-9298, CVE-2015-1798, CVE-2015-1799, CVE-2015-5146, CVE-2015-5194, CVE-2015-5195, CVE-2015-5196, CVE-2015-5219, CVE-2015-5300, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7704, CVE-2015-7705, CVE-2015-7850, CVE-2015-7852, CVE-2015-7853, CVE-2015-7855, CVE-2015-7871, CVE-2015-7973, CVE-2015-7974, CVE-2015-7976, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2015-8138, CVE-2015-8158, CVE-2016-0727, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-2516, CVE-2016-2518, CVE-2016-4954, CVE-2016-4955, and CVE-2016-4956. ➤ Applied updates to web server to address vulnerabilities noted in CVE-2016-2183 and CVE-2016-6329. ➤ Addressed issue which in previous firmware versions sometimes allowed the clock time to be off by up to 500 µs before returning to the correct time.	
SEL-2488-R102-V0-Z003001-D20151116	➤ Added SNMP trap server support. ➤ Added serial number and part number LCD screen. ➤ Updated local syslog to store all event logs. ➤ Updated local syslog report time stamp. ➤ Enhanced network settings to restrict IP addresses within the same range. ➤ Added gratuitous ARP messaging.	20151116
SEL-2488-R101-V0-Z002001-D20150317	➤ Updated LCD startup sequence screen with additional information. ➤ Updated location of “time quality” indication on the front-panel LCD. ➤ Updated initial LCD startup screen to display `Schweitzer Engineering Laboratories`. ➤ Added support for alarms to self-heal once the alarm condition has been resolved. ➤ Updated cable delay settings to be set in nanoseconds. ➤ Added the ability to disable the timeout for the LCD backlight.	20150317

Table A.1 Firmware Revision History (Sheet 6 of 6)

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
	➤ Added mouse-over tool tips on the Syslog page. ➤ Added Local Time Offset from UTC on the front LCD screen. ➤ Added Local Time Offset on the Dashboard's Time Input section. ➤ Removed System Date settings from the Global Setting section. ➤ Added "Precision Time Protocol (PTP)" and reordered subsection titles under the **Time Management** navigation pane. ➤ Updated OpenSSL to mitigate the POODLE vulnerability. ➤ Updated web interface to remove host header vulnerability. ➤ Updated manual time setting to set time quality bit to 4 for IRIG when manual time is configured. ➤ Updated **NTP** LED status functionality. ➤ Enhanced handling of leap-second events when SSV is enabled. ➤ Removed support for MD5 from TLS/SSL. ➤ Disallowed downgrade below R101 to prevent backward compatibility issues with updated hardware.	
SEL-2488-R100-V0-Z001001-D20140620	➤ Initial version.	20140818

Instruction Manual

The date code at the bottom of each page of this manual reflects the creation or revision date.

Table A.2 lists the instruction manual versions and revision descriptions. The most recent instruction manual version is listed first.

Table A.2 Instruction Manual Revision History (Sheet 1 of 8)

Date Code	Summary of Revisions
20241003	General ➤ Added *Section 26: Frequency Outputs*. Preface ➤ Updated *Safety Information*. Section 1 ➤ Updated *Figure 1.2: Rear-Panel View Including Optional Frequency Outputs*. ➤ Updated *BNC Time Outputs*. ➤ Added *SMA Frequency Outputs*. ➤ Updated *Figure 1.3: SEL-2488 Device Webpage With Dashboard Display*. ➤ Updated *Unit Placement and Maintenance Physical Location*. ➤ Updated *Figure 1.4: Front-and Rear-Panel Diagrams*. ➤ Updated *Power Supplies*. ➤ Updated *Figure 1.17: Device Hardware Diagnostics.* ➤ Updated *Specifications*. Section 2 ➤ Added *Example 7* and *Example 8*. Section 3 ➤ Updated *Figure 3.10: Diagnostics Status Widget: Time Synchronization.*

Table A.2 Instruction Manual Revision History (Sheet 2 of 8)

Date Code	Summary of Revisions
	Section 4 ➤ Updated *Figure 4.1: Location of Pinhole Reset*. Section 23 ➤ Updated *Figure 23.3: Location of Pinhole Reset*. Section 27 ➤ Updated *Table 27.1: Troubleshooting Procedure*. Appendix A ➤ Updated for firmware version R111-V0. Appendix D ➤ Updated *Table D.4: Event Logs*. Appendix I ➤ Updated section title.
20240124	General ➤ Added *Section 25: Active-Backup Port Bonding*. Preface ➤ Updated *Safety Marks*. ➤ Added *Battery Change Instructions*. Section 1 ➤ Updated *Figure 1.3: SEL-2488 Device Webpage With Dashboard Display*. ➤ Added *Unit Placement and Maintenance Physical Location*. ➤ Updated *Specifications*. Section 2 ➤ Added *Example 6*. Section 3 ➤ Updated *Figure 3.6: Satellite Information on Bar Graph* and *Figure 3.7: Satellite Information on SkyView*. Section 4 ➤ Updated *Settings* and *Dashboard*. Section 5 ➤ Updated *Settings*. Section 6 ➤ Updated *Operation*. Section 7 ➤ Updated *Settings* and *Dashboard*. Section 8 ➤ Updated *Settings* and *Dashboard*. Section 10 ➤ Updated *Passphrases*. Section 12 ➤ Updated *Overview* and *Active Certificate*. Section 13 ➤ Updated *Settings*. Section 14 ➤ Updated *Figure 14.1: Event Notification Dialog*. Section 16 ➤ Updated *Settings* and *Figure 16.2: Syslog Settings Page*.

Table A.2 Instruction Manual Revision History (Sheet 3 of 8)

Date Code	Summary of Revisions
	Section 17 ➤ Updated *Dashboard*. **Section 19** ➤ Updated *Figure 19.7: Dashboard—Satellite Status When in Manual Date/Time Mode*. **Section 23** ➤ Updated *Device Reboot* and *Dashboard*. **Section 24** ➤ Updated *Overview, Operation, Settings,* and *Dashboard*. **Section 26** ➤ Updated *Table 25.1: Troubleshooting Procedure*. **Appendix A** ➤ Updated for firmware version R110-V0. **Appendix D** ➤ Updated *Table D.4: Event Logs*.
20231222	**Appendix A** ➤ Updated for firmware versions R108-V1 and R109-V1.
20221027	**Specifications** ➤ Updated to include UKCA Mark.
20220824	**General** ➤ Updated for PTP over PRP support and the addition of a second PRP interface using physical Ethernet ports **ETH 3** and **ETH 4**. ➤ Updated Captive Port instructions. **Section 1** ➤ Updated *Getting Started*. ➤ Added proximity recommendations when mounting multiple GNSS antennas. ➤ Updated *Specifications*. **Section 2** ➤ Added *Example 5*. **Section 4** ➤ Updated *ETH F Interface Reset*. ➤ Added *IP Configuration With PRP Enabled*. ➤ Added *Figure 4.1: Location of Pinhole Reset*. ➤ Added *Figure 4.2: LCD ETH F Information Screen*. ➤ Added *Figure 4.4: IP Configuration Page: Both PRP Interfaces Enabled*. **Section 5** ➤ Added *Static Routes Settings With PRP Enabled*. ➤ Added *Figure 5.2: Static Routes Settings Page: Both PRP Interfaces Enabled*. **Section 6** ➤ Updated *Operation*. **Section 7** ➤ Updated *Definitions*. ➤ Updated *Operation*. ➤ Updated *Settings*. ➤ Added *PTP Settings With PRP Enabled*. ➤ Updated *PTP Diagnostics*. ➤ Added *Figure 7.2: PTP Settings Page: Both PRP Interfaces Enabled*. ➤ Added *Figure 7.3: PTP Diagnostics Widget: Both PRP Interfaces Enabled*.

Table A.2 Instruction Manual Revision History (Sheet 4 of 8)

Date Code	Summary of Revisions
	Section 8 ➤ Added *NTP Settings With PRP Enabled*. ➤ Added *Figure 8.3: NTP Settings Page: Both PRP Interfaces Enabled*. **Section 19** ➤ Updated *Manual Date/Time*. **Section 21** ➤ Updated for the addition of the Diagnostics Report. ➤ Added *Figure 21.9: Diagnostics Report Tab*. ➤ Added *Figure 21.10: Diagnostics Report Complete*. **Section 23** ➤ Updated *Factory-Default Reset*. ➤ Added *Figure 23.3: Location of Pinhole Reset*. **Section 24** ➤ Updated for the addition of a second PRP interface that uses **ETH 3** and **ETH 4**. **Section 25** ➤ Updated *Table 25.1: Troubleshooting Procedure*. **Appendix A** ➤ Updated for firmware version R109. **Appendix D** ➤ Updated *Table D.4: Event Logs*.
20220401	**Appendix A** ➤ Updated for firmware version R108.
20211227	**Section 1** ➤ Updated *Figure 1.4: Front-and Rear-Panel Diagrams*, *Figure 1.11 SEL-9330-A 125–250 Vac/Vdc*, and *Figure 1.13: SEL-9330-C 24–48 Vdc*. ➤ Updated *Specifications*.
20211101	**General** ➤ Updated PTP information to include the updated Power System profile (IEEE C37.238-2017). ➤ Updated Manual Date/Time information for high-accuracy time quality relative to UTC on all time outputs. **Section 1** ➤ Updated *PTP* under *General* in *Specifications*. **Section 3** ➤ Updated *Figure 3.1: GNSS Settings Web Interface*. **Section 6** ➤ Updated *Holdover* in *Operation*. **Section 7** ➤ Added *Operation*. ➤ Added *Holdover*. ➤ Updated *Settings*. ➤ Updated *Figure 7.1: PTP Settings Web Interface*. ➤ Updated *Table 7.1: PTP Settings*. **Section 8** ➤ Updated *Operation*. ➤ Added *Holdover*. **Section 19** ➤ Updated *Manual Date/Time*. ➤ Updated *Figure 19.4: Manual Date/Time Setting Tab*. ➤ Updated *Figure 19.8: Time Input Screen—Manual Date/Time Mode*.

Table A.2 Instruction Manual Revision History (Sheet 5 of 8)

Date Code	Summary of Revisions
	Appendix A ➤ Updated for firmware version R107.
20210727	**Section 1** ➤ Updated *Figure 1.5: Dimensions for Rack- and Panel-Mount Models*. ➤ Updated *Specifications*.
20210630	**Section 1** ➤ Updated *Specifications*.
20210614	**General** ➤ Updated PTP information to include the Power Utility Automation profile (IEC/IEEE 61850-9-3:2016). **Section 1** ➤ Updated *Specifications*. **Section 7** ➤ Updated *Profile*. ➤ Updated *Figure 7.1: PTP Settings Web Interface*. ➤ Updated *Table 7.1: PTP Settings*. **Appendix A** ➤ Updated for firmware version R106-V0.
20210324	**Section 1** ➤ Updated UL certification in *Specifications*.
20210223	**General** ➤ Updated web browser recommendation. **Section 1** ➤ Updated *Getting Started* and *Specifications*. ➤ Updated *Figure 1.16: Initial Startup Sequence*. **Section 17** ➤ Updated *Table 17.1: SNMP Profile Settings*. ➤ Updated *Settings Import Warning—SNMP v3 Profiles*. **Appendix A** ➤ Updated for firmware version R105. **Appendix D** ➤ Updated *Table D.4: Event Logs*.
20201106	**Section 1** ➤ Updated UL certification in *Specifications*.
20200212	**Section 1** ➤ Added UL MX certification to *Specifications*.
20181031	**Appendix A** ➤ Updated for firmware versions R103-V1 and R104-V1.
20170711	**General** ➤ Added *Section 24: Parallel Redundancy Protocol (PRP)*. **Preface** ➤ Updated *Open Source Software*. **Section 1** ➤ Updated *Specifications*. **Section 3** ➤ Updated *Satellite Lock Requirements*. ➤ Removed *Device Information Status*.

Table A.2 Instruction Manual Revision History (Sheet 6 of 8)

Date Code	Summary of Revisions
	Section 4 ➤ Added *Note* to *Settings* subsection. **Section 7** ➤ Added *Note* to *Settings* subsection. **Section 8** ➤ Added *Note* to *Settings* subsection. **Section 20** ➤ Updated *Figure 20.2: Device Information Screen—System Contact*. **Section 21** ➤ Updated *Figure 21.7: Firmware Version Screen*. ➤ Updated *Figure 21.8: Device Information Screen—Firmware Version*. **Section 22** ➤ Updated *Figure 22.3: Firmware Version LCD Screen*. **Section 25** ➤ Updated *Table 25.1: Troubleshooting Procedure*. **Appendix A** ➤ Updated for firmware version R104. **Appendix D** ➤ Updated *Table D.4: Event Logs*.
20161207	**Preface** ➤ Added *Trademarks*. **Section 1** ➤ Updated *Table 1.1: DB-9 Port Pinout*. **Section 2** ➤ Updated *Figure 2.4:* SEL-2488 *Overcomes Single Point of Failure With Multiple Connections to a Redundant Ethernet Network Topology*. **Section 3** ➤ Added *Antenna Diagnostics* subsection to *Operation*. ➤ Updated *Figure 3.10: Device Information Screen: Receiver Firmware*. **Section 4** ➤ Added *SNMP*. ➤ Updated *Figure 4.1: IP Configuration Web Interface*. ➤ Updated *Table 4.2: ETH F Network Interface Settings* and *Table 4.3: ETH 1–4 Network Interface Settings*. ➤ Updated *Figure 4.7: Ethernet Dashboard Indicators: Additional Information*. **Section 6** ➤ Updated *Output Drive Capacity* under *Operation*. **Section 8** ➤ Updated *Figure 8.1: Settings Web Interface: NTP Aspect*. **Section 17** ➤ Updated *Overview*. ➤ Updated *Settings*. ➤ Added *SNMP Read*, *Passphrases*, and *Settings Import Warning—SNMP v3 Profiles*. ➤ Updated *Table 17.1: SNMP Profile Settings*. ➤ Updated *Figure 17.1: SNMP Configuration Tab*, *Figure 17.2: SNMP Profile Settings Tab*, and *Figure 17.3: SNMP Trap Server Settings Tab*. ➤ Updated *Dashboard*. ➤ Updated *Table 17.3: SNMP Alerts and Notifications*.

Table A.2 Instruction Manual Revision History (Sheet 7 of 8)

Date Code	Summary of Revisions
	Section 19 ➤ Updated *Figure 19.8: Time Input Screen—Manual Date/Time Mode*. Section 20 ➤ Updated *Figure 20.2: Device Information Screen—System Contact*. Section 21 ➤ Updated *Figure 21.7: Firmware Version Screen* and *Figure 21.8: Device Information Screen—Firmware Version*. Section 22 ➤ Updated *Figure 22.3: Firmware Version LCD Screen*. Section 24 ➤ Updated *Table 24.1: Troubleshooting Procedures*. Appendix A ➤ Updated for firmware version R103. Appendix D ➤ Updated *Table D.4: Event Logs*. Appendix I ➤ Added *Appendix I: Cybersecurity*.
20160203	General ➤ Updated cable information to include RG-8X. Section 1 ➤ Updated *Power Supplies*.
20151116	General ➤ Added *Section 17: SNMP Settings*. Section 1 ➤ Updated *Figure 1.3:* SEL-2488 *Device Webpage With Dashboard Display*. ➤ Updated *Table 1.5: Hardware Alerts and Notifications*. ➤ Updated *Specifications*. Section 3 ➤ Updated *Figure 3.10: Device Information Screen: Receiver Firmware*. Section 4 ➤ Updated *Overview*. ➤ Updated *Figure 4.1: IP Configuration Web Interface*. Section 8 ➤ Updated *Figure 8.1: Settings Web Interface: NTP Aspect*. ➤ Updated *Figure 8.2: NTP Settings Web Interface*. ➤ Updated *Figure 8.5: Additional Diagnostics Information for Ethernet Interfaces*. Section 14 ➤ Updated *Overview*. ➤ Updated *Major vs. Minor Events*. Section 16 ➤ Updated *Local Syslog Reporting*. ➤ Updated *Figure 16.1: Syslog Report*. ➤ Updated *Remote Syslog Reporting*. ➤ Updated *Settings*. ➤ Updated *Figure 16.2: Syslog Web Interface*. Section 20 ➤ Updated *Figure 20.2: Device Information Screen—System Contact*.

Table A.2 Instruction Manual Revision History (Sheet 8 of 8)

Date Code	Summary of Revisions
	Section 21 ➤ Updated *Figure 21.6: File Management/Firmware Upgrade*. ➤ Updated *Figure 21.7: Firmware Version Screen*. ➤ Updated *Figure 21.8: Device Information Screen—Firmware Version*. **Section 22** ➤ Updated *Overview*. ➤ Updated *Figure 22.3: Firmware Version LCD Screen*. ➤ Added *Serial and Part Number* to *Front Panel*. **Section 24** ➤ Updated *Table 24.1: Troubleshooting Procedure*. ➤ Updated *Table 24.2: Diagnostics and Troubleshooting Alerts and Notifications*. **Appendix A** ➤ Updated for firmware version R102. **Appendix B** ➤ Updated *Figure B.1: Firmware Upgrade Tab*. **Appendix D** ➤ Updated *Table D.4: Event Logs*.
20150909	**Section 1** ➤ Updated antenna information with the SEL-9524 GNSS Antenna. **Section 23** ➤ Updated *Table 23.1: Troubleshooting Procedure* with the SEL-9524 GNSS Antenna. **Appendix C** ➤ Updated *Table C.1: Antenna Gain and Noise Figure* and *Table C.3: Typical Losses* with information on the SEL-9524 GNSS Antenna.
20150701	**Section 1** ➤ Updated *Specifications*.
20150515	**General** ➤ Corrected number of satellites per constellation required to maintain satellite lock status to three satellites. **Preface** ➤ Updated *Safety Information*. **Section 1** ➤ Updated compliance information in *Specifications*.
20150317	**General** ➤ Redesigned and reorganized manual to focus on feature specific content. **Appendix A** ➤ Updated for firmware version R101.
20141001	**Section 1** ➤ Updated *Rear Panel*. ➤ Updated *Figure 1.2: Rear-Panel View*. ➤ Updated *Figure 1.3: Typical Surge Protector Installation*. ➤ Updated *Table 1.9: DB-9 Port Pinout*. ➤ Updated *Specifications*. **Section 5** ➤ Updated *Table 5.1: GNSS Settings*. Updated *Time Management*. **Section 6** Updated *Table 6.4: Troubleshooting Procedure*.
20140818	➤ Initial version.

This page intentionally left blank

Appendix B
Precision Time Protocol Field Upgrade Instructions

Introduction

These instructions provide you with the steps to add the Precision Time Protocol (PTP) firmware option to your SEL-2488. For instructions on upgrading the *firmware* in your SEL-2488, see *Firmware Upgrade Instructions on page 21.3*.

Upgrade Process

To add PTP to your SEL-2488, you will need to contact your SEL sales representative to purchase the upgrade. You will receive the latest firmware update as well as a model option table (MOT) upgrade file and a new part number label. The MOT upgrade file updates the SEL-2488 part number to enable PTP on the device. PTP support for the SEL-2488 is available, starting with firmware release R101.

NOTE: If you try to perform the PTP upgrade on R100 firmware, the SEL-2488 will provide the following failure notification: `The firmware update from R100 to new version failed with an error of "-1." Please contact Schweitzer Engineering Laboratories, Inc. for assistance.`

If you are running firmware version R100, you will need to upgrade the firmware to R101 or higher first, then perform the MOT upgrade to enable the PTP feature.

Load the MOT upgrade file in the same manner you would use to perform a firmware upgrade. An MOT upgrade will not overwrite existing SEL-2488 settings.

Perform the following steps to upgrade the SEL-2488 firmware and perform the MOT upgrade for PTP support for the SEL-2488:

Step 1. Log in to the device by using an account with the Administrator role.

Step 2. Browse to the **File Management** page and select the **Firmware Upgrade** tab, which displays the version of the presently running firmware and allows you to choose the upgrade file for upload to the unit (see *Figure B.1*).

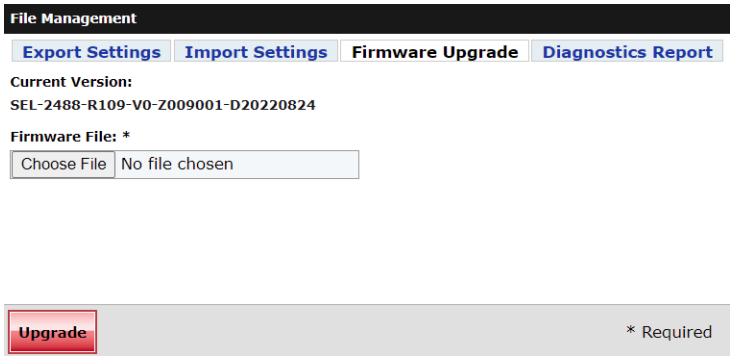


Figure B.1 Firmware Upgrade Tab

Step 3. Select **Choose File** and navigate to the location of the firmware upgrade file. Select the file and select **Open**.

Step 4. Select the **Upgrade** button to upload and install the new firmware. The page displays the status of the firmware upgrade, periodically updating operation progress. Completion of a firmware update takes about 10 minutes.

Step 5. Once the firmware upgrade is complete, log in to the device by using an account with the Administrator role.

Step 6. Select the **File Management** link from the navigation panel.

Step 7. In the **File Management** window, select the **Firmware Upgrade** tab.

Step 8. Select **Choose File** and navigate to the location of the MOT upgrade file. Select the file and select **Open**.

Step 9. Select the **Upgrade** button at the bottom of the page to upload and install the new MOT upgrade. The page displays status of the MOT upgrade, periodically updating operation progress. Once the upgrade completes, your SEL-2488 part number changes to reflect the addition of PTP support.

Appendix C
Link Budget Analysis

Overview

A Global Navigation Satellite System (GNSS) based time synchronization receiver system consists of the following three components, as shown in *Figure C.1*.

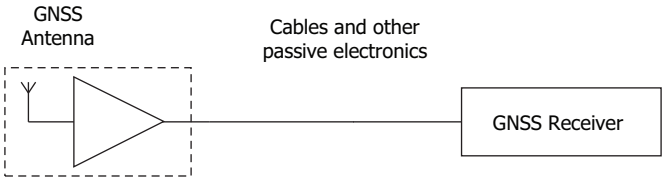


Figure C.1 GNSS-Based Time Synchronization System

GNSS Antenna

GNSS antennas play an important role in the overall performance of any GNSS-based time synchronization system. *Figure C.1* shows a representation of an active antenna that includes an antenna element and a Low Noise Amplifier (LNA) for amplifying the low power GNSS (GPS and GLONASS) signals that are received. Even the best GNSS receiver cannot recover satellite signals that are lost because of poor antenna performance and installation. For optimal performance, antennas should have the following:

- **Good visibility to the sky.** The position of the antenna is critical for any time synchronization system based on GNSS. Antennas must have an unobstructed view of the sky to ensure direct line of sight with as many satellites as possible. SkyView for the SEL-2488 provides a visual aid of both GPS and GLONASS satellites on the web interface dashboard. This can be used as a tool to adjust the antenna mounting. It is also important to place the antennas away from intentional radiators that could interfere with the signal reception.
- **High-gain LNA with low noise figure (NF).** Active GNSS antennas have an integrated LNA while passive antennas contain a radiating element only (e.g., ceramic patch, etc.) Active antennas provide a couple of benefits. First, because signals are amplified prior to being sent through the cables by the LNA, the losses in the cables have a small effect on the overall NF of the GNSS system. Second, the LNA helps in reducing the overall NF of the system and thereby improves the receive sensitivity of the system. Active antennas are usually

powered by the same cable that connects the antenna to the GNSS receivers via a dc voltage source. A good active antenna has an LNA gain of at least 30 dB.

Noise Figure

Noise figure is a measure of the amount of noise each part of a system introduces that affects the receiver sensitivity. This could be an amplifier, receiver, cable, and any other electronics in the receive chain of a system.

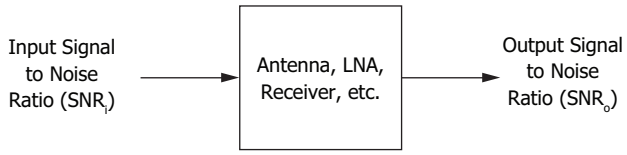


Figure C.2 Illustration of Noise Figure

The calculation for noise figure is:

$$\text{Noise Figure} = 10*\log_{10}(SNR_i/SNR_o)\ \text{dB}$$

$$\text{Noise Factor (Noise Figure expressed in linear terms)} = F = SNR_i/SNR_o$$

where SNR_i and SNR_o are Signal to Noise ratios of Input and Output, respectively, and the resulting ratio, when expressed in the logarithmic form, is referred to as noise figure.

For passive electronics like cables, splitters etc., NF is just the loss because of these components expressed in dB.

Table C.1 shows the gain and noise figure of the SEL-9524 GNSS Antenna.

Table C.1 Antenna Gain and Noise Figure

Antenna Type	Typ. Gain (dB)	NF (dB)	SEL Part Number
GNSS Antenna	40	< 2 dB (25 C)	SEL-9524

Cables and Passive Electronics

Cables and passive electronics are used to connect the antenna to the GNSS receivers. It is important to select proper cables based on the installation. Most of the available GNSS antennas are designed for a 50 Ω electrical load. The SEL-2488 GNSS receiver electronics is a 50 Ω system. It is important to select a cable with a characteristic impedance of 50 ohms to match the impedance of the antenna and the SEL-2488 for optimal power transfer (low loss) from the antenna onto the cable and from the cable to the SEL-2488 GNSS receiver. Any mismatch in the impedance can result in signal loss affecting the performance of the system.

Table C.2 shows some important parameters associated with cables that contribute to the overall performance of the GNSS system.

Table C.2 Cable Parameters

Cable Type (Number)	Characteristic Impedance	Loss per 100 ft
LMR-400 (SEL-C961)	50 Ω	5.2 dB
RG-8X (SEL-C965)	50 Ω	9.4 dB

Connectors like adapters and surge arrestors also contribute small losses to the GNSS signals. *Table C.3* shows typical losses for the connectors and adapters provided with SEL clocks.

Table C.3 Typical Losses

Connection Type	Loss (dB)	Notes
Antenna		SEL-9524 GNSS Antenna
TNC connection 1	0.075	Male to female
Cable 2	5.2 dB/100 ft 9.4 dB/100 ft	LMR-400 RG-8X
TNC connection 2	0.075	Male to female
Surge arrester	0.036	
TNC connection 3	0.075	Male to female
Cable 1	5.2 dB/100 ft 9.4 dB/100 ft	LMR-400 RG-8X
TNC connection 4	0.075	Male to female
SEL-2488		Satellite-Synchronized Clock

GNSS Receiver

GNSS receivers consist of electronics that are capable of tracking multiple satellite signals, as well as multiple constellations, to simultaneously provide accurate time information.

Figure C.3 shows the complete GNSS-based time synchronization system to illustrate the link margin.

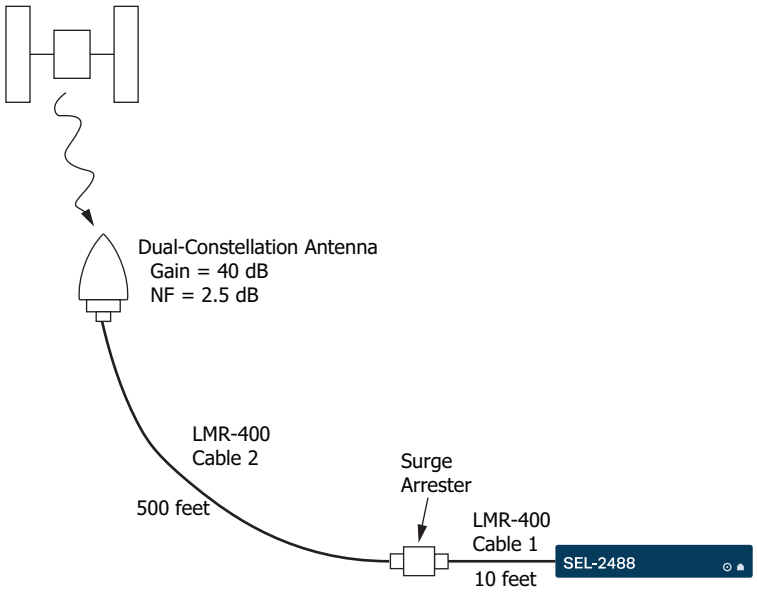


Figure C.3 Link Margin Calculation for a GNSS System

NOTE: dBm = $10\log_{10}$ (power in mW).

The average signal strength received at the antenna for GPS signals is approximately –130 dBm. These signals get attenuated as they traverse through cables, connectors, and surge arrestors. Receive sensitivity is defined

as the lowest level of signal required by the receiver to extract information without errors from the satellite signals. A lower value of the sensitivity specification for a receiver indicates a greater ability to receive weak signals. In addition, it is important that the actual signal power of the received signals is higher than the receive sensitivity of the system. The difference between the receive sensitivity of the system and the actual signal power is known as link margin.

For the system shown in *Figure C.3*, the overall receiver system sensitivity is:

$$S = RS + NF \qquad \textbf{Equation C.1}$$

where:

S = Sensitivity—The sensitivity of the overall receiver system (Antenna, Cables, GPS receiver, etc.)

RS = Receiver Sensitivity—The receiver sensitivity[a] of the GPS receiver in the SEL-2488, which is –149.5 dBm at cold start.

NF = Noise Figure—The noise figure of the receiver system because of antenna, cables, connectors etc.)

[a] Typical receiver sensitivity for a GNSS receiver is –149.5 dBm while acquiring satellite signal lock and is –158 dBm when tracking satellites after achieving lock.

The system NF is computed using the cascaded noise figure equation.

$$F = F_1 + \frac{F_2 - 1}{G_1} \qquad \textbf{Equation C.2}$$

where:

F = The noise factor for the combined antenna stage and the cable/connector

F_1, F_2 = The noise factors on the individual stages (antenna and cable + connector)

G_1 = The gain of the first stage and in this case this is the gain of the antenna

G_{dB} = Gain in dB for the antenna = 40 dB

$$G_1 = 10^{(G_{dB}/10)}$$

G1 = 10000

$$F_1 = 10^{(NF_1/10)}$$

NF_1 = Noise figure of the GNSS antenna = 2.5 dB

F1 = 1.77

$$F_2 = 10^{(NF2/10)}$$

NF_2 = Noise figure[a] (cable + surge arrestor system) = 26.52 dB (510 ft of LMR-400) + 0.036 dB (surge arrestor)

F2 = 452.48

[a] Connector losses are ignored, as they are negligible.

Using *Equation C.2*:

F = 1.815

Noise figure is converted to:

NF = 2.6 dB

It is important to note that the active antenna with a gain of 40 dB has significantly reduced the effect of the noise (attenuation/loss) added to the signal because of the downstream passive elements like cables and connectors. This shows the importance of having an active antenna with good gain right where the signals are received for installations that have long cable runs.

Using *Equation C.1*, the overall Receive Sensitivity of the system is:

$$S = RS + NF = -149.5 + 2.6 = -146.9 \text{ dBm}$$

The available margin for the system described in the example is

$$-130\text{dBm} - (-146.9) \text{ dBm} = 16.9 \text{ dB}$$

The SEL-2488 dashboard on the web interface provides satellite signal strengths for each satellite vehicle in the units of dB-Hz also known as Carrier to Noise ratio or C/N_o.

The receiver signal strength and C/N_o are related by the following equation

$$\text{Signal Strength} = \frac{C}{N_O} - 174 \text{ dBm/Hz} + NF \qquad \textbf{Equation C.3}$$

where NF is the noise figure in dB.

For the SEL-2488, C/N_o or dB-Hz should be 30 or higher for at least four satellites to acquire initial satellite lock.

This page intentionally left blank

Appendix D
Syslog

Introduction

The Syslog Protocol, defined in RFC 3164, provides a transport mechanism by which a device can send system event notification messages across Internet Protocol (IP) networks to remote syslog servers. Syslog is commonly used to send system logs such as security events, system events, and status messages useful in troubleshooting, auditing, and event investigations. The syslog packet size is limited to 1024 bytes and is formatted into three parts: PRI, HEADER, and MSG.

1. **PRI:** The priority part of a syslog packet is a number enclosed in angle brackets that represents both the facility and severity of the message. The priority value is calculated by multiplying the facility numerical code by 8 and adding the numerical value of the severity. For example, a kernel message (facility = 0) with a severity of Emergency (severity = 0) would have a priority of 0, while a "local use 4" message (facility = 20) with a severity of Notice (severity = 5) would have a priority value of 165. In the PRI part of the syslog message, these values would be placed between the angle brackets as <0> and <165>, respectively.

The severity code (*Table D.1*) is a number indicative of message importance.

Table D.1 Syslog Message Severities

Numerical Code	Severity
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational
7	Debug

The facility code (*Table D.2*) defines the application group from which the message originated.

Table D.2 Syslog Message Facilities (Sheet 1 of 2)

Numerical Code	Facility
0	Kernel messages
1	User-level messages
2	Mail system

Table D.2 Syslog Message Facilities (Sheet 2 of 2)

Numerical Code	Facility
3	System daemons
4	Security/authorization messages[a]
5	Messages generated internally by Syslog Protocol
6	Line printer subsystem
7	Network news subsystem
8	UUCP subsystem
9	Clock daemon[b]
10	Security authorization messages[a]
11	FTP daemon
12	NTP subsystem
13	Log audit[a]
14	Log audit[a]
15	Clock daemon[b]
16	Local use 0 (local 0)
17	Local use 1 (local 1)
18	Local use 2 (local 2)
19	Local use 3 (local 3)
20	Local use 4 (local 4)
21	Local use 5 (local 5)
22	Local use 6 (local 6)
23	Local use 7 (local 7)

[a] Various operating systems have been found to use Facilities 4, 10, 13, and 14 for security/authorization, audit, and alert messages that seem to be similar.
[b] Various operating systems have been found to use both Facilities 9 and 15 for clock (cron/at) messages. Source: www.faqs.org/rfcs/rfc3164.html.

2. **HEADER:** The header of a syslog packet contains the time stamp and the source of the message. The IP address or the hostname defines the source of the message. Time stamps are based on the time at the originating host, so it is critical to have time synchronized across devices for the entire network to accurately perform log analysis and event correlation.
3. **MSG:** The message part of a syslog packet contains the source program that triggered the message and the human-readable body of the message.

A sample syslog message follows. This particular message shows an invalid login attempt on July 09, 2009, at 08:17:29 to "myhostname" from the IP address 192.168.1.1. The priority of this message is 37.

```
<37>Jul 09 2009 08:17:29 myhostname Login: Login to web:
failed from 192.168.1.1
```

The syslog message has been divided into each respective part, as shown in *Table D.3*.

Table D.3 Syslog Message Components

PRI	HEADER	MSG
<37>	Jul 09 2009 08:17:29 myhostname	Login: Login to web: failed from 192.168.1.1

Remote Syslog Servers

Syslog messages are stored locally and optionally sent to remote syslog servers. The local buffers are circular in nature, with newer messages overwriting older messages after the buffer fills. Support for multiple remote syslog servers provides the added benefits of centralized logging, including larger storage capacity, centralized event analysis and correlation, and archival event logs. In *Figure D.1*, remote devices are configured to send syslog messages to the remote syslog server on the other end of the VPN tunnel. In this example, syslog-compatible devices can send logs to the central syslog server for centralized logging, reporting, and event correlation. The Syslog protocol uses User Datagram Protocol (UDP) Port 514 to send syslog messages to remote syslog servers.

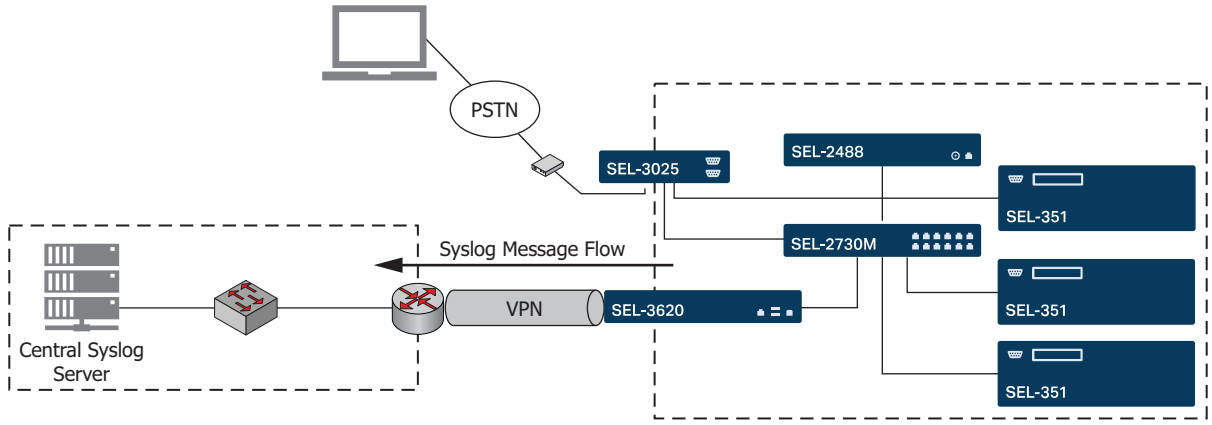


Figure D.1 Central Syslog Server

Open Source Syslog Servers

Most Linux and UNIX distributions include a native syslog server that can be used for a central syslog server solution. Syslog-ng (www.balabit.com) is also an excellent solution that, if not already included in your distribution, can be used for added functionality. Syslog server solutions for Microsoft Windows are typically commercially available or have limited feature sets if offered at no charge.

SEL-2488 Event Logs

The SEL-2488 records and time-stamps all events in the syslog format consistent with the syslog description from RFC 3164. *Table D.4* lists all of the events that the SEL-2488 logs and the record the clock generates with each event.

Log messages may contain words or phrases in brackets such as {0}. This notation indicates a variable that the SEL-2488 replaces with the value being logged. For example, the SEL-2488 would replace the {0} in the Syslog message `User account {0} locked out due to consecutive failed login attempts` with the actual username that was locked out.

Table D.4 Event Logs (Sheet 1 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
Failure: Antenna open/absent	Diagnostics	Alert	SYSTEM	Major	–
Failure: Antenna short	Diagnostics	Alert	SYSTEM	Major	–
Failure: Flash	Diagnostics	Alert	SYSTEM	Major	–
Failure: FPGA	Diagnostics	Alert	SYSTEM	Major	–
Failure: GNSS Receiver A	Diagnostics	Alert	SYSTEM	Major	–
Failure: GNSS Receiver B	Diagnostics	Alert	SYSTEM	Major	–
Failure: Holdover Clock	Diagnostics	Alert	SYSTEM	Major	–
Failure: Power Supply A	Diagnostics	Alert	SYSTEM	Major	–
Failure: Power Supply B	Diagnostics	Alert	SYSTEM	Major	–
Failure: RAM	Diagnostics	Alert	SYSTEM	Major	–
Failure: Frequency Outputs	Diagnostics	Alert	SYSTEM	Major	–
Failure: Internal Clock	Diagnostics	Critical	SYSTEM	Major	–
The firmware update from {0} to new version failed with an error of "{1}". Please contact Schweitzer Engineering Laboratories, Inc. for assistance	Firmware	Critical	SYSTEM	Major	Configuration
The Part Number for the device has changed from {0} to {1}.	PartNumber	Critical	SYSTEM	Major	Chassis
Imported from another device, please reset SNMP v3 profile passwords.	SNMPConfig	Critical	USER	Major	Configuration
Imported settings, or upgraded from a firmware version, with an SNMP profile utilizing the unsupported DES Encryption Protocol. Please select a supported Encryption Protocol for the affected SNMP profile(s).	SNMPConfig	Critical	USER	Major	Configuration
Holdover Alert.	TimeSync	Critical	CLOCK	Major	Time Synchronization
Alarm Contact: configuration changed by {username} at {user_ip}	AlarmContact	Notice	USER	Minor	Configuration
Captive Port: disabled by {username} at {user_ip}	CaptivePortConfig	Notice	USER	Minor	Configuration
Captive Port: enabled by {username} at {user_ip}	CaptivePortConfig	Notice	USER	Minor	Configuration
System Contact Information: changed by {username} at {user_ip}	Config	Notice	USER	Minor	Configuration
Usage Policy: changed by {username} at {user_ip}	Config	Notice	SECURITY	Minor	Configuration
Local Time Settings: Changed by {username} at {user_ip}.	DateTimeConfig	Notice	USER	Minor	Configuration
Failure: LCD	Diagnostics	Error	SYSTEM	Minor	–
OK: Antenna connection	Diagnostics	Error	SYSTEM	Minor	–
OK: Power Supply A	Diagnostics	Error	SYSTEM	Minor	–
OK: Power Supply B	Diagnostics	Error	SYSTEM	Minor	–
Failure: Internal Clock Battery	Diagnostics	Warning	SYSTEM	Minor	–

Table D.4 Event Logs (Sheet 2 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
Failure: Internal Clock Battery absent	Diagnostics	Warning	SYSTEM	Minor	–
OK: Internal Clock Battery	Diagnostics	Warning	SYSTEM	Minor	–
The firmware version downgrade is not compatible with the current firmware	Firmware	Error	SYSTEM	Minor	Configuration
Uploaded firmware update package is corrupted; unable to either decrypt the firmware update package or validate the signature on the firmware update package	Firmware	Error	SYSTEM	Minor	Configuration
Firmware update to new version initiated by {username} at {user_ip}	Firmware	Notice	USER	Minor	Configuration
Firmware update from {0} to {1} succeeded	Firmware	Warning	SYSTEM	Minor	Configuration
Front Panel Contrast: Changed by user at Front Panel.	FrontPanelConfig	Notice	USER	Minor	Configuration
Front Panel Settings: Changed by {username} at {user_ip}.	FrontPanelConfig	Notice	USER	Minor	Configuration
GNSS Notification Settings: Changed by {username} at {user_ip}.	GNSSConfig	Notice	USER	Minor	Configuration
GNSS Settings: Changed by {username} at {user_ip}.	GNSSConfig	Notice	USER	Minor	Configuration
Host Settings: Added host {0} with IP address {1} by {username} at {user_ip}.	HostConfig	Notice	USER	Minor	Configuration
Host Settings: Changed hostname {0} with IP address {1} to {2} with IP address {3} by {username} at {user_ip}.	HostConfig	Notice	USER	Minor	Configuration
Host Settings: Removed host {0} with IP address {1} by {username} at {user_ip}.	HostConfig	Notice	USER	Minor	Configuration
Configuration file export started by {username} at {user_ip}	ImportExport	Notice	USER	Minor	Configuration
Configuration file export successful	ImportExport	Notice	USER	Minor	Configuration
Configuration file export failed	ImportExport	Warning	USER	Minor	Configuration
Configuration file import started by {username} at {user_ip}	ImportExport	Notice	USER	Minor	Configuration
Configuration file import successful	ImportExport	Notice	USER	Minor	Configuration
Configuration file import failed	ImportExport	Warning	USER	Minor	Configuration
Diagnostic Report generated by {username} at {user_ip}	Diagnostics	Notice	USER	Minor	–
LDAP Bind DN changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP Bind DN Password changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP disabled by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration

Table D.4 Event Logs (Sheet 3 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
LDAP enabled by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP Group Filter changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP group mapping {0} changed to {1} by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP group mapping {0} mapping created by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP group mapping {0} mapping deleted by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP Group Membership Attribute changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP Search Base changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP server {0}:{1} created by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP server {0}:{1} deleted by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP server {0}:{1} hostname changed to {2} by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP server {0}:{1} port changed to {2} by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP settings changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP Synchronization Interval changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP TLS disabled by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP TLS enabled by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
LDAP User ID Filter changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY	Minor	Configuration
Port {0} changed link state to down	LinkUpDown	Notice	SYSTEM	Minor	Link
Port {0} changed link state to up	LinkUpDown	Notice	SYSTEM	Minor	Link
Login to {interface}: failed from {user_ip}	Login	Notice	SECURITY	Minor	Authentication
Login to {interface}: successful by {username} at {user_ip}	Login	Notice	SECURITY	Minor	Authentication
Logout {interface}: {username} at {user_ip}	Login	Notice	SECURITY	Minor	Authentication
User account {0} locked out due to consecutive failed login attempts	Login	Warning	SECURITY	Minor	Authentication
User account {0} timeout	Login	Warning	SECURITY	Minor	Authentication
Network Interface {0}: changed by {username} at {user_ip}	NetworkConfig	Notice	USER	Minor	Configuration

Table D.4 Event Logs (Sheet 4 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
Network Settings: changed by {username} at {user_ip}	NetworkConfig	Notice	USER	Minor	Configuration
Static Route Settings: changed by {username} at {user_ip}	NetworkConfig	Notice	USER	Minor	Configuration
NTP Server Settings: Changed by {username} at {user_ip}.	NTPServerConfig	Notice	USER	Minor	Configuration
NTP Server: Disabled on port {0}, {1} by {username} at {user_ip}.	NTPServerConfig	Notice	USER	Minor	Configuration
NTP Server: Enabled on port {0}, {1} by {username} at {user_ip}.	NTPServerConfig	Notice	USER	Minor	Configuration
Device reset because of hardware watchdog	Power	Critical	SYSTEM	Minor	Chassis
Device rebooted by {username} at {user_ip}	Power	Error	USER	Minor	Chassis
Device initialization completed	Power	Notice	SYSTEM	Minor	Chassis
LAN A of {prp_interface} is down	PRP	Warning	SYSTEM	Minor	Link
LAN B of {prp_interface} is down	PRP	Warning	SYSTEM	Minor	Link
LAN A of {prp_interface} is restored	PRP	Notice	SYSTEM	Minor	Link
LAN B of {prp_interface} is restored	PRP	Notice	SYSTEM	Minor	Link
PRP Settings: changed by {username} at {user_ip}	PRPConfig	Notice	USER	Minor	Configuration
The Active port for {bond_interface} is {0}	ActiveBackup	Warning	SYSTEM	Minor	Link
Both ports of {bond_interface} are down	ActiveBackup	Warning	SYSTEM	Minor	Link
Port Bonding Settings: changed by {username} at {user_ip}	BondConfig	Notice	USER	Minor	Configuration
PTP Settings Misconfiguration Repaired	PTPConfig	Notice	USER	Minor	Configuration
PTP Settings Misconfigured. Either PTP is enabled on an interface that is disabled, or PTP is enabled using Default (UDP) on a port that has no IP address	PTPConfig	Notice	USER	Minor	Configuration
PTP Settings: changed by {username} at {user_ip}	PTPConfig	Notice	USER	Minor	Configuration
Front management port reset initiated through pinhole button	PushbuttonReset	Alert	USER	Minor	Chassis
Device factory reset initiated through pinhole button	PushbuttonReset	Notice	USER	Minor	Chassis
SNMP Trap destination {0} added by {username} at {user_ip}.	SNMPConfig	Notice	USER	Minor	Configuration
SNMP Trap destination {0} modified by {username} at {user_ip}.	SNMPConfig	Notice	USER	Minor	Configuration
SNMP Trap destination {0} removed by {username} at {user_ip}.	SNMPConfig	Notice	USER	Minor	Configuration
SNMP Trap Server Misconfiguration Repaired.	SNMPConfig	Notice	USER	Minor	Configuration

Table D.4 Event Logs (Sheet 5 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
SNMP Trap Server Misconfiguration. Trap server will only operate with v2c profiles.	SNMPConfig	Notice	USER	Minor	Configuration
SNMP v2c profile {0} added by {username} at {user_ip}.	SNMPConfig	Notice	USER	Minor	Configuration
SNMP v2c profile {0} modified by {username} at {user_ip}.	SNMPConfig	Notice	USER	Minor	Configuration
SNMP v2c profile {0} removed by {username} at {user_ip}.	SNMPConfig	Notice	USER	Minor	Configuration
SNMP v3 profile {0} added by {username} at {user_ip}.	SNMPConfig	Notice	USER	Minor	Configuration
SNMP v3 profile {0} modified by {username} at {user_ip}.	SNMPConfig	Notice	USER	Minor	Configuration
SNMP v3 profile {0} removed by {username} at {user_ip}.	SNMPConfig	Notice	USER	Minor	Configuration
Syslog Destination {0}: created by {username} at {user_ip}	SyslogConfig	Notice	USER	Minor	Configuration
Syslog Destination {0} Settings: modified by {username} at {user_ip}	SyslogConfig	Warning	USER	Minor	Configuration
Syslog Destination {0}: deleted by {username} at {user_ip}	SyslogConfig	Warning	USER	Minor	Configuration
GNSS signal verification failed.	SystemIntegrity	Error	CLOCK	Minor	System Integrity
GNSS signal verification successful.	SystemIntegrity	Error	CLOCK	Minor	System Integrity
GNSS signal verification is not operational.	SystemIntegrity	Warning	CLOCK	Minor	System Integrity
GNSS signal verification is operational.	SystemIntegrity	Warning	CLOCK	Minor	System Integrity
Time Code Output Settings: Changed by {username} at {user_ip}.	TimeCode-OutputsConfig	Notice	USER	Minor	Configuration
Timer Contact Settings: Changed by {username} at {user_ip}.	TimerContact-Config	Notice	USER	Minor	Configuration
1µs ≤ Time Quality < 1ms.	TimeSync	Notice	CLOCK	Minor	Time Synchronization
Time Quality < 1µs.	TimeSync	Notice	CLOCK	Minor	Time Synchronization
Time Quality ≥ 1ms.	TimeSync	Notice	CLOCK	Minor	Time Synchronization
Time set manually by {username} at {user_ip}.	TimeSync	Notice	USER	Minor	Time Synchronization
Time source has changed to {0}.	TimeSync	Warning	CLOCK	Minor	Time Synchronization
User {0}: attributes changed by {username} at {user_ip}	UserConfig	Notice	SECURITY	Minor	Configuration
User {0}: disabled by {username} at {user_ip}	UserConfig	Notice	SECURITY	Minor	Configuration
User {0}: enabled by {username} at {user_ip}	UserConfig	Notice	SECURITY	Minor	Configuration
User {0}: created by {username} at {user_ip}	UserConfig	Warning	SECURITY	Minor	Configuration

Table D.4 Event Logs (Sheet 6 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
User {0}: deleted by {username} at {user_ip}	UserConfig	Warning	SECURITY	Minor	Configuration
User {0}: password set by {username} at {user_ip}	UserConfig	Warning	SECURITY	Minor	Configuration
Web Server Certificate: changed from {0} to {1} by {username} at {user_ip}	WebServerConfig	Warning	USER	Minor	Configuration
Web Server Settings: changed by {username} at {user_ip}	WebServerConfig	Warning	USER	Minor	Configuration
X.509 certificate {0} has expired; communications requiring X.509 based authentication may have stopped	X509Config	Error	SYSTEM	Minor	Configuration
X.509 certificate {0} Alias: certificate changed to {1} by {username} at {user_ip}	X509Config	Notice	USER	Minor	Configuration
X.509 certificate {0} deleted by {username} at {user_ip}	X509Config	Notice	SECURITY	Minor	Configuration
X.509 certificate {0} set as default web certificate by {username} at {user_ip}	X509Config	Notice	SECURITY	Minor	Configuration
X.509 certificate {0} will expire in {1} days; communications requiring X.509 based authentication may be affected when it expires	X509Config	Notice	SYSTEM	Minor	Configuration
X.509 certificate {0}: certificate import completed successfully	X509Config	Notice	SECURITY	Minor	Configuration
X.509 certificate import started by {username} at {user_ip}	X509Config	Notice	SECURITY	Minor	Configuration
X.509 certificate {0} will expire in {1} days; communications requiring X.509 based authentication may be affected when it expires	X509Config	Warning	SYSTEM	Minor	Configuration
X.509 certificate import failed	X509Config	Warning	SECURITY	Minor	Configuration
Device commissioned by {0} at {user_ip}	Commissioning	Notice	SECURITY	None	–
Device factory reset initiated by {username} at {user_ip}	Commissioning	Notice	SECURITY	None	–
Daylight Saving Time began.	DateTime	Informational	CLOCK	None	–
Daylight Saving Time ended.	DateTime	Informational	CLOCK	None	–
Leap Second deleted.	DateTime	Informational	CLOCK	None	–
Leap Second inserted.	DateTime	Informational	CLOCK	None	–
Daylight Saving Time adjustment pending.	DateTime	Notice	CLOCK	None	–
Leap Second adjustment pending.	DateTime	Notice	CLOCK	None	–
The {0} event queue overflowed	EventSystem	Error	SYSTEM	None	–
The {0} event queue left the overflow condition. Approximately {1} events were lost.	EventSystem	Notice	SYSTEM	None	–
LDAP: {0}:{1} does not respond	LDAP	Error	SECURITY	None	–

Table D.4 Event Logs (Sheet 7 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
LDAP: An error occurred during authentication or authorization on server {0}:{1}	LDAP	Error	SECURITY	None	–
LDAP: An error occurred during Bind DN authentication on server {0}:{1}	LDAP	Error	SECURITY	None	–
LDAP: An error occurred when searching for a DN on the server {0}:{1}	LDAP	Error	SECURITY	None	–
LDAP: An error occurred when searching for the user's DN on the server {0}:{1}	LDAP	Error	SECURITY	None	–
LDAP: Bind DN authentication failed on server {0}:{1}	LDAP	Error	SECURITY	None	–
LDAP: Group Filter syntax invalid for server {0}:{1}	LDAP	Error	SECURITY	None	–
LDAP: LDAP version used by server {0}:{1} is not supported	LDAP	Error	SECURITY	None	–
LDAP: One or more of the user-configured DNs for server {0}:{1} contains syntax errors.	LDAP	Error	SECURITY	None	–
LDAP: Search base entry not found on server {0}:{1}	LDAP	Error	SECURITY	None	–
LDAP: Server {0}:{1} returned a DN that was longer than 4096 bytes. That DN was ignored.	LDAP	Error	SECURITY	None	–
LDAP: The certificate presented by {0}:{1} is expired	LDAP	Error	SECURITY	None	–
LDAP: The certificate presented by {0}:{1} is invalid	LDAP	Error	SECURITY	None	–
LDAP: The hostname of the certificate presented by {0}:{1} does not match	LDAP	Error	SECURITY	None	–
LDAP: The issuing authority of the certificate presented by {0}:{1} is untrusted	LDAP	Error	SECURITY	None	–
LDAP: Unable to connect to server at {0}:{1}	LDAP	Error	SECURITY	None	–
LDAP: Unable to start TLS session with {0}:{1}	LDAP	Error	SECURITY	None	–
LDAP: User ID Filter syntax invalid for server {0}:{1}	LDAP	Error	SECURITY	None	–
LDAP: Group Filter search on server {0}:{1} returned no groups	LDAP	Warning	SECURITY	None	–
LDAP: No Group Mappings set for server {0}:{1}	LDAP	Warning	SECURITY	None	–
Port {0} changed PTP state to Master	PTP	Notice	SYSTEM	None	–
Port {0} changed PTP state to Passive	PTP	Notice	SYSTEM	None	–
Local Syslog Event Queue contains >= 90% unacknowledged events.	Syslog	Critical	SYSTEM	None	–
Local Syslog Event Queue contains <= 65% unacknowledged events.	Syslog	Notice	SYSTEM	None	–

Table D.4 Event Logs (Sheet 8 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
Local Syslog Event Queue contains <= 80% unacknowledged events.	Syslog	Notice	SYSTEM	None	–
Syslog events acknowledged by {username} at {user_ip}	Syslog	Notice	USER	None	–
Local Syslog Event Queue contains >= 75% unacknowledged events.	Syslog	Warning	SYSTEM	None	–
X.509 certificate {0} will expire in {1} days; communications requiring X.509 based authentication may be affected when it expires	X509Config	Informational	SYSTEM	None	–

This page intentionally left blank

Appendix E
IRIG-B

Overview

IRIG-B is a serial data time format consisting of a 1-second frame that contains 100 pulses divided into fields. The time-synchronized device decodes the second, minute, hour, and day fields and sets the device internal time clock upon detecting valid time data in the IRIG-B time mode. The SEL-2488 provides both modulated and demodulated IRIG-B outputs according to the IRIG 200-04 and IEEE C37.118.1-2011 standard. Modulated IRIG-B is IRIG-B12X. Demodulated IRIG-B time code is IRIG-B00X. The last digit, either 2 or 4, indicates the coded expression(s).

The SEL-2488 generates IRIG-BXX4 with IEEE C37.118-2011 control bit extensions. The extension includes year, leap second, and daylight-saving time indicators, time offset, time quality, parity, continuous time quality, and straight binary seconds. This format is backward-compatible with IEEE C37.118-2005 extensions, and standard BXX4 and BXX0 formats. This format is backward-compatible for BXX2 format; however, if the BXX2 clients are having difficulty with this format, there is a separate option for generating BXX2 format.

NOTE: IRIG-B004 and B124 are new time formats that replace and are backward-compatible with IRIG-B000 and B120. The new formats contain the same control bits, but also include continuous time quality.

The following comparison section presents the expected information contained in the base IRIG-B message and control bit extensions and a comparison table. Details of the meaning of the control bits and time quality indicators follow the comparison section. For more information on the control bit functions, see Annex D of the IEEE C37.118.1-2011 standard.

Comparison of IRIG-B Formats

Table E.1 show the message contents of various IRIG-B and IEEE C37.118 formats.

Table E.1 IRIG-B Format Legend (Sheet 1 of 2)

Bit Values as Determined by IRIG Standard	
S	Seconds
TS	Tens of Seconds
M	Minutes
TM	Tens of Minutes
H	Hours
TH	Tens of Hours
D	Days

Table E.1 IRIG-B Format Legend (Sheet 2 of 2)

TD	Tens of Days
HD	Hundreds of Days
Y	Years
TY	Tens of Years
SBS	Straight Binary Seconds (SBS 00 is LSB)
Index Bits as Determined by IRIG Std.	
I	Index (Always 0 Bit Value)
Reference Bits as Determined by IRIG Std.	
R	Reference
P*n*	Position Identifier
Control Bits as Determined by IRIG Std.	
C*n*	Control Bits (User Defined)
Bit Values as Determined by C37.118 Standard	
Y	Years
TY	Tens of Years
LSP	Leap Second Pending
LS	Leap Second Type
DSP	Daylight Saving Pending
DST	Daylight Saving Active
TOS	Time Offset Sign
TO	Time Offset
TQ	Time Quality
P	Parity
CTQ	Continuous Time Quality

The SEL-2488 outputs IRIG-BXX4 with C37.118-2011 control bit extensions. For slave devices that cannot decode this format, IRIG-BXX2 is an available signaling option.

Table E.2 IRIG-B Format Comparison (Sheet 1 of 4)

Bit	C37.118 2011	C37.1182005	BXX4	BXX0	BXX2
00	R	R	R	R	R
01	S1	S1	S1	S1	S1
02	S2	S2	S2	S2	S2
03	S4	S4	S4	S4	S4
04	S8	S8	S8	S8	S8
05	Index	Index	Index	Index	Index
06	TS1	TS1	TS1	TS1	TS1
07	TS2	TS2	TS2	TS2	TS2
08	TS4	TS4	TS4	TS4	TS4
09	P1	P1	P1	P1	P1
10	M1	M1	M1	M1	M1
11	M2	M2	M2	M2	M2

Table E.2 IRIG-B Format Comparison (Sheet 2 of 4)

Bit	C37.118 2011	C37.1182005	BXX4	BXX0	BXX2
12	M4	M4	M4	M4	M4
13	M8	M8	M8	M8	M8
14	Index	Index	Index	Index	Index
15	TM1	TM1	TM1	TM1	TM1
16	TM2	TM2	TM2	TM2	TM2
17	TM4	TM4	TM4	TM4	TM4
18	Index	Index	Index	Index	Index
19	P2	P2	P2	P2	P2
20	H1	H1	H1	H1	H1
21	H2	H2	H2	H2	H2
22	H4	H4	H4	H4	H4
23	H8	H8	H8	H8	H8
24	Index	Index	Index	Index	Index
25	TH1	TH1	TH1	TH1	TH1
26	TH2	TH2	TH2	TH2	TH2
27	Index	Index	Index	Index	Index
28	Index	Index	Index	Index	Index
29	P3	P3	P3	P3	P3
30	D1	D1	D1	D1	D1
31	D2	D2	D2	D2	D2
32	D4	D4	D4	D4	D4
33	D8	D8	D8	D8	D8
34	Index	Index	Index	Index	Index
35	TD1	TD1	TD1	TD1	TD1
36	TD2	TD2	TD2	TD2	TD2
37	TD4	TD4	TD4	TD4	TD4
38	TD8	TD8	TD8	TD8	TD8
39	P4	P4	P4	P4	P4
40	HD1	HD1	HD1	HD1	HD1
41	HD2	HD2	HD2	HD2	HD2
42	Index	Index	Index	Index	Index
43	Index	Index	Index	Index	Index
44	Index	Index	Index	Index	Index
45	Index	Index	Index	Index	Index
46	Index	Index	Index	Index	Index
47	Index	Index	Index	Index	Index
48	Index	Index	Index	Index	Index
49	P5	P5	P5	P5	P5
50	Y1	Y1	Y1	C1	Index
51	Y2	Y2	Y2	C2	Index
52	Y4	Y4	Y4	C3	Index

Table E.2 IRIG-B Format Comparison (Sheet 3 of 4)

Bit	C37.118 2011	C37.1182005	BXX4	BXX0	BXX2
53	Y8	Y8	Y8	C4	Index
54	Index	Index	Index	Index	Index
55	TY1	TY1	TY1	C5	Index
56	TY2	TY2	TY2	C6	Index
57	TY4	TY4	TY4	C7	Index
58	TY8	TY8	TY8	C8	Index
59	P6	P6	P6	P6	P6
60	LSP	LSP	C9	C9	Index
61	LS	LS	C10	C10	Index
62	DSP	DSP	C11	C11	Index
63	DST	DST	C12	C12	Index
64	TOS	TOS	C13	C13	Index
65	TO1	TO1	C14	C14	Index
66	TO2	TO2	C15	C15	Index
67	TO4	TO4	C16	C16	Index
68	TO8	TO8	C17	C17	Index
69	P7	P7	P7	P7	P7
70	TO.5	TO.5	C18	C18	Index
71	TQ1	TQ1	C19	C19	Index
72	TQ2	TQ2	C20	C20	Index
73	TQ4	TQ4	C21	C21	Index
74	TQ8	TQ8	C22	C22	Index
75	P	P	C23	C23	Index
76	CTQ1	–	C24	C24	Index
77	CTQ2	–	C25	C25	Index
78	CTQ4	–	C26	C26	Index
79	P8	P8	P8	P8	P8
80	SBS 00	SBS 00	SBS 00	SBS 00	Index
81	SBS 01	SBS 01	SBS 01	SBS 01	Index
82	SBS 02	SBS 02	SBS 02	SBS 02	Index
83	SBS 03	SBS 03	SBS 03	SBS 03	Index
84	SBS 04	SBS 04	SBS 04	SBS 04	Index
85	SBS 05	SBS 05	SBS 05	SBS 05	Index
86	SBS 06	SBS 06	SBS 06	SBS 06	Index
87	SBS 07	SBS 07	SBS 07	SBS 07	Index
88	SBS 08	SBS 08	SBS 08	SBS 08	Index
89	P9	P9	P9	P9	P9
90	SBS 09	SBS 09	SBS 09	SBS 09	Index
91	SBS 10	SBS 10	SBS 10	SBS 10	Index
92	SBS 11	SBS 11	SBS 11	SBS 11	Index
93	SBS 12	SBS 12	SBS 12	SBS 12	Index

Table E.2 IRIG-B Format Comparison (Sheet 4 of 4)

Bit	C37.118 2011	C37.1182005	BXX4	BXX0	BXX2
94	SBS 13	SBS 13	SBS 13	SBS 13	Index
95	SBS 14	SBS 14	SBS 14	SBS 14	Index
96	SBS 15	SBS 15	SBS 15	SBS 15	Index
97	SBS 16	SBS 16	SBS 16	SBS 16	Index
98	Index	Index	Index	Index	Index
99	P0	P0	P0	P0	P0

Control function extensions are described in Annex F of IEEE C37.118.1-2011.

Table E.3 IRIG-B Control Bit Assignments

Control Bit	IRIG-B Bit	Designation	Description
1	50	Year, BCD 1	Last digit of year in binary-coded decimal (BCD)
2	51	Year, BCD 2	
3	52	Year, BCD 3	
4	53	Year, BCD 4	
5	54	Not used	NA
6	55	Year, BCD 10	Ten's digit of year in BCD
7	56	Year, BCD 20	
8	57	Year, BCD 40	
9	58	Year, BCD 80	
–	59	P6	Position identifier #6
10	60	Leap Second Pending (LSP)	Becomes 1 at 59 seconds before leap second insert
11	61	Leap Second (LS)	0 = Add leap second, 1 = Delete leap second
12	62	Daylight Saving Pending (DSP)	Becomes 1 at 59 seconds before DST change
13	63	Daylight-Saving Time (DST)	Becomes 1 during daylight-saving time
14	64	Time Offset Sign	Time offset sign 0 = +, 1= –
15	65	Time Offset—Binary 1	Time offset coded IRIG-B to UTC. IRIG-B coded time minus time offset equals UTC at all times (bits 15–18).
16	66	Time Offset—Binary 2	
17	67	Time Offset—Binary 4	
18	68	Time Offset—Binary 8	
–	69	P7	Position identifier #7
19	70	Time Offset—0.5 hours	0 = none, 1 = additional 0.5 hour time offset
20	71	Time Quality—Binary 1	Four-bit code representing the approximate clock time quality. See *Table E.4* for Time Quality indicator code (bits 20–23).
21	72	Time Quality—Binary 2	
22	73	Time Quality—Binary 4	
23	74	Time Quality—Binary 8	
24	75	Parity	Parity on all preceding data bits
25	76	Continuous Time Quality—Binary 1	Three-bit code representing the maximum time inaccuracy of the transmitted message. CTQ indicates error at all times. See *Table E.5* for CTQ indicator code (bits 25–27).
26	77	Continuous Time Quality—Binary 2	
27	78	Continuous Time Quality—Binary 4	
–	79	P8	Position identifier #8

Table E.4 Four-Bit IRIG-B Time Quality (TQ) Code—IRIG-B Bits 71-74

Binary	Hex	Value
1111	F	Time not traceable to UTC
1011	B	Time within 10 seconds of UTC
1010	A	Time within 1 second of UTC
1001	9	Time within 100 ms of UTC
1000	8	Time within 10 ms of UTC
0111	7	Time within 1 ms of UTC
0110	6	Time within 100 µs of UTC
0101	5	Time within 10 µs of UTC
0100	4	Time within 1 µs of UTC
0011	3	Time within 100 ns of UTC
0010	2	Time within 10 ns of UTC
0001	1	Time within 1 ns of UTC
0000	0	Clock is locked

Table E.5 Three-Bit Continuous Time Quality (CTQ) Code—IRIG-B Bits 76-78

Binary	Hex	Value
111	7	Maximum time inaccuracy ≥ 10 ms or unknown
110	6	Maximum time inaccuracy < 10 ms
101	5	Maximum time inaccuracy < 1 ms
100	4	Maximum time inaccuracy < 100 µs
011	3	Maximum time inaccuracy < 10 µs
010	2	Maximum time inaccuracy < 1 µs
001	1	Maximum time inaccuracy < 100 ns
000	0	Not used (set to 0 if using IRIG-BXX0 or BXX2)

IRIG-B has modulated and demodulated time-code formats. The demodulated signal is a pulse train of positive pulses at a rate based on the designated format. The rising edge of the reference pulse coincides with the seconds change in the time source and provides a very precise time reference. The modulated format is an amplitude-modulated sine wave with amplitude between 1 Vp-p and 6 Vp-p for the mark (peak), with a mark-to-space amplitude ratio of approximately 3:1.

Sample IRIG-B Waveform

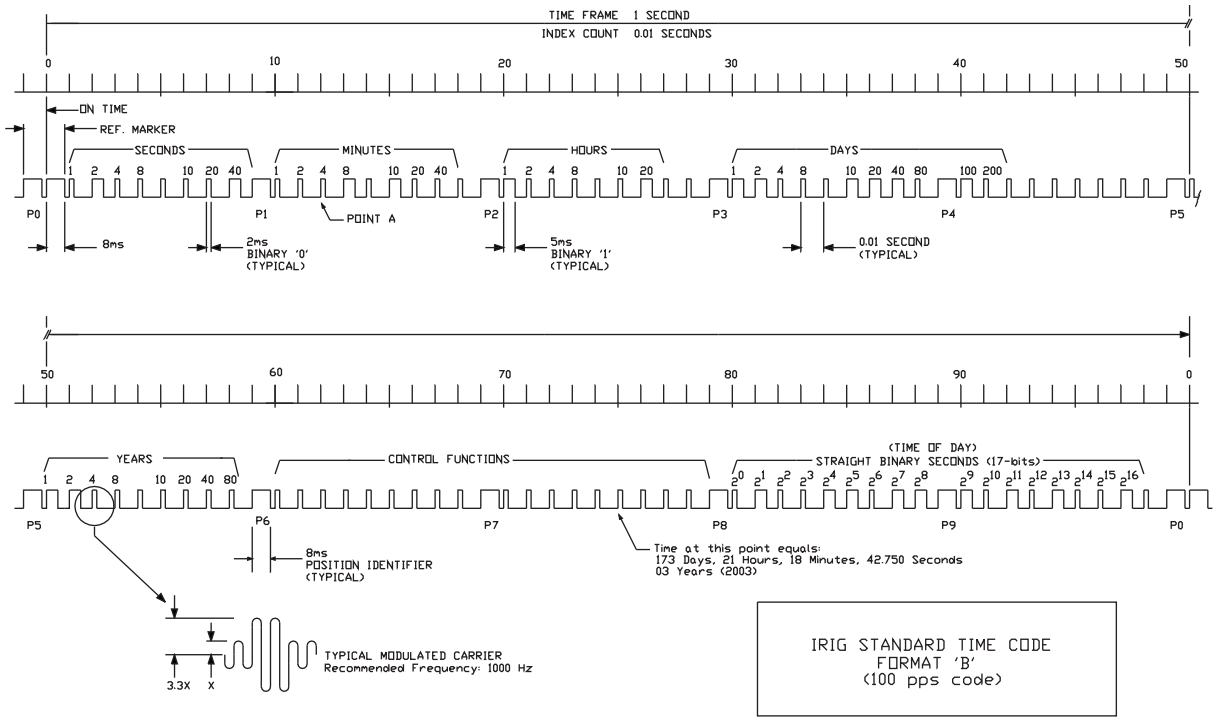


Image from Range Commanders Council Telecommunications and Timing Group IRIG Standard 200-04.

Figure E.1 IRIG-B Time-Code Format

This page intentionally left blank

Appendix F
X.509

Introduction

In cryptography, X.509 is an International Telecommunication Union standard for public key infrastructure (PKI). X.509 specifies formats for public key certificates and validation paths for authentication. The SEL-2488 uses X.509 certificates in the web server for secure device management, and for IPsec authentication.

Public Key Cryptography

Public key cryptography is distinguished by the use of asymmetric keys instead of the more traditional symmetric keys. Asymmetric keys are mathematically related so that whatever one key encrypts, the other key must be used to decrypt. There is no way to derive one key from knowledge of its paired key. These key pairs are known as public and private keys. The private key must be kept secret, while the public key can be distributed freely. This allows for many methods of protecting and authorizing messages that are not possible with symmetric key cryptography.

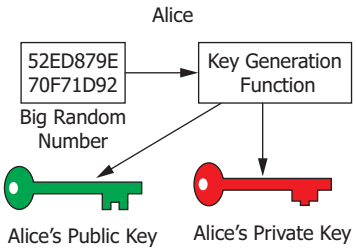


Figure F.1 Asymmetric Keys

Symmetric key cryptography, which has been used in various forms for thousands of years, uses a single key that both encrypts and decrypts the message. This key must be shared between the sender and receiver in advance. If the key cannot be shared securely, the confidentiality of any transmission encrypted with that key cannot be known.

In public key cryptography, the encryption key is not the same as the decryption key. If a message is encrypted with the publicly known key, only the private key can be used to decrypt it. This private key is known only to the owner of the key pair. Only the sender and the intended receiver will know the message, ensuring confidentiality.

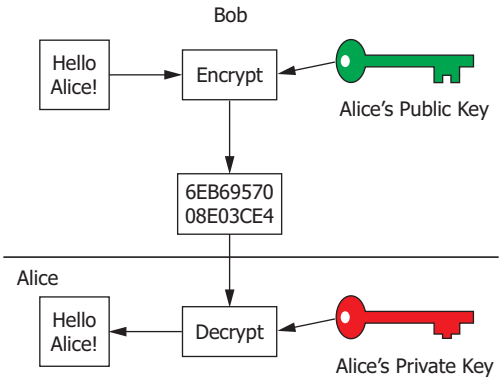


Figure F.2 Confidentiality With Asymmetric Keys

Public key cryptography is much more computation-intensive than symmetric key cryptography. This makes it infeasible to send large amounts of data, or secure a series of transmissions, using this technology. Public key cryptography offers confidentiality and the corresponding ability to exchange symmetric keys securely and confidentially. This is known as hybrid cryptography and is one way that IPsec uses public key cryptography.

You can also use public key cryptography for authentication. Do this by using a private key, rather than the public key, as the encryption key. The public key you use to decrypt the message will identify the sender. This is known as an electronic signature.

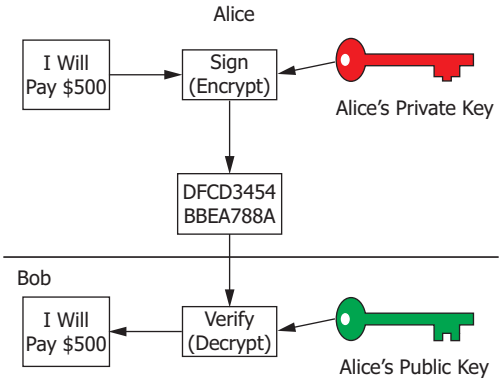


Figure F.3 Authentication With Asymmetric Keys

X.509 Certificates

Digital certificates, also known as public key certificates, provide a formal method for associating pairs of asymmetric keys with their owners. You can use these electronic documents, through the use of digital signatures, to bind public keys to their owners.

Digital Signatures

A digital signature is a more formal method of authenticating data than an electronic signature. They can be compared to the wax seals that were placed on envelopes before email was available. To create a digital signature of data, you would first compute a hash of the data to be signed and then encrypt that hash with the signer's private key. You would then attach this signature to the data to be signed. To verify the authenticity of the data, the receiver's system first separates data and signature. The receiver computes a hash of the data and then uses the issuer's public key to decrypt the signature. We compare these two hashes and, if they match, we know the data are authentic.

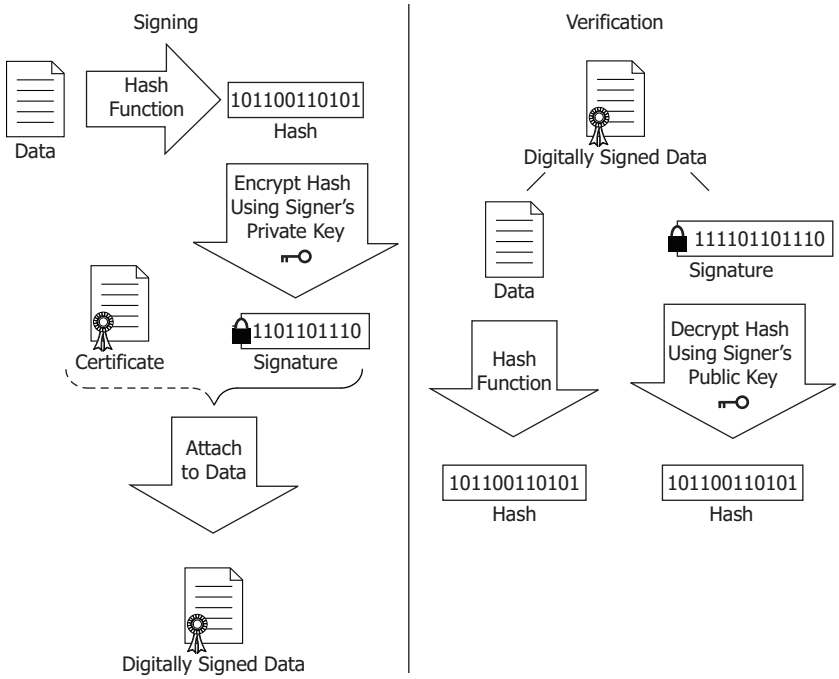


Figure F.4 Digital Signatures

Public Key Infrastructure

One of three common uses for digital certificates is in a public key infrastructure (PKI). PKI is a formal, hierarchical system where a digital certificate may contain the signature of one or a chain of more trusted certificate issuers. At the top of the PKI hierarchy is the most trusted certificate, a root certificate. A root certificate is self-signed, highly protected, and should only be used to sign Certificate Authority (CA) certificates. Root certificates have to be manually made trusted by a system administrator, or they must be included by the software vendor in a cache of trusted root certificates. Most modern operating systems, such as Microsoft Windows preload a collection of root certificates for commonly used (and trusted) certificate authorities (e.g., VeriSign, Thawte, etc.) in the "Trusted Root" certificate store. If a root certificate is compromised, we must assume all certificates below it to be compromised as well.

A certificate authority (CA) is an entity that issues, or signs, other certificates. To obtain a certificate, an entity (the "subject") will generate a key pair, and send the public key and proof of identity to a CA. The CA will verify the identity of the requester and issue the certificate containing the subject's identity, the public key, and the CA's digital signature. A CA is responsible for saying "yes" these people are whom they claim to be and this is their public key. CAs are authenticated by other CAs or by a root certificate.

An attacker can subvert this process. This can happen when an attacker steals the private key of a CA or of a party to whom a certificate was issued. It can also happen when an attacker impersonates another party when requesting a certificate. In either case, this can result in the issuance of untrustworthy certificates. An attacker might also steal a subject's private key. In such cases, these certificates must be revoked by the issuing authority.

Web of Trust

Another of the three common uses of digital certificates is in the web of trust. This is a less formal method of authentication than PKI provides, but is still in common use. The largest use of the web of trust model is in Pretty Good Privacy (PGP) used for email security. This model is very similar to PKI in that a trusted third party is verifying the authenticity of a certificate. The difference is that this trusted third party is not a CA, but rather a person who endorses the authenticity of another person. Signing the public key of the person requiring endorsement (or trust) with the endorser's (trusted entity) own private key establishes a web of trust. *Figure F.5* below illustrates a simple example of a web of trust. If Alice trusts Bob, and Bob trusts Charlie, then Alice implicitly trusts Charlie.

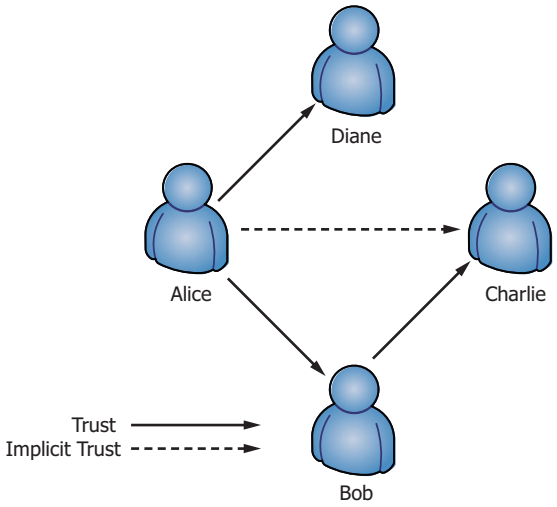


Figure F.5 Web of Trust

Simple Public Key Infrastructure

The third common use of digital certificates is in the simple public key infrastructure (SPKI). This model evolved from the need to limit the complexity inherent in PKI and the web of trust. There is no trusted third party

in SPKI, because the owner and issuer of the certificate are the same entity. For SPKI to be secure, certificates must be preshared among all entities who communicate on that system. This ensures that all knowledge for security decisions resides locally.

Online Certificate Status Protocol (OCSP)

In consideration of the case where an authentic certificate has been stolen, there are methods to revoke certificates. One method is the certificate revocation list (CRL). The CRL method has a few problems that allow a revoked certificate to still be used. This arises from the lag associated with producing CRLs. Also, a certificate will be accepted by default, even if revoked, if the CRL is not accessible.

The online certificate status protocol (OCSP) was created to fix some of these problems. OCSP requires less bandwidth than CRLs and enables near real-time status checks to verify a certificate's status. OCSP also allows a certificate to be denied by default if the OCSP server is not accessible.

OCSP is a request/response protocol that provides real-time revocation status information for X.509 certificates. When an OCSP-enabled certificate is presented to an application, such as a web browser, the browser uses OCSP to check the certificate and ensure it is valid before proceeding with the session. OCSP uses the following response indicators to help determine certificate revocation status:

- Good: Indicates that the certificate is valid and has not been revoked
- Revoked: Indicates that the certificate has been revoked
- Unknown: Indicates that the responder does not know about the certificate being requested

The system performs a real-time revocation check for each certificate so that if a certificate is compromised or for some other reason requires revocation, it will no longer appear as valid.

Sample X.509 Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,

OU=Certification Services Division,

CN=Thawte Server CA/Email=server-certs@thawte.com

```
        Validity
            Not Before: Aug  1 00:00:00 1996 GMT
            Not After: Dec 31 23:59:59 2020 GMT
        Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting
cc,
                 OU=Certification Services Division,
                 CN=Thawte Server CA/Email=server-certs@thawte.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                    68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                    85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                    6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                    6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                    29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                    6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                    5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                    3a:c2:b5:66:22:12:d6:87:0d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: md5WithRSAEncryption
        07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
        a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
        3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
        4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
        8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
        e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
        b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
        70:47
```

Appendix G
Configuring Windows Network Parameters

Using DHCP Configuration

The following steps show how to set a computer's network connection for automatic configuration through Dynamic Host Configuration Protocol (DHCP).

Step 1. Open the **Microsoft Windows Network Connections Control Panel**. Do this by typing **ncpa.cpl** in the Windows **Run** dialog box, as shown in *Figure G.1*. Selecting **OK** opens the **Network Connections** window, which contains a list of the network devices available on the computer.

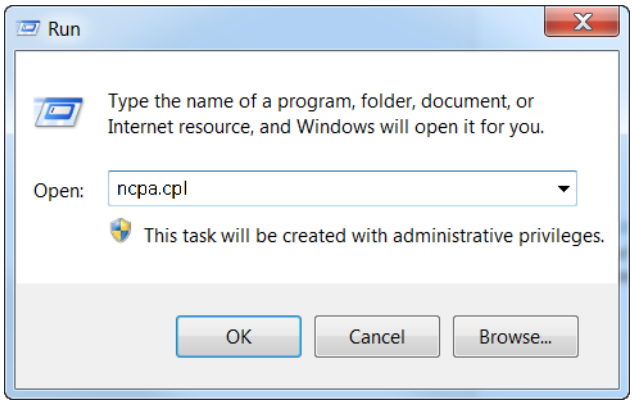


Figure G.1 Open Network Connections With Run Command

Step 2. Right-click the connection you will be using to communicate with the device and select **Properties** to display the **Connection Properties** window (see *Figure G.2*). The connection may be labeled **Local Area Connection**, as *Figure G.2* indicates.

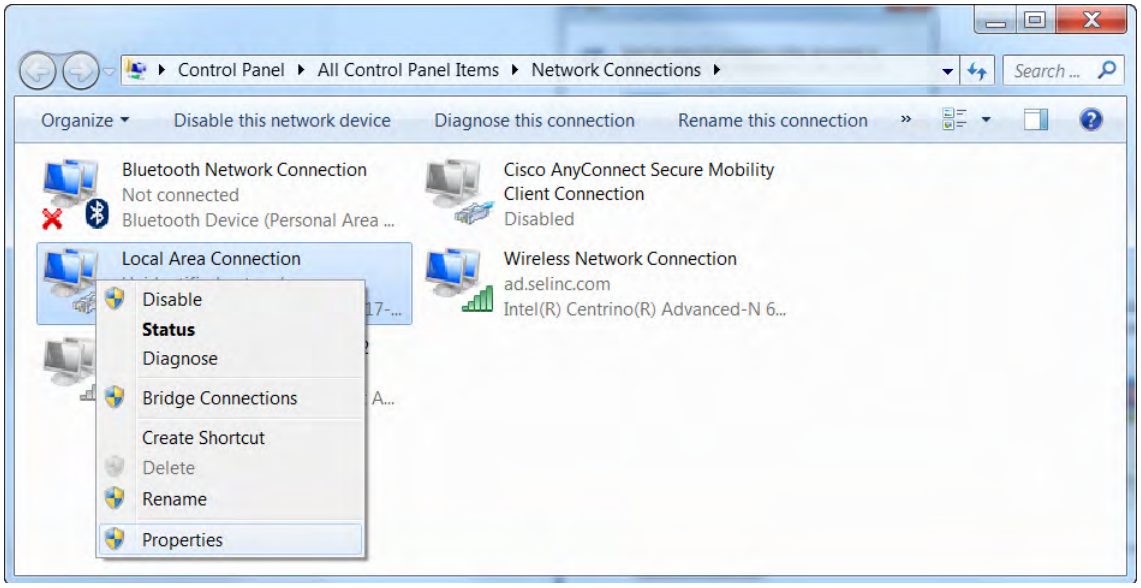


Figure G.2 Open Connection Properties

Step 3. Select **Internet Protocol Version 4 (TCP/IPv4)** and select **Properties**.

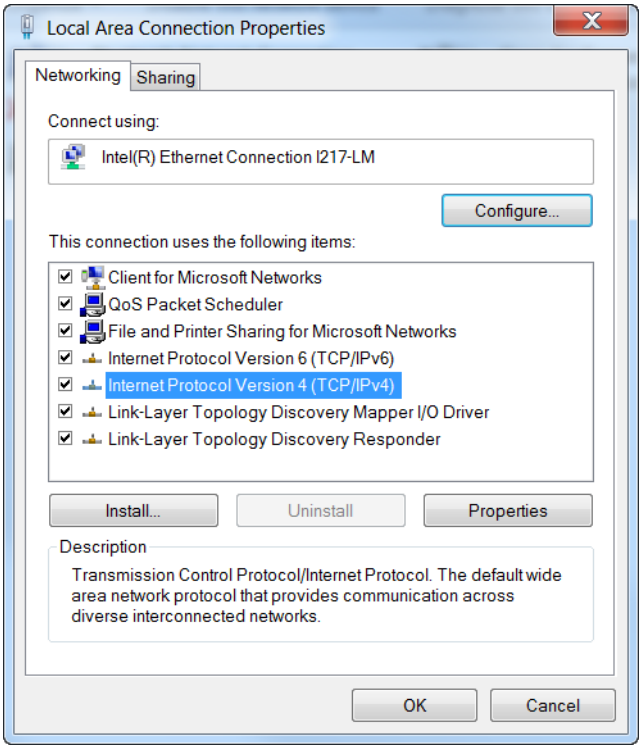


Figure G.3 Local Area Connection Properties

Step 4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. These are the usual settings for computers on a company network.

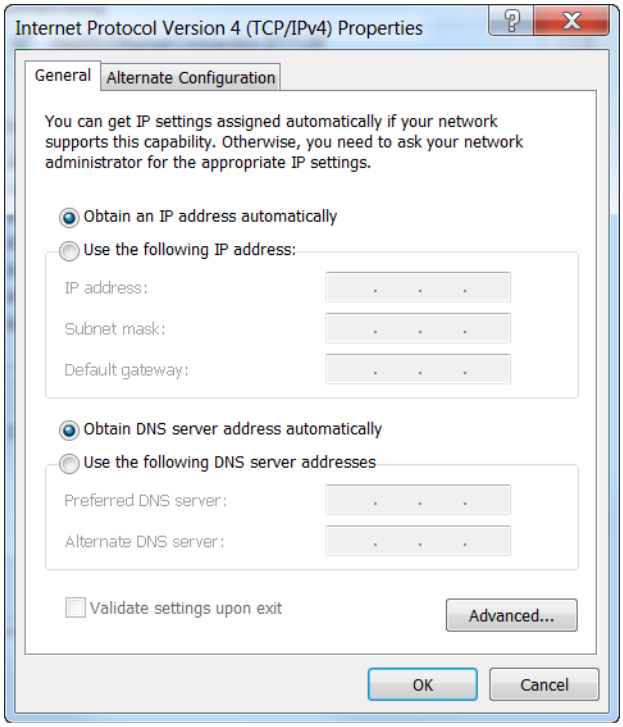


Figure G.4 TCP/IPv4 Properties–DHCP Configuration

Step 5. Select the **OK** button.

Using Static IP Configuration

The following steps show how to connect to the SEL-2488 by setting a computer's network configuration to a static Internet Protocol (IP) address.

Step 1. Open the **Microsoft Windows Network Connections Control Panel**. Do this by typing **ncpa.cpl** in the Windows **Run** dialog box, as shown in *Figure G.5*. Selecting **OK** opens the **Network Connections** window, which lists the network devices available on the computer.

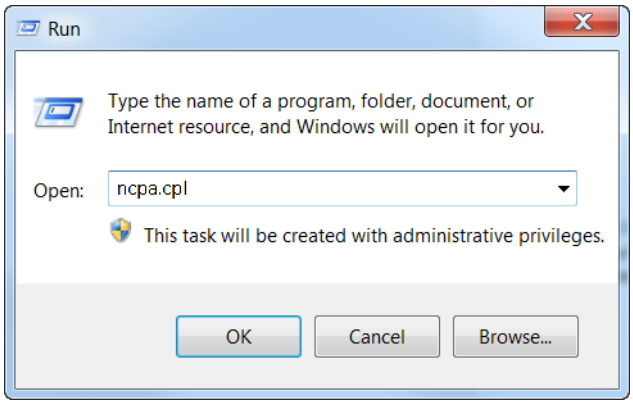


Figure G.5 Open Network Connections With Run Command

Step 2. Right-click on the connection you will use to communicate with the device and select the **Properties** option to display the Connection Properties window (see *Figure G.6*). The connection may be labeled **Local Area Connection**, as *Figure G.6* indicates.

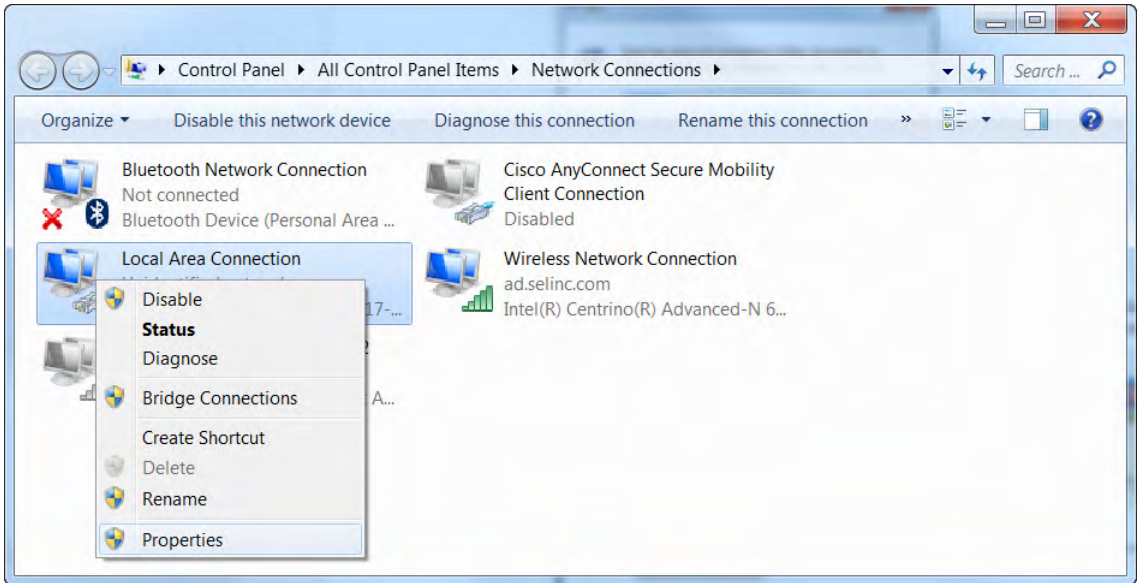


Figure G.6 Open Connection Properties

Step 3. Select **Internet Protocol Version 4 (TCP/IP)** and choose **Properties**.

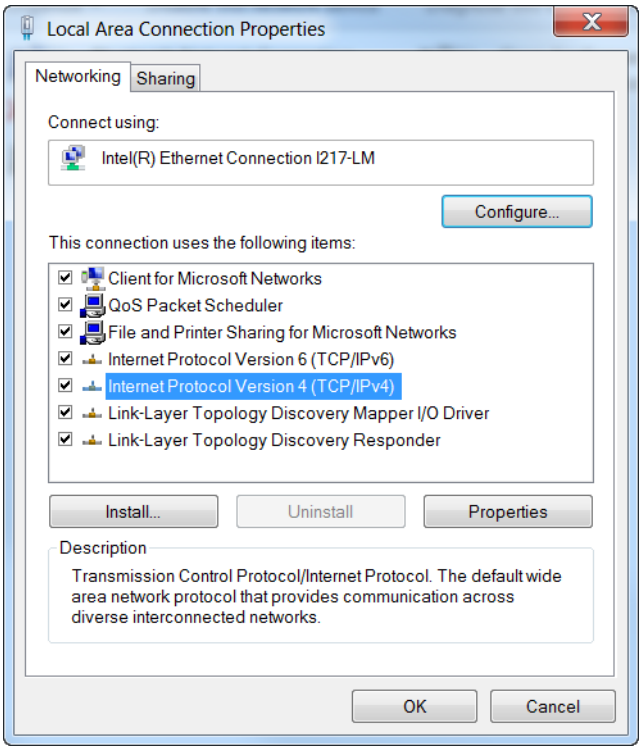


Figure G.7 Local Area Connection Properties

Step 4. Select **Use the Following IP Address** and choose an IP address and subnet for the computer. The subnet determines the valid range of IP addresses. By default, the subnet field is set to 255.255.255.0. This means that the first three sets of numbers in the IP address must be the same for both the clock and your computer.

By default, the IP address of the **ETH F** port is 192.168.1.2. If you leave the subnet mask at its default value, your computer can connect by using any IP address in the 192.168.1.*xxx* range where *xxx* is either 1 or a number from 3 to 254.

You do not have to choose a gateway. Although the domain name service (DNS) is set to manual configuration, you do not need to enter a configuration.

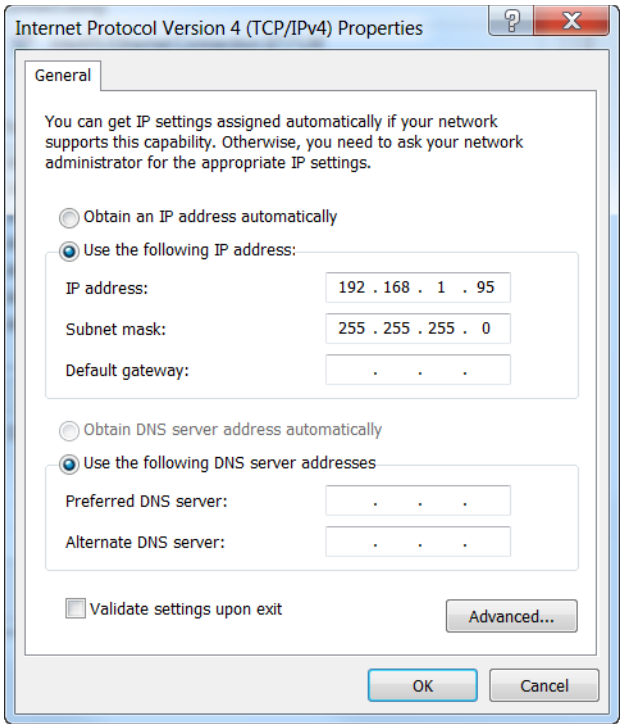


Figure G.8 TCP/IPv4 Properties—Manual Configuration

NOTE: If you configure your computer to use a static IP address, you will need to enter the IP address of the clock's management interface into your browser to access the clock.

Step 5. Select the **OK** button.

This page intentionally left blank

Appendix H

Lightweight Directory Access Protocol

The SEL Lightweight Directory Access Protocol (LDAP) client requires several pieces of information to configure the client to communicate with the LDAP servers. You can provide this form to the LDAP administrators to collect the information necessary to set up the SEL LDAP client.

Table H.1 LDAP Settings Form

LDAP Hosts (Input these settings on the Hosts page. At least one entry is necessary for each of the Hostname and Internet Protocol (IP) Address settings):	
Hostname:	IP Address:
Hostname:	IP Address:
LDAP Settings (Input these settings on the LDAP Settings page):	
TLS Required (Yes/No):	Synchronization Interval (Hours):
Search Base:	
User ID Attribute:	
Group Member Attribute:	
Bind DN (optional, if left blank device will use anonymous binds):	
Bind DN Password (optional, required only if you are not using anonymous binds):	
LDAP Servers (Input these settings on the LDAP Settings page At least one entry is necessary for each of the Hostname and Port Number settings):	
Hostname:	Port Number:
Hostname:	Port Number:
Device Roles (Entry of these settings on the LDAP settings page is necessary to map user privileges):	
Administrator Group/User DN:	
Engineer Group/User DN:	
User Manager Group/User DN:	
Monitor Group/User DN:	

In addition, you must provide the Certificate Authority root certificate for the LDAP servers if TLS authentication is required for connection to the LDAP servers.

This page intentionally left blank

Appendix I
Cybersecurity Features

The SEL-2488 Satellite-Synchronized Network Clock has a number of security features to assist users with meeting their cybersecurity design requirements.

Ports and Services

Physical Ports

The SEL-2488 has four Ethernet ports on the rear panel, and one Ethernet maintenance port on the front panel.

By default, only the front-panel maintenance port (**ETH F**) is enabled. All ports can be enabled or disabled. Ports that are not in use should be disabled.

IP Ports

All TCP/UDP ports can be disabled, and all are disabled by default (except for HTTPS and Captive Port [DHCP] on the **ETH F** interface). The **ETH F** interface is used to commission the device. There are a number of additional IP ports that can be opened by enabling services on the SEL-2488. *Table I.1* provides a summary of network ports and the settings that control them.

Table I.1 IP Port Numbers

IP Port Default	Port Selection Setting	Network Port Editable	Default Port State	Port Enable Setting	Purpose
68	UDP	No	Enabled	Enable DHCP	Dynamic Host Configuration Protocol (DHCP) on front-panel management port only
123	UDP	No	Disabled	Enable NTP server	Network Time Protocol (NTP)
161	UDP	No	Disabled	Enable SNMP	Simple Network Management Protocol (SNMP)
80	TCP	No	Disabled[a]	Enable Web Management	HTTPS web management interface (redirects to port 443)
443	TCP	No	Disabled[a]	Enable Web Management	HTTPS web management interface
319/320	UDP	No	Disabled	Enable PTP UDP mode	Precision Time Protocol

[a] HTTP/HTTPS on the ETH F interface is enabled by default. At least one interface must have HTTP/HTTPS enabled on the device at all times.

Authentication and Authorization Controls

The SEL-2488 has no default accounts or passwords. The first account, an administrator, is created when the unit is commissioned. Once commissioned, administrators can add additional accounts and define their roles as local accounts or by using centrally managed accounts.

The SEL-2488 has four predefined security roles on the device that dictate user privileges. These roles are administrator, engineer, user manager, and monitor.

User-Based Centrally Managed Accounts

The SEL-2488 supports the use of Lightweight Directory Access Protocol (LDAP) to implement role-based access controls using user-based accounts. Authorization level is based upon security group memberships of users. Communication with the LDAP server is protected by use of TLS.

Revocation or authorization changes for user-based accounts are centrally managed by your organization's directory service (e.g., Active Directory).

User-Based Local Accounts

The SEL-2488 supports local accounts for use when the directory service cannot be used. Administrators or user managers can create local accounts, assign the account role, and set or reset passwords. Local accounts can be removed or have their level of privilege changed through the web management interface.

The SEL-2488 supports and enforces strong passwords for local accounts. Passwords for local accounts must be at least 8 characters long, can have as many as 72 characters, and must include at least one uppercase character, one lowercase character, one numeral, and one symbol.

Local account passwords can be changed using the web management interface. Engineer and monitor users can change only their own account password. All account changes, including password changes, are logged.

Authentication Failures

The SEL-2488 logs authentication events. See *Logging Features* for more details.

On the third failure to authenticate (bad username or bad password) using either a local or centrally managed account, the SEL-2488 introduces a 30-second delay to prevent attempts to defeat account passwords by brute force. These events, as well as authentication failures, are logged.

X.509 Certificates

The SEL-2488 uses TLS with X.509 certificates to protect communications with the web management interface. The default certificate installed on the product is intended to be used for initial communication with the device at commissioning. This certificate must be replaced with a certificate provided by the customer's certificate authority. The SEL-2488 supports use of SHA-256 for signing and a key size of 1024, 2048, or 4096 bits.

Malware Protection Features

Software/Firmware Verification

The SEL-2488 has the ability to install firmware updates in the field via the web management interface. Firmware updates are signed by SEL and the signature is verified by the device before installation to ensure their authenticity and integrity.

Operating System/ Firmware

The SEL-2488 is an embedded device that does not allow third-party software to be installed. The SEL-2488 firmware includes a self-test that periodically checks the running firmware for integrity and activates the alarm contact if any corruption is detected. The SEL-2488 does not incorporate any other anti-malware features.

Logging Features

Security Events

The SEL-2488 logs include the following events that are significant to security:

- User login
- User logout
- Failed user login
- Login failure threshold (three failed logins in a row) reached
- Port state changes (link up/down)
- Hardware faults
- Settings changes
- Firmware upgrade
- Login session time-outs
- Internal log storage—75 percent and 90 percent of storage consumed by unacknowledged events
- GNSS satellite signal verification

Logins, logouts, login failures, login failure threshold reached, settings changes, and hardware failures will also result in activation of an alarm contact on the device.

Syslog

The SEL-2488 uses syslog to report events to as many as three network syslog servers, as well as activating an alarm contact for significant events.

SNMP

The SEL-2488 supports SNMP v2c notification generation with designation of as many as three SNMP Trap Servers to receive notification events (authentication success/failure, hardware faults, settings changes, link up/down events, and time events). SNMP capabilities of the SEL-2488 are described in management information base (MIB) files that can be downloaded from the web management interface of the device.

Internal Log Storage

The SEL-2488 stores logged events in internal memory as well as transmitting them to an external server. Internal storage can hold as many as 60,000 events. In the event that storage is full, new events will replace the oldest events.

Configuration Control Support

Product Version Information

The SEL-2488 firmware revision number (FID) provides the current firmware version/patch level.

The FID can be found on the **Dashboard** page of the web management interface or on the front-panel LCD.

Backup and Restore

Saving and Restoring Settings

The SEL-2488 supports export and import of all configuration information through use of the web management interface or ACSELERATOR QuickSet SEL-5030 Software. Settings information files can be encrypted with a user-supplied password.

Decommissioning

Preparing for Recycling or Disposal

Typically, you should erase the settings from the device when it is removed from service. You can completely erase all the configuration settings and logging information from the SEL-2488 and return it to factory-default settings by using the **Device Reset** page of the web management interface or by using the pinhole reset on the rear panel of the SEL-2488.

Once this procedure is complete, all internal user settings and passwords will be erased. Depending on the reason for return, you may not want to erase settings information when returning an SEL-2488 to SEL for service. Settings information is useful to SEL for diagnosing many problems. For security reasons, all local accounts should be set to new strong passwords before the unit is returned.

Vulnerability Notification Process

Security Vulnerability Process

SEL provides security disclosure alerts to customers, and SEL manuals document all releases. SEL security vulnerability disclosures are described in SEL's policy document “The SEL Process for Disclosing Security Vulnerabilities” located at selinc.com/security_vulnerabilities/.

Emailed Security Notification

The SEL webpage offers a place for customers to sign up for direct notification by email when SEL releases security vulnerability notices or service bulletins at selinc.com/support/security-notifications/.

Contact SEL

For further questions or concerns about product security please contact SEL by email at security@selinc.com or by phone at 1.509.332.1890.