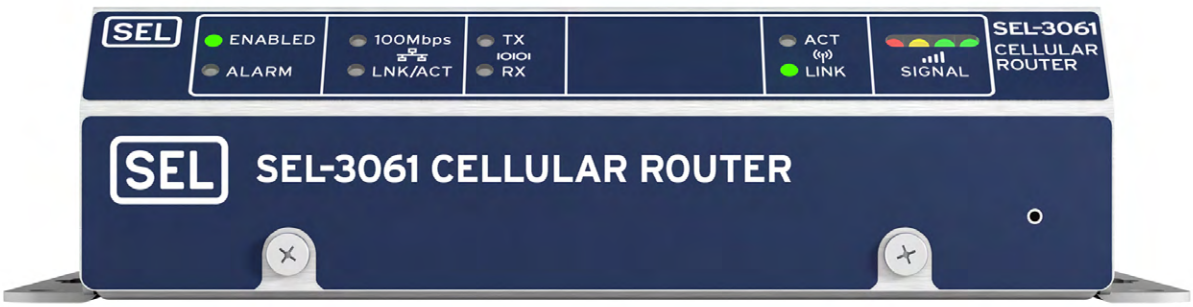
SEL-3061

Cellular Router

Instruction Manual



20210715

SEL SCHWEITZER ENGINEERING LABORATORIES

PM3061-01

Table of Contents

This page intentionally left blank

List of Tables

This page intentionally left blank

List of Figures

This page intentionally left blank

Preface

Overview

This manual provides information and instructions for installing, setting, configuring, and operating the SEL-3061 Cellular Router. The manual is for use by communications engineers, technicians, and others experienced in communications and network infrastructure.

Preface. Provides the manual overview, as well as safety and general information about the product.

Section 1: Introduction and Specifications. Introduces SEL-3061 features, summarizes functions, and lists specifications, type tests, and ratings.

Section 2: Installation and Getting Started. Explains the basic steps to install, configure, and commission the SEL-3061.

Section 3: Applications. Describes typical scenarios that benefit from applying the SEL-3061.

Section 4: Network Settings. Provides information on setting up an Ethernet network (LAN), cellular network (WAN), PPP-IP Passthrough mode (modem), and Generic Routing Encapsulation (GRE) tunnels.

Section 5: Systems. Describes system settings including access configuration, Global settings, date and time, usage policy, user accounts, RADIUS, file management, X.509, and device reset.

Section 6: Serial Communications. Provides information to set serial port communications.

Section 7: Security. Describes security features that include IPsec VPN and firewalls.

Section 8: Diagnostics and Logging. Explains system diagnostics; events logging; alarm notifications, such as Syslog, notifications/alarms, alarm contacts; and methods of sending alarms via email and SMS.

Section 9: Troubleshooting. Describes techniques for maintenance and troubleshooting the SEL-3061.

Section 10: Job Done Examples. Describes several Job Done examples for typical applications, such as configuring IPsec VPN and data collection by using DNP3 and Modbus.

Section 11: SNMP. Provides information to configure SNMP servers and trap servers.

Appendix A: Firmware and Manual Versions. Lists the current firmware versions and details differences between the current and previous versions.

Appendix B: Firmware Upgrade Instructions. Describes the process for upgrading firmware.

Appendix C: Syslog. Lists the available SEL-3061 Syslog messages for local and remote notification.

Appendix D: X.509. Describes the SEL-3061 security certificates for the Ethernet and wireless interfaces.

Appendix E: SEL RADIUS Dictionary. Contains the descriptions of the attributes that are supported by the SEL-3061.

Appendix F: Notifications and Alarms List. Provides a list of events that can be reported via SNMP, email, and text messages (short message service [SMS]).

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 Renata CR1632 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 Renata CR1632 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.
For use in Pollution Degree 2 environment.	Pour utilisation dans un environnement de Degré de Pollution 2.
Terminal Ratings Wire Material Use 75°C (167°F) copper conductors only. Tightening Torque Terminal Blocks: 0.79 Nm (7 in-lb)	Spécifications des bornes Type de filage Utiliser seulement conducteurs en cuivre 75°C (167°F). Couple de serrage Borniers : 0,79 Nm (7 livres-pouce)
The separate protective earthing terminal shall be permanently connected to earth.	Courant de fuite éléve. Raccordement à la terre indispensable avant le raccordement au réseau.

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** Mettre hors tension ou 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.
⚠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, blesser 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 Atmospheric electrical charge accumulation can impose a standing electric potential difference between the conductor and shield of the feed line. In extreme cases, a lightning strike imposes a dangerous voltage surge. A surge protector should be installed to prevent damage to equipment or injury to personnel.	**⚠AVERTISSEMENT** L'accumulation de charges électriques peut être la cause d'une différence de potentiel électrique entre le conducteur et le blindage de la ligne d'alimentation. Dans des cas extrêmes, la foudre entraîne une surtension dangereuse. Un parafoudre devrait être installé pour prévenir les dommages à l'équipement ou les blessures au personnel.
⚠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.

Other Safety Marks (Sheet 2 of 2)

⚠CAUTION In order to avoid losing system logs on a factory-default reset, configure the SEL-3061 to forward Syslog messages to a remote Syslog server.	**⚠ATTENTION** Pour éviter de perdre l'historique du système (Syslog) sur un redémarrage défini par défaut, configurer le SEL-3061 pour transmettre les messages Syslog à un serveur Syslog à distance.
⚠CAUTION Do not remove the front panel or replace the SIM card while the device is energized.	**⚠ATTENTION** Ne pas enlever le panneau avant ou remplacer la carte SIM lorsque le dispositif est sous tension.

General Information

Typographic Conventions

This instruction manual uses several example illustrations and instructions to explain how to effectively operate the SEL-3061. These examples are for demonstration purposes only; the firmware identification information and settings values included may not match those in your SEL-3061.

The instructions in this manual indicate these options with specific font and formatting attributes. The following table lists these conventions:

Example	Description
STATUS	Commands, command options, and command variables typed at a command line interface on a PC.
<Enter>	Single keystroke on a PC keyboard.
<Ctrl+D>	Multiple/combination keystroke on a PC keyboard.
Start > Settings	PC software dialog boxes and menu selections. The > character indicates submenus.
ENABLE	Relay front- or rear-panel labels.

Trademarks

All brand or product names appearing in this document are the trademark or registered trademark of their respective holders. No SEL trademarks may be used without written permission.

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

SEL Trademarks	
Axion®	Job Done®
Falcon™	

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

Introduction and Specifications

Overview

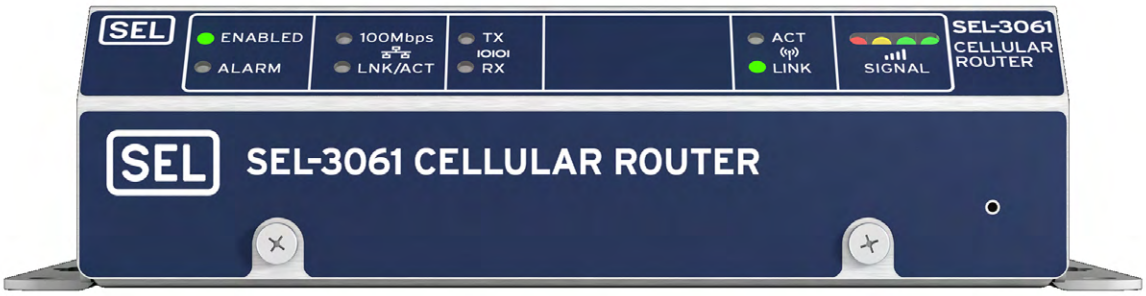


Figure 1.1 SEL-3061 Cellular Router

The SEL-3061 Cellular Router provides network connectivity through 4G LTE cellular networks and is designed for the harsh environments commonly found in the energy, industrial, and utility sectors. The SEL-3061 provides secure wireless connectivity to a variety of field devices or serves as a backhaul through the use of the cellular network. The SEL-3061 has three variants; two of them operate on 4G LTE networks and one on HSPA+ networks (also known as 3G networks). The three cellular operator carriers that are supported in the U.S. are: AT&T, Verizon, and T-Mobile. The SEL-3061 supports Telus, Rogers, and Bell networks in Canada.

The SEL-3061 operates as either a router (Layer 3 device) or a cellular modem in PPP-IP Passthrough mode (Layer 2 device).

- As a router, the SEL-3061 provides secure network access through a cellular gateway or cell towers.
- In PPP-IP Passthrough mode, the SEL-3061 provides network access for the connected device as a modem.

System Benefits

The SEL-3061 can serve as the wireless communications link for field devices, such as a recloser control, or as a backhaul for concentrated data from a network. Using a well-established wireless broadband network eliminates the need for a physical network connection. This connection freedom allows for installation anywhere there is a cellular signal.

You can add one or more SEL-3061 Cellular Routers to expand your network without making adjustments to existing network devices. The SEL-3061 uses industry standard protocols that can help in the integration of devices or networks depending on your application needs (see *Section 3: Applications*).

The following is a list of key benefits of the SEL-3061:

- Cellular wireless connectivity provides access to remote equipment and installations.
- Comprehensive security methods ensure the confidentiality integrity of data.
- A web interface simplifies configuration and provides device management and diagnostic information.
- Broad carrier support enables fast deployment across the U.S.A.
- Designing and testing to protective relay standards ensures electromagnetic compatibility and surge immunity.

Product Overview

Front-Panel Overview

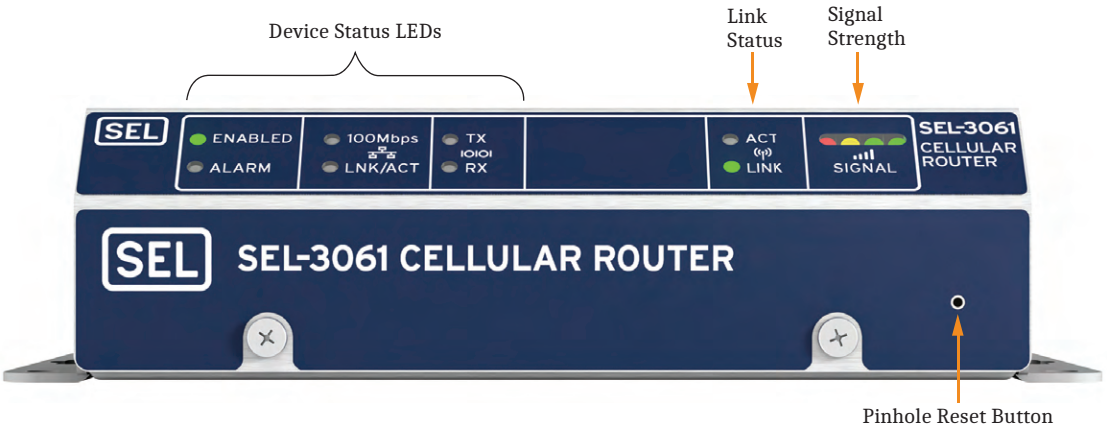


Figure 1.2 Front-Panel Overview

Device Status LEDs

The green **ENABLED** LED illuminates when the unit has passed the self-tests and is operational. This LED is not illuminated during startup. The **ALARM** LED illuminates when the unit asserts an alarm. A one-second blink indicates a minor alarm, while solid red indicates a major alarm. The **ALARM** LED is described in more detail in *Notifications and Alarms on page 8.13*.

Port Activity

The SEL-3061 includes duplicate LEDs of the rear-panel, Ethernet LEDs on the front panel to conveniently indicate rear-panel, Ethernet port status and activity. The amber **100Mbps** LED indicates port speed, and the green **LINK/ACT** LED indicates link activity. See *Ethernet Network Interface (LAN) on page 4.1* for more information.

Additionally, a pair of front-panel LED indicators display serial port activity. The green **TX** LED indicates serial port data transmission and the red **RX** LED indicates serial port data reception. See *Section 6: Serial Communications* for more information.

Cellular Link Indicator LEDs

The cellular link LEDs indicate the status and quality of the cellular connection.

The green **LINK** LED illuminates when the SEL-3061 establishes a connection with a cellular network.

The green **ACT** LED illuminates when the SEL-3061 is actively communicating data across the cellular network.

The four-segment multicolored **LINK QUALITY** indicator represents the received signal strength of the cellular coverage.

Pinhole Reset Button

The front panel includes a pinhole reset button with three functions:

- To illuminate all front-panel LEDs for a lamp test
- To restart the device
- To reset the SEL-3061 to factory defaults

See *Pinhole Reset Button on page 5.33*.

Rear-Panel Overview

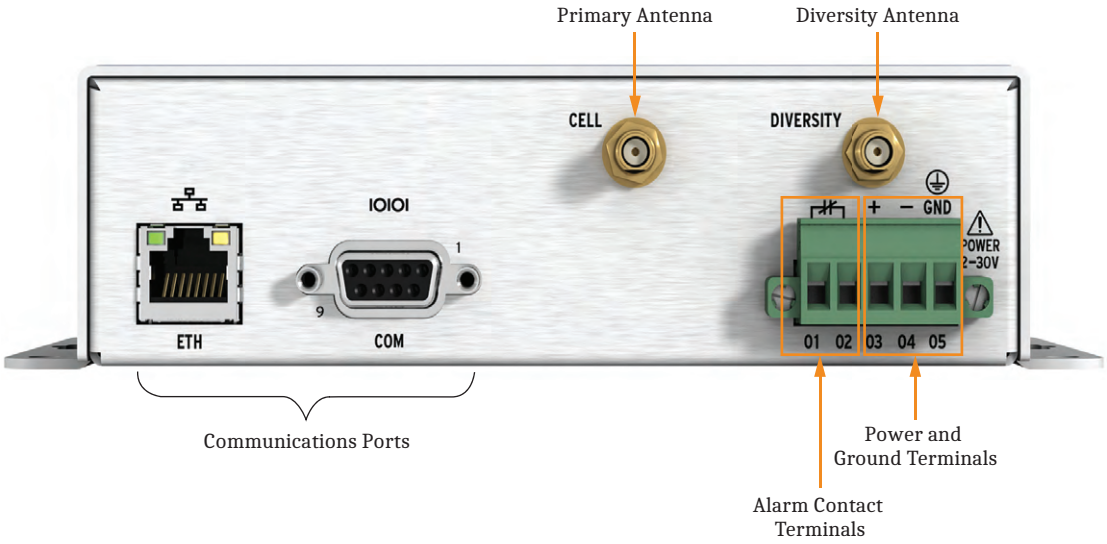


Figure 1.3 Rear-Panel Overview

Ethernet Port and Serial Port

The Ethernet port supports 10/100 Mbps via copper connectors. The serial port is a DCE DB-9 female connector. The Ethernet port includes LED indicators that provide the same status and activity display that is available on the front panel.

Cellular Antennas

The SEL-3061 is equipped with two SubMinature version A (SMA) antenna input ports. The **Cell** port is the main cellular antenna and the **Diversity** port is the diversity cellular antenna. *Antenna on page 2.1* describes the diversity antenna feature.

Alarm Contact

The rear-panel connector provides one Form B output mechanical alarm contact. This contact provides notifications of various alarms on the system. *Alarm Contact and LEDs on page 8.18* describes the alarm contact in more detail.

SEL-3061 Web Interface

Commission and manage the SEL-3061 through use of the HTTPS web interface. The SEL-3061 supports Dynamic Host Configuration Protocol (DHCP) on the Ethernet port to provide an easy initial connection to the device. Secure access is controlled by using X.509 certificates, user-based accounts stored locally on the device, and Remote Authentication Dial-In User Service (RADIUS). The device interface includes a dashboard display of the device status and diagnostics, as shown in *Figure 1.4*.

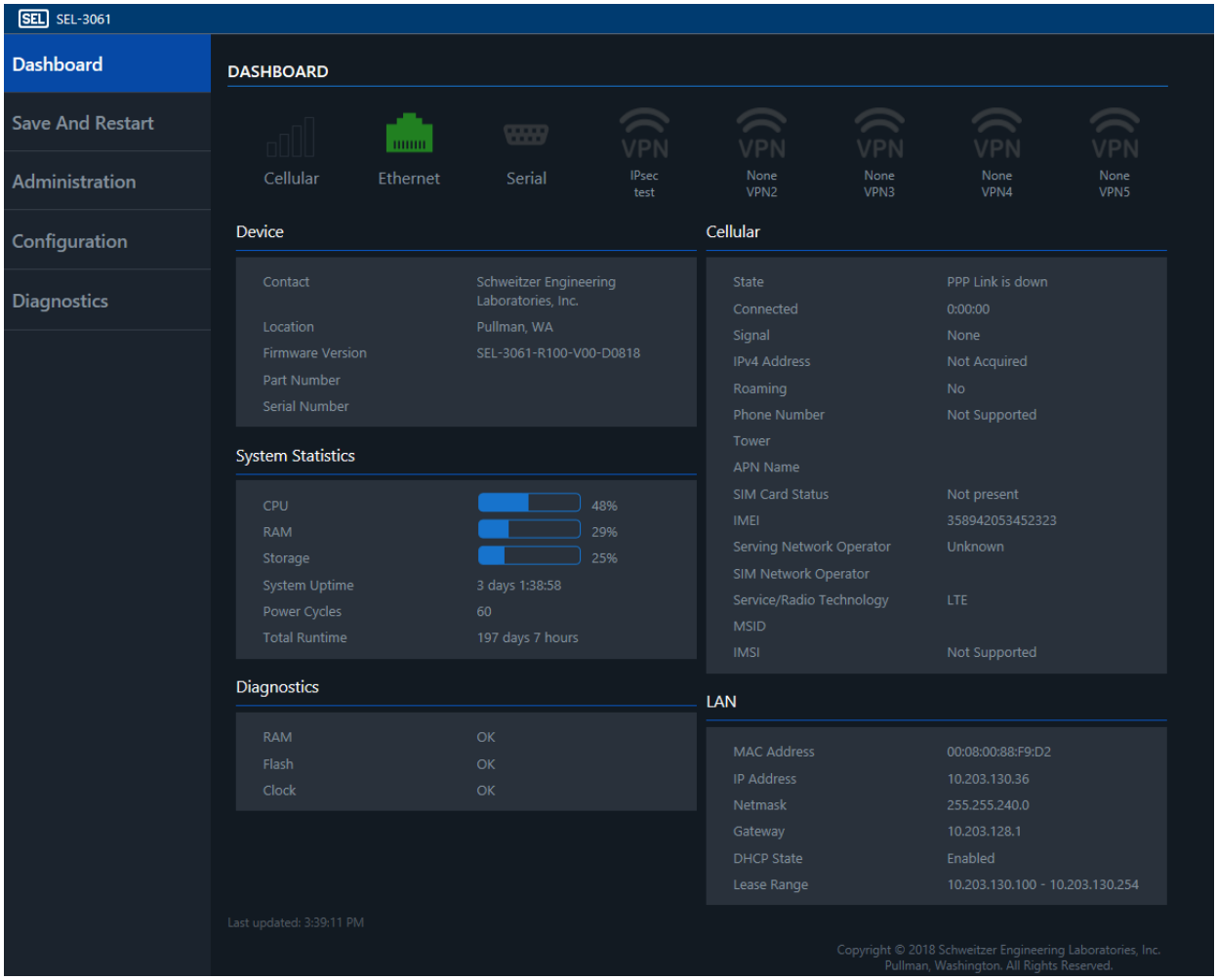


Figure 1.4 Device Interface Dashboard Display

Options

Device Options

The SEL-3061 has the following product options:

Carrier Network

The SEL-3061 hardware varies depending on the carrier network. In the U.S. the SEL-3061 supports AT&T, Verizon, and T-Mobile networks. In Canada, the SEL-3061 supports Telus, Rogers, and Bell networks. SEL does not offer SIM cards or data plans.

Accessories

For more information on the SEL-3061 accessories and antenna installation, see *Section 2: Installation and Getting Started* or the *SEL Radio Accessories Guide* on the SEL website (selinc.com).

Specifications

Compliance

Designed and manufactured under an ISO 9001 certified quality management system

Networking

Network Management

HTTPS Web User Interface

Settings Import/Export

Virtual Private Networks

Maximum Concurrent Sessions:	5
Security Protocol:	IPsec
Key Exchange:	IKEv1, IKEv2
Authentication:	Passphrase
Nonaccelerated Encryption Algorithms:	AES, 3DES
Encryption Key Strength:	128-bit, 256-bit

Firewall Functions

Network Address Translation:	Port Forwarding (DNAT)
Network Address Translation:	Outbound NAT (SNAT)

Input Traffic Filtering

Output Traffic Filtering

Forward Traffic Filtering

Ethernet Protocols

Address Resolution Protocol (ARP)

Distributed Network Protocol 3 (DNP3)

Dynamic Host Configuration Protocol (DHCP) Client

Encapsulating Security Payload (ESP)

File Transfer Protocol (FTP)

Hypertext Transfer Protocol Secure (HTTPS)

Internet Control Message Protocol (ICMP)

Internet Key Exchange (IKEv1/v2)

Internet Protocol Security (IPsec) Protocol Suite

Internet Secure Association and Key Management Protocol (ISAKMP)

Modbus TCP/IP

Network Time Protocol (NTP) Client

Online Certificate Revocation Protocol (OCSP)

Remote Authentication Dial-In User Service (RADIUS)

Secure Shell version 2 (SSHv2) Client/Server

Simple Network Management Protocol (SNMP)

Spanning Tree Protocol (STP) Syslog

Transmission Control Protocol (TCP)

Transport Layer Security (TLS)

User Datagram Protocol (UDP)

Security

User-Based Accounts

Password Length:	8–4096 characters
Password Set:	A–Z, a–z, 0–9, special characters
User Roles:	Administrator, Engineer, Monitor

Syslog

Storage for 30,000 local Syslog messages

SNMP

Monitors diagnostics through SNMP v1, v2c, and v3 read operations

Sends notifications by using SNMP v1, v2c, and v3 traps

Supports as many as three active SNMP servers and SNMP trap servers

Firewall

Implementation:	iptables

Cellular WAN

Frequency Band (MHz):	4G: 700 (B17)/850 (B5)/AWS1700 (B4)/1900 (B2)/700 (B13)
3G/2G (AT&T and T-Mobile Only):	850 (B5)/1900 (B2)
Technology:	4G, LTE 3G/2G fallback (AT&T and T-Mobile Only)

Data Rate

As much as 100 Mbps downlink

As much as 50 Mbps uplink

Transmit Output Power

0.2 W (23 dBm), Class 3

General

Operating Temperature

–40° to +75°C (–40° to +167°F)

Storage Temperature

–40° to +75°C (–40° to +167°F)

Operating Environment

Pollution Degree:	2
Relative Humidity:	15%–93%, noncondensing
Maximum Altitude:	2000 m

Dimensions

Wall Mount:	151 mm x 104 mm x 44 mm (5.96 in x 4.08 in x 1.73 in)

Alarm Output

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

Communications Ports

Ethernet Port

Port:	1, rear

10/100BASE-T Copper (RJ45 Connector)

Rear Connectors:	RJ45
Standard:	IEEE 802.3

Serial Port

Port:	1 EIA-232
Rate:	300 bps, 600 bps, 1200 bps, 1800 bps, 2400 bps, 4800 bps, 9600 bps, 19200 bps, 38400 bps, and 57600 bps
Rear Connectors:	9-pin D-Subminiature

Power Supply

Input Voltage Range:	12–30 Vdc
Power Consumption:	<5 W

Product Standards

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

Note: Tests apply to the SEL-3061 only and not to data transfer over the cellular WAN.

Type Tests

Environmental Tests

Vibration Resistance:	IEC 60255-21-1:1988 Class 2 Endurance, Class 2 Response IEC 60255-21-3:1993 Class 2
Shock Resistance:	IEC 60255-21-2:1988 Class 1 Shock Withstand Bump, Class 2 Shock Response
Cold:	IEC 60068-2-1:2007 –40°C, 16 hours
Damp Heat, Cyclic:	IEC 60068-2-30:2005 25–55°C, 95% relative humidity, 6 cycles
Dry Heat:	IEC 60068-2-2:2007 +75°C, 16 hours

Dielectric Strength and Impulse Tests

Dielectric (HiPot):	IEC 60255-27:2013 IEEE C37.90-2005
Impulse:	IEC 60255-5:2000 0.5 J, 5 kV 1.0 kV on Ethernet Ports

RFI and Interference Test

Electrostatic Discharge:	IEC 61000-4-2:2009 Severity Level 4 8 kV contact discharge 15 kV air discharge IEEE C37.90.3-2001 Severity Level 3 8 kV contact discharge 15 kV air discharge
Radiated RF Immunity:	IEC 61000-4-3:2005+A1:2008+A2:2010 10 V/m
Fast Transient Burst Immunity:	IEC 61000-4-4:2012 4 kV @ 5.0 kHz for power port 2 kV @ 5.0 kHz for communications ports
Power Frequency Magnetic Field:	IEC 61000-4-8:2009 1000 A/m for 3 seconds, 100 A/m for 1 minute
Interruptions and Voltage:	IEC 61000-4-11:2004 +A1:2017
Variations on DC Input:	IEC 61000-4-17:1999+A1:2001+ A2:2008
Power Port:	IEC 61000-4-29:2000
Surge Withstand:	IEC 61000-4-18:2005+A1:2010
Capability Immunity:	2.5 kV common-mode, 1 kV differential-mode
Conducted RF Immunity:	IEC 61000-4-6:2013 10 Vrms
Surge Immunity:	IEC 61000-4-5:2005 Zone B: 0.5; 1.0 kV; line-to-line Zone B: 0.5; 1.0; 2.0 kV; line-to-earth

EMC Emissions

Radiated Emissions:	CISPR 11:2009+A1:2010 CISPR 22:2008 ANSI C63.4:2015 47 CFR Part 15.107, 109

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

FCC Part 15, Class A

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 is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Section 15.21

User's manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Canada ICES-001(A) / NMB-001(A)

This page intentionally left blank

SECTION 2

Installation and Getting Started

Installation

SIM Card

NOTE: SEL does not offer SIM cards or data plans. Consult your network provider to purchase a data plan.

⚠CAUTION
Do not remove the front panel or replace the SIM card while the device is energized.

The SEL-3061 Cellular Router requires a Subscriber Identity Module (SIM) card to access the network. A SIM card is specific to a particular network operator.

A standard SIM card, also known as 2FF or Mini, is required. Its size is 25 x 15 mm.

To install the SIM card:

Step 1. Unscrew the two screws on the front panel of the device.

Step 2. Lift the hinged front panel.

Step 3. Insert the SIM card into the SIM card holder located on the top of the smaller circuit board, and push the card all the way to the end. Ensure the card is oriented in the correct direction with the metallic side of the card facing down and the 45-degree corner of the SIM card facing the front panel of the device.

To remove the SIM card, pull the SIM card out of the SIM card holder.

Antenna

The SEL-3061 uses public cellular carriers as the wireless service provider. Before installing the SEL-3061, confirm that you have cellular coverage in the desired area. If the cellular coverage is poor, you can improve your signal by raising the antenna to provide better line of sight to cell towers or by using low-loss cables. Refer to the *SEL Radio Accessories Guide* for more information.

The SEL-3061 requires two antennas operating simultaneously to provide diversity. The SEL-3061 receives signals by using both antennas and transmits signals by using the primary antenna. Use two of the available antennas offered by SEL for your installation (see *Table 2.1*). SEL recommends using the same antenna for both the primary antenna and the diversity antenna.

Table 2.1 Available Antennas

Part Number	Description
235-0003	Low-Profile 3 dBi Omnidirectional, 698–960 MHz, 1710–2700 MHz, N Female Connector
235-0242	Indoor Right-Angle Antenna, 698–960 MHz, 1710–2700 MHz, SMA Male Connector

In a permanent indoor installation, place the cellular antennas above the building roof, above maximum snow accumulation, and away from roof maintenance activities. If the SEL-3061 is in an outdoor cabinet, mount the antennas to a utility pole by using the optional antenna-mounting hardware shown in *Table 2.2*.

Table 2.2 Optional Antenna-Mounting Hardware

Part Number	Description
915900497	Mounting bracket for two 235-0003 antennas

Feed Lines

A significant amount of signal strength can be lost in the feed line cables, so choosing the correct cabling is important. Coaxial cables should have low attenuation and be rated for outdoor use. Keep the feed lines as short as possible to minimize signal loss between the radio and antenna. Use LMR-400 coaxial cables for most cable runs. If you require longer lengths or less loss for the radio link, larger cables, such as Andrew HELIAX, can be used. Cable losses are dependent on the signal frequency, with higher frequency signals experiencing more loss. The highest frequency supported by the SEL-3061 is 2155 MHz. *Table 2.3* lists the signal losses (in dB) for the indicated lengths of each cable type at this frequency. Usually, the losses are significantly less if the radio is operating at lower frequencies.

Table 2.3 Signal Loss at 2155 MHz

Cable Type	Characteristic Impedance	3.05 m (10 ft)	12.24 m (50 ft)	30.48 m (100 ft)
RG-8X (SEL-C980 or SEL-C964)	50 Ω	2.0 dB	10.1 dB	Do Not Use
LMR-400 (SEL-C966 or SEL-C968)	50 Ω	0.6 dB	3.1 dB	6.2 dB
7/8" HELIAX (SEL-C978)	50 Ω	Do Not Use	1.0 dB	1.9 dB

SEL offers a variety of cables to support the SEL-3061 feed lines. Every feed line should consist of a cable from the SEL-3061 to the surge protector and another cable from the surge protector to the antenna. The SEL-3061 is equipped with SMA female connectors. The surge protector and antenna have N female connectors.

The following sections describe three different installation scenarios, which correspond to different feed line configurations.

Cabinet Installation

In a cabinet installation, you need two short cables going from the SEL-3061 to the surge protectors mounted on the base of the cabinet and additional cables going to the antennas. In installations with good cellphone service coverage, having the antennas 10 to 15 feet above the cabinet is likely to be satisfactory. It may be beneficial to increase the antenna height to improve line of sight to the cell tower, but that comes with increased cable loss.

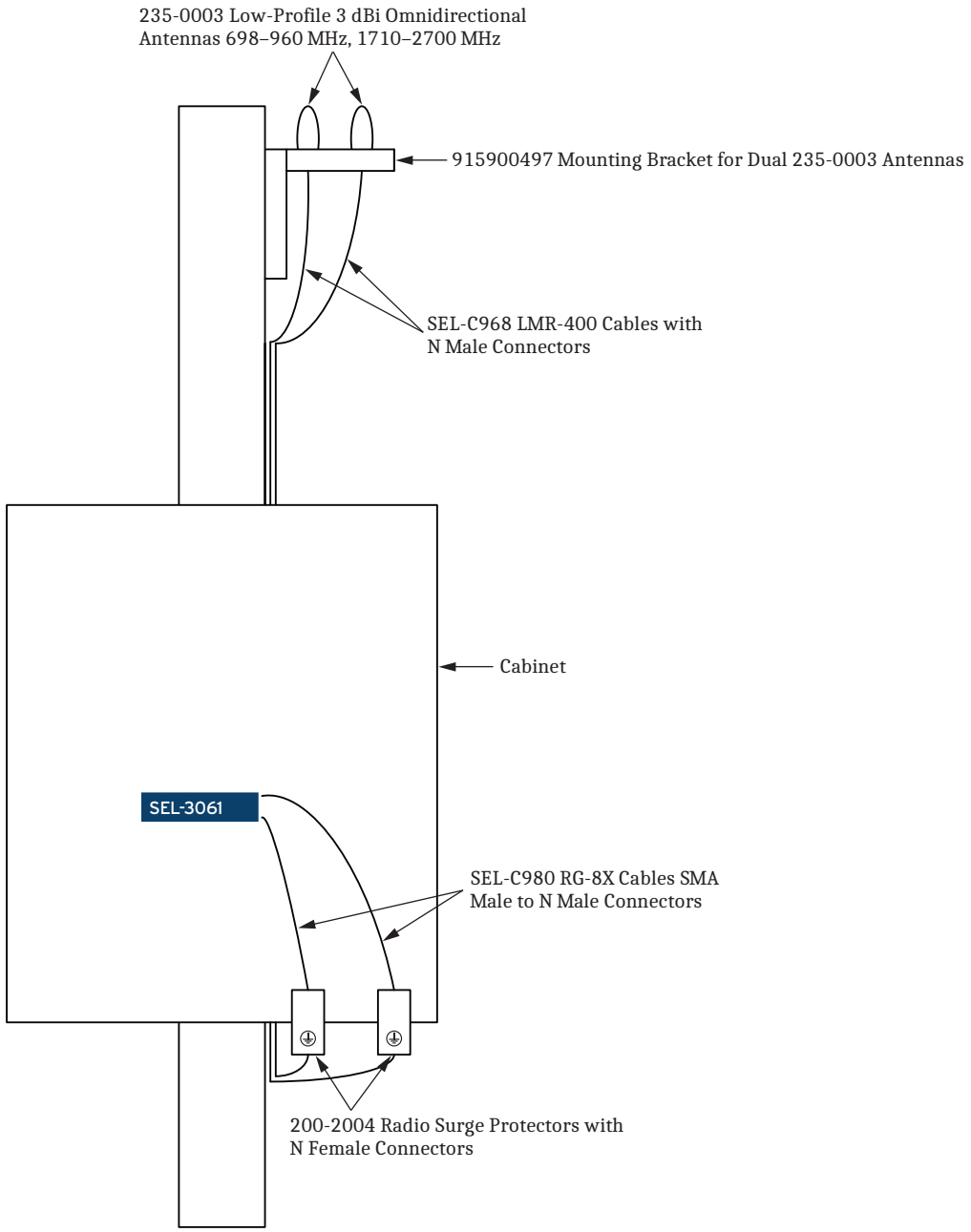


Figure 2.1 Cabinet Installation

Indoor Installation—Short Cable Run

In an indoor installation, you need two short cables going from the SEL-3061 to the surge protectors mounted on a grounded plate at the exit of the building and additional cables going to the antennas. In installations with good cellphone service coverage, place the antennas near the top of the building above possible snow buildup. It may be beneficial to increase the antenna height to improve line of sight to the cell tower, but that comes with increased cable loss.

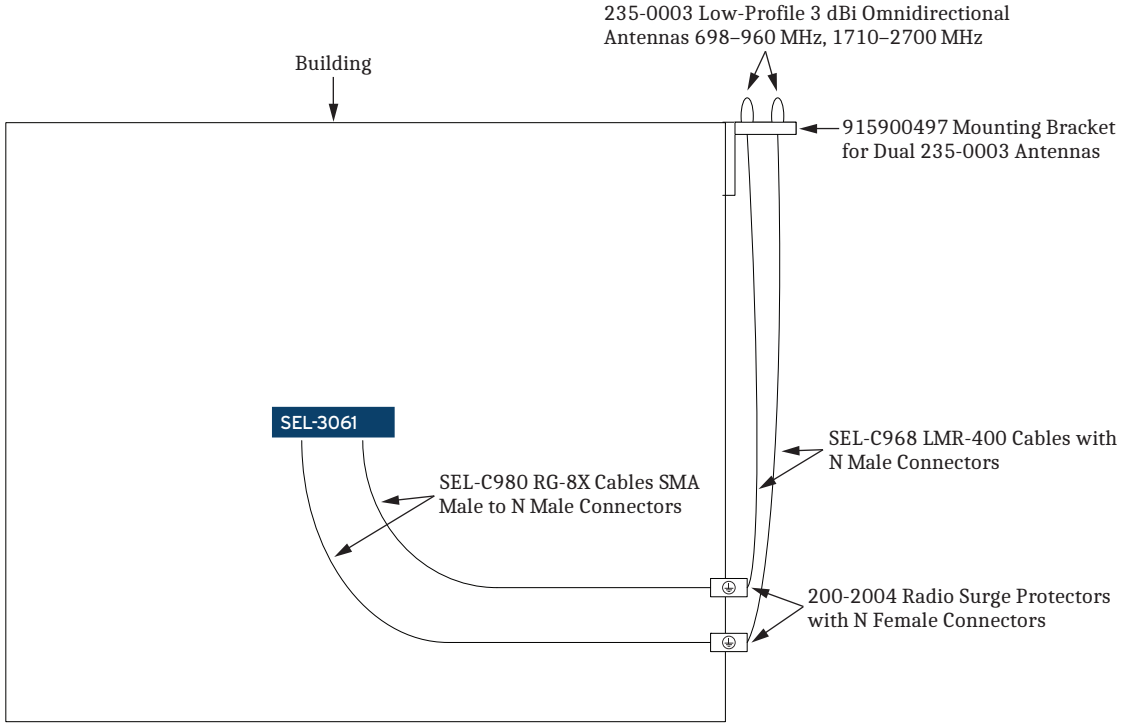


Figure 2.2 Indoor Installation—Short Cable Run

Indoor Installation—Long Cable Run

Limit the distance between the antennas and the SEL-3061 to reduce cable loss, but if the cable run is long (typically longer than 50 ft), use LMR-400 cables instead of RG-8X cables. By adding the SEL-C981 Cable at the antenna port, you can convert the radio output to a TNC Male connector. From there, it resembles other SEL radios, and you can attach LMR-400 cables. Do not connect LMR-400 cable directly to the SMA connector because the cable is too heavy and rigid. Instead, use a short SEL-C981 patch cable (1 ft) with SMA-to-TNC connectors, as shown in *Figure 2.3*.

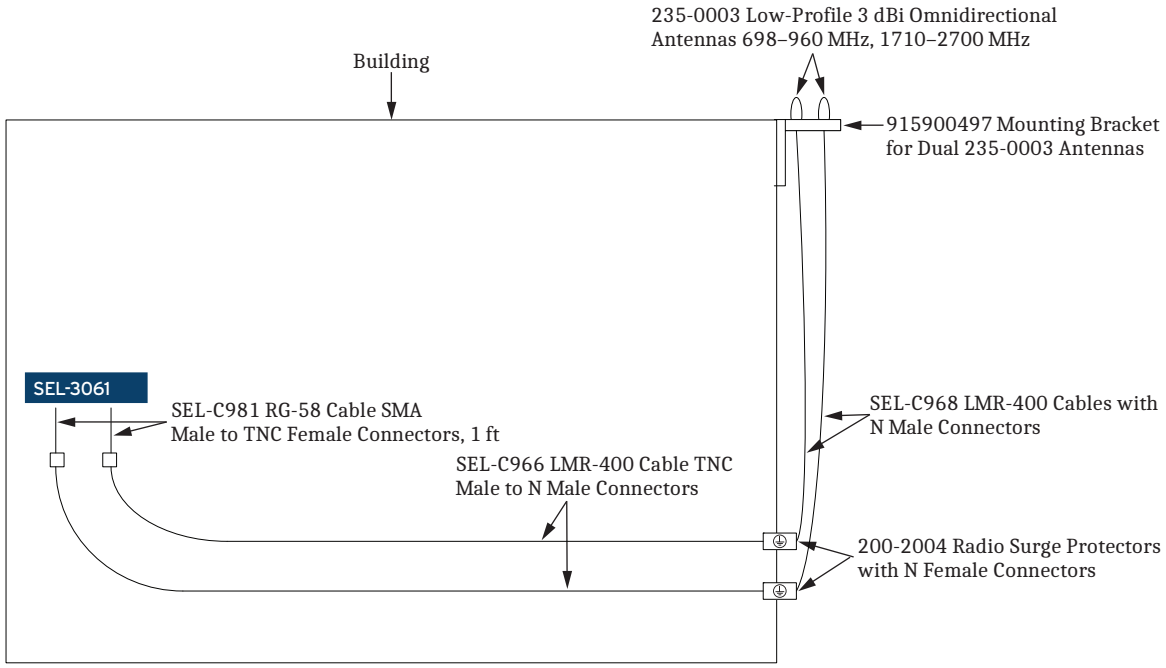


Figure 2.3 Indoor Installation—Long Cable Run

Lightning Protection

⚠WARNING
Atmospheric electrical charge accumulation can impose a standing electric potential difference between the conductor and shield of the feed line. In extreme cases, a lightning strike imposes a dangerous voltage surge. A surge protector should be installed to prevent damage to equipment or injury to personnel.

The higher you mount the antenna on a support structure, the greater the probability of equipment damage resulting from a lightning strike. Use Radio Surge Protectors with N Female Connectors (SEL Part Number 200-2004) to equalize the difference in potential that can occur between the center conductors and the shield of the coaxial cables between the antenna and the wireless router. In all surge-protector applications, mount the surge protectors at the building or enclosure entrance and ground the surge-protector bodies. Ground the wireless router to the same point as the surge-protector ground to avoid ground-rise-potential damage. When you use the surge protectors, order additional cables and place these cables between the SEL-3061 and the surge protector. Because the distance varies from the SEL-3061 to the surge protectors, be sure to approximate these cables at the correct length (plus 10 to 20 percent for installation variability).

Review the SEL application guide, “Radio System Lightning Protection Best Practices” (AG2014-36) at selinc.com/literature/application-guides for detailed instructions on surge protection.

Power Connections

The **POWER** terminals on the rear panel (labeled + and –) must connect to the correct supply voltage (12–30 Vdc). The **POWER** terminals are not isolated from chassis ground. Use 0.8 mm^2 (18 AWG) wire to connect to the **POWER** terminals. Place an external circuit breaker or switch no more than 3.0 m (9.8 ft) from the equipment. The circuit breaker (or equivalent approved disconnect device appropriate for the country of installation) must comply with IEC 60947-1 and IEC 60947-3, be identified as the disconnect device for the equipment, and be located near the equipment. This disconnect device must interrupt both the positive (+) and the negative (–) power leads. The maximum current rating for the power disconnect circuit breaker or overcurrent device (fuse) must be 20 A. An internal power supply fuse protects the operational power supply. Be sure to use fuses that comply with IEC 60127-2.

After applying power to the SEL-3061, it is in an alarm stage with the **ALARM** LED illuminated in red. Approximately 30 seconds later, the alarm clears, and the **ENABLED** LED illuminates in green. This indicates that the SEL-3061 is turned on and has passed all of its self-tests; however, the web interface is not accessible and may not be accessible for another two minutes. The SEL-3061 will go in and out of the alarm state, indicating that the device completed initialization, and the web interface is accessible.

Grounding (Earthing) Connections

You must connect the ground terminal labeled with the ground ⏚ symbol to a rack frame or switchgear ground for proper safety and performance. Use 0.8 mm^2 (18 AWG) wire, less than 2.0 m (6.6 ft) in length, for the ground connection.

Commissioning the Device

The following steps describe how to create the first administrative account for the SEL-3061. The SEL-3061 includes an HTTPS web server for configuration and management functions. The following browsers have been tested to work with the SEL-3061 web interface:

- Firefox version 60.0.1 (64-bit) or later
- Google Chrome browser version 67.0.3396.79 (64-bit) or later
- Microsoft Edge 41.16299.402.0 or later

The following items are required for the initial connection to the SEL-3061:

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

Connect the SEL-3061 to your computer, as shown in *Figure 2.4*. Using a standard RJ45 Ethernet cable, connect the Ethernet port of your computer to the Ethernet port (**ETH**) of the device. If your computer is configured as a Dynamic Host Configuration Protocol (DHCP) client, DHCP sets your computer to a compatible subnet with the SEL-3061. Wait at least 10 seconds for the connection to be configured.

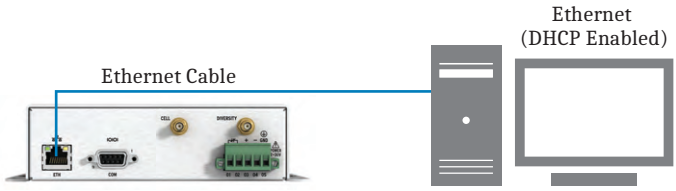


Figure 2.4 Connect the SEL-3061 to the Computer

See *Ethernet Network Interface (LAN) on page 4.1* for more information about the DHCP feature.

A new SEL-3061 has the Ethernet port enabled and the DHCP feature turned on.

Use the following procedure to configure the network connection of the computer:

NOTE: You may receive a certificate error from your browser. The message depends 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 provides instructions for doing this. For information on creating an X.509 certificate to eliminate this error, see *X.509 on page 5.27*.

Step 1. Open a web browser.

Step 2. With your computer configured to support DHCP, enter the default URL, **192.168.2.1**, in the address bar.

The commissioning page only appears during initial setup of a new unit or after a factory-default reset (see *Device Reset on page 5.31*). After the device has been commissioned, the initial page will be the login page. If an administrator forgets his or her password, the device can be reset to its factory-default settings by inserting an object into the pinhole reset on the front panel of the device. The factory reset erases all log events and user-created content, sets all setting/configuration parameters to default values, and deletes all local user accounts. Once the factory reset is performed, users have to go through the commissioning page to make the device usable. Whenever the pinhole reset button is pressed while the device is energizing, all front-panel LEDs turn on and stay on as long as the button is held. The LEDs turn off after 30 seconds.

To perform a factory reset, push the pinhole reset button and hold it for more than 30 seconds. To perform a device restart, push the pinhole reset button and hold it between 10 and 30 seconds. To perform a lamp test, push the pinhole reset button and hold it for less than 10 seconds.

For more information, see *Device Reset on page 5.31*.

Step 3. Enter the username for the first administrative user, and select **OK** (see *Figure 2.5*).

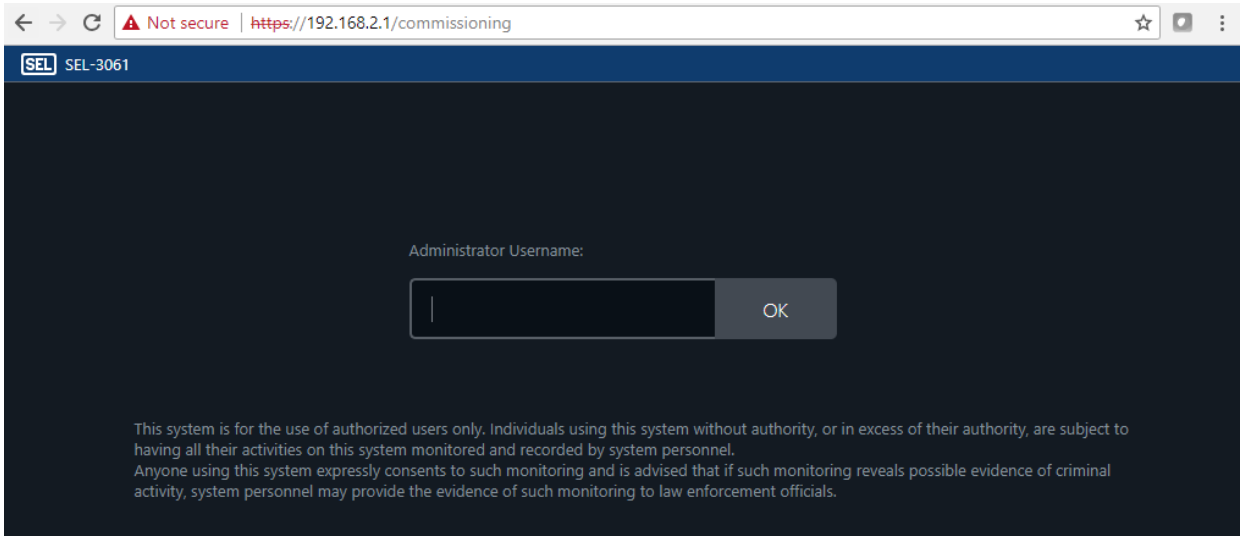


Figure 2.5 Enter the Username

Step 4. Enter the password for the first administrative account and select **OK** (see *Figure 2.6*). Confirm the password.

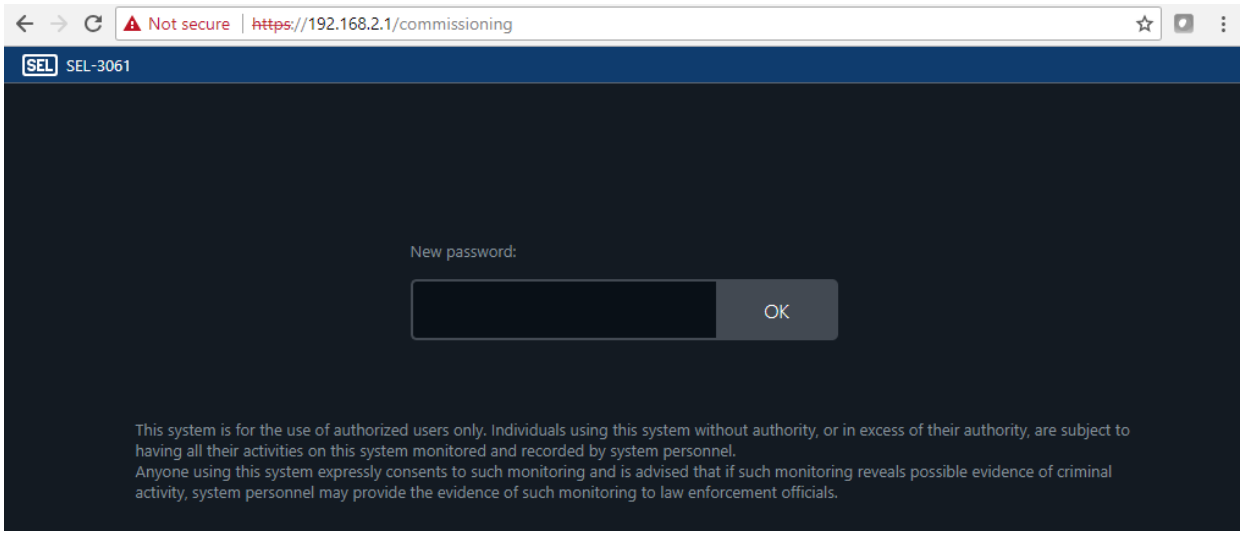


Figure 2.6 Enter the New Password

Step 5. 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-3061 redirects you to the dashboard page.

Step 6. In the Operating Mode dialog box that appears, choose one of the following two operating modes.

- ➢ The Network Router mode is the default and establishes the device as a cellular network router.
- ➢ The PPP-IP Passthrough mode is designed for installations where you already have a router connected to the end device, and you just need a cellular modem to pass Ethernet traffic. The PPP-IP Passthrough mode gives the Ethernet-attached routing device an IP address that it receives from the cellular provider. In this mode, the SEL-3061 only allows one DHCP lease. Do not

NOTE: In PPP-IP Passthrough mode, many of the SEL-3061 services described in this document are non-configurable and do not appear in the device configuration menu. All IP traffic passes between the Ethernet-attached device and the cellular provider with no firewall functionality.

use PPP-IP Passthrough mode to connect directly to critical infrastructure systems such as relays or controls. A router with a full suite of security functionalities such as the SEL-3620 Ethernet Security Gateway or the SEL-3622 Security Gateway must be connected between the SEL-3061 and the end device.

Step 7. Ensure the device is set up with the appropriate Access Point Name (APN). If you are using a Verizon network, this should be configured automatically. Otherwise, configure the APN in the **Configuration > WAN > Cellular Configuration** page. In the APN field, put the APN assigned by the carrier. If you intend to use a public APN, such as i2gold, enter that into the APN field.

NOTE: Because the cellular module requires a restart whenever there is a setting change, it is recommended that you make all changes first and then select **Save And Restart**. A typical device restart takes about 5 minutes.

Step 8. After you log in for the first time as the administrator, the Save And Restart button is highlighted in red. Select **Save And Restart** to save the new configuration.

Step 9. Log back into the device to test that you have network access. Go to the **Diagnostics > Diagnostics** page. Under Ping, enter selinc.com to ping SEL. Select **Ping**. If the diagnostics report shows a response, your device is successfully connected to the network.

Typical Cellular Installation

Router Installation

Typically, you configure your system with a remote SEL-3061 and access it through your own network through a router with a firewall. In that case, the SEL-3061 has a VPN (provided by the network operator) or IPsec VPN to the router attached to the private network.

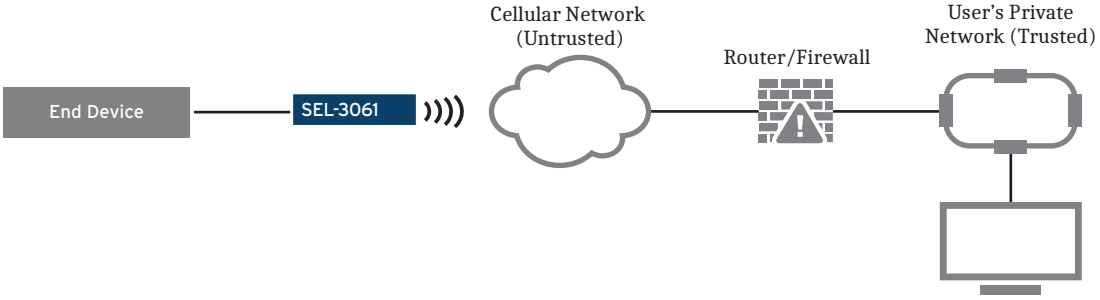


Figure 2.7 Typical Cellular Router Installation

PPP-IP Passthrough Installation

For PPP-IP Passthrough installation, the SEL-3061 functions as a cellular modem. The SEL-3061 provides cellular connectivity for its attached device. If a secure connection is required, the connected device is responsible for the secure connections.

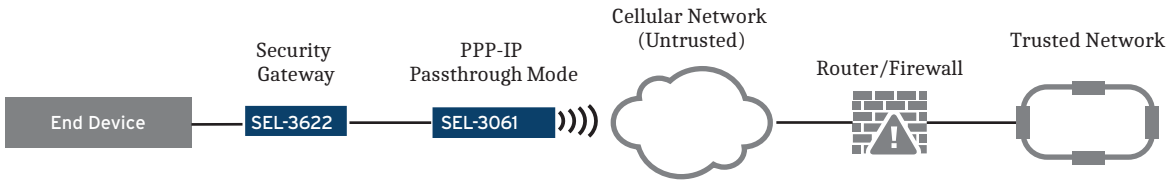


Figure 2.8 PPP-IP Passthrough Mode Operation

SECTION 3

Applications

Application Overview

The SEL-3061 serves as the communications link for field devices or backhaul communications device. For electric utilities, the SEL-3061 provides connectivity to devices such as recloser controls, motor-operated switches, capacitor banks, voltage regulators, meters, and other IEDs. The combination of serial and Ethernet ports on the SEL-3061, along with secure tunneling, provides application flexibility and makes installation easy without sacrificing security.

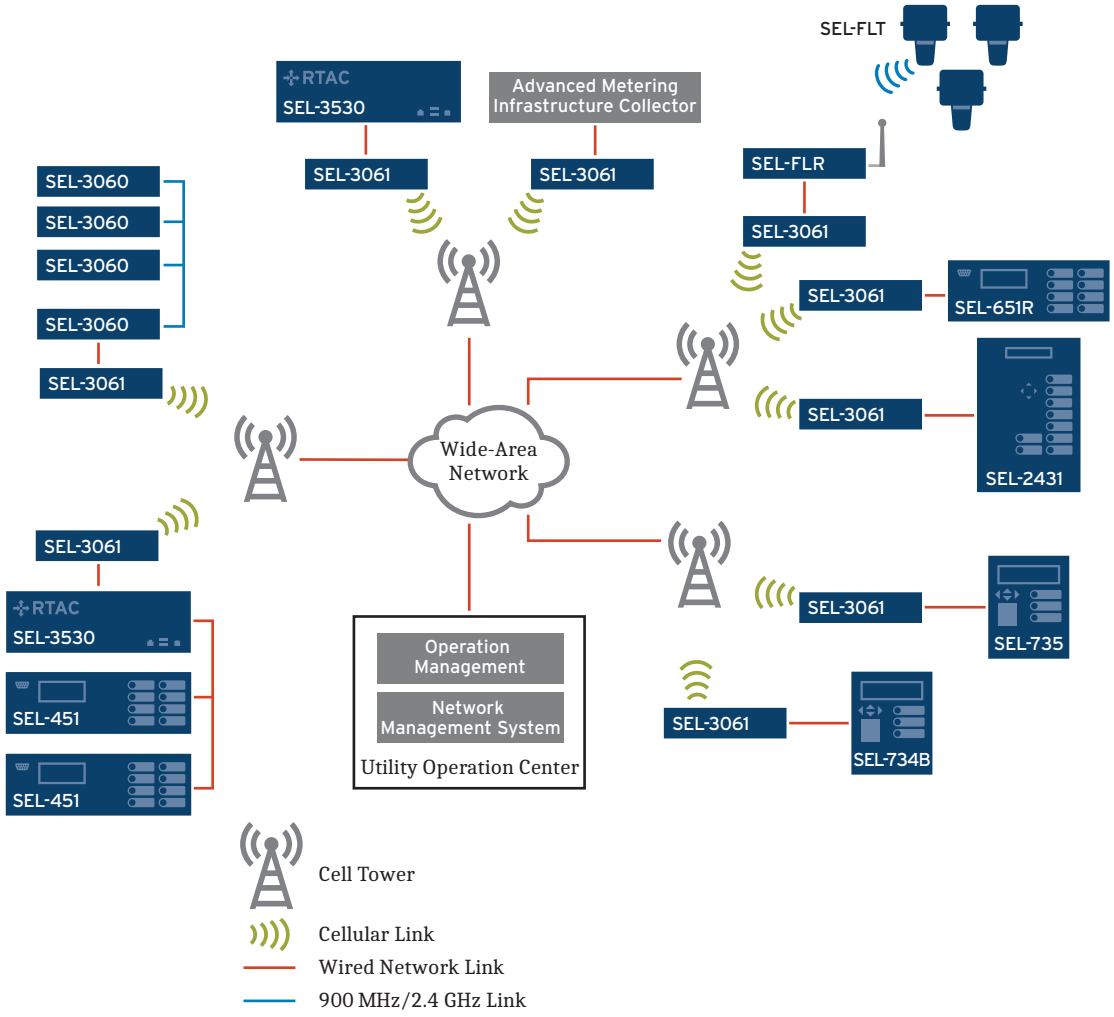


Figure 3.1 Application Overview

SCADA

The SEL-3061 provides the communications link to aggregate data from field devices and forwards it to SCADA systems and HMIs. The SEL-3061 can be applied for data acquisition and slow-to-medium speed control applications. SCADA includes analog and discrete I/O monitoring and metering. The SCADA control includes set-point changes of processes and operations of discrete I/Os. Field devices connect directly to either the Ethernet port or serial port on the SEL-3061. The SEL-3061 links these devices to a SCADA system via cellular WAN connections and allows the SCADA to poll each device by using DNP3 over TCP/IP and Modbus TCP/IP.

Engineering Access

The SEL-3061 allows users to access IEDs to view and modify settings and download oscillographic event reports through VPNs.

Distributed Data Acquisition

Modern automation systems can be distributed over a large geographical area. These automation systems monitor and process input signals, execute logic, and enable or disable outputs. In some instances, it is necessary to perform data acquisition on the status or value of the connected I/O. A distributed data acquisition system uses an automation controller as the data concentrator and a computer as the SCADA host. The system uses remote, discrete, and analog I/Os. As shown in *Figure 3.2*, a single SEL-3061 at each site both provides the connectivity between these remote I/Os with the automation controller and backhauls the collected data to the SCADA computer.

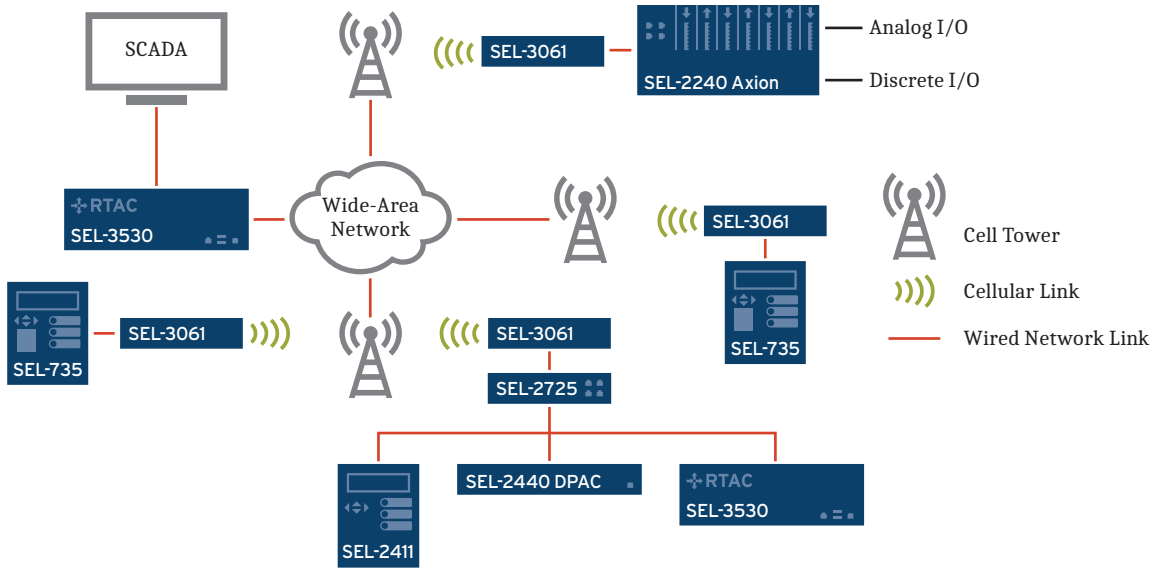


Figure 3.2 SCADA, Engineering Access, and Distributed Data Acquisition

Distribution Automation

The SEL-3061 provides cellular connectivity to remotely monitor and control recloser controls and sectionalizers for distribution power systems, as shown in *Figure 3.3*. In cases where customers rely on communications schemes for power restoration, the SEL-3061 provides the connectivity. The main difference between the distribution automation (DA) systems that use line-of-sight radios and DA systems that use an SEL-3061 is that the SEL-3061 and DA can be installed at any IED location that has cellular coverage. The DA controller polls data from each recloser control for monitoring and sends control signals through the WAN and the SEL-3061.

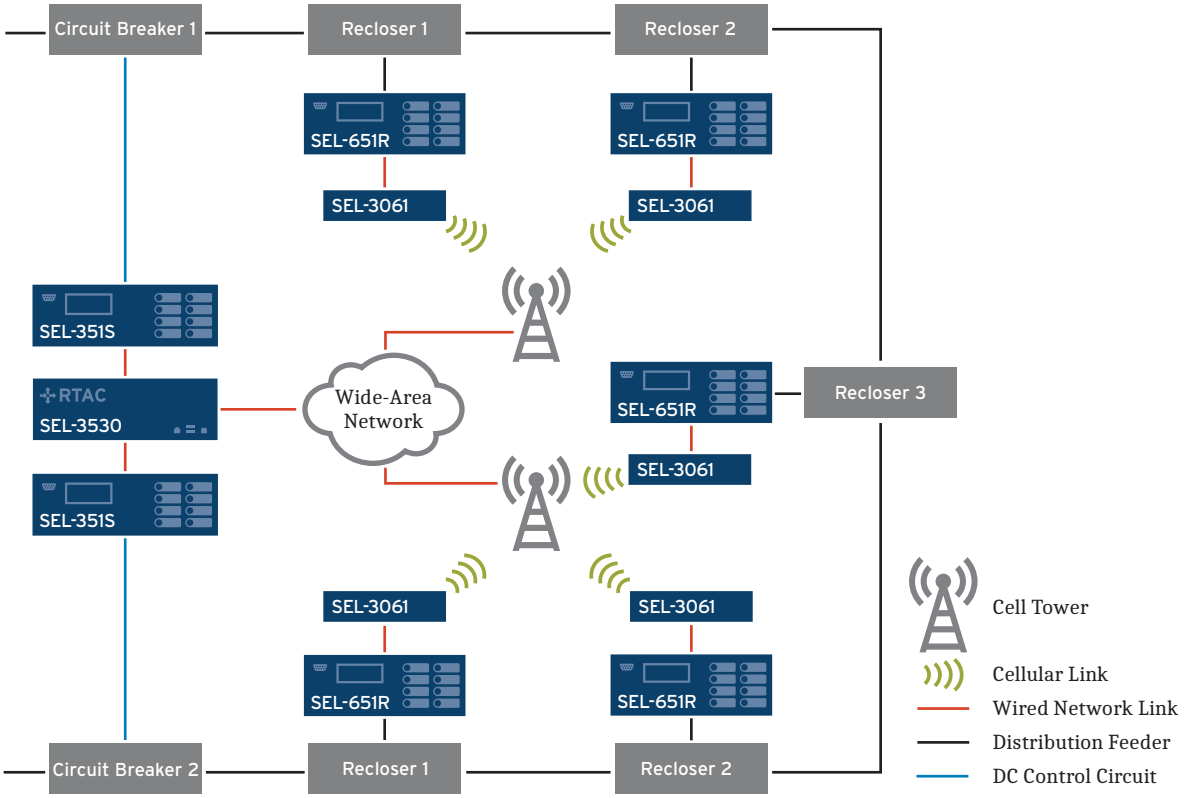


Figure 3.3 Distribution Automation

SEL-FLT/SEL-FLR Network Backhaul

The SEL-FLT and SEL-FLR Fault and Load Transmitter and Receiver System provides wide-area load monitoring and fault location from line-powered SEL-FLT devices. The SEL-FLR collects load data and fault information from the SEL-FLT devices and sends the collected data to an Operation Management System (OMS) or Energy Management System (EMS) via a WAN. The SEL-3061 provides the communications link between the OMS and the SEL-FLR. When connected to the SEL-FLR the SEL-3061 provides wireless connectivity for the SEL-FLT/SEL-FLR networks, as illustrated in *Figure 3.4*.

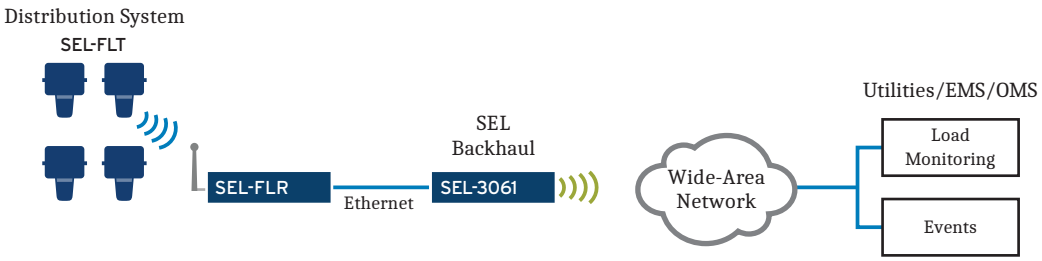


Figure 3.4 Backhaul Communication for Distribution Line Sensors

Distributed Generation

The SEL-3061 provides the connectivity to remotely monitor and control relays, devices, and equipment at distributed generation (DG) sites. In most applications, an automation controller interfaces with devices located inside the DG facility. The SEL-3061 can be connected to the controller to provide backhaul connectivity for devices located at the DG sites. The SEL-3061 is suitable for monitoring and non-protection speed control of the DG site.

Voltage Regulators

Voltage regulators installed outside the substation use the SEL-3061 to report their status and receive control commands from either a controller or the SCADA system. Connect the voltage regulator to the SEL-3061 by using either the serial or Ethernet interface.

Capacitor Bank Controls

The SEL-3061 provides communication for remote monitoring and automated or manual control of capacitor banks.

Pump Automation Controls

Monitor and control critical infrastructure, such as water and wastewater pumps, by using the SEL-3061 to provide remote access to SEL-2411P Pump Automation Controllers. During both routine operations and natural disasters, the cellular network provides a reliable path from a control center to the field. Use an Ethernet switch to connect more than one controller to a single SEL-3061.

Network Backhaul

A radio or Advanced Metering Infrastructure (AMI) network usually has an access point that concentrates data from remote endpoints. The access point is usually connected to a WAN or another wireless network. The SEL-3061 can be used as the link between the access point and the WAN or the wireless network by providing backhaul for these networks.

This page intentionally left blank

SECTION 4

Network Settings

Ethernet Network Interface (LAN)

NOTE: This section covers the SEL-3061 Network Router and PPP-IP Passthrough operating modes. *Section 6: Serial Communications* covers the Serial Modem operating mode. The operating mode is selected during product commissioning. See *Commissioning the Device on page 2.6*.

The SEL-3061 rear-panel Ethernet network interface provides connectivity for initial commissioning, device management, LAN communications, remote status, and event reporting. The Ethernet port connector is a female RJ45 port, labeled **ETH** on the rear-panel.

The Ethernet port is always enabled for device management with an initial IP address of 192.168.2.1. The interface operates in Layer 3 mode, providing an HTTPS service with a web-based user interface. The Dynamic Host Configuration Protocol (DHCP) service is enabled by default.

HTTPS

HTTPS allows a client web browser to connect to the device to manage configuration settings. This service is always enabled on the Ethernet port interface (LAN). The service can also be enabled for WAN-side access.

Access the Ethernet Network Interface settings shown in *Figure 4.1* by navigating to **Configuration > Network > IP Configuration** on the SEL-3061 web interface.

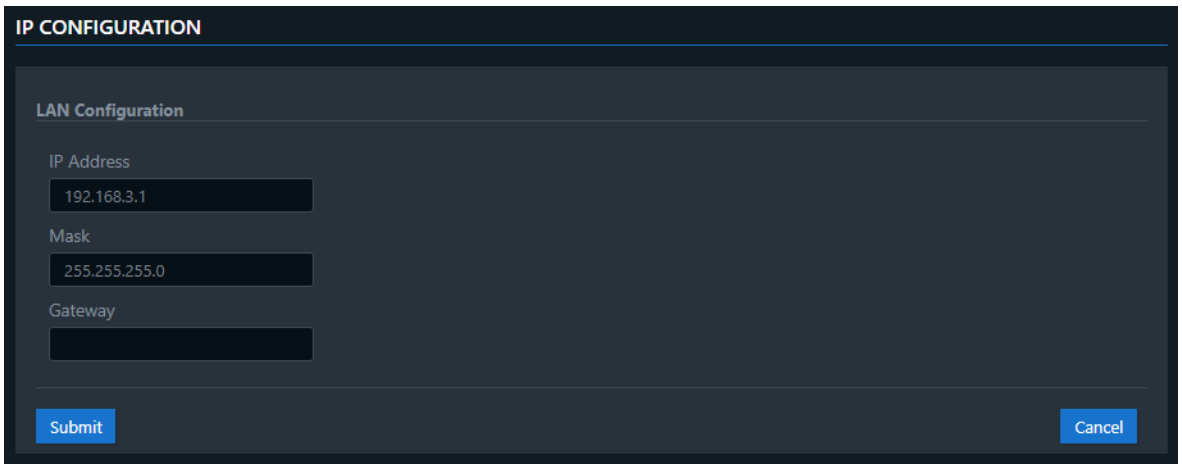


Figure 4.1 IP Configuration

The network interface settings must adhere to the following IP address guidelines:

- IP addresses must be in the range of 1.0.0.0–223.255.255.254.
- Interface IP addresses cannot be set to the network or broadcast addresses (first or last address in the range defined by the mask).

- Interface IP address cannot be the same as the default gateway.
- Interface IP address cannot be the same as the remote Syslog server or Remote Authentication Dial-In User Service (RADIUS) server addresses.

Table 4.1 Ethernet Interface Settings

Setting Name	Value	Default	Description
IP Address	Unicast IP address	192.168.2.1	Establishes the IP address of the interface.
Mask	*xxx.xxx.xxx.xxx* or */n* where *xxx* is from 0 to 255 or */n* where *n* is from 1 to 32.	255.255.255.0 or /24	The device uses both classless interdomain routing (CIDR) notation and explicit notation to assign the subnet mask.
Gateway	Unicast IP address	[Empty]	Used to transfer packets to another network.

DHCP Service

The DHCP service is enabled by default and assists with the automatic network configuration of devices directly connected to the Ethernet port. A network device, such as a computer, with the DHCP client enabled will receive an IP address, a default gateway, and a Domain Name System (DNS) resolver when connected to the Ethernet interface with DHCP enabled. It forwards the requests to the address designated by the Ethernet port configuration. See *DNS on page 4.5*.

To use the Ethernet port for managing the SEL-3061, connect a DHCP client-enabled computer to the SEL-3061 ETH port. Wait a few minutes for the service to complete its configuration, then open a web browser. Enter **192.168.2.1** into the address bar. The browser automatically redirects to the commissioning page (for a non-commissioned device) or to the login page (for a commissioned device). This is a fully functional DHCP implementation. The SEL-3061 can supply addresses to all devices connected to its ETH port if configured to do so. It is recommended that DHCP be disabled after completing the configuration of the Ethernet interface on SEL-3061.

Access the DHCP settings by navigating to **Configuration > Network > Advanced**, then select **DHCP** at the top of the configuration window shown in *Figure 4.2* in the web interface.

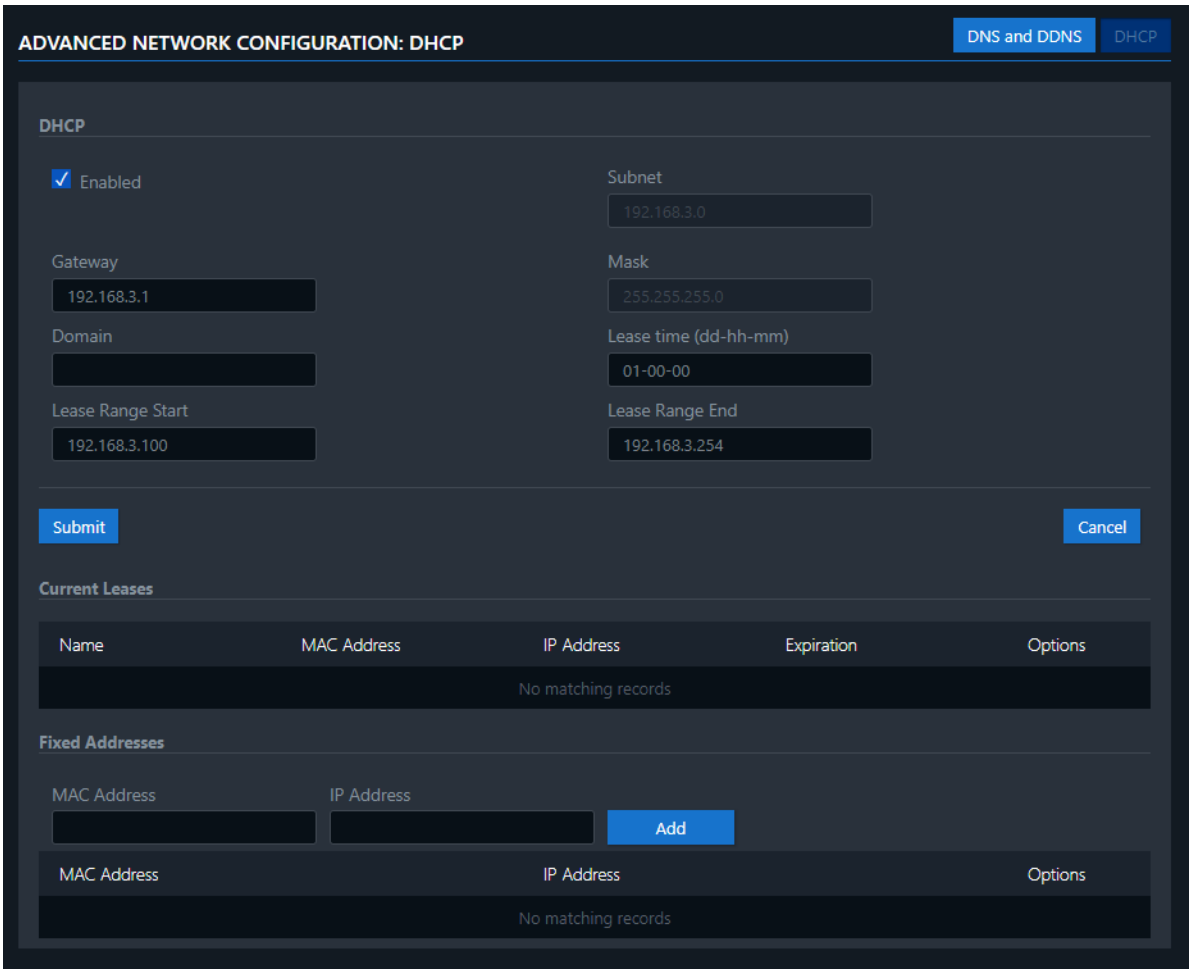


Figure 4.2 DHCP Configuration

DHCP assigns IP addresses to the DHCP client according to the DHCP configuration. A change of DHCP settings causes DHCP reconfiguration and results in the SEL-3061 assigning addresses based on the new settings. The client must request a new DHCP lease to continue working. Force a client to request a new lease by disconnecting and reconnecting the Ethernet cable.

DHCP Settings

The DHCP server leases an IP address from a group of IP addresses that are part of the settings. A gateway, lease time, and IP address lease range are required for DHCP. *Table 4.2* shows the DHCP settings parameters.

Table 4.2 DHCP Settings Parameters (Sheet 1 of 2)

Setting Name	Value	Default	Description
Enabled	Checked or unchecked	Checked	Enable the DHCP. It is enabled by default.
Gateway	Unicast IP address	IP address of the LAN interface.	Typically the same as the IP address of the SEL-3061 Ethernet port.
Domain	Unicast IP address or domain name	[Empty]	Either the local subnetwork or the descriptor for a site on the network.
Lease Range Start	Unicast IP address	*xxx.yyy.zzz*.100, where *xxx.yyy.zzz* are the first trio of the Gateway.	The start lease IP address.

Table 4.2 DHCP Settings Parameters (Sheet 2 of 2)

Setting Name	Value	Default	Description
Lease Range Start	Unicast IP address	*xxx.yyy.zzz*.254, where *xxx.yyy.zzz* are the first trio of the Gateway.	The last lease IP address.
Lease Time	dd-hh-mm	01-00-00	Set in days, hours, minutes. Setting 00-00-00 provides an infinite lease.

The list of leases is shown in the Current Leases table (see *Figure 4.2*). Select the garbage bin to remove a leased IP address or select the plus sign to add a current lease IP address to the fixed IP address list.

DHCP also supports fixed IP addresses with specific MAC addresses. To add a fixed IP address, enter the MAC address and IP address, then select **Add**. The MAC address box cannot be empty. Once a fixed MAC address and IP address are added, the list below these settings shows the list of MAC and fixed IP addresses that have been added (see *Figure 4.2*).

DNS and DDNS

Access the DNS and Dynamic Domain Name System (DDNS) settings shown in *Figure 4.3* by navigating to **Configuration > Network > Advanced**, then select the **DNS and DDNS** button on the top of the configuration window.

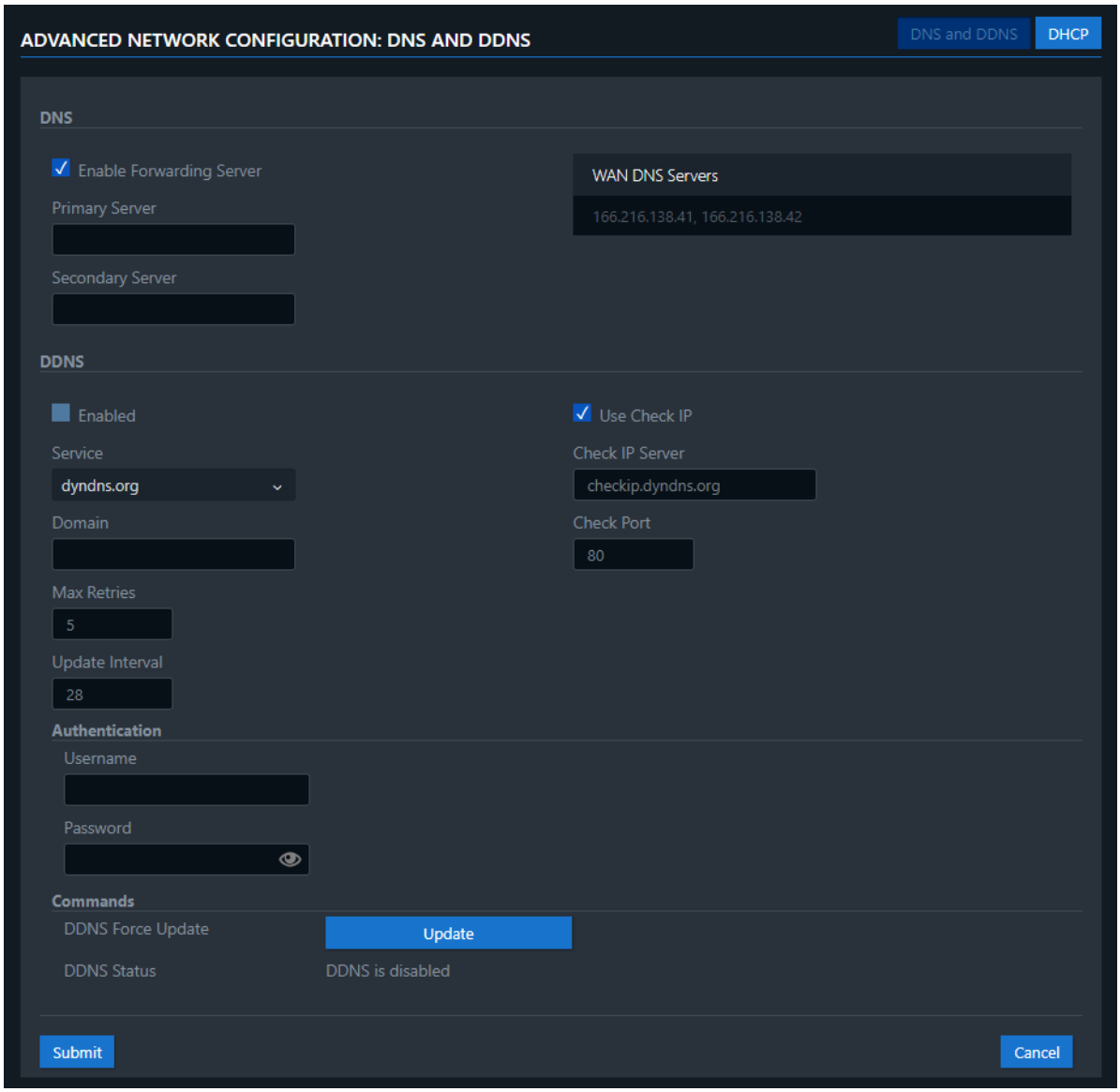


Figure 4.3 DNS and DDNS Configuration

DNS

DNS are hierarchical decentralized servers on the network that translate domain names, such as google.com, to the numerical IP address. The DNS helps network devices to locate and identify other devices and services on the network. The SEL-3061 uses the DNS-translated domain names, if needed, once it is connected to the network. By default, the Forwarding Server is enabled, which configures the SEL-3061 to automatically obtain the cellular network WAN DNS servers. It is recommended that DNS Forwarding Server be disabled after completing the commissioning of the SEL-3061 and if this feature is not used for your applications. You can also use specific DNS servers on the network by entering the Primary and Secondary (if available) server IP addresses on the DNS configuration page.

Table 4.3 DNS Configuration Settings

Setting Name	Value	Default	Description
Enable Forwarding Server	Checked or unchecked	Checked	Forward DNS queries for external DNS names to DNS servers outside the network.
Primary Server	Unicast IP Address	[Empty]	The primary DNS server of your LAN (optional).
Secondary Server	Unicast IP Address	[Empty]	The secondary DNS server of your LAN (optional).
WAN DNS Servers	Unicast IP Address	[Empty]	External DNS servers, populated by the router. This field is not editable.

DDNS

DDNS is a service that dynamically updates DNS entries with the IP address of the device. This is used when the device is getting its address through DHCP and it can change often. DDNS allows you to access the SEL-3061 with a domain name instead of an IP address. DDNS supports dynamic IP addresses, if needed. DDNS is disabled by default. Once it is enabled, DDNS allows you to choose a service from a drop-down list of publicly available services or your internal custom domain name system server. If Use Check IP is enabled, the DDNS settings allow the device to query a server to determine its IP address before it performs the DDNS update. If it is disabled, the device performs the DDNS update by using an IP address obtained from the PPP link.

For DDNS server authentication, enter the credentials in the Username and Password boxes.

Table 4.4 shows the DDNS settings.

Table 4.4 DDNS Configuration Settings

Setting Name	Value	Default	Description
DDNS Enabled	Checked or unchecked	Unchecked	Enable or disable DDNS.
Service	List of available publicly known or custom services		Selecting custom exposes additional settings[a].
Domain	Unicast IP address or domain name	[Empty]	The domain name to identify the device on the network.
Max Retries	0–100	5	Maximum number of retries allowed if the update fails.
Update Interval	1–99	28	Maximum number of days between each push of the IP address of the device to the DDNS server. Note that this number should be less than the number of days until DDNS expires because of inactivity.
Username	0–250 characters	[Empty]	The username of the device to authenticate against the DDNS server.
Password	0–250 characters	[Empty]	The password of the account on the DDNS server.
Use Check IP	Checked or unchecked	Checked	If this setting is enabled, the device uses a server to obtain the IP address. If it is disabled, the device uses the IP address to obtain the PPP link for the DDNS.
Check IP Server	Domain name	Checkup.dyndns.org	The server on the network that provides the IP address of the device.
Port	1–65535	80	The port used to check its IP address.

[a] When a custom service is selected in the Service field, the device allows you to set the DDNS server IP address, its port, and the domain name, as shown in *Figure 4.3*. The server is the IP address of the DDNS server.

The SEL-3061 allows you to perform a DDNS Force Update by selecting **Update**. This forces the DDNS server to update with the latest status of the device.

Cellular Network (WAN)

General Configuration Settings

To enter the cellular network parameters, navigate to the **Configuration > WAN > Cellular Configuration** page. The cellular network is enabled by default. See *Table 4.5* for details on the cellular configuration settings. A Subscriber Identity Module (SIM) card is required for the cellular network connection. See *Section 2: Installation and Getting Started* for SIM card installation.

Table 4.5 Cellular Configuration—General Configuration Settings

Setting Name	Value	Default	Description
Enabled	Checked or unchecked	Checked	Enables or disables the cellular network connection.
Dial on Demand	Checked or unchecked	Unchecked	Enables or disables the Dial on Demand feature. When enabled, the SEL-3061 automatically establishes a connection when the LAN requires cellular network access. An additional Idle Timeout setting defines the maximum duration (30–86,400 seconds) to maintain the connection after the LAN goes quiet. Enable the Dial on Demand when Wake Up On Call is enabled to allow the SEL-3061 to sleep after it wakes up.
Connection Timeout	20–900 seconds	90	The amount of time the SEL-3061 waits for a network connection attempt before it declares that the connection has failed.
Dialing Max Retries	0–100	0	The number of retries the SEL-3061 attempts to connect to the network before it declares a failed network connection. The default value is zero, which specifies an unlimited number of retries.
SIM Pin	0–9999	[Empty]	The pin required to unlock the SIM card for use.
APN	0–126 characters	[Empty]	The assigned Access Point Name (APN) given by the service provider that the SEL-3061 uses to access the network. The APN is service provider-specific and can be left blank.

To control data transfer over the cellular interface, you can enable Dial On Demand, which directs the SEL-3061 to establish a connection with the cellular network and maintain a cellular connection while LAN activity is present. The Idle Timeout setting defines the maximum inactive period, after which the SEL-3061 disconnects from the cellular network.

Authentication

Some carriers require the device to authenticate the cellular network before establishing network connections. The SEL-3061 supports PAP, CHAP, and PAP-CHAP authentication protocols. By default, none of the authentication protocols are selected. Once a protocol is selected, enter your credentials to authenticate the cellular network.

Table 4.6 Cellular Configuration—Authentication

Setting Name	Value	Default	Description
Authentication Type	NONE, PAP, CHAP, PAP-CHAP	NONE	The types of authentication when establishing PPP connection. The default value is NONE, where the cellular service provider does not require authentication.
Username	0–120 characters	[Empty]	The username for network authentication.
Password	8–4096 characters	[Empty]	The required password for network authentication.

Keep Alive Feature

Keep Alive is a feature that allows the SEL-3061 to stay connected to the network. To do this, the SEL-3061 continuously sends a message to a remote site and waits for a response.

To keep the network connection alive, the SEL-3061 uses either ICMP or TCP. By default, the Keep Alive feature is disabled. Once it is enabled, you can configure the interval (in seconds) that the device checks with the remote site and determines its network connection status. The remote site can be a server or any device that supports either ICMP or TCP.

Table 4.7 Cellular Configuration—Keep Alive

Setting Name	Value	Default	Description
Enabled	Checked or unchecked	Unchecked	Enables or disables the Keep Alive feature.
Interval	60–86400 seconds	60	The time between network connectivity Keep Alive checks.
Keep Alive Type	ICMP, TCP	ICMP	The protocol selection for Keep Alive checks. When TCP is selected, a TCP Port selection is also required.
ICMP Count	4–10	4	The number of keep-alive packets the SEL-3061 sends if ICMP is used.
Hostname	Unicast name or domain name	[Empty]	The device to which the SEL-3061 sends keep-alive messages to verify the keep-alive status.

Data Receive Monitor

Enable the Data Receive Monitor to avoid repeatedly dropping and reestablishing a network connection during degraded signal conditions. The SEL-3061 continuously monitors the network for lost packets over a selectable window (period). The device drops and then attempts to reestablish a connection with the network only after there has been a complete loss of packets through the entire window.

Table 4.8 Cellular Configuration—Data Receive Monitor

Setting Name	Value	Default	Description
Enabled	Checked or unchecked	Checked	Enables or disables the feature the SEL-3061 uses to monitor the network link.
Interval	1–1440 minutes	60	The number of minutes that can pass without receiving network traffic before the network link is disconnected and reestablished.

Wake Up On Call

Wake Up On Call allows the SEL-3061 to wake up, initiate, and establish a cellular connection when there is an incoming call, SMS, or LAN activity.

Access the Wake Up On Call settings shown in *Figure 4.4* by navigating to **Configuration > WAN > Advanced**.

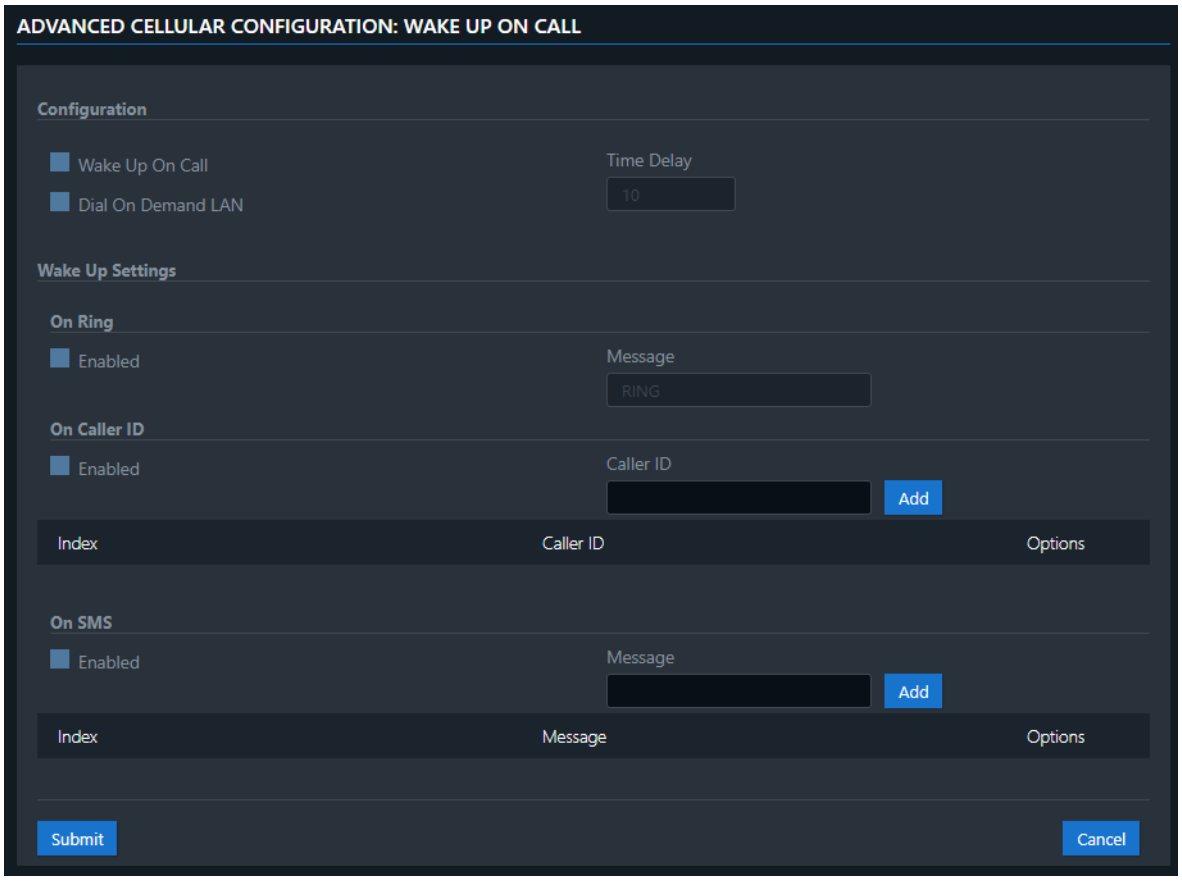


Figure 4.4 Wake Up On Call Webpage

Wake Up On Call is disabled by default. When it is enabled, a wake-up trigger must be set. You can use On Ring, On Caller ID, or On SMS as the trigger. By default, On Ring is the trigger once Wake Up On Call is enabled.

Wake Up Settings

When On Ring is enabled, an incoming call wakes up the device and it initiates and establishes the cellular link. This means that the device wakes up on the ring.

When On Call ID is enabled, the SEL-3061 allows you to enter a list of caller IDs. To add a caller ID to the On Caller ID list, enter a phone number or caller ID into the Caller ID box and select **Add**. Only incoming calls from the Caller ID list wakes the device to initiate and establish the cellular link.

When On SMS is enabled, an incoming SMS message that matches one of the messages in the message list wakes the device. To use this trigger, SMS services must be enabled (see *SMS and SMTP on page 8.8*). To add a message to the On SMS list, enter the message in the Message box and select **Add**.

PPP-IP Passthrough Mode

In PPP-IP Passthrough mode, the SEL-3061 functions as a cellular modem without security features, such as IPsec, and firewalls. By default, the cellular interface is enabled. Use PPP-IP Passthrough mode when you are using an external device to manage the security features. The SEL-3061 assigns the IP address that it receives from the cellular provider to the Ethernet-attached routing device that is connected to the SEL-3061. Once the connected device receives the IP address, the device is connected to the network. In this mode of operation, the SEL-3061 allows one DHCP lease. The following list of features are available in PPP-IP Passthrough mode:

- User Accounts (see *User Accounts on page 5.15*).
- Access Configuration (see *Ethernet Network Interface (LAN) on page 4.1*). Note that it is not possible to access the web user interface from the cellular network in this mode of operation. The web server via WAN is not available.
- Usage Policy (see *Usage Policy on page 5.14*).
- System (see *System on page 5.11*).
- Syslog (see *Syslog on page 8.3*).
- File management (see *File Management on page 5.25*).
- Statistics (see *Statistics on page 8.1*).
- Local Syslog Events (see *Local Syslog Reporting on page 8.4*).
- Diagnostics (see *Diagnostics on page 8.17*). Note that the DoS and ping functions are not available in PPP-IP mode.

The dashboard in the SEL-3061 web interface contains fewer fields compared to the Network Router mode, as shown in *Figure 4.5*. The dashboard contains information for the device, system statistics, diagnostics, and cellular interface information.

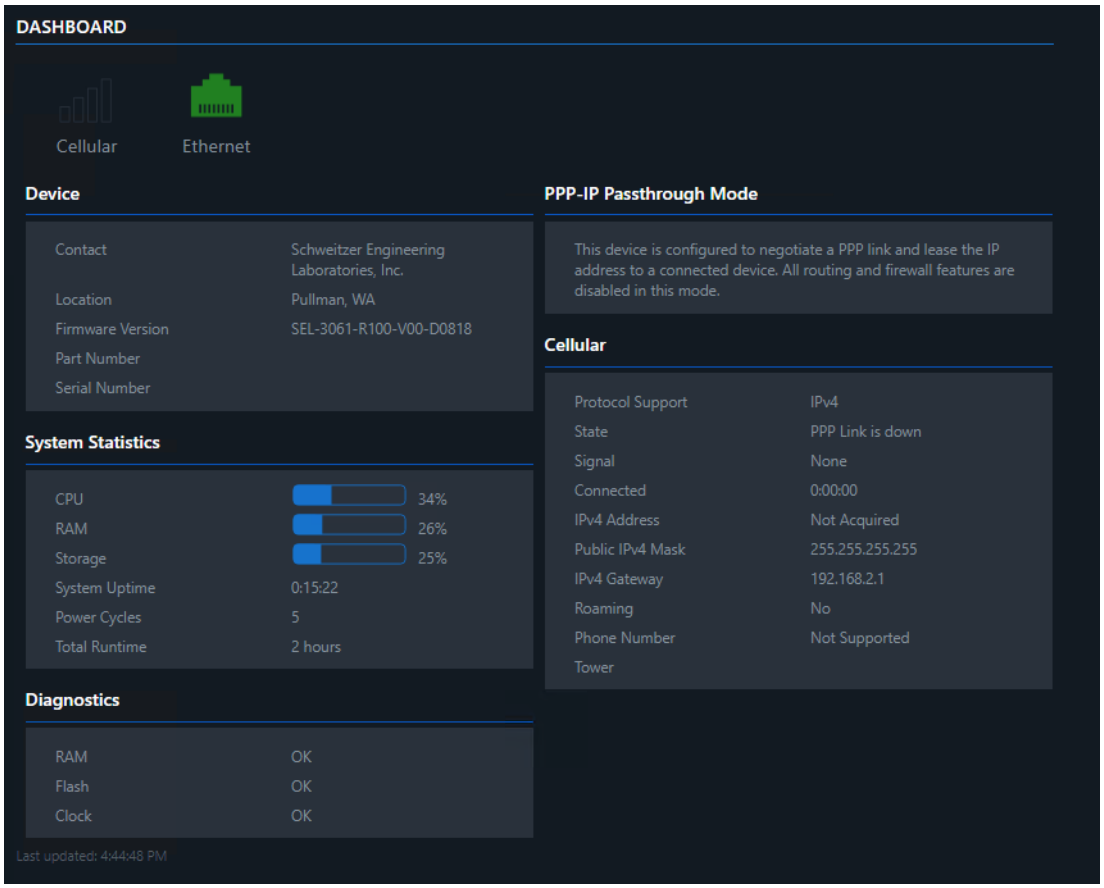


Figure 4.5 PPP-IP Passthrough Mode Dashboard

Access the PPP-IP Passthrough mode settings shown in *Figure 4.6* by navigating to **Configuration > PPP-IP Passthrough** in the SEL-3061 web interface. See *Table 4.9* for more information about the PPP-IP Passthrough mode settings.

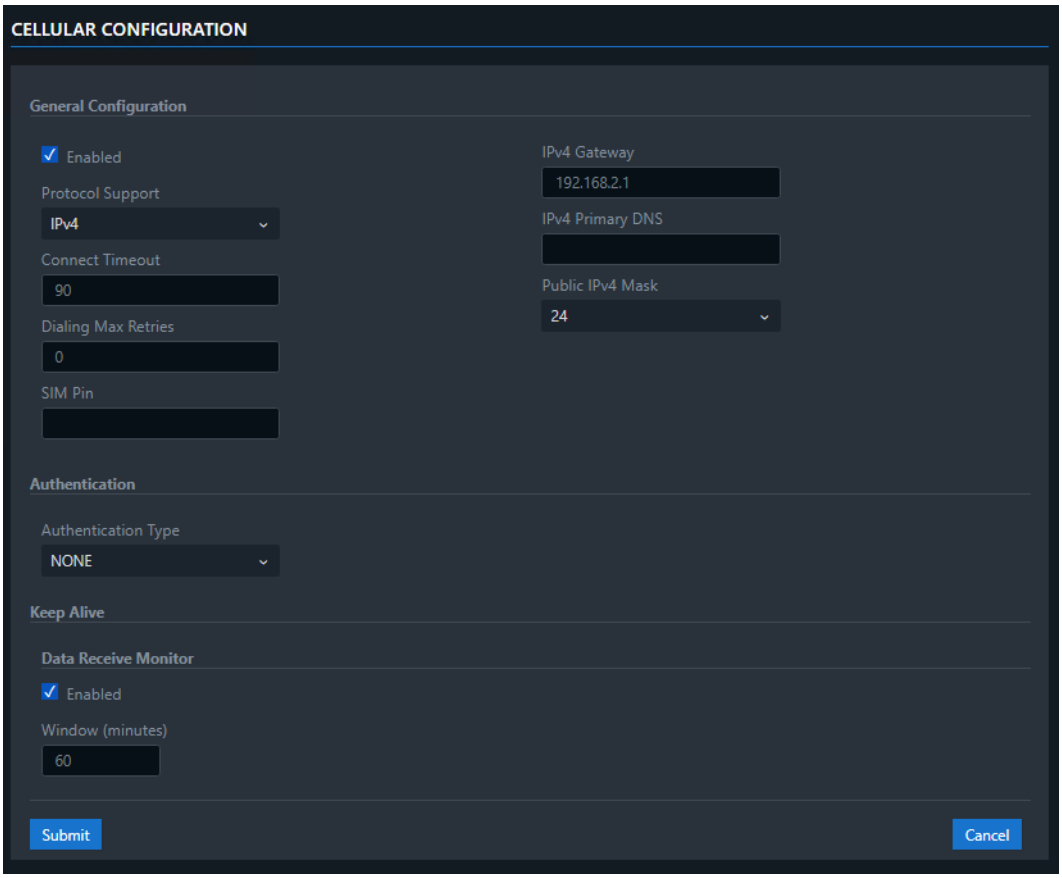


Figure 4.6 PPP-IP Passthrough Mode Settings

Table 4.9 PPP-IP Passthrough Mode Settings

Setting Name	Value	Default	Description
Protocol Support	IPv4 or IPv6	IPv4	The SEL-3061 supports these two versions of IP protocols.
IPv4 Gateway	Unicast IP address	192.168.2.1	The LAN interface IP address. Use the Ethernet port to configure the device in PPP-IP Passthrough mode.
IPv4 Primary DNS	Unicast IP address	[Empty]	The SEL-3061 uses the DNS server for naming translations.
Public IPv4 Mask	/24 or /32	/32	The SEL-3061 allows the connected device to set either /24 or /32 as the mask for the received IP address.

Generic Routing Encapsulation (GRE)

NOTE: GRE tunnels are not secure for transferring data.

GRE is a communications protocol for establishing direct, point-to-point connections between network devices. GRE provides a method of transporting data over a network by encapsulating (or tunneling) the packets.

To create a GRE tunnel, navigate to **Configuration > Tunnel > GRE Tunnels** and select **Add Tunnel** in the SEL-3061 web interface to access the GRE configuration page shown in *Figure 4.7*. After entering the GRE Tunnel settings, select **Submit**. Repeat the process for additional GRE tunnels.

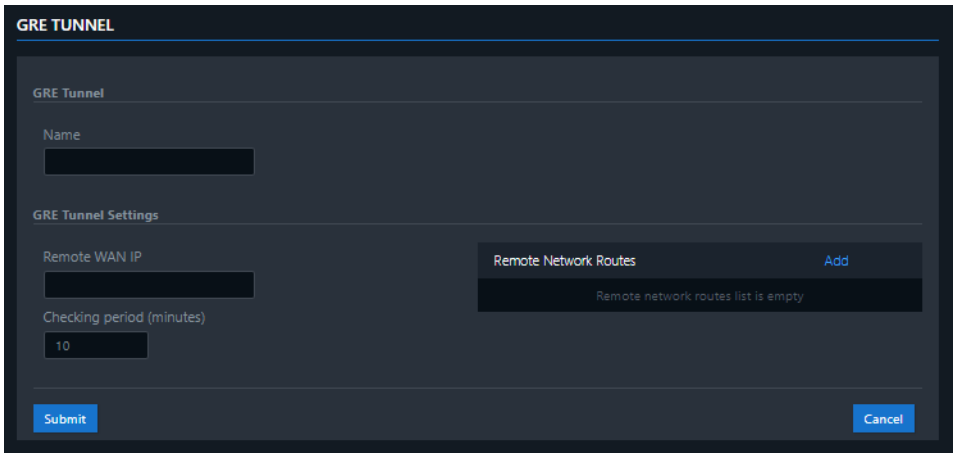


Figure 4.7 GRE Tunnel Configuration

The SEL-3061 allows multiple remote network routes for a GRE tunnel. The remote network routes define how each packet is forwarded (routed) once it reaches the GRE endpoint. Depending on the applications, it is possible for packets to be forwarded to different remote destinations.

Table 4.10 GRE Tunnel Settings

Setting Name	Value	Default	Description
Name	1–15 characters	[Empty]	Used by the SEL-3061 to track GRE tunnels.
Remote WAN IP	Unicast Address or domain name	[Empty]	Remote GRE endpoint IP address or domain name.
Checking period (minutes)	1–120 minutes	60 minutes	Used by the SEL-3061 to check remote GRE endpoint device.
Remote Network Route	Unicast Address or domain name	[Empty]	Remote network addresses.
Remote Network Mask	*xxx.xxx.xxx.xxx* or */n* where *xxx* is from 0 to 255 or */n* where *n* is from 1 to 32.	[Empty]	The device uses both classless interdomain routing (CIDR) notation and explicit notation to assign the subnet mask.

This page intentionally left blank

SECTION 5

Systems

The SEL-3061 web interface provides the means to enable and configure various features, including security.

The following sections include the menu path for each feature:

- *Web Interface Basics on page 5.1*
- *Access Configuration on page 5.8*
- *System on page 5.11*
- *Usage Policy on page 5.14*
- *User Accounts on page 5.15*
- *X.509 on page 5.27*
- *Device Reset on page 5.31*

Web Interface Basics

The SEL-3061 web server provides a convenient interface to manage the router.

Date, Time, and Present User Indication

While a user session is active, the top of each SEL-3061 web interface page displays the date, time, and user information, as shown in *Figure 5.1*. The Login screen does not include these fields.

Figure 5.1 Top Line of Web Interface

The date and time reflect the internal time in the SEL-3061, which might differ from the PC time. The time updates periodically, and you can force it to update by selecting the browser refresh button. The date and time settings are discussed in *User Accounts on page 5.15*.

The presently logged in user and their role is displayed on the top right of each webpage, alongside an open door icon. Select the door icon to close your session and log off.

Menu Area

The left-hand side of the web interface normally contains the menu entries, with Dashboard highlighted, as shown in *Figure 5.2*. If the browser window is not wide enough to display the menu, the menu automatically hides, and three expansion bars will appear, as shown in *Figure 5.3*.

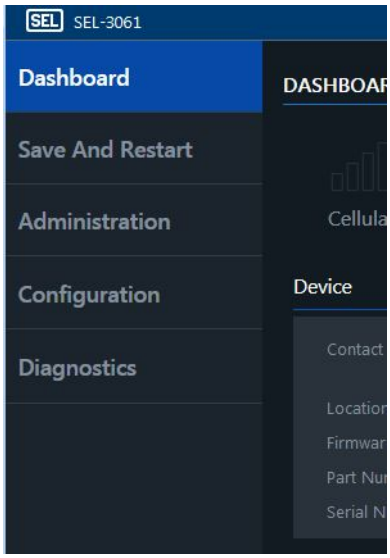


Figure 5.2 Menu Buttons

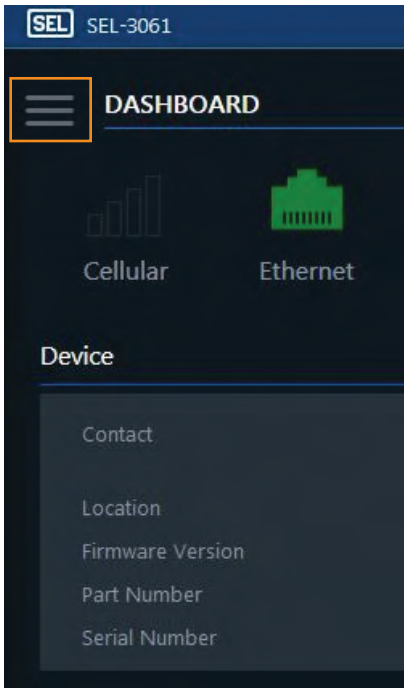


Figure 5.3 Hidden Menu With Expansion Bars

Select the expansion bars to open the menu. To close the menu, select the large **X** that appears beside the open menu (see *Figure 5.4*).

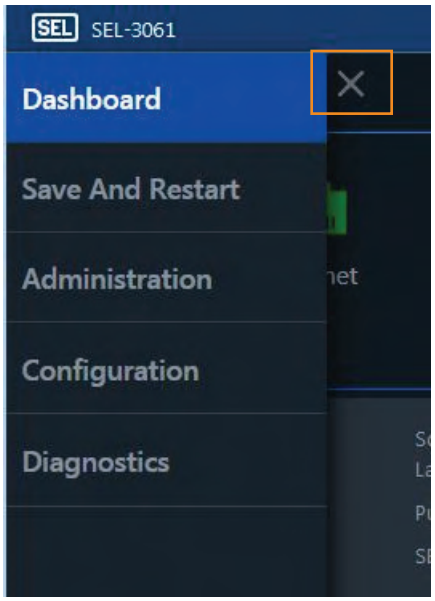


Figure 5.4 Close Button

Menu Buttons

The menu consists of the following five buttons. The various menu functionality is explained throughout this manual in the context of each topic.

Dashboard

Displays a read-only overview of the SEL-3061 status, status of network connections, hardware statistics and diagnostic readings, and device parameters (see *Figure 5.5*). The screen is arranged in panes to group each class. Some panes are hidden when a feature is not enabled.

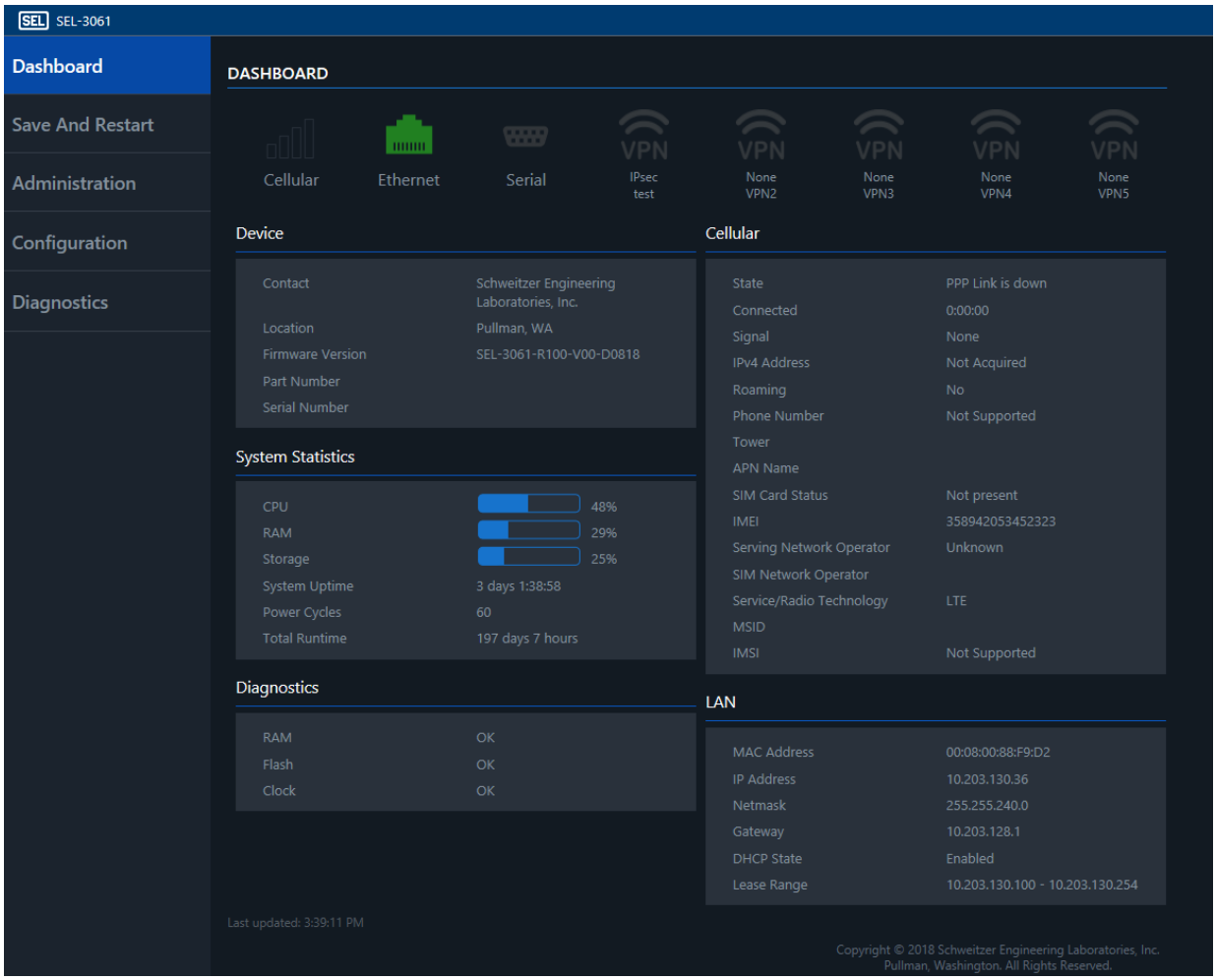


Figure 5.5 Dashboard Page

Save And Restart

This control must be pressed after making any settings changes. The button turns red, as shown in *Figure 5.6*, and slowly pulses when there are pending settings changes. When the button is pressed, a confirmation box appears (as shown in *Figure 5.7*). If accepted, the settings save and the device restarts. If the confirmation is dismissed, the button resumes flashing. If you do not want to save the recent settings changes, restart the device, as described in *Device Reboot on page 5.32*.

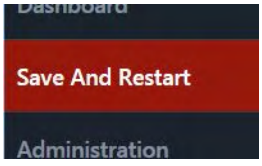


Figure 5.6 Save And Restart Shown in Red With Pending Changes

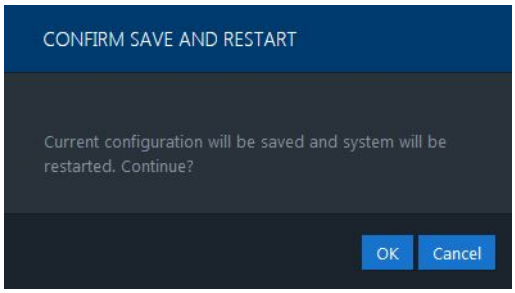


Figure 5.7 Confirm Save And Restart Dialog Box

Administration

Displays additional menu items, as shown in *Figure 5.8*.

Figure 5.8 Administration Menu

Configuration

Displays additional menu items, as shown in *Figure 5.9*.

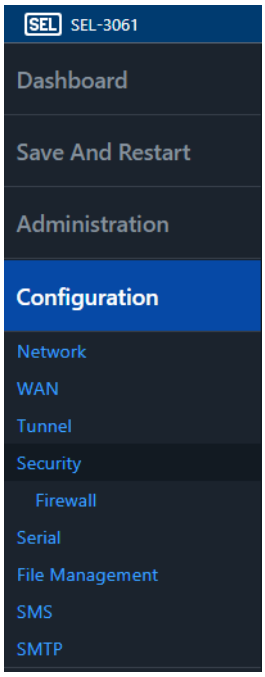


Figure 5.9 Configuration Menu

Diagnostics

Displays additional menu items, as shown in *Figure 5.10*.

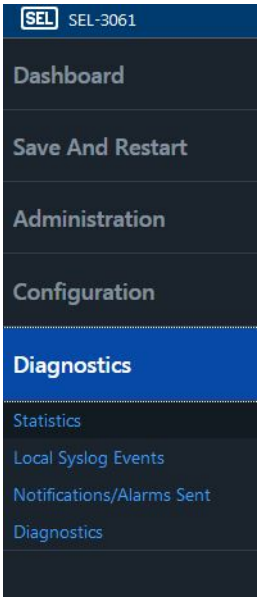


Figure 5.10 Diagnostics Menu

Notification Area

The SEL-3061 web interface includes a notification area, which is in the same location on any interface screen, highlighted in *Figure 5.11*. The SEL-3061 displays pop-up messages when informational events or system conditions and alarms occur.

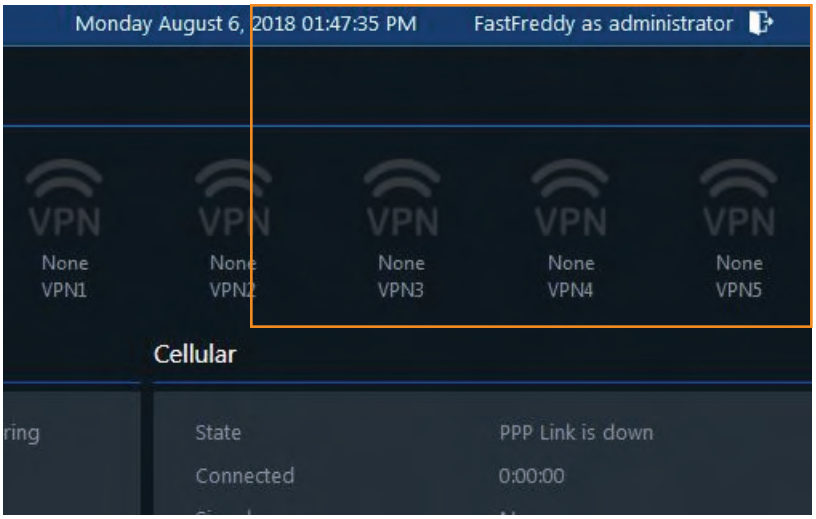


Figure 5.11 Notification Area—No Notifications Present

Red Notifications

Alarm items are displayed in a red box in the notification area, as shown in *Figure 5.12*. Red box notifications remain on the screen until acknowledged. Multiple red box indications extend down the page. To acknowledge and dismiss a red pop-up message, select the text within the red box. Multiple red boxes must be separately acknowledged. The presence of an unacknowledged red box indication has no direct effect on the web interface, except it can obscure webpage content or controls.

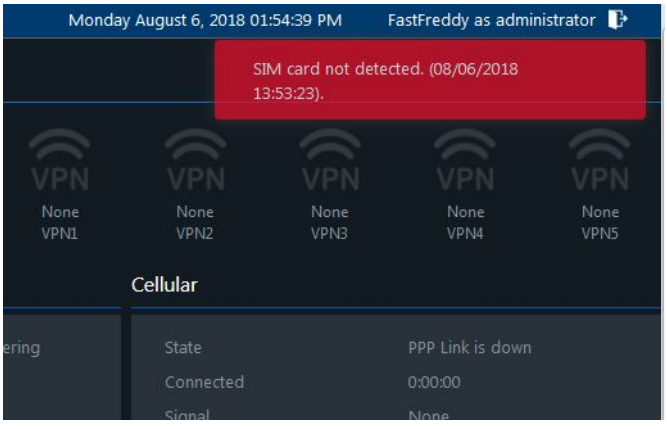


Figure 5.12 Notification Area—Red Box Sample

Green Notifications

The notifications in a green box appear for approximately five seconds, then automatically disappear. *Figure 5.13* shows a green box notification that appears after a settings change.

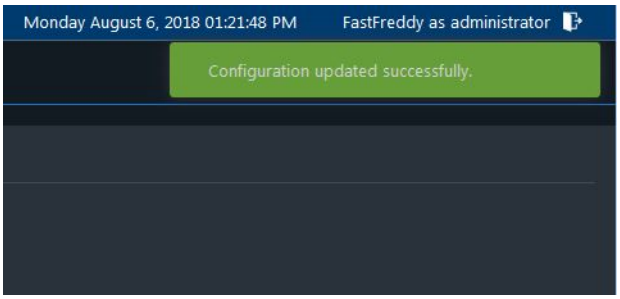


Figure 5.13 Notification Area—Green Box Sample

Tool Tips Help

The SEL-3061 provides tool tips when the cursor hovers over the description of a setting, as shown in *Figure 5.14*. Tool tips provide some basic information that can help users when entering settings.

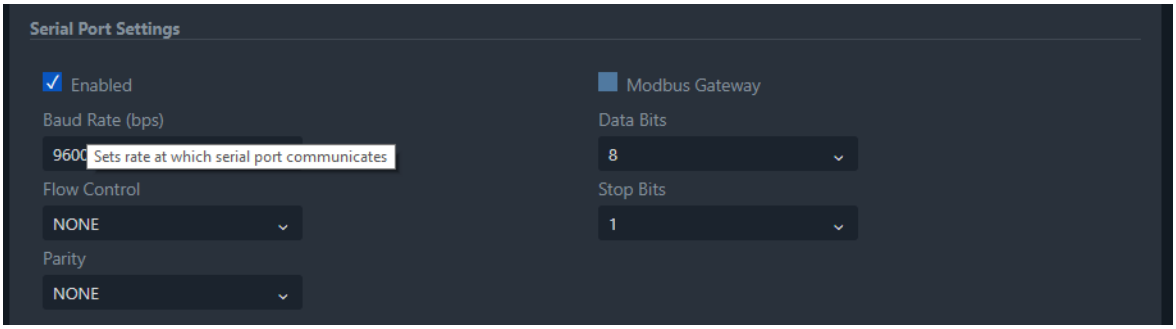


Figure 5.14 Tool Tip

Access Configuration

NOTE: All of the web server attributes are available in SEL-3061 Network Router mode. The PPP-IP Passthrough mode offers a subset.

The Access Configuration page under Administration includes configurations for web server HTTPS, Secure Shell (SSH), Internet Control Message Protocol (ICMP), and a set of cybersecurity features called IP Defense. All HTTPS, SSH, and ICMP selections are disabled by default, with the exception of HTTPS via LAN.

Web Server HTTPS

HTTPS is a service that allows the internet browser client to connect to the device to manage configuration settings. By default, HTTPS is enabled for LAN (Ethernet) only. The port number is 443 and cannot be changed, as shown in *Figure 5.15*. To access the web server from the network, you can enable via WAN. In this case, you can access the web user interface from a public network or nonsecure network, which can increase the likelihood of cybersecurity vulnerabilities and cellular data usage.

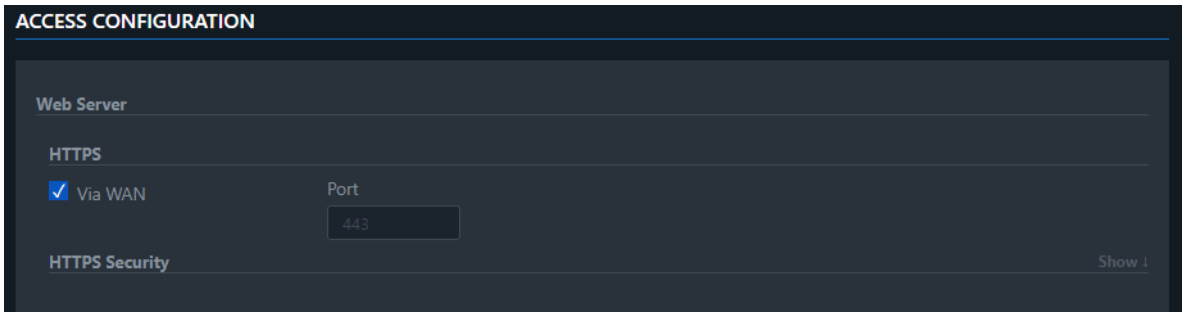


Figure 5.15 Web Server HTTPS Configuration

Transport Layer Security (TLS) protocol handles HTTPS security. TLSv1.2 is enabled on the web server by default, and TLSv1.1 is disabled by default, as shown in *Figure 5.16*. Select **Show** to see the status of the HTTPS secure settings.

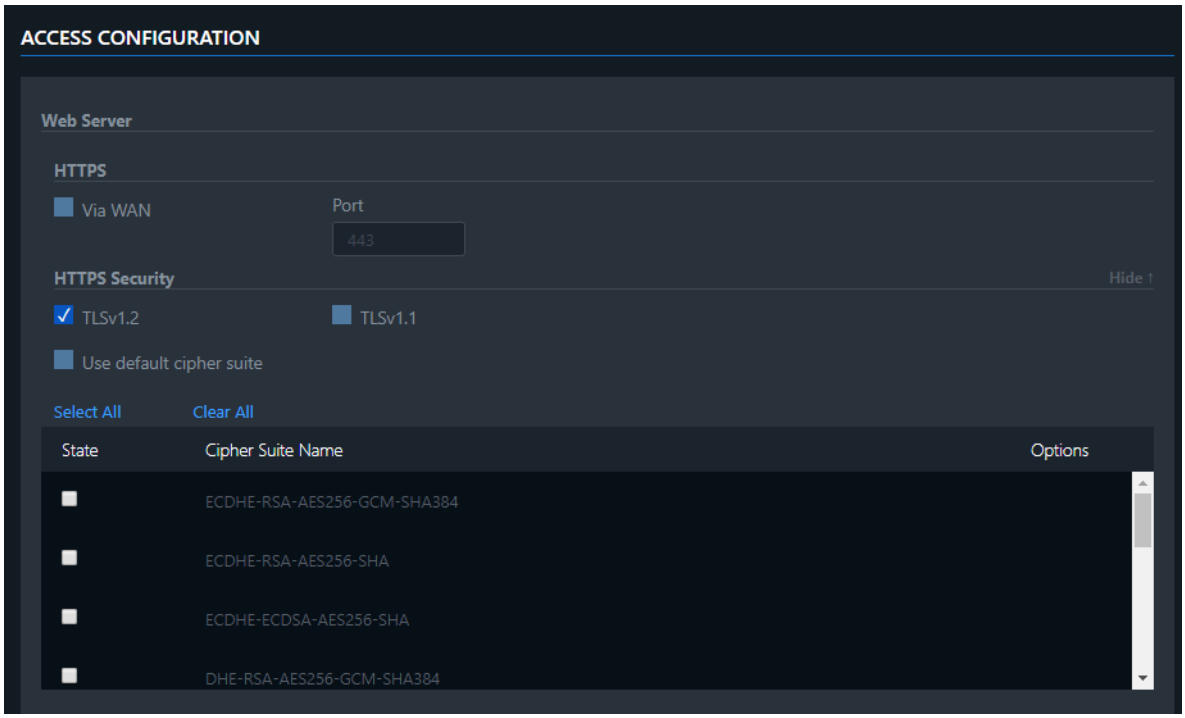


Figure 5.16 TLS Cipher Suites

The Use default cipher suite check box is selected by default, which means that the SEL-3061 uses any of the listed cipher suites to negotiate with a web browser when establishing a web interface session. If you clear the Use default cipher suite check box, the SEL-3061 allows you to select specific cipher suite(s) for establishing HTTPS. The list of available cipher suite are:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA
- ECDHE-ECDSA-AES256-SHA
- DHE-RSA-AES256-GCM-SHA384
- AES256-SHA
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256

- ECDHE-RSA-AES128-SHA
- ECDHE-ECDSA-AES128-SHA
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA
- AES128-SHA

ICMP Settings

NOTE: The ping protocol, ICMP, is disabled by default. If you cannot ping the Ethernet port of the SEL-3061, ensure that ICMP is enabled.

ICMP allows you to ping the device from either the LAN or WAN interface and is disabled by default. When it is first enabled, the ping response via LAN is initially enabled, and the WAN response is disabled. You can enable a ping response via WAN; however, this exposes the device to have to respond to ping requests from the public or nonsecure network. Enabling the response via WAN can increase the likelihood of cybersecurity vulnerabilities because anyone on the network can ping the SEL-3061.

IP Defense

IP Defense is a set of features that can prevent or slow down denial-of-service (DoS) attacks or other malicious actions taken against the SEL-3061. The features include DoS Prevention, Ping Limit, and Brute Force Prevention, as shown in *Figure 5.17*. DoS Prevention and Ping Limit are disabled by default, and Brute Force Prevention is enabled by default.

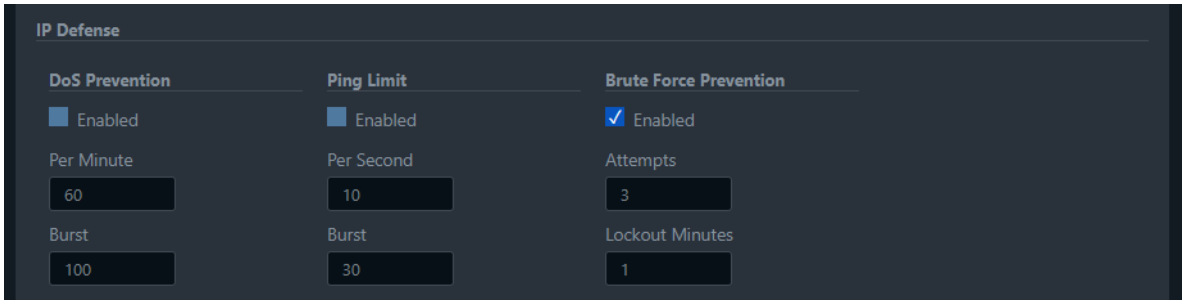


Figure 5.17 IP Defense Configuration

DoS Prevention

DoS Prevention limits the average number of new connection requests per minute, and Burst limits the number of allowable sessions. By reducing these numbers, the device may slow down the DoS attack or other malicious actions taken against the SEL-3061.

Table 5.1 DoS Prevention Settings

Setting Name	Value	Default	Description
DoS Enabled	Checked or unchecked	Unchecked	Enable DoS Prevention.
Per Minute	1–10000	60	Number of new connection requests accepted per minute.
Burst	1–10000	100	Number of new connections accepted/allowed by burst.

Ping Limit

The Ping Limit defines the average number of pings per second that the SEL-3061 can receive before dropping pings, and Burst limits the number of pings allowed per burst. By limiting these numbers, it is unlikely that the SEL-3061 will be kept busy responding to ping requests. Once the ping request exceeds the number of ping per second, the SEL-3061 ignores additional ping requests.

Table 5.2 Ping Limit Settings

Setting Name	Value	Default	Description
Ping Limit Enabled	Checked or unchecked	Unchecked	Enable Ping Limit.
Per Second	1–99999	10	Average number of ping requests the SEL-3061 receives before it starts dropping them.
Burst	1–99999	30	Number of pings allowed per burst.

Brute Force Prevention

Brute Force Prevention protects the SEL-3061 from brute force attackers attempting to log in and is enabled by default. The Attempt setting limits the number of attempts to log in to the SEL-3061 before it locks out. The Lockout Minutes setting defines how long the device remains locked once the number of attempts have been reached. By default, the number of attempts is 3 and Lockout Minutes is 1.

Table 5.3 Brute Force Prevention Settings

Setting Name	Value	Default	Description
Brute Force Prevention	Checked or unchecked	Unchecked	Enable Brute Force Prevention.
Attempts	1–99999	3	Number of attempts to log in with incorrect credentials to the SEL-3061.
Lockout Minutes	1–99999	1	Number of minutes the SEL-3061 locks itself once the number of attempts has been reached.

System

Global Settings

Access **Administration > System > Global Settings** to customize the settings for the web interface user session, the SEL-3061 data history, and the system contact information.

Settings

The Global Settings page contains the User Session, Statistics, and System Contact Information categories, as shown in *Figure 5.18*. See *Table 5.4* for settings descriptions.

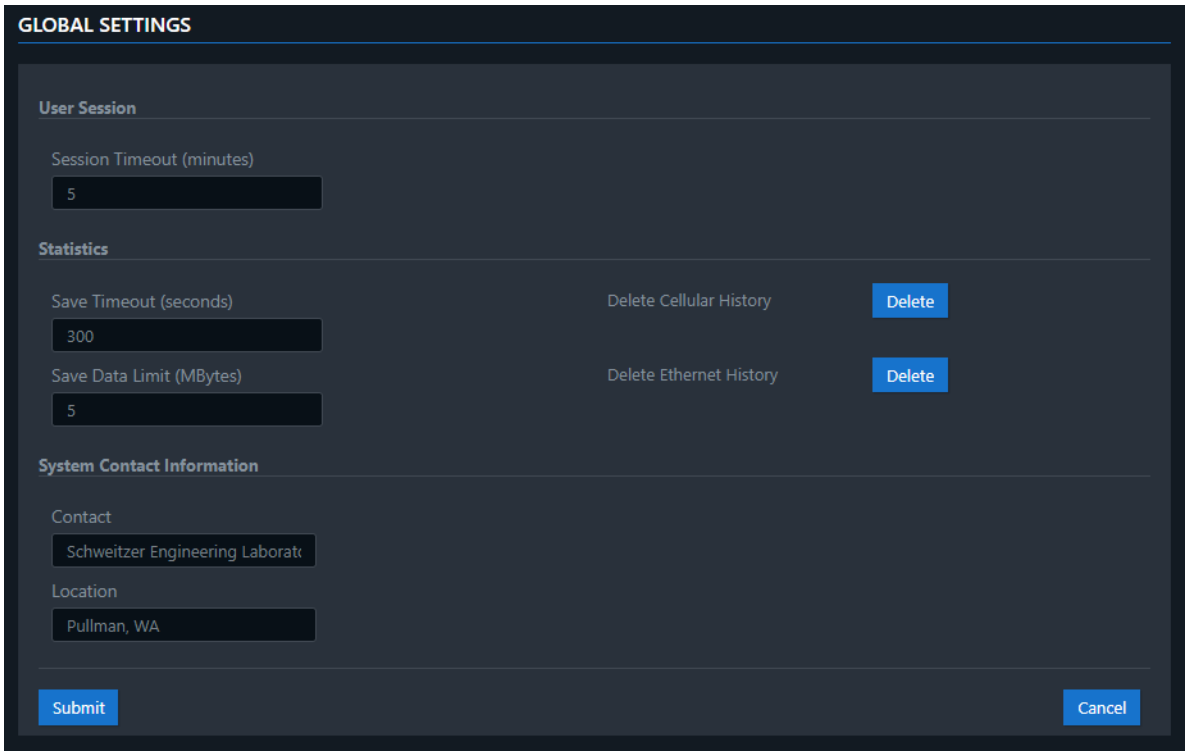


Figure 5.18 Global Settings Menu

Table 5.4 Global Settings

Setting Name	Values	Default	Description
Session Timeout	1–60 minutes	60 minutes	Minutes that pass without activity before the secure session times out and you are logged out of the SEL-3061.
Save Timeout	60–86,400 seconds	300 seconds	Defines the statistics update interval.
Save Data Limit	1–100 MB	5 MB	Defines the maximum amount of data traffic before a statistics update if the Save Timeout interval has not yet elapsed.
Contact	0–128 characters	Schweitzer Engineering Laboratories, Inc.	Contact information for the device.
Location	0–32 characters	Pullman, WA	Location of the device.

Date/Time

The SEL-3061 uses date and time information to time-stamp Syslog events, SMS messages, email notifications, and several functions available in the web interface. The SEL-3061 uses a battery-backed clock to retain date and time through a loss-of-power event.

The SEL-3061 supports both manual date and time adjustment, as well as automatic date and time synchronization through the use of SNTP.

Access the local time settings shown in *Figure 5.19* by navigating to **Administration > System > Date/Time** on the SEL-3061 web interface.

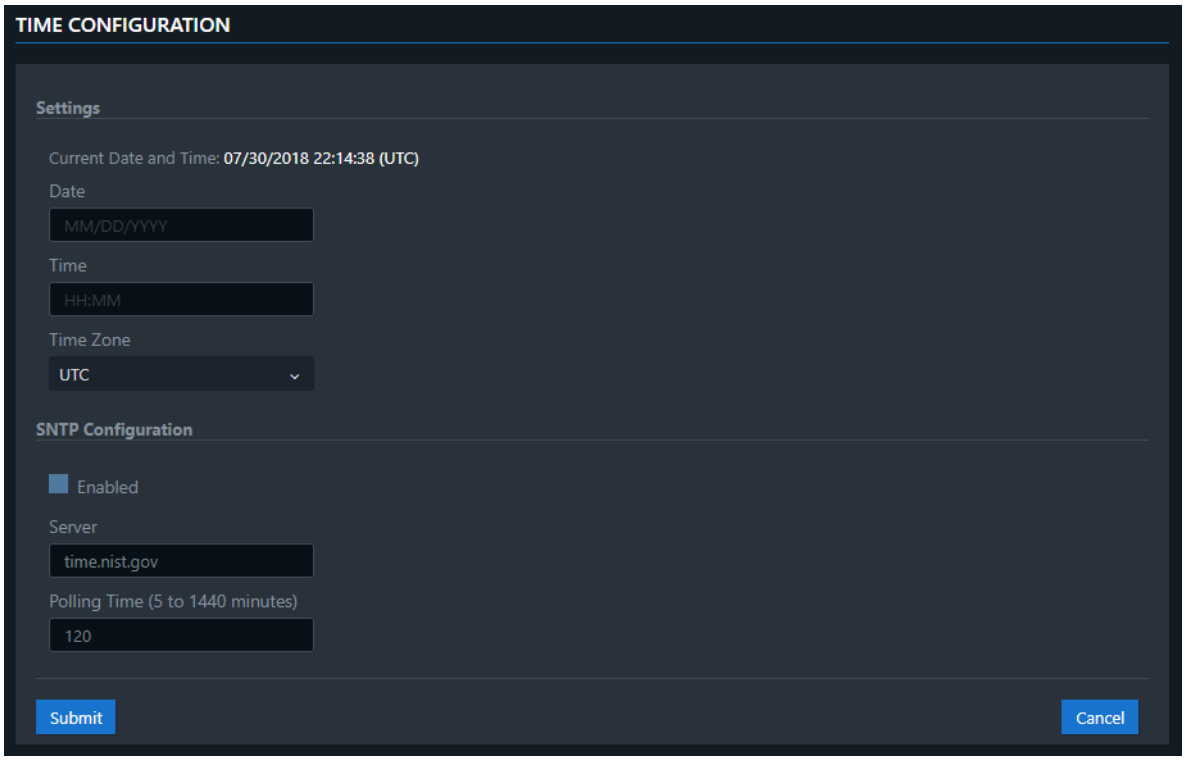


Figure 5.19 Time Configuration

Time Source

The SEL-3061 date and time can be either set manually through the use of the web interface or synchronized automatically through use of SNTP. Setting the time source to SNTP overrides any manual date and time adjustments. An SNTP server is required to receive automatic synchronization when using an SNTP time source. You must enter a polling time for the SEL-3061 to adjust and synchronize its time with the SNTP server. By default, SNTP is disabled.

Manual Date/Time

NOTE: The SEL-3061 does not provide automatic daylight-saving time adjustments.

To set Date and Time manually, enter the date and time in the setting fields. When you select the Date field, a calendar appears for you to select the date. You must enter the time manually. You can set the time zone by selecting one of the zones from the Time Zone drop-down list. Select **Submit** to apply the changes. *Table 5.5* describes the manual date and time settings.

Table 5.5 Manual Date and Time Settings

Setting Name	Value (format)	Default	Description
Date	MM/DD/YYYY	[Empty]	Current date. Use the calendar to select the date.
Time	HH:MM (HH: 0–24 and MM: 0–59)	[Empty]	Current time. You have to enter the time manually.
Time Zone	List of standard time zones	UTC	Time zone where the device is installed. The time zone includes all international time zones and UTC.

SNTP Configuration

SNTP is a version of Network Time Protocol (NTP), which is used to synchronize device clocks on a network. The SEL-3061 is an SNTP client that requires an SNTP server to synchronize the time. The SNTP server must be network-reachable from the SEL-3061. By default, SNTP is disabled. The SNTP settings are described in *Table 5.6*.

Table 5.6 SNTP Settings

Setting Name	Value (format)	Default	Description
Enabled	Checked or unchecked	Unchecked	Enable or disable SNTP.
Server	Unicast name or domain name	time.nist.gov	SNTP server the SEL-3061 uses to adjust its time.
Polling Time	5–1440 minutes	120 minutes	Interval the SEL-3061 uses to request the SNTP server to adjust its time.

Usage Policy

Overview

The SEL-3061 presents a usage policy to all users accessing the login or commissioning pages, designed to notify users regarding what constitutes appropriate use of the SEL-3061, what actions are necessary to ensure the SEL-3061 is not used inappropriately, and what actions will be taken if abuse is discovered. This system message can be changed by the organization. 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

Configure the SEL-3061 Usage Policy via the settings interface in a web browser by using the **Administration > Usage Policy** menu option.

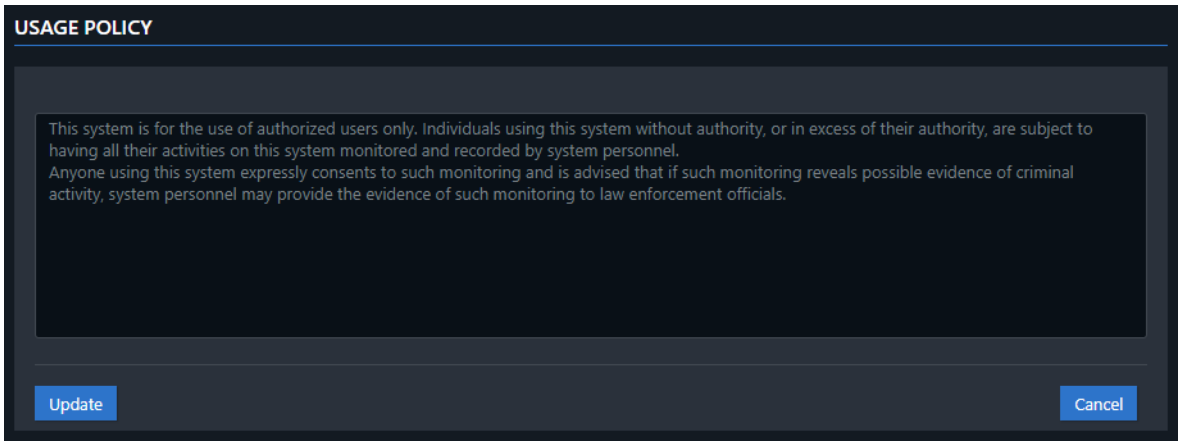


Figure 5.20 Usage Policy

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

If the Usage Policy window is empty and you select **Update**, a message appears and asks you if you want to keep the default usage policy shown in *Figure 5.20*. Select **OK** to keep the default policy or **Cancel** to leave the usage policy empty.

User Accounts

User accounts allow for engineering access on SEL products. SEL has historically used global accounts, such as Access Level 1 and Access Level 2 (accessible via the ACC and 2AC commands, respectively), to control access.

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, the SEL-3061 provides a user-based account structure.

The SEL-3061 stores user accounts in nonvolatile memory. This allows the device to maintain account status through power cycles and other unexpected events. This section includes the following:

Logging In With SEL User-Based Accounts

Upon connecting to the SEL-3061, the device usage policy and a login prompt appears. To log in, enter a valid username and the corresponding password. Usernames are case-sensitive and unique to each individual with authority to access the SEL-3061. Passwords are case-sensitive.

NOTE: Before accessing the SEL-3061 for the first time, see *Commissioning the Device on page 2.6* to create the initial account.

If the SEL-3061 determines a username or password to be invalid, it rejects the access attempt and alerts the user that the login credentials were incorrect. By default, after three consecutive failed login attempts, the SEL-3061 blocks access attempts with that username for 1 minute. This setting can be changed in Access Configuration (see *Access Configuration on page 5.8*). Each failed login attempt generates a Syslog event. Additionally, a Syslog event and a minor alarm are generated when an account is locked out after too many failed login attempts. These security features are designed to prevent and slow down password guessing attacks. Login failure can occur for three reasons: the username is invalid, the password is incorrect, or the user account is disabled. 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, 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. User-based accounts have the ability to disable or remove an individual account without affecting access for other users. 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 both the need to write passwords down and 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. 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 who they claim to be.

Authorization is the process of granting privileges to users of a system. User-based accounts allow you to assign specific privileges to each user of a system.

Accountability is the idea that individual users can be held responsible for their actions on a system. User-based accounts provide the ability to clearly authenticate users of the system based on their credentials. All actions are tracked to a specific user account, and users can only perform actions allowed by their account privileges. Accountability is important for event tracking and forensic investigations.

Roles

Device permissions are organized into roles, and access is granted through role-based access controls. The SEL-3061 has three roles: Administrator, Engineer, and Monitor. User account privileges are based on the 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 SEL-3061.
- **Engineer**: Users have access to most SEL-3061 settings and information, but cannot access user account management.
- **Monitor**: Users have read-only access to SEL-3061 settings.

Table 5.7 User-Based Accounts Role Access

Navigation Pane Options	User Roles		
	Administrator	Engineer	Monitor
Dashboard	Read	Read	Read
Administration			
User Accounts	Read/Write	Not visible (can change own password only)	Not visible (can change own password only)
RADIUS	Read/Write	Read	Not visible
Access Configuration	Read/Write	Read	Read
Usage Policy	Read/Write	Read	Read
System			
Global Settings	Read/Write	Read	Read
Date/Time	Read/Write	Read/Write	Not visible
Device Reset	Read/Write	Not visible	Not visible
Syslog	Read/Write	Read	Read
Notifications/Alarms	Read/Write	Read	Not visible
X.509 Certificates	Read/Write	Read	Not visible
Configuration			
Network			
IP Configuration	Read/Write	Read/Write	Not visible
Advanced	Read/Write	Read/Write	Not visible
WAN			
Cellular Configuration	Read/Write	Read/Write	Read
Advanced	Read/Write	Read/Write	Not visible
Tunnel			
IPsec VPN 1 or GRE 1	Read/Write	Read/Write	Read
IPsec VPN 2 or GRE 2	Read/Write	Read/Write	Read
IPsec VPN 3 or GRE 3	Read/Write	Read/Write	Read
IPsec VPN 4 or GRE 4	Read/Write	Read/Write	Read
IPsec VPN 5 or GRE 5	Read/Write	Read/Write	Read
Security			
Firewall	Read/Write	Read/Write	Read
Serial			
File Management			
Settings	Read/Write	Not visible	Not visible
Firmware Upgrade	Read/Write	Not visible	Not visible
Diagnostics			
Statistics	Read	Read	Read
Local Syslog Events	Read	Read	Read
Notifications/Alarms Sent	Read	Read	Read
Diagnostics	Read	Read	Read

Administration of User-Based Accounts

The SEL-3061 is shipped from the factory with no user accounts installed. To access the product, you must create an initial account through the use of the device commissioning page. This account will be an Administrator account, which has authorization to add, remove, enable, and disable system users. Only the individual who creates this account should have knowledge of this account password. Note that you cannot delete the account that you are logged into, but the SEL-3061 allows you to modify its contents, such as password and other related information.

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

Passwords (Passphrases)

Passwords or passphrases provide users the ability to create strong and easy-to-remember passwords that protect access to a system. A strong password includes many different characters from many different character sets. Longer passwords provide greater security than shorter passwords. SEL-3061 user-based accounts require complex passphrases that must include the following:

- 8–4096 characters
- An uppercase character
- A lowercase character
- A number
- A special character

Sample passphrases include the following:

Strong: W3b$ter!

Stronger: A phras3 is 3v3n Str0ng3r!

NOTE: Although an administrator-level user may change any other user's passphrase, they cannot view an existing user passphrase.

Users with access to user account management (i.e., Administrator) can set or change passphrases for any user. Users without such access can only change their own password. For the protection of your account, the SEL-3061 never displays, transmits, or stores a passphrase in plaintext.

Managing User Accounts

This section discusses the settings used to configure and manage local user accounts on the SEL-3061. If the current (logged in) user has access to user account management (i.e., Administrator), access the user accounts settings shown *Figure 5.21* by navigating to **Administration > User Accounts** on the SEL-3061 web interface.

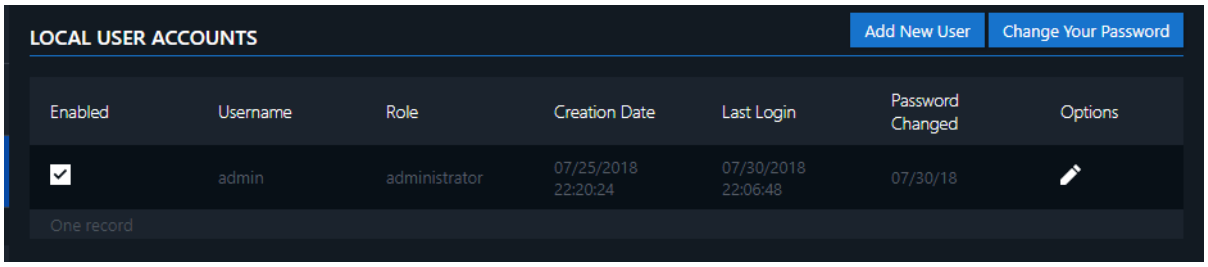


Figure 5.21 Managing User Accounts

Add New User

Select **Add New User**. Complete all the fields shown in *Figure 5.22* and select **Submit**.

Only two fields are required: Username and User Role. All other fields are optional.

Usernames are case-sensitive and may not contain spaces. Allowable characters include letters, numbers, hyphens, and underscores. A username cannot start with a hyphen character.

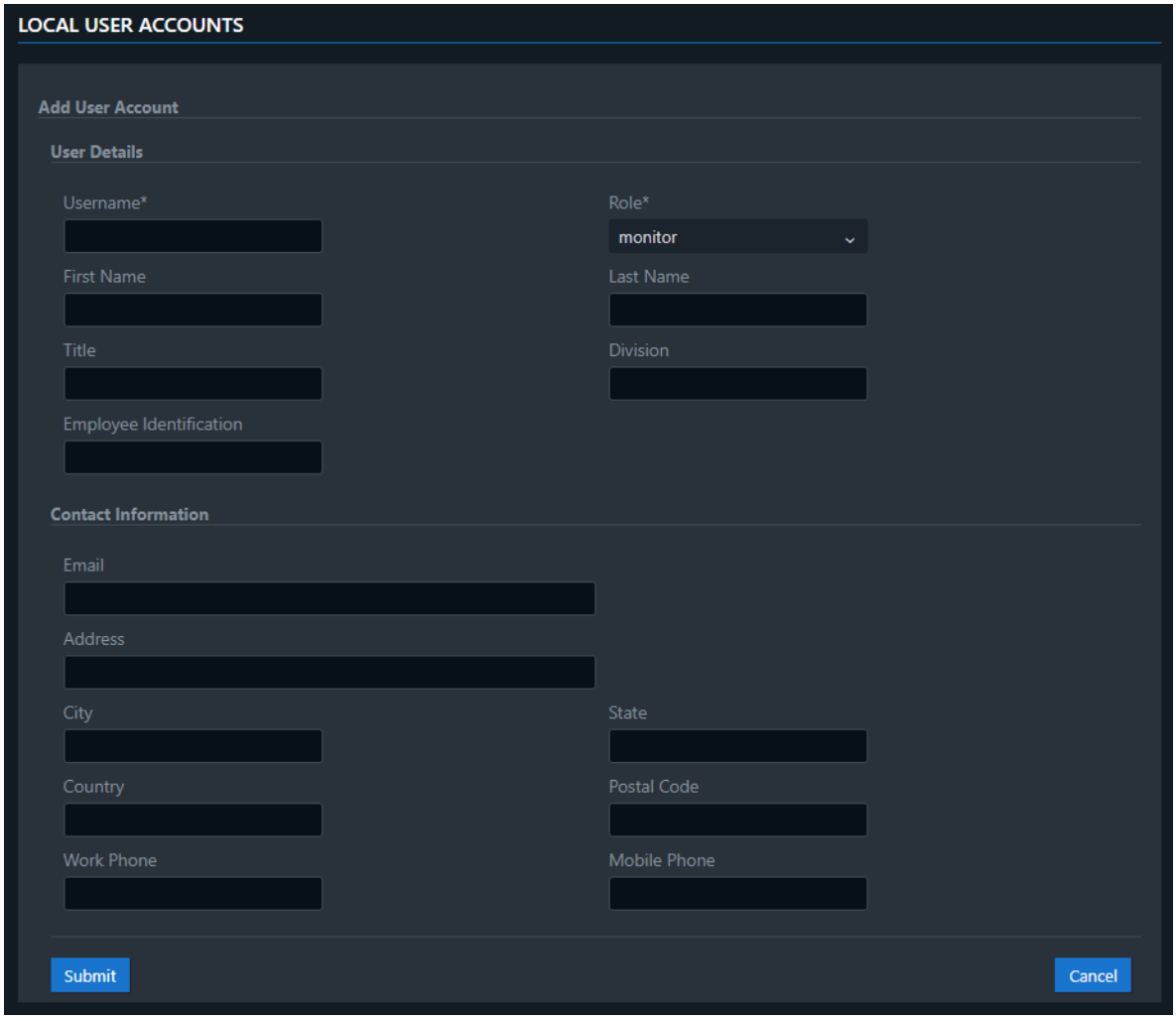


Figure 5.22 Add User Accounts

The SEL-3061 prompts you to enter a new password for the username you created, as shown in *Figure 5.23*.

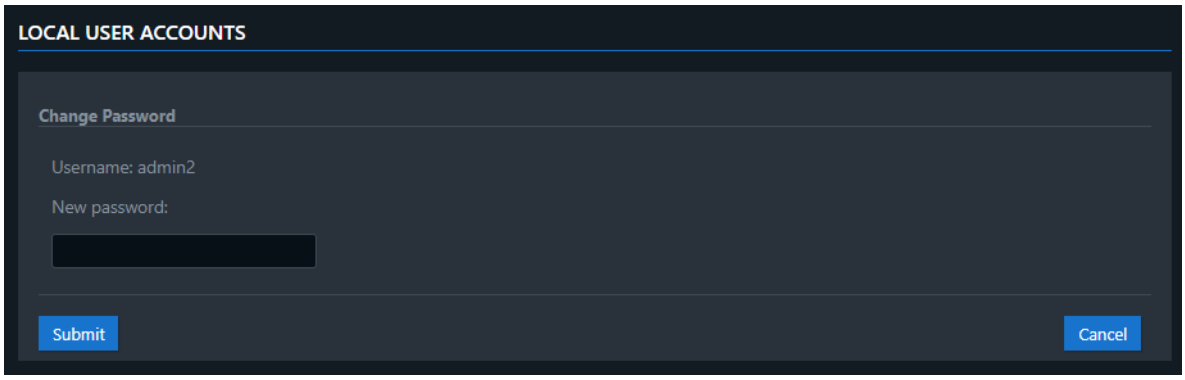


Figure 5.23 Enter a New Password

Select **Submit** and the SEL-3061 prompts you to confirm your password by entering the same password again, as shown in *Figure 5.24*. The passwords must match to create the account.

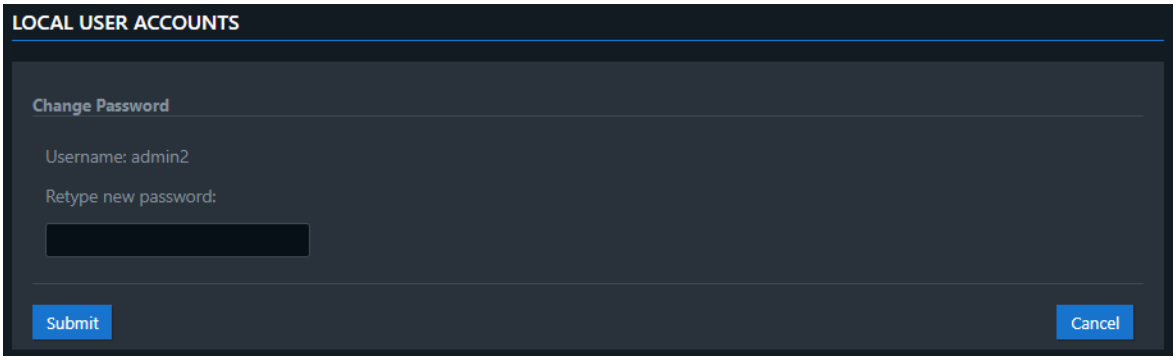


Figure 5.24 Confirm New Password

Edit User

Select the pencil icon associated with a user account to edit an existing user. The dialog box is similar to that for adding a new user, except that the Username field is already defined and cannot be changed (see *Figure 5.25*).

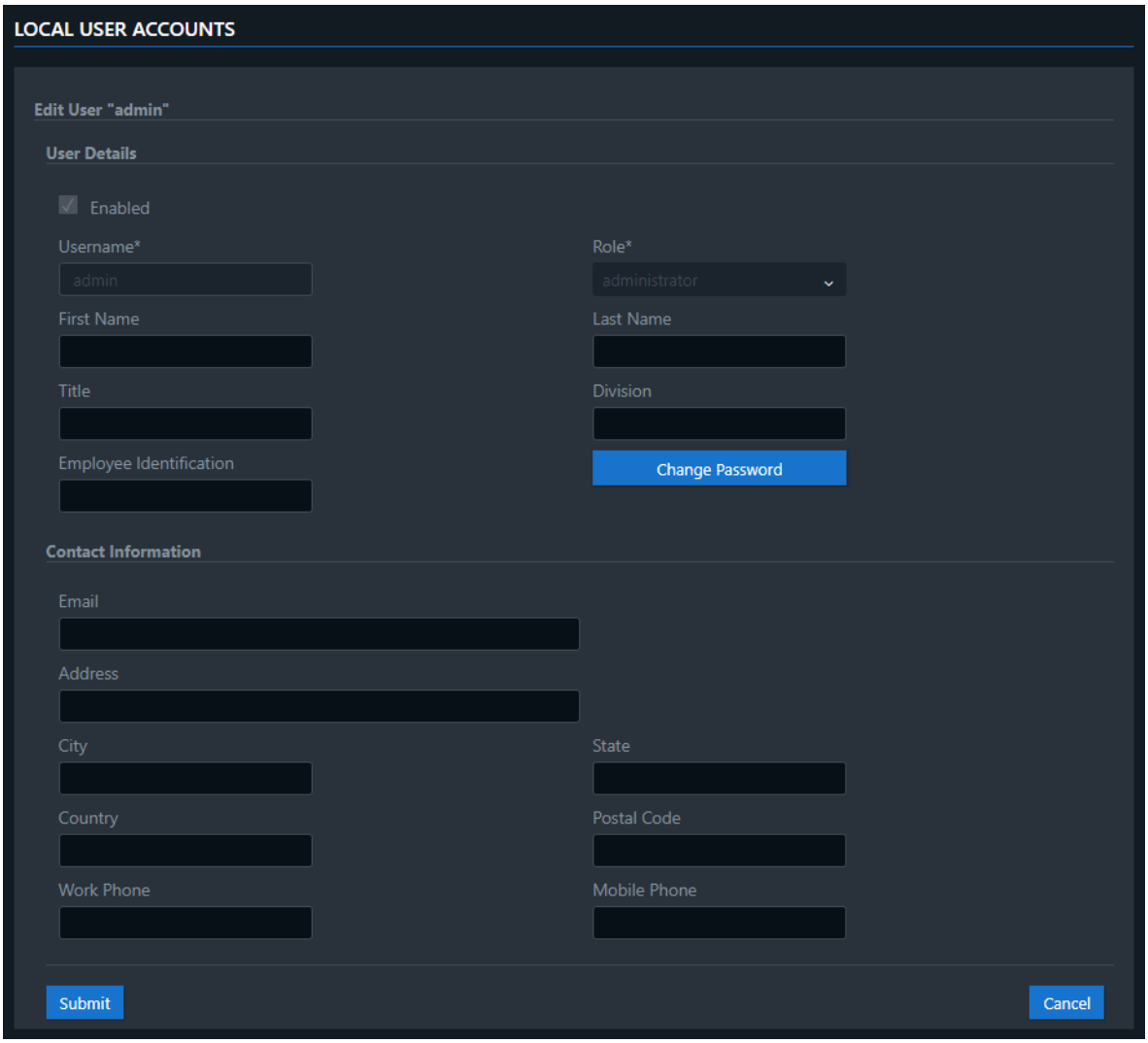


Figure 5.25 Edit User Account

Delete User

Select the trash can icon associated with a user account to delete that user account. The SEL-3061 requires that an Administrator-level account be available and enabled at all times. You can only delete an Administrator-level account if you are logged in to a separate Administrator account. You cannot disable or delete the account used for logging into the SEL-3061.

Change Password

To change the password of the current user or reset password of another account, select the pencil icon and then select **Change Password**. This allows the user to change the password on the user account that is currently accessing the SEL-3061. Before changing the password, you must enter the current password (see *Figure 5.26*). The new password must meet the password policy, as described in *Passwords (Passphrases) on page 5.18*. Select **Submit**, and then select **Save And Restart** to apply the new password settings.

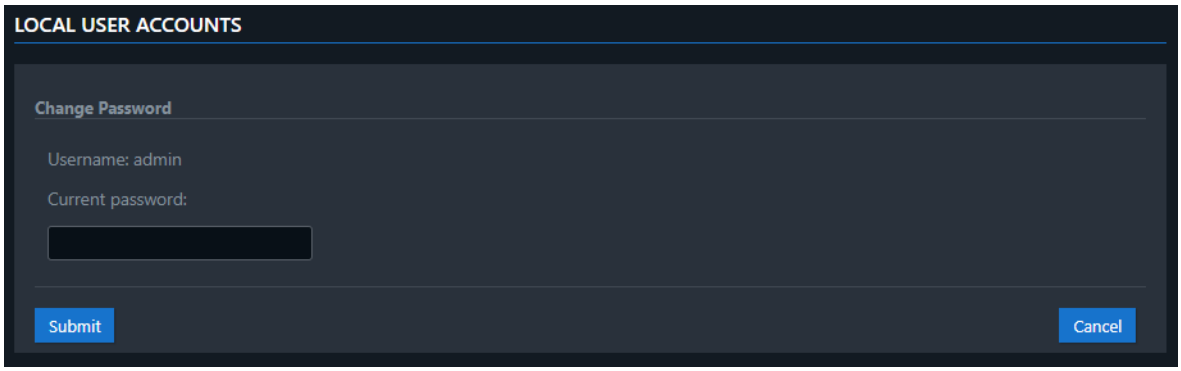


Figure 5.26 Enter Current Password

Dashboard Indications

The current user and role are always displayed in the upper right corner of the SEL-3061 web interface. You can change the password or log out by selecting the user icon shown in *Figure 5.27*.

Figure 5.27 User Icon

RADIUS

The Remote Authentication Dial-In User Service (RADIUS) protocol is a high-performance way to allow a computer system or device to delegate user authentication. RADIUS allows a system that needs to authenticate a user to give the user credentials to a central authority for processing and to receive either an access-granted or an access-denied message. The encryption built into the RADIUS protocol protects the connection between the requester and the RADIUS server. Some organizations already use RADIUS for user authentication, so providing centralized access control to SCADA devices by using RADIUS with the device is a natural choice. SEL has application guides (see selinc.com/literature/application-guides) that provide step-by-step instructions to help you configure the following RADIUS servers:

- FreeRADIUS 2.0+ (open source at http://freeradius.org)
- RSA Authentication Manager
- Cisco Secure ACS
- Cisco Secure ISE
- Microsoft Windows NPS
- OpenOTP RADIUS Bridge

Centralized User Accounts

To enforce distinct, centrally managed privileges for RADIUS user authentication, user accounts must normally belong to security groups in your enterprise directory (e.g., Active Directory) that can be mapped to the different user roles supported by the SEL-3061. The RADIUS server receives group membership information to an authenticating user and uses this information to determine the

role of the user when logging into the SEL-3061 or the Authentication Proxy. The user role for logging into the SEL-3061 is returned to the client in the SEL-User-Role attribute. The user role for the Authentication Proxy is returned in the SEL-Proxy-Group attribute. It is also possible to use the RADIUS server with accounts and privilege information in a local configuration file maintained on the RADIUS server, but this is not the best practice for reasons of security and scalability.

User Roles for Login

An Administrator has full administrative control privileges. Users with Administrator privileges can read and write all settings and information on the device. An Engineer has access to most device settings and information, but cannot access user account management and some administrative control privileges. A Monitor has read-only access. Users with Monitor privileges are able to read most settings and data but cannot write any settings. In particular, a Monitor user cannot view or modify settings that affect user authentication (e.g., user accounts or RADIUS).

Configuring Your RADIUS Server

To use the SEL-3061 with the RADIUS server of your organization, configure the RADIUS server to include certain SEL Vendor-Specific Attributes (VSAs) in the Access-Accept message returned when you successfully log in. These attributes are used to send information to the SEL-3061 about your role and proxy group. They are defined in the dictionary.sel file that you can download from the RADIUS configuration page on the device website. This file can also be found on the SEL-3061 CD or in *Appendix E: SEL RADIUS Dictionary*.

The RADIUS client implementation sends four RADIUS Attribute Value Pairs (AVP) when making an initial Access-Request to a remote RADIUS server: User-Name (AVP Type 1), User-Password (AVP Type 2), and NAS-Identifier (AVP Type 32).

For more information about configuring particular RADIUS environments, refer to the Literature tab on the SEL-3620 product page of the SEL website (selinc.com/products/3620/).

Configuring the SEL-3061 as a RADIUS Client

Configuring the SEL-3061 as a RADIUS client involves setting the network address information for one or two RADIUS servers, selecting options, and setting the shared secret (i.e., password) used to encrypt the RADIUS protocol. Currently, only PAP authentication is supported. *Figure 5.28* shows the RADIUS Settings page of the SEL-3061. You are required to set the Primary Server, Authentication Port, and the Shared Secret Key. See *Table 5.8* for more information about the RADIUS settings.

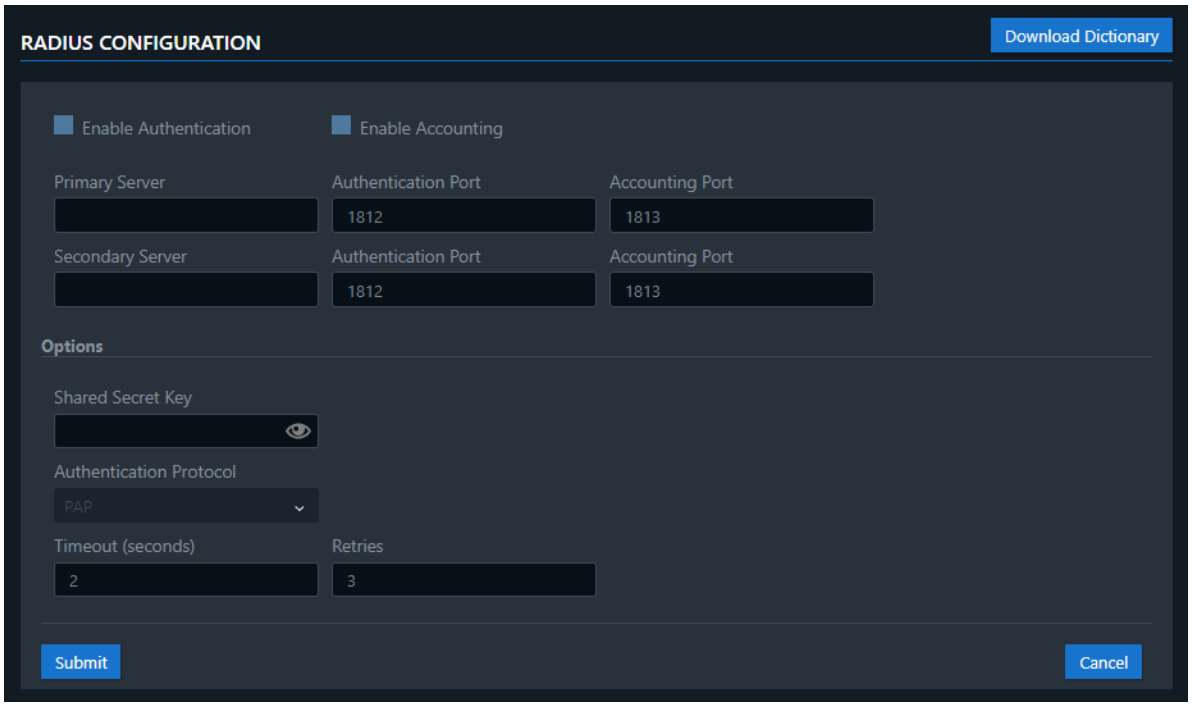


Figure 5.28 RADIUS Configuration

Table 5.8 RADIUS Settings (Sheet 1 of 2)

Setting Name	Value	Default	Description
Enable Authentication	Checked or unchecked	Unchecked	Configures the device to forward requests for authentication of users to your RADIUS server if the username is not found in the local accounts on the device.
Enable Accounting	Checked or unchecked	Unchecked	Configures the device to send information about the user's session to the RADIUS server for logging.
Primary Server	Unicast Address or domain name	[Empty]	Network address for your RADIUS server, either as a hostname (in the table of the host) or as an IP address. Choose either IP Address, or select one of the hosts listed. The server receives all RADIUS requests (unless it is offline), does not respond, or times out three times in a row.
Secondary Server	Unicast Address or domain name	[Empty]	Used when the primary server is offline. The primary server will be tried again on the next request after five minutes have elapsed since it was found to be offline.
Authentication Port	1–65563	1812	UDP port number on the RADIUS server that listens for authentication requests.
Accounting Port	1–65563	1813	UDP port number on the RADIUS server that listens for accounting information messages.
Shared Secret Key	22–128 characters	[Empty]	A string of 22–128 characters that is set on both the RADIUS server and the SEL-3061 to provide cryptographic protection for the data in authentication requests and replies from the server. Normally, you get this information from your RADIUS administrator. The RADIUS Shared Secret must be set to use RADIUS.
Authentication Protocol	PAP	PAP	Describes how authentication data are encoded in the messages between the device and your RADIUS server. Normally, this value will be given to you by your RADIUS administrator. PAP is currently the only supported protocol.

Table 5.8 RADIUS Settings (Sheet 2 of 2)

Setting Name	Value	Default	Description
Timeout	1–10 seconds	2 seconds	This value, in seconds, is set to exceed the longest time expected in which to receive a reply from the RADIUS server. The device switches to the secondary RADIUS server after the number of set retries occurs without a reply from the primary server within the timeout interval.
Retries	1–5	3	The number of retries on the primary server before switching to the secondary server.

The Download Dictionary button, which is not a setting, allows you to retrieve the RADIUS dictionary file from the device. This file defines the SEL VSAs that must be defined on your RADIUS server and that are used by your device to appropriately grant or restrict privileges for users.

To configure your SEL-3061 to use your RADIUS server, configure the shared secret and your device to the same values used by your RADIUS server. Obtain these setting values from your RADIUS administrator. Your RADIUS server needs to have SEL-specific role and privilege attributes to be able to work with the SEL-3061. That information is found in the SEL RADIUS dictionary, which defines the vendor number for SEL, as well as identifiers for user attributes that are set by using values from your Active Directory. Select the **Download Dictionary** button on the top of the web interface to send the SEL dictionary file to your browser as a text file.

File Management

The web interface manages two processes: backing up all system settings by exporting and importing settings files and performing firmware upgrades. Exporting system settings is useful for providing SEL-3061 configuration backups for disaster recovery, as well as for creating a template configuration that you can use to commission a large number of devices. For example, if all SEL-3061 routers share the same configuration, with the exception of a few device-specific settings such as an IP address, you only need to create the configuration once and then export it as a template. Once you import the configuration file into a new SEL-3061, you only need to make minor changes before the SEL-3061 is fully configured.

Export Settings

The settings export functionality is useful for creating a copy of the SEL-3061 configuration as a device backup. You can use this copy for disaster recovery purposes in the event of lost device configuration. There is a single backup file that includes all of the SEL-3061 settings, user account information, and passwords. Settings are exported in a compressed format with a .tar.gz filename extension, which can be opened by using a file compression utility, such as 7-Zip. Although the exported file is unencrypted, it does not allow offline editing. Once the file is edited offline, the device may not accept the exported settings file when importing.

Access the Import/Export settings by navigating to **Configuration > File Management > Settings** in the SEL-3061 web interface. Select **Export Setting** (see *Figure 5.29*) to export the settings into a file. A file will be automatically downloaded into your Downloads folder.

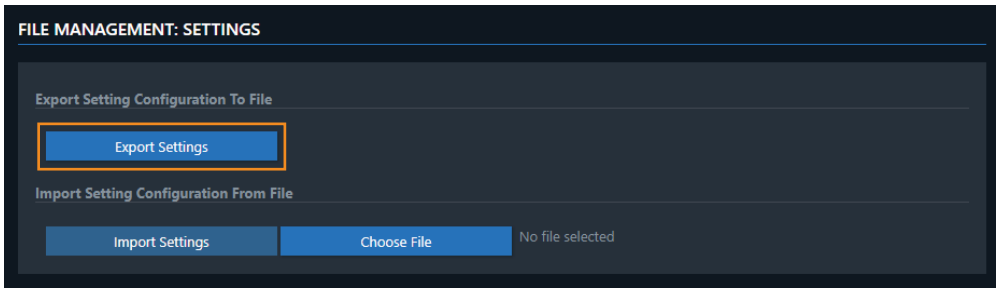


Figure 5.29 Export Settings

Import Settings

NOTE: If you replace the settings of an SEL-3061 with an imported settings file, the user accounts of the SEL-3061 are replaced with the user accounts of the imported file.

NOTE: Import a settings file for AT&T to a Verizon unit or vice-versa. The SEL-3061 will accept the import, but the SEL-3061 will not establish the PPP link with the cellular network.

Importing settings allows you to restore the SEL-3061 with a backup file and replace any existing settings. This process cannot be undone. After the settings have been imported, select **Save And Restart**.

Access the Import/Export settings by navigating to **Configuration > File Management > Settings** on the SEL-3061 web interface. Select **Choose File** (see *Figure 5.30*) to choose a file to import.

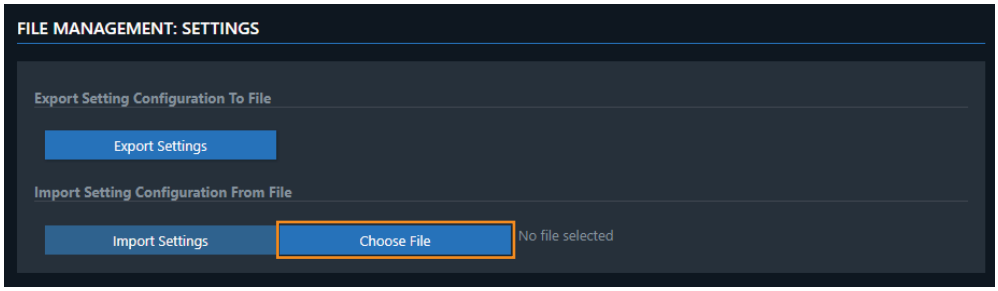


Figure 5.30 Choose a File to Import

Once a settings file is selected, select **Import Settings**. After importing the settings the SEL-3061 restarts, and the user is logged out. Importing settings updates local user accounts, so to log in, you must use an account that was imported into the SEL-3061.

Firmware Upgrades

SEL occasionally offers firmware upgrades to enhance or improve the performance of the SEL-3061. The SEL-3061 stores the firmware image in nonvolatile memory.

The SEL-3061 web interface manages firmware upgrades. The SEL-3061 firmware can be upgraded either from the Ethernet port or over a cellular connection. For instructions on upgrading firmware, see *Appendix B: Firmware Upgrade Instructions*.

X.509

HTTPS (SSL/TLS) connections must be authenticated to confirm that the user is communicating with the correct server. For the SEL-3061, an X.509 certificate provides this authentication. The SEL-3061 automatically generates the initial, self-signed certificate. Because the certificate is self-signed, a connecting client web browser may issue a security alert. This alert requires a security exception to be accepted before authentication can continue.

The initial, self-signed certificate can be replaced with an organization-generated X.509 server certificate signed by a trusted Certificate Authority (CA). Replacing the default certificate with a CA-signed certificate that the client web browser trusts removes the security alert caused by the initial self-signed certificate.

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 a client device trusts the certificate and allows communication with the server. All devices connecting to the SEL-3061 web management interface receive the public key. Only the owner of each device has the private key specific to that device. If a private key is compromised or distributed to unauthorized personnel, replace all certificates corresponding to that key.

For an overview and examples on the function of X.509 certificates, see *Appendix D: X.509*.

X.509 Certificates

Access the X.509 Certificates page shown *Figure 5.31* by navigating to **Administration > X.509 Certificate** on the SEL-3061 web interface. To import a valid certificate, you must import or upload the root CA that signed the certificate or the intermediate CA that signed the certificate. If an intermediate CA is used, the root CA of the intermediate CA must also be imported.

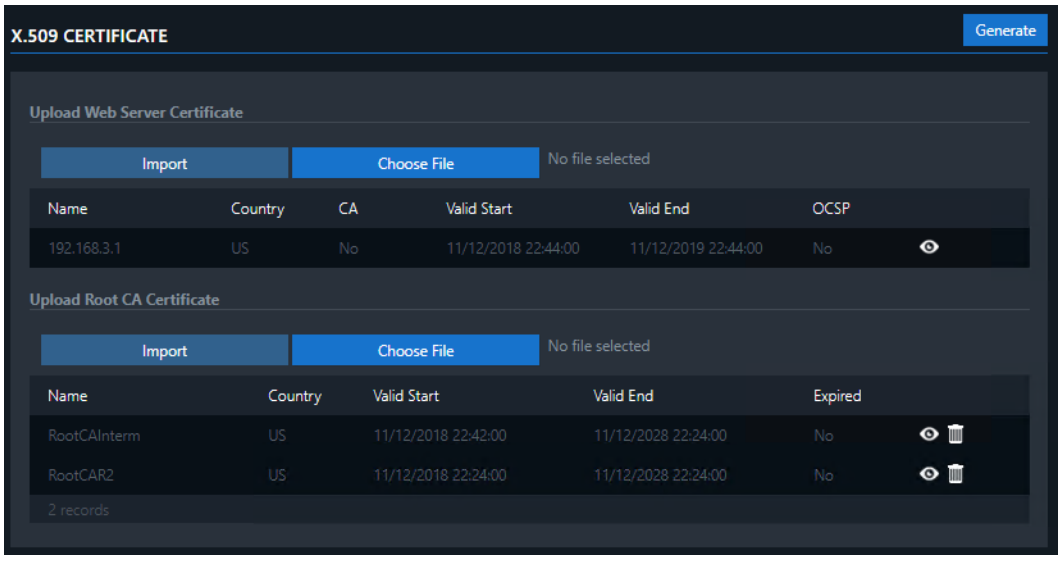


Figure 5.31 X.509 Certificate Page

The SEL-3061 supports X.509 certificates with the Base64 encoded format, shown in *Figure 5.34*. The file extension name is .pem plus a private key. The CA and intermediate CA certificates supported by the SEL-3061 also support the Base64 encoded format shown in *Figure 5.34*, but the file extension name does not have a private key.

Import a Web Server Certificate

The Import button shown in *Figure 5.32* allows you to add a new web server certificate to the SEL-3061.

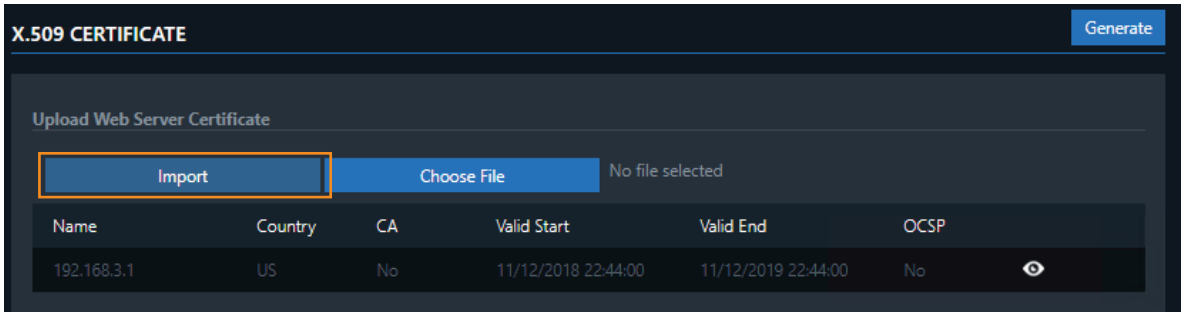


Figure 5.32 Import Certificates

Select **Choose File** and browse to the certificate you want to add, then select **Open**. Select **Import** to import the certificate. Once a new certificate is uploaded, the SEL-3061 automatically replaces the previous certificate. Select **Save And Restart** after uploading the certificate. Only one web server certificate is active at a time.

Import a CA Certificate

The Import button shown in *Figure 5.33* allows you to add a new CA or intermediate CA certificate.

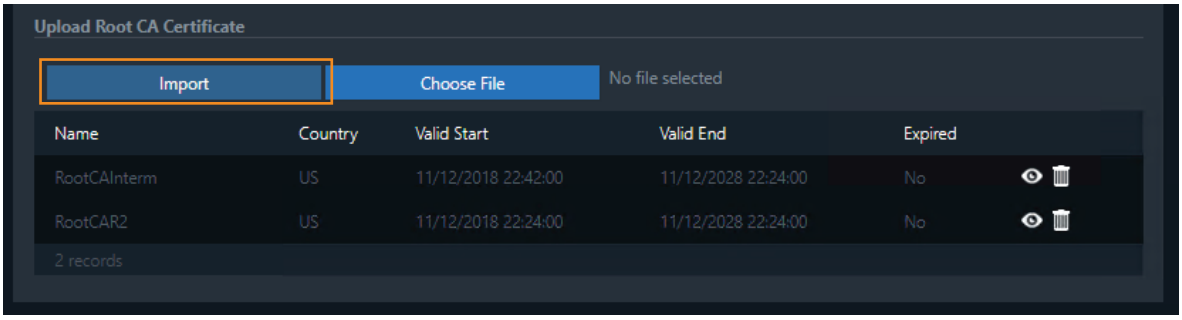


Figure 5.33 Import CA Certificate Button

Select **Choose File** and browse to the CA or intermediate CA certificate you want to add, then select **Open**. Select **Import** to import the certificate. Once a new certificate is uploaded, select **Save And Restart**. The list shows the list of CA and intermediate CA certificates that have been imported to the SEL-3061.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAsdSiAH8sN43q9GKYnHnGNFXbTKnwoFvQyROtWbqOigTEEPOM
ld8GWuc723C9KzWZ1xcXHbaPowQW6xd1/yf1wj8H2Q8pV8Zvt2nZ32n8v8FR23Qj
nxNWfaXV5i3SU1ClKEcGFnzapMEDyC3FvtrwlTpAkMIwqvDkU5THp2ClAIgdr5gF
OFmh8dHoftm47ufkfBX1qoDDIhHjJRoz73XMRLnNGeF8z9MqsPZqpkuEyIWZRmpa
cLfFytwaB9ducFl3a5ejHqFtBG74US9RIucq5sbePiCHpRSdjLjwZgPwhW1BqoFt
3KEnXSrs2Mt8kc1yMAAH8bsnZaRGeGbLO7ShOwIDAQABAoIBABpUF/Qo3/wNp/as
zlmEcgL3nzNXicfEMEJFBopdaTNyBzFXTb42ufMlfyg7JdbK5c8BnSuKBvQku9vs
qkyvtuQefuP1KbLUL2AhbN92CrS9Q4hRRqDbtRd/QQ8GQ7iQHRO8iDs2Gwz/grbV
iAx8z9fYOwzzoO77wWJaicDPPz63qTNCDyWig1/rwdwVlBjbM5FiAsB7YlwWF2hF
BaeCrc63ZzLUe6qvLx4PMlHoSE96/csPTmYecRELAVlctCDfgeg6oqQnSSmO8bOo
UeOTRDHCxEltMsB9Jm9DuYs+geAGX1JnWv2OgN9Qt4taXX5dfLNwOTisxuo1djzi
b2wOR+ECgYEA2kUhqyoZIacqYjIwdn5IUDo//p/ZVlhhuuZ59UpF8WUIXrjEjTpR
UkHjcC+BjY7rpNmJrdn8KNFYVSKcenxPwwv23pehOWgqk9UTnOPP2EVPMPcRzXt4
flYijDf7+bTcN1uBtzmfBvEbv7ZG7AHXelgHkl7ntGvs6XExR4Rp1yMCgYEAOJH6
ZK7qLHxiTMLSXEIMZndaU/OeFt7V+m7lh6/4Elka1ftH4BDoPtJ6rqlFb2iVJVAQ
apeblB+VmBYeIQ3TBGblQO5a1X8IBB21B/bgB2JOYqIe8so8WfwkwyKbDKwOFOuz
FcY+Zd5WY6r55YZOD6uEJJrffalDQ4hQBjSnDZECgYAGMdgWx4cXEWt+hfYiJste
m4idbWP5s2BysX/cmlMJ2tg1+AB8EZ+lOgF+eZqvrdK6RwJFUN57OhXLtMPEJisN
WhWTk7IgA1jSAUYhOcX4WV86AIkcz9hHnaI1YJFiMOPfHlW8IYKF6+nhswaoRBUd
f8oXOWJSGI4Mwg2n/fYTCQKBgGTK1t2HJgWfioWb9Lq+9GOkKpO9fF2DDJc8tlGP
OWvsgap9B6wBn6qUXtM/XB3NxZ3FhllssLOxW8KmlaLVom9TJmITYJQiEoaisJSL
upH28Ph7bkdYcjfuQPnIJHPIWFbv3JieOBNUkhOSSDeiYuDxuydRbMW2YZomKr4E
/eHxAoGAXOJ1VMJg8zIB7fnHPcAPOR3ANOxSaJOIO6rP1mRGbjLkGNXhu4ZL9R22
sr+5kGroW9286slJU4FDmVT9of+zPvJnHH2boVbXK19u5rjNSTOnNOmK986SrW2w
hNCz13zrXSP3OijEmiKKROA+WSAQwMOoOGBsikCpkoXa8iPAZ28=
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIEGzCCAwOgAwIBAgIBAzANBgkqhkiG9w0BAQsFADB6MQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCVOExEDAOBgNVBAcTB1B1bGxtYW4xDDAKBgNVBAoTA1NFTDEMMAoG
A1UECxMDRENTMRAwDgYDVQQDDAdUZXNOXONBMR4wHAYJKoZIhvcNAQkBFg9OZXNO
QHNlbGluYy5jb2OwHhcNMTgwOTExMTYxMDAwWhcNMTkwOTExMTYxMDAwWjCBgTEL
MAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdQdWxsbWFuMQwwCgYD
VQQKEwNTRUwxDDAKBgNVBAsTAORDUzEUMBIGA1UEAxMLMTkyLjE2OC4yLjExITAf
BgkqhkiG9wOBCQEWEnN1cHBvcnRAc2VsaW5jLmNvbTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALHUogB/LDeN6vRimJx5xjRV2Oyp8KBbOMkTrVm6tIoE
xBDzjJXfBlrnO9twvSs1mdcXFx22j6MEFusXdf8n9cI/B9kPKVfGb7dp2d9p/L/B
UdtOI58TVn2l1eYtOlNQpShHBhZ82qTBA8gtxb7a8JU6QJDCMKrw5FOUx6dgpQCI
Ha+YBdBZofHR6H7ZuO7n5HwV9aqAwyIR4yUaM+91zES5zRnhfM/TKrD2aqZLhMiF
mUZqWnC3xcrcGgfXbnBZd2uXox6hbQRu+FEvUSLnKubG3j4gh6UUnYy48GYD8IVt
QaqBbdyhJ1Oq7NjLfJHNcjAAB/G7J2WkRnhmy9OOodMCAwEAAaOBozCBoDAMBgNV
HRMBAf8EAjAAMBOGA1UdDgQWBBQzhPZvxnPwg3yfAFj++Z4aUZCMVDALBgNVHQ8E
BAMCBeAwIAYDVR0lAQH/BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMA8GA1UdEQQI
MAaHBMCoAgEwEQYJYIZIAYb4QgEBBAQDAgZAMB4GCWCGSAGG+EIBDQQRFg94Y2Eg
Y2VydGlmaWNhdGUwDQYJKoZIhvcNAQELBQADggEBAGCu5BV1ZoFJx+Ll3DBO9BOn
TwEMOuEgwsE/XCD8pdU3i+LFqEXBa6tdP5XlwrlJNeQ1xWdqumI7sKic21d532iH
7HZPNtyOqv8GLMVKc18zmKzigFJhKpjRRZVYOAyUqGIaDWJKU7vXpEU8GZBA4N9+
GliMyyUMfgR1CGuWwIuhTRQV/iTZUZc1+VDOCwZbTksIojJa4Mhg8QWtluiDGKVI
//4hl7Uuzw5YdOqbue7Q1UO2iYXa2+kvMJSO+vGE8YdTIDfcSBNpsM82z2fp6rhd
bCM5pXIgCbI+HwA8/IoL/8M8PIzVyYuafOaV8FCJc7uOB1WTV8RpOoKwR4rl+tA=
-----END CERTIFICATE-----
```

Figure 5.34 X.509 Certificate Example

Figure 5.35 shows the imported certificate in the user interface.

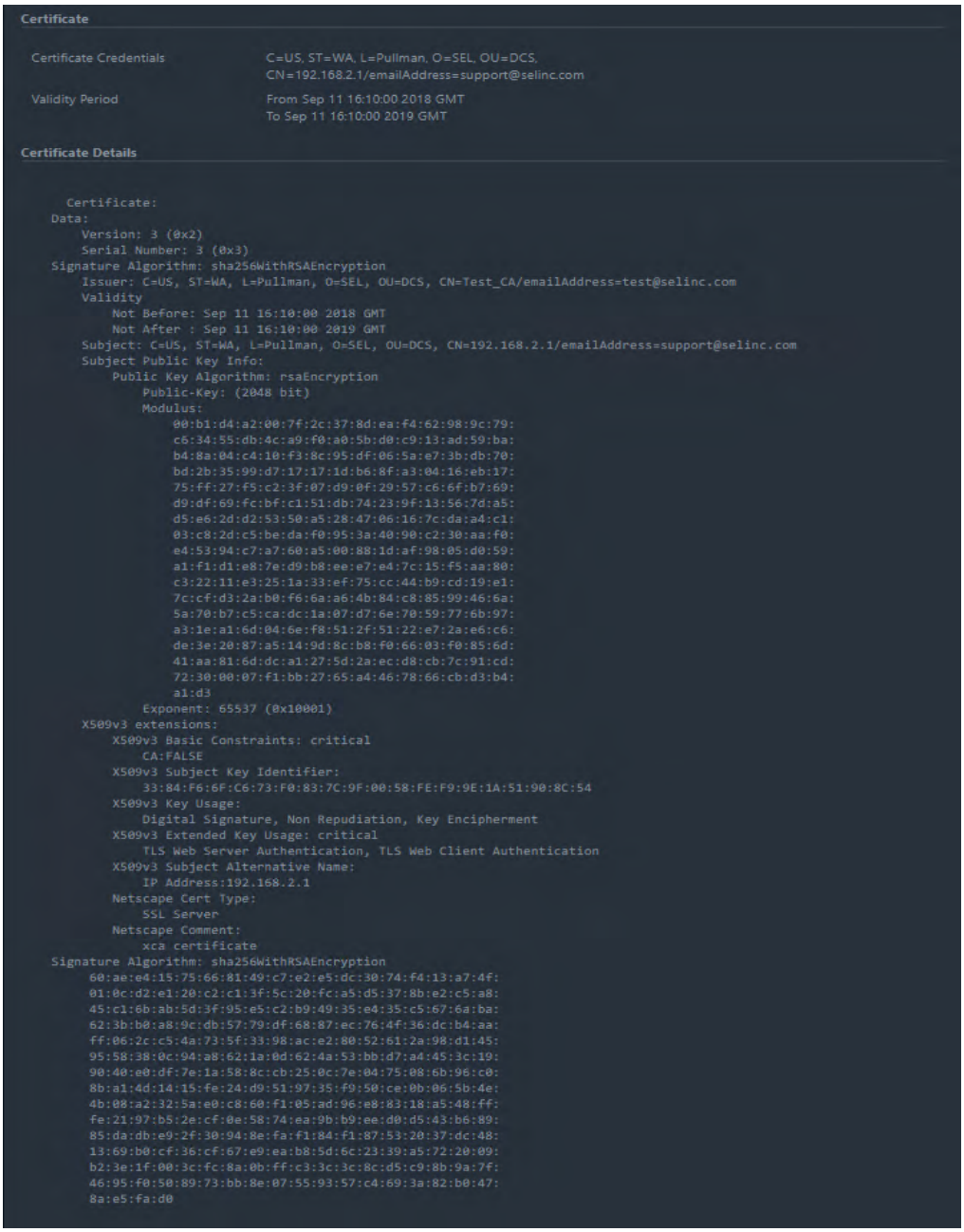


Figure 5.35 Imported Certificate in the User Interface

Generate Certificate

The SEL-3061 allows you to generate self-signed certificates. To generate a self-signed certificate, select **Generate** on the web user interface. This process requires you to enter several pieces of information to generate the certificate, as shown in *Figure 5.36*.

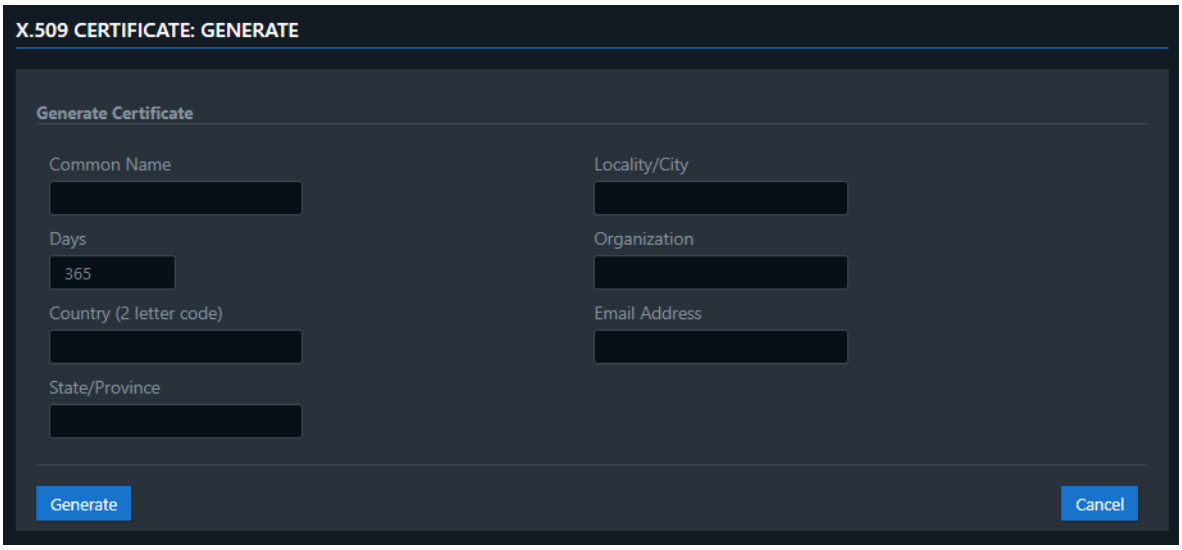


Figure 5.36 Generate X.509 Certificate

Table 5.9 X.509 Generate Certificate Fields

Setting Name	Description
Common Name	Either a hostname, such as google.com, or an IP address.
Days	Number of days that the certificate is valid.
Country	Two-letter country code.
State/Province	State or province name.
Locality/City	City name.
Organization	Organization name.
Email Address	Email address.

Device Reset

Overview

The SEL-3061 can be restarted or reset through use of the web interface or the pinhole reset button.

Web Interface Device Reset

The SEL-3061 has two web interface options for restarting or resetting the device. You can choose to perform a basic device restart or a factory-default reset. Access the Device Reset settings page shown in *Figure 5.37* by navigating to **Administration > System > Device Reset** on the SEL-3061 web interface.

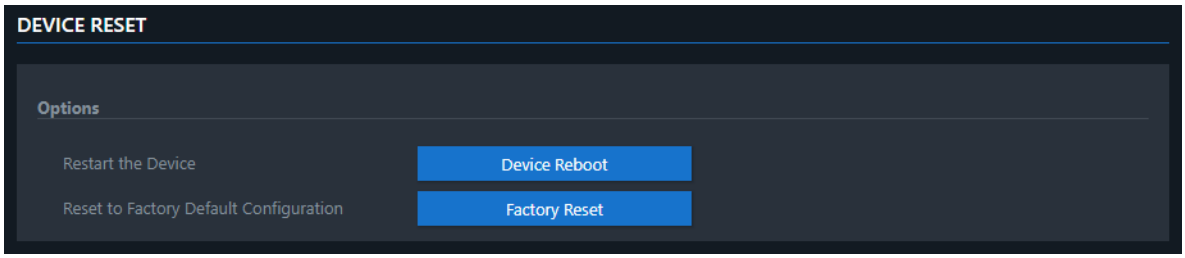


Figure 5.37 Device Reset Web Interface

Device Reboot

The Device Reboot option acts similarly to cycling power on the SEL-3061. All communication through the device will be lost while the device restarts, and it may take several minutes to reestablish communication. A restart operation does not affect the settings, communications options, or network configuration.

After selecting **Device Reboot**, the SEL-3061 web interface displays a confirmation dialog box similar to *Figure 5.38*.

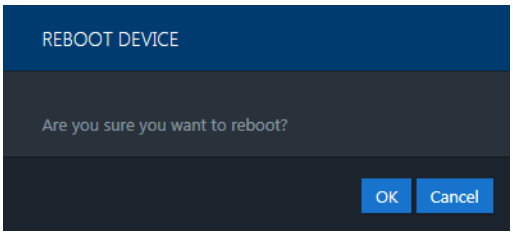


Figure 5.38 Device Reboot Confirmation Dialog

Factory Reset

Performing a factory reset decommissions the SEL-3061.

NOTE: The factory-reset function is intended for local use. Using the function via remote access is not recommended because Ethernet configurations will be reset to default values, and you may no longer be able to access the device.

A factory reset returns all settings to their default values, deletes all user accounts, ceases cellular network communications, and removes all stored Syslog messages from the device. You will not be able to revert to your previous configuration unless you back up your configuration prior to resetting the device.

After selecting **Factory Reset**, the SEL-3061 web interface displays a confirmation dialog box similar to *Figure 5.39*.

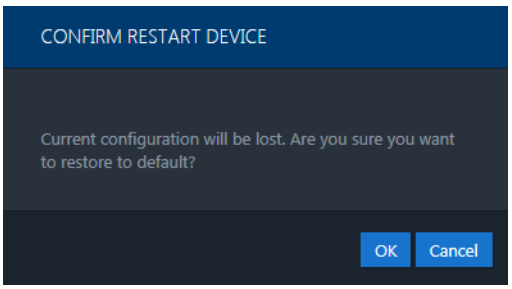


Figure 5.39 Factory-Reset Confirmation Dialog

Because all settings are reset (including communications settings and local user account credentials), the web session terminates after a factory reset.

Pinhole Reset Button

The SEL-3061 front panel includes a recessed pinhole reset button (shown in *Figure 5.40*) with the following three functions:

- To test the front-panel LEDs
- To restart the SEL-3061
- To reset the SEL-3061 settings to factory defaults

Figure 5.40 Front-Panel Reset Pinhole Location

Lamp Test

NOTE: Do not press the pinhole reset button for more than 10 seconds, otherwise the Device Reboot function may be activated.

To verify SEL-3061 front-panel LED operation, insert a tool (such as a straightened paper clip) into the pinhole (see *Figure 5.40*) and press the recessed button for less than 10 seconds. This action illuminates the front-panel LEDs. The SEL-3061 must be in the enabled state for this function to operate.

The SEL-3061 Alarm output enters the alarm state while the recessed pinhole button is pressed and resumes normal operation after the button is released.

Device Reboot

The Device Reboot option is similar to cycling power on the SEL-3061. All communication through the device will be lost while the device restarts, and it may take several minutes to reestablish communication. A restart operation does not affect the settings, communications options, or network configuration.

To initiate the device restart operation, insert a tool (such as a straightened paper clip) into the pinhole (see *Figure 5.40*) and press and hold the recessed button for at least 10 seconds but no longer than 30 seconds. While device is rebooting, a "spinner" is shown as in *Figure 5.41*.

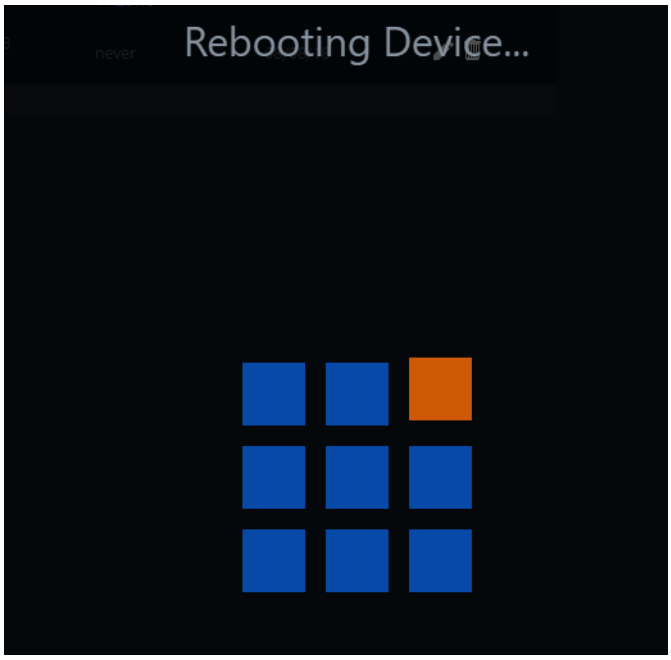


Figure 5.41 System Reboot Screen

Factory Reset

If the login credentials for all administrator and user manager accounts are lost, you must perform a factory-default reset of the SEL-3061 by using the pinhole reset option.

A factory reset returns all settings to their default values, deletes all user accounts, ceases cellular network communications, and removes all stored Syslog messages from the device. You will not be able to revert to your previous configuration unless you back up your configuration prior to resetting the device.

To initiate the factory-reset operation, insert a tool (such as a straightened paper clip) into the pinhole reset (see *Figure 5.40*) and press and hold the recessed button for at least 30 seconds, then release. The device will stop communications and commence the initialization process. This operation erases user accounts, so the SEL-3061 must be commissioned, as described in *Commissioning the Device on page 2.6*.

Settings

The SEL-3061 settings are retained after a lamp test or device restart. After a factory-default reset, all settings within the SEL-3061 are reset to their default values. All communications will be disabled. Subsequent product usage requires a local connection to the Ethernet port. See *Commissioning the Device on page 2.6*.

Front Panel

During a device reset/restart, the front-panel LEDs and Alarm contact change state as the device enters various phases of the start up. When the restart process completes, the SEL-3061 **ALARM** LED is off, the **ENABLED** LED illuminates, and the web interface becomes active.

Dashboard

During a device restart/reset, the web interface displays the progress of the restart/reset. Once the restart/reset is complete and the connection is reestablished, the web interface returns to the login screen.

In some situations, the web browser may time out. If the **ENABLED** LED illuminates for several minutes with no browser activity, select the browser refresh button to reestablish the connection.

This page intentionally left blank

SECTION 6

Serial Communications

Serial Configuration

The SEL-3061 has one DCE DB-9 serial port that is configured as EIA-232, supporting speeds from 300 to 57600 bps. The SEL-3061 serial data transfer over the cellular network is Ethernet tunneled serial where the serial traffic is encapsulated inside of Ethernet packets. The SEL-3061 serial port supports SEL protocol, Modbus, and DNP3.

Access the Serial Port settings shown in *Figure 6.1* by navigating to **Configuration > Serial** on the SEL-3061 web interface.

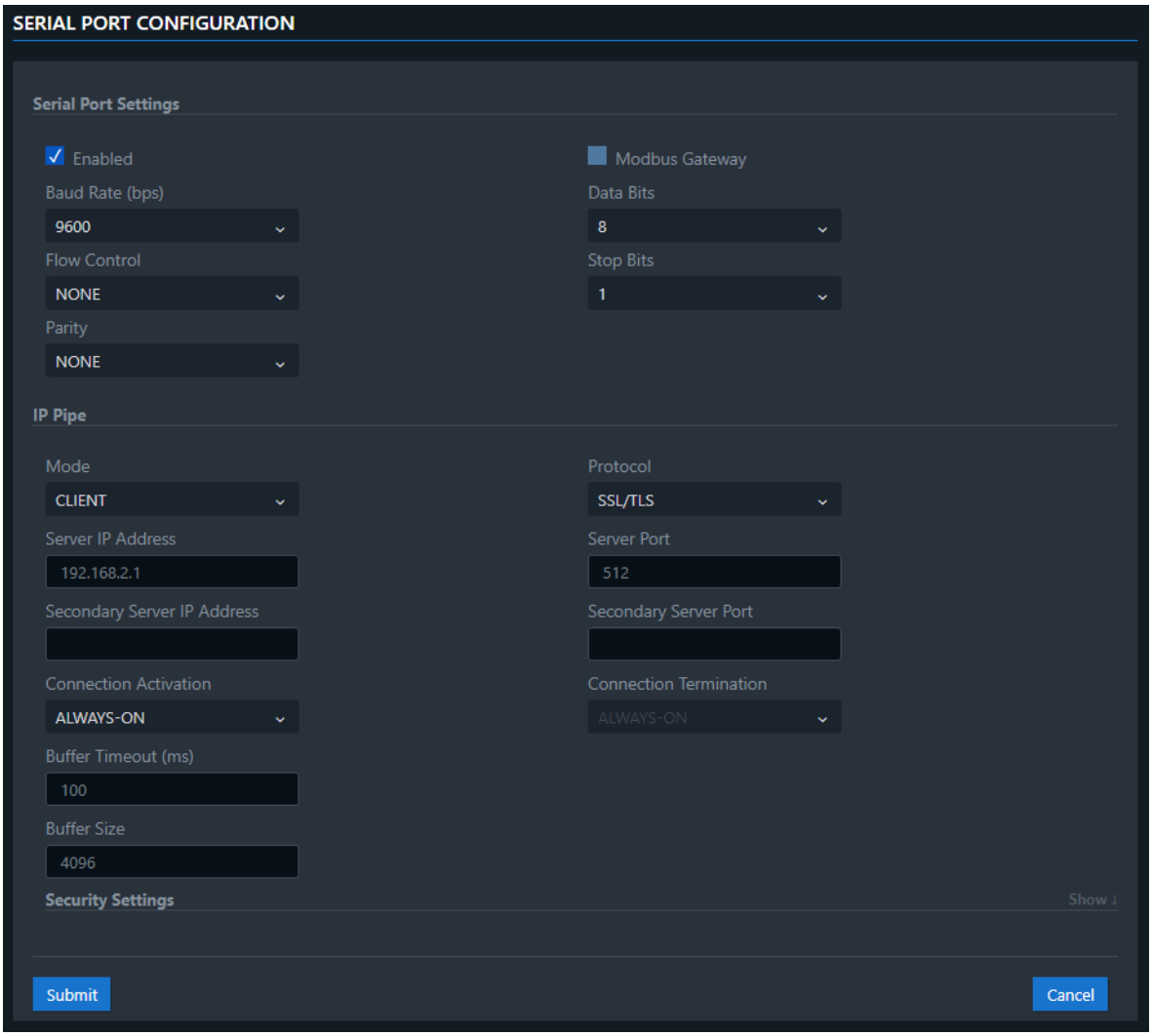


Figure 6.1 Serial Port Configuration

The SEL-3061 serial connection is disabled by default. It has three configuration sections once it is enabled. The serial port settings include Baud Rate, Data Bits, Stop Bits, Flow Control, and Parity (see *Table 6.1*). These settings must match the settings of the serial interface for the connected device. The IP Pipe setting section includes the settings of either the cellular interface or LAN Ethernet interface. The Modbus Gateway is disabled by default. When Modbus Gateway is enabled, the IP Pipe setting section changes the settings for Modbus communications.

Table 6.1 Serial Port Settings

Setting Name	Value	Default	Description
Baud Rate	300 to 57600 bps	57600 bps	Serial port speed
Data Bits	7, 8	8	Number of bits for a single-byte serial transmission
Stop Bits	1, 2	1	Number of stop bits for a single-byte serial transmission
Flow Control	NONE, RTS-CTS	NONE	Hardware flow control for serial transmission
Parity	NONE, ODD, EVEN	NONE	Type of parity check for serial transmission

An SEL-C246 serial cable connects an SEL relay or automation controller with the SEL-3061 if hardware flow control is not used in the SEL-3061. *Figure 6.2* shows the pinouts.

NOTE: It is recommended to use the SEL-C246 cable for Modbus and DNP3 communications.

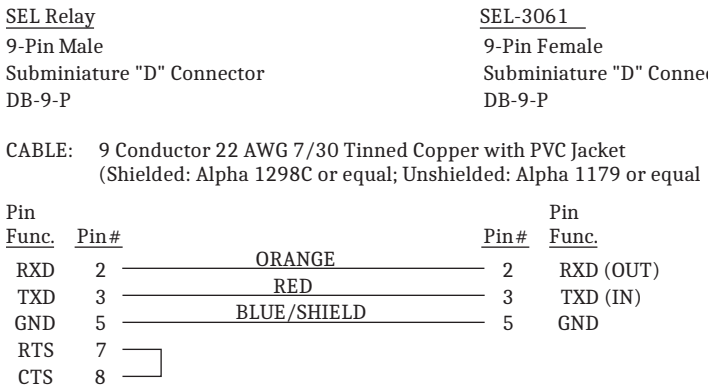


Figure 6.2 SEL-C246 Cable: SEL Relay to SEL-3061

An SEL-C285 serial cable also connects the SEL-3061 to an SEL relay or automation controller if hardware flow control is used. *Figure 6.3* shows the pinouts.

NOTE: The SEL-C285 does not work with DNP3 serial communications.

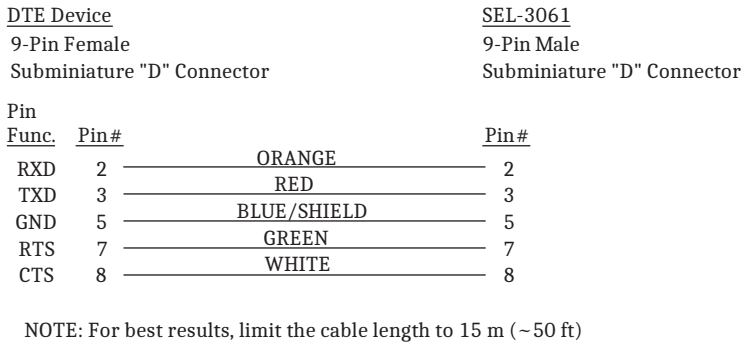


Figure 6.3 SEL-C285 Cable: SEL-3061 to DTE Device (SEL Relay)

This serial cable can be used when the SEL-3061 is configured as either a serial client or serial server.

The IP pipe of the serial port of the SEL-3061 can be configured as a client or a server. When it is configured as a client, it must have the IP address of the server. The following sections are two typical general applications.

Serial Server

NOTE: The serial router operates in Network Router mode and must have security features such as IPsec VPN and firewall turned on for security purposes.

In *Figure 6.4*, the SEL-3061 is configured as a server and uses a serial cable to connect to the field device (SEL relay). The SEL Real-Time Automation Controller (RTAC) is configured as the client and uses an Ethernet connection. The protocol in the SEL RTAC must be Ethernet tunneled serial protocol.

Figure 6.4 Serial-Server Application

Serial Client and Server (Cable Extension)

This application requires two SEL-3061 routers; the first is configured as the client and the second is configured as the server, as shown in *Figure 6.5*. The client must have the IP address of the server, and it can be either the WAN IP address or LAN IP address of the device (IPsec VPN, for example). Both the SEL RTAC and the SEL relay must be configured by using serial ports.

Figure 6.5 Serial Client and Server Application

Table 6.2 IP Pipe Settings in Server and Client Mode

Setting Name	Value	Default	Description
Mode	Client, Server	Server	The device can be configured as client or server.
Protocol	UDP, TCP, SSL/TLS	TCP	Protocol used by the SEL-3061 on the Ethernet traffic side.
Server IP Address[a]	Unicast IP address	[Empty]	IP address of the serial server.
Secondary Server IP Address[a]	Unicast IP address	[Empty]	IP address of a secondary serial server, if applicable.
Buffer Timeout	0–1000 ms	0 ms	The device sends the data out when this time out expires and the buffer is not full.
Server Port	1–65535	3000	Port to receive IP pipe traffic.
Buffer Size	1–65535	1024	When the buffer is full, the device sends the data out before the time out. Otherwise, it waits until the time out.
Connection Termination	ALWAYS-ON, On Demand[a], CR[a], TIMEOUT, SEQUENCE	ALWAYS-ON	On Demand: The IP pipe connection is established based on demand. TIMEOUT: If this option is selected, a configurable Timeout field is shown. The IP pipe connection disconnects if the timer expires with no data in the pipe. SEQUENCE: The device disconnects if it receives this sequence of characters.

[a] Client Mode only.

Serial Port Settings for Modbus Gateway Communications

NOTE: If your application does not need this translation, either Serial Server or Cable Replacement configuration can be used instead.

The Modbus Gateway feature translates Modbus/IP to Modbus RTU and vice versa. When Modbus Gateway is enabled, Flow Control and Data Bits cannot be changed from their default values. The supported protocols on the IP Pipe is either TCP or SSL/TLS.

SECTION 7

Security

IPsec VPN

IPsec is a secure network protocol that authenticates and encrypts the packets sent over a shared or public network. IPsec includes protocols for establishing mutual authentication between devices of two networks at the beginning of the session and negotiates cryptographic keys to use during the communication session. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality by using encryption, and replay protection.

The SEL-3061 uses either Internet Key Exchange (IKE) or IKEv2 protocols and the shared secret key for establishing an IPsec VPN tunnel. IKEv2 should be used for IPsec VPNs. IKEv1 is offered in order for the SEL-3061 to be compatible with third-party devices. When IKEv1 is used, the shared secret should be at least 19 characters long and should use a complex combination of alphanumerical characters and special characters. To establish an IPsec VPN tunnel, the SEL-3061 performs two phase operations.

In Phase 1, the SEL-3061 authenticates IPsec peers and sets up a secure channel between the peers to enable IKE exchanges. This phase can occur in two modes: Main mode and Aggressive mode. In the Main mode, the SEL-3061 performs three two-way exchanges between the initiator and receiver. These exchanges include the algorithms and hashes used to secure the IKE communications, Deffie-Hellman to generate session keys, and verification of their mutual identities. The Main mode should be always used when establishing IPsec VPNs.

In the Aggressive mode, the device performs fewer exchanges and exchange information is packed in fewer packets. This mode is faster than Main mode. In this phase, an encryption method, an authentication method, and a key group are part of the settings. The Aggressive mode is not secure but is offered for compatibility with third-party products.

In Phase 2, the SEL-3061 negotiates IPsec parameters to set up the IPsec tunnel for secure data transfer. In this phase, an encryption method, an authentication method, and a key group are part of the settings.

To configure the IPsec settings, navigate to **Configuration > Tunnel > IPSec Tunnels**, and enter the settings listed in *Table 7.1*. Select **Add Tunnel** on the web interface, enter the settings for the first IPsec tunnel, and select **Submit**. Repeat for as many as five total IPsec tunnels. As each tunnel is entered, the SEL-3061 includes it in a list. To edit an existing entry, select the corresponding pencil icon. Select the trash can icon to delete that tunnel.

The IKE has a Basic setting and an Advanced setting. The Basic setting uses the same set of settings for Phase 1 and Phase 2. The Advanced settings allow you to set specific settings for each phase.

Table 7.1 IPsec Settings

Setting Name	Value	Default	Description
Name	1–15 characters	[Empty]	Name used to identify IPsec tunnels. The name must start with a letter and include an alphanumeric hyphen and an underscore.
Remote WAN IP	Unicast Address or domain name	[Empty]	Remote IPsec endpoint IP address or domain name.
Remote Network Route	Unicast Address or domain name	[Empty]	Remote network.
Remote Network Mask	*www.xxx.yyy.zzz* or */nn*	[Empty]	The subnet mask or size of the remote network.
Pre-Shared Key	1–4096 characters	[Empty]	Shared secret key known to the IPsec endpoints.
Tunnel Protocol	IKE or IKEv2	[Empty]	The SEL-3061 supports both Internet Key Exchange (IKE) and IKEv2.
IKE Mode	Main or Aggressive	[Empty]	The Main mode uses three two-way exchanges between the initiator and receiver.
Encryption Method	Basic or Advanced	Basic	Basic mode uses the same encryption, authentication, and key group settings for both phases. Advanced mode allows separate settings to be entered for Phase 2.
Encryption	3DES, AES-128, AES-256	AES-128	The SEL-3061 uses 3DES, AES-128, and AES-256 for Phase 1 and Phase 2 encryption.
Authentication	SHA1, SHA2-256, SHA2-384, SHA2-512	SHA2-256	The SEL-3061 uses SHA1, SHA2-256, SHA2-384, and SHA2-512 for Phase 1 and Phase 2 authentication.
Key Group	DH2 (1024-bit), DH5 (1536-bit), DH14 (2048-bit), DH15 (3072-bit), DH16 (4096-bit), DH24 (2048-bit)	DH2 (1024-bit)	The SEL-3061 uses DH2, DH5, DH14, DH15, DH16, and DH24 for Phase 1 and Phase 2 key groups.
IKE Lifetime	1–8 hours	1	How long the user has until the IPsec tunnel needs to be reestablished.
Checking period	1–120 minutes	10	Frequency to check IKE and Key lifetime.
Key Life	0–24 hours	8	How long the user has until the keys must be renewed.
Max Retries	0–999	0	Number of retires for establishing the IPsec tunnel.
Compression	Checked or unchecked	Unchecked	Enable or disable the compression algorithm.
Enable UID	Checked or unchecked	Unchecked	Enable or disable the unique identifier string.

Note that when an IPsec VPN has been established between two SEL-3061 Routers or between an SEL-3061 and a gateway (e.g., SEL-3620, SEL-3622, or a third-party router), the SEL-3061 does not allow traffic to go through the IPsec VPN until firewall rules are put in place. The firewall rules determine what devices can send traffic through the IPsec VPN. This allows the SEL-3061 to whitelist the devices that can send traffic through the IPsec VPN.

Firewall

The SEL-3061 configurable, stateful firewall inspects all traffic that passes through, denying or permitting packets according to a set of defined rules. You can use the firewall to filter traffic according to the following:

- Transport Protocol
- IP Address
- Port Number

The device logs firewall configuration changes. A stateful firewall protects the internal network by monitoring the state of network connections, such as TCP streams, that route through the network. This operation minimizes processing necessary for packets that are part of an existing session, so the firewall functions very efficiently.

The SEL-3061 has two types of firewall rules: user-defined and system-generated. The user-defined rules have precedence over the system-generated rules. The default policy of the rules is the drop-all rule, which means the device drops any traffic that does not match any of the rules defined by users or the system.

The firewall settings have a Basic (or Normal) setting page and an Advanced setting page. In the Basic setting page, three sections are available: Port Forwarding, Input Filter, and Output Filter rules (see *Figure 7.1*). In the Advanced setting page, five sections are available: Pre-routing, Input Filter, Forward Filter, Output Filter, and Post-routing rules (see *Figure 7.2*). To add a rule, select **Add** on the appropriate settings page.

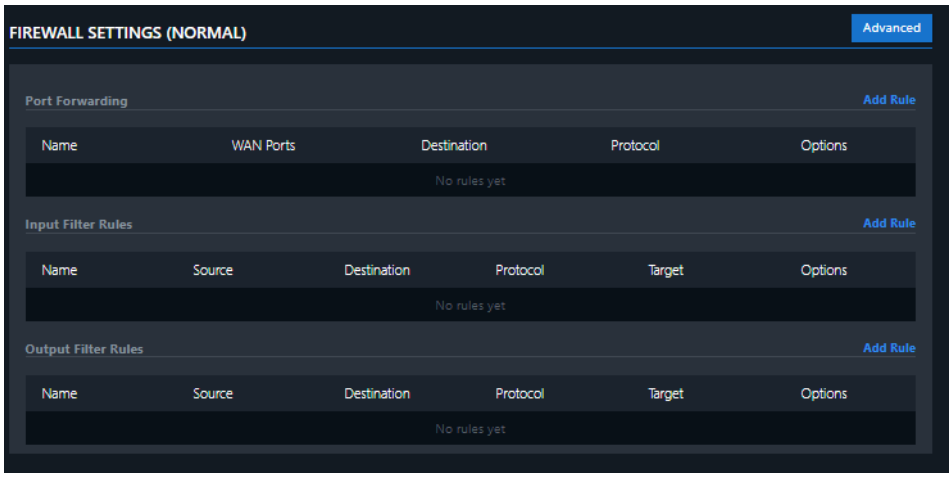


Figure 7.1 Firewall Settings (Normal)

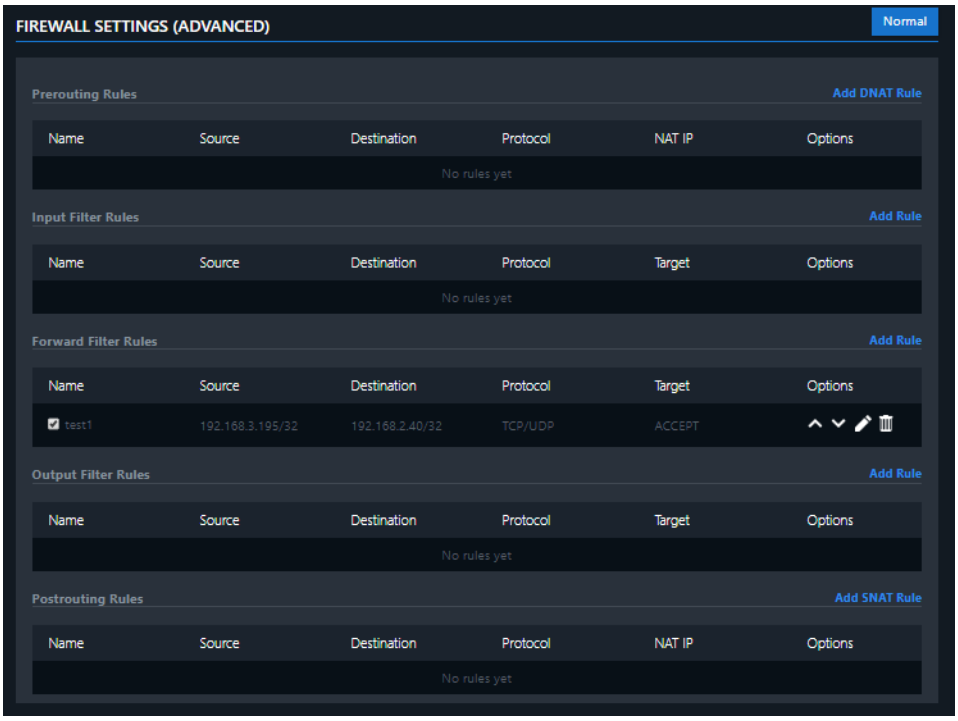


Figure 7.2 Firewall Settings (Advanced)

The Input Filter rule allows you to define rules for traffic entering the device. The Output Filter rules allow you to define rules for traffic initiated by and sent from the device. Forward Filter rules allow you to define rules that go through the device.

Port Forwarding

Port Forwarding is a form of Destination Network Address Translation (DNAT) and is similar to the NAT functions of a home cable or DSL modem that allow a source on the public internet to send data directly to a device on a private network. For Port Forwarding to occur, a user must create Port Forwarding rules, and the incoming traffic originating from the public network interface must match one or more of the rules. When a Port Forwarding rule is created, the SEL-3061 creates two rules in the Advanced settings: a Pre-routing rule and a Forward Filter rule. *Figure 7.3* shows an example of Port Forwarding.

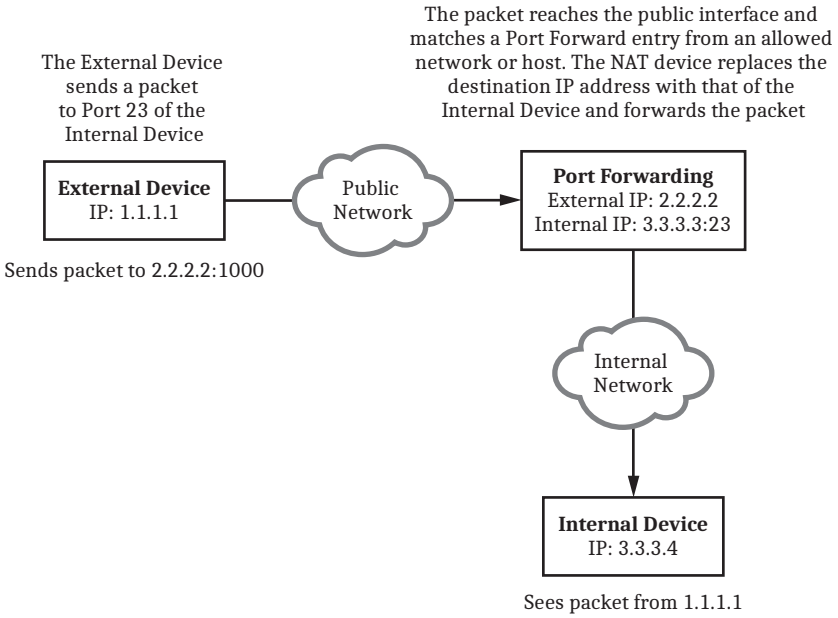


Figure 7.3 Port Forwarding Example

Table 7.2 Port Forwarding Settings

Setting Name	Value	Default	Description
Name	1–4096 characters	[Empty]	Name of the port forwarding rule. The name must start with a letter, and contain alphanumeric, space, hyphen, and underscore characters.
Description	1–200 characters	[Empty]	Description of the rule (optional).
External WAN ports	1–66536, ANY	ANY	The SEL-3061 forwards traffic received from these ports. The ports can be separated by a comma. Use a dash (-) for a range of ports.
Destination LAN IP	Unicast Address or domain names	[Empty]	The destination address of the LAN network.
Destination LAN port(s)	1–65535	[Empty]	The SEL-3061 forwards traffic to this port or ports of the LAN device.
Protocol	TCP/UDP, TCP, UDP, and ANY	TCP/UDP	The protocol that the SEL-3061 filters. ANY is for any transport layer application protocols.
External Source IP	Unicast Address or domain names	ANY	The SEL-3061 uses this field to filter specific source IP addresses.
Mask	1–32	32	This mask determines whether the source is a single device (/32) or a network (/24).
External Source Port	1–66536	ANY	Port or ports of the external device IP from where the traffic comes.
Enable NAT Loopback	Enabled or Disabled	Disabled	This feature redirects LAN packets destined for the public IP address of the WAN.

Forwarding Filter Rules

The SEL-3061 uses Forwarding Filter rules to filter packets that go through the SEL-3061. The Forwarding Filter rule has three sections in the setting page, as shown in *Figure 7.4*.

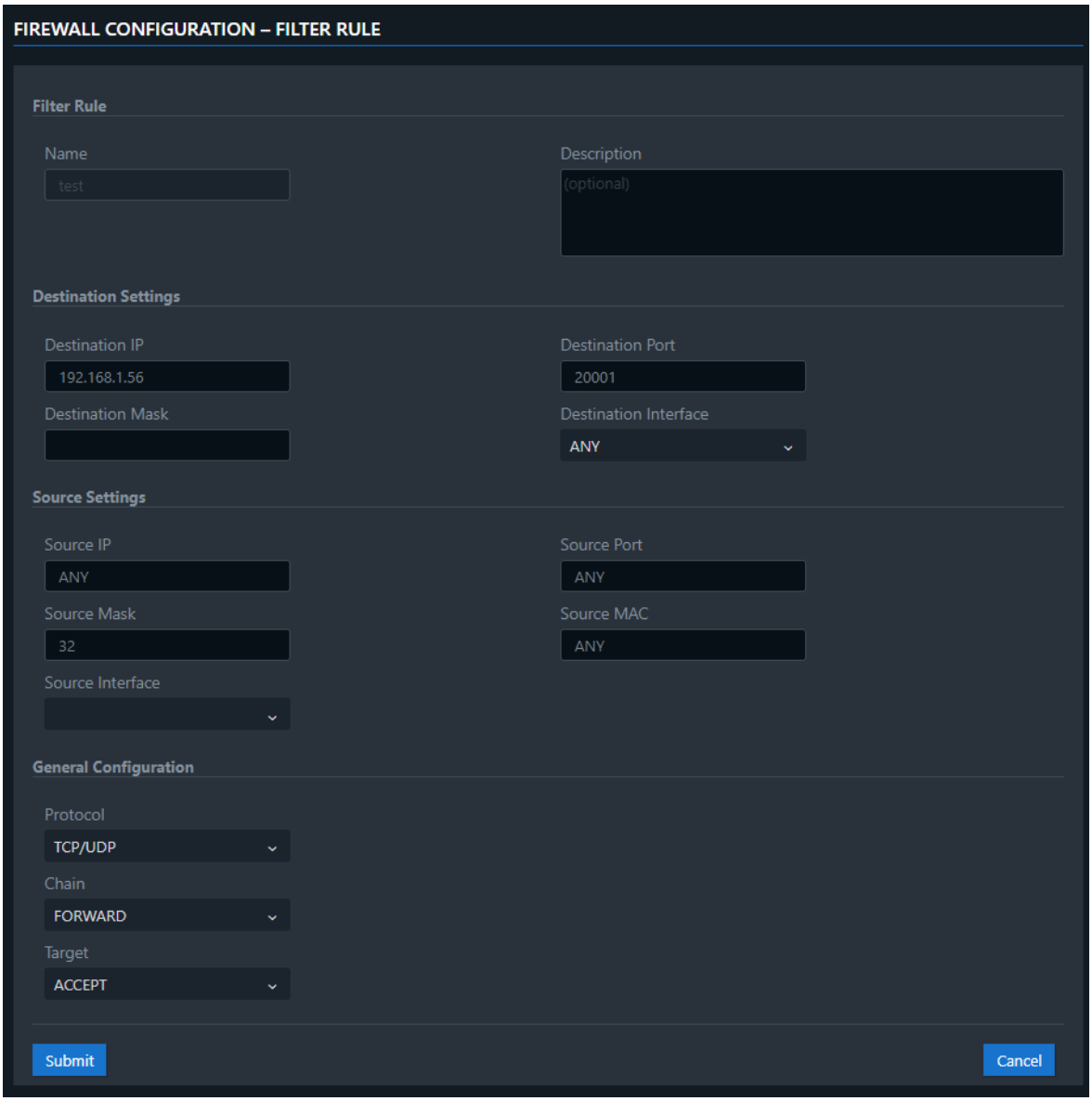


Figure 7.4 Forwarding Filter Rule Page

In the Destination settings, the SEL-3061 allows you to define the destination IP, its mask, and ports. In the Source settings, the SEL-3061 allows you to define source IP, its mask, port, and MAC. The General Configuration section allows you to define the type of protocols, the chain, and the target. The protocols include ANY, TCP, UDP, and TCP/UDP. The chain can be defined for Input, Forward, and Output. The target allows the device to either Accept, Reject, Drop, or Log specific traffic.

Table 7.3 shows the Forwarding Filter rules.

Table 7.3 Filter Rule Settings (Sheet 1 of 2)

Setting	Description
Name	Name of the filter rule.
Description	Description of the filter rule.
Destination IP	Destination IP address.

Table 7.3 Filter Rule Settings (Sheet 2 of 2)

Setting	Description
Destination Port	Destination port.
Destination Mask	Destination mask for the IP address.
Destination Interface	The interface that the traffic to destination is delivered.
Source IP	IP address of the source.
Source Port	Port of the source IP address.
Source Mask	Source mask.
Source MAC	Source MAC address.
Source Interface	Interface where the packets enter SEL-3061. The rule will only be applied to traffic that enters the SEL-3061 on the Source Interface.
Protocol	Protocols that can be TCP, UDP, TCP/UDP, or ANY.
Chain	Filter rule that applies to either INPUT, OUTPUT or FORWARD.
Target	The action to perform on traffic, it is either ACCEPT, REJECT, DROP, or LOG.

Input Filter Rules

The SEL-3061 uses Input Filter rules to filter packets that enter and are intended for the SEL-3061. See *Table 7.3* for defining Input Filter Rules. Input Filter rules can also be used to define the devices that can access the SEL-3061. For example, the SEL-3061 can whitelist a list of devices that can ping the router.

Output Filter Rules

The SEL-3061 uses Output Filter rules to filter packets that are initiated by the SEL-3061 and sent to other destinations. See *Table 7.3* for defining Output Filter Rules.

Pre-Routing Rules (DNAT)

Pre-routing rules modify the packet to change the destination address to a new destination address. Usually, this will be from the WAN address to a new address within the LAN. This packet modification happens before any firewall forwarding rules are evaluated. Pre-routing rules provide the ability to use private IP space within the LAN, while having the WAN in public space. Pre-routing rules make the LAN accessible from public addresses and routes. Pre-routing rules are automatically created as part of a port forwarding configuration.

Post-Routing Rules (SNAT)

Post-routing rules modify the packet to change the source address to a new source address. Usually, this will be from an address within the LAN to the WAN address. This packet modification happens after any firewall forwarding rules are evaluated. Post-routing provides the ability for devices within private IP space to have bi-directional communications with devices in public IP space. In most situations, SNAT rules do not need to be manually created because the SEL-3061 dynamically creates the SNAT rules needed to communicate with public IP space from the LAN.

This page intentionally left blank

SECTION 8

Diagnostics and Logging

Statistics

The SEL-3061 maintains communications statistics. To assemble the statistics, navigate to **Diagnostics > Statistics**.

The statistics include statistics of Ethernet (LAN), cellular and serial interfaces, and VPN tunnels, such as GRE and IPsec. By default, the Statistics page shows daily usage of the LAN and cellular interfaces. The statistics for LAN include packets, bytes, errors, dropped, overruns, and others, as shown in *Figure 8.1*. To see the daily usages of a specified period, change the Start Date and End Date.

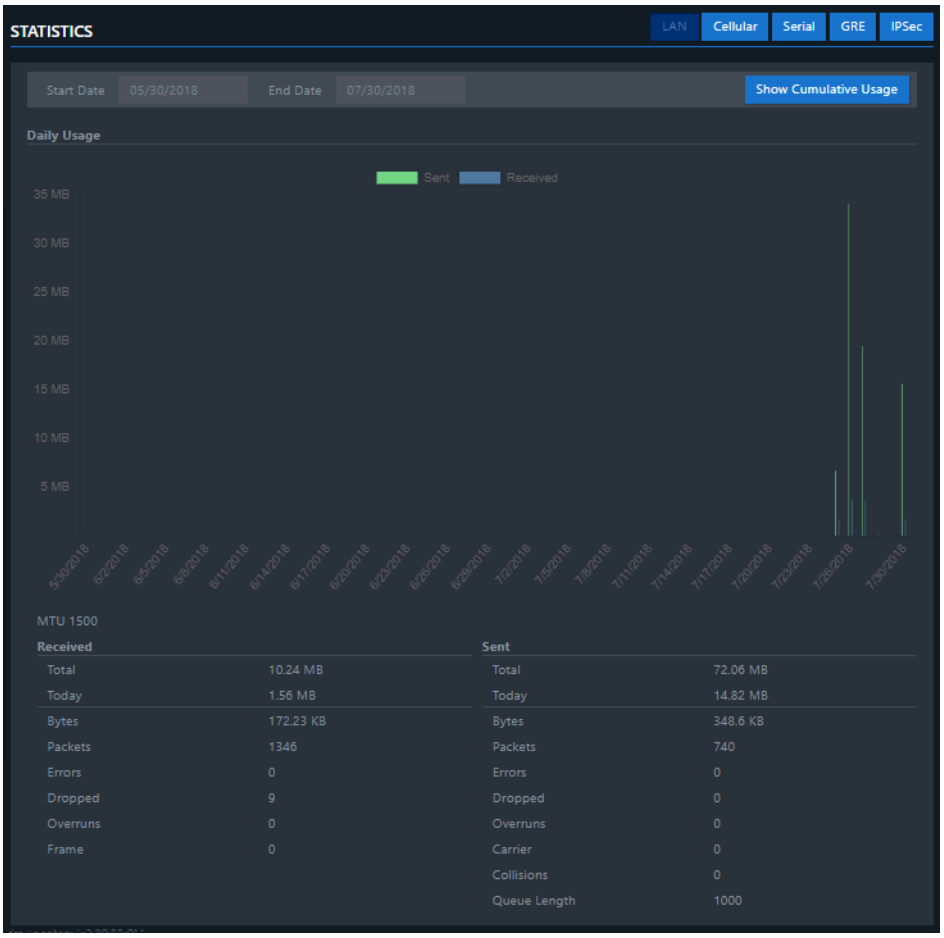


Figure 8.1 Daily Usage Page—LAN

Select **Cellular** on the top of the interface to show the cellular communications statistics.

Select **Show Cumulative Usage** to see the cumulative usage of the period. See *Figure 8.2* for a LAN example (the cellular report is similar). You can change the Start Date and End Date to adjust the cumulative usage period.

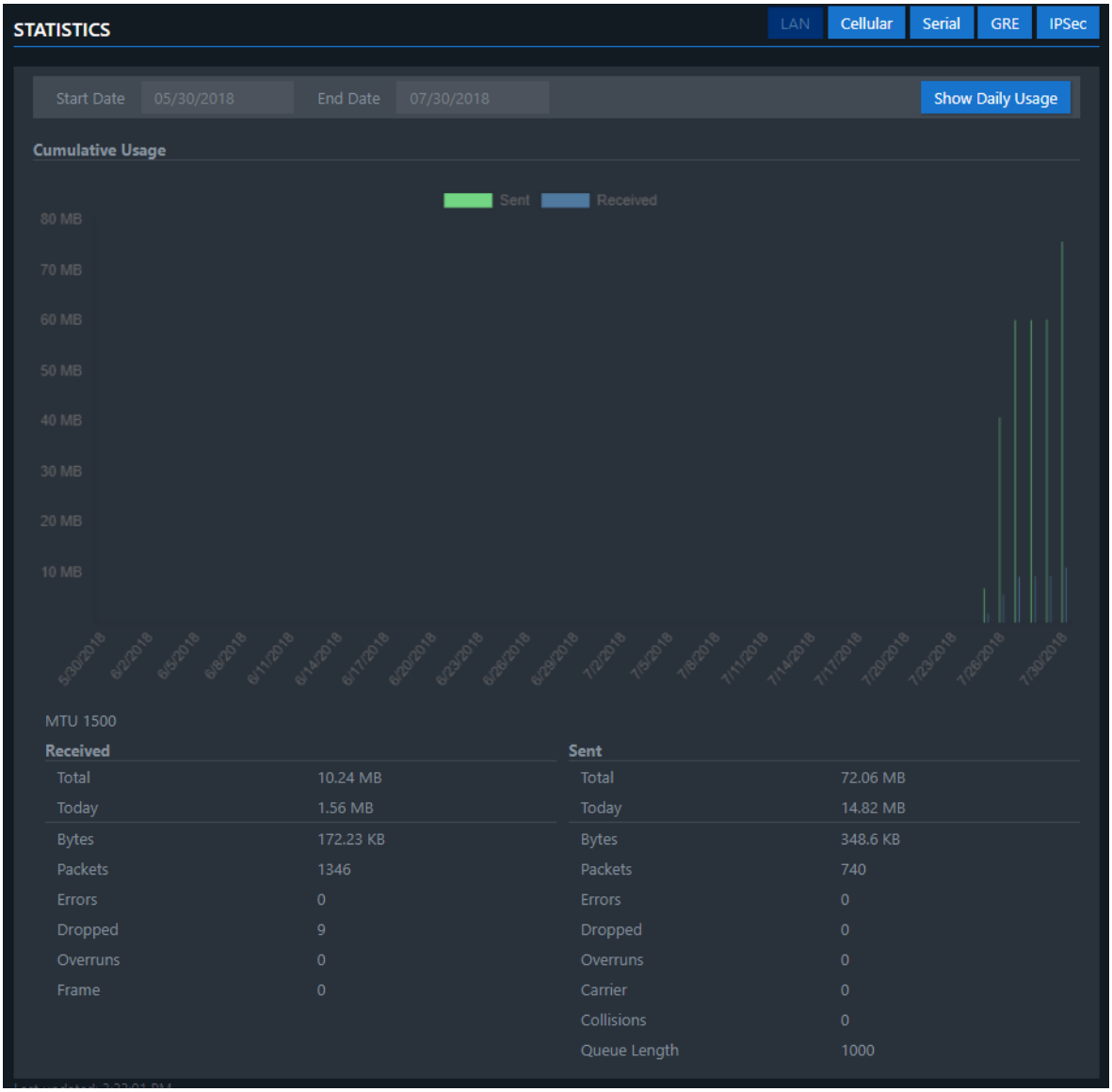


Figure 8.2 Cumulative Usage–LAN

Select the **Serial** tab to see statistics of serial port communications (see *Figure 8.3*). The statistics include bytes sent and received from the serial port in bytes and the status of Data Carrier Detect (DCD).

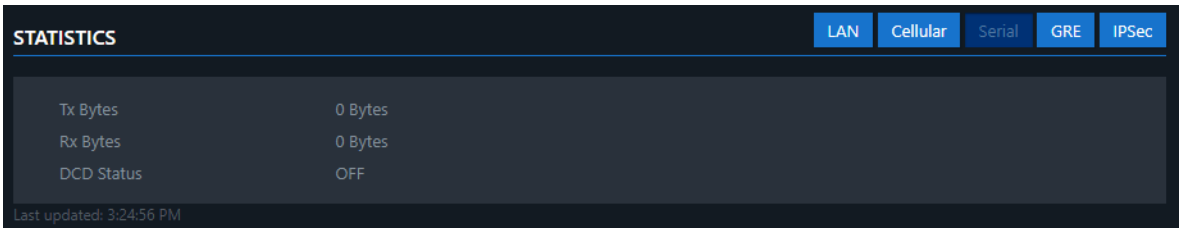


Figure 8.3 Serial Interface Statistics

To visualize tunnel statistics, select either **GRE** or **IPSec**. The page shows the GRE and IPsec traffic statistics once the tunnels are up and active, as shown in *Figure 8.4* and *Figure 8.5*.

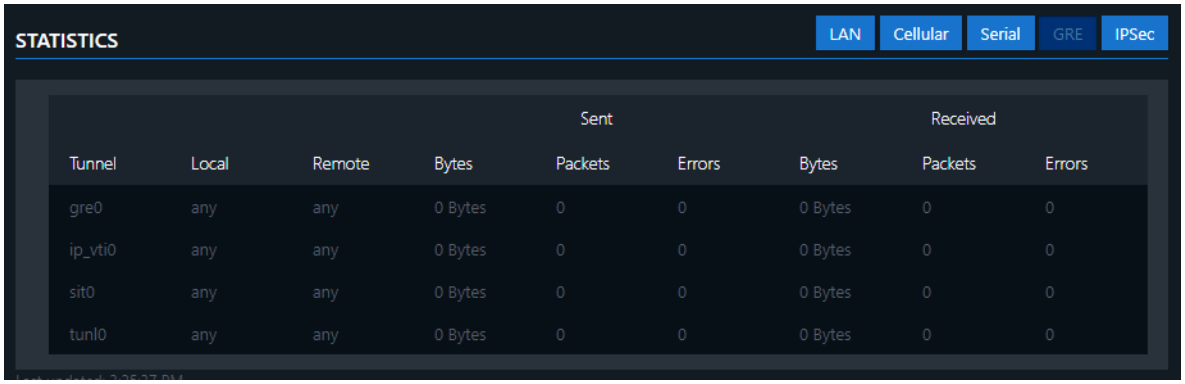


Figure 8.4 Tunnel Statistics–GRE

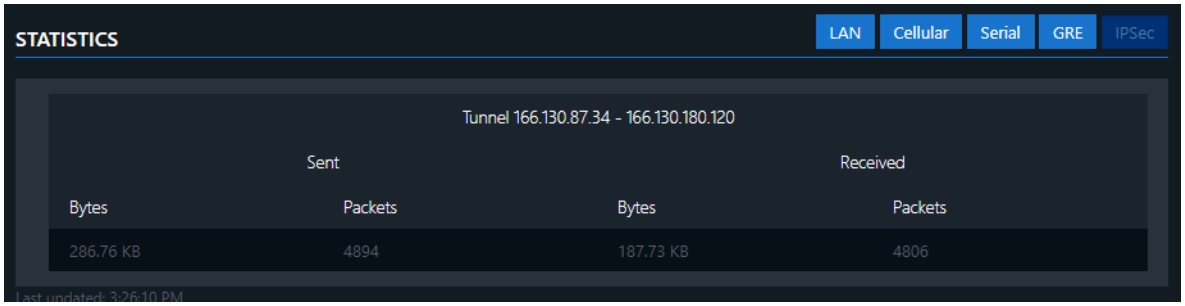


Figure 8.5 Tunnel Statistics–IPsec

Syslog

The SEL-3061 Syslog reporting is part of the event reporting system that provides notifications through two mechanisms: a local Syslog report and formatted network message traffic.

Syslog Severity

The Syslog Protocol includes a Severity field with predefined values representing increasing or decreasing levels of event severity. The following are the values used by the SEL-3061 (in order of priority from highest to lowest):

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

The Syslog settings allow 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 (i.e., the SEL-3061 will

only log events or send messages with the selected priority or higher). This filtering occurs 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-3061 logs or sends to 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 remote Syslog destination through use of the remote Syslog settings.

Local Syslog Reporting

The SEL-3061 uses a format that contains the same information that Syslog messages provide as a local reporting method. Access the local Syslog report shown in *Figure 8.6* by navigating to **Diagnostics > Local Syslog Events** on the SEL-3061 web interface.

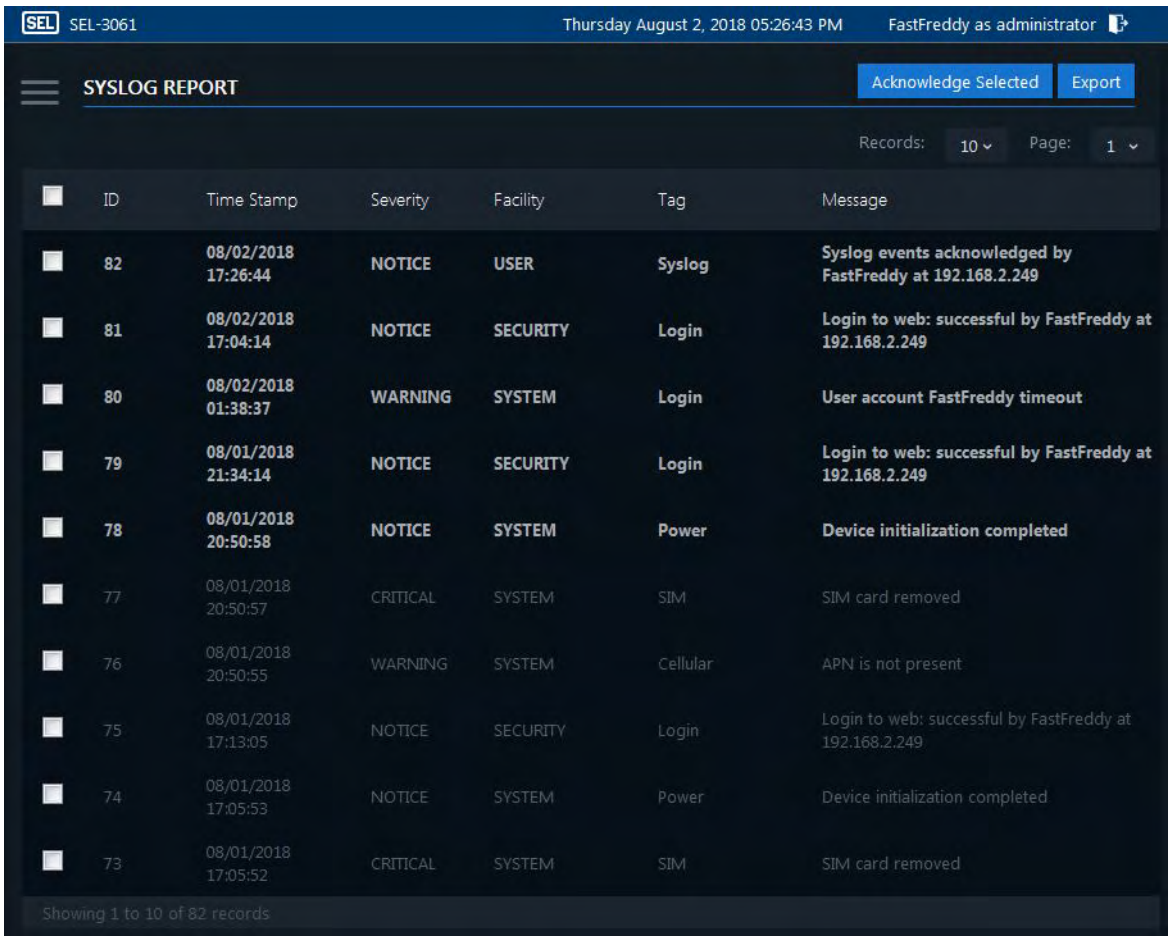


Figure 8.6 Local Syslog Events

The SEL-3061 stores information from every event locally. The report maintains as many as 30,000 events. When the maximum is reached, each new event overwrites the oldest event record. The report contains seven fields: six fields provide information from the event (ID, Timestamp, Severity, Facility, Tag, and Message), and the seventh field (Acknowledged) allows you to acknowledge that event. Newest records are displayed first by default.

Local Syslog Report Fields

- **ID** represents an index in sequential order for when that event occurred. This number will continue to increment for each event until an SEL-3061 factory-default reset (see *Device Reset on page 5.31* for details).
- **Timestamp** represents the time the event occurred on the device, using the present device time.
- **Severity** represents the level of concern the event represents. The severity levels are representative of the values in the Syslog Protocol (RFC 3164). You cannot adjust the severity levels for the events.
- **Facility** is a classification from the Syslog Protocol and provides a method of classifying the subsystem that triggered the event.
- **Tag** represents the name of the process that generated the event. For example, if the event was generated by an SEL-3061 or from the integrated radio module, that will be indicated in the Tag field.
- **Message** details the action that generated the event. Events that were generated by an SEL-3061 include the Device Address in the Message field.

Appendix C: Syslog provides a full list of local Syslog report messages.

Acknowledge Events

After reviewing event records, acknowledge them to aid in tracking new event records. Acknowledging an entry does not remove the event, but marks the event as being acknowledged. It is not possible to reverse the acknowledgment of an event.

There are two methods for acknowledging records. The first method is to select the **Acknowledge Selected** button for each desired record. A notification appears, indicating that the event has been successfully acknowledged. With this method, you can select multiple records and acknowledge them together.

The other method is to select the check box to the left of ID to select all events, then select **Acknowledge Selected** to acknowledge all unacknowledged records on all pages. Acknowledging all records generates a new event record, indicating that all events have been acknowledged. Acknowledging records generates a new Syslog event record, indicating acknowledgment of one or more events.

Exporting Events

Exporting the local Syslog report allows you to download all locally stored event records on the device to a CSV formatted file. Select **Export** to download the Event.csv file. If there is a large number of event records, the download time may be significant. If you open the CSV file directly from Microsoft Excel, the Message column may not display properly because of the automatic default formatting set by Microsoft Excel. To properly view and import the Syslog CSV file by using Excel, use the following steps:

Step 1. Open a blank worksheet in Excel.

Step 2. In the Get External Data group under the Data tab, select **From Text**.

Step 3. Navigate to the Syslog CSV file and 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**.

d. Select **Next**.

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 select **Finish**.

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

Your 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 drop-down list at the top of the page allows you to choose how many records to display on each page (10, 25, 50, and 100).

Local Syslog Settings

Set up local Syslog settings by navigating to **Administration > Syslog** on the SEL-3061 web interface, as shown in *Figure 8.7*. You can set or change the minimum local logging threshold from this page. To set or change the minimum threshold, select the **Minimum Local Logging Threshold** drop-down list and choose one of the following options: Critical, Error, Warning, Notice, and Informational. Select **Submit**, and then select **Save And Restart**.

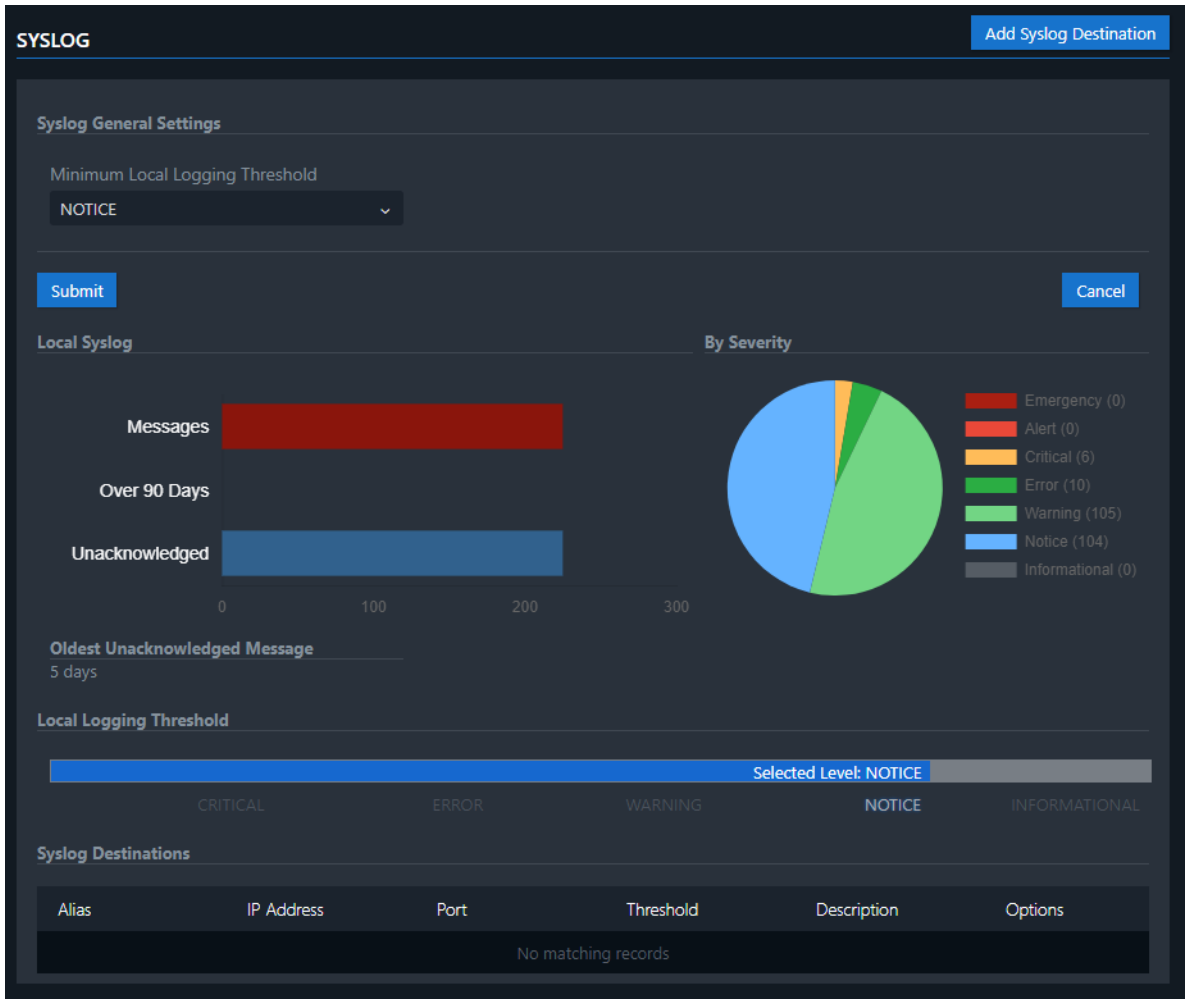


Figure 8.7 Local Syslog Events Statistics

The selected minimum logging threshold is displayed and the graphics show the number of messages, unacknowledged events over 90 days, and the partition of the events based on the severity. Note that Emergency and Alert messages are not available for user selection.

Remote Syslog Reporting

The SEL-3061 formats and transmits event messages according to the Syslog Protocol defined in RFC 3164. The SEL-3061 can transmit the event messages to multiple different remote Syslog destinations.

Remote Syslog Settings

Set up remote Syslog destinations by navigating to **Administration > Syslog** on the SEL-3061 web interface, as shown in the lower portion of *Figure 8.7*. You can edit or delete any existing remote Syslog destinations from this page.

To create a new remote Syslog destination, select **Add Syslog Destination** to present the dialog box shown in *Figure 8.8*. Set the destination by configuring the Alias, IP address, Port, and Minimum Remote Logging Threshold settings, as shown in *Table 8.1*, and select **Save** to apply your changes.

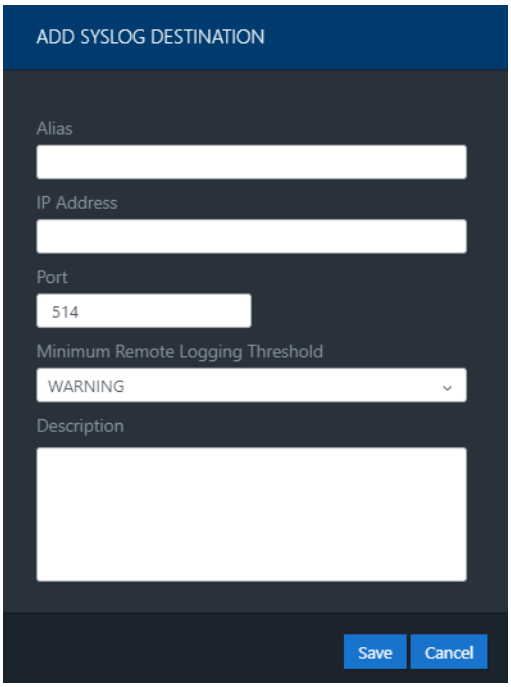


Figure 8.8 Add Syslog Destination

Table 8.1 Syslog Destination Settings

Setting Name	Values	Default	Description
Alias	1–32 characters	[Empty]	A name that is associated with the Syslog destination
IP Address	Unicast IP address	[Empty]	IP address of the Syslog destination
Port	1–65535	514	Port number for the Syslog destination
Minimum Remote Logging Threshold	Emergency Alert Critical Error Warning Notice Informational	Warning	Minimum severity level that an event must have before the SEL-3061 will forward it to the destination
Description	0–1024 characters	[Empty]	Description of the Syslog destination

SMS and SMTP

The SEL-3061 provides two methods to transmit notifications and alarms:

- Short message service (SMS) is a text messaging service, enabling the SEL-3061 to send short text messages to cellphones and receive and process a limited set of command messages.
- SMTP is a protocol that allows the SEL-3061 to communicate with a mail server so that the SEL-3061 can send emails to users.

See *Notifications and Alarms on page 8.13* for the configuration procedure for the different event classes.

SMS

SMS services allow the SEL-3061 to send short text messages (160 characters or less) to cellphones and to receive SMS messages. SMS is disabled by default. Once SMS is configured and enabled, the SEL-3061 sends messages to one or more cellphone numbers when select notification or alarm events occur.

The SEL-3061 allows a selection of messages from an Event Group to be sent to a particular SMS destination, as explained in *Notifications and Alarms on page 8.13*.

The SEL-3061 may also be configured to accept a selection of SMS commands from authorized (whitelisted) numbers. These commands either initiate actions in the router (such as restarting) or request SMS messages containing status information (such as radio statistics).

The SEL-3061 also allows manually entered text messages to be sent out, which can be useful for testing.

The router can be configured to resend failed SMS messages and to automatically log as many as 1000 sent and 1000 received SMS messages. The resend and logging settings are listed in *Table 8.2*. The log content can be manually deleted via the web interface.

Access SMS settings shown in *Figure 8.9* by navigating to **Configuration > SMS** on the SEL-3061 web interface.

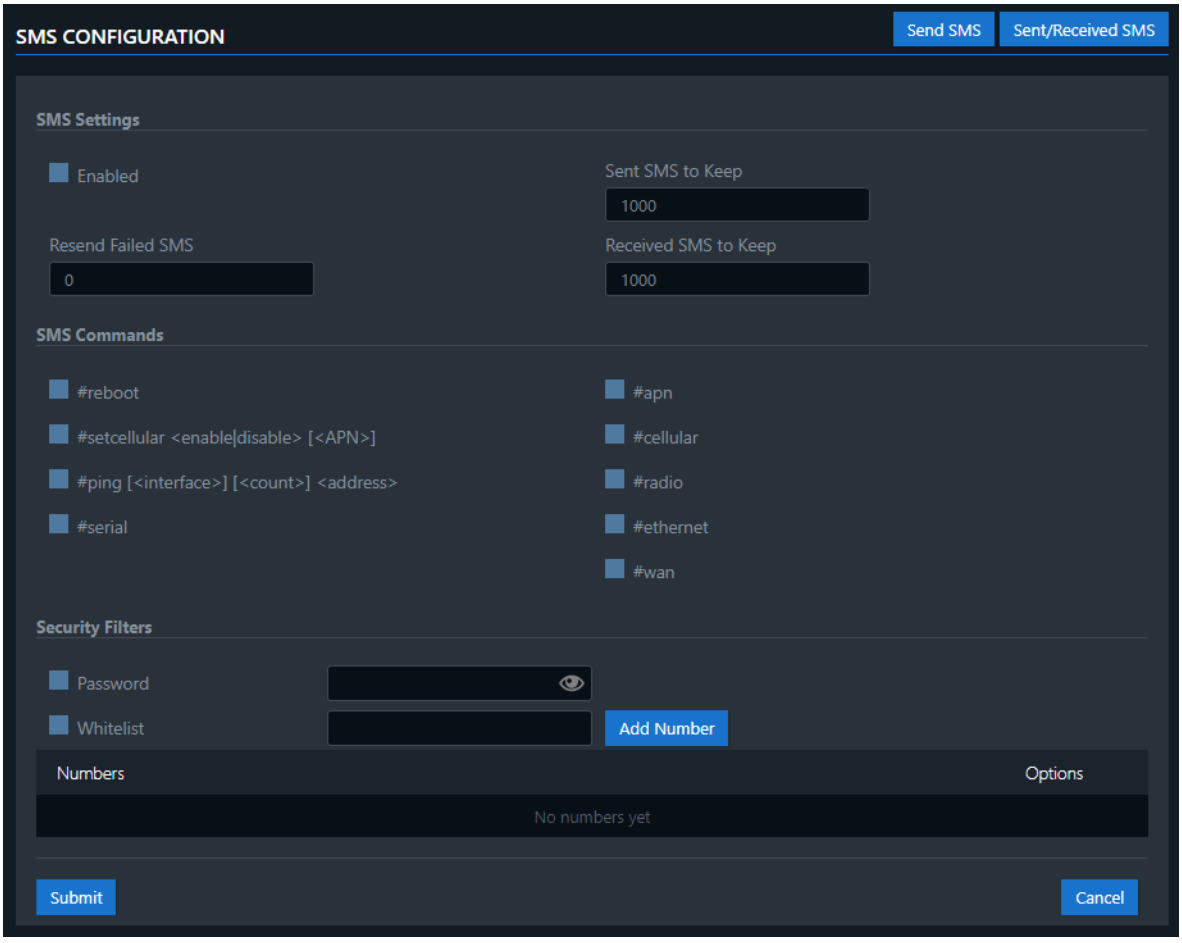


Figure 8.9 SMS Configuration

Table 8.2 SMS Settings

Setting Name	Value	Default	Description
Resend Failed SMS	0–10	10	The SEL-3061 resends failed SMS messages.
Sent SMS to Keep	0–1000	1000	The SEL-3061 can keep as many as 1000 sent SMS messages. If the value is 0, then no SMS messages will be kept.
Received SMS to Keep	0–1000	1000	The SEL-3061 can keep as many as 1000 received SMS messages. If the value is 0 then no SMS messages will be kept.

Send SMS

Select the **Send SMS** button at the top of the SEL-3061 SMS Configuration page.

Enter a valid cellphone number in the Recipient field and select **Add**. Note that the same SMS message is sent to each recipient. Enter the message in the Message area. As you type the message, the character counter below the message window updates to indicate the message length and how many characters remain before the limit of 160 is reached. The Enter key may be used to start a new line, but it counts for one character in the message. Once the count reaches 160 characters, the message window stops accepting characters. Once you finish typing the message, select **Send** to send the SMS message.

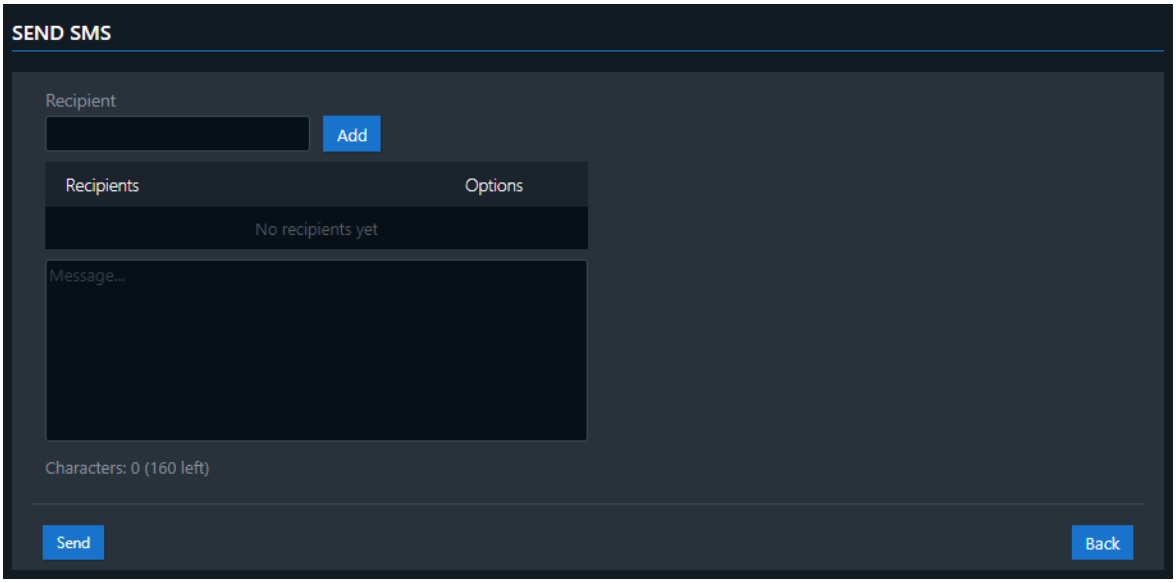


Figure 8.10 Send SMS

View Sent and Received SMS Messages

To view the logs of sent and received SMS messages, select the **Sent/Received SMS** button on the top right corner of the SMS Configuration screen. The Sent SMS log displays a history of sent messages, including the status, send time, recipient, and message text for each entry.

Similarly, the Received SMS log displays a history of received messages, including the receipt time, sender, and message text for each entry. Select **Delete All** on the top of right corner of the web interface to delete both sent and received SMS message logs. To make them easier to read, the displayed logs are not updated

while being viewed, but the data logging subsystem still operates. Select the **Auto Refresh** box on the top of the web interface to allow new entries to appear in the reports whenever new SMS activity occurs.

Figure 8.11 Sent/Received SMS

SMS Commands

Table 8.3 shows a list of supported SMS commands. By default, all commands are disabled. Each command can be independently enabled.

Optional SMS password protection provides one layer of security. A whitelist feature provides additional security by only allowing the SEL-3061 to accept SMS commands from listed senders.

Table 8.3 SMS Commands (Sheet 1 of 2)

SMS command	Description	Examples on your cellphone[a]
#reboot	Reboots the device.	#reboot p 1tomato2 #reboot
#setcellular<enable | disable> [<APN>]	Allows you to enable or disable the cellular interface. Once it is disabled, you can no longer access to the device via cellular interface. This command also allows you to set or change the APN. Note that SMS services are independent of cellular data traffic. Although the cellular interface is disabled, the SMS can be active if it is enabled.	#setcellular disable p 1tomato2 #setcellular enable p 1tomato2 #setcellular enable i2gold
#ping [<interface>][<count>]<address>	Allows the device to ping an IP address. The interface is either cellular or Ethernet (LAN). If the interface is not specified, the default gateway interface is used. The count is 4 by default and its range is from 1 to 20.	#ping cellular 8 168.12.1.2 p 1tomato2 #ping cellular 8 168.12.1.2
#serial	Obtains the details of the serial port configuration.	#serial p 1tomato2 #serial
#apn	Returns the APN string of the device.	#apn p 1tomato2 #apn
#cellular	Returns the PPP link status.	#cellular p 1tomato2 #cellular

Table 8.3 SMS Commands (Sheet 2 of 2)

SMS command	Description	Examples on your cellphone[a]
#radio	Provides the cellular link status.	#radio p 1tomato2 #radio
#ethernet	Returns the Ethernet port configuration details.	#ethernet p 1tomato2 #ethernet
#wan	Returns the WAN configuration details.	#wan p 1tomato2 #wan

[a] SMS command examples are shown for regular (nonsecured) systems and for systems with the password security filter enabled with password = 1tomato2.

To add a cellphone number to the whitelist, enable the whitelist, enter the cellphone number, and select **Add Number**. If SMS is enabled, the SEL-3061 can only receive SMS commands from a number in the whitelist. The SEL-3061 rejects command attempts from numbers not in the whitelist.

To add a password for authenticating the received command, enable and then enter the password. The sender must include **p *password*** before the command in the syntax. For example, **p 12345 #serial** (where 12345 is the password and #serial is the SMS command).

All commands sent and replied to or received by your cellphone can be viewed from the Sent/Received SMS list.

SMTP

Once it is enabled and configured, the SEL-3061 SMTP subsystem sends notifications or alarms via email. The SMTP service is disabled by default.

The SEL-3061 allows a selection of messages from an Event Group to be sent to a particular email destination, as explained in *Notifications and Alarms on page 8.13*. Access SMTP settings shown in *Figure 8.12* by navigating to **Configuration > SMTP** on the SEL-3061 web interface. Enter the settings for your email server, including the account credentials, and select **Enabled**. The settings list is shown in *Table 8.4*.

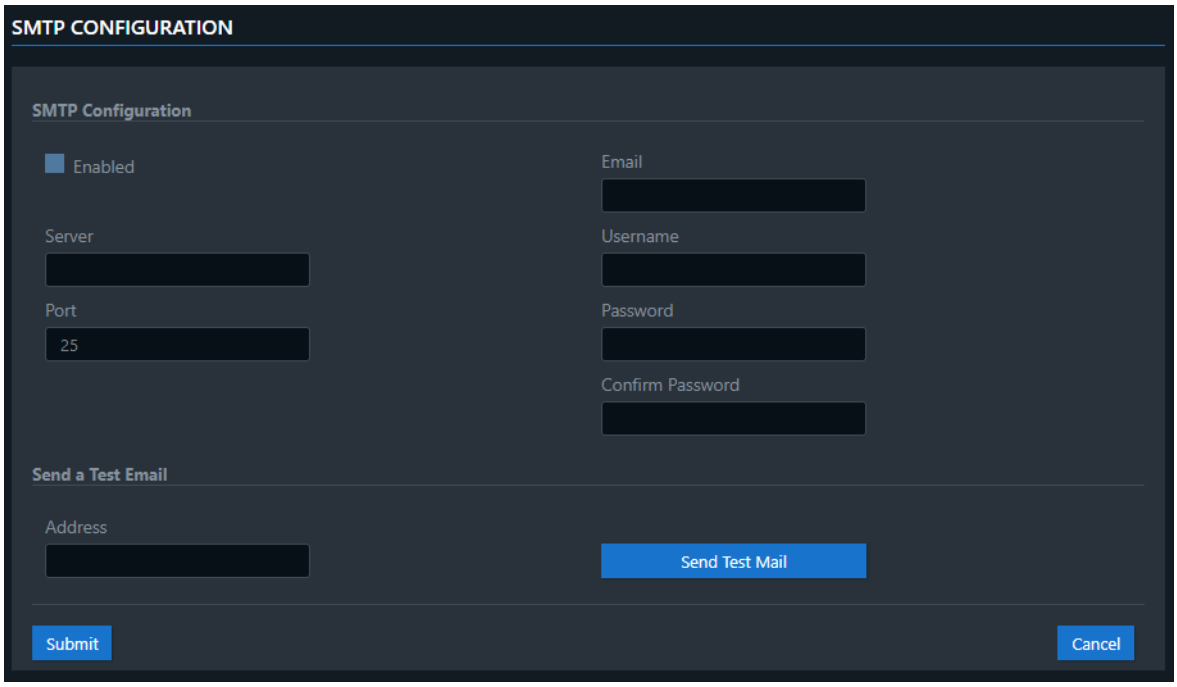


Figure 8.12 SMTP Configuration

Table 8.4 SMTP Settings

Setting Name	Value	Default	Description
Server	Unicast IP address or a valid domain name	[Empty]	The IP address or the domain name of the mail server.
Port	1–65563	25	The port of the mail server.
Email	*xxx@yyy*.com	[Empty]	The email address of the router. This email address shows up as the sender email address for sent emails.
Username	0–250 characters	[Empty]	The username that the SEL-3061 uses to authenticate access to the SMTP server.
Password	0–250 characters	[Empty]	The password of the username that the SEL-3061 uses to authenticate access to the SMTP server.

The SEL-3061 provides a feature that allows you to test and verify SMTP configurations by sending a test email. To send a test email, enter a valid email address and select **Send Test Email**.

Notifications and Alarms

Overview

The SEL-3061 can be configured to directly send notifications and alarms to external clients over two subsystems:

- Text messaging via SMS
- Email via SMTP

All notifications and alarm interfaces are disabled by default.

NOTE: The Notifications and Alarms system is separate from the Syslog server and local Syslog interfaces, which are described in *Syslog on page 8.3*.

The notifications and alarms are arranged into six event groups:

- Authentication
- Chassis
- Configuration
- Link
- Security
- Cellular

Event groups can be individually enabled, and notifications and alarms can be sent to unique recipient groups. Each recipient group may contain one or more phone numbers for text messages (SMS) and one or more email addresses for SMTP.

Notification/Alarms Web Interface

Navigate to the **Administration > Notification/Alarms** page of the web interface to view or change the Event Notification settings and the recipient groups. The SMTP and SMS settings share the Notification/Alarms interface. *Figure 8.13* shows the Notification/Alarms web interface with sample entries.

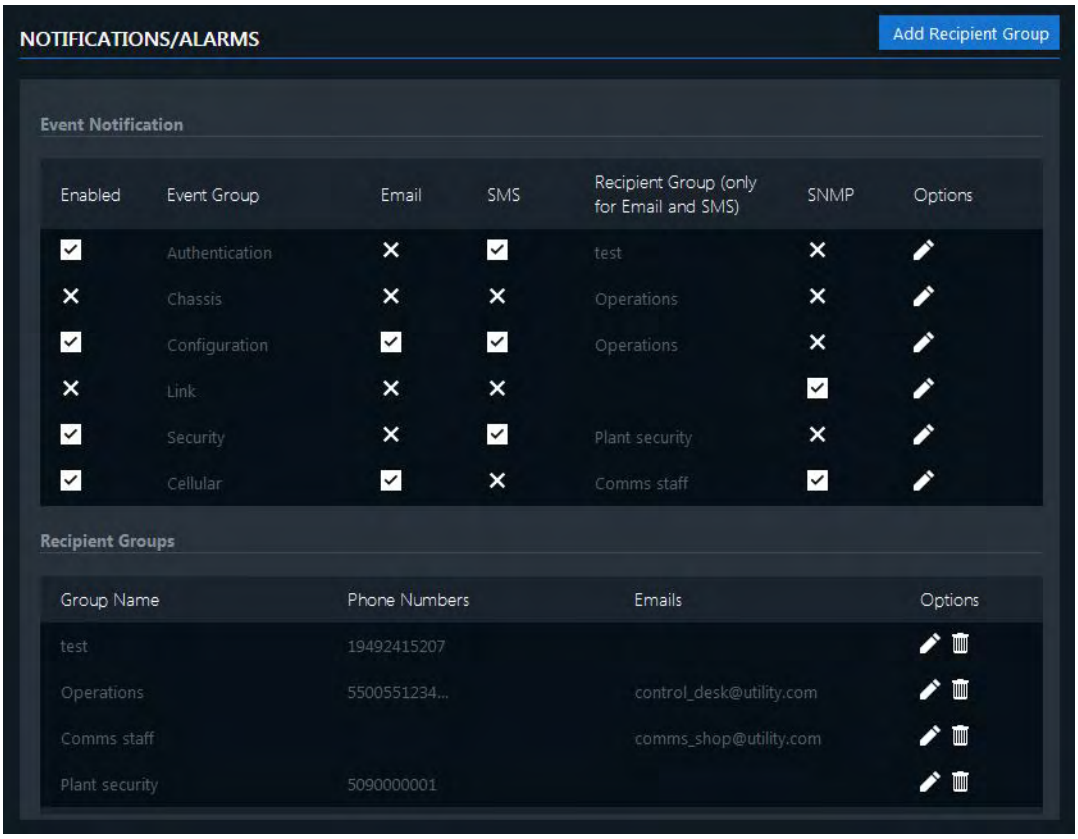


Figure 8.13 Notifications and Alarms Screen

The SMS and SMTP Recipient group settings appear on a shared page, as shown in *Figure 8.14*.

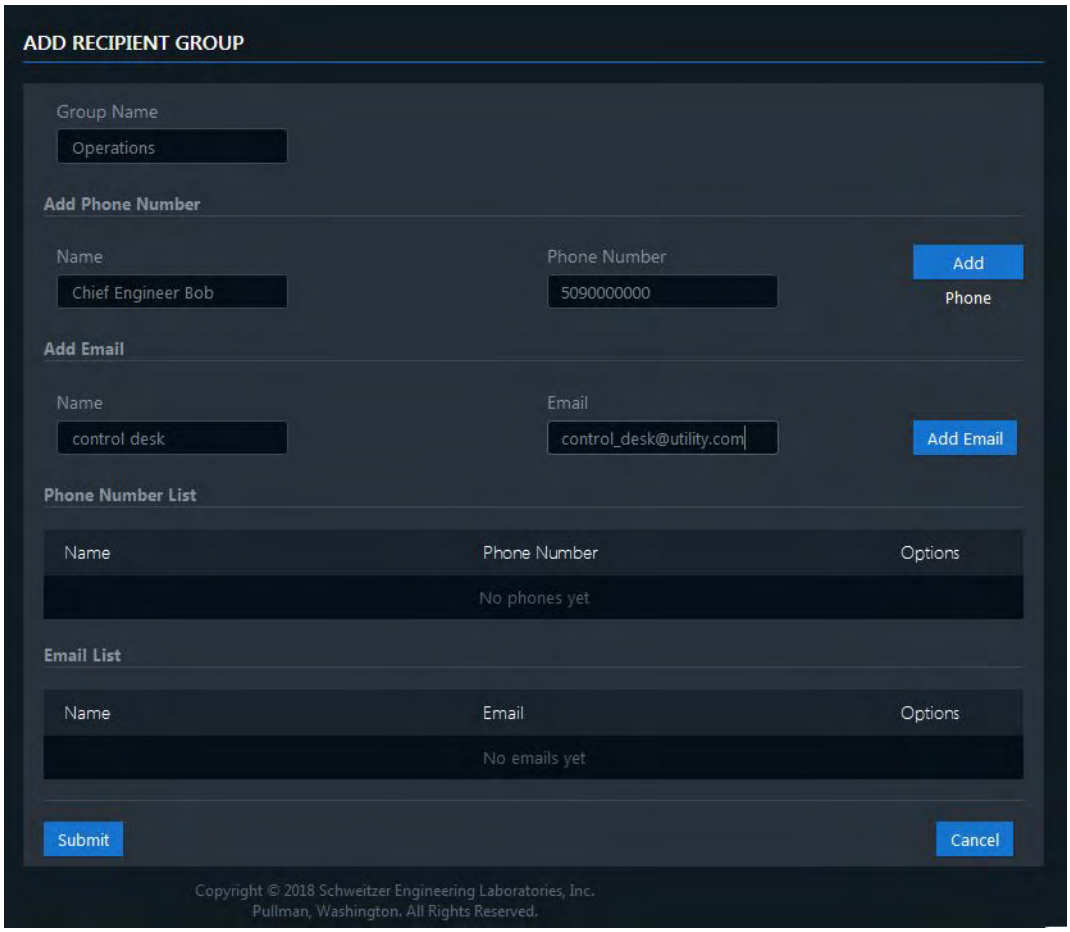


Figure 8.14 Add Recipient Group Screen

If you are configuring both servers, some of the following steps can be combined.

Configure SMS and Recipient Groups

To configure SMS notifications and alarms, first configure the SMS, following the instructions in *SMS on page 8.9*.

Navigate to **Administration > Notifications/Alarms** and select **Add Recipient Group** on the top of the page, or select the pencil icon beside an existing Recipient Group to update the group. The Add Recipient Group screen shown in *Figure 8.14* opens.

Enter a **Group Name**, then complete the **Name** and **Phone Number** boxes and select **Add Phone**. The newly entered name and number now appears in the Phone Number List. To add more numbers to a recipient group, enter them into the Phone Number box and select **Add Phone**. After adding all names and numbers for the group, select **Submit**.

Follow the steps in *Enabling Event Group Notifications and Alarms on page 8.16*.

Configure SMTP and Recipient Groups

To configure SMTP notifications and alarms, first configure the SMTP subsystem by following the instructions in *SMTP on page 8.12*.

Navigate to **Administration > Notifications/Alarms** and select **Add Recipient Group** on the top of the page (see *Figure 8.14*), or select the pencil icon beside an existing Recipient Group to update the group. The Add Recipient Group screen opens, as shown in *Figure 8.14*.

Enter a **Group Name**, then complete the **Name** and **Email** boxes and select **Add Email**. The newly entered name and email address now appears in the Email List. To add more emails to the recipient group, enter them into the Email box and select **Add Email**. After adding all names and emails for the group, select **Submit**.

Follow the steps in *Enabling Event Group Notifications and Alarms.*

Enabling Event Group Notifications and Alarms

After configuring the recipient groups for SMS or SMTP, navigate to **Administration > Notifications/Alarms**, and select the pencil icon at the end of the row of the event group you want to enable. In the window that appears (see *Figure 8.15*), check the **Enabled** box to enable the event group. Leave the box empty to disable the group. Enable or disable the notification options by using the check boxes. If you enable SMTP or SMS, you must also select the desired Recipient group from the drop-down list.

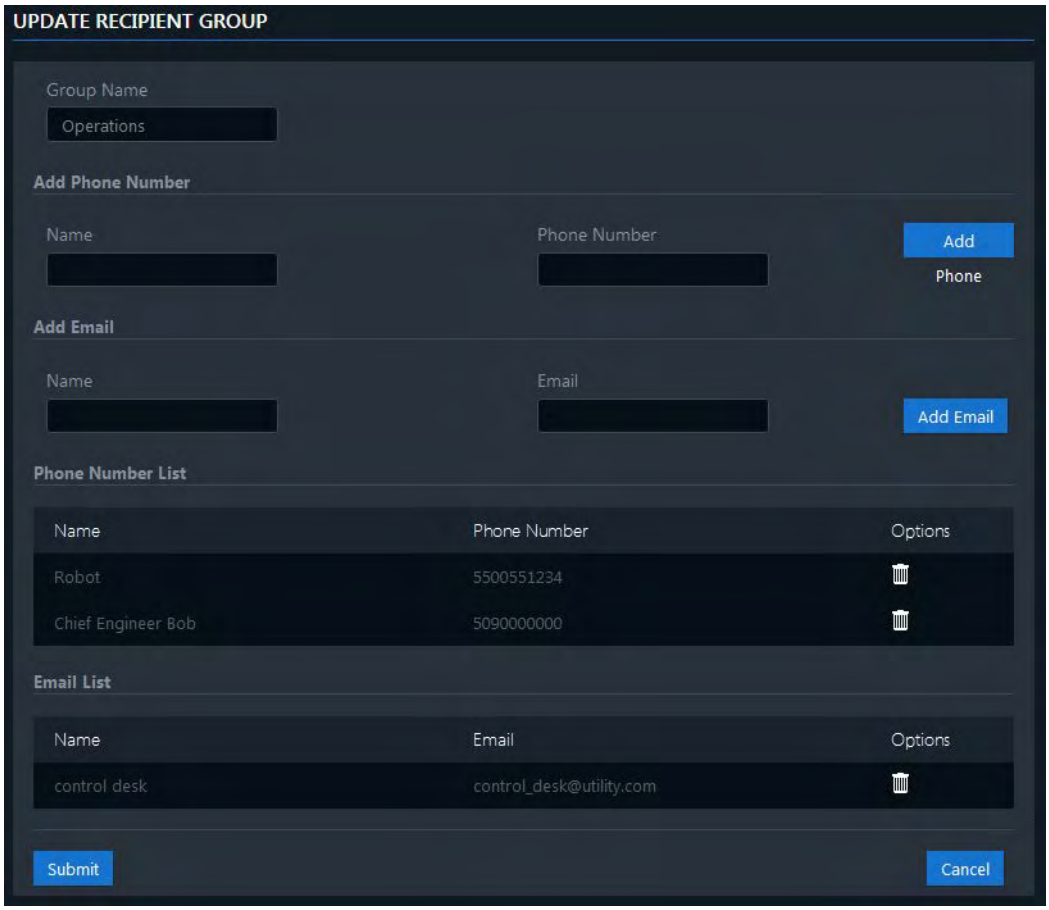


Figure 8.15 Update Recipient Group Screen

Select **OK** to enable the event group. Once an Event Group is enabled, a check mark appears in the Enabled column and in either the Email or SMS column. To later disable or modify an event group, select the pencil icon for the event group.

Select **Save And Restart** on the web interface menu to submit the settings.

Viewing the Notifications and Alarms Log

Navigate to **Diagnostics > Notifications/Alarms Sent**. The list shows the events sent via either SMS or SMTP. The log displays the columns defined in *Table 8.5*.

Table 8.5 Notifications and Alarms Log Definitions

Column Name	Description
Date	Date and time of the event.
Event Group	Name of the Event Group.
Message	Description of the event.
Email	A check mark indicates that the event was sent to one or more email addresses (in the recipient group).
SMS	A check mark indicates that the event was sent to one or more cellphone numbers (in the recipient group).
Recipient Group	Name of the recipient group.

Diagnostics

Diagnostics shows the statistics of communications interfaces, locally logged Syslog events, the list of event notifications and alarms sent, interface information, VPN status and links, and the status of device pings.

The Diagnostics tab shows the status of firewall rules, network state, IPsec status, and state and links, as shown in *Figure 8.16*. Select **Update Diagnostic** to update the information.

To ping a device on the network, enter the IP address, select the Network Interface, and select the **Ping** button shown in *Figure 8.16*. The upper right-hand corner displays the status of the Ping.

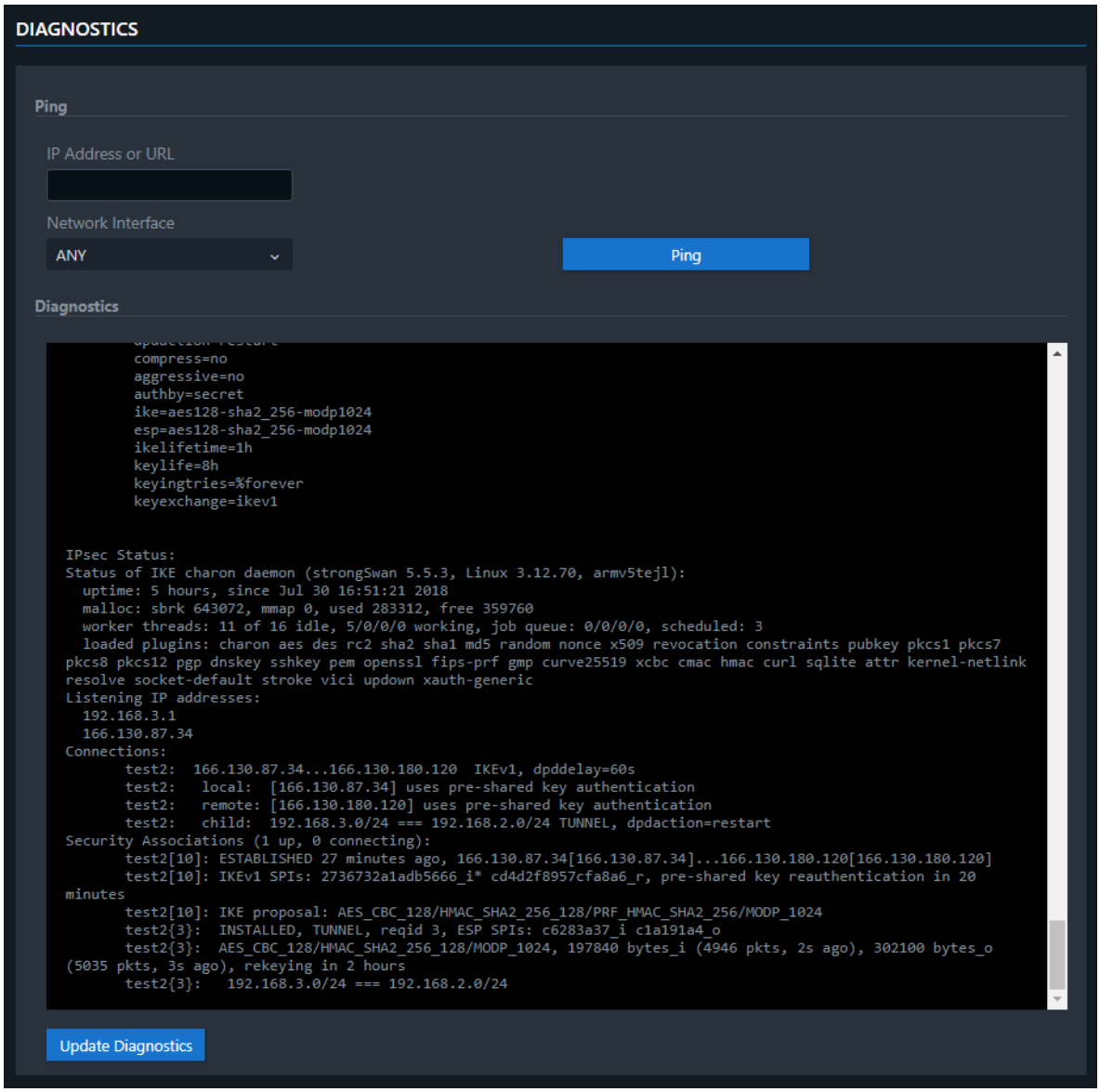


Figure 8.16 Diagnostics Page

Alarm Contact and LEDs

SEL-3061 Alarm Contact

The SEL-3061 alarm contact is part of the event reporting system that notifies users of an event through the operation of a mechanical Form B contact. The mechanical contact is operated by an output coil. When the coil is de-energized, the contact is closed. This is called a normally closed (NC) contact. The NC symbol and terminal location is shown in *Figure 8.17*.

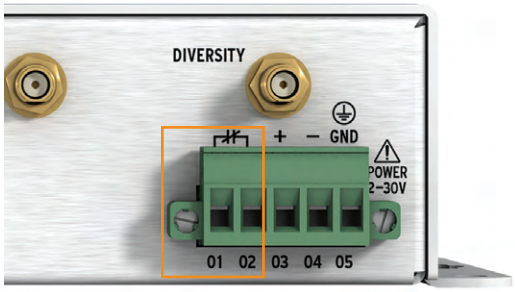


Figure 8.17 SEL-3061 Alarm Contact

The SEL-3061 energizes the alarm output coil during typical operating conditions (i.e., when the device is energized and in operation). The SEL-3061 de-energizes the alarm output coil after an alarm event. The coil is also de-energized when the SEL-3061 is turned off. The alarm output is a dry contact. See *Specifications on page 1.6* for contact electrical ratings.

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 alarm output coil and latch in that mode until it is cleared.

A minor alarm pulses the contact once by de-energizing the output coil for 1 second and then re-energizing the contact. Any additional minor alarms that occur during an active alarm are ignored.

SEL-3061 Front-Panel ALARM LED

The red **ALARM** LED on the front panel, shown in *Figure 8.18*, illuminates when the device is energized and in an alarm condition (i.e., when the alarm coil is de-energized). The **ALARM** LED pulses for minor alarms and latches for major alarms. Major alarms are cleared when the alarm notification is acknowledged or if the alarm event ceases to occur.

Figure 8.18 ALARM LED

This page intentionally left blank

SECTION 9

Troubleshooting

Overview

This section provides guidelines for maintaining and troubleshooting the SEL-3061.

Maintenance

The SEL-3061 is designed to be maintenance free, minimizing your total cost of ownership.

Troubleshooting

Table 9.1 Troubleshooting (Sheet 1 of 5)

Issue/Indicator	Possible Causes	Test and Solution
Device will not connect to the cellular network with a SIM in place.	The SEL-3061 reads the SIM contents periodically and requires that you select **Save And Restart** to use a new SIM card.	Select **Save And Restart** on the user interface.
Settings do not take effect.	The SEL-3061 requires that you select **Save And Restart** to accept the settings.	Select **Save And Restart** on the user interface. The Save And Restart button has red shading when there are unsaved settings.
The **ENABLED** LED is not illuminated and the **ALARM** LED is illuminated.	The SEL-3061 has experienced a diagnostics failure that prevents it from operating.	Contact SEL for further support.
The yellow **100Mbps** LED is flashing.	A network communication collision is detected.	Configure attached network devices for full-duplex communications.
ENABLED and **ALARM** LEDs turn on and off, and the Alarm contact clicks.	SEL-3061 is restarting.	This is expected behavior when the system is restarting after each subsystem starts up and reports its status.
	An Alarm condition exists.	Inspect the **Diagnostics > Notifications/ Alarms Sent** or **Diagnostics > Local Syslog Events** pages to check for unexpected activity. These reports may not contain anything if they have not been configured. See *Notifications and Alarms on page 8.13* and *Syslog on page 8.3*.
	A remote user is logging in or issuing a command (which causes an alarm).	
All LEDs are off	Power supply outage.	Check the power supply voltage with a portable meter. Check the wired connections in the removable connector. If proper voltage is present, remove and reapply power.

Table 9.1 Troubleshooting (Sheet 2 of 5)

Issue/Indicator	Possible Causes	Test and Solution
The yellow **100Mbps** LED is off after making a connection, or network speeds are slower than expected.	The attached network device is configured for 10 Mbps.	Set connection settings for the attached network device to 100 Mbps or Auto Sense.
The green **LNK/ACT** LED is off after making a connection.	The attached network device interface is disabled.	Enable the attached network device interface.
	The Ethernet cabling is faulty.	Inspect cabling and replace if necessary.
	Wrong network.	Verify the IP address.
The normally green **LINK** LED near the antenna symbol on the SEL-3061 front panel is off. This indicates there is no link to the cellular data network.	The WAN feature is not enabled or is incorrectly configured.	Navigate to **Configuration > WAN > Cellular Configuration** and verify the Enabled box is checked. Update other settings as necessary.
	The wireless signal quality is poor.	Refer to the next table entry regarding **SIGNAL** LEDs.
	There is no SIM card installed, or the SIM card is for the wrong carrier.	Install an appropriate SIM card and restart the unit.
	The cellular data network is down, or the account has not been activated.	Check for data connectivity on another device, such as a smartphone. Contact the carrier if the wireless data system is not working.
	The SEL-3061 is not ready for use.	Wait for the SEL-3061 to initialize. After a settings change or restart, it can take 2 additional minutes for system initialization. After a firmware update, it can take as long as 10 minutes for the unit to fully activate.
Two or fewer **SIGNAL** LEDs are illuminated. Normally there should be one or two green LEDs asserted, plus the red and yellow LEDs.	There is a bad antenna cable connection or antenna location.	Check the antenna cable connections, and adjust the antenna height or position. Check **Dashboard > Cellular > Signal reading**, which should ideally be above –85 dBm.
	The wireless signal quality is always poor at the installed location.	Consult the carrier coverage map. Check the signal reading on another device that is on the same carrier network, such as a smartphone. If the signal is low, consider raising the antenna height or relocating the equipment.
	For periodic symptoms, the carrier network traffic loading might cause service to switch to a more distant tower.	Contact the carrier.
	There is an interfering radio source.	
Suspected LED failure.	Hardware defect.	Insert a small object, such as a bent paper clip, in the front-panel pinhole, and press for 5 seconds. All LEDs should illuminate as long as the button is held. See *Lamp Test on page 5.33*.
Serial Port does not work.	Incorrect serial cable.	Be sure to use SEL-C246 or SEL-C285 serial cable. For more details, see *Section 6: Serial Communications*.
	Buffer Timeout is set to zero.	Change the Buffer Timeout to 100 ms. You may need to repeat the test and adjust the process several times.
	Incorrect protocol.	Ensure the protocol is correct (TCP, UDP, or SSL/TLS). See *Section 6: Serial Communications* for details.

Table 9.1 Troubleshooting (Sheet 3 of 5)

Issue/Indicator	Possible Causes	Test and Solution
Cannot ping the SEL-3061 LAN Ethernet interface.	The ICMP protocol is disabled by default.	Log in to the web user interface and enable ICMP. See *ICMP Settings on page 5.10* for more information.
AT&T device has the incorrect IP address.	The device is using the incorrect APN.	Log in to the web user interface and enter its assigned APN, then select **Save And Restart**. See *Cellular Network (WAN) on page 4.7* for more information.
The login page is inaccessible from the **ETH** interface.	The laptop is not configured or is on a different network.	Enable DHCP on your laptop/computer.
A user cannot log in to the SEL-3061 web interface.	The user account is missing or disabled.	Log in to the SEL-3061 as Administrator and verify the details of the user account. See *Systems on page 5.1* for more information.
	The user password is incorrect.	
Users cannot log in to the SEL-3061 by using a RADIUS account.	RADIUS Authentication and Accounting are disabled by default.	Enable RADIUS through the use of the web user interface.
	No RADIUS primary and secondary servers are defined.	Set up a RADIUS server. See *RADIUS on page 5.22*.
	The Shared Secret Key does not match with the RADIUS server.	Ensure the Shared Secret Key matches.
	Device supports only PAP.	Ensure the RADIUS servers are configured to use PAP.
The device locks out after three failed consecutive attempts.	Expected operation. IP Defense Brute Force Prevention recognized the multiple failed attempts and locked out the account for a short period of time to stop what it believes is a security attack on the device.	Change Brute Force Prevention for Access Configuration. See *Brute Force Prevention on page 5.11*.
Date and time are incorrect.	The SEL-3061 clock battery is depleted.	Replace the battery only with Renata CR1632 or equivalent recommended by manufacturer.
	The time zone is incorrectly set.	Navigate to **Administration > System > Date/Time** and set the time zone. Select **Submit**, then **Save And Restart**.
	The time zone has returned to its default value after a factory reset.	
	Daylight-saving time has just started or ended.	The device does not support automatic daylight-saving time adjustments.
	SNTP is not correctly configured or cannot reach the (S)NTP server.	Ensure SNTP is enabled and its server IP address is correct.
No remote Syslog messages are received from the SEL-3061.	No Syslog servers are defined.	Set up a remote Syslog destination. See *Remote Syslog Settings on page 8.7* for more details.
	The Syslog severity threshold is unexpectedly high.	Reconfigure the severity threshold for the remote Syslog destination to the desired severity level. See *Section 8: Diagnostics and Logging* for more information.
	The Syslog server is not reachable from the network containing the SEL-3061.	Ensure that the Syslog server IP address is valid and reachable. See *Section 8: Diagnostics and Logging* for more information. If the Syslog server is on another network, ensure that a network gateway is configured and available to route the Syslog traffic.
Not receiving all expected remote Syslog messages.	The remote Syslog severity threshold on the SEL-3061 is unexpectedly high.	Reconfigure the severity threshold for the remote Syslog destination to the desired security level. See *Syslog on page 8.3* for more information.

Table 9.1 Troubleshooting (Sheet 4 of 5)

Issue/Indicator	Possible Causes	Test and Solution
Not receiving Email Notifications/Alarms.	Email server is not defined.	Set up an email server with your network Administrator. See *SMTP on page 8.12* for more information.
	Email server is incorrect in the device settings.	Verify the Email server is correct. See *SMTP on page 8.12* for more information.
	Email account is incorrect.	Ensure the email account for the device is correct. See *SMTP on page 8.12* for more information.
	Notifications/Alarms settings are disabled.	Enable notification group in Notifications/Alarms. See *Configure SMTP and Recipient Groups on page 8.15* for details.
	Email server is not reachable from the SEL-3061 network.	Ensure that the mail server is valid and is on a network that the SEL-3061 can reach.
Not receiving SMS notifications/Alarms.	SMS is disabled.	Ensure the SMS is enabled. See *SMS on page 8.9*.
	Notifications/Alarms settings are disabled. SMS messages are not able to route.	Enable notification group in Notifications/Alarms. See *Configure SMS and Recipient Groups on page 8.15* for details.
Cannot import X.509 certificate.	Certificate format is incorrect.	The format must be as shown in *Figure 5.34*.
	Neither the CA or intermediate CA is available.	You must upload the CA and intermediate CA that signed the X.509 certificate. See *X.509 on page 5.27*.
PPP Link is down.	APN setting is not present (for AT&T).	Ensure the APN has the correct APN settings. See *Cellular Network (WAN) on page 4.7* for more information.
	Network Authentication is incorrect.	Reconfigure Authentication Type, username, and password. See *Authentication on page 4.7* for more information.
	Cellular Network is unavailable.	Check cellular received signal strength on the dashboard. It is possible that there is no cellular coverage.
	SIM card is missing or incorrectly installed.	Ensure the SIM card is present and installed correctly. See *Section 1: Introduction and Specifications* for details.
IPsec VPN cannot be established.	Remote WAN IP is incorrect.	Verify the remote WAN IP address. See *IPsec VPN on page 7.1* for more information.
	Remote Network is incorrect.	Verify the remote network settings. See *IPsec VPN on page 7.1* for more information.
	Pre-Shared Key does not match with the IPsec VPN peer.	Verify the Pre-Shared Key settings. See *IPsec VPN on page 7.1* for more information.
	IKE protocol does not match with the IPsec VPN peer.	Verify IKE protocol settings. See *IPsec VPN on page 7.1* for more information.
	Remote endpoint is not available or there is a network issue.	Use the ping tool in Diagnostics to ping a remote endpoint. See *Diagnostics on page 8.17* for details.
	Forward filter rules are missing.	Define the forward filter rules to allow traffic to go through the IPsec VPN.

Table 9.1 Troubleshooting (Sheet 5 of 5)

Issue/Indicator	Possible Causes	Test and Solution
Port Forwarding Rules do not work.	Incorrect Source settings.	Verify Source settings. See *Firewall on page 7.3* for details.
	Incorrect Destination settings.	Verify Destination settings. See *Firewall on page 7.3* for details.
	Incorrect Protocol, Chain, or Target settings.	Verify Protocol, Chain, or Target settings. See *Firewall on page 7.3* for details.

This page intentionally left blank

SECTION 10

Job Done Examples

Introduction

This section has four Job Done examples on how to set up the SEL-3061 for several common applications.

Job Done Example 1: Setting Up an IPsec VPN Between Two SEL-3061 Routers

Although this example describes how to set up an IPsec VPN between two SEL-3061 routers, it can be used as a reference for setting up an IPsec VPN between an SEL-3061 and third-party routers/gateways. The SEL-3061 requires a two-step process to set up an IPsec VPN tunnel.

Step 1. Establish an IPsec VPN tunnel between the two routers with the settings under *Set Up IPsec VPN Tunnel*.

Step 2. Enable tunnel traffic by using the firewall rules (see *Configure Firewall Rules for the IPsec VPN Tunnel*).

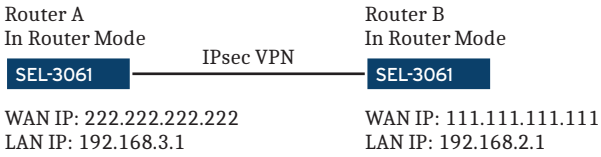


Figure 10.1 Example of an IPsec VPN Tunnel Between Two SEL-3061 Routers

Set Up IPsec VPN Tunnel

To set up an IPsec VPN tunnel, go to **Configuration > Tunnel > IPsec Tunnels**, and select **Add Tunnel**. Set the following settings on each SEL-3061 (see *Figure 10.2* and *Figure 10.3*):

- Enter the IP address of the remote router obtained from the cellular network into the Remote WAN IP box. Router A has the WAN IP address of Router B, and Router B has the WAN IP address of Router A.
- Enter the LAN IP address of the remote router into the remote network route box. Router A has a remote network route in the 192.168.2.*x* range, and Router B has a remote network route in the 192.168.3.*x* range.

- Enter the LAN IP mask of the remote router. The Remote Network Mask determines the number of devices that can be in the network behind the routers.
- Match the remaining settings between the two routers or between an SEL-3061 and a third-party router/gateway.

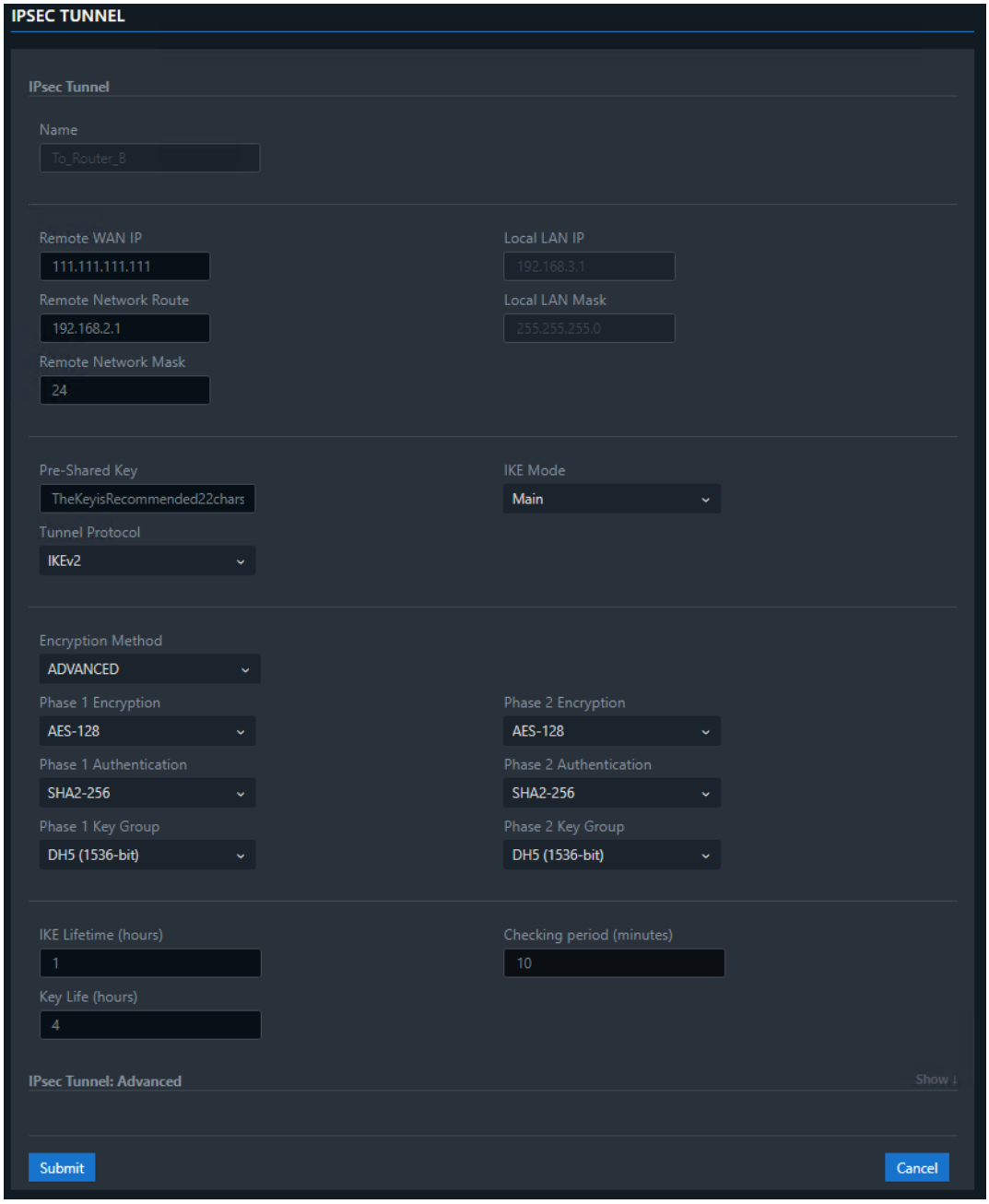


Figure 10.2 Router A Tunnel Settings

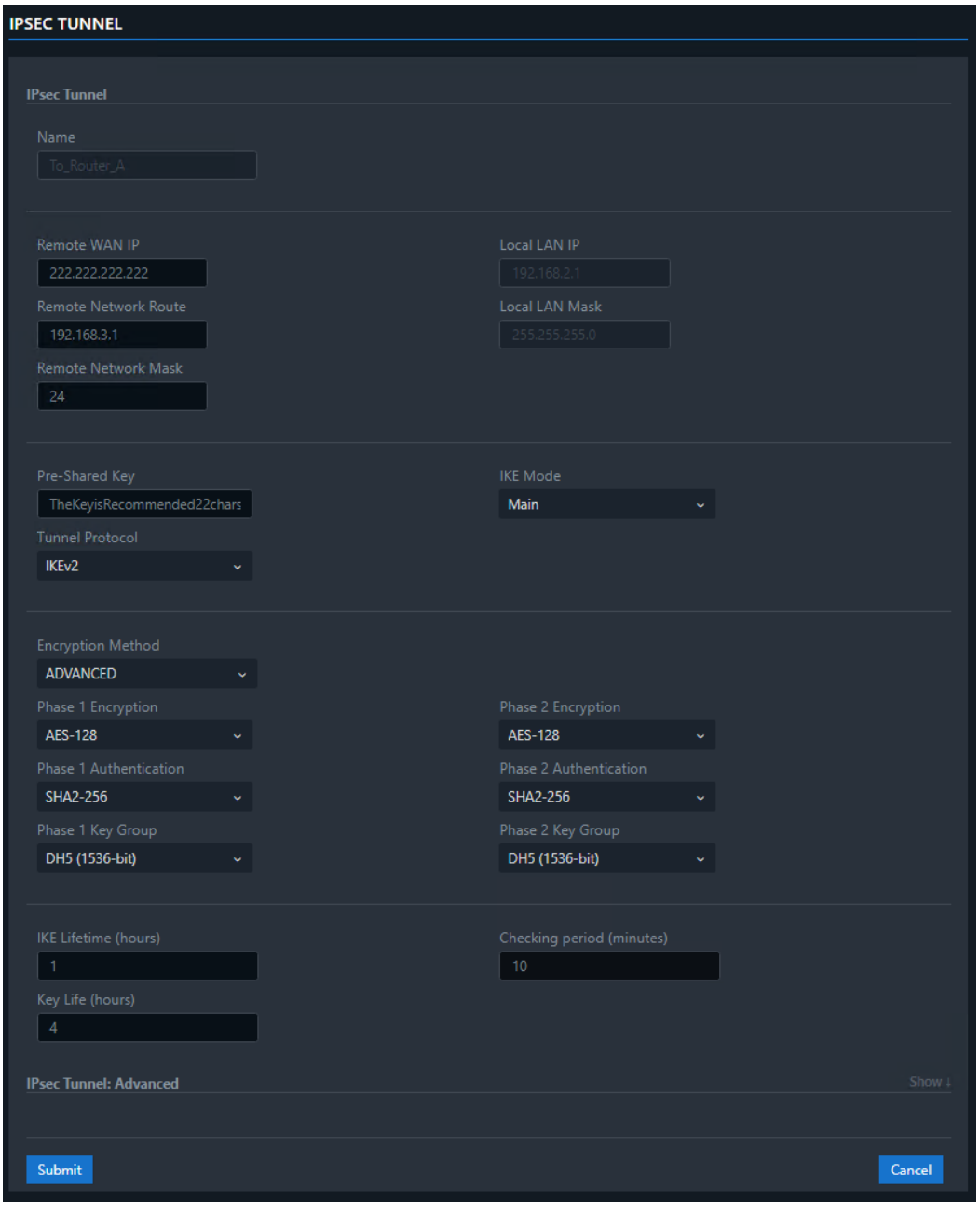


Figure 10.3 Router B Tunnel Settings

You can replace Router B with a third-party router or gateway, or the SEL-3620 Ethernet Gateway. If you already have secure network access on the data collection side of the link, a second SEL-3061 is not necessary.

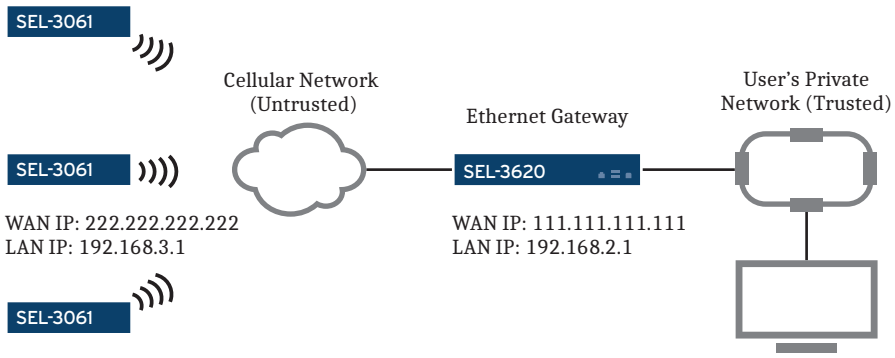


Figure 10.4 IPsec VPN With an SEL-3620 Secure Gateway

In this example, Router B is replaced with the SEL-3620. The VPN and firewall rules for the SEL-3061 remain the same, using the SEL-3620 IP addresses as the Remote LAN IP and Remote WAN IP. *Figure 10.5* shows the VPN settings for the SEL-3620 if it is used as Router B instead of the SEL-3061. The SEL-3620 supports a maximum of 16 concurrent VPN sessions.

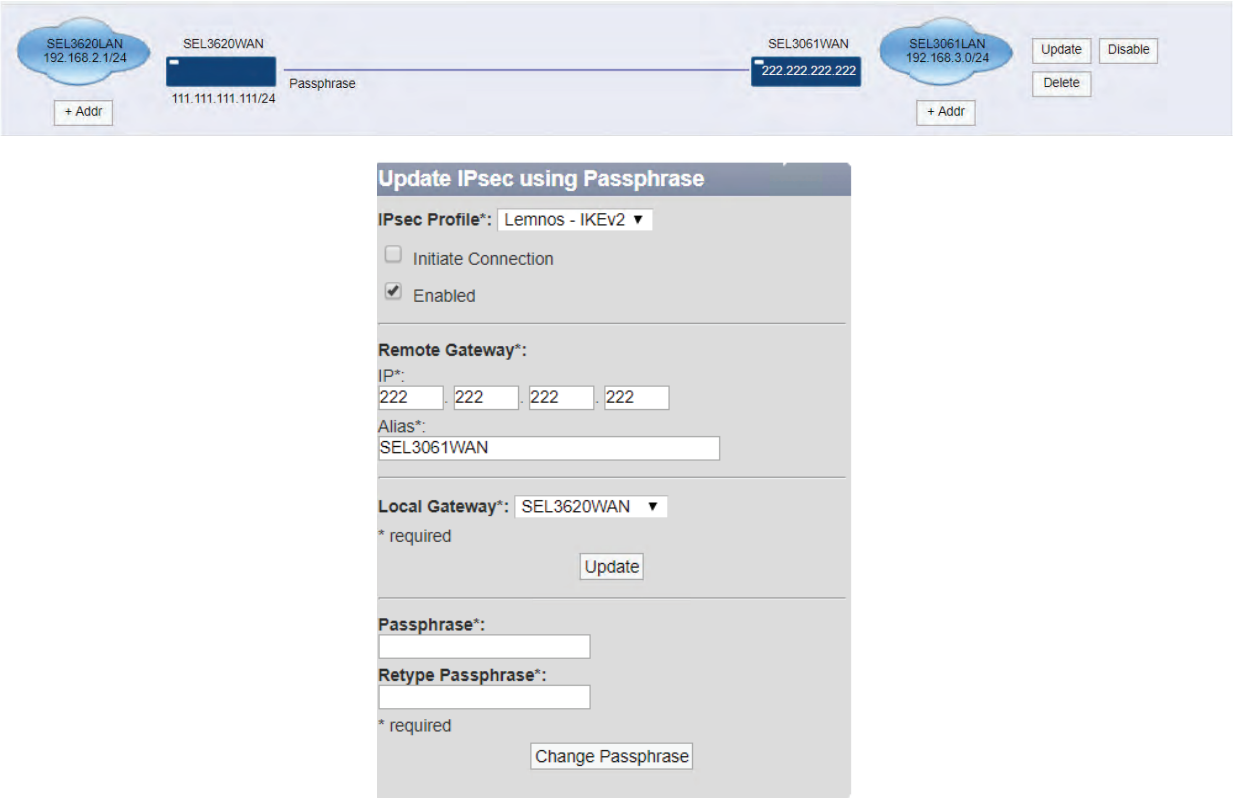


Figure 10.5 SEL-3620 IPsec Settings

Configure Firewall Rules for the IPsec VPN Tunnel

To enable IPsec VPN traffic, firewall rules are required. Two types of traffic can go through the IPsec VPN. One type of traffic goes through the tunnel and the remote cellular router and goes to a device that is attached to the remote cellular router LAN network. The other type of traffic goes through the tunnel and goes in the remote cellular router. Applications that ping the remote cellular router or access the remote cellular web user interface use this type of traffic. To configure firewall rules, go to **Configuration > Security > Firewall**. By default, the

SEL-3061 is in Normal mode, in which you can configure three types of firewall rules: Port Forwarding, Input Filter, and Output Filter. The first type of traffic requires forward filter rules, and the second type of traffic requires both forward and input filter rules.

To allow traffic through the IPsec VPN tunnel, the SEL-3061 routers require Forward Filter rules only. Select **Advanced** to set Forward Filter rules. Select **Add Rule**.

The Filter Rule settings page allows the device to whitelist source and destination IP addresses and ports. It also allows you to whitelist a specific MAC address of the source, if needed.

In this case, enable traffic from Router A to Router B. For both routers, the source IP address is the A side IP addresses, and the destination IP address is the Router B IP addresses. Because the connection is stateful, response traffic is allowed as well.

The General Configuration section allows you to select the protocol, chain, and target (see *Figure 10.6*).

Step 1. Select the **Protocol** drop-down arrow and select **TCP/UDP** to have the SEL-3061 filter TCP/UDP.

Step 2. Select the **Chain** drop-down arrow and select **FORWARD** to define the rule as a forward rule.

Step 3. Select the **Target** drop-down arrow to select **ACCEPT** so that all packets that meet the criteria of the filter rule can pass through the IPsec tunnel.

Step 4. Select **Submit** to save the filter rule. For the rule to be applied, select the check box next to the filter rule and select **Save And Restart**.

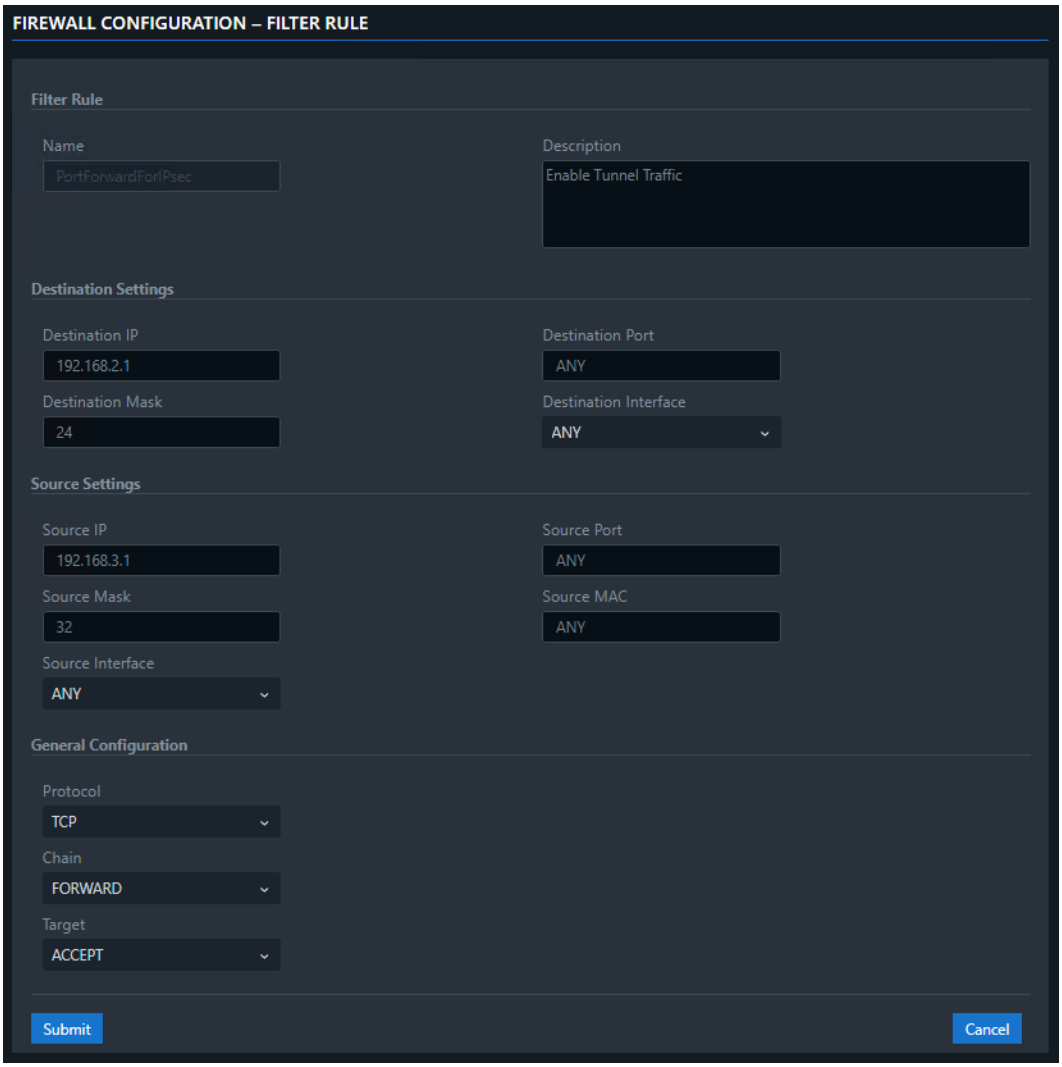


Figure 10.6 Router A and Router B Filter Rules

If Router B is replaced with an SEL-3620, use the settings shown in *Figure 10.6* for filter rules.

To access the remote cellular router, input filter rules are required. The Input Filter rule shown in *Figure 10.7* allows a device that is attached to Router B to ping Router A. Note that for a device to be able to ping Router A, Router A is required to have ping enabled via LAN.

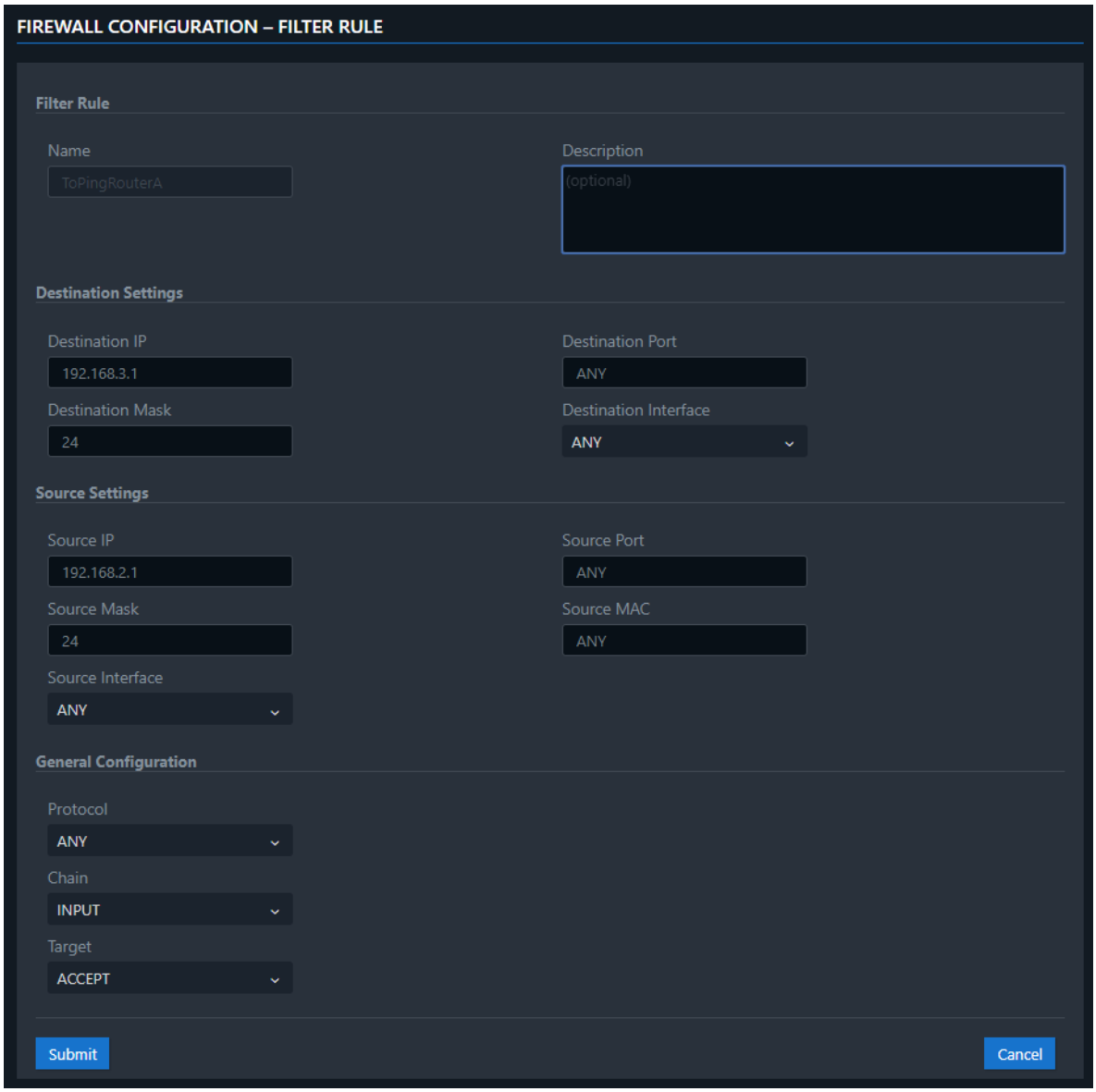


Figure 10.7 Input Rule for Ping

Job Done Example 2: Configuring Port Forwarding in an SEL-3061

In this example, we configure the SEL-3061 Port Forwarding rules for an SEL-651R Recloser Control that is connected to the SEL-3061, as shown in *Figure 10.8*. The port to forward is Port 10000 of the SEL-3061, and the destination is Port 23 of the SEL-651R.

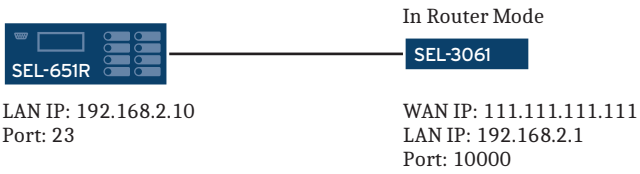


Figure 10.8 Port Forwarding Example

Port Forwarding is applicable to the WAN (cellular) interface. To configure a Port Forwarding rule, go to **Configuration > Security > Firewall**, and select **Add Rule** for Port Forwarding. Configure the Port Forwarding rule, as shown in *Figure 10.9*.

Step 1. Enter the port that you want the SEL-3061 to forward traffic to in the External WAN Port(s) box.

Step 2. Enter the SEL-651R IP address into the Destination LAN IP box and the SEL-651R port in the Destination LAN Port(s) box. For this Job Done example, the External WAN Port is 10000 and the Destination LAN Port is 23.

Step 3. Select **TCP/UDP** from the Protocol drop-down list to have the SEL-3061 filter that protocol.

The settings in the Inbound Filter Rule section allow you to whitelist source IP addresses and ports for this Port Forwarding rule.

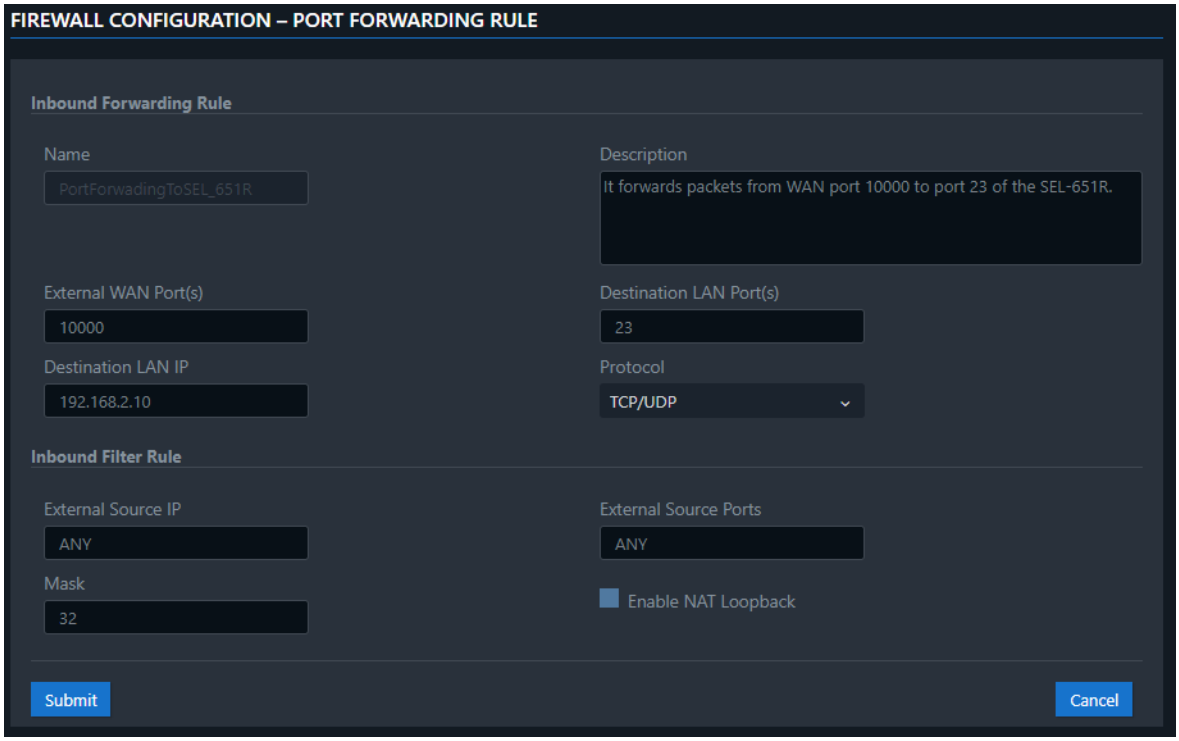


Figure 10.9 Port Forwarding Rule

Job Done Example 3: Using Two SEL-3061 Routers to Extend a Serial Cable

For the serial cable extension (or replacement) application, the setup requires two SEL-3061 Routers. The first SEL-3061 is configured as a client, and the second is configured as a server, as shown in *Figure 10.10*. Note that the server can communicate with one client only. In this application, the SEL Real-Time Automation Controller (RTAC) collects data from the SEL-651R by using serial cables.

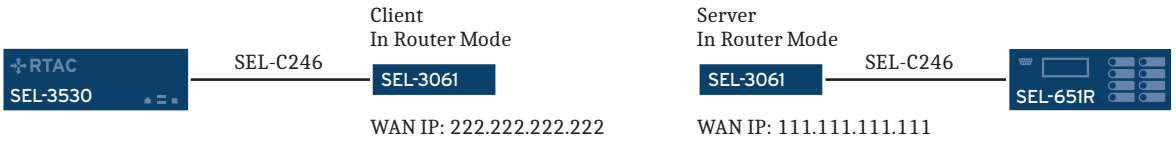


Figure 10.10 Serial Cable Replacement Example

Figure 10.11 shows the setting for the client. The client must have the IP address of the server. The IP address of the server is the IP address of the remote site. If an IPsec VPN is between the client and the server, the IP address of the server is the Ethernet interface of the server router. The port must match between the client and the server. The Buffer Timeout is recommended to be 100 ms for SEL, Modbus, and DNP3 protocols. Note that you may need to adjust the Buffer Timeout for your application, and if the data set sent by the SEL-651R are large, you may want to increase the Buffer Size.

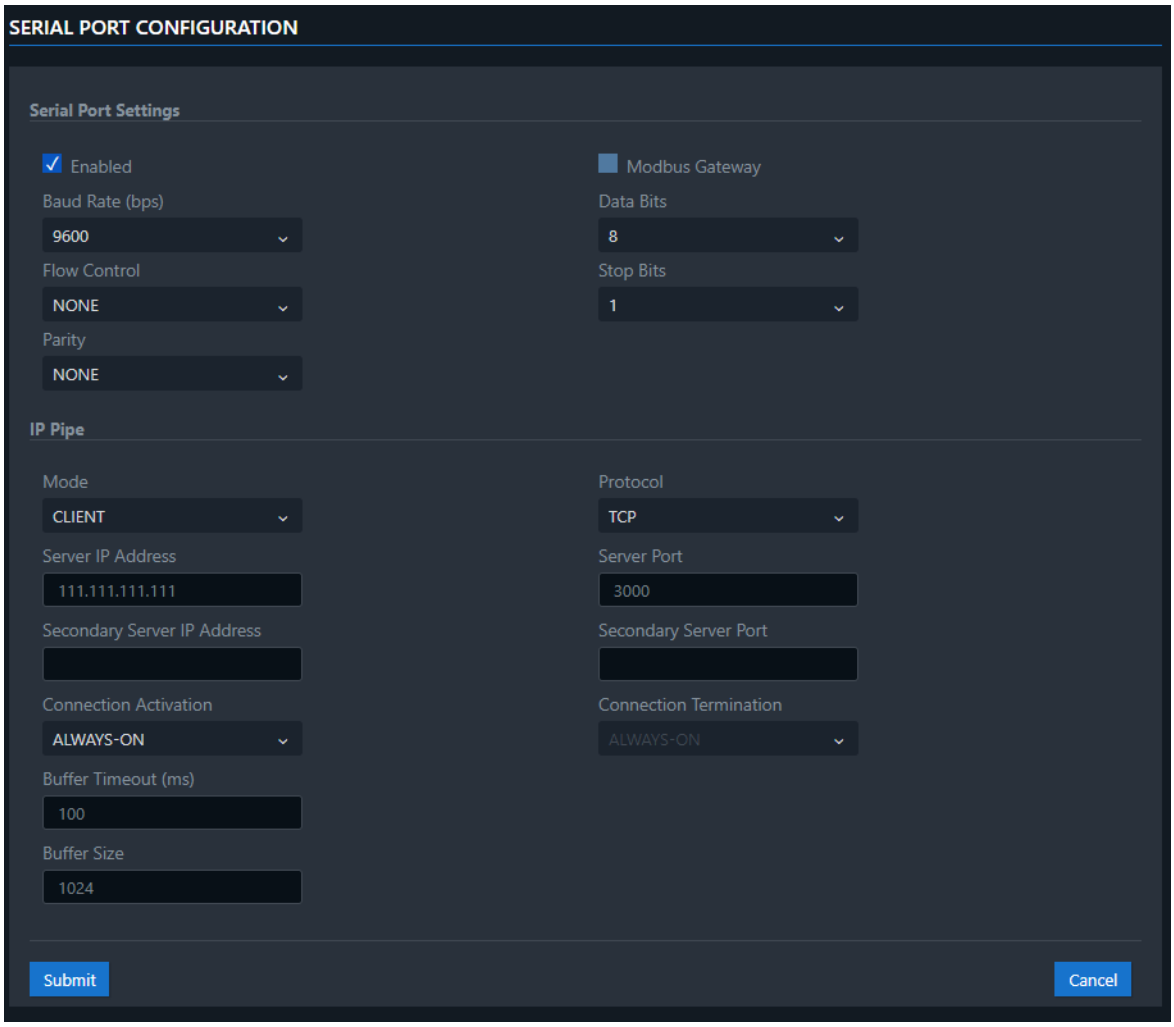


Figure 10.11 Serial Client Settings

To accomplish this Job Done example, the SEL-651R serial connection settings must match the server serial settings. Similarly, the SEL-3530 serial connection settings must match the client serial settings. Note that for DNP3 communications, the setting PREDLY must be set to OFF, as shown in *Figure 10.12*.

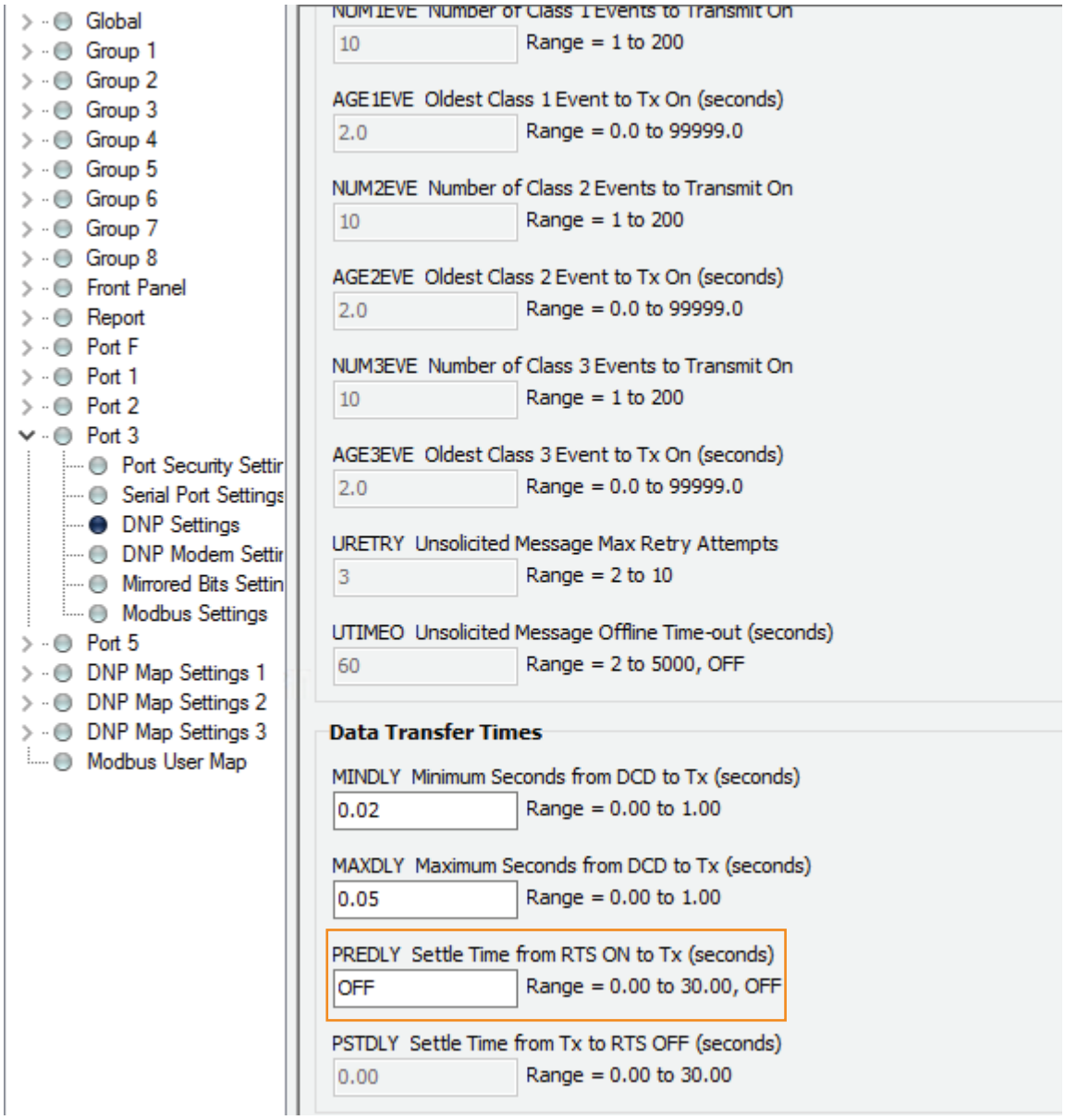


Figure 10.12 SEL-651R DNP3 Settings

Because of latency in the cellular network, the SEL-3530 is required to use an Intermessage Transmit Delay for Modbus communications. This delay depends on the network latency and Modbus polling rates. Use 500 ms as your starting point for testing.

Job Done Example 4: Using Serial Communication for Data Collection

In this example, the SEL-3530 collects data by using serial-connected devices for SEL, Modbus, and DNP3 protocols, as shown in *Figure 10.13*.

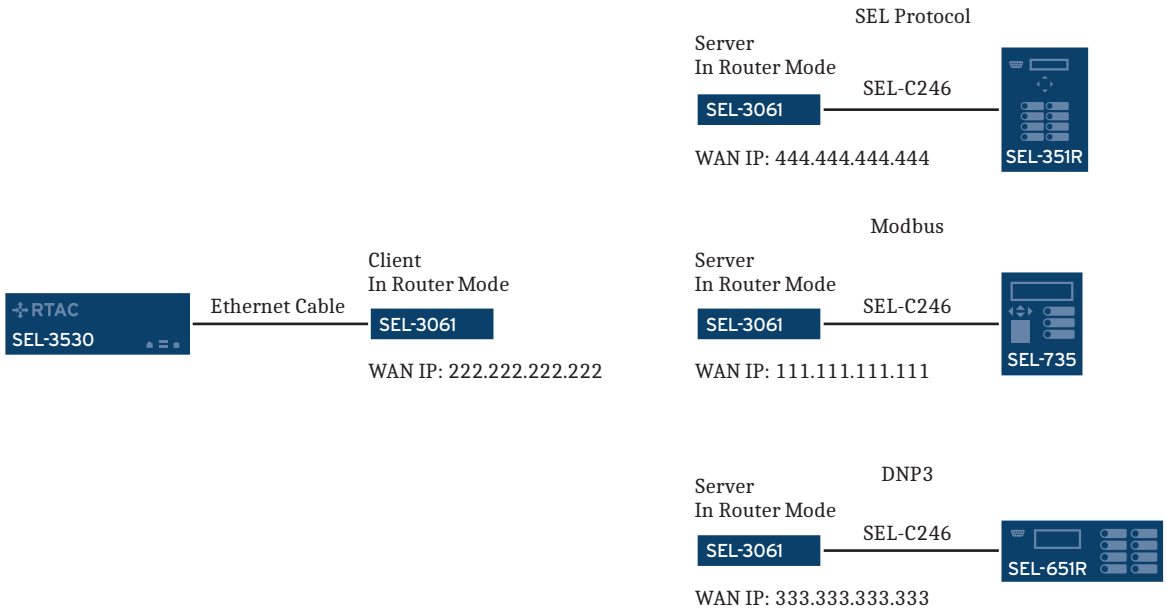


Figure 10.13 Using Ethernet Tunneled Serial for Data Collection

Configure the SEL-351R Falcon Recloser Control to use SEL protocol, the SEL-735 Power Quality and Revenue Meter to use Modbus protocol, and the SEL-651R to use DNP3 protocol. Configure the SEL-3530 for multiple clients by using Ethernet Tunneled Serial for SEL, Modbus, and DNP3. In this example, the SEL-3530 must be on the client side so that it can communicate with multiple servers. The SEL-3061 server settings are the same, as shown in *Figure 10.14*. Note that this example has set ALWAYS-ON for Connection Termination. For additional options, see *Section 6: Serial Communications*.

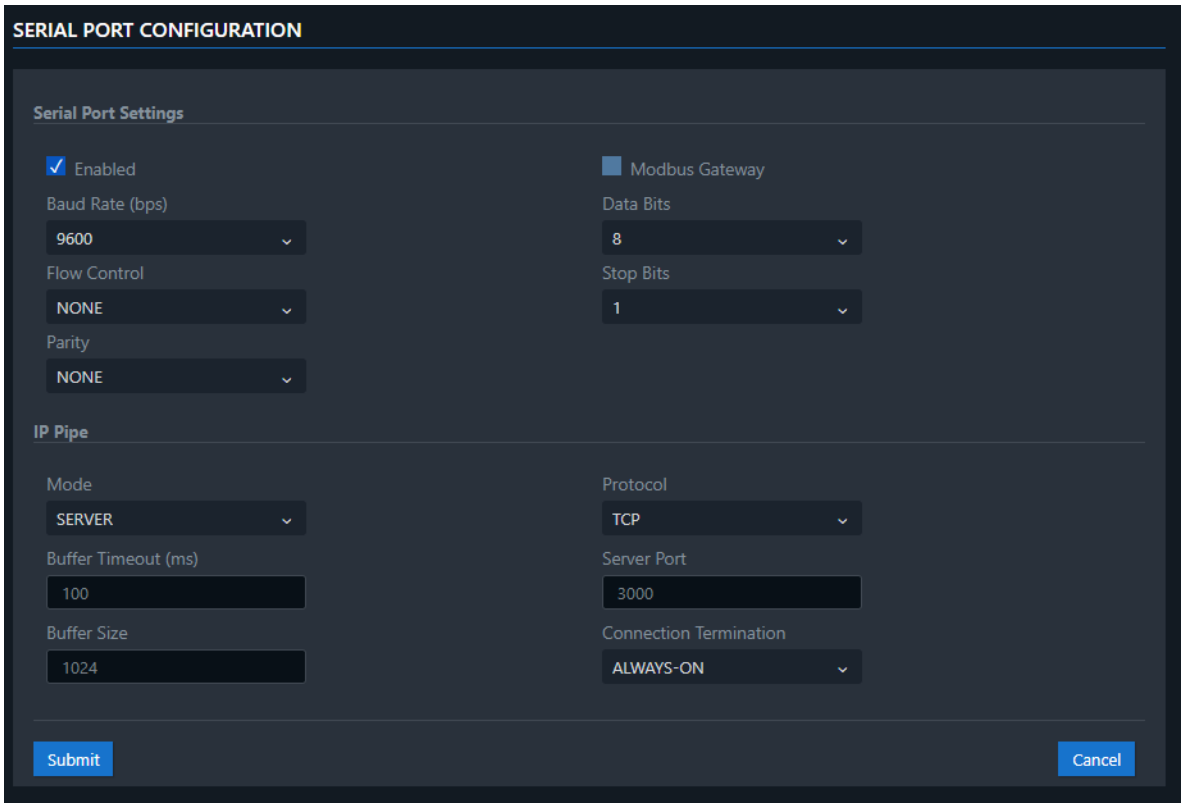


Figure 10.14 Serial Server Settings

In this example, the SEL-3061 client requires serial configuration because it is using Ethernet. The SEL-3061 must be configured to communicate simultaneously with all SEL-3061 servers on the network.

Use the following settings to configure the SEL-3530 for SEL, Modbus, and DNP3:

- Set the Server IP Address for Modbus or DNP3 to the IP address of the SEL-3061 (111.111.111.111), or set the IP address of the Ethernet interface of the SEL-3061 if there is an IPsec VPN between the routers.
- Match the Server IP Port with the SEL-3061 port.
- Set the Serial Tunneling Mode to Raw TCP to match the protocol setting of the router.
- For SEL protocol, set the Poll Period long enough for the cellular network connections.
- For Modbus protocol, add Intermessage Transmit Delay.
- For DNP3 protocol, set PREDLY to OFF.

This page intentionally left blank

SECTION 11

SNMP

Overview

The SEL-3061 provides SNMP read request and notification (trap) support. Through SNMP read requests, you can access SEL-3061 diagnostic and status information from your SNMP client or Network Management System (NMS). You can configure the SEL-3061 to send SNMP notifications to a central location, which provides event monitoring and correlation across the network infrastructure. The SEL-3061 supports SNMP v1, v2c, and v3 for both responding to read requests and sending trap messages to a trap server. By default, SNMP read and SNMP traps are disabled. Both can be enabled via either LAN or WAN (the cellular interface).

SNMP Read

You can access the current status information of the SEL-3061 through the SNMP read operations from your client. The status information is presented as value responses to OIDs (identifiers used for SNMP operations). Most of the information is grouped by using the same grouping found on the user interface. SEL provides customized Management Information Base (MIB) modules to install on your SNMP client to assist with finding the information and decoding the responses. These MIBs are available for download directly from the SEL-3061. *Figure 11.1* shows a list of the MIBs supporting the information inquiry.

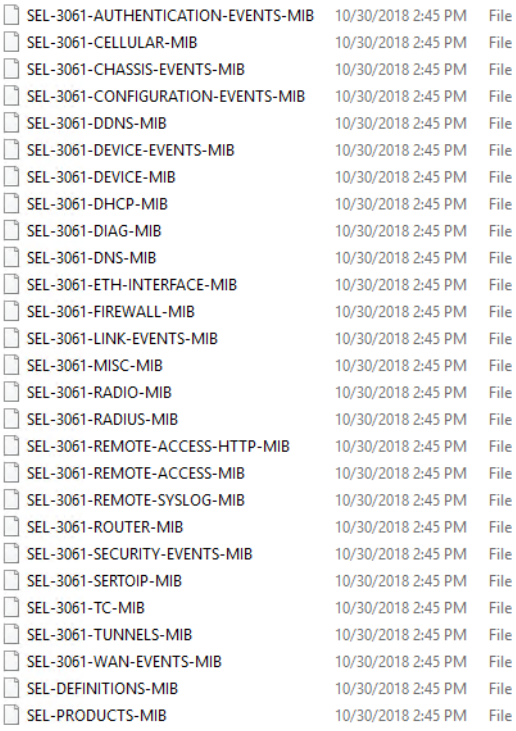


Figure 11.1 List of Supported MIBs

SNMP Read Server Settings

Access the SNMP settings by navigating to **Administration > SNMP** on the SEL-3061 web interface, as shown in *Figure 11.2*.

Once SNMP is enabled, the SNMP server, by default, is enabled via LAN and disabled via WAN. You can enable the SNMP server via WAN. Once the SNMP server is enabled, the SEL-3061 becomes a SNMP server that provides responses to read requests from a client or NMS. The responses include diagnostics and status information of the SEL-3061. Select **Download MIB** to see the MIB files that are available in SEL-3061.

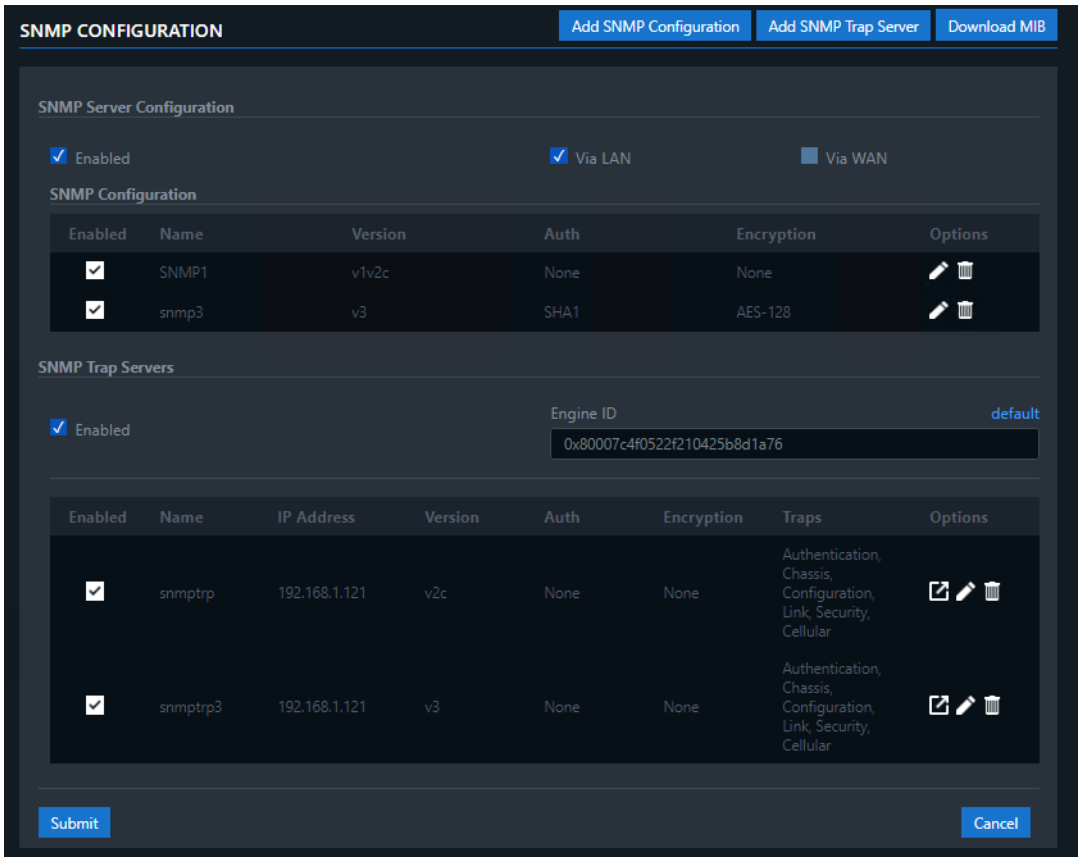


Figure 11.2 SNMP Configuration Menu

To configure the device SNMP server for read access, select **Add SNMP Configuration** to access the menu shown in *Figure 11.3* and refer to *Table 11.1* for information on the SNMP configuration settings.

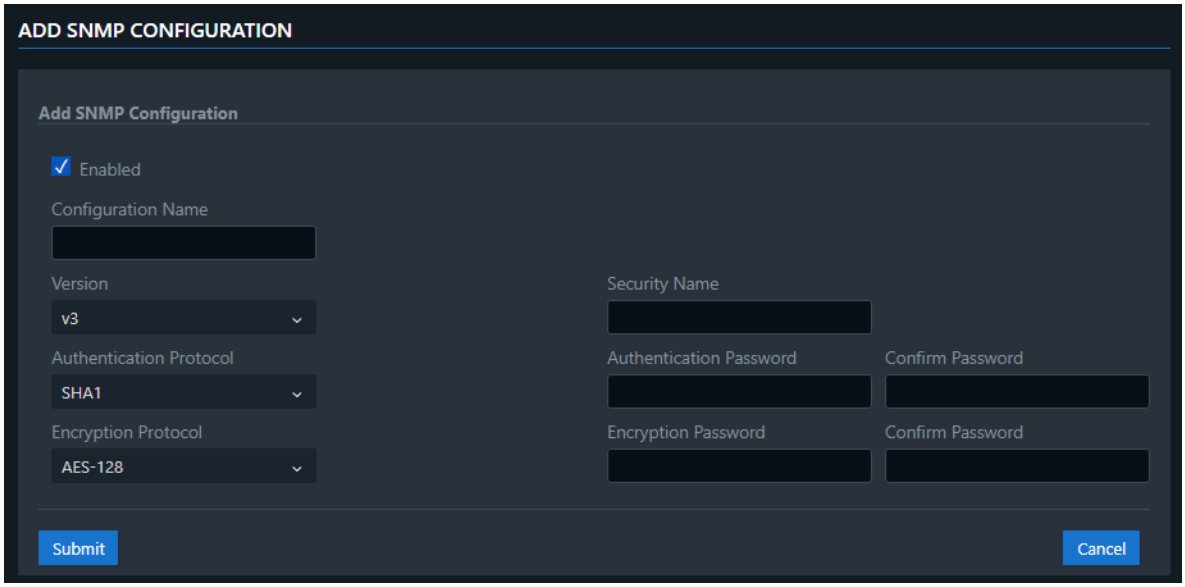


Figure 11.3 Add SNMP Configuration

Table 11.1 SNMP Configuration Settings

Setting Name	Value	Default	Description	Applicable Version
Enabled	Enabled or Disabled	Disabled	Enable or disable SNMP configuration settings.	v1/v2c and v3
Configuration Name	Alphanumeric characters, dashes, underscores, and spaces are acceptable. Maximum 31 characters.	[Empty]	The name of the SNMP server settings.	v1/v2c and v3
Version	v1, v2c, or v3	[Empty]	The version of SNMP protocol.	—
Community String	Alphanumeric characters, dashes, underscores, and spaces are acceptable. Maximum 128 characters.	[Empty]	The community string that the SNMP protocol uses (for v1/v2c only).	v1/v2c
Authentication Protocol	None, MD5, or SHA1	None	Authentication protocol used by SNMP.	v3
Encryption Protocol	None, DES, AES-128	None	Encryption protocol used by SNMP.	v3
Security Name	Alphanumeric characters, dashes, underscores, and spaces are acceptable. Maximum 31 characters.	[Empty]	User security name.	v3

Once SNMP configurations are added, these configurations are shown in the SNMP Configuration list. You can either modify or delete existing SNMP configurations.

SNMP Traps

By default, the SNMP Trap Server is disabled. Once it is enabled, the SEL-3061 becomes a client that can send notifications (traps) to a list of SNMP servers or NMS. A maximum of three SNMP trap servers is supported. The SNMP traps in the SEL-3061 work along with the notifications and alarms sent by the SEL-3061 (see *Notifications and Alarms on page 8.13*). The settings in this section configure the SNMP servers that receive traps but do not enable the SEL-3061 to start sending traps to the servers. To enable the SEL-3061 to send traps, navigate to Notifications/Alarms and enable **SNMP** in the web user interface (see *Section 8: Diagnostics and Logging*). To view or verify the traps that the SEL-3061 has sent, go to **Diagnostics > Notifications/Alarms Sent**. This page lists notifications the SEL-3061 sent to the SNMP trap servers.

SNMP Trap Server Settings

The SNMP server(s) can be on LAN or WAN, depending whether either LAN or WAN is enabled individually or both are enabled together. Once the SNMP server(s) is enabled, the SEL-3061 starts sending traps to these servers. See *Appendix F: Notifications and Alarms List* for a list of available SNMP traps (events). The MIB files also contain the list of traps that the SEL-3061 can send.

To add a SNMP trap server, select **Add SNMP Trap Server** to access the menu shown in *Figure 11.4* and refer to *Table 11.2* for information on the SNMP trap server settings fields for SNMP versions v1 and v2c and *Table 11.3* for SNMP version v3.

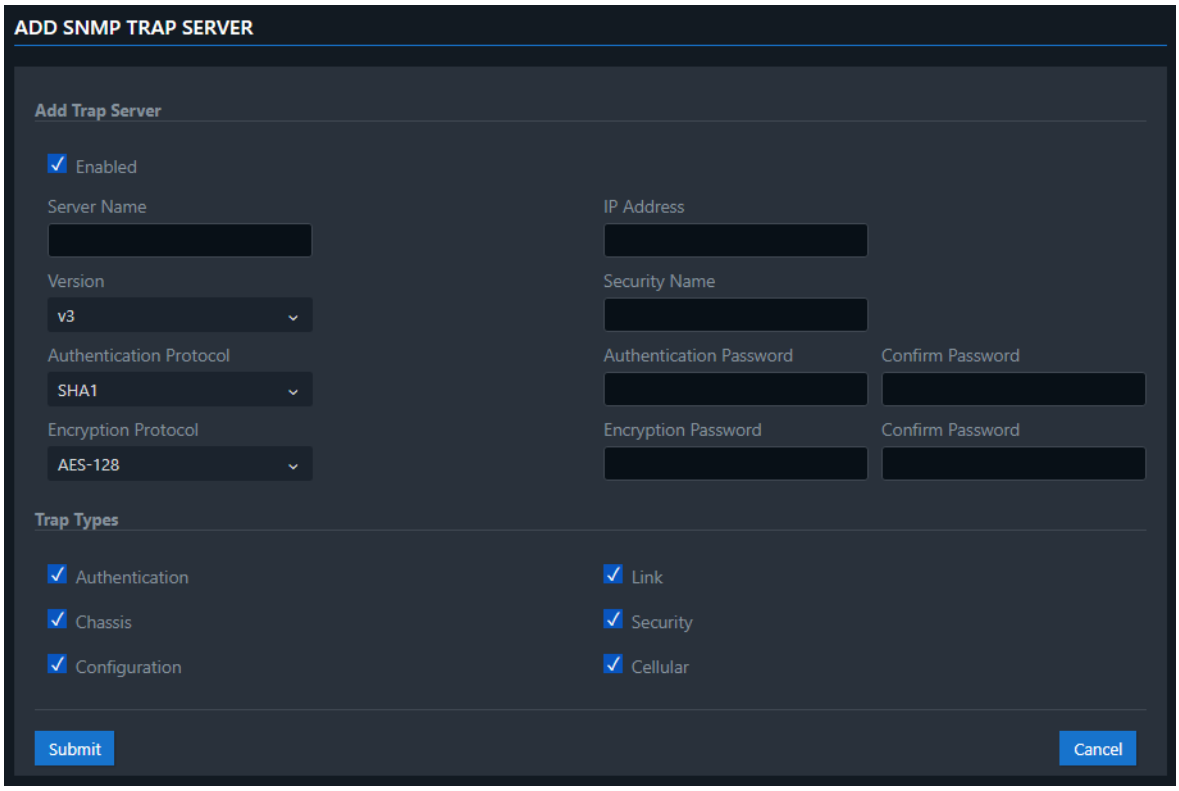


Figure 11.4 Add SNMP Trap Server

Table 11.2 SNMP Version v1 and v2c Trap Server Setting

Setting Name	Value	Default	Description
Enabled	Enabled or Disabled	Enabled	Enable or disable SNMP v1 and v2c trap server.
Server Name	Alphanumeric characters, dashes, underscores, and spaces are acceptable. Maximum 31 characters.	[Empty]	SNMP trap server name.
Version	v1 or v2c	v1	The version of SNMP protocol.
IP Address	Unicast address	[Empty]	The IP address of the server.
Community String	Alphanumeric characters, dashes, underscores, and spaces are acceptable. Maximum 128 characters.	[Empty]	The community string that the SNMP protocol uses.
Trap Types	Authentication, Chassis, Configuration, Link, Security, and Cellular	All trap types are selected.	Each type has a set of traps. You can find the list of traps for each type in the MIB files or *Appendix F: Notifications and Alarms List*. Once a type is enabled, the list of traps in the type will be sent by the device.

For v3, the SNMP trap server settings require authentication protocols, authentication credentials, encryption protocols, and encryption credentials, as shown in *Table 11.3*.

Table 11.3 SNMP Version v3 Trap Server Settings

Setting Name	Value	Default	Description
Enabled	Enabled or Disabled	Enabled	Enable or disable SNMP v3 trap server.
Server Name	Alphanumeric characters, dashes, underscores, and spaces are acceptable. Maximum 31 characters.	[Empty]	SNMP trap server name.
Version	v3	v3	The version of SNMP protocol.
IP Address	Unicast address	[Empty]	The IP address of the server.
Security Name	Alphanumeric characters, dashes, underscores, and spaces are acceptable. Maximum 31 characters.	[Empty]	User security name.
Trap Types	Authentication, Chassis, Configuration, Link, Security, and Cellular	All trap types are selected.	Each type includes a set of traps (events), see *Appendix F: Notifications and Alarms List* for details. Once a type is enabled, the list of traps in the type will be sent by the device.
Authentication Protocol	None, MD5, or SHA1	None	List of authentication protocols.
Authentication Password	Alphanumeric characters, dashes, underscores, and spaces are acceptable. Maximum 250 characters.	[Empty]	If an authentication protocol is selected, a password is required.
Encryption Protocol	None, Des, or AES-128	None	List of encryption protocols.
Encryption Password	Alphanumeric characters, dashes, underscores, and spaces are acceptable. Maximum 250 characters.	[Empty]	If an encryption protocol is selected, a password is required.

APPENDIX A

Firmware and Manual Versions

Firmware

Determining the Firmware Version

To determine the firmware version, navigate to the Dashboard page. The Firmware Identification (FID) number is shown under the Device Information heading, as shown in *Figure A.1*.

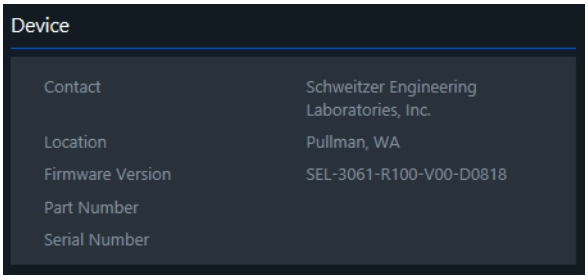


Figure A.1 Firmware Version

The firmware version number is after the R. For example, the following is firmware version number R100, release date August 2018.

FID=SEL-3061-**R100**-V00-D0818

The release date is after the D. For example, the following is firmware version number R100, release date August 2018.

FID=SEL-3061-R100-V00-D**0818**

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.

Table A.1 Firmware Revision History

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-3061-R101-V00-D1118	➤ Added SNMP. ➤ Modified X.509 to accept any CA and intermediate CA signed certificate. ➤ Removed APN name field in the dashboard for Verizon units. ➤ Increased DHCP lease time for PPP-Passthrough mode.	20181128
SEL-3061-R100-V00-D0818	➤ Initial version.	20180831

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

Date Code	Summary of Revisions
20210715	Section 1 ➤ Updated *EMC Emissions* in *Specifications*.
20191217	Section 1 ➤ Updated *Overview* and *Options* for Canadian networks. Section 2 ➤ Updated *Installation* and *Options* for U.S. and networks. Section 6 ➤ Updated *Table 6.2: IP Pipe Settings in Server and Client Mode*. Section 7 ➤ Updated *Table 7.2: Port Forwarding Settings*. Section 8 ➤ Updated *Table 8.1: Syslog Destination Settings*. Section 10 ➤ Updated *Job Done Example 1: Setting Up an IPsec VPN Between Two SEL-3061 Routers*. ➤ Updated *Figure 10.2: Router A Tunnel Settings, Figure 10.3: Router B Tunnel Settings*, *Figure 10.6: Router A and Router B Filter Rule*, and *Figure 10.10: Serial Cable Replacement Example*.
20181128	➤ Added *Section 11: SNMP*. ➤ Added *Appendix F: Notifications and Alarms List*. Section 1 ➤ Updated *Specifications*. Section 5 ➤ Updated *X.509*. Appendix D ➤ Updated *Figure D.4: Digital Signatures*.
20180831	➤ Initial version.

APPENDIX B

Firmware Upgrade Instructions

Overview

These instructions guide you through the process of upgrading the firmware in the SEL-3061. Note that these instructions are only intended for upgrading firmware from an older revision to a newer revision. Downgrading firmware—going from a newer to an older revision—should not be attempted. Please contact SEL if you need to downgrade the firmware.

A standard release is identified by a change in the R-number of the device firmware identification (FID) number.

Existing firmware:

FID=SEL-3061-**R100**-V00-Dxxxx

Standard release firmware:

FID=SEL-3061-**R101**-V00-Dxxxx

The release date is after the D. For example, the following is firmware version number R100, release date August 2018.

FID=SEL-3061-R100-V00-**D0818**

Introduction

SEL occasionally offers firmware upgrades to improve the performance of your device. The SEL-3061 stores firmware in nonvolatile memory. Opening the case or changing physical components is not necessary. These instructions give a step-by-step procedure to upgrade the device firmware by uploading a file from a personal computer to the device via the web interface. Firmware releases are enhancements to improve functionality that change the way your device is configured or maintained.

Determine the existing firmware by opening the web interface Dashboard and looking in the Device section, as shown in *Figure B.1*

Figure B.1 Example Device Pane of Dashboard Showing Firmware Version

Upgrade Procedure

These instructions provide a step-by-step procedure for upgrading the SEL-3061 firmware by uploading a firmware file from a personal computer via the web interface, and the common procedure to use the File Management interface to select and transfer firmware to the SEL-3061.

Firmware Files

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

The SEL-3061 firmware upgrade files have a .bin file extension.

An example firmware file name is SEL_3061_v101.bin.

Export Existing Settings

The firmware upgrade procedure is designed to retain user configuration, including user accounts, time zone selection, and Syslog entries. As a precaution, SEL recommends exporting the existing SEL-3061 settings prior to commencing a firmware upgrade, in case of unforeseen circumstances that cause settings loss.

To export settings, navigate to the **Configuration > File Management > File Transfer > Settings page**, and select **Export Settings**. To export the Local Syslog, navigate to the **Diagnostics > Local Syslog Events** page, and select **Export**.

Perform the Upgrade

Step 1. Access the SEL-3061 Firmware Upgrade page by navigating to **Configuration > File Management > Firmware Upgrade** on the SEL-3061 web interface, as shown in *Figure B.2*.

Step 2. Select **Choose File** and navigate to the location where the firmware file is stored. Select the file and select **Open**.

Step 3. Select **Start Upgrade** to upload and install the new firmware. The firmware upgrade process takes less than 10 minutes.

Step 4. Manually refresh your browser if the Login screen does not automatically appear after 10 minutes.

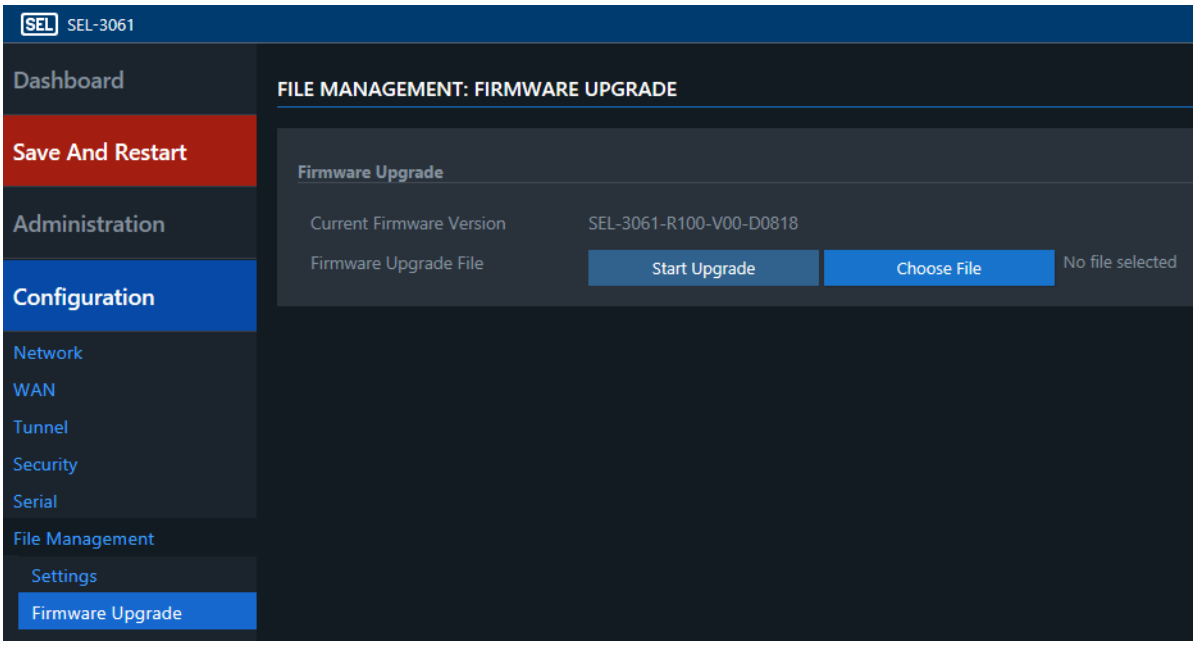


Figure B.2 Firmware Upgrade Page

This page intentionally left blank

APPENDIX C

Syslog

Introduction

The Syslog Protocol, defined in RFC 3164, provides a transport mechanism by which an SEL-3061 can send system event notification messages across 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 C.1*) is a number that indicates message importance.

Table C.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 C.2*) defines the application group from which the message originated.

Table C.2 Syslog Message Facilities (Sheet 1 of 2)

Numerical Code	Facility
0	Kernel messages
1	User-level messages
2	Mail system
3	System daemons

Table C.2 Syslog Message Facilities (Sheet 2 of 2)

Numerical Code	Facility
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.

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 C.3*.

Table C.3 Example 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 C.1*, remote devices are configured to send Syslog messages to the remote Syslog server through use of a secure network or a nonsecure network with a 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.

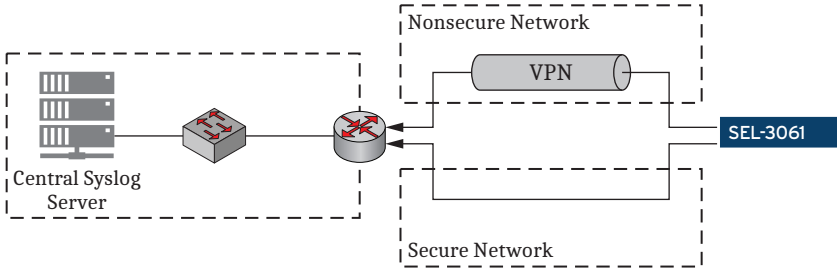


Figure C.1 Central Syslog Server

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 (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-3061 Event Logs

The SEL-3061 records and time-stamps all events in the Syslog format consistent with the Syslog description from RFC 3164. *Table C.4* lists all of the events that the SEL-3061 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-3061 replaces with the value being logged. For example, the SEL-3061 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 C.4 Event Logs (Sheet 1 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
Failure: Flash	Diagnostics	Alert	System	Major	—
Failure: RAM	Diagnostics	Alert	System	Major	—
Failure: STC	Diagnostics	Critical	System	Major	—

Table C.4 Event Logs (Sheet 2 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
Failure: Internal Clock Battery	Diagnostics	Warning	System	Minor	—
OK: Power Supply	Diagnostics	Error	System	Minor	—
OK: Internal Clock Battery	Diagnostics	Error	System	Minor	—
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
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
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
RADIUS authentication enabled by {username} at {user_ip}	RADIUSConfig	Notice	Security	Minor	Configuration
RADIUS authentication disabled by {username} at {user_ip}	RADIUSConfig	Warning	Security	Minor	Configuration
RADIUS accounting enabled by {username} at {user_ip}	RADIUSConfig	Notice	Security	Minor	Configuration
RADIUS accounting disabled by {username} at {user_ip}	RADIUSConfig	Warning	Security	Minor	Configuration
RADIUS authentication settings changed by {username} at {user_ip}	RADIUSConfig	Notice	Security	Minor	Configuration
RADIUS accounting settings changed by {username} at {user_ip}	RADIUSConfig	Warning	Security	Minor	Configuration
RADIUS Authentication Connection: Requested time out	RADIUS	Error	Security	Minor	Authorization
RADIUS Authentication Connection: Active server changed to server {0}	RADIUS	Error	Security	Minor	Authorization
RADIUS Authentication Server {0} Authorization: Access-Accept does not contain SEL-User-Role attribute for {username}	RADIUS	Error	Security	Minor	Authorization
RADIUS Authentication Server {0} Authorization: Access-Accept received with invalid SEL-User-Role attribute for {username}	RADIUS	Error	Security	Minor	Authorization
RADIUS Authentication Server {0} X.509: certificate does not match the server name or address	RADIUS	Error	Security	Minor	Authorization
RADIUS Authentication Server {0} X.509: unknown or untrusted certificate authority	RADIUS	Error	Security	Minor	Authorization
RADIUS Authentication Server {0} X.509: certificate is expired or it is not yet valid	RADIUS	Error	Security	Minor	Authorization
RADIUS Accounting Connection: Accounting server does not respond	RADIUS	Error	Security	Minor	Authorization
RADIUS Accounting Connection: Active server changed to server {0}	RADIUS	Error	Security	Minor	Authorization
Web Server HTTPS via WAN enabled by {username} at {user_ip}	AccessConfig	Warning	Security	Minor	Configuration

Table C.4 Event Logs (Sheet 3 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
Web Server HTTPS via WAN disabled by {username} at {user_ip}	AccessConfig	Notice	User	None	Configuration
Web Server HTTPS via LAN changed by {username} at {user_ip}	AccessConfig	Notice	User	None	Configuration
SSH enabled by {username} at {user_ip}	AccessConfig	Notice	Security	None	Configuration
SSH disabled by {username} at {user_ip}	AccessConfig	Notice	User	None	Configuration
SSH via WAN enabled by {username} at {user_ip}	AccessConfig	Warning	Security	Minor	Configuration
SSH via WAN disabled by {username} at {user_ip}	AccessConfig	Notice	User	None	Configuration
SSH via LAN changed by {username} at {user_ip}	AccessConfig	Notice	User	None	Configuration
ICMP enabled by {username} at {user_ip}	AccessConfig	Notice	Security	None	Configuration
ICMP disabled by {username} at {user_ip}	AccessConfig	Notice	User	None	Configuration
ICMP respond to WAN enabled by {username} at {user_ip}	AccessConfig	Warning	Security	Minor	Configuration
ICMP respond to WAN disabled by {username} at {user_ip}	AccessConfig	Notice	User	None	Configuration
ICMP respond to LAN changed by {username} at {user_ip}	AccessConfig	Notice	User	None	Configuration
IP Defense settings changed by {username} at {user_ip}	AccessConfig	Notice	Security	None	Configuration
Device commissioned by {0} at {user_ip}	Commissioning	Notice	Security	None	—
Usage Policy: changed by {username} at {user_ip}	Config	Notice	Security	Minor	Configuration
System Contact Information: changed by {username} at {user_ip}	Config	Notice	Security	Minor	Configuration
Session timeout changed by {username} at {user_ip}	GlobalConfig	Notice	User	None	Configuration
Save timeout changed by {username} at {user_ip}	GlobalConfig	Notice	User	None	Configuration
Save data limit changed by {username} at {user_ip}	GlobalConfig	Notice	User	None	Configuration
Cellular history statistics deleted by {username} at {user_ip}	GlobalConfig	Warning	User	None	Configuration
Ethernet history statistics deleted by {username} at {user_ip}	GlobalConfig	Warning	User	None	Configuration
VPN history statistics deleted by {username} at {user_ip}	GlobalConfig	Warning	User	None	Configuration
Serial port history statistics deleted by {username} at {user_ip}	GlobalConfig	Warning	User	None	Configuration
Local Time Settings: Changed by {username} at {user_ip}	DateTimeConfig	Notice	User	None	Configuration
NTP Server Settings Changed by {username} at {user_ip}	NTPServerConfig	Notice	User	None	Configuration
NTP Server: Disabled by {username} at {user_ip}	NTPServerConfig	Notice	User	None	Configuration
NTP Server: Enabled by {username} at {user_ip}	NTPServerConfig	Notice	User	None	Configuration
Device factory reset initiated through pinhole button	PushbuttonReset	Notice	User	Minor	Chassis
Device reboot initiated through pinhole button	PushbuttonReset	Notice	User	Minor	Chassis
Device factory reset initiated by {username} at {user_ip}	Commissioning	Notice	Security	None	—
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
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
Syslog Settings changed by {username} at {user_ip}	SyslogConfig	Notice	USER	Minor	Configuration

Table C.4 Event Logs (Sheet 4 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
Local Syslog Event Queue contains >= 90% unacknowledged events	Syslog	Critical	System	None	—
Local Syslog Event Queue contains <= 65% unacknowledged events	Syslog	Notice	System	None	—
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	—
The {0} event queue overflowed	Syslog	Critical	System	None	—
The {0} event queue left the overflow condition. Approximately {1} events were lost	Syslog	Notice	System	None	—
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 Server {0} added by {username} at {user_ip}	SNMPConfig	Notice	USER	Minor	Configuration
SNMP Server {0} modified by {username} at {user_ip}	SNMPConfig	Notice	USER	Minor	Configuration
SNMP Server {0} removed by {username} at {user_ip}	SNMPConfig	Notice	USER	Minor	Configuration
SNMP Enabled by {username} at {user_ip}	SNMPConfig	Notice	USER	Minor	Configuration
SNMP Disabled by {username} at {user_ip}	SNMPConfig	Notice	USER	Minor	Configuration
SNMP Via LAN changed by {username} at {user_ip}	SNMPConfig	Notice	USER	Minor	Configuration
SNMP Via WAN enabled by {username} at {user_ip}	SNMPConfig	Notice	USER	Minor	Configuration
SNMP Via WAN Disabled by {username} at {user_ip}	SNMPConfig	Notice	USER	Minor	Configuration
Event notification {0} enabled by {username} at {user_ip}	NotificationConfig	Notice	USER	Minor	Configuration
Event notification {0} disabled by {username} at {user_ip}	NotificationConfig	Notice	USER	Minor	Configuration
Recipient group {0} added by {username} at {user_ip}	NotificationConfig	Notice	USER	None	Configuration
Recipient group {0} updated by {username} at {user_ip}	NotificationConfig	Notice	USER	None	Configuration
Recipient group {0} deleted by {username} at {user_ip}	NotificationConfig	Notice	USER	None	Configuration
Unable to send notification {0} to group {1}	Notification	Warning	USER	Minor	—
X.509 certificate {0} has expired; communications requiring X.509 based authentication may have stopped	X509Config	Error	System	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}: certificate import failed	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

Table C.4 Event Logs (Sheet 5 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
X.509 certificate generation started by {username} at {user_ip}	X509Config	Notice	Security	Minor	Configuration
X.509 certificate generated completed successfully	X509Config	Notice	Security	Minor	Configuration
X.509 certificate generation failed	X509Config	Notice	Security	Minor	Configuration
Network Interface Settings: changed by {username} at {user_ip}	NetworkConfig	Notice	User	Minor	Configuration
DNS settings changed by {username} at {user_ip}	NetworkConfig	Notice	User	None	Configuration
DDNS settings changed by {username} at {user_ip}	NetworkConfig	Notice	User	None	Configuration
DDNS enabled by {username} at {user_ip}	NetworkConfig	Notice	User	None	Configuration
DDNS disabled by {username} at {user_ip}	NetworkConfig	Notice	User	None	Configuration
DNS Server cannot be acquired	Network	Warning	User	None	—
DNS Server {0} acquired	Network	Notice	User	None	—
DHCP settings changed by {username} at {user_ip}	NetworkConfig	Notice	User	None	Configuration
DHCP enabled by {username} at {user_ip}	NetworkConfig	Notice	User	None	Configuration
DHCP disabled by {username} at {user_ip}	NetworkConfig	Notice	User	None	Configuration
Cellular configuration enabled by {username} at {user_ip}	CellularConfig	Notice	User	None	Configuration
Cellular configuration disabled by {username} at {user_ip}	CellularConfig	Notice	User	None	Configuration
Cellular configuration setting changed	CellularConfig	Notice	User	None	Configuration
SIM PIN changed by {username} at {user_ip}	CellularConfig	Warning	Security	Minor	Configuration
APN changed by {username} at {user_ip}	CellularConfig	Warning	Security	None	Configuration
Cellular authentication settings changed by {username} at {user_ip}	CellularConfig	Notice	User	None	Configuration
Cellular keep alive enabled	CellularConfig	Notice	User	None	Configuration
Cellular keep alive disabled	CellularConfig	Notice	User	None	Configuration
Cellular keep alive settings changed	CellularConfig	Notice	User	None	Configuration
Cellular data receive monitor enabled	CellularConfig	Notice	User	None	Configuration
Cellular data receive monitor disabled	CellularConfig	Notice	User	None	Configuration
SIM card inserted	SIM	Warning	System	Minor	—
SIM card removed	SIM	Warning	System	Minor	—
APN is not present	Cellular	Warning	System	None	—
APN invalid	Cellular	Warning	System	None	—
Cellular PPP authentication failed	Cellular	Warning	System	Minor	—
Cellular PPP authentication completed successfully	Cellular	Warning	System	Minor	—
Cellular PPP link is up	Cellular	Warning	System	Minor	—
Cellular keep alive failed	Cellular	Warning	System	Minor	—
Cellular wakeup on call enabled by {username} at {user_ip}	CellularConfig	Notice	User	None	Configuration
Cellular wakeup on call disabled by {username} at {user_ip}	CellularConfig	Notice	User	None	Configuration
Cellular dial on demand LAN enabled by {username} at {user_ip}	CellularConfig	Notice	User	None	Configuration
Cellular dial on demand LAN disabled by {username} at {user_ip}	CellularConfig	Notice	User	None	Configuration

Table C.4 Event Logs (Sheet 6 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
Cellular wakeup settings changed by {username} at {user_ip}	CellularConfig	Notice	User	None	Configuration
Cellular wakeup on call failed	Cellular	Warning	System	Minor	—
VPN {0} created by {username} at {user_ip}	VPNConfig	Warning	Security	Minor	Configuration
VPN {0} settings updated by {username} at {user_ip}	VPNConfig	Warning	Security	Minor	Configuration
VPN {0} deleted by {username} at {user_ip}	VPNConfig	Warning	Security	Minor	Configuration
VPN {0} GRE Remote WAN IP changed by {username} at {user_ip}	VPNConfig	Warning	Security	Minor	Configuration
VPN {0} GRE Remote Network changed by {username} at {user_ip}	VPNConfig	Warning	Security	Minor	Configuration
VPN {0} IPSec Remote WAN IP changed by {username} at {user_ip}	VPNConfig	Warning	Security	Minor	Configuration
VPN {0} IPSec Remote Network changed by {username} at {user_ip}	VPNConfig	Warning	Security	Minor	Configuration
VPN {0} IPSec Tunnel Type changed by {username} at {user_ip}	VPNConfig	Warning	Security	Minor	Configuration
VPN {0} IPSec Pre-Shared Key changed by {username} at {user_ip}	VPNConfig	Warning	Security	Minor	Configuration
VPN {0} IPSec Authentication changed by {username} at {user_ip}	VPNConfig	Warning	Security	Minor	Configuration
VPN {0} IPSec Encryption changed by {username} at {user_ip}	VPNConfig	Warning	Security	Minor	Configuration
VPN {0} IPSec Advanced Settings changed by {username} at {user_ip}	VPNConfig	Warning	Security	Minor	Configuration
VPN {0} link is up	VPN	Warning	System	Minor	—
VPN {0} link is down	VPN	Warning	System	Minor	—
Firewall static route {0} added by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall static route {0} updated by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall static route {0} deleted by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall port forwarding {0} added by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall port forwarding {0} updated by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall port forwarding {0} deleted by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall port outbound {0} added by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall port outbound {0} updated by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall port outbound {0} deleted by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall MAC filtering {0} added by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall MAC filtering {0} updated by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall MAC filtering {0} deleted by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration

Table C.4 Event Logs (Sheet 7 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
Firewall prerouting rules (DNAT) {0} added by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall prerouting rules (DNAT) {0} updated by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall prerouting rules (DNAT) {0} deleted by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall port filtering {0} added by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall port filtering {0} updated by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall port filtering {0} deleted by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall postrouting rules (SNAT) {0} added by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall postrouting rules (SNAT) {0} updated by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
Firewall postrouting rules (SNAT) {0} deleted by {username} at {user_ip}	FirewallConfig	Warning	Security	Minor	Configuration
{Protocol} packet from {source_ip}:{source_port} to {destination_ip}:{destination_port} dropped	Firewall	Notice	System	None	—
{Protocol} packet from {source_ip}:{source_port} to {destination_ip}:{destination_port} rejected	Firewall	Notice	System	None	—
{Protocol} packet from {source_ip}:{source_port} to {destination_ip}:{destination_port} established	Firewall	Notice	System	None	—
{Protocol} packet from {source_ip}:{source_port} to {destination_ip}:{destination_port} terminated	Firewall	Notice	System	None	—
{count} connection/connections established	Firewall	Notice	System	None	—
{count} connection/connections terminated	Firewall	Notice	System	None	—
{count} packet/packets dropped	Firewall	Notice	System	None	—
{count} packet/packets rejected	Firewall	Notice	System	None	—
Trusted Ips inbound enabled by {username} at {user_ip}	TruestedConfig	Warning	Security	Minor	Configuration
Trusted Ips inbound disabled by {username} at {user_ip}	TruestedConfig	Warning	Security	Minor	Configuration
Trusted Ips inbound addresses added by {username} at {user_ip}	TruestedConfig	Warning	Security	Minor	Configuration
Trusted Ips inbound addresses deleted by {username} at {user_ip}	TruestedConfig	Warning	Security	Minor	Configuration
Trusted Ips outbound enabled by {username} at {user_ip}	TruestedConfig	Warning	Security	Minor	Configuration
Trusted Ips outbound disabled by {username} at {user_ip}	TruestedConfig	Warning	Security	Minor	Configuration
Trusted Ips outbound addresses added by {username} at {user_ip}	TruestedConfig	Warning	Security	Minor	Configuration
Trusted Ips outbound addresses deleted by {username} at {user_ip}	TruestedConfig	Warning	Security	Minor	Configuration
Serial port enabled by {username} at {user_ip}	SerialConfig	Notice	User	None	Configuration
Serial port Modbus gateway enabled by {username} at {user_ip}	SerialConfig	Notice	User	None	Configuration
Serial port IP pipe settings changed by {username} at {user_ip}	SerialConfig	Notice	User	None	Configuration

Table C.4 Event Logs (Sheet 8 of 8)

Message	Tag	Severity	Facility	Alarm Category	Alarm Class
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
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
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 import started by {username} at {user_ip}	ImportExport	Notice	User	Minor	Configuration
Configuration file import successful	ImportExport	Notice	User	Minor	Configuration
Configuration file export failed	ImportExport	Warning	User	Minor	Configuration
Configuration file import failed	ImportExport	Warning	User	Minor	Configuration
Ethernet port is disconnected	LinkUpDown	Notice	System	Minor	Link
Ethernet port is connected	LinkUpDown	Notice	System	Minor	Link
SMS enabled by {username} at {user_ip}	SMSConfig	Notice	User	None	Configuration
SMS disabled by {username} at {user_ip}	SMSConfig	Notice	User	None	Configuration
SMS settings changed by {username} at {user_ip}	SMSConfig	Notice	User	None	Configuration
SMS command changed by {username} at {user_ip}	SMSConfig	Notice	User	None	Configuration
SMS security filter password enabled by {username} at {user_ip}	SMSConfig	Notice	User	None	Configuration
SMS security filter password disabled by {username} at {user_ip}	SMSConfig	Notice	User	None	Configuration
SMS security filter whitelist changed by {username} at {user_ip}	SMSConfig	Notice	User	None	Configuration
SMS security filter added number {0} by {username} at {user_ip}	SMSConfig	Notice	User	None	Configuration
SMS security filter deleted number {0} by {username} at {user_ip}	SMSConfig	Notice	User	None	Configuration
SMS message {0} received from receipient {0}	SMSConfig	Notice	User	None	Configuration
SMS message {0} sent to receipient {0}	SMSConfig	Notice	User	None	Configuration
SMS message was unable to send to recipient {0}	SMSConfig	Notice	System	None	—
SMTP enabled by {username} at {user_ip}	SMTPConfig	Notice	User	None	Configuration
SMTP disabled by {username} at {user_ip}	SMTPConfig	Notice	User	None	Configuration
SMTP settings changed by {username} at {user_ip}	SMTPConfig	Notice	User	None	Configuration
SMTP: Email was unable to send to recipient {0}	SMSConfig	Notice	System	None	—
Router settings change reboot by {username} at {user_ip}	Config	Notice	System	None	Configuration

APPENDIX D

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-3061 uses X.509 certificates in the web server for secure device management and for IPsec authentication.

This appendix includes the following:

Symmetric-Key Cryptography

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.

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, as shown in *Figure D.1*. 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.

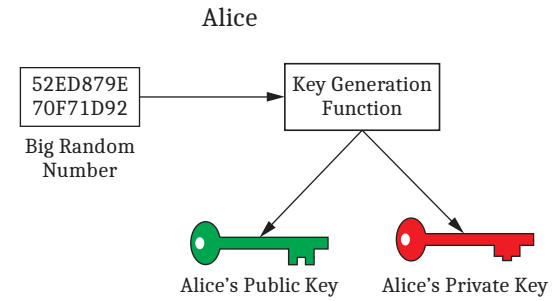


Figure D.1 Asymmetric Keys

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, as shown in *Figure D.2*. 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.

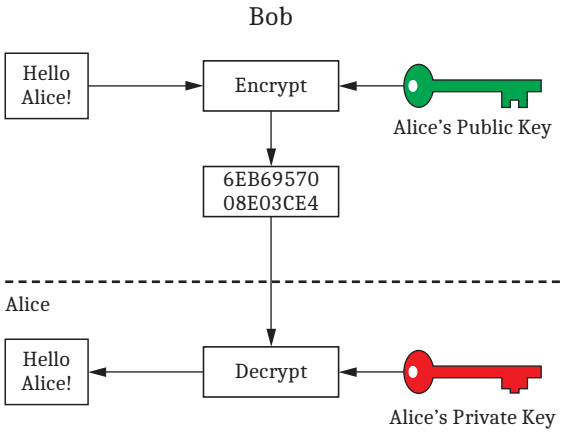


Figure D.2 Confidentiality With Asymmetric Keys

Public-key cryptography requires more computation than symmetric-key cryptography. This makes it infeasible to send large amounts of data, or secure a series of transmissions, by 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 (as shown in *Figure D.3*). The public key you use to decrypt the message will identify the sender. This is known as an electronic signature.

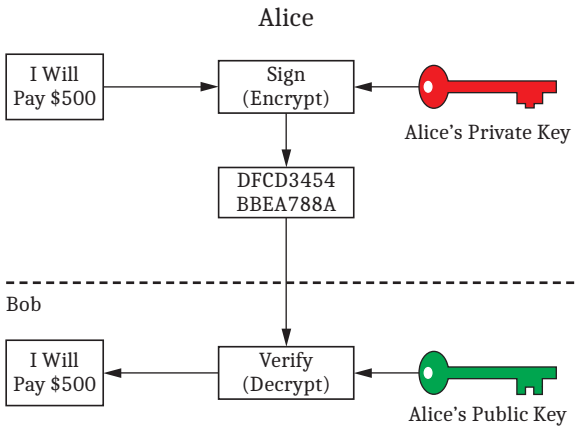


Figure D.3 Authentication With Asymmetric Keys

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 first compute a hash of the data to be signed and then encrypt that hash with the signer's private key. You 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 their own hash of the data and then uses the issuer's public key to decrypt the signature (i.e., the sender's encrypted hash). The two hashes are then compared, and if they match (as shown in *Figure D.4*), the data are verified as authentic.

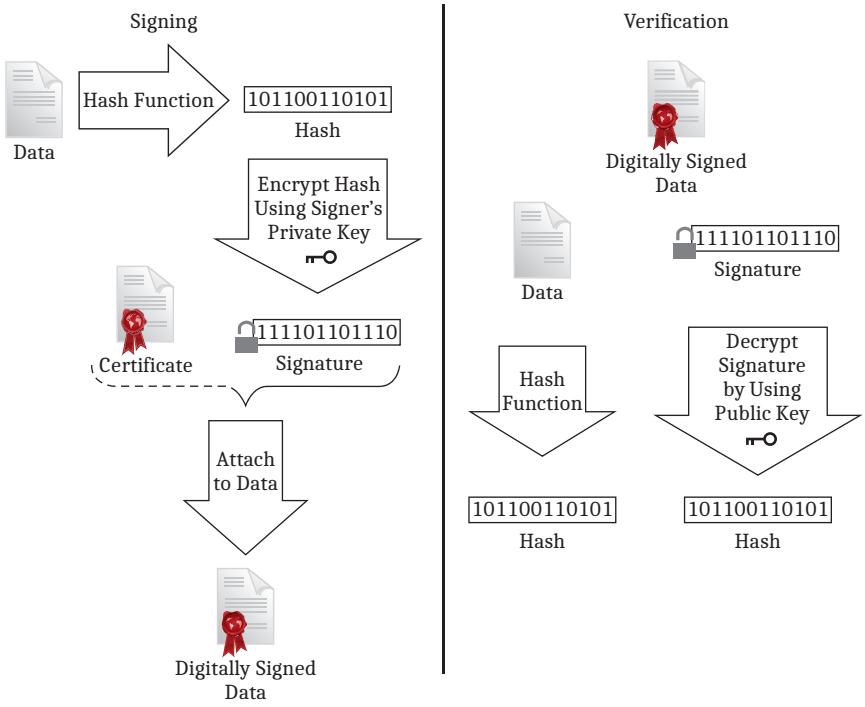


Figure D.4 Digital Signatures

Public-Key Infrastructure

One of three common uses for digital certificates is in a 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 and 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 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." By saying "yes", the CA accepts that the requester is who they claim to be and that 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 D.5* illustrates a simple example of a web of trust. If Alice trusts Bob, and Bob trusts Charlie, then Alice implicitly trusts Charlie.

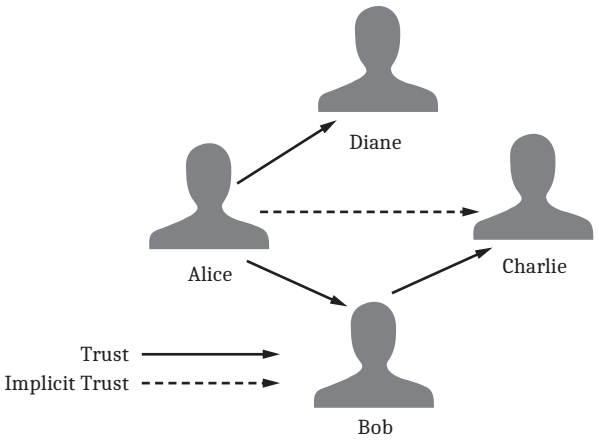


Figure D.5 Web of Trust

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 associated 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
```

This page intentionally left blank

APPENDIX E

SEL RADIUS Dictionary

```
##############################################################################
# COPYRIGHT (C) 2013 SCHWEITZER ENGINEERING LABS, INC., PULLMAN, WASHINGTON
#
# FILE DESCRIPTION: SEL VENDOR SPECIFIC ATTRIBUTES
# VERSION: 2.0
##############################################################################

# This file contains two dictionary formats, one for FreeRadius, and one for the
# RSA RADIUS Server. The settings for the RSA RADIUS Server have been 'commented out'.
# To use this file with the RSA RADIUS Server, comment out the lines between:
# FREERADIUS STARTS HERE and FREERADIUS END, and uncomment the lines between:
# RSA STARTS HERE and RSA END

##############################################################################

# SEL-User-Role is used to assign a device role to a user for device access.
# Valid for Access-Accept messages only.
# SEL RADIUS-supporting devices require at least one authorization attribute per user.
# The predefined authorization values differ for each SEL device.
# Please check the device manual for which of the following authorization roles are accepted:
# Administrator
# Technician
# Engineer
# Monitor
# User Manager

# SEL-Proxy-Group is used to assign proxy groups to a user for accessing managed devices.
# The value of SEL-Proxy-Group should be the name of a proxy group the user is a member of.
# Valid for Access-Accept messages only.
# SEL-Proxy-Group is required only for managed device access.
# Multiple SEL-Proxy-Group attributes may be used.
# Only one proxy group allowed per attribute.

# SEL-Syslog-Message is used to provide user actions on the system.
# The value of SEL-Syslog-Message will be the Syslog message.
# Valid for Accounting-Request messages only.
# Only one SEL-Syslog-Message per message is allowed.
# SEL-Acct-Info is used to provide informational messages.
# The value of SEL-Acct-Info will be a text message.
# Valid for Accounting-Request messages only.
# Only one SEL-Acct-Info per message is allowed.

#-----------------------------------------------------------------------------
# FREERADIUS STARTS HERE
```

```
VENDOR                  Schweitzer-Engineering-Laboratories-Inc.        31823
BEGIN-VENDOR  Schweitzer-Engineering-Laboratories-Inc.

ATTRIBUTE               SEL-User-Role           1                       string
ATTRIBUTE               SEL-Proxy-Group         2                       string
ATTRIBUTE               SEL-Syslog-Message      1                       string
ATTRIBUTE               SEL-Acct-Info           12                      string

END-VENDOR      Schweitzer-Engineering-Laboratories-Inc.

# FREERADIUS END
#-----------------------------------------------------------------------------

# RSA STARTS HERE

# @radius.dct
# MACRO                 SEL-VSA(type,syntax)    26                      [vid=31823 type1=%type%
                                                                        len1=+2 data=%syntax%]
# ATTRIBUTE             SEL-User-Role           SEL-VSA(1, string)      r
# ATTRIBUTE             SEL-Proxy-Group         SEL-VSA(2, string)      r
# ATTRIBUTE             SEL-Syslog-Message      SEL-VSA(11, string)     c
# ATTRIBUTE             SEL-Acct-Info           SEL-VSA(12, string)     c

# RSA END
#-----------------------------------------------------------------------------
```

APPENDIX F

Notifications and Alarms List

Table F.1 Authentication

ID	Description
LockedOut	User account was locked out.
LoginFail	Login attempt to port failed.
LoginLogout	User exited from a port.
LoginSuccess	User successfully logged in to a port.
LoginTimeout	User port session timed out.

Table F.2 Chassis

ID	Description
DeviceInitComplete	Device was successfully booted.
DeviceWebReboot	User restarted the devices from the web interface.
DeviceWithReboot	User restarted the device through the use of the pinhole reset button.
EthernetInterfaceDisconnected	Ethernet interface was disconnected.
ResetWithPinhole	Device reset to factory defaults through the use of the pinhole reset button.

Table F.3 Configuration (Sheet 1 of 3)

ID	Description
APNChange	APN changed.
DateTimeManUpdate	Date or time was manually updated.
DDNSSettingChange	User modified a DDNS setting.
DHCPSettingChange	User modified a DHCP setting.
DNSSettingChange	User modified a DNS setting.
FirewallDNATChange	User updated a DNAT.
FirewallDNATCreate	User added a DNAT.
FirewallDNATDelete	User deleted a DNAT.
FirewallForwardRuleChange	User updated a forwarding rule.
FirewallForwardRuleCreate	User added a forwarding rule.
FirewallForwardRuleDelete	User deleted a forwarding rule.
FirewallInputRuleChange	User updated an input firewall rule.
FirewallInputRuleCreate	User added an input firewall rule.
FirewallInputRuleDelete	User deleted an input firewall rule.
FirewallOutputRuleCreate	User added an output firewall rule.
FirewallOutputRuleDelete	User deleted an output firewall rule.
FirewallOutputRuleChange	User updated an output firewall rule.

Table F.3 Configuration (Sheet 2 of 3)

ID	Description
FirewallSNATChange	User updated a SNAT.
FirewallSNATCreate	User added a SNAT.
FirewallSNATDelete	User deleted a SNAT.
GRETunnelChange	User updated a GRE tunnel.
GRETunnelCreate	User added a GRE tunnel.
GRETunnelDelete	User deleted a GRE tunnel.
IPSecTunnelChange	User updated a IPsec tunnel.
IPSecTunnelCreate	User added a IPsec tunnel.
IPSecTunnelDelete	User deleted a IPsec tunnel.
LANInterfaceChange	User modified the LAN interface.
LocalUserChange	Administrative user modified attributes other than the user-name or password of a local user.
LocalUserCreate	Administrative user added a new local user.
LocalUserDelete	Administrative removed a local user.
LocalUserDisable	Administrative user disabled a local user account.
LocalUserEnable	Administrative user enabled a local user account.
LocalUserPasswordChange	User password was modified.
NTPDisable	NTP settings was disabled.
NTPEnable	NTP server configuration was updated.
RADIUSAdvSettingChange	User modified a RADIUS Advanced settings.
RADIUSAuthTypeChange	User modified Authentication Type.
RADIUSPrimIPChange	User modified RADIUS Primary Server IP or Ports.
RADIUSSecondIPChange	User modified RADIUS Secondary Server IP or Ports.
RADIUSSettingDisable	User disabled RADIUS settings.
RADIUSSettingEnable	User enabled RADIUS setting.
RADIUSShareKeyChange	User modified share key.
SeriaPortSettingChange	User modified a serial port setting.
SetFileExportFail	Setting export failed.
SetFileExportStart	Setting export started.
SetFileExportSuccess	Setting export succeeded.
SetFileImportFail	Setting import started.
SetFileImportStart	Setting import failed.
SetFileImportSuccess	Setting import succeeded.
SMSSettingChange	User modified SMS settings.
SMTPSettingChange	User modified SMTP settings.
SNMPSettingChange	User modified SNMP settings.
SyslogDestChange	Syslog destination setting updated.
SyslogDestCreate	Syslog destination added.
SyslogDestRemove	Syslog destination removed.
SyslogSettingChange	Syslog setting modified, not destination related.
TimezoneUpdate	Time zone configuration updated.

Table F.3 Configuration (Sheet 3 of 3)

ID	Description
X509CertCreate	User generated a X.509 certificate.
X509CertImportFail	Import X.509 certificate failed.
X509CertImportInit	User initiated the importing of an X.509 certificate.
X509CertImportSuccess	User successfully imported an X.509 certificate.
X509CertExpire	A used X.509 certificate expired.
X509CertExpireCritical	A used X.509 certificate is going to expire in <7 days.
X509CertExpireNotice	A used X.509 certificate is going to expire in 90, 45, or 28 days.
X509CertExpireWarning	A used X.509 certificate is going to expire in ≥7 days and <28 days.

Table F.4 Link

ID	Description
CellLinkStateDown	The cellular connection is down.
CellLinkStateUp	The cellular connection is up.
PortLinkStateDown	The Ethernet port lost link.
PortLinkStateUp	The Ethernet port obtained a link status of up.
SIMCardNot Present	SIM card is not present.

Table F.5 Security

ID	Description
HttpsViaWanEnable	HTTPS was enabled via WAN.
ICMPViaWanRespond	ICMP was enabled to respond to WAN.
IPDefenseDisable	IP Defense was disabled.

Table F.6 WAN

ID	Description
WANInterfaceFail	WAN interface failover.
WANIPChange	WAN IP address changed.

This page intentionally left blank

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 U.S.A.
Phone: +1.509.332.1890 • Fax: +1.509.332.7990
selinc.com • info@selinc.com