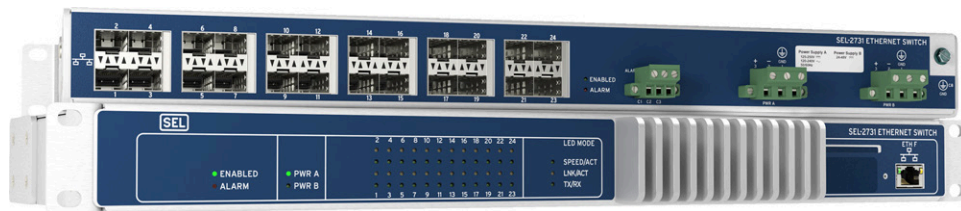


Rapid Spanning Tree Protocol for the SEL Managed Ethernet Switch

User's Guide



20250220

© 2023–2025 Schweitzer Engineering Laboratories, Inc.

Content subject to change without notice. Unless otherwise agreed in writing, all SEL product sales are subject to SEL's terms and conditions located here: <https://selinc.com/company/termsandconditions/>.

Table of Contents

Preface

User's Guide Overview.....	ix
Safety Information.....	ix

Section 1: Introduction and Specifications

Introduction.....	1
Product Overview.....	1
Product Features.....	1
Software System Requirements.....	2
Specifications.....	2

Section 2: Installation

Introduction.....	5
Commissioning.....	5
Device Dashboard.....	6

Section 3: Managing Users

Introduction.....	11
User-Based Accounts.....	11
Centralized User Accounts.....	14

Section 4: Settings and Commands

Introduction.....	27
Reports.....	27
Switch Management.....	29

Appendix A: Firmware and User's Guide Versions

Firmware.....	59
User's Guide.....	60

Appendix B: Firmware Upgrade Instructions

Introduction.....	63
Firmware Upgrade Procedure.....	63
Technical Support.....	64

Appendix C: Syslog

Introduction.....	65
Remote Syslog Servers.....	67
Switch Event Logs.....	67

Appendix D: Cybersecurity Features

Introduction and Security Environment.....	73
Version Information.....	73
Commissioning and Decommissioning.....	73
External Interfaces.....	74
Access Controls.....	74
Logging Features.....	75
Backup and Restore.....	75
Malware Protection Features.....	76
Product Updates.....	76
Contact SEL.....	76

This page intentionally left blank

List of Figures

Figure 2.1 Device Dashboard.....	6
Figure 2.2 Network Interfaces.....	7
Figure 2.3 Version Information.....	8
Figure 2.4 System Statistics.....	8
Figure 2.5 Diagnostics.....	9
Figure 3.1 Add New User Form.....	12
Figure 3.2 Edit Hosts.....	15
Figure 3.3 Host Settings.....	15
Figure 3.4 LDAP Configuration Summary.....	16
Figure 3.5 LDAP Connection Settings.....	17
Figure 3.6 Adding an LDAP Server.....	19
Figure 3.7 Group Mappings Showing a Single Group.....	20
Figure 3.8 Adding a New Role.....	20
Figure 3.9 Selecting a Group From the Tree Display.....	20
Figure 3.10 RADIUS Webpage.....	21
Figure 3.11 RADIUS Protocol Settings.....	22
Figure 3.12 Download Dictionary.....	24
Figure 4.1 Sample Syslog Report.....	28
Figure 4.2 VLAN View.....	30
Figure 4.3 Editing VLAN Settings.....	30
Figure 4.4 Editing a VLAN Within a Range.....	30
Figure 4.5 Port View.....	31
Figure 4.6 RSTP Configuration Page.....	32
Figure 4.7 Root Bridge Notification.....	33
Figure 4.8 Common RSTP Settings.....	34
Figure 4.9 Port RSTP Settings.....	34
Figure 4.10 Port Mirroring.....	38
Figure 4.11 Setting Rate Limiting on the Port Settings Page.....	39
Figure 4.12 Priority Settings Page (Default Settings).....	40
Figure 4.13 SNMP Settings Page.....	43
Figure 4.14 Add v2c Profile.....	44
Figure 4.15 Add v3 Profile.....	45
Figure 4.16 Syslog Settings.....	48
Figure 4.17 Renaming Certificates.....	50
Figure 4.18 Uploading a New X.509 Certificate.....	50
Figure 4.19 Successful Upload of a New X.509 Certificate.....	50
Figure 4.20 New Certificate Is Activated.....	51
Figure 4.21 Alarm Contact Page (Default Settings).....	53
Figure 4.22 Export Settings Page.....	56
Figure 4.23 Diagnostics Report Complete.....	57
Figure 4.24 Import Settings Page.....	57
Figure B.1 File Management.....	63

This page intentionally left blank

List of Tables

Table 2.1	Network Interface Icon Colors.....	7
Table 2.2	System Statistics.....	8
Table 3.1	Edit Hosts Settings.....	15
Table 3.2	General RADIUS Settings.....	22
Table 3.3	Additional Settings for EAP Protocols.....	23
Table 3.4	Configured Servers Settings.....	23
Table 3.5	Additional Request Attributes.....	25
Table 4.1	VLAN Settings.....	29
Table 4.2	RSTP Settings.....	35
Table 4.3	Port Settings.....	35
Table 4.4	STP Mode.....	36
Table 4.5	MAC Security Fields.....	37
Table 4.6	Priority Settings.....	40
Table 4.7	Default PCP-to-Priority Mapping.....	40
Table 4.8	PTP Settings.....	41
Table 4.9	Global IP Settings.....	41
Table 4.10	ETH F Network Interface Settings.....	41
Table 4.11	Mgmt Network Interface Settings ^a	42
Table 4.12	SNMP v2c Profile Settings.....	45
Table 4.13	SNMP v3 Profile Settings.....	45
Table 4.14	Severity Levels.....	48
Table 4.15	Syslog Threshold Values.....	49
Table 4.16	Syslog Destination Settings.....	49
Table 4.17	Web Settings.....	51
Table 4.18	System Contact Information Settings.....	51
Table 4.19	Features.....	51
Table 4.20	Alarm Contact Categories.....	53
Table 4.21	Alarm Contact Behaviors.....	54
Table 4.22	Latch (Automatic Clear) Behavior.....	54
Table 4.23	Pulse Duration Settings ^a	54
Table A.1	SEL-2741 Firmware Revision History.....	60
Table A.2	SEL-2731 Firmware Revision History.....	60
Table A.3	User's Guide Revision History.....	60
Table C.1	Syslog Message Severities Reported by the SEL-2731.....	65
Table C.2	Syslog Message Facilities.....	65
Table C.3	Event Logs.....	67

This page intentionally left blank

Preface

User's Guide Overview

This user's guide describes the functionality and use of the Rapid Spanning Tree Protocol (RSTP) for SEL managed Ethernet switches. It includes information necessary to install, configure, and operate this device.

The following provides an overview of the user's guide layout and the topics that are addressed:

Preface. Describes the user's guide organization and conventions used to present information.

Section 1: Introduction and Specifications. Provides the product features and software system requirements. This section also lists specifications.

Section 2: Installation. Provides information for commissioning RSTP and installing a web certificate. This section also provides an overview of the device Dashboard.

Section 3: Managing Users. Explains how users are managed.

Section 4: Settings and Commands. Lists and describes all the settings and commands for the switch.

Appendix A: Firmware and User's Guide Versions. Lists firmware and user's guide revisions.

Appendix B: Firmware Upgrade Instructions. Provides instructions to update the firmware.

Appendix C: Syslog. Introduces the Syslog Protocol and its uses in SEL switches.

Appendix D: Cybersecurity Features. Describes the various features of the switch that impact cybersecurity.

Safety Information

CAUTION

To ensure proper safety and operation, the equipment ratings, installation instructions, and operating instructions must be checked before commissioning or maintenance of the equipment. The integrity of any protective conductor connection must be checked before carrying out any other actions. It is the responsibility of the user to ensure that the equipment is installed, operated, and used for its intended function in the manner specified in this manual. If misused, any safety protection provided by the equipment may be impaired.

Dangers, Warnings, and Cautions

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

DANGER

Indicates a potentially 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 Marks

The following statements apply to this device.

Table 1 Other Safety Marks

 WARNING Use of this equipment in a manner other than specified in this manual can impair operator safety safeguards provided by this equipment.	 WARNING 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.	 WARNING Seules des personnes qualifiées peuvent travailler sur cet appareil. Si vous n'êtes pas qualifiés pour ce travail, vous pourriez vous blesser avec d'autres personnes ou endommager l'équipement.
 WARNING Do not perform any procedures or adjustments that this instruction manual does not describe.	 WARNING Ne pas appliquer une procédure ou un ajustement qui n'est pas décrit explicitement dans ce manuel d'instruction.
 CAUTION In order to avoid losing system logs on a factory-default reset, configure the SEL-2731 to forward Syslog messages.	 CAUTION Pour éviter de perdre les enregistrements du système sur un redémarrage défini par défaut, configurer le SEL-2731 pour envoyer les messages de l'enregistreur du système ("Syslog").

General Information

Copyrighted Software

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

Legal Department
GPL Compliance
Schweitzer Engineering Laboratories, Inc.
One Schweitzer Drive
Pullman, WA 99163-5603 U.S.A.

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

Technical Support

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

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

This page intentionally left blank

Introduction and Specifications

Introduction

This section includes the following information about the SEL's Rapid Spanning Tree Protocol (RSTP) managed switch firmware:

- *Product Overview on page 1*
- *Product Features on page 1*
- *Software System Requirements on page 2*
- *Specifications on page 2*

Product Overview

SEL's RSTP managed switch firmware is optimized for operational technology (OT) environments commonly found in the energy and utility industries. This managed switch technology supports critical infrastructure applications like IEC 61850, protection-class Ethernet networks, engineering access, supervisory control and data acquisition (SCADA), and process control systems (PCS). This firmware is designed for extended product life cycles and very high reliability, and is backed by a ten-year warranty, customer support, and dedication to quality.

Product Features

- **Rapid Spanning Tree Protocol.** Use IEEE 802.1Q-2014 RSTP to prevent network loops and perform network healing for redundancy after a topology change, such as a link loss.
- **Ease-of-Use.** Simplify configuration and maintenance with a secure web interface that provides convenient setup and management.
- **IEEE 1588 PTP Transparent Clock.** Use an IEEE 1588-2008 compliant PTP Transparent Clock (TC) to allow high-accuracy network synchronization using IEEE C37.238-2017 Power Profile.
- **Virtual Local Area Networks (VLANs).** Segregate traffic and improve network organization and performance. Take advantage of IEEE 802.1Q-2014 VLANs to separate traffic with as many as 4094 LANs.
- **Traffic Prioritization.** Support critical substation messaging by classifying and prioritizing traffic into one of four priority levels through VLAN-based 802.1Q-2014 Class of Service (CoS).
- **Bridge Protocol Data Unit (BPDU) Guard.** Improve network robustness by enabling BPDU Guard to disable a port when unexpected BPDUs are received.
- **Multicast MAC Filtering.** Filter multicast traffic to reduce the network load on end devices.

- **Port Rate Limiting.** Prevent network storms from disabling your network by configuring maximum allowed rates for ingress (incoming) or egress (outgoing) traffic on each port.
- **Selectable Port Mode.** Optimize each port for the best network integration with learning or fast port for edge connections.
- **MAC-Based Port Security.** Limit network access to authorized devices.
- **MAC Address Table.** Use SNMP to view the MAC table or download a comma-separated value table of MAC addresses. Use the table for troubleshooting and locating devices on the network.
- **Time Synchronization.** Synchronize time by using network time protocol (NTP). Time-align events and user activity across your system.
- **Syslog.** Log events for speedy alerts, consistency, compatibility, and centralized collection. Use the switch to forward Syslog system and security logs to as many as three central servers.
- **Dynamic Host Configuration Protocol (DHCP).** Easily connect a laptop computer during initial setup by using settings that enable the front-panel 100/1000BASE-T Ethernet port to function as a DHCP server.
- **Security and Monitoring.** Use SNMPv3 and HTTPS for secure configuration and monitoring. SNMPv3 provides secure network management and is interoperable with existing network management systems (NMS). An HTTPS web interface provides secure and intuitive switch management.
- **Alarm Contact.** Map system and security events to configurable alarm contact behavior for alarming through an external system, such as an existing SCADA network.
- **Port Mirroring.** Monitor selectable ingress and egress traffic for viewing network statistics and performing troubleshooting.
- **Port Monitoring.** Monitor port and link health to protect the network from impacts caused by link flapping and frame check sequence cyclical redundancy check (CRC) errors.
- **Device and Network Monitoring.** Monitor diagnostics and health of the network through the use of standards-based SNMP MIBs.
- **User-Based Accounts.** Provide user accountability and separate authorization levels for configuration and maintenance. Use LDAP or RADIUS with two-factor authentication for centralized user authentication.

Software System Requirements

Engineering access is managed through the internal HTTPS server. This requires a web browser capable of HTTPS communications. The recommended browsers are Google Chrome, Mozilla Firefox, and Microsoft Edge.

Specifications

Compliance

Designed and manufactured under an ISO 9001 certified quality management system

General

Switching Properties

Switching Method:	Store and Forward
Switching Latency:	<15 μ s
Switch Fabric Throughput:	Model dependent
Priority Queues:	4
Maximum VLANs:	4094
MAC Learning Architecture:	Shared VLAN Learning (SVL)
VLAN ID Range:	1–4094
MAC Address Table Size:	8192 addresses

Warranty

10 years

Network Management

HTTPS Web User Interface

SNMP v2c/v3

Settings Import/Export

User-Based Accounts

Maximum Local Accounts:	256
Password Length:	8–72 characters
Password Set:	All printable ASCII characters
User Roles:	Administrator, Engineer, User Manager, Monitor
Central User Account Management	LDAP RADIUS

Syslog

Storage for 60,000 local Syslog messages.

Support for three remote Syslog destinations.

Standard

IEEE 802.3-2012

IEEE 802.3-2012 excluding 10 Gbps and above

IEEE 802.3-2008/Cor 1

IEEE 802.3bd

IEEE 802.3bf

IEEE 802.1q-2014

IEC 61850-90-4

This page intentionally left blank

Installation

Introduction

This section includes the following information:

- *Commissioning on page 5*
- *Device Dashboard on page 6*

Commissioning

The switch is commissioned through the front port. The front port is enabled by default and has an IP address of 192.168.1.2 and a subnet mask of /24. To access this static address, configure your computer to be on the same subnet, use a standard RJ45 Ethernet cable connected between your computer and the switch, and then navigate to the switch using your preferred browser. If setting your computer to a static address is not desired, the front port also has a captive portal feature. This feature allows you to set your computer's network interface to DHCP and the SEL switch will lease an address to the computer. Simply open a browser and navigate to 192.168.1.2. A factory-default switch comes configured with a self-signed certificate. This may cause your browser to issue a security warning; please follow the browser instructions on how to proceed and connect. This web server certificate can be replaced by a trusted certificate from your organization by using the certificate management settings (see *Installing a New Web Certificate on page 50*).

When connecting for the first time, the switch will present a screen to configure the administrative user. Enter a desired username and password for this local account. The password must have at least eight characters and at least one uppercase letter, one lowercase letter, one number, and one special character. Once this account is created, the switch will return to the login screen and you can log in to the device using the newly created administrative user.

SEL

Device Commissioning

No users have been configured for this device. Please set up this device's Administrator account.

Administrator Username:

Administrator Password:

Confirm Password

Web Access For Authorized Personnel Only

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 monitoring to law enforcement officials.

When you log in, the left frame of the device web interface is the navigation panel. Selecting any link on this panel will take you to the associated page that includes the settings and configurations for that part of the system. The navigation panel is always present on the web interface.

Device Dashboard

The device Dashboard is displayed when a user logs in to the device. The Dashboard provides a quick overview of the state of the device. To access the Dashboard from another device webpage, select the **Dashboard** link on the left navigation panel.

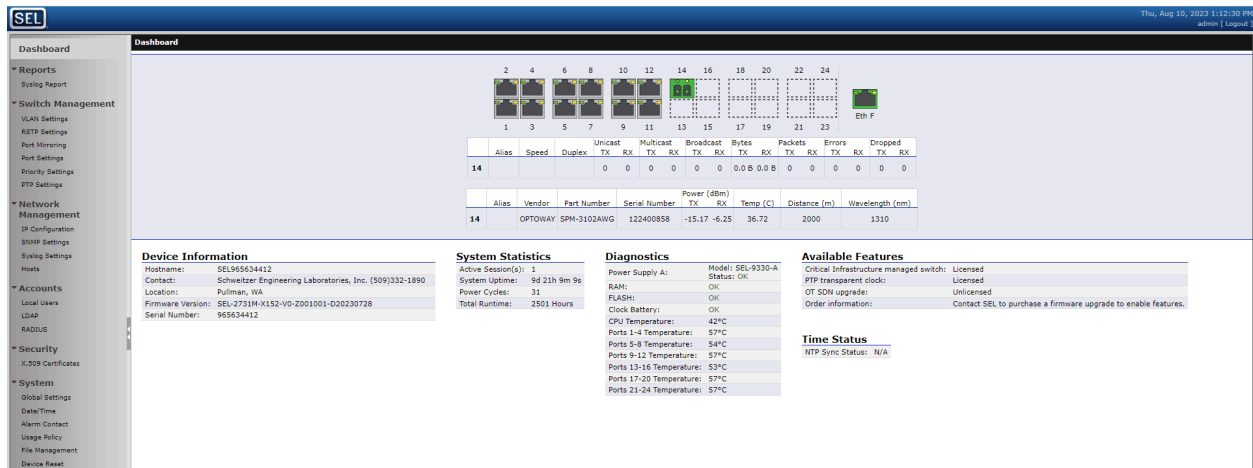


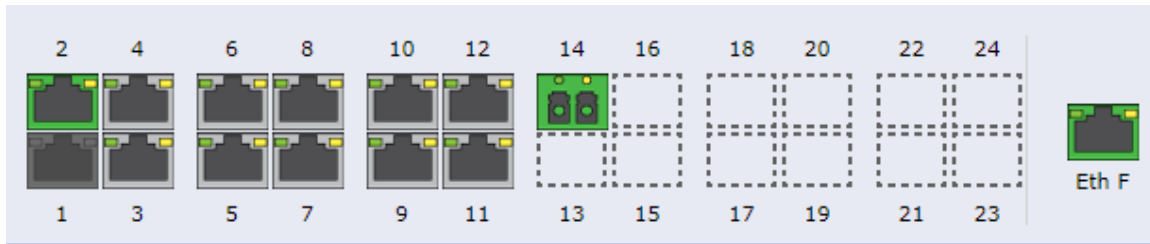
Figure 2.1 Device Dashboard

The system status and statistics information on the **Dashboard** page is updated periodically. The dashboard is broken into the following six categories:

- Network Interfaces
- Device Information
- System Statistics
- Diagnostics
- Available Features
- Time Status




Network Interfaces

The Network Interfaces section of the Dashboard contains icons representing each physical Ethernet network interface on the device. You can hover your mouse over any of the network interface port icons to see the alias and current status information of the port. Selecting one of these icons adds a status area to the Dashboard and a line to it containing the statistics for that interface.

**Figure 2.2** Network Interfaces

The network interface icons are color-coded to indicate the configuration state of that interface. The interface icon colors and their meanings can be found in *Table 2.1*.

Table 2.1 Network Interface Icon Colors

Interface Icon	Status
 (Green)	Enabled (link up)
 (Gray)	Enabled (link down)
 (Dark Gray)	Disabled (not configured)

Device Information

This section of the Dashboard provides version information, including the part number, serial number, and firmware identification string. This information is useful when technical support or firmware upgrades are necessary. The product name is SEL-27xx Ethernet Switch, where xx is filled in with the exact product number; for example, SEL-2731 Ethernet Switch. The firmware version indicates many additional attributes. The following table illustrates how to read the firmware identification string.

Firmware Identification and Spotlighted Attribute	Meaning of the Bolded Attribute
SEL-27xxM-R100-V0-Z001001-D20231115	Product Name
SEL-27xx M -R100-V0-Z001001-D20231115	This indicates the control plane technology integrated in the firmware. This letter is appended to the product number. The following letters are used for the various technologies: <ul style="list-style-type: none">➤ "U" indicates an unmanaged switch➤ "M" indicates an RSTP-based managed switch➤ "S" indicates an OT SDN-based managed switch
SEL-27xxM- R100 -V0-Z001001-D20231115	This indicates the major version number of the firmware. These versions could include new settings and features.
SEL-27xxM-R100- V0 -Z001001-D20231115	This indicates the minor version number of the firmware. These versions do not include new settings or features.

Firmware Identification and Spotlighted Attribute	Meaning of the Bolded Attribute
SEL-27xxM-R100-V0- Z001001 -D20231115	This indicates the version of hardware supported in the firmware.
SEL-27xxM-R100-V0-Z001001- D20231115	This is the date code of the production build. This is when the firmware was built. The date the firmware is publicly released can be found on the SEL product webpage under the Support tab.

Device Information

Hostname:	SEL965634412
Contact:	Schweitzer Engineering Laboratories, Inc. (509)332-1890
Location:	Pullman, WA
Firmware Version:	SEL-2731M-X152-V0-Z001001-D20230728
Serial Number:	965634412

Figure 2.3 Version Information

System Statistics

The System Statistics area (see *Figure 2.4*) of the Dashboard provides some basic statistics of device operations. This information quickly helps determine whether the device firmware is operating properly.

System Statistics

Active Session(s):	1
System Uptime:	0d 0h 4m 30s
Power Cycles:	46
Total Runtime:	2133 Hours

Figure 2.4 System Statistics

Table 2.2 explains the meaning of each of these statistics.

Table 2.2 System Statistics

Statistic	Meaning
Active Session(s)	Number of users currently logged on to the management web interface
System Uptime	How long the unit has been running since it was last turned on or restarted
Power Cycles	Number of times power has been cycled; increases by one every time the unit restarts
Total Runtime	Total number of hours for which the unit has been running

Diagnostics

The Diagnostics section (see *Figure 2.5*) of the Dashboard provides simple status indications for the basic hardware systems of the switch. This information helps determine the health of the device hardware and whether it is operating properly. The power supply model shows SEL-9330-A for high voltage or SEL-9330-C for low voltage. These power supplies are selected when ordering the switch.

Diagnostics

Power Supply A:	Model: SEL-9330-A Status: OK
RAM:	OK
FLASH:	OK
Clock Battery:	OK
CPU Temperature:	42°C
Ports 1-4 Temperature:	61°C
Ports 5-8 Temperature:	54°C
Ports 9-12 Temperature:	57°C
Ports 13-16 Temperature:	52°C
Ports 17-20 Temperature:	57°C
Ports 21-24 Temperature:	57°C

Figure 2.5 Diagnostics

Available Features

The dashboard displays the available features and their licensing status. PTP and OT SDN are optional updates to the switch. PTP licensing allows the switch to support PTP transparent clock functionality. OT SDN licensing allows the switch to be converted to an SDN switch.

Available Features

Critical Infrastructure managed switch:	Licensed
PTP transparent clock:	Licensed
OT SDN upgrade:	Licensed
Order information:	Contact SEL to purchase a firmware upgrade to enable features.

Time Status

The dashboard displays the status of the time synchronization when using NTP. There are three status possibilities: Synced, Not Synced, and N/A.

Time Status

NTP Sync Status:	Synced
------------------	--------

This page intentionally left blank

Managing Users

Introduction

This section includes the following information:

- *User-Based Accounts on page 11*
 - Adding a Local User
 - Editing a Local User and Resetting a Password
 - Removing a Local User
 - Enabling or Disabling a Local User
 - Changing a User Password
- *Centralized User Accounts on page 14*
 - Edit Hosts
 - LDAP
 - RADIUS

User-Based Accounts

The switch has user-based access control in order to provide better authentication, authorization, and accountability. Individuals responsible for configuring, monitoring, or maintaining the device will have their own unique user accounts. User-based access controls are organized to answer, "Who did what and when?" and allow flexibility for detailed auditing.

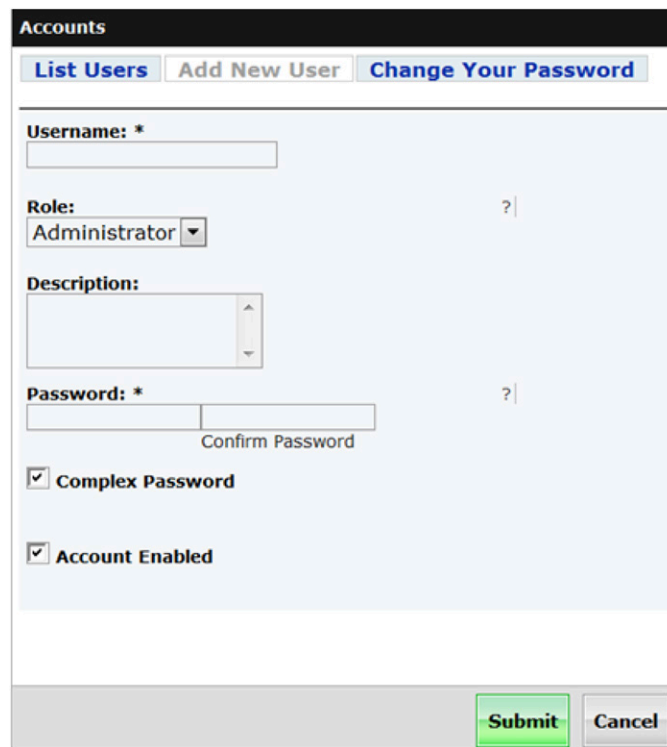
Device permissions are organized into roles, and access is granted through role-based access controls (RBACs). The device has four roles: Administrator, Engineer, User Manager, and Monitor. User account privileges are based on the group (i.e., role) in which the user is a member. The following provides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

- Users with the Administrator role have full access to the device.
- Users with the Engineer role have access to most settings and information on the device. The main exception to this is user account management.
- Users with the User Manager role can manage users on the device. Access to other settings is restricted.
- Users with the Monitor role have read-only access to most of the device settings.

Adding a Local User

The device supports as many as 256 unique local user accounts. Perform the following steps to create a new user account:

- Step 1. Log in to the device with an account that is a member of the Administrator or User Manager group. The account you created during commissioning is one such account.
- Step 2. Select the **Local Users** link from the navigation menu of the web management interface. This link opens the User Accounts page.
- Step 3. Select **Add New User**.
- Step 4. Enter the **Username**, **Role**, and **Password** of the new user. The password must be entered twice to confirm that it has been entered correctly.



The screenshot shows a web interface titled "Accounts". At the top, there are three buttons: "List Users", "Add New User", and "Change Your Password". Below these buttons is a form for adding a new user. The form contains the following fields and options:

- Username: ***: A text input field.
- Role:**: A dropdown menu with "Administrator" selected.
- Description:**: A text area with up and down arrow controls.
- Password: ***: A text input field, followed by a "Confirm Password" label and another text input field.
- ☒ **Complex Password**
- ☒ **Account Enabled**

At the bottom right of the form, there are two buttons: "Submit" (highlighted in green) and "Cancel".

Figure 3.1 Add New User Form

- Step 5. Select the **Submit** button. This adds the new user to the device.

Editing a Local User and Resetting a Password

The device provides an Administrator or User Manager account the ability to edit existing account information. With this function, users with the Administrator or User Manager role can reset another user's forgotten passwords, reassign group membership, and enable or disable an account. Perform the following steps to reset an account's password:

- Step 1. Log in to the device with an account that is a member of the Administrator or User Manager group. The account you created during commissioning is one such account.
- Step 2. Select the **Local Users** link from the navigation menu of the web management interface. This opens the User Accounts page.
- Step 3. Select the **Edit** button associated with the account that you want to edit. This opens the Edit User form.
- Step 4. To change the user's password, enter the new password, confirm the new password, and select the **Submit** button.

Removing a Local User

In the case where an employee leaves the company, you should remove the employee's account to prevent security breaches. Perform the following steps to remove an account.

- Step 1. Log in to the device with an Administrator or User Manager account. The account you created during commissioning is one such account.
- Step 2. Select the **Local Users** link from the navigation menu of the web management interface. This opens the User Accounts page.
- Step 3. Select the **Delete** button associated with the account you are removing.
- Step 4. Verify that the user being deleted is the correct user.
- Step 5. Once verified, select **Yes**. If this person is not the correct user, select **No** to go back to the User Accounts page.

Enabling or Disabling a Local User

Accounts are enabled by default on creation. Disabling an account maintains the account information while preventing unauthorized access to the system until the account is re-enabled. Perform the following steps to enable or disable a user's account:

- Step 1. Log in to the device with an account that is a member of the Administrator or User Manager group. The account you created during commissioning is one such account.
- Step 2. Select the **Local Users** link from the navigation menu of the web management interface. This opens the User Accounts page.
- Step 3. Select the **Edit** button associated with the account that you are editing. This opens the Edit User form.
- Step 4. If an account is currently enabled, deselect the **Account Enabled** check box to disable the account. To enable an account that has been disabled, select the **Account Enabled** check box.

Changing a User Password

Local users with any role can change their own password. When changing a password, the current password must be entered and then the new password must be entered twice following the complexity rules.

If You Forget Your Administrative Account Password

Use of the Captive Port feature to gain access to your switch reestablishes network communication with the device, but you must still know the credentials for an administrative account. If you have lost all administrative account credentials, you must perform a full factory-default reset.

Turn off power to your switch, insert a tool such as a straightened paper clip into the pinhole reset hole just to the left of the front port, and press the recessed reset button. Keep pressing the reset button while applying power. After thirty seconds, release the reset button.

Wait for the green **ENABLED** LED on the front panel to illuminate, which indicates that your switch has reset to factory-default settings and is ready. **ETH F** will be enabled, the Captive Port feature will be on, and the IP address for the unit will be 192.168.1.2. You can access the Commissioning page by entering a hostname, such as selinc.com, or you can browse directly to the IP address (<https://192.168.1.2>) for the unit.

Centralized User Accounts

The switch supports two types of centralized authentication protocols: LDAP and RADIUS. Only one may be active at a time. When a user attempts to log in, the switch authenticates the account in the following order:

Local Users	OR	Local Users
LDAP (if enabled)		RADIUS (if enabled)

Each of the central authentication services can configure primary and backup servers. When using LDAP or RADIUS settings, the switch attempts to contact the primary server first; if the response times out, the switch tries to contact the backup server. If any other error or rejection occurs, the switch rejects the login attempt and stops processing the login.

Both protocols use the **Hosts** page to resolve Hostname settings into IP addresses and the **X.509** page for X.509 certificate management for EAP protocols.

Edit Hosts

The **Edit Hosts** page allows you to add or remove hosts or networks from the Permitted Hosts list. Perform the following steps to add a host or network:

- Step 1. From the **Hosts Settings** page, select **Add Hosts**. This will take you to the page shown in *Figure 3.2*.



Figure 3.2 Edit Hosts

- Step 2. Select **Add Host** and enter the alias you would like to use for the host or network being added.
- Step 3. Enter either the host IP address or network ID under the **Host** field.
The **Edit Hosts** page allows you to enter as many as 16 entries.
- Step 4. Select **Submit** to complete.

Table 3.1 Edit Hosts Settings

Field Name	Values	Default	Description
Alias	1–32 characters	N/A	A name that is associated with the host or network.
Host	Host IP address (e.g., 192.168.10.10/32) or Network ID (e.g., 192.168.10.0/24)	N/A	IP address or network allowed access to the SNMP service of the device.

LDAP

Lightweight Directory Access Protocol (LDAP) is included in the switch to provide a mechanism for centralized user management. With LDAP, users can be managed at a central server. Parameters must be configured in the switch to allow it to communicate with your LDAP server. LDAP parameters in the switch are managed by users with administrative privileges.

NOTE

This device is not compatible with LDAP deployments that permit commas in usernames.

Hosts

The device needs to know the name and IP address of your LDAP server to know how to contact it. Select **Hosts** from the navigation panel on your webpage to view and edit the **Hosts** settings.

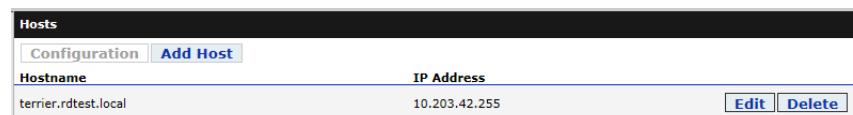


Figure 3.3 Host Settings

The Host Settings page provides a method to statically map IP addresses with external device hostnames, such as your LDAP servers. To map an IP address to a hostname, select **Add Host**. The switch supports as many as 64 hosts.

LDAP Certificates

LDAP requires X.509 authentication to create binds (authenticated connections) between the server and client. The device requires that the root certificate of the LDAP server's certificate chain be stored locally.

LDAP Settings

After adding LDAP servers, configure the device to access those servers. Select **Accounts / LDAP** in the navigation panel to view the LDAP configuration.

The screenshot shows the 'LDAP' configuration page with a dark header bar. Below the header are four tabs: 'Configuration' (selected), 'LDAP Connection Settings', 'Group Maps', and 'Flush LDAP User Cache'. The main content area is titled 'General Connection Settings' and contains several configuration options. 'LDAP Enabled' and 'TLS Required' are both checked. The 'Synchronization Interval' is set to 8 hours. The 'Group Membership Attribute' is 'memberOf'. The 'Search Base' is 'dc=rdtest,dc=local'. The 'User ID Filter' is '(sAMAccountName={USERNAME})'. The 'Group Filter' is a complex LDAP query. 'Use Anonymous Bind' is unchecked. The 'Bind DN' is 'CN=ldap_bind,CN=Users,DC=rdtest,DC=local'. The 'Bind Password' field is empty, with a 'Confirm Password' label below it. At the bottom, there is a 'Configured Servers' section and two buttons: 'Submit' and 'Cancel'.

LDAP

[Configuration](#) [LDAP Connection Settings](#) [Group Maps](#) [Flush LDAP User Cache](#)

General Connection Settings

☒ **LDAP Enabled**

☒ **TLS Required**

Synchronization Interval:
8 (Hours)

Group Membership Attribute:
memberOf

Search Base:
dc=rdtest,dc=local

User ID Filter:
(sAMAccountName={USERNAME})

Group Filter:
((|(objectClass=organizationalUnit)(objectClass=container)
(objectClass=group)(objectClass=groupOfNames)
(objectClass=groupOfUniqueNames)(objectClass=posixGroup))

☐ **Use Anonymous Bind**

Bind DN:
CN=ldap_bind,CN=Users,DC=rdtest,DC=local

Bind Password:
Confirm Password

Configured Servers

[Submit](#) [Cancel](#)

Figure 3.4 LDAP Configuration Summary

The LDAP Connection Settings form is used to enter all your server configurations. Consult with your LDAP administrator to retrieve the settings that should be used in this form.

LDAP

Configuration

LDAP Connection Settings

Group Maps

Flush LDAP User Cache

☒ TLS Required

Synchronization Interval:

8

 (Hours)

Group Membership Attribute:

memberOf

Search Base:

dc=rdtest,dc=local

User ID Filter:

(sAMAccountName={USERNAME})

Group Filter:

(!(objectClass=organizationalUnit)(objectClass=container)(objectClass=group)(objectClass=groupOfNames)(objectClass=groupOfUniqueNames)(objectClass=posixGroup))

☐ Use Anonymous Bind

Bind DN:

CN=ldap_bind,CN=Users,DC=rdtest,DC=local

Bind Password:

Confirm Password

Configured Servers

Priority	Hostname	Port	
1	terrier.rdtest.local	389	✕
+			

Submit

Cancel

Figure 3.5 LDAP Connection Settings

The **LDAP Enabled** check box must be selected to make centrally managed accounts available to the switch for logins. With LDAP enabled, the switch consults the enterprise directory by using LDAP to attempt to authenticate the user if the credentials entered by the user are not found in the locally configured accounts on the switch. If LDAP authentication is successful, the directory service supplies the user attributes that indicate the privilege level of the user when logging in to this device.

The **TLS Required** setting determines whether the connection to the LDAP server is protected by a TLS session. Using TLS requires that the LDAP server be provided with a suitable X.509 server certificate and that the switch imports a suitable CA or server certificate.

The **Synchronization Interval** setting exists to reduce the overhead associated with pulling account information from an LDAP server. The device locally caches the credentials and privileges of centralized users for the period of time configured. The synchronization interval can be set from 0 to 24 hours. If the

synchronization interval is set to 0, the device resynchronizes at every login. The synchronization interval exists to speed up the login process. The switch continues to verify the authenticity of users against the central directory even if their privilege information is locally cached.

Group Membership Attribute, Search Base, User ID Filter, and Group Filter settings are used by the switch to construct queries to the LDAP server to locate the user and verify their credentials. The exact form and content of these items must be entered with information supplied by the LDAP administrator.

NOTE

The Internet-Draft RFC 2307 specifies that the `groupOfMembers` object class can also be used as the convenient structural class for the LDAP entries of the group service. Such group entries can have member attribute values specifying group membership in Distinguished Names (DNs). LDAP clients support such group entries and use the member attribute values for group membership resolution.

The LDAP clients also support group entries that use the `groupOfUniqueNames` object class and the `uniqueMember` attribute. However, using this object class and attribute is not recommended.

The existing method of defining the group entries with the `posixGroup` object class and the `memberUid` attribute is still supported.

The **Search Base** can be thought of as the root directory from which to begin your user search. It is formed by listing all the components of the search base, separated by commas, going from the most specific component to the broadest component. In *Figure 3.5*, the Search Base is configured as "DC=centralauth,DC=local." In this search base, DC refers to domain component. The domain components are later combined with "." to create the search domain. In this case, the search domain is centralauth.local. This search base can be interpreted to mean "search the directory residing on an LDAP server in the centralauth.local domain."

NOTE

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

One other common component of LDAP queries is common name (CN). It is a name that refers to a specific object that may or may not be unique. Examples of CNs are groups and usernames.

The User ID and Group Member attributes are the LDAP labels that identify the usernames and groups of users of the system. If these are not correctly entered, the device is not able to determine which LDAP fields to search for usernames or privileges. The User ID should be configured similarly to (`sAMAccountName={USERNAME}`) or (`uid={USERNAME}`). In these examples, "sAMAccountName" or "uid" is the name of the attribute on the directory server that identifies the ownership of a user account. The {USERNAME} portion of the User ID is the variable that holds the username of the person attempting to log in to the device. For example, if the User ID were configured as (`sAMAccountName={USERNAME}`), and a person with the username **jsmith** were to attempt to log in to the device, then the device would search the LDAP directory for an entry with a sAMAccountName attribute that contained a value of "jsmith". This field


is extendable, so you can search for entries matching multiple criteria. For example, the search field "(&(sAMAccountName={USERNAME})(memberOf=cn=activeusers,dc=your,dc=domain))" would only allow access to users with a valid username who are members of the active users group of your domain.

The **Use Anonymous Bind** setting determines how the switch accesses the LDAP server. The device supports both authenticated and anonymous binds to your LDAP servers. Authenticated binds use a service account to access the LDAP server. If the service account is revoked or the password expires, the device is not able to access the LDAP server, and centralized users are unable to access the device. Anonymous binds forgo the use of service accounts.

If you do not use anonymous binds, you will need to supply the service account username in the **Bind DN** field, and you will need to supply the password in the **Bind DN Password** fields.

LDAP Servers

The **Configured Servers** section lists the LDAP servers that the switch uses to authenticate logins.

To improve availability when the primary LDAP server may be inaccessible, the device supports accessing a secondary LDAP server. To add an LDAP server, select the plus () button below the Configured Servers table to add a new row to the table. Enter the hostname and port number of your secondary server and select **Submit**.

Configured Servers

Priority	Hostname	Port	
1	terrier.rctest.local	389	✕
2			✕

+

Figure 3.6 Adding an LDAP Server

LDAP servers are identified by their hostname and port numbers. Use Port 389 unless a different port number is specified by your LDAP administrator.


The device allows for two LDAP servers to be configured for redundancy and increased reliability. LDAP servers are assigned a priority and are queried in the order of priority until the user accessing the device is found, or the list has been exhausted.

Group Mappings

The device has specific roles that can be mapped to LDAP group memberships on the **Group Maps** tab. The view shown in *Figure 3.7* has a single group defined for administrators.

LDAP		
Configuration LDAP Connection Settings Group Maps Flush LDAP User Cache		
Device Role	Mapped DN	
Administrator	cn=subb_admin,ou=groups,ou=subb,ou=control_systems,dc=rdtest,dc=lo	✕
Engineer	cn=subb_engineers,ou=groups,ou=subb,ou=control_systems,dc=rdtest,dc=lo	✕
+		

Figure 3.7 Group Mappings Showing a Single Group

Select the plus () button at the end of the table to configure a new group mapping in a new row of the table. In the new table row, select the device role from the dropdown list in the left column. You can enter the Mapped DN string yourself, or you can select the list icon at the end of the Mapped DN field. When you select the list icon, the switch queries your LDAP server and shows a hierarchical tree of directory groups that can be searched using your Search Base. Scroll through the tree, select the correct group, and then select **Submit**.

LDAP		
Configuration LDAP Connection Settings Group Maps Flush LDAP User Cache		
Device Role	Mapped DN	
Administrator	cn=subb_admin,ou=groups,ou=subb,ou=control_systems,dc=rdtest,dc=lo	✕
Engineer	cn=subb_engineers,ou=groups,ou=subb,ou=control_systems,dc=rdtest,dc=lo	✕
Administrator		✕
+		

Figure 3.8 Adding a New Role

To expand the tree of groups for a row of the table, select the list icon at the end of the **Mapped DN** field. Selecting the icon again closes the tree of groups. *Figure 3.9* shows the tree of possible groups that appears after selecting the list icon.

LDAP		
Configuration LDAP Connection Settings Group Maps Flush LDAP User Cache		
Device Role	Mapped DN	
Administrator	cn=subb_admin,ou=groups,ou=subb,ou=control_systems,dc=rdtest,dc=lo	✕
Engineer	<div> <div>cn=subb_engineers,ou=groups,ou=subb,ou=control_systems,dc=rdtest,dc=lo</div> <div>dc=rdtest,dc=local</div> <div> <div>▶ cn=computers,dc=rdtest,dc=local</div> <div>▶ ou=control_systems,dc=rdtest,dc=local</div> <div>▶ ou=corporate,dc=rdtest,dc=local</div> <div>▶ ou=domain controllers,dc=rdtest,dc=local</div> <div>▶ cn=foreignsecurityprincipals,dc=rdtest,dc=local</div> <div>▶ ou=global,dc=rdtest,dc=local</div> <div>▶ cn=program data,dc=rdtest,dc=local</div> <div>▶ cn=system,dc=rdtest,dc=local</div> </div> </div>	✕
+		

Figure 3.9 Selecting a Group From the Tree Display

If you cannot find an appropriate group, your server administrator may need to create new groups and assign members appropriate for these mappings.

The last tab on the LDAP page is Flush LDAP User Cache. Selecting the **Flush Cache** button flushes the LDAP user cache, causing all LDAP users to be logged out of the device and forcing authentication information to be refreshed from the server on each account's next login.

RADIUS

The switch supports the basic NAS client authentication functionality of the RADIUS protocol. By configuring the RADIUS settings, users can log in using credentials not stored in the Local Users table on the switch. The switch also supports two-factor authentication through RADIUS.

There are three types of settings used by the RADIUS feature:

- RADIUS Protocol settings (see *RADIUS Protocol Settings on page 21*), viewable on the **Configuration** page and configurable through the use of the **RADIUS Connection Settings** page under the RADIUS navigation menu link
- Hosts (required if a hostname is used in hostname setting in Configured Server), located on the **Hosts** page
- X.509 Certificates (required if an EAP Authentication Protocol is used), located on the **X.509 Certificates** page

SEL cannot guarantee that the device will be compatible with all possible RADIUS server architectures and implementations.

The **RADIUS** page on the switch is divided into three tabs (as shown in *Figure 3.10*): **Configuration** for viewing RADIUS settings, **RADIUS Connection Settings** for configuring RADIUS settings, and **Download Dictionary** for downloading the RADIUS dictionary file. You can access these tabs by selecting the **RADIUS** navigation menu item under **Accounts**.



Figure 3.10 RADIUS Webpage

RADIUS Protocol Settings

The RADIUS settings are divided into three categories: general, additional (for EAP protocols), and configured servers. *Figure 3.11* shows the RADIUS Connection Settings tab.

RADIUS

Configuration
RADIUS Connection Settings
Download Dictionary

General Connection Settings

☐ **Enable RADIUS**

Retransmission Timeout: *
 (Seconds)

Authentication Protocol:

Shared Secret:

 Confirm Shared Secret

Additional Settings for EAP Protocols

☒ **Don't send username in cleartext**

☒ **Validate server hostname against common name**

Configured Servers

Priority	Hostname	Port	
1	RADIUSServer	1812	✕

+

Figure 3.11 RADIUS Protocol Settings

General RADIUS settings that appear in the web interface and configuration file are listed in *Table 3.2*.

Table 3.2 General RADIUS Settings

Settings	Valid Values	Default	Feedback	Rules	Description
Enable RADIUS	Enabled, Disabled	Disabled	—	—	Enables RADIUS for authenticating users logging in to the switch.
Retransmission Timeout	1–10 seconds	1 second	—	—	If the switch does not receive a response from the active RADIUS server within the set Timeout amount of seconds, it makes another attempt (up to the value set in the general RADIUS settings). The total time-out period for a login attempt is Attempts * Retransmission Timeout * the number of configured RADIUS servers.
Authentication Protocol	PAP, EAP-PEAPv0/MSCHAPv2, EAP-TTLS/PAP	PAP	—	—	The authentication protocol that defines how the switch authenticates with the RADIUS server. SEL recommends using an EAP protocol for enhanced security.

Settings	Valid Values	Default	Feedback	Rules	Description
Shared Secret	1–128 printable ASCII characters		If RADIUS is enabled with no shared secret: Shared secret is required because no shared secret previously configured. If the shared secret is too long: The shared secret can't be more than 128 characters.	Required upon enabling RADIUS for the first time. The setting appears empty when the page loads. If the user does not successfully submit a new shared secret, the last shared secret continues to be used.	Shared secret between the switch and the RADIUS server. This value must be the same between the switch and the RADIUS server. SEL recommends using long shared secrets.
Confirm Shared Secret	Same as shared secret		If different than shared secret: The shared secret and confirm shared secret settings do not match.	Must be identical to the shared secret.	—

EAP protocols also have two additional settings, as listed in *Table 3.3*. SEL recommends enabling these settings if the RADIUS server supports them. These do not apply if the PAP authentication protocol is selected.

Table 3.3 Additional Settings for EAP Protocols

Setting	Valid Values	Default	Feedback	Rules	Description
Don't send username in cleartext	Enabled, Disabled	Disabled	—	—	The username is normally sent in clear text in the User-Name attribute or Identity field (for EAP protocols). If this setting is enabled, then the switch sends "anonymous" instead of the username.
Validate server hostname against common name	Enabled, Disabled	Enabled	—	—	As part of setting up the TLS connection, the RADIUS server sends a certificate to the switch. One of the attributes of this certificate is the common name. If this setting is enabled, the switch checks the server hostname as entered into the hostname setting on the RADIUS page and the common name in the X.509 certificate and rejects any login attempt from that RADIUS server if they are not identical.

Configured server settings are listed in *Table 3.4*. There are no default values for the Hostname or Port setting.

Table 3.4 Configured Servers Settings

Setting	Valid Values	Feedback	Rules	Description
Hostname	The hostname as listed in the host table or the IP address	—	—	The address at or through which the switch may reach the RADIUS server. The hostname only needs to be present on the Hosts page when the switch is contacting that RADIUS server.
Port	1–65535 (typically 1812)	—	—	The UDP port at or through which the switch can reach the RADIUS server.

The primary server (Priority 1) must be configured. You can optionally add a backup server (Priority 2). The switch first attempts to contact the primary server, and if no responses are received, it attempts to contact the backup server if one is configured. If no servers are configured during the time RADIUS is enabled, then the feedback is as follows:

At least one configured server required

You can enter a hostname, as entered in the **Hosts** page, or an IP address, into the **Hostname** setting and the appropriate authentication port into the **Port** setting. This is typically **1812**. To add a backup server, select the plus (+) button and enter the hostname and port. The hostname is not required on the **Hosts** page when entered, but the switch skips any server with a hostname that is not present on the **Hosts** page. The primary and backup server information must be unique (i.e., the hostname and either the IP address that the hostname resolves to or the port must be different). If the configured servers are identical, the feedback is as follows:

Configured servers must be unique. Either the hostname, and their resolved IP addresses, or the ports must be different

Select the ✕ button to delete a server.

SEL-User-Role VSA

Similar to logging in through LDAP or a Local User, the user does not select their role. The RADIUS server determines the user role through the reply message. To successfully authenticate a user, the RADIUS server must return the user role in the format accepted by the switch. This format is defined by an SEL vendor attribute SEL-User-Role, which can be downloaded by selecting **Download Dictionary** at the top of the **RADIUS** page.

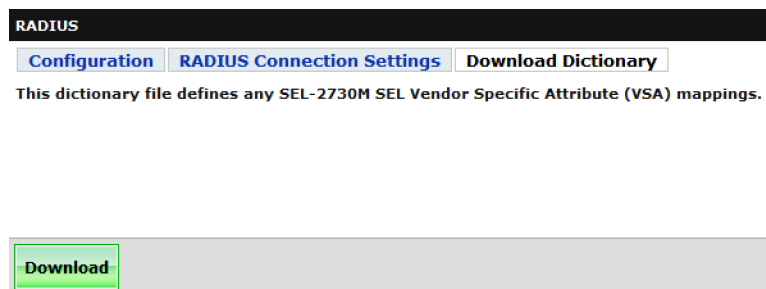


Figure 3.12 Download Dictionary

Setting Up RADIUS On the Switch

When enabling RADIUS, you must configure the RADIUS Shared Secret setting (configured on the RADIUS server) and have at least one configured server with a defined Hostname or IP address and the UDP port. If you are using a hostname, add the appropriate hostname and IP address to the **Hosts** page. If you are using an EAP protocol, you must have the appropriate X.509 certificate added to the **X.509 Certificate** page. To enable RADIUS, select the **Enable RADIUS** check box on the **RADIUS** page, configure the settings, and select **Submit**. RADIUS is then enabled and ready for the next login attempt.

On the RADIUS Server

The RADIUS server must be configured with the same shared secret and configured to return the appropriate SEL-User-Role attribute for each user.

RADIUS Attributes

In addition to the RADIUS attributes defined by the authentication protocol, the switch supports three other attributes, listed in *Table 3.5*. These appear in each request message to the RADIUS server.

Table 3.5 Additional Request Attributes

Attribute	Value
NAS-IP-Address	The IP address of the port through which the switch contacts the server (i.e., the IP address of the front- or rear-panel ports)
NAS-Identifier	The hostname setting as configured on the IP Configuration page
Calling-Station-Id	The IP address of the user logging in to the switch

RADIUS Communications

The switch sends an Access-Request message, using PAP, to the RADIUS server with the username and the hashed password. When using EAP protocols, certificates are exchanged so that the RADIUS communications are encrypted. If the RADIUS server authenticates the users, it replies with an Access-Accept message that includes the user role in the SEL-User-Role VSA. The switch then accepts the login attempt, logging in the user with the role specified in the SEL-User-Role VSA returned by the RADIUS server. The login attempt is rejected if the RADIUS server returns any other message, such as an Access-Reject message, or if the Access-Accept message does not contain a valid user role in the SEL-User-Role VSA. If the RADIUS server does not respond, the switch attempts to contact the backup server. If the switch receives no response from the backup server, the login is rejected. When two-factor authentication is used, the user first generates or receives a token. This may be on a keychain or a smart phone. The user then appends this token to their password.

RADIUS Events

When the switch does not receive a response within the time-out period, it logs the following event:

```
Rejected login attempt because no response from the RADIUS
server received within the retransmission timeout
```

The login attempt is rejected if all attempts time out.

The RADIUS server authenticates and logs a user in by responding with a user role in the response. The user role must be one of the supported roles in the switch. If there is no user role in the response acceptance message, the login attempt is rejected and sends the following event:

```
Rejected login attempt by user <username> because RADIUS server
<priority> replied without an SEL-User-Role attribute
```

If the user role is not recognized, the switch rejects the login attempt and sends the following event:

```
Rejected login attempt by user <username> because RADIUS server
<priority> replied with an SEL-User-Role attribute containing
an unrecognized user role
```

The switch attempts to use the primary server first. If all attempts to contact the primary RADIUS server fail, and the backup server is configured, the switch logs the following event and then attempts to contact the backup server:

```
Active RADIUS server is now 2
```

At the next login attempt, the switch again attempts to connect to the primary server first.

The EAP authentication protocols have additional optional checks. During the initial handshake, the RADIUS server sends its X.509 certificate. If the user has enabled the **Validate server hostname against common name** setting, and the hostname does *not* match the common name, the switch rejects the login attempt and logs the following event:

```
Rejected login attempt because the common name in the X.509  
certificate sent by the RADIUS server <priority> did not match  
the hostname of the RADIUS server on the RADIUS page
```

If the certificate sent by the RADIUS server has an authority issue, the switch rejects the login attempt and logs the following event:

```
Reject login attempt because RADIUS server <priority> sent  
an X.509 certificate with an unknown or untrusted certificate  
authority
```

If the X.509 time is incorrect (e.g., expired), the switch rejects the login attempt and logs the following event:

```
Rejected login attempt because RADIUS server <priority> sent an  
expired or not yet valid X.509 certificate
```

If a user enables, disables, or modifies one or more RADIUS settings, the switch logs the following events:

```
<username> at <user_ip> enabled RADIUS  
  
<username> at <user_ip> disabled RADIUS  
  
<username> at <user_ip> modified RADIUS settings
```

Settings and Commands

Introduction

This section explains the settings and commands of the device:

- *Reports on page 27*
 - Syslog Report
 - MAC Address Table
- *Switch Management on page 29*
 - VLAN Settings
 - RSTP Settings
 - Port Settings
 - MAC Port Filtering
 - Multicast MAC Filtering
 - Port Mirroring
 - Port Monitoring
 - Priority Settings
 - Managing Precision Time Protocol
 - Network Settings
 - Security
 - System

Reports

Syslog Report

The switch uses the Syslog message format to record event data. The device has storage for 60,000 of these messages. The device can also forward Syslog messages to three destinations.

The Syslog message format includes five fields:

- Severity
- Facility
- Tag name
- Timestamp
- Message

A message can have seven different severity ratings, ranging from informational to emergency. There are three facilities on the device: user, system, and security. The Tag field indicates which part of the system generated the message. The Timestamp and Message fields include the time stamp of when the message was generated and the message description. For more information about Syslog, refer to *Appendix C: Syslog*.

Select the **Syslog Report** link from the navigation panel to show the device's local system logs (see *Figure 4.1*).

Syslog Report						
Download	Acknowledge Selected	Acknowledge All				
Acknowledged	ID	Timestamp	Tag	Severity	Facility	Message
<input type="checkbox"/>	104	2023-08-10 20:10:24.771032+00	DateTimeConfig	Notice	USER	Time Source: set to LOCAL by admin at 192.168.1.1
<input type="checkbox"/>	103	2023-08-10 20:09:00.156091+00	Login	Notice	SECURITY	Login to web: successful by admin at 192.168.1.1
<input type="checkbox"/>	102	2023-08-10 18:29:47.690597+00	DateTime	Notice	SYSTEM	System Time: synchronized via NTP
<input type="checkbox"/>	101	2023-08-10 18:28:13.869424+00	Link Up/Down	Notice	SYSTEM	Front Port changed link state to up
<input type="checkbox"/>	100	2023-08-10 18:28:10.941683+00	Power	Notice	SYSTEM	Device initialization completed
<input type="checkbox"/>	99	2023-08-10 18:28:09.699707+00	SpanningTree	Notice	SYSTEM	Spanning Tree: Port 14 transitioned from Learning to Forwarding
<input type="checkbox"/>	98	2023-08-10 18:28:09.651188+00	SpanningTree	Notice	SYSTEM	Spanning Tree: Port 14 transitioned from Discarding to Learning
<input type="checkbox"/>	97	2023-08-10 18:28:09.593514+00	SpanningTree	Notice	SYSTEM	Spanning Tree: Port 8 transitioned from Learning to Forwarding
<input type="checkbox"/>	96	2023-08-10 18:28:09.519046+00	SpanningTree	Notice	SYSTEM	Spanning Tree: Port 8 transitioned from Discarding to Learning
<input type="checkbox"/>	95	2023-08-10 18:28:09.432824+00	SpanningTree	Notice	SYSTEM	Spanning Tree: Port 2 transitioned from Learning to Forwarding
<input type="checkbox"/>	94	2023-08-10 18:28:09.33469+00	SpanningTree	Notice	SYSTEM	Spanning Tree: Port 2 transitioned from Discarding to Learning
<input type="checkbox"/>	93	2023-08-10 18:28:06.946673+00	SpanningTree	Notice	SYSTEM	Spanning Tree: Port 2 transitioned from Disabled to Designated
<input type="checkbox"/>	92	2023-08-10 18:28:06.599425+00	SpanningTree	Notice	SYSTEM	Spanning Tree: Port 8 transitioned from Disabled to Designated
<input type="checkbox"/>	91	2023-08-10 18:28:06.428191+00	SpanningTree	Notice	SYSTEM	Spanning Tree: Port 14 transitioned from Disabled to Designated
<input type="checkbox"/>	90	2023-08-10 18:27:55.96944+00	ImportExport	Notice	USER	Configuration file import successful
<input type="checkbox"/>	89	2023-08-10 18:27:55.96944+00	Firmware	Warning	SYSTEM	Firmware update from X152 to X155 succeeded
<input type="checkbox"/>	88	2023-08-10 13:28:29.145892+00	Firmware	Notice	USER	Firmware: update to new version initiated by admin at 192.168.1.1
<input type="checkbox"/>	87	2023-08-10 13:26:54.849006+00	SpanningTree	Notice	SYSTEM	Spanning Tree: Port 8 transitioned from Learning to Forwarding
<input type="checkbox"/>	86	2023-08-10 13:26:54.827737+00	SpanningTree	Notice	SYSTEM	Spanning Tree: Port 8 transitioned from Discarding to Learning
<input type="checkbox"/>	85	2023-08-10 13:26:51.867645+00	Link Up/Down	Notice	SYSTEM	Port 8 changed link state to up

Figure 4.1 Sample Syslog Report

Device system logs are displayed in the order of their generation. Select a field label at the top of the list to reorder the messages according to the value of that field. For example, selecting the Severity label reorders the list by severity.

Event messages in the device have two states: unacknowledged and acknowledged. These two states exist to make identification of abnormal event generation easier. Large numbers of unacknowledged messages can indicate high levels of activity on the device.

Message acknowledgment also assists with log documentation. In your periodic examination of logs, acknowledge existing logs. When you examine logs in the future, the previously acknowledged logs limit the logs of concern to only those logs the device has generated since the last examination.

Select the **Acknowledge Selected** button to acknowledge selected system logs. All system logs can be acknowledged by selecting the **Acknowledge All** button. You cannot remove system logs from the device without issuing a factory-default reset.

The **Download** button allows you to save log messages in an offline format.

MAC Address Table

SEL RSTP-managed switches can report the device MAC address(es) connected to each port. The report can be sorted by the following:

- Address
- Port

- Alias
- Type
 - Learned
 - Static
 - User set
- Multicast address

This report can be viewed in the web interface or through SNMP, and can be downloaded into a comma-separated value table for local storage and export. When viewing the MAC table in the web interface, you can sort it by using any of the columns.

Switch Management

VLAN Settings

By default, the switch is not in VLAN-aware mode and is a simple layer two switch. To enable VLAN-aware mode, navigate to the Global settings and enable the VLAN-aware mode. You can configure VLAN settings when the switch is not in the VLAN-aware mode in preparation for these settings to become active once VLAN-aware mode is enabled. The switch supports a shared VLAN learning (SVL) architecture, so the MAC addresses of hosts are learned and shared across all VLANs. Therefore, the switch expects that each host has a unique MAC address, even if those hosts are on different VLANs. Using SVL reduces flooding when learning MAC addresses, which in turn reduces network burden. The default VID for untagged traffic is one.

Table 4.1 VLAN Settings

Field Name	Values	Default	Description
VID	1 to 4094	N/A	The VLAN Identifier (VID) identifies the VLAN in IEEE 802.1Q-2014 tagged frames.
VLAN Name	0 to 64 characters	N/A	User-defined name of the VLAN.
Tagged Ports	Available ports	N/A	Tagged ports determine which ports can ingress and egress frames for the VLAN. Tagged ports are sometimes called Trunk Ports. Tagged ports can be used to connect to a VLAN-aware device or to another switch.
Untagged Ports	Available ports	N/A	Untagged ports are used to connect to non-VLAN-aware devices.

VLAN View

The **VLAN View** page (see *Figure 4.2*) shows a table that provides a VLAN-centered view of the configuration of the VLANs and the member ports. The fields of the table can be edited; to apply the finished set of changes to the configuration of the VLANs, select the **Submit** button at the bottom. In the VLAN view, groups of VLANs with similar settings are shown as a VID range.

VLAN Settings				
<div>VLAN View</div> <div>Port View</div>				
VID	VLAN Name	Tagged Ports	Untagged Ports	
1	Default		1-4,9-24	✕
2	Process Network 1		5-8	✕
101-105		16		✎
+				

Figure 4.2 VLAN View

To edit a VLAN entry, select the table item to be changed and edit the data. The affected table item will be highlighted, and an undo link will appear next to it to allow you to revert the change. Selecting the **Submit** button at the bottom of the page applies all the edited changes to the VLAN configuration. *Figure 4.3* shows an example where several fields have been edited but not yet applied.

VLAN Settings				
<div>VLAN View</div> <div>Port View</div>				
VID	VLAN Name	Tagged Ports	Untagged Ports	
1	Default		1-3,9-24	✕
2	Process Network 1		5-8	✕
102	OneHundredTwo	8	4	✕
101-105		16		✎
+				

Figure 4.3 Editing VLAN Settings

To delete a VLAN entry, select the ✕ button in the last column of the table.

To edit a VLAN in a group, select the edit (✎) button in the last column of the entry, enter the VLAN number, and then make the necessary changes in the table row that is added for that VLAN. *Figure 4.4* shows how to select the VLAN that you wish to edit.

VLAN Settings

VLAN View

Port View

VID	VLAN Name	Tagged Ports	Untagged Ports	
1	Default		1-3,9-24	✕
2	Process Network 1		5-8	✕
101-105		16		✎
+				

Which VLAN would you like to edit?

Choose a value from the range 101-105:

Cancel

OK

Figure 4.4 Editing a VLAN Within a Range

To delete a VLAN group (single row of the VLAN table), select the **Port View** tab and delete the affected VID range from the **Allowed VLANs** column for the affected ports.

Tagged Ports

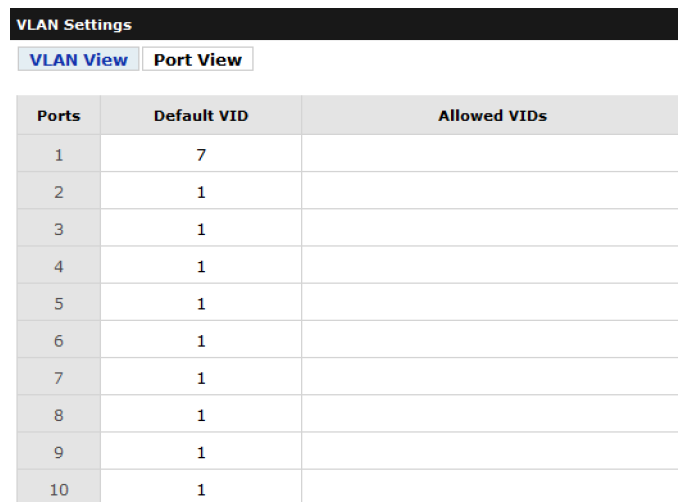
The **Tagged Ports** column lists those ports that can send or receive frames with VLAN tags. The switch does not strip tags during egress and expects tagged traffic on ingress.

Untagged Ports

The Untagged Ports column lists those ports that can send and receive frames without VLAN tags. The switch strips tags during egress and expects untagged traffic on ingress. This allows devices that do not tag traffic to communicate with other devices in the same VLAN.

Port View

The **Port View** page (see *Figure 4.5*) provides a port-centered view of each port's VLAN configuration. The same features for VLANs are available in both views.



VLAN Settings		
VLAN View Port View		
Ports	Default VID	Allowed VIDs
1	7	
2	1	
3	1	
4	1	
5	1	
6	1	
7	1	
8	1	
9	1	
10	1	

Figure 4.5 Port View

VLAN Configuration in Port View

Configure the Default VID column to the desired value to which untagged traffic will be associated. One Default VID is required for each port. Allowed VIDs are the tagged traffic allowed on that port. One or more Allowed VIDs are supported and optional for each port. Allowed VIDs are the traffic the switch expects to be tagged on ingress and will egress tagged. Default VIDs are the traffic the switch expects to be untagged on ingress and which will egress untagged.

VLAN Configuration Considerations

The switch VLAN configurations are streamlined to accelerate the network engineering of services that are in a publish/subscribe model like Sampled Values and GOOSE.

Because of this flexibility, it is important to configure the redundant links in the network to have the same VLAN membership so that when there is a network event that triggers a failover, like a link or switch failure, all communications will continue. A simple way to validate this is to confirm that all switch-to-switch links have the same VLAN profile.

Many hosts in OT have redundant connections to the network. It is important to verify that both connections from the same host have the same VLAN profile to ensure that communications will continue when that host fails over to the secondary interface.

Rapid Spanning Tree Protocol (RSTP) Settings

Communications networks are typically designed with interconnecting switches to provide network redundancy. RSTP is designed to support these network topologies and provide loop-free redundant paths to end devices. RSTP ensures a loop-free network and provides an alternative path in the event of a network failure.

RSTP is enabled by default. You can disable RSTP through the Spanning Tree Mode setting on the Global Settings page. Exercise caution when disabling RSTP because doing so could introduce network loops.

Settings can be modified while RSTP is disabled; these settings are not active until you enable RSTP through the Spanning Tree Mode setting in Global Settings.

Configuration

Figure 4.6 shows the RSTP configuration of the device.

RSTP Settings

Configuration

Edit RSTP Settings

Edit Port Settings

RSTP Settings

Bridge ID	Root Bridge	Root Port	Time Since Topology Change		BPDU Guard Timeout		
-	-	-	- Seconds		Disabled		
Bridge Priority		Hello Time		Max Age	Forward Delay		
32768		2 Seconds		20 Seconds	15 Seconds		

Port Settings

Port	Protocol Version	Port State	Port Role	Port Priority	Port Path Cost	Edge Port	BPDU Count
1	-	-	-	128	20000	-	-
2	-	-	-	128	20000	-	-
3	-	-	-	128	20000	-	-
4	-	-	-	128	20000	-	-
5	-	-	-	128	20000	-	-
6	-	-	-	128	20000	-	-
7	-	-	-	128	20000	-	-
8	-	-	-	128	20000	-	-
9	-	-	-	128	200000	-	-
10	-	-	-	128	200000	-	-
11	-	-	-	128	200000	-	-
12	-	-	-	128	200000	-	-
13	-	-	-	128	200000	-	-

Figure 4.6 RSTP Configuration Page

Bridge ID

The Bridge ID field consists of the bridge priority and the bridge MAC address. Each RSTP-capable device in the network has a unique bridge ID that RSTP uses to determine the root bridge.

Root Bridge

The root bridge is the logical center of the network. There is one root bridge within the network. Determination of the root bridge of the network occurs through RSTP selection. RSTP selects the bridge with the lowest Bridge Priority value. If two or more devices have equal bridge priority values, then RSTP next compares the MAC addresses and selects the device with the lowest MAC address as the root bridge. To guarantee a device is selected as the root bridge within the network, the bridge priority value must be set to a lower value than all other bridges in the network. Root bridge selection should always be a network-engineered effort to make sure the root bridge is the device you want it to be. The root should be the switch that balances your network. Hosts have switch modes when they have dual network interfaces and these devices should not be the root bridge of your network. SEL RSTP-managed switches generate a log anytime the root bridge changes in the network. This log includes the root bridge identifier, which is the MAC address of the root bridge.

The following message displays at the top of the **RSTP Settings** page when the device is the root bridge in the spanning tree topology.

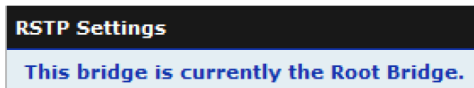


Figure 4.7 Root Bridge Notification

Root Port

The root port is a port with the shortest path to the root bridge. All RSTP-enabled devices must have exactly one root port with the exception of the root bridge, which does not have a root port.

Time Since Topology Change

The device displays the time since the last topology change occurred. Common scenarios for a topology change occurring are when physical changes are made to the network or when bridges stop receiving logical confirmations from their peers.

BPDU Guard Timeout

This interval is the time for which a port configured with BPDU Guard will be disabled after the switch receives a BPDU on that port. When this time-out expires, the port starts learning to forward again based on the STP Mode to which the port is set.

Bridge Priority

The bridge priority consists of two components: the bridge priority and the MAC address.

Hello Time

The hello time is the interval in which the device sends bridge protocol data units (BPDUs).

Max Age

The max age is the maximum number of hops from the root that a switch accepts a BPDU. If the number of hops from the root bridge (Message Age) is greater than this setting, the switch discards the BPDU.

Forward Delay

The forward delay is the time that a port must spend in the listening and learning states before transitioning to forwarding.

The max age and forward delay derive from the root bridge.

Editing RSTP Settings

RSTP Settings are made on the **RSTP Settings** page. The **Edit RSTP Settings** tab (see *Figure 4.8*) is used to edit settings that are common to all ports, and the **Port Settings** tab (see *Figure 4.9*) is used to set the **STP Mode**, the **Port Priority**, and **Path Cost** for each port. Editing these settings may disrupt network communications.

The screenshot shows the 'RSTP Settings' dialog with the 'Configuration' tab selected. It contains the following fields and controls:

- Bridge Priority:** A dropdown menu showing '32768'.
- Hello Time: *** A text input field containing '2'.
- Max Age: *** A text input field containing '20'.
- Forward Delay: *** A text input field containing '15'.
- Enable BPDU Guard Timeout:** An unchecked checkbox.
- BPDU Guard Timeout:** A text input field containing '5', followed by '(Minutes)'.

Figure 4.8 Common RSTP Settings

Figure 4.9 shows the **Port Settings** dialog used to set those RSTP parameters that are individual for each port.

The screenshot shows the 'RSTP Settings' dialog with the 'Port Settings' tab selected. It displays a table with four columns: Port, Port Priority, Port Path Cost*, and STP Mode. There are four rows representing ports 1 through 4. A dropdown menu for the STP Mode of port 1 is open, showing options: Auto, Fast Port BPDU Guard, Fast Port, Non-STP BPDU Guard, and Auto.

Port	Port Priority	Port Path Cost*	STP Mode
1	128	20000	Auto
2	128	20000	Auto
3	128	20000	Auto
4	128	20000	Auto

Figure 4.9 Port RSTP Settings

Table 4.2 RSTP Settings

Field Name	Values	Default	Description
BPDU Guard Timeout	1–60 min	5 min	The amount of time that a port configured with BPDU Guard will be disabled after receiving a BPDU frame.
Bridge Priority	0–61440 in increments of 4096	32768	Bridge priority determines the root bridge. The bridge with the lowest value becomes the root bridge.
Hello Time	1–10 s	2 s	Interval in which the device sends BPDUs.
Max Age	6–40	20	Maximum number of hops before a BPDU is discarded.
Forward Delay	4–30 s	15 s	The time that a port must spend in the listening and learning states before transitioning to forwarding.

Port Settings

Table 4.3 Port Settings

Field Name	Values	Default	Description
Priority	0–240	128	Port priority determines which port the device selects as a root port when there is a tie between two ports. The port with the lower value will become the root port.
Path Cost	1–200000000	Based on port speed	Path cost helps determine which path the device selects to a root bridge. The device selects paths with the lowest overall cost first.
STP Mode	Auto, Fast Port BPDU Guard, Fast Port, Non-STP BPDU Guard	Auto	See the following discussion.

SEL RSTP-managed switches should always use auto-negotiate when using the built in copper ports. This ensures the link uses the maximum bandwidth and resolves to full-duplex communication whenever possible. When not using auto-negotiate, if one side of the link attempts to negotiate and the other side of the link does not respond, the link defaults to half-duplex communication at 10 Mbps, resulting in no link for the managed switches.

Switches communicate RSTP through BPDU frames that travel between adjacent switches. These frames allow switches to determine the root switch, as well as the state and role of each switch port. When ports connect to an end device that does not participate in RSTP, the proposal/agreement mechanism is unavailable, and the switch must rely on STP timers. In this case, the Forward Delay controls how long the port will listen for incoming BPDUs before starting to forward traffic. With the default Forward Delay value of 15, the switch takes longer than 15 seconds to transition the port into the forwarding state. Because no BPDUs have been received, the port is considered an edge port. After this time-out, the port remains in the forwarding state until a topology change, at which time the switch reinitiates the learning process.

You can configure the STP Mode to Auto, Fast Port BPDU Guard, Fast Port, or Non-STP BPDU Guard. In these modes, each port transitions quickly to the forwarding state, but behaves differently in how it reacts to received BPDUs and whether the switch sends BPDUs out of that port. In Fast Port BPDU Guard or Fast Port mode, the switch still sends out BPDU packets; in Non-STP BPDU Guard mode, the switch does not send BPDUs out of the port.

BPDUs Guard prevents devices connected to the port from affecting the spanning tree of the switch. If the switch receives a BPDU on a port with BPDU Guard enabled, the switch disables that port, preventing traffic from passing to and from the port. Enabling this setting on every port not connected to another RSTP switch can help protect against miswirings and malicious attacks to the spanning tree. It is important to not use these modes for ports that connect switch-to-switch links because it could cause network storms. Ports of RSTP switches connected to other RSTP switches must be set to Auto STP Mode. Non-STP BPDU Guard mode is recommended for connections to non-RSTP switches.

The differences among the four modes are summarized in *Table 4.4*.

Table 4.4 STP Mode

STP Mode	Switch Sends BPDUs Out the Port?	Switch Shuts Off Port if it Receives a BPDU?	Moves Instantly Into the Forwarding State?	For Connecting to...
Auto	Yes	No	No	RSTP switches
Fast Port BPDU Guard	Yes	Yes	Yes	End devices
Fast Port	Yes	No	Yes	End devices
Non-STP BPDU Guard	No	Yes	Yes	End devices

MAC Port Filtering

SEL RSTP-managed switches can apply an allow list to each port to ensure that only traffic from authorized MAC addresses is forwarded. All other traffic will be dropped.

When enabled, MAC-based port security has two modes: Static and Dynamic. Static mode has a source MAC list for each port and only allows incoming packets from MAC addresses on the list for the given port. Once a MAC address is listed for a port running in Static mode, that MAC address is not allowed on any other port regardless of what mode that port is operating in. Dynamic mode also has a MAC list but instead of per port, like Static mode, the Dynamic mode list is for the switch. Dynamic mode configuration is still performed per port but the MAC addresses authorized per port are allowed on any port operating in Dynamic mode or disabled mode. Static mode is sometimes referred to in the industry as "sticky" and Dynamic mode as "non-sticky" MAC filtering.

When enabling MAC-based port security, the MAC table for the port is flushed and authorized MAC lists must be configured. When changing from Static to Dynamic modes, the authorized MAC list for that port is retained and those MAC addresses are added to the Dynamic authorized MAC list. When changing from Dynamic mode to Static mode, the MAC list is flushed for that port but the Dynamic MAC list is retained. When using the automated learning modes, it may be possible to drop the first ingress packet.

The SEL RSTP-managed switch provides two methods of dynamically building the MAC filter for a port and an additional method to statically assign MAC addresses to the filter. The methods for dynamically building the MAC filter for a port include count lock and time lock. You can use all methods independently or in conjunction to build the MAC filter for the port. For example, you can specify that you would like to learn five MAC addresses for the port and lock in the configuration. You can also specify that you would like to learn five MAC addresses for ten minutes, and the configuration will either lock after five

addresses have been learned, or ten minutes have elapsed. You can also choose to statically configure the MAC filter on the port by manually entering one or more MAC addresses. An SEL RSTP-managed switch supports as many as 1,000 MAC address entries across all ports.

To configure a port with MAC security, navigate to the MAC security page in the web interface menu and select **Edit** for the desired port. This opens the MAC security configuration form. Once you enable MAC security for the port, the remaining fields become editable. The fields on the form are described in *Table 4.5*.

Table 4.5 MAC Security Fields

Field Name	Values	Description
Count Lock	0–1000	The number of MAC addresses that will be added to the filter.
Time Lock	0–1440 Minutes	Time period in which new MAC addresses may be added to the filter.
Select MAC Addresses for deletion	Unicast MAC Address	Field to remove MAC addresses from the filter.
Add additional whitelist MAC Addresses	Unicast MAC Address	Field to add MAC addresses to filter.
Mode	Static or Dynamic	MAC filter mode on which the port will operate.

The MAC security report page provides an overall view of the status of each port and the MAC addresses locked on each port.

Multicast MAC Filtering

SEL RSTP-managed switches support multicast MAC filtering allowing you to subscribe a group of ports to each multicast publisher. When a multicast frame ingresses a port, the device inspects the multicast destination address to see if it matches any configured multicast MAC filter. If no match is found, the switch forwards the multicast frame out of every port on the VLAN. If a match does occur, the switch forwards the frame out of every port that is a member of the specified filter in the VLAN. Use the following steps to configure a multicast MAC filter:

- Step 1. Log in to the switch with Engineer or Administrative privileges.
- Step 2. Navigate to the Multicast MAC Filtering page in the user interface and select **Add Filter**.
- Step 3. Enter the multicast MAC address that you would like to filter and select a group of member ports.
- Step 4. Select **Submit** to commit the filter to the switch and update the settings.

Port Mirroring

You would typically use port mirroring for troubleshooting network problems and for monitoring traffic on a selected source port through the use of a network protocol analyzer or an intrusion detection system attached to a target port. Port mirroring mirrors the network traffic the device sends and receives on the source port to the target port. This allows the use of a non-intrusive troubleshooting technique for gathering network traffic information.

The device can mirror network traffic from multiple source ports to one target port. The source port may be any physical port on the device except the target port that the device uses for mirroring and the front Ethernet management port (ETH F).

The source port may be selected as ingress, egress, or for passage of both types of traffic to the target port.

The target port cannot receive ingress traffic while in the monitoring session.

In *Figure 4.10*, the device has been configured to mirror both ingress and egress traffic from Port 9 to Port 16. To configure port mirroring, navigate to the **Port Mirroring** page and select **Enable Port Mirroring**. Select the source port, target port, and the traffic you want mirrored to the target port, by selecting either **Mirror Ingress Traffic** or **Mirror Egress Traffic**. You can also select both to mirror ingress and egress traffic from the source port to the target port.

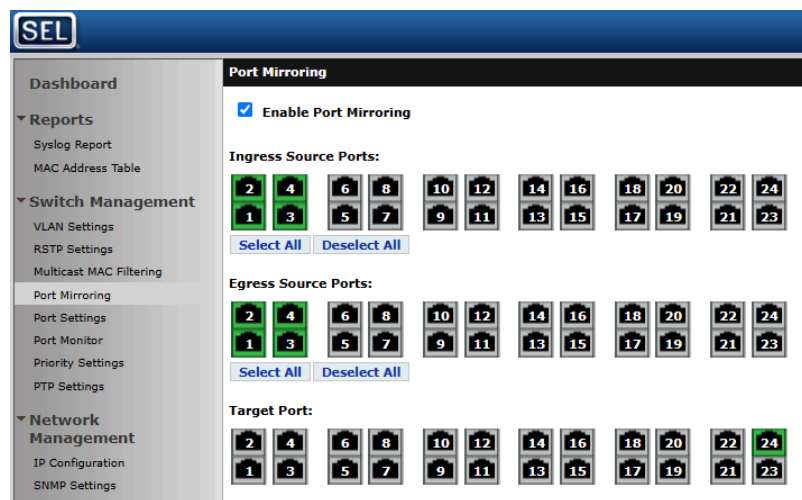


Figure 4.10 Port Mirroring

Port Monitoring

Port monitoring allows you to monitor the health of the port and link for each switch. This feature is always on. Two states are monitored: link and received CRC frame errors. When the link state for a port goes up and down repeatedly in a short amount of time it is typically called "link flapping" and can indicate that the connector is not secured or the neighboring switch may be having issues. When repeated CRC frame errors are received, it can indicate that the link is not reliable. For example, the fiber could be dirty or clouding. Either of these situations could cause the network as a whole to be unreliable if they continue by causing repeated RSTP topology change requests in the event of the link state changing or lost traffic in the event of the CRC frame errors.

SEL RSTP-managed switches monitor these events in a 60-second window. The default link flap threshold is three seconds and the CRC frame error count is five seconds. When these thresholds are reached, the default behavior for the SEL switch is to log the event. You may change the configuration for the switch to disable the port and log the event. The link flap threshold can be configured to a value between one and ten seconds. The CRC frame error count can be configured to a value between one and one million. The 60-second window to monitor for these events cannot be changed. When a port is disabled due to a port monitor event, that port can be re-enabled through the user interface of the switch by using the port settings or the port monitor configuration.

Port Settings Page

The **Port Settings** page allows you to enable and disable ports, set an alias for a port, and configure Rating Limiting protection. The device configures fiber ports automatically to their maximum speed and sets these to full-duplex. The device sets copper ports to Auto.

Rate Limiting

The switch allows you to set the maximum data rate for either ingress or egress traffic for any of the device ports slider controls on the Switch Management/Port Settings page. This protects the link from being oversubscribed. When using egress rate limiting, the class of service priority queues change from the 8:4:2:1 round-robin structure to operate with a 1:1:1:1 structure. *Figure 4.11* shows how limiting can be configured for each port.

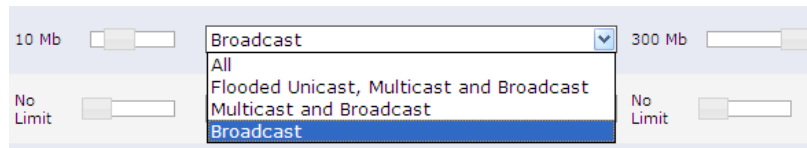


Figure 4.11 Setting Rate Limiting on the Port Settings Page

The Ingress Rate limit can be set using a slider control to **0.1, 0.5, 1, 10, 50, 100, 250, or 500** Mbps for 1 Gbps ports and **0.1, 0.5, 1, 10, 50** Mbps for 100 Mbps ports. For the Ingress traffic, the limit can be set to **All** traffic, **Broadcast**, or mixes of unicast, broadcast, and multicast. The Egress Rate is applied to the overall rate (all traffic from the port).

Priority Settings

Priority settings control the egress order of frames out of a port by using the transmission policy and the assigned priority of each frame, which is based on the priority code point (PCP) or a default value. The PCP value is mapped to the egress priority queue, and the weighted round-robin (WRR) or strict algorithms manage the egress of buffered packets. When changing the PCP value mapping to the switch egress priority, care should be taken in how the chosen egress algorithm will impact congested traffic. Critical priority should be reserved for network control plane traffic.

There are two groups of settings (described in *Table 4.6*): one to control the order in which frames are transmitted from a port and one to configure the PCP-to-priority mapping.

Priority Settings

Transmission Policy:

☒ **Weighted Round Robin**
☐ **Strict**

PCP Mapping:

PCP	Priority
0	Low ▼
1	Low ▼
2	Medium ▼
3	Medium ▼
4	Medium ▼
5	High ▼
6	High ▼
7	High ▼

Figure 4.12 Priority Settings Page (Default Settings)

Table 4.6 Priority Settings

Setting	Valid Values	Default Value	Rules	Description
Transmission Policy	Weighted Round Robin, Strict	Weighted Round Robin	—	Sets the transmission policy for all ports.
PCP Mapping	Priority: Low, Medium, High, Critical	See <i>Table 4.7</i>	Disabled if VLAN-aware is disabled.	Sets the priority for each PCP value for all ports.

The switch supports two transmission policies to decide which packet to egress first when packets of more than one priority are waiting to egress, weighted round robin (WRR) and strict. WRR uses an 8:4:2:1 allocation. Packets of the same priority egress in the order in which they are added to the queue. Strict always egresses higher-priority packets before lower priority packets.

There are eight PCP values (0–7) defined by IEEE 802.1D and IEEE 802.1Q. The PCP Mapping setting is a fixed table with a row for each possible PCP value. If VLAN-aware is enabled, you can modify the priority for each PCP value. By default, the SEL RSTP-managed switches assign the PCP to the priority listed in *Table 4.7*. This mapping applies to all switch ports.

Table 4.7 Default PCP-to-Priority Mapping

PCP	Priority
0	Low
1	Low
2	Low
3	Medium
4	Medium

PCP	Priority
5	Medium
6	High
7	High

Managing Precision Time Protocol

The switch is an IEEE C37.238-2017 Power Profile peer-to-peer (P2P) transparent clock (TC) with syntonization support. The switch can also be used in an IEEE C37.238-2011 and IEEE 1588 Default P2P network to update PTP event messages. The switch does not use PTP to set the system time. PTP is disabled by default, but can be enabled globally for the switch. The switch has the following configuration support shown in *Table 4.8*.

Table 4.8 PTP Settings

Setting	Value	Configurable
P2P Delay Request Interval	1 (in seconds)	Fixed
Domain	0	0–255
VID	None (all PTP messages sourced from the switch are untagged)	Fixed

Network Settings IP Configuration

The **IP Configuration** page provides the configuration options for the IP settings of the device. **ETH F** is used for initial commissioning and local access. A second IP interface, under the **Mgmt** section of the page, can be configured to access the device over the back ports. The Mgmt interface is used for services such as remote management of the device, sending Syslog, or receiving SNMP requests.

Table 4.9 Global IP Settings

Field Name	Values	Default	Description
Hostname ^a	1–63 characters	SEL<SERIAL#>	The unique name identifying the device on the network.
Domain Name ^a	0–253 characters	N/A	The domain name of which the device is a member.
Default Gateway	Unicast network address	N/A	The IP address of the device used to transfer packets to another network. If this setting is left blank, the device will not be able to communicate outside of the local subnet.

^aThe Hostname and Domain Name combined length must be less than 255 characters.

Table 4.10 ETH F Network Interface Settings

Field Name	Values	Default	Description
Alias	1–32 characters	ETH F	A name that is associated with the network interface.
Enabled	Enabled, Disabled	Enabled	Administratively enables or disables the interface.
IP Address	Unicast IP address	192.168.1.2/24	IP address of the interface. The device uses classless inter-domain routing (CIDR) notation to assign the subnet mask. ^a

Field Name	Values	Default	Description
HTTPS	Enabled, Disabled	Enabled	Enables or disables HTTPS on the interface.
Captive Port	Enabled, Disabled	Enabled	Enables or disables captive port on the interface.
SNMP	Enabled, Disabled	Disabled	Enables or disables SNMP on the interface.

^aThe IP address and subnet for ETH F cannot be the same as any of the switch ports or of the Management Network Interface.

Table 4.11 Mgmt Network Interface Settings^a

Field Name	Values	Default	Description
Alias	1–32 characters	Mgmt	A name that is associated with the network interface.
Enabled	Enabled, Disabled	Disabled	Administratively enables or disables the interface.
IP Address	Unicast address	N/A	IP address of the interface. The device uses classless inter-domain routing (CIDR) notation to assign the subnet mask.
VLAN ID	1–4094	1	The VLAN with which to associate the interface. The VLAN must be present to be selected as the management VLAN. This setting is not visible when the device is not in VLAN-aware mode.
HTTPS	Enabled, Disabled	Enabled	Enables or disables HTTPS on the interface.
SNMP	Enabled, Disabled	Disabled	Enables or disables SNMP on the interface.

^aIf you put the management port on a nondefault VLAN, the switch must restart to complete the settings change.

If You Forget Your Switch IP Address

If you forget the IP address for your switch and do not want to perform a full factory reset, the Captive Port feature provides you access to the web management interface.

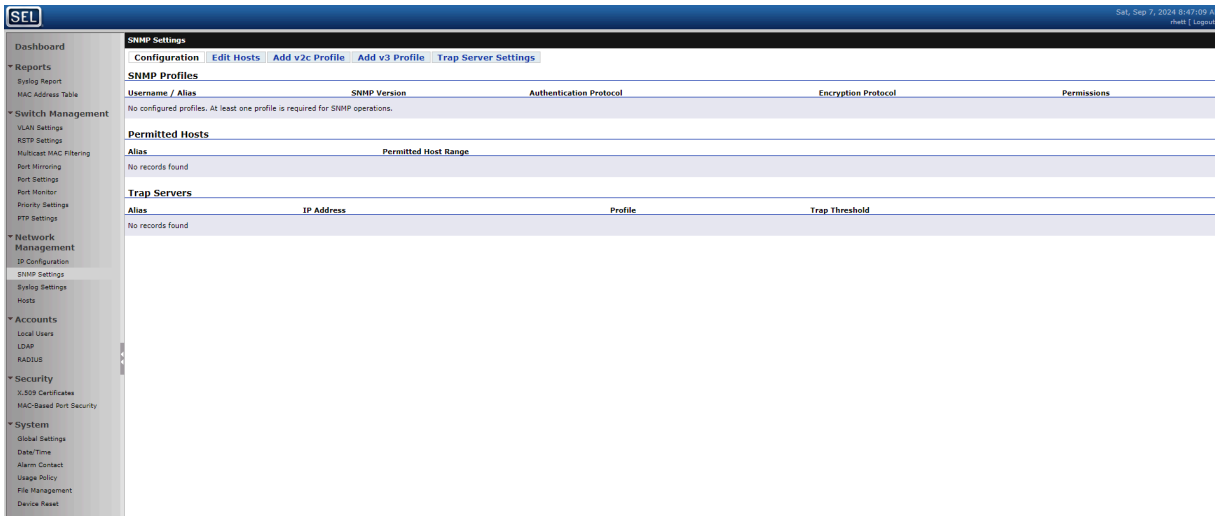
To activate the Captive Port feature on **ETH F**, while the switch is powered on, insert a tool, such as a straightened paper clip, into the pinhole reset hole above Port 2 on the rear panel and press the recessed reset button for 5 seconds. This enables the front Ethernet port and turns on the Captive Port feature.

The Captive Port feature provides special DHCP service to the computer connected to **ETH F**. The DHCP server assigns the computer an IP address adjacent to the IP address of your switch, so the computer will be on the same subnet and capable of communicating with it. This also sets the DNS server for the computer to the IP address of the switch. Once this occurs, any DNS requests from the computer resolve to the switch, so that browsing to any host, such as www.selinc.com, results in opening the web management interface of your switch, and you may also navigate directly to <https://192.168.1.2>.

SNMP Settings

The device supports SNMP v2c, v3, and trap operations. Use SNMP to monitor device health, status, and to gather data. *Figure 4.13* shows the SNMP Settings page.

The SNMP Engine ID for the switch is a sequence of 11 bytes consisting of 80 00 7C 4F 03, followed by the MAC address of the unit. Example: For a unit with MAC address of 00:30:A7:04:5A:CF, the SNMP engine ID would be (shown in hexadecimal) : 80 00 7C 4F 03 00 30 A7 04 5A CF.

**Figure 4.13** SNMP Settings Page

SNMP is disabled by default. You must enable SNMP on the Mgmt interface for the device to respond to SNMP communications.

The **SNMP Profiles** section on the page displays the SNMP profiles configured on the device. The device requires an SNMP profile for it to respond to SNMP requests. The **Add v2c Profile** and **Add v3 Profile** pages provide the interfaces from which you can add SNMP profiles. The SNMP manager requesting SNMP information from the device must be configured with the matching SNMP profile information for the device to respond to the SNMP requests. The device supports as many as eight SNMP profiles. The SEL-2731 does not support none for the SNMPv3 profile—you must select a cryptographic algorithm. The SEL-2731 does not support DES. When importing settings from other SEL RSTP-managed switches that use DES, those settings will not be imported and are left as their default values.

The **Trap Servers** section on the page displays the SNMP trap servers to which the device is configured to send SNMP trap information. An SNMP profile with trap permission is necessary prior to configuring a trap server. The **Trap Servers** web interface page allows you to configure and add a new trap server. The switch sends all the same events over SNMP trap as it does through syslog. For details on what events are logged see *Appendix C: Syslog*.

Add v2c Profile

The **Add v2c Profile** page allows you to add an SNMP v2c profile. You may use v2c version formatted reads. Perform the following steps to add an SNMP v2c profile:

- Step 1. From the **SNMP Settings** page, select **Add v2c Profile**. This will take you to the page shown in *Figure 4.14*.

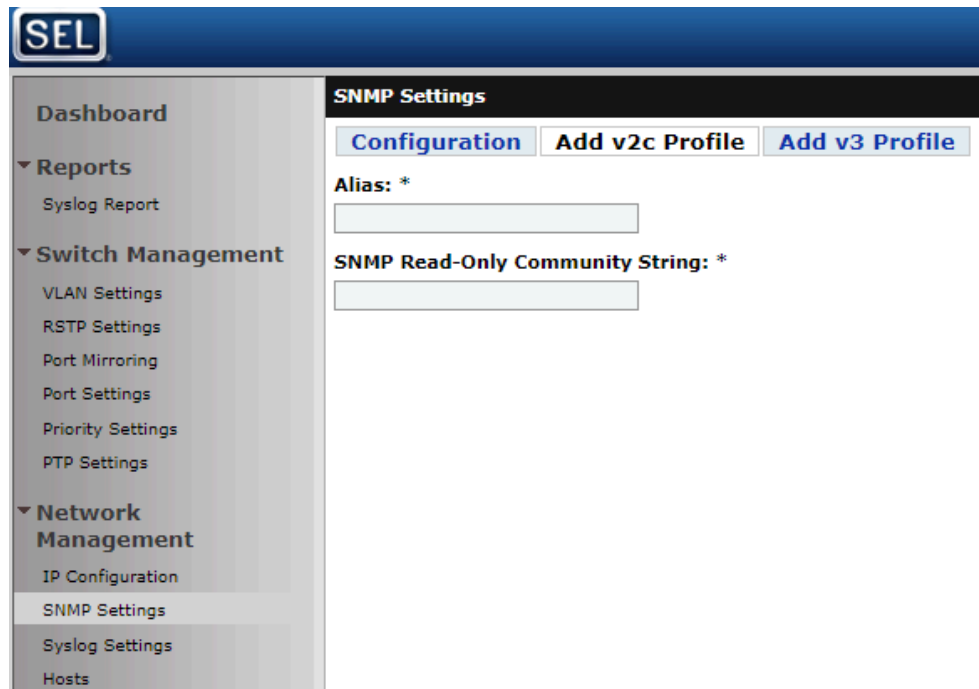


Figure 4.14 Add v2c Profile

Step 2. Enter the **Alias** you will be using for the SNMP profile.

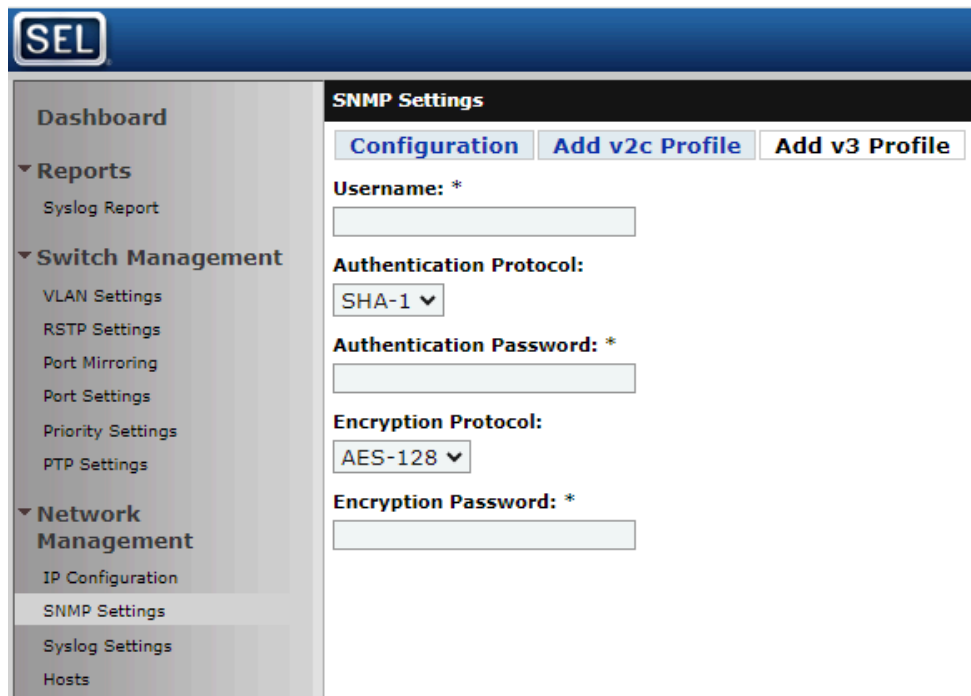
Step 3. Enter the **SNMP Read Only Community String**.

Step 4. Select **Submit** to add the SNMP profile.

Add v3 Profile

The **Add v3 Profile** page allows you to add an SNMP v3 profile. Perform the following steps to add an SNMP v3 profile:

Step 1. From the **SNMP Settings** page, select **Add v3 Profile**.

**Figure 4.15** Add v3 Profile

- Step 2. Enter the **Username** you will be using for the SNMP v3 user.
- Step 3. Specify the **Authentication Protocol**, **Authentication Password**, **Encryption Protocol**, and **Encryption Password**.
- Step 4. Select **Submit** to add the SNMP profile.

Table 4.12 SNMP v2c Profile Settings

Field Names	Values	Default	Description
Alias	1–64 characters	N/A	SNMP v2c alias
SNMP Read Only Community String	1–128 characters	N/A	The read-only community string used to authenticate SNMP sessions

Table 4.13 SNMP v3 Profile Settings

Field Name	Values	Default	Description
Username	1–64 characters	N/A	SNMP v3 username
Authentication Protocol	MD5, SHA-1, SHA-256, SHA-512	SHA-1	Authentication protocol to use for authenticating SNMP messages between this SNMP user and SNMP manager
Authentication Password	8–128 characters	N/A	Cannot be the same as the Encryption Password
Encryption Protocol	AES-128, AES-256	AES-128	Encryption protocol to use for encrypting SNMP messages between this SNMP user and SNMP manager
Encryption Password	8–128 characters	N/A	Cannot be the same as the Authentication Password

Add a Trap Server

The Add Trap Server page allows you to add the SNMP trap servers that the device sends the SNMP trap information to. At least one SNMP profile must be configured before you add a trap server. The device sends trap information to all configured trap servers through the use of the SNMP profiles. The device supports three trap servers. Perform the following steps to add a trap server:

- Step 1. From the SNMP Settings page, select **Add Trap Server**.
- Step 2. Enter the Alias and IP address of the trap server you would like to send SNMP trap information to.
- Step 3. Select the SNMP profile you would like to use.
- Step 4. Enter the desired severity threshold for your trap server.
- Step 5. Select **Submit** to add the SNMP trap server.

MIB Downloads

SNMP Management Information Base (MIB) modules contain definitions and other information about the properties of services and resources of the device. The MIBs can be downloaded from the SEL website on the switch's product page under the support tab. The following table shows the supported MIBs and OIDs.

MIB	Supported OIDs
SNMPv2-MIB	.1.3.6.1.2.1.1.1 sysDescr .1.3.6.1.2.1.1.2 sysObjectID .1.3.6.1.2.1.1.3 sysUpTime .1.3.6.1.2.1.1.4 sysContact .1.3.6.1.2.1.1.5 sysName .1.3.6.1.2.1.1.6 sysLocation
ENTITY-MIB	.1.3.6.1.2.1.47.1.1.1 entPhysicalTable
UCD-SNMP-MIB	.1.3.6.1.4.1.2021.4.5 memTotalReal .1.3.6.1.4.1.2021.4.6 memAvailReal .1.3.6.1.4.1.2021.4.11 memTotalFree .1.3.6.1.4.1.2021.9.1.1 dskIndex .1.3.6.1.4.1.2021.9.1.6 dskTotal .1.3.6.1.4.1.2021.9.1.7 dskAvail .1.3.6.1.4.1.2021.9.1.8 dskUsed .1.3.6.1.4.1.2021.9.1.9 dskPercent
IF-MIB	.1.3.6.1.2.1.2.2 ifTable .1.3.6.1.2.1.31.1.1.1.1 ifName .1.3.6.1.2.1.31.1.1.1.2 ifInMulticastPkts .1.3.6.1.2.1.31.1.1.1.3 ifInBroadcastPkts .1.3.6.1.2.1.31.1.1.1.4 ifOutMulticastPkts .1.3.6.1.2.1.31.1.1.1.5 ifOutBroadcastPkts
LLDP-MIB	.1.0.8802.1.1.2.1.3.7 lldpLocPortTable .1.0.8802.1.1.2.1.4.1 lldpRemTable

MIB	Supported OIDs
BRIDGE-MIB	.1.3.6.1.2.1.17.1.1 dot1dBaseBridgeAddress .1.3.6.1.2.1.17.1.2 dot1dBaseNumPorts .1.3.6.1.2.1.17.1.4.1.1 dot1dBasePort .1.3.6.1.2.1.17.1.4.1.2 dot1dBasePortIfIndex .1.3.6.1.2.1.17.2.1 dot1dStpProtocolSpecification .1.3.6.1.2.1.17.2.2 dot1dStpPriority .1.3.6.1.2.1.17.2.3 dot1dStpTimeSinceTopologyChange .1.3.6.1.2.1.17.2.4 dot1dStpTopChanges .1.3.6.1.2.1.17.2.5 dot1dStpDesignatedRoot .1.3.6.1.2.1.17.2.6 dot1dStpRootCost .1.3.6.1.2.1.17.2.7 dot1dStpRootPort .1.3.6.1.2.1.17.2.8 dot1dStpMaxAge .1.3.6.1.2.1.17.2.11 dot1dStpForwardDelay .1.3.6.1.2.1.17.2.12 dot1dStpBridgeMaxAge .1.3.6.1.2.1.17.2.13 dot1dStpBridgeHelloTime .1.3.6.1.2.1.17.2.14 dot1dStpBridgeForwardDelay .1.3.6.1.2.1.17.2.15 dot1dStpPortTable .1.3.6.1.2.1.17.2.15.1.1 dot1dStpPort .1.3.6.1.2.1.17.2.15.1.2 dot1dStpPortId .1.3.6.1.2.1.17.2.15.1.3 dot1dStpPortState .1.3.6.1.2.1.17.2.15.1.4 dot1dStpPortEnable .1.3.6.1.2.1.17.2.15.1.5 dot1dStpPortPathCost .1.3.6.1.2.1.17.2.15.1.6 dot1dStpPortDesignatedRoot .1.3.6.1.2.1.17.2.15.1.7 dot1dStpPortDesignatedCost .1.3.6.1.2.1.17.2.15.1.8 dot1dStpPortDesignatedBridge .1.3.6.1.2.1.17.2.15.1.9 dot1dStpPortDesignatedPort .1.3.6.1.2.1.17.4.3.1.1 dot1dTpFdbAddress .1.3.6.1.2.1.17.4.3.1.2 dot1dTpFdbPort .1.3.6.1.2.1.17.4.3.1.3 dot1dTpFdbStatus .1.3.6.1.2.1.17.5.1.1.2 dot1dStaticReceivePort .1.3.6.1.2.1.17.5.1.1.1 dot1dStaticAddress
SNMP-FRAMEWORK_MIB	.1.3.6.1.6.3.10.2.1.1 snmpEngineID .1.3.6.1.6.3.10.2.1.2 snmpEngineBoots .1.3.6.1.6.3.10.2.1.3 snmpEngineTime .1.3.6.1.6.3.10.2.1.4 snmpEngineMaxMessageSize
Q-BRIDGE-MIB	.1.3.6.1.2.1.17.7.1.4.2.1.1 dot1qVlanTimeMark .1.3.6.1.2.1.17.7.1.4.2.1.2 dot1qVlanIndex .1.3.6.1.2.1.17.7.1.4.2.1.3 dot1qVlanFdbId .1.3.6.1.2.1.17.7.1.4.2.1.4 dot1qVlanCurrentEgressPorts .1.3.6.1.2.1.17.7.1.4.2.1.5 dot1qVlanCurrentUntaggedPorts .1.3.6.1.2.1.17.7.1.4.2.1.6 dot1qVlanStatus .1.3.6.1.2.1.17.7.1.4.2.1.7 dot1qVlanCreationTime .1.3.6.1.2.1.17.7.1.4.3.1.1 dot1qVlanStaticName .1.3.6.1.2.1.17.7.1.4.3.1.2 dot1qVlanStaticEgressPorts .1.3.6.1.2.1.17.7.1.4.3.1.3 dot1qVlanForbiddenEgressPorts .1.3.6.1.2.1.17.7.1.4.3.1.4 dot1qVlanStaticUntaggedPorts .1.3.6.1.2.1.17.7.1.4.3.1.5 dot1qVlanStaticRowStatus
SEL-2700-POWER-SUPPLY-MIB	.1.3.6.1.4.1.31823.1.2700.2.1.1.1.1 sel2700PowerSupplyIndex .1.3.6.1.4.1.31823.1.2700.2.1.1.1.2 sel2700PowerSupplyAlias .1.3.6.1.4.1.31823.1.2700.2.1.1.1.3 sel2700PowerSupplyState .1.3.6.1.4.1.31823.1.2700.2.1.1.1.4 sel2700PowerSupplyStatus
RSTP-MIB	.1.3.6.1.2.1.17.2.16 dot1dStpVersion .1.3.6.1.2.1.17.2.17 dot1dStpTxHoldCount

SNMP Trap

MIB	OID
SYSLOG-MSG-MIB	.1.3.6.1.2.1.192.0 syslogMsgNotifications

Syslog Settings

Syslog is a specification that describes both the method and format in which the device stores logs locally and sends them to a collector. The device logs many different types of events such as system startup, log in attempts, network events, and configuration changes. The device can send log information to as many as three remote destinations and store as many as 60,000 event logs locally in nonvolatile memory. Each destination, including the local device, has a configurable logging threshold. The device logs all configuration changes to Syslog.

Select the **Syslog Settings** link from the navigation menu to configure the Syslog settings for the device. The **Syslog Settings** page (see *Figure 4.16*) allows you to configure the logging threshold for local logging and remote Syslog destinations, which determines what severity levels are logged. *Table 4.14* lists what severity levels are logged for each logging threshold. See *Appendix C: Syslog* for a list of Syslog events and their associated severity levels.

Table 4.14 Severity Levels

Logging Threshold	Severity Levels Logged
Alert (Highest Severity) ^a	Alert
Critical ^a	Alert, Critical
Error	Alert, Critical, Error
Warning	Alert, Critical, Error, Warning
Notice	Alert, Critical, Error, Warning, Notice
Informational (Lowest Severity)	Alert, Critical, Error, Warning, Notice, Informational

^aNot available for Local Logging Threshold.

Syslog Settings

Local Logging Threshold: ? |
Notice ▾

Syslog Destinations

Alias	IP Address* ?	Logging Threshold* ?	
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	Warning ▾	<input type="button" value="Clear"/>
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	Warning ▾	<input type="button" value="Clear"/>
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	Warning ▾	<input type="button" value="Clear"/>

Figure 4.16 Syslog Settings

Table 4.15 Syslog Threshold Values

Field Name	Values	Default	Description
Local Logging Threshold	Error	Notice	Controls the severity levels logged to the device (see <i>Table 4.14</i>).
	Warning		
	Notice		
	Informational		

The settings under Syslog Destinations are for configuring remote Syslog destinations. You can configure as many as three remote destinations. To configure the device to send Syslog events to a remote Syslog server, enter the **Alias** and **IP Address** of the remote Syslog server, and select the logging threshold of the Syslog events to be sent to the remote Syslog server.

Table 4.16 Syslog Destination Settings

Field Name	Values	Default	Description
Alias	0–32 characters		A name that is associated with the Syslog destination.
IP Address	Unicast IP Address		The IP address of the Syslog destination.
Logging Threshold	Alert	Warning	Controls the severity levels logged to the device (see <i>Table 4.14</i>).
	Critical		
	Error		
	Warning		
	Notice		
	Informational		

Security

X.509 Certificates

HTTPS (SSL/TLS) connections require authentication to confirm that the server you are communicating with is the correct server. This authentication is through X.509 certificates. By default, the device has a self-signed X.509 certificate that can cause your web browser to issue a security alert. This security alert will require a security exception for authentication to continue. To prevent this security alert from appearing, install a CA-signed X.509 certificate on the device. If your web browser has been configured to trust the CA issuing and signing the certificate, the X.509 certificate will be trusted and the security alert will no longer appear.

The device supports one X.509 certificate that is used for HTTPS communications between the client web browser and the web server running on the device. The X.509 Certificates page has options to view, rename, export, import, and regenerate the X.509 certificate. Descriptions follow for each of these options.

LDAP and RADIUS also use X.509 certificates.

View

This option provides a detailed view of the installed certificate.

Rename

This option provides a form for renaming the certificate. The Certificate Name can contain as many as 128 characters.

— X.509 Certificate Rename —

Certificate Name:
Default_Web_Cert

Figure 4.17 Renaming Certificates

Installing a New Web Certificate

The switch comes configured with a self-signed X.509 certificate. SEL recommends installing a CA-signed X.509 certificate on the device. Perform the following steps to install a new web certificate on the switch.

- Step 1. Navigate to the **X.509 Certificates** page.
- Step 2. Select **Import** (at the top of the page).
- Step 3. Add a **Certificate Alias** and a **Password** (if required).
- Step 4. Select **Browse** and select the new web certificate.

X.509 Certificates

[List Certificates](#) [Import](#)

Certificate Alias:
Web Certificate

Password:

Certificate: *
[Browse...](#) Web Certificate.pem

Figure 4.18 Uploading a New X.509 Certificate

- Step 5. Select **Submit**. If the certificate is valid, it will appear in the list of certificates with an **Activate** button.

X.509 Certificates

X.509 certificate imported successfully.

[List Certificates](#) [Import](#)

Certificate Alias	Common Name (CN)	Valid End	
✓ Default_Web_Cert	http://www.selinc.com/EthernetCommunications/	2032-05-07 00:00:00+00	View Rename
RADIUS	CA.commslab.local	2023-07-12 00:00:00+00	View Rename Delete
Web Certificate	Valid Cert	2012-06-29 00:00:00+00	View Rename Delete Activate

Figure 4.19 Successful Upload of a New X.509 Certificate

- Step 6. Select **Activate** for the new certificate and then **Yes** to continue. The switch will refresh the web interface; when the **Activating certificate** button turns green, select it to return to the web interface.

You can confirm that the X.509 certificate is active by navigating to the **X.509 Certificates** page.

There should be a check mark (✓) to the left of the alias of the certificate you activated. You may remove the self-signed certificate by selecting the **Delete** button for the Default_Web_Cert certificate.

X.509 Certificates			
List Certificates Import			
Certificate Alias	Common Name (CN)	Valid End	
RADIUS	CA.commslab.local	2023-07-12 00:00:00+00	View Rename Delete
<input checked="" type="checkbox"/> Web Certificate	Valid Cert	2012-06-29 00:00:00+00	View Rename

Figure 4.20 New Certificate Is Activated

System

Global Settings

Web Settings

The web settings allow for modification of settings related to the web management interface of the device.

Table 4.17 Web Settings

Field Name	Values	Default	Description
Language	English, Spanish	English	The default language for the device.
Maximum Sessions	1–20	5	Maximum number of concurrent web user sessions.
Sessions Timeout	1–60 minutes	5	Amount of time a user's session is inactive before the device terminates the session.

System Contact Information

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

Table 4.18 System Contact Information Settings

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

Table 4.19 Features

Field Name	Values	Default	Description
VLAN-aware	Enabled, Disabled	Disabled	Determines the operational mode of the device with respect to VLANs.
Spanning Tree Mode	RSTP, Off	RSTP	Configures the spanning tree mode for the device. The device does not provide network loop prevention if this setting is disabled.
LLDP	Enabled, Disabled	Enabled	Enables or disables Link Layer Discovery Protocol (LLDP) on the device.

Date/Time

The date and time functions of the device allow accurate timekeeping for time-stamping internally generated system events. The date and time of the device can be manually set, or the device can synchronize its internal clock to Network Time Protocol (NTP) servers over the network. One benefit of synchronizing time by using NTP is that all devices synchronized to the NTP servers share the same time, and event correlation across multiple systems is possible. Having the same time reference for time-stamped events makes auditing system and security events across multiple systems easier to manage.

Manually Updating Date/Time

Time zone selection is important in how the switch determines daylight-saving adjustments. To select a time zone, find the appropriate time zone entry in the **Time Zone** dropdown list and select **Submit**.

Note: Updating the time zone or time may cause the web management session to expire. You will need to log back onto the device after changing the time zone or time.

In installations where NTP sources are unavailable, manual date and time configuration is necessary. To manually configure the date and time of the device, select the current date from the calendar, enter the current time, and select **Submit**.

NTP

NTP is a method for synchronizing system clocks over IP networks. NTP typically maintains accuracies of 10 ms across public networks and 200 μ s or better in private networks under ideal conditions.

The switch uses NTP version 4.0 and is backward-compatible with older versions, including NTPv3 and NTPv2, but not NTPv1.

To use NTP as the time source for the device, you must select **Enable NTP Client** and enter at least one NTP Server's IP address. When more than one NTP server is entered, the switch will look to synchronize on the primary server entered in position 1. When that server is not available, the switch will try and synchronize to the server in position 2 and then to position 3. Select the **Submit** button.

Alarm Contact

Each switch has one Form C alarm contact output that can be used to alert system personnel about system- or security-related events. The events are divided into seven categories that can either be configured with one of three alarm contact behaviors or disabled so that the switch does not operate the alarm contact for those events. The alarm contact on and off duration for latching and pulsing are configurable. These durations apply to all pulsing and latching events.

Settings

There are three groups of settings: one to enable the event categories (see *Table 4.20*), one to select the alarm contact behavior (see *Table 4.21*), and one for the on and off durations (see *Table 4.23*).

Alarm Contact

Pulse Duration:

On Time

1

second(s)

Off Time

1

second(s)

Alarm Contact Output Triggers

Contact Behavior

☒

Authentication

Pulse

☒

Chassis

Pulse

☐

Configuration

Pulse

☐

Eth F Link

Pulse

☐

Link

Pulse

☐

Port Security

Pulse

☐

Rapid Spanning Tree Protocol

Pulse

☒

System Integrity

Latch (Automatic Clear)

Figure 4.21 Alarm Contact Page (Default Settings)

Table 4.20 Alarm Contact Categories

Category	Default Enable Setting	Default Contact Behavior	Description
Authentication	Enabled	Pulse	Authentication-related events
Chassis	Enabled	Pulse	Physical hardware-related events
Configuration	Disabled	Pulse	Configuration events related to settings changes
Eth F Link	Disabled	Pulse	Front-port interface events related to link up/link down status.
Link	Disabled	Pulse	Interface events related to link up/link down status
Port Security	Disabled	Pulse	MAC-based port security violations
Rapid Spanning Tree Protocol	Disabled	Pulse	RSTP-related events, such as topology changes
System Integrity	Enabled	Latch (Automatic Clear)	System event, such as component failure or a part number change (also referred to as Major Alarms)

Table 4.21 Alarm Contact Behaviors

Behavior	Description
Pulse	The alarm contact asserts for the on time and then deasserts for the off time.
Latch (Manual Clear) or Latch (Automatic Clear)	The alarm contact asserts for at least as long as the on time. The alarm contact then deasserts for at least as long as the off time after the user manually clears the alarm via the web interface for both types of latches. Automatically clearing latches are automatically cleared if the underlying cause of the event is resolved. If cleared during the on time period, the alarm contact deasserts immediately after the on time expires.

The Latch (Automatic Clear) behavior depends on the category of the alarm, as shown in *Table 4.22*.

Table 4.22 Latch (Automatic Clear) Behavior

Alarm Category	Alarm Is Automatically Cleared When...
Authentication	Alarm is manually cleared.
Chassis	The switch is turned off and back on.
Configuration	
Eth F Link	Front port is up.
Link	All enabled back ports are up. ^a
Port Security	Alarm is manually cleared.
Rapid Spanning Tree Protocol	The switch is turned off and back on.
System Integrity	Alarm is manually cleared. ^b The switch is turned off and back on. ^b The underlying cause is corrected (e.g., the battery is replaced).

^aLatching is caused by at least one port being down but enabled. The latch remains asserted until all links are up and On Time and Off Time shall be honored. For example, if 10 ports lose their link (link down) and 5 of those ports recover their link, the alarm remains latched. Once the last five ports recover their link, the alarm autoclears as the On Time and Off Time are honored.

^bThe alarm reasserts if the underlying cause is still present during the next diagnostics cycle, e.g., if the battery is still missing.

Table 4.23 Pulse Duration Settings^a

Setting	Default	Range	Description
On Time	1 s	1–10 s	Minimum duration for which the alarm contact asserts.
Off Time	1 s	1–10 s	Minimum duration for which the alarm contact deasserts.

^aThese apply to latching events as well as pulsing events.

To enable a category, select the check box to the left of the category name. To change the behavior of the alarm contact for that category, use the dropdown box to the right of the category name.

System Integrity alarms representing diagnostics are pooled once per cycle. If the alarm is manually cleared and the underlying cause persists, the configured alarm contact behavior event reoccurs.

For both Link Alarms (Link: **ETH F** or Link: Ports 1–24), there are no warnings to the user when they enable a Link alarm when the physical port is disabled. For example, if Link alarm for **ETH F** is enabled but in the IP Configuration, the physical **ETH F** is disabled, the user will not be warned and **ETH F** will never trigger a Link alarm. This is true for Ports 1–24 as well. If Ports 13–24 are physically disabled and the Link alarm for Ports 1–24 are enabled. The user is not warned that some ports are physically disabled, but alarms occur for port activity on the physically enabled Ports 1–12.

Alarm Contact Behavior

If no other event in an enabled event category occurs while the alarm contact is pulsing or latching, the alarm contact follows the behavior described in *Table 4.21*.

If more than one event occurs during the on or off time of a latch or pulse the alarm contact operates according to the following rules:

- A latching event always interrupts a pulse, regardless of whether the on or off time has expired.
- Pulsing events are ignored during the on time of a pulse or a latch.
- If one or more pulsing events occur during the off time of a pulse or a latch, or if one or more latching events occur and are cleared during the off time of the latch, the alarm contact pulses once more after the off time has expired.
- During a latching event, the alarm contact always asserts for at least the on time and remains asserted until all latching events are cleared, including all latching events that occurred during the on time of the original latching event.
- Once in the off time of a latch, the alarm contact remains deasserted until at least the off time expires, regardless of any pulsing or latching events that occur during this time.

To unambiguously differentiate between a latching event and a pulsing event, use a manually clearing latch behavior. Events are also logged to the Syslog Report page and sent to any configured Syslog servers regardless of the alarm contact settings or behavior.

Usage Policy

The device presents a usage policy to all users accessing the login page. This policy notifies users of what constitutes the appropriate use of this device what actions are taken to ensure the device is not used inappropriately, and what actions will be taken if abuse is discovered. The device comes with the following default usage policy:

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

The usage policy is configurable from 0 to as many as 4095 characters. Select the **Usage Policy** link from the navigation menu to modify the usage policy.

File Management

File management provides an interface from which you can import and export settings, as well as perform firmware upgrades and download diagnostics reports. Exporting system settings is useful for providing device configuration backups for disaster recovery, as well as for creating a template configuration that you can use in commissioning large numbers of devices. For example, if all devices share the same configuration except for a few device-specific configuration items such as hostname and IP address, the configuration can be created once and then exported as a template. When the configuration file is imported into a new device, only a couple of changes are necessary before the device is fully configured. The SEL-2730M settings files are supported when importing to other SEL RSTP-managed switches. When there are settings compatibility issues between imports, the switch sets the defaults.

Export Settings

Settings can be exported either encrypted or unencrypted in XML format. The encrypted settings export is useful for creating an encrypted copy of the device configuration as a device backup. You can use this backup for disaster recovery purposes in the event the configuration on the device must be restored. The other option is to export the device settings in unencrypted XML format, which allows for offline editing.

Note: Settings files should be stored in a secure location because they contain sensitive information.

The **Export Settings** page provides an interface to export settings to either an encrypted or unencrypted settings file. Follow these steps to export a settings file:

Step 1. Log in to the device and browse to the **File Management** page.

You should be on the **Export Settings** page shown in *Figure 4.22*.

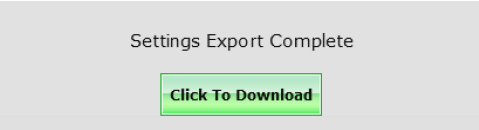
Figure 4.22 Export Settings Page

Step 2. If you would like to export settings in an encrypted format, select the **Encrypt Export** check box and enter an encryption password for use in encrypting the settings file. You must use this password when you perform an import of the encrypted settings file, so be sure you store the password in a secure location.

If you would like to export settings in an unencrypted format, clear the **Encrypt Export** check box.

Step 3. Select the **Export** button.

The settings export will initialize and show the export progress for each module. The device will present you with the following message when the export is complete.



- Step 4. Select the **Click to Download** button. Your browser then downloads the file.

Diagnostics Report

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

- Step 1. Log in to the device and browse to the **File Management** page.
- Step 2. Select **Diagnostics Report**.
- Step 3. Select **Generate**.
- Step 4. Select **Click to Download** (see *Figure 4.23*) to download the hostname_diagnostics.log file that you can share with your SEL representative.

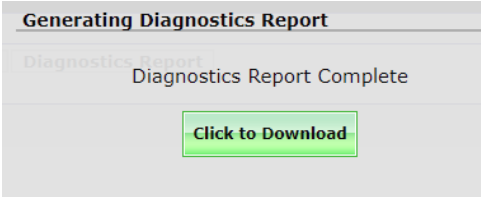


Figure 4.23 Diagnostics Report Complete

Import Settings

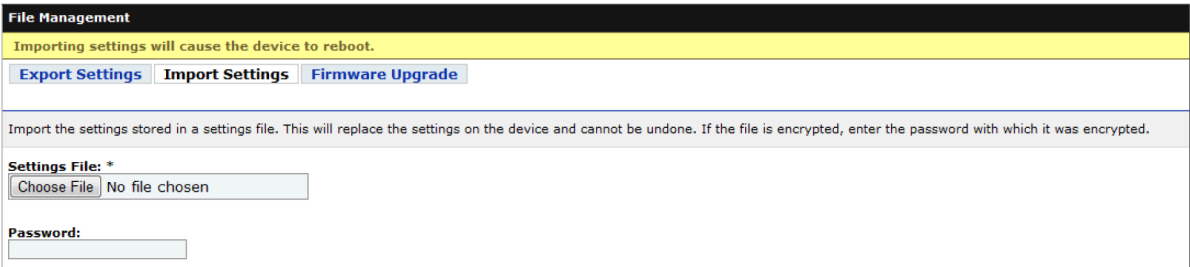


Figure 4.24 Import Settings Page

The **Import Settings** page provides an interface to import settings from either an encrypted or unencrypted settings file. Perform the following to import a settings file:

- Step 1. Log in to the device and browse to the **File Management** page.
- Step 2. Select the **Import Settings** tab at the top of the page.

⚠ WARNING
Importing settings will replace the current settings and reboot the device.

- Step 3. Select **Choose File** and browse to the location of the settings file you would like to import.
- Step 4. If the file was encrypted during the export process, enter the encryption password into the **Password** field. If the file was not encrypted during the export process, leave the **Password** field blank.
- Step 5. Select the **Import** button.

The settings import feature supports the ability to import settings from the same switch model and from other switch models from SEL that use RSTP. For example, SEL-2730M exported settings file can be imported into the SEL-2731. Settings discrepancies between the file being imported and the receiving switch are resolved as follows:

- When the switch you are importing the settings file into has a setting that is also in the file being imported, the value of that setting will be applied.
- When the switch you are importing the settings file into has a setting that is not in the file being imported, the value of that setting will be left at default.
- When the file being imported has a setting that is not in the switch, the setting in the import file is not applied.

Firmware Upgrade

The **Firmware Upgrade** page provides an interface from which you can upgrade device firmware. Firmware upgrades are digitally signed and validated before the switch installs the new firmware in order to maintain the firmware integrity. During a firmware upgrade there are many stages that are displayed allowing progress to be tracked. The switch will reboot at the end of the firmware upgrade process and boot into the new firmware. Network communications may be disrupted during the firmware upgrade.

Device Reset

Device Reboot

The device reboot function turns the device off and back on. All communication through the device is lost while the device restarts.

Factory Reset

The device provides a factory-reset function to restore the unit to its factory configuration. You should only use this feature when you decommission the device. The factory-reset, function erases the device log files and returns device settings back to their factory-default values. To perform a factory-default reset, press and hold the **Reset** button while applying power. Hold the **Reset** button through the boot cycle and wait for the switch to enable and pulse the alarm LED on the front again. (This typically takes approximately 30 seconds.) After a factory reset, you must recommission the device.

Firmware and User's Guide Versions

Firmware

Determining the Firmware Version

To determine the firmware version, log in to the web interface and check the Dashboard page. The Device Information section displays the Firmware Identification (FID) number.

The firmware version will be either a standard release or a point release. A standard release adds new functionality to the firmware beyond the specifications of the existing version. A point release is reserved for modifying firmware functionality to conform to the specifications of the existing version.

A standard release is identified by a change in the R-number of the device FID number. The RSTP managed switch technology is designed to operate in many products. The switch product numbers are indicated by the SEL-2731. The "M" is the indication that this firmware is an RSTP-based managed switch.

Existing firmware:

FID=SEL-2731M-**R100**-V0-Z001001-Dxxxxxxxx

Standard release firmware:

FID=SEL-2731M-**R101**-V0-Z001001-Dxxxxxxxx

A point release is identified by a change in the V-number of the device FID number.

Existing firmware:

FID=SEL-2731M-R100-**V0**-Z001001-Dxxxxxxxx

Point release firmware:

FID=SEL-2731M-R100-**V1**-Z001001-Dxxxxxxxx

The date code is after the D. For example, the following is firmware version number R100, release date October 31, 2023.

FID=SEL-2731M-R100-V0-Z001001-**D20231031**

Revision History

Table A.1 and *Table A.2* list the firmware versions, revision descriptions, and corresponding user's guide date codes.

Changes that address security vulnerabilities are marked with "[Cybersecurity]". Other improvements to cybersecurity functionality that should be evaluated for potential cybersecurity importance are marked with "[Cybersecurity Enhancement]".

Table A.1 SEL-2741 Firmware Revision History

Firmware Identification (FID) Number	Summary of Revisions	User's Guide Date Code
SEL-2741M-R101-V0-Z002001-D20250220	➤ Initial version.	20250220

Table A.2 SEL-2731 Firmware Revision History

Firmware Identification (FID) Number	Summary of Revisions	User's Guide Date Code
SEL-2731M-R101-V0-Z001001-D20240930	<ul style="list-style-type: none"> ➤ Added support for static and dynamic MAC port security. ➤ Added support for multicast MAC filtering. ➤ Added support to provide the MAC table via the user interface, SNMP using the Bridge MIB, or by downloading the information to a .csv file. ➤ Added support to monitor port link flapping and CRC errors. ➤ Added support for SNMP to add allowed hosts. ➤ Added support to monitor the power supply status through SNMP SEL-2700-POWER-SUPPLY MIB. ➤ Added support for 100/1000BASE-T copper SFPs. ➤ Added support for SHA-256 in SNMPv3. ➤ Added support to log an event when SFPs are inserted or removed. ➤ Added support to include the root bridge identifier when root changes. ➤ Added support to configure the PTP domain. ➤ Added support for the strict port priority queue transmission policy. ➤ Addressed an issue in the previous release where egress rate limiting was not weighting the traffic with the applied priority algorithm. ➤ Enhanced the port diagnostics to include packets dropped because they were tagged with a VLAN that the switch port is not configured to support. ➤ Added support to include the LLDP Port VLAN IDs. 	20240930
SEL-2731M-R100-V1-Z001001-D20240523	Includes all the functions of SEL-2731M-R100-V0-Z001001-D20231120 with the following addition: <ul style="list-style-type: none"> ➤ Improved flash memory reliability. 	20240523
SEL-2731M-R100-V0-Z001001-D20231120	➤ Initial version.	20231120

User's Guide

The date code at the bottom of each page of this user's guide reflects the creation or revision date.

Table A.3 lists the user's guide versions and revision descriptions. The most recent user's guide revisions are listed first.

Table A.3 User's Guide Revision History

Date Code	Summary of Revisions
20250220	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Updated <i>Product Features and Specifications</i>. <p>Section 4</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 4.10: Port Mirroring</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for SEL-2741 firmware version R101-V0.

Date Code	Summary of Revisions
20240930	<p>Section 1</p> <ul style="list-style-type: none"> ► Updated <i>Product Features and Specifications</i>. <p>Section 3</p> <ul style="list-style-type: none"> ► Updated <i>If You Forget Your Administrative Account Password</i>. <p>Section 4</p> <ul style="list-style-type: none"> ► Updated <i>Introduction, Reports, Root Bridge, Port Settings, Priority Settings, Managing Precision Time Protocol, and Network Settings</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ► Updated for SEL-2731 firmware version R101-V0. <p>Appendix C</p> <ul style="list-style-type: none"> ► Updated <i>Table C.3: Event Logs</i>. <p>Appendix D</p> <ul style="list-style-type: none"> ► Updated <i>Ports and Services</i>.
20240523	<p>Section 4</p> <ul style="list-style-type: none"> ► Updated <i>Port Settings</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ► Updated for SEL-2731 firmware version R100-V1.
20231120	<ul style="list-style-type: none"> ► Initial version.

This page intentionally left blank

Firmware Upgrade Instructions

Introduction

These instructions guide you through the process of upgrading firmware in the device. The firmware upgrade will be either a standard release or a point release. A standard release adds new functionality to the firmware beyond the specifications of the existing version. A point release is reserved for modifying firmware functionality to conform to the specifications of the existing version.

Firmware Files

Switch firmware upgrade files have a tar.gz file name extension. An example firmware filename is install_2731M_R100.tar.gz.

The firmware packages are cryptographically signed to enable the device to recognize official SEL firmware. Any uploaded files that cannot be verified as being produced by SEL will not be processed.

Firmware Upgrade Procedure

To perform an upgrade, you will need the appropriate firmware upgrade file and access to an administrative account on the device. Upgrade the device firmware by uploading a file from the device via the web interface. All firmware updates are logged. Perform the following steps to upgrade the switch firmware:

- Step 1. Log in using an account with administrative-level privileges. Nonadministrative accounts cannot perform firmware upgrades.
- Step 2. Select the **File Management** link from the navigation panel. This will show the File Management page where firmware upgrades may be performed.
- Step 3. In the **File Management** window, select the **Firmware Upgrade** button to display the version of the currently running firmware, and select the upgrade file to upload to the unit (see *Figure B.1*).

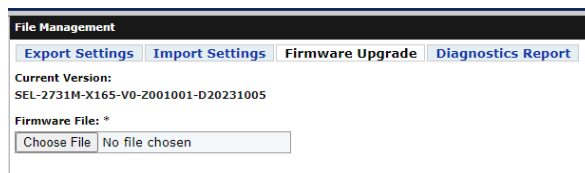


Figure B.1 File Management

- Step 4. Enter the path name for the upgrade file. To locate the file instead using the Windows file browser, select the **Browse** button, navigate to the location where the upgrade file is stored, select it, and select **Open**.

- Step 5. Select the **Upgrade** button at the bottom of the page to upload and install the new firmware. The **Upgrading Firmware** status display will appear and periodically update the displayed progress of the upgrade operation as it proceeds. The firmware update takes about 10 minutes to complete.

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

Syslog

Introduction

The Syslog Protocol, defined in RFC 3164, provides a transport that allows a device to 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, that are 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. Also, 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.

Higher severities have lower numerical codes, as shown in *Table C.1*.

Table C.1 Syslog Message Severities Reported by the SEL-2731

Numerical Code	Severity
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational

The Facility code, shown in *Table C.2*, defines from which application group the message originated.

Table C.2 Syslog Message Facilities

Numerical Code	Facility
0	Kernel messages
1	User-level messages
2	Mail system
3	System daemons
4	Security/authorization messages ^a
5	Messages generated internally by Syslog

Numerical Code	Facility
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 ^b
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)

^aVarious 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.

^bVarious operating systems have been found to use both Facilities 9 and 15 for clock (cron/at) messages.

Source: www.faqs.org/rfcs/rfc5424.html

- 2. HEADER:** The header of a Syslog packet contains the time stamp and the source of the message. The IP address or the hostname defines the source of the message originator. Time stamps are based on the time of 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 has been provided below. This particular message shows an invalid login attempt on July 09, 2009, at 08:17:29 to "myhostname" for user root from the IP address 192.168.1.1. The priority of this message is 34.

```
<34>Jul 09 2009 08:17:29 myhostname Invalid login attempt by:
root at 192.168.1.1
```

The Syslog message has been divided into each respective part as shown.

PRI	HEADER	MSG
<34>	Jul 09 2009 08:17:29 myhostname	Invalid login attempt by: root at 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 so that newer messages overwrite older messages after the buffer is filled. Support for multiple remote Syslog servers provide the added benefits of centralized logging, which includes larger storage capacity, centralized event analysis and correlation, and archival of event logs.

Switch Event Logs

The switch records and time-stamps all events in the Syslog format consistent with the Syslog description from RFC 3164. *Table C.3* lists all of the events that the switch logs and the record that is generated with each of these events.

Log messages may contain words or phrases in brackets such as {username}. This notation indicates that this is a variable that will be replaced with the value being logged. For example, the {username} in Syslog message User account {username} locked out due to consecutive failed login attempts would be replaced with the actual username that was locked out.

Table C.3 Event Logs

Message	Tag Name	Severity	Facility
Alarm Contact: configuration changed by {username} at {user_ip}	Alarm Contact	Notice	USER
Captive Port: disabled by {username} at {user_ip}	CaptivePortConfig	Notice	USER
Captive Port: enabled by {username} at {user_ip}	CaptivePortConfig	Notice	USER
Device commissioned by {0} at {user_ip}	Commissioning	Notice	SECURITY
Device factory reset initiated by {username} at {user_ip}	Commissioning	Notice	SECURITY
Usage Policy: changed by {username} at {user_ip}	Config	Notice	SECURITY
Port Settings: changed by {username} at {user_ip}	Config	Notice	SYSTEM
Spanning Tree: Configuration changed by {username} at {user_ip}	Config	Notice	USER
Priority assigned to PCP value {0} changed from {1} to {2} by {username} at {user_ip}	Config	Notice	USER
Transmission policy changed from {0} to {1} by {username} at {user_ip}	Config	Notice	USER
System Contact Information: changed by {username} at {user_ip}	Config	Notice	USER
RADIUS Accounting disabled by {username} at {user_ip}	Config	Notice	USER
RADIUS Accounting enabled by {username} at {user_ip}	Config	Notice	USER
RADIUS Accounting Connection: Accounting server does not respond	Config	Notice	USER
RADIUS Accounting settings change by {username} at {user_ip}	Config	Notice	USER
RADIUS Accounting Connection: Active server changed to server {0}	Config	Notice	USER
System Time: manually synchronized to external source by {username} at {user_ip}	DateTime	Notice	USER
System Time: lost synchronization to external source	DateTime	Warning	SYSTEM
System Time: synchronized via NTP	DateTime	Notice	SYSTEM
NTP Server {0}: created by {username} at {user_ip}	DateTimeConfig	Notice	USER

Message	Tag Name	Severity	Facility
NTP Server {0}: deleted by {username} at {user_ip}	DateTimeConfig	Notice	USER
System Time: changed from {0} to {1} by {username} at {user_ip}	DateTimeConfig	Notice	USER
Time Source: set to {0} by {username} at {user_ip}	DateTimeConfig	Notice	USER
Time Zone: changed from {0} to {1} by {username} at {user_ip}	DateTimeConfig	Notice	USER
Error: Device rebooted due to unrecoverable system error: {0}	Diagnostics	Critical	SYSTEM
Diagnostics Report generated by {username} at {user_ip}	Diagnostics	Notice	USER
Uploaded firmware update package is corrupted; unable to decrypt the firmware update package or validate the signature on the firmware update package	Firmware	Error	SYSTEM
The firmware version downgrade is not compatible with the current firmware	Firmware	Error	SYSTEM
Firmware: reversion to previous version initiated by {username} at {user_ip}	Firmware	Warning	USER
Firmware update from {0} to {1} succeeded	Firmware	Warning	SYSTEM
Firmware: update to new version initiated by {username} at {user_ip}	Firmware	Notice	USER
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
Host Settings: Added host {0} with IP address {1} by {username} at {user_ip}.	HostConfig	Notice	USER
Host Settings: Removed host {0} with IP address {1} by {username} at {user_ip}.	HostConfig	Notice	USER
Host Settings: Changed hostname {0} with IP address {1} to {2} with IP address {3} by {username} at {user_ip}.	HostConfig	Notice	USER
Configuration file export failed	ImportExport	Warning	USER
Configuration file export started by {username} at {user_ip}	ImportExport	Notice	USER
Configuration file export successful	ImportExport	Notice	USER
Configuration file import failed	ImportExport	Warning	USER
Configuration file import started by {username} at {user_ip}	ImportExport	Notice	USER
Configuration file import successful	ImportExport	Notice	USER
LDAP: An error occurred during Bind DN authentication on server {0}: {1}	LDAP	Error	SECURITY
LDAP: An error occurred when searching for the user's DN on the server {0}:{1}	LDAP	Error	SECURITY
LDAP: Group Filter syntax invalid for server {0}:{1}	LDAP	Error	SECURITY
LDAP: Group Filter search on server {0}:{1} returned no groups	LDAP	Warning	SECURITY
LDAP: One or more of the user-configured DN's for server {0}:{1} contains syntax errors	LDAP	Error	SECURITY
LDAP: No Group Mappings set for server {0}:{1}	LDAP	Warning	SECURITY
LDAP: Search base entry not found on server {0}:{1}	LDAP	Error	SECURITY
LDAP: {0}:{1} does not respond	LDAP	Error	SECURITY
LDAP: Unable to connect to server at {0}:{1}	LDAP	Error	SECURITY

Message	Tag Name	Severity	Facility
LDAP: LDAP version used by server {0}:{1} is not supported	LDAP	Error	SECURITY
LDAP: Bind DN authentication failed on server {0}:{1}	LDAP	Error	SECURITY
LDAP: The hostname of the certificate presented by {0}:{1} does not match	LDAP	Error	SECURITY
LDAP: The certificate presented by {0}:{1} is invalid	LDAP	Error	SECURITY
LDAP: The certificate presented by {0}:{1} is expired	LDAP	Error	SECURITY
LDAP: The issuing authority of the certificate presented by {0}:{1} is untrusted	LDAP	Error	SECURITY
LDAP: Unable to start TLS session with {0}:{1}	LDAP	Error	SECURITY
LDAP: Server {0}:{1} returned a DN that was longer than 4096 bytes. That DN was ignored.	LDAP	Error	SECURITY
LDAP: An error occurred when searching for a DN on the server {0}:{1}	LDAP	Error	SECURITY
LDAP: User ID Filter syntax invalid for server {0}:{1}	LDAP	Error	SECURITY
LDAP: An error occurred during authentication or authorization on server {0}:{1}	LDAP	Error	SECURITY
LDAP disabled by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP Bind DN changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP Bind DN Password changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP enabled by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP Group Filter changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP Group Membership Attribute changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP server {0}:{1} hostname changed to {2} by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP group mapping {0} changed to {1} by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP group mapping {0} mapping created by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP group mapping {0} mapping deleted by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP server {0}:{1} port changed to {2} by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP Search Base changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP server {0}:{1} created by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP server {0}:{1} deleted by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP settings changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP Synchronization Interval changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP TLS disabled by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP TLS enabled by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
LDAP User ID Filter changed by {username} at {user_ip}	LDAPConfig	Warning	SECURITY
Front Port changed link state to down	Link Up/Down	Notice	SYSTEM
Front Port changed link state to up	Link Up/Down	Notice	SYSTEM
Port {0} changed link state to down	Link Up/Down	Notice	SYSTEM

Message	Tag Name	Severity	Facility
Port {0} changed link state to up	Link Up/Down	Notice	SYSTEM
Login to {interface}: failed from {user_ip}	Login	Notice	SECURITY
SFP inserted into port {0}	SFPchange	Notice	SYSTEM
SFP removed from port {0}	SFPchange	Notice	SYSTEM
Invalid SFP inserted into port {0}	SFPchange	Notice	SYSTEM
Login to {interface}: successful by {username} at {user_ip}	Login	Notice	SECURITY
User account {0} locked out due to consecutive failed login attempts	Login	Warning	SECURITY
User account {0} timeout	Login	Warning	SECURITY
Logout {interface}: {username} at {user_ip}	Login	Notice	SECURITY
Network Settings: changed by {username} at {user_ip}	NetworkConfig	Notice	USER
Network Interface {0}: changed by {username} at {user_ip}	NetworkConfig	Notice	USER
Port Mirroring disabled on {0} by {username} at {user_ip}	PortMirroringConfig	Notice	USER
Port Mirroring enabled on {0} by {username} at {user_ip}	PortMirroringConfig	Notice	USER
Port Mirroring source ports changed by {username} at {user_ip}	PortMirroringConfig	Notice	USER
Port Mirroring target port changed from {0} to {1} by {username} at {user_ip}	PortMirroringConfig	Notice	USER
Port Monitor changed by {username} at {user_ip}	PortMonitor	Notice	USER
Port {0} exceeded link flap threshold	PortMonitor	Error	SYSTEM
Port {0} disabled: exceeded link flap threshold	PortMonitor	Error	SYSTEM
Port {0} disabled: exceeded Rx checksum error rate	PortMonitor	Error	SYSTEM
Port {0} detected {1} Rx checksum errors within the monitor window	PortMonitor	Error	SYSTEM
Port {0} restored by {username} at {user_ip}	PortMonitor	Notice	USER
Device initialization completed	Power	Notice	SYSTEM
Device rebooted by {username} at {user_ip}	Power	Error	USER
PTP Settings: changed by {username} at {user_ip}.	PTPConfig	Notice	USER
Device factory reset initiated through pinhole button	PushbuttonReset	Notice	USER
Front management port reset initiated through pinhole button	PushbuttonReset	Alert	USER
Active RADIUS server is now {0}	RADIUS	Notice	SECURITY
Rejected login attempt because no response from the RADIUS server received within the retransmission timeout	RADIUS	Warning	SECURITY
Rejected login attempt because response was invalid	RADIUS	Error	SECURITY
Rejected login attempt by user {0} because RADIUS server {1} replied with an SEL-USER-ROLE attribute containing an unrecognized user role	RADIUS	Error	SECURITY
Rejected login attempt by user {0} because RADIUS server {1} replied without an SEL-USER-ROLE attribute	RADIUS	Error	SECURITY
Rejected login attempt because RADIUS server {0} sent an X.509 certificate with an unknown or untrusted certificate authority	RADIUS	Error	SECURITY
Rejected login attempt because the common name in the X.509 certificate sent by the RADIUS server {0} did not match the hostname of the RADIUS server on the RADIUS page	RADIUS	Error	SECURITY

Message	Tag Name	Severity	Facility
Rejected login attempt because RADIUS server {0} sent an expired or not yet valid X.509 certificate	RADIUS	Error	SECURITY
{username} at {user_ip} disabled RADIUS	RADIUSConfig	Warning	SECURITY
{username} at {user_ip} enabled RADIUS	RADIUSConfig	Warning	SECURITY
{username} at {user_ip} modified RADIUS settings	RADIUSConfig	Notice	SECURITY
Rate Limiting Settings: changed on port {0} by {username} at {user_ip}	RateLimitingConfig	Notice	USER
SNMP Settings: changed by {username} at {user_ip}	SNMPConfig	Informational	USER
LLDP mode disabled by {username} at {user_ip}	SNMPConfig	Notice	USER
LLDP mode enabled by {username} at {user_ip}	SNMPConfig	Notice	USER
BPDU received, port {0} disabled.	SpanningTree	Error	SYSTEM
BPDU Guard timeout reached. Port {0} enabled.	SpanningTree	Notice	SYSTEM
BPDU Guard overridden by {username} at {user_ip}. Port {0} enabled.	SpanningTree	Notice	SYSTEM
Spanning Tree: Root switch changed from {0} to {1}	SpanningTree	Notice	SYSTEM
Spanning Tree: Port {0} transitioned from {1} to {2}	SpanningTree	Notice	SYSTEM
Spanning Tree: This switch has become the root bridge	SpanningTree	Notice	SYSTEM
Spanning Tree: Port {0} transitioned from {1} to {2}	SpanningTree	Notice	SYSTEM
The {0} event queue overflowed	Syslog	Critical	SYSTEM
The {0} event queue left the overflow condition. Approximately {1} events were lost.	Syslog	Notice	SYSTEM
Syslog events acknowledged by {username} at {user_ip}	Syslog	Notice	USER
Local Syslog Event Queue contains >= 75% unacknowledged events	Syslog	Warning	SYSTEM
Local Syslog Event Queue contains >= 90% unacknowledged events	Syslog	Critical	SYSTEM
Local Syslog Event Queue contains <= 65% unacknowledged events	Syslog	Notice	SYSTEM
Local Syslog Event Queue contains <= 80% unacknowledged events	Syslog	Notice	SYSTEM
Syslog Destination {0}: created by {username} at {user_ip}	SyslogConfig	Notice	USER
Syslog Destination {0}: deleted by {username} at {user_ip}	SyslogConfig	Warning	USER
Syslog Destination {0} Settings: modified by {username} at {user_ip}	SyslogConfig	Warning	USER
Syslog Settings: changed by {username} at {user_ip}	SyslogConfig	Notice	USER
System real-time clock has failed its self-diagnostic tests.	SystemIntegrity	Critical	SYSTEM
System clock battery has failed its self-diagnostic tests.	SystemIntegrity	Warning	SYSTEM
System FLASH has failed its self-diagnostic tests.	SystemIntegrity	Alert	SYSTEM
Power supply A has failed its self-diagnostic tests.	SystemIntegrity	Alert	SYSTEM
Power supply B has failed its self-diagnostic tests.	SystemIntegrity	Alert	SYSTEM
System RAM has failed its self-diagnostic tests.	SystemIntegrity	Alert	SYSTEM
Device reset because of hardware watchdog	SystemIntegrity	Critical	SYSTEM
User {0}: attributes changed by {username} at {user_ip}	UserConfig	Notice	SECURITY
User {0}: created by {username} at {user_ip}	UserConfig	Warning	SECURITY
User {0}: deleted by {username} at {user_ip}	UserConfig	Warning	SECURITY

Message	Tag Name	Severity	Facility
User {0}: disabled by {username} at {user_ip}	UserConfig	Notice	SECURITY
User {0}: enabled by {username} at {user_ip}	UserConfig	Notice	SECURITY
User {0}: password set by {username} at {user_ip}	UserConfig	Warning	SECURITY
VLAN {0}: created by {username} at {user_ip}	VLANConfig	Notice	USER
VLAN-aware mode disabled by {username} at {user_ip}	VLANConfig	Notice	USER
VLAN-aware mode enabled by {username} at {user_ip}	VLANConfig	Notice	USER
VLAN {0}: deleted by {username} at {user_ip}	VLANConfig	Notice	USER
Port {0} VLAN membership changed from {1} to {2} by {username} at {user_ip}	VLANConfig	Notice	USER
VLAN {0}: updated by {username} at {user_ip}	VLANConfig	Notice	USER
X.509 certificate {0} set as default web certificate by {username} at {user_ip}	X509Config	Notice	SECURITY
X.509 certificate {0} Alias: certificate changed to {1} by {username} at {user_ip}	X509Config	Notice	USER
X.509 certificate {0} deleted by {username} at {user_ip}	X509Config	Notice	SECURITY
X.509 certificate {0} has expired; communications requiring X.509 based authentication may have stopped	X509Config	Error	SYSTEM
X.509 certificate import started by {username} at {user_ip}	X509Config	Notice	SECURITY
X.509 certificate import failed	X509Config	Warning	SECURITY
X.509 certificate {0}: certificate import completed successfully	X509Config	Notice	SECURITY
X.509 certificate {0} will expire in {1} days; communications requiring X.509 based authentication may be affected when it expires	X509Config	Warning	SYSTEM
X.509 certificate {0} will expire in {1} days; communications requiring X.509 based authentication may be affected when it expires	X509Config	Informational	SYSTEM
X.509 certificate {0} will expire in {1} days; communications requiring X.509 based authentication may be affected when it expires	X509Config	Notice	SYSTEM

Cybersecurity Features

Introduction and Security Environment

Product Function

This firmware is an Ethernet-managed switch. The security features of the firmware provide secure communications between the user interface and the computer used to interact with the device for configuration and monitoring and are focused on maintaining the availability and integrity of the LAN operations.

Security Requirements

The RSTP-based firmware was designed for a security model that includes hardware, firmware, user interface, data plane, and control plane. The SEL switch options have controls at each of these layers to protect the integrity of the device operations. This security model relies on other devices to monitor the logs, alarms, and health of the product. The data plane and control plane prioritize interoperability for Ethernet and Rapid Spanning Tree protocols.

Version Information

Obtaining Version Information

The device firmware identification (FID) number can be obtained through the web user interface and the SNMP Entity MIB. The firmware is provided in a single digitally signed file. The switch will validate the digital signature of the firmware before upgrading.

Integrity Indicators

The firmware protects the integrity of the operating firmware through validation of digital signatures.

Commissioning and Decommissioning

Commissioning

No service accounts are used, and on the first startup, the landing page of the user interface requires the input of the first administrator username and password.

Secure Operation Recommendations

SEL recommends enabling only the user access on the interface of the product you intend to use. By default, only the front port is enabled. SEL also recommends collecting the logs from the switch centrally on a server that can collect the Syslogs and monitor the alarm contact.

Decommissioning

To remove all settings and return the device to its factory-default state, please use the Factory Reset feature.

External Interfaces

Ports and Services

All management of the switch is done through the web management interface. By default, only the web-based engineering access is enabled on the front port and SNMP is disabled on both.

Logical Ports

IP Port Default	Network Protocol	Default Port State	Port Configurable	Purpose
80	HTTP	Enabled on ETH F	No	Redirect to HTTPS port for web user interface
443	HTTPS	Enabled on ETH F	No	Web user interface
161	SNMP	Disabled	No	SNMP read-only

File System Interfaces

The firmware is an embedded device operating on a single image and does not support any external file systems. You can export and import device settings by using an active and authorized user through the user interface.

Access Controls

Privilege Levels

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

- Users with the Administrator role have full access to the device.
- Users with the Engineer role have access to most settings and information on the device. The main exception to this is user account management.

- Users with the User Manager role have access to manage users on the device. Access to other settings is restricted.
- Users with the Monitor role have read-only access to most of the device settings.

Centrally Managed Accounts

LDAP and RADIUS with multifactor authentication are supported.

Local Accounts

The firmware supports as many as 256 local user accounts.

Passwords

The firmware requires complex passwords of eight characters in length that contain at least one upper case letter, one lower case letter, one number, and one special character.

Digital Trust

The firmware uses X.509 certificates for digital trust in the web server, LDAP, and RADIUS.

Logging Features

Security Events

The firmware supports SNMP and Syslog for remote event monitoring. The firmware also supports management of the local alarm contact of the switch for out-of-band event notifications.

Internal Log Storage

The firmware supports storage for as many as 60,000 local logs. The firmware does not allow logs to be deleted without a full device factory reset. Logs are overwritten in a first-in, first-out method, so the newest logs overwrite the oldest.

Backup and Restore

The firmware includes the ability to create backup files of the device and a restore feature to import a backup and apply the configuration.

Malware Protection Features

The firmware is designed to operate on an embedded device that does not allow the installation of additional software and which only accepts digitally signed firmware upgrades. The firmware includes a self-test that continually checks running code against the known good baseline version of code in nonvolatile memory. See "The SEL Process for Mitigating Malware Risk to Embedded Devices" at selinc.com/malware_protection for more details.

Product Updates

Table A.1 and *Table A.2* contain descriptions of each firmware update. The product page at selinc.com shows the latest available firmware version. To obtain product updates, contact any sales or technical support contact. For the SEL disclosure process and details on vulnerability disclosures, see "The SEL Process for Disclosing Security Vulnerabilities" at selinc.com/security_vulnerabilities.

Update Verification

The firmware automatically checks firmware authenticity and integrity and only loads firmware files that have been signed by SEL. The authenticity and integrity of firmware updates can be verified by checking the firmware hash. For instructions and firmware hash values, see selinc.com/products/firmware.

Contact SEL

For further questions or concerns about product security, contact SEL at security@selinc.com or +1.509.332.1890.



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