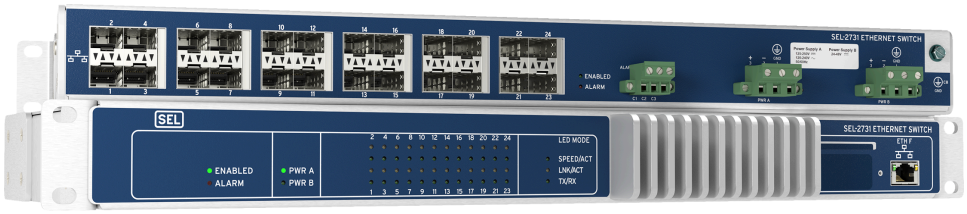
# Software-Defined Networking

## for the SEL Managed Ethernet Switch

## User's Guide




20241205

SEL SCHWEITZER ENGINEERING LABORATORIES

# Table of Contents

This page intentionally left blank

# List of Tables

This page intentionally left blank

# Preface

## User's Guide Overview

This user's guide describes the functionality and use of the operational technology (OT) software-defined networking (SDN) 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: Product Overview*. Provides the product overview.

*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: Events*. Provides information about the Syslog event logs.

*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**<br>Use of this equipment in a manner other than specified in this manual can impair operator safety safeguards provided by this equipment. | **⚠WARNING**<br>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**<br>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**<br>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**<br>Do not perform any procedures or adjustments that this instruction manual does not describe. | **⚠WARNING**<br>Ne pas appliquer une procédure ou un ajustement qui n'est pas décrit explicitement dans ce manuel d'instruction. |
| **⚠CAUTION**<br>In order to avoid losing system logs on a factory-default reset, configure the SEL-2731 to forward Syslog messages. | **⚠CAUTION**<br>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

SECTION 1

# Introduction and Specifications

## Introduction

This section includes the following information about the SEL's operational technology (OT) software-defined networking (SDN) for SEL Ethernet managed switch firmware:



OT SDN provides the reliability, performance, and security demanded by critical infrastructure networks. With deny-by-default, zero-trust, packet inspection from Layer 1 through 4 at each switch port and a secure control plane, OT SDN provides industry leading cybersecurity. OT SDN is not an IT technology applied to OT, it is an OT technology specifically designed to operate in critical control systems with sub-millisecond network healing and proactive traffic engineering control over every conversation. This results in every host on the network only getting the traffic the system owner wants each host to receive. OT SDN provides protection class Ethernet networking designed to perform reliably even in the harsh environmental conditions commonly found in electric and industrial applications. OT SDN is ideal for IEC 61850 base digital substations supporting even the most demanding Ethernet communications, such as IEC 61850-9-2 sampled values or Ethernet communications found in process control systems (PCS), distributed control systems (DCS), and supervisory control and data acquisition (SCADA).

OT SDN improves situational awareness allowing you to know exactly what devices and conversations are on your network at all times. Your network only forwards the conversations you have engineered, reduces your engineering time, and improves your accuracy with end-to-end circuit provisioning, transactional change management, automated topology management, commissioning, and simplified troubleshooting. Centrally manage your switches with the SEL-5056 Software-Defined Network (SDN) Flow Controller. OT SDN provides the confidence of knowing exactly what is on your networks, that they are protected, and that they will not change without your explicit request.

## Product Features

- **OT SDN.** Use interoperable industry standard OpenFlow with large flow, group, and meter tables with detailed counter support for a robust programmable switch fabric.
- **High Performance.** Designed to meet the strict requirements for real time protection signals by healing network faults in less than a millisecond.
- **Cybersecure.** Designed with a secure control plane to meet FIP 140-3 cryptographic standards .

- **Automated Commissioning.** Integrated with the SEL-5056 Flow Controller, the OT SDN switch can be commissioned before or after deployment and is autocommissioned when adopted into the network.
- **Simplified Troubleshooting.** Displays the port status and activity LEDs and the device status for simple onsite and remote troubleshooting.
- **Situational Awareness.** Integrates with the SEL-5056 Flow Controller for central configuration, change management, operational diagnostics, and telemetry statistics.
- **Ease-of-Use.** Supports orchestration interfaces for end-to-end circuit provisioning, automated commissioning, and change management.
- **Reliable Operations.** Retains flow configuration through power cycles even when the flow controller is offline.
- **Flexible Traffic Monitoring.** Provides traffic taps, diagnostic counters, and detailed device logs.
- **Zero-Trust Cybersecurity.** Supports deny-by-default network access control and secure communications management.
- **Configurable Alarm Contact.** Supports programmable options to drive the out-of-band alarm contact.
- **Network Access Control.** Provides multilayer packet inspection on all network forwarding for each flow on Layers 1, 2, 3, and 4.
- **Quality of Service (QoS).** Provides traffic priority management through four 8:4:2:1 weighted round-robin (WRR) priority queues.
- **Time Synchronization.** Precision Time Protocol (PTP) transparent clocks provide support for the IEEE C37.238 2017 profile and switch synchronization through Network Time Protocol (NTP) or Authenticated Controller Time Synchronization (ACTS).
- **Improves PRP.** Supports traffic management protecting against single attached node flooding.
- **Logging and Diagnostics.** Generates and sends log events directly to a central server through UDP or protected packets with TLS, and supports SNMPv3 for switch diagnostics.

# Software System Requirements

The SEL-5056 Flow Controller is required for engineering access to the OT SDN switches.

# Specifications

| Compliance | |
|---|---|
| Designed and manufactured under an ISO 9001 certified quality management system | |
| **General** | |
| Priority Queues: | 4 |
| Priority Queue Method: | 8:4:2:1 weighted round-robin (WRR) |

## Network Management

| | |
|---|---|
| Syslog UDP and TCP/TLS | |
| SNMPv2c/v3 | |
| Switch Control Plane: | OpenFlow 1.3 |
| Flow Tables: | 4 (2 for the SEL-2731) |
| Table Size: | 8,192 flows |
| Group Entries: | 256 |
| Action Buckets per Group: | 30 |
| Meters: | 64 |
| Meter Limit: | Rate and Burst |
| Group Types: | All, Select, Indirect, Fast Failover |
| Instructions: | Write-Actions, Apply-Actions, Meter, Clear-Actions, Goto Table |
| Actions: | Output, Group, PushVlan, PopVlan, SetQueue, SetVlanVid, SetVlanPcp |

## Precision Time Protocol

| | |
|---|---|
| Profile: | IEEE C37.238 2017 (Power Profile) Transparent Clock |

This page intentionally left blank

SECTION 2

# Product Overview

## Introduction

The OT SDN technology is designed to provide the highest level of reliability and security to protect critical infrastructure networks. The OT SDN underlay control plane replaces the legacy RSTP managed switch control plane. Achieve microsecond network healing, deny-by-default network access control, multi-layer packet inspection and filtering for the highest level of cybersecurity, as well as centralized situational awareness, with an easy-to-use and flexible SDN switch built for OT.

The SEL-5056 Flow Controller and a wide variety of switches enable you to design the perfect network for your project. The SEL-5056 Flow Controller is the central software that commissions and configures OT SDN switches.

OT SDN switches do not have a user interface, which reduces the administrative burden and makes them more secure. All OT SDN switches are configured by the SEL-5056 Flow Controller. This central configuration software provisions all the switches through automated tools, allowing you to provision end-to-end circuits rather than logging into every switch and entering individual settings.

## Centrally Manage and Monitor With the SEL-5056 Flow Controller

All configuration and monitoring of the OT SDN switches happens through the SEL-5056 Flow Controller. Refer to the *SEL-5056 Software-Defined Network (SDN) Flow Controller Instruction Manual* for all switch configuration and monitoring options.

## Commissioning and Adoption

By default, OT SDN switches publish an OpenFlow discovery packet every few seconds. OpenFlow discovery packets are structured by Link Layer Discovery Protocol (LLDP), so they are Layer 2 packets that stay within the subnet. This packet announces the presence of a new SDN switch and provides the default IP address to communicate with the switch. The out-of-band port, **ETH F**, has a default IP address in the 169.254.*x.x/16* subnet. The in-band management ports, all the data plane ports, have a default IP address in the 192.168.*x.x/16* subnet. The last two octets are random and change during a factory-default reset action. The SEL-5056 Flow Controller commissions the OT SDN switch by setting the IP address, subnet, time, certificates, and the flow controller IP address of the switch by using the representational state transfer (REST) interface. The computer the SEL-5056 is operating on does not have to be in the same subnet as the default addresses. The OT SDN switch listens for incoming connections to the REST interface on Port 443. Once commissioned, the

OT SDN switch attempts to communicate with the configured flow controller by using OpenFlow with a destination TCP port of 6653. When you use the SEL-5056 Flow Controller, the adoption process is automated for simple one-touch commissioning. The term "adoption" refers to the switch and the flow controller being successfully connected and communicating on the OpenFlow and REST interfaces.

OT SDN switches support out-of-band or in-band adoption, and there is no connection between the out-of-band ports and the in-band ports. The SEL-5056 Flow Controller manages all the flows in the switches automatically, allowing them to communicate with the SEL-5056. The OT SDN switches communicate with one flow controller and, once commissioned, stops publishing the OpenFlow discovery packet. To adopt the OT SDN switch to a different flow controller, the switch must be factory-default reset either through the current flow controller settings or through the pinhole reset button on the front of the switch.

Configuration details for the commissioning settings of the OT SDN switch can be found in the *Configuration Objects* section in the *SEL-5056 Software-Defined Network (SDN) Flow Controller Instruction Manual*.

# Time Synchronization

OT SDN switches support synchronizing the local time with Network Time Protocol (NTP) or Authenticated Controller Time Synchronization (ACTS). The switch time is set at adoption to synchronize with the SEL-5056 Flow Controller time. When ACTS or NTP are enabled, those services maintain time synchronization with their respective time sources. The method used for time synchronization is configured in the switch configuration node of the SEL-5056. NTP can be configured with as many as three time servers.

# Managing Precision Time Protocol

The OT SDN switches are IEC 61850-9-3:2016 or IEEE C37.238-2017 or -2011 Power Profile peer-to-peer (P2P) transparent clock (TC) with syntonization support. PTP is disabled by default and can be enabled through the configuration node of the switch in the SEL-5056 Flow Controller. Fixed PTP settings for the OT SDN switches are shown in *Table 2.1*.

**Table 2.1 Fixed PTP Settings**

| Setting | Value |
|---|---|
| P2P Delay Request Interval | 1 (in seconds) |
| Domain | Configurable between 0 and 255[a] |
| VID | None (all PTP messages sourced from the SEL-2741 are untagged) |

[a] Configurable between 0 and 255 on the SEL-2731; 0 on all other switches.

To meet the performance requirements of IEEE C37.238 Power Profile, the user must configure the network and end devices correctly, ensuring the following:

- The PTP domain of the clock must match the configuration of the switch for the switch to syntonize.
- All equipment between the PTP clock and the switch must meet the Power Profile requirements.
- The following flows must be present on each switch between the PTP master and clients:
  - Send P2P messages to the local port to enable the P2P delay mechanism
  - Forward synchronization and announce messages between PTP masters and between each PTP master and client

PTP flows can automatically be provisioned using Circuit Provisioning in the SEL-5056 Flow Controller. Use multicast Circuit Provisioning and make sure all the devices that you want to receive the PTP synchronization message subscribe to the multicast circuit, including every switch. Interruptions to the PTP flow interrupt synchronization. The OT SDN switch continuously sends untagged P2P delay requests outside of the OpenFlow pipeline at the P2P delay request interval. The local port on the switch accepts both single-tagged and untagged packets.

# Logging

The OT SDN switch logs events through Syslog and can store 4,096 local events. The SEL-5056 Flow Controller also collects the logs from each switch and, if configured as such, sends Syslog log messages to any configured log server and records them to the Windows event log files.

Syslog is configured for the OT SDN switch through the logging settings in the SEL-5056 Flow Controller. The OT SDN switch supports UDP (RFC 3164 and RFC 5424) and TLS Syslog (RFC 5424 over RFC 5425) protocols.

The Syslog delivery failure message "Log delivery was not confirmed to behavior {behavior type} for event with id {Id}" appears once for each message if that message cannot be sent to at least one Syslog server with the TLS transport method type when the acknowledgment of the TCP delivery is not received. OpenFlow changes can happen rapidly and the logs from the OT SDN switch will combine many of the OpenFlow actions into a single log. The Syslog message "OpenFlow changes ({numberOfChanges}): {Change Description}" reports the number of changes and a list of as many as 50 of the changes in 10-second intervals. The list is comma-separated and includes an abbreviation and number. All numbers are in hexadecimal format.

# SNMP

The OT SDN switch supports SNMP for read-only status monitoring. SNMPv2c and SNMPv3 are supported. SNMP is disabled by default and either or both can be enabled. When you use SNMPv2c, you can set the community string. If no string is supplied, the string defaults to "public". When you use SNMPv3, refer to SNMP Configuration in the *SEL-5056 Software-Defined Network (SDN) Flow Controller Instruction Manual* for details.

The following MIBs are supported:

- If-MIB
- Entity-MIB for the entPhysicalTable
- System-MIB for Description, Name, Location, Object Identifier, and System Up Time
- SEL-274XS-Alarm-Contact-MIB
- SEL-274XS-Digital-Input-MIB
- SEL-274XS-Module-MIB
- SEL-274X-PoE-MIB
- SEL-274XS-Power-Supply-MIB
- SEL-274XS-Switch-Configuration-MIB
- SEL-Definitions-MIB
- SEL-Products-MIB

You can download the MIBs and read their details at each switch's product page at https://selinc.com.

Configuration details for SNMP on the OT SDN switch can be found in the *Configuration Objects* section in the *SEL-5056 Software-Defined Network (SDN) Flow Controller Instruction Manual*.

# OpenFlow

The OT SDN switch uses OpenFlow version 1.3 as the underlay control plane. All other control plane technology is removed, simplifying the design of the switch, and improving performance, situational awareness, and cybersecurity. For detailed information on OpenFlow version 1.3, refer to opennetworking.org.

The OT SDN switch supports out-of-band and in-band management. When using out-of-band management, the SEL-5056 Flow Controller communicates with the switch through the **ETH F** port. When using in-band management, the SEL-5056 communicates with the switch through any port except **ETH F**.

The OT SDN switch supports the full range of port settings defined in the OpenFlow standard allowing each port on the switch to be autonegotiated or specified to operate in the desired mode.

*Table 2.2* shows the OpenFlow resources available in the OT SDN switch.

**Table 2.2 Complete List of Supported OpenFlow Parameters**

| Parameter | Supported |
|---|---|
| Priority Queues Per Port | 4 |
| Flow Tables | 4 (2 in SEL-2731) |
| Flow Entries Per Table | 2048 (4096 in SEL-2731) |
| Group Entries | 256 |
| Action Buckets Per Group | 30 |
| Unique Action Buckets | 128 |
| Meter Entries | 64 |
| Meter Bands Per Meter Entry | 1 |

Configuration details on the supported OpenFlow capabilities and port settings of the OT SDN switch from SEL can be found in the *OpenFlow* section in the *SEL-5056 Software-Defined Network (SDN) Flow Controller Instruction Manual*.

# Device View

Each OT SDN switch has a device view which can be opened through the SEL-5056 Flow Controller when the switch of interest is selected in the network topology space. The device view provides diagnostic, status, logs, and alarm details for that device.

Each switch has a slightly different device view. The device view contains insight text to help you understand what each value represents and how to navigate within the device view. The device view dashboard is interactive. To get diagnostic details on a port, select the desired port from the switch image.

# Digital Inputs

Some OT SDN switches have digital inputs that can be used for logically controlling a reset functionality or to provide a settings lock-in.

At least one input (a digital input or the front pinhole reset button) must be enabled for factory reset functionality. When using a digital input, the input must be asserted for five seconds to initiate a factory reset. If a digital input is configured for factory reset functionality, the front pinhole reset button can be disabled if desired.

When a digital input is set to settings lock, the input controls when the switch will accept settings changes from the authorized flow controller. When a digital input is set to settings lock and that input is asserted, the switch does not accept any settings changes even from the authorized flow controller, including settings changes to the digital inputs themselves.

# Gigabit Copper Fast Failover

The IEEE standard requires 1 Gbps copper Ethernet ports to wait 720 ms before declaring a link down. Since the OT SDN switch heals networks in less than a millisecond, waiting this extra time is extensive. The OT SDN switch allows the disabling of the standards-based wait time, which accelerates the heal times of 1 Gbps copper link failures.

# Link State Change Management

The OT SDN switch allows you to manage how link state changes are handled by the alarm contact. The OT SDN switch allows full flexibility to set, link-up, and link-down state changes to either pulse or latch the alarm contact or to not operate on link state changes. When a latch is selected, you can set the latch system to either self-clear the alarm, if the alarm state returns to normal, or require the latch alarm to be manually cleared.

This provides you flexibility to set the behavior of the alarm contact for each link state change. For example, you can set the alarm contact to latch when a link goes down, then self-clear and deassert the alarm when the link comes back up. You can also set an unused port to latch the alarm if that port gets added to a link that goes up to provide an alert if a port gets used unexpectedly.

APPENDIX A

# Firmware and User's Guide Versions

## Firmware

### Determining the Firmware Version

To determine the firmware version, navigate to the device view dashboard of the OT SDN switch in the SEL-5056 Flow Controller.

The OT SDN switch comes with firmware preinstalled, and the firmware can be updated through use of the SEL-5056 Flow Controller. If a switch must be replaced, you can use the SEL-5056 to apply the configuration of a switch to the replacement switch through the adoption process or the replace action. When a switch must be removed from service, you can decommission it, which removes all device configuration and restores factory-default settings.

Note that these instructions are only intended for upgrading firmware from an older revision to a newer revision. Downgrading firmware—going from a newer to an older revision—should not be attempted. It may result in the loss of MAC addresses and other device configuration information. Contact SEL if you need to downgrade the firmware.

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 firmware identification (FID) number. The SDN managed switch technology is designed to operate in many products. The switch product numbers are indicated by the indicated by the SEL-27xx (either SEL-2731 or SEL-2741). The "S" is the indication that this firmware is an SDN-based managed switch.

Existing firmware:

FID = SEL-27xxS-**R100**-V0-Z001001-Dxxxxxxxx

Standard release firmware:

FID = SEL-27xxS-**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-27xxS-R100-**V0**-Z001001-Dxxxxxxxx

Point release firmware:

FID = SEL-27xxS-R100-**V1**-Z001001-Dxxxxxxxx

The date code is after the D. For example, the following is firmware version number R100, date code February 09, 2024.

FID = SEL-27xxS-R100-V0-Z001001-**D20240209**

## Firmware Files

Switch firmware upgrade files have a tar.gz file name extension. The following is an example firmware file name:

**27xxS.R100.V0.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.

# Revision History

*Table A.1* and *Table A.2* list the different switch's firmware versions, revision descriptions, and corresponding instruction manual date codes. The most recent firmware version is listed first.

Starting with revisions published after March 1, 2022, changes that address security vulnerabilities are marked with "[Cybersecurity]". Other improvements to cybersecurity functionality that should be evaluated for potential cybersecurity importance are marked with "[Cybersecurity Enhancement]".

**Table A.1 SEL-2731 Firmware Revision History**

| Firmware Identification (FID) Number | Summary of Revisions | User's Guide Date Code |
|---|---|---|
| SEL-2731S-R100-V4-Z001001-D20241205 | Includes all the functions of SEL-2731S-R100-V3-Z001001-D20240523 with the following additions:<br>➤ Resolved an issue that reduced the flow table size.<br>➤ Resolved an issue that could cause the OpenFlow session to stop responding for a brief period of time when using TLS 1.3.<br>➤ Resolved an SFP compatibility issue. | 20241205 |
| SEL-2731S-R100-V3-Z001001-D20240523 | Includes all the functions of SEL-2731S-R100-V2-Z001001-D20240501 with the following addition:<br>➤ Improved flash memory reliability. | 20240523 |
| SEL-2731S-R100-V2-Z001001-D20240501 | Includes all the functions of SEL-2731S-R100-V1-Z001001-D20240301 with the following additions:<br>➤ [Cybersecurity] Addressed a denial-of-service vulnerability in a third-party software component that could allow a malicious client to temporarily affect the availability of the web server.<br>➤ Resolved an issue where logs were not being stored locally for NTP Sync events. | 20240501 |
| SEL-2731S-R100-V1-Z001001-D20240301 | Includes all the functions of SEL-2731S-R100-V0-Z001001-D20240209 with the following addition:<br>➤ Resolved an adoption compatibility issue with the Windows operating system version of the SEL-5056. | 20240301 |
| SEL-2731S-R100-V0-Z001001-D20240209 | ➤ Initial version. | 20240209 |

**Table A.2 SEL-2741 Firmware Revision History**

| Firmware Identification (FID) Number | Summary of Revisions | User's Guide Date Code |
|---|---|---|
| SEL-2741S-R100-V8-Z001001-D20240523 | Includes all the functions of SEL-2741S-R100-V7-Z001001-D20240501 with the following addition:<br>➤ Improved flash memory reliability. | 20240523 |
| SEL-2741S-R100-V7-Z001001-D20240501 | Includes all the functions of SEL-2741S-R100-V6-Z001001-D20230919 with the following additions:<br>➤ [Cybersecurity] Addressed a denial-of-service vulnerability in a third-party software component that could allow a malicious client to temporarily affect the availability of the web server.<br>➤ Resolved an issue where the front port could stop operating properly under heavy network loads.<br>➤ Resolved an issue where logs were not being stored locally for NTP Sync events. | 20240501 |
| SEL-2741S-R100-V6-Z001001-D20230919 | Includes all the functions of SEL-2741S-R100-V4-Z001001-D20230508 with the following additions:<br>➤ [Cybersecurity] Addressed an issue in previous releases where tampering with TLS negotiation could result in weakening the key strength for OpenFlow and Syslog/TLS.<br>➤ Resolved an issue in previous releases where flow loss will occur approximately 40 days after adoption if the device remains continuously powered.<br>➤ Resolved an issue in previous releases where packet-out requests from the controller directed to the flow tables would not be forwarded.<br>➤ Resolved an issue in previous releases where the device could erroneously log a Device Initialization Complete event.<br>➤ Enhanced PTP handling to drop end-to-end delay requests and delay responses. | 20230919 |
| **Note:** Firmware version R100–V5 did not release. | | |
| SEL-2741S-R100-V4-Z001001-D20230508 | Includes all the functions of SEL-2741S-R100-V3-Z001001-D20230418 with the following additions:<br>➤ [Cybersecurity Enhancement] Addressed an issue in previous releases where syslog messages were not sent to the configured destination.<br>➤ Reduced the time it takes for the switch to syntonize to the PTP clock.<br>➤ Resolved an issue in previous releases where the firmware upgrade log did not include the firmware versions from which and to which the switch was upgraded.<br>➤ Resolved an issue in previous releases that did not allow ports to be administratively disabled when PTP was enabled.<br>➤ Enhanced the front-panel Ethernet port (ETH F) indication LEDs to operate the same as those on the back panel.<br>➤ Resolved an issue in previous releases where disabled ports would enable after a restart.<br>➤ Resolved an issue in previous releases that required a restart when changing from a 100BASE FX SFP to a copper SFP.<br>➤ Resolved an issue in previous releases where copper SFP auto-negotiation settings were not being retained through a power cycle.<br>➤ Resolved an issue in previous releases that caused an extra synchronization after adoption if the port event settings were non-default. | 20230508 |

| Firmware Identification (FID) Number | Summary of Revisions | User's Guide Date Code |
|---|---|---|
| SEL-2741S-R100-V3-Z001001-D20230418 | Includes all the functions of SEL-2741S-R100-V2-Z001001-D20230313 with the following additions:<br>➤ Enhanced the PTP performance of the SEL qualified copper SFP, 8115-01, to meet PTP Power Profile at 1 Gbps.<br>➤ Changed device functionality to not modify correctionField or networkTimeInaccuracy field when PTP transparent clock is disabled.<br>➤ Addressed an issue present in previous releases where the device's peer delay response was incorrect for two-step operations. | 20230418 |
| SEL-2741S-R100-V2-Z001001-D20230313 | Includes all the functions of SEL-2741S-R100-V1-Z001001-D20230208 with the following additions:<br>➤ Addressed an issue present in previous releases where the PTP network time inaccuracy correction field could incorrectly report a larger than expected value.<br>➤ Added support for copper 100/1000BASE-T SFPs | 20230313 |
| SEL-2741S-R100-V1-Z001001-D20230208 | Includes all the functions of SEL-2741S-R100-V0-Z001001-D20230131 with the following additions:<br>➤ Addressed an issue in R100-V0 in which some port setting modifications were not retained through a power cycle.<br>➤ Enhanced the PTP transparent clock synchronization performance on link state changes. | 20230208 |
| SEL-2741S-R100-V0-Z001001-D20230131 | ➤ Initial version. | 20230131 |

# 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 |
|---|---|
| 20241205 | Appendix A<br>➤ Updated for SEL-2731S firmware version R100-V4.<br>➤ Updated 20240301 User's Guide Revision History summary to specify SEL-2731S R100-V1. |
| 20240523 | Section 2<br>➤ Updated *Managing Precision Time Protocol*, *Logging*, *Device View*, *Digital Inputs*, and *Link State Change Management*.<br><br>Appendix A<br>➤ Updated for SEL-2731S firmware version R100-V3.<br>➤ Updated for SEL-2741S firmware version R100-V8.<br><br>Appendix B<br>➤ Updated *Firmware Upgrade Procedure*. |
| 20240501 | Appendix A<br>➤ [Cybersecurity] Updated the SEL-2731S for firmware version R100-V2.<br>➤ [Cybersecurity] Updated the SEL-2741S for firmware version R100-V7. |
| 20240301 | Appendix A<br>➤ Updated for SEL-2731S firmware version R100-V1. |
| 20240209 | ➤ Initial version. |

APPENDIX B

# Firmware Upgrade Instructions

## Firmware Upgrade Procedure

To upgrade the OT SDN switch, you need the appropriate firmware upgrade file and access to the device through the SEL-5056 Flow Controller with Permission Level 3 privileges. Upgrade the device firmware by uploading a file from a personal computer to the device via the SEL-5056 web interface. All firmware updates are logged. Follow these steps to upgrade the switch firmware:

Step 1. Log in to the SEL-5056 as an authorized user with the role of Permission Level 3.

Step 2. Navigate to the Topology page under the Configuration menu.

Step 3. Select the OT SDN switch that you want to upgrade.

Step 4. In the primary panel, navigate to the configuration pane. Select **Firmware Upload** and choose the desired firmware file. Once the file is uploaded, press **Select** to start the firmware upgrade process. The SEL-5056 will display status messages throughout the process. The switch will reboot to complete the firmware upgrade process. (Upgrading firmware does not change any device configuration.)

### Status Messages

Firmware upgrades may take as long as ten minutes. The current status of the upload and upgrade appears above the Firmware Upload.

### Completion

Once the upgrade process is complete and the switch has restarted, log in and navigate to the **Device View** option in the Configuration pane. You will see the new FID.

This page intentionally left blank

APPENDIX C

# Events

## Introduction

The Syslog Protocol is used to convey event notification messages. The OT SDN switch creates Syslog messages as defined in RFC 3164 and RFC 5424 through use of either UDP or TLS. This section also lists the category for each event on the switch.

The Syslog message is divided into five parts: priority, time stamp, source, tag, and message. The Syslog messages forwarded by switches are formatted as follows:

<priority><time stamp><hostname><tag><message>

The priority is calculated from the severity and facility of the message by the following equation:

Priority = Facility • 8 + Severity

*Table C.1* and *Table C.2* list the possible values for severity and facility, respectively, used by the switch.

**Table C.1 Syslog Severity Levels**

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

**Table C.2 Syslog Facility Levels**

| Numerical Code | Severity |
|---|---|
| 1 | User |
| 3 | System |
| 4 | Security/Authorization |

The switch sends out Syslog messages for the given Syslog severity in the Syslog Server settings, as well as any Syslog messages with a higher severity level code (which corresponds to a lower severity code). For example, if the user configures a Syslog server with a severity level of Warning (code 4), the switch sends out Syslog messages with that severity, as well as those with severity levels of Error, Critical, Alert, and Emergency (codes 3, 2, 1, and 0, respectively).

**Table C.3 Event Logs**

| Message | Tag Name | Severity | Facility | Category |
|---|---|---|---|---|
| Device initialization completed. | System | Notice | System | Chassis and Module |
| Device reset because of hardware watchdog. | System | Critical | System | Chassis and Module |
| Failure: Power Supply A expected to be installed but absent. | System | Alert | System | Chassis and Module |
| Failure: Power Supply A. | System | Alert | System | Chassis and Module |
| Failure: Power Supply B expected to be installed but absent. | System | Alert | System | Chassis and Module |
| Failure: Power Supply B. | System | Alert | System | Chassis and Module |
| OK: Power Supply A. | System | Notice | System | Chassis and Module |
| OK: Power Supply B. | System | Notice | System | Chassis and Module |
| Certificate with common name {commonName} and thumbprint {thumbprint} internally {revokeState} | TrustAuthority | Informational | User | Configuration |
| Commissioning failed | CommissioningManager | Warning | User | Configuration |
| Commissioning succeeded | CommissioningManager | Informational | User | Configuration |
| Device factory reset initiated by user {userName} with role {roleName} from IP Address {ipAddress} | DeviceReset | Notice | Security/ Authorization | Configuration |
| Device reboot initiated by user {userName} with role {roleName} from IP Address {ipAddress} | DeviceReset | Error | User | Configuration |
| LED Mode: Changed by user at Front Panel. | System | Notice | User | Configuration |
| System Time: lost synchronization to external source. | System | Warning | System | Configuration |
| System Time: synchronized via NTP. | System | Notice | System | Configuration |
| User {userName} with role {roleName} from {ipAddress} acknowledged all local events. | LocalEventStore | Notice | User | Configuration |
| Port {port_num} changed link state to down. | System | Notice | System | Link |
| Port {port_num} changed link state to up. | System | Notice | System | Link |
| Device connected to OpenFlow controller at {ip} on port {port} | Openflow | Notice | System | Openflow |
| Device lost connection to OpenFlow controller at {ip} on port {port} | Openflow | Notice | System | Openflow |
| OpenFlow changes ({numberOfChanges}): {stringOfChanges} | Openflow | Informational | System | Openflow |
| A firmware version downgrade is not compatible with the current firmware. | FirmwareUpgrade | Error | System | System Integrity |
| Device factory reset initiated through digital input | System | Notice | User | System Integrity |
| Device factory reset initiated through pinhole button. | System | Notice | User | System Integrity |

| Message | Tag Name | Severity | Facility | Category |
|---|---|---|---|---|
| Device reset because of {reason} | DeviceReset | Warning | System | System Integrity |
| Event storage capacity ({storageCapacity}) exceeded. Oldest {numberRemoved} events removed. | LocalEventStore | Warning | User | System Integrity |
| Firmware upgrade from {oldVersion} to {newVersion} failed at step {failedStep} of {failedStepCount}. | FirmwareUpgrade | Critical | System | System Integrity |
| Firmware upgrade from {oldVersion} to {newVersion} succeeded. | FirmwareUpgrade | Warning | System | System Integrity |
| Firmware upgrade was initiated by user {username} with role {role} from IP address {ipaddress}. | FirmwareUpgrade | Notice | User | System Integrity |
| Local event storage contains <= 65% unacknowledged events. | LocalEventStore | Notice | System | System Integrity |
| Local event storage contains <= 80% unacknowledged events. | LocalEventStore | Notice | System | System Integrity |
| Local event storage contains >= 75% unacknowledged events. | LocalEventStore | Warning | System | System Integrity |
| Local event storage contains >= 90% unacknowledged events. | LocalEventStore | Warning | System | System Integrity |
| Reverted to fallback firmware version {firmwareVersion}. Previous device settings are in effect. Please contact Schweitzer Engineering Laboratories, Inc. for assistance. | FirmwareUpgrade | Critical | System | System Integrity |
| The firmware image is corrupted. | FirmwareUpgrade | Error | System | System Integrity |

The Syslog message "OpenFlow changes ({numberOfChanges}): {stringOfChanges}" (see *Table C.3*) reports the number of changes and a list of as many as 50 of the changes in 10-second intervals. The list is comma-separated and includes an abbreviation and number. All numbers are in hexadecimal format. *Table C.4* describes the meaning of the abbreviation and what the number represents.

**Table C.4 OpenFlow Changes Event Description**

| Abbreviation | Description | Number (in Hexadecimal Format) |
|---|---|---|
| Fa | Flow entry added | Flow ID |
| Fd | Flow Entry deleted | Flow ID |
| Fm | Flow entry modified | Flow ID |
| Fr | Flow replaced | Flow ID |
| Fto | Flow entry deleted because of time-out | Flow ID |
| Ga | Group entry added | Group ID |
| Gd | Group entry deleted | Group ID |
| Gm | Group entry modified | Group ID |
| Ma | Meter entry added | Meter ID |
| Md | Meter entry deleted | Meter ID |

| Abbreviation | Description | Number (in Hexadecimal Format) |
|---|---|---|
| Mm | Meter entry modified | Meter ID |
| Pa | OpenFlow port added | Port ID |
| Pd | OpenFlow port deleted | Port ID |
| Pm | OpenFlow port modified | Port ID |

APPENDIX D

# Cybersecurity Features

Security features of the OT SDN switches provide secure communications between the SEL-5056 Flow Controller and the switch. The switch does not provide access for engineers or technicians; all configuration and monitoring is done by using the SEL-5056.

## Version Information

### Device Firmware

The device firmware identification (FID) number can be obtained through the SEL-5056 Flow Controller. The OT SDN switch firmware is provided in a single digitally signed file.

## Decommissioning

### Preparing for Recycling or Disposal

It is often desirable to delete settings from the product when it is removed from service.

To delete the OT SDN switch settings, either factory-reset the switch through the SEL-5056 Flow Controller or press the pinhole reset button on the front of the switch.

## External Interfaces

### Ports and Services

#### Physical Ports

The OT SDN switch has one front port that is used only for the management of the switch itself. There are multiple data plane ports used for management and data plane packet forwarding. All physical ports are always enabled, but the OT SDN switch is a deny-by-default network switch and does not forward packets unless the flows are configured to do so.

## Logical Ports

**Table D.1 Port Numbers**

| IP Port Default | Network Protocol | Default Port State | Port Configurable | Purpose |
|---|---|---|---|---|
| 3002 | UDP | Enabled | No | Only available to commission the switch. Once commissioned, the port is disabled and can only be enabled again in a factory-default reset state. |
| 443 | TCP | Enabled | No | HTTPS REST interface for switch settings managed by SEL 5056 |
| 161 | SNMP | Disabled | Yes | SNMP read-only IFMIB |

# Access Controls

The OT SDN switch does not have any local user access because all the configuration and monitoring is done by using the SEL-5056 Flow Controller. The OT SDN switch supports OpenFlow communications with TLS, providing mutual authentication and encryption between the flow controller and the switch.

## X.509 Certificates

The OT SDN switch uses TLS with X.509 certificates to protect communications for OpenFlow and the REST interface.

The default certificate installed on the switch is intended to be used for the initial setup only and replaced by a certificate provided by the SEL-5056 Flow Controller once the switch is commissioned. Unique default certificates are generated when the switch is manufactured.

The OT SDN switch supports using SHA2 for signature generation and supports RSA with a 2,048 bit key size.

## Physical Access Controls

The OT SDN switch is designed to make it difficult to physically tamper with the device and its connections without disrupting communications, generating a log, and generating an alarm.

# Logging Features

## Security Events

The OT SDN switch logs events by using Syslog. The OT SDN switch supports either UDP or TCP TLS Syslog and can send events to as many as three network Syslog servers while also activating an alarm contact for certain events. Failure of the delivery of any syslog message is logged and causes activation is itself logged and causes activation of the alarm contact. See *Appendix C: Events* for the list of logged events.

## Internal Log Storage

The OT SDN switch stores logged events internally. Internal storage can hold as many as 4,096 events. In the event that storage is full, new events replace the oldest events.

## Alarm Contact

The OT SDN switch uses an alarm contact that is configurable to operate on the desired event severity level.

# Backup and Restore

## Saving and Restoring Settings

The SEL-5056 Flow Controller saves all configurations of the OT SDN switch. Simple device replacement is supported by the adoption process in the SEL-5056.

# Malware Protection Features

## Operating System and Firmware

The OT SDN switch is an embedded device that does not allow additional software to be installed. The switch only accepts digitally signed firmware upgrades and includes a self-test that continually checks running code against accepted code in nonvolatile memory. See "The SEL Process for Mitigating Malware Risk to Embedded Devices" at https://selinc.com/malware_protection for more details.

# Revision Management

*Appendix A: Firmware and User's Guide Versions* contains a description of each firmware update.

See "The SEL Process for Disclosing Security Vulnerabilities" at https://selinc.com/security_vulnerabilities for details on vulnerability disclosure.

## Update Verification

The OT SDN switch automatically checks the firmware authenticity and integrity of firmware files and only loads files that have been signed by SEL.

The authenticity and integrity of firmware files can be verified by checking the firmware hash. For instructions and firmware hash values, see https://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