



# Stratix 5800 Managed Switches

Catalog Numbers 1783-MMS10B, 1783-MMS10BE, 1783-MMS10, 1783-MMS10E, 1783-MMS10R, 1783-MMS10ER, 1783-MMS10EA, 1783-MMS10EAR, 1783-MMX8T, 1783-MMX8E, 1783-MMX8S, 1783-MMX8SA, 1783-MMX6T2S, 1783-MMX16T, 1783-MMX16E, 1783-MMX14T2S, 1783-MMX8EA



***Allen-Bradley***

by ROCKWELL AUTOMATION

User Manual

Original Instructions

## Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.



**WARNING:** Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.

---



**ATTENTION:** Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

---

### IMPORTANT

Identifies information that is critical for successful application and understanding of the product.

---

Labels may also be on or inside the equipment to provide specific precautions.



**SHOCK HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.

---



**BURN HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

---



**ARC FLASH HAZARD:** Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

---

	<b>Preface</b> .....	9
	About This Publication .....	9
	Download Firmware, AOP, EDS, and Other Files .....	9
	Summary of Changes.....	9
	Additional Resources .....	10
	 <b>Chapter 1</b>	
<b>About the Switches</b>	Stratix 5800 Switches and Expansion Modules.....	11
	EtherNet/IP Interface .....	12
	Software Features.....	12
	Hardware Features.....	13
	Front Panel Overview .....	13
	Power Connectors .....	14
	Alarm Connector .....	15
	Console Ports .....	16
	10/100/1000 BASE-T Downlink Ports .....	18
	10/100/1000 PoE Ports .....	20
	100/1000 SFP Slots.....	21
	Status Indicators .....	21
	 <b>Chapter 2</b>	
<b>Express Setup</b>	Express Setup Modes.....	23
	Express Setup Requirements and Recommendations.....	24
	Express Setup Button .....	25
	Run Express Setup in Short Press Mode.....	26
	Run Express Setup in Medium Press Mode .....	27
	Run Express Setup in Long Press Mode .....	28
	Complete Express Setup via the WebUI .....	28
	Complete Express Setup via the Logix Designer Application.....	33
	Add the Switch to the Controller Project .....	33
	Default Global Macro.....	37
	 <b>Chapter 3</b>	
<b>WebUI Basics</b>	Requirements and Restrictions.....	39
	Access the WebUI .....	40
	Use the WebUI Toolbar .....	43
	Set WebUI Preferences .....	44
	Customize the Dashboard .....	45
	Sort, Filter, and Customize Data in Columns .....	46

## Configure the Switch

### Chapter 4

Authentication, Authorization, and Accounting (AAA) .....	49
AAA Configuration .....	50
Configure AAA via the WebUI Wizard .....	50
Configure AAA Method Lists via the WebUI .....	55
Configure AAA Servers and Server Groups via the WebUI .....	58
Configure AAA Advanced Settings via the WebUI .....	64
Access Control Lists (ACLs) .....	68
Configure ACLs via the WebUI .....	68
Discovery Protocols .....	70
Cisco Discovery Protocol (CDP) .....	70
Link Layer Discovery Protocol (LLDP) .....	70
Configure Discovery Protocols via the WebUI .....	71
Enhanced Interior Gateway Routing Protocol (EIGRP) .....	73
Feature Summary .....	73
Network Operation .....	73
Configure EIGRP via the WebUI .....	74
Ethernet Ports .....	76
Advanced Port Configuration .....	76
Configure Ethernet Interfaces via the WebUI .....	76
Configure Ethernet Ports via the Logix Designer Application ....	82
Flow-based SPAN (FSPAN) .....	84
Configure FSPAN via the WebUI .....	84
Logical Interfaces .....	86
Port Channels or EtherChannels .....	86
EtherChannel Modes .....	86
Loopback Interfaces .....	86
Configure Logical Interfaces via the WebUI .....	87
Configure EtherChannels via the Logix Designer Application ....	89
Hot Standby Router Protocol (HSRP) .....	91
Configure HSRP via the WebUI .....	91
Intermediate System-to-Intermediate System (IS-IS) .....	93
Network Operation .....	93
Configure IS-IS via the WebUI .....	93
Multicast Services .....	94
Configure Multicast Services via the WebUI .....	95
NetFlow .....	95
Configure NetFlow via the WebUI .....	96
Network Address Translation (NAT) .....	98
Configuration Overview .....	98
VLAN Assignments .....	101
Traffic Permits and Fixups .....	102
Configure NAT via the WebUI .....	104
Configure NAT via the Logix Designer Application .....	108
Open Shortest Path First (OSPF) Routing Protocol .....	113
Create an OSPF Route via the WebUI .....	114
Parallel Redundancy Protocol (PRP) .....	116
RedBox PRP Channel Groups .....	117
Traffic and Supervisory Frames .....	118



Node and V DAN Limitations .....	118
Configuration Considerations .....	118
Configure a Stratix 5800 Switch as a RedBox via the WebUI ....	119
Port Security .....	122
Configure Port Security via the WebUI .....	122
Configure Port Security via the Logix Designer Application.....	122
Quality of Service (QoS) .....	123
Auto QoS Macros .....	123
Configure QoS via the WebUI.....	124
Remote Switch Port Analyzer (RSPAN).....	126
Configure RSPAN via the WebUI.....	126
Resiliency Ethernet Protocol (REP) .....	127
Default REP Configuration .....	127
Configuring the REP Administrative VLAN .....	127
REP Port Types .....	127
Configure REP via the WebUI .....	128
Routing .....	130
Configure Static Routing via the WebUI .....	130
Routing Information Protocol (RIP) .....	132
Configure RIP via the WebUI .....	132
Smartports .....	134
Requirements and Restrictions .....	134
Avoid Smartport Mismatches .....	134
Smartport Roles .....	134
Assign Smartport Roles via the WebUI.....	135
Assign Smartport Roles via the Logix Designer Application ....	137
Spanning Tree Protocol (STP) .....	138
Requirements and Restrictions .....	138
STP Modes.....	139
Configure STP via the WebUI.....	139
Configure STP via the Logix Designer Application .....	140
Switched Port Analyzer (SPAN).....	140
Requirements and Restrictions .....	140
Configure SPAN via the WebUI .....	141
TrustSec .....	142
TrustSec Security Groups .....	142
Security Group Tag Exchange Protocol .....	142
TrustSec Policies .....	142
CTS Interface Configuration.....	143
Configure TrustSec via the WebUI .....	143
Virtual Local Area Networks (VLANs) .....	150
Switch Virtual Interfaces (SVIs).....	150
Supported VLANs .....	150
Management VLAN.....	151
Configure SVIs and VLANs via the WebUI .....	151
Configure VLANs via the Logix Designer Application .....	154
Virtual Router Redundancy Protocol (VRRP).....	156
VLAN Trunking Protocol (VTP).....	156
Requirements and Restrictions .....	156
VTP Modes.....	156

Configure VTP via the WebUI.....	157
.....	157

## Chapter 5

### Administer the Switch

Alarm Profiles .....	159
Alarm Types.....	159
Alarm Actions .....	160
Default Alarm Profile .....	160
Create an Alarm Profile via the WebUI.....	161
Alarm Settings.....	162
External Alarm Devices .....	162
Global Alarm Types .....	162
Alarm Actions for Global Alarms .....	162
Configure Alarm Settings via the WebUI.....	163
Back Up, Restart, and Restore Procedures .....	166
Back Up and Restore Configuration Files via the WebUI.....	166
Restart the Switch via the WebUI .....	168
Sync the Switch with an SD Card via the WebUI .....	168
Back Up, Restore, and Sync Configuration Files via the Logix Designer Application .....	169
Common Industrial Protocol (CIP) .....	171
Configure CIP via the WebUI .....	171
Command-line Interface (CLI) .....	172
CLI Modes .....	172
Run CLI Commands via the WebUI .....	172
Device Settings .....	173
Configure Device Settings via the WebUI .....	173
Configure Device Settings via the Logix Designer Application ..	175
Device Time .....	177
Set Time Manually.....	177
Set Time via NTP .....	177
Set Time via PTP.....	178
Configure Device Time via the WebUI .....	178
Configure Device Time via the Logix Designer Application .....	183
Domain Name System (DNS) .....	188
Add a DNS Server via the WebUI.....	188
Dynamic Host Configuration Protocol (DHCP) .....	190
DHCP Persistence .....	190
DHCP Snooping.....	191
Configure DHCP via the WebUI .....	192
Configure DHCP via the Logix Designer Application .....	195
File Manager .....	198
HTTP/HTTPS/Netconf Access .....	200
Certificate Authority (CA) Trustpoints.....	200
Configure HTTP/HTTPS/Netconf Access via the WebUI.....	200
Requirements and Restrictions .....	201
Configure MODBUS via the WebUI .....	202
Power over Ethernet (PoE) .....	203
Requirements and Restrictions .....	203

## Security Requirements (IEC-62443-4-2)

PoE Port Modes .....	203
Configure PoE via the WebUI .....	204
Configure PoE via the Logix Designer Application .....	206
PROFINET .....	207
Configure PROFINET via the WebUI .....	207
SDM-Template .....	209
Simple Network Management Protocol (SNMP) .....	210
Supported SNMP Versions .....	210
SNMPv3 User Security Modes and Authentication .....	210
Configure SNMP via the WebUI .....	210
Software Upgrade .....	215
User Administration .....	216
Privilege Levels .....	216
Password Policies .....	216
Create a User Account via the WebUI .....	216

## Chapter 6

Switch Security Features .....	219
Telnet .....	220
Verify Telnet Settings .....	220
Disable Telnet .....	221
TLS 1.2 .....	222
Verify TLS 1.2 Settings .....	222
Enable TLS 1.2 .....	223
Additional Resources .....	223

## Monitor the Switch

## Chapter 7

Switch Status .....	225
Neighbors .....	226
Common Industrial Protocol (CIP) .....	228
Dynamic Host Configuration Protocol (DHCP) Clients .....	230
Network Address Translation (NAT) .....	231
MODBUS (Modicon Communication Bus) .....	237
Ports .....	239
Parallel Redundancy Protocol (PRP) .....	242
Resiliency Ethernet Protocol (REP) .....	246
System .....	247
Time .....	250

## Troubleshoot the Switch

## Chapter 8

Configure and View System Logs .....	253
Message Severity Levels .....	253
Download Core Files .....	256
Download a Debug Bundle .....	257
Troubleshoot with Ping and Trace Route .....	258
Ping Destinations .....	259
Discover Route Information .....	259
Troubleshoot the Installation .....	260

	Bad or Damaged Cable .....	260
	Ethernet and Fiber Cables .....	260
	Port Status .....	260
	SFP Module Issues .....	261
	Port Settings .....	261
	Troubleshoot IP Addresses .....	261
	Troubleshoot the WebUI .....	262
	Troubleshoot Switch Performance .....	262
	<b>Appendix A</b>	
<b>Status Indicators</b>	Stratix 5800 Status Indicators .....	263
	Power Status Indicators .....	264
	Power over Ethernet Status Indicator .....	264
	Setup Status Indicator .....	264
	EIP Status Indicators .....	265
	Alarm Status Indicators .....	265
	Port Status Indicators .....	266
	<b>Appendix B</b>	
<b>Data Types</b>	10-Port Data Types .....	267
	18-Port Data Types .....	269
	26-Port Data Types .....	271
	<b>Appendix C</b>	
<b>Port Assignments for CIP Data</b>	Port Assignments .....	275
	<b>Appendix D</b>	
<b>Port Numbering</b>	Switch Port Numbering .....	277
	Expansion Module Port Numbering .....	279
	<b>Appendix E</b>	
<b>MODBUS Register Lists</b>	10-port Register Files .....	281
	18-port Register Files .....	282
	26-port Register Files .....	285
	System Register File .....	288
	<b>Index</b> .....	289



## About This Publication

This publication describes how to configure, manage, and troubleshoot Stratix® 5800 managed Ethernet switches and expansion modules.

This manual assumes that you understand the following:

- Ethernet concepts and terminology
- Local area network (LAN) switch fundamentals

## Download Firmware, AOP, EDS, and Other Files

Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes from the Product Compatibility and Download Center at [rok.auto/pcdc](http://rok.auto/pcdc).

## Summary of Changes

This publication contains the following new or updated information. This list includes substantive updates only and is not intended to reflect all changes.

Topic	Page
Discovery Protocols	70
Enhanced Interior Gateway Routing Protocol (EIGRP)	73
Flow-based SPAN (FSPAN)	84
Hot Standby Router Protocol (HSRP)	91
Intermediate System-to-Intermediate System (IS-IS)	93
Multicast Services	94
Neighbors	226
PROFINET	208
PRP Supported on Expansion Module	119
Quality of Service (QoS)	122
Remote Switch Port Analyzer (RSPAN)	127
Routing Information Protocol (RIP)	133
SDM-Template	210
Security Requirements (IEC-62443-4-2)	219
TrustSec	143
Virtual Router Redundancy Protocol (VRRP)	157

## Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

Resource	Description
Stratix Ethernet Device Specifications Technical Data, publication <a href="#">1783-TD001</a>	Provides specifications for the switches and other devices.
Stratix 5800 Modular Managed Ethernet Switches Installation Instructions, publication <a href="#">1783-IN013</a>	Describes how to install Stratix 5800 switches and expansion modules.
Online Help within the Web user interface (WebUI) (provided with the switch)	Provides context-sensitive Help for pages within the WebUI.
EtherNet/IP Network Devices User Manual, <a href="#">ENET-UM006</a>	Describes how to configure and use EtherNet/IP™ devices with a Logix 5000™ controller and communicate with various devices on the Ethernet network.
Ethernet Reference Manual, publication <a href="#">ENET-RM002</a>	Describes basic Ethernet concepts, infrastructure components, and infrastructure features.
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, publication <a href="#">ENET-TD001</a>	Represents a collaborative development effort from Rockwell Automation® and Cisco Systems®. Adds to design guidelines from the Cisco® Ethernet-to-the-Factory (EttF) solution and the Rockwell Automation Integrated Architecture® system.
Industrial Automation Wiring and Grounding Guidelines, publication <a href="#">1770-4.1</a>	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, <a href="#">rok.auto/certifications</a>	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at [rok.auto/literature](#).

# About the Switches

Topic	Page
Stratix 5800 Switches and Expansion Modules	11
EtherNet/IP Interface	12
Software Features	12
Hardware Features	13

The Stratix® 5800 managed switch supports Layer 2 and Layer 3 switching on an all gigabit platform. The hybrid design includes both standalone and modular switches. The platform supports up to 26 ports with a variety of copper, PoE, and fiber SFP options, providing flexibility for high-performance network applications.

## Stratix 5800 Switches and Expansion Modules

The following table describes the types of Stratix 5800 modules. Some switch and expansion modules support advanced Ethernet features and Power over Ethernet (PoE). For details by catalog number, see the Stratix Ethernet Device Specifications Technical Data, publication [1783-TD001](#).

**IMPORTANT** Only one expansion module can be attached to a modular switch.



Stratix 5800 Switches and Expansion Modules

Devices	Description
Fixed switches	Gigabit Ethernet, Layer 2, fixed switches. Available in 10-port versions.
Modular switches	Gigabit Ethernet, Layer 2 or Layer 3, modular switches. Advanced feature support on some models. Available in 10-port versions..
Expansion modules	Gigabit Ethernet expansion modules. Advanced feature support on some models. Available in 8- and 16-port versions.

## EtherNet/IP Interface

Stratix 5800 switches contain an EtherNet/IP™ network interface. The EtherNet/IP network is an industrial automation network specification from the Open DeviceNet® Vendor Association (ODVA). The network uses the Common Industrial Protocol (CIP™) for its application layer. CIP is a messaging protocol for devices in industrial automation control systems.

For more information about the EtherNet/IP protocol and CIP, see the Ethernet Reference Manual, publication [ENET-RM002](#).

## Software Features

Switch software features can be configured in the web user interface (WebUI) for the switch, the Studio 5000 Logix Designer® application, or both, as shown in [Table 1](#).

All features, including additional features that are not described in this publication, are configurable via the Cisco® command-line interface (CLI). See [Command-line Interface \(CLI\) on page 172](#).

**Table 1 - Supported Catalog Numbers and Software for Switch Features**

Feature	Catalog Numbers	WebUI	Logix Designer Application
Authentication, authorization, and accounting (AAA)	All	Yes	No
Access control lists (ACLs)	All	Yes	No
Alarm profiles	All	Yes	No
Cisco® Discovery Protocol (CDP)	All	Yes	No
Common Industrial Protocol (CIP) monitoring	All	Yes	No
Domain name system (DNS)	All	Yes	No
Dynamic Host Configuration Protocol (DHCP)	All	Yes	Yes
Enhanced Interior Gateway Routing Protocol (EIGRP)	1783-MMS10R, 1783-MMS10ER, 1783-MMS10EAR	Yes	No
Express Setup	All	Yes	Yes
HTTP/HTTPS	All	Yes	No
Intermediate System-to-Intermediate System (IS-IS)	1783-MMS10R, 1783-MMS10ER, 1783-MMS10EAR	Yes	No
Link Layer Discovery Protocol (LLDP)	All	Yes	No
Logical interfaces (EtherChannel/Port Channel)	All	Yes	Yes
Multicast services and Internet Group Management Protocol (IGMP)	All	Yes	No
NetFlow	1783-MMS10, 1783-MMS10E, 1783-MMS10EA, 1783-MMS10R, 1783-MMS10ER, 1783-MMS10EAR	Yes	No
Network Address Translation (NAT)	1783-MMS10, 1783-MMS10E, 1783-MMS10EA, 1783-MMS10R, 1783-MMS10ER, 1783-MMS10EAR	Yes	Yes
Network Time Protocol (NTP)	All	Yes	Yes
Open Shortest Path First (OSPF)	1783-MMS10R, 1783-MMS10ER, 1783-MMS10EAR	Yes	No
Parallel Redundancy Protocol (PRP)	1783-MMS10EA, 1783-MMS10EAR, 1783-MMX8EA, 1783-MMX8TA, 1783-MMX8SA	Yes	Yes
Port mirroring/Switch Port Analyzer (SPAN)	All	Yes	No
Port security (MAC ID-based)	All	Yes	Yes
Port thresholds	All	Yes	No
Power over Ethernet (PoE)	1783-MMS10BE, 1783-MMS10E, 1783-MMS10EA, 1783-MMS10ER, 1783-MMS10EAR, 1783-MMX8E, 1783-MMX8EA, 1783-MMX16E	Yes	Yes
Precision Time Protocol (PTP)	All	Yes	Yes
Quality of Service (QoS)	All	Yes	No
Resilient Ethernet Protocol (REP)	All	Yes	No
Routing, Layer 3	1783-MMS10R, 1783-MMS10ER, 1783-MMS10EAR	Yes	No
Routing, static and connected	All	Yes <sup>(1)</sup>	No



**Table 1 - Supported Catalog Numbers and Software for Switch Features (Continued)**

Feature	Catalog Numbers	WebUI	Logix Designer Application
Simple Network Management Protocol (SNMP)	All	Yes	No
Smartports	All	Yes	Yes
Spanning Tree Protocol (STP)	All	Yes	Yes
Syslog	All	Yes	No
TrustSec	1783-MMS10EA, 1783-MMS10EAR, 1783-MMX8EA, 1783-MMX8TA, 1783-MMX8SA	Yes	No
Virtual local area networks (VLANs)	All	Yes	Yes
VLAN Trunk Protocol (VTP)	All	Yes	No
VRF-Lite	1783-MMS10R, 1783-MMS10ER, 1783-MMS10EAR	Yes	No

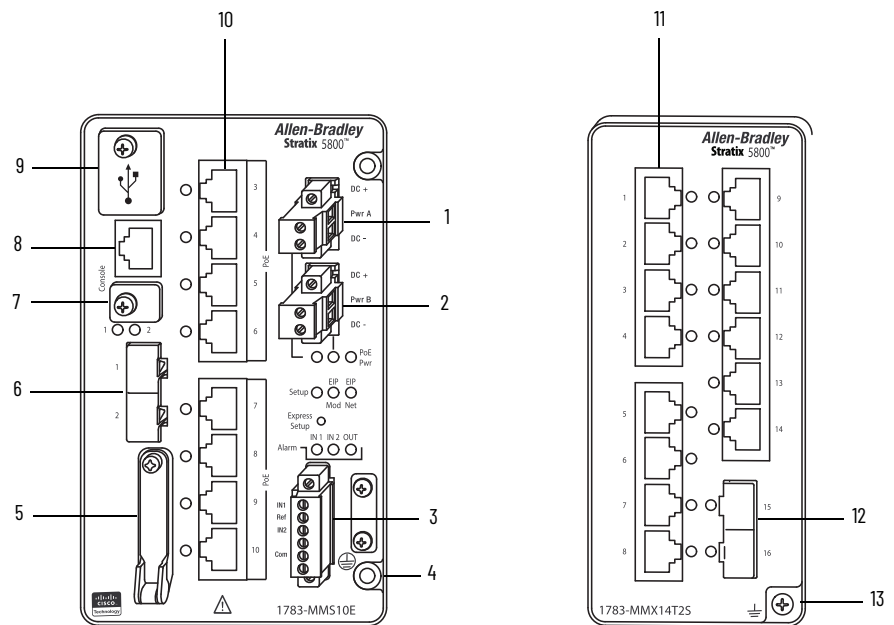
(1) Only static routing can be configured via the WebUI. Connected routing is enabled by default and cannot be disabled.

## Hardware Features

For detailed hardware specifications, see the Ethernet Device Specifications Technical Data, publication [1783-TD001](#).

## Front Panel Overview

For illustration purposes, the switch and expansion catalog numbers that are shown in the following example have PoE ports. Port types and combinations vary by catalog number, and not all models have PoE ports.



### Table 2 - Front Panel

Item	Description
1	Power connector (Pwr A)
2	Power connector (Pwr B)
3	Alarm connector
4	Protective ground connection
5	SD card slot

**Table 2 - Front Panel**

Item	Description
6	SFP module slots (uplink ports)
7	USB mini-Type B console port
8	RJ45 console port
9	2 USB Type A ports
10	Ethernet PoE/PoE+ ports (downlink ports)
11	Ethernet ports (downlink ports)
12	SFP module slots (downlink ports)
13	Electromagnetic compatibility (EMC) ground connection <sup>(1)</sup>

(1) When an expansion module is connected, it must be grounded using the screw on the expansion module. This is an EMC ground, not a protective ground, unlike the one on the switch.

## Power Connectors

You connect the DC power to the switch through the front panel connectors. The switch has a dual-feed DC power supply:

- One connector provides primary DC power.
- A second connector provides secondary DC power.

The two connectors are physically identical. There is no separate power connector for PoE.

The switch can operate with one power source or with dual power sources. When both power sources are operational, the switch draws power from the DC source with the higher voltage. If one of the two power sources fail, the other continues to power the switch without interruption.

## Alarm Connector

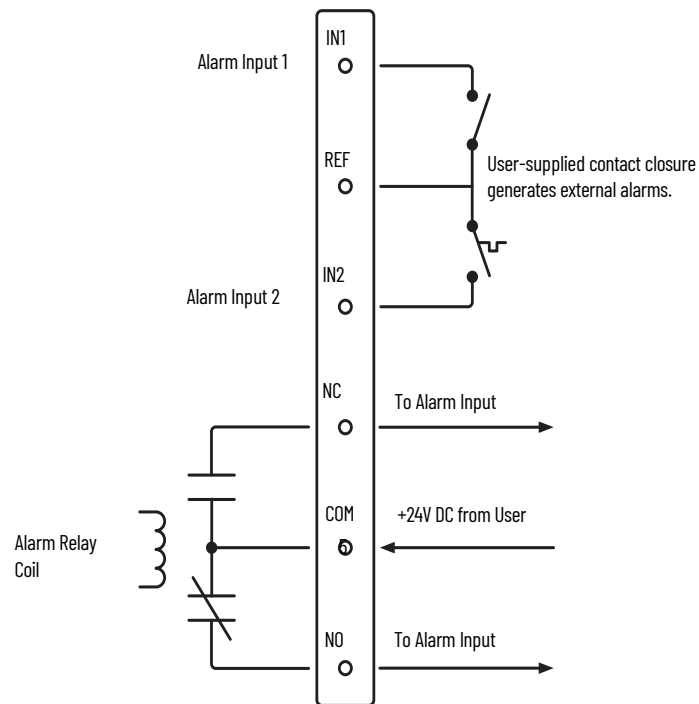
You connect the alarm signals to the switch through the alarm connector. The alarm connector is attached to the switch front panel with the provided captive screws.

The switch supports two alarm inputs and one alarm output relay.

- In the WebUI for the switch, you can configure each alarm input as an open or closed contact. See [Configure Alarm Relays on page 163](#).
- The alarm output circuit is a relay with a normally open and a normally closed contact. Normally open contacts close. Normally closed contacts open. The alarm output relay can be used to control an external alarm device, such as a bell or a light.

For information about how to configure alarm settings, see [page 162](#).

**Figure 1 - Wiring for Alarm Connector**



**Table 3 - Alarm Connector Labels**

Label	Connection
IN1	Alarm Input 1
REF	Alarm Input Reference Ground connection
IN2	Alarm Input 2
NC	Alarm Output Normally Closed (NC) connection
COM	Alarm Output Common connection
NO	Alarm Output Normally Open (NO) connection

## Console Ports

The console ports on the switch enable you to configure, monitor, and manage the switch via the Cisco command-line interface (CLI). Use the console ports to connect to a workstation with terminal software on a Microsoft® Windows machine.

You can connect to either the RJ45 console port or the USB mini-Type B console port, also referred to as the USB-mini console port. Only one console port can be active at one time.

The console ports use the following connectors:

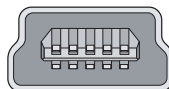
- RJ45 to DB-9 female cable for the RJ45 console port
- 5-pin mini-Type B to USB Type A cable for the USB-mini console port
- RJ45 to USB Type A cable for the RJ45 console port (Allen-Bradley® catalog number 9300-USBCBL-CNSL)

The USB-mini console interface speeds are the same as the RJ45 console interface speeds.

To use the USB-mini console port, you must install the USB device driver on the device that is connected to the USB-mini console port. The mini USB driver is available at the Product Compatibility and Download Center (PCDC) at <http://www.rockwellautomation.com/global/support/pcdc.page>. With the Windows USB device driver, Windows HyperTerminal operations are not affected if you connect and disconnect the USB cable from the console port. Mac OS X or Linux requires no special drivers.

The 5-pin mini-Type B connectors resemble the 4-pin mini-Type B connectors, but they are not compatible. Use only the 5-pin mini-Type B as shown in [Figure 2](#).

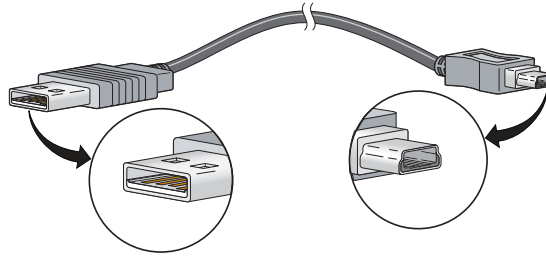
**Figure 2 - USB Mini-Type B Port**





The USB console port uses a USB Type A to 5-pin mini-Type B cable as shown in [Figure 3](#). The USB cable is not provided with the switch.

**Figure 3 - USB Cable**



If the USB-mini console port is activated, but no input activity occurs for a configured time period, the timeout reactivates the RJ45 console port. When the USB-mini console port deactivates due to a timeout, disconnect and reconnect the USB cable to restore its operation.

[Table 4](#) lists the pinouts for the console port, the RJ45-to-DB-9 adapter cable, and the console device. The adapter cable is not supplied with the switch.

**Table 4 - Pinouts with DB-9 Pin**

Switch Console Port (DTE)	RJ45-to-DB-9 Terminal Adapter	Console Device
Signal	DB-9 Pin	Signal
RTS	8	CTS
DTR	6	DSR
TxD	2	RxD
GND	5	GND
GND	5	GND
RxD	3	TxD
DSR	4	DTR
CTS	7	RTS

[Table 5](#) lists the pinouts for the console port, RJ45-to-DB-25 female DTE adapter, and the console device. The RJ45-to-DB-25 female DTE adapter is not supplied with the switch.

**Table 5 - Pinouts with DB-25 Pin**

Switch Console Port (DTE)	RJ45-to-DB-25 Terminal Adapter	Console Device
Signal	DB-25 Pin	Signal
RTS	5	CTS
DTR	6	DSR
TxD	3	RxD
GND	7	GND
GND	7	GND
RxD	2	TxD
DSR	20	DTR
CTS	4	RTS

## 10/100/1000 BASE-T Downlink Ports

The copper Ethernet ports can operate at 10,100, or 1000 Mbps and full-duplex or half-duplex. You can also set these ports for speed and duplex autonegotiation in compliance with IEEE 802.3AB. The default setting is autonegotiated.

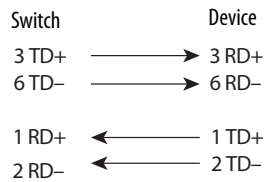
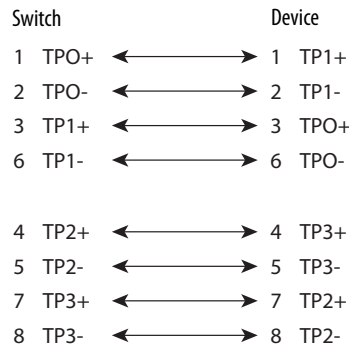
When set for autonegotiation, the port senses the speed and duplex settings of the attached device. If the connected device also supports autonegotiation, the switch port negotiates the connection with the fastest line speed that both devices support. The port also negotiates full-duplex transmission if the attached device supports it. The port then configures itself accordingly. In all cases, the attached device must be within 100 m (328 ft) of the switch.

When the auto-MDIX feature is enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. The auto-MDIX feature is enabled by default.

Follow these cabling guidelines when the auto-MDIX feature has been disabled:

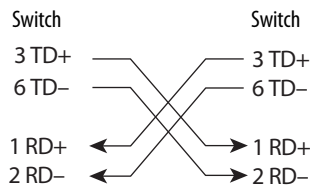
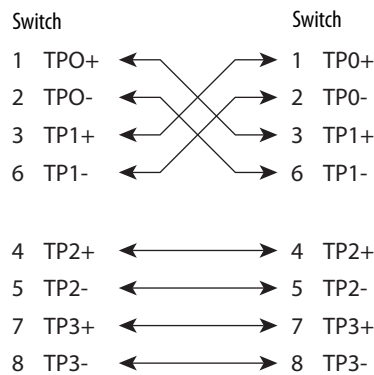
- To connect two ports when only one port is designated with an X, use a straight-through cable. To connect two ports when both ports are designated with an X or when both ports do not have an X, use a crossover cable.
- To connect the ports to compatible devices, such as workstations, servers, and routers, use a two or four twisted-pair, straight-through cable that is wired for 10Base-T, 100Base-TX, 1000Base-T:
  - 10Base-T traffic can use Category 3 or Category 4 cables.
  - 100Base-TX traffic requires Category 5 cables.
  - 1000Base-T traffic requires four twisted-pair Category 5 cables.

[Figure 4](#) and [Figure 5](#) show the cable schematics.

**Figure 4 - Two Twisted-pair Straight-through Cable Schematics****Figure 5 - Four Twisted-pair Straight-through Cable Schematics**

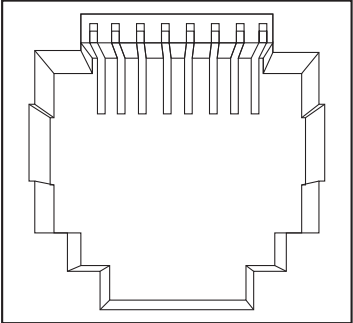
To connect the ports to 10Base-T- and 100Base-TX-compatible devices, such as switches or repeaters, you can use a two or four twisted-pair, crossover cable. To identify a crossover cable, compare the two modular ends of the cable. Hold the cable ends side by side, with the tab at the back. Be sure that the wires for the pins on the outside of the left plug and inside of the right plug are different colors.

[Figure 6](#) and [Figure 7](#) show the cable schematics.

**Figure 6 - Two Twisted-pair Crossover Cable Schematics****Figure 7 - Four Twisted-pair Crossover Cable Schematics**

Copper Ethernet ports use standard RJ45 connectors and Ethernet pinouts with internal crossovers.

Figure 8 - 10/100/100 Connector Pinouts

Pin	Label	1	2	3	4	5	6	7	8
1	TP0+								
2	TP0-								
3	TP1+								
4	TP2+								
5	TP2-								
6	TP1-								
7	TP3+								
8	TP3-								

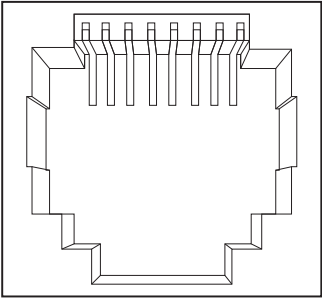
10/100/1000 PoE Ports

Gigabit Ethernet PoE/PoE+ ports are available on some switches and expansion modules. The ports provide full-duplex 10 Mbps, 100 Mbps, or 1000 Mbps connectivity. These ports can be configured for PoE (IEEE 802.3af) or PoE+ (IEEE 802.3at Type 2). You can configure PoE/PoE+ ports in any combination of PoE and PoE+.

PoE/PoE+ ports require four twisted-pair Category 5 cables.

PoE/PoE+ ports integrate power and data signals on the same wires. The ports use standard RJ45 connectors and Ethernet pinouts with internal crossovers.

Figure 9 - 10/100/1000 PoE Connector Pinouts and Power Sourcing Equipment (PSE) Voltage

Pin	Label	Alternative A (MDI)	1	2	3	4	5	6	7	8
1	RD+	Positive V PSE								
2	RD-	Positive V PSE								
3	TD+	Negative V PSE								
4	NC									
5	NC									
6	TD-	Negative V PSE								
7	NC									
8	NC									



## 100/1000 SFP Slots

The IEEE 802.3u 1000 Mbps SFP slots provide full-duplex 1000 Mbps connectivity over multimode (MM) fiber cables or singlemode (SM) fiber cables. These ports use an SFP module that accepts a dual LC connector.



---

**ATTENTION:** Only use SFP modules from Rockwell Automation. For details about supported modules, see the Stratix Ethernet Device Specifications Technical Data, publication [1783-TD001](#).  
Stratix 5800 switches do **not** support SFP catalog numbers 1783-SFP100T, 1783-SFP10GSRE, and 1783-SFP10GLRE.

---

## Status Indicators

The status indicators on the front panel of the switch enable you to monitor the switch status, activity, and performance. For more information about status indicators, see [Appendix A](#).

**Notes:**

## Express Setup

Topic	Page
Express Setup Modes	23
Express Setup Requirements and Recommendations	24
Express Setup Button	25
Run Express Setup in Short Press Mode	26
Run Express Setup in Medium Press Mode	27
Run Express Setup in Long Press Mode	28
Complete Express Setup via the WebUI	28
Complete Express Setup via the Logix Designer Application	33
Default Global Macro	37

Use the Express Setup process to perform these initial setup tasks:

- Assign the switch an IP address. You can then access the switch through the IP address for additional configuration.
- Run the global macro to set initial configuration parameters as described on [page 37](#).

## Express Setup Modes

Express Setup has three modes:

**Short Press mode**—You want to use a directly connected computer to enter the initial IP address of the switch. You can then configure additional network settings via the WebUI. To run Short Press mode, see [page 26](#).

**Medium Press mode**—You want to use a DHCP server to assign the switch an IP address. You can then configure additional network settings via the WebUI or the Studio 5000 Logix Designer® application. To run Medium Press mode, see [page 27](#).

**Long Press mode**—You want to reset the switch to use factory default settings. To run Long Press mode, see [page 28](#).

---

**IMPORTANT** The Studio 5000 Logix Designer application supports only Medium Press mode.

---

[Table 6](#) summarizes the function of each mode.

Table 6 - Express Setup Modes

Attribute	Short Press Mode	Medium Press Mode	Long Press Mode
Enable method	Press and hold the Express Setup button until the Setup status indicator flashes green during seconds 1...5, and then release.	Press and hold the Express Setup button until the Setup status indicator flashes red during seconds 6...10, and then release.  Between seconds 11...15 and after 21 seconds, the Setup status indicator turns off. If you release the Express Setup button while the Setup status indicator is off, no Express Setup mode is enabled.	Press and hold the Express Setup button until the Setup status indicator flashes alternating green and red during seconds 16...20, and then release.
Setup status indicator	Flashes green between seconds 1...5.	Flashes red between seconds 6...10.	Flashes green and red between seconds 16...20.
Function	The Express Setup management interface is selected. The switch acts as a DHCP server on VLAN 1000 with an address of 192.168.1.254. Once the DHCP session is successfully established, the switch assigns the computer an IP address of 192.168.1.1. The default login credentials are set to the following: User name: admin Password: switch	The switch sends a DHCP client request out of all ports on VLAN 1. DHCP assigns VLAN 1 an IP address. The default login credentials are set to the following: User name: admin Password: switch CIP™ (Common Industrial Protocol) is enabled on VLAN 1 with the CIP password set to <b>switch</b> .	All configuration settings (config.text, vlan.dat, and private-config.text files) in internal memory or on the SD card are reset to factory defaults. The switch restarts with factory default settings.
Software Tool for Express Setup Configuration	WebUI only	WebUI or Logix Designer application	Not applicable

## Express Setup Requirements and Recommendations

All Express Setup modes require a small tool, such as a paper clip to press the Express Setup button.

In Short Press mode, you are required to complete Express Setup parameters via the WebUI. You need the following:

- A workstation with a supported operating system and browser. See [Table 7](#).
- A straight-through or crossover Category 5 Ethernet cable to connect your workstation to the switch port.

In Medium Press mode, you can complete Express Setup parameters via the WebUI or the Logix Designer application. You need the following:

- For the WebUI, you need a supported operating system and browser. See [Table 7](#).
- For the Logix Designer application, you need the Add-on Profile (AOP) for Stratix® switches, version 19.01.07 or later.
- A DHCP server and a Category 5 Ethernet cable to connect to the DHCP server.

Table 7 - Express Setup Recommendations

Component	Minimum Version
<b>Operating System</b>	
Microsoft® Windows	7 or higher
Apple Mac OS	10.9.5 or later
<b>Browser</b>	
Google Chrome	38 or later
Microsoft Edge	11 or later
Mozilla Firefox	25 or later
Apple Safari	7 or later
<b>Screen Resolution</b>	
1280 x 800 or higher	

Before you begin, do the following:

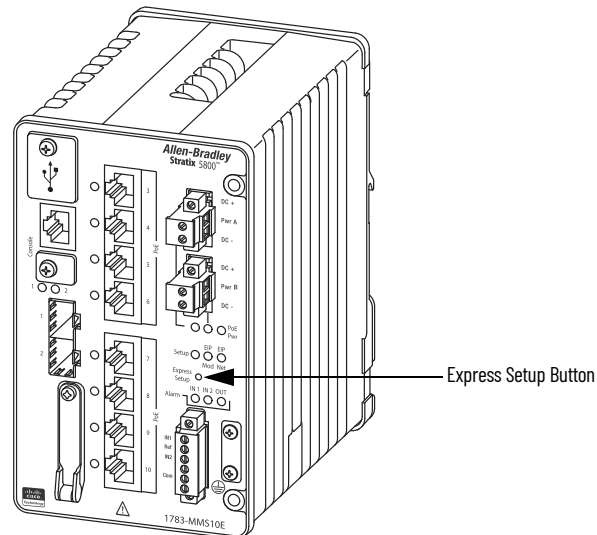
- To run Express Setup in Short Press mode:
  - Disable other networks in your system.
  - Set your computer to determine its IP address automatically versus statically.
  - Disable static DNS servers.
  - Disable any wireless interface on your computer.
- Disable browser proxy settings.
- Make sure at least one switch Ethernet port is available for Express Setup.

## Express Setup Button

Use the Express Setup button on the physical switch to perform Express Setup. This Express Setup button is recessed behind the panel. To reach the button, use a small tool, such as a paper clip.



**WARNING:** When you press the Express Setup button while power is on, an electric arc can occur, which could cause an explosion in hazardous location installations.



## Run Express Setup in Short Press Mode

Be aware of the following conditions that cause the switch to exit Short Press mode.

**Table 8 - Conditions in Short Press Mode**

Condition	Status Indicator Behavior
A non-default configuration exists on the switch.	The Setup status indicator turns red for 10 seconds.
You do not connect to the Express Setup port within 2 minutes from when the port status indicator flashes green.	The unconnected port status indicator and the Setup status indicator turn off.
No DHCP request is received for 2 minutes from when you connect to the Express Setup port.	The Setup status indicator turns red for 10 seconds.
No browser session is started for 60 minutes after an IP address is assigned to the computer.	The Setup status indicator turns off, but the connected port status indicator remains on.
You disconnect your computer from the switch before the setup process is complete.	All temporary configurations that are applied by Express Setup, such as DHCP server, are removed.

To run Express Setup in Short Press mode, follow these steps.

1. Apply power to the switch.

When the switch powers on, it begins its power-on sequence. The power-on sequence can take as long as 90 seconds to complete.

2. **Make sure that the power-on sequence has completed by verifying that the EIP Mod and Setup status indicators are flashing green.**

If the switch fails the power-on sequence, the EIP Mod status indicator turns red.

If you do not press the Express Setup button within 5 minutes after the power-on sequence is complete, the Setup status indicator turns off. However, you can still run Express Setup after the Setup status indicator turns off.

3. Press and hold the Express Setup button until the Setup status indicator flashes green during seconds 1...5, and then release.

The switch selects a port to use for Express Setup.

4. Connect a Category 5 Ethernet cable from the flashing switch port to the Ethernet port on your workstation:
  - The status indicator for the port connected to the computer changes from flashing green to solid green.
  - The switch acts as a DHCP server on VLAN 1000 with an address of 192.168.1.254.
  - The switch assigns the computer an IP address of 192.168.1.1.
  - The Setup status indicator changes from flashing green to solid green.
5. Proceed to [Complete Express Setup via the WebUI on page 28](#).

## Run Express Setup in Medium Press Mode

Be aware of the following conditions that cause the switch to exit Medium Press mode.

**Table 9 - Conditions in Medium Press Mode**

Condition	Status Indicator Behavior
A non-default configuration exists on the switch.	The Setup status indicator turns red for 10 seconds.
No DHCP response is received for 10 minutes from when the switch broadcast the request.	
No browser session is started for 60 minutes after an IP address is assigned to the computer.	The Setup status indicator turns off, but the connected port status indicator remains on.
<b>IMPORTANT</b> Before you begin, make sure that your system has a DHCP server that is configured to assign the switch an IP address.	

To run Express Setup in Medium Press mode, follow these steps.

1. Apply power to the switch.

When the switch powers on, it begins its power-on sequence. The power-on sequence can take as long as 90 seconds to complete.

2. **Make sure that the power-on sequence has completed by verifying that the EIP Mod and Setup status indicators are flashing green:**
  - If the switch fails the sequence, the EIP Mod status indicator turns red.
  - If you do not press the Express Setup button within 5 minutes after the sequence completes, the Setup status indicator turns off. However, you can still run Express Setup after the Setup status indicator turns off.
3. Press and hold the Express Setup button until the Setup status indicator flashes red during seconds 6...10, and then release.

---

**IMPORTANT** You must complete the switch setup within 10 minutes of releasing the Express Setup button. Otherwise, the switch exits Express Setup.

---

The following occurs:

- The switch sends a DHCP request out of all ports on VLAN 1.
- DHCP assigns VLAN 1 an IP address.
- The default login credentials are set to the following:
  - User name: admin
  - Password: switch
  - CIP is enabled on VLAN 1 with CIP security password set to **switch**.
- 4. Complete the Express Setup configuration via the WebUI or the Logix Designer application:
  - To use the WebUI, proceed to [Complete Express Setup via the WebUI on page 28](#).
  - To use the Logix Designer application, proceed to [Complete Express Setup via the Logix Designer Application on page 33](#).



## Run Express Setup in Long Press Mode

---

**IMPORTANT** Long Press mode overwrites all existing configuration files in internal or external memory and resets the switch to use factory default settings.

---

Press and hold the Express Setup button until the Setup status indicator flashes alternating green and red during seconds 16...20, and then release.

Upon release of the Express Setup button, the switch restarts with factory default settings.

## Complete Express Setup via the WebUI

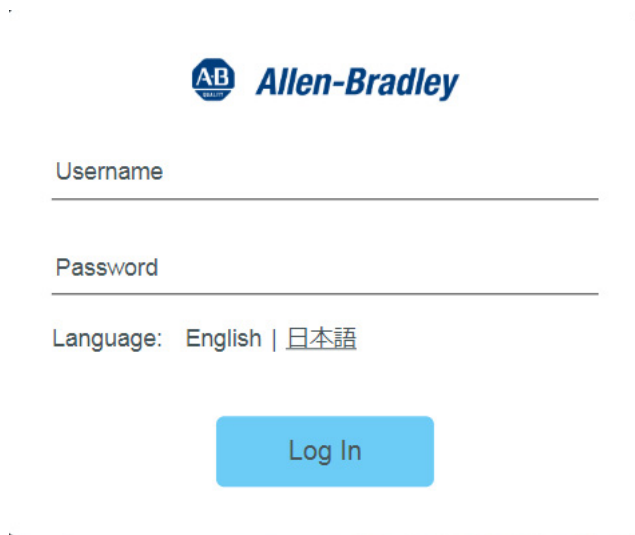
To complete the initial setup of the switch via the WebUI, follow these steps.

1. Start a web browser session and go to the IP address of the switch.

For help with browser security options, see [page 40](#).

If the Login page does not appear, try the following:

- Verify that your network adapter is set to accept a DHCP address.
  - Enter the URL of a well-known website in your browser to be sure that the browser is working correctly. Your browser then redirects to Express Setup.
  - Verify that any proxy settings or popup blockers are disabled on your browser.
  - Verify that any wireless interface is disabled on the computer.
2. On the Login page, enter the administrator user name and password, and click Login Now.



The image shows a screenshot of the Allen-Bradley Express Setup login page. At the top, there is the Allen-Bradley logo. Below the logo, there are two input fields: 'Username' and 'Password'. Under the 'Password' field, there is a 'Language' dropdown menu currently set to 'English', with '日本語' (Japanese) as an alternative option. At the bottom of the form, there is a blue 'Log In' button.

3. Configure account settings as described in [Table 10](#), and then click Basic Settings.

The screenshot shows the Express Setup wizard with three tabs: ACCOUNT SETTINGS, BASIC SETTINGS, and SUMMARY. The ACCOUNT SETTINGS tab is active, displaying the 'Create New Account' section with fields for Login Name\* (admin), Login User Password\*, Confirm Login User Password\*, and Command Line Password (Sync to Login Password). Below this is the 'Device ID Settings' section with fields for Device Name\*, NTP Server, and Date & Time Mode (NTP Time). The BASIC SETTINGS tab is also visible, showing device hardware and software details.

**Table 10 - Account Settings**

Field	Description
<b>Create New Account</b>	
Login Name	Enter a user name for the administrator.
Login User Password	Enter a password for the administrator.
Confirm Login User Password	Reenter the password for the administrator user.
Command Line Password	To set the password for entering commands in the Cisco® command-line interface (CLI), choose one of the following options: Sync to Login Password—Sets the password to the same password you specified for the current user login name. Set New Password—Sets a new password that you specify. No Password—Does not require a password to enter CLI commands.
<b>Device ID Settings</b>	
Device Name	Enter a unique name to identify the physical switch.
NTP Server	Enter the IP address of the Network Time Protocol (NTP) server.
Date & Time Mode	Choose one of the following options to set the date and time on the switch: NTP Time—Upon initial setup, the switch uses the date and time set on the connected workstation. Once the switch is connected to your network, it then syncs the date and time to match the NTP server on the network. Manually Enter Time—The switch uses the date and time that you manually enter in the following Date and Time fields.
Date	(Appears only if you choose Manually Enter Time in the Date & Time Mode field). Enter the date and time to set on the switch.
Time	

4. Configure basic settings as described in [Table 11](#), and then click Day 0 Config Summary.

✓

ACCOUNT SETTINGS

●

BASIC SETTINGS

●

SUMMARY

Device Management Settings

IP Address

☒ Static

☐ DHCP

VLAN ID\*

IP Address\*

Subnet Mask\*

Default Gateway (optional)

Associate VLAN with interfaces

Available ( 0 )

Selected ( 26 )

GigabitEthernet1/1 ←

< Account Settings

Day 0 Config Summary >

To view all basic settings, scroll down the page.

✓

ACCOUNT SETTINGS

●

BASIC SETTINGS

●

SUMMARY

Associate VLAN with interfaces

Available ( 0 )

No Interfaces available

Selected ( 26 )

GigabitEthernet1/1 ←

GigabitEthernet1/2 ←

GigabitEthernet1/3 ←

GigabitEthernet1/4 ←

Select All

Deselect All

Telnet

☐ DISABLED

SSH

☐ DISABLED

< Account Settings

Day 0 Config Summary >

ACCOUNT SETTINGS BASIC SETTINGS SUMMARY

**Device CIP Settings**

CIP Status **ENABLED**

Same as Management VLAN **ENABLED**

CIP VLAN\* 3660

CIP IP Address 10.223.66.31

Subnet Mask 255.255.255.128

CIP Password

Confirm CIP Password

(If skipped, will set login user password as CIP password)

< Account Settings Day 0 Config Summary >

Table 11 – Basic Settings

Field	Description
<b>Device Management Settings</b>	
IP Address	<p>Click to determine how the IP information is assigned to the switch:            Static—You manually assign IP information. We recommend that you manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the WebUI for the switch.            DHCP—A DHCP server automatically assigns an IP address, subnet mask, default gateway, primary and secondary DNS server to the switch. Unless restarted, the switch continues to use the DHCP-assigned information, and you are able to use the DHCP-assigned address to access the WebUI.            The default mode is Static.  <b>IMPORTANT:</b> For a manually assigned IP address in a network that uses a DHCP server, the IP address cannot be within the range of addresses that the DHCP server assigns. Otherwise, IP address conflicts can occur between the switch and another device.</p>
VLAN ID	<p>Enter an ID for the management VLAN through which the switch is managed. The management VLAN is the broadcast domain through which management traffic is sent between specific users or devices. The management VLAN provides the following:            Broadcast control and security for management traffic that must be limited to a specific group of users, such as the administrators of your network.            Secure administrative access to all devices in the network.            The default management VLAN ID is 1.  <b>IMPORTANT:</b> Be sure that the switch and your network management station are in the same VLAN. Otherwise, you can lose management connectivity to the switch.</p>
IP Address	<p>(Applies only to static IP addresses). Enter the IP address and associated subnet mask to assign to the switch:  <b>IMPORTANT:</b> If you run Express Setup in Medium Press mode, the IP Address field displays the IP address from the DHCP server. If you change the address, the connection drops. To re-establish the connection with the new address, close your web browser and go to the address you specified.            Make sure that the IP address that you assign to the switch is not assigned to another device in your network. The IP address and the default gateway cannot be the same.</p>
Subnet Mask	Enter the subnet mask to assign to the switch. The default is 255.255.255.0.
Default Gateway (optional)	<p>(Applies only to static IP addresses). Enter the IP address for the default gateway that enables the switch to communicate with devices in other networks or subnetworks:            The default gateway IP address must be part of the same subnet as the switch IP address.            The switch IP address and the default gateway IP address cannot be the same.            If all of your devices are in the same network and a default gateway is not used, you do not need to enter an IP address in this field.            If your network management station and the switch are in different networks or subnetworks, you must specify a default gateway. Otherwise, the switch and your network management station cannot communicate with each other.</p>
Associate VLAN with interfaces	To assign switch interfaces to the management VLAN, click an interface in the Available column to move it into the Selected column.
Telnet	<p>To use Telnet to access the switch via the command-line interface (CLI), click to Enable Telnet. Telnet uses the local account user name and password.  <b>IMPORTANT:</b> We recommend that you use SSH instead of Telnet for access to the switch. SSH provides more security for remote connections than Telnet through strong encryption.</p>

Table 11 - Basic Settings (Continued)

Field	Description
SSH	To allow Secure Shell (SSH) sessions on the switch, click to enable SSH. SSH uses the local account user name and password. SSH provides a secure, remote connection to the switch. SSH provides more security for remote connections than Telnet through strong encryption.
Domain Name for SSH	(Appears only if SSH is enabled). Enter the SSH domain name, such as server.company.com.
<b>Device CIP Settings</b>	
CIP Status	To provide application-level connections from the switch to other industrial automation and control systems for management and monitoring, click to enable CIP status.
Same as Management VLAN	To use the switch management VLAN as the CIP VLAN, click to enable this setting.
CIP VLAN	Enter the VLAN on which CIP is enabled. The CIP VLAN can be the same as the management VLAN, or you can isolate CIP traffic on another VLAN.
CIP IP Address	If the CIP VLAN differs from the switch management VLAN, enter the IP address for the CIP VLAN. Make sure that the IP address is not used by another device in your network.
Subnet Mask	If the CIP VLAN differs from the switch management VLAN, enter the subnet mask for the CIP VLAN.
CIP Password	Enter the CIP password, or leave this field blank if you do not want to change the password.
Confirm CIP Password	If you entered a CIP password, reenter the password.

5. On the Summary page, review your configuration settings.
6. To view the CLI commands to execute once you submit the configuration, click CLI Preview.
7. Once you approve of the configuration, click Submit.

The switch initializes its configuration for typical industrial EtherNet/IP™ applications by running the global macro as described on [page 37](#). You can then log on to the WebUI for further configuration or exit the application.

The screenshot shows the 'SUMMARY' page of the WebUI. At the top, there is a progress bar with three steps: ACCOUNT SETTINGS (checked), BASIC SETTINGS (checked), and SUMMARY (active). Below the progress bar, the 'SUMMARY' section is highlighted. A blue button labeled 'CLI Preview' is located in the top right corner. The main content area contains a message: 'This screen provides the summary of all the steps configured as a part of the day zero configuration. Please click Submit to configure the device.' Below this message, there are two expandable sections: 'General Information' and 'Basic Device Configuration'. The 'General Information' section shows: User Name: admin, Host Name: s5800-66-31, NTP Server: Not Configured, Date & Time: 29 Nov 2018 11:03:05. The 'Basic Device Configuration' section shows: VLAN: 3660, IP Address: 10.223.66.31, Subnet Mask: 255.255.255.128, Default Gateway: 10.223.66.1, Telnet: Enabled, SSH: Disabled, CIP VLAN: 3660(10.223.66.31). At the bottom, there are two buttons: '< Basic Settings' and 'Submit >'.

8. Disconnect the cables to the switch.
9. If you ran Express Setup in Short Press mode, refresh the computer IP address:
  - For a dynamically assigned IP address, disconnect the computer from the switch and reconnect the computer to the network. The network DHCP server assigns a new IP address to the computer.
  - For a statically assigned IP address, change it to the previously configured IP address.

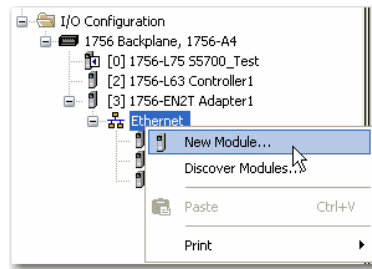
## Complete Express Setup via the Logix Designer Application

To complete the initial setup of the switch via the Logix Designer application, follow these procedures. For details about how to use the Logix Designer application, refer to its online Help.

Before you perform following procedures, you must run Express Setup on the switch in Medium Press mode, and the switch must receive its IP address from a DHCP server.

### Add the Switch to the Controller Project

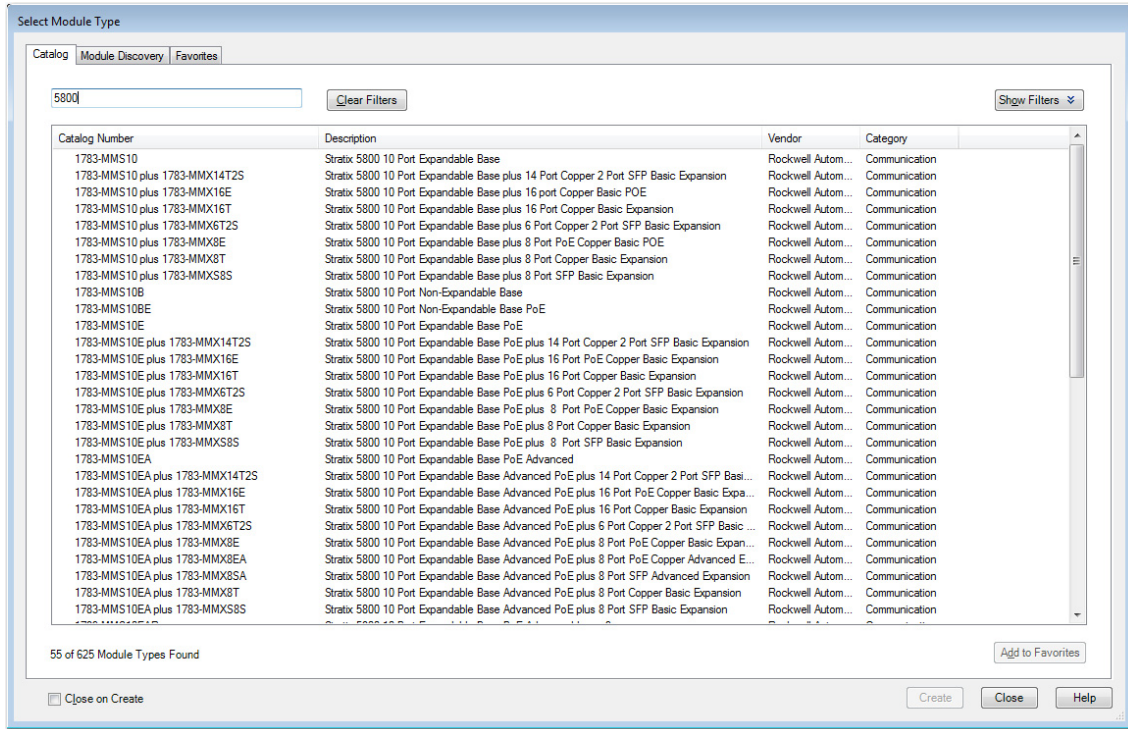
1. Open the project file for the controller to monitor the switch.
2. Right-click Ethernet and choose New Module.



- On the Select Module Type page, select the switch and click Create.

If you do not see the switch in the list of catalog numbers, obtain the AOP from the Rockwell Automation support site:

[https://www.rockwellautomation.com/en\\_NA/support/overview.page?](https://www.rockwellautomation.com/en_NA/support/overview.page?)



- Complete the fields as described in [Table 12](#).

Be sure to specify the IP address that the DHCP server assigned.

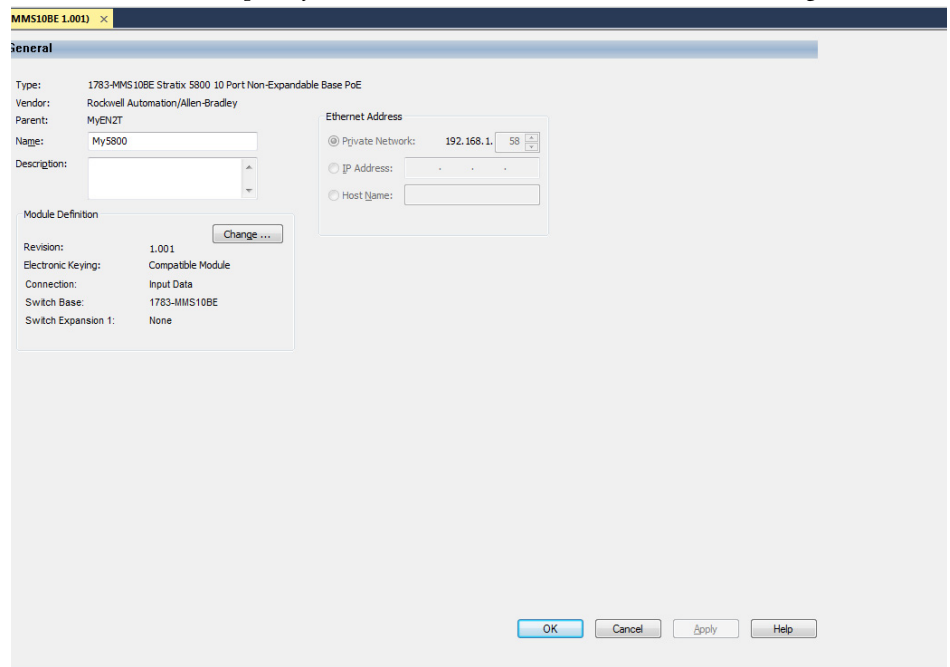




Table 12 - General View

Field	Description
Name	Enter a name to identify the switch.
Description	Enter a description of the switch.
Ethernet Address	Click IP Address, and then enter the IP address that the DHCP server assigned to the switch during Express Setup.

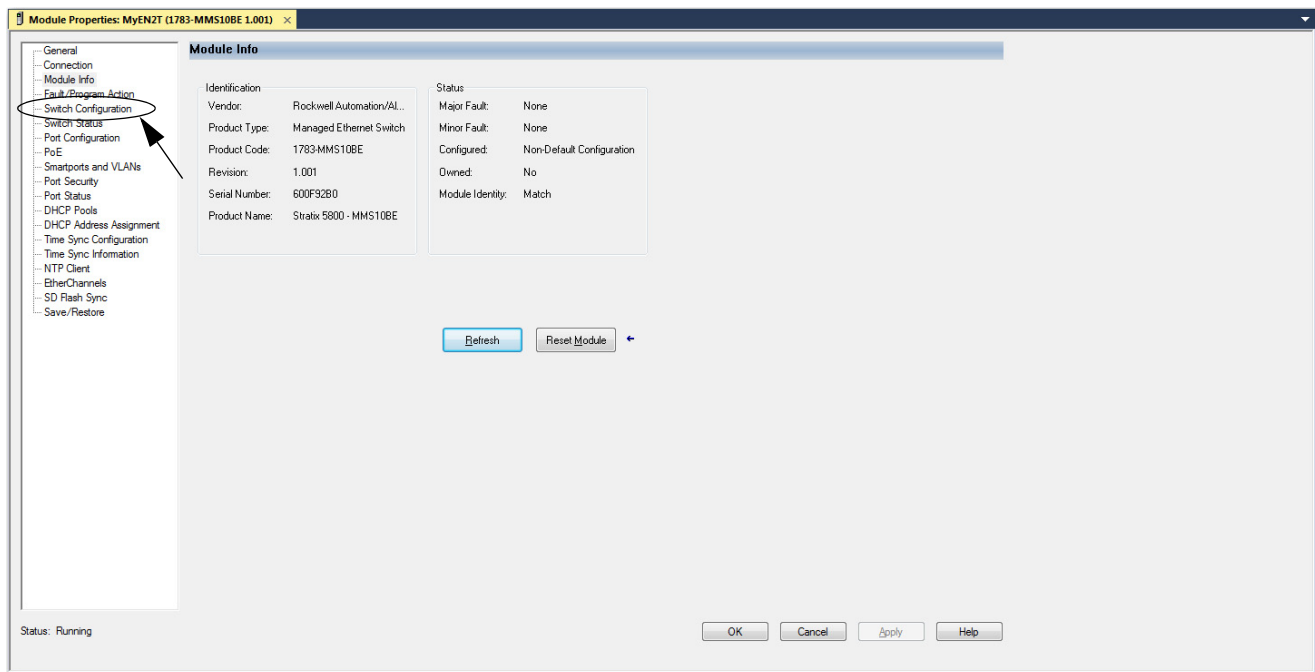
5. In the Module Definition area, click Change.
6. Complete the fields as described in [Table 13](#), and then click OK.

Table 13 - Module Definition

Field	Description
Revision	Choose the major and minor revision of the switch: Major revision: 1...128 Minor revision: 1...255
Electronic Keying	Choose one of the following: Compatible Module (default) Exact Match Disable Keying
Connection	Choose one of the following: Input Data (default): Enables only an input data connection. Data: Enables an input and output data connection. <b>ATTENTION:</b> This selection enables output tags, which can disable ports and interrupt connections to and through the switch. You can disable a switch port by setting the corresponding bit in the output tag. The output bits are applied every time that the switch receives the output data from the controller when the controller is in Run mode. When the controller is in Program mode, the output bits are not applied. When the corresponding output bit is 0, the port is enabled. If you enable or disable a port via the WebUI or the CLI, the output bits from the controller can override the port setting on the next cyclic update of the I/O connection. The output bits always take precedence, regardless of whether the WebUI or the CLI was used to enable or disable the port.
Switch Base	Choose a base module from the pull-down menu.
Switch Expansion 1	Choose an expansion module from the pull-down menu.
Data Connection Password	(Data connections only). Enter the password for the switch.

7. On the General view, click Apply.
8. Go online with the controller, and then open the Module Properties page for the switch.

9. In the navigation pane, click Switch Configuration.



10. On the Express Setup page, complete the fields.

The 'Express Setup' dialog box contains the following sections and fields:

**Express Setup has been initiated.**  
Please provide the following information to complete the initialization of the switch

**Internet Protocol (IP) Settings**

- ☒ Manually Configure IP settings
- ☐ Obtain IP settings automatically using DHCP

**IP Settings Configuration**

Physical Module IP Address:	<input type="text" value="192 . 168 . 1 . 5"/>	Subnet Mask:	<input type="text" value="255 . 255 . 255 . 0"/>
Host Name:	<input type="text"/>	Gateway Address:	<input type="text" value="192 . 168 . 1 . 225"/>
		Network Time Protocol (NTP) Server:	<input type="text" value=". . ."/>

**Create Password**

User:	<input type="text" value="Admin"/>
Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

**Switch Management**

Management Interface VLAN:

Buttons at the bottom right: 'OK', 'Cancel', 'Help'.

Table 14 - Express Setup Fields

Field	Description
Internet Protocol (IP) Settings	Click the method to use for assigning the switch an IP address: Manually Configure IP settings (default)—The switch uses a manually assigned, static IP address. If the switch uses a static IP address and your network uses a DHCP server, make sure that the IP address is not within the range of addresses that the DHCP server assigns. Otherwise, IP address conflicts can occur between the switch and another device. Obtain IP settings automatically using DHCP—A Dynamic Host Configuration Protocol (DHCP) server automatically assigns the switch an IP address, subnet mask, and default gateway. Unless restarted, the switch continues to use the DHCP-assigned information.
Physical Module IP Address	Displays the IP address that the DHCP server assigned to the switch during Express Setup. This value must match the IP address on the General view. If you change the assigned IP address, make sure that the new IP address is not assigned to another device in your network. The IP address and the default gateway cannot be the same. <b>IMPORTANT:</b> If you reconfigure your switch with another IP address, you can lose communication with the switch when you click OK. To correct this problem, you must return to the Express Setup and General view, set the new IP address, and download to the controller.
Subnet Mask	Displays the subnet mask that the DHCP server assigned to the switch during Express Setup.
Host Name	Enter a name to identify the switch. The name can be up to 64 characters and can include alphanumeric and special characters (comma and dash).
Gateway Address	Displays the gateway address that the DHCP server assigned to the switch during Express Setup. A gateway is a router or a dedicated network device that enables the switch to communicate with devices in other networks or subnetworks. The default gateway IP address must be part of the same subnet as the switch IP address. The switch IP address and the default gateway IP address cannot be the same. If all of your devices are in the same network and a default gateway is not used, you do not need to enter an IP address in this field. If your network management station and the switch are in different networks or subnetworks, you must specify a default gateway. Otherwise, the switch and your network management station cannot communicate with each other. <b>IMPORTANT:</b> Communication is disrupted when you change the gateway (IP) address.
Network Time Protocol (NTP) Server	(Optional). Type the IP address of the NTP server. NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
User	Displays the default user name: <b>Admin</b>
Password, Confirm Password	Enter a password for the switch. The default password is <b>switch</b> . To complete initial setup, you must change the password from the default password. This password is also used as the Control Industrial Protocol (CIP) security password. You must provide a password to the switch to secure access to the WebUI.
Management Interface (VLAN)	Choose a management VLAN. The default management VLAN ID is 1. The management VLAN through which the switch is managed. The management VLAN is the broadcast domain through which management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that must be limited to a specific group of users, such as the administrators of your network. It also provides secure administrative access to all devices in the network. <b>IMPORTANT:</b> Be sure that the switch and your network management station are in the same VLAN. Otherwise, you lose management connectivity to the switch.

## Default Global Macro

Once you complete Express Setup, the switch runs a default global macro (ab-global). This macro configures the switch for industrial automation applications that use the EtherNet/IP protocol. This macro sets many parameters, including these major settings:

- Enable IGMP snooping and querier
- Enable CIP, if configured during Express Setup
- Enables alarms, SYSLOG, and SNMP notifications
- Enables Multiple Spanning Tree (MST) protocol, BPDU Guard, BPDU Filter, and loop guard
- Configure Quality of Service (QoS) settings and classify CIP, PTP, and other traffic

If you do not run Express Setup to initialize the switch, the global macro does not run. You can use the CLI to run the global macro. See [Command-line Interface \(CLI\) on page 172](#).

**Notes:**

## WebUI Basics

Topic	Page
Requirements and Restrictions	39
Access the WebUI	40
Use the WebUI Toolbar	44
Set WebUI Preferences	45
Customize the Dashboard	45
Sort, Filter, and Customize Data in Columns	47

The web user interface (WebUI) provides a secure connection to the switch from anywhere in your network through a supported web browser.

### Requirements and Restrictions

To make sure that the WebUI runs properly, disable any popup blockers or proxy settings in your browser. If directly connected to a network, consider disconnecting from any wireless networks on your workstation.

**IMPORTANT** The WebUI automatically logs you out if you are inactive for 20 minutes or longer.

To configure the inactivity timeout value for web sessions, from the Administration menu, choose HTTP/HTTPS/Netconf, and then enter a timeout value in the Session Idle Timeout field.

Be sure that the workstation you use to access the WebUI meets the requirements in [Table 15](#).

**Table 15 - WebUI Requirements**

Component	Minimum Version
<b>Operating System</b>	
Microsoft® Windows	7 or higher
Apple Mac OS	10.9.5 or later
<b>Browser</b>	
Google Chrome	38 or later
Microsoft Edge	11 or later
Mozilla Firefox	25 or later
Apple Safari	7 or later
<b>Screen Resolution</b>	
1280 x 800 or higher	

# Access the WebUI

Because the WebUI provides a secure connection, security messages from your browser can appear when you access the WebUI.

To access the WebUI, follow these steps.

- 11. Start a web browser session and go to the switch IP address.

For information about setting the initial switch IP address, see [Chapter 2, Express Setup](#).

- 12. If security messages from your browser appear, complete the procedures in the following table.

Browser	Procedure
Google Chrome	Click Advanced. Click Proceed to [IP address]. See <a href="#">Figure 10 on page 41</a> .
Microsoft Edge	Click Details. Click Go on the webpage. See <a href="#">Figure 11 on page 42</a> .
Mozilla Firefox	Click Advanced. Click Accept the Risk and Continue. See <a href="#">Figure 12 on page 42</a> .
Apple Safari	Click Show Details. Click visit this website. See <a href="#">Figure 13 on page 43</a> .

- 13. On the Login page, enter the switch Username and Password, and then click Log In.



Figure 10 - Security Messages—Chrome

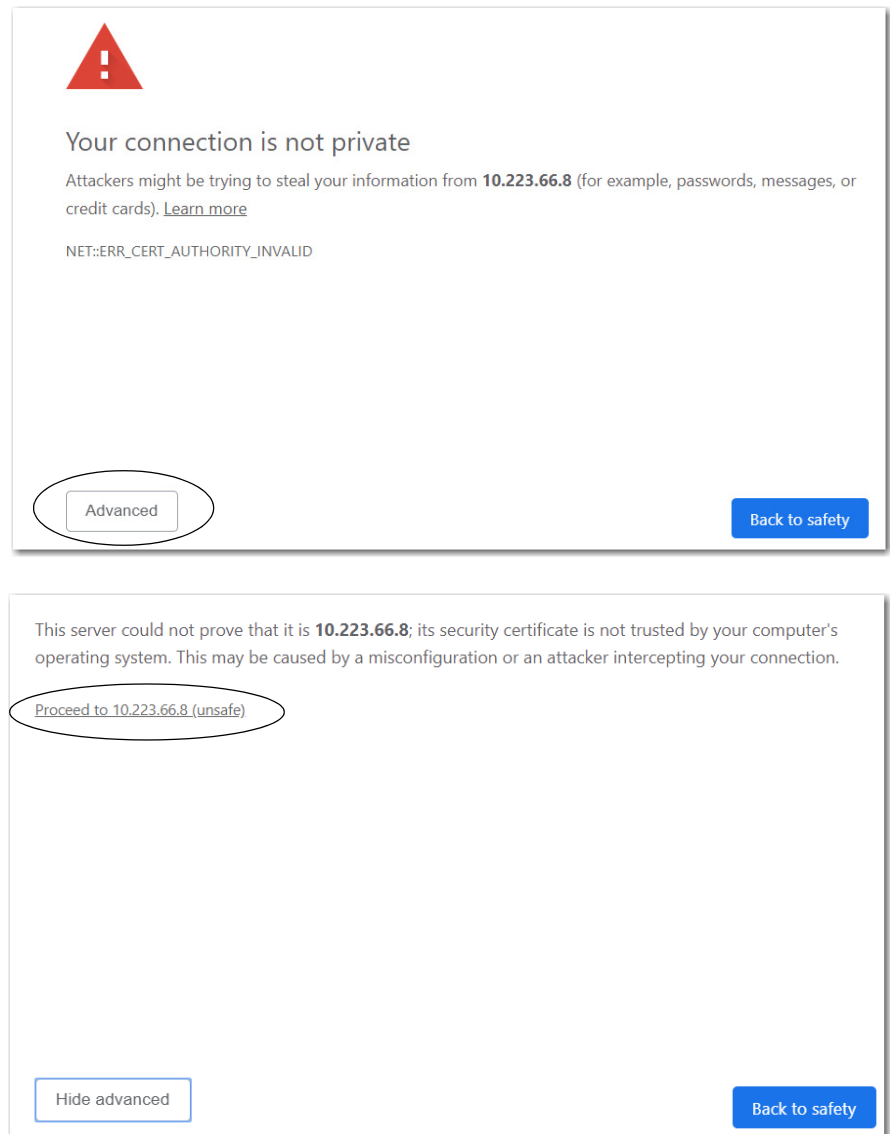




Figure 11 - Security Messages—Edge

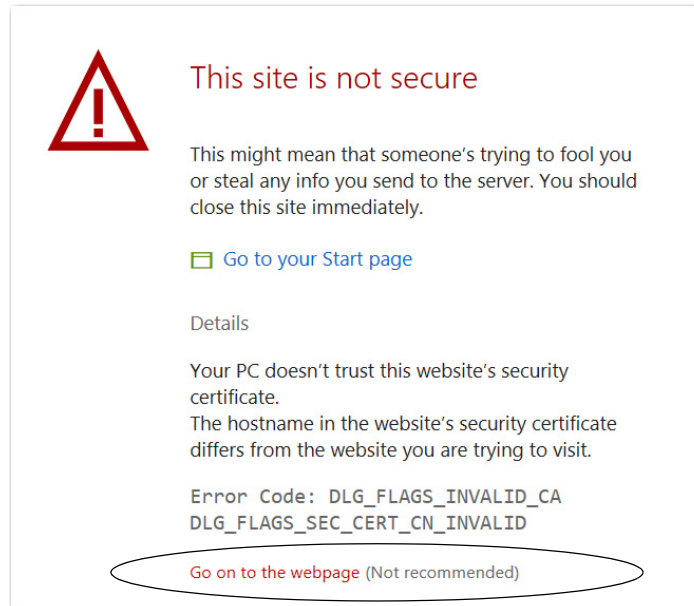
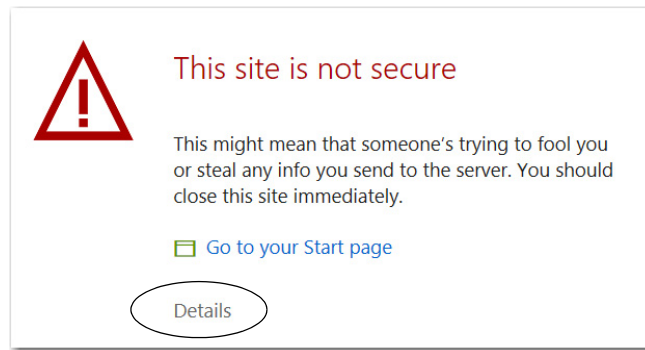


Figure 12 - Security Messages—Firefox

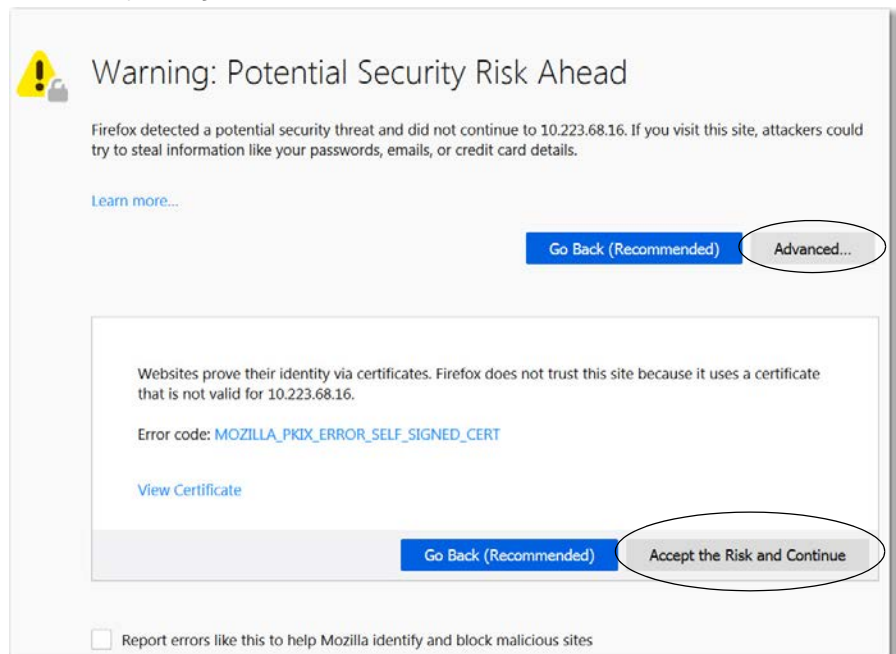
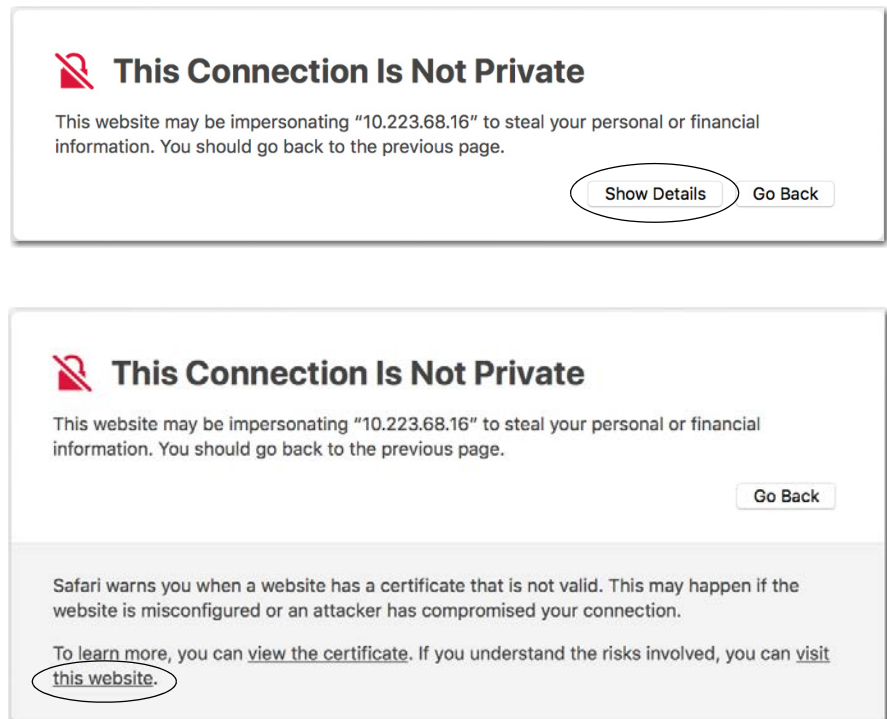


Figure 13 - Security Messages—Safari



# Use the WebUI Toolbar

The WebUI toolbar appears in the upper-right corner of the WebUI. The toolbar functions described in [Table 16](#) enable you to make global changes to the WebUI.

Figure 14 - WebUI Toolbar

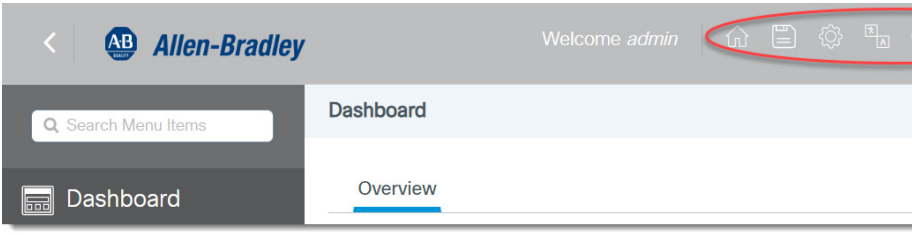









Table 16 - Global Toolbar

Icon	Description
Home	
	Takes you to the home page.
Save Configuration	
	Saves the Running configuration of the switch to the Startup configuration of the switch: Changes saved to the Running configuration are lost after you restart the switch unless you save them to the Startup configuration. Changes made to the switch via the WebUI pages are saved only to the Running configuration. Changes saved to the Startup configuration are stored in the internal memory of the switch and are retained after you restart the switch. <b>IMPORTANT:</b> You must click the Save Configuration button on the toolbar to save the Running configuration to the Startup configuration and retain the changes after a power cycle.
Preferences	
	Allows you to change the default home page, grid size, login tracking, and login tracking interval. See <a href="#">Set WebUI Preferences on page 45</a> .
Language	
	Displays the language options available for the WebUI. The current options are English and Japanese.
Help	
	Launches the Help for the WebUI.
Refresh	
	Refreshes the current WebUI page.
Log Out	
	Exits the WebUI.

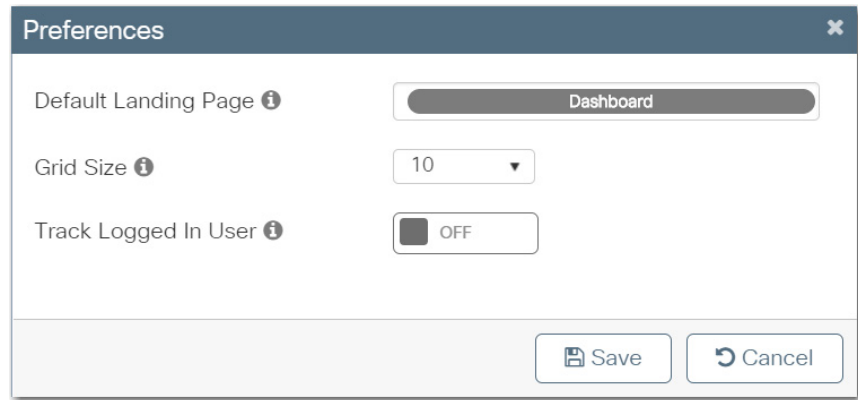
## Set WebUI Preferences

Each user with a WebUI account can set these preferences:

- Default page that appears when the user logs on to the WebUI.
- Default number of grid rows to display per page.
- Login activity for the user account.

In the upper-right corner of the WebUI, click the Preferences icon .

**Figure 15 - WebUI Preferences**



**Table 17 - WebUI Preferences**

Field	Description
Default Landing Page	Begin to type the default landing page to appear after logging in to the WebUI, and then choose the setting from the list that is automatically generated. By default, the switch directs you to the dashboard.
Grid Size	Choose the default number of grid rows to display per page. This setting is the default for all grids in the WebUI. However, you can change the number of rows that display per page while viewing individual grids in real time. Valid values: 10 (default) 20 50 100
Track Logged In User	Click to enable the switch to track the following information for the user account: The time of the last failed login attempt by the user The number of failed login attempts by the user The number of times the user successfully logged into the WebUI If you enable tracking, the switch automatically configures AAA. For more information about AAA, see <a href="#">page 49</a> . If you enable this preference, a message appears prompting you to confirm your choice. To enable tracking and AAA, click Yes.
Tracking Interval (hrs)	If you enabled the preceding tracking preference, enter the number of hours during which to capture login data for the user. Valid values: 1...24

## Customize the Dashboard

The Dashboard page has dashlets that display a snapshot of the overall status and statistics of the switch. [Table 18](#) describes the dashlets.

**Table 18 - Dashlets**

Dashlet	Description
Switch View	This image shows the ports, status indicators, and other features on the front panel of the switch.
CPU & Memory Pressure Graph	Displays CPU usage on the processors on each core, every 5 minutes, every 1 minute, and every 5 seconds. The Memory Utilization section displays a chart of the device memory usage. To view the used space and free space percentage, hover over the chart.

Table 18 - Dashlets

Dashlet	Description
Temperature	Displays the temperature of the device. If the temperature is yellow or red, your device needs attention.
System Information	Displays a snapshot of the specific details of the device.
PoE Power Consumption	Displays Power over Ethernet (PoE) information for the switch, including the total power supported and the device power usage. To view the unused power and used power percentage, hover over the pie chart.

The time stamp that is associated with each dashlet indicates how recent the status information and statistics are.

Figure 16 - Dashlet Time Stamp




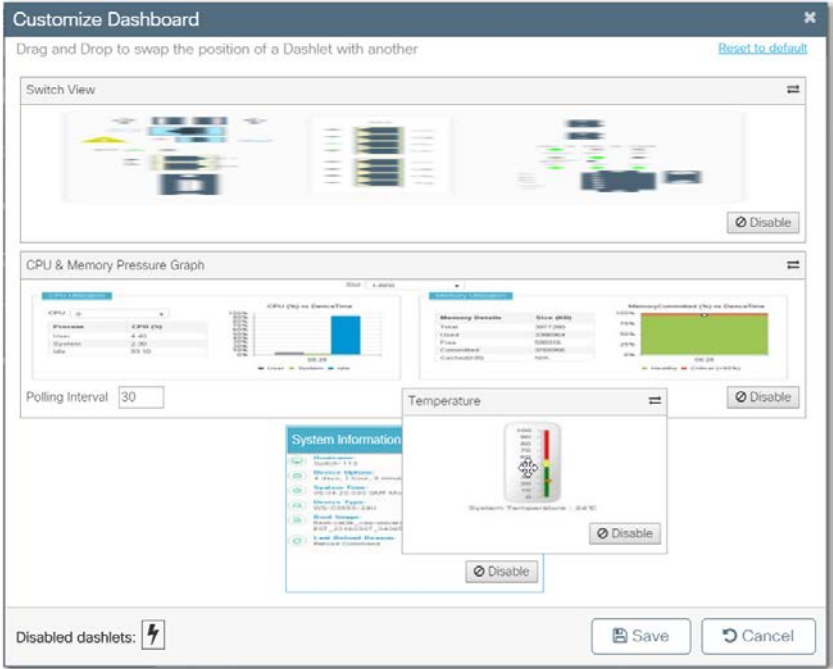
To customize the dashboard, click the Customize Dashboard icon  in the top-right corner of the page. On the Customize Dashboard page, you can set the order of appearance for each dashlet or disable specific dashlets to hide their appearance on the dashboard. Any disabled dashlets are available as icons on the dashboard and can be enabled at any time to be a part of the dashboard.

Figure 17 - Customize Dashboard



# Sort, Filter, and Customize Data in Columns

The WebUI provides options to help view data in columns. For example, the Ethernet Ports page features a table of interfaces on the switch. To display options to view data, click the drop-down arrow in a column header, as shown in [Figure 18](#).

Figure 18 - Column Header Options

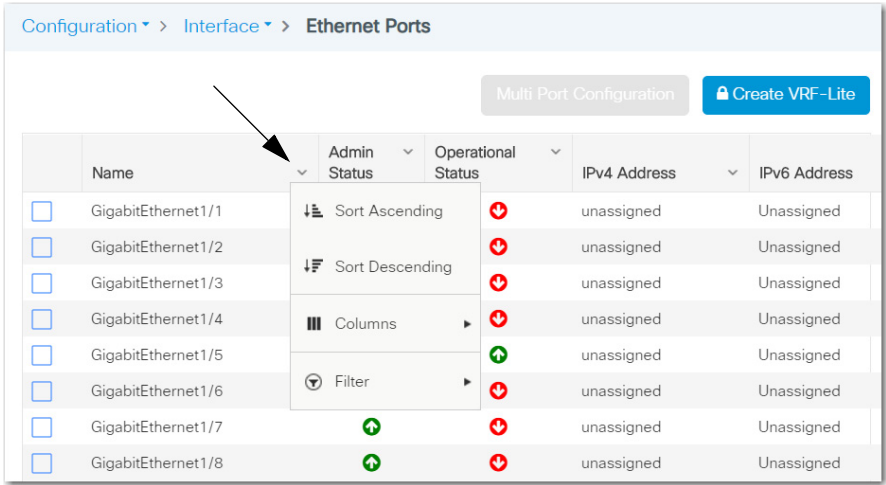


Table 19 - Column Header Options

Option	Description
Sort Ascending 	Click to view column data in ascending order.
Sort Descending 	Click to view column data in descending order.
Columns 	Click to display a list of columns to show or hide on the page. For example, to hide the IPv4 Address column on the Ethernet Ports page, clear the IPv4 Address checkbox. 
Filter 	Click to display filter options for data in the column. For example, to view only ports with a down state in the Operational Status column, choose Is equal to, and then choose down. 

**Notes:**

## Configure the Switch

Topic	Page
Authentication, Authorization, and Accounting (AAA)	49
Access Control Lists (ACLs)	68
Discovery Protocols	70
Enhanced Interior Gateway Routing Protocol (EIGRP)	73
Ethernet Ports	76
Flow-based SPAN (FSPAN)	84
Logical Interfaces	86
Hot Standby Router Protocol (HSRP)	91
Intermediate System-to-Intermediate System (IS-IS)	93
Multicast Services	94
NetFlow	95
Network Address Translation (NAT)	98
Open Shortest Path First (OSPF) Routing Protocol	113
Parallel Redundancy Protocol (PRP)	116
Port Security	121
Quality of Service (QoS)	122
Remote Switch Port Analyzer (RSPAN)	127
Resiliency Ethernet Protocol (REP)	128
Routing Information Protocol (RIP)	133
Smartports	135
Spanning Tree Protocol (STP)	139
Switched Port Analyzer (SPAN)	141
TrustSec	143
Virtual Local Area Networks (VLANs)	151
Virtual Router Redundancy Protocol (VRRP)	157
VLAN Trunking Protocol (VTP)	157

### Authentication, Authorization, and Accounting (AAA)

AAA Network Security Services provide the primary framework for intelligently controlling access to resources, policy enforcement, and usage audits. For more information about AAA, see the Ethernet Reference Manual, publication [ENET-RM002](#).

Terminal Access Controller Access-Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), and Lightweight Directory Access Protocol (LDAP) are security protocols that control access to networks. You can configure the switch as a TACACS+, RADIUS, or LDAP client to authenticate and authorize users.



## AAA Configuration

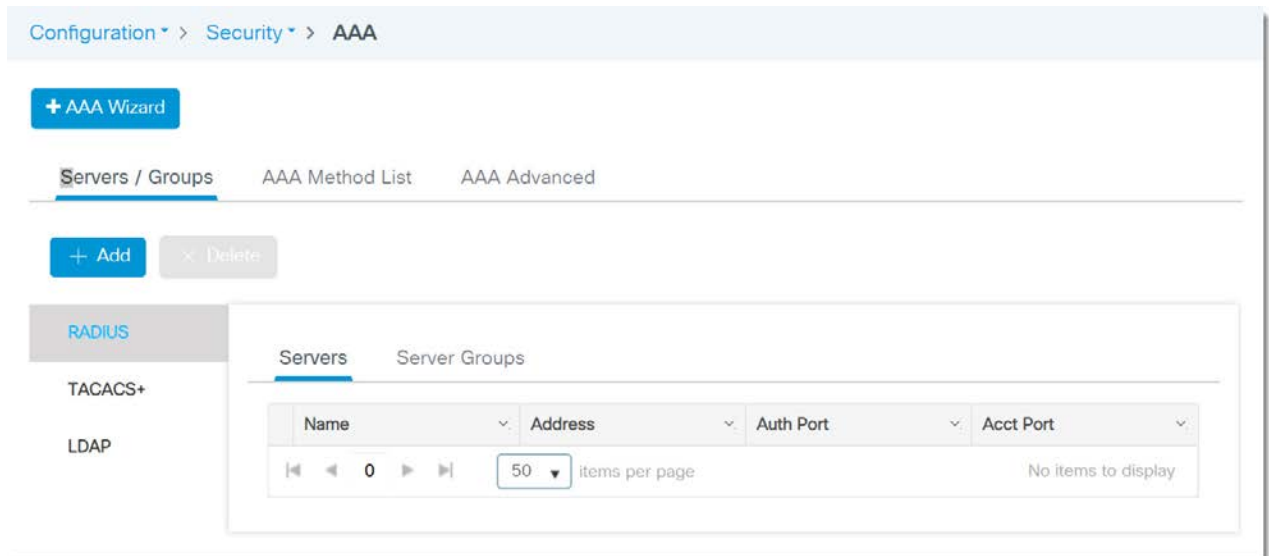
You can configure the AAA components in [Table 22](#) by using the WebUI for the switch. The WebUI also provides a configuration wizard for these components. To use the wizard, see [page 50](#).

**Table 22 - AAA Configuration Components**

Component	Page
Authentication Configuration	55
Authorization Configuration	56
Accounting Configuration	57
RADIUS Server Configuration	58
RADIUS Server Group Configuration	59
TACACS+ Server Configuration	60
TACACS+ Server Group Configuration	61
LDAP Server Configuration	62
LDAP Server Group Configuration	63
RADIUS Fallback Configuration	65
Policy Password Configuration	66

## Configure AAA via the WebUI Wizard

From the Configuration menu, click AAA.



To use the AAA wizard, follow these steps.

1. Click AAA Wizard.
2. In the upper-right corner, click Basic or Advanced:
  - Basic—The wizard displays only basic configuration fields.
  - Advanced—The wizard displays both basic and advanced configuration fields.
3. Configure security servers as described in [Table 23](#), and then click Next.

**Add Wizard**

Basic    **Advanced**

SERVER    SERVER GROUP ASSOCIATION    MAP AAA

RADIUS ☒    TACACS+ ☒    LDAP ☒

**RADIUS**    TACACS+    LDAP

Name\*

IPv4 / IPv6 Server Address\*

PAC Key ☐

Key Type

Key\*

Confirm Key\*

Auth Port

Acct Port

Server Timeout (seconds)

Retry Count

Support for CoA **ENABLED** ☒

**Table 23 - Server Configuration**

Field	Description
RADIUS	To display the RADIUS tab in the configuration wizard, check RADIUS.
TACACS+	To display the TACACS+ tab in the configuration wizard, check TACACS+.
LDAP	To display the LDAP tab in the configuration wizard, check LDAP.
<b>RADIUS Tab</b>	
Name	Enter a name to identify the RADIUS server.
IPv4/IPv6 Server Address	Enter the IP address for the RADIUS server.
PAC Key	Check PAC Key to enter a Protected Access Credential (PAC).
PAC Key Type	(Appears only if you check PAC Key). Choose a PAC key type.
PAC Key	(Appears only if you check PAC Key). Enter the PAC to use to authentication between the server and your device.
Confirm PAC Key	(Appears only if you check PAC Key). Reenter the PAC key to confirm it.
Key Type	Choose a key type: 0—Requires you to enter an unencrypted key. LINE—Requires you to enter an unencrypted (cleartext) shared key. Default value: 0
Key	(Appears only if you clear the PAC Key checkbox). Enter the shared secret key to use for authentication between the server and your device.
Confirm Key	(Appears only if you clear the PAC Key checkbox). Reenter the key to confirm the value.
Auth Port	(Advanced configuration). Enter the UDP port number of the RADIUS server for authentication. Valid values: 1...65535 Default value: 1812
Acct Port	(Advanced configuration). Enter the UDP port number of the RADIUS server for accounting. Valid values: 1...65535 Default value: 1813
Server Timeout (seconds)	(Advanced configuration). Enter the number of seconds between retransmissions. Valid values: 1...1000 seconds
Retry Count	(Advanced configuration). Enter the number of times the device can retry transmission. Valid values: 1...100 seconds
Support for CoA	(Advanced configuration). Click to enable or disable support change-of-authorization (CoA) messages. CoA messages modify session authorization attributes such as data filters. Default value: Enabled
<b>TACACS+ Tab</b>	
Name	Enter a name to identify the TACACS+ server.
IPv4/IPv6 Server Address	Enter the IP address of the TACACS+ server.
Key	Enter the shared secret key to be used for authentication between the server and your device.
Confirm Key	Reenter the key to confirm the value.

**Table 23 - Server Configuration (Continued)**

Field	Description
Port	(Advanced configuration). Enter the UDP port number of the TACACS server. Valid values: 1...65535 Default value: 9
Server Timeout (seconds)	(Advanced configuration). Enter the number of seconds between retransmissions. Valid values: 1...1000
<b>LDAP Tab</b>	
Server Name	Enter a name to identify the LDAP server.
IPv4/IPv6Server Address	Enter the IP address of the LDAP server.
Port Number	Enter the UDP port number of the LDAP server. Valid values: 1...65535 Default value: 389
Simple Bind	Choose the local authentication bind method for the LDAP server: Anonymous—Allows anonymous access to the LDAP server. Authenticated—Requires a user name and password to secure access. Default value: Anonymous
Bind User name	(Appears only if you choose Authenticated in the Simple Bind field). Enter a user name for local authentication to the LDAP server. The user name can contain a maximum of 80 characters. If the user name starts with "cn=", the controller does not append the user base distinguished name (DN). This designation allows the authenticated bind user to be outside the user base DN.
Bind Password	(Appears only if you choose Authenticated in the Simple Bind field). Enter a username to be used for local authentication to the LDAP server. The user name can contain a maximum of 80 characters.
Confirm Bind Password	(Appears only if you choose Authenticated in the Simple Bind field). Reenter the bind password to confirm the value.
User Base DN	Enter the distinguished name (DN) of the subtree in the LDAP server that contains a list of all users. <b>EXAMPLE:</b> ou=organizational unit, .ou=next organizational unit, and o=corporation.com. If the tree of users is the base DN, enter the following: . o=corporation.com, or dc=corporation, dc=com.
User Attribute	(Advanced configuration). Enter the name of the attribute in the user record that contains the user name. You can obtain this attribute from your directory server.
User Object Type	(Advanced configuration). Enter the value of the LDAP objectType attribute that identifies the record as a user. Often, user records have several values for the objectType attribute, some of which are unique to the user and some of which are shared with other object types.
Server Timeout (seconds)	(Advanced configuration). Enter the number of seconds between retransmissions. Valid values: 1...1000 seconds
Secure Mode	(Advanced configuration). Check Secure Mode to configure a CA Trustpoint.
Trustpoint Name	(Advanced configuration). If you checked Secure mode, choose a Trustpoint name.

4. Configure server group associations as described in [Table 24](#), and then click Next.

**Add Wizard**

Basic    **Advanced**

SERVER    **SERVER GROUP ASSOCIATION**    MAP AAA

**RADIUS**    TACACS+    LDAP

Name\*

Group Type **RADIUS**

MAC-Delimiter **none**

MAC-Filtering **none**

Dead-Time (mins) **1-1440**

Available Servers    Assigned Servers

Radius1

**Table 24 - Server Group Association**

Field	Description
<b>RADIUS Tab</b>	
Name	Enter a name to identify the RADIUS server group.
Group Type	(System-generated). Displays RADIUS.
MAC-Delimiter	Choose the delimiter to use in the MAC addresses that are sent to the RADIUS server: <ul style="list-style-type: none"> <li>• none</li> <li>• colon</li> <li>• hyphen</li> <li>• single-hyphen</li> </ul>
MAC-Filtering	Choose a value to use to filter MAC addresses: <ul style="list-style-type: none"> <li>none</li> <li>MAC</li> <li>Key</li> </ul>
Dead-Time (mins)	Enter the amount of time, in minutes, after which a server is assumed to be dead. After this time, AAA traffic for the server group is redirected to alternative groups of servers that have different operational characteristics. Valid values: 1...1440
Available Server Assigned Servers	In the Available Servers list, select the servers to include in the server group, and click to move them to the Assigned Servers list.
<b>TACACS+ Tab</b>	
Name	Enter a name to identify the TACACS+ server group.
Group Type	(System-generated). Displays TACACS.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the servers to include in the server group, and click to move them to the Assigned Server Groups list.
<b>LDAP Tab</b>	
Name	Enter a name to identify the LDAP server group.
Group Type	(System-generated). Displays LDAP.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the servers to include in the server group, and click to move them to the Assigned Servers Groups list.

5. Map the AAA as described in [Table 25](#), and then click Save & Apply to Device.

**Add Wizard**

Basic ☐ Advanced ☒

SERVER ☒ SERVER GROUP ASSOCIATION ☒ MAP AAA ☐

Authentication ☒ Authorization ☒ Accounting ☒

**Authentication**    Authorization    Accounting

Method List Name\*

Type\*

Group Type

Fallback to local ☐

Available Server Groups: radius, ldap, tacacs+, TEST

Assigned Server Groups:

← Previous    Apply to Device

Table 25 - Map AAA

Field	Description
<b>Authentication Tab</b>	
Method List Name	Enter a name to identify the method list.
Type	Choose the type of authentication to perform before you allow access to the network: dot1x login
Group Type	Choose the type of server to authenticate access to the network: group local
Fallback to local	(Appears only if you choose group in the Group Type field). Check Fallback to local to configure a local server to act as a fallback method when servers in the group are unavailable.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the server groups to use to authenticate access to your network, and click to move them to the Assigned Server Groups list.
<b>Authorization Tab</b>	
Method List Name	Enter a name to identify the method list.
Type	Choose the type of authorization to perform before you allow access to the network: <ul style="list-style-type: none"> <li>network—Enables authorization for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP.</li> <li>exec—Enables authorization to determine if a user is allowed to run an EXEC shell.</li> <li>credential-download—Enables authorization that is based on credentials.</li> </ul>
Group Type	Choose the type of server to authorize access to the network: <ul style="list-style-type: none"> <li>group—Assigns a group of servers as your access server.</li> <li>local—Uses a local server to authenticate access.</li> </ul>
Fallback to local	(Appears only if you choose group in the Group Type field). Check Fallback to local to configure a local server to act as a fallback method when servers in the group are unavailable.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the server groups to use to authorize access to your network, and click to move them to the Assigned Server Groups list.
<b>Accounting Tab</b>	
Method List Name	Enter a name to identify the method list.
Type	Choose the type of accounting to perform before you allow access to the network: <ul style="list-style-type: none"> <li>exec—Provides accounting records for user EXEC terminal sessions on the network access server, including user name, date, start and stop times.</li> <li>identity</li> <li>network—Enables authorization for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP.</li> <li>commands—Provides accounting information about specific, individual EXEC commands associated with a specific privilege level.</li> </ul>
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the server groups to use to track access to your network, and click to move them to the Assigned Server Groups list.

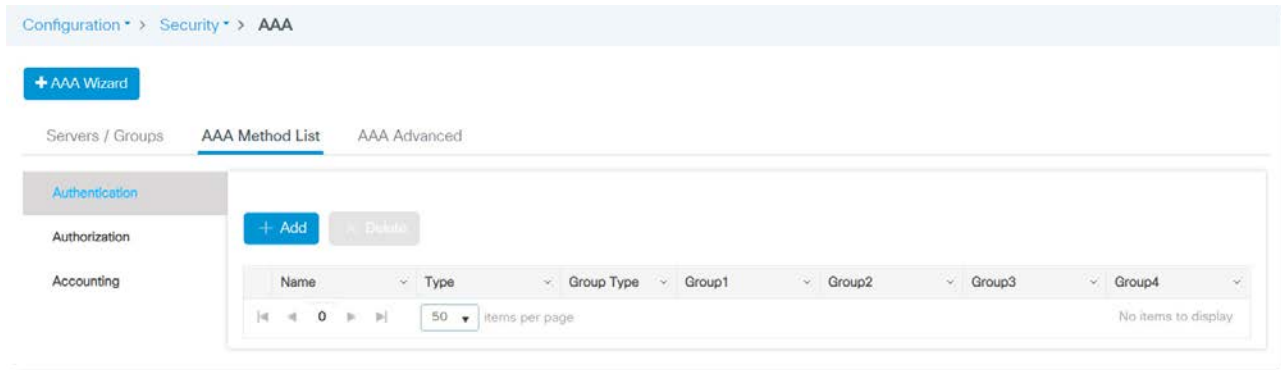
## Configure AAA Method Lists via the WebUI

You can configure an AAA method list outside of the AAA wizard. To use the wizard, see [page 50](#).

From the Configuration menu, click AAA.

### Authentication Configuration

On the AAA Method List tab, click Authentication, and then click Add.



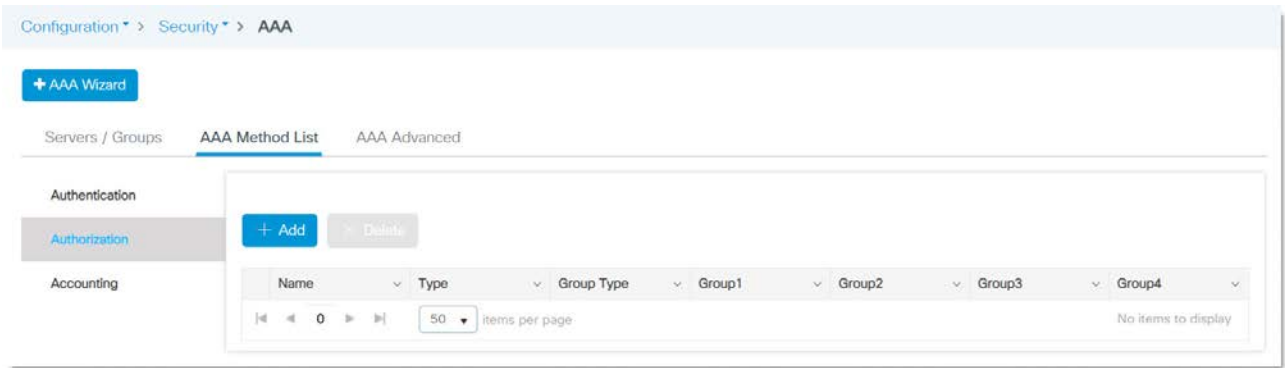
On the Quick Setup: AAA Authentication page, complete the fields as described in [Table 26](#), and then click Apply to Device.

**Table 26 - Quick Setup: AAA Authentication**

Field	Description
Method List Name	Enter a name to identify the method list.
Type	Choose the type of authentication to perform before you allow access to the network: <ul style="list-style-type: none"> <li>• dot1x</li> <li>• login</li> </ul>
Group Type	Choose the type of server to authenticate access to the network: <ul style="list-style-type: none"> <li>• group—Assigns a group of servers as your access server.</li> <li>• local—Uses a local server to authenticate access.</li> </ul>
Fallback to local	Check Fallback to local to configure a local server to act as a fallback method when servers in the group are unavailable.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the server groups to use to authenticate access to your network, and click to move them to the Assigned Server Groups list.

Authorization Configuration

On the AAA Method List tab, click Authorization, and then click Add.



On the Quick Setup: AAA Authorization page, complete the fields as described in [Table 27](#), and then click Apply to Device.

Quick Setup: AAA Authorization

Method List Name\*

default

Type\*

Select a value

Group Type

group

Fallback to local

☐

Authenticated

☐

Available Server Groups

radius  
ldap  
tacacs+

Assigned Server Groups

Cancel

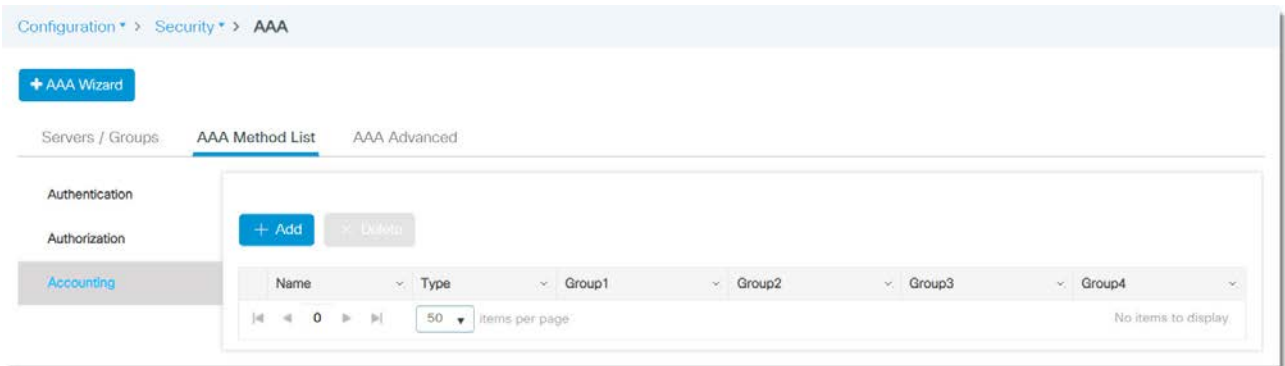
Apply to Device

Table 27 - Quick Setup: AAA Authorization

Field	Description
Method List Name	Enter a name to identify the method list.
Type	Choose the type of authorization to perform before you allow access to the network: <ul style="list-style-type: none"><li>network—Enables authorization for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP.</li><li>exec—Enables authorization to determine if a user is allowed to run an EXEC shell.</li><li>credential-download—Enables authorization based on credentials.</li></ul>
Group Type	Choose the type of server to authorize access to the network: <ul style="list-style-type: none"><li>group—Assigns a group of servers as your access server.</li><li>local—Uses a local server to authenticate access.</li></ul>
Fallback to local	Check Fallback to local to configure a local server to act as a fallback method when servers in the group are unavailable.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the server groups to use to authorize access to your network, and click to move them to the Assigned Server Groups list.

## Accounting Configuration

On the AAA Method List tab, click Accounting, and then click Add.



On the Quick Setup: AAA Accounting page, complete the fields as described in [Table 28](#), and then click Apply to Device.

**Table 28 - Quick Setup: AAA Accounting**

Field	Description
Method List Name	Enter a name to identify the method list.
Type	Choose the type of accounting to perform before you allow access to the network: <ul style="list-style-type: none"> <li>• exec—Provides accounting records for user EXEC terminal sessions on the network access server, including user name, date, start and stop times.</li> <li>• identity</li> <li>• network—Enables authorization for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP.</li> <li>• commands—Provides accounting information about specific, individual EXEC commands associated with a specific privilege level.</li> </ul>
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the server groups to use to track access to your network, and click to move them to the Assigned Server Groups list.



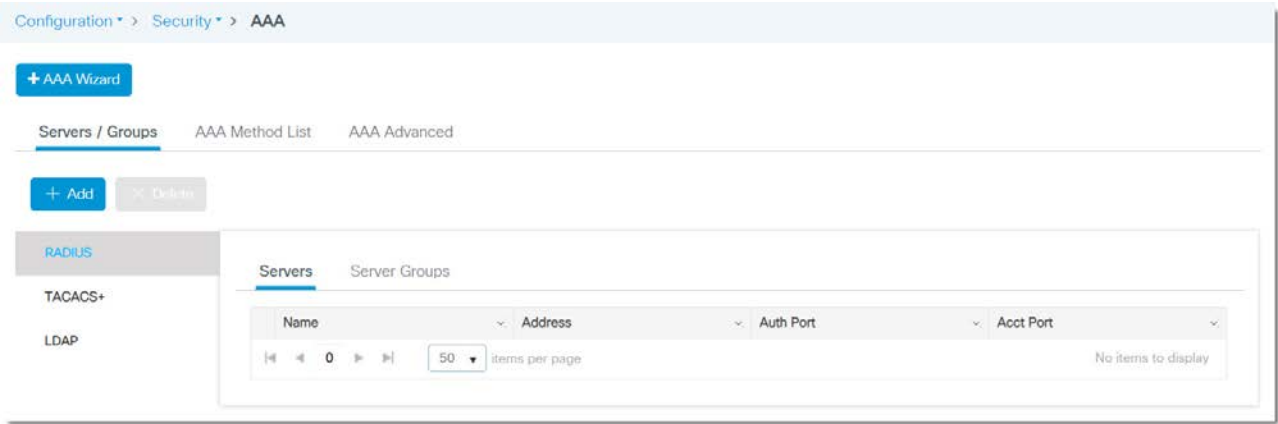
## Configure AAA Servers and Server Groups via the WebUI

You can configure AAA servers and server groups outside of the AAA wizard. To use the wizard, see [page 50](#).

From the Configuration menu, click AAA.

### RADIUS Server Configuration

On the Servers/Groups tab, click RADIUS, Servers, and then click Add.



On the Quick Setup: AAA Radius Server page, complete the fields as described in [Table 29](#), and then click Apply to Device.

Create AAA Radius Server

Name\*

IPv4 / IPv6 Server Address\*

XXXX / XXXX:X

PAC Key

☐

Key Type

0

Key\*

Confirm Key\*

Auth Port

1812

Acct Port

1813

Server Timeout (seconds)

1-1000

Retry Count

0-100

Support for CoA

ENABLED

Cancel

Apply to Device

Table 29 - Create AAA Radius Server

Field	Description
Name	Enter a name to identify the RADIUS server.
IPv4 / IPv6 Server Address	Enter the IP address for the RADIUS server.
PAC Key	Check PAC Key to enter a Protected Access Credential (PAC).
PAC Key Type	(Appears only if you check PAC Key). Choose a PAC key type.
PAC Key	(Appears only if you check PAC Key). Enter the PAC to use to authentication between the server and your device.
Confirm PAC Key	(Appears only if you check PAC Key). Reenter the PAC key to confirm it.

**Table 29 - Create AAA Radius Server (Continued)**

Field	Description
Key	(Appears only if you clear PAC Key). Enter the shared secret key to use for authentication between the server and your device.
Confirm Key	(Appears only if you clear PAC Key). Reenter the key to confirm the value.
Auth Port	Enter the UDP port number of the RADIUS server for authentication. Valid values: 1...65535 Default value: 1812
Acct Port	Enter the UDP port number of the RADIUS server for accounting. Valid values: 1...65535 Default value: 1813
Server Timeout (seconds)	Enter the number of seconds between retransmissions. Valid values: 1...1000 seconds
Retry Count	Enter the number of times the device can retry transmission. Valid values: 1...100 seconds
Support for CoA	Click to enable or disable support change-of-authorization (CoA) messages. CoA messages modify session authorization attributes such as data filters. Default value: Enabled

### RADIUS Server Group Configuration

On the Servers/Groups tab, click RADIUS, Server Groups, and then click Add.

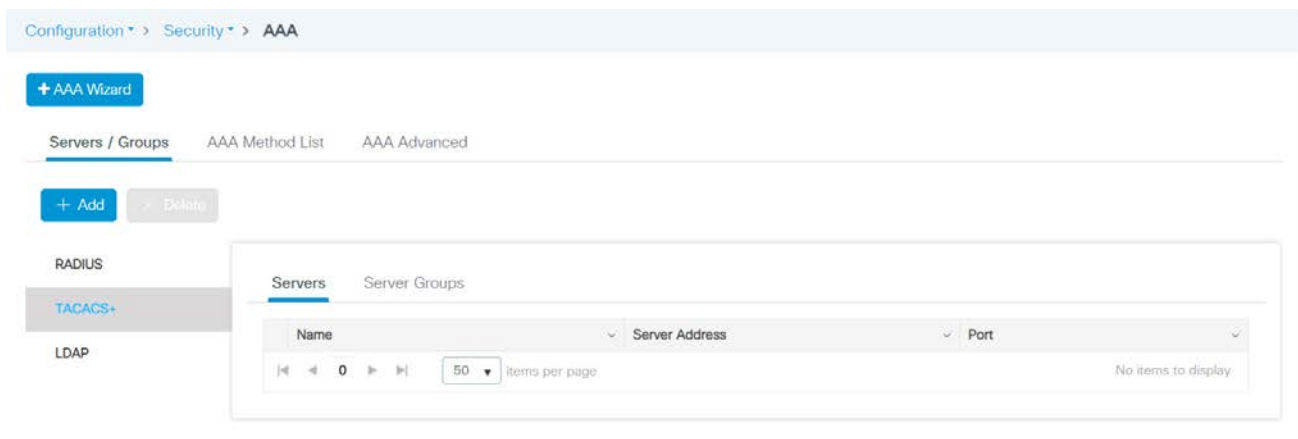
On the Quick Setup: AAA Radius Server page, complete the fields as described in [Table 30](#), and then click Apply to Device.

**Table 30 - Create AAA Radius Server Group**

Field	Description
Name	Enter a name to identify the RADIUS server group.
Group Type	(System-generated). Displays RADIUS.
MAC-Delimiter	Choose the delimiter to use in the MAC addresses that are sent to the RADIUS server: <ul style="list-style-type: none"> <li>• none</li> <li>• colon</li> <li>• hyphen</li> <li>• single-hyphen</li> </ul>
MAC-Filtering	Choose a value to use to filter MAC addresses: <ul style="list-style-type: none"> <li>• none</li> <li>• MAC</li> <li>• Key</li> </ul>
Dead-Time (mins)	Enter the amount of time, in minutes, after which a server is assumed to be dead. After this time, AAA traffic for the server group is redirected to alternative groups of servers that have different operational characteristics. Valid values: 1...1440
Available Servers Assigned Servers	In the Available Servers list, select the servers to include in the server group, and click to move them to the Assigned Servers list.

### TACACS+ Server Configuration

On the Servers/Groups tab, click TACACS+, Servers, and then click Add.



On the Create AAA TACACS Server page, complete the fields as described in [Table 31](#), and then click Apply to Device.

Create AAA Tacacs Server

Name\*

IPv4 / IPv6 Server Address\*

X.X.X.X / X:X:X:X::X

Key\*

Confirm Key\*

Port

49

Server Timeout (seconds)

1-1000

Cancel

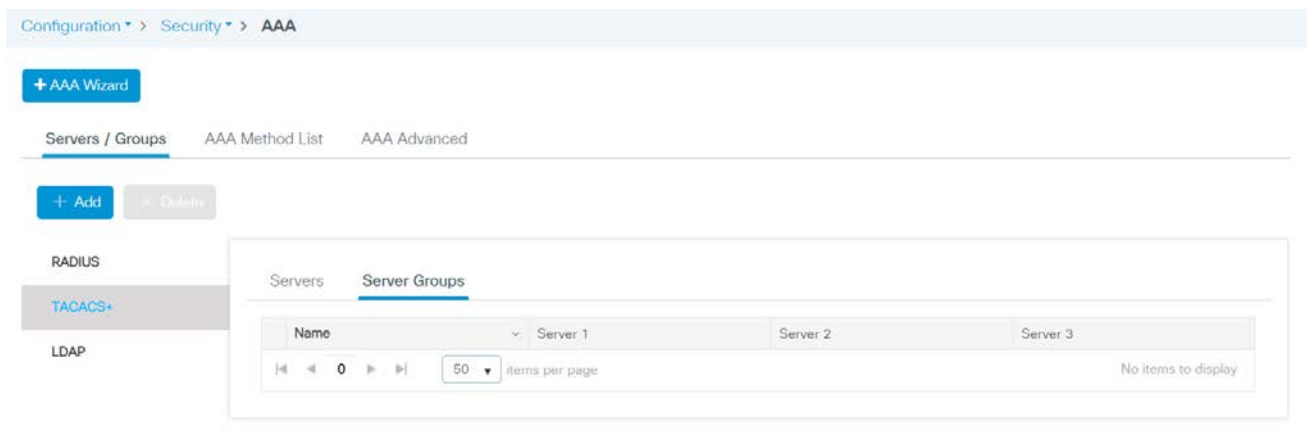
Apply to Device

**Table 31 - Create AAA TACACS Server**

Field	Description
Name	Enter a name to identify the TACACS+ server.
IPv4 / IPv6 Server Address	Enter the IP address of the TACACS+ server.
Key	Enter the shared secret key to be used for authentication between the server and your device.
Confirm Key	Reenter the key to confirm the value.
Port	Enter the UDP port number of the TACACS server. Valid values: 1...65535 Default value: 49
Server Timeout (seconds)	Enter the number of seconds between retransmissions. Valid values: 1...1000

### TACACS+ Server Group Configuration

On the Servers/Groups tab, click TACACS+, Server Groups, and then click Add.



On the Create AAA TACACS Server Group page, complete the fields as described in [Table 32](#), and then click Apply to Device.

Create AAA Tacacs Server Group

Name\*

Group Type

TACACS

Available Servers

Assigned Servers

Cancel

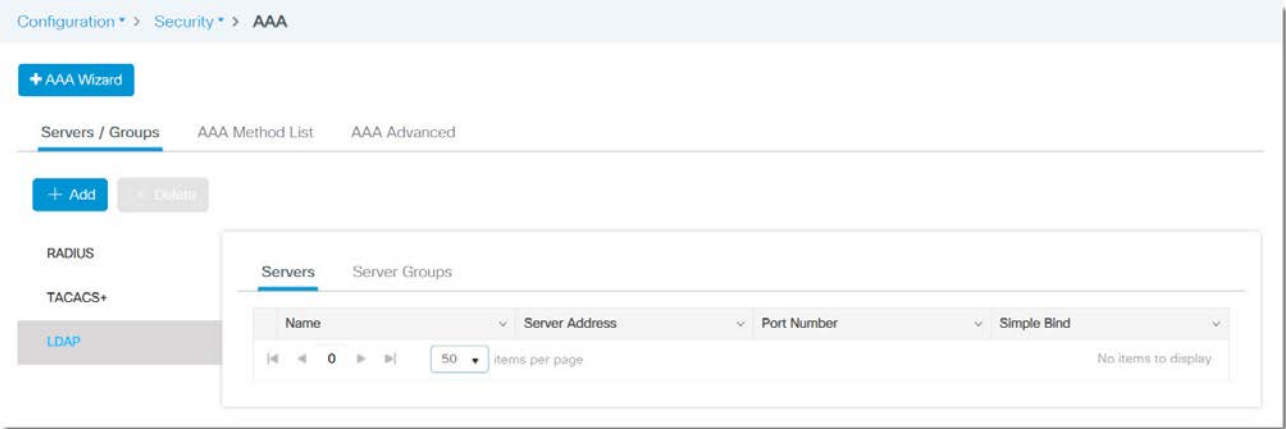
Apply to Device

**Table 32 - Create AAA TACACS Server Group**

Field	Description
Name	Enter a name to identify the TACACS+ server group.
Group Type	(System-generated). Displays TACACS.
Available Server Groups Assigned Server Groups	In the Available Server Groups list, select the servers to include in the server group, and click to move them to the Assigned Server Groups list.

LDAP Server Configuration

On the Servers/Groups tab, click LDAP, Servers, and then click Add.



On the Create AAA LDAP Server page, complete the fields as described in [Table 33](#), and then click Apply to Device.

Create AAA LDAP Server

Server Name\*

IPv4 / IPv6 Server Address\*

X.X.X.X / X:X:X:X::X

Port Number\*

389

Simple Bind

Anonymous

User Base DN\*

User Attribute

None

User Object Type

User Object Type

Remove

Server Timeout (seconds)

30

Secure Mode

Trustpoint Name

None

Cancel

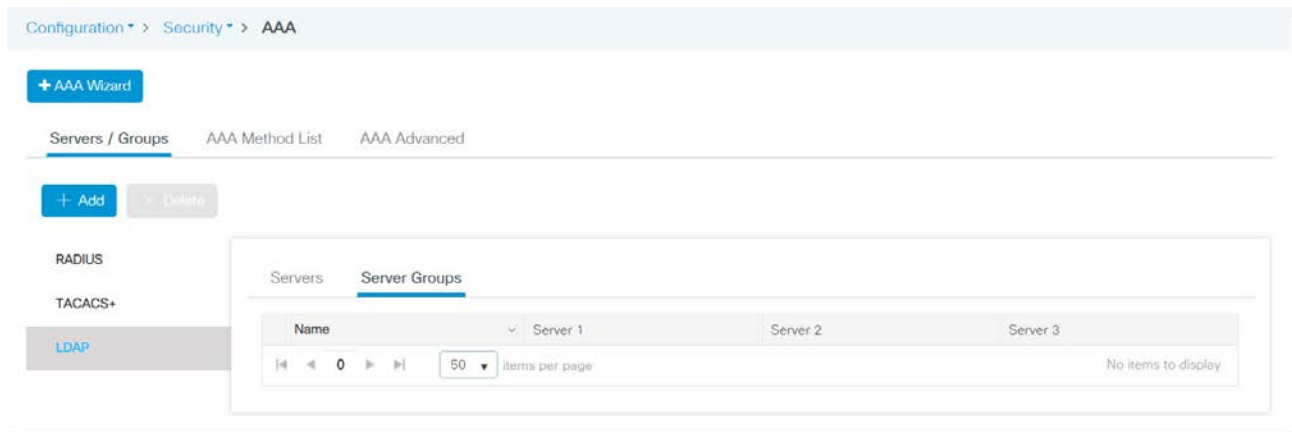
Apply to Device

Table 33 - Create AAA LDAP Server

Field	Description
Server Name	Enter a name to identify the LDAP server.
IPv4/IPv6Server Address	Enter the IP address of the LDAP server.
Port Number	Enter the UDP port number of the LDAP server. Valid values: 1...65535 Default value: 389
Simple Bind	Choose the local authentication bind method for the LDAP server: <ul style="list-style-type: none"> <li>Anonymous—Allows anonymous access to the LDAP server.</li> <li>Authenticated—Requires that a user name and password be entered to secure access.</li> </ul> Default value: Anonymous
Bind User name	(Appears only if you choose Authenticated in the Simple Bind field). Enter a user name to be used for local authentication to the LDAP server. The user name can contain a maximum of 80 characters. If the user name starts with "cn=" (in lowercase letters), the controller assumes that the user name includes the entire LDAP database path and does not append the user base DN. This designation allows the authenticated bind user to be outside the user base DN.
Bind Password	(Appears only if you choose Authenticated in the Simple Bind field). Enter a username to be used for local authentication to the LDAP server. The user name can contain a maximum of 80 characters.
Confirm Bind Password	(Appears only if you choose Authenticated in the Simple Bind field). Reenter the bind password to confirm the value.
User Base DN	Enter the distinguished name (DN) of the subtree in the LDAP server that contains a list of all the users. <b>EXAMPLE:</b> ou=organizational unit, .ou=next organizational unit, and o=corporation.com. If the tree containing users is the base DN, enter the following: . o=corporation.com, or dc=corporation, dc=com.
User Attribute	Enter the name of the attribute in the user record that contains the user name. You can obtain this attribute from your directory server.
User Object Type	Enter the value of the LDAP objectType attribute that identifies the record as a user. Often, user records have several values for the objectType attribute, some of which are unique to the user and some of which are shared with other object types.
Server Timeout (seconds)	Enter the number of seconds between retransmissions. Valid values: 1...1000 seconds
Secure Mode	Check Secure Mode to configure a CA Trustpoint.
Trustpoint Name	If you checked Secure mode, choose a Trustpoint name.

### LDAP Server Group Configuration

On the Servers/Groups tab, click LDAP, Server Groups, and then click Add.



On the Create AAA LDAP Server page, complete the fields as described in [Table 33](#), and then click Apply to Device.

Create AAA Ldap Server Group

Name\*

Group Type

LDAP

Available Server Groups

Assigned Server Groups

Cancel

Save & Apply to Device

Table 34 - Create AAA LDAP Server Group

Field	Description
Name	Enter a name to identify the LDAP server group.
Group Type	(System-generated). Displays LDAP.
Available Server Groups	In the Available Server Groups list, select the servers to include in the server group, and click to move them to the Assigned Server Groups list.
Assigned Server Groups	

Configure AAA Advanced Settings via the WebUI

You can configure AAA advanced settings outside of the AAA wizard. To use the wizard, see [page 50](#).

From the Configuration menu, click AAA.

Allen-Bradley

Welcome admin

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups    AAA Method List    **AAA Advanced**

Global Config

RADIUS Falback

Password Policy

**AAA Interface**

Authentication

Authorization

Accounting

Console

VTY

HTTP

None

None

None

None

None

None

None

None

None

Apply

Global Config

On the AAA Advanced tab, click Global Config, complete the fields as described in [Table 35](#), and then click Apply.

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups    AAA Method List    **AAA Advanced**

**Global Config**

RADIUS Fallback

Password Policy

**AAA Configurations** Apply

Local Authentication Method List ▼

Authentication Method List Select a value ▼

Local Authorization Method List ▼

Authorization Method List Select a value ▼

Radius Server Load Balance ENABLED ☒

**802.1x Global Configurations**

Send Eapol on Auth-fail ENABLED ☒

System Auth-control ENABLED ☒

Table 35 - AAA Advanced—Global Config

Field	Description
<b>AAA Configurations</b>	
Local Authentication	Choose a local authentication method: <ul style="list-style-type: none"> <li>None—Do not use local authentication. If you choose None for local authentication, you must also choose None for local authorization.</li> <li>Default—Use the default local authentication.</li> <li>Method List—Choose a local authentication method list from the Authentication Method List field.</li> </ul>
Authentication Method List	(Appears for Method List local authentication only). Choose a method list to use for local authentication.
Local Authorization	<ul style="list-style-type: none"> <li>None—Do not use local authorization. If you choose None for local authorization, you must also choose None for local authentication.</li> <li>Default—Use the default local authorization.</li> <li>Method List—Choose a local authentication method list from the Authentication Method List field.</li> </ul>
Authorization Method List	(Appears for Method List local authorization only). Choose a method list to use for local authorization.
Radius Server Load Balance	Click to enable or disable load balancing for the global RADIUS server group.
<b>802.1x Global Configurations</b>	
Send Eapol on Auth-fail	Click to enable or disable Extensible Authentication Protocol over LAN (EAPOL) success messages. When enabled, the switch sends an EAPOL-Success message when it successfully authenticates a critical port.
System Auth-control	Click to globally enable or disable 802.1x authentication.

### *RADIUS Fallback Configuration*

On the AAA Advanced tab, click RADIUS Fallback, complete the fields as described in [Table 36](#), and then click Apply to Device.



The screenshot shows the 'AAA Advanced' configuration page. On the left, there is a sidebar with 'Global Config', 'RADIUS Fallback', and 'Password Policy'. The 'RADIUS Fallback' section is active. The main area contains three input fields: 'Retransmit Count' with a value of 3, 'Timeout Interval (seconds)' with a value of 5, and 'Dead Time (Minutes)' with a value of 1-1440. An 'Apply' button is located to the right of these fields.

Table 36 - AAA Advanced—RADIUS Fallback

Field	Description
Retransmit Count	Enter the time after which the server should attempt retransmission.
Timeout Interval (seconds)	Enter the number of seconds between retransmissions. Valid values: 1...1000 seconds
Dead Time (Minutes)	Enter the amount of time, in minutes, after which a server is assumed to be dead.

*Policy Password Configuration*

On the AAA Advanced tab, click Policy Password, and then click Add.

The screenshot shows the 'AAA Advanced' configuration page with the 'Password Policy' section active. It features a '+ Add' button and a '- Delete' button. Below these is a 'Policy Name' dropdown menu. At the bottom, there is a pagination control showing '0' items per page and a 'No items to display' message.

On the Quick Setup: Password Policy page, complete the fields as described in [Table](#), and then click Apply to Device.

Quick Setup: Password Policy

Policy Name\*

Minimum Length

1

Maximum Length

127

Upper Count

0

Lower Count

0

Numeric Count

0

Special Count

0

Character Changes

4

Validity

Never Expires

Cancel

Apply to Device

### Quick Setup: Password Policy

Field	Description
Policy Name	Enter a name to identify the policy. The policy defines the criteria for the password.
Minimum Length	Enter the minimum length to require for the password. Default value: 1
Maximum Length	Enter the maximum length to require for the password. Default value: 127
Upper Count	Enter the number of uppercase letters to require for the password.
Lower Count	Enter the number of lowercase letters to require for the password.
Numeric Count	Enter how many numbers to require in the password.
Special Count	Enter how many special characters to require in the password.
Character Changes	Enter how many characters are required to be different from the previous password. Default value: 4
Validity	Choose the validity period for the password: <ul style="list-style-type: none"> <li>Never Expires</li> <li>User Defined—Enter the number of years, months, days, hours, minutes, or seconds that the password remains valid.</li> </ul>

# Access Control Lists (ACLs)

ACLs provide basic security for a network by filtering traffic as it passes through a switch. ACLs permit or deny packets as they cross specified interfaces or VLANs. For more information about ACLs, see the Ethernet Reference Manual, publication [ENET-RM002](#).

## Configure ACLs via the WebUI

From the Configuration menu, choose ACL.

Configuration > Security > ACL

+ Add

✕ Delete

Associate Interfaces

	ACL Name	ACL Type	ACE Count	Downloaded ACL
<input checked="" type="checkbox"/>	101	IPv4 Extended	1	No
<input type="checkbox"/>	102	IPv4 Extended	1	No
<input type="checkbox"/>	103	IPv4 Extended	1	No
<input type="checkbox"/>	104	IPv4 Extended	1	No
<input type="checkbox"/>	105	IPv4 Extended	2	No
<input type="checkbox"/>	106	IPv4 Extended	1	No
<input type="checkbox"/>	107	IPv4 Extended	1	No
<input type="checkbox"/>	IP-Adm-V4-Int-ACL-global	IPv4 Extended	2	No
<input type="checkbox"/>	implicit_deny	IPv4 Extended	1	No
<input type="checkbox"/>	implicit_permit	IPv4 Extended	1	No
<input type="checkbox"/>	meraki-fqdn-dns	IPv4 Extended	0	No
<input type="checkbox"/>	preauth_v4	IPv4 Extended	6	No
<input type="checkbox"/>	implicit_deny_v6	IPv6	1	No
<input type="checkbox"/>	implicit_permit_v6	IPv6	1	No
<input type="checkbox"/>	preauth_v6	IPv6	10	No

1

50 items per page

1 - 15 of 15 items

From the Access Control List page, you can add, edit, and delete ACLs:

- To add an ACL, see [page 68](#). After you create an ACL, you must associate it with an interface to make it effective.
- To edit an access list, click the ACL in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an ACL, check its associated checkbox in the grid, and then click Delete.
- To associate ACLs to interfaces, see [page 69](#).

### Add an Access Control List

On the Access Control List page, click Add, complete the fields as described in [Table 37](#), and then click Apply to Device.

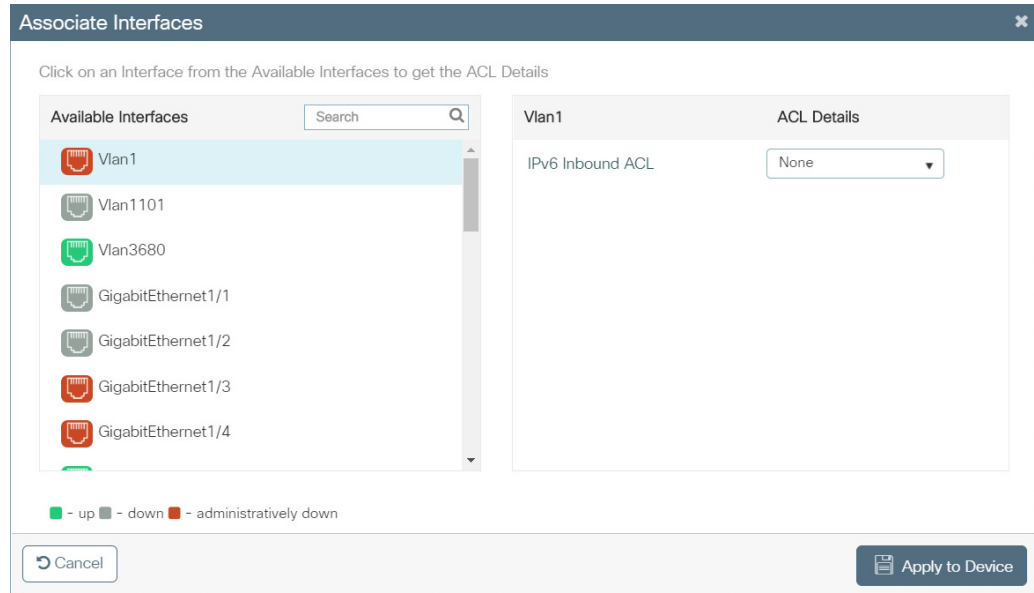
Table 37 - Add ACL Setup

Field	Description
ACL Name	Enter a name to identify the ACL.
ACL Type	Choose the IP version to which the source or destination addresses belong: <ul style="list-style-type: none"> <li>• IPv4 Standard</li> <li>• IPv4 Extended</li> <li>• IPv6</li> </ul>
Sequence	Enter a sequence number for the ACL.
Action	Choose if you want to deny or permit traffic using this ACL. The default action is permit.
Source Type	Choose the source type: <ul style="list-style-type: none"> <li>• any</li> <li>• Host</li> <li>• IP</li> </ul>
Host	(Appears only if the source type is Host). Enter the hostname to indicate the source address.
Source IP	(Appears only if the source type is IP). Enter the source IP address. For IPv4 addresses, enter the subnet mask and for IPv6 addresses, enter the prefix length.
Source Wildcard/Prefix	(Appears only if the source type is IP). Enter the wildcard mask to identify the source addresses affected by the ACL: <ul style="list-style-type: none"> <li>• For IPv4 addresses, enter the subnet mask.</li> <li>• For IPv6 addresses, enter the prefix length.</li> </ul>
Destination Type	(Appears only if the ACL type is IPv4 Extended or IPv6). Choose the destination type: <ul style="list-style-type: none"> <li>• any</li> <li>• Host</li> <li>• IP</li> </ul>
Destination IP	(Appears only if the destination type is IP). Enter the destination IP address. For IPv4 addresses, enter the subnet mask and for IPv6 addresses, enter the prefix length.
Destination Wildcard/Prefix	(Appears only if the destination type is IP). Enter the wildcard mask to identify the destination addresses affected by the ACL: <ul style="list-style-type: none"> <li>• For IPv4 Extended addresses, enter the subnet mask.</li> <li>• For IPv6 addresses, enter the prefix length.</li> </ul>
Protocol	(Appears only if the ACL type is IPv4 Extended or IPv6). Choose the protocol to use for this ACL. The device can permit or deny only the IP packets in an ACL. Other types of packets, such as Address Resolution Protocol (ARP) packets, cannot be specified.
Source Port/Start Port/End Port	(Appears only if the protocol is TCP or UDP). Choose a source port or port range. The port or range is used by applications that send and receive data to and from the networking stack. Some ports are designated for specific applications such as Telnet, SSH, and HTTP.
Destination Port/Destination Port/End Port	(Appears only if the protocol is TCP or UDP). Choose a destination port or a port range. The port or range is used by applications that send and receive data to and from the networking stack. Some ports are designated for specific applications such as Telnet, SSH, and HTTP.
Log	Check Log to enable ACL logging.
DSCP	To use the ACL to mark associated packets with a DSCP value, choose a value.
Add	To add the sequence to the ACL, click Add. The sequence appears in the grid. To add an additional sequence, click Add and complete the fields in the Rules area.
Delete	To delete an ACL sequence and remove it from the grid, check its associated checkbox in the grid, and then click Delete.

### Associate ACLs with Interfaces

1. On the Access Control List page, click Associate Interfaces.

2. In the list of available interfaces, select the interface to associate with ACLs.
3. From each ACL Details pull-down menu, choose an ACL name to associate with the corresponding traffic on the interface.
4. Click Apply to Device.



## Discovery Protocols

The switch supports configuration of Layer 2 discovery protocols via the WebUI. You can use the protocols together or separately.

### Cisco Discovery Protocol (CDP)

CDP is a Cisco® proprietary protocol that allows devices to communicate regardless of IP connectivity. The primary purpose of CDP is to communicate protocol addresses and device capabilities.

CDP allows network management applications, such as FactoryTalk® Network Manager™, to discover Cisco devices that are neighbors of already known devices. With CDP, network management applications can learn the device type and the Simple Network Management Protocol (SNMP) agent address of neighboring devices running lower-layer, transparent protocols. This feature enables applications to send SNMP queries to neighboring devices.

### Link Layer Discovery Protocol (LLDP)

LLDP is defined in international standard IEEE 802.1AB and 802.3. Network devices use LLDP to advertise information about themselves to other devices on the network. Because LLDP runs over the data-link layer, two systems that run different network layer protocols can learn about each other.

LLDP supports a set of attributes to discover neighbor devices. These attributes contain type, length, and value descriptions and are referred to as

type-length-value (TLV) structures. LLDP supported devices can use TLV structures to send and receive information from their neighbors. By using LLDP, devices can advertise details, such as configuration information, device capabilities, and device identity.

[Table 38](#) describes the TLV structures.

**Table 38 - LLDP TLV Structures**

TLV Structure	Description
4-wire-power-management	The 4-pair related capabilities and requirements of Cisco Universal Power Over Ethernet (UPoE) devices.
mac-phy-cfg	The IEEE 802.3 MAC/Phy configuration/status.
management-address	The IP address used for management.
port-description	The source port.
port-vlan	The VLAN present on the access port.
power-management	The power classes, wattage requirements, and priority of PoE devices.
system-capabilities	The device features.
system-description	The IOS version.
system-name	The device name.

## Configure Discovery Protocols via the WebUI

From the Configuration menu, choose Discovery Protocols. On the Discovery Protocols page, you can configure CDP and LLDP.

### Configure CDP

On the CDP tab, complete the fields in as described in [Table 39](#), and then click Apply to Device.

Configuration > Layer2 > Discovery Protocols

CDP    LLDP

CDP ENABLED

Hold Time

Timer

[Apply to Device](#)

**Table 39 - Discovery Protocols—CDP**

Field	Description
CDP	Click to enable or disable CDP globally on the switch. CDP is enabled by default.
Hold Time	Enter the amount of time in seconds that the switch holds the CDP advertisement from a transmitting device before discarding it. Valid values: 10...255 Default value: 180
Timer	Enter the transmission frequency of CDP updates in seconds. Valid values: 5...254 Default value: 60

Configure LLDP

On the LLDP tab, complete the fields in as described in [Table 40](#), and then click Apply to Device.

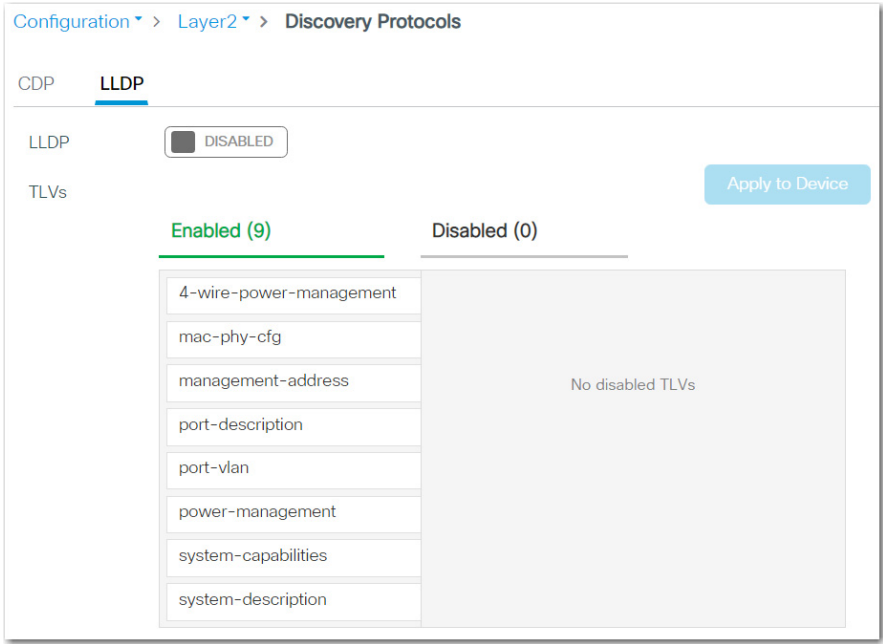


Table 40 - Discovery Protocols–LLDP

Field	Description
LLDP	Click to enable or disable LLDP. LLDP is disabled by default.
TLVs	Specify which TLV structures to enable or disable by moving them to the respective columns. For a description of each TLV structure, see <a href="#">Table 38 on page 71</a> . By default, all TLV structures are enabled.

## Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is a Cisco proprietary, distance-vector-routing protocol. The following capabilities distinguish EIGRP from other routing protocols:

- Fast convergence
- Support for variable-length subnet mask
- Support for partial updates
- Support for multiple network layer protocols

---

**IMPORTANT** EIGRP is available only on Layer 3 switch models. For supported catalog numbers, see [Table 1 on page 12](#).

---

### Feature Summary

EIGRP features include the following:

- Hybrid Distance Vector/Link State algorithm
- Classless routing protocol
- Support for Variable Length Subnet Mask (VLSM) and Classless Interdomain Routing (CIDR)
- Support for summaries and discontinuous networks
- Performs partial updates as needed
- Consumes less bandwidth (no broadcasts, no periodic updates, updates contain only changes)
- Efficient neighbor discovery and fast convergence
- Best path selection via Diffusing Update Algorithm (DUAL)
- Support for IP, IPX, and AppleTalk via protocol-dependent modules

### Network Operation

A device that runs EIGRP stores all neighbor routing tables so that it can quickly adapt to alternate routes. If no appropriate route exists, EIGRP queries its neighbors to discover an alternate route. These queries continue until an alternate route is found. Variable-length subnet masks enable routes to be automatically summarized on a network number boundary. EIGRP can also summarize on any bit boundary at any interface. EIGRP does not make periodic updates. Instead, it sends partial updates only when the metric for a route changes. Partial updates are limited so that only routers that need the information are updated.

Neighbor discovery is the process that the EIGRP device uses to dynamically learn of other routers on directly attached networks. EIGRP devices send multicast hello packets to announce their presence on the network. You can also define static neighbors, which receive unicast packets. When the device receives a hello packet from a new neighbor, it sends its topology table to the neighbor with an initialization bit set. When the neighbor receives the topology update with the initialization bit set, the neighbor sends its topology table back to the EIGRP device. Once this neighbor relationship is established, routing updates are not exchanged unless there is a change in the network topology.

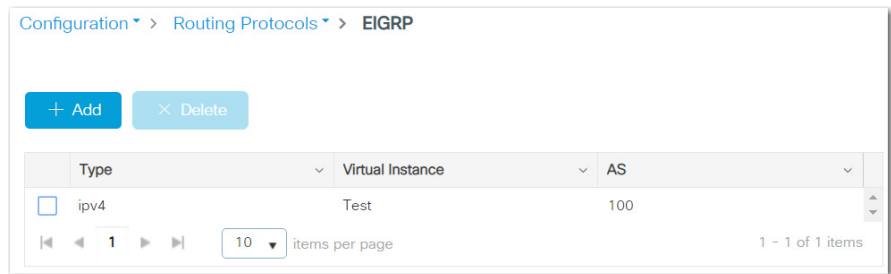


EIGRP uses the Diffusing Update Algorithm (DUAL), which provides loop-free operation at every instance throughout a route computation. DUAL allows all devices that are involved in a topology change to synchronize simultaneously. Routers that are unaffected by topology changes are not involved in re-computations.

To configure EIGRP, create an EIGRP instance and associate networks. EIGRP sends updates to the interfaces in the specified networks. If you do not specify an interface network, it is not advertised in any EIGRP update.

## Configure EIGRP via the WebUI


From the Configuration menu, choose EIGRP.



From the EIGRP page, you can add, edit, and delete EIGRP instances:

- To add an EIGRP instance, click Add, complete the fields as described in [Table 41](#), and then click Apply to device
- To edit an EIGRP instance, click the EIGRP instance in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an EIGRP instance, check its associated checkbox in the grid, and then click Delete.

Table 41 - Create EIGRP

Field	Description
Basic or Advanced	Click to determine the level of configuration: <ul style="list-style-type: none"> <li>Basic—The page displays only basic configuration fields. Basic is the default value.</li> <li>Advanced—The page displays both basic and advanced configuration fields.</li> </ul>
<b>Basic Settings</b>	
Virtual Instance	Enter a name to identify the EIGRP route in the network.
IPv4, IPv6, IPv4/IPv6	Click the IP version for which to configure EIGRP.
Address Family IPv4	Specify the following information for IPv4, IPv6, or both: <ol style="list-style-type: none"> <li>1. Check VRF, and then choose the VRF name.</li> <li>2. To enable unicast transmission, check Unicast.</li> <li>3. Check AS, and then enter the AS number. Valid values: 1...65535</li> </ol>
<b>Advanced Settings</b>	
Router ID	Enter a router ID to manually configure the router for EIGRP. The router ID identifies the originating router for external routes. If an external route is received with the local router ID, the route is discarded. EIGRP automatically selects an IP address to use as the router ID when an EIGRP process is started. The highest IP address assigned to a loopback interface is selected as the router ID. If there are not any loopback addresses configured, the highest IP address assigned to any other interface is chosen as the router ID. The highest local IP address is selected and loopback interfaces are preferred. The router ID can be configured with any IP address with two exceptions: 0.0.0.0 and 255.255.255.255 are not valid values. Configure a unique value for each router.
Network	(IPv4 only). Check Network, and then enter the network IP address and the wildcard mask. To list the network IP address and wildcard details, click the plus sign (+).
Disable Split Horizon	Split horizon controls the sending of EIGRP update and query packets. When split horizon is enabled on an interface, update and query packets are not sent to destinations for which this interface is the next hop. Controlling update and query packets in this manner reduces the possibility of routing loops. In general, we recommend that you keep split horizon enabled unless you are certain that your application requires the change in order to properly advertise routes. To disable split horizon on an interface, do the following: <ol style="list-style-type: none"> <li>1. Check Disable Split Horizon.</li> <li>2. From the pull-down menu, choose an interface.</li> <li>3. Click the plus sign (+) to add the interface to the grid.</li> </ol> By default, split horizon is enabled on all interfaces.
Outgoing Interface Stub	This static configuration must be performed on both neighbors, and the specified IP address must belong to the same subnet as the specified outgoing interface. To configure the outgoing interface, do the following: <ol style="list-style-type: none"> <li>1. Check Outgoing Interface.</li> <li>2. From the pull-down menu, choose an interface.</li> <li>3. Click the plus sign (+) to add the interface to the grid.</li> </ol>
Stub	The EIGRP stub routing feature improves network stability, reduces resource utilization, and simplifies the stub device configuration. To enable the stub routing feature, do the following: <ol style="list-style-type: none"> <li>1. Check Stub.</li> <li>2. To set the device as a receive-only neighbor, check Receive only.</li> <li>3. To advertise redistributed routes from other protocols and autonomous systems, check Redistribute.</li> <li>4. To advertise static routes, check Static.</li> <li>5. To advertise summary routes, check Summary.</li> </ol>
Variance	The variance number is used to load balance over unequal cost paths. The variance number is multiplied by the local best metric then includes the routes with the lesser or equal metric. Enter the variance number. Valid values: 1...128 Default value: 1 (equal-cost load balancing)
Redistribute	Redistribution is the use of a routing protocol to advertise routes that are learned by some other means, such as by another routing protocol, static routes, or directly connected routes. Check each protocol or routing type to redistribute, and then enter the metrics for each type.
Auth Key	Enter an authentication key.
Enable Best Practices	To enable the default features, check Enable Best Practices. To view the list of default features, hover your mouse over the information icon  .

## Ethernet Ports

Configure Ethernet ports, or interfaces, on the switch to determine how data is received and sent between the switch and the attached device. You can change these settings to fit your network needs and to troubleshoot network problems. The settings on a switch port must be compatible with the port settings of the connected device.

### Advanced Port Configuration

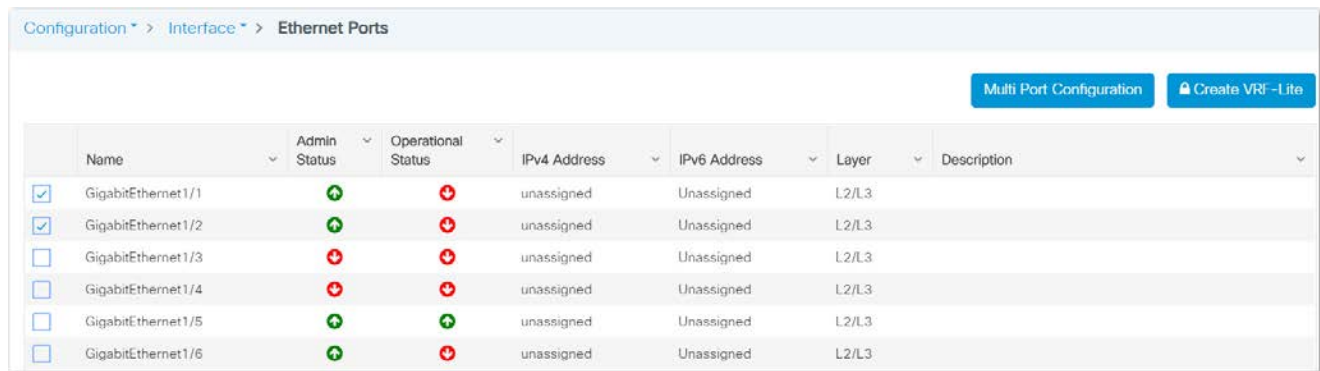
Advanced port configuration includes these features:

- DHCP relay
- DHCP snooping
- Quality of Service (QoS) policy management
- Port security
- Port thresholds and storm control

For more information about these features, see the Ethernet Reference Manual, publication [ENET-RM002](#).

### Configure Ethernet Interfaces via the WebUI

From the Configure menu, choose Ethernet Ports.



	Name	Admin Status	Operational Status	IPv4 Address	IPv6 Address	Layer	Description
<input checked="" type="checkbox"/>	GigabitEthernet1/1	🟢	🔴	unassigned	Unassigned	L2/L3	
<input checked="" type="checkbox"/>	GigabitEthernet1/2	🟢	🔴	unassigned	Unassigned	L2/L3	
<input type="checkbox"/>	GigabitEthernet1/3	🔴	🔴	unassigned	Unassigned	L2/L3	
<input type="checkbox"/>	GigabitEthernet1/4	🔴	🔴	unassigned	Unassigned	L2/L3	
<input type="checkbox"/>	GigabitEthernet1/5	🟢	🟢	unassigned	Unassigned	L2/L3	
<input type="checkbox"/>	GigabitEthernet1/6	🟢	🔴	unassigned	Unassigned	L2/L3	

From the Ethernet Ports page, you can do the following:

- Configure individual ports as described on [page 76](#).
- Configure multiple ports simultaneously as described on [page 77](#).
- Configure VRF-Lite as described on [page 81](#).

#### Configure Individual Ports

1. In the grid, click the port to configure.
2. On the General tab, complete the fields as described in [Table 42 on page 79](#).

The screenshot shows the 'Configure Interface GigabitEthernet1/4' dialog box with the 'General' tab selected. The 'Interface' field is 'GigabitEthernet1/4'. The 'Description' field is empty with a '(1-200 Characters)' hint. 'Speed' and 'Duplex' are both set to 'auto'. 'Admin Status' is 'UP' with a green up arrow icon. 'Port Fast' is set to 'disable'. 'Enable Layer 3 Address' is a toggle switch labeled 'DISABLED'. 'Switchport Mode' is set to 'access'. 'Access Vlan' is set to '1'. At the bottom, there are 'Cancel' and 'Update & Apply to Device' buttons.

- On the Advanced tab, complete the fields as described in [Table 43 on page 80](#).

The screenshot shows the 'Configure Interface GigabitEthernet1/4' dialog box with the 'Advanced' tab selected. Under 'Access Lists', 'IPv4 Inbound ACL' and 'IPv6 Inbound ACL' are both set to 'None'. Under 'DHCP Relay', 'Relay Information Option' and 'DHCP Snooping Trust' are both toggle switches labeled 'DISABLED'. Under 'Policy Management', 'Auto QoS' is a toggle switch labeled 'DISABLED'. 'Input User Defined QoS' is set to 'CIP-PTP-Traffic'. 'Output User Defined QoS' is set to 'Policymap-Output-D'. 'Interface Template' is set to 'None'. At the bottom, there are 'Cancel' and 'Update & Apply to Device' buttons.

- Click Update & Apply to Device.

### Configure Multiple Ports Simultaneously

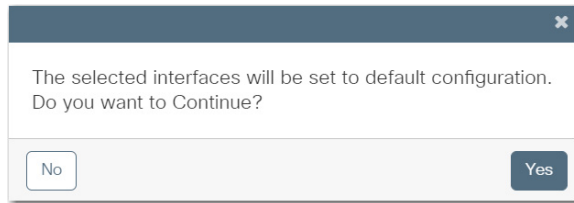


**WARNING:** Multiport configuration resets the current settings for the selected ports to the default settings. You must reconfigure all settings for the selected ports. Upon completion, the selected ports configurations are identical.

- In the grid, click the checkbox next to each port to configure.
- Click Multi Port Configuration.

The screenshot shows the 'Ethernet Ports' configuration page. The breadcrumb trail is 'Configuration > Interface > Ethernet Ports'. At the bottom right, there are two buttons: 'Multi Port Configuration' (which is circled in blue) and 'Create VRF-Lite'.

A warning appears.



3. To reset the current settings for the selected ports and proceed with the reconfiguration of the selected ports, click Yes.
4. On the General tab, complete the fields as described in [Table 42](#).

The "Multi Port Configuration" dialog box is shown with the "General" tab selected. The "Interfaces" field is set to "GigabitEthernet1/1-2". The "Description" field is empty, with a note "(1-200 Characters)". The "Speed" and "Duplex" dropdown menus are both set to "auto". The "Admin Status" is set to "UP" with a green up arrow icon. The "Port Fast" dropdown is set to "disable". The "Enable Layer 3 Address" checkbox is unchecked, with the label "DISABLED" next to it. The "Switchport Mode" dropdown is set to "access". The "Access VLAN" dropdown is set to "1". At the bottom, there are "Cancel" and "Apply to Device" buttons.

5. On the Advanced tab, complete the fields as described in [Table 43](#).

The "Multi Port Configuration" dialog box is shown with the "Advanced" tab selected. Under the "Access Lists" section, both "IPv4 Inbound ACL" and "IPv6 Inbound ACL" dropdown menus are set to "None". Under the "DHCP Relay" section, both "Relay Information Option" and "DHCP Snooping Trust" checkboxes are unchecked, with the label "DISABLED" next to each. Under the "Policy Management" section, the "Auto QoS" checkbox is unchecked, with the label "DISABLED" next to it, and the "Input User Defined QoS" dropdown is set to "CIP-PTP-Traffic". At the bottom, there are "Cancel" and "Apply to Device" buttons.

6. Click Apply to Device.

Table 42 - Configure Interface—General Tab

Field	Description
Interface(s)	Displays the port type(s) and number(s).
Description	Enter a description for the interface. We recommend that you provide a port description to help identify the port during monitoring and troubleshooting. The description can be the location of the connected device or the name of the person using the connected device.
Speed	<p>Choose the operating speed of the switch port in Mbps:</p> <ul style="list-style-type: none"> <li>• 10</li> <li>• 100</li> <li>• 1000</li> <li>• auto</li> </ul> <p>If the connected device can negotiate the link speed with the switch port, choose auto (autonegotiation). The default speed is auto. We recommend that you use autonegotiation so that the speed of the switch port automatically matches the speed of the connected device. If the connected device requires a specific speed, change the speed of the switch port.</p>
Duplex	<p>Choose the duplex mode of the switch port:</p> <ul style="list-style-type: none"> <li>• full— (Full-duplex mode). Both devices can send and receive data at the same time.</li> <li>• half— (Half-duplex mode). The connected device must alternate sending or receiving data.</li> <li>• auto—(Autonegotiation). The connected device can negotiate the duplex mode with the switch.</li> </ul> <p>Default value: auto</p> <p>We recommend that you use autonegotiation so that the mode on the switch port automatically matches the mode of the connected device. If the connected device requires a specific duplex mode, change the mode of the switch port.</p>
Admin Status	<p>Click to enable or disable the operational status of the interface:</p> <ul style="list-style-type: none"> <li>• Up—The interface is operational.</li> <li>• Down—The interface is not operational.</li> </ul> <p>Default value: Up</p>
Port Fast	<p>Choose whether to enable PortFast on the port:</p> <ul style="list-style-type: none"> <li>• disable—Does not enable PortFast.</li> <li>• access—Enables PortFast when the port is operating as an access port.</li> <li>• trunk—Enables PortFast when the port is operating as a trunk port.</li> </ul> <p>Devices that connect to ports that are enabled for PortFast can connect to the network immediately. Otherwise, the devices wait for the port to transition from the listening and learning states to the forwarding state. If the switch port connects to endpoints (for example, to computers and not to other switches or routers), enable PortFast on the port.</p>
Enable Layer 3 Address	<p>Click to enable or disable Layer 3 functionality on the port. When enabled, this elevates the interface from a switch port (Layer 2) to a routed port (Layer 3).</p> <p>Default value: Disabled</p>
IP Options	<p>(Appears when a Layer 3 address is enabled.) Choose one of the following IP address types:</p> <ul style="list-style-type: none"> <li>• IPV4</li> <li>• IPV6</li> </ul>
Switchport Mode	<p>Choose one of the following administrative port modes:</p> <ul style="list-style-type: none"> <li>• access—The port operates permanently as an access port and negotiates to convert a neighbor port into an access port even if the neighbor port is a trunk port. If you choose this option, also choose an access VLAN. An access port belongs to and carries the traffic of only one VLAN.</li> <li>• trunk—The port operates permanently as a trunk port and negotiates to convert a neighbor port into a trunk port even if the neighbor port is not a trunk port. If you choose Trunk mode, be sure to also choose a native VLAN and allowed VLANs.</li> <li>• dynamic auto—The port converts to a trunk port if the neighbor port is set to Trunk mode or Dynamic Desirable mode. If you choose Dynamic Auto mode, be sure to also specify these VLANs: <ul style="list-style-type: none"> <li>– Choose an access VLAN to use when the port is in Access mode.</li> <li>– Choose a native VLAN and allowed VLANs to use when the port is in Trunk mode.</li> </ul> </li> <li>• dynamic desirable—If the neighbor port is set to Trunk, Dynamic Desirable, or Auto mode, the port converts to a trunk port. If you choose Dynamic Desirable mode, be sure to also specify these VLANs: <ul style="list-style-type: none"> <li>– Choose an access VLAN to use when the port is in Access mode.</li> <li>– Choose a native VLAN and allowed VLANs to use when the port is in Trunk mode.</li> </ul> </li> </ul> <p>Default value: dynamic auto</p>
Access Vlan	Choose the VLAN to assign to the port when the port operates as an access port. The port carries traffic for only its assigned VLAN.
Allowed Vlan	<p>Click to specify the VLANs to assign to the port when the port operates as a trunk port:</p> <ul style="list-style-type: none"> <li>• All— The port carries traffic for all available VLANs.</li> <li>• Vlan IDs—The port carries traffic for only the VLANs you specify.</li> </ul>
VLAN IDs	(Appears only when you click VLAN IDs in the Allowed VLAN field). Enter the VLAN IDs to allow on the port. You can enter a series of IDs or a range of IDs, such as 2, 4, 6-10.
Native Vlan	Choose the VLAN to transport untagged packets on the switch when the port operates as a trunk port.

Table 43 - Configure Interface—Advanced Tab

Field	Description
<b>Access Lists</b>	
IPv4 Inbound ACL	Choose the IPv4 access control list (ACL) to apply to ingress traffic on the port.
IPv6 Inbound ACL	Choose the IPv6 access control list (ACL) to apply to ingress traffic on the port.
<b>DHCP Relay</b>	
Relay Information	Click to enable or disable a DHCP server from forwarding relay information. Default value: Disabled
DHCP Snooping Trust	Click to enable or disable DHCP snooping. DHCP snooping configures the port as a trusted source of DHCP messages. Default value: Disabled
<b>Policy Management</b>	
Auto QoS	Click to enable or disable Auto QoS on the port. Auto QoS deploys QoS features by determining the network design and enabling the configurations that allow the switch to prioritize different traffic flows. Default value: Disabled
Input User Defined QoS	Choose an QoS policy for ingress traffic on the port.
Output User Defined	Choose an QoS policy for egress traffic on the port.
Interface Template	Choose a QoS template for the port.
<b>Port Security</b> (This section is not included in the Multi Port Configuration page.)	
Port Security	Click to enable or disable port security. Port security restricts access to a port. A security violation occurs in the following scenarios: <ul style="list-style-type: none"> <li>When a device with a MAC address that is different from any identified, secure MAC address attempts to access the switch port</li> <li>When the number of MAC addresses on a port exceeds the maximum number that is allowed on that port. MAC addresses for allowed devices are manually configured or learned by the switch.</li> </ul> Default value: Disabled
Maximum MAC Count	Enter the maximum number of static MAC addresses to allow on the port.
MAC Address	To add the MAC address of a device that is not currently connected to the Static MAC Table, enter the address in the MAC Address field and click +.
Static MAC Table	To remove a MAC address from the Static MAC Table, click the x in the table row for that MAC address. To add the MAC addresses of all devices that are connected to this port to the Static MAC Table, click Add Learned MAC.
<b>Port Threshold</b>	
Broadcast Threshold Level	To enable broadcast storm control on the port, check Broadcast Threshold Level. Choose one of the following units, and then type values in each of the two fields in the correct range: <ul style="list-style-type: none"> <li>% (0...100)</li> <li>bps (bits per second, 0...10 billion)</li> <li>pps (packets per second, 0...10 billion)</li> </ul> When the threshold value is reached, the port blocks traffic until the traffic rate drops below the threshold.
Multicast Threshold Level	To enable multicast storm control on the port, check Multicast Threshold Level. Choose one of the following units, and then type values in each of the two fields in the correct range: <ul style="list-style-type: none"> <li>% (0...100)</li> <li>bps (bits per second, 0...10 billion)</li> <li>pps (packets per second, 0...10 billion)</li> </ul> When the threshold value is reached, the port blocks traffic until the traffic rate drops below the threshold.
Unicast Threshold Level	To enable unicast storm control on the port, check Unicast Threshold Level. Choose one of the following units, and then type values in each of the two fields in the correct range: <ul style="list-style-type: none"> <li>% (0...100)</li> <li>bps (bits per second, 0...10 billion)</li> <li>pps (packets per second, 0...10 billion)</li> </ul> When the threshold value is reached, the port blocks traffic until the traffic rate drops below the threshold. By default, unicast storm control is disabled.
Outgoing Threshold Level	To enable outgoing thresholds on the port, check Outgoing Threshold Level. Enter a percentage value in the range of 0...100.
<b>802.1x Configurations</b>	
Authenticator	Click to enable or disable Authenticator on 802.1x configurations.
Access-Session	Click to open or close Access-Session on the 802.1x configurations. The default is Open when the Authenticator setting is disabled, and Closed when enabled.
Authentication Order	Choose an Authentication Order for the 802.1x configuration on the port. <ul style="list-style-type: none"> <li>None</li> <li>dot1x</li> <li>Mab</li> <li>dot1x-&gt;Mab</li> <li>Mab-&gt;dot1x</li> </ul> dot1x is the default when the Authenticator setting is enabled.

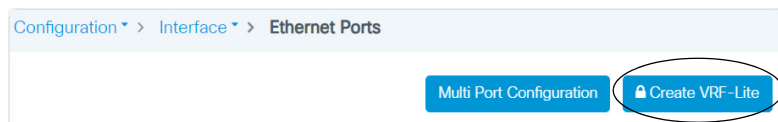
**Table 43 - Configure Interface—Advanced Tab (Continued)**

Field	Description
Port Mode	Choose a Port Mode for the 802.1x configuration on the port. <ul style="list-style-type: none"> <li>• None</li> <li>• Auto</li> <li>• Force Authorized</li> <li>• Force Unauthorized</li> </ul> Force Authorized is the default when the Authenticator setting is enabled.
Host Mode	Choose a Host Mode for the 802.1x configuration on the port. <ul style="list-style-type: none"> <li>• None</li> <li>• Single Host</li> <li>• Multiple Host</li> <li>• Multiple Domain</li> <li>• Multiple Authentication</li> </ul> Multiple Authentication is the default when the Authenticator setting is enabled.
<b>IP Device Tracking</b>	
IP Device Tracking	Click to enable or disable IP device tracking on the port. IP device tracking maintains a list of devices that are connected to the port via an IP address.

### Configure VRF-Lite

Virtual Routing and Forwarding (VRF) is a feature that supports two or more Virtual Private networks (VPNs), where IP addresses can be overlapped among the VPNs. VRF-lite uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF.

1. On the Ethernet Ports page, click Create VRF-Lite.



2. On the Create VRF Lite page, complete the fields as described in [Table 44](#), and click Apply to Device.



**Table 44 - Create VRF-Lite Fields**

Field	Description
IPv4, IPv6, IPv4/IPv6	Click the address type.
VRF Name	Enter a name for the VRF.
Route Distinguisher	Create a VRF table by specifying a route distinguisher. Enter either an Autonomous System (AS) number and an arbitrary number (xxx:y) or an IP address and arbitrary number (A.B.C.D:y).
Route-Target Import	Create a list of import route target communities for the VRF. Enter either an AS system number and an arbitrary number (xxx:y) or an IP address and an arbitrary number (A.B.C.D:y).
Route-Target Export	Create a list of export route target communities for the VRF. Enter either an AS system number and an arbitrary number (xxx:y) or an IP address and an arbitrary number (A.B.C.D:y).

## Configure Ethernet Ports via the Logix Designer Application

1. In the navigation pane, click Port Configuration.
2. Complete the fields as described in [Table 45](#), and then click Set.

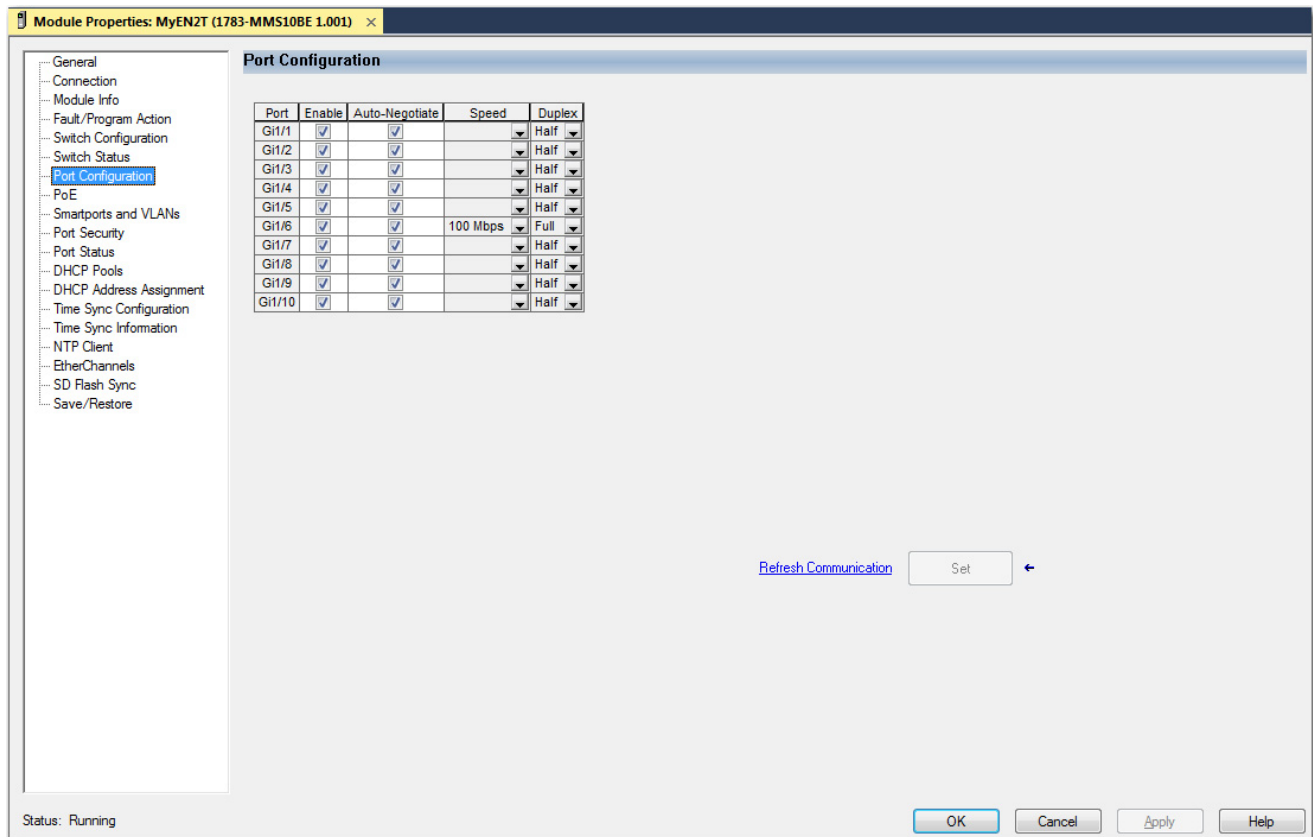


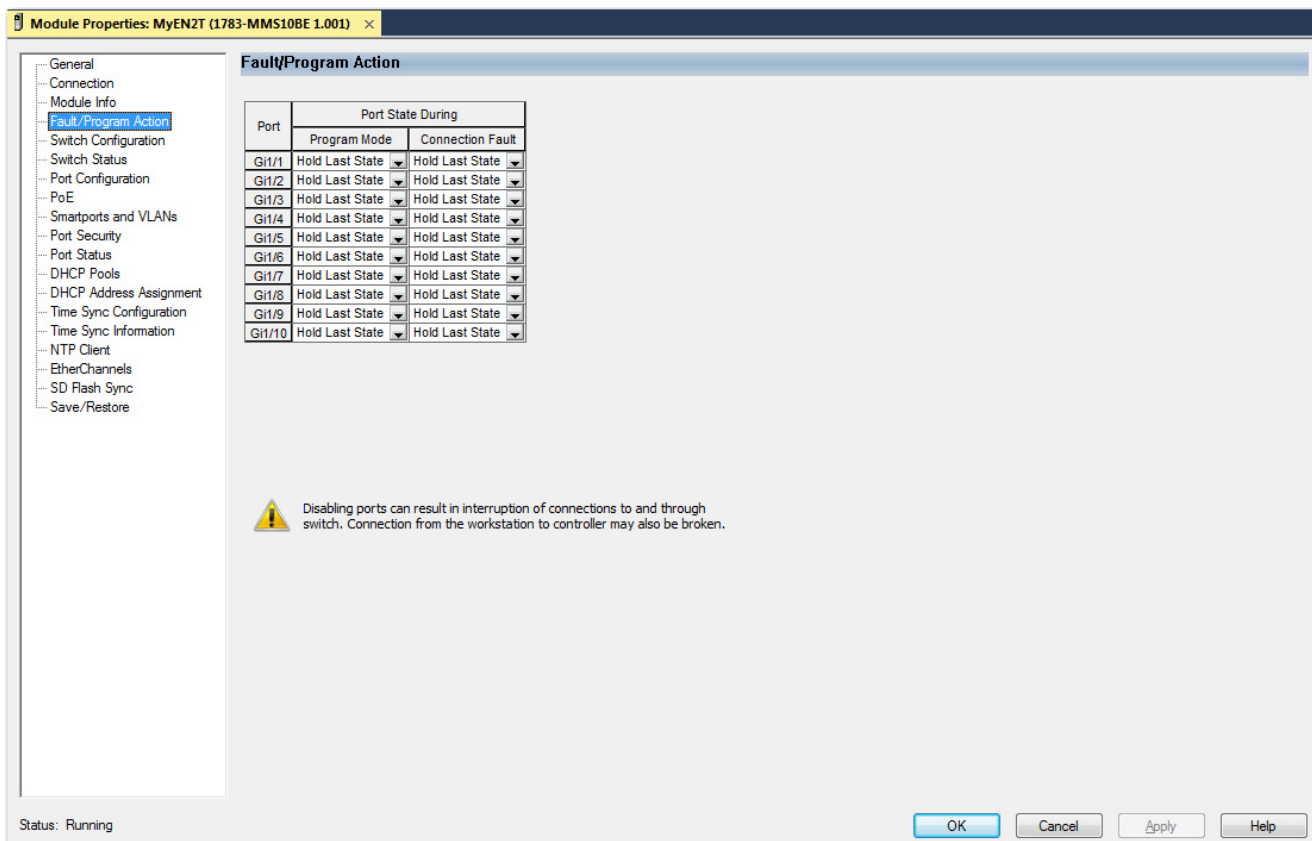
Table 45 - Port Configuration

Field	Description
Port	The port that is selected for configuration.
Enable	To enable the port, check the checkbox. To disable the port manually, clear the checkbox. If the port is not in use and is not attached to a device, we recommend that you disable the port. You can troubleshoot a suspected unauthorized connection by manually disabling the port.
Auto-negotiate	If you want the port and end-device to auto-negotiate the link speed and Duplex mode, check the checkbox. To specify the desired port speed and Duplex mode manually, clear the checkbox. We recommend that you use the default (auto-negotiate) so that the speed and duplex settings on the switch port automatically match the setting on the connected device. Change the switch port speed and duplex if the connected device requires a specific speed and duplex. If you set the speed and duplex for the switch port, the connected device must be configured for the same speed and duplex and not set to auto-negotiate. Otherwise, a speed/duplex mismatch occurs. Fiber-optic ports do not support auto-negotiation.
Speed	Choose the operating speed of the port: <ul style="list-style-type: none"> <li>• 10 Mbps</li> <li>• 100 Mbps</li> <li>• 1 Gbps</li> </ul>
Duplex	Choose one of these Duplex modes: <ul style="list-style-type: none"> <li>• Half-duplex—Both devices cannot send data simultaneously. Half-duplex is not available when speed is set to 1 Gbps or higher.</li> <li>• Full-duplex—Both devices can send data simultaneously.</li> </ul>

### Configure Port States During Program Mode and Connection Faults

You can configure the state of each port when these changes occur at the controller:

- The controller transitions to Program mode
  - Communication is disrupted between the controller and the switch
1. In the navigation pane, click Fault/Program Action.
  2. Complete the fields as described in [Table 46](#), and then click Apply.



**Table 46 - Fault/Program Action**

Field	Description
Port	Displays the port type and number.
Program Mode	Choose what happens at the port when the controller transitions to Program mode: <ul style="list-style-type: none"> <li>• Hold Last State—The port maintains the current state.</li> <li>• Disable—The port is disabled.</li> <li>• Enable—The port is enabled.</li> </ul> Default value: Hold Last State
Connection Fault	Choose what happens at the port when communication is lost between the controller and the switch: <ul style="list-style-type: none"> <li>• Hold Last State—The port maintains the current state.</li> <li>• Disable—The port is disabled.</li> <li>• Enable—The port is enabled.</li> </ul> The default is Hold Last State.

## Flow-based SPAN (FSPAN)

FSPAN is used to mirror traffic based on filter criteria. FSPAN supports three types of access control lists (ACLs) to the SPAN session and filtering based on VLAN.

You can control the type of network traffic to be monitored in SPAN or RSPAN sessions by using flow-based SPAN (FSPAN) or flow-based RSPAN (FRSPAN), which apply ACLs to the monitored traffic on the source ports. The FSPAN ACLs can be configured to filter IPv4, IPv6, and VLAN monitored traffic. You can use SPAN for troubleshooting connectivity issues and calculating network utilization and performance.

## Configure FSPAN via the WebUI

From the Configuration Menu, choose SPAN.

Configuration > Layer2 > SPAN

+ Add
× Delete

Session ID	Session Type	Source Interfaces	Destination Interfaces	Filter Type	Filter Condition
<div> <span>◀</span> <span>▶</span> <span>0</span> <span>▶</span> <span>▶▶</span> </div> <div> 10 Items per page </div> <div>No items to display</div>					

*ⓘ* A maximum of two monitor sessions is supported on this platform.

To configure FSPAN, use the following steps:

1. Select one or more source interfaces from the list of available interfaces on the left and click the arrow to add them to the Selected list on the right.
2. Check or uncheck the Ingress checkboxes to specify the direction of source packets to be monitored.
3. Select Enable FSPAN for local source, and then select the Filter Type and Filter Condition from the drop-down lists.
4. When you are finished, Click Apply to Device.

Create SPAN

Span Source Type

Local

Select Source Interface(s)

Available (23)

Search

Selected (0)

Interfaces	Ingress	Egress
No Interfaces Enabled		

Span Destination Type

Local

Select Destination Interface(s)

Available (19)

Search

Selected (0)

Interfaces	Ingress	Egress
No Interfaces Enabled		

Platform does not support SPAN filtering when

- Source interface is configured in the egress direction.
- SPAN is enabled on vlans.
- One of the SPANs is remote FSPAN.

Enable FSPAN

☐

Cancel

Apply to Device

---

**IMPORTANT** This platform does not support SPAN filtering when:

- Source interface is configured in the egress direction.
- SPAN is enabled on VLANs.
- One of the SPANs is remote FSPAN.

---

# Logical Interfaces

A logical interface is a virtual interface, rather than a physical interface. You can configure these logical interfaces on the switch:

- Port channels, also known as EtherChannels
- Loopback interfaces

## Port Channels or EtherChannels

A port channel, or EtherChannel, is a group of switch ports that are bundled into one logical link to create a higher bandwidth between two switches. For example, four switch ports that are all configured to operate at 100 Mbps can be assigned to an EtherChannel to provide full-duplex bandwidth of up to 400 Mbps. If one of the ports in the EtherChannel becomes unavailable, traffic is carried over the remaining ports within the EtherChannel. For more information about port channels, see the Ethernet Reference Manual, publication [ENET-RM002](#).

## EtherChannel Modes

In the Logix Designer application, you can assign the EtherChannel modes as described in [Table 47](#).

Table 47 - EtherChannel Modes

Mode	Description
Static	All ports join the EtherChannel, without negotiations. This mode can be useful if the remote device does not support the protocols that other modes require. The switches at both ends of the link must be configured in Static mode.
Link Aggregation Control Protocol (LACP) (active)	This mode enables LACP unconditionally. The port sends LACP packets to other ports to initiate negotiations to create EtherChannels. A port in active LACP mode can form an EtherChannel with another port that is in active or passive LACP mode. The ports must be configured for full-duplex.

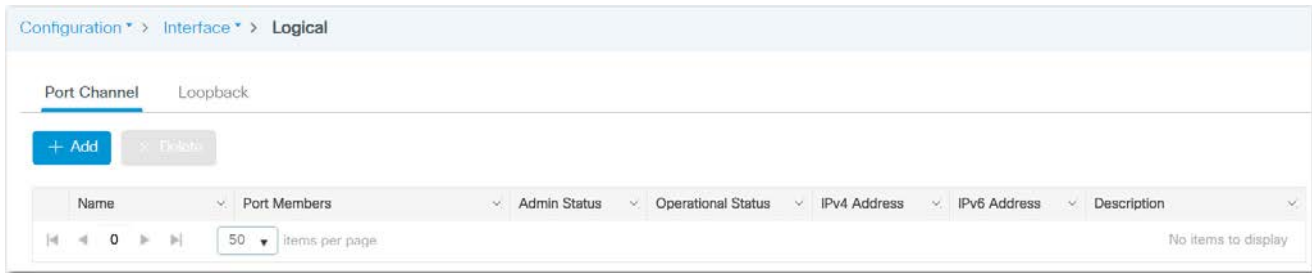
## Loopback Interfaces

A loopback interface is a virtual interface that remains in an up (operational) state. A loopback interface can provide a stable interface on which you can assign a Layer 3 address. This address can be configured as the source address when the networking device must send data for protocols, such as Cisco Discovery Protocol (CDP), to another device in your network and you always want the receiving device to see the same source IP address from the networking device. This is an issue in networks with multiple equal-cost paths because of the following:

- Under normal circumstances the packets that are generated by a networking device use the IP address from the outbound interface as the source address for the packets
- From the networking device to the receiving host, each packet can use a different outbound interface.

## Configure Logical Interfaces via the WebUI

From the Configure menu, choose Logical.



From the Logical page, you can configure logical interfaces. Logical interfaces include port channels and loopback interfaces:

- To configure port channels, see the following instructions.
- To configure loopback interfaces, see [page 88](#).

### Configure Port Channels

From the Port Channels tab, you can add, edit, and delete port channels:

- To add a port channel, click Add, complete the fields as described in [Table 48](#), and then click Apply to Device.
- To edit a port channel, check the checkbox for the interface in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a port channel, check its associated checkbox in the grid, and then click Delete.

The 'Add Port Channel Interface' dialog box contains the following fields and sections:

- Port Channel Number\*:** A text input field with '1 - 6' entered.
- Description:** An empty text input field.
- Admin Status:** A dropdown menu showing 'UP' with a green up arrow icon.
- Port Fast:** A dropdown menu showing 'disable'.
- Enable Layer 3 Address:** A checkbox labeled 'DISABLED'.
- Port Members:**
  - Available (24):** A list of available interfaces: Gi1/1, Gi1/2, and Gi1/5, each with a right-pointing arrow.
  - Associated (0):** A section with a search bar and a message 'No Interface Associated'.

At the bottom, there are 'Cancel' and 'Apply to Device' buttons.

**Table 48 - Add Port Channel Interface**

Field	Description
Port Channel Number	Enter a number to identify the port channel. Valid values: 1...6
Description	Enter a description for the port channel.
Admin Status	Click to enable or disable the operational status of the interface: <ul style="list-style-type: none"> <li>Up—The interface is operational.</li> <li>Down—The interface is not operational.</li> </ul> Default value: Up
PortFast	Choose whether to enable PortFast on the port channel: <ul style="list-style-type: none"> <li>disable—Does not enable PortFast.</li> <li>access—Enables PortFast when the port channel is operating as an access interface.</li> <li>trunk—Enables PortFast when the port channel is operating as a trunk interface.</li> </ul> Devices that connect to port channels that are enabled for PortFast can connect to the network immediately. Otherwise, the devices wait for the interface to transition from the listening and learning states to the forwarding state. If the port channel connects to endpoints (for example, to computers and not to other switches or routers), enable PortFast on the port channel.
Enable Layer 3 Address	Click to enable or disable Layer 3 functionality on the port. When enabled, this elevates the interface from a switch port (Layer 2) to a routed port (Layer 3). Default value: Disabled
Port Members	In the Available list, click to move interfaces to the Associated list and make them members of the port channel.

### Configure Loopback Interfaces

From the Loopback tab, you can add, edit, and delete loopback interfaces:

- To add a loopback interface, click Add, complete the fields as described in [Table 49](#), and then click Apply to Device.
- To edit a loopback interface, click the interface in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a loopback interface, check its associated checkbox in the grid, and then click Delete.

Add Loopback Interface

Loopback Number\*
0 - 2147483647

Description

Admin Status
UP

VRF
None

Relay Information Option
DISABLED

IP Options
☐ IPV4
☐ IPV6

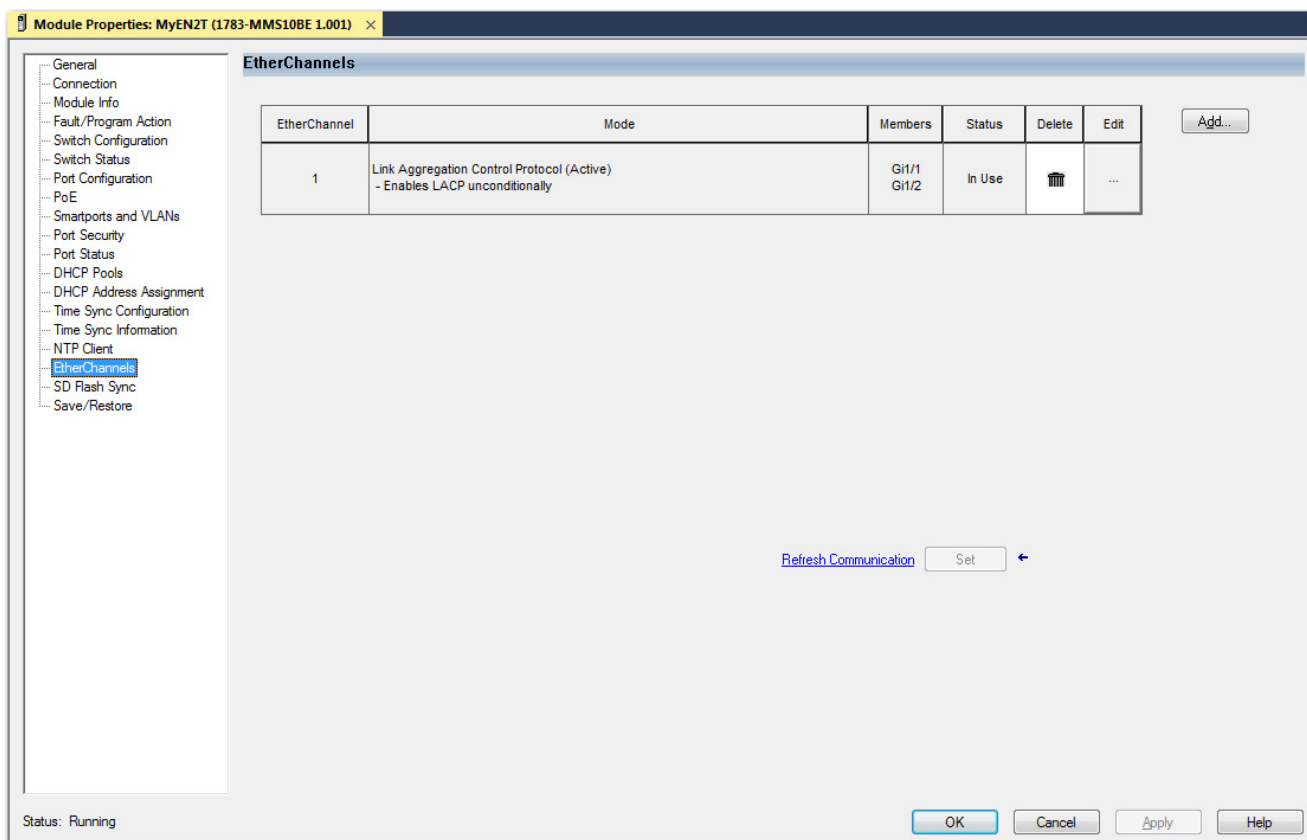
Cancel
Apply to Device

**Table 49 - Add Loopback Interface**

Field	Description
Loopback Number	Enter a number to identify the loopback interface. Valid values: 0...2147483647
Description	Enter a description for the loopback interface.
Admin Status	Click to enable or disable the operational status of the interface: <ul style="list-style-type: none"> <li>Up—The interface is operational.</li> <li>Down—The interface is not operational.</li> </ul> Default value: Up
VRF	Choose a Virtual Routing and Forwarding (VRF) instance to assign to the loopback interface.
Relay Information	Click to enable or disable a DHCP server from forwarding relay information. Default value: Disabled
IP Options	To configure an IPv4 interface, check IPV4, and then specify the IPv4 address information. To configure an IPv6 interface, check IPV6, and then specify the IPv6 address information.

## Configure EtherChannels via the Logix Designer Application

In the navigation pane, click EtherChannels.





On the EtherChannels view, you can add, edit, and delete EtherChannels:

- To add an EtherChannel, click Add, complete the fields as described in [Table 50](#), click Set, and then click Close.
- To edit an EtherChannel, click the Ellipses icon in the Edit column, modify the fields, click Set, and then click Close.
- To delete an EtherChannel, click the Trash icon in the Delete column.

Port	Use for EtherChannel
Gi1/1	<input type="checkbox"/>
Gi1/2	<input type="checkbox"/>
Gi1/3	<input type="checkbox"/>
Gi1/4	<input type="checkbox"/>
Gi1/5	<input type="checkbox"/>
Gi1/6	<input type="checkbox"/>
Gi1/7	<input type="checkbox"/>
Gi1/8	<input type="checkbox"/>

Table 50 - Add EtherChannel

Field	Description
EtherChannel	Choose a number to identify the EtherChannel.
Channel Mode	Choose a mode to determine how ports become active. With Link Aggregation Control Protocol, negotiations occur to determine which ports become active. Incompatible ports are put into an independent state and continue to carry data traffic, but do not participate in the EtherChannel. <b>IMPORTANT:</b> Make sure that all ports in an EtherChannel are configured with the same speed and duplex mode. For a description of each mode, see <a href="#">Table 47 on page 86</a> .
Port Members	To make a port a member of this EtherChannel, check its associated checkbox in the grid.

## Hot Standby Router Protocol (HSRP)

HSRP (Hot Standby Router Protocol) is a redundancy protocol to provide gateway redundancy without any additional configuration on the end devices in the subnet. With HSRP configured between a set of routers (treated as HSRP group or a standby group), they work together to present the appearance of a single virtual router to the hosts on the LAN.

### Configure HSRP via the WebUI

From the Configuration menu, choose Redundancy Protocols. From there, find the HSRP page and click Add.

[Configuration](#) > [Redundancy Protocols](#) > [HSRP](#)

[+ Add](#)
[× Delete](#)

Group	Interface	IPv4 Address	IPv6 Address	State
<div style="display: flex; align-items: center; justify-content: center;"> <span>⏪</span> <span>⏩</span> <span>0</span> <span>⏪</span> <span>⏩</span> </div> <div style="display: flex; align-items: center; justify-content: center; margin-top: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 5px;">10</div> <span>items per page</span> </div>				

From the Redundancy Protocol page, you can find the HSRP page. To configure the HSRP, click Add.

Create HSRP group
×

Group\*

0

HSRP Version\*

1 ▼

Interface\*

Vlan1 ▼

IP Options\*

☐

IPv4

Priority

100

NOTE: Switch with highest value becomes the active switch

Delay

0

Preempt

☐

Track Interface

None ▼

Interface Priority

10

Track object Number

1-1000

Type

line-protocol ▼

Hello Time

3

Hold Time

10

↶ Cancel

📄 Apply to Device

**Table 51 - HSRP Configuration Options**

Field	Description
Group	0...255
HSRP Version	<ul style="list-style-type: none"> <li>v1 (default)</li> <li>v2</li> </ul>
Interface	Layer 3 interface on which the HSRP will be enabled.
IP Options	The IP address of the hot standby router interface and optional secondary IP address.
Priority <sup>(1)</sup>	1...255 (default of 100)
Delay	0s ...3600s (default of 0)
Preempt	Choose a value to cause the local router to postpone taking over the active role for the configured number of seconds.
Track Interface <sup>(2)</sup>	Choose an interface for Track Interface.
Interface Priority	1...255 (default of 10)
Track Object Number	1...1000
Type	<ul style="list-style-type: none"> <li>line-protocol</li> <li>ip routing</li> <li>ipv6 routing</li> </ul>
Hello Time	1s...254s (default of 3)
Hold Time	4...255 (default of 10)

(1) The switch with the highest value becomes the active switch.

(2) If the line protocol of the specified interface goes down, the HSRP priority is reduced. This means that another HSRP router with higher priority can become the active router if that router has standby preempt enabled.

## Intermediate System-to-Intermediate System (IS-IS)

IS-IS is a link-state Interior Gateway Protocol (IGP). Link-state protocols create the information that is required to build a complete network connectivity map on each participating device. That map is then used to calculate the shortest path to destinations. IS-IS provides fast convergence, scalability, and efficient use of network bandwidth.

### Network Operation

IS-IS operates by reliably flooding link state information throughout a network of routers. Each IS-IS router independently builds a database of the network topology to aggregate the flooded network information. Like the Open Shortest Path First (OSPF) protocol, IS-IS uses an algorithm for computing the best path through the network. Packets (datagrams) are then forwarded based on the computed ideal path through the network to the destination.

Unlike other IP routing protocols, IS-IS runs directly on the data link layer (Layer 2). On Stratix 5800 switches, IS-IS supports route redistribution and load balancing.

To configure ISIS, you create an ISIS route and associate an interface.

### Configure IS-IS via the WebUI

From the Configuration menu, choose ISIS.



From the ISIS page, you can add, edit, and delete ISIS routes:

- To add an ISIS route, click Add, complete the fields as described in [Table 52](#), and then click Apply to device
- To edit an ISIS route, click the ISIS route in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an ISIS route, check its associated checkbox in the grid, and then click Delete.

Add Route

Router ISIS

Enter the name

Level \*

level-1

Interface

None

Net

Area

IP Address

Redistribute

IPv4

IPv6

Cancel

Apply to Device

Table 52 - Add Route

Field	Description
Router ISIS	Enter a name for the ISIS process.
Level	Choose a configuration for the ISIS router: <ul style="list-style-type: none"><li>level-1—The router acts as only a station router.</li><li>level-1-2—The router acts as both a station router and an area router.</li><li>level-2-only—The router acts as only an area router.</li></ul>
Interface	Choose an interface to route ISIS.
Net	The NET is the address of a Network Service Access Point (NSAP), which identifies an instance of the ISIS routing protocol running on an IS. Enter the Network Entity Title (NET) area and IP address for the routing process. Click the plus + sign to add the information to the grid.
Redistribute	Check each IP protocol to use for route redistribution.

Multicast Services

Multicast services include Internet Group Management Protocol (IGMP) snooping settings. Switches can use IGMP snooping to constrain the flooding of multicast traffic. IGMP snooping dynamically configures interfaces so that multicast traffic is forwarded to only those interfaces that are associated with IP multicast devices. For more information about IGMP snooping, see the Ethernet Reference Manual, publication [ENET-RM002](#).

Multicast services are supported on both Layer 2 and Layer 3 interfaces.

## Configure Multicast Services via the WebUI

From the Configuration menu, choose Multicast.

Configuration > Services > Multicast

IGMP Snooping Querier ENABLED

IGMP Snooping ENABLED

Last Member Querier Interval (milliseconds)

Apply

Complete the fields as described in [Table 53](#), and then click Apply to Device.

**Table 53 - Multicast**

Field	Description
IGMP Snooping Querier	Click to enable or disable IGMP snooping with querier. Default value: Enabled
IGMP Snooping	Click to enable or disable IGMP snooping. Default value: Enabled
Last Member Querier Interval (milliseconds)	To configure a last member query interval for IGMP snooping, enter a value in milliseconds. The query interval is the length of time after which a group record is deleted if no reports are received. Default value: 1000 ms

## NetFlow

NetFlow is an application that provides statistics on packets that flow through the switch. NetFlow applications include network traffic accounting, usage-based network billing, network planning, security, denial-of-service, and network monitoring.

---

**IMPORTANT** NetFlow is available only on select modular switch models. For supported catalog numbers, see [Table 1 on page 12](#).

---

A flow is a unidirectional stream of packets that have the same flow key values. NetFlow consists of these components:

- **Flow Record**—A flow record defines the unique keys that are used to identify packets in the flow, and other fields that NetFlow gathers for the flow. Device Manager provides predefined flow record templates that you can use to configure NetFlow and begin to monitor the network traffic.
- **Flow Monitor**—Flow monitors are applied to ports to perform network traffic monitoring. Flow data is collected from the network traffic and added to the flow monitor cache based on the key and nonkey fields in the flow record. You define the size of the data that you want to collect for a flow by using a monitor.

- **Flow Sampler**—Flow samplers are used to reduce the load on the switch that is running NetFlow by limiting the number of packets that are selected for analysis. Samplers use random sampling techniques.

Flow sampling exchanges monitoring accuracy for router performance. When you apply a sampler to a flow monitor, the overhead load on the switch that is running the flow monitor is reduced because the monitor must analyze fewer packets. The reduction in packets causes a corresponding reduction in the accuracy of the information that is stored in the cache of the flow monitor.

- **Flow Exporter**—You can export the data that NetFlow gathers for your flow by using an exporter. Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage.

There can be one record per monitor and one monitor per port. You can have multiple exporters per monitor. The flow records, flow monitor, flow exporter, and sampler cannot be modified once applied to a port.

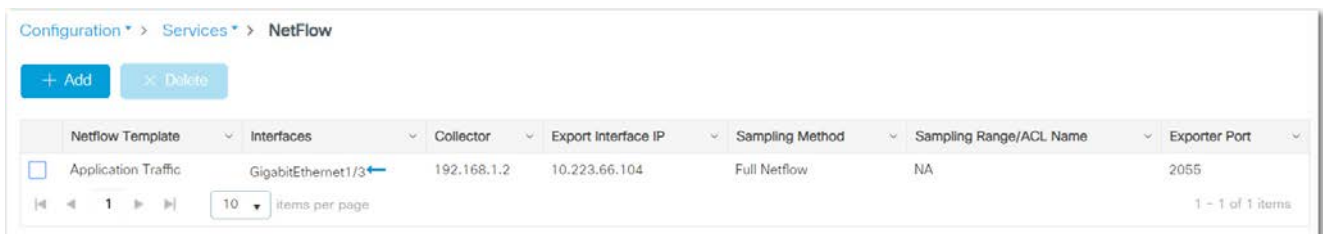
There are two primary methods to access NetFlow data:

- The command-line interface (CLI)—Use show commands to view data and troubleshoot.
- An application reporting tool—Export flows to a reporting server, which is known as a NetFlow collector. The NetFlow collector uses the flows to produce reports for traffic and security analysis.

For more information about NetFlow, see [www.cisco.com](http://www.cisco.com).

## Configure NetFlow via the WebUI

From the Configuration menu, choose NetFlow.



From the NetFlow page, you can add, edit, and delete NetFlow templates:

- To add a NetFlow template, click Add, complete the fields as described in [Table 54](#), and then click Apply to device
- To edit a NetFlow template, click the NetFlow template in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a NetFlow template, check its associated checkbox in the grid, and then click Delete.

**Table 54 - Create NetFlow**

Field	Description
Netflow Template	Choose a NetFlow template: <ul style="list-style-type: none"> <li>• Application Traffic—Monitors application traffic.</li> <li>• Server Utilization—Monitors packets to analyze server usage in the network.</li> <li>• Security—Monitors packets for network security.</li> <li>• Capacity Planning—Monitors packets to analyze network capacity and usage.</li> <li>• StealthWatch—Monitors packets to detect threats and security vulnerabilities.</li> </ul>
Collector Address	Enter the collector IP address of where to send the NetFlow data.
Exporter Port	Enter the port number on which your NetFlow collector is listening.
Export Interface IP	Choose e export address to use when sending the NetFlow data.
Interfaces	In the Available list, click the arrows to move interfaces to the Selected list to associate them with the NetFlow template.



## Network Address Translation (NAT)

NAT is a service that translates one IP address to another IP address via a NAT-configured switch. The switch translates the source and destination addresses within data packets as traffic passes between subnets.

---

**IMPORTANT** NAT is available only on select modular switch models. For supported catalog numbers, see [Table 1 on page 12](#).

---

This service is useful if you reuse IP addresses throughout a network. NAT enables devices that share one IP address on a private subnet to be segmented into multiple, identical private (inside) subnets while maintaining unique identities on the public (outside) subnet.<sup>(1)</sup>

The implementation of NAT in Stratix® switches is distinct in these ways:

- One-to-one NAT—The switch uses one-to-one NAT, rather than one-to-many NAT. One-to-one NAT requires that each source address translates to one unique destination address. Unlike one-to-many NAT, multiple source addresses cannot share a destination address.
- Layer 2 implementation—The implementation of NAT operates at the Layer 2 level. At this level, the switch can replace only IP addresses and does not act as a router.

See also the NAT Whitepaper, publication [ENET-WP032](#).

### Configuration Overview

To configure NAT, create one or more unique NAT instances. A NAT instance contains entries that define each address translation and other configuration parameters.

The translations that you define depend on whether traffic is routed through a Layer 3 switch or router or a Layer 2 switch.

---

**IMPORTANT** As a best practice, we recommend that you route traffic through a Layer 3 switch or router.

---

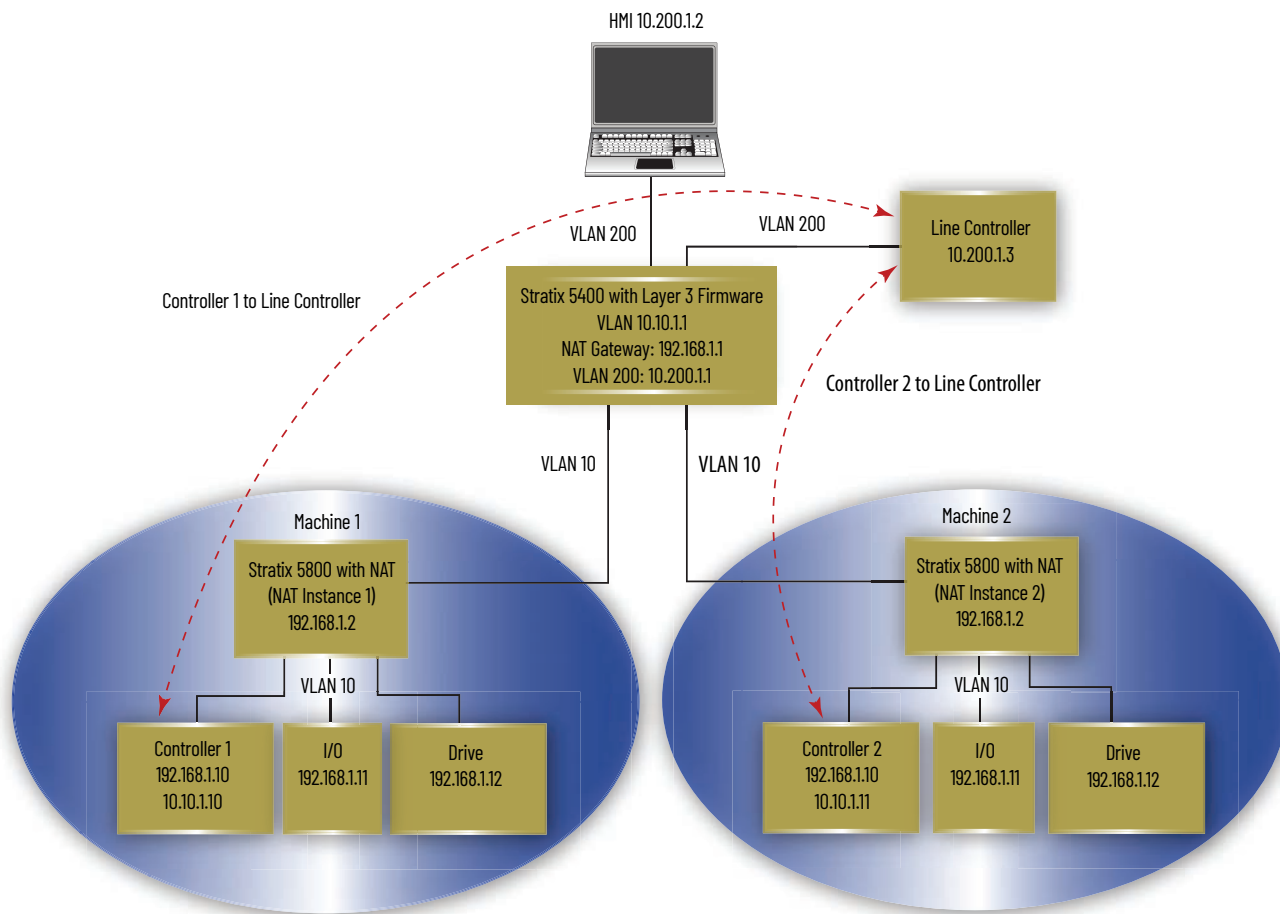
If traffic is routed through a Layer 3 switch or router ([Figure 19](#)), you define the following:

- A private-to-public translation for each device on the private subnet that communicates on the public subnet.<sup>(2)</sup>
- A gateway translation for the Layer 3 switch or router.

You do not need to configure NAT for all devices on the private subnet. For example, you can choose to omit some devices from NAT to increase security, decrease traffic, or conserve public address space. By default, untranslated packets are dropped at the NAT boundary.

(1) The terms private and public differentiate the two networks on either side of the NAT device. The terms do not mean that the public network must be Internet routable.

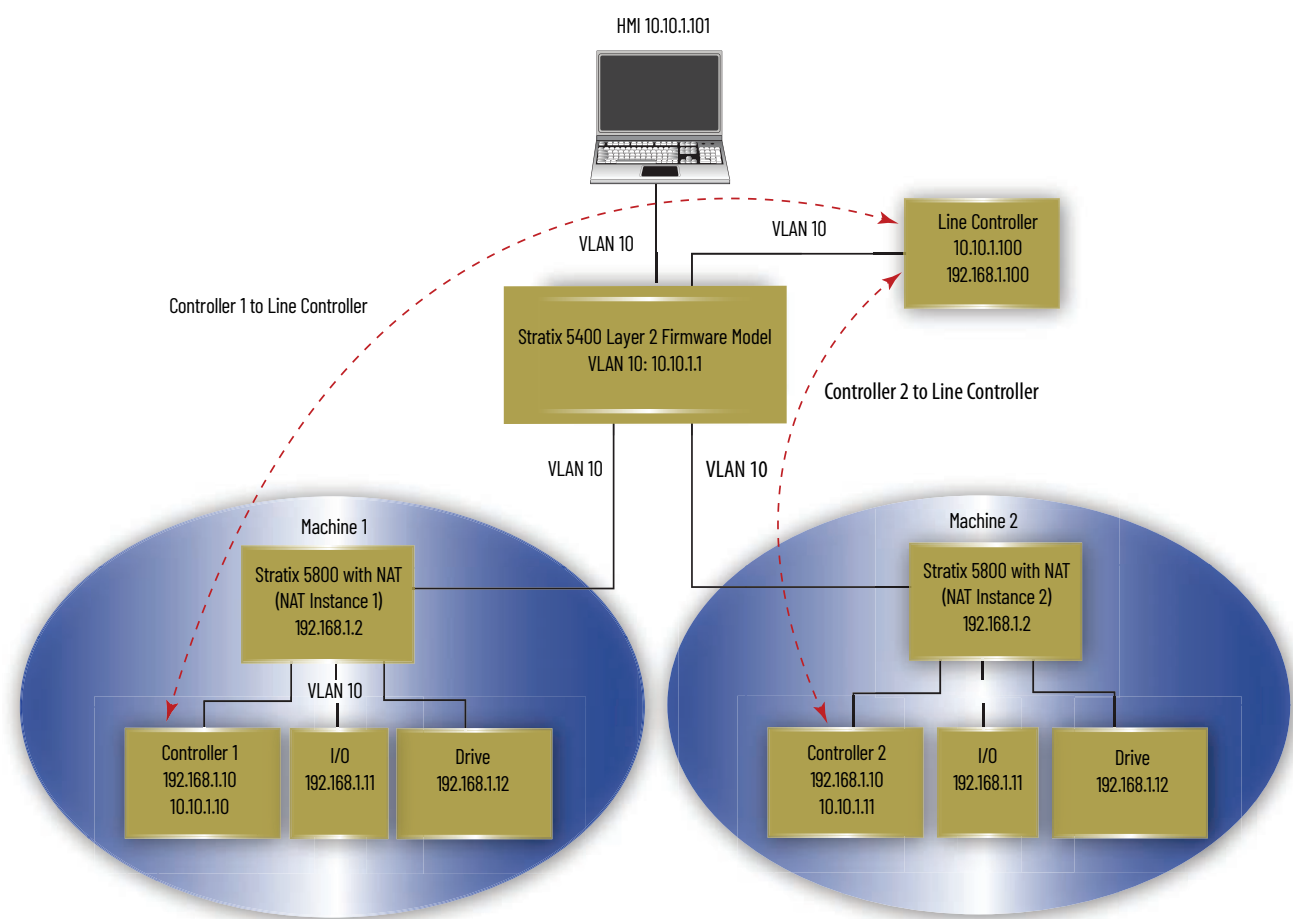
(2) Machines that communicate with each other within the same VLAN and subnet across a NAT boundary also require public-to-private translations.

**Figure 19 - Layer 3 Example with NAT in Stratix 5800 Switch**

If traffic is routed through a Layer 2 switch ([Figure 20](#)), you define the following.

- A private-to-public translation for each device on the private subnet that communicates on the public subnet.
- A public-to-private translation for each device on the public subnet that communicates on the private subnet.

Figure 20 - Layer 2 Example with NAT in Stratix 5800 Switch



An address translation can be one of three types. The type of translation determines the number of translation entries as shown in [Table 55](#).

Table 55 - Number of Translation Entries by Translation Type

Translation Type	Translation Entries	Description
Single	1	Translates one IP address. Consists of the following: <ul style="list-style-type: none"><li>• One private IP address</li><li>• One public IP address</li></ul>
Range	Multiple	Translates a range of IP addresses. Consists of the following: <ul style="list-style-type: none"><li>• One starting private IP address</li><li>• One starting public IP address</li><li>• Multiple entries that are based on the range you specify</li></ul>
Network	1	Translates all IP addresses within a subnet or portion of a subnet. Consists of the following: <ul style="list-style-type: none"><li>• One starting private IP address</li><li>• One starting public IP address that is aligned on valid subnet boundaries</li><li>• Subnet mask</li></ul>

---

**EXAMPLE** The following combination counts as 10 translation entries:

- Single translation for one device
- Range translation for eight devices
- Subnet translation for all devices on the subnet

Single and range translation types have a one-to-one relationship between translations entries and addresses to be translated. However, subnet translations have a one-to-many relationship that allows one translation entry for many addresses.

---

## VLAN Assignments

When configuring NAT, you can assign one or more VLANs to a NAT instance. When you assign a VLAN to a NAT instance, the traffic that is associated with that VLAN is subject to the configuration parameters of the NAT instance. Configuration parameters include whether traffic is translated, fixed up, blocked, or passed through.

---

**IMPORTANT** Changes to the native VLAN on a port that is assigned to a NAT instance can break existing NAT configurations. If you change the VLAN assigned to a port associated with a NAT instance, you must reassign VLANs to that NAT instance.

Make sure all VLANs and Smartport roles are configured before NAT configuration.

---

When assigning VLANs to a NAT instance, consider the following.

- NAT supports both trunk ports and access ports.
- NAT does not change VLAN tags.
- You can assign a maximum of 128 VLANs to one or more instances.
- You can assign the same VLAN to multiple instances as long as the VLAN is associated with different ports. For example, you can assign VLAN 1 to both instance A and instance B. However, VLAN 1 must be associated with port Gi1/1 on instance A and port Gi1/2 on instance B.
- By default, each instance is assigned to all VLANs on port Gi1/1 and no instances on port Gi1/2.

VLANs associated with a trunk port can or cannot be assigned to a NAT instance:

- If a VLAN is assigned to a NAT instance, its traffic is subject to the configuration parameters of the NAT instance.
- If a VLAN is unassigned to a NAT instance, its traffic remains untranslated and is always permitted to pass through the trunk port.

### *Management Interface and VLANs*

The management interface can be associated with a VLAN that is or is not assigned to a NAT instance:

- If its associated VLAN is assigned to a NAT instance, the management interface resides on the private subnet by default. To manage the switch from the private subnet, no additional configuration is required. To manage the switch from the public subnet, you must configure a private-to-public translation.
- If its associated VLAN is not assigned to a NAT instance, the traffic of the management interface remains untranslated and is always permitted to pass through the port.

### **Traffic Permits and Fixups**

While a NAT-configured port can translate many types of traffic, only unicast and broadcast traffic are supported. You can choose to block or pass through the following unsupported traffic types.

- Untranslated unicast traffic
- Multicast traffic
- IGMP traffic

Use caution when you configure traffic permits and fixups. We recommend that you use the default settings. By default, all preceding traffic types are blocked.

Some traffic types must be fixed up to work properly with NAT because their packets contain embedded IP addresses. The switch supports fixups for these traffic types:

- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)

By default, fixups are enabled for both ARP and ICMP.

## Requirements and Restrictions

Before configuring NAT, know the following requirements and restrictions:

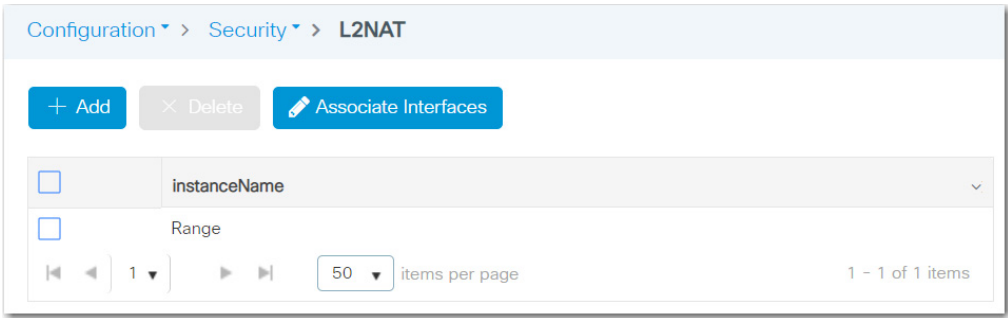
- Available interfaces for NAT instances are Gi1/1 and Gi1/2. Both interfaces are SFP slots.
- Some NAT configurations can result in greater-than-expected traffic loads on both private and public subnets. Also, unintended traffic can be visible. NAT is not a substitute for a firewall. Make sure that your configuration is performance qualified before use in a production environment.
- Configure all Smartport roles and VLANs before creating NAT instances. If you change a Smartport role or the native VLAN for a port that is associated with a NAT instance, you must reassign VLANs to the NAT instance.
- As a result of Layer 2 forwarding, current traffic sessions remain established until manually disconnected. If you change an existing translation, you must manually disconnect all associated traffic sessions before the new translation can take effect.
- The switch can translate only IPv4 addresses.
- The switch can have a maximum of 128 NAT instances and 128 translation entries across all NAT ports. Note that a subnet translation counts as only one translation entry, but includes translations for many devices.

Ports that are configured for NAT do **not** support the following across the NAT boundary due to embedded IP addresses that are not fixed up, encrypted IP addresses, or reliance on multicast traffic:

- Traffic encryption and integrity-checking protocols incompatible with NAT, including IPsec Transport mode (1756-EN2TSC module)
- Applications that use dynamic session initiations, such as NetMeeting
- File Transfer Protocol (FTP)
- Microsoft® Distributed Component Object Model (DCOM), which is used in Open Platform Communications (OPC)
- Multicast traffic, including applications that use multicast, such as CIP Sync™ (IEEE1588) and ControlLogix redundancy

## Configure NAT via the WebUI

From the Configuration menu, choose L2NAT.



From the L2NAT page, you can add, edit, and delete NAT instances and associate NAT instances with interfaces and VLANs:

- To add a NAT instance, proceed to [page 104](#).
- To edit a NAT instance, click the instance in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a NAT instance, check its associated checkbox in the grid, and then click Delete.
- To associate a NAT instance with an interface and VLANs, proceed to [page 107](#).

### Add NAT Instances

1. From the L2 NAT page, click Add.
2. In the Name field, enter a unique name to identify the instance.  
When editing a NAT instance, you cannot change this field.
3. On the Translations tab, define translations based on your application, and then click Apply to Device.

For information about how to complete the Inside and Outside fields, refer to the corresponding descriptions in [Table 56 on page 105](#).

Application	Required Translations
Traffic is routed through a Layer 3 switch or router, as shown in <a href="#">Figure 19 on page 99</a>	<div>A private-to-public (inside) translation for each device in the private subnet that communicates on the public subnet. a. From the Inside pull-down menu, choose a translation type, and then complete the fields to the right. b. Click the plus sign (+) to add the translation to the grid. c. Repeat these steps for each device that requires a translation entry.</div> <div>A single gateway (outside) translation for the Layer 3 switch or router. a. From the Outside pull-down menu, choose a translation type, and then complete the fields to the right. b. Check Gateway. c. Click the plus sign (+) to add the translation to the grid. d. Repeat these steps for to add the gateway translation to the grid.</div>
Traffic is routed through a Layer 2 switch, as shown in <a href="#">Figure 20 on page 100</a>	<div>A private-to-public (inside) translation for each device in the private subnet that communicates on the public subnet. a. From the Inside pull-down menu, choose a translation type, and then complete the fields to the right. b. Click the plus sign (+) to add the translation to the grid. c. Repeat these steps for to add the translation to the grid. d. Repeat these steps for each device that requires a translation entry.</div> <div>A public-to-private (outside) translation for each device on the public subnet that communicates on the private subnet. a. From the Outside pull-down menu, choose a translation type, and then complete the fields to the right. b. Make sure that the Gateway checkbox is cleared, and then click the plus sign (+) to add the translation to the grid. c. Repeat these steps for to add the translation to the grid. d. Repeat these steps for each device that requires a translation entry.</div>

Configure Nat Instance

Name\*

Translations    Advanced

Inside
Single
xxx.xxx.xxx.xxx
\*
xxx.xxx.xxx.xxx
\*
2-128
xxx.xxx.xxx.xxx
+

Translation Type
Private IP
Public IP
Range
Mask
0

Outside
Single
xxx.xxx.xxx.xxx
\*
xxx.xxx.xxx.xxx
\*
2-128
xxx.xxx.xxx.xxx
☐ Gateway +

Translation Type
Public IP
Private IP
Range
Mask
Gateway
0

Cancel
Apply to Device

Table 56 - Configure NAT Instance Grids—Translations Tab

Field	Description
<b>Inside</b> (private-to-public translations)	
Translation Type	<p>The type of translation:</p> <ul style="list-style-type: none"> <li>Single—Translates one private address to one public address.</li> <li>Network—Translates all or a portion of the addresses in the private subnet to addresses on the public subnet.</li> <li>Range—Translates many sequential private addresses to many sequential public addresses.</li> </ul>
Private IP	<p>For single translation types, this is the existing address for the device on the private subnet.</p> <p>For network translation types, this is the network address for the private subnet. This address must correspond to the size of the subnet mask to translate. See <a href="#">Table 57</a>.</p> <p>For range translation types, this is the first address in the range of sequential addresses.</p>
Public IP	<p>For single translation types, this is the unique public address to represent the device.</p> <p>For network translation types, this is the network address for the public subnet. This address must correspond to the size of the subnet mask to translate. See <a href="#">Table 57</a>.</p> <p>For range translation types, this is the first address in the range of sequential addresses.</p>
Range	<p>(Applies only to Range translation types). The number of addresses to translate.</p> <p><b>IMPORTANT:</b> Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.</p>
Mask	(Applies only to Network translation types). The subnet mask for the addresses to translate.
<b>Outside</b> (public-to-private translations)	
Translation Type	<p>The type of translation:</p> <ul style="list-style-type: none"> <li>Single—Translates one public address to one private address.</li> <li>Network—Translates all or a portion of the addresses in the public subnet to addresses on the private subnet.</li> <li>Range—Translates many sequential public addresses to many sequential private addresses.</li> </ul>
Public IP	<p>For single translation types, this is the unique public address to represent the device.</p> <p>For network translation types, this is the network address for the public subnet. This address must correspond to the size of the subnet mask to translate. See <a href="#">Table 57</a>.</p> <p>For range translation types, this is the first address in the range of sequential addresses.</p>
Private IP	<p>For single translation types, this is the existing address for the device on the private subnet.</p> <p>For network translation types, this is the network address for the private subnet. This address must correspond to the size of the subnet mask to translate. See <a href="#">Table 57</a>.</p> <p>For range translation types, this is the first address in the range of sequential addresses.</p>



**Table 56 - Configure NAT Instance Grids—Translations Tab (Continued)**

Field	Description
Range	(Applies only to Range translation types). The number of addresses to translate. <b>IMPORTANT:</b> Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.
Mask	(Applies only to Network translation types). The subnet mask for the addresses to translate.
Gateway	Indicates whether the translation is a gateway translation. A gateway translation enables devices on the public subnet to communicate with devices on different VLANs on the private subnet. Valid values: <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul>

**Table 57 - Subnet Mask Starting Address**

Subnet Mask	Subnet Address
255.255.0.0	The last two octets must end in 0. <b>EXAMPLES:</b> 192.168.0.0 or 10.200.0.0
255.255.255.0	The last octet must end in 0. <b>EXAMPLES:</b> 192.168.1.0 or 10.200.1.0.
255.255.255.128	The last octet must end in 0 or 128. <b>EXAMPLES:</b> 192.168.1.0 or 192.168.1.128; 10.200.1.0 or 10.200.1.128
255.255.255.192	The last octet must end in one of the following: 0, 64, 128, 192. <b>EXAMPLES:</b> 192.168.1.64 or 10.200.1.64
255.255.255.224	The last octet must end in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. <b>EXAMPLES:</b> 192.168.1.32 or 10.200.1.32
255.255.255.240	The last octet must end in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. <b>EXAMPLES:</b> 192.168.1.16 or 10.200.1.16

- To configure traffic permits and packet fixups, click the Advanced tab, configure the fields as described in [Table 58](#), and then click Apply to Device.

**Configure Nat Instance**

Name\*

Translations    **Advanced**

**PERMIT**

All ☐

None ☐

**FIXUP**

All ☒

None ☐

**Table 58 - Configure NAT Instance—Advanced Tab**

Field	Description
PERMIT	Only unicast traffic is subject to translation. By default, all unmatched, multicast, and IGMP packets are dropped. Specify how to handle packets that are not handled by NAT: <ul style="list-style-type: none"> <li>All—Check to permit the packets to pass across the NAT boundary.</li> <li>None—Check to drop the packets.</li> </ul>
FIXUP	Protocols, such as ARP and ICMP, do not work transparently across the NAT boundary. By default, these protocols are fixed up to support translations. Specify whether to enable or disable fixups for protocol packets: <ul style="list-style-type: none"> <li>All—Check to enable fixups for all protocol packets.</li> <li>None—Check to disable fixups for all protocol packets.</li> </ul>

### Associate NAT Instances with Interfaces and VLANs

1. From the L2 NAT page, click Associate Interfaces.
2. From the Interfaces pull-down menu, choose the NAT instance to associate with interfaces and VLANs.
3. In the list of available interfaces, select GigabitEthernet1/1 or GigabitEthernet1/2.
4. On the right, specify the VLANs to associate with the NAT instance, and then click Apply to Device.

Field	Description
VLAN IDs	Enter a single VLAN ID or a range of VLAN IDs, such as 2, 4, or 6-10.
Native VLAN ID	Displays the native VLAN for the selected interface.
Associated Instances	Instances that specify the address translations.

Associate Interfaces

Instances

Range

Click on an Interface from the Available Interfaces to get and set the instance vlans

Available Interfaces

Search

GigabitEthernet1/1

GigabitEthernet1/2

GigabitEthernet1/1

Vlan IDs

2-4094

(e.g., 2,4,6-10)

Native VLAN ID

3680

Associated Instances

None

up

down

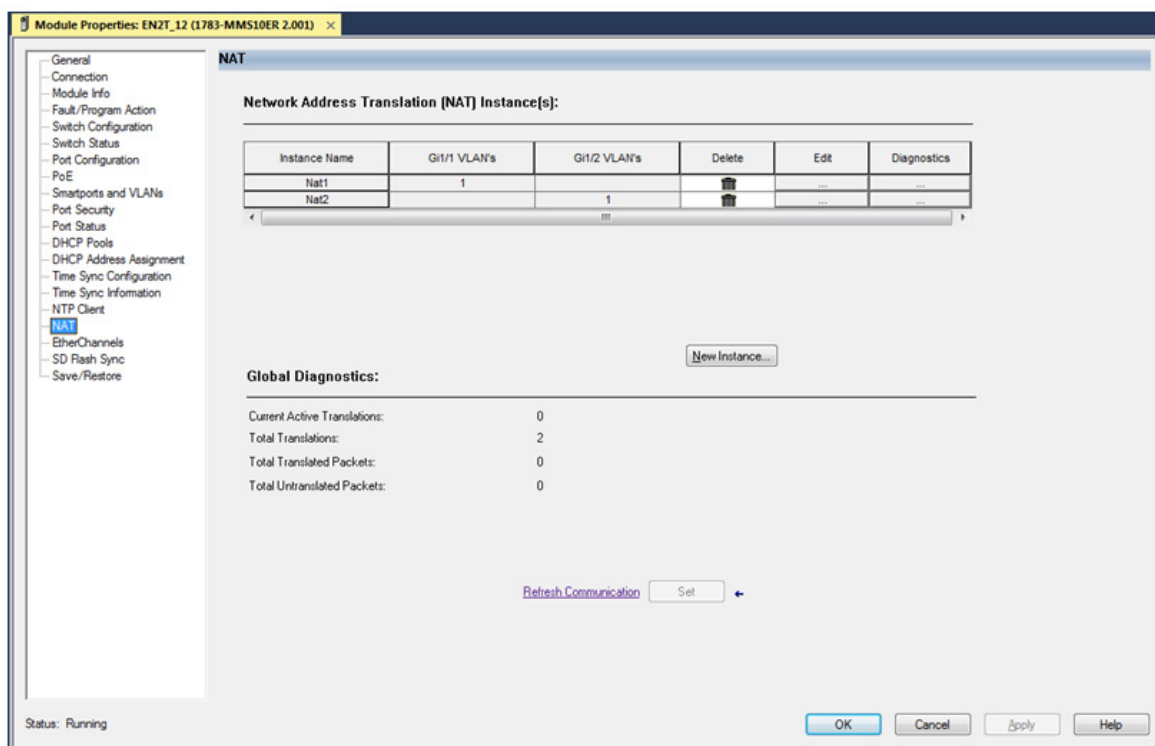
administratively down

Cancel

Apply to Device

## Configure NAT via the Logix Designer Application

In the navigation pane, click NAT.



On the NAT view, you can add, edit, delete, and monitor NAT instances:

- To add a NAT instance, click New Instance, and then proceed to [page 109](#).
- To edit a NAT instance, click the Ellipses icon in the Edit column, modify the fields, and then click Close.
- To delete a NAT instance, click the Trash icon in the Delete column.
- To monitor NAT statistics, see [page 233](#).

### Add NAT Instances

1. From the NAT view, click New Instance to display the New Instance dialog box.

NAT Instance: New Table

General Public to Private Advanced

Name: NAT1

**Private to Public NAT Table:**  
Provide Private subnet devices unique IP addresses on the Public subnet.

	Private	Public	Subnet Mask	Delete
*	192.1.0.0	10.0.0.0		

VLAN Association

Gi1/1 ☒ 1

Gi1/2 ☐ 1

Gateway Translation:

Public: . . .

Private: . . .

New Entry

Refresh Communication Set

Close Help

2. In the Name field, type a unique name to identify the instance.  
The instance name cannot include spaces or exceed 32 characters.
3. In the VLAN Association area, check the checkbox next to each VLAN to assign to the instance.  
For more information about VLAN assignments, see [page 101](#).
4. Define translations based on your application as described in [Table 59](#).
5. To configure traffic permits and packet fixups for the instance, see [page 113](#).
6. Click Set.

New Entry—Private to Public Translation

Provide "Private" subnet devices unique IP addresses on the "Public" subnet.

Number of Entries Available: 128

Type of Entry: Single

Starting Private IP Address: . . .

Starting Public IP Address: . . .

Range: 1

Subnet Mask: 255.255.255.0

Effective Private Addresses:

Effective Public Addresses:

OK Cancel Help

New Entry—Public to Private Translation

Provide "Public" subnet devices unique IP addresses on the "Private" subnet.

Number of Entries Available: 127

Type of Entry: Single

Starting Public IP Address: 10 . 0 . 0 . 0

Starting Private IP Address: 192 . 0 . 0 . 0

Range: 1

Subnet Mask: 255.255.255.0

Effective Public Addresses: 10.0.0.0

Effective Private Addresses: 192.0.0.0

OK Cancel Help

**Table 59 - Translations Required by Application**

Application	Required Translations
Traffic is routed through a Layer 3 switch or router, as shown in <a href="#">Figure 19 on page 99</a>	<p>A private-to-public (inside) translation for each device in the private subnet that communicates on the public subnet.</p> <ol style="list-style-type: none"> <li>On the General tab, click New Entry.</li> <li>Do one of the following: <ul style="list-style-type: none"> <li>To translate one address for a device on the private subnet that communicates on the public subnet, see <a href="#">Table 60</a>.</li> <li>To translate a range of addresses for devices on the private subnet that communicates on the public subnet, see <a href="#">Table 61</a>.</li> <li>To translate all addresses in the private subnet or a portion of the private subnet, see <a href="#">Table 62</a>.</li> </ul> </li> <li>Click OK.</li> </ol> <p>A single gateway (outside) translation for the Layer 3 switch or router.</p> <ol style="list-style-type: none"> <li>In the Gateway Translations Public field, enter the default gateway address of the Layer 3 switch or router that is connected to the uplink port of the switch.</li> <li>In the Gateway Translations Private field, enter a unique IP address to represent the Layer 3 switch or router on the private network.</li> <li>Click OK.</li> </ol>
Traffic is routed through a Layer 2 switch, as shown in <a href="#">Figure 20 on page 100</a>	<p>A private-to-public (inside) translation for each device in the private subnet that communicates on the public subnet.</p> <ol style="list-style-type: none"> <li>On the General tab, click New Entry.</li> <li>Do one of the following: <ul style="list-style-type: none"> <li>To translate one address for a device on the private subnet that communicates on the public subnet, see <a href="#">Table 60</a>.</li> <li>To translate a range of addresses for devices on the private subnet that communicates on the public subnet, see <a href="#">Table 61</a>.</li> <li>To translate all addresses in the private subnet or a portion of the private subnet, see <a href="#">Table 62</a>.</li> </ul> </li> </ol> <p>A public-to-private (outside) translation for each device on the public subnet that communicates on the private subnet.</p> <ol style="list-style-type: none"> <li>Click the Public to Private tab.</li> <li>Click New Entry.</li> <li>Do one of the following: <ul style="list-style-type: none"> <li>To translate one address for a device on the public subnet that communicates on the private subnet, see <a href="#">Table 63</a>.</li> <li>To translate a range of addresses for devices on the public subnet that communicates on the private subnet, see <a href="#">Table 64</a>.</li> <li>To translate all addresses on the public subnet or a portion of the public subnet that communicate on the private subnet, see <a href="#">Table 65</a>.</li> </ul> </li> <li>Click OK.</li> </ol>

**Table 60 - Single Translation—Private to Public Translation**

Field	Description
Type of Entry	Choose Single. Single is the default value.
Starting Private IP Address	Type the existing address for the device on the private subnet.
Starting Public IP Address	Type a unique public address to represent the device.
Effective Private Addresses	Displays the existing address for the device on the private subnet that is configured for translation. If blank, verify that the values in the preceding fields are valid.
Effective Public Addresses	Displays the unique public address to represent the device. If blank, verify that the values in the preceding fields are valid.

**Table 61 - Range Translation—Private to Public Translation**

Field	Description
Type of Entry	Choose Range.
Starting Private IP Address	Type the existing starting address for the device on the private subnet.
Starting Public IP Address	Type a unique, starting public address to represent the device.
Range	Type the number of addresses to include in the range. Valid values: 2...128 Default value = 1 <b>IMPORTANT:</b> Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.
Effective Private Addresses	Displays the range of existing addresses for devices on the private subnet that are configured for translation. If blank, verify that the values in the preceding fields are valid.
Effective Public Addresses	Displays the range of unique public addresses to represent the devices. If blank, verify that the values in the preceding fields are valid.

**Table 62 - Network Translation—Private to Public Translation**

Field	Description
Type of Entry	Choose Subnet.
Starting Private IP Address	Type the existing starting address for a device on the private subnet. This address must correspond to the size of the subnet mask to translate. See <a href="#">Table 66</a> .
Starting Public IP Address	Type a unique, starting public address to represent the devices. This address must correspond to the size of the subnet mask to translate. See <a href="#">Table 66</a> .
Subnet Mask	Choose the subnet mask for the addresses to translate. Valid values: <ul style="list-style-type: none"> <li>• 255.255.0.0</li> <li>• 255.255.255.0</li> <li>• 255.255.255.128 (provides 128 addresses per translation entry)</li> <li>• 255.255.255.192 (provides 64 addresses per translation entry)</li> <li>• 255.255.255.224 (provides 32 addresses per translation entry)</li> <li>• 255.255.255.240 (provides 16 addresses per translation entry)</li> </ul>
Effective Private Addresses	Displays the range of existing addresses for devices on the private subnet that are configured for translation. If blank, verify that the values in the preceding fields are valid.
Effective Public Addresses	Displays the range of unique public addresses to represent the devices. If blank, verify that the values in the preceding fields are valid.

**Table 63 - Single Translation—Public to Private Translation**

Field	Description
Type of Entry	Choose Single. Single is the default value.
Starting Public IP Address	Type the existing address for the device on the public subnet.
Starting Private IP Address	Type a unique private address to represent the device.
Effective Public Addresses	Displays the existing address for the device on the public subnet that is configured for translation. If blank, verify that the values in the preceding fields are valid.
Effective Private Addresses	Displays the unique private address to represent the device. If blank, verify that the values in the preceding fields are valid.

**Table 64 - Range Translation—Public to Private Translation**

Field	Description
Type of Entry	Choose Range.
Starting Public IP Address	Type the existing starting address for the device on the public subnet.
Starting Private IP Address	Type a unique, starting private address to represent the devices.
Range	Type the number of addresses to include in the range. Valid values: 2...128 Default value = 1 <b>IMPORTANT:</b> Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.
Effective Public Addresses	Displays the range of existing addresses for devices on the public subnet that are configured for translation. If blank, verify that the values in the preceding fields are valid.
Effective Private Addresses	Displays the range of unique private addresses to represent the devices. If blank, verify that the values in the preceding fields are valid.

**Table 65 - Network Translation—Public to Private Translation**

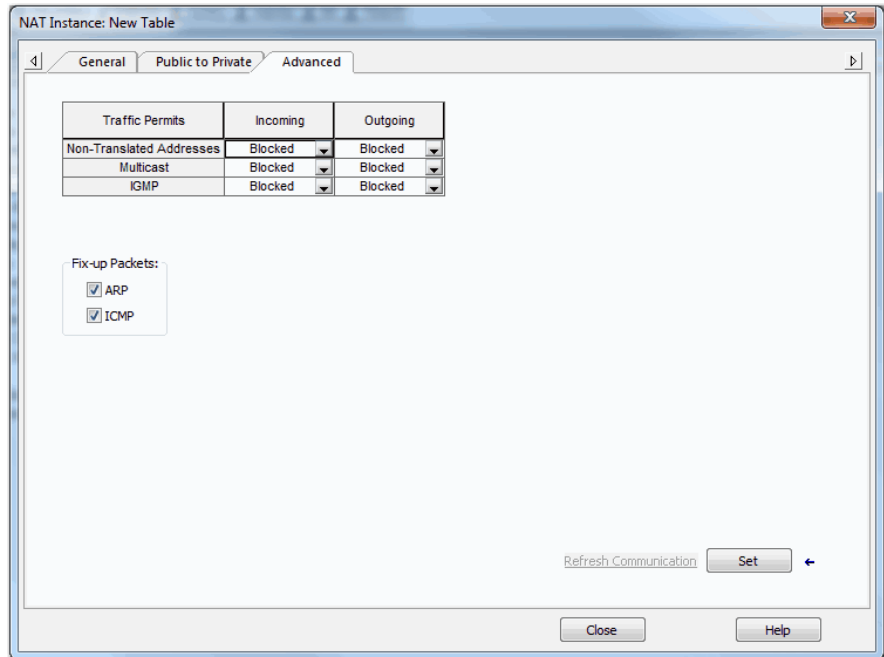
Field	Description
Type of Entry	Choose Subnet.
Starting Public IP Address	Type the existing starting address for a device on the public subnet. This address must correspond to the size of the subnet mask to translate. See <a href="#">Table 66</a> .
Starting Private IP Address	Type a unique, starting private address to represent the devices. This address must correspond to the size of the subnet mask to translate. See <a href="#">Table 66</a> .
Subnet Mask	Choose the subnet mask for the addresses to translate. Valid values: <ul style="list-style-type: none"> <li>• 255.255.0.0</li> <li>• 255.255.255.0</li> <li>• 255.255.255.128 (provides 128 addresses per translation entry)</li> <li>• 255.255.255.192 (provides 64 addresses per translation entry)</li> <li>• 255.255.255.224 (provides 32 addresses per translation entry)</li> <li>• 255.255.255.240 (provides 16 addresses per translation entry)</li> </ul>
Effective Public Addresses	Displays the range of existing addresses for devices on the public subnet that are configured for translation. If blank, verify that the values in the preceding fields are valid.
Effective Private Addresses	Displays the range of unique private addresses to represent the devices. If blank, verify that the values in the preceding fields are valid.

**Table 66 - Subnet Mask Starting Address**

Subnet Mask	Subnet Address
255.255.0.0	The last two octets must end in 0. <b>EXAMPLES:</b> 192.168.0.0 or 10.200.0.0
255.255.255.0	The last octet must end in 0. <b>EXAMPLES:</b> 192.168.1.0 or 10.200.1.0.
255.255.255.128	The last octet must end in 0 or 128. <b>EXAMPLES:</b> 192.168.1.0 or 192.168.1.128; 10.200.1.0 or 10.200.1.128
255.255.255.192	The last octet must end in one of the following: 0, 64, 128, 192. <b>EXAMPLES:</b> 192.168.1.64 or 10.200.1.64
255.255.255.224	The last octet must end in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. <b>EXAMPLES:</b> 192.168.1.32 or 10.200.1.32
255.255.255.240	The last octet must end in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. <b>EXAMPLES:</b> 192.168.1.16 or 10.200.1.16

### Configure Traffic Permits and Fixups

1. From the NAT Instance view, click the Advanced tab.



2. In the Traffic Permits table, choose one of these options for unsupported incoming and outgoing packets:
  - Pass-Through—Permit the packets to pass across the NAT boundary.
  - Blocked—Drop the packets.
3. In the Fix-up Packets area, check or clear the checkboxes to enable or disable protocol fixups for ARP and ICMP.  
By default, fixups are enabled for both ARP and ICMP.
4. Click Set.

## Open Shortest Path First (OSPF) Routing Protocol

OSPF is a standards-based routing protocol that uses the Shortest Path First (SPF) algorithm to determine the best route to its destination. Each router in an OSPF area contains an identical link-state database, which is a list of each of the router usable interfaces and reachable neighbors.

---

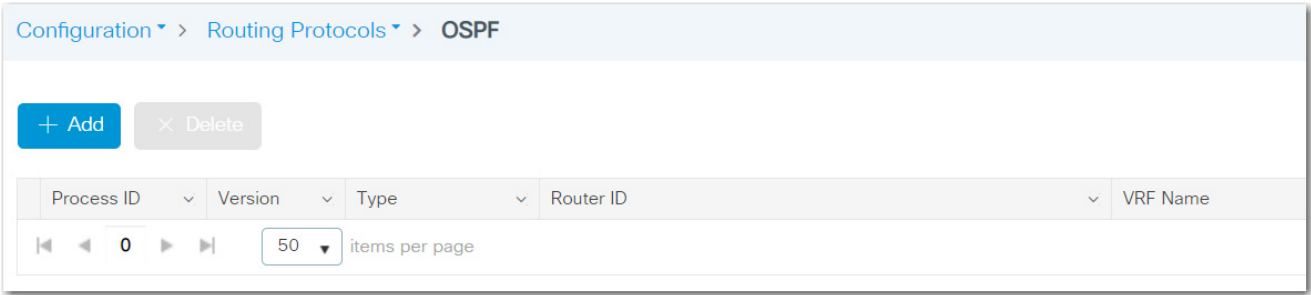
**IMPORTANT** OSPF is available only on select modular switch models. For supported catalog numbers, see [Table 1 on page 12](#).

---



## Create an OSPF Route via the WebUI

From the Configuration menu, choose OSPF.



From the OSPF page, you can add, edit, and delete OSPF routes:

- To add a route, click Add, complete the fields as described in [Table 67](#) for OSPF or [Table 68](#) for OSPFv3, and then click Apply to Device.
- To edit a route, click the route in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a route, check its associated checkbox in the grid, and then click Delete.

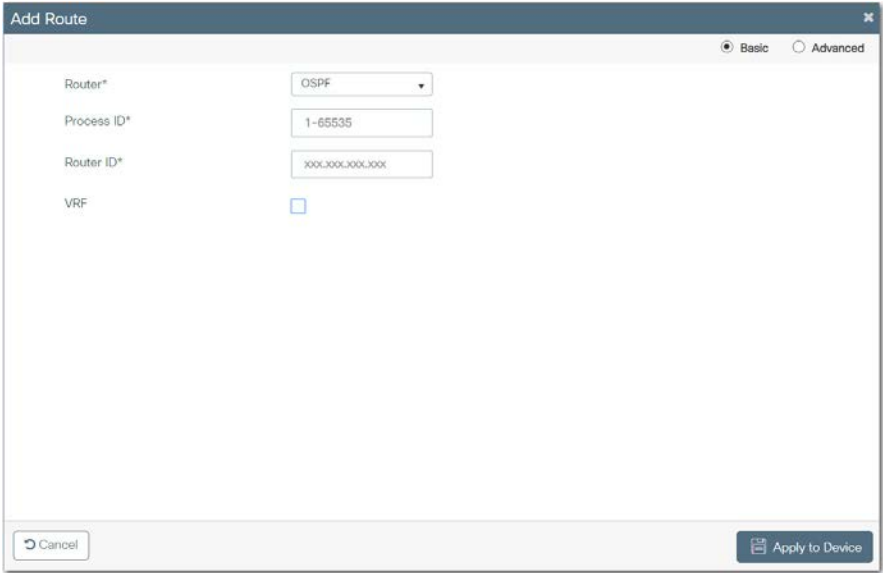


Table 67 - Add Route—OSPF

Field	Description
<b>Basic or Advanced</b>	Click to determine the level of configuration: <ul style="list-style-type: none"><li>• Basic—The page displays only basic configuration fields. Basic is the default value.</li><li>• Advanced—The page displays both basic and advanced configuration fields.</li></ul>
<b>Basic Settings</b>	
Router	Choose OSPF.
Process ID	Enter a unique process ID to enable other routers to identify the OSPF routing process of this router.
Router ID	Enter a unique router ID for the OSPF process.

**Table 67 - Add Route—OSPF**

Field	Description
VRF	To create a virtual routing and forwarding (VRF) interface for the OSPF process, check the VRF checkbox, and then enter a name to identify the VRF interface.
<b>Advanced Settings</b>	
Network	<ol style="list-style-type: none"> <li>1. In the IP Address field, enter the IP address of the destination network for this route.</li> <li>2. In the Wildcard field, enter the subnet mask used on that network.</li> <li>3. In the Area field, enter the OSPF area number for the network. Each router in a particular OSPF area maintains a topological database for that area.</li> <li>4. Click + to add the network information to the grid.</li> </ol>

**Table 68 - Add Route—OSPFv3**

Field	Description
<b>Basic or Advanced</b>	Click to determine the level of configuration: <ul style="list-style-type: none"> <li>• Basic—The page displays only basic configuration fields. Basic is the default value.</li> <li>• Advanced—The page displays both basic and advanced configuration fields.</li> </ul>
<b>Basic Settings</b>	
Router	Enter a unique process ID to enable other routers to identify the OSPFv3 routing process of this router.
Process ID	Enter a unique router ID for the OSPFv3 process.
Router ID	<ol style="list-style-type: none"> <li>1. Enter a unique router ID for the OSPFv3 process.</li> <li>2. Choose IPv4, IPv6, or IPv4/IPv6.</li> </ol>
<b>Address Family</b>	
VRF	A VRF must be created based on type (IPv4, IPv6 and IPv4/IPv6) if none is available in the device. Otherwise, the VRF option is not selectable. Check VRF to specify an OSPF VPN routing and forwarding (VRF) instance, and then enter the VRF name.
Router ID	Enter the IP address of the router associated with the OSPFv3 route.
<b>Advanced Settings</b>	
Area	<ol style="list-style-type: none"> <li>1. In the Area field, enter the OSPF area number for the network. Each router in a particular OSPF area maintains a topological database for that area.</li> <li>2. Choose Stub. Stub areas are areas into which information on external routes is not sent.</li> <li>3. Click + to add the area information to the table.</li> </ol>

# Parallel Redundancy Protocol (PRP)

PRP is defined in international standard IEC 62439-3 and provides high-availability in Ethernet networks. PRP technology creates seamless redundancy by sending duplicate frames to two independent network infrastructures, which are known as LAN A and LAN B.

A PRP network includes the following components.

Component	Description
LAN A and LAN B	Redundant, active Ethernet networks that operate in parallel.
Double attached node (DAN)	An end device with PRP technology that connects to both LAN A and LAN B.
Single attached node (SAN)	An end device without PRP technology that connects to either LAN A or LAN B. A SAN does not have PRP redundancy.
Redundancy box (RedBox)	A switch with PRP technology that connects devices without PRP technology to both LAN A and LAN B.
Virtual double attached node (VDAN)	An end device without PRP technology that connects to both LAN A and LAN B through a RedBox. A VDAN has PRP redundancy and appears to other nodes in the network as a DAN.
Infrastructure switch	A switch that connects to either LAN A or LAN B and is not configured as a RedBox.

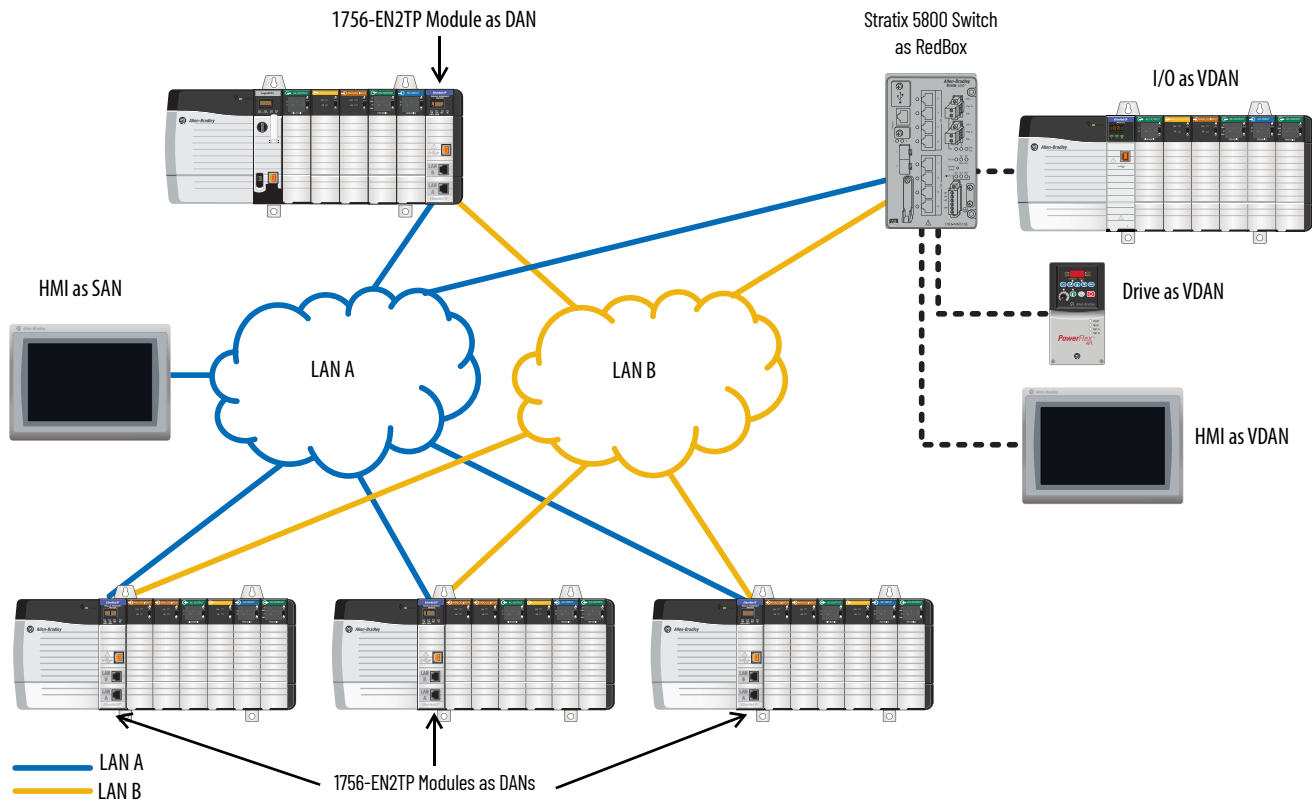
For more information about PRP, see the EtherNet/IP Parallel Redundancy Protocol Application Technique, publication [ENET-AT006](#).

**IMPORTANT** PRP is available only on select modular switch models. For supported catalog numbers, see [Table 1 on page 12](#).

[Figure 21](#) illustrates the Stratix 5800 switch as RedBox.

**IMPORTANT** Before connecting the cables between devices in a PRP system, complete the configuration of the devices.

Figure 21 - PRP Topology with Stratix 5400 Switch as RedBox



## RedBox PRP Channel Groups

For RedBox functionality, Stratix 5800 switches have designated ports for PRP channel groups. A PRP channel or channel group is a logical interface that aggregates two Gigabit Ethernet interfaces (access, trunk, or routed) into a single link. In the channel group, the lower numbered Gigabit Ethernet member port is the primary port and connects to LAN A. The higher numbered port is the secondary port and connects to LAN B. The PRP channel remains up as long as at least one of these member ports remains up and sends traffic. When both member ports are down, the channel is down. The total number of supported PRP channel groups is 2 per switch.

There are two pairs of port than can be used for channel group 1:

- Gi1/1 and Gi1/2
- Gi1/3 and Gi1/4

Channel 2 can only be configured on a 1783-MMX8EA or 1783-MMX8SA expansion module. The only two ports that can be used are Gi2/1 and Gi2/2.

## Traffic and Supervisory Frames

Traffic that egresses the RedBox PRP channel group can be destined to either SANs connected only on either LAN A or LAN B or to DANs. To avoid duplication of packets for SANs, the switch learns source MAC IDs from supervisory frames for DAN entries and non-PRP frames for SAN entries. Learned MAC IDs are maintained in the Node table. When forwarding packets out of the PRP channel to SAN MAC IDs, the switch looks up the entry and determines which LAN to send to rather than duplicating the packet.

A RedBox with VDANs sends supervisory frames on behalf of those VDANs. For traffic entering on all other ports and exiting PRP channel ports, the switch learns source MAC IDs, adds them to the VDAN table, and starts sending supervisory frames for these addresses. Learned VDAN entries are subject to aging.

All Allen-Bradley products with PRP technology support supervisory frames. If your PRP system includes a device that does not support supervisory frames, the switch identifies the device as a DAN, even if it is a SAN or VDAN. In this scenario, we recommend that you manually add the device to the Node or VDAN table, so the switch can correctly identify the device as a DAN, SAN, or VDAN and manage traffic appropriately.

## Node and VDAN Limitations

When you configure nodes and VDANs, be aware of the following limitations:

- The switch supports a maximum of 512 SAN and DAN entries in the Node table.
- Hash collisions can limit the number of MAC IDs. If the Node table is out of resources for learning a MAC ID from a node, the switch treats that node as a DAN by default.
- After restarting and before any MAC ID is learned, the switch temporarily treats an unlearned node as a DAN and duplicates the egress packets until an ingress packet or supervisory frame is received from the node to populate an entry into the Node table.
- The switch supports a maximum of 512 VDAN entries in the VDAN table. If the VDAN table is full, the switch cannot send supervisory frames for new VDANs.

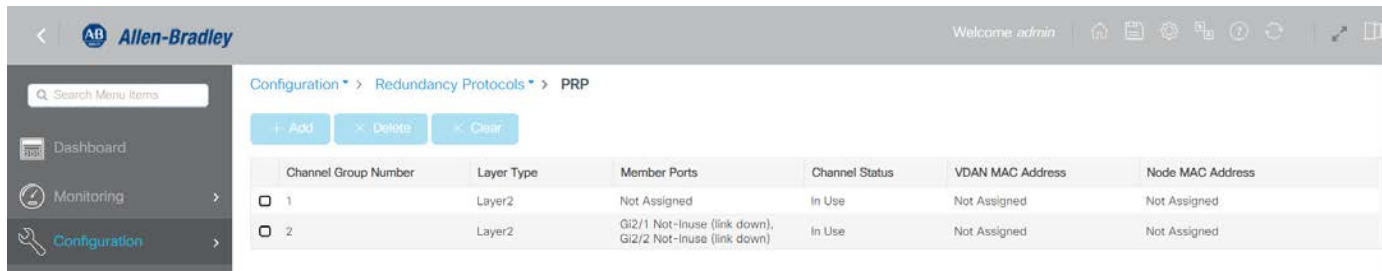
## Configuration Considerations

For requirements related to the following features, see the EtherNet/IP Parallel Redundancy Protocol Application Technique, publication [ENET-AT006](#):

- Device IP addresses
- Frame sizes
- Spanning Tree Protocol (STP)
- Multicast traffic and IGMP querier
- CIP Sync time synchronization (Precision Time Protocol)

## Configure a Stratix 5800 Switch as a RedBox via the WebUI

From the Configuration menu, choose PRP.



From the PRP page, you can add, edit, and delete channel groups and clear dynamic VDAN and Node table entries:

- To add a channel group, click Add, complete the fields as described in [Table 69](#), and then click Apply to Device.
- To edit a channel group, click the channel in the grid, modify the fields, and then click Update & Apply to Device.
- If you have an advanced expansion module, you can add a second channel group.
- To delete a channel group, check its associated checkbox in the grid, and then click Delete.
- To clear all dynamic entries from the VDAN and Node tables, check the associated checkbox for one or both channels in the grid, and then click Clear. On the dialog box that appears, select whether to clear entries from the VDAN table, Node table, or to clear all entries, and then click Save & Apply to Device.

Configure PRP
✕

PRP Channel

Channel Group Number\*

Port 1\*

Port 2\*

IGMP General Query\*

Admin Status\*

Description

Switchport Mode\*

Access Vlan

1

▼

▼

▼

ENABLE

(Applicable during LAN recovery only)

UP

↑

PRP Channel

(1-200 Characters)

access

▼

3680

▼

VDAN

VDAN MAC Address

xxxx.xxxx.xxxx

+

(48 bit redbox MAC address)

-

Table 69 - Configure PRP

Field	Description
<b>PRP Channel</b>	
Channel Group Number	Choose an available channel group number. Valid values: 1 or 2 (Channel group 2 can only be configured on a 1783-MMX8EA or 1783-MMX8SA expansion modules)
Port 1	There are two pairs of port than can be used for channel group 1: <ul style="list-style-type: none"> <li>Option 1: Gi1/1</li> <li>Option 2: Gi1/3</li> </ul> Channel 2 can only be configured on a 1783-MMX8EA or 1783-MMX8SA expansion module. The fixed port is Gi2/1
Port 2	(System-generated). Displays the port assignment for LAN B: <ul style="list-style-type: none"> <li>Channel Group 1 <ul style="list-style-type: none"> <li>Option 1: Gi1/2</li> <li>Option 2: Gi1/4</li> </ul> </li> <li>Channel 2 can only be configured on a 1783-MMX8EA or 1783-MMX8SA expansion module. The fixed port is Gi2/2.</li> </ul>
IGMP General Query	Click whether to enable or disable the RedBox from sending general query packets for PRP LAN recovery. If a PRP LAN is down, a querier update is triggered for faster multicast reconvergence. General queries collect multicast group membership information. By default, general queries are disabled.
Admin Status	Click whether to activate the switch ports in the channel group: <ul style="list-style-type: none"> <li>Up—The ports are active.</li> <li>Down—The ports are inactive.</li> </ul>
Description	Enter a description for the channel group. The description can contain a maximum of 200 characters.
Administrative Mode	Choose one of the following modes for the PRP channel group: <ul style="list-style-type: none"> <li>access—The channel group carries traffic for a single VLAN.</li> <li>trunk—The channel group carries traffic for multiple VLANs.</li> <li>routed—Layer 3</li> </ul>
Access Vlan	(Access mode only). Choose the VLAN to which the PRP channel group belongs. Default value: 1
Allowed Vlan	(Trunk mode only). Click one of these options to specify the VLANs to transmit traffic from this channel group in tagged format: <ul style="list-style-type: none"> <li>All—Click to allow all VLANs to transmit traffic from this channel group.</li> <li>Vlan IDs—Click to allow only the VLANs you specify to transmit traffic from this channel group. Enter each VLAN ID separated by a comma or use a dash for ranges, such as 1,5,7-12,17.</li> </ul>
Native Vlan	(Trunk mode only). Choose the VLAN to send and receive untagged traffic on the trunk port. Default value: 1

Table 69 - Configure PRP (Continued)

Field	Description
IP Assignment Mode	(Routed mode only). Click one of these options to specify the IP address of this PRP channel group. <ul style="list-style-type: none"> <li>No IP Address—Do not assign an IP address.</li> <li>Static—Manually assign a static IP address. Enter the IP address and the subnet mask.</li> <li>DHCP—Allow a DHCP server to assign an IP address automatically.</li> </ul>
<b>VDAN</b> —Add static entries to the VDAN table.	
VDAN MAC Address	Enter the MAC ID of the VDAN to add, and then click the plus (+) sign. To delete a VDAN, click the minus (-) sign.
<b>Node</b> —Add static entries to the Node table.	
Node MAC Address	Enter the MAC ID of the DAN or SAD to add, and then click the plus (+) sign. To delete a DAN or SAN, click the minus (-) sign.
Node	Choose the type of PRP node: <ul style="list-style-type: none"> <li>DAN—Double attached node.</li> <li>LAN-A (SAN-A)—Single attached node on LAN A.</li> <li>LAN-B (SAN-B)—Single attached node on LAN B.</li> </ul>

## Port Security

You can configure port security based on the MAC ID of the switch. A MAC ID is a unique address that is assigned to each Ethernet-capable device. Switches can enforce communication either dynamically or statically per MAC ID:

- With dynamic port security, a switch port communicates with some number of devices. The port tracks only the number of devices rather than the MAC IDs of those devices.
- Static port security adds devices to the port security table on a per MAC ID basis. With static dynamic port security, only devices with the MAC IDs in the security table are able to communicate on that port.

### Configure Port Security via the WebUI

In the WebUI, you can configure port security in the advanced settings for Ethernet ports. See [Advanced Port Configuration on page 76](#).



## Configure Port Security via the Logix Designer Application

In the navigation pane, click Port Security.

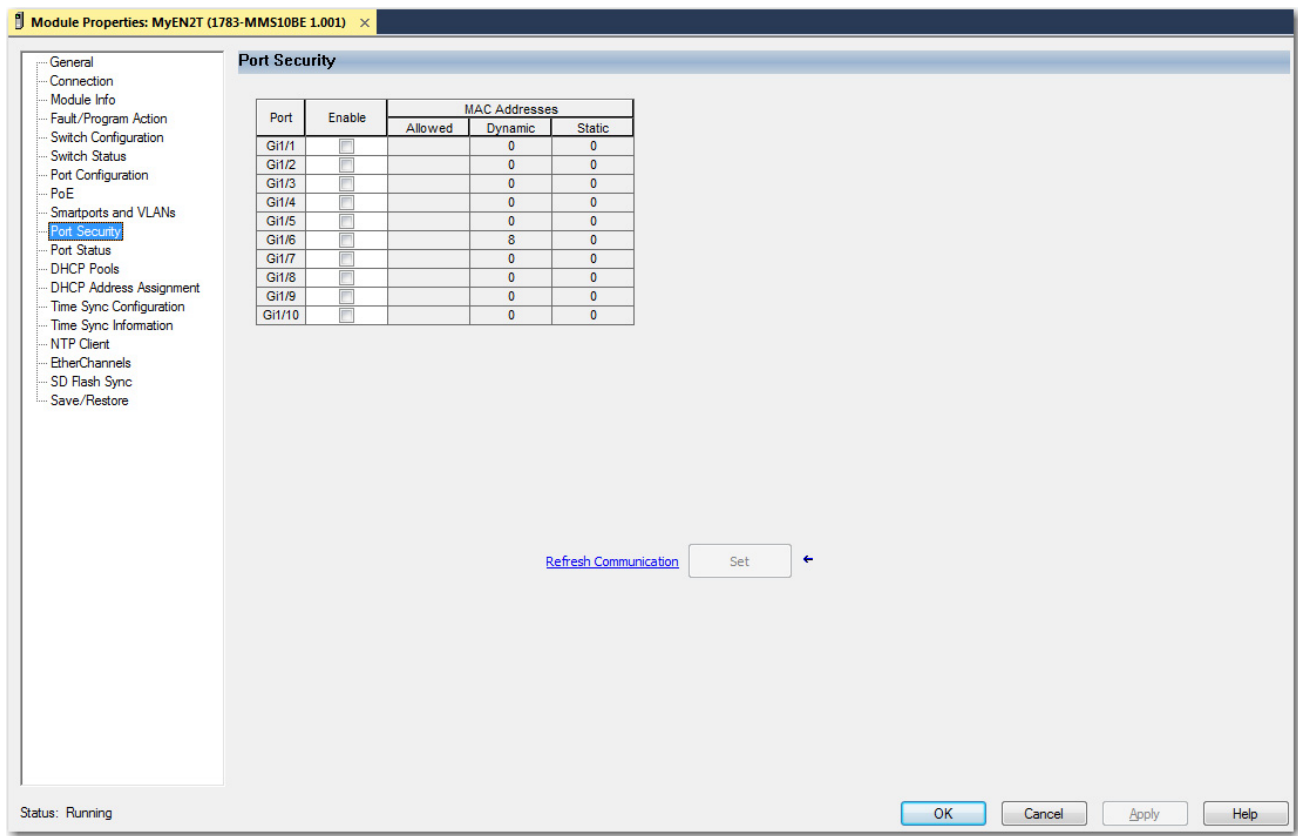


Table 70 - Port Security

Field	Description
Port	Displays the port type and number.
Enable	To enable or disable port security on a port, check or clear its associated checkbox on the grid.
MAC Addresses	<div>The number of supported dynamic or static MAC IDs.</div> <div><ul style="list-style-type: none"><li>Allowed—1...80.</li><li>Dynamic—The number of dynamically defined MAC IDs (devices) currently connected to the port.</li><li>Static—The number of statically defined MAC IDs (devices).</li></ul></div> <div>This number must be greater than the sum of the numbers in the Dynamic and Static fields for a port. To set the number to less, disconnect the devices and let their entries in the port security table time out.</div>

## Quality of Service (QoS)

QoS determines how packets are marked, classified, and treated. Allen-Bradley EtherNet/IP™ devices prioritize traffic internally. QoS implementations at the switch level add another level of prioritization. QoS does not increase bandwidth—QoS gives preferential treatment to some network traffic at the expense of others. For more information about QoS, see the Ethernet Reference Manual, publication [ENET-RM002](#).

QoS is supported on both Layer 2 and Layer 3 interfaces.

## Auto QoS Macros

[Table 71](#) describes QoS macros available on the switch. You can apply a QoS macro when you enable the Auto QoS feature via the WebUI for the switch.

**Table 71 - QoS Macros**

Macro	Description
classify police	Automatically configures QoS policing for untrusted devices within a QoS domain.
classify	Automatically configures QoS classification for untrusted devices within a QoS domain.
trust cos	Trusts the CoS packet classification.
trust dscp	Trusts the Differentiated Services Code Point (DSCP) packet classification.
trust	Automatically configures QoS classification for trusted devices within a QoS domain.
video cts	Specifies a port that is connected to a TelePresence System and automatically configures QoS for video.
video ip-camera	Specifies a port that is connected to an IP camera and automatically configures QoS for video.
video media-player	Specifies a port that is connected to a CDP-capable digital media player and automatically configures QoS for video.
voip phone	Specifies a port that is connected to an IP phone, and automatically configures QoS for VoIP. The QoS labels of incoming packets are trusted only when the telephone is detected.
voip softphone	Specifies a port that is connected to a device running SoftPhone, and automatically configures QoS for VoIP.
voip trust	Specifies a port that is connected to a trusted device, and automatically configures QoS for VoIP. The QoS labels of incoming packets are trusted. For nonrouted ports, the CoS value of the incoming packet is trusted. For routed ports, the DSCP value of the incoming packet is trusted.

## Configure QoS via the WebUI

You can use standard QoS, or you can use Auto QoS to simplify the deployment of QoS features. Auto QoS determines the network design and enables QoS configurations so that the switch can prioritize different traffic flows.

You can enable or disable Auto QoS on a per-port basis in the advanced settings for Ethernet ports. See [Advanced Port Configuration on page 76](#).

From the Configuration menu, choose QoS.

QoS - Policy

[+ Add](#) [Delete](#)

Policy Name	Associated Class-Maps	Associated Interfaces/Profiles
<input type="checkbox"/> Policymap-Output-Wireless	class-default, class-0, class-1, class-2	Not Assigned
<input type="checkbox"/> Voice-Map	voip-data, voip-control	Not Assigned
<input type="checkbox"/> Output-accesspoint	class-default, class-0, class-1, class-2	Not Assigned
<input type="checkbox"/> Policymap-Output-Default	class-default, class-0, class-1, class-2	GigabitEthernet1/1 →, GigabitEthernet1/2 →, GigabitEthernet1/3 →, GigabitEthernet1/4 →, GigabitEthernet1/5 →, GigabitEthernet1/6 →, GigabitEthernet1/7 →, GigabitEthernet1/8 →, GigabitEthernet1/9 →, GigabitEthernet2/1 →, GigabitEthernet2/2 →, GigabitEthernet2/3 →, GigabitEthernet2/4 →, GigabitEthernet2/5 →, GigabitEthernet2/6 →, GigabitEthernet2/7 →, GigabitEthernet2/8 →, GigabitEthernet2/9 →, GigabitEthernet2/10 →, GigabitEthernet2/11 →, GigabitEthernet2/12 →, GigabitEthernet2/13 →, GigabitEthernet2/14 →, GigabitEthernet2/15 →, GigabitEthernet2/16 →, GigabitEthernet1/10 →
<input type="checkbox"/> PTP-Event-Priority	class-default, class-0, class-1, class-2	Not Assigned
<input type="checkbox"/> CIP-PTP-Traffic	CIP-Implicit_dscp_55, CIP-Implicit_dscp_47, CIP-Implicit_dscp_43, CIP-Implicit_dscp_any, CIP-Other, 1588-PTP-Event, 1588-PTP-General	GigabitEthernet1/1 ←, GigabitEthernet1/2 ←, GigabitEthernet1/3 ←, GigabitEthernet1/4 ←, GigabitEthernet1/5 ←, GigabitEthernet1/6 ←, GigabitEthernet1/7 ←, GigabitEthernet1/8 ←, GigabitEthernet1/9 ←, GigabitEthernet2/1 ←, GigabitEthernet2/2 ←, GigabitEthernet2/3 ←, GigabitEthernet2/4 ←, GigabitEthernet2/5 ←, GigabitEthernet2/6 ←, GigabitEthernet2/7 ←, GigabitEthernet2/8 ←, GigabitEthernet2/9 ←, GigabitEthernet2/10 ←, GigabitEthernet2/11 ←, GigabitEthernet2/12 ←, GigabitEthernet2/13 ←, GigabitEthernet2/14 ←, GigabitEthernet2/15 ←

From the QoS page, you can add, edit, and delete QoS policies:

- To add a policy, click Add, complete the fields as described in [Table 72](#), and then click Save & Apply to Device.
- To edit a policy, click the policy in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a policy, check its associated checkbox in the grid, and then click Delete.

**Table 72 - Add QoS**

Field	Description
Auto QoS	Click to enable or disable Auto QoS. Default value: Disabled
Auto QoS Macro	(Appears only if Auto QoS is enabled). Choose a policy to apply to interfaces on the switch. For a description of each policy, see <a href="#">Table 71 on page 123</a> .
Policy Name	Enter a name to identify the QoS policy.
Description	Enter a description for the QoS policy.
<b>+ Add Class-Maps</b> —Click to name a specific traffic flow (or class) and isolate it from all other traffic. The class map defines the criteria that are used to match against a specific traffic flow to classify it. Configure the following fields, and then click Save to save the class map.	
AVC/User Defined	Choose
Match	If any one of the match criteria must be met to classify traffic as part of the traffic class, click Any. If all of the match criteria must be met to classify traffic as part of the traffic class, click All.
Match Type	Choose the type of protocol to match: <ul style="list-style-type: none"> <li>• DSCP</li> <li>• ACL</li> </ul>
Match Value	Enter a value to specify the differentiated services code point value. Valid values: 0...63
Mark Type	Choose the type of marking label for packets: <ul style="list-style-type: none"> <li>• None</li> <li>• DSCP</li> </ul>
Police (kbps)	Enter the policing rate. Valid values: 64...10000000

Table 72 - Add QoS (Continued)

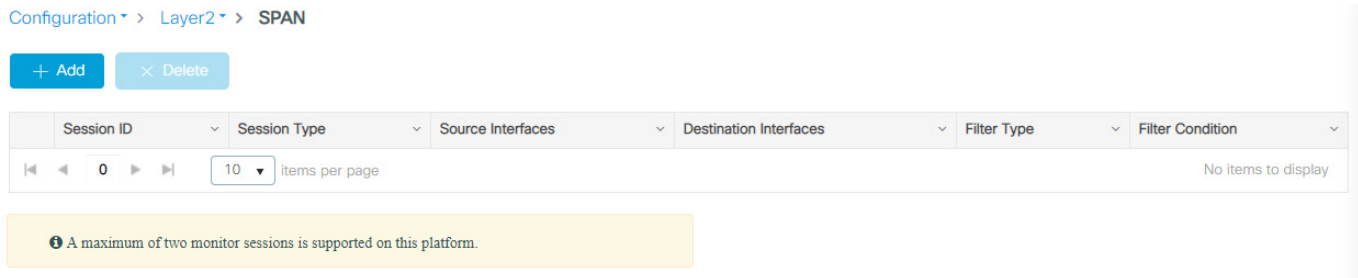
Field	Description
<b>Class Default</b> —The class default is used to match all unclassified packets.	
<b>Mark</b>	Choose <ul style="list-style-type: none"><li>• None</li><li>• DSCP</li></ul>
<b>Police (kbps)</b>	Enter a Valid values: 64...10000000
Available Selected	To attach the policy to interfaces, click to move the interfaces from the Available list to the Selected list. To specify the direction in which the policy is applied, check the checkboxes for Ingress or Egress.

## Remote Switch Port Analyzer (RSPAN)

You can analyze network traffic passing through ports or VLANs by using Switched Port Analyzer (SPAN) or Remote SPAN (RSPAN) to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. You can use SPAN for troubleshooting connectivity issues and calculating network utilization and performance.

### Configure RSPAN via the WebUI

From the configuration menu, choose SPAN.



In the Create SPAN window, select the Span Source Type, Remote.

Create SPAN

Span Source Type

Remote

VLAN ID\*

2-1001,1006-4094

Span Destination Type

Local

Select Destination Interface(s)

Available (19)

Search

GigabitEthernet1/1

GigabitEthernet1/2

GigabitEthernet1/3

Selected (0)

No Interfaces Enabled

Platform does not support SPAN filtering when

- Source interface is configured in the egress direction.
- SPAN is enabled on vlans.
- One of the SPANs is remote FSPAN.

Cancel

Apply to Device

To configure the RSPAN, use the following steps:

1. For remote source, enter the VLAN ID of the remote source interface.
2. From the list of available interfaces on the left, select a destination interface and click the arrow to add it to the selected list on the right.
3. When you are finished, Click Apply to Device.

# Resiliency Ethernet Protocol (REP)

REP provides an alternative to Spanning Tree Protocol (STP) to control network rings and loops, handle link failures, and improve convergence time. REP also provides a basis for constructing more complex networks and supports VLAN load balancing. For more information about REP, see the Ethernet Reference Manual, publication [ENET-RM002](#).

## Default REP Configuration

REP is disabled on all interfaces. When enabled, the interface is a regular segment port unless it is configured as an edge port.

When REP is enabled, the task of sending a segment topology change notice (STCN) is disabled, all VLANs are blocked, and the administrative VLAN is VLAN 1.

When VLAN load balancing is enabled, the default is manual preemption with the delay timer disabled. If VLAN load balancing is not configured, the default after manual preemption is to block all VLANs in the primary edge port.

## Configuring the REP Administrative VLAN

To avoid the delay created by link-failure messages, and VLAN-blocking notifications during load balancing, REP floods packets to a regular multicast address at the hardware flood layer. These messages are flooded to the whole network, and not just the REP segment. You can control the flooding of these messages by configuring an administrative VLAN for the whole domain or for a particular segment.

Follow these guidelines when configuring the REP administrative VLAN:

- If you do not configure an administrative VLAN, the default is VLAN 1.
- You can configure one admin VLAN on the switch for all segments or configure an admin VLAN per segment.
- The administrative VLAN cannot be the RSPAN VLAN.

## REP Port Types

[Table 73](#) describes the types of REP ports available for configuration.

**Table 73 - REP Port Types**

REP Port Type	Description
Edge	A secondary edge port that participates in VLAN load balancing.
Edge No-neighbor	A secondary edge port that is connected to a non-REP switch.
Preferred	A secondary edge port that is the preferred alternate port for VLAN load balancing.
Edge No-neighbor Preferred	A secondary edge port that is connected to a non-REP switch and is the preferred port for VLAN load balancing.
Edge No-neighbor Primary	A secondary edge port that always participates in VLAN load balancing in this REP segment and is connected to a non-REP switch.
Edge No-neighbor Primary Preferred	An edge port that always participates in VLAN load balancing in this REP segment, is connected to a non-REP switch, and is the preferred port for VLAN load balancing.

**Table 73 - REP Port Types**

REP Port Type	Description
Edge Preferred	A secondary edge port that is the preferred alternate port for VLAN load balancing.
Edge Primary	An edge port that always participates in VLAN load balancing in this REP segment.
Edge Primary Preferred	An edge port that always participates in VLAN load balancing in this REP segment and is the preferred port for VLAN load balancing.
None	The port is not part of the REP segment. The default port type is None.
Transit	A non-edge port in the REP segment.

## Configure REP via the WebUI

From the Configuration menu, choose REP.

**REP**

Admin VLAN

Interface	Enable	Mode	Segment ID	Port Type	STCN Interface	STCN Segment	STCN STP
Gi1/1	Enable	trunk	20	Edge No-neighbor Primary	Gi1/1		Enable
Gi1/2	Disable	dynamic auto		None	None		Disable
Gi1/3	Disable	access		None	None		Disable
Gi1/4	Disable	dynamic auto		None	None		Disable
Gi1/5	Disable	dynamic auto		None	None		Disable
Gi1/6	Disable	dynamic auto		None	None		Disable
Gi1/7	Disable	dynamic auto		None	None		Disable
Gi1/8	Disable	dynamic auto		None	None		Disable
Gi1/9	Disable	dynamic auto		None	None		Disable
Gi1/10	Disable	dynamic auto		None	None		Disable
Gi2/1	Disable	dynamic auto		None	None		Disable
Gi2/2	Disable	dynamic auto		None	None		Disable
Gi2/3	Disable	dynamic auto		None	None		Disable
Gi2/4	Disable	dynamic auto		None	None		Disable
Gi2/5	Disable	dynamic auto		None	None		Disable
Gi2/6	Disable	dynamic auto		None	None		Disable
Gi2/7	Disable	dynamic auto		None	None		Disable
Gi2/8	Disable	dynamic auto		None	None		Disable
Gi2/9	Disable	dynamic auto		None	None		Disable
Gi2/10	Disable	dynamic auto		None	None		Disable

1 - 20 of 26 items

From the REP page, you can specify the administrative VLAN for all REP segments or edit the REP configuration for an interface:

- To change the administrative VLAN, enter a VLAN ID in the Admin VLAN field:
  - The default administrative VLAN is 1.
  - Valid values are 2...4094.
- To edit the REP configuration for an interface, click the interface, modify the fields as described in [Table 74](#), and then click Update & Apply to Device.



Edit Rep Interface Gi1/2

Enable

DISABLED

Mode

dynamic auto

Segment ID\*

(1-1024)

Port Type

None

STCN Interface

None

STCN Segment

STCN STP

DISABLED

Cancel

Update & Apply to Device

Table 74 - Edit REP Interface

Field	Description
Enable	Click to enable or disable REP on the interface. When enabled, the interface is a regular segment port unless it is configured as an edge port. Default value: Disabled
Mode	(System-generated). Displays the Switchport mode that is configured for the interface. You can configure the Switchport mode in the basic settings for Ethernet ports. See <a href="#">Ethernet Ports on page 76</a> .
Segment ID	Enter the segment ID. Valid values: 1...1024
Port Type	Choose a REP port type. For a description of REP port types, see <a href="#">Table 73 on page 128</a> .
STCN Interface	(Optional) Choose a physical interface to receive segment topology change notices (STCNs).
STCN Segment	(Optional) Enter one or more segments to receive STCNs. Valid values: 1...1024
STCN STP	Click to enable or disable STCNs on STP networks. Spanning Tree (MST) mode is required on edge no-neighbor nodes to send STCNs to STP networks.

## Routing

The switch provides two types of routing:

- Connected routing—Enables all devices on any VLAN that use the switch to communicate with each other if they use the switch as their default gateway.

---

**IMPORTANT** Connected routing is enabled by default and cannot be disabled.

---

- Static routing—Defines explicit paths between two devices (routers and switches). You must manually define the route information, including the destination IP address, destination subnet mask, and next hop router IP address.

### Configure Static Routing via the WebUI

From the Configuration menu, choose Static Routing.

From the Static Routing page, you can add, edit, and delete IP routes:

- To add an IP route, click Add, complete the fields as described in [Table 75](#), and then click Save & Apply to Device.
- To edit a route, click the route in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a route, check its associated checkbox in the grid, and then click Delete.

You can also specify a default gateway to direct packets addressed to networks not explicitly listed in the routing table. When the default gateway is configured, the switch has connectivity to the remote networks with which a host must communicate. To configure a default gateway, enter the IP address of the default gateway and click Apply to Device.

Create Static Route

IP Type

☒ IPv4

☐ IPv6

Prefix\*

Prefix Mask\*

Metric

VRF

☐

Route Path

☐ Interface

☒ Next Hop IP

☐ DHCP

NextHop IP\*

Cancel

Apply to Device

Table 75 - Create Static Route

Field	Description
IP Type	Click the type of static route.
Prefix	Enter the prefix for your IPv4 or IPv6 address.
Prefix Mask	(Appears only for IPv4). Enter the prefix for your IPv4 address.
Metric	(Appears only for IPv4). Enter the metric for your IPv4 address. <sup>(1)</sup> Valid values: 1...55
Prefix Length	(Appears only for IPv6). Enter the prefix length for your IPv6 address. Valid values: 0...128
Administrative Distance	(Appears only for IPv6). Enter the metric to choose the best path when there are two or more routes to the same destination from two different routing protocols. <sup>(1)</sup> Valid values: 1...254
VRF	If you want the static route to support Virtual Routing and Forwarding (VRF) instances, check VRF.
VRF Name	(Appears only if VRF is checked). Choose the VRF name.
Route Path	Click to specify a route path: <ul style="list-style-type: none"><li>Interface</li><li>Next Hop IP</li><li>DHCP (IPv4 only)</li></ul>
Interface	(Appears only if the route path is Interface). Choose the forwarding interface.
NextHop IP	If the route path is an interface or next hop IP, enter the IPv4 or IPv6 IP address.

(1) A router prefers a static route over a dynamic route because the router considers a route with a low number to be the shortest. If you want a dynamic route to override a static route, specify an administrative distance for the static route. For example, if there are two dynamic routes with an administrative distance of 120, specify an administrative distance that is greater than 120 for the static route.

## Routing Information Protocol (RIP)

RIP is a commonly used routing protocol in small to medium TCP/IP networks. It is a stable protocol that uses a distance-vector algorithm to calculate the best route to a destination based on the number of hops in the path.

### Configure RIP via the WebUI

On the Configuration > Routing Protocols > RIP page, configure the device to receive and send only RIP Version 1 or RIP Version 2 packets. By default, the device receives Version 1 and 2 but sends only Version 1.

**Figure 22 - Basic RIP Configuration**

Configuration > Routing Protocols > RIP

The screenshot shows the 'Basic RIP Configuration' web interface. At the top right, there is an 'Apply' button and two radio buttons for 'Basic' (selected) and 'Advanced'. The configuration fields are as follows:

- Version:** A dropdown menu set to 'V1'.
- Network Address:** A text input field containing 'xxx.xxx.xxx.xxx' with a '+' button to the right.
- Neighbor:** A text input field containing 'xxx.xxx.xxx.xxx' with a '+' button to the right.
- Below each address field, there is a table-like structure with a header 'IP Address' and a 'Remove' button. The content area of these tables says 'No items to display'.

**Table 76 - Basic RIP Configuration Fields**

Field	Description
Version	Choose one of the following versions for your RIP configuration: <ul style="list-style-type: none"> <li>V1 - Does not support authentication of update messages (plain-text or MD5).</li> <li>V2 - Supports plain text and message digest algorithm 5 (MD5) authentication, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs).</li> </ul>
Network Address	Enter the network address to associate a network with a RIP routing process, and click + to add the address. <sup>(1)</sup>
Neighbor	Enter the IP address of a neighboring device to exchange routing information, and click + to add the address.

(1) You can specify multiple network addresses. RIP routing updates are sent and received through interfaces only on these networks.

Choose the Advanced option to configure optional RIP settings.

Configuration > Routing Protocols > RIP

The screenshot shows the RIP configuration page with the 'Advanced' tab selected. The configuration options are as follows:

- Auto Summary:** ☐
- Passive Interface:** ☐
- Timers:** ☐
- Distance:**
- Maximum Paths:**
- IPv6:** ☐

An 'Apply' button is located in the top right corner.

**Table 77 - Advanced RIP Configuration Fields**

Field	Description
Auto Summary	Select the Auto Summary checkbox to disable automatic summarization. By default, the switch summarizes subprefixes when crossing classful network boundaries. Disable summarization (RIP Version 2 only) to advertise the subnet and host routing information to classful network boundaries.
Passive Interface	Select Passive Interface to configure one or more interfaces to operate in RIP passive mode. A passive interface does not send out routing updates but can listen to incoming updates from other RIP speaking neighbors. These updates are used in the routing table.
Timers	Select the Timer checkbox if you want to adjust the protocol timer for the following: <ul style="list-style-type: none"> <li>Update Time - The rate (time in seconds between updates) routing updates are sent. The default is 30 seconds</li> <li>Invalid Time - The time (in seconds) after a route is declared invalid. The interval should be at least three times the value of update time. The interval is measured from the last update received for the route. The route becomes invalid when there is an absence of updates during the invalid time that refresh the route. The default is 180 seconds.</li> <li>Hold Time - The interval (in seconds) where routing information regarding better paths is suppressed. The default is 180 seconds.</li> <li>Flush Time - The amount of time (in seconds) before a route is removed from the routing table. The default is 240 seconds.</li> </ul>
Distance	Define the administrative distance assigned to routes discovered by RIP or to change the preference of RIP routes over other protocol routes. The device uses the administrative distance to determine which routing protocol to use if two protocols provide route information for the same destination. The reliability of a protocol is determined by how small the administrative distance is. The range is 1...255. The default value is 120.
Maximum Paths	Select the maximum number of equal cost parallel routes that RIP can install into the routing table.
IPv6	Check the IPv6 checkbox to configure RIP for IPv6. <ul style="list-style-type: none"> <li>Process Name - Enter a name for the IPv6 RIP routing process.</li> <li>Distance - Define the administrative distance assigned to routes discovered by RIP or to change the preference of RIP routes over other protocol routes. The device uses the administrative distance to determine which routing protocol to use if two protocols provide route information for the same destination. The reliability of a protocol is determined by how small the administrative distance is. The range is 1...254, and the default value is 120.</li> <li>Maximum Paths - Select the maximum number of equal-cost routes that IPv6 RIP can support. The range is 1...32.</li> </ul>

## Smartports

Smartports are recommended configurations for switch ports. These configurations, called Smartport roles, optimize the switch connections and provide security, transmission quality, and reliability for traffic from the switch ports. Smartport roles also help prevent port misconfigurations.

### Requirements and Restrictions

Assign Smartport roles immediately after the initial setup of the switch to configure the switch ports before they connect to devices.

Observe these guidelines:

- We recommend that you do not change port settings after assigning a Smartport role. Any port setting changes can alter the effectiveness of the Smartport role.
- Before assigning Smartport roles, decide which switch port is connected to which device type.
- Before attaching a device to the port or reconnecting any devices that have been moved, verify which Smartport role is assigned to a port.
- You cannot assign Smartport roles to routed ports.

### Avoid Smartport Mismatches

A Smartport mismatch occurs when an attached device does not match the Smartport role that is applied to the switch port. Mismatches can have adverse effects on devices and your network.

Mismatches can result in the following conditions:

- Affect the behavior of the attached device
- Lower network performance (reduce the level of QoS) on CIP™, voice, wireless, switch, and router traffic
- Reduce restrictions on guest access to the network
- Reduce protection from denial-of-service (DoS) attacks on the network
- Disable or shut down the port

Before you attach a device to a port, verify which Smartport role is assigned to the port.

### Smartport Roles

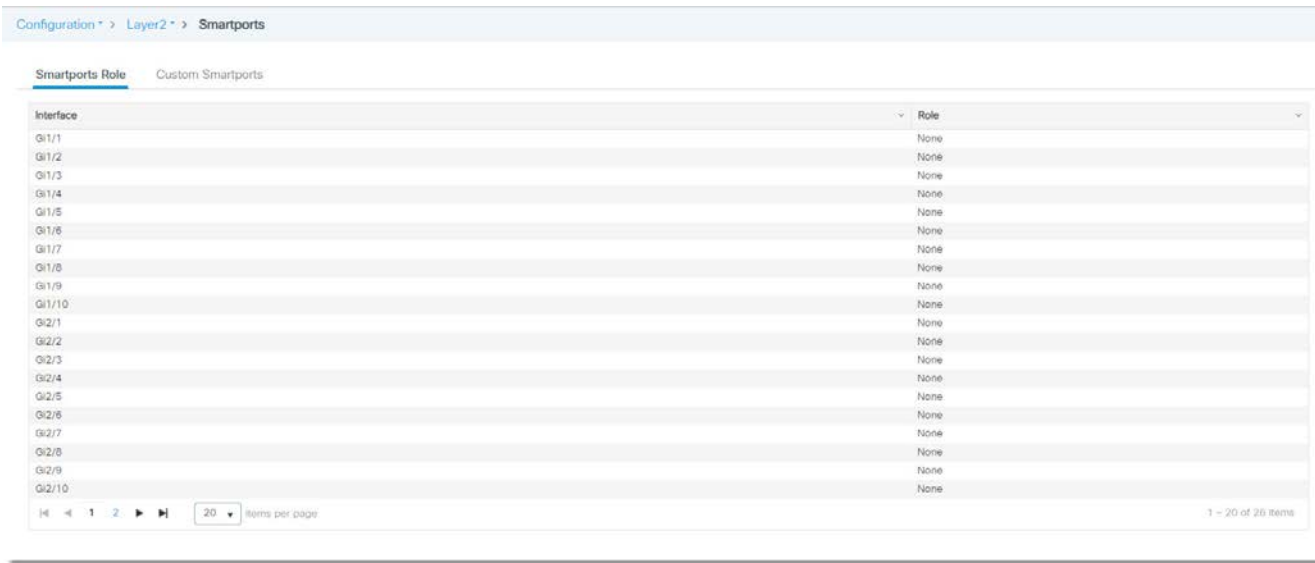
[Table 79](#) describes the Smartport roles that you can assign to switch port. The port roles are based on the type of devices that connect to the switch ports. For example, the Desktop for Automation port role is specifically for switch ports to be connected to desktop and laptop computers.

You can create a maximum of 10 custom Smartport roles for various custom applications.

The default Smartport role is None.

## Assign Smartport Roles via the WebUI

From the Configuration menu, choose Smartports.



From the Smartports page, you can assign Smartports roles and configure Custom Smartports roles:

- To assign a Smartports role, see [page 136](#).
- To configure Custom Smartports roles, see [page 138](#).

### VLAN Type

When you assign a Smartport role to a port, you must also assign a VLAN to the port. [Table 78](#) describes the types of VLANs you can assign depending on the type of Smartport role. For example, if you choose the Phone for Automation role, you can assign an access VLAN and a voice VLAN.

**Table 78 - VLAN Type**

VLAN Type	Description
Native	A native VLAN is for ports that can belong to a VLAN trunk (a port belonging to multiple VLANs). The native VLAN for ports that are assigned to these Smartport roles: <ul style="list-style-type: none"><li>• Switch for Automation</li><li>• Router for Automation</li><li>• Wireless for Automation</li></ul>
Access	An access VLAN is for ports that can belong to only one VLAN. The access VLAN ID for ports that are assigned to these Smartport roles: <ul style="list-style-type: none"><li>• Automation Device</li><li>• Multiport Automation Device</li><li>• Desktop for Automation</li><li>• Virtual Desktop for Automation</li><li>• Phone for Automation</li></ul>
Voice	The voice VLAN helps to make sure that all voice traffic has better Quality of Service and is not mixed with data traffic. The voice VLAN ID for ports that are assigned to the Phone for Automation Smartport role.

### Assign Smartports Roles

On the Smartports Role tab, click an interface in the grid. On the Assign Macro page, choose an appropriate role per the descriptions in [Table 79](#), and then click Update & Apply to Device.

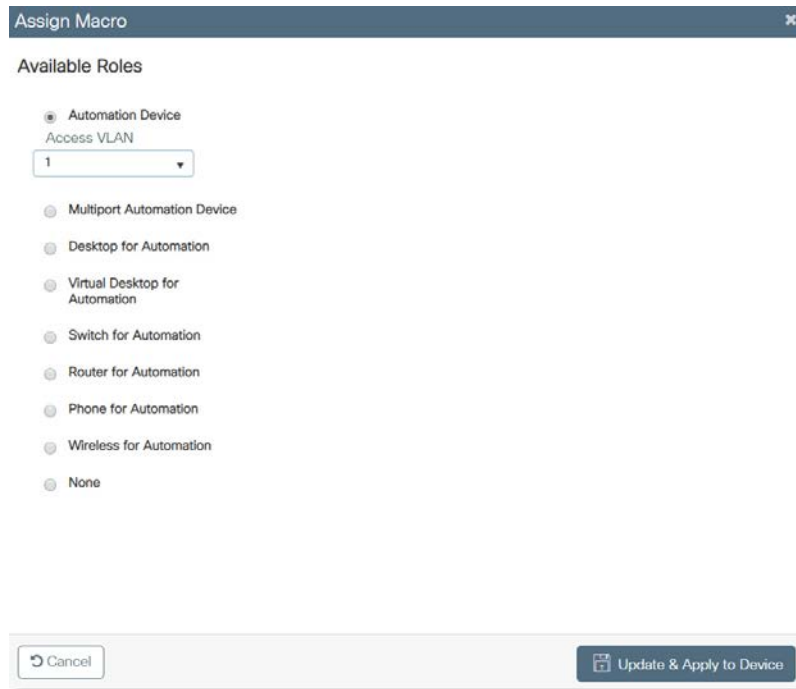


Table 79 - Assign Macro

Field	Description
<b>Smartports Role</b>	
Automation Device	<p>Apply this role to ports that connect to EtherNet/IP (Ethernet Industrial Protocol) devices, such as logic controllers and I/O:</p> <ul style="list-style-type: none"> <li>• Port is set to Access mode.</li> <li>• Port security supports only one MAC ID.</li> <li>• Optimized queue management for CIP traffic.</li> </ul>
Multiport Automation Device	<p>Apply this role to DLR-enabled ports and ports that connect to multiport EtherNet/IP devices. For example, devices can include multiport EtherNet/IP devices that are arranged in a linear or daisy chain topology, the 1783-ETAP module (for connection to only the device port), unmanaged switches:</p> <ul style="list-style-type: none"> <li>• Port is set to Access mode.</li> <li>• No port security.</li> <li>• Optimized queue management for CIP traffic.</li> </ul>
Desktop for Automation	<p>Apply this role to ports that connect to desktop devices, such as desktop computers, workstations, notebook computers, and other client-based hosts:</p> <ul style="list-style-type: none"> <li>• Port is set to Access mode.</li> <li>• PortFast enabled.</li> <li>• Port security supports only one MAC ID.</li> </ul> <p><b>IMPORTANT:</b> Do not apply the Desktop for Automation role to ports that connect to switches, routers, or access points.</p>
Virtual Desktop for Automation	<p>Apply this role to ports that connect to a computer with virtualization software. You can use this role with devices running up to two MAC IDs:</p> <ul style="list-style-type: none"> <li>• Port is set to Access mode.</li> <li>• PortFast is enabled.</li> <li>• Port security supports two MAC IDs.</li> </ul> <p><b>IMPORTANT:</b> Do not apply the Virtual Desktop for Automation role to ports that connect to switches, routers, or access points.</p>
Switch for Automation	<p>Apply this role to ports that connect to other switches.</p> <p>Port is set to Trunk mode.</p>
Router for Automation	<p>Apply this role to ports that connect to routers or Layer 3 switches with routing services enabled.</p> <p>Port is set to Trunk mode.</p>
Phone for Automation	<p>Apply this role to ports that connect to IP phones. A desktop device, such as a computer, can connect to the IP phone. Both the IP phone and the connected computer have network access through the port:</p> <ul style="list-style-type: none"> <li>• Port is set to Trunk mode.</li> <li>• Port security supports three MAC IDs to this port.</li> </ul> <p>This role prioritizes voice traffic over general data traffic to provide clear voice reception on the IP phones.</p>
Wireless for Automation	<p>Apply this role to ports that connect to wireless access points. The access point can provide network access to as many as 30 wireless users.</p>
None	<p>Apply this role to ports if you do not want a specialized Smartport role on the port. You can apply this role to ports that connect to any device, including a device with another Smartport role.</p>
CS1...CS10	<p>Custom Smartport roles. You can create a customized port role with a user-defined name.</p>



Configure Custom Smartport Roles

On the Custom Smartports tab, you can add, delete, import, and export custom Smartport roles:

- To add a custom Smartports role, click Add, complete the fields as described in [Table 80](#), and then click Apply to Device.
- To delete a Custom Smartports role, click the role in the grid, and then click Delete.
- To import a Custom Smartports role, click Import and then Select File to browse to the location of the file to upload from your computer or network drive. Click Apply to Device.
- To export a Custom Smartports Macro, click the role in the grid, and then click Export. Select the directory where you want to export the file.

Add custom smartports macro

Name\*

1-100 Characters

Icon

CS1

Available Parameters

\$access\_vlan,\$native\_vlan,\$voice\_vlan

Macro Definition:\*

Antimacro Definition:\*

Cancel

Apply to Device

Table 80 - Add Custom Smartports Macro

Field	Description
Name	Enter a name to identify the custom Smartport role.
Icon	Choose an icon to identify the custom Smartport role. Valid values: CS1...CS10
Available Parameters	Displays the available parameters: \$native_vlan, \$access_vlan, and \$voice_vlan You can use these parameters to ensure proper VLAN configuration in your custom smartport roles.
Macro Definition	Enter the commands to define the custom role with one command per line. A macro definition can have up to 3000 characters. Use the @ character to end the macro. Use the # character at the beginning of a line to enter comment text within the macro. We recommend that you do not use the exit or end commands or change the command mode by using interface interface-id in a macro. This can cause any commands following exit, end, or interface interface-id to execute in another command mode. For best results, all commands in a macro must be in the same configuration mode.
Antimacro Definition	Enter the commands to remove the custom role with one command per line. The antimacro is the portion of the applied macro that removes the macro when you replace it or remove it. Before you can apply the macro definition to the port, you must first define the antimacro with the proper commands to set the port back to its original state. An antimacro definition can have a maximum of 3000 characters. Use the @ character to end the macro. Use the # character at the beginning of a line to enter comment text within the macro.

Assign Smartport Roles via the Logix Designer Application

In the navigation pane, click Smartports and VLANs.

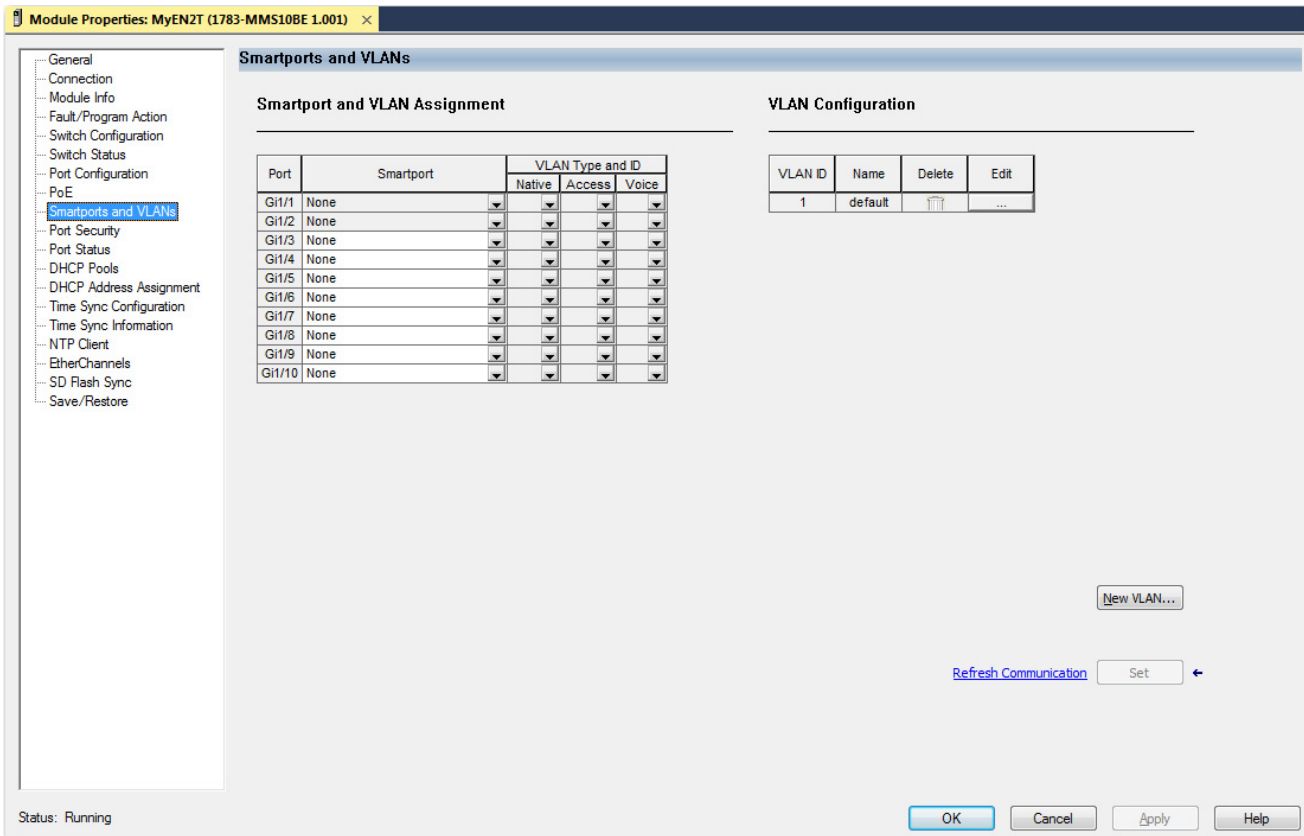


Table 81 - Smartports and VLANs

Field	Description
Port	Displays the port type and number.
Smartport	Choose the role that corresponds to the type of device to be connected to the port. For a description of each role, see <a href="#">Table 79 on page 137</a> .
VLAN Type and ID	Choose the VLANs to assign to the port. The types of VLANs you can assign depend on the type of Smartport role. For a description of each VLAN type, see <a href="#">Table 78 on page 136</a> .

## Spanning Tree Protocol (STP)

STP is a Layer 2 link management protocol that provides path redundancy and helps to prevent loops in the network. A spanning-tree algorithm selects one switch in a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a Layer 2 network. For more information about STP, see the Ethernet Reference Manual, publication [ENET-RM002](#).

### Requirements and Restrictions

We recommend that you leave STP enabled to help prevent network loops and provide a redundant path if the active path becomes unavailable.

---

**IMPORTANT**    Disabling STP can affect connectivity to the network.

---

## STP Modes

[Table 82](#) describes the STP modes that you can assign to the switch. The default mode is MST.

**Table 82 - STP Modes**

STP Mode	Description
MST	Multiple Spanning Tree (MST) is based on the IEEE 802.1s standard. MST uses Rapid Spanning Tree Protocol (RSTP) for rapid convergence. This mode maps a group of VLANs into one spanning tree instance, with each instance having a spanning tree topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning tree instances that are required to support many VLANs.
PVST	Per VLAN Spanning Tree Plus (PVST+) protocol based on the IEEE 802.1D standard. PVST+ runs on each VLAN on the switch up to the maximum supported, to help create a loop-free path through the network. PVST+ provides Layer 2 load balancing for the VLAN on which it runs. You can create different logical topologies by using the VLANs on your network to make sure that all of your links are used but that no one link is oversubscribed. Each instance of PVST+ on a VLAN has one root switch. This root switch propagates the spanning-tree information that is associated with that VLAN to all other switches in the network. Because each switch has the same information about the network, this process maintains the network topology.
RPVST	Rapid per VLAN Spanning Tree Plus (Rapid PVST+) protocol based on the IEEE 802.1w standard. RPVST+ is the same as PVST+ except that it uses a rapid convergence based on the IEEE 802.1w standard. To provide rapid convergence, the rapid PVST+ immediately deletes dynamically learned MAC ID entries on a per-port basis upon receiving a topology change. By contrast, PVST+ uses a short aging time for dynamically learned MAC ID entries. Only one version can be active on the switch at any time. For example, all VLANs run PVST+, all VLANs run rapid PVST+, or all VLANs run MSTP.

## Configure STP via the WebUI

1. From the Configuration menu, choose Spanning Tree.
2. Complete the fields as described in [Table 83](#).
3. To enable or disable STP on a VLAN or change the bridge priority, click the VLAN in the grid, modify the fields, and then click Update & Apply to Device.

Spanning Tree Protocol

STP Mode: MST

BPDU Filtering: ENABLED

BPDU Guard: ENABLED

VLAN ID	VLAN Name	Enable Spanning Tree	Priority
1	default	Enable	32768
3680	VLAN3680	Enable	32768

1 - 2 of 2 items

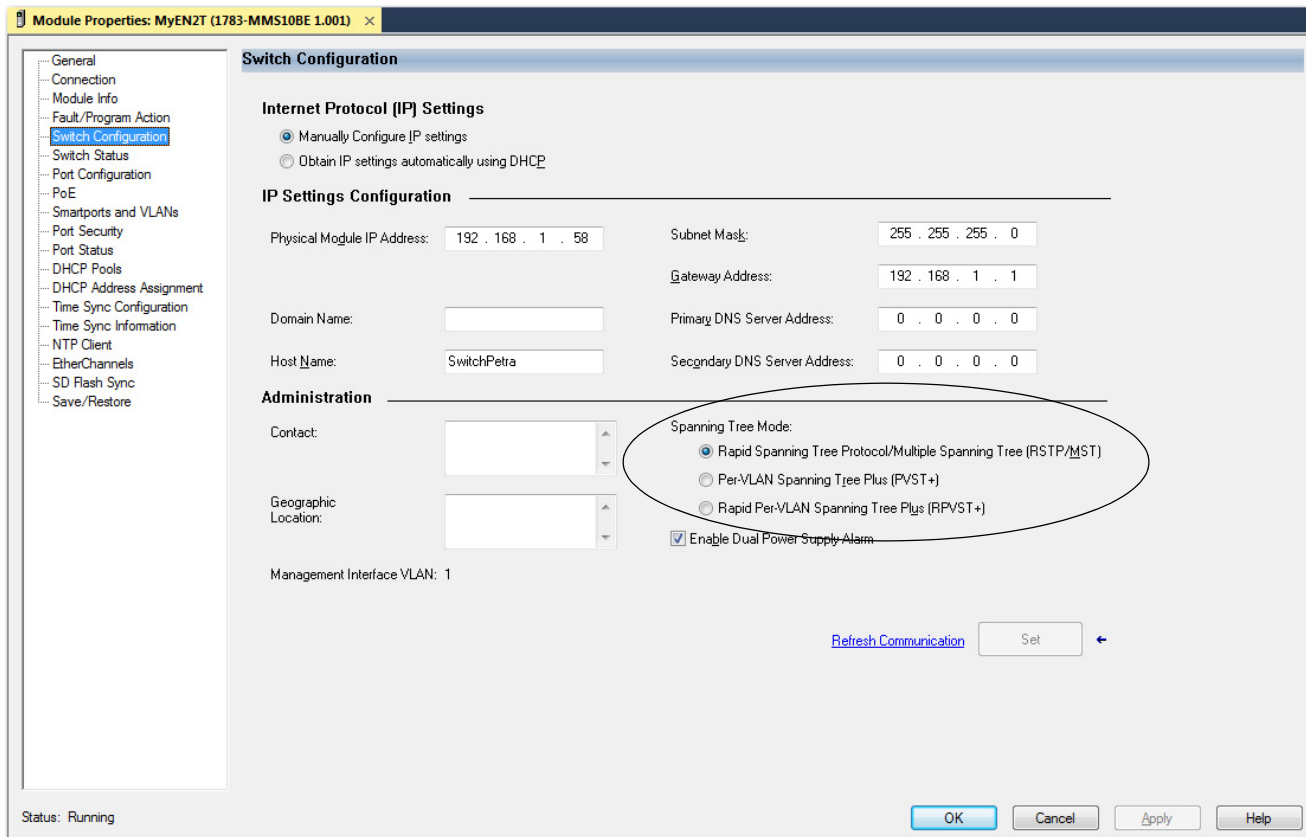
**Table 83 - Spanning Tree Protocol**

Field	Description
STP Mode	Choose the STP mode to apply to the switch. For a description of each mode, see <a href="#">Table 82 on page 140</a> . The default mode is RPVST.
BPDU Filtering	Click to enable or disable BPDU filtering. BPDU filtering avoids transmitting bridge protocol data units (BPDUs) on PortFast-enabled ports that are connected to an end system. When you enable PortFast on the device, STP places ports in the forwarding state immediately, instead of going through the listening, learning, and forwarding states first.
BPDU Guard	Click to enable or disable BPDU guard. BPDU guard helps to prevent loops by moving a nontrunk port into an err-disable state when a BPDU is received on that port. When you enable BPDU guard on the switch, STP shuts down PortFast-configured interfaces that receive BPDUs instead of putting them into the STP blocking state. In a valid configuration, PortFast-configured interfaces do not receive BPDUs. If a PortFast-configured interface receives a BPDU, an invalid configuration exists. BPDU guard provides a secure response to invalid configurations because the administrator must manually put the interface back in service.

## Configure STP via the Logix Designer Application

1. In the navigation pane, click Switch Configuration.
2. In the Spanning Tree Mode field, click to specify an STP mode, and then click Apply.

For a description of each mode, see [Table on page 140](#).



## Switched Port Analyzer (SPAN)

SPAN, also known as port mirroring, copies traffic from one port to a monitoring port where a network analyzer tool can capture the traffic. You can use SPAN to troubleshoot network issues and calculate network utilization and performance. For more information about SPAN, see the Ethernet Reference Manual, publication [ENET-RM002](#).

## Requirements and Restrictions

Observe these guidelines:

- You can configure a maximum of two monitor sessions on the switch. Session IDs are 1 and 2.
- There can be multiple source interfaces and only one destination interface.
- Source interfaces cannot be a combination of VLAN and physical interfaces.
- If using more than one source port, you can lose traffic if the combined source throughput is more than the output port is capable of.

## Configure SPAN via the WebUI

From the Configuration menu, choose SPAN.



From the SPAN page, you can add, edit, and delete SPAN monitor sessions:

- To add a SPAN session, click Add, complete the fields as described in [Table 84](#), and then click Apply to Device.
- To edit a SPAN session, click the session in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a session, check its associated checkbox in the grid, and then click Delete.

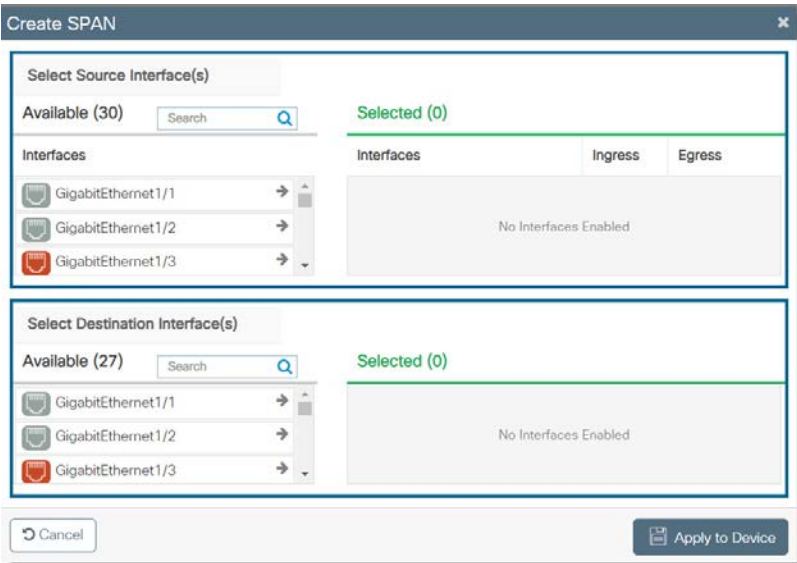


Table 84 - Create SPAN

Field	Description
Select Source Interfaces	In the Available list, click to move one or more source interfaces to the Selected list on the right. To specify the direction of source packets to be monitored, check the Ingress and Egress checkboxes.
Select Destination Interfaces	In the Available list, click to move a destination interface to the Selected list on the right. Stratix 5800 switches support only one destination interface.

## TrustSec

Cisco TrustSec builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms.

### TrustSec Security Groups

TrustSec uses the device and user credentials acquired during authentication for classifying the packets by security groups as they enter the network. A security group is a grouping of users, endpoint devices, and resources that share access control policies. Once a device is authenticated, TrustSec tags any packet that originates from that device with a security group tag (SGT) that contains the security group number of the device. The packet carries this SGT throughout the network within the TrustSec header. The SGT is a single label that determines the privileges of the source within the entire enterprise.

You can map an SGT to a subnet, VLAN, or interface as described in [Table 85](#).

**Table 85 - SGT Mappings**

Mapping Type	Description
IPv4 subnet-to-SGT	Binds an SGT to all host addresses of a specified subnet. TrustSec imposes the SGT on an incoming packet when the source IP address in the packet belongs to the specified subnet.
VLAN-to-SGT	Binds an SGT to packets from a specified VLAN. This type of mapping is useful in networks with these characteristics: <ul style="list-style-type: none"> <li>• Do not have authentication enabled</li> <li>• Use third-party switches</li> <li>• Have devices that do not support Cisco TrustSec</li> </ul>
L3IF-SGT	Directly maps SGTs to traffic of any of the following Layer 3 interfaces regardless of the underlying physical interface: <ul style="list-style-type: none"> <li>• Routed port</li> <li>• SVI (VLAN interface)</li> <li>• Layer 3 subinterface of a Layer 2 port</li> <li>• Tunnel interface</li> </ul>

### Security Group Tag Exchange Protocol

The Security Group Tag (SGT) Exchange Protocol (SXP) is a control protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets. This helps propagate the SGTs across network devices that do not have hardware support for TrustSec.

### TrustSec Policies

To control the operations performed by a user, you can use Cisco TrustSec (CTS) policies. CTS policies include a selection of security group access control lists (SGACLs). A list specifies the permissions to be applied to packets from an IP address belonging to a source security group and having a destination IP address that belongs to the destination security group.

You must enable SGACL policy enforcement on specific VLANs to apply access control to switched traffic within a VLAN, or to traffic that is forwarded to an SVI associated with a VLAN.

You can enable Monitor mode on a global or per-policy basis to test security policies without enforcing them to make sure that the policies function as intended.

## CTS Interface Configuration

By enabling CTS Manual Configuration mode on an interface, you can configure a physical port so that a single SGT is imposed on all traffic entering the port. This SGT is applied on all IP traffic exiting the port until a new binding is learned.

CTS configuration is available for the following ports:

- Routed ports
- Ports in Access mode
- Ports in Trunk mode

When manually configuring Cisco TrustSec on an interface, consider these usage guidelines and restrictions:

- If no Security Association Protocol (SAP) parameters are defined, MACsec encapsulation or encryption is not performed.
- If the selected SAP mode allows SGT insertion and an incoming packet carries no SGT, the packet is tagged with the SGT configured for the interface.
- If the selected SAP mode allows SGT insertion and an incoming packet carries an SGT, the tagging policy is as follows:
  - If the policy is configured without the trusted keyword, the SGT is replaced with the SGT configured for the interface.
  - If the policy is configured with the trusted keyword, no change is made to the SGT.

## Configure TrustSec via the WebUI

From the Configuration menu, choose TrustSec. From the Trustsec page, you can configure the following:

- Global settings as described on [page 145](#).
- SGT mappings as described on [page 145](#).
- SGT Exchange Protocol (SXP) as described on [page 146](#).
- CTS policies as described on [page 148](#).
- CTS interfaces as described on [page 149](#).

---

**IMPORTANT**

To configure global settings, CTS policies, and CTS interfaces, you must have one of the following:

- A switch with advanced features with no expansion module attached
  - A switch with advanced features attached to an expansion module with advanced features
-

## Configure TrustSec Global Settings

On the General tab, complete the fields as described in [Table 86](#), and then click Apply.

Configuration > Security > Trustsec

Global   SGT Mapping   SXP   CTS Policies   CTS Link Configuration

CTS Credentials [Modify](#) Apply

CTS Device ID

CTS Password

CTS Authorization List none + Add AAA Method List

CTS Device SGT 2-65519 ⓘ

**Table 86 - Trustsec—Global Tab**

Field	Description
CTS Credentials	Click Modify, and then enter the Cisco TrustSec device ID and password.
CTS Device ID	Displays the CTS device ID.
CTS Password	Displays the CTS device password.
CTS Authorization List	Choose the Cisco TrustSec global authorization list to configure on the switch. To add a new method list, click + Add AA Method List.
CTS Device SGT	Enter the ID of the security group tag to configure on the switch. Valid values: 2...65519.

## Configure SGT Mappings

Configuration > Security > Trustsec

Global   **SGT Mapping**   SXP   CTS Policies   CTS Link Configuration

+ Add Delete

IP - SGT Mappings Switch to VLAN List/L3IF-SGT Mappings

IP Type	IP Address	SGT	VRF	Source
<input type="checkbox"/> IPv4	192.168.1.2	523	-	CLI

10 items per page   1 - 1 of 1 items

On the SGT Mapping tab, you can add, edit, and delete SGT mappings:

- To add an SGT mapping, click Add, complete the fields as described in [Table 85](#), and then click Apply to Device.
- To edit an SGT mapping, click the interface in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an SGT mapping, check its associated checkbox in the grid, and then click Delete.



Add SGT mapping

Add Mapping

☒ IPv4

☐ VLAN LIST

☐ L3IF

Host/Subnet Address(IPv4)

A.B.C.D or A.B.C.D/nn

VRF

None

SGT Value

2-65519

Cancel

Apply to Device

Table 87 - Add SGT Mapping

Field	Description
Mapping	Click the type of SGT mapping to add. For a description of each type of mapping, see <a href="#">Table 85</a> .
Host/Subnet Address(IPv4)	(Appears only for IPv4 mappings). Enter an IPv4 network address in dotted decimal notation.
VRF	(Appears only for IPv4 mappings). Choose a VRF interface. For information about creating a VRF interface, see <a href="#">page 81</a> .
VLAN List	(Appears only for VLAN LIST mappings). Enter the VLAN IDs to apply to the SGT mapping.
Layer-3 Interface	(Appears only for L3IF mappings). Choose an interface configured for Layer 3. For information about configuring a Layer 3 interface, see <a href="#">page 76</a> .
SGT Value	Enter a number to identify the mapping. Valid values: 0...65519

Configure SXP

To configure SXP, follow these steps.

1. Click the SXP tab.
2. In the SXP Parameters area, complete the fields as described in [Table 88](#), and then click Apply.

Configuration > Security > Trustsec

Global

SGT Mapping

SXP

CTS Policies

CTS Link Configuration

SXP Parameters

Apply

SXP Status

ENABLED

Default Source IP

X.X.X.X / X:X:X:X::X

Default Password

\*\*\*\*\*

Reconciliation Period (sec)

120

Retry Period (sec)

120

Peer Connections

+ Add

- Delete

Peer IP

Source IP

Mode(Local Device)

Connection Status

10 items per page

No items to display

146

Rockwell Automation Publication 1783-UM012E-EN-P - March 2021

**Table 88 - SXP Parameters**

Field	Description
SXP Status	Click to enable or disable TrustSec SXP. You must enable SXP before you can configure peer connections.
Default Source IP	Enter an SXP default source IP address. SXP uses the default source IP address for all new TCP connections where a source IP address is not specified. There is no effect on existing TCP connections when you configure the default SXP source IP address.
Reconciliation Period (sec)	Enter a reconciliation period in seconds. After a peer terminates an SXP connection, an internal timer starts. If the peer reconnects before the internal timer expires, the SXP reconciliation period timer starts. While the SXP reconciliation period timer is active, TrustSec retains the SGT mapping entries learned from the previous connection and removes invalid entries. Setting the reconciliation period to 0 seconds disables the timer and causes all entries from the previous connection to be removed. Default value: 120 seconds (2 minutes)
Default Password	Enter an SXP default password. By default, SXP uses no password when setting up connections. Spaces and special characters are not allowed.
Retry Period (sec)	Enter a retry period in seconds. The SXP retry period determines how often TrustSec retries an SXP connection. When an SXP connection is not successfully set up, TrustSec makes a new attempt to set up the connection after the SXP retry period timer expires. Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted. Default value: 120 seconds (2 minutes)

3. In the Peer Connections area, you can add, edit, and delete peer connections:

- To add a peer connection, click Add, complete the fields as described in [Table 89](#), and then click Apply to Device.

You must configure the SXP peer connection on both of the devices. One device is the speaker and the other is the listener. When using password protection, make sure to use the same password on both ends.

- To edit a peer connection, click the connection in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a peer connection, check its associated checkbox in the grid, and then click Delete.

**Table 89 - Add Peer Connection**

Field	Description
Mode of Local Device	Choose one of the following modes for the remote peer device: <ul style="list-style-type: none"> <li>listener—The device is the listener in the connection.</li> <li>speaker—The device is the speaker in the connection.</li> <li>both—The device is both the listener and the speaker in the connection.</li> </ul> Default value: listener
Peer IP	Enter the IPv4 address of the peer device.

Table 89 - Add Peer Connection

Field	Description
Source IP	Enter the IPv4 address of the source device. If you do not specify an address, the connection uses the default source address, if configured, or the address of the port.
Password	Choose one of the following options to specify the password that SXP uses for the connection: <ul style="list-style-type: none"><li>• default—Uses the default SXP password.</li><li>• none—Does not use a password.</li></ul> Default value: default
VRF	Choose one of the following to specify the VRF to the peer: <ul style="list-style-type: none"><li>• None</li><li>• [VRF name]</li></ul> Default value: None

Configure CTS Policies

To configure CTS policies, follow these steps.

1. Click the CTS Policies tab.
2. In the Policy Enforcement area, complete the fields as described in [Table 90](#), and then click Apply.

The screenshot shows the 'CTS Policies' configuration page. At the top, there are tabs for 'Global', 'SGT Mapping', 'SXP', 'CTS Policies' (which is selected), and 'CTS Link Configuration'. Below the tabs, there's a 'Policy Enforcement' section with a text input for 'VLAN List' containing '1-4094' and a 'Global' toggle switch set to 'DISABLED'. An 'Apply' button is to the right. Below this is a 'Manage Policies' section with '+ Add' and '- Delete' buttons. To the right of these are 'Monitor mode for all' (a toggle switch set to 'DISABLED') and a 'Refresh' button. At the bottom, there's a table header with columns: 'From SGT', 'To SGT', 'IP Type', 'SGACL List', 'Policy Type', and 'Monitor Mode'. Below the header is a pagination bar showing '0' items per page and 'No items to display'.

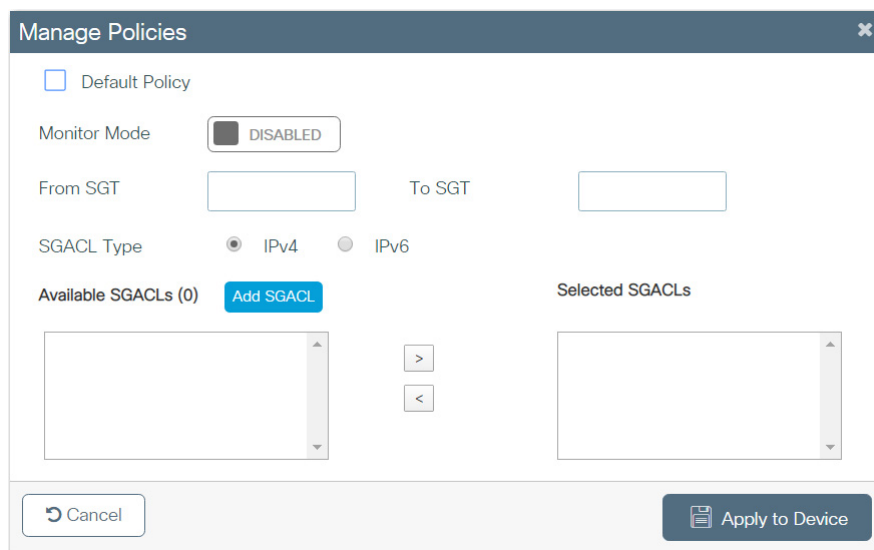
Table 90 - Policy Enforcement

Field	Description
VLAN List	Enter the VLAN IDs on which to enforce Cisco TrustSec policies. Valid values: 1...4094
Global	Click to enable or disable global CTS role-based enforcement. <b>IMPORTANT:</b> You must enable policy enforcement globally for TrustSec-enabled routed interfaces. Default value: Disabled

3. In the Manage Policies area, you can add, edit, and delete policies:
  - To add a policy, click Add, complete the fields as described in [Table 91](#), and then click Apply to Device.
  - To edit a policy, click the connection in the grid, modify the fields, and then click Update & Apply to Device.
  - To delete a policy, check its associated checkbox in the grid, and then click Delete.
4. In the Monitor mode for all field, click to enable or disable the Monitor mode for all policies.

For more information about Monitor mode, see [TrustSec Policies on page 143](#).

5. To force an immediate refresh of TrustSec policies, click Refresh.



The 'Manage Policies' dialog box contains the following fields and controls:

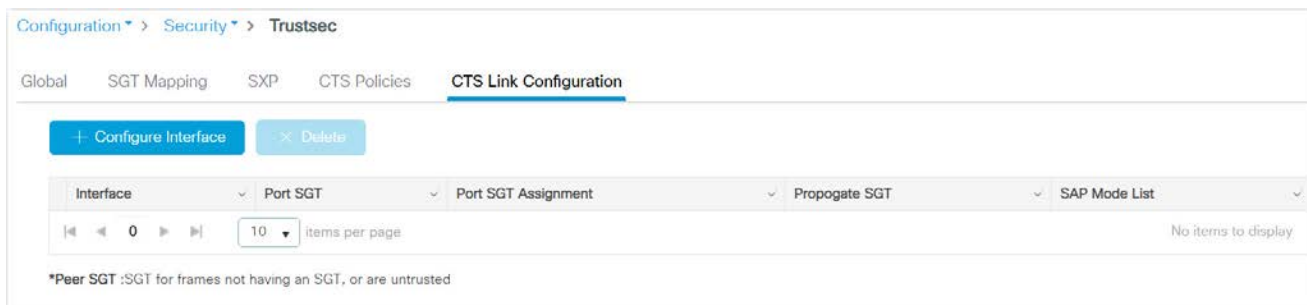
- Default Policy:** A checkbox.
- Monitor Mode:** A button labeled 'DISABLED'.
- From SGT:** A text input field.
- To SGT:** A text input field.
- SGACL Type:** Radio buttons for 'IPv4' (selected) and 'IPv6'.
- Available SGACLs (0):** A list box with an 'Add SGACL' button next to it.
- Selected SGACLs:** A list box.
- Navigation:** '>' and '<' buttons between the two list boxes.
- Buttons:** 'Cancel' and 'Apply to Device' at the bottom.

**Table 91 - Manage Policies**

Field	Description
Default Policy	Check to make this policy the default policy.
Monitor Mode	Click to enable or disable Monitor mode for this policy. Default value: Disabled For more information about Monitor mode, see <a href="#">TrustSec Policies on page 143</a> .
From SGT	Enter the source security number for this policy.
To SGT	Enter the destination security group number for this policy.
SGACL Type	Click the type of IP addresses that belong to the security groups for this policy: <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>
Available SGACLs	To select the SGACLs to include in this policy, click an SGACL in the Available SGACLs column to move it into the Selected SGACLs column. To create a new SGACL, click Add SGACL. See <a href="#">Add an Access Control List on page 68</a> .

### Configuring CTS Interfaces

To configure CTS interfaces, click the CTS Link Configuration tab.



The 'CTS Link Configuration' tab shows the following interface:

- Breadcrumbs:** Configuration > Security > Trustsec
- Tabs:** Global, SGT Mapping, SXP, CTS Policies, **CTS Link Configuration**
- Buttons:** '+ Configure Interface' and 'X Delete'
- Table Headers:** Interface, Port SGT, Port SGT Assignment, Propagate SGT, SAP Mode List
- Table Content:** A table with 0 items displayed. Navigation controls show '10 items per page'.
- Footer:** '\*Peer SGT :SGT for frames not having an SGT, or are untrusted'

On the CTS Link Configuration tab, you can configure, edit, and delete STC interfaces:

- To configure an interface, click Configure Interface, complete the fields as described in [Table 92](#), and then click Apply to Device.
- To edit an interface, click the interface in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an interface, check its associated checkbox in the grid, and then click Delete.

Configure Interface

Interface Name

GigabitEthernet1/1

CTS Manual

ENABLED

Port SGT value

2-65519

☐ Trusted

Propagate SGT

DISABLED

SAP Parameters

PMK

Mode List

Available Modes

gcm-encrypt

gmac

no-encap

null

>

<

Selected Modes

Cancel

Apply to Device

Table 92 - Configure Interface

Field	Description
Interface Name	Choose the interface to configure.
CTS Manual	To manually configure Cisco TrustSec on the interface, click to enable Manual Configuration mode. To remove the ability to manually configure Cisco TrustSec on the interface, click to disable Manual Configuration mode. The remaining fields on the page become unavailable for configuration. Default value: Enabled
Port SGT value	To configure a static authorization policy on this interface, enter an SGT tag value. Valid values: 2...65519
Trusted	Check to indicate that ingress traffic on the interface with this SGT should not have its tag overwritten.

**Table 92 - Configure Interface**

Field	Description
Propagate SGT	To allow the interface to transmit the SGT to the peer, click to enable the Propagate SGT function. To prevent the interface from transmitting the SGT to the peer, click to disable the Propagate SGT function. Disable the function when the peer is incapable of processing an SGT.
PMK	To enable Security Association Protocol (SAP), enter the pairwise-master key. The key is a hexadecimal value with an even number of characters and a maximum length of 32 characters. In Manual Configuration mode, SAP is disabled by default.
Mode List	To select SAP operation modes, click a mode in the Available Modes column to move it into the Selected Modes column. SAP operations modes: <ul style="list-style-type: none"> <li>• gcm encrypt—Authentication and encryption</li> <li>• gmac—Authentication, no encryption</li> <li>• no-encap—No encapsulation</li> <li>• null—Encapsulation, no authentication or encryption</li> </ul>

## Virtual Local Area Networks (VLANs)

A VLAN is a switched network segmented on a functional application rather than a physical or geographical basis. The isolation of different types of traffic helps to preserve the quality of the transmission and to minimize excess traffic among the logical segments. A VLAN also gives you the ability to control access and security to a group of devices independent of their physical location. For more information about VLANs, see the Ethernet Reference Manual, publication [ENET-RM002](#).

## Switch Virtual Interfaces (SVIs)

An SVI is a virtual interface in the switch that allows a VLAN to have an IP address and additional configuration. An SVI allows traffic to be routed out of a Layer 2 domain without requiring a physical interface.

You can configure SVIs via the WebUI with these restrictions:

- 8 SVIs total
- 1 SVI per VLAN
- 1 SVI per subnet

## Supported VLANs

The switch supports VLANs in VTP client, server, and transparent modes. VLANs are identified by a number from 1...4094:

- VLAN 1 is the default VLAN and is created during system initialization.
- VLAN IDs 1002...1005 are reserved for token rings and Fiber Distributed Data Interface (FDDI) switching.

All VLANs except 1002...1005 are available for configuration. All VLAN Trunking Protocol (VTP) versions support both normal and extended range VLANs, but the switch only propagates extended range VLAN configuration information with VTP version 3. When extended range VLANs are created in VTP versions 1 and 2, their configuration information is not propagated. Even the local VTP database entries on the switch are not updated, but the extended

range configuration information is created and stored in the running configuration file.

You can configure a maximum of 256 VLANs on the switch.

## Management VLAN

The management VLAN provides administrative access to the switch. VLAN 1 is the default VLAN and also the default management VLAN. During Express Setup, you can change the default VLAN ID for the management VLAN. To have administrative access to the switch, you must assign one of the switch ports to the management VLAN.

## Configure SVIs and VLANs via the WebUI

From the Configuration menu, choose VLAN.

Name	Admin Status	Operational Status	IPv4 Address	IPv6 Address	Description
<input type="checkbox"/> Vlan1	down	down	unassigned	Unassigned	
<input type="checkbox"/> Vlan3680	up	up	10.223.68.16	Unassigned	

From the VLAN page, you can configure SVIs, VLANs, and VLAN groups:

- To configure SVIs, see [page 152](#).
- To configure VLANs, see [page 154](#).
- To configure VLAN groups, see [page 154](#).

### Configure SVIs

From the SVI tab, you can add, edit, and delete SVIs:

- To add an SVI, click Add, complete the fields as described in [Table 93](#), and then click Apply to Device.
- To edit an SVI, click the interface in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an SVI, check its associated checkbox in the grid, and then click Delete.

**Table 93 - Create SVI**

Field	Description
VLAN Number	Enter a unique number to identify the VLAN. If you enter a VLAN number that does not exist, the switch creates a new VLAN. Be sure to assign ports to newly created VLANs. Valid values: 1...4094
Description	Enter a description for the VLAN.
Admin Status	Click to enable or disable the operational status of the interface: <ul style="list-style-type: none"> <li>Up—The interface is operational.</li> <li>Down—The interface is not operational.</li> </ul> Default value: Up
MTU (bytes)	Only populate this field if you specifically want to limit MTU on the associated VLAN. If this field is left blank, the SVI defaults to the global MTU, which is set in the System MTU (Bytes) field on General tab of the Administration   Device page. Enter the maximum transmission unit (MTU) for the VLAN. Valid values: 68...1500
IP Options	To configure an IPv4 SVI, check IPv4. To configure an IPv6 SVI, check IPv6. You can configure multiple IPv6 addresses on the same interface.
IPv4 Type	(Appears only for IPv4). Choose the IP address type: <ul style="list-style-type: none"> <li>Static</li> <li>DHCP</li> <li>Local Pool</li> </ul>
Host Name	(Appears only DHCP IPv4 types). (Optional) Enter the DHCP server address.
DHCP Pool List	(Appears only for Local Pool IPv4 types). Choose a DHCP pool from which to assign addresses.
IP Address	(Appears only Static IPv4 types). Enter the IP address for the SVI.
Subnet Mask	(Appears only for Static IPv4 types). Enter the subnet mask for the SVI.
Secondary IP	(Appears only for Static IPv4). Check Secondary IP
Static	(Appears only for IPv6). Choose an IPv6 address type, and then enter an IPv6 address or prefix. To add an address or prefix, click +.
DHCP	(Appears only for IPv6). Check DHCP to use the Rapid Commit feature.
Rapid Commit	(Appears only for DHCP IPv6 types). To allow a two-message exchange method for address assignment, check Rapid Commit.
AutoConfig	(Appears only for IPv6). To simplify the configuration, check AutoConfig, and then choose from the following: <ul style="list-style-type: none"> <li>None</li> <li>Default—If a default device is selected on this interface, a default route is installed.</li> </ul>
Act as an IPv6 DHCP Client	(Appears only for IPv6). To make the interface act as a DHCPv6 client, check the checkbox, and then enter a prefix name.



Configure VLANs

From the VLAN tab, you can add, edit, and delete VLANs:

- To add a VLAN, click Add, complete the fields as described in [Table 94](#), and then click Apply to Device.
- To edit a VLAN, click the VLAN in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a VLAN, check its associated checkbox in the grid, and then click Delete.

Create VLAN

VLAN ID\*

2-4094

Name

State

ACTIVATED

IGMP Snooping

DISABLED

Port Members

Q Search

Available (26)

Gi1/1

→

Gi1/2

→

Gi1/3

→

Gi1/4

→

Gi1/5

→

Associated (0)

No Associated Members

Cancel

Apply to Device

Table 94 - Create VLAN

Field	Description
VLAN ID	Enter a VLAN ID. Valid values: 2...4094
Name	Enter a name to identify the VLAN.
State	Click to activate or deactivate the VLAN.
IGMP Snooping	Click to enable or disable IGMP snooping on the VLAN.
Port Members	In the Available list, click one or more ports to move them to the Associated list and make them members of the VLAN.

Configure VLAN Groups

From the VLAN Group tab, you can add, edit, and delete VLAN groups:

- To add a VLAN group, click Add, complete the fields as described in [Table 95](#), and then click Apply to Device.
- To edit a VLAN group, click the group in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a VLAN group, check its associated checkbox in the grid, and then click Delete.

Create VLAN Group

VLAN Group Name\*

VLAN List\*

1-4094

(Ex: 1,2,5-7)

Cancel

Apply to Device

Table 95 - Create VLAN Group

Field	Description
VLAN Group Name	Enter a name to identify the VLAN group.
VLAN List	To map one VLAN or a range of VLANs to the group, enter VLAN IDs. For example, you can enter 1, 2, 5-7. Valid values: 1...4094

## Configure VLANs via the Logix Designer Application

In the navigation pane, choose Smartports and VLANs.

Module Properties: MyEN2T (1783-MMS10BE 1.001)

- General
- Connection
- Module Info
- Fault/Program Action
- Switch Configuration
- Switch Status
- Port Configuration
- PoE
- Smartports and VLANs**
- Port Security
- Port Status
- DHCP Pools
- DHCP Address Assignment
- Time Sync Configuration
- Time Sync Information
- NTP Client
- EtherChannels
- SD Flash Sync
- Save/Restore

Smartports and VLANs

Smartport and VLAN Assignment

Port	Smartport	VLAN Type and ID		
		Native	Access	Voice
Gi1/1	None			
Gi1/2	None			
Gi1/3	None			
Gi1/4	None			
Gi1/5	None			
Gi1/6	None			
Gi1/7	None			
Gi1/8	None			
Gi1/9	None			
Gi1/10	None			

VLAN Configuration

VLAN ID	Name	Delete	Edit
1	default		

New VLAN...

Refresh Communication

Set

Status: Running

OK

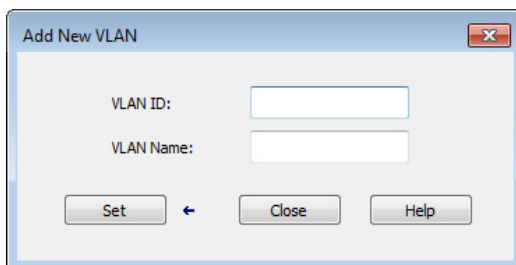
Cancel

Apply

Help

In the VLAN Configuration area, you can add, edit, and delete VLANs:

- To add a VLAN, click New VLAN, enter a VLAN ID and description, click Set, and then click Close.

A screenshot of a software dialog box titled "Add New VLAN". The dialog has a light blue header bar with a close button (X) in the top right corner. Inside the dialog, there are two text input fields: "VLAN ID:" and "VLAN Name:". Below these fields, there are three buttons: "Set", "Close", and "Help". A small blue arrow icon is positioned between the "Set" and "Close" buttons.

- To edit a VLAN, click the Ellipses icon in the Edit column, modify the fields, click Set, and then click Close.
- To delete a VLAN, click the Trash icon in the Delete column.

## Virtual Router Redundancy Protocol (VRRP)

The VRRP specifies an election protocol that assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address associated with a virtual router is called the Master and forwards packets sent to these IP addresses. The election process provides dynamic failover in the forwarding responsibility should the Master become unavailable. This allows any of the virtual router IP addresses on the LAN to be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

## VLAN Trunking Protocol (VTP)

VTP reduces administration and minimizes misconfiguration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. VTP avoids the need to configure the same VLAN on multiple switches in a network. For more information about VTP, see the Ethernet Reference Manual, publication [ENET-RM002](#).

### Requirements and Restrictions

Observe these guidelines:

- VTP has three versions. Only version 3 provides enhanced authentication, support for extended range VLAN (VLANs 1006...4094) database propagation, and support for any database in a domain. For example, version 3 can propagate Multiple Spanning Tree (MST) protocol database information. If extended VLANs are configured in the domain, you cannot convert from VTP version 3 to VTP version 2.
- Before configuring VTP, configure a trunk port so that the switch can send and receive VTP advertisements to and from other switches in the domain.

### VTP Modes

You can configure a switch to operate in the VTP modes described in [Table 97](#).

**Table 96 - VTP Modes**

Mode	Description
Server	You can create, modify, and delete VLANs, and specify other configuration parameters (such as the VTP version) for the entire VTP domain. VTP servers advertise their VLAN configurations to other switches in the same VTP domain. The servers also synchronize their VLAN configurations with other switches based on advertisements that are received over trunk links.
Off	The switch functions in the same manner as a VTP transparent switch, except that it does not forward VTP advertisements on trunks.
Client	A VTP client behaves like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another switch in the domain that is in server mode. Before adding a VTP client switch to a VTP domain, always verify that its VTP configuration revision number is lower than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. If you add a switch that has a revision number higher than the revision number in the VTP domain, it can erase all VLAN information from the VTP server and VTP domain.
Transparent	A VTP transparent switch does not participate in VTP. It does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2 or version 3, transparent switches do forward VTP advertisements that they receive from other switches through their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode. In VTP versions 1 and 2, the switch must be in VTP transparent mode when you create extended-range VLANs. VTP version 3 also supports creating extended-range VLANs in server mode only.

## Configure VTP via the WebUI

1. From the Configuration menu, choose VTP.
2. Complete the fields as described in [Table 97](#), and then click Apply to Device.

Configuration > Layer2 > VTP

Domain Name\*

Password

Version V3

VLAN Mode Server

MST Mode Transparent

Force ON

Primary ON

Apply

**Table 97 - VTP**

Field	Description
Domain Name	Enter a VTP domain name. The domain name is an ASCII string from 1...32 characters that identifies the VTP administrative domain for the device. The domain name is case sensitive.
Password	(Optional) Enter the administrative domain password. This password is for the generation of the 16-byte secret value that is used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case-sensitive.
Version	Choose the VTP version: <ul style="list-style-type: none"> <li>• V1—Supports only normal-range VLANs (VLAN IDs 1...1005).</li> <li>• V2—Supports only normal-range VLANs (VLAN IDs 1...1005).</li> <li>• V3—Supports the entire VLAN range (VLANs 1...4096).</li> </ul> The default version is 1.
VLAN Mode	Choose the VLAN mode. For a description of each mode, see <a href="#">Table 96 on page 157</a> . The default mode is Server. For Server mode, click the Primary field to indicate the operational state of the primary server: <ul style="list-style-type: none"> <li>• ON—Changes the operational state of a switch from a secondary server (the default) to a primary server and advertises the configuration to the domain.</li> <li>• OFF—Does not change the operational state of a switch from a secondary server (the default) to a primary server.</li> </ul>
MST Mode	(Optional, VTP version 3 only). Choose a VTP mode for the MST database. For a description of each mode, see <a href="#">Table 96 on page 157</a> . The default mode is Server. For Server mode, click the Primary field to indicate the operational state of the primary server: <ul style="list-style-type: none"> <li>• ON—Changes the operational state of a switch from a secondary server (the default) to a primary server and advertises the configuration to the domain.</li> <li>• OFF—Does not change the operational state of a switch from a secondary server (the default) to a primary server.</li> </ul>
Force	(Optional, VTP Version 3 only, and VLAN Server mode and MST Server mode only). Click to indicate whether to overwrite the configuration of any conflicting servers: <ul style="list-style-type: none"> <li>• ON—Overwrite configurations that conflict.</li> <li>• OFF—Do not overwrite configurations that conflict.</li> </ul>

---

## Notes:



## Administer the Switch

Topic	Page
Alarm Profiles	159
Alarm Settings	162
Back Up, Restart, and Restore Procedures	166
Common Industrial Protocol (CIP)	172
Command-line Interface (CLI)	172
Device Settings	174
Device Time	178
Domain Name System (DNS)	189
Dynamic Host Configuration Protocol (DHCP)	191
File Manager	199
HTTP/HTTPS/Netconf Access	201
MODBUS (Modicon Communication Bus)	201
Netconf Yang Configuration	202
Power over Ethernet (PoE)	204
PROFINET	208
SDM-Template	210
Simple Network Management Protocol (SNMP)	211
Software Upgrade	216
Stratix 5800 Boot Order	217
User Administration	218

### Alarm Profiles

Alarm profiles enable you to apply a group of alarm settings to multiple interfaces. These port-specific alarm settings specify the type of alarms and actions to trigger for the ports.

### Alarm Types

An alarm profile can include the following alarm types.

**Table 98 - Alarm Types for Alarm Profiles**

Alarm	Description
Link Fault	The switch triggers the alarm when problems with a port physical layer cause unreliable data transmission. A typical link fault condition is loss of signal or clock. The link fault alarm clears automatically when the link fault condition is clear. The severity for this alarm is error condition, level 3.



**Table 98 - Alarm Types for Alarm Profiles**

Alarm	Description
Port Not Forwarding	The switch triggers the alarm when a port is not forwarding packets. This alarm clears automatically when the port begins to forward packets. The severity for this alarm is warning, level 4.
Port Not Operating	The switch triggers the alarm when the port fails during the startup self-test. When triggered, the port not-operating alarm is only clear when the switch restarts and the port is operational. The severity for this alarm is error condition, level 3.
Fcs Bit Error Rate	The switch triggers the alarm when the actual frame check sequence (FCS) bit error-rate is close to the configured rate. You can set the FCS Threshold on the Port page under Administration > Alarm Settings in the WebUI. The severity for this alarm is error condition, level 3.

## Alarm Actions

For each port-specific alarm, you can trigger the following actions.

**Table 99 - Alarm Actions**

Alarm Action	Description
DM Alarms	Not available in the current release.
SNMP trap	Alarm traps are sent to an SNMP server. SNMP is enabled on the SNMP page under Administration > Management in the WebUI.
HW relay	The alarm relay is triggered for the switch, and the switch sends a fault signal to a connected external alarm device, such as a bell, light, or other signal device.
Syslog	Alarm traps are recorded in the syslog. You can view the syslog on the Syslog page under Troubleshooting in the WebUI.

## Default Alarm Profile

Express Setup configures all ports to use the default alarm profile called ab-alarm.

Edit Profile Instance

Name\*

ab-alarm

Alarm Name	DM Alarms	SNMP Trap	HW Relay	Syslog
Link Fault	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Port Not Forwarding	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Port Not Operating	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fcs Bit Error Rate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

## Create an Alarm Profile via the WebUI

From the Administration menu, choose Alarm Profiles.



From the Alarm Profiles page, you can add, edit, and delete alarm profiles:

- To add an alarm profile, click Add, complete the fields as described in [Table 100](#), and then click Apply to Device.
- To edit an alarm profile, click the profile in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an alarm profile, check its associated checkbox in the grid, and then click Delete.

Add Profile Instance

Name\*(1-32 Characters)

Alarm Name	DM Alarms	SNMP Trap	HW Relay	Syslog
Link Fault	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port Not Forwarding	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port Not Operating	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fcs Bit Error Rate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel

Apply to Device

Table 100 - Add Profile Instance

Field	Description
Name	Enter a unique profile name.
Alarm Name	See <a href="#">Alarm Types on page 159</a> .
DM Alarms	Check each type of action to trigger for the associated alarm type. See <a href="#">Alarm Actions on page 160</a> .
SNMP Trap	
HW Relay	
Syslog	

## Alarm Settings

The switch monitors alarm conditions on a per-port or a global basis. If conditions on the switch or on a port do not match the parameters that you configure for an alarm, the switch triggers an alarm or a system message.

### External Alarm Devices

You can configure the switch to trigger an external alarm device by using the alarm relay. The switch supports one alarm output with both a normally closed and a normally open contact. The switch software is configured to detect faults, which are used to energize the relay coil and, change the state on both of the relay contacts. You can wire the external alarm to be triggered when the circuit is open or closed.

### Global Alarm Types

You can configure the following types of global alarms on the switch.

**Table 101 - Global Alarm Types**

Alarm	Description
Power Supply	The switch triggers the alarm if a power supply fails or is missing. The alarm clears when the power supply is present or working.
Temperature—Primary	The switch triggers the primary alarm when the system temperature is higher or lower than the configured thresholds. By default, this alarm cannot be disabled. You can change the default temperature thresholds by entering new values. Default high threshold value: +90 °C (+194 °F) Default low threshold value: -40°C (-40°F) Valid threshold range: -55...+125°C (-67...+257°F)
Input—Alarm 1 Input—Alarm 2	The switch triggers the two input alarms based on the alarm relay configuration.
SD-Card	The switch triggers the alarm when the SD Card is removed and it is cleared when it is inserted. <sup>(1)</sup>
Temperature—Secondary	The switch triggers the secondary alarm when the system temperature is higher or lower than the configured thresholds. By default, this alarm is disabled. You can change the default temperature thresholds by entering new values. Default high threshold value: +90 °C (+194 °F) Default low threshold value: 0°C (+32°F) Valid threshold range: -55...+125°C (-67...+257°F)

(1) To enable the HW Relay alarm for SD-card, the DM alarm also needs to be enabled.

### Alarm Actions for Global Alarms

For each global alarm, you can trigger the following actions.

Alarm Action	Description
DM alarm	Not available in the current release.
SNMP trap	Alarm traps are sent to an SNMP server. SNMP is enabled on the SNMP page under Administration > SNMP in the WebUI.
HW relay	The alarm relay is triggered for the switch, the switch sends a fault signal to a connected external alarm device, such as a bell, light, or other signal device.
Syslog	Alarm traps are recorded in the syslog. You can view the syslog on the Syslog page under Troubleshooting in the WebUI.

## Configure Alarm Settings via the WebUI

To configure alarm settings, from the Administration menu, choose Alarm Settings.

From the Alarm Settings page, you can configure alarm relays, global alarms, and port alarms:

- To configure alarm relays, see [page 163](#).
- Configure global alarms, see [page 164](#).
- Configure port alarms, see [page 165](#).

### Configure Alarm Relays

On the Alarm Relay Setup tab, complete the fields as described in [Table 102](#). When you make changes, a message appears in the lower-right corner of the WebUI to confirm that the configuration was successfully applied.

**Table 102 - Alarm Settings—Alarm Relay Setup**

Field	Description
Output Relay	Click to determine the normal state of the output relay circuit: <ul style="list-style-type: none"> <li>• Opened—When an alarm state occurs, the output relay circuit closes.</li> <li>• Closed—When an alarm state occurs, the output relay circuit opens.</li> </ul>
Input Relay 1	Click to determine the normal state of input relay 1: <ul style="list-style-type: none"> <li>• Opened—An alarm triggers when the input relay circuit closes.</li> <li>• Closed—An alarm triggers when the input relay circuit opens.</li> </ul>
Input Relay 2	Click to determine the normal state of input relay 2: <ul style="list-style-type: none"> <li>• Opened—An alarm triggers when the input relay circuit closes.</li> <li>• Closed—An alarm triggers when the input relay circuit opens.</li> </ul>

Configure Global Alarms

On the Global tab, you can change the frame check sequence (FCS) error hysteresis threshold and edit global alarms:

- To change the (FCS) error hysteresis threshold, enter a percentage value from 1...10 and click Apply to Device. The default value is 10 percent.

The frame check sequence (FCS) error hysteresis threshold is used to determine when an alarm condition is cleared. This value is expressed as a percentage of fluctuation from the FCS bit error rate. You can adjust the percentage to help prevent toggling the alarm condition when the FCS bit error rate fluctuates near the configured bit error rate. You can also configure this setting for individual ports.



- To edit a global alarm, click the alarm in the grid, complete the fields as described in [Table 103](#), and then click Update & Apply to Device.

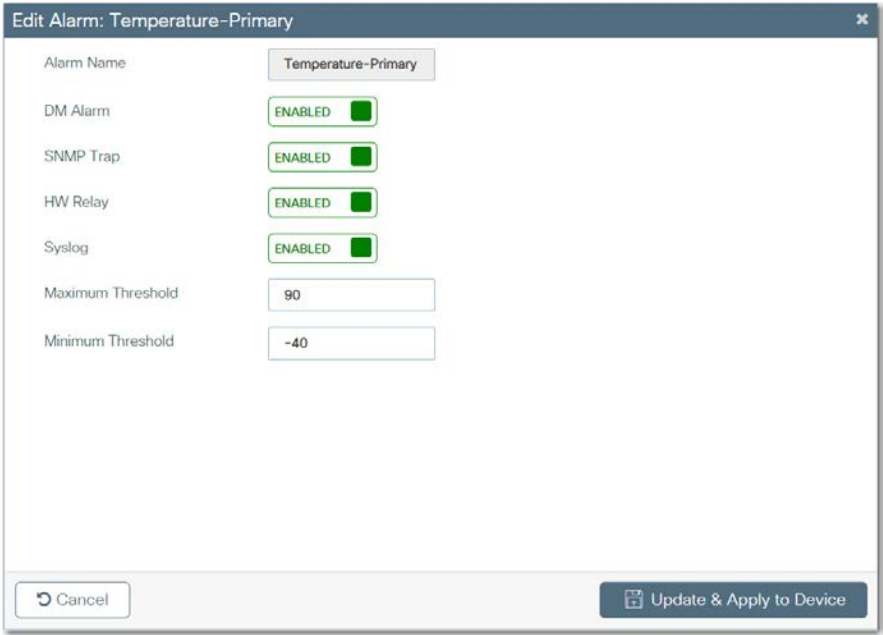


Table 103 - Alarm Settings—Global

Field	Description
Alarm Name	(System-generated). Displays the name of the global alarm. See <a href="#">Global Alarm Types on page 162</a> .
DM Alarm	Click to enable or disable the action from being triggered by the associated alarm type. See <a href="#">Alarm Actions for Global Alarms on page 162</a> .
SNMP Trap	
HW Relay	
Syslog	
Max Threshold in °C	Enter a maximum temperature in degrees Celsius. Valid threshold range: -55...+125°C
Min Threshold in °C	Enter a minimum temperature in degrees Celsius. Valid threshold range: -55...+125°C

### Configure Port Alarms

On the Port tab, you can view and edit port alarms.



To edit a port alarm, on the Port tab, click the alarm in the grid, complete the fields as described in [Table 104](#), and click Update & Save to Device.

Edit Alarm: GigabitEthernet1/1

Port Name

GigabitEthernet1/1

Alarm Profile

ab-alarm

FCS Threshold

8

Cancel

Update & Apply to Device

Table 104 - Alarm Settings—Port

Field	Description
Port Name	Displays the port type and number.
Alarm Profile	Choose an alarm profile. The default profile that is configured via Express Setup is ab-alarm.
FCS Threshold	Enter a percentage value from 6...8. This value is expressed as a percentage of fluctuation from the FCS bit error rate. You can adjust the percentage to help prevent toggling the alarm condition when the FCS bit error rate fluctuates near the configured bit error rate. You can also configure this setting at the global level. Default value: 8

## Back Up, Restart, and Restore Procedures

You can perform these procedures on the switch:

- Back up and restore configuration files.
- Restart the switch and choose whether to save the running configuration, discard the running configuration, or reset the configuration to factory default.
- Sync the SD card with the internal memory of the switch.

### Back Up and Restore Configuration Files via the WebUI

Configuration files contain the IOS software commands that are used to customize the functionality of your switch. The WebUI uses these configuration files:

- The Startup configuration file (startup-config) is used during system startup to configure the software.
- The Running configuration file (running-config) contains the current configuration of the software.

The two configuration files can be different. For example, you can change the configuration for a short time period rather than permanently.

---

<b>IMPORTANT</b>	Changes made to the Running configuration are lost after you restart the switch. The switch uses its Startup configuration after a power cycle.
------------------	---

---

1. From the Administration menu, choose Backup & Restore.

On the Config File Management tab, you can copy configuration files to the switch or from the switch.

2. Complete the fields as described in [Table 105](#).
3. If you are copying a file to the switch, click Upload File.

or

If you are copying a file from the switch, click Download File.

4. To reload the switch, click Reload.

---

<b>IMPORTANT</b>	A downloaded configuration does not take effect until after a reload.
------------------	---

---

Administration > Management > Backup & Restore

Config File Management   Sync

Copy To Device ▼

File Type Configuration ▼

Transfer Mode TFTP ▼

Backup existing startup config to flash? ☒ Yes ☐ No

**Server Details**

IP Address (IPv4/IPv6)\*

File Path

File Name\*

✓ Download File ↻ Reload

Table 105 - Backup &amp; Restore—Config File Management

Field	Description
Copy	Choose whether to copy the configuration file to the device or from the device: <ul style="list-style-type: none"> <li>To Device (default)</li> <li>From Device</li> </ul>
File Type	Choose Configuration.
Transfer Mode	Choose the protocol to use for the file transfer: <ul style="list-style-type: none"> <li>TFTP (default)</li> <li>SFTP</li> <li>FTP</li> <li>HTTP</li> </ul>
Back up existing startup config to flash	If you chose to transfer a file to the device, click whether to back up the existing startup config to flash: <ul style="list-style-type: none"> <li>Yes—The switch saves the current startup configuration in its internal memory as a backup.</li> <li>No—The switch does not save the current startup configuration.</li> </ul>
<b>Server Details</b>	
IP Address (IPv4/IPv6)	(Appears only for TFTP, SFTP, and FTP transfers.) Enter the IP address of the TFTP or FTP server.
File Path	(Appears only for TFTP, SFTP, and FTP transfers.) Enter the file location for the configuration file on the TFTP, FTP server.
File Name	(Appears only for TFTP, SFTP, and FTP transfers.) Enter the name of the configuration file to transfer.
Server Login UserName	(Appears only for SFTP transfers.) Type the user name of the server to be accessed.
Server Login Password	(Appears only for SFTP transfers.) Type the password of the server to be accessed.
Logon Type	(Appears only for FTP transfers.) Choose the type of logon required to access the FTP site: <ul style="list-style-type: none"> <li>Anonymous (default)</li> <li>Authenticated</li> </ul>
Source File Path	(Appears only for HTTP transfers.) Click Select File and then browse to the .config file.



## Restart the Switch via the WebUI

You can restart the switch with or without saving the Running configuration to the Startup configuration. You can also reset the switch to its factory default state.

1. From the Administration menu, choose Reload.
2. Click an option as described in [Table 106](#), and then click Apply to Device.

Administration > Reload

☒ Save Configuration and Reload.
 ☐ Reload without Saving Configuration.
 ☐ Reset to Factory Default and Reload.
 Apply

**Table 106 - Backup & Restore—Reload**

Field	Description
Save Configuration and Reload	Click to restart the switch and save the Running configuration to the Startup configuration. The current Running configuration is retained when the switch restarts.
Reload without Saving Configuration	Click to restart the switch without saving the Running configuration. The switch restarts with the Startup configuration stored in its internal memory.
Reset to Factory Default and Reload	Click to restart the switch and overwrite all applied and saved configuration parameters and return to the factory default. You are prompted for confirmation to reset the configuration. All configuration data files are deleted, and the device is restored to its factory default state when the switch restarts. To restore the base configuration, you can run Express Setup on the switch.

## Sync the Switch with an SD Card or USB Device via the WebUI

You can use either an SD card or a USB device with the switch to do the following:

- Update or restore configuration settings with chosen device instead of the internal memory of the switch.
  - Start up the switch with the configuration on the chosen device.
  - Copy the IOS image file and Startup configuration file from your computer or from the switch to the chosen device. You can then use the chosen device to copy the IOS image file and Startup configuration file to other switches.
1. From the Administration menu, choose Backup & Restore.
  2. Click the Sync tab.
  3. Click an option to synchronize the configuration and image files between the chosen device and internal memory of the switch:
    - If the switch started up from the chosen device, click to synchronize the files from the chosen device to internal memory.
    - If the switch started up from internal memory, click to synchronize the files from internal memory to the chosen device.
  4. To synchronize the device configuration file, click Sync Configuration.
  5. To synchronize the IOS file, click Sync IOS Image.

**IMPORTANT** The sync cannot be performed between SD card and USB device.

Administration &gt; Management &gt; Backup &amp; Restore

Config File Management Sync

Device Flash → sdflash:




 <p>Device Flash</p> <ul style="list-style-type: none"> <li>✓ Card Present : Yes</li> <li>✓ Booted from : Yes</li> <li>Free Space : 375.2 MB</li> </ul>	<p>Sync Status</p> <ul style="list-style-type: none"> <li>✗ Configuration not in sync</li> <li>✓ IOS Image in sync</li> </ul>	 <p>SD Card</p> <ul style="list-style-type: none"> <li>✓ Card Present : Yes</li> <li>Free Space : 7.0 GB</li> </ul>
--	---	--

Config File Management Sync

Device Flash → usbflash0:




 <p>Device Flash</p> <ul style="list-style-type: none"> <li>✓ Card Present : Yes</li> <li>✓ Booted from : Yes</li> <li>Free Space : 375.2 MB</li> </ul>	<p>Sync Status</p> <ul style="list-style-type: none"> <li>✗ Configuration not in sync</li> <li>✗ IOS Image not in sync</li> </ul>	 <p>USB Flash</p> <ul style="list-style-type: none"> <li>✓ USB Flash Present : Yes</li> <li>Free Space : 14.7 GB</li> </ul>
--	---	---

## Back Up, Restore, and Sync Configuration Files via the Logix Designer Application

The Logix Designer application uses these configuration files:

- Text file with configuration parameters (config.text)
- Binary file with VLAN information (vlan.dat)

You can sync the configuration files between the switch and an SD card or save and restore the configuration files.

### Sync Configuration Files with an SD Card

1. In the navigation pane, click SD Flash Sync.
2. Complete the fields as described in [Table 107](#), and then click Apply.

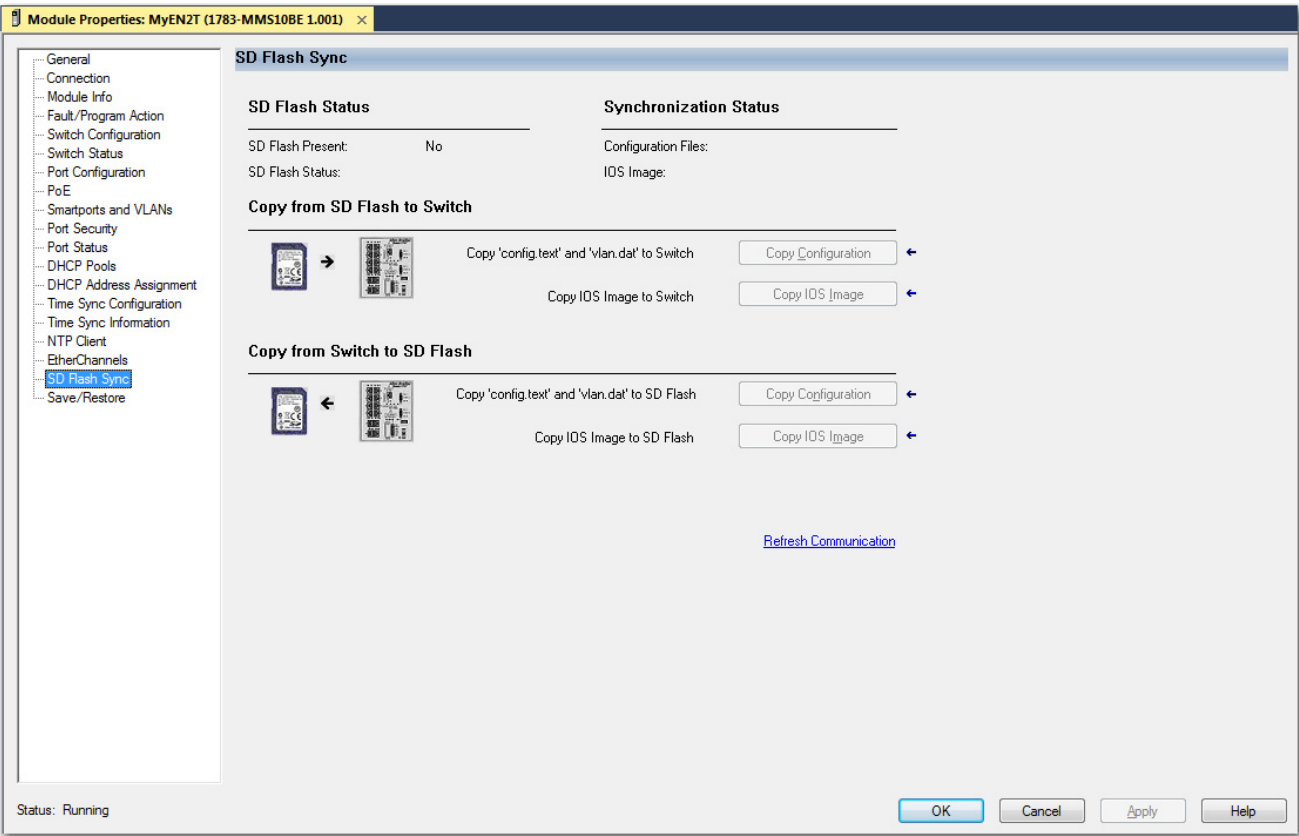
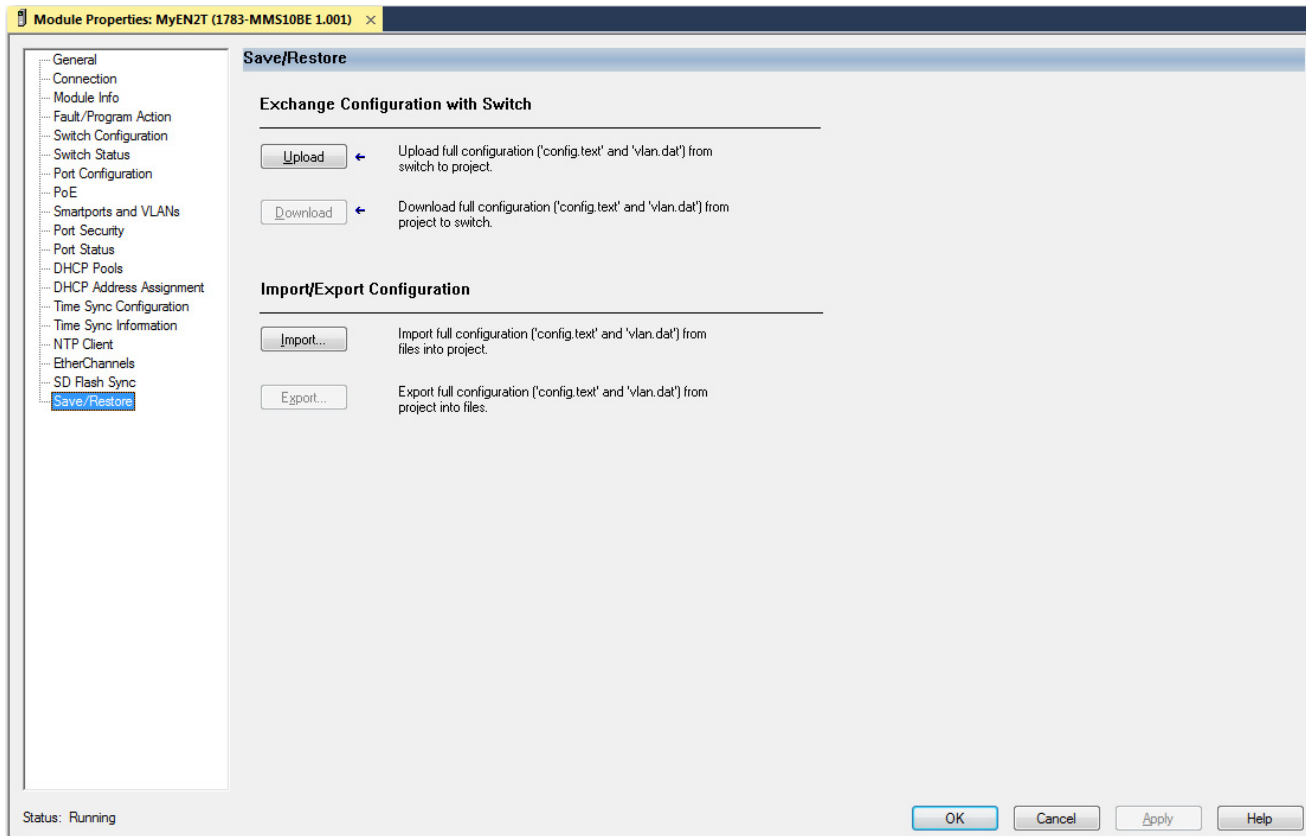


Table 107 - SD Flash Sync

Field	Description
SD Flash Status	Indicates whether the SD card is present and the status of the card
Synchronization Status	Indicates whether the configuration files and the IOS are synchronized or unsynchronized.
Copy from SD Flash to Switch	Click to sync one of the following from the SD card to the switch: <ul style="list-style-type: none"><li>• Copy Configuration</li><li>• Copy IOS Image</li></ul>
Copy from Switch to SD Flash	Click to sync one of the following from the switch to the SD card: <ul style="list-style-type: none"><li>• Copy Configuration</li><li>• Copy IOS Image</li></ul>

*Save and Restore Configuration Files*

1. In the navigation pane, click Save/Restore.
2. Perform the following save and restore actions as needed, and then click Apply:
  - To restore a configuration that is stored on your local computer to the controller project, click Import.
  - To save the configuration that is stored in the controller project to your computer, click Export.
  - To copy the configuration from the switch to the controller project, click Upload.
  - To download the configuration from the controller project to the switch, click Download.



# Common Industrial Protocol (CIP)

CIP™ is a messaging protocol for devices in industrial automation control systems. CIP is the application layer for the EtherNet/IP™ network. For more information about CIP, see the Ethernet Reference Manual, publication [ENET-RM002](#).


## Configure CIP via the WebUI


**IMPORTANT** To manage the switch via the Logix Designer application, CIP must be enabled on the switch.

To configure CIP on the switch, from the Administration menu, choose CIP.

Administration ▾ > Industrial Protocols ▾ > CIP

CIP Status

ENABLE 



CIP VLAN

3680 ▾

IP Address

10.223.68.16

Subnet Mask

255.255.255.0

CIP Password

\*\*\*\*\*

Confirm CIP Password\*

\*\*\*\*\*

Table 108 - CIP

Field	Description
CIP Status	Click to enable or disable CIP messaging.
CIP VLAN	Choose a CIP VLAN. CIP can be enabled on only one VLAN.
IP Address	Displays the IP address and subnet mask for the CIP connection on the VLAN you chose in the CIP VLAN field. To change these values, modify the SVI on the Configure > VLAN page.
Subnet Mask	
CIP Password	Enter a CIP password.
Confirm CIP Password	Reenter the CIP password to confirm it.

# Command-line Interface (CLI)

Apart from software and web-based applications, you can manage the switch via the Cisco® command-line interface (CLI). The CLI enables you to execute Cisco IOS commands. Technical Support representatives from Rockwell Automation can also use the CLI to troubleshoot the switch. For more information about the CLI, refer to [www.cisco.com](http://www.cisco.com).

For other Stratix® switches, the CLI is accessible only via a console port, Telnet session, or Secure Shell (SSH) session. For Stratix 5800 switches, the CLI is available via the same methods as other switches, but they also provide access to the CLI via the WebUI.

## CLI Modes

Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode you are currently in. The WebUI provides two command modes:

- **Exec mode**—Most commands in Exec mode are one-time commands. For example, show commands provide important status information, and clear commands clear counters or interfaces.
- **Configure mode**—Configure mode enables you to make changes to the running configuration.

## Run CLI Commands via the WebUI

From the Administration menu, choose Command Line Interface.

Administration > Command Line Interface

☒ Exec ☐ Configure

Run Command Clear Copy Export

Enter The Exec Command Here

Control+X: Clear | Control+M: Switch Mode | Control+Return(⏏): Execute Command | Control+Y: Copy | Control+Shift+E: Export | Shift+Up Arrow(↑)/Down Arrow(↓): Lookup History

From the Command Line Interface page, you execute and manage commands:

- To run a command, click a CLI mode, enter the command in the text box, and then click Run Command. The command output appears in the bottom area of the page.
- To delete commands or output, click Clear.
- To copy the command output to your clipboard, click Copy.
- To export the command output to a text file on your local computer, click Export.

# Device Settings

Device settings are system-wide values for the switch.

## Configure Device Settings via the WebUI

From the Administration menu, choose Device.

Administration ▾ > Device

General

FTP/SFTP/TFTP

Host Name\*

S5800-68-16

Apply

Banner

Stratix 5800 Ethernet Managed Switch

System MTU(Bytes)

1500

VTY Line

Ex: 0 or 0-97

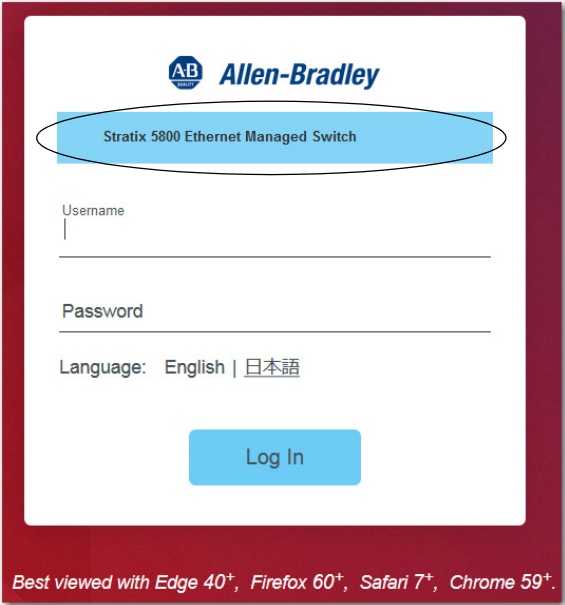
View VTY options

VTY Transport Mode

Select a value ▾

On the General tab, complete the fields as described in [Table 109](#), and then click Apply to Device.

Table 109 - Device Settings—General

Field	Description
Host Name	Enter a unique name to identify the switch.
Banner	<div>To display a message on the Login page of the WebUI, enter the text to appear in the banner area, as shown in the following example.</div> <div></div>
System MTU (Bytes)	Enter the maximum transmission unit (MTU) value in bytes for all interfaces on the switch that operate at 10 or 100 Mbps. Valid values: 1500...1998 Default value: 1500
VTY Line	Enter the virtual terminal line (VTY) line number or a range.
VTY Transport Mode	Choose a transport mode for the VTY: <ul style="list-style-type: none"><li>• Telnet &amp; SSH</li><li>• Telnet</li><li>• SSH</li><li>• None</li></ul>

On the FTP/TFTP tab, complete the fields in [Table 110](#), and then click Apply.

**Table 110 - Device Settings—FTP/SFTP/TFTP**

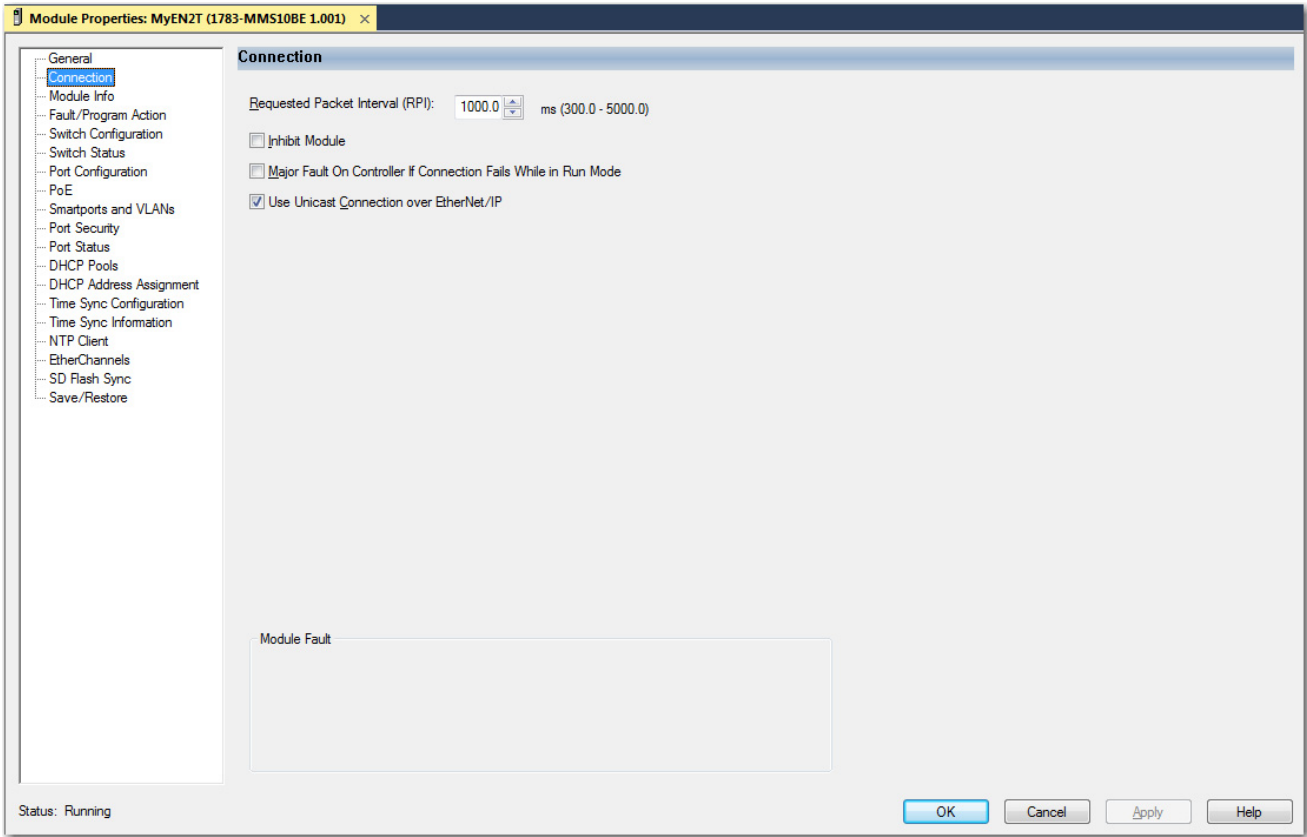
Field	Description
<b>FTP Settings</b>	
Source Interface	Choose the interface on the switch to use during any FTP session.
User name	Enter the user name.
Password	Enter the password.
<b>SFTP Settings</b>	
Source Interface	Choose the interface on the switch to use during any SFTP session.
<b>TFTP Settings</b>	
Source Interface	Choose the interface on the switch to use during any TFTP session.
User name	Enter the user name.
Password	Enter the password.

## Configure Device Settings via the Logix Designer Application

### Configure Connection Properties

1. In the navigation pane, click Connection.
2. Complete the fields as described in [Table 111](#), and then click Apply.





**Table 111 - Connection Fields**

Field	Description
Requested Packet Interval (RPI)	Enter a value between 300...5000.
Inhibit Module	Check to disable communication between the controller and the switch. Clear the checkbox to restore communication.
Major Fault on Controller If Connection Fails While in Run mode	Check to have the controller create a major fault if connection fails in Run mode.
Use Unicast Connections over EtherNet/IP	Check to use Unicast connections with the EtherNet/IP network.
Module Fault	Displays the fault code from the controller and the text that indicates the module fault has occurred.

*Configure Switch Information*

In the navigation pane, click Switch Configuration.

3. Complete the fields as described in [Table 111](#), and then click Apply.

**Module Properties: MyEN2T (1783-MMS10BE 1.001)**

**Switch Configuration**

**Internet Protocol (IP) Settings**

☒ Manually Configure IP settings  
☐ Obtain IP settings automatically using DHCP

**IP Settings Configuration**

Physical Module IP Address: 192 . 168 . 1 . 58      Subnet Mask: 255 . 255 . 255 . 0  
 Gateway Address: 192 . 168 . 1 . 1  
 Domain Name:       Primary DNS Server Address: 0 . 0 . 0 . 0  
 Host Name: SwitchPetra      Secondary DNS Server Address: 0 . 0 . 0 . 0

**Administration**

Contact:   
 Geographic Location:   
 Management Interface VLAN: 1

Spanning Tree Mode:  
☒ Rapid Spanning Tree Protocol/Multiple Spanning Tree (RSTP/MST)  
☐ Per-VLAN Spanning Tree Plus (PVST+)  
☐ Rapid Per-VLAN Spanning Tree Plus (RPVST+)  
☒ Enable Dual Power Supply Alarm

[Refresh Communication](#)   

Status: Running

Table 112 - Switch Configuration

Field	Description
<b>Internet Protocol (IP) Settings</b>	
Manually configure IP settings or Obtain IP settings automatically using DHCP	<p>Click the method to use for assigning the switch an IP address:</p> <ul style="list-style-type: none"> <li>Manually Configure IP settings (default)—The switch uses a manually assigned, static IP address. If the switch has a static IP address and your network uses a DHCP server, make sure that the IP address is not within the range of DHCP address pool. Otherwise, IP address conflicts can occur between the switch and another device.</li> <li>Obtain IP settings automatically using DHCP—A Dynamic Host Configuration Protocol (DHCP) server automatically assigns the switch an IP address, subnet mask, and default gateway. Unless restarted, the switch continues to use the DHCP-assigned information. We recommend that you manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the switch.</li> </ul>
<b>IP Settings Configuration</b> —Applies to manually assigned IP addresses.	
Physical Module IP Address	<p>Enter the IP address for the switch. This value must match the IP address on the General view. If you change the assigned IP address, make sure that the new IP address is not assigned to another device in your network. The IP address and the default gateway cannot be the same.</p> <p><b>IMPORTANT:</b> If you reconfigure your switch with another IP address, you can lose communication with the switch when you click Apply. To correct this problem, you must return to the Express Setup and General view, set the new IP address, and download to the controller.</p>
Subnet Mask	<p>Enter the subnetwork (subnet) for the switch. Subnets are used to segment the devices in a network into smaller groups. The subnet mask is a 32-bit number. Set each octet between 0...255. The default is 255.255.255.0.</p>
Gateway Address	<p>Enter the gateway address for the switch. A gateway is a router or a dedicated network device that enables the switch to communicate with devices in other networks or subnetworks. The default gateway IP address must be part of the same subnet as the switch IP address. The switch IP address and the default gateway IP address cannot be the same. If all of your devices are in the same network and a default gateway is not used, you do not need to enter an IP address in this field. If your network management station and the switch are in different networks or subnetworks, you must specify a default gateway. Otherwise, the switch and your network management station cannot communicate with each other.</p> <p><b>IMPORTANT:</b> Communication is disrupted when you change the gateway (IP) address.</p>
Primary DNS Server Address	Enter the IP addresses of the primary domain name system (DNS) IP server available to a DHCP client.
Secondary DNS Server Address	Enter the secondary domain name system (DNS) IP server available to a DHCP client.
Host Name	Enter a name to identify the switch. The name can be up to 64 characters and can include alphanumeric and special characters (comma and dash).
<b>Administration</b>	

Table 112 - Switch Configuration (Continued)

Field	Description
Contact	(Optional). Enter contact information for the switch. The contact information can include a maximum of 200 characters, alphanumeric and special characters (dash and comma), and a carriage return.
Geographic Location	(Optional). Enter a geographic location of the switch. The geographic location can include a maximum of 200 characters, alphanumeric and special characters (dash and comma), and a carriage return.
Management Interface VLAN	Displays the VLAN through which the switch is managed. The management VLAN is the broadcast domain through which management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that must be limited to a specific group of users, such as the administrators of your network. It also provides secure administrative access to all devices in the network. <b>IMPORTANT:</b> Be sure that the switch and your network management station are in the same VLAN. Otherwise, you can lose management connectivity to the switch.
Spanning Tree Mode	See <a href="#">Configure STP via the Logix Designer Application on page 141</a> .
Enable Dual-Power Supply Alarm	To enable dual-power supply alarms, check the checkbox.

## Device Time

You can set the time on the switch by using the following methods:

- Set the time manually
- Set the time via a Network Time Protocol (NTP) server
- Set the time via Precision Time Protocol (PTP), known as CIP Sync™ Time in the Logix Designer application

### Set Time Manually

If you do not use a network-based method of synchronizing time, such as NTP or PTP, you can set the time of the switch by using these methods:

- Sync the switch time with the time on your computer
- Manually complete the fields in the WebUI

---

**IMPORTANT** Manual time settings override time and date settings from the NTP server.

---

### Set Time via NTP

Network Time Protocol (NTP), defined in RFC 1305, synchronizes clocks across packet-based networks. NTP uses a two-way time transfer mechanism between a master and a slave. For more information about NTP, see the Ethernet Reference Manual, publication [ENET-RM002](#).

### Set Time via PTP

CIP Sync time synchronization refers to the IEEE 1588 standard for Precision Time Protocol (PTP). The protocol enables precise synchronization of clocks in measurement and control systems. Clocks are synchronized with nanosecond accuracy over the EtherNet/IP communication network. PTP enables systems that include clocks of various precisions, resolution, and stability to synchronize. PTP generates a master-slave relationship among the clocks in the system. All clocks ultimately derive their time from a clock that is selected as the Grandmaster clock. For more information about PTP and CIP Sync, see the Ethernet Reference Manual, publication [ENET-RM002](#).

[Table 113](#) describes the PTP modes that you can apply to a Stratix 5800 switch.

**Table 113 - PTP Modes**

PTP Mode	Description
Forward	The switch passes PTP packets as normal multicast traffic. All switch ports are enabled by default.
Boundary	Allows the switch to participate in selecting the best master clock. If the switch does not detect a better clock, it becomes the Grandmaster clock and parent clock to all connected devices. If the best master is to be a clock that is connected to the switch, the switch becomes a child to that clock, and acts as a parent clock to devices connected to other ports. The clock selection process is determined in part by the relative priority of the switches in the network.
End to End Transparent	The switch transparently synchronizes all clocks with the master clock that is connected to it. All ports are enabled by default. The switch corrects the delay that is incurred by every packet passing through it (referred to as residence time). This mode causes less jitter and error accumulation than Boundary mode.
GMC-BC	This mode is also known as NTP-PTP Clock mode. Allows the switch to act as a Grandmaster. Derives PTP clock time from an NTP time source. If not the Grandmaster, the switch operates in Boundary mode.

## Configure Device Time via the WebUI

From the Administration menu, choose Time.

Administration > Time

Source: NTP Jul 10, 2019

MON TUE **WED** THU FRI SAT SUN

**16:34:41**  
(UTC+00:00) Casablanca, Dublin, ...

[Sync with System Time](#) [Change Date and Time](#)

System Time: 12:34:41 Jul 10, 2019 (UTC -04:00)

**NTP**

PTP

**NTP Server Details**

[+ Add](#) [× Delete](#) [Refresh NTP Table](#)

	Host Name	Status	Source Address
<input type="checkbox"/>	10.80.1.41	Synchronized	None

1 - 1 of 1 items

From the Time page, you can set time manually, via NTP, or via PTP:

- To set time manually, see [page 179](#).
- To set time via NTP, see [page 180](#).
- To set time via PTP, see [page 181](#).

### Set Time Manually

- To synchronize the time on the switch with the time on your computer, click Sync with System Time.

The WebUI session is re-established and you are redirected to the login page.

- To enter date and time settings manually, click Change Date and Time, complete the fields as described in [Table 114](#), and then click Apply to Device.

Date and Time Setting

Date

10 Sep 2019

Time

18:30:25

Time Zone

(UTC+00:00) Casablanca, Dublin, Lisbon, London, Edinburgh

Daylight Savings

☒

From

Monday

1

January

HH:MM

To

Monday

1

January

HH:MM

Cancel

Apply to Device

Table 114 - Date and Time Setting

Field	Description
Date	Enter the date and time to set on the device.
Time	
Time Zone	From the pull-down menu, choose a time zone. Default value: Coordinated Universal Time (UTC)
Daylight Saving	Check to set the Daylight Saving observance period.
From	From the Day, Week, and Month pull-down menus, choose the beginning date of Daylight Saving observance, and then enter the Time of day.
To	From the Day, Week, and Month pull-down menus, choose the end date of Daylight Saving observance, and then enter the Time of day.

Set Time via NTP

On the Time page, click NTP.

NTP

PTP

NTP Server Details

+ Add

✕ Delete

Refresh NTP Table

	Host Name	Status	Source Address
<input type="checkbox"/>	10.80.1.41	Synchronized	None

1

20 items per page

1 - 1 of 1 items

Under NTP Server Details, you can add, edit, and delete NTP servers.

- To add an NTP server, click Add, complete the fields as described in [Table 115](#), and then click Apply to Device.
- To edit an NTP server, click the server in the grid, modify the fields, and then click Update & Apply to Device.
- To delete an NTP server, check its associated checkbox in the grid, and then click Delete.
- To reload the NTP server details, click Refresh NTP Table.

Create NTP Server

Host Name\*

Prefer

☐

IP for DNS Resolution

None

Source Address

None

Cancel

Apply to Device

Table 115 - Create NTP Server

Field	Description
Host Name	Enter the host name or IP address to identify the NTP server.
Prefer	Check Prefer to make this server the preferred server if multiple servers are synchronized.
IP for DNS Resolution	Choose an IP protocol to resolve the DNS server name: <ul style="list-style-type: none"> <li>None (default)</li> <li>IP—Uses an IPv4 address.</li> <li>IPv6—Uses an IPv6 server address.</li> </ul>
Source Address	Choose the source to use for establishing a connection to the NTP server. <ul style="list-style-type: none"> <li>None (default)—The switch automatically chooses a source.</li> <li>Vlan</li> <li>Interface</li> </ul>
Vlan	If you chose VLAN in the Source Address field, choose a VLAN ID from the list.
Interface	If you chose Interface in the Source Address field, choose an interface from the list.

### Set Time via PTP

On the Time page, click the PTP tab.

NTP

PTP

PTP Details

Mode

Boundary

Priority1

128

Priority2

128

Configure

Apply to Device

Interface	State	Enabled	Delay Request Interval	Announce Timeout	Announce Interval	Sync Interval	Sync Fault Limit	VLAN ID
Gi1/1	FAULTY	TRUE	5	3	1	0	500000	N/A
Gi1/2	FAULTY	TRUE	5	3	1	0	500000	N/A
Gi1/3	DISABLED	FALSE	5	3	1	0	500000	N/A
Gi1/4	FAULTY	TRUE	5	3	1	0	500000	N/A
Gi1/5	MASTER	TRUE	5	3	1	0	500000	N/A
Gi1/6	FAULTY	TRUE	5	3	1	0	500000	N/A

To configure PTP in NTP-PTP Clock mode, follow these steps.

1. Be sure that you have an NTP server configured as described in [Set Time via NTP on page 180](#).
2. From the Mode pull-down menu, choose NTP-PTP Clock.
3. Click Apply to Device.

To configure PTP in Boundary mode, follow these steps.

1. From the Mode pull-down menu, choose Boundary.

- 2. In the Priority1 field, enter a priority value in the range of 0...255 to override the default criteria (clock quality, clock class, and so on) for best master clock selection.

A lower value takes precedence. The default value is 128.

- 3. In the Priority2 field, enter a second priority in the range of 0...255 to use as a tie-breaker between two devices that are otherwise equally matched in the default criteria.

For example, you can give a specific switch priority over other identical switches.

- 4. Click Apply to Device.
- 5. Click Configure.

The screenshot shows the 'Configure PTP' window. On the left, there is a section for 'Interface' with a list of disabled interfaces (0) and a list of enabled interfaces (26). Below this are buttons for 'Enable All', 'Disable All', and 'Cancel'. The main part of the window is a table with the following columns: Interface, Delay Request Interval, Announce Timeout, Announce Interval, Sync Interval, and Sync Fault Limit. The table lists seven interfaces: Gi1/1 through Gi1/7. Each interface has corresponding input fields for the PTP settings, all of which are currently set to default values: Delay Request Interval is 5, Announce Timeout is 3, Announce Interval is 1, Sync Interval is 0, and Sync Fault Limit is 500000. At the bottom right, there is an 'Apply to Device' button.

Interface	Delay Request Interval	Announce Timeout	Announce Interval	Sync Interval	Sync Fault Limit
Gi1/1	5	3	1	0	500000
Gi1/2	5	3	1	0	500000
Gi1/3	5	3	1	0	500000
Gi1/4	5	3	1	0	500000
Gi1/5	5	3	1	0	500000
Gi1/6	5	3	1	0	500000
Gi1/7	5	3	1	0	500000

- 6. To disable PTP on specific interfaces, click each interface to move it from the Enabled list to the Disabled list.

or

To disable all interfaces, click Disable All.

- 7. To enable PTP on specific interfaces, click each interface to move it from the Disabled list to the Enabled list.

or

To enable all interfaces, click Enable All.

- 8. To change the PTP values for each interface, modify the fields as described in [Table 116](#).
- 9. Click Apply to Device.

Table 116 - Configure PTP

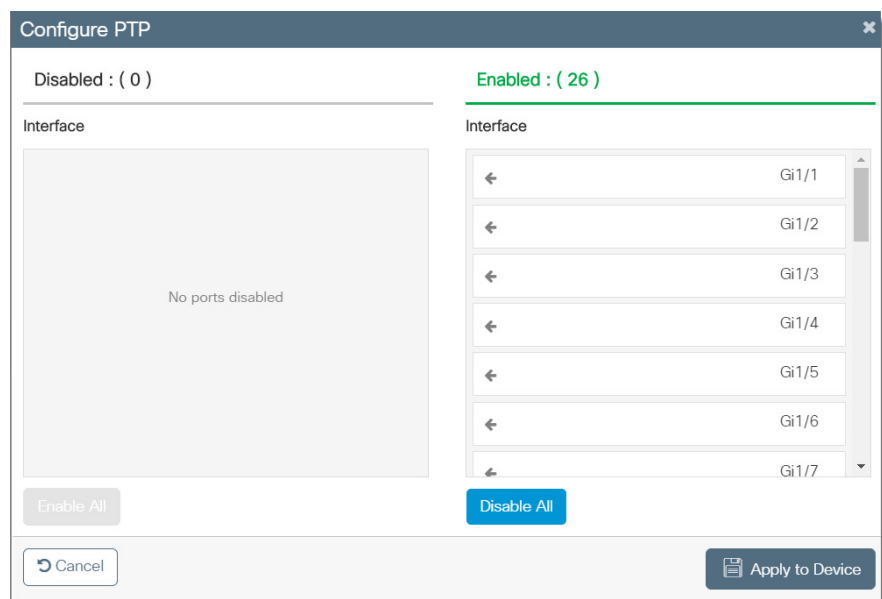
Field	Description
Delay Request Interval	Enter the time for the member devices to send delay request messages when the port is in the master state. Valid values: -1...6 seconds Default value: 5
Announce Timeout	Enter the time for announcing timeout messages. Valid values: 2...10 seconds Default value: 3

**Table 116 - Configure PTP**

Field	Description
Announce Interval	Enter the time for sending announce messages. Valid values: 0...4 seconds Default value: 1
Sync Interval	Enter the time for sending synchronization messages. Valid values: -1...1 seconds Default value: 1
Sync Fault Limit	Enter the maximum clock offset value before PTP attempts to resynchronize. The range is 50...500000000 nanoseconds. The default is 50,000 nanoseconds. Valid values: 50... 500000000 nanoseconds Default value: 50000

To configure PTP in End to End Transparent mode, follow these steps.

1. From the Mode pull-down menu, choose End to End Transparent.
2. Click Apply to Device.
3. Click Configure.



4. To disable PTP on specific interfaces, click each interface to move it from the Enabled list to the Disabled list.

or

To disable all interfaces, click Disable All.

5. To enable PTP on specific interfaces, click each interface to move it from the Disabled list to the Enabled list.

or

To enable all interfaces, click Enable All.

6. Click Apply to Device.

To configure PTP in Forward mode, follow these steps.

1. From the Mode pull-down menu, choose Forward.
2. Click Apply to Device.



## Configure Device Time via the Logix Designer Application

In the Logix Designer application, you can manage device time in these ways:

- To configure CIP Sync Time (PTP), see [page 184](#)
- To view CIP Sync Time information, [page 186](#)
- To manage NTP servers, see [page 188](#)

### Configure CIP Sync Time (PTP)

1. In the navigation pane, click Time Sync Configuration.
2. From the Clock Type pull-down menu, choose a mode.

For a description of each mode, see [Table 113 on page 179](#).

3. Complete the fields, and then click Set:
  - To configure Boundary mode, see [page 184](#).
  - To configure End to End Transparent mode, see [page 186](#).

There is no configuration for Forward mode.

The screenshot shows the 'Time Sync Configuration' window in the Logix Designer application. The 'Clock Type' is set to 'Boundary'. The 'Clock Identity' is '0x34:C0:F9:FF:FE:E5:0F:C0'. The 'Grandmaster Selection Priority 1' and 'Grandmaster Selection Priority 2' are both set to 128. The 'Offset From Master' is 0. A table lists ports Gi1/1 through Gi1/10, all with 'Time Sync Enable' checked, 'Time Sync State' as 'Not Synced', and various timeout and interval values. At the bottom, there are buttons for 'Refresh Communication', 'Set', 'OK', 'Cancel', 'Apply', and 'Help'.

Port	Time Sync Enable	Time Sync State	Delay Request	Announce Timeout	Announce Interval	Sync Interval	Sync Fault Limit
Gi1/1	<input checked="" type="checkbox"/>	Not Synced	5	3	1	0	500000
Gi1/2	<input checked="" type="checkbox"/>	Not Synced	5	3	1	0	500000
Gi1/3	<input checked="" type="checkbox"/>	Not Synced	5	3	1	0	500000
Gi1/4	<input checked="" type="checkbox"/>	Not Synced	5	3	1	0	500000
Gi1/5	<input checked="" type="checkbox"/>	Not Synced	5	3	1	0	500000
Gi1/6	<input checked="" type="checkbox"/>	Not Synced	5	3	1	0	500000
Gi1/7	<input checked="" type="checkbox"/>	Not Synced	5	3	1	0	500000
Gi1/8	<input checked="" type="checkbox"/>	Not Synced	5	3	1	0	500000
Gi1/9	<input checked="" type="checkbox"/>	Not Synced	5	3	1	0	500000
Gi1/10	<input checked="" type="checkbox"/>	Not Synced	5	3	1	0	500000

Table 117 - Boundary Mode

Field	Description
Clock Identity	Displays a unique identifier for the clock.
Grandmaster Selection Priority 1	Type a value to override the default criteria (clock quality, clock class, and so on) for the best master clock selection. A lower value takes precedence. Valid values: 0...255 Default: 128
Grandmaster Selection Priority 2	Type a value to use as a tie-breaker between two devices that are otherwise equally matched in the default criteria. For example, you can give a specific switch priority over other identical switches. A lower value takes precedence. Valid values: 0...255 Default: 128

Table 117 - Boundary Mode (Continued)

Field	Description
Offset from Master	Displays the time offset in nanoseconds between the slave and master clocks.
Port	Displays the port type and number.
Enable	Check the checkbox for each port on which to enable PTP. You can enable one or more switch ports. By default, PTP is enabled on all ports.
State	<p>The synchronization state of the switch port with the parent or Grandmaster clock:</p> <ul style="list-style-type: none"> <li>• Initializing—The switch port is waiting while a parent or Grandmaster clock is selected.</li> <li>• Listening—The switch port is waiting while a parent or Grandmaster clock is selected.</li> <li>• Pre-master—The switch port is transitioning to change to Master state.</li> <li>• Master—The switch is acting as a parent clock to the devices connected to that switch port.</li> <li>• Passive—The switch has detected a redundant path to a parent or Grandmaster clock. For example, two different switch ports claim the same parent or Grandmaster clock. To help prevent a loop in the network, one of the ports changes to Passive state.</li> <li>• Uncalibrated—The switch port cannot synchronize with the parent or Grandmaster clock.</li> <li>• Slave—The switch port is connected to and synchronizing with the parent or Grandmaster clock.</li> <li>• Faulty—Either PTP is not operating properly on the switch port or nothing is connected to the port.</li> <li>• Disabled—PTP is not enabled on the switch port.</li> </ul>
Delay Request	<p>The logarithmic mean interval in seconds for connected devices to send delay request messages when the switch port is in the master state.</p> <p>Default value: 5 (32 seconds)</p>
Announce Timeout	<p>The number of announce intervals in seconds that must pass without receipt of an announce message from the parent or Grandmaster clock before the switch selects a new parent or Grandmaster clock.</p> <p>Valid values: 2...10</p> <p>Default value: 3 (8 seconds)</p>
Announce Interval	<p>The logarithmic mean time interval in seconds for sending announce messages.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• 0...1 second</li> <li>• 1...2 seconds</li> <li>• 2... 4 seconds</li> <li>• 3... 8 seconds</li> <li>• 4...16 seconds</li> </ul> <p>Default value: 1 (2 seconds)</p>
Sync Interval	<p>The logarithmic mean time interval in seconds for sending synchronization messages.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• -1...half second</li> <li>• 0...1 second</li> <li>• 1... 2 seconds</li> </ul> <p>Default value: 0 (1 second)</p>
Sync Fault Limit	<p>Type the maximum clock offset before PTP attempts to reacquire synchronization.</p> <p>Valid values: 50...500000000 nanoseconds</p> <p>Default value: 50,000 nanoseconds</p> <p><b>IMPORTANT:</b> We recommend against setting the sync limit below the default (50,000 nanoseconds). Use values below 50,000 nanoseconds only in networks with a very high-precision Grandmaster clock. These networks have a critical need to keep sensitive devices synchronized.</p>

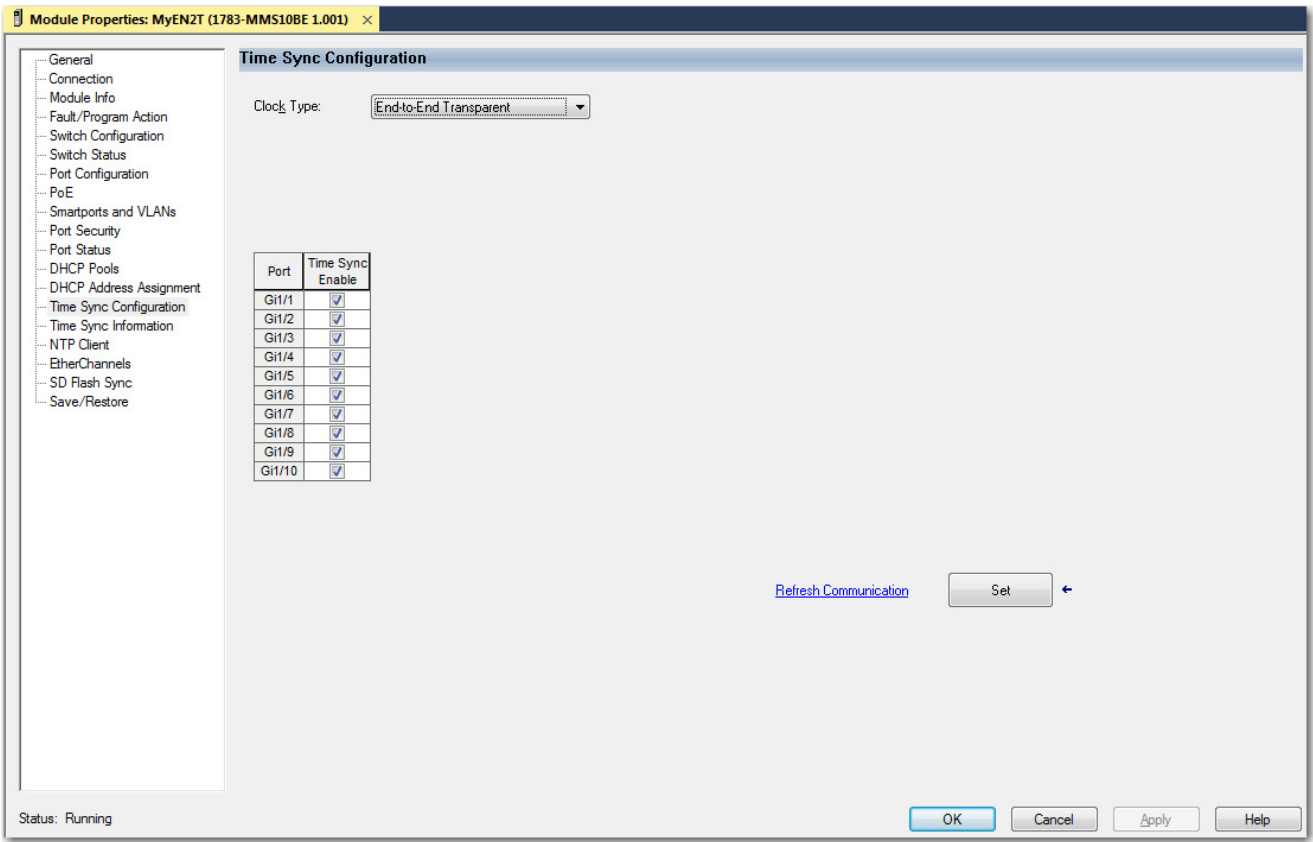


Table 118 - End to End Transparent Mode

Field	Description
Port	Displays the port type and number.
Time Sync Enable	To enable or disable time synchronization on a port, check or clear its associated Time Sync Enable checkbox.

*View Time Sync Information*

The Time Sync Information view shows current information about the real-time clocks in the network.

In the navigation pane, click Time Sync Information.

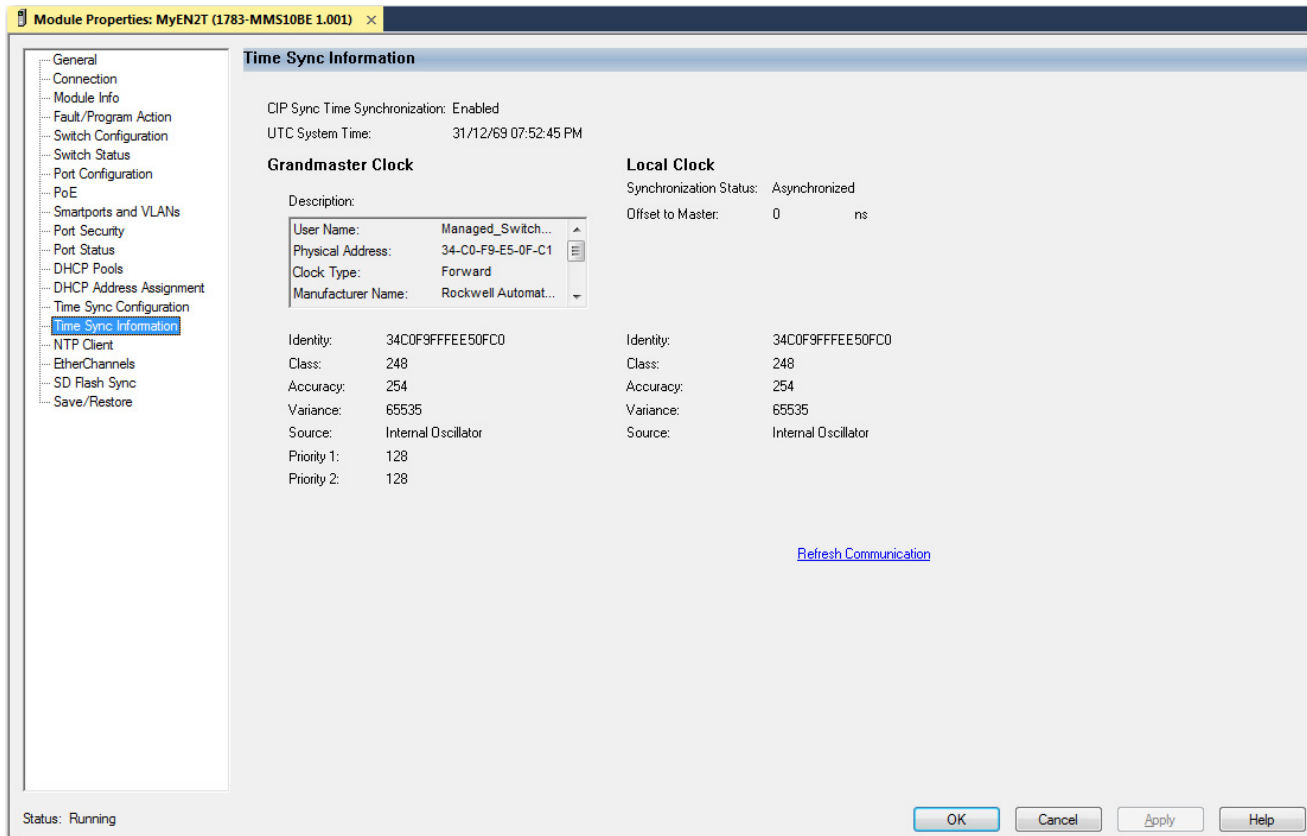


Table 119 - Time Sync Information

Field	Description
CIP Sync Time Synchronization	Displays whether the Precision Time Protocol is enabled or disabled on the device.
UTC System Time	Displays the current system time in units of microseconds.
<b>Grandmaster Clock</b>	
Description	Displays information to identify the Grandmaster clock, including the configured clock type.
Identity	Displays the unique identifier for the Grandmaster clock. The format depends on the network protocol.
Class	Displays a measure of the quality of the Grandmaster clock. Values are defined from 0...255 with 0 as the best clock.
Accuracy	Indicates the expected absolute accuracy of the Grandmaster clock relative to CIP Sync time synchronization epoch (31 December, 1969 23:59:51.99918 UTC). The accuracy is specified as a graduated scale starting at 25 ns and ending at greater than 10 seconds or unknown. For example, a GPS time source has an accuracy of approximately 250 ns. A hand-set clock typically has an accuracy less than 10 seconds. The lower the accuracy value, the better the clock.
Variance	Displays the measure of inherent stability properties of the Grandmaster clock. The value is in offset scaled log units. The lower the variance, the better the clock.
Source	Displays the clock time source: <ul style="list-style-type: none"><li>• Atomic Clock</li><li>• GPS</li><li>• Terrestrial Radio</li><li>• CIP Time Synchronization</li><li>• NTP</li><li>• HAND Set</li><li>• Other</li><li>• Internal Oscillator</li></ul>
Priority 1	Displays the relative priority of the Grandmaster clock to other clocks in the system. The value is between 0...255. The highest priority is 0.
Priority 2	
<b>Local Clock</b>	
Synchronization Status	Displays whether the local clock is synchronized or asynchronized with the Grandmaster clock.
Offset to Master	Displays the offset value between the local clock and the master clock.
Identity	Displays the unique identifier for the local clock. The format depends on the network protocol. <ul style="list-style-type: none"><li>• The Ethernet protocol encodes the MAC ID into the identifier.</li><li>• The DeviceNet® and ControlNet® protocols encode the Vendor ID and serial number into the identifier.</li></ul>
Class	Displays a measure of the quality of the local clock. Values are defined from 0...255 with 0 as the best clock.

Table 119 - Time Sync Information (Continued)

Field	Description
Accuracy	Indicates the expected absolute accuracy of the local clock relative to CIP Sync time synchronization epoch (31 December, 1969 23:59:51.99918 UTC). The accuracy is specified as a graduated scale starting at 25 ns and ending at greater than 10 seconds or unknown. For example, a GPS time source has an accuracy of approximately 250 ns. A hand-set clock typically has an accuracy less than 10 seconds. The lower the accuracy value, the better the clock.
Variance	Displays the measure of inherent stability properties of the local clock. The value is in offset scaled log units. The lower the variance, the better the clock.
Source	Displays the clock time source: <ul style="list-style-type: none"><li>• Atomic Clock</li><li>• GPS</li><li>• Terrestrial Radio</li><li>• CIP Time Synchronization</li><li>• NTP</li><li>• HAND Set</li><li>• Other</li><li>• Internal Oscillator</li></ul>

Manage NTP Servers

In the navigation pane, click the NTP Client.

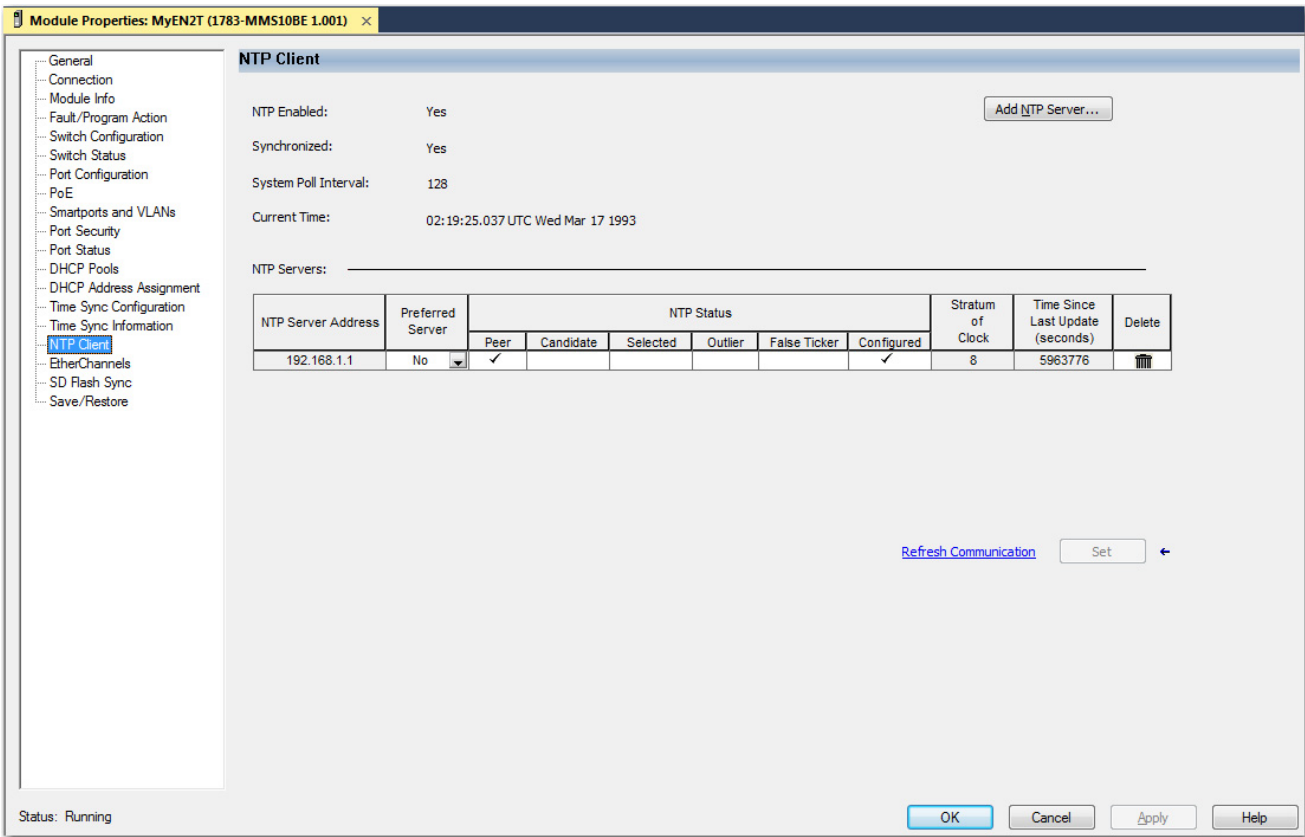


Table 120 - NTP Client

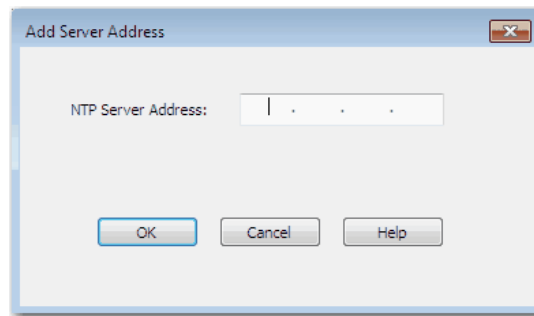
Field	Description
NTP Enabled	Displays whether NTP is enabled or disabled.
Synchronized	Displays the status of NTP clock synchronization: <ul style="list-style-type: none"><li>• Synchronized</li><li>• Unsynchronized</li></ul>
System Poll Interval	Displays the poll interval of the peer.
Current Time	Displays the reference time stamp.
<b>NTP Servers</b>	

Table 120 - NTP Client

Field	Description
NTP Server Address	Displays the specified IP address for the association: <ul style="list-style-type: none"> <li>For a peer association, the IP address identifies the peer providing, or being provided, the clock synchronization.</li> <li>For a server association, the IP address identifies the time server providing the clock synchronization.</li> </ul>
Preferred Server	Choose whether the peer or server is the preferred one that provides synchronization.
NTP Status	Displays the status of the NTP peer association.
Stratum of Clock	Displays the stratum of the peer.
Time Since Last Update (seconds)	Displays the time the system last updated its NTP information.

On the NTP Client view, you can add and delete NTP servers:

- To add an NTP server, see the following procedure.
  - To delete an NTP server, click the Trash icon in the Delete column.
  - To reload the NTP server details, click Refresh Communication.
- Click Add NTP Server.



- In the NTP Server Address field, enter one of the following, and then click OK:
  - For a peer association, enter the IP address of the peer providing, or being provided, the clock synchronization.
  - For a server association, enter the IP address of the time server providing the clock synchronization.

The IP address that you specify appears in the NTP Servers table.

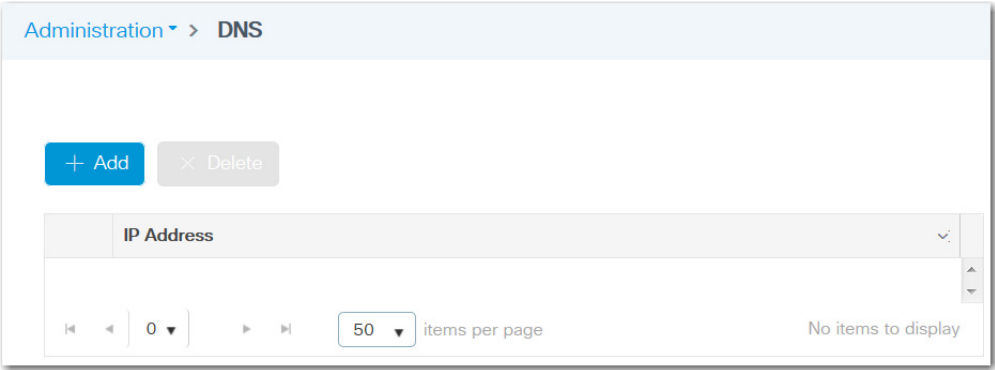
- To make the peer or server the preferred one that provides synchronization, on the NTP Client view, choose Yes in the Preferred Server column.

## Domain Name System (DNS)

DNS is a name resolution protocol that enables you to identify devices by names rather than IP addresses. For DNS to work, a DNS server is configured to hold a table of names and the associated IP addresses. When a device attempts to send a message to a device with an unknown name, it requests the IP address of the named device from the DNS server. For more information about DNS, see the Ethernet Reference Manual, publication [ENET-RM002](#).

### Add a DNS Server via the WebUI

From the Administration menu, choose DNS.



From the DNS page, you can add, edit, and delete DNS servers:

- To add a DNS server, click Add, complete the fields as described in [Table 121](#), and then click Apply to Device.
- To edit a DNS server, click the server in the grid, modify the fields, and then click
- To delete a DNS server, click its associated checkbox in the grid, and then click Delete.

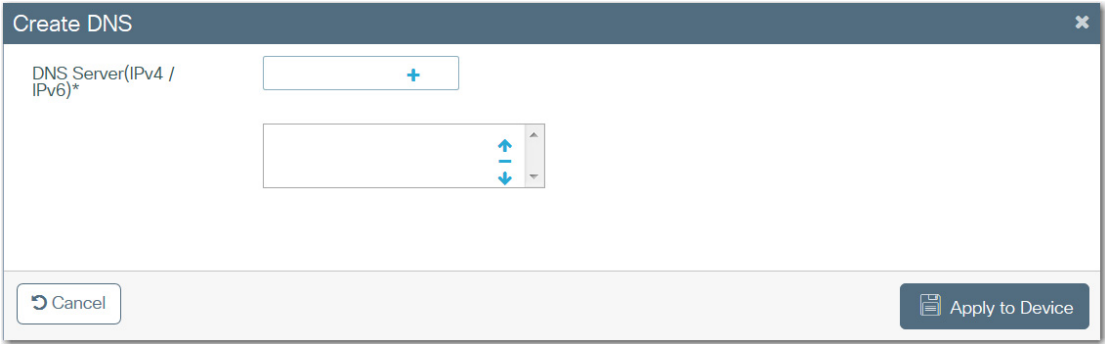



Table 121 - Create DNS

Field	Description
DNS Server (IPv4/IPv6)	Enter the IP address of a DNS server and click + to add it to the list. You can add multiple DNS servers for backup.
[DNS server list]	To change the order of DNS servers in the list, click a server in the list, and then click the up and down arrows  .  <b>IMPORTANT:</b> The first server in the list is the primary server. The device sends DNS queries to the primary server first. If that query fails, the device queries the backup servers.

## Dynamic Host Configuration Protocol (DHCP)

Every device in an IP-based network must have a unique IP address. DHCP assigns IP address information from a pool of available addresses to newly connected devices (DHCP clients) in the network. The switch can operate as a DHCP server by automatically assigning IP addresses to connected devices. If a device leaves and then rejoins the network, the device receives the next available IP address. For more information about DHCP, see the Ethernet Reference Manual, publication [ENET-RM002](#).

### DHCP Persistence

DHCP persistence, or port-based address allocation, is a feature that enables DHCP to maintain the same IP address on an Ethernet switch port. The device that is connected to that port always receives the same IP address regardless of the MAC address of the connected device. You can assign an IP address from an IP address pool.

DHCP persistence is useful in networks that you configure in advance, where dependencies on the exact IP addresses of some devices exist. Use DHCP persistence when the attached device has a specific role to play and when other devices know its IP address. If the device is replaced, the replacement device is assigned the same IP address, and the other devices in the network require no reconfiguration.

When the DHCP persistence feature is enabled, a switch acts as a DHCP server for other devices on the same subnet, including devices that are connected to other switches. If the switch receives a DHCP request, it responds with any unassigned IP addresses in its pool.

When DHCP persistence is enabled and a DHCP request is made from a connected device on that port, the switch assigns the IP address for that port. It also broadcasts the DHCP request to the remainder of the network. If another DHCP server with available addresses is on the network and receives this request, it can try to respond. The response can override the initial IP address the switch assigns depending on how the end device behaves (takes first IP address response or the last). To keep the IP address from being overridden, enable DHCP snooping on the appropriate VLAN. DHCP snooping blocks the broadcast of this DHCP request so that no other server, including another switch with DHCP persistence enabled, responds.

If you are using DHCP persistence, we recommend that you initially assign static IP addresses to end devices. If an end device fails and is replaced, the DHCP persistence feature assigns an IP address from the DHCP persistence table. The device functions properly with this IP address, but we recommend that you reassign a static IP address to the replaced devices.

The following figure and table illustrate DHCP persistence behavior.



Figure 23 - DHCP Persistence

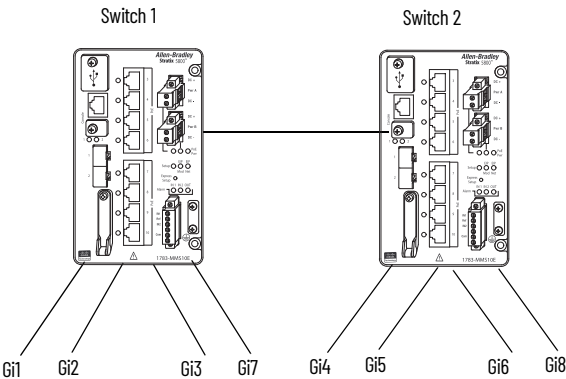


Table 122 - DHCP Persistence Behavior

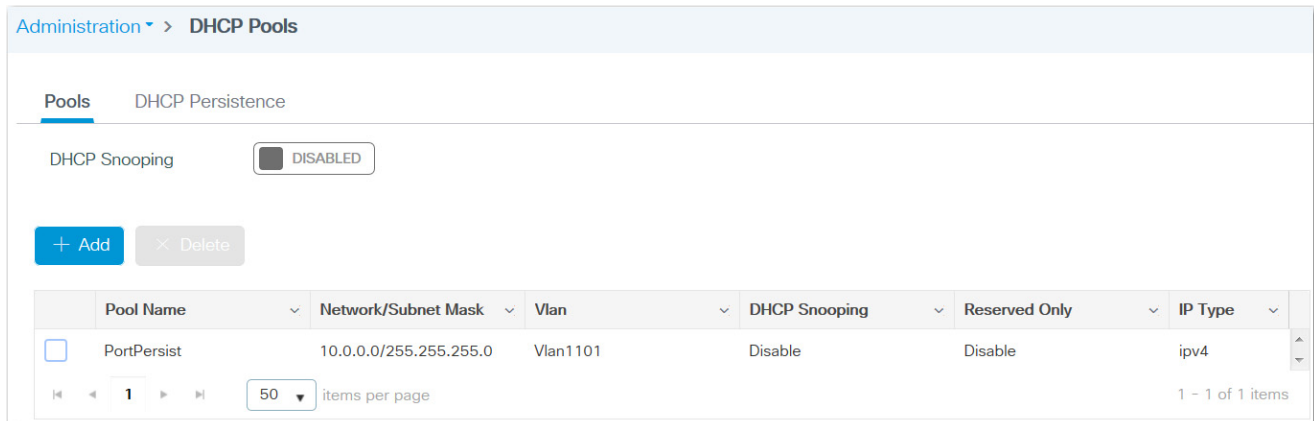
If	Then
<ul style="list-style-type: none"><li>Switch 1 has ports Gi1...Gi3 in its persistence table</li><li>Switch 2 has ports Gi4, Gi5, Gi6, and Gi8 in its persistence table</li><li>Reserved Only is disabled and DHCP snooping is disabled</li></ul>	A new device that is connected to switch 1 Gi1 receives an IP address from the switch 1 persistence table. A broadcast request is also sent across the network. Switch 2 responds if there is an unassigned address in its pool. The response can override the assignment that is made by switch 1.
<ul style="list-style-type: none"><li>Switch 1 has ports Gi1...Gi3 in its persistence table</li><li>Switch 2 has ports Gi4, Gi5, Gi6, and Gi8 in its persistence table</li><li>Reserved Only is enabled in both switches and DHCP snooping is disabled</li></ul>	A new device that is connected to switch 1 Gi1 receives an IP address from the switch 1 persistence table. A broadcast request is also sent across the network. Switch 2 does not respond to the request. If the device is connected to Gi7 of switch 1, it does not receive an IP address from the switch pool because it is not defined in the persistence table. Also, unused addresses in the pool are blocked.
<ul style="list-style-type: none"><li>Switch 1 has ports Gi1...Gi3 in its persistence table</li><li>Switch 2 has ports Gi4, Gi5, Gi6, and Gi8 in its persistence table</li><li>Reserved Only is enabled in switch 1 and DHCP snooping is disabled</li><li>Reserved Only is disabled in switch 2</li></ul>	A new device is connected to Gi1 receives an IP address from the persistence table. A broadcast request is also sent across the network. Switch 2 does not respond to the request. In addition, a device that is connected to Gi4 receives an IP address from the switch 2 persistence table. A broadcast request is sent out, and switch 1 responds with an unused IP address from its pool. The response can override the assigned port.
<ul style="list-style-type: none"><li>Switch 1 has ports Gi1...Gi3 in its persistence table</li><li>Switch 2 has ports Gi4, Gi5, Gi6, and Gi8 in its persistence table</li><li>DHCP Snooping is enabled</li><li>Reserved Only is enabled</li></ul>	A new device that is connected to switch 1 Gi1 receives an IP address from the persistence table in switch 1. A broadcast request is not sent across the network, so switch 2 does not respond. If a device is connected to Gi7 of switch 1, it does not receive an IP address from the switch pool because it is not defined in the persistence table. Also, unused addresses in the pool are blocked.
<ul style="list-style-type: none"><li>Switch 1 has ports Gi1...Gi3 in its persistence table</li><li>Switch 2 has ports Gi4, Gi5, Gi6, and Gi8 in its persistence table</li><li>DHCP Snooping is enabled</li><li>Reserved Only is enabled</li></ul>	A new device that is connected to switch 1 Gi1 receives an IP address from the persistence table in switch 1. A broadcast request is not sent across the network, therefore switch 2 does not respond. If a device is connected to Gi7 (not defined in the DHCP persistence table) of switch 1, it receives an unassigned IP address from the switch 1 pool.

DHCP Snooping

DHCP snooping restricts the broadcast of DHCP requests beyond the connected switch. As a result, devices receive address assignments from only the connected switch. This option is available only on ports that are assigned to a VLAN.

## Configure DHCP via the WebUI

From the Administration menu, choose DHCP Pools.

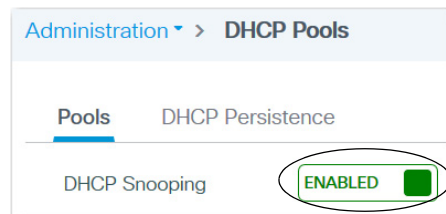


From the DHCP page, you can enable or disable DHCP snooping and configure DHCP pools and DHCP persistence:

- To enable or disable DHCP snooping, see [page 193](#).
- To configure DHCP pools, see [page 194](#).
- To configure DHCP persistence, see [page 195](#).

### Enable or Disable DHCP Snooping

On the Pools tab, click to enable or disable DHCP snooping. By default, DHCP snooping is disabled. A message appears in the lower-right corner of the WebUI to confirm that the configuration was successfully applied.



Configure DHCP Pools

On the Pools tab, you can add, edit, and delete DHCP pools:

- To add a pool, click Add, complete the fields as described in [Table 123](#), and then click Apply to Device.
- To edit a pool, click the pool in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a pool, check its associated checkbox in the grid, and then click Delete.

Create DHCP Pool

BasicAdvanced

DHCP Pool Name\*

(1-236 Characters)

IP Type

IPv4

Network\*

xxx.xxx.xxx.xxx

Subnet Mask\*

255.255.255.0

Starting ip\*

xxx.xxx.xxx.xxx

Ending ip\*

xxx.xxx.xxx.xxx

Reserved Only

DISABLED

Lease\*

Never Expires

(0-365 days)

(0-23 hours)

(0-59 minutes)

Enable DNS Proxy

☐

Cancel

Apply to Device

Table 123 - Create DHCP Pool

Field	Description
Basic or Advanced	Click to determine the fields that appear on the Create DHCP Pool page: <ul style="list-style-type: none"><li>• Basic (default)—Only basic fields on appear on the page.</li><li>• Advanced—Both basic and advanced fields appear on the page. Advanced fields include configuration of Domain Name System (DNS) or</li><li>• NetBIOS™ servers for IPv4 address types.</li></ul>
<b>Basic</b>	
DHCP Pool Name	Enter a unique name for the DHCP address pool.
IP Type	Choose the IP protocol to use for this DHCP address pool. <ul style="list-style-type: none"><li>• IPv4 (default)</li><li>• IPv6</li></ul>
<b>IPv4</b>	
Network	Enter the IP address of the network served by this DHCP address pool. This IP address is used by the management interface with Netmask applied, as configured on the Interface page.
Subnet Mask	Choose the subnet mask to assign to the DHCP clients.
Starting IP	Enter the first of the contiguous addresses in the DHCP address pool. Any new DHCP client joining the LAN receives an IP address between this starting address and the ending address.
Ending IP	Enter the last contiguous address in the address pool.
Reserved Only	To limit address assignments to only ports that are defined in the DHCP persistence table, click to enable Reserved Only.
Lease	Choose the duration of the lease for an IP address that is assigned to a DHCP client: <ul style="list-style-type: none"><li>• Never Expires (default)—The DHCP client can use the assigned IP address indefinitely.</li><li>• User Defined—The DHCP client can use the assigned IP address for a limited time.</li></ul> If you choose User Defined, enter the duration of the lease in the numbers of days, hours, and minutes.

**Table 123 - Create DHCP Pool (Continued)**

Field	Description
<b>IPv6</b>	
DNS Server(s)	Enter the IP addresses of a DNS server for a DHCP client, and then click the plus sign to add the translation to the grid. Repeat for each address.
DNS Domain Name	Enter the domain name for the DHCP client, and then click the plus sign to add the name to the grid. Repeat for each domain name. The name can have a maximum of 31 alphanumeric characters. The name cannot contain a ? or a tab.
IPv6 Address Allocation	Enter an IP addresses allocated to IPv6 protocol, and then click the plus sign to add the address to the grid. Repeat for each address.
<b>Advanced</b>	
Enable DNS Proxy	(Appears only for IPv4 address types). Check Enable DNS Proxy to add default routers to DNS servers.
<b>DHCP Options List—DHCP provides an internal framework for passing configuration parameters and other control information to clients on your network. DHCP options carry parameters as tagged data stored within protocol messages that are exchanged between the DHCP server and its clients.</b>	
DHCP Options	Enter a DHCP option value from 2...251 and click Add. You can also enter a range of options, such as 7...11.
Options Value	Enter a string value for the DHCP option.

### Configure DHCP Persistence

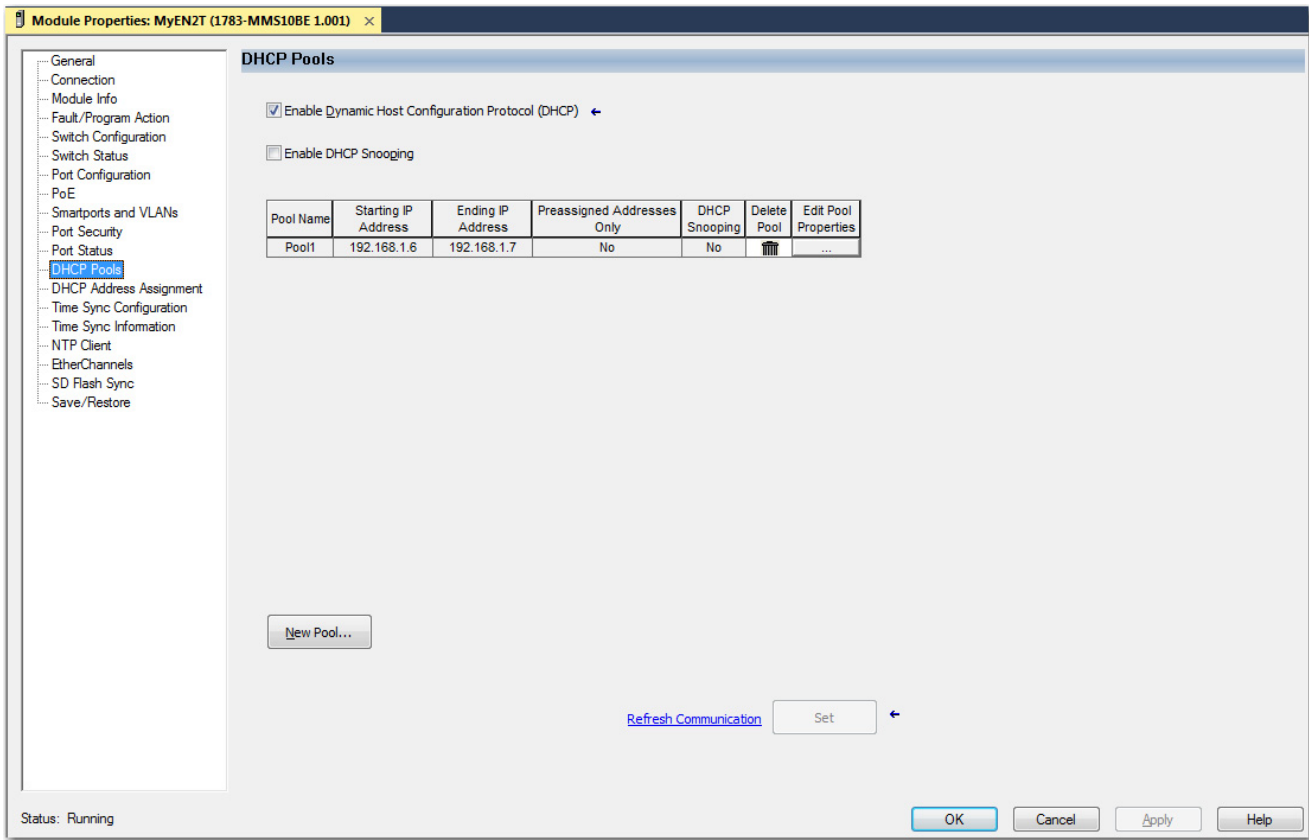
On the DHCP Persistence tab, click an interface in the grid, modify the fields as described in [Table 124](#), and then click Update & Apply to Device.

**Table 124 - DHCP Persistence**

Field	Description
Interface	Displays the interface type and number.
Pool Name	Choose the DHCP address pool that includes the IP address to assign to this interface.
Reserved IP Address	Enter the IP address reserved for the device that connects to this interface. The IP address that you assign is reserved for only this port and is not available for normal DHCP dynamic assignment. The IP address must be in the range of the assigned DHCP address pool.

## Configure DHCP via the Logix Designer Application

In the navigation pane, click DHCP Pools.



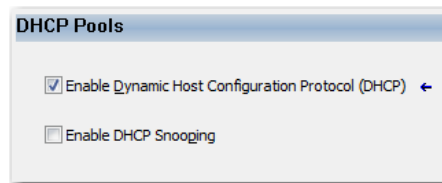
From the DHCP Pools view, you can enable or disable DHCP and DHCP snooping and configure DHCP pools:

- To enable or disable DHCP and DHCP snooping, see [page 196](#).
- To add a DHCP pool, see [page 197](#).
- To edit a DHCP pool, click the Ellipses icon in the Edit Pool Properties column, modify the fields, and then click Close.
- To delete a DHCP pool, click the Trash icon in the Delete Pool column.
- To configure DHCP persistence, see [page 198](#).

### Enable or Disable DHCP or DHCP Snooping

On the DHCP Pools view, check the checkboxes to enable DHCP and DHCP snooping. Clear the checkboxes to disable the features.

By default, DHCP is enabled, and DHCP snooping is disabled.



### Add a DHCP Pool

1. Click New Pool.
2. Complete the fields as described in [Table 125](#), click Set, and then click Close.
3. Click Apply.

The screenshot shows the 'Add/Edit DHCP Pool Definition' window. It has a title bar with a close button. The main area contains several input fields and checkboxes. On the left, there are fields for 'DHCP Pool Name', 'DHCP Pool Network', 'Subnet Mask', 'Default Gateway', and 'Domain Name'. On the right, there are fields for 'Starting IP Address' and 'Ending IP Address'. Below these are two checkboxes: 'Use Preassigned Addresses Only' and 'Enable DHCP Snooping for this Pool'. In the center, there is a 'Lease Length' section with radio buttons for 'Never Expires' (selected) and 'Custom'. If 'Custom' is selected, there are spinners for 'Days', 'Hrs', and 'Mins'. Below that is a 'DHCP Server' section with fields for 'Primary DNS Address', 'Secondary DNS Address', 'Primary WINS Address', and 'Secondary WINS Address'. At the bottom right is a 'Set' button with a left arrow. At the bottom center are 'Close' and 'Help' buttons.

**Table 125 - Add/Edit DHCP Pool Definition**

Field	Description
DHCP Pool Name	The name of the DHCP IP address pool that is configured on the switch. A DHCP IP address pool is a range (or pool) of available IP addresses that the switch can assign to connected devices.
DHCP Pool Network	The subnetwork IP address of the DHCP IP address pool.
Subnet Mask	The network address that identifies the subnetwork (subnet) of the DHCP IP address pool. Subnets segment the devices in a network into smaller groups.
Default Gateway	The default gateway IP address for the DHCP client.
Domain Name	The domain name for the DHCP client.
Starting IP Address	The starting IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address that is written as four numbers that are separated by periods. Each number can be from 0...255. Be sure that none of the IP addresses that you assign are being used by another device in your network. This field is required.
Ending IP Address	The ending IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address that is written as four numbers that are separated by periods. Each number can be from 0...255. Make sure that none of the IP address you assign are being used by other devices in your network. This field is required.
Use Preassigned Addresses Only	If checked, IP addresses are assigned only when configured for specific ports on the DHCP Address Assignment or DLR DHCP views.
Enable DHCP Snooping for this Pool	If checked, devices only receive address assignments from the connected switch.
Never Expires or Custom	The duration of the lease for an IP address that is assigned to a DHCP client. Click one of the following: <ul style="list-style-type: none"> <li>• Never Expires</li> <li>• Custom</li> </ul> If you click Custom, enter the duration of the lease in the numbers of days, hours, and minutes. This lease length is used for all assignments.
Primary DNS Address	The IP addresses of the primary domain name system (DNS) IP servers available to a DHCP client.
Secondary DNS Address	The IP addresses of the secondary domain name system (DNS) IP servers available to a DHCP client.
Primary WINS Address	The IP address of the primary Microsoft® NetBIOS name server (WINS server) available to a DHCP client.
Secondary WINS Address	The IP address of the secondary Microsoft NetBIOS name server (WINS server) available to a DHCP client.

Configure DHCP Persistence

To make sure that a device that is connected to a specific port receives the same IP address, assign a specific IP address to the port.

- 1. In the navigation pane, click DHCP Address Assignment.
- 2. Complete the fields as described in [Table 126](#), and then click Set.
- 3. Click Apply.

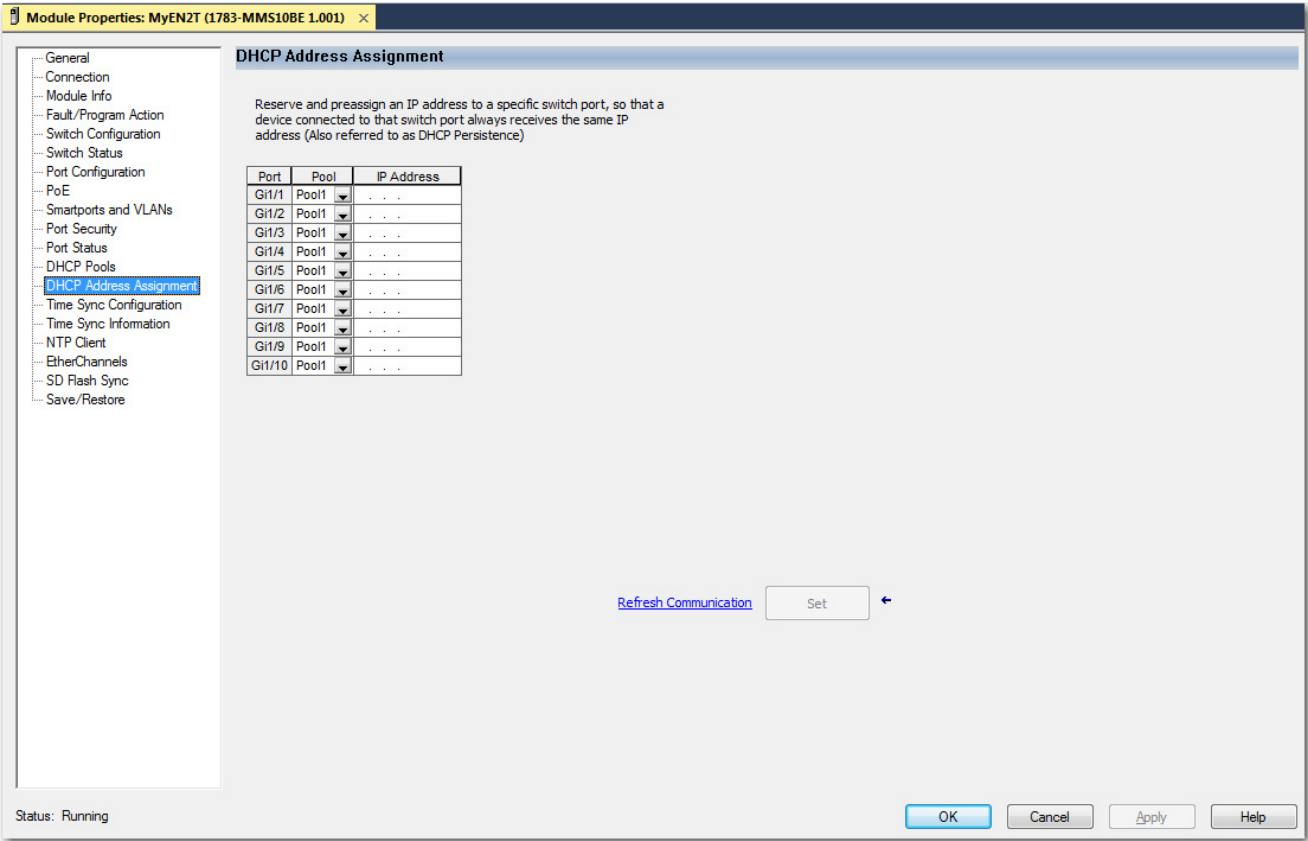


Table 126 - DHCP Address Assignment

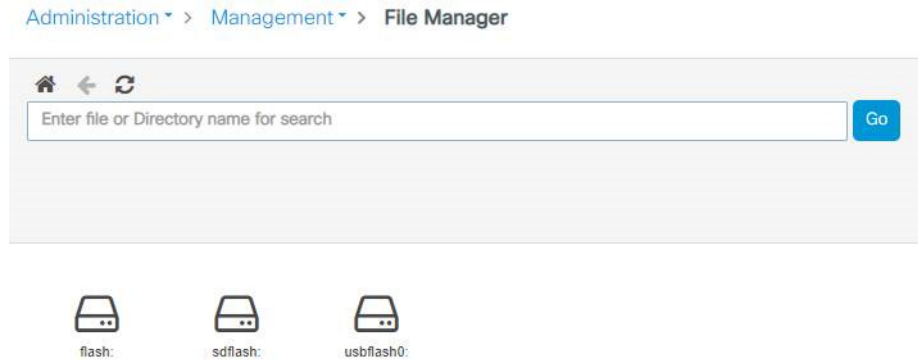
Field	Description
Port	Displays the port type and number.
Pool	Choose the DHCP address pool that includes the IP address to assign to this port.
IP Address	Enter the IP address reserved for the port that connects to this interface. The IP address that you assign is reserved for only this port and is not available for normal DHCP dynamic assignment. The IP address must be in the range of the assigned DHCP address pool.

## File Manager

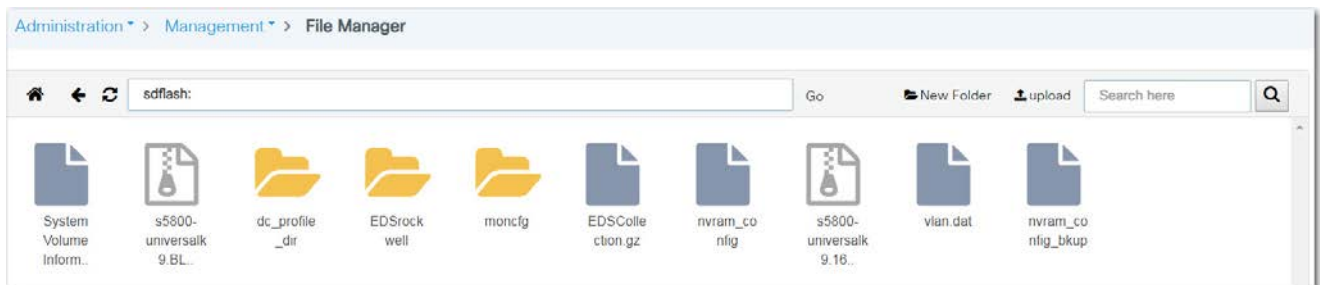
In the WebUI, you can manage files in the flash and sdflash file systems on the device. You can upload and download files such as logs, scripts, data files, and so on. Also, you can create folders, display folder contents, and search for files.

From the Administration menu, choose File Manager.

To display the files and directories in the file system, double-click flash or sdflash. You can also type the path to a file in the directory search field, or you can search for a file name from within a directory or folder.



The contents of the file system appears.



Within a file system, you can do the following:

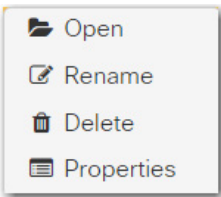
- To return to a previous level in the file system, click the left arrow, or click the Home icon to return to the top level.
- To create a folder, click New Folder, enter a folder name, and then click OK.



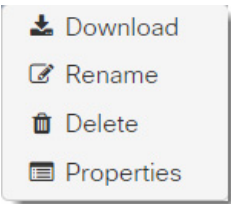
- To upload a file, click upload, browse to the file to upload, and then click Open.



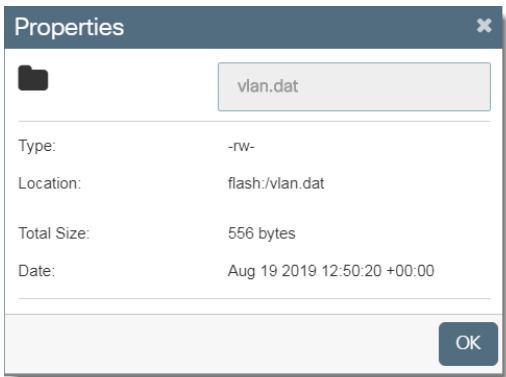
- To open, rename, delete, or view file properties, right-click a folder.



- To download, rename, delete, or view file properties, right-click a file.



- To view folder or file details, click Properties.



Field	Description
Type	The permissions file types: <ul style="list-style-type: none"><li>• d = directory</li><li>• r = read</li><li>• w = write</li><li>• x = execute</li><li>• - (dash)= used when a particular permission is not granted</li></ul>
Location	The path to the folder or file.
Total Size	The size of the folder contents or file size.
Date	The date and time stamp of folder or file.

## HTTP/HTTPS/Netconf Access

On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent. HTTP with SSL encryption provides a secure connection between two devices, such as a switch and your web browser.

With Personal Identity Verification (PIV), the identity of a user is verified using a certificate and the login user name and password. Prerequisites to enable PIV include configuring a PKI trust store and installing the root CA certificate, and then enabling PKI from HTTP.

### Certificate Authority (CA) Trustpoints

CA Trustpoints manage certificate requests and issue certificates to participating network devices. These services provide centralized security key and certificate management for the participating devices. Specific CA servers are known as trustpoints. For more information about CA Trustpoints, see the Ethernet Reference Manual, publication [ENET-RM002](#).

**IMPORTANT** CA trustpoints must be configured on each device individually. Copying them from other devices makes them invalid on the device.

### Configure HTTP/HTTPS/Netconf Access via the WebUI

1. From the Administration menu, choose HTTP/HTTPS/Netconf.
2. Complete the fields as described in [Table 127](#), and then click Apply.

**Table 127 - HTTP/HTTPS/Netconf**

Field	Description
<b>HTTP/HTTPS Access Configuration</b>	
HTTP Access	Click to enable or disable HTTP connections. By default, HTTP access is enabled. <b>IMPORTANT:</b> If both HTTP and HTTPS are enabled, HTTP redirects to HTTPS.
HTTPS Access	Click to enable or disable HTTPS connections. By default, HTTPS access is enabled.
Personal Identity Verification	Click to enable or disable PIV. <b>IMPORTANT:</b> If you enable PIV before setting it up, you are not able to access the switch.
<b>HTTP Trust Point Configuration</b>	
Enable Trust Point	Click to enable or disable certificate authority (CA) trustpoints. See <a href="#">Certificate Authority (CA) Trustpoints on page 201</a> .
Trust Points	If trustpoints are enabled, choose a trustpoint from the list.

**Table 127 - HTTP/HTTPS/Netconf (Continued)**

Field	Description
<b>Netconf Yang Configuration</b>	
Status	Click to enable or disable Netconf on the device.
SSH Port	Enter the port number for Netconf-over-SSH sessions. Valid values: 1...65535 Default value: 830
<b>Timeout Policy Configuration</b>	
<b>HTTP Timeout-policy (secs)</b>	Enter the number of seconds to determine how long a connection to the HTTP server remains open.
Session Idle Timeout (secs)	Enter the number of seconds of inactivity allowed before the session times out.
Server Life (secs)	Enter the server life time in seconds. Valid values: 1...86400
Max Number of Requests	Enter the maximum number of concurrent requests the device can accept. Valid values: 1...86400

## MODBUS

MODBUS is an application layer protocol for client-server communication between two devices on the network, where the Stratix 5800 switch acts as the server, and a device with MODBUS client software can query the switch for information. This MODBUS implementation is read-only and only provides data.

### Requirements and Restrictions

Before you configure MODBUS, know the following:

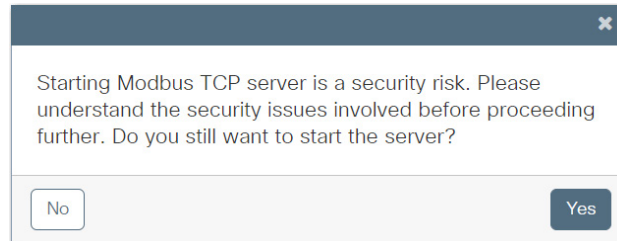
- If a firewall or other security services are enabled, the switch TCP port can be blocked, and the switch and the client cannot communicate.
- If a firewall and other security services are disabled, a denial-of-service attack can occur on the switch.
- To add security when using MODBUS TCP, configure an ACL to permit traffic from specific clients or configure QoS to rate-limit traffic.

## Configure MODBUS via the WebUI

To configure MODBUS, follow these steps.

1. From the Administration menu, choose MODBUS.
2. In the Status field, click to enable or disable MODBUS.

By default, MODBUS is disabled. If you enable MODBUS, a security warning appears.




---

**IMPORTANT** Before proceeding, observe and understand the security risk involved in starting the MODBUS TCP server.

---

3. To proceed through the security warning, click Yes.
4. Complete the fields as described in [Table 128](#), and then click Apply to Device.

Administration ▾ > Industrial Protocols ▾ > MODBUS

Status	ENABLE <input checked="" type="checkbox"/>	
TCP Server Port Number	<input type="text" value="502"/>	
TCP Server Connections	<input type="text" value="2"/>	

**Table 128 - MODBUS**

Field	Description
Status	Click to enable or disable MODBUS. By default, MODBUS is disabled.
TCP Server Port Number	Enter the port number of the MODBUS TCP server. Valid values: 1...65535 Default value: 502
TCP Server Connections	Enter the number of simultaneous connection requests sent to the switch. Valid values: 1...5 Default value: 2

For a list of MODBUS register addresses, see [Appendix E](#).

# Power over Ethernet (PoE)

Power over Ethernet (PoE) provides power to end devices over a copper Ethernet cable. Switches and expansion modules with PoE ports are software-configurable and provide automatic detection and power budgeting. PoE is implemented following the specifications in IEEE 802.3af (2003) and IEEE 802.3at (2009), which accommodate different power levels. For more information about PoE, see the Ethernet Reference Manual, publication [ENET-RM002](#).

**IMPORTANT**

A mismatch between the total power that is supported and the power supply can damage the switch. Do not oversubscribe the power supply. If you intend to connect the switch to a power supply that allows more wattage than configured, first change the power supply and then enter the total power supported. If you intend to connect the switch to a power supply that allows less wattage than configured, first change the total power that is supported to an appropriate value and then change the power supply.

## Requirements and Restrictions

There is a power budget of 360 W shared across PoE/PoE+ ports.

## PoE Port Modes

You can assign the following modes to PoE ports.

Table 129 - PoE Modes

Mode	Description
Disabled	The switch disables powered-device detection and never powers the PoE port even if an unpowered device is connected.
Auto (default)	The switch automatically detects if the connected device requires power and automatically assigns the required capacity.
Static	The switch preallocates power to the port, even when a non-PoE device is connected, and makes sure that power is available to the port.

## Configure PoE via the WebUI

The Power Management page is available for devices that have PoE support.

From the Administration menu, choose Power Management.

Administration > Power Management

Total Power Supported:  Watts

Total Power Used: 0 Watts

Total Power Available: 125 Watts

PSU 1: ● Power Up

PSU 2: ● Power Down

Interface	Mode	Status	Power	Max Power	Override Power	Device	Class
GigabitEthernet1/3	Auto	Off	0.0	30.0	N/A	N/A	N/A
GigabitEthernet1/4	Auto	Off	0.0	30.0	N/A	N/A	N/A
GigabitEthernet1/5	Auto	Off	0.0	30.0	N/A	N/A	N/A
GigabitEthernet1/6	Auto	Off	0.0	30.0	N/A	N/A	N/A
GigabitEthernet1/7	Auto	Off	0.0	30.0	N/A	N/A	N/A
GigabitEthernet1/8	Auto	Off	0.0	30.0	N/A	N/A	N/A
GigabitEthernet1/9	Auto	Off	0.0	30.0	N/A	N/A	N/A
GigabitEthernet1/10	Auto	Off	0.0	30.0	N/A	N/A	N/A

50 items per page 1 - 8 of 8 items

From the Power Management page, you can view and configure PoE information:

- The fields at the top of the page show information about the total power on the switch. See [Table 130](#).

To configure the total power supported, modify the value in the Total Power Supported field. A warning appears. Misconfiguration of this setting can result in damage to the switch. Click Yes to apply the configuration, which power cycles any PoE devices currently connected.

**Table 130 - Power Management**

Field	Description
Total Power Supported	The total amount of power that the switch can support for external devices. To limit the total PoE power budget, enter a value based on the power source. Valid values: 4...480 watts
Total Power Used	The amount of power used on the switch for PoE.
Total Power Available	The amount of power available on the switch for PoE.
PSU1	The status of the power supply connected to the Pwr A power connector.
PSU2	The status of the power supply connected to the Pwr B power connector.

- To configure PoE for an individual switch interface, click the interface in the grid, complete the fields as described in [Table 131](#), and then click Update & Apply to Device.

Edit POE InterfaceGigabitEthernet1/3

Interface

GigabitEthernet1/3

Mode

Auto

Status

On

Power

15.4

Max Power

30.0

Override Power

N/A

Device

ieee PD

Class

3

Table 131 - Edit PoE Interface

Field	Description
Interface	The interface type and number.
Mode	Choose a PoE mode to apply to the interface. For a description of each mode, see <a href="#">Table 129 on page 204</a> .
Status	Displays whether PoE is in use on the interface. The status turns to On once a PoE device is connected to the interface.
Power	Enter the amount of power in watts to allocate to the interface.
Max Power	Enter the maximum power that can be allocated to the interface. Valid values: 4...30 watts
Override Power	Displays either N/A or the power that is configured for the interface. To configure this parameter, enter the following command in command-line interface (CLI) where X is the wattage value: power inline consumption default wattage X
Device	The device that is connected to the interface.
Class	Displays the power classification of the powered device.

## Configure PoE via the Logix Designer Application

1. In the navigation pane, click PoE.
2. Complete the fields as described in [Table](#), and then click Set.

**Power over Ethernet (PoE) Port Configuration**

Port	Mode	Status	Power Limit (W)	Power Used (W)
Gi1/3	Auto	Off	30.0	0.0
Gi1/4	Auto	Off	30.0	0.0
Gi1/5	Auto	Off	30.0	0.0
Gi1/6	Auto	Off	30.0	0.0
Gi1/7	Auto	Off	30.0	0.0

**Switch Statistics:**

Total Power Supported: 125 W

Total Power Used: 0 W

Remaining Power Available: 125 W

[Refresh Communication](#)

Status: Running

Field	Description
<b>Power over Ethernet (PoE) Port Configuration</b>	
Port	Displays the port type and number.
Mode	Choose a PoE mode to apply to the port. For a description of each mode, see <a href="#">Table 129 on page 204</a> .
Status	Displays whether PoE is enabled (On) or disabled (Off) on the port.
Power Limit (W)	Enter the maximum power in that can be allocated to the interface. If the port is in Auto mode, you can enter a value. Valid values: 4...30 watts
Power Used (W)	Displays the amount of power in watts currently in use by the port.
<b>Switch Statistics</b>	
Total Power Supported	The total amount of power that the switch can support for external devices. To limit the total PoE power budget, enter a value based on the power source. Valid values: 4...720 watts
Total Power Used	The amount of power used on the switch for PoE.
Remaining Power Available	The amount of power available on the switch for PoE.



## PROFINET

PROFINET is the PROFIBUS International (PI) open Industrial Ethernet Standard that uses TCP/IP and IT standards for automation control.

The Stratix 5800 switch supports the forwarding of these PROFINET traffic types:

- TCP/IP
- Real-Time (RT)

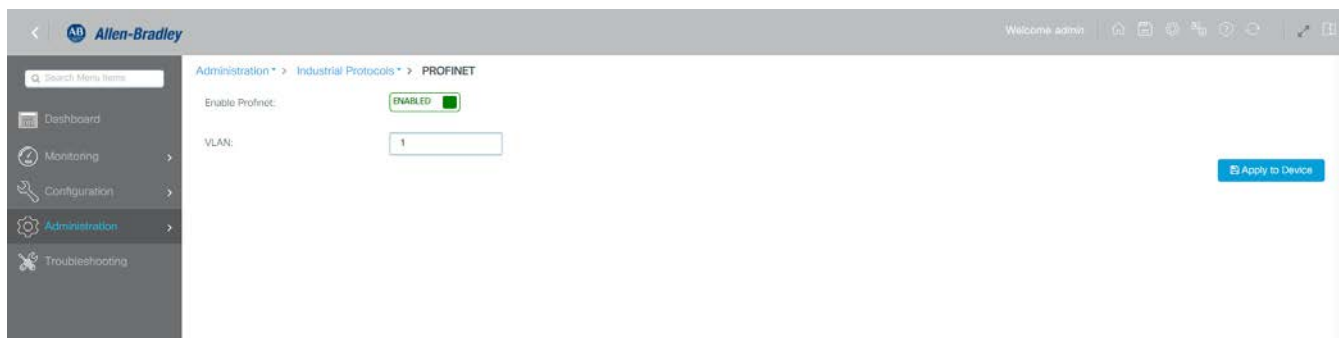
Stratix switches do not support the forwarding of Isochronous Real-Time (IRT) traffic.

PROFINET conformance classes define the capabilities of a device. All Stratix switches are Conformance Class B certified.

### Configure PROFINET via the WebUI

To configure PROFINET, from the Administration Menu, choose Industrial Protocols. An option for PROFINET is present.

From the following screen, you are able to choose to enable PROFINET.



After you enable PROFINET, it is available in the Monitoring tab.

The screenshot shows the Allen-Bradley Monitoring interface. The left sidebar contains navigation links: Dashboard, Monitoring (selected), Configuration, Administration, and Troubleshooting. The main content area is titled 'Monitoring > General > PROFINET'. It displays the PROFINET status and a table of sessions.

**Status**

Profinet:	Disabled	Profinet ID:	
Connection Status:	Disconnected	GSD version:	Unknown
VLAN:	1	Reduct Ratio:	128

**Sessions**

Session Number	Connected	No. of IO CRs	No. of diffModules
Session 1	No	0	0
Session 2	No	0	0
Session 3	No	0	0
Session 4	No	0	0

Navigation: 1 - 4 of 4 items, 5 items per page

From the PROFINET Monitoring screen, you can choose the status and session parameters.

**Table 132 - PROFINET Status Parameters**

Parameter	Description
Profinet	Shows whether PROFINET is enabled or disabled on the switch.
Connection Status	Shows whether the switch is connected to the PROFINET PLC (I/O Controller).
VLAN	The VLAN number for PROFINET traffic.
Profinet ID	PROFINET device identifier.
GSD version	Shows whether the General Station Description (GSD) file for the switch matches the GSD file in the controller configuration software.
Reduct Ratio	Reduction Ratio denotes the rate at which the real time (RT) packets are exchanged between controller and the IO devices. By default, the value is set to 128 ms. This denotes that the transmit and receive occurs at every 128th send clock. Other values like 256 and 512 can also be configured from the TIA tool.
MRP	Shows whether MRP is enabled or disabled.
MRP License Status	Shows whether the MRP license is active.
MRP Max Rings Allowed	The maximum number of MRP rings that can be configured based on the license.

**Table 133 - PROFINET Session Parameters**

Parameter	Description
Session Number	Number of the PROFINET session.
Connected	Shows whether the session is currently connected.
Number of I/O Communication Relationships	Number of IO Communication Relationships (CRs) for the session.
Number of diffModules	A value greater than zero means that there is a difference in expected (configured from TIA) and the actual submodules in the device. This number denotes the count of the differences. The presence of diffmodule blocks in the response shows the details of missing or additional submodules in the device from the ones configured.

# SDM-Template

Switch Management Database (SDM) templates optimize how system resources are allocated to support specific features, depending on how the switch is used in the network. In the WebUI, you can apply an SDM template to the switch.

To apply an SDM template to the switch, follow these steps.

- 1. From the Administration menu, choose SDM-Template.

The only SDM-Template available is the ‘Default’ template.

- 2. To select a template to apply to the switch, click a template in the List of Resources column, and then click Apply to Device.

Administration > Management > SDM-Template

SDM Template Config Select a value Advanced View

Current SDM Template | Default

List of Resources	No.of Resources Allocated
number of SVIs	32
number of VLANs	256
number of unicast mac addresses	8K
number of multicast groups (L2/L3)	1K
number of IPv4 unicast routes	2K
number of directly-connected IPv4 hosts	2K
number of indirect IPv4 routes	2K
number of IPv6 unicast routes	0.5K
number of directly-connected IPv6 addresses	0.5K
number of indirect IPv6 unicast routes	0.5K
number of IPv4 policy based routing aces	0
number of IPv4/MAC qos aces	2K

## Simple Network Management Protocol (SNMP)

SNMP enables the switch to be remotely managed through other network management software. SNMP defines the method of communication among the devices and also denotes a manager for the monitoring and supervision of the devices. For more information about SNMP, see the Ethernet Reference Manual, publication [ENET-RM002](#).

### Supported SNMP Versions

Stratix 5800 switches support SNMP versions 1, 2c, and 3. Your configuration requirements depend on the SNMP version you use. You can choose an SNMP version on the Hosts tab of the SNMP page of the WebUI for the switch.

SNMP Version	Required Configuration Components
SNMPv1	<ul style="list-style-type: none"> <li>A community string to authenticate access to the device.</li> <li>A host defined to be the recipient of SNMP notifications.</li> </ul>
SNMPv2C	<ul style="list-style-type: none"> <li>A community string to authenticate access to the device.</li> <li>A host defined to be the recipient of SNMP notifications.</li> </ul>
SNMPv3	<ul style="list-style-type: none"> <li>User security modes and authentication.</li> <li>A host defined to be the recipient of SNMP notifications.</li> </ul>

### SNMPv3 User Security Modes and Authentication

SNMPv3 enables you to configure an authentication strategy for a user. A combination of security modes and authentication protocols determines the security mechanism that is applied to an SNMP packet.

The following table describes the combinations of security modes and authentication you can configure for each user.


**Table 134 - User Security Modes and Authentication**

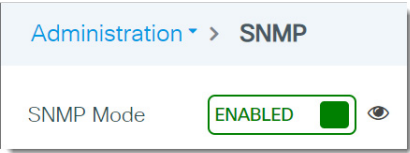
Security Mode	Authentication	Encryption	Result
AuthPriv (default)	Message digest algorithm 5 (MD5) or Secure hash algorithm (SHA)	Data Encryption Standard (DES)	Provides authentication based on the hashed message authentication code (HMAC)-MD5 or HMAC-SHA algorithms. In addition to authentication, provides DES 56-bit encryption based on the cipher block chaining (CBC)-DES (DES-56) standard.
AuthNoPriv	Message digest algorithm 5 (MD5) or Secure hash algorithm (SHA)	No	Provides authentication based on the hashed message authentication code (HMAC)-MD5 or HMAC-SHA algorithms.
NoAuthNoPriv	User name	No	Uses a user name match for authentication.

### Configure SNMP via the WebUI

From the Administration menu, choose SNMP.

From the SNMP page, you can configure these aspects of SNMP:

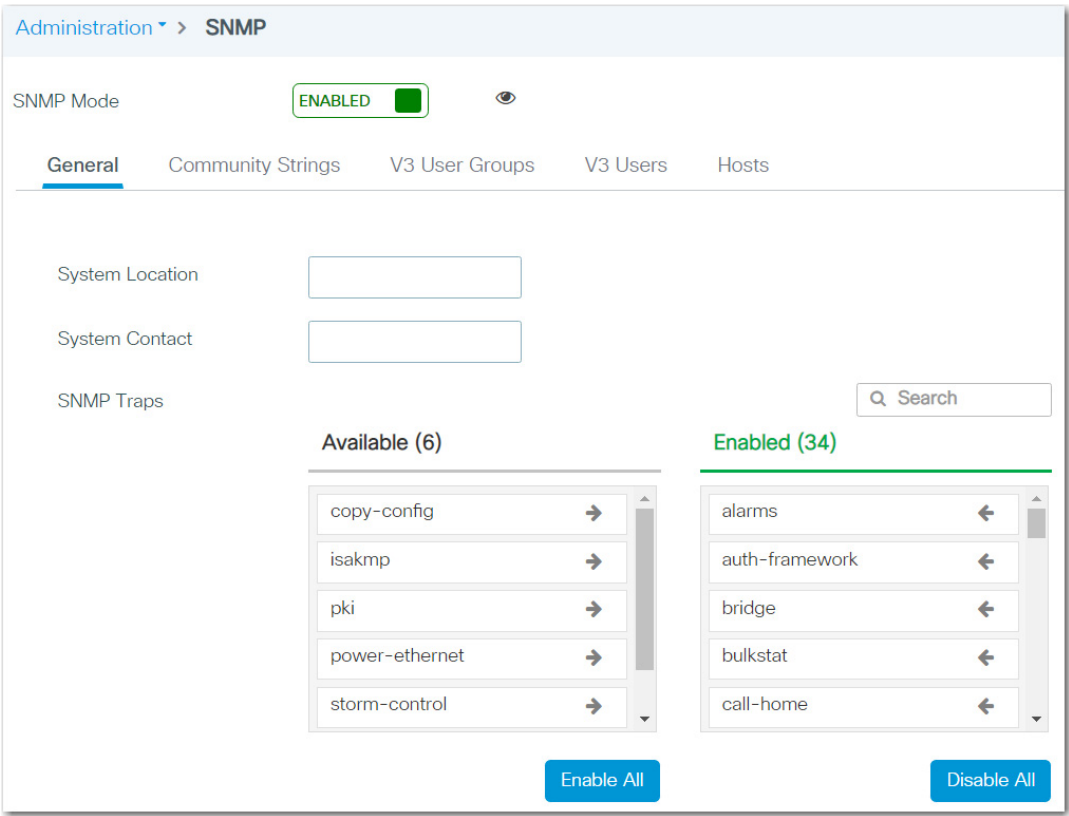
- To enable or disable SNMP mode, click the SNMP Mode field. To see all SNMP views that are included and excluded, click the eye  icon.




- To configure system information and enable or disable traps, see [page 212](#).
- To configure community strings, see [page 213](#). Community strings to provide a remote manager read-only or read/write access to the switch. Community strings are required for SNMP versions 1 and 2c.
- To configure SNMPv3 users and authentication, see [page 214](#). This feature requires that you choose SNMPv3 on the Hosts tab.
- To configure SNMP hosts, see [page 215](#).

*Configure System Information and SNMP Traps*

On the General tab, complete the fields as described in [Table 135](#), and then click Apply.



**Table 135 - SNMP—General**

Field	Description
SNMP Mode	Click to enable or disable SNMP. By default, SNMP is enabled. To see all SNMP views that are included and excluded, click the eye  icon.

**Table 135 - SNMP—General**

Field	Description
System Location	Enter the location of the device.
System Contact	Enter the contact details of the device administrator.
SNMP Traps	To enable one or more traps: <ul style="list-style-type: none"> <li>Click each trap to move it from the Available list to the Enabled list.</li> <li>or</li> <li>Click Enable All.</li> </ul> To disable one or more traps: <ul style="list-style-type: none"> <li>Click each trap to move it from the Enabled list to the Available list.</li> <li>or</li> <li>Click Disable All.</li> </ul>

### Configure Community Strings

On the Community Strings tab, you can add, edit, and delete community strings:

- To add a community string, click Add, complete the fields as described in [Table 136](#), and then click Apply to Device.
- To edit a community string, click the community name in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a community string, check its associated checkbox in the grid, and then click Delete.

**Table 136 - SNMP—Community Strings**

Field	Description
Community Name	Enter a name to identify the community. The name must be a unique, case-sensitive, alphanumeric string of up to 16 characters.
Access Mode	Choose the level of access to grant to this community: <ul style="list-style-type: none"> <li>Read Only (default)</li> <li>Read/Write</li> </ul>

### Configure V3 User Groups

On the V3 User Groups tab, you can add, edit, and delete SNMP V3 user groups and their authentication methods.

- To add a user group, click Add, complete the fields as described in [Table](#), and then click Apply to Device.
- To edit a user group, click the user group name in the grid, modify the fields, and then click Apply to Device.
- To delete a user, check its associated checkbox in the grid, and then click Delete.

V3 User Groups

Group Name\*

Security Level\*

Auth

Cancel

Apply to Device

Table 137 - V3 User Groups

Field	Descriptions
Group Name	Enter a name for the user group.
Security Level	Choose a security level: <ul style="list-style-type: none"><li>• Auth</li><li>• No Auth</li><li>• Priv</li></ul>

Configure SNMP Users and Authentication

On the V3 Users tab, you can add, edit, and delete SNMPv3 users and their authentication methods:

- To add a user, click Add, complete the fields as described in [Table 138](#), and then click Apply to Device.
- To edit a user, click the user name in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a user, check its associated checkbox in the grid, and then click Delete.

V3 Users

User Name\*

Group Name\*

None

+

Security Mode\*

AuthPriv

i

Authentication Protocol

MD5

Authentication Password\*

Privacy Protocol

3DES

Privacy Password\*

Cancel

Apply to Device

Table 138 - SNMP—V3 Users

Field	Description
User Name	Enter a name for the user.
Group Name	Choose an existing group name, or to create a new group name, click the plus sign (+).
Security Mode	Choose a security mode. See <a href="#">SNMPv3 User Security Modes and Authentication on page 211</a> .
Authentication Protocol	(Applies only to AuthPriv and AuthNoPriv security modes). Choose an algorithm to configure authentication based on the Hashed message authentication code (HMAC)-MD5 or HMAC-SHA algorithms: <ul style="list-style-type: none"><li>• MD5 (default)</li><li>• SHA</li></ul>

**Table 138 - SNMP—V3 Users (Continued)**

Field	Description
Authentication Password	(Applies only to AuthPriv and AuthNoPriv security modes). Enter a password to authenticate user access.
Privacy Protocol	(Applies only to AuthPriv security mode). Choose an encryption method: <ul style="list-style-type: none"> <li>• 3DES (default)</li> <li>• AES128</li> <li>• AES192</li> <li>• AES256</li> <li>• DES</li> </ul> AES 128, AES 192, and AES 256 use Cipher Feedback (CFB) mode with encryption key sizes of 128 bits, 192 bits, or 256 bits respectively. 3DES uses the cipher block chaining (CBC)-DES (DES-56) standard with a 168-bit key size for encryption.
Privacy Password	(Applies only to AuthPriv security mode). Enter a password for the user.

### Add SNMP Hosts

On the Hosts tab, you can add, edit, and delete SNMP hosts, or recipients of SNMP notifications:

- To add a host, click Add, complete the fields as described in [Table 139](#), and then click Apply to Device.
- To edit a host, click the user name in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a host, check its associated checkbox in the grid, and then click Delete.

**Table 139 - SNMP—Hosts**

Field	Description
IPv4/IPv6 Address	Enter the IP address for the device to accept and use to send SNMP packets. An AND operation is performed between the requesting entity IP address and the subnet mask before being compared to the IP address. If the subnet mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. Default value: 0.0.0.0
Version	Choose the SNMP version. See <a href="#">Supported SNMP Versions on page 211</a> .
Community String	For SNMP versions 1 and 2c, enter the SNMP community that you want to use.
Port	Enter the UDP port number for the remote SNMP agent of the device where the user resides. Valid values: 0...65535 Default value: 162
Type	Choose traps to enable the device to send SNMP traps to this host.



## Software Upgrade

In the WebUI of the switch, you can upgrade the software image on your switch.

1. From the Administration menu, choose Software Upgrade.
2. Complete the fields as described in [Table 140](#), and then click Download.
3. To restart the switch with the new software, click Save Configuration & Reload.

Administration > Software Upgrade

Software Upgrade

Upgrade Mode: BUNDLE  
Current Mode (until next reload): BUNDLE

Transport Type: My Desktop

Source File Path\*: [Select File](#)

Destination: Flash     Free Space: 1277.86 MB

[Download](#)

**Manage**  
[Remove Inactive Files](#)  
[Rollback](#)



If you need more free space, there is an option under the Manage heading, to “Remove Inactive Files.”

**Table 140 - Software Upgrade**

Field	Description
Upgrade Mode	There are two modes: <ul style="list-style-type: none"> <li>• BUNDLE (recommended)-allows for the download of the bundle of files to local storage media</li> <li>• INSTALL</li> </ul>
Transport Type	Choose the method to use for sending the software image to your device: <ul style="list-style-type: none"> <li>• TFTP</li> <li>• SFTP</li> <li>• FTP</li> <li>• Device</li> <li>• Desktop (HTTPS)</li> </ul>
Source File Path	(Applies only for Desktop transport types.) Click to select the .bin file from your local device. If you inadvertently select a file that is not a .bin file, an error message appears.
Server IP Address (IPv4/IPv6)	(Applies only to TFTP, SFTP, or FTP transport types.) Enter the IP address of the FTP or TFTP server to use.
(SFTP/FTP) Username	(Applies only to SFTP or FTP transport types.) Enter the SFTP or FTP user name.
(SFTP/FTP) Password	(Applies only to SFTP or FTP transport types.) Enter the SFTP or FTP password.
File System	(Applies only to Device transport type.) Choose a file system for the file: <ul style="list-style-type: none"> <li>• Flash</li> <li>• SD</li> <li>• USB Flash (Available when USB is inserted)</li> </ul>
File Path	Specify the complete path from where you want to download the software image file, including the name of the file. <b>EXAMPLE:</b> FolderOnFTP/s5800-universalk9.16.10.01i.SPA.bin
Destination	(Applies to all transport types except Device.) Choose a destination for the file: <ul style="list-style-type: none"> <li>• SD Flash</li> <li>• Flash</li> <li>• USB Flash (Available when USB is inserted)</li> </ul>

## Stratix 5800 Boot Order

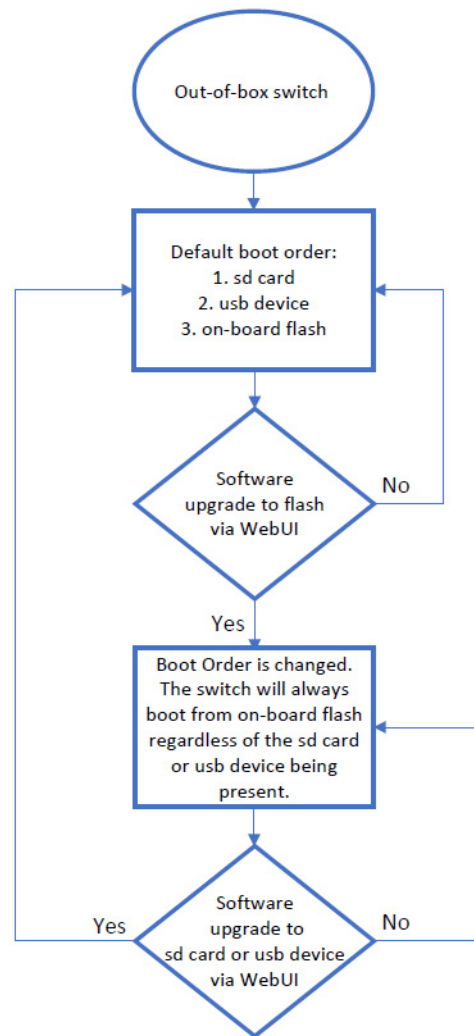
The boot order of the switch changes based on software updates using WebUI. By default, the boot order is:

1. SD Card
2. USB Device
3. On-board Flash

However, if a software upgrade is made to the on-board flash via WebUI, the boot order changes and the device boots from the on-board flash regardless of whether or not an SD card or USB device is plugged in.

The boot order can be reverted back to the original order by performing a software upgrade to the SD card or USB device.

**Figure 24 - Boot Order**



## Command Line Interface (CLI) Boot Order

Unlike the WebUI, a software upgrade to the switch using the CLI does not change the boot order.

### *View the CLI Boot Order*

The `ENABLE_FLASH_PRIMARY_BOOT` flag under the 'show boot' command decides the boot order of the switch. If this flag is set to 'No', the default boot order of SD card, USB device, and On-Board Flash is followed. If this flag is set to 'Yes', the switch will always boot from the On-board flash.

### *Configure or Change the Boot Order*

The `ENABLE_FLASH_PRIMARY_BOOT` flag is changed with the CLI under the global configuration mode. Use the 'boot flash-primary' command to set the flag to 'yes'. Use the 'no boot flash-primary' command to set the flag to 'No'.



If you upgrade software to the SD card or the USB device then the boot order stays the same.

## User Administration

You can maintain user accounts with specified privilege levels and password policies to help prevent unauthorized users from reconfiguring the switch and viewing its configuration.

### Privilege Levels

A privilege level defines what commands a user can enter by using the CLI after logging on to the switch. There are two methods of configuring a privilege level:

- Basic—Allows admin, read-only, or no access privileges.

Users with read-only privileges are restricted from viewing the configuration, administration, and troubleshooting pages in the WebUI.

- Advanced—Allows privilege level between 0...15. Privilege 1 allows access in User Exec mode. Privilege 15 allows access in Privileged Exec mode.

### Password Policies

A password policy is a security mechanism for defining rules, constraints, and restrictions to specify user passwords. You can create a password policy via the CLI, and then apply the policy to users when creating accounts.

## Create a User Account via the WebUI

From the Administration menu, choose User Administration.

Administration > User Administration

+ Add X Delete

Name	Privilege	Policy
<input type="checkbox"/> admin	Admin	None

1 50 items per page 1 - 1 of 1 items

From the User Administration page, you can add, edit, and delete users:

- To add a user, click Add, complete the fields as described in [Table 141](#), and then click Apply to Device.
- To edit a user, click the name in the grid, modify the fields, and then click Update & Apply to Device.
- To delete a user, check its associated checkbox in the grid, and then click Delete.

Create User Administration

User Name\*

Policy

Privilege

Password\*


Confirm Password\*

Important guidelines to create new Password

- ✓ Must contain at least 6 characters
- ✓ Must contain at most 127 characters

Cancel Apply to Device

Table 141 - Create User Administration

Field	Description
User Name	Enter a unique user name.
Policy	(Optional). Choose a password policy. See <a href="#">Password Policies on page 218</a> .
Privilege	To assign a basic privilege level, choose Admin, Read Only, or No Access. To assign an advanced privilege level, click the  icon, and then choose a numeric value. See <a href="#">Privilege Levels on page 218</a> .
Password	Enter the password to authenticate the user when they log on to the switch. See the guidelines in the upper-right corner of the page. The password must meet these requirements: <ul style="list-style-type: none"><li>• Minimum length: 6 characters</li><li>• Maximum length: 27 characters</li><li>• If you specified a password policy, the password must meet all criteria in the policy.</li></ul>
Confirm Password	Reenter the password.

## Security Requirements (IEC-62443-4-2)

Topic	Page
Switch Security Features	219
Telnet	220
TLS 1.2	222
Additional Resources	223

Stratix® 5800 switches with IOS release 16.12.01 and later support IEC-62443-4-2 SIL 1 and SIL 2 security requirements.

### Switch Security Features

For the Stratix 5800 switch to comply with the certification requirements, implement the security features in the following table in the order listed.

✓	Switch Security Feature	Required to Meet IEC-62443-4-2	Details
	IOS Release is certified for IEC-62443-4-2	Yes	To verify if your IOS release is certified for IEC-62443-4-2, access product release notes from the Product Compatibility and Download Center at <a href="http://rok.auto/pcdc">rok.auto/pcdc</a> .
	Configure Certificate Authority (CA)	Yes	A CA provides a chain of trusts for devices in the network. This mechanism provides the ability for a user or process to trust the connection to one of these devices on the network by validating its identity. For more information, see the Security Configuration Guide available at <a href="https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg.html">https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg.html</a> .
	Configure Authentication, Authorization, and Accounting (AAA)	Yes	AAA services provide flexible administrative control and accounting for network access. For more information, see <a href="#">Authentication, Authorization, and Accounting (AAA) on page 49</a> and the Security Configuration Guide available at <a href="https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg.html">https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg.html</a> .
	Disable Telnet <sup>(1)</sup>	Yes	Telnet is disabled by default during Express Setup. Keep Telnet disabled to secure remote access to the switch, such as when you are using the command-line interface (CLI) to manage the switch from a computer. To verify that Telnet is disabled or disable Telnet if needed, see <a href="#">Telnet on page 220</a> .
	Transport Layer Security (TLS) 1.2	Yes	TLS 1.2 is enabled by default during Express Setup. Keep this feature enabled to secure the exchange of data through encryption. To verify that TLS 1.2 is enabled or to enable TLS 1.2 if needed, see <a href="#">TLS 1.2 on page 222</a> .
	Configure Type 9 password hashing	Yes	Hashing makes password storage more secure by transforming a password into data that cannot be converted back to the original password. For more information, see the User Security Configuration Guide at <a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/xs-16-12/sec-usr-cfg-xe-16-12-book.html">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/xs-16-12/sec-usr-cfg-xe-16-12-book.html</a> .

(1) When both Telnet and Secure Shell (SSH) are disabled, the only way to access the switch is via console cable or HTTPS.



Secure web access to the switch is enforced via HTTPS. Attempts to access the switch via HTTP automatically redirect to secure access via HTTPS.

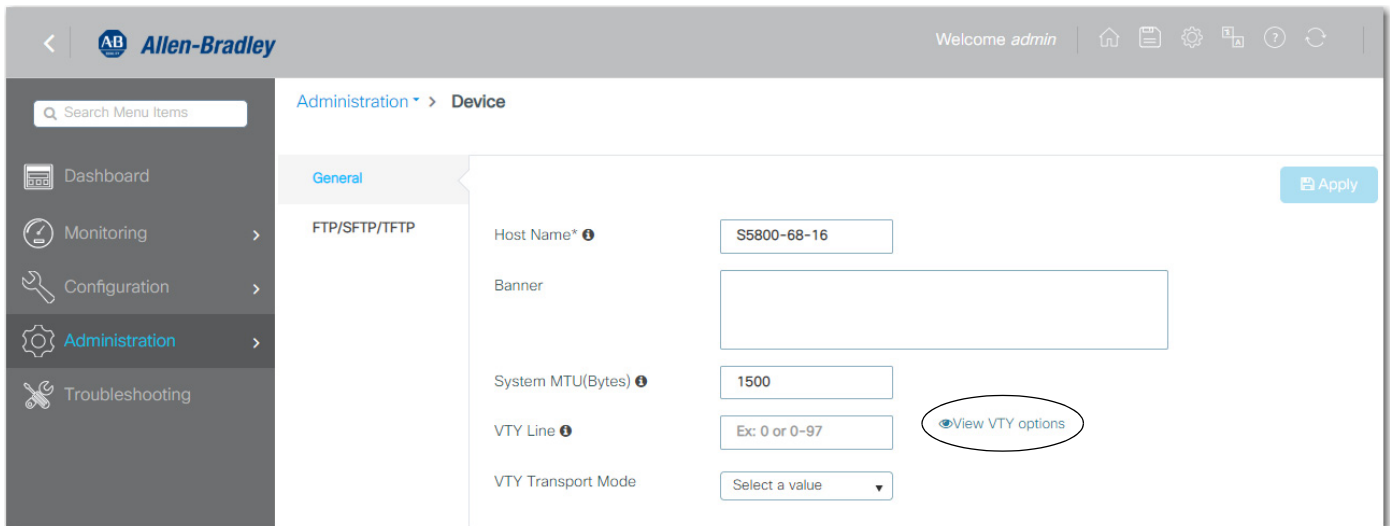
## Telnet

Telnet must be disabled to comply with IEC-62443-4-2 requirements. By default, Telnet is disabled during Express Setup. The following procedures describe how you can verify that Telnet is disabled and disable it if needed.

### Verify Telnet Settings

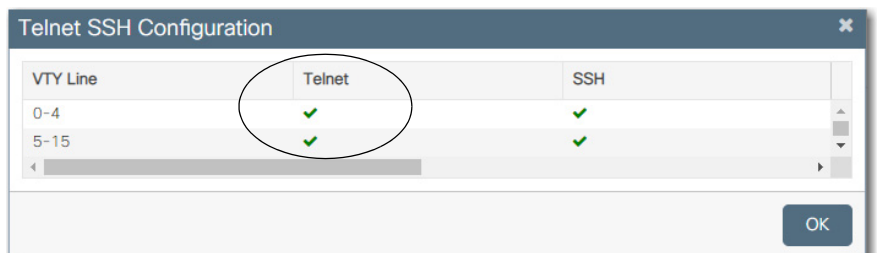
To verify that Telnet is disabled, follow these steps.

1. From the Administration menu, choose Device.
2. On the General tab, click View VTY options.



3. On the Telnet SSH Configuration dialog box, note which lines must be disabled, and then click OK.

Telnet is currently enabled on any single lines or range with a checkbox in the Telnet column.



4. If Telnet is enabled on any lines to the switch, proceed to [Disable Telnet on page 221](#).

## Disable Telnet

To disable Telnet on lines to the switch, follow these steps.

1. From the Administration menu, choose Device.
2. In the VTY Line field, enter a single line or range of lines on which to disable Telnet.
3. In the VTY Transport Mode field, choose one of these values, and then click Apply:
  - SSH—SSH is enabled, and Telnet is disabled.
  - None—Both SSH and Telnet are disabled.

The screenshot shows the Allen-Bradley configuration interface. The left sidebar contains a search bar and a menu with items: Dashboard, Monitoring, Configuration, Administration (highlighted), and Troubleshooting. The main content area is titled 'Administration > Device'. Under the 'General' tab, the 'FTP/SFTP/TFTP' section is active. It contains the following fields: 'Host Name\*' with value 'S5800-68-16', 'Banner' (empty), 'System MTU(Bytes)' with value '1500', 'VTY Line' with value '0-2', and 'VTY Transport Mode' with a dropdown menu showing 'None'. A blue 'Apply' button is located in the top right corner. A black oval is drawn around the 'VTY Line' and 'VTY Transport Mode' fields.



## TLS 1.2

TLS 1.2 must be enabled and all other TLS versions must be disabled to comply with IEC-62443-4-2 requirements. By default, TLS 1.2 is enabled during Express Setup and all other versions are disabled. The following procedures describe how you can verify that TLS 1.2 is enabled and then enable it if needed.

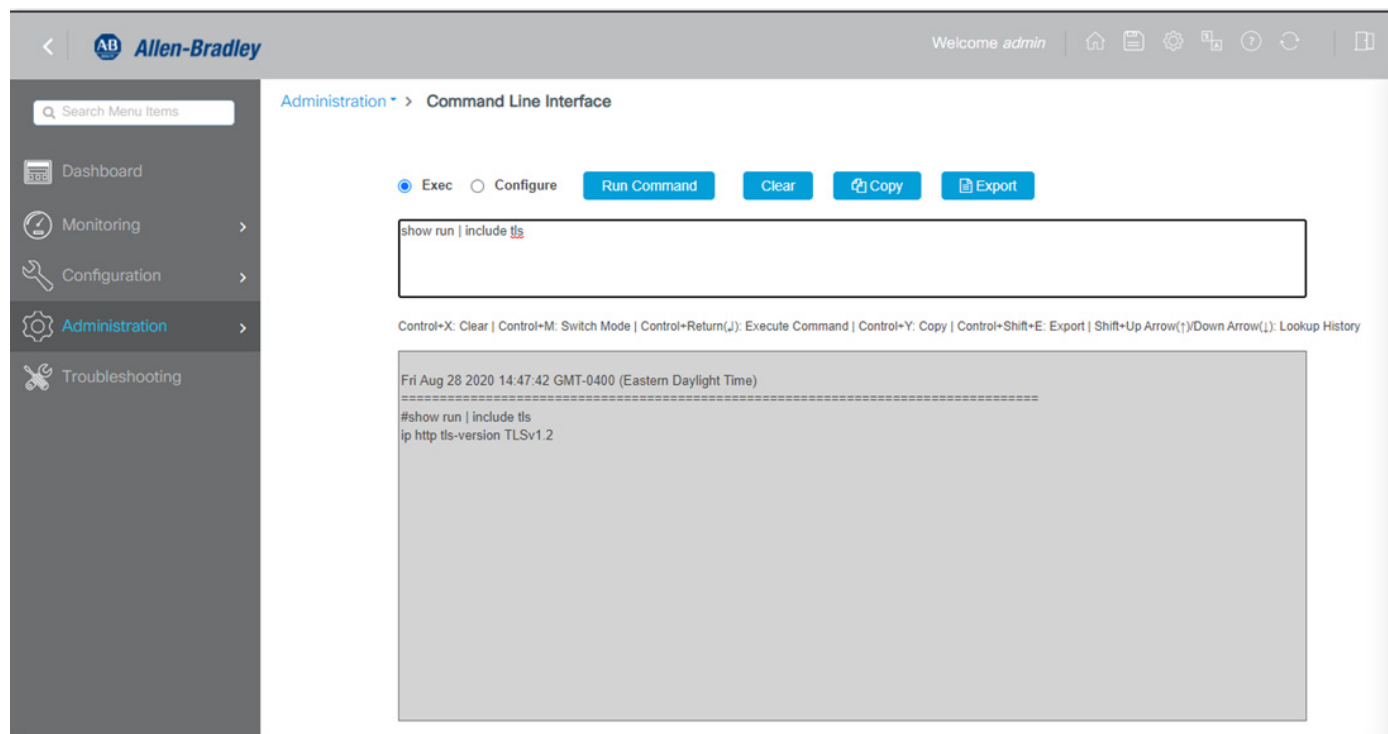
### Verify TLS 1.2 Settings

To verify that TLS 1.2 is enabled, follow these steps.

1. From the Administration menu, choose Command Line Interface.
2. Click Exec to run the command in Executive mode.
3. In the text box, type the following command, and then click Run Command:

**show run | include tls**

4. If the result is **ip http tls-version TLSv1.2**, then TLS 1.2 is enabled and only that version of TLS is allowed.
5. If any version other than 1.2 shows, proceed to [Enable TLS 1.2 on page 223](#).



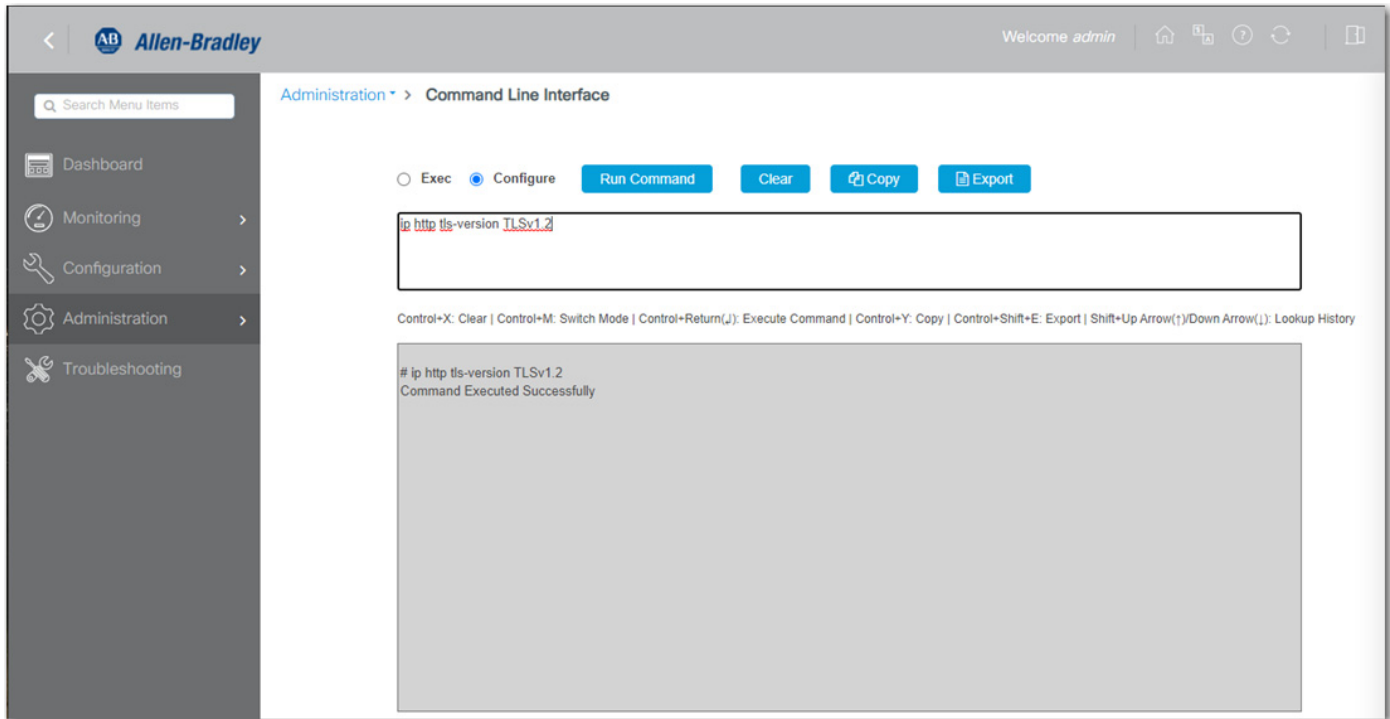
## Enable TLS 1.2

To enable TLS 1.2, follow these steps.

1. From the Administration menu, choose Command Line Interface.
2. Click Configure to run the command in Configure mode.
3. In the text box, type the following command, and then click Run Command:

**ip http tls-version TLSv1.2**

The command enables TLS 1.2 and disallows any other version of TLS.



## Additional Resources

For more information about how to implement security requirements, see the following resources.

Resource	Description
User Security Configuration Guide available at <a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/xr-16-12/sec_usr_cfg-xe-16-12-book.html">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/xr-16-12/sec_usr_cfg-xe-16-12-book.html</a>	Cisco® publication that provides details about how to secure user access to the switch. For the User Security Configuration Guide that corresponds to the current IOS version on your switch, search <a href="http://www.cisco.com">www.cisco.com</a> .
Security Configuration Guide available at <a href="https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg.html">https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg.html</a>	Cisco publication that provides details about how to secure the switch on your network. For the Security Configuration Guide that corresponds to the current IOS version on your switch, search <a href="http://www.cisco.com">www.cisco.com</a> .
Security Configuration User Manual, publication <a href="#">SECURE-UM001</a>	Describes how to configure and use Rockwell Automation products to improve the security of your industrial automation system.
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, publication <a href="#">ENET-TD001</a> .	Defines manufacturing-focused reference architectures to help accelerate the successful deployment of standard networking technologies and convergence of manufacturing and enterprise/business networks.

**Notes:**

## Monitor the Switch

Topic	Page
Switch Status	225
Neighbors	226
Common Industrial Protocol (CIP)	228
Dynamic Host Configuration Protocol (DHCP) Clients	230
Network Address Translation (NAT)	231
MODBUS (Modicon Communication Bus)	237
Ports	239
Parallel Redundancy Protocol (PRP)	242
Resiliency Ethernet Protocol (REP)	246
System	247
Time	250

## Switch Status

In the Logix Designer application, you can view overall switch status information as shown in the following figure.

In the navigation pane, click Switch Status.

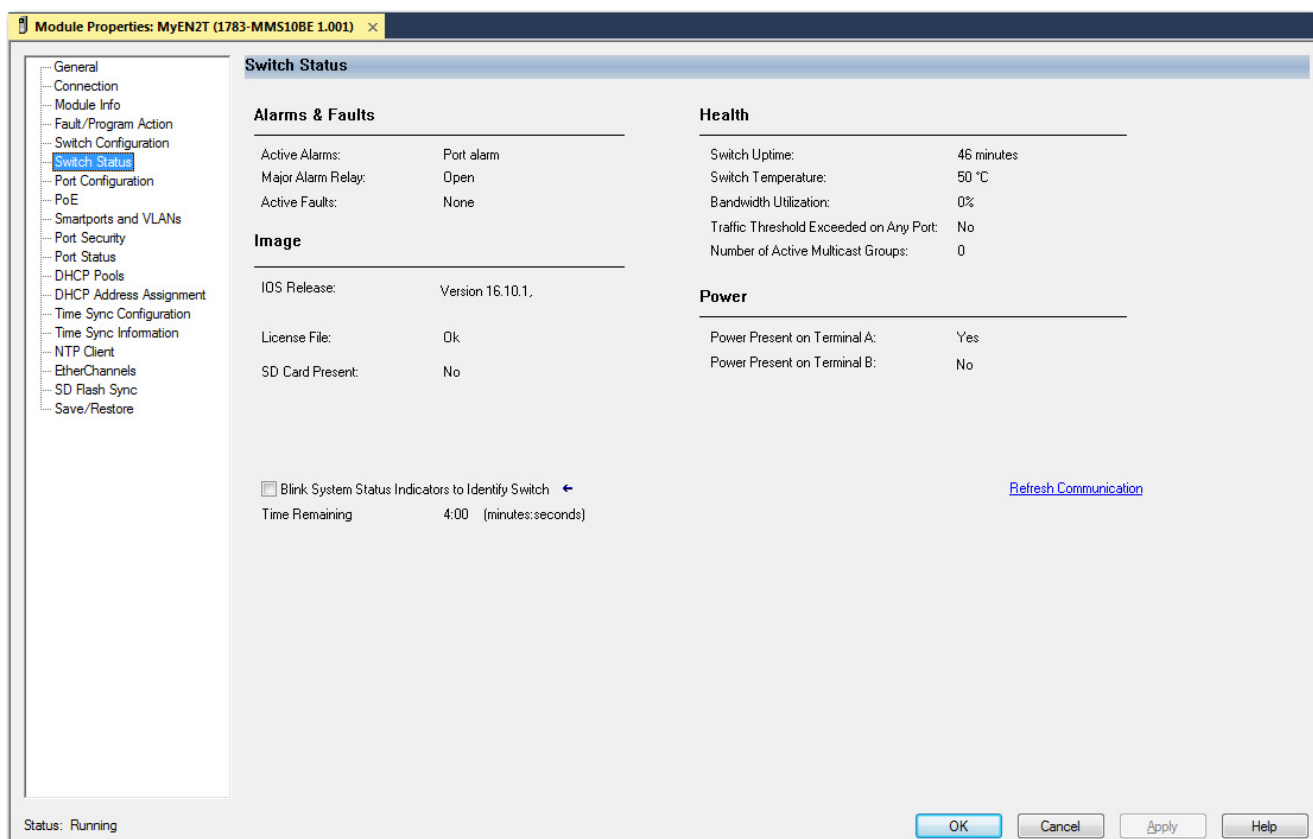


Table 142 - Switch Status

Field	Description
<b>Alarms &amp; Faults</b>	
Active Alarms	The current active alarm: <ul style="list-style-type: none"> <li>• None</li> <li>• Port alarm</li> <li>• Dual Mode Power Supply alarm</li> <li>• Primary Temperature alarm</li> </ul>
Major Alarm Relay	The status of the alarm relay: <ul style="list-style-type: none"> <li>• Open</li> <li>• Closed</li> </ul>
Active Faults	The current active fault: <ul style="list-style-type: none"> <li>• None</li> <li>• Port fault</li> <li>• Hardware fault</li> </ul> If the port and hardware faults are active, the Hardware fault status appears.
<b>Health</b>	
Switch Uptime	The days, hours, and minutes that the switch has been functioning since the last restart.
Switch Temperature	The current internal temperature (in degree Celsius) of the switch.
Bandwidth Utilization	The total percentage of the switch bandwidth being used.
Traffic Threshold Exceeded on Any Port	Indicates whether the current unicast, multicast, and broadcast thresholds have been exceeded on any port.
Number of Active Multicast Groups	The number of active multicast groups.
<b>Image</b>	
IOS Release	The current version of the switch operating system.
License File	Indicates whether the license file is valid.
SD Card Present	Indicates whether the SD card is installed.
<b>Power</b>	
Power Present on Terminal A	Indicates whether power is present on terminal A.
Power Present on Terminal B	Indicates whether power is present on terminal B.

## Neighbors

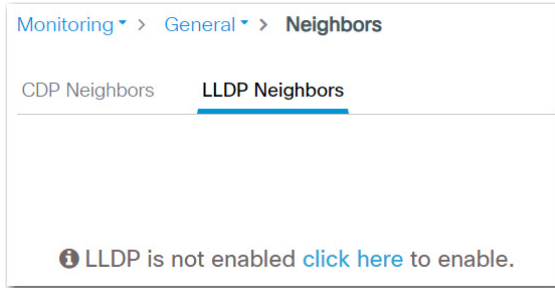
In the WebUI, you can view neighbor information that uses Cisco® Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP).

When CDP or LLDP is enabled, you can use the neighbor information from each node to determine complete network topology.

From the Monitoring menu, choose Neighbors:

- To view CDP neighbor information, see the information on the CDP Neighbors tab as described in [Table 143](#). For more information about CDP, see [page 70](#).
- To view LLDP neighbor information, see the information on the LLDP Neighbors tab as described in [Table 144](#). For more information about LLDP, see [page 70](#).

If LLDP is not enabled on the switch, a message appears. To enable LLDP, click the link in the message.



Monitoring > General > Neighbors

CDP Neighbors LLDP Neighbors

Local Port	Neighbor Name	Neighbor Port	TTL	Capability	Platform
GigabitEthernet1/5	Lab3850.stratix.com	GigabitEthernet1/0/13	178	Switch IGMP	cisco WS-C3850-48P

10 items per page

Table 143 - Monitor CDP Neighbors

Field	Description
Local Port	The port number on the local switch.
Neighbor Name	The name of the CDP neighbor device.
Neighbor Port	The port number on the CDP neighbor device.
TTL	The time left in seconds before each CDP neighbor entry expires.
Capability	The functional capability of the neighbor device: <ul style="list-style-type: none"> <li>Router</li> <li>Trans Bridge</li> <li>Source Route Bridge</li> <li>Switch</li> <li>Host</li> <li>IGMP</li> <li>Repeater</li> <li>Remotely Managed Device</li> </ul>
Platform	The platform of the CDP neighbor device.

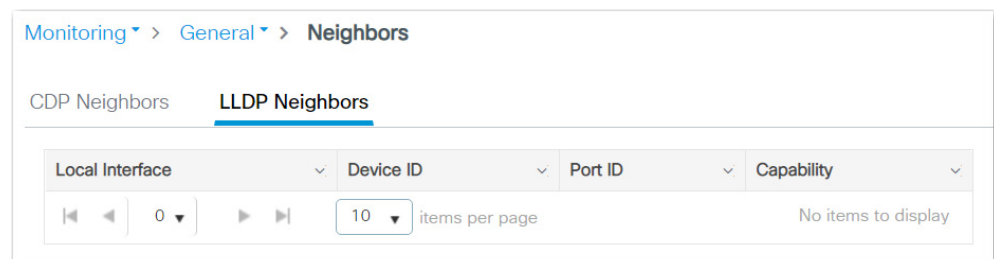


Table 144 - Monitor LLDP Neighbors

Field	Description
Local Interface	The local interface through which this neighbor is connected.
Device ID	The ID of the neighboring device.
Port ID	The interface and port number of the neighboring device.
Capability	The device type of the neighbor, indicated by the capability code discovered on the device: <ul style="list-style-type: none"> <li>Router</li> <li>Trans Bridge</li> <li>Source Route Bridge</li> <li>Switch</li> <li>Host</li> <li>IGMP</li> <li>Repeater</li> <li>Remotely Managed Device</li> </ul>

## Common Industrial Protocol (CIP)

In the WebUI, you can monitor information about CIP™ status and statistics since the switch was last powered on, was restarted, or the counters were last reset.

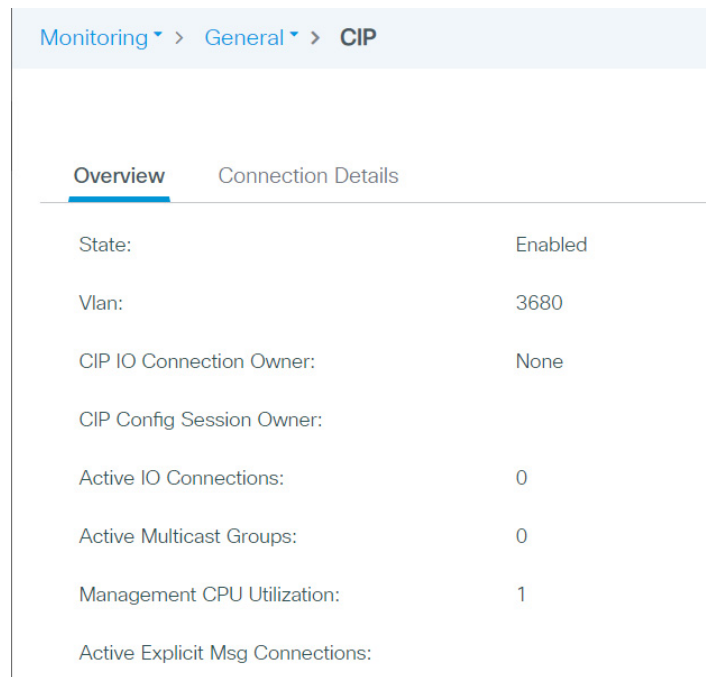
### IMPORTANT

Except for Active Multicast Groups, all other categories are related to the CIP server in the switch. The categories pertain to CIP traffic directed to the switch as a CIP target device. The categories do not refer to CIP (EtherNet/IP™) traffic that flows through the switch among these devices:

- Various CIP controllers
- HMI devices
- Configuration tools
- Other CIP target devices, such as drives, I/O modules, motor starters, sensors, and valves

From the Monitoring menu, choose CIP:

- To view general CIP information, such as status, VLAN, and total number of connections, see the information on the Overview tab as described in [Table 145](#).
- To view connection details, see the information on the Connection Details tab as described in [Table 146](#).



**Table 145 - Monitor CIP—Overview Tab**

Field	Description
State	The state of the CIP protocol: <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
Vlan	The CIP VLAN ID.
CIP IO Connection Owner	The IP address of the device to and from which application-specific I/O output data is sent.
CIP Config Session Owner	The IP address of the device controlling the CIP configuration session.
Active IO Connections	The number of active application-specific connections between a producing application and one or more consuming applications.
Active Multicast Groups	The number of multicast groups, including the CIP multicast group, configured on the device.
Management CPU Utilization	The CPU usage (%) for the CIP configuration session owner.
Active Explicit Msg Connections	The number of active explicit message connections (generic, multipurpose communication) between devices.

Monitoring > General > CIP

Overview	Connection Details
Open Requests:	0
Open Format Rejects:	0
Open Resource Rejects:	0
Open Other Rejects:	0
Close Requests:	0
Close Format Rejects:	0
Close Other Rejects:	0
Connection Timeouts:	0

**Table 146 - Monitor CIP—Connection Details Tab**

Field	Description
Open Requests	The number of Forward Open requests to establish a connection with an industrial device in the network.
Open Format Rejects	The number of Forward Open requests that failed because the request was not in the proper format
Open Resource Rejects	The number of Forward Open requests that failed to establish a new connection for reasons such as insufficient memory.
Open Other Rejects	The number of Forward Open requests that failed for reasons such as incompatible electronic keying.
Close Requests	The number of Forward Close requests received after a connection is successfully established with an industrial device in the network.
Close Format Rejects	The number of Forward Close requests that failed because the request was not in the proper format.
Close Other Rejects	The number of Forward Close requests that failed for reasons such as incompatible electronic keying.
Connection Timeouts	The number of connection timeouts that have occurred.



# Dynamic Host Configuration Protocol (DHCP) Clients

In the WebUI, you can view information about devices that receive IP addresses from the switch when it is configured as a DHCP server. These devices are known as DHCP clients.

The table contains an entry for each device that meets this criteria:

- The device received its IP address from the switch via DHCP, and the IP address lease is active.
- A VLAN is assigned to the DHCP client port that connects to the switch, and DHCP snooping is enabled for that VLAN.

From the Monitor menu, choose DHCP Clients.

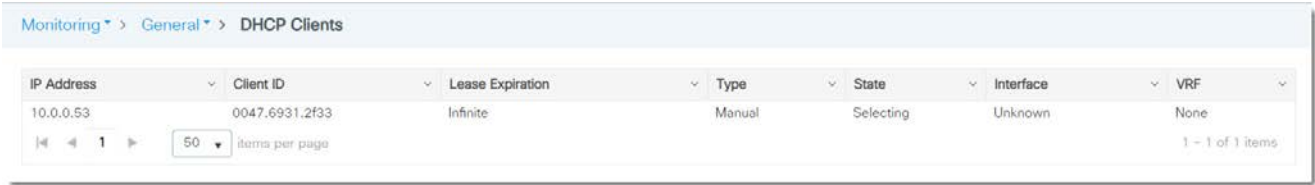


Table 147 - Monitor DHCP Clients

Field	Description
IP Address	The IP address that the switch assigned to the DHCP client.
Client ID	The MAC ID of the DHCP client.
Lease Expiration	The lease expiration date of the IP address.
Type	The manner in which the IP address was assigned to the host: <ul style="list-style-type: none"><li>• Automatic—The IP address of the DHCP client was dynamically assigned from the DHCP pool of IP addresses.</li><li>• Manual—The IP address of the DHCP client was set to a specific IP address via the DHCP Persistence feature.</li></ul>
State	The state port that connects to the DHCP client.
Interface	The port that connects to the DHCP client.
VRF	The table that provides virtual routing and forwarding.

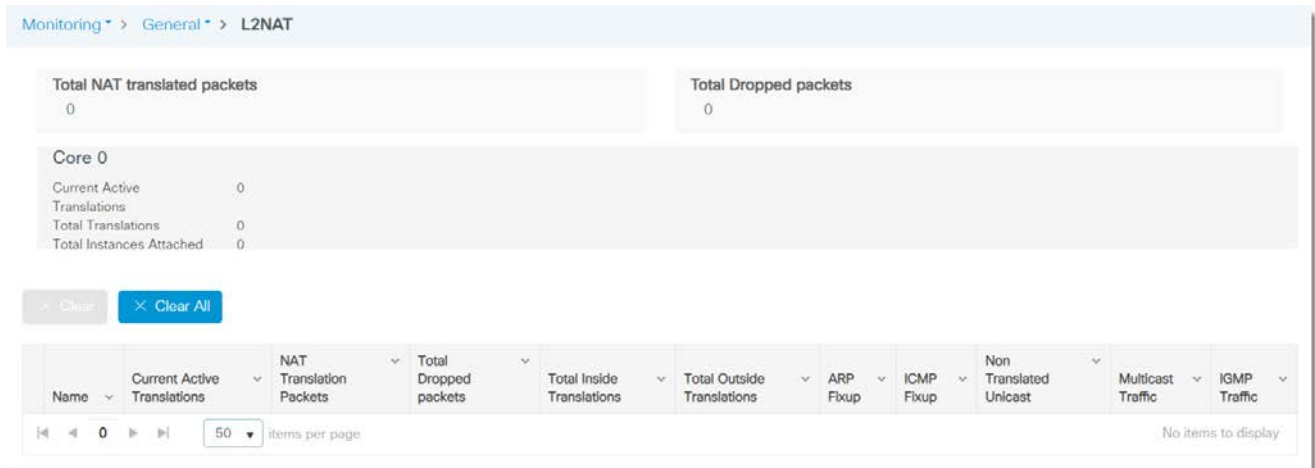
## Network Address Translation (NAT)

You can view details about NAT globally and per instance in both the WebUI and the Logix Designer application.

### Monitor NAT Statistics via the WebUI

From the Monitoring menu, choose L2NAT:

- To view global and per instance statistics, see the header and grid area on the L2NAT page as described in [Table 148](#).
- To view statistics for a single NAT instance, click the instance in the grid to display the Instance Details page as described in [Table 149](#) and [Table 150](#).
- To reset counters to zero, click Clear All.



**Table 148 - L2NAT**

Field	Description
<b>Global Statistics</b>	
Total NAT translated packets	The number of packets that were translated by the switch.
Total Dropped packets	The number of packets that were dropped due to NAT rules.
Core 0	Statistics for Core 0 (on the Stratix® 5800, there is only one core named Core 0).
Current Active Translations	The number of translations in applied NAT instances.
Total Translations	The total number of private and public translations.
Total Instances Attached	The number of NAT instances.
<b>Instance Statistics</b>	
Name	The name of the NAT instance.
Current Active Translations	The number of translations in the NAT instance.
NAT Translation Packets	The number of translated packets in the NAT instance.
Total Dropped packets	The number of packets that were dropped due to settings in the NAT instance.
Total Inside Translations	The number of internal addresses translated to external addresses in the NAT instance.
Total Outside Translations	The number of external addresses translated to internal addresses in the NAT instance.
ARP Fixup	The number of packets handled with the ARP Fixup to change dynamic ARP entries into static entries in the NAT instance.
ICMP Fixup	The number of packets handled with the ICMP Fixup to change dynamic ICMP entries into static entries in the NAT instance.
Non Translated Unicast	The number of unicast traffic packets that were not translated in the NAT instance.
Multicast Traffic	The number of multicast traffic packets in the NAT instance.
IGMP Traffic	The number of ICMP traffic packets in the NAT instance.

Instance Details		
General		Translations
Translations		
Current Active		0
Total NAT Packets		0
Private to Public		1
Public to Private		0
Total Dropped packets		1
Fixups		
ARP		0
ICMP		0
Total		0
Traffic		
Non Translated Unicast		0
Multicast		0
IGMP		0

Table 149 - Instance Details—General Tab

Field	Description
<b>Translations</b>	
Current Active Translations	The number of translations in the NAT instance.
Total NAT Packets	The number of translated packets in the NAT instance.
Private to Public	The number of private addresses translated to public addresses in the NAT instance.
Public to Private	The number of public addresses translated to private addresses in the NAT instance.
Total Dropped packets	The number of packets that were dropped due to settings in the NAT instance.
<b>Fixups</b>	
ARP	The number of packets handled with ARP Fixup to change dynamic ARP entries into static entries in the NAT instance.
ICMP	The number of packets handled with the ICMP Fixup to change dynamic ICMP entries into static entries in the NAT instance.
Total	The total number of packets that were fixed up.
<b>Traffic</b>	
Non Translated Unicast	The number of unicast traffic packets that were not translated.
Multicast	The number of multicast traffic packets.
IGMP	The number of ICMP traffic packets.

The screenshot shows the 'Instance Details' window with the 'Translations' tab selected. The window has a sidebar with 'General' and 'Translations' tabs. The 'Translations' tab contains a table with the following data:

Private IP	Public IP	Mask	Total Packets	Total Active Packets
1.1.1.1	4.4.4.4	false	0	0

Below the table, there is a pagination bar showing '1' items per page and '1 - 1 of 1 items'. An 'OK' button is located at the bottom right of the window.

**Table 150 - Instance Details—Translations Tab**

Field	Description
Private IP	The IP address on the private (inside) network.
Public IP	The IP address on the public (outside) network.
Mask	The subnet mask for the network IP address.
Total Packets	The total number of translated packets.
Total Active Packets	The total number of active packets translated.

## Monitor NAT Statistics via the Logix Designer Application

In the navigation pane, click NAT:

- To view NAT statistics across all NAT instances, see the Global Diagnostics area described in [Table 151](#).
- To view statistics for a specific NAT instance, click the Ellipse button in the Diagnostics column for the instance. See [Table 152](#).

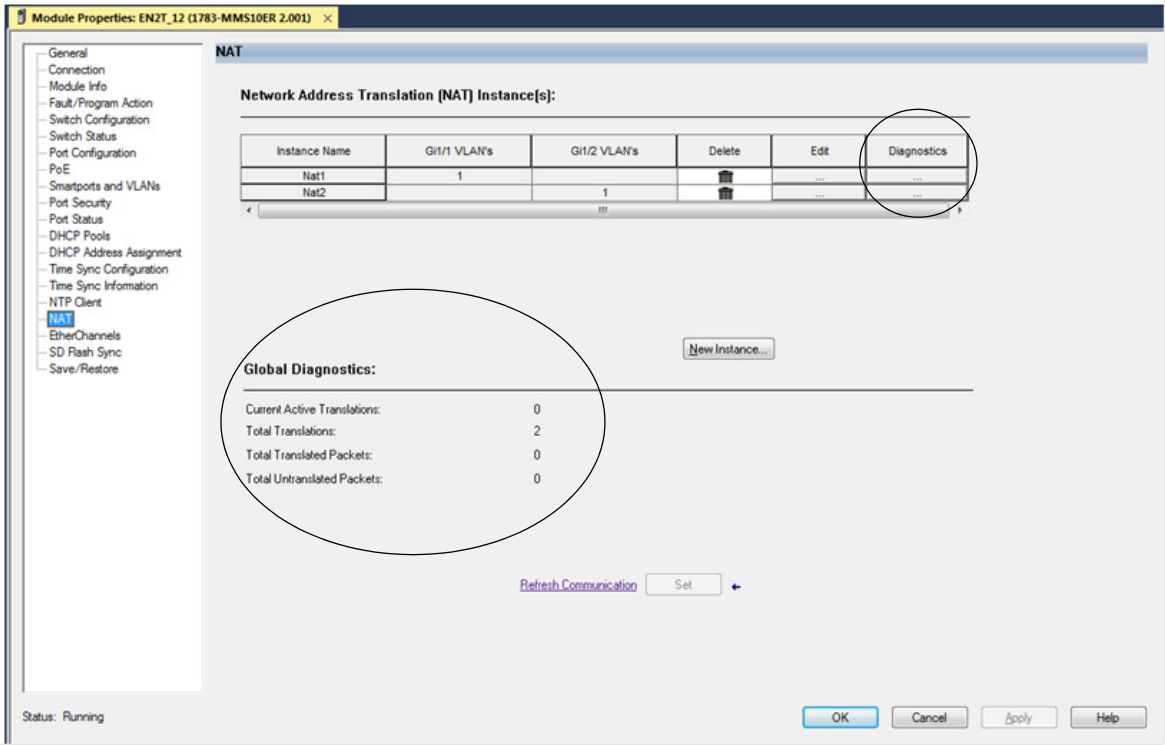


Table 151 - Global Diagnostics

Field	Description
<b>Current Active Translations</b>	The total number of translations that occurred within the last 90 seconds across all NAT instances.
<b>Total Translations</b>	The total number of translations across all NAT instances.
<b>Total Translated Packets</b>	The total number of translated packets across all NAT instances.
<b>Total Untranslated Packets</b>	The total number of packets that have been bypassed across all NAT instances.

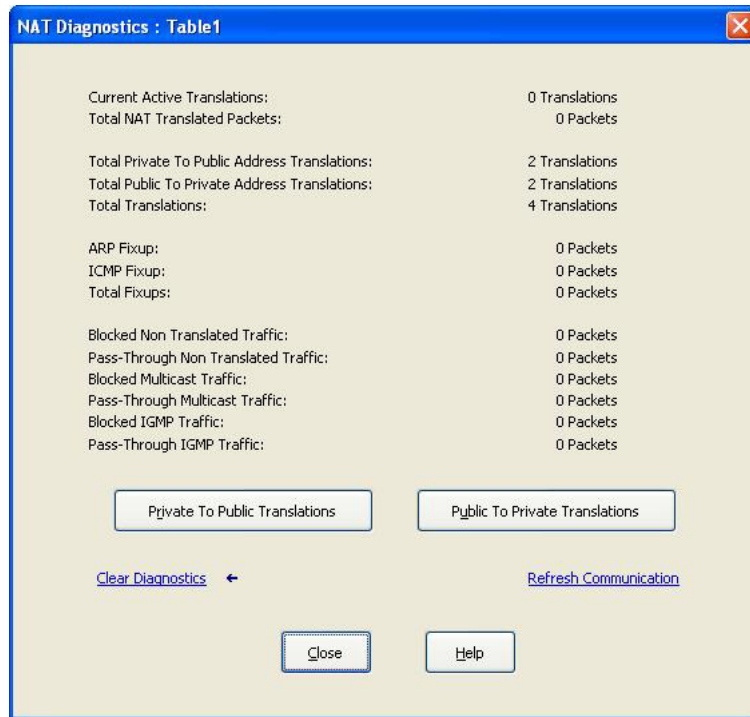


Table 152 - Per Instance Diagnostics

Field	Description
Current Active Translations	The number of translations that have occurred within the last 90 seconds across all NAT instances.
Total NAT Translated Packets	The total number of packets that have been translated for this instance.
Total Private to Public Address Translations	The total number of private-to-public translations for this instance.
Total Public to Private Address Translations	The total number of public-to-private translations for this instance.
ARP Fixup	The number of ARP packets that have been fixed up for this instance.
ICMP Fixup	The number of ICMP packets that have been fixed up for this instance.
Total Fixups	The number of ARP and ICMP packets that have been fixed up for this instance.
Incoming Non Translated Traffic (Pass-Through)	The number of incoming packets with untranslated traffic that NAT passed through for this instance.
Outgoing Non Translated Traffic (Blocked)	The number of outgoing packets with untranslated traffic that NAT blocked for this instance.
Incoming Multicast Traffic (Blocked)	The number of incoming packets with multicast traffic that NAT blocked for this instance.
Outgoing Multicast Traffic (Pass-Through)	The number of outgoing packets of multicast traffic that NAT passed through for this instance.
Incoming IGMP Traffic (Blocked)	The number of incoming packets with IGMP traffic that NAT blocked for this instance.
Outgoing IGMP Traffic (Blocked)	The number of outgoing packets with IGMP traffic that NAT blocked for this instance.
Private to Public Translations	Click to view private-to-public translations that have changed within the last 90 seconds. See <a href="#">Table 153</a> .
Public to Private Translations	Click to view public-to-private translations that have changed within the last 90 seconds. See <a href="#">Table 154</a> .

Table1 : Private To Public Translations

Active Translations in last 90 Seconds:

Private	Public	Subnet	Number Of Packets
128.7.0.3	192.7.0.3	<input type="checkbox"/>	0
128.7.0.1	192.7.0.1	<input type="checkbox"/>	0

Done

Table 153 - Private-to-Public Translations

Field	Description
Private	The existing address for a device on the private subnet.
Public	The unique public address that represents the corresponding device on the private subnet.
Subnet	Indicates whether the translation is part of a subnet entry type.
Number of Packets	The number of packets that contain the translation.

Table1 : Public To Private Translations

Active Translations in last 90 Seconds:

Public	Private	Subnet	Number Of Packets
128.7.0.2	192.7.0.2	<input type="checkbox"/>	0
128.7.1.2	192.7.1.2	<input type="checkbox"/>	0

Done

Table 154 - Public-to-Private Translation Diagnostics

Field	Description
Public	The unique IP address on the public subnet that represents the corresponding IP address on the private subnet.
Private	The IP address on the private subnet that was changed to a unique IP address on the public subnet.
Subnet	Indicates whether the translation is part of a subnet entry type.
Number of Packets	The number of packets that contain the translation.

## MODBUS (Modicon Communication Bus)

In the WebUI, you can view statistics for the MODBUS TCP server and connections from MODBUS TCP clients.

From the Monitoring menu, choose MODBUS:

- To view server details, see the information on the Server Details tab as described in [Table 155](#).
- To view client details, see the information on the Client Details tab as described in [Table 156](#).
- To reset all counters to zero, click Clear Statistics.

Monitoring > General > MODBUS				
				Clear Statistics
Server Details		Client Details		
Status :	Enabled			
<b>CONNECTION STATISTICS</b>				
Port Number :	502	Max Simultaneous Connections :	2	Current Client Connections :
Total Accepted Connections :	0	Accept Connection Errors :	0	Closed Connections :
Close Connection Errors :	0			
<b>SEND STATISTICS</b>				
TCP Messages :	0	TCP Bytes :	0	TCP Errors :
Responses :	0	Exceptions :	0	Send Errors :
<b>RECEIVE STATISTICS</b>				
TCP Messages :	0	TCP Bytes :	0	TCP Errors :
Requests :	0	Receive Errors :	0	

**Table 155 - MODBUS—Server Details Tab**

Field	Description
<b>Server Details</b>	
Status	Shows whether MODBUS is enabled on the switch as configured on the Administration MODBUS page.
<b>CONNECTION STATISTICS</b>	
Port Number	The MODBUS TCP server port number as configured on the Administration MODBUS page. Valid values: 1...65535 Default value: 502
Max Simultaneous Connections	Maximum number of simultaneous connection requests sent to the switch, configured on the Administration MODBUS page. Valid values: 1...5 Default value: 2
Current Client Connections	Number of MODBUS clients currently connected to the MODBUS server.
Total Accepted Connections	Number of MODBUS client connections that the MODBUS server accepted.
Accept Connection Errors	Number of times that the MODBUS server accepted a connection request and an error occurred.
Closed Connections	Number of closed client connections.
Close Connection Errors	Number of times that a connection was closed and an error occurred.
<b>SEND STATISTICS</b>	
TCP Messages	Number of TCP messages sent on the MODBUS TCP server port.
TCP Bytes	Number of TCP bytes sent on the MODBUS TCP server port.
TCP Errors	Number of TCP errors in packets sent on the MODBUS TCP server port.
Responses	Number of responses sent on the MODBUS TCP server port.
Exceptions	Number of MODBUS Exceptions responses on the MODBUS TCP server port.
Send Errors	Number of send errors on the MODBUS TCP server port.
<b>RECEIVE STATISTICS</b>	
TCP Messages	Number of TCP messages received on the MODBUS TCP server port.



Table 155 - MODBUS—Server Details Tab (Continued)

Field	Description
TCP Bytes	Number of TCP bytes received on the MODBUS TCP server port.
TCP Errors	Number of TCP errors in packets received on the MODBUS TCP server port.
Requests	Number of requests received on the MODBUS TCP server port.
Receive Errors	Number of receive errors on the MODBUS TCP server port.
Client Details	Indicates the amount of client connections to the server.

Monitoring > General > MODBUS		Clear Statistics	
Server Details		Client Details	
Client 1			
Connection IP :	10.208.90.250	Connection Port :	60643
SEND STATISTICS			
TCP Messages :	6	TCP Bytes :	54
Responses :	0	Exceptions :	6
RECEIVE STATISTICS			
TCP Messages :	6	TCP Bytes :	74
Requests :	6	Receive Errors :	0

Table 156 - Monitor MODBUS—Client Details Tab

Field	Description
Client Details	
Connection IP	IP address of the MODBUS TCP client.
Connection Port	Port number of MODBUS TCP client.
SEND STATISTICS	
TCP Messages	Number of TCP messages sent to the MODBUS TCP client.
TCP Bytes	Number of TCP bytes sent to the MODBUS TCP client.
TCP Errors	Number of TCP errors in packets sent to the MODBUS TCP client.
Responses	Number of responses sent to the MODBUS TCP client.
Exceptions	Number of MODBUS Exception responses sent to the MODBUS TCP client.
Send Errors	Number of errors when sending messages to the MODBUS TCP client.

Table 156 - Monitor MODBUS—Client Details Tab (Continued)

Field	Description
<b>RECEIVE STATISTICS</b>	
TCP Messages	Number of TCP messages received from the MODBUS TCP client.
TCP Bytes	Number of TCP bytes received from the MODBUS TCP client.
TCP Errors	Number of TCP errors in packets received from the MODBUS TCP client.
Requests	Number of requests received from the MODBUS TCP client.
Receive Errors	Number of errors when receiving messages from the MODBUS TCP client.

## Ports

You can monitor the ports on the switch both in the WebUI and the Logix Designer application.

### Monitor Ports via the WebUI

From the Monitoring menu, choose Ports:

- To view port connection status, the VLAN associated with each port, and the bits per second received and transmitted on each port, see the fields on the Ports page described in [Table 157](#).
- To view more details for a specific port, click the port in the grid to display the Ports page. See [Table 158](#).

Monitoring ▾ > General ▾ > Ports						
Port Name ▾	Description ▾	Status ▾	VLAN/IP ▾	RX [Bits/Sec] ▾	TX [Bits/Sec] ▾	
Vlan1		↓	3680	0	0	
Vlan1101		↓		0	0	
Vlan3680		↑		4000	0	
GigabitEthernet1/1		↓	1	0	0	
GigabitEthernet1/2		↓	1	0	0	
GigabitEthernet1/3		↓	routed	0	0	
GigabitEthernet1/4		↓	routed	0	0	
GigabitEthernet1/5		↑	3680	16000	125000	
GigabitEthernet1/6		↓	3680	0	0	
GigabitEthernet1/7		↓	3680	0	0	
GigabitEthernet1/8		↓	3680	0	0	
GigabitEthernet1/9		↓	3680	0	0	
GigabitEthernet1/10		↓	3680	0	0	
GigabitEthernet2/1		↓	3680	0	0	
GigabitEthernet2/2		↓	3680	0	0	
GigabitEthernet2/3		↓	3680	0	0	
GigabitEthernet2/4		↓	3680	0	0	
GigabitEthernet2/5		↓	3680	0	0	
GigabitEthernet2/6		↓	3680	0	0	

Table 157 - Ports

Field	Description
Port Name	The port type and number.
Description	The description associated with the port.
Status	The connection status of the port.
VLAN/IP	The VLAN ID or the IP address that is associated with the port.
RX [Bits/Sec]	The received bits per second.
TX [Bits/Sec]	The transmitted bits per second.

The screenshot shows a 'Ports' window with three sections: Input Information, Output Information, and General. The Input section shows 0/375/0/0 for the queue, 0 for CRC, 0 for input rate, and never for last input. The Output section shows 0/40 for the queue, 0 for protocol drop, 14 for output rate, and 00:00:00 for last output. The General section shows GigabitEthernet1/9 as the interface name, 34c0.f9e5.1549 as the MAC address, Full-duplex as the duplex mode, 1000Mb/s as the speed, 1500 bytes as the MTU, 10 usec as the delay, 1000000 Kbit/sec as the bandwidth, and 1/255 for both Rx and Tx load.

Input Information	
Input Queue	0/375/0/0
CRC	0
Input Rate[_packets/sec]	0
Last Input	never

Output Information	
Output Queue	0/40
Protocol Drop	0
Output Rate[_packets/sec]	14
Last Output	00:00:00

General	
Interface Name	GigabitEthernet1/9
Mac Address	34c0.f9e5.1549
Duplex	Full-duplex
Speed	1000Mb/s
MTU	1500 bytes
Delay	10 usec
Bandwidth	1000000 Kbit/sec
RxLoad	1/255
TxLoad	1/255

Table 158 - Ports

Field	Description
<b>Input Information</b>	
Input Queue	Information about packets in the input queue (size/max/drops/flushes). <b>EXAMPLE:</b> 30/75/187/0 In this example, 30 packets are in the input queue. The queue depth is 75 packets and there have been 187 drops since the interface counters were last cleared.
CRC	The cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
Input Rate [Packets/sec]	The number of packets received per second for the port.
Last Input	The number of hours, minutes, and seconds since the last packet was successfully received by the port. This is useful for knowing when the port failed.
<b>Output Information</b>	
Output Queue	Information about packets in the output queue (size/max total/threshold/drops). <b>EXAMPLE:</b> 0/1000/64/0 In this example, 0 packets are in the output queue. The queue depth is 1000 packets and there have been 64 drops since the interface counters were last cleared.
Protocol Drop	The number of packets dropped by the port due to a full queue.
Output Rate [Packets/sec]	The number of packets output per second for the port.
Last Output	The number of hours, minutes, and seconds since the last packet was successfully transmitted by the port.
<b>General</b>	
Interface Name	The type and number of the port.
Mac Address	The Ethernet address of the port.
Duplex	The duplex mode of the port.
Speed	The speed of the port.
MTU	The maximum transmission unit set for the port in bytes.
Delay	The delay of the port in microseconds. Higher-level protocols can use delay information to make operating decisions. For example, IGRP can use delay information to differentiate between a satellite link and a land link.
Bandwidth	The bandwidth of the port in kilobits per second.

Table 158 - Ports (Continued)

Field	Description
RxLoad	The amount of traffic being received on the port. RxLoad is a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
TxLoad	The amount of traffic being sent from the port. TxLoad is a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Reliability	The reliability of the port as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.

## Monitor Port Status via the Logix Designer Application

In the Logix Designer application, you can monitor alarms, statuses, thresholds, and bandwidth utilization for each switch port. You can also access port and cable diagnostics.

From the navigation pane, click Port Status.

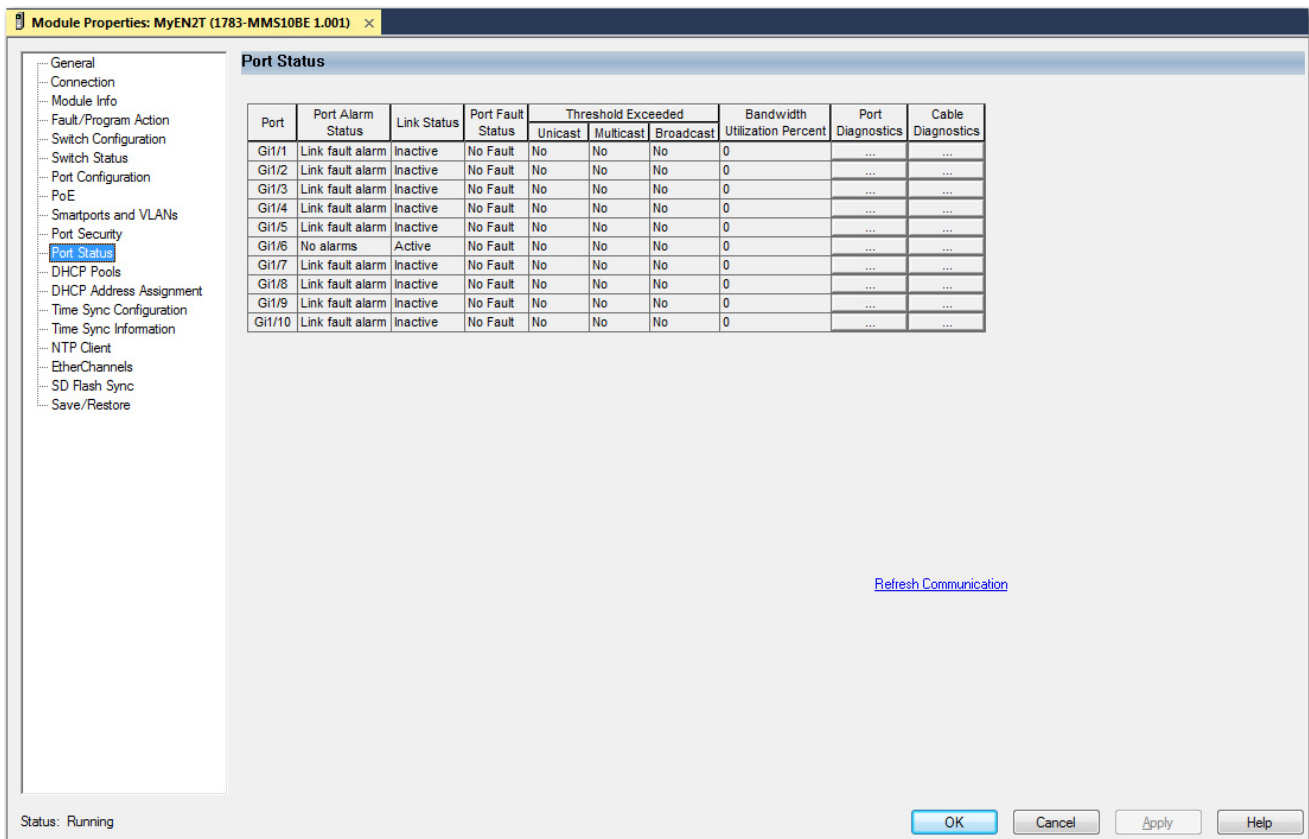


Table 159 - Port Status

Field	Description
Port	The port type and number.
Port Alarm Status	The status of the port alarm: <ul style="list-style-type: none"> <li>Link fault alarm</li> <li>Port not forwarding alarm</li> <li>Port not operating alarm</li> <li>High bit error rate alarm</li> <li>No alarms</li> </ul>
Link Status	The status of the port: <ul style="list-style-type: none"> <li>Active</li> <li>Inactive</li> </ul>

Table 159 - Port Status (Continued)

Field	Description
Port Fault Status	The fault status of the port: <ul style="list-style-type: none"><li>• Error - Disable event</li><li>• SFP error - Disabled</li><li>• CDP native VLAN mismatch</li><li>• MAC address flap</li><li>• Port security violation</li><li>• No fault</li></ul>
Threshold Exceeded	Indicates whether the threshold value has been exceeded for these traffic types: <ul style="list-style-type: none"><li>• Unicast—Displays Yes or No to indicate whether the current unicast traffic has exceeded the threshold value.</li><li>• Multicast—Displays Yes or No to indicate whether the current multicast traffic has exceeded the threshold value.</li><li>• Broadcast—Displays Yes or No to indicate whether the current broadcast traffic has exceeded the threshold value.</li></ul>
Bandwidth Utilization Percent	The percentage of the bandwidth being used. Note whether the percentage of usage is what you expect during the given time of network activity. If usage is higher than expected, an issue can exist.
Port Diagnostics	Click to display information to diagnose a network performance issue for the corresponding port.
Cable Diagnostics	Click to display information to diagnose a cable issue for the corresponding port.

## Parallel Redundancy Protocol (PRP)

You can monitor PRP statistics in both the WebUI and the Logix Designer application.

### Monitor PRP via the WebUI

From the Monitoring menu, choose PRP, and then click the VDAN and Node tabs to view statistics for each type of connected device.

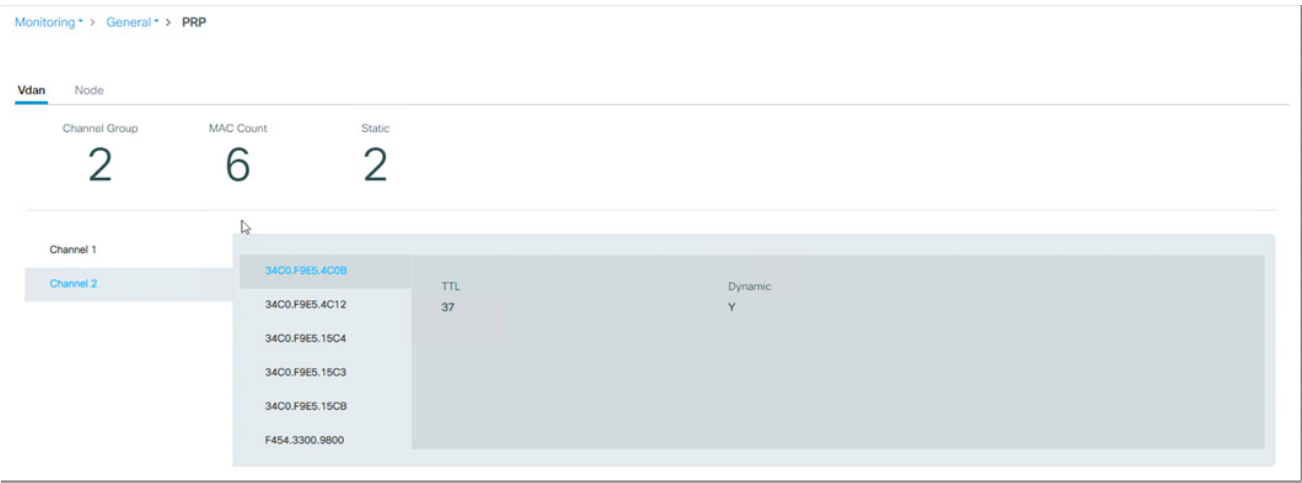


Table 160 - Monitor PRP—VDAN Tab

Field	Description
Channel Group	The channel group selected on the page.
MAC Count	The total number of static and dynamic MAC addresses for the channel group.
Static	The total number of static entries for the channel group.
Channel 1, Channel 2	Click Channel 1 or Channel 2 to display VDAN table entries for the selected channel group.
TTL	The amount of time before the selected dynamic MAC address expires.
Dynamic	Indicates whether the selected MAC address is a dynamic or static entry: Y—The entry is dynamic. N—The entry is static.

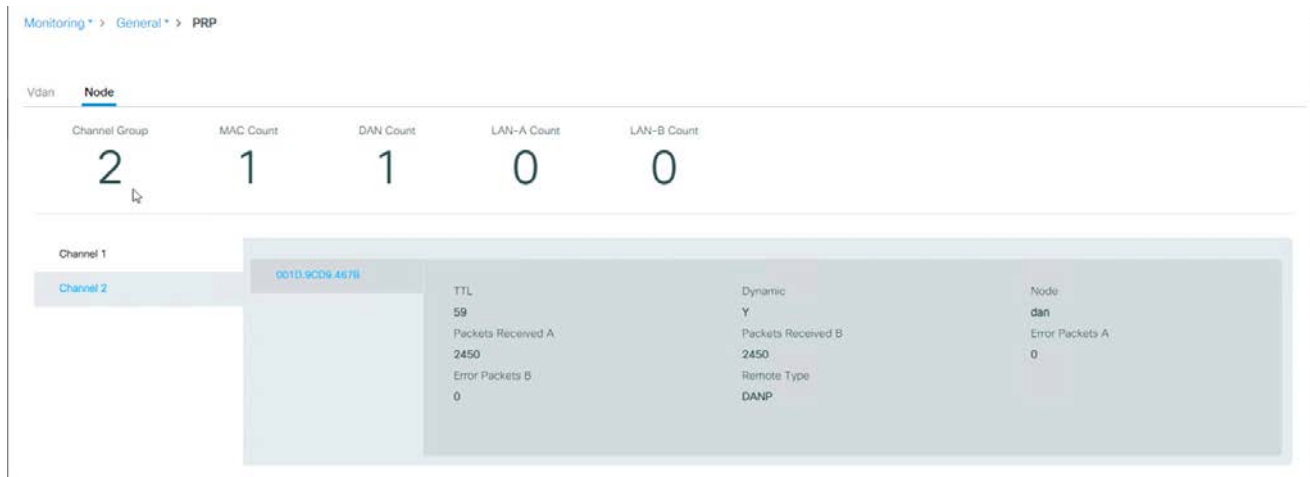


Table 161 - Monitor PRP—Node Tab

Field	Description
Channel Group	The channel group number.
MAC Count	The total number of static and dynamic MAC addresses for the channel group.
DAN Count	The total number of DAN MAC addresses for the channel group.
SAN-A Count	The total number of SANs on LAN A.
SAN-B Count	The total number of SANs on LAN B.
Channel 1, Channel 2	Click Channel 1 or Channel 2 to display Node table entries for the selected channel group.
TTL	The amount of time before the selected MAC address expires.
Dynamic	Indicates whether the selected MAC address is a dynamic or static entry: <ul style="list-style-type: none"> <li>Y—The entry is dynamic.</li> <li>N—The entry is static.</li> </ul>
Node	The type of PRP node: <ul style="list-style-type: none"> <li>DAN—Double attached node</li> <li>SAN-A—Single attached node on LAN A</li> <li>SAN-B—Single attached node on LAN B</li> </ul>
Packets Received A	The number of packets received on LAN A.
Packets Received B	The number of packets received on LAN B.
Error Packets A	The number of packets received on LAN A having the wrong LAN A destination.
Error Packets B	The number of packets received on LAN B having the wrong LAN B destination.

## Monitor PRP via the Logix Designer Application

In the navigation pane, click Parallel Redundancy Protocol (PRP):

- To view the port numbers for each PRP channel group, see the fields as described in [Table 162](#).
- To view statistics for a PRP channel group, click Channel Group 1 or Group 2 in the navigation pane. See [Table 163](#).

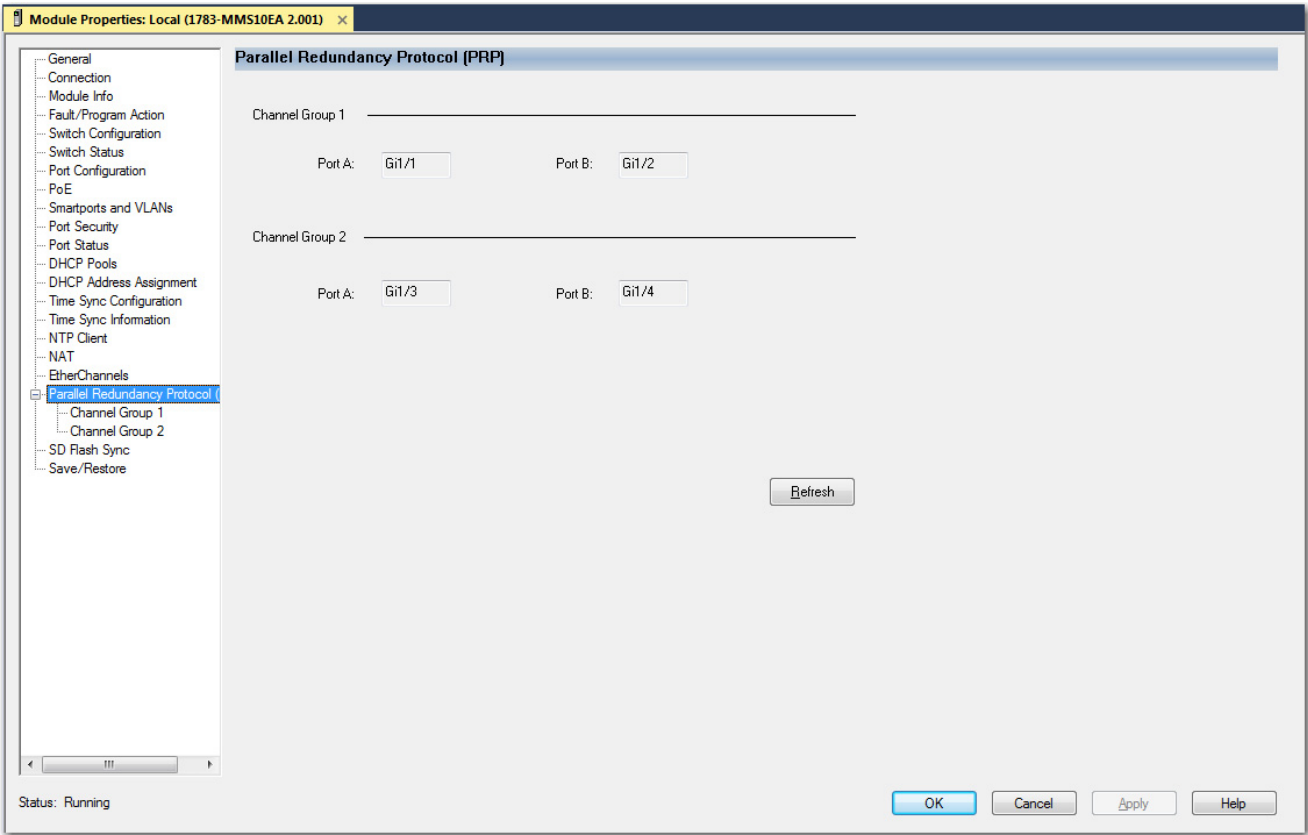


Table 162 - Parallel Redundancy Protocol (PRP)

Field	Description
<b>Channel Group 1</b>	
Port A	The port type and number for channel group 1, port A.
Port B	The port type and number for channel group 1, port B.
<b>Channel Group 2</b>	
Port A	The port type and number for channel group 2, port A.
Port B	The port type and number for channel group 2, port B.

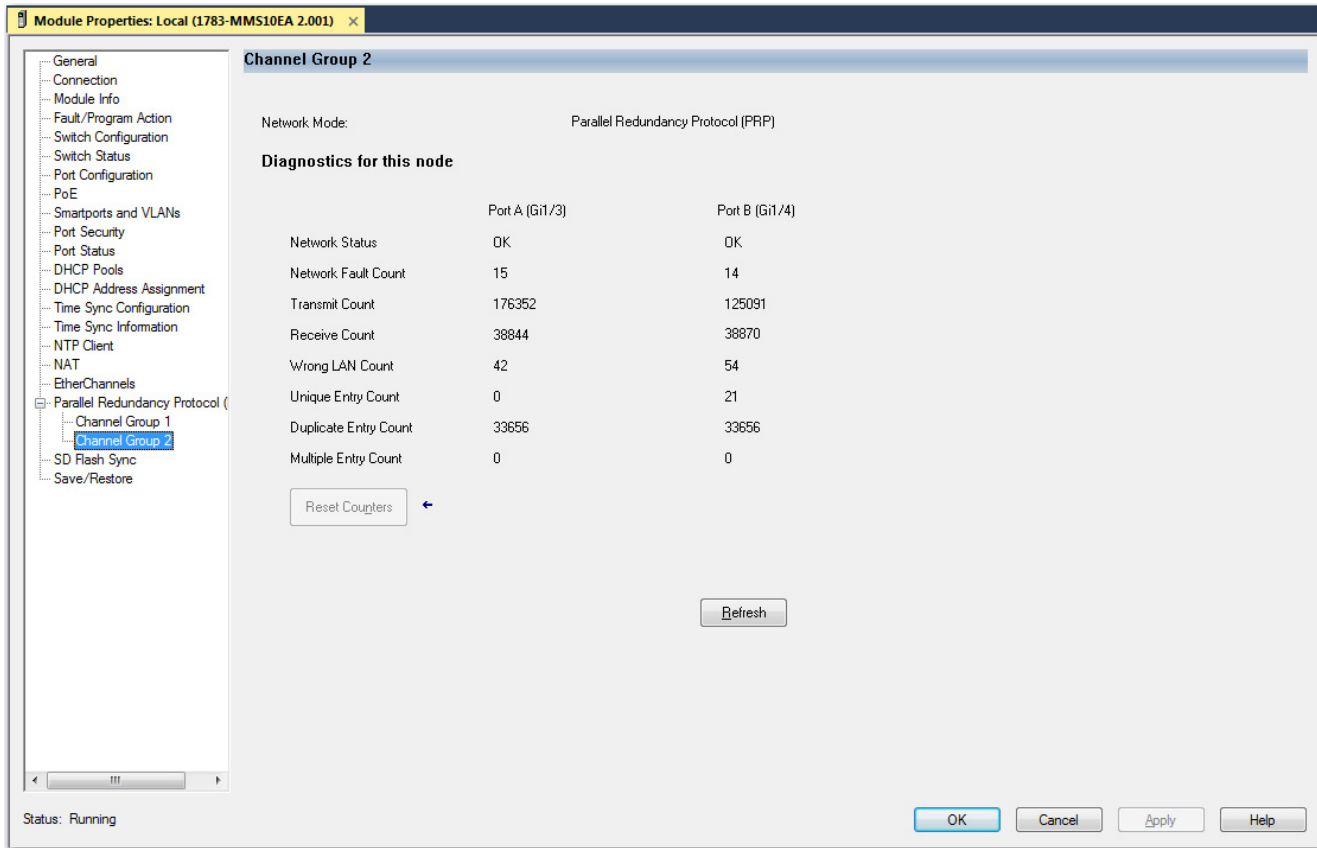


Table 163 - Channel Group

Field	Description
Network Mode	The module is online for a PRP-enabled device.
<b>Diagnostics for this node</b>	
Network Status	The network state of each PRP port on the device: <ul style="list-style-type: none"> <li>OK—Indicates that there is no problem with the PRP network.</li> <li>Fault—Indicates that there is a problem with the PRP network.</li> </ul>
Network Fault Count	The number of times the network status for each PRP port changed from OK to Fault since the last counter reset or power cycle.
Transmit Count	The number of PRP-tagged frames transmitted over each PRP port since the last counter reset or power cycle.
Receive Count	The number of PRP-tagged frames received on each PRP port since the last counter reset or power cycle.
Wrong LAN Count	The number of PRP-tagged frames received on the wrong PRP port since the last counter reset or power cycle.
Unique Entry Count	The number of PRP-tagged frames received on one PRP port, but not received on the other PRP port since the last counter reset or power cycle. Usually indicative of a loss of connection or loss of frames on the other PRP port.
Duplicate Entry Count	The number of PRP-tagged frames received on the PRP port that were already received on the other PRP port since the last counter reset or power cycle. <b>IMPORTANT:</b> This count increments during normal operation and is not an indication of a fault.
Multiple Entry Count	The number of PRP-tagged frames for which multiple duplicates were received on each PRP port since the last counter reset or power cycle. Usually indicative of a misconfigured network, such as a routing loop.
Reset Counters	Sets the PRP port counter values to zero, and then refreshes the values with the current counter values.



# Resiliency Ethernet Protocol (REP)

In the WebUI, you can view the Resilient Ethernet Protocol (REP) topology that is configured on a network segment. You can also view the previously topology of a network segment. When a fault occurs on the segment, the topology dynamically changes.

From the Monitor menu, choose REP:

- To display the current REP topology configured on that segment, from the Segment ID pull-down menu on the Global tab, choose a network segment ID. See [Table 164](#).
- To view the previous topology of a network segment, from the Segment ID pull-down menu on the Archived Topology tab, choose a network segment ID. See [Table 165](#).

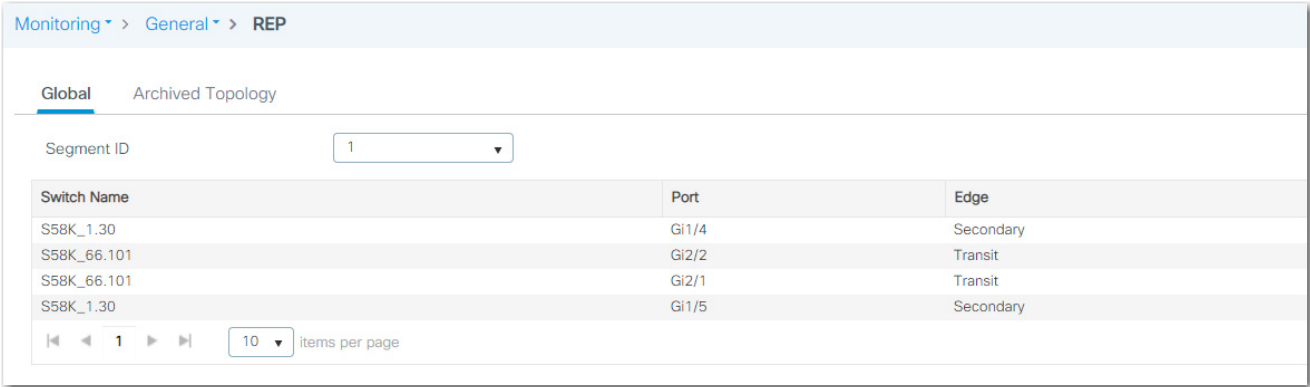


Table 164 - REP—Global Tab

Field	Description
Switch Name	The name of the switch.
Port	The port type and number.
Edge	The REP port type. For a description of REP port types, see <a href="#">Table 73 on page 128</a> .
Role	The role of the REP port: <ul style="list-style-type: none"><li>• Open</li><li>• Alternate</li><li>• Failed</li></ul>

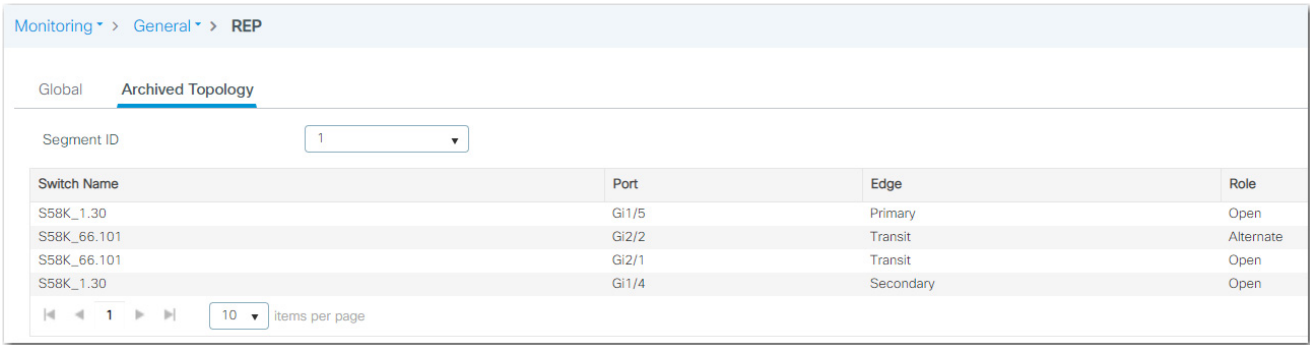


Table 165 - REP—Archived Topology Tab

Field	Description
Switch Name	The archived name of the switch.
Port	The archived port type and number.
Edge	The archived REP port type. For a description of REP port types, see <a href="#">Table 73 on page 128</a> .
Role	The archived role of the REP port: <ul style="list-style-type: none"><li>• Open</li><li>• Alternate</li><li>• Failed</li></ul>

## System

In the WebUI, you can monitor hardware details, memory utilization, and CPU utilization.

From the Monitoring menu, choose System.

## Inventory

Monitoring > General > System

Inventory Memory Utilization CPU Utilization

**INVENTORY DETAILS**

Name	Product Description	Serial Number	PID	VID
Chassis	Stratix 5800 Expandable Advanced Chassis	FOC2218Y21T	1783-MMS10EA	V01
Supervisor	Stratix 5800 Expandable System: 2 Port SFP + 8 Port GE PoE+ Adv (4GB)	FOC2218Y21T	1783-MMS10EA	V01
Expansion Module	14 Port GE Copper + 2 Port SFP Fiber Mixed Exp Module Basic	FOC2217Y2HE	1783-MMX14T2S	V00

50 items per page 1 - 3 of 3 items

**SWITCH DETAILS**

Switch Number	Role	MAC Address	Priority	H/W Version	Current State	Product Description	Serial Number	CIP Serial Number
1	Active	34c0.f9e5.1540	1	02	Ready	Stratix 5800 Expandable Advanced Chassis	FOC2218Y21T	0x600f9330

50 items per page 1 - 1 of 1 items

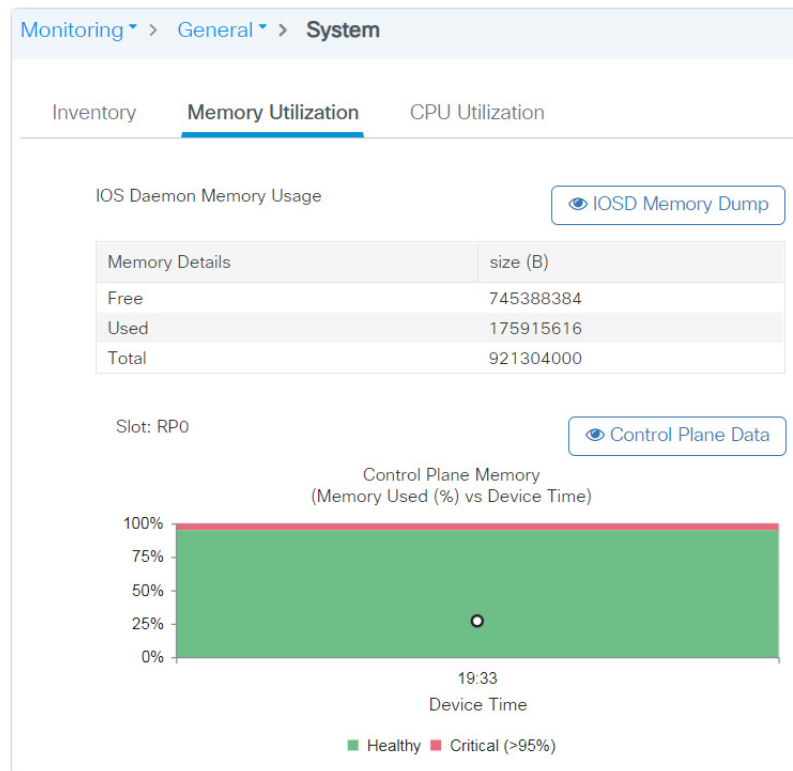
**Table 166 - System—Inventory Tab**

Field	Description
<b>Inventory Details</b>	
Name	The type of hardware product.
Product Description	The description of the hardware product.
Serial Number	The serial number of the hardware product.
PID	The catalog number of the hardware product.
VID	The version of the hardware product.
<b>Switch Details</b>	
Switch Number	The number of the switch in a stacked environment. The Stratix 5800 switch platform does not currently support stacking, so the switch number is always 1.
Role	The current role of the switch in a stacked environment: <ul style="list-style-type: none"> <li>Active</li> <li>Member</li> </ul>
MAC Address	The MAC address of the switch.
Priority	The priority of the switch from 1...15. The default priority value is 1.
H/W Version	The hardware version number associated with the switch. Different device models can have the same hardware version, provided they support the same system-level features.
Current State	The current state of the switch in a stacked environment: <ul style="list-style-type: none"> <li>Ready—The switch is fully operational.</li> <li>Progressing—The stack master is communicating with the new switch joining the stack.</li> <li>Provisioned—When a switch that previously joined a stack is removed, the port numbers remain in the running configuration, and the missing device has a state of a Provisioned. The Provisioned state is caused by a switch that is no longer connected to the stack.</li> <li>v-mismatch—When a new switch that is in Installed mode tries to join the stack that is in Bundled Boot mode, the new switch has a state of v-mismatch. Auto-upgrade is supported in installed mode only.</li> <li>Lic-mismatch—When there is a license mismatch.</li> </ul> The Stratix 5800 switch platform does not currently support stacking, so the current state is always Ready.
Product Description	The switch model description.
Serial Number	The serial number of the switch.
CIP Serial Number	The CIP serial number of the switch.

## Memory Utilization

The Memory Utilization tab shows the used, free, and total memory on the IOS daemon:

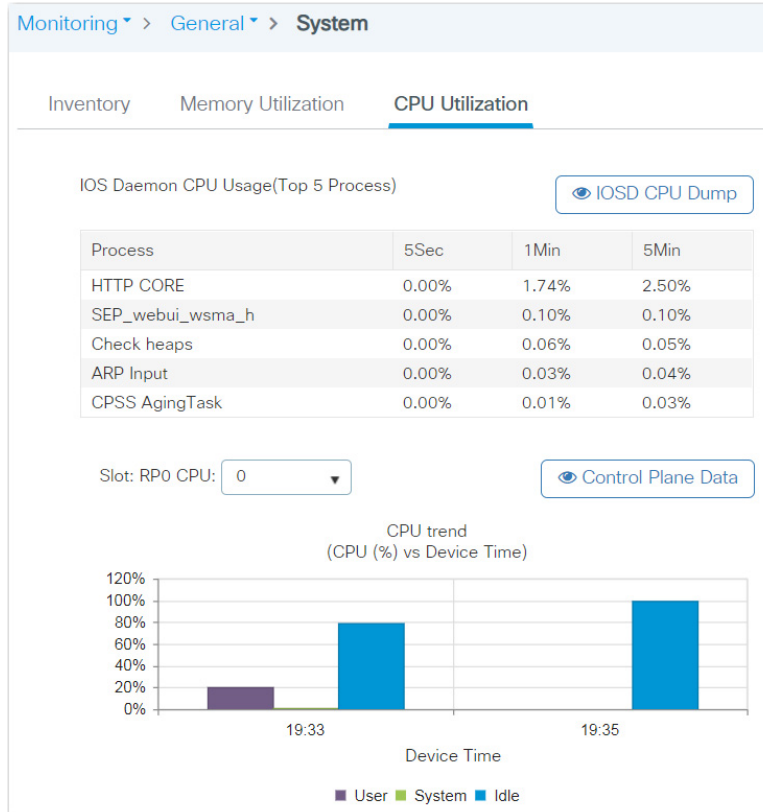
- To export memory data to a spreadsheet, click IOSD Memory Dump and then click Export to Excel.
- To export control plane memory data as a PDF, click Control Plane Data and then click Export as PDF.



## CPU Utilization

The CPU Utilization tab shows the CPU utilization of the top five processes over the last 5 seconds, 1 minute, and 5 minutes.

- To export the CPU utilization data to a spreadsheet, click IOSD CPU Dump and then click Export to Excel.
- To export control plane CPU data as a PDF, click Control Plane Data and then click Export as PDF.

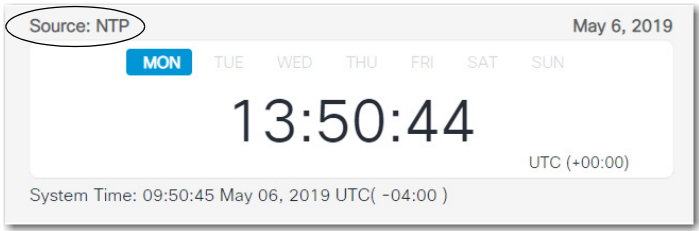


Time

In the WebUI, you can monitor time details for the time source that is configured on the switch.

From the Monitor menu, choose Time.

The clock at the top of the page shows the local time and the time source. The time source indicates where the switch is receiving its time, such as from an NTP server, PTP, or the local computer.



PTP Details

PTP Details shows the properties of the local PTP clock and the clock identity.

Monitoring > General > Time

Source: NTPJul 2, 2019

MONTUEWEDTHUFRISSATSUN

19:24:54

UTC (+00:00)

System Time: 15:24:53 Jul 02, 2019 UTC( -04:00 )

PTP

PTP Details

PTP Clock Settings

PTP Parent Property

Mode:

Priority1:

Priority2:

Clock ID:

Offset From Master(ns):

PTP Enabled Ports:

Boundary

128

128

0x34:C0:F9:FF:FE:E5:15:40

Gi1/1, Gi1/2, Gi1/3, Gi1/4, Gi1/5, Gi1/6, Gi1/7, Gi1/8, Gi1/9, Gi1/10, Gi2/1, Gi2/2, Gi2/3, Gi2/4, Gi2/5, Gi2/6, Gi2/7, Gi2/8, Gi2/9, Gi2/10, Gi2/11, Gi2/12, Gi2/13, Gi2/14, Gi2/15, Gi2/16

Table 167 - Monitor Time—PTP Details

Field	Description
Mode	The PTP mode configured for the switch: <ul style="list-style-type: none"><li>• Forward</li><li>• Boundary</li><li>• End to End Transparent</li><li>• GMC-BC (NTP-PTP Clock)</li></ul>
Priority 1	(Appears only for Boundary and NTP-PTP mode). Priority 1 preference value of the PTP clock. The priority1 clock is considered first during clock selection.
Priority 2	(Appears only for Boundary and NTP-PTP mode). Priority 2 preference value of the PTP clock. The priority2 clock is considered after all other clock sources during clock selection.

Table 167 - Monitor Time—PTP Details (Continued)

Field	Description
Clock ID	(Appears only for Boundary and NTP-PTP mode). The unique clock identity.
Offset From Master (ns)	(Appears only for Boundary and NTP-PTP mode). The time offset between the slave and master clocks.
PTP Enabled Ports	(Appears only for Boundary and End to End Transparent modes).The list of ports that are assigned to the PTP clock.

## PTP Clock Settings

PTP Clock Settings shows the settings of the local PTP clock when PTP is in Boundary and End to End Transparent mode.

The screenshot shows the 'Monitoring > General > Time' navigation path. A digital clock display shows the time as 21:17:41 on Monday, July 29, 2019, with a UTC offset of +00:00. Below this, the 'PTP' section is active, showing 'PTP Clock Settings'. The settings are as follows:

- PTP Device Type:** Boundary Clock
- Number of PTP Ports:** 26
- Clock Quality:**
  - Class:** 13
  - Accuracy:** Within 1s
  - Offset (log variance):**
  - Steps Removed:** 0
  - Local Clock Time:** 20:19:39 UTC Jul 29 2019

Table 168 - Monitor Time—PTP Clock Settings

Field	Description
PTP Device Type	The PTP clock type as determined by the PTP mode configured on the switch. <ul style="list-style-type: none"> <li>• Forward Clock</li> <li>• Boundary Clock</li> <li>• End to End Transparent Clock</li> <li>• GMC-BC (NTP-PTP Clock)</li> </ul>
Number of PTP Ports	The number of ports that are assigned to the PTP clock.
Class	(Appears only for Boundary and NTP-PTP clock type). The time and frequency traceability of the Grandmaster clock.
Accuracy	(Appears only for Boundary and NTP-PTP clock type. Applies only when the Best Master Clock algorithm is in use.) This is an enumerated list of ranges of accuracy to UTC.
Offset (log variance)	(Appears only for Boundary and NTP-PTP clock type). The offset between the Grandmaster clock and the parent clock.
Steps Removed	The number of hops from the local clock to the Grandmaster clock.
Local Clock Time	The time of the local PTP clock.

## PTP Parent Property

PTP Parent Property shows the properties of the PTP parent clock when PTP is in Boundary and NTP-PTP mode.

Monitoring > General > Time

Source: Jul 9, 2019

MON TUE WED THU FRI SAT SUN

09:02:43

EST (-04:00)

System Time: 09:02:42 Jul 09, 2019 UTC( -04:00 )

PTP

PTP Details

PTP Clock Settings

PTP Parent Property

Parent Clock:

Parent Clock Identity: 0xF4:54:33:FF:FE:DC:94:0

Parent Port Number: 15

Grandmaster Clock:

Grandmaster Clock Identity: 0xF4:54:33:FF:FE:DC:94:0

Table 169 - Monitor Time—PTP Parent Property

Field	Description
Parent Clock	The clock to which the member-slave clocks synchronize.
Parent Clock Identity	The unique parent clock identity.
Parent Port Number	The clock port ID of the parent port.
Grandmaster Clock	The root of the master-slave clock hierarchy.
Grandmaster Clock Identity	The unique Grandmaster clock identity.

## Troubleshoot the Switch

Topic	Page
Configure and View System Logs	253
Download Core Files	256
Download a Debug Bundle	257
Troubleshoot with Ping and Trace Route	258
Troubleshoot the Installation	260
Troubleshoot IP Addresses	261
Troubleshoot the WebUI	262
Troubleshoot Switch Performance	262

### Configure and View System Logs

In the WebUI for the switch, the system log (syslog) displays events that occur on the switch and its ports. The events are based on alarm settings.

### Message Severity Levels

[Table 170](#) lists the syslog message levels from the most severe level to the least severe level.

**Table 170 - Syslog Message Severity Levels**


Severity Level	Numerical Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warnings conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG



From the Troubleshooting menu, click Logs.

The image shows two screenshots of a network switch's web interface. The top screenshot shows the 'Troubleshooting' menu with four options: 'Logs' (circled), 'Core Dump and System Report', 'Debug Bundle', and 'Ping and Trace Route'. The 'Logs' option is described as 'Manage Syslog, Webserver Log, License Log'. The bottom screenshot shows the 'Syslog' page, which has tabs for 'Syslog', 'Web Server Logs', and 'License logs'. The 'Syslog' tab is active. It features a 'Number of latest Syslog entries to display\*' input field set to '100', with 'View' and 'Clear' buttons. A 'Manage Syslog Servers' button is also present. Below these controls is a scrollable list of log entries, each starting with a timestamp and a log message, such as 'Jul 29 19:22:19.151 UTC: %WEBSERVER-5-LOGIN\_PASSED: R0/0: nginx: Login Successful from host 10.88.141.231 by user 'admin' using crypto cipher 'ECDHE-RSA-AES128-GCM-SHA256''.

From the Troubleshooting: Syslog page, you can manage Syslog servers and entries, and view Web server and License logs:

- To manage Syslog servers, click Manage Syslog Servers, complete the fields in [Table 171](#), and then click Apply to Device.
- To change the number of log entries on the page, enter the number of entries to display, and then click View. For example, if you type 100, the most recent 100 lines in the syslog are displayed.
- To display Web server logs, click the Web Server Logs tab. To display License Logs, click the License logs tab. To download entire Web server or License logs, click Download Full Log on the respective tabs.
- To delete all of the log entries, click Clear.
- To download the log entries to your local computer, click  .

**Manage Syslog Configuration**

**Log Level Settings**

Syslog: informational

Message Console: Unconfigured

Message Buffer: debugging

**IP Configuration**

IPv4/IPv6: ☒


IPv4 / IPv6 Server Address\*: X.X.X.X / X:X:X:X::X

VRF Name: None

IP Address	VRF Name	Remove
No items to display		

Cancel Apply to Device

Table 171 - Manage Syslog Configuration Fields

Field	Description
<b>Log Level Settings</b>	
Syslog	Choose the kind of messages, by severity level, to send to the Syslog server. For information about message severity levels, see <a href="#">Table 170 on page 253</a> . Default value: informational
Message Console	Choose the severity level for the messages you want sent to the device console.
Message Buffer	Choose the severity level for the messages you want sent to the internal buffer on the device.
<b>IP Configuration</b>	
IPv4/IPv6	Check to specify the IPv4 or IPv6 address of the server on which to store message logs.
IPv4/IPv6 Server Address	Enter the IPv4 or IPv6 address of the server on which to store message logs.
VRF Name	Choose the VPN routing/forwarding (VRF) table.
	Click to add the IP address and VFR (if applicable) to the grid. You can add multiple servers. To delete a server, click X in the Remove column.

## Download Core Files

When the switch encounters a significant error, it can take a snapshot of the data currently stored in its memory at the time of the error. Technical Support can refer to this snapshot of data, also known as a core dump, at a later time for troubleshooting. In the WebUI, you can download a core dump and share the data with technical support for intensive troubleshooting.

From the Troubleshooting menu, click Core Dump and System Report.



The information from the switch appears on the Troubleshooting: Core Dump and System Report page.

Review the date and time stamp to identify the files to download, and then click Download to save to your computer. The core files are downloaded to the location configured for your browser.



## Download a Debug Bundle

A debug bundle is the output of CLI commands stored in a zip file that you can download for analysis and troubleshooting. The WebUI enables you to create a debug bundle and download it to your local computer.

From the Troubleshooting menu, click Debug Bundle.



The Troubleshooting: Debug Bundle page appears.

### Troubleshooting : Debug Bundle

[← Back to TroubleShooting Menu](#)

*Name of the debug bundle*

?

This supports user to create a compressed package with required info like CLI outputs, logs etc for reporting and debugging the issues

*Enter the CLIs of which output needs to be packaged. Maximum 5 CLIs are allowed.*

View
Add

✓ sh run ×

☐ Web Server log
   
☐ Core File

Create Debug Bundle

From the Troubleshooting: Debug Bundle page, you can create and download a debug bundle:

- To create a debug bundle, complete the fields in [Table 172](#), and then click Create Debug Bundle. A window opens to display the status.
- To download the debug bundle once it is created, click Download Debug Bundle.

**Table 172 - Troubleshooting: Debug Bundle**

Field	Description
Name of the debug bundle	Enter a name to identify the debug bundle. The name can have a maximum of 25 characters and can include lowercase or uppercase letters, numbers 0...9, and the underscore (_).
Enter the CLIs of which ouptut needs to be packaged	Enter a maximum of 5 CLI commands to identify the content to capture in the debug bundle. To verify the output of the CLI commands, click View. To add a CLI command to the debug bundle, click Add. To remove a CLI command from the debug bundle, click the X to the right of the command.
Web Server log	To include the web server log in the debug file, check Web Server log.
Core File	To include core files from the internal memory of the switch in the debug bundle, check Core File. A window opens with a list of core files on the device. You can select a maximum of two core files from this list.

**Troubleshoot with Ping and Trace Route**

To troubleshoot connectivity problems, communication delays and packet loss, you can use the ping and trace route feature in the WebUI of the switch.

From the Troubleshooting menu, click Ping and Trace Route.



The Troubleshooting: Ping and Traceroute page appears.

**Troubleshooting : Ping and Traceroute**

← Back to TroubleShooting Menu

Destination\* 8.8.8.8

Source GigabitEthernet1/2

Ping Traceroute

Source (Device) Destination

GigabitEthernet1/2 8.8.8.8

Click on ping or traceroute to start

## Ping Destinations

Sending ping packets to a destination can help you verify connectivity.

1. In the Destination field, enter a destination or choose a predefined destination from the pull-down menu.  
Ping packets are sent to the specified destination.
2. (Optional) In the Source field, enter the source IP address on the switch to initiate the ping.  
The ICMP echo response is sent to the specified source.
3. Click Ping.

## Discover Route Information

Discovering route information can help you identify the path of a Layer 3 transmission.

1. In the Destination field, enter a destination interface or choose a predefined destination from the pull-down menu.
2. In the Source field, enter the source IP address for which to run Traceroute.
3. Click Traceroute.  
Traceroute discovers the route and the number of Layer 3 hops that packets take when traveling to their destination.

## Troubleshoot the Installation

The status indicators on the front panel provide troubleshooting information about the switch. They show port connectivity problems and overall switch performance. You can also get statistics from the browser interface, the command-line interface (CLI), or a Simple Network Management Protocol (SNMP) workstation.

### Bad or Damaged Cable

Always make sure that the cable does not have damage. Even if a cable can connect at the physical layer, subtle damage to the wiring or connectors can corrupt packets.

This situation is likely when the port has many packet errors or the port constantly loses and regains the link. To troubleshoot, try the following:

- Swap the copper or fiber-optic cable with a known, undamaged cable.
- Look for broken, bent, or missing pins on cable connectors.
- Rule out any bad patch panel connections or media convertors between the source and destination.  
If possible, bypass the patch panel, or eliminate faulty media convertors (fiber-optic-to-copper).
- Try the cable in another port or interface to determine if the problem follows the cable.

### Ethernet and Fiber Cables

Make sure that you have the correct cable type for the connection:

- For 1000 Mbps connections, use Category 5e or Category 6 UTP or STP cable.
- For fiber-optic connectors, verify that you have the correct cable for the distance and the port type.
- Make sure that the connected device ports both match and use the same type of encoding, optical frequency, and fiber type.

### Port Status

Verify that both sides of the port connection have a network connection. A port status indicator does not indicate that the cable is fully functional. The cable can encounter physical stress that causes it to function at a marginal level. If the port status indicator for the port is off, do the following:

- Connect the cable from the switch to a known good device.
- Make sure that both ends of the cable are connected to the correct ports.
- Verify that both devices have power.
- Verify that you are using the correct cable type.
- Rule out loose connections. Sometimes a cable appears to be seated, but is not. Disconnect the cable, and then reconnect it.
- Verify the port settings, as described on [page 261](#).

## SFP Module Issues

Use SFP modules only from Rockwell Automation. Each SFP module has an internal serial EEPROM that is encoded with security information. This encoding identifies and validates that the module meets the requirements for the switch.

If you encounter SFP module issues, try the following:

- Verify that the SFP module is valid and functional. Exchange a suspect module with a known good module on this platform. For supported modules, see the Ethernet Device Specifications Technical Data, publication [1783-TD001](#).
- Make sure that all fiber connections are properly cleaned and securely connected.
- Be sure that the fiber cable is compatible with the SFP module. For example, do not use single-mode cable with a multi-mode SFP module.
- Be sure to use an SFP module with same speed on both ends.
- Be sure that the fiber cable is installed correctly on the SFP module (RX connected to TX, and TX connected to RX).

## Port Settings

A disabled port can cause a port connectivity failure:

- Verify that operational status of the port on the Configuration > Ethernet Ports page, as described on [page 76](#). Users with read-only access can verify port status on the Monitoring > Ports page, as described on [page 239](#).
- Verify the operational status of the VLAN assigned to the port on the Configuration > VLAN page, as described on [page 152](#).

If a port or interface is manually shut down on one side of the connection, you must re-enable the port on the Configuration > Ethernet Ports page, as described on [page 76](#).

## Troubleshoot IP Addresses

The following table includes basic troubleshooting for issues that are related to the switch IP address.

Issue	Resolution
The switch does not receive an IP address from the DHCP server	If the switch does not receive an IP address from an upstream device operating as a DHCP server, make sure that the device is operating as a DHCP server and that the switch is configured for DHCP IP address assignment. Repeat Express Setup.
The switch has the wrong IP address	If the switch is installed in your network, but you cannot access the switch because it has the wrong IP address, run Express Setup and configure the correct IP address. If the device is set for DHCP and receiving the wrong address, verify the configuration settings on your DHCP server.



## Troubleshoot the WebUI

The following table includes basic troubleshooting for issues that are related to the WebUI.

Issue	Resolution
WebUI does not appear	<p>If you cannot display the WebUI from your computer, make sure that you entered the correct switch IP address in the browser. If you entered the correct switch IP address in the browser, make sure that the switch and your computer are in the same network:</p> <ul style="list-style-type: none"> <li>For example, if your switch IP address is 172.20.20.85 and your computer address is 172.20.20.84, both devices are in the same network.</li> <li>For example, if your switch IP address is 172.20.20.85 and your computer IP address is 10.0.0.2, the devices are in different networks and cannot directly communicate without a router. You must either change the switch IP address or change the computer IP address.</li> </ul>
WebUI does not operate properly	Open the WebUI in a new browser window by using a private browsing mode.

## Troubleshoot Switch Performance

The following table includes basic troubleshooting for issues that are related to switch performance.

Issue	Resolution
Speed, duplex, and autonegotiation	<p>Port statistics that show a large amount of alignment errors, frame check sequence (FCS), or late-collisions errors can indicate a speed or duplex mismatch. Common speed and duplex issues occur when duplex settings are mismatched between two switches, between a switch and a router, or between the switch and a computer. These issues can occur from manually setting the speed and duplex or from autonegotiation issues between the two devices. A mismatch occurs under these circumstances:</p> <ul style="list-style-type: none"> <li>A manually set speed or duplex parameter differs from the manually set speed or duplex parameter on the connected port.</li> <li>A port is set to autonegotiate, and the connected port is set to full-duplex with no autonegotiation.</li> </ul> <p>To maximize switch performance and be sure of a link, follow one of these guidelines when changing the settings for duplex and speed:</p> <ul style="list-style-type: none"> <li>Let both ports autonegotiate both speed and duplex.</li> <li>Manually set the same speed and duplex parameters for the ports on both ends of the connection to the same values.</li> <li>If a remote device does not autonegotiate, configure the duplex settings on the two ports to the same values.</li> </ul> <p>The speed parameter can adjust itself even if the connected port does not autonegotiate.</p>
Autonegotiation and network interface cards (NICs)	<p>Issues sometimes occur between the switch and third-party network interface cards (NICs). By default, the switch ports and interfaces are set to autonegotiate. It is common for devices like laptops or other devices to be set to autonegotiate as well, yet sometimes autonegotiation issues occur. To troubleshoot autonegotiation issues, try manually setting both sides of the connection. If the issues persist, try upgrading the NIC driver to the latest firmware or software.</p>
Cable distance	If the port statistics show excessive FCS, late-collision, or alignment errors, verify that the cable distance from the switch to the connected device meets the recommended guidelines.

## Status Indicators

Topic	Page
Stratix 5800 Status Indicators	263
Power Status Indicators	264
Power over Ethernet Status Indicator	264
Setup Status Indicator	264
EIP Status Indicators	265
Alarm Status Indicators	265
Port Status Indicators	266

### Stratix 5800 Status Indicators

Stratix® 5800 switches and expansion modules have status indicators on the front panel. The color and behavior of each status indicator helps you to monitor the status of the switch, network, power, alarms, and individual ports.

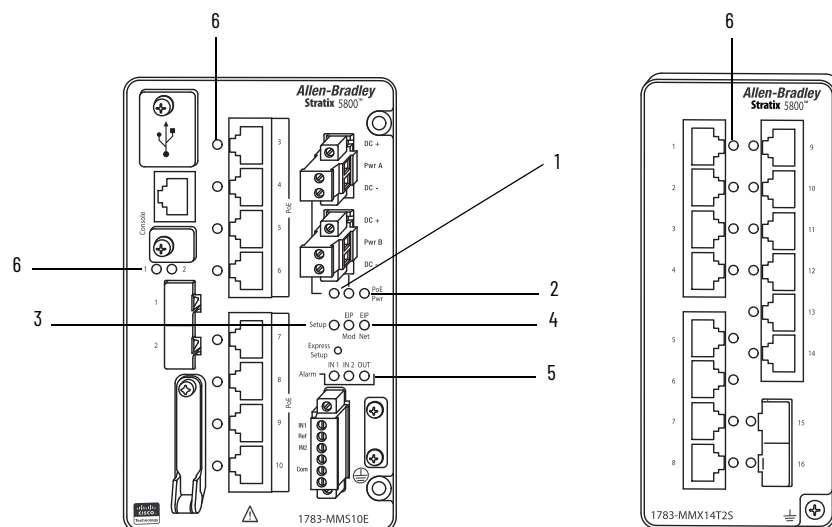


Table 173 -

Item	Status Indicators
1	Power (Pwr A and Pwr B indicated by lines to corresponding power connector)
2	Power over Ethernet (PoE Pwr) <sup>(1)</sup>
3	Setup
4	EIP (EIP Mod, EIP Net)
5	Alarms (Alarm IN1, Alarm IN2, Alarm OUT)
6	Ports

(1) The PoE Pwr status indicator appears only on switch models that support Power over Ethernet (PoE).

## Power Status Indicators

The switch can operate with one or two DC power sources. Each DC input has an associated status indicator that shows the status of the corresponding DC input (Pwr A, Pwr B). If power is present on the circuit, the status indicator is green. If power is not present, the status indicator color depends on the alarm configuration. If alarms are configured, the status indicator is red when power is not present; otherwise, the status indicator is off.

If the switch has dual power sources, the switch draws power from the power source with the higher voltage. If one of the DC sources fails, the alternate DC source powers the switch, and the corresponding power status indicator is green. The power status for the failed DC source is either off or red, depending on the alarm configuration.

If the power input drops below the low valid level, the power status indicators show that power is not present on the switch. If the voltage at the switch input exceeds the valid level, the power status indicators only show that power is present.

**Table 174 - Power Status Indicators**

Indicator	Status	Description
Pwr A Pwr B	Off	Power is not present on the circuit.
	Solid green	Power is present on the associated circuit.
	Solid red	Power is not present on the associated circuit, and the power supply alarm is configured.

## Power over Ethernet Status Indicator

The Power over Ethernet status indicator (PoE Pwr) is available only on switch models that support PoE.

**Table 175 - Power over Ethernet Status Indicator**

Indicator	Status	Description
PoE Pwr	Off	The switch is not providing PoE power to any connected devices.
	Solid green	The switch is providing PoE power to one or more connected devices.
	Solid amber	PoE for the port is disabled. (PoE is enabled by default.)
	Flashing amber	PoE is off due to a fault. <b>IMPORTANT:</b> Non-compliant cabling or powered devices can cause a PoE port fault. Use only standard-compliant cabling to connect compliant PoE devices. You must remove any cable or device that causes a PoE fault.
	Alternating green and amber	PoE is denied because providing power to a connected device exceeds the switch power capacity.

## Setup Status Indicator

The Setup status indicator displays the Express Setup state during the initial configuration. For more details about the Setup status indicator and conditions during Express Setup, see [Chapter 2, Express Setup on page 23](#).

**Table 176 - Setup Status Indicator**

Indicator	Status	Description
Setup	Off	The switch is configured as a managed switch or is operating normally.
	Solid green	The switch has successfully connected with a computer after the Express Setup button is pressed.
	Flashing green	<ul style="list-style-type: none"> <li>The switch has completed its power-on sequence. If you do not press the Express Setup button within 5 minutes after the power-on sequence is complete, the Setup status indicator turns off.</li> <li>The Express Setup button is pressed for a duration of 1...5 seconds to enable Express Setup in Short Press mode.</li> </ul>
	Solid red	The switch failed to start Express Setup because of the following: <ul style="list-style-type: none"> <li>There is no available switch port to which to connect the management station. Disconnect a device from a switch port, and then press the Express Setup button.</li> <li>A configuration is already present on the switch. In this scenario, the status indicator is red for 10 seconds.</li> <li>A condition caused Express Setup to time out.</li> </ul>
	Flashing red	The Express Setup button is pressed for a duration of 6...10 seconds to enable Express Setup in Medium Press mode.
	Flashing green and red	The Express Setup button is pressed for a duration of 16...20 seconds to enable Express Setup in Long Press mode.

## EIP Status Indicators

The EIP status indicators (EIP Mod and EIP Net) operate in conformance with ODVA standards:

- The EIP Mod status indicator shows whether the switch is receiving power and is functioning properly.
- The EIP Net status indicator shows the network status for the switch.

**Table 177 - EIP Status Indicators**

Indicator	Status	Description
EIP Mod	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch is operating properly.
	Flashing green	The switch has not been configured.
	Solid red	The switch has detected a major non-recoverable fault.
	Flashing Red	The switch has detected a major recoverable fault, such as an incorrect or inconsistent configuration.
	Flashing green and red	The switch is running a power on self test (POST).
EIP Net	Off	Power to the switch is off or not properly connected.
	Solid green	The switch has an established CIP™ connection to one or more attached devices.
	Flashing green	The switch has an IP address, but does not have an established CIP connection to one or more attached devices.
	Solid red	The switch has detected that its IP address is already in use by another device in the network.
	Flashing red	One or more connections to attached devices have timed out.
	Flashing green and red	The switch is running a power on self test (POST).

## Alarm Status Indicators

The alarm status indicators show the status of the two alarm inputs and one alarm output.

**Table 178 - Alarm Status Indicators**

Indicator	Status	Description
Alarm IN1 Alarm IN2	Shows the status of the alarm inputs.	
	Off	Alarm IN1 or IN2 is not configured.
	Solid green	Alarm IN1 or IN2 is configured; no alarm is detected.
	Solid red	The switch has detected a minor alarm.
	Flashing red	The switch has detected a major alarm.
Alarm OUT	Shows the status of the alarm output.	
	Off	Alarm OUT is not configured, or the switch is off.
	Solid green	Alarm OUT is configured; no alarm is detected.
	Solid red	The switch has detected a minor alarm.
	Flashing red	The switch has detected a major alarm.

## Port Status Indicators

The port status indicators show the connection and activity status of the port.

**Table 179 - Port Status Indicator**

Indicator	Status	Description
Port	Off	The port is not connected to a device.
	Solid green	The port is connected to a device, but there is no activity.
	Flashing green	The port connection has activity and is sending or receiving data.
	Solid amber	The port is not forwarding data.
	Alternating green and amber	The port connection has a link fault.

## Data Types

Topic	Page
10-Port Data Types	267
18-Port Data Types	269
26-Port Data Types	271

In the Studio 5000 Logix Designer® application, predefined tags for Input and Output data types have a structure that corresponds to the switch selected when it was added to the I/O tree. Its members are named in accordance with the port names.

You can disable a switch port by setting the corresponding bit in the output tag. The output bits are applied every time that the switch receives the output data from the controller when the controller is in Run mode. When the controller is in Program mode, the output bits are not applied.

The port is enabled if the corresponding output bit is 0. If you enable or disable a port via the WebUI or the command-line interface (CLI), the output bits override the port setting the next time the bits are applied. The output bits always take precedence, regardless of whether the WebUI or the CLI is used to enable or disable the port.

The following tables list module-defined data types for Stratix® 5800 switches and expansion modules.

### 10-Port Data Types

The following tables list the input and output data types for a 10-port base switch with no expansion module attached.

**Table 180 - Stratix 5800 Input Data Types (10 Ports)**

AB:STRATIX_5800_10PORT_MANAGED:I:0			
Member Name	Type	Default Display Style	Valid Values
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortGi1_1Connected	BOOL	Decimal	LinkStatus:1
PortGi1_2Connected	BOOL	Decimal	LinkStatus:2
PortGi1_3Connected	BOOL	Decimal	LinkStatus:3
PortGi1_4Connected	BOOL	Decimal	LinkStatus:4
PortGi1_5Connected	BOOL	Decimal	LinkStatus:5
PortGi1_6Connected	BOOL	Decimal	LinkStatus:6

Table 180 - Stratix 5800 Input Data Types (10 Ports) (Continued)

AB:STRATIX_5800_10PORT_MANAGED:I:0			
Member Name	Type	Default Display Style	Valid Values
PortGi1_7Connected	BOOL	Decimal	LinkStatus:7
PortGi1_8Connected	BOOL	Decimal	LinkStatus:8
PortGi1_9Connected	BOOL	Decimal	LinkStatus:9
PortGi1_10Connected	BOOL	Decimal	LinkStatus:10
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortGi1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortGi1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortGi1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortGi1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortGi1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortGi1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortGi1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortGi1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortGi1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortGi1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortGi1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortGi1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortGi1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortGi1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortGi1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortGi1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
AllPortsUtilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
PortGi1_3Utilization	SINT	Decimal	
PortGi1_4Utilization	SINT	Decimal	
PortGi1_5Utilization	SINT	Decimal	
PortGi1_6Utilization	SINT	Decimal	
PortGi1_7Utilization	SINT	Decimal	
PortGi1_8Utilization	SINT	Decimal	
PortGi1_9Utilization	SINT	Decimal	
PortGi1_10Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupActive	DINT	Binary	

Table 181 - Stratix 5800 Output Data Types (10 Ports)

AB:STRATIX_5800_10PORT_MANAGED:O:0			
Member Name	Type	Default Display Style	Valid Values
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortGi1_1Disable	BOOL	Decimal	DisablePort:1
PortGi1_2Disable	BOOL	Decimal	DisablePort:2
PortGi1_3Disable	BOOL	Decimal	DisablePort:3
PortGi1_4Disable	BOOL	Decimal	DisablePort:4

**Table 181 - Stratix 5800 Output Data Types (10 Ports)**

<b>AB:STRATIX_5800_10PORT_MANAGED:0:0</b>			
<b>Member Name</b>	<b>Type</b>	<b>Default Display Style</b>	<b>Valid Values</b>
PortGi1_5Disable	BOOL	Decimal	DisablePort:5
PortGi1_6Disable	BOOL	Decimal	DisablePort:6
PortGi1_7Disable	BOOL	Decimal	DisablePort:7
PortGi1_8Disable	BOOL	Decimal	DisablePort:8
PortGi1_9Disable	BOOL	Decimal	DisablePort:9
PortGi1_10Disable	BOOL	Decimal	DisablePort:10

## 18-Port Data Types

The following table lists the input and output data types for a 10-port base switch with an 8-port expansion module attached.

**Table 182 - Stratix 5800 Input Data Types (18 Ports)**

<b>AB:STRATIX_5800_18PORT_MANAGED:1:0</b>			
<b>Member Name</b>	<b>Type</b>	<b>Default Display Style</b>	<b>Valid Values</b>
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortGi1_1Connected	BOOL	Decimal	LinkStatus:1
PortGi1_2Connected	BOOL	Decimal	LinkStatus:2
PortGi1_3Connected	BOOL	Decimal	LinkStatus:3
PortGi1_4Connected	BOOL	Decimal	LinkStatus:4
PortGi1_5Connected	BOOL	Decimal	LinkStatus:5
PortGi1_6Connected	BOOL	Decimal	LinkStatus:6
PortGi1_7Connected	BOOL	Decimal	LinkStatus:7
PortGi1_8Connected	BOOL	Decimal	LinkStatus:8
PortGi1_9Connected	BOOL	Decimal	LinkStatus:9
PortGi1_10Connected	BOOL	Decimal	LinkStatus:10
PortGi2_1Connected	BOOL	Decimal	LinkStatus:11
PortGi2_2Connected	BOOL	Decimal	LinkStatus:12
PortGi2_3Connected	BOOL	Decimal	LinkStatus:13
PortGi2_4Connected	BOOL	Decimal	LinkStatus:14
PortGi2_5Connected	BOOL	Decimal	LinkStatus:15
PortGi2_6Connected	BOOL	Decimal	LinkStatus:16
PortGi2_7Connected	BOOL	Decimal	LinkStatus:17
PortGi2_8Connected	BOOL	Decimal	LinkStatus:18
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortGi1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortGi1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortGi1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortGi1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortGi1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortGi1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortGi1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortGi1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortGi2_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortGi2_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortGi2_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13



Table 182 - Stratix 5800 Input Data Types (18 Ports) (Continued)

AB:STRATIX_5800_18PORT_MANAGED:I:0			
Member Name	Type	Default Display Style	Valid Values
PortGi2_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortGi2_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortGi2_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortGi2_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortGi2_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortGi1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortGi1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortGi1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortGi1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortGi1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortGi1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortGi1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortGi1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortGi2_1Threshold	BOOL	Decimal	ThresholdExceeded:11
PortGi2_2Threshold	BOOL	Decimal	ThresholdExceeded:12
PortGi2_3Threshold	BOOL	Decimal	ThresholdExceeded:13
PortGi2_4Threshold	BOOL	Decimal	ThresholdExceeded:14
PortGi2_5Threshold	BOOL	Decimal	ThresholdExceeded:15
PortGi2_6Threshold	BOOL	Decimal	ThresholdExceeded:16
PortGi2_7Threshold	BOOL	Decimal	ThresholdExceeded:17
PortGi2_8Threshold	BOOL	Decimal	ThresholdExceeded:18
AllPortsUtilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
PortGi1_3Utilization	SINT	Decimal	
PortGi1_4Utilization	SINT	Decimal	
PortGi1_5Utilization	SINT	Decimal	
PortGi1_6Utilization	SINT	Decimal	
PortGi1_7Utilization	SINT	Decimal	
PortGi1_8Utilization	SINT	Decimal	
PortGi1_9Utilization	SINT	Decimal	
PortGi1_10Utilization	SINT	Decimal	
PortGi2_1Utilization	SINT	Decimal	
PortGi2_2Utilization	SINT	Decimal	
PortGi2_3Utilization	SINT	Decimal	
PortGi2_4Utilization	SINT	Decimal	
PortGi2_5Utilization	SINT	Decimal	
PortGi2_6Utilization	SINT	Decimal	
PortGi2_7Utilization	SINT	Decimal	
PortGi2_8Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupActive	DINT	Binary	

**Table 183 - Stratix 5800 Output Data Types (18 Ports)**

<b>AB:STRATIX_5800_18PORT_MANAGED:0:0</b>			
<b>Member Name</b>	<b>Type</b>	<b>Default Display Style</b>	<b>Valid Values</b>
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortGi1_1Disable	BOOL	Decimal	DisablePort:1
PortGi1_2Disable	BOOL	Decimal	DisablePort:2
PortGi1_3Disable	BOOL	Decimal	DisablePort:3
PortGi1_4Disable	BOOL	Decimal	DisablePort:4
PortGi1_5Disable	BOOL	Decimal	DisablePort:5
PortGi1_6Disable	BOOL	Decimal	DisablePort:6
PortGi1_7Disable	BOOL	Decimal	DisablePort:7
PortGi1_8Disable	BOOL	Decimal	DisablePort:8
PortGi1_9Disable	BOOL	Decimal	DisablePort:9
PortGi1_10Disable	BOOL	Decimal	DisablePort:10
PortGi2_1Disable	BOOL	Decimal	DisablePort:11
PortGi2_2Disable	BOOL	Decimal	DisablePort:12
PortGi2_3Disable	BOOL	Decimal	DisablePort:13
PortGi2_4Disable	BOOL	Decimal	DisablePort:14
PortGi2_5Disable	BOOL	Decimal	DisablePort:15
PortGi2_6Disable	BOOL	Decimal	DisablePort:16
PortGi2_7Disable	BOOL	Decimal	DisablePort:17
PortGi2_8Disable	BOOL	Decimal	DisablePort:18

## 26-Port Data Types

The following table lists the input and output data types for a 10-port base switch with a 16-port expansion module attached.

**Table 184 - Stratix 5800 Input Data Types (26 Ports)**

<b>AB:STRATIX_5800_26PORT_MANAGED:I:0</b>			
<b>Member Name</b>	<b>Type</b>	<b>Default Display Style</b>	<b>Valid Values</b>
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortGi1_1Connected	BOOL	Decimal	LinkStatus:1
PortGi1_2Connected	BOOL	Decimal	LinkStatus:2
PortGi1_3Connected	BOOL	Decimal	LinkStatus:3
PortGi1_4Connected	BOOL	Decimal	LinkStatus:4
PortGi1_5Connected	BOOL	Decimal	LinkStatus:5
PortGi1_6Connected	BOOL	Decimal	LinkStatus:6
PortGi1_7Connected	BOOL	Decimal	LinkStatus:7
PortGi1_8Connected	BOOL	Decimal	LinkStatus:8
PortGi1_9Connected	BOOL	Decimal	LinkStatus:9
PortGi1_10Connected	BOOL	Decimal	LinkStatus:10
PortGi2_1Connected	BOOL	Decimal	LinkStatus:11
PortGi2_2Connected	BOOL	Decimal	LinkStatus:12
PortGi2_3Connected	BOOL	Decimal	LinkStatus:13
PortGi2_4Connected	BOOL	Decimal	LinkStatus:14
PortGi2_5Connected	BOOL	Decimal	LinkStatus:15
PortGi2_6Connected	BOOL	Decimal	LinkStatus:16
PortGi2_7Connected	BOOL	Decimal	LinkStatus:17
PortGi2_8Connected	BOOL	Decimal	LinkStatus:18
PortGi2_9Connected	BOOL	Decimal	LinkStatus:19

Table 184 - Stratix 5800 Input Data Types (26 Ports) (Continued)

AB:STRATIX_5800_26PORT_MANAGED:I:0			
Member Name	Type	Default Display Style	Valid Values
PortGi2_10Connected	BOOL	Decimal	LinkStatus:20
PortGi2_11Connected	BOOL	Decimal	LinkStatus:21
PortGi2_12Connected	BOOL	Decimal	LinkStatus:22
PortGi2_13Connected	BOOL	Decimal	LinkStatus:23
PortGi2_14Connected	BOOL	Decimal	LinkStatus:24
PortGi2_15Connected	BOOL	Decimal	LinkStatus:25
PortGi2_16Connected	BOOL	Decimal	LinkStatus:26
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortGi1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortGi1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortGi1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortGi1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortGi1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortGi1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortGi1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortGi1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortGi2_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortGi2_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortGi2_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortGi2_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortGi2_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortGi2_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortGi2_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortGi2_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortGi2_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortGi2_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
PortGi2_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:21
PortGi2_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:22
PortGi2_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:23
PortGi2_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:24
PortGi2_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:25
PortGi2_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:26
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortGi1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortGi1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortGi1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortGi1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortGi1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortGi1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortGi1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortGi1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortGi2_1Threshold	BOOL	Decimal	ThresholdExceeded:11
PortGi2_2Threshold	BOOL	Decimal	ThresholdExceeded:12
PortGi2_3Threshold	BOOL	Decimal	ThresholdExceeded:13
PortGi2_4Threshold	BOOL	Decimal	ThresholdExceeded:14
PortGi2_5Threshold	BOOL	Decimal	ThresholdExceeded:15

Table 184 - Stratix 5800 Input Data Types (26 Ports) (Continued)

AB:STRATIX_5800_26PORT_MANAGED:I:0			
Member Name	Type	Default Display Style	Valid Values
PortGi2_6Threshold	BOOL	Decimal	ThresholdExceeded:16
PortGi2_7Threshold	BOOL	Decimal	ThresholdExceeded:17
PortGi2_8Threshold	BOOL	Decimal	ThresholdExceeded:18
PortGi2_9Threshold	BOOL	Decimal	ThresholdExceeded:19
PortGi2_10Threshold	BOOL	Decimal	ThresholdExceeded:20
PortGi2_11Threshold	BOOL	Decimal	ThresholdExceeded:21
PortGi2_12Threshold	BOOL	Decimal	ThresholdExceeded:22
PortGi2_13Threshold	BOOL	Decimal	ThresholdExceeded:23
PortGi2_14Threshold	BOOL	Decimal	ThresholdExceeded:24
PortGi2_15Threshold	BOOL	Decimal	ThresholdExceeded:25
PortGi2_16Threshold	BOOL	Decimal	ThresholdExceeded:26
AllPortsUtilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
PortGi1_3Utilization	SINT	Decimal	
PortGi1_4Utilization	SINT	Decimal	
PortGi1_5Utilization	SINT	Decimal	
PortGi1_6Utilization	SINT	Decimal	
PortGi1_7Utilization	SINT	Decimal	
PortGi1_8Utilization	SINT	Decimal	
PortGi1_9Utilization	SINT	Decimal	
PortGi1_10Utilization	SINT	Decimal	
PortGi2_1Utilization	SINT	Decimal	
PortGi2_2Utilization	SINT	Decimal	
PortGi2_3Utilization	SINT	Decimal	
PortGi2_4Utilization	SINT	Decimal	
PortGi2_5Utilization	SINT	Decimal	
PortGi2_6Utilization	SINT	Decimal	
PortGi2_7Utilization	SINT	Decimal	
PortGi2_8Utilization	SINT	Decimal	
PortGi2_9Utilization	SINT	Decimal	
PortGi2_10Utilization	SINT	Decimal	
PortGi2_11Utilization	SINT	Decimal	
PortGi2_12Utilization	SINT	Decimal	
PortGi2_13Utilization	SINT	Decimal	
PortGi2_14Utilization	SINT	Decimal	
PortGi2_15Utilization	SINT	Decimal	
PortGi2_16Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupActive	DINT	Binary	

Table 185 - Stratix 5800 Output Data Types (26 Ports)

AB:STRATIX_5800_26PORT_MANAGED:O:0			
Member Name	Type	Default Display Style	Valid Values
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortGi1_1Disable	BOOL	Decimal	DisablePort:1
PortGi1_2Disable	BOOL	Decimal	DisablePort:2
PortGi1_3Disable	BOOL	Decimal	DisablePort:3

Table 185 - Stratix 5800 Output Data Types (26 Ports)

AB:STRATIX_5800_26PORT_MANAGED:0:0			
Member Name	Type	Default Display Style	Valid Values
PortGi1_4Disable	BOOL	Decimal	DisablePort:4
PortGi1_5Disable	BOOL	Decimal	DisablePort:5
PortGi1_6Disable	BOOL	Decimal	DisablePort:6
PortGi1_7Disable	BOOL	Decimal	DisablePort:7
PortGi1_8Disable	BOOL	Decimal	DisablePort:8
PortGi1_9Disable	BOOL	Decimal	DisablePort:9
PortGi1_10Disable	BOOL	Decimal	DisablePort:10
PortGi2_1Disable	BOOL	Decimal	DisablePort:11
PortGi2_2Disable	BOOL	Decimal	DisablePort:12
PortGi2_3Disable	BOOL	Decimal	DisablePort:13
PortGi2_4Disable	BOOL	Decimal	DisablePort:14
PortGi2_5Disable	BOOL	Decimal	DisablePort:15
PortGi2_6Disable	BOOL	Decimal	DisablePort:16
PortGi2_7Disable	BOOL	Decimal	DisablePort:17
PortGi2_8Disable	BOOL	Decimal	DisablePort:18
PortGi2_9Disable	BOOL	Decimal	DisablePort:19
PortGi2_10Disable	BOOL	Decimal	DisablePort:20
PortGi2_11Disable	BOOL	Decimal	DisablePort:21
PortGi2_12Disable	BOOL	Decimal	DisablePort:22
PortGi2_13Disable	BOOL	Decimal	DisablePort:23
PortGi2_14Disable	BOOL	Decimal	DisablePort:24
PortGi2_15Disable	BOOL	Decimal	DisablePort:25
PortGi2_16Disable	BOOL	Decimal	DisablePort:26

## Port Assignments for CIP Data

Topic	Page
Port Assignments	275

### Port Assignments

The following table identifies the instance numbers of the Ethernet link objects that are associated with each port on Stratix® 5800 switches and expansion modules. Instance 0 does not apply to all ports as it does for bit maps.

The bit numbers identify each port when they are contained in a structure of all ports, such as in the output assembly. Bit 0 refers to any or all ports.

The 10-port column shows port assignments for a 10-port base switch with no expansion module attached.

The 18-port column shows port assignments for a 10-port base switch with an 8-port expansion module attached.

The 26-port column shows port assignments for a 10-port base switch with a 16-port expansion module attached.

**Table 186 - Stratix 5800 Port Assignments**

Bit	10 Ports	18 Ports	26 Ports
0	Any/All ports	Any/All ports	Any/All ports
1	Gi1/1	Gi1/1	Gi1/1
2	Gi1/2	Gi1/2	Gi1/2
3	Gi1/3	Gi1/3	Gi1/3
4	Gi1/4	Gi1/4	Gi1/4
5	Gi1/5	Gi1/5	Gi1/5
6	Gi1/6	Gi1/6	Gi1/6
7	Gi1/7	Gi1/7	Gi1/7
8	Gi1/8	Gi1/8	Gi1/8
9	Gi1/9	Gi1/9	Gi1/9
10	Gi1/10	Gi1/10	Gi1/10
11		Gi2/1	Gi2/1
12		Gi2/2	Gi2/2
13		Gi2/3	Gi2/3
14		Gi2/4	Gi2/4
15		Gi2/5	Gi2/5
16		Gi2/6	Gi2/6
17		Gi2/7	Gi2/7
18		Gi2/8	Gi2/8

**Table 186 - Stratix 5800 Port Assignments (Continued)**

Bit	10 Ports	18 Ports	26 Ports
19			Gi2/9
20			Gi2/10
21			Gi2/11
22			Gi2/12
23			Gi2/13
24			Gi2/14
25			Gi2/15
26			Gi2/16

## Port Numbering

Topic	Page
Switch Port Numbering	277
Expansion Module Port Numbering	279

### Switch Port Numbering

The port ID consists of the following:

- Port type (Gigabit Ethernet)
- Unit number (always 1 for base unit)
- Port number (1...10)

Gigabit Ethernet is abbreviated as Gi.

**Table 187 - Stratix 5800 Switch Port Numbering**

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-MMS10B	10-port (8 Ethernet ports, 2 SFP ports), non-expandable base switch, Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10
1783-MMS10BE	10-port (8 Ethernet PoE/PoE+ ports, 2 SFP ports), non-expandable base switch, Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10
1783-MMS10	10-port (8 Ethernet ports, 2 SFP ports), expandable base switch, Layer 2 firmware	1	Gi1/1
		2	Gi1/2
		3	Gi1/3
		4	Gi1/4
		5	Gi1/5
		6	Gi1/6
		7	Gi1/7
		8	Gi1/8
		9	Gi1/9
		10	Gi1/10



Table 187 - Stratix 5800 Switch Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-MMS10E	10-port (8 Ethernet PoE/PoE+ ports, 2 SFP ports), expandable base switch, Layer 2 firmware	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10
1783-MMS10R	10-port (8 Ethernet ports, 2 SFP ports), expandable base switch, Layer 3 firmware	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10
1783-MMS10ER	10-port (8 Ethernet PoE/PoE+ ports, 2 SFP ports), expandable base switch, Layer 3 firmware	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10
1783-MMS10EA	10-port (8 Ethernet PoE/PoE+ ports, 2 SFP ports), expandable base switch, Layer 2 firmware, advanced feature support	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10
1783-MMS10EAR	10-port (8 Ethernet PoE/PoE+ ports, 2 SFP ports), expandable base switch, Layer 3 firmware, advanced feature support	1 2 3 4 5 6 7 8 9 10	Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9 Gi1/10

## Expansion Module Port Numbering

The port ID consists of the following:

- Port type (Gigabit Ethernet)
- Unit number (always 2 for expansion module)
- Port number (1...8 or 1...16)

Gigabit Ethernet is abbreviated as Gi.

**Table 188 - Stratix 5800 Expansion Module Port Numbering**

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-MMX8T	8-port (8 Ethernet ports) expansion module	1 2 3 4 5 6 7 8	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8
1783-MMX8E	8-port (8 Ethernet PoE/PoE+ ports) expansion module	1 2 3 4 5 6 7 8	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8
1783-MMX8S	8-port (8 SFP ports) expansion module	1 2 3 4 5 6 7 8	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8
1783-MMX6T2S	8-port (6 Ethernet ports, 2 SFP ports) expansion module	1 2 3 4 5 6 7 8	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8
1783-MMX16T	16-port (16 Ethernet ports) expansion module	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8 Gi2/9 Gi2/10 Gi2/11 Gi2/12 Gi2/13 Gi2/14 Gi2/15 Gi2/16

Table 188 - Stratix 5800 Expansion Module Port Numbering (Continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-MMX16E	16-port (16 Ethernet PoE/PoE+ ports) expansion module	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8 Gi2/9 Gi2/10 Gi2/11 Gi2/12 Gi2/13 Gi2/14 Gi2/15 Gi2/16
1783-MMX14T2S	16-port (14 Ethernet, 2 SFP ports) expansion module	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8 Gi2/9 Gi2/10 Gi2/11 Gi2/12 Gi2/13 Gi2/14 Gi2/15 Gi2/16
1783-MMX8EA	8-port (8 Ethernet PoE/PoE+ ports) expansion module, advanced feature support	1 2 3 4 5 6 7 8	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8
1783-MMX8SA	8-port (8 SFP ports) expansion module, advanced feature support	1 2 3 4 5 6 7 8	Gi2/1 Gi2/2 Gi2/3 Gi2/4 Gi2/5 Gi2/6 Gi2/7 Gi2/8

## MODBUS Register Lists

Topic	Page
10-port Register Files	281
18-port Register Files	282
26-port Register Files	285
System Register File	288

### 10-port Register Files

The following table lists the 10-port register files.

**Table 189 - MODBUS 10-port Register Files**

Address	Number of Registers	Description	Read/Write	Format
1000	64	Port 1 Name	R	Text
1040	64	Port 2 Name	R	Text
1080	64	Port 3 Name	R	Text
10C0	64	Port 4 Name	R	Text
1100	64	Port 5 Name	R	Text
1140	64	Port 6 Name	R	Text
1180	64	Port 7 Name	R	Text
11C0	64	Port 8 Name	R	Text
1200	64	Port 9 Name	R	Text
1240	64	Port 10 Name	R	Text
1280	1	Port 1 State	R	UInt16
1281	1	Port 2 State	R	UInt16
1282	1	Port 3 State	R	UInt16
1283	1	Port 4 State	R	UInt16
1284	1	Port 5 State	R	UInt16
1285	1	Port 6 State	R	UInt16
1286	1	Port 7 State	R	UInt16
1287	1	Port 8 State	R	UInt16
1288	1	Port 9 State	R	UInt16
1289	1	Port 10 State	R	UInt16
128A	4	Port 1 Statistics—Number of packets received	R	UInt64
128E	4	Port 2 Statistics—Number of packets received	R	UInt64
1292	4	Port 3 Statistics—Number of packets received	R	UInt64
1296	4	Port 4 Statistics—Number of packets received	R	UInt64
129A	4	Port 5 Statistics—Number of packets received	R	UInt64
129E	4	Port 6 Statistics—Number of packets received	R	UInt64
12A2	4	Port 7 Statistics—Number of packets received	R	UInt64
12A6	4	Port 8 Statistics—Number of packets received	R	UInt64
12AA	4	Port 9 Statistics—Number of packets received	R	UInt64
12AE	4	Port 10 Statistics—Number of packets received	R	UInt64

**Table 189 - MODBUS 10-port Register Files (Continued)**

Address	Number of Registers	Description	Read/Write	Format
12B2	4	Port 1 Statistics—Number of packets sent	R	Uint64
12B6	4	Port 2 Statistics—Number of packets sent	R	Uint64
12BA	4	Port 3 Statistics—Number of packets sent	R	Uint64
12BE	4	Port 4 Statistics—Number of packets sent	R	Uint64
12C2	4	Port 5 Statistics—Number of packets sent	R	Uint64
12C6	4	Port 6 Statistics—Number of packets sent	R	Uint64
12CA	4	Port 7 Statistics—Number of packets sent	R	Uint64
12CE	4	Port 8 Statistics—Number of packets sent	R	Uint64
12D2	4	Port 9 Statistics—Number of packets sent	R	Uint64
12D6	4	Port 10 Statistics—Number of packets sent	R	Uint64
12DA	4	Port 1 Statistics—Number of bytes received	R	Uint64
12DE	4	Port 2 Statistics—Number of bytes received	R	Uint64
12E2	4	Port 3 Statistics—Number of bytes received	R	Uint64
12E6	4	Port 4 Statistics—Number of bytes received	R	Uint64
12EA	4	Port 5 Statistics—Number of bytes received	R	Uint64
12EE	4	Port 6 Statistics—Number of bytes received	R	Uint64
12F2	4	Port 7 Statistics—Number of bytes received	R	Uint64
12F6	4	Port 8 Statistics—Number of bytes received	R	Uint64
12FA	4	Port 9 Statistics—Number of bytes received	R	Uint64
12FE	4	Port 10 Statistics—Number of bytes received	R	Uint64
1302	4	Port 1 Statistics—Number of bytes sent	R	Uint64
1306	4	Port 2 Statistics—Number of bytes sent	R	Uint64
130A	4	Port 3 Statistics—Number of bytes sent	R	Uint64
130E	4	Port 4 Statistics—Number of bytes sent	R	Uint64
1312	4	Port 5 Statistics—Number of bytes sent	R	Uint64
1316	4	Port 6 Statistics—Number of bytes sent	R	Uint64
131A	4	Port 7 Statistics—Number of bytes sent	R	Uint64
131E	4	Port 8 Statistics—Number of bytes sent	R	Uint64
1322	4	Port 9 Statistics—Number of bytes sent	R	Uint64
1326	4	Port 10 Statistics—Number of bytes sent	R	Uint64

## 18-port Register Files

The following table lists the 18-port register files.

**Table 190 - 18-port Register Files**

Address	Number of Registers	Description	Read/Write	Format
1000	64	Port 1 Name	R	Text
1040	64	Port 2 Name	R	Text
1080	64	Port 3 Name	R	Text
10C0	64	Port 4 Name	R	Text
1100	64	Port 5 Name	R	Text
1140	64	Port 6 Name	R	Text
1180	64	Port 7 Name	R	Text
11C0	64	Port 8 Name	R	Text
1200	64	Port 9 Name	R	Text
1240	64	Port 10 Name	R	Text
1280	64	Port 11 Name	R	Text
12C0	64	Port 12 Name	R	Text
1300	64	Port 13 Name	R	Text

Table 190 - 18-port Register Files (Continued)

Address	Number of Registers	Description	Read/Write	Format
1340	64	Port 14 Name	R	Text
1380	64	Port 15 Name	R	Text
13C0	64	Port 16 Name	R	Text
1400	64	Port 17 Name	R	Text
1440	64	Port 18 Name	R	Text
1480	1	Port 1 State	R	UInt16
1481	1	Port 2 State	R	UInt16
1482	1	Port 3 State	R	UInt16
1483	1	Port 4 State	R	UInt16
1484	1	Port 5 State	R	UInt16
1485	1	Port 6 State	R	UInt16
1486	1	Port 7 State	R	UInt16
1487	1	Port 8 State	R	UInt16
1488	1	Port 9 State	R	UInt16
1489	1	Port 10 State	R	UInt16
148A	1	Port 11 State	R	UInt16
148B	1	Port 12 State	R	UInt16
148C	1	Port 13 State	R	UInt16
148D	1	Port 14 State	R	UInt16
148E	1	Port 15 State	R	UInt16
148F	1	Port 16 State	R	UInt16
1490	1	Port 17 State	R	UInt16
1491	1	Port 18 State	R	UInt16
1492	4	Port 1 Statistics—Number of packets received	R	UInt64
1496	4	Port 2 Statistics—Number of packets received	R	UInt64
149A	4	Port 3 Statistics—Number of packets received	R	UInt64
149E	4	Port 4 Statistics—Number of packets received	R	UInt64
14A2	4	Port 5 Statistics—Number of packets received	R	UInt64
14A6	4	Port 6 Statistics—Number of packets received	R	UInt64
14AA	4	Port 7 Statistics—Number of packets received	R	UInt64
14AE	4	Port 8 Statistics—Number of packets received	R	UInt64
14BA	4	Port 9 Statistics—Number of packets received	R	UInt64
14BE	4	Port 10 Statistics—Number of packets received	R	UInt64
14C2	4	Port 11 Statistics—Number of packets received	R	UInt64
14C6	4	Port 12 Statistics—Number of packets received	R	UInt64
14CA	4	Port 13 Statistics—Number of packets received	R	UInt64
14CE	4	Port 14 Statistics—Number of packets received	R	UInt64
14D2	4	Port 15 Statistics—Number of packets received	R	UInt64
14D6	4	Port 16 Statistics—Number of packets received	R	UInt64
14DA	4	Port 17 Statistics—Number of packets received	R	UInt64
14DE	4	Port 18 Statistics—Number of packets received	R	UInt64
14E2	4	Port 1 Statistics—Number of packets sent	R	UInt64
14E6	4	Port 2 Statistics—Number of packets sent	R	UInt64
14EA	4	Port 3 Statistics—Number of packets sent	R	UInt64
14EE	4	Port 4 Statistics—Number of packets sent	R	UInt64
14F2	4	Port 5 Statistics—Number of packets sent	R	UInt64
14F6	4	Port 6 Statistics—Number of packets sent	R	UInt64
14FA	4	Port 7 Statistics—Number of packets sent	R	UInt64
14FE	4	Port 8 Statistics—Number of packets sent	R	UInt64
1502	4	Port 9 Statistics—Number of packets sent	R	UInt64
1506	4	Port 10 Statistics—Number of packets sent	R	UInt64

Table 190 - 18-port Register Files (Continued)

Address	Number of Registers	Description	Read/Write	Format
150A	4	Port 11 Statistics—Number of packets sent	R	UInt64
1506	4	Port 12 Statistics—Number of packets sent	R	UInt64
150A	4	Port 13 Statistics—Number of packets sent	R	UInt64
150E	4	Port 14 Statistics—Number of packets sent	R	UInt64
1512	4	Port 15 Statistics—Number of packets sent	R	UInt64
1516	4	Port 16 Statistics—Number of packets sent	R	UInt64
151A	4	Port 17 Statistics—Number of packets sent	R	UInt64
151E	4	Port 18 Statistics—Number of packets sent	R	UInt64
1522	4	Port 1 Statistics—Number of bytes received	R	UInt64
1526	4	Port 2 Statistics—Number of bytes received	R	UInt64
152A	4	Port 3 Statistics—Number of bytes received	R	UInt64
152E	4	Port 4 Statistics—Number of bytes received	R	UInt64
1532	4	Port 5 Statistics—Number of bytes received	R	UInt64
1536	4	Port 6 Statistics—Number of bytes received	R	UInt64
153A	4	Port 7 Statistics—Number of bytes received	R	UInt64
153E	4	Port 8 Statistics—Number of bytes received	R	UInt64
1542	4	Port 9 Statistics—Number of bytes received	R	UInt64
1546	4	Port 10 Statistics—Number of bytes received	R	UInt64
154A	4	Port 11 Statistics—Number of bytes received	R	UInt64
154E	4	Port 12 Statistics—Number of bytes received	R	UInt64
1552	4	Port 13 Statistics—Number of bytes received	R	UInt64
1556	4	Port 14 Statistics—Number of bytes received	R	UInt64
155A	4	Port 15 Statistics—Number of bytes received	R	UInt64
155E	4	Port 16 Statistics—Number of bytes received	R	UInt64
1562	4	Port 17 Statistics—Number of bytes received	R	UInt64
1566	4	Port 18 Statistics—Number of bytes received	R	UInt64
156A	4	Port 1 Statistics—Number of bytes sent	R	UInt64
156E	4	Port 2 Statistics—Number of bytes sent	R	UInt64
1572	4	Port 3 Statistics—Number of bytes sent	R	UInt64
1576	4	Port 4 Statistics—Number of bytes sent	R	UInt64
157A	4	Port 5 Statistics—Number of bytes sent	R	UInt64
157E	4	Port 6 Statistics—Number of bytes sent	R	UInt64
1582	4	Port 7 Statistics—Number of bytes sent	R	UInt64
1586	4	Port 8 Statistics—Number of bytes sent	R	UInt64
158A	4	Port 9 Statistics—Number of bytes sent	R	UInt64
158E	4	Port 10 Statistics—Number of bytes sent	R	UInt64
1592	4	Port 11 Statistics—Number of bytes sent	R	UInt64
1596	4	Port 12 Statistics—Number of bytes sent	R	UInt64
159A	4	Port 13 Statistics—Number of bytes sent	R	UInt64
159E	4	Port 14 Statistics—Number of bytes sent	R	UInt64
15A2	4	Port 15 Statistics—Number of bytes sent	R	UInt64
15A6	4	Port 16 Statistics—Number of bytes sent	R	UInt64
15AA	4	Port 17 Statistics—Number of bytes sent	R	UInt64
15AE	4	Port 18 Statistics—Number of bytes sent	R	UInt64

## 26-port Register Files

The following table lists the 26-port register files.

**Table 191 - MODBUS 26-port Register Files**

Address	Number of Registers	Description	Read/Write	Format
1000	64	Port 1 Name	R	Text
1040	64	Port 2 Name	R	Text
1080	64	Port 3 Name	R	Text
10C0	64	Port 4 Name	R	Text
1100	64	Port 5 Name	R	Text
1140	64	Port 6 Name	R	Text
1180	64	Port 7 Name	R	Text
11C0	64	Port 8 Name	R	Text
1200	64	Port 9 Name	R	Text
1240	64	Port 10 Name	R	Text
1280	64	Port 11 Name	R	Text
12C0	64	Port 12 Name	R	Text
1300	64	Port 13 Name	R	Text
1340	64	Port 14 Name	R	Text
1380	64	Port 15 Name	R	Text
13C0	64	Port 16 Name	R	Text
1400	64	Port 17 Name	R	Text
1440	64	Port 18 Name	R	Text
1480	64	Port 19 Name	R	Text
14C0	64	Port 20 Name	R	Text
1500	64	Port 21 Name	R	Text
1540	64	Port 22 Name	R	Text
1580	64	Port 23 Name	R	Text
15C0	64	Port 24 Name	R	Text
1600	64	Port 25 Name	R	Text
1640	64	Port 26 Name	R	Text
1680	1	Port 1 State	R	UInt16
1681	1	Port 2 State	R	UInt16
1682	1	Port 3 State	R	UInt16
1683	1	Port 4 State	R	UInt16
1684	1	Port 5 State	R	UInt16
1685	1	Port 6 State	R	UInt16
1686	1	Port 7 State	R	UInt16
1687	1	Port 8 State	R	UInt16
1688	1	Port 9 State	R	UInt16
1689	1	Port 10 State	R	UInt16
168A	1	Port 11 State	R	UInt16
168B	1	Port 12 State	R	UInt16
168C	1	Port 13 State	R	UInt16
168D	1	Port 14 State	R	UInt16
168E	1	Port 15 State	R	UInt16
168F	1	Port 16 State	R	UInt16
1690	1	Port 17 State	R	UInt16
1691	1	Port 18 State	R	UInt16
1692	1	Port 19 State	R	UInt16
1693	1	Port 20 State	R	UInt16
1694	1	Port 21 State	R	UInt16
1695	1	Port 22 State	R	UInt16



Table 191 - MODBUS 26-port Register Files (Continued)

Address	Number of Registers	Description	Read/Write	Format
1696	1	Port 23 State	R	UInt16
1697	1	Port 24 State	R	UInt16
1698	1	Port 25 State	R	UInt16
1699	1	Port 26 State	R	UInt16
169A	4	Port 1 Statistics—Number of packets received	R	UInt64
169E	4	Port 2 Statistics—Number of packets received	R	UInt64
16A2	4	Port 3 Statistics—Number of packets received	R	UInt64
16A6	4	Port 4 Statistics—Number of packets received	R	UInt64
16AA	4	Port 5 Statistics—Number of packets received	R	UInt64
16AE	4	Port 6 Statistics—Number of packets received	R	UInt64
16B2	4	Port 7 Statistics—Number of packets received	R	UInt64
16B6	4	Port 8 Statistics—Number of packets received	R	UInt64
16BA	4	Port 9 Statistics—Number of packets received	R	UInt64
16BE	4	Port 10 Statistics—Number of packets received	R	UInt64
16C2	4	Port 11 Statistics—Number of packets received	R	UInt64
16C6	4	Port 12 Statistics—Number of packets received	R	UInt64
16CA	4	Port 13 Statistics—Number of packets received	R	UInt64
16CE	4	Port 14 Statistics—Number of packets received	R	UInt64
16D2	4	Port 15 Statistics—Number of packets received	R	UInt64
16D6	4	Port 16 Statistics—Number of packets received	R	UInt64
16DA	4	Port 17 Statistics—Number of packets received	R	UInt64
16DE	4	Port 18 Statistics—Number of packets received	R	UInt64
16E2	4	Port 19 Statistics—Number of packets received	R	UInt64
16E6	4	Port 20 Statistics—Number of packets received	R	UInt64
16EA	4	Port 21 Statistics—Number of packets received	R	UInt64
16EE	4	Port 22 Statistics—Number of packets received	R	UInt64
16F2	4	Port 23 Statistics—Number of packets received	R	UInt64
16F6	4	Port 24 Statistics—Number of packets received	R	UInt64
16FA	4	Port 25 Statistics—Number of packets received	R	UInt64
16FE	4	Port 26 Statistics—Number of packets received	R	UInt64
1702	4	Port 1 Statistics—Number of packets sent	R	UInt64
1706	4	Port 2 Statistics—Number of packets sent	R	UInt64
170A	4	Port 3 Statistics—Number of packets sent	R	UInt64
170E	4	Port 4 Statistics—Number of packets sent	R	UInt64
1712	4	Port 5 Statistics—Number of packets sent	R	UInt64
1716	4	Port 6 Statistics—Number of packets sent	R	UInt64
171A	4	Port 7 Statistics—Number of packets sent	R	UInt64
171E	4	Port 8 Statistics—Number of packets sent	R	UInt64
1722	4	Port 9 Statistics—Number of packets sent	R	UInt64
1726	4	Port 10 Statistics—Number of packets sent	R	UInt64
172A	4	Port 11 Statistics—Number of packets sent	R	UInt64
172E	4	Port 12 Statistics—Number of packets sent	R	UInt64
1732	4	Port 13 Statistics—Number of packets sent	R	UInt64
1736	4	Port 14 Statistics—Number of packets sent	R	UInt64
173A	4	Port 15 Statistics—Number of packets sent	R	UInt64
173E	4	Port 16 Statistics—Number of packets sent	R	UInt64
1742	4	Port 17 Statistics—Number of packets sent	R	UInt64
1746	4	Port 18 Statistics—Number of packets sent	R	UInt64
174A	4	Port 19 Statistics—Number of packets sent	R	UInt64
174E	4	Port 20 Statistics—Number of packets sent	R	UInt64
1752	4	Port 21 Statistics—Number of packets sent	R	UInt64

Table 191 - MODBUS 26-port Register Files (Continued)

Address	Number of Registers	Description	Read/Write	Format
1756	4	Port 22 Statistics—Number of packets sent	R	UInt64
175A	4	Port 23 Statistics—Number of packets sent	R	UInt64
175E	4	Port 24 Statistics—Number of packets sent	R	UInt64
1762	4	Port 25 Statistics—Number of packets sent	R	UInt64
1766	4	Port 26 Statistics—Number of packets sent	R	UInt64
176A	4	Port 1 Statistics—Number of bytes received	R	UInt64
176E	4	Port 2 Statistics—Number of bytes received	R	UInt64
1772	4	Port 3 Statistics—Number of bytes received	R	UInt64
1776	4	Port 4 Statistics—Number of bytes received	R	UInt64
177A0	4	Port 5 Statistics—Number of bytes received	R	UInt64
177E	4	Port 6 Statistics—Number of bytes received	R	UInt64
1782	4	Port 7 Statistics—Number of bytes received	R	UInt64
1786	4	Port 8 Statistics—Number of bytes received	R	UInt64
178A	4	Port 9 Statistics—Number of bytes received	R	UInt64
178E	4	Port 10 Statistics—Number of bytes received	R	UInt64
1792	4	Port 11 Statistics—Number of bytes received	R	UInt64
1796	4	Port 12 Statistics—Number of bytes received	R	UInt64
179A	4	Port 13 Statistics—Number of bytes received	R	UInt64
179E	4	Port 14 Statistics—Number of bytes received	R	UInt64
17A2	4	Port 15 Statistics—Number of bytes received	R	UInt64
17A6	4	Port 16 Statistics—Number of bytes received	R	UInt64
17AA	4	Port 17 Statistics—Number of bytes received	R	UInt64
17AE	4	Port 18 Statistics—Number of bytes received	R	UInt64
17B2	4	Port 19 Statistics—Number of bytes received	R	UInt64
17B6	4	Port 20 Statistics—Number of bytes received	R	UInt64
17BA	4	Port 21 Statistics—Number of bytes received	R	UInt64
17BE	4	Port 22 Statistics—Number of bytes received	R	UInt64
17C2	4	Port 23 Statistics—Number of bytes received	R	UInt64
17C6	4	Port 24 Statistics—Number of bytes received	R	UInt64
17CA	4	Port 25 Statistics—Number of bytes received	R	UInt64
17CE	4	Port 26 Statistics—Number of bytes received	R	UInt64
17D2	4	Port 1 Statistics—Number of bytes sent	R	UInt64
17D6	4	Port 2 Statistics—Number of bytes sent	R	UInt64
17DA	4	Port 3 Statistics—Number of bytes sent	R	UInt64
17DE	4	Port 4 Statistics—Number of bytes sent	R	UInt64
17E2	4	Port 5 Statistics—Number of bytes sent	R	UInt64
17E6	4	Port 6 Statistics—Number of bytes sent	R	UInt64
17EA	4	Port 7 Statistics—Number of bytes sent	R	UInt64
17EE	4	Port 8 Statistics—Number of bytes sent	R	UInt64
17F2	4	Port 9 Statistics—Number of bytes sent	R	UInt64
17F6	4	Port 10 Statistics—Number of bytes sent	R	UInt64
17FA	4	Port 11 Statistics—Number of bytes sent	R	UInt64
17FE	4	Port 12 Statistics—Number of bytes sent	R	UInt64
1802	4	Port 13 Statistics—Number of bytes sent	R	UInt64
1806	4	Port 14 Statistics—Number of bytes sent	R	UInt64
180A	4	Port 15 Statistics—Number of bytes sent	R	UInt64
180E	4	Port 16 Statistics—Number of bytes sent	R	UInt64
1812	4	Port 17 Statistics—Number of bytes sent	R	UInt64
1816	4	Port 18 Statistics—Number of bytes sent	R	UInt64
181A	4	Port 19 Statistics—Number of bytes sent	R	UInt64
181E	4	Port 20 Statistics—Number of bytes sent	R	UInt64

**Table 191 - MODBUS 26-port Register Files (Continued)**

Address	Number of Registers	Description	Read/Write	Format
1822	4	Port 21 Statistics—Number of bytes sent	R	UInt64
1826	4	Port 22 Statistics—Number of bytes sent	R	UInt64
182A	4	Port 23 Statistics—Number of bytes sent	R	UInt64
182E	4	Port 24 Statistics—Number of bytes sent	R	UInt64
1912	4	Port 25 Statistics—Number of bytes sent	R	UInt64
1916	4	Port 26 Statistics—Number of bytes sent	R	UInt64

## System Register File

The following table shows the details of the system register file.

**Table 192 - MODBUS System Register File**

Address	Number of Registers	Description	Read/Write	Format
800	64	Product ID	R	Text
840	64	Software Image Name	R	Text
880	64	Software Image Version	R	Text
8C0	64	Host Name	R	Text
900	64	Alarm 1—Description	R	Text
940	64	Alarm 2—Description	R	Text
980	1	Alarm 1—Status	R	UInt16
981	1	Alarm 2—Status	R	UInt16
982	1	Number of 10/100 Ethernet Ports	R	UInt16
983	1	Number of Gig Ethernet Ports	R	UInt16
984	1	Number of Alarms	R	UInt16
985	1	Number of Power Supplies	R	UInt16
986	1	PS1—Status	R	UInt16
987	1	PS2—Status	R	UInt16
988	1	System Temperature (in Celsius)	R	UInt16

## Numerics

**10/100/100 ports** 18

## A

### AAA

about 49  
configuration 50  
configure via WebUI 50  
map 53  
method lists 55  
policy password 66

**access control list. See ACL**

**access port** 79, 88, 136

**access the WebUI** 40

**access VLAN** 79, 135

**accounts, user** 216

### ACL

about 68  
associate with interface 69  
configure via WebUI 68

**adapter pinouts** 17

**add switch to controller project** 33

**Add-on Profile. See AOP**

**address pools** 190

**administrative VLAN, REP** 127

### administrator

login name 29  
password 29, 37  
user name 37

**alarm actions** 160, 162

**alarm configuration** 165

**alarm connector** 15

**alarm labels** 15

### alarm profile

about 159  
configure via WebUI 161  
default 160

**alarm relay setup** 163

### alarm settings

about 162  
configure via WebUI 163

**alarm status indicators** 265

**alarm types** 159, 162

**alarm, input** 15

**alarm, output** 15

**allowed VLANs** 79

**announce interval** 184

**announce timeout** 184

### AOP 24

**assign VLAN to NAT instance** 101

**authenticate users** 49, 210

**Authentication, Authroization, and Accounting.**

**See AAA**

**authorize users** 49

**auto QoS** 123

**auto-MDIX** 18

### autonegotiation

about 18  
configure 79, 83  
troubleshoot 262

## B

**back up configuration** 166, 169

**BASE-T ports** 18

**bit numbers** 275

**Boundary mode** 178, 183

**BPDU filtering** 139

**BPDU guard** 139

**broadcast storm** 80

### browser

Express Setup 24  
requirements for WebUI 39  
troubleshoot 262

**bundle, debug** 257

## C

**CA Trustpoints** 200

**cable diagnostics** 242

### cable schematics

twisted-pair crossover 19  
twisted-pair straight through 18

### cables

crossover 19  
damaged 260  
Ethernet and fiber 260  
guidelines 18  
straight-through 19

**CDP** 70, 226

**certificate authority** 200

### CIP

about 12, 171  
configure via WebUI 171  
data 275  
device settings 32  
enable 32  
IP address 32  
password 24, 27, 32  
status and statistics 228  
VLAN 24, 27, 32

**CIP Sync time** 178, 183

**Cisco Discovery Protocol. See CDP**

### CLI

about 172  
modes 172  
password 29  
run commands via WebUI 172

**clients, DHCP** 230

**clock modes** 178

Boundary 183  
End to End Transparent 185

**clock settings, monitor** 251

**command, CLI** 172

**command-line interface. See CLI**

**Common Industrial Protocol. See CIP**

- community strings, SNMP** 212
- comparison, software** 12
- configuration**
  - back up and restore via Logix Designer application 169
  - back up and restore via WebUI 166
- configuration software** 12
- connection faults** 83
- connection settings** 175
- connectors** 17
  - alarm 15
  - dual LC 21
  - front panel 14
  - PoE pinout 20
  - power 14
- console port** 17
  - connectors 16
  - location on switch 13
- contacts, normally closed** 15
- contacts, normally open** 15
- controller project** 33
- core dump** 256
- CPU utilization** 248
- crossover cables** 19
- custom Smartport roles** 137
- customize WebUI dashboard** 45

## D

- dashboard**
  - customize 45
  - dashlet descriptions 45
- data types** 267
- date and time settings** 29
- DB-25 pin** 17
- DB-9 pin** 17
- DC power connectors** 14
- debug bundle** 257
- default alarm profile** 160
- default gateway**
  - NAT 98
- default gateway IP address** 31
- default global macro** 37
- delay request interval** 184
- device name** 29
- device settings**
  - configure via Logix Designer application 175
  - configure via WebUI 173
- device settings, CIP** 32
- device temperature** 45
- device time**
  - configure via Logix Designer application 183
  - configure via WebUI 178
  - set manually 177, 179
  - set via NTP 177
  - set via PTP 178, 180
- DHCP** 31, 37, 190
  - troubleshoot 261
- DHCP clients, monitor** 230
- DHCP persistence** 190

- DHCP pools** 190
  - configure via Logix Designer application 195
  - configure via WebUI 192
- DHCP snooping** 191
- disable switch port** 267
- discovery protocols** 70
- DNS**
  - about 188
  - add server 188, 189
- domain name system. See DNS**
- download**
  - core files 256
  - debug bundle 257
- driver, USB device** 16
- dual LC connector** 21
- dump, core** 256
- Duplex mode** 79, 83
  - troubleshoot 262
- Dynamic Host Control Protocol. See DHCP**

## E

- edge port** 127
- EIGRP** 73
- EIP status indicators** 265
- enable CIP** 32
- End to End Transparent mode** 178, 185
- Enhanced Interior Gateway Routing Protocol. See EIGRP**
- EtherChannels**
  - about 86
  - configure 89
  - modes 86
- Ethernet ports**
  - configuration via Logix Designer application 82
  - configure via WebUI 76
  - Duplex mode 79, 83
  - fault/program action 83
  - numbering 277
  - speed 79, 83
  - status indicators 266
- EtherNet/IP interface** 12
- EtherNet/IP protocol** 136
- expansion modules** 11
- Express Setup**
  - button 25
  - global macro 37
  - Long Press mode 28
  - Medium Press mode 27
  - modes 23
  - requirements 24
  - Short Press mode 26
  - status indicator 264
  - via Logix Designer application 33
  - via WebUI 28
- external alarm** 162

## F

- factory default settings** 28
- fallback, RADIUS** 65
- fault/program action** 83

**faults, connection** 83

**features**

hardware 13  
software 12

**fiber**

multimode 21  
singlemode 21

**File Manager** 198

**fixed switches** 11

**flash** 169, 170

**Forward mode** 178

**front panel**

connectors 14  
overview 13  
status indicators 263

**FTP/TFTP settings** 174

**full-duplex** 18

## G

**gateway IP address** 31, 37

**global alarm actions** 162

**global alarm configuration** 164

**global alarm types** 162

**global macro** 37

**GMC** 250, 251

## H

**half-duplex** 18

**hardware features** 13

**hosts, SNMP** 214

**HTTP/HTTPS** 200

## I

**ID, management VLAN** 31

**IEEE 1588** 178

**IEEE 802.1AB** 70

**IEEE 802.1D** 139

**IEEE 802.1s** 139

**IEEE 802.1w** 139

**IEEE 802.3** 70, 203

**IGMP snooping** 95

**IGMP snooping querier** 95

**input alarm** 15

**installation instructions** 10

**interfaces, logical** 86

**interfaces, loopback** 86

**Intermediate System-to-Intermediate System.**

**See IS-IS**

**IP address**

CIP 32  
default gateway 31, 37  
DHCP 37  
NTP server 29  
static 37  
SVI 150  
switch 31, 37  
troubleshoot 261

**IP address pools** 190

**IS-IS** 93

## L

**labels, alarm** 15

**Layer 2 Network Address Translation (L2NAT)**  
231

**LC connector** 21

**LDAP**

server configuration 62  
server group configuration 63

**LED. See status indicators**

**Link Layer Discovery Protocol. See LLDP**

**LLDP** 70, 226

**llei** 242

**Logical** 86

**logical interfaces** 86

**login name**

administrator 29  
WebUI user 216

**logs, system** 254

**Long Press mode, Express Setup** 23, 28

**loopback interfaces** 86

## M

**MAC table** 80

**macros**

default global 37  
QoS 123

**management interface**

NAT 102

**management VLAN** 37, 151

**mask, subnet** 31, 32

**Medium Press mode, Express Setup** 23, 24, 27

**memory utilization** 248

**method lists, AAA** 55

**mismatch prevention, Smartports** 134

**MODBUS** 200, 237

**modes**

Access 136  
Boundary 178, 183  
CLI 172  
clock 178  
Duplex 79, 83  
End to End Transparent 178, 185  
EtherChannel 86  
Express Setup 23  
Forward 178  
PoE 203  
Program 83  
PTP 178  
STP 139  
Trunk 136  
user security 210

**modular switches** 11

**module-defined data types** 267

**modules, expansion** 11

## **monitor**

- CIP status 228
- clock settings 251
- CPU utilization 248
- DHCP clients 230
- port status 239, 241
- PTP 250
- REP 246
- status indicators 263
- switch memory 248

## **MTU 152**

## **Multi Port Configuration 82**

## **multicast services 95**

## **multimode fiber 21**

# **N**

## **NAT**

- configuration considerations 103
- configuration overview 98
- configure via Logix Designer application 113
- diagnostics 233 - 236
- management interface 102
- traffic permits and fixups 102
- translation entry types 100

## **native VLAN 79, 135**

## **neighbors 70, 226**

## **Netconf 201**

## **NetFlow 95**

## **Network Time Protocol. See NTP**

## **network, EtherNet/IP 12**

## **normally closed contacts 15**

## **normally open contacts 15**

## **NTP 177**

## **NTP server 29, 37**

# **O**

## **ODVA 12**

## **Open Shortest Path First (OSPF) Routing Protocol 98**

## **operating system**

- Express Setup 24
- requirements for WebUI 39

## **OSPF 113**

## **output alarm 15**

## **output bits 267**

# **P**

## **Parallel Redundancy Protocol (PRP) 116**

## **password**

- administrator 29
- CIP 32
- CLI 29

## **password policies 216**

## **password, administrator 37**

## **password, CIP 24, 27**

## **password, policy 66**

## **persistence, DHCP 190**

## **pin**

- DB-25 17
- DB-9 17

## **ping 258**

## **pinouts**

- DB-25 pin 17
- DB-9 pin 17
- PoE 20

## **PoE**

- about 203
- configure via Logix Designer application 206
- configure via WebUI 204
- modes 203
- pinouts 20
- power consumption 45
- requirements and restrictions 203
- status indicator 264

## **PoE ports 20**

## **policies, password 216**

## **policy password 66**

## **pools, DHCP 192**

## **pools, IP address 190**

## **pop-up blockers 39**

## **port**

- configuration 82
- states 83

## **port alarms**

- configure 165

## **port assignments for CIP data 275**

## **port channels**

- about 86
- configure 87

## **port configuration 76, 82**

## **port mirroring**

- about 140
- configure via WebUI 141
- requirements and restrictions 140

## **port numbering 277**

## **port security 80**

- about 122
- configure via Logix Designer application 122
- configure via WebUI 122, 124

## **port speed 18, 79**

## **port state 83**

## **port status indicators 266**

## **port status, monitor 239, 241**

## **port thresholds 80**

## **port types, REP 127**

## **PortFast 79**

## **ports**

- 10/100/1000 18
- BASE-T 18
- PoE 20

## **power connectors 14**

## **power consumption, PoE 45**

## **power management 204**

## **Power over Ethernet. See PoE**

## **power status indicators 264**

## **privilege levels, user 216**

## **profile, alarm**

- about 159
- configure via WebUI 161

## **Program mode 83**

**project, controller** 33  
**proxy settings** 39  
**PRP** 116  
    node and VDAN limitations 118  
    RedBox 116  
    traffic and supervisory frames 118  
**PTP**  
    configure via WebUI 183  
    monitor 250  
**PTP modes** 178  
    Boundary 183  
    End to End Transparent 185  
    Forward 178

## Q

**QoS**  
    about 123  
    configure via WebUI 124  
    macros 123  
    settings 37  
**Quality of Service. See QoS**  
**querier, IGMP snooping** 95

## R

**RADIUS**  
    fallback 65  
    server configuration 58  
    server group configuration 59  
**rapid commit** 152  
**RedBox** 116  
**relay** 15  
**reload configuration** 168  
**REP**  
    about 127  
    administrative VLAN 127  
    configure via WebUI 128  
    default configuration 127  
    monitor 246  
    port types 127  
    segment 129  
**requirements**  
    Express Setup 24  
    WebUI 39  
**Resiliency Ethernet Protocol. See REP**  
**restart with factory default settings** 28  
**restore configuration** 166, 169  
**roles, Smartport** 134  
**routing, static**  
    configure via WebUI 130  
**routing,static** 130  
**run CLI commands** 172

## S

**schematics, cable** 19  
**screen resolution**  
    Express Setup 24  
    requirements for WebUI 39  
**SD card**  
    sync with configuration 168, 169  
**SD flash** 169, 170

**security, port** 80, 122  
**segment, REP** 129  
**server**  
    DNS 188, 189  
    NTP 29, 37  
**server configuration**  
    LDAP 62  
    RADIUS 58  
    TACACS+ 60  
**server group configuration**  
    LDAP 63  
    RADIUS 59  
    TACACS+ 61  
**services, multicast** 95  
**set switch IP address** 31  
**settings**  
    date and time 29  
    factory default 28  
**Setup status indicator** 264  
**SFP modules** 21  
**SFP slots** 21  
**Short Press mode, Express Setup** 23, 24, 26  
**Simple Network Management Protocol. See SNMP**  
**singlemode fiber** 21  
**slots, SFP** 21  
**Smartports**  
    about 134  
    assign via Logix Designer application 137  
    assign via WebUI 135  
    custom roles 137  
    mismatch prevention 134  
    requirements and restrictions 134  
    roles 134  
    VLAN types 135  
**SNMP**  
    about 210  
    community strings 212  
    configure via WebUI 210  
    hosts 214  
    supported versions 210  
    traps 211  
**SNMPv3** 210, 213  
**snooping, DHCP** 191  
**snooping, IGMP** 95  
**software comparison** 12  
**software features** 12  
**software upgrade** 215  
**software, configuration** 12  
**SPAN**  
    about 140  
    configure via WebUI 141  
    requirements and restrictions 140  
**Spanning Tree Protocol. See STP**  
**specifications, switch** 10  
**speed**  
    about 18  
    configure 79, 83  
    troubleshoot 262  
**SSH** 32  
**static IP address** 31, 37  
**static MAC table** 80



## **static routing**

- about 130
- configure via WebUI 130

## **status indicators**

- alarm 265
- EIP Mod 265
- EIP Net 265
- front panel 263
- PoE 264
- port 266
- power 264
- setup 264

## **storm**

- broadcast 80
- unicast 80

## **STP**

- about 138
- configure via Logix Designer application 140
- configure via WebUI 139
- modes 139
- requirements and restrictions 138

## **straight-through cable** 19

## **subnet mask** 31, 32

## **subnet translation** 101, 110

## **supported SFP modules** 21

## **SVI** 150, 152

## **switch**

- installation instructions 10
- IP address 37
- setup 23
- specifications 10
- status 225
- troubleshoot 260, 261

## **switched port analyzer. See SPAN**

## **switches, fixed** 11

## **switches, modular** 11

## **sync configuration with SD card** 169

## **sync interval** 184

## **sync limit** 184

## **system logs** 254

## **system report** 256

# **T**

## **TACACS+ server configuration** 60

## **TACACS+ server group configuration** 61

## **Telnet** 31

## **temperature of device** 45

## **thresholds, port** 80

## **time**

- CIP Sync 178, 183
- configure via Logix Designer application 183
- configure via WebUI 178, 183
- PTP 183
- set manually 177, 179
- set via NTP 177
- set via PTP 180
- via PTP 178

## **time sync information**

- view via Logix Designer application 185

## **TLV structures** 71

## **toolbar, WebUI** 43

## **trace route** 258

## **traffic fixups and NAT** 102

## **traffic permits and NAT** 102

## **translation entry types** 100

## **traps, SNMP** 211

## **troubleshoot**

- core dump 256
- debug bundle 257
- DHCP 261
- IP address problems 261
- ping and trace route 258
- speed, duplex, and autonegotiation 262
- status indicators 263
- switch performance 262
- system logs 254
- system report 256
- WebUI 262
- wrong IP address 261

## **trunk port** 79, 88, 136

## **trustpoints** 200

## **TrustSec** 142

# **U**

## **unicast storm** 80

## **upgrade software** 215

## **USB device driver** 16

## **USB-mini console** 16

## **user administration** 216

## **user authentication** 210

## **user name, administrator** 37

## **user password policies** 216

## **user privilege levels** 216

## **user security modes** 210

## **users**

- authenticate 49
- authorize 49
- SNMPv3 213
- WebUI accounts 216

# **V**

## **V3 User Groups** 213

## **virtual local area network. See VLAN**

## **VLAN**

- about 150
- access 79
- allowed 79
- CIP 32
- configure via Logix Designer application 154
- configure via WebUI 151
- for Smartports 135
- management 31, 37, 151
- native 79
- REP administrative 127
- support 150
- trunking protocol 156

## **VLAN Trunking Protocol. See VTP**

## **VLANs**

- assign to NAT instance 101, 109

## **voice VLAN** 135

## **VTP**

- about 156
- configure via WebUI 157

---

## W

### WebUI

- AAA wizard 50
- access 40
- dashboard 45
- preferences 44
- requirements 39
- toolbar 43
- troubleshoot 262
- user accounts 216

### WebUI wizard 50

**wire alarm connector** 15

**wizard, AAA** 50





# Rockwell Automation Support

Use these resources to access support information.

<b>Technical Support Center</b>	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	<a href="http://rok.auto/support">rok.auto/support</a>
<b>Knowledgebase</b>	Access Knowledgebase articles.	<a href="http://rok.auto/knowledgebase">rok.auto/knowledgebase</a>
<b>Local Technical Support Phone Numbers</b>	Locate the telephone number for your country.	<a href="http://rok.auto/phonesupport">rok.auto/phonesupport</a>
<b>Literature Library</b>	Find installation instructions, manuals, brochures, and technical data publications.	<a href="http://rok.auto/literature">rok.auto/literature</a>
<b>Product Compatibility and Download Center (PCDC)</b>	Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes.	<a href="http://rok.auto/pcdc">rok.auto/pcdc</a>

## Documentation Feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at [rok.auto/docfeedback](http://rok.auto/docfeedback).

## Waste Electrical and Electronic Equipment (WEEE)



At the end of life, this equipment should be collected separately from any unsorted municipal waste.

Rockwell Automation maintains current product environmental compliance information on its website at [rok.auto/pec](http://rok.auto/pec).

Allen-Bradley, expanding human possibility, FactoryTalk Network Manager, Integrated Architecture, Logix 5000, Rockwell Automation, Rockwell Software, Stratix, and Studio 5000 Logix Designer are trademarks of Rockwell Automation, Inc.





CIP, CIP Sync, ControlNet, DeviceNet, and EtherNet/IP are trademarks of ODVA, Inc.

Cisco and Cisco Systems are trademarks of Cisco Systems, Inc.

Microsoft is a trademark of Microsoft Corporation.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, İçerenköy, İstanbul, Tel: +90 (216) 5698400 EEE Yönetmeliğine Uygundur

Connect with us.    

**rockwellautomation.com** — expanding **human possibility**™

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1783-UM012E-EN-P - March 2021

Supersedes Publication 1783-UM012D-EN-P - December 2020

Copyright © 2021 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.