Moxa Managed Switch TSN-G5000 Series
User Manual

Version 2.5, December 2025

www.moxa.com/products

Moxa Managed Switch TSN-G5000 Series User Manual

Copyright Notice

Trademarks

Disclaimer

- Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.
- Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.
- Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.
- This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. About This Manual

Thank you for purchasing Moxa's managed switch. Read this user's manual to learn how to connect your Moxa switch with various interfaces and how to configure all settings and parameters via the user-friendly web interface.

Three methods can be used to connect to the Moxa's switch, which all will be described in the next two chapters. See the following descriptions for each chapter's main functions.

Chapter 2: Getting Started

In this chapter, we explain the instruction on how to initialize the configuration on Moxa's switch. We provide three interfaces to access the configuration settings: RS-232 console interface, telnet interface, and web interface.

Chapter 3: Web Interface Configuration

In this chapter, we explain how to access a Moxa switch's various configuration, monitoring, and management functions. The functions can be accessed by web browser. We describe how to configure the switch functions via web interface, which provides the most user-friendly way to configure a Moxa switch.

Appendix A: Account Privileges List

This appendix describes the read/write access privileges for different accounts on Moxa's Managed Ethernet Series switch.

Appendix B: Event Log Description

In this appendix, users can check the event log name and its event log description. When any event occurs, this appendix helps users quickly check the detailed definition for each event.

Appendix C: SNMP MIB File

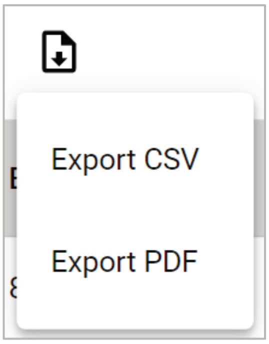
This appendix contains the SNMP MIB files so that users can manage the entities in a network with Moxa's switch.

Symbols for the Meanings in the Web Interface Configurations

The Web Interface Configuration includes various symbols. For your convenience, refer to the following table for the meanings of the symbols.

Symbols	Meanings
+	Add
▤	Read detailed information
≡	Clear all
≡✓	Column selection
↻	Refresh
💾	Enable/Disable Auto Save When Auto Save is disabled, users need to click this icon to save the configurations.
🗎	Export*
✎	Edit
🔄	Re-authentication
🗑	Delete
⛶	Panel View
∨	Expand
∧	Collapse
ⓘ	Hint Information
🎚	Settings
⇄	Data Comparison
⋮	Menu icon
🎓	Change mode
⌖	Locator
⏻	Reboot
⟲	Reset to default
⇥	Logout
↑	Increase
↓	Decrease
⇵	Equal
☰	Menu
🔍	Search

*The **Export** function helps users save the current configurations or information for the specific functions. It is located on the upper part of the configuration area. There are two formats available: **CVS**, or **PDF**. Select the format and save in your local computer.



About Note, Attention, and Warning

Throughout the whole manual, users will see some notes, attentions, and warnings. Here are the explanations for each definition.

Note: It indicates the additional explanations for the situation that users might encounter. Here is the example:

NOTE

By default, the password assigned to the Moxa switch is moxa. Be sure to change the default password after you first log in to help keep your system secure.

Attention: It indicates the situations where users might take some extra care or it might bring some problems. Here is the example:

ATTENTION

When a different type of module has been inserted into the switch, we suggest you configure the settings, or use reset-to-default.

Warning: It indicates the situations where users need to pay particular attention to, or it might bring serious damage to the system or the switch. Here is an example:

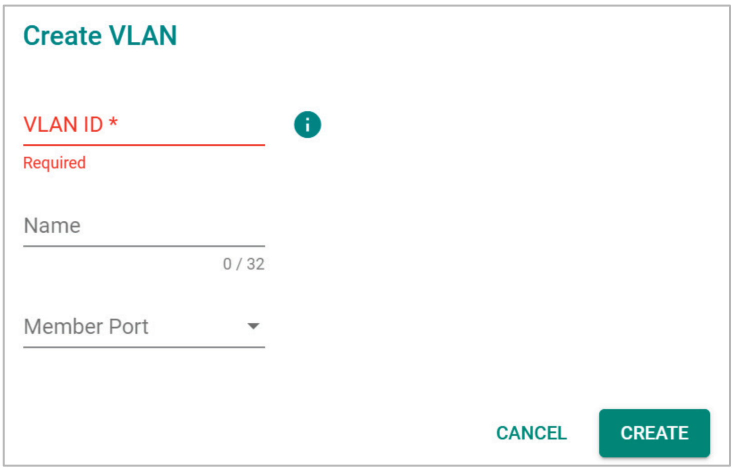
WARNING

There is a risk of explosion if the battery is replaced by an incorrect type.

Configuration Reminders

In this section, several examples will be used to remind users when configuring the settings for Moxa's switch.

A: About Mandatory Parameters



Create VLAN

VLAN ID *

Required

Name

0 / 32

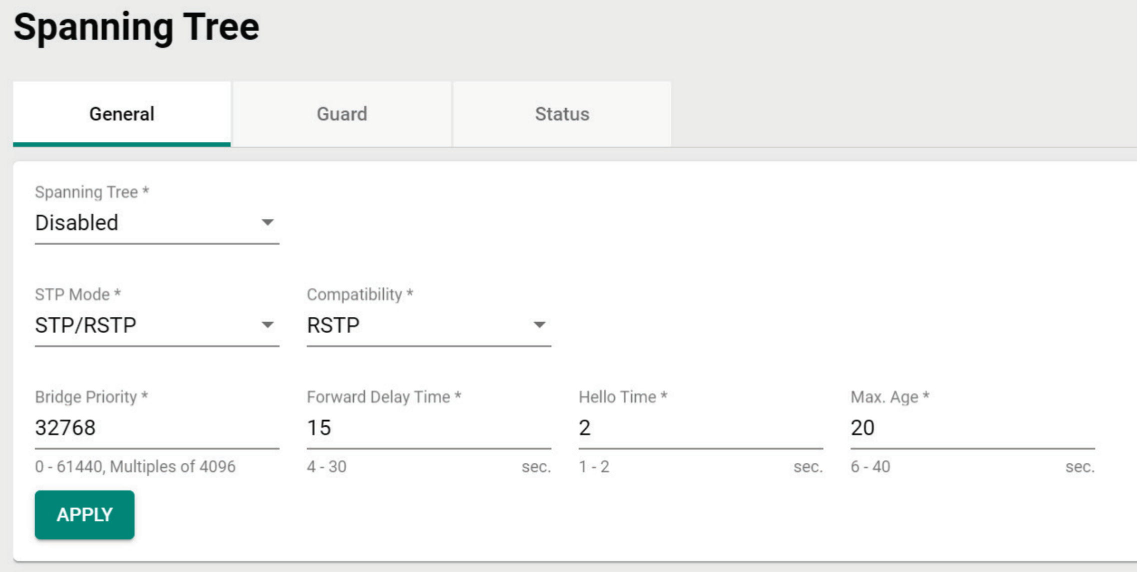
Member Port

1. The items with asterisks mean they are mandatory parameters that must be provided. In the figure above, the parameters for VLAN, Version, and Query Interval all need to be provided, or it will not be created or applied.
2. If the item is marked with red it means this item has been skipped. You need to fill in the parameters or you cannot apply or create the function.

In addition, some parameter values will be limited to a specific range. If the values exceed the range, it cannot be applied or created.

B: Configurations before Enable/Disable

In another situation, some settings can be configured first, but remain disabled. Users can decide to enable them when necessary without configuring the same settings again. This is particularly convenient and user-friendly when configuring various settings. For example, in Spanning Tree configuration page, users can configure the Guard settings first, but later select to disable the Guard settings in the **General** tab. When users decide to enable the Guard settings, they only need to select **Enable** in General settings, so that the Guard setting can be enabled at the same time.



Spanning Tree

Spanning Tree *
Disabled

STP Mode *
STP/RSTP

Compatibility *
RSTP

Bridge Priority *
32768
0 - 61440, Multiples of 4096

Forward Delay Time *
15
4 - 30 sec.

Hello Time *
2
1 - 2 sec.

Max. Age *
20
6 - 40 sec.

2. Getting Started

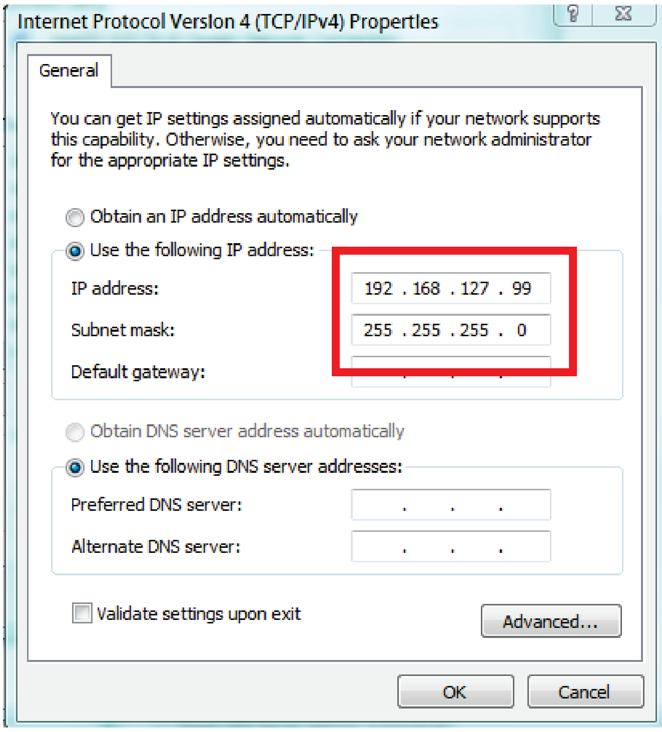
In this chapter, we explain how to log in a Moxa's switch for the first time. There are three ways to access the Moxa switch's configuration settings: RS-232 console, or web-based interface.

Log In Via Web Interface

You can directly connect Moxa's switch to your computer with a standard network cable or install your computer at the same intranet as your switch. Then you need to configure your computer's network setting. The default IP address for the Moxa's switch is:

192.168.127.253

For example, you can configure the computer's IP setting as **192.168.127.99**, and the subnet mask as 255.255.255.0.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 127 . 99

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

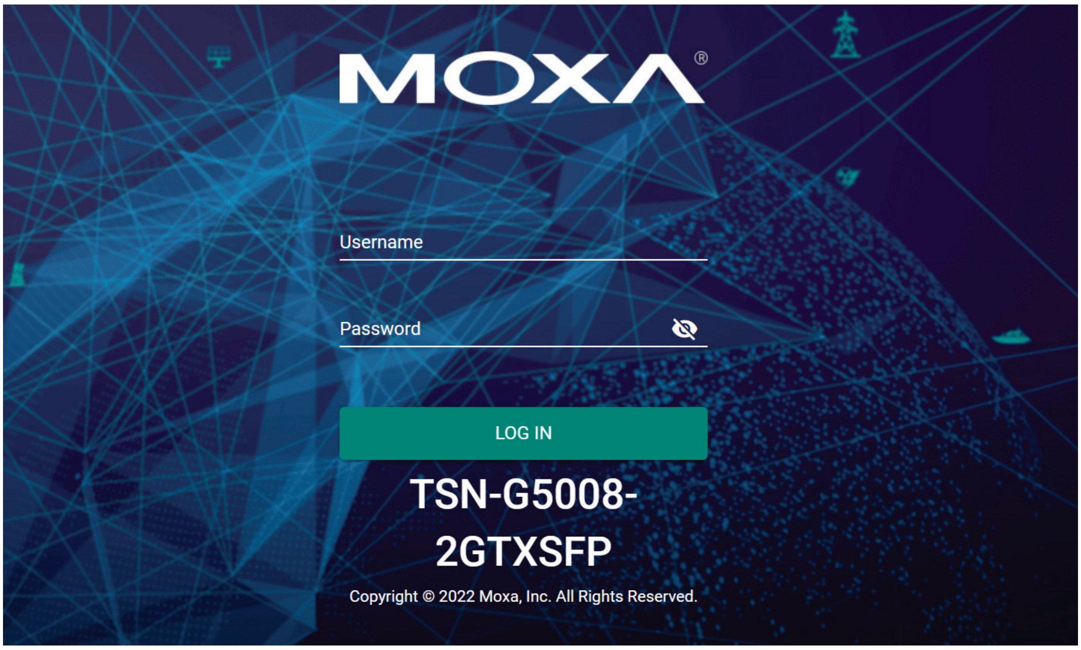
□ Validate settings upon exit

Click **OK** when finished.

Connecting to the Switch

Open a browser, such as Google Chrome, and connect to the following IP address:

http://192.168.127.253



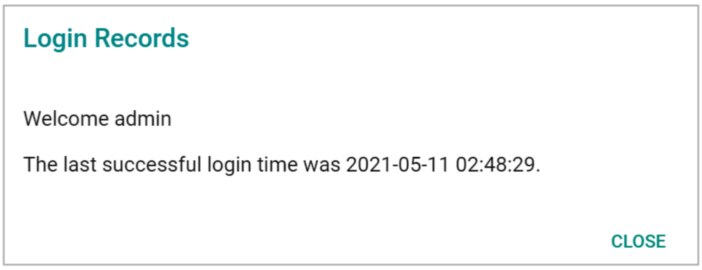
TSN-G5008-2GTXSFP

Copyright © 2022 Moxa, Inc. All Rights Reserved.

The default username and password are:

Username: **admin**
Password: **moxa**

Click **LOG IN** to continue. If you have logged in before, you will see a screen indicating the previous login information. Click **CLOSE**.

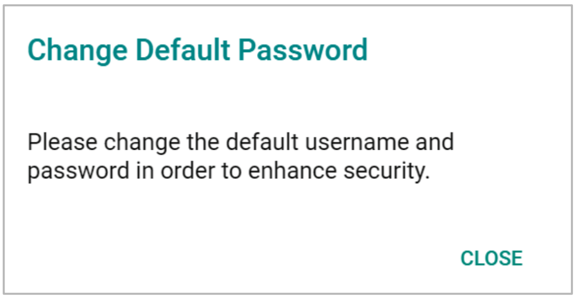


Login Records

Welcome admin

The last successful login time was 2021-05-11 02:48:29.

Another system message will appear, reminding you to change the default password. We recommend you change your password, or a message will appear whenever you log in. You can change the password in the **Account Management** section. Click **CLOSE** to continue.



Change Default Password

Please change the default username and password in order to enhance security.

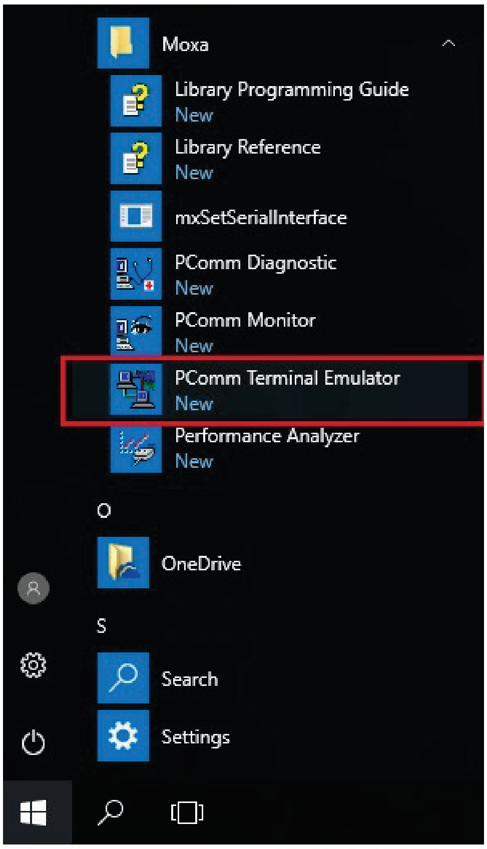
Log In Via RS-232 Console

The Moxa's managed switch offers a serial console port, allowing users to connect to the switch and configure the settings. Do the following steps for the serial connection and configuration.

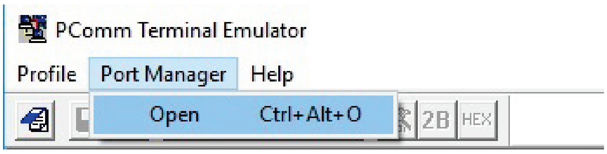
1. Prepare an RS-232 serial cable with an RJ45 interface.
2. Connect the RJ45 interface end to the console port on the switch, and the other end to the computer.
3. We recommend you use **PComm Terminal Emulator** for serial communication. The software can be downloaded free of charge from Moxa's website.

After installing PComm Terminal Emulator, open the Moxa switch's console as follows:

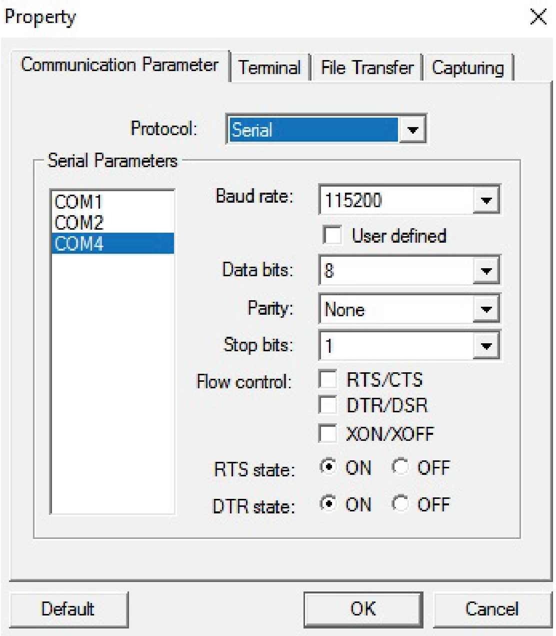
1. From the Windows desktop, click **Start > Moxa > PComm Terminal Emulator**.



2. Select **Open** under the **Port Manager** menu to open a new connection.



3. The **Property** window should open. On the **Communication Parameter** tab for **Ports**, select the COM port that is being used for the console connection. Set the other fields as follows: **115200** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits**.



Protocol: Serial

Serial Parameters

COM1
COM2
COM4

Baud rate: 115200

□ User defined

Data bits: 8

Parity: None

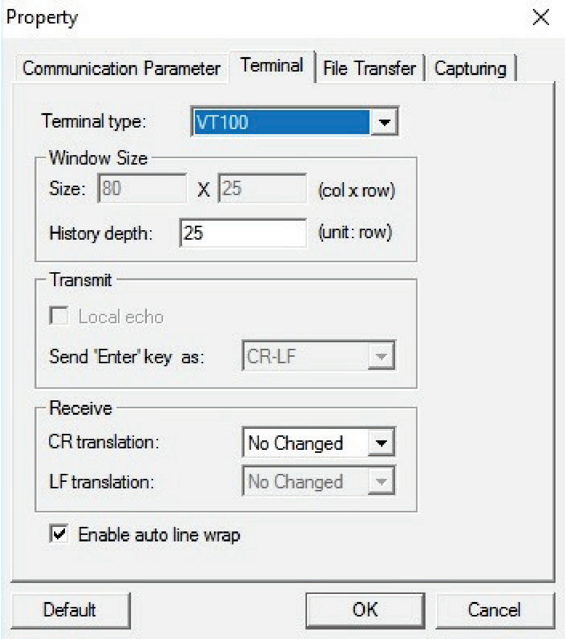
Stop bits: 1

Flow control: □ RTS/CTS □ DTR/DSR □ XON/XOFF

RTS state: ● ON ○ OFF

DTR state: ● ON ○ OFF

4. On the **Terminal** tab, select **VT100** for **Terminal Type**, and then click **OK** to continue.



Terminal type: VT100

Window Size

Size: 80 X 25 (col x row)

History depth: 25 (unit: row)

Transmit

□ Local echo

Send 'Enter' key as: CR-LF

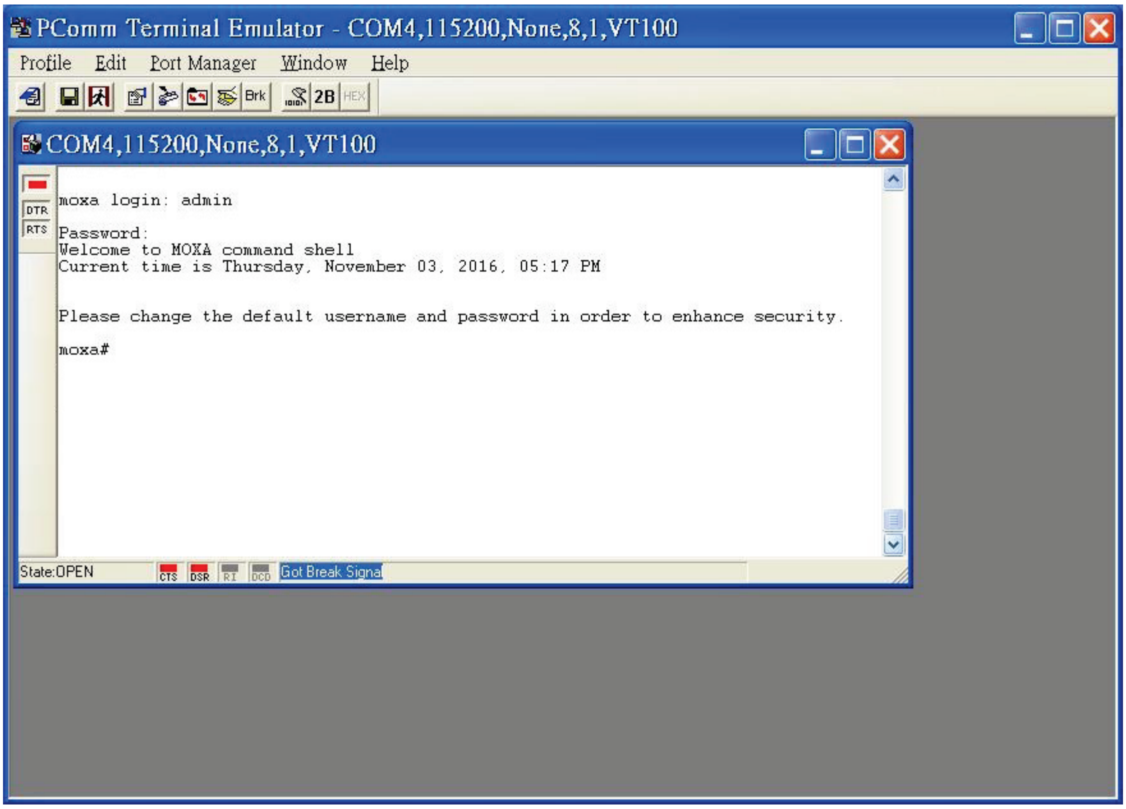
Receive

CR translation: No Changed

LF translation: No Changed

☑ Enable auto line wrap

5. The console will prompt you to log in. The default login name is **admin**, and the default password is **moxa**. This password will be required to access any of the consoles (web, serial, Telnet).



```
moxa login: admin

Password:
Welcome to MOXA command shell
Current time is Thursday, November 03, 2016, 05:17 PM

Please change the default username and password in order to enhance security.

moxa#
```

6. After successfully connecting to the switch by serial console, users can start configuring the switch parameters by using command line instructions. Refer to the **Moxa Command Line Interface Manual**.

NOTE

By default, the password assigned to the Moxa switch is **moxa**. Be sure to change the default password after you first log in to help keep your system secure.

Log In Via Telnet

Opening the Moxa switch’s Telnet or web console over a network requires that the PC host and Moxa switch are on the same logical subnet. You might need to adjust your PC host’s IP address and subnet mask. By default, the Moxa switch’s IP address is 192.168.127.253 and the Moxa switch’s subnet mask is 255.255.255.0. Your PC’s IP address must be set to 192.168.xxx.xxx if the subnet mask is 255.255.0.0, or to 192.168.127.xxx if the subnet mask is 255.255.255.0.

NOTE

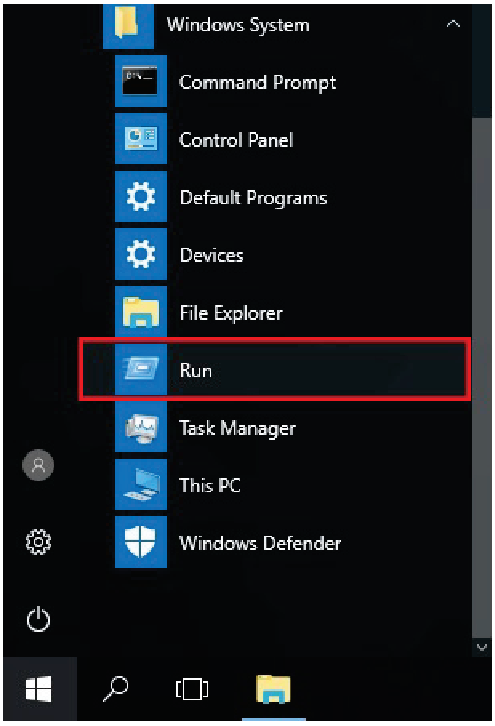
When connecting to the Moxa switch’s Telnet or web console, first connect one of the Moxa switch’s Ethernet ports to your Ethernet LAN, or directly to your PC’s Ethernet port. You can use either a straight-through or cross-over Ethernet cable.

NOTE

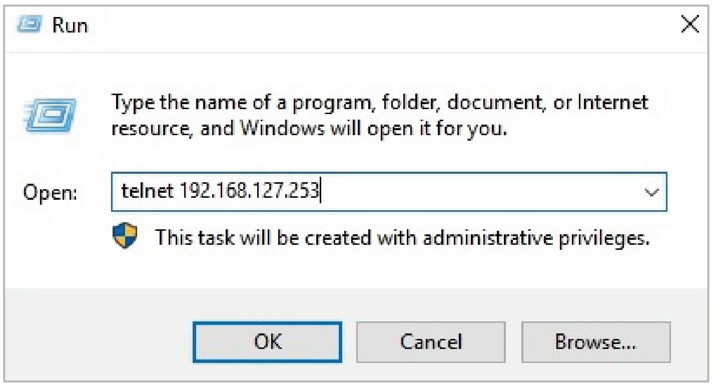
The Moxa switch’s default IP address is 192.168.127.253.

After making sure that the Moxa switch is connected to the same LAN and logical subnet as your PC, open the Moxa switch’s Telnet console as follows:

1. Click **Start > Run** from the Windows Start menu and then Telnet to the Moxa switch’s IP address from the Windows **Run** window. You can also issue the Telnet command from a DOS prompt.



2. Next, use Telnet to connect the Moxa switch’s IP address (192.168.127.253) from the Windows **Run** window. You can also issue the Telnet command from a DOS prompt.

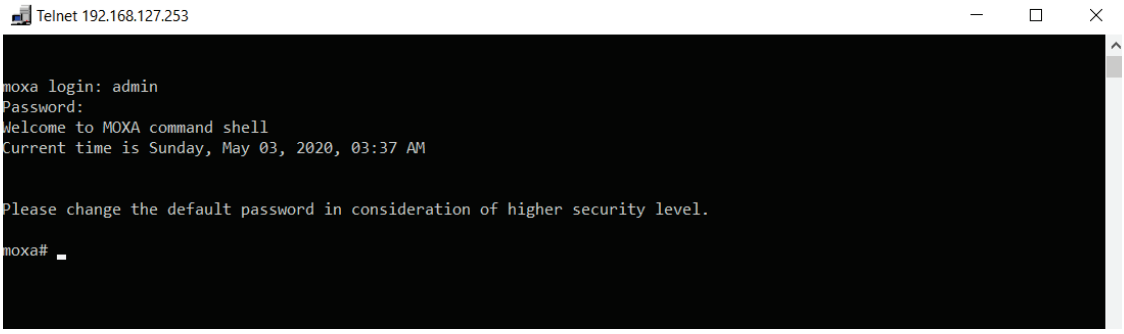


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: telnet 192.168.127.253

This task will be created with administrative privileges.

3. The Telnet console will prompt you to log in. The default login name is **admin**, and the password is **moxa**. This password will be required to access any of the consoles (web, serial, Telnet).



```
moxa login: admin
Password:
Welcome to MOXA command shell
Current time is Sunday, May 03, 2020, 03:37 AM


Please change the default password in consideration of higher security level.

moxa#
```

4. After successfully connecting to the switch by Telnet, users can start configuring the switch parameters by using command line instructions. Refer to the **Moxa Command Line Interface Manual**.

NOTE

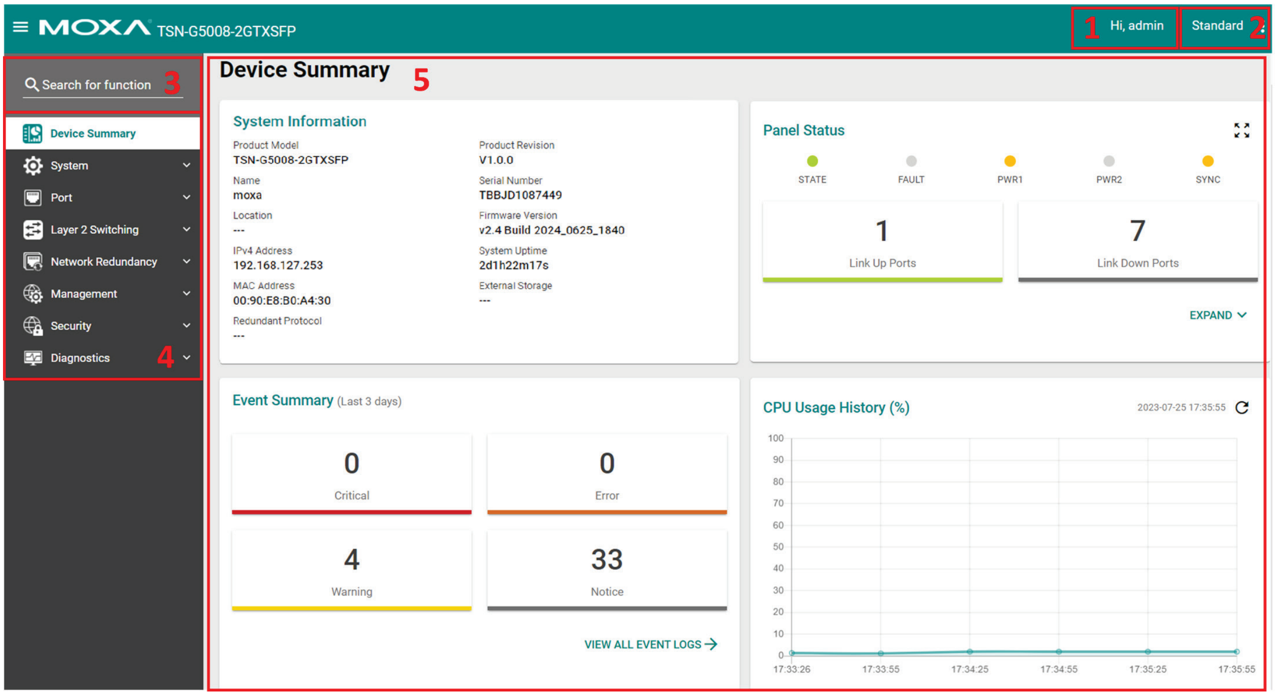
By default, the password assigned to the Moxa switch is **moxa**. Be sure to change the default password after you first log in to help keep your system secure.

3. Web Interface Configuration

Moxa’s managed switch offers a user-friendly web interface for easy configurations. Users find it simple to configure various settings over the web interface. All configurations for the Moxa’s managed switch can be easily set up and done via this web interface, essentially reducing system maintenance and configuration effort.

Function Introduction

This section describes the web interface design, providing a basic visual concept for users to understand the main information or configuration menu for the web interface pages.



System Information

Product Model: TSN-G5008-2GTXSFP
Product Revision: V1.0.0
Name: moxa
Serial Number: TBBJD1087449
Location: ---
Firmware Version: v2.4 Build 2024_0625_1840
IPv4 Address: 192.168.127.253
System Uptime: 2d1h22m17s
MAC Address: 00:90:E8:B0:A4:30
External Storage: ---
Redundant Protocol: ---

Panel Status

STATE, FAULT, PWR1, PWR2, SYNC

1 Link Up Ports
7 Link Down Ports

EXPAND

Event Summary (Last 3 days)

0 Critical
0 Error
4 Warning
33 Notice

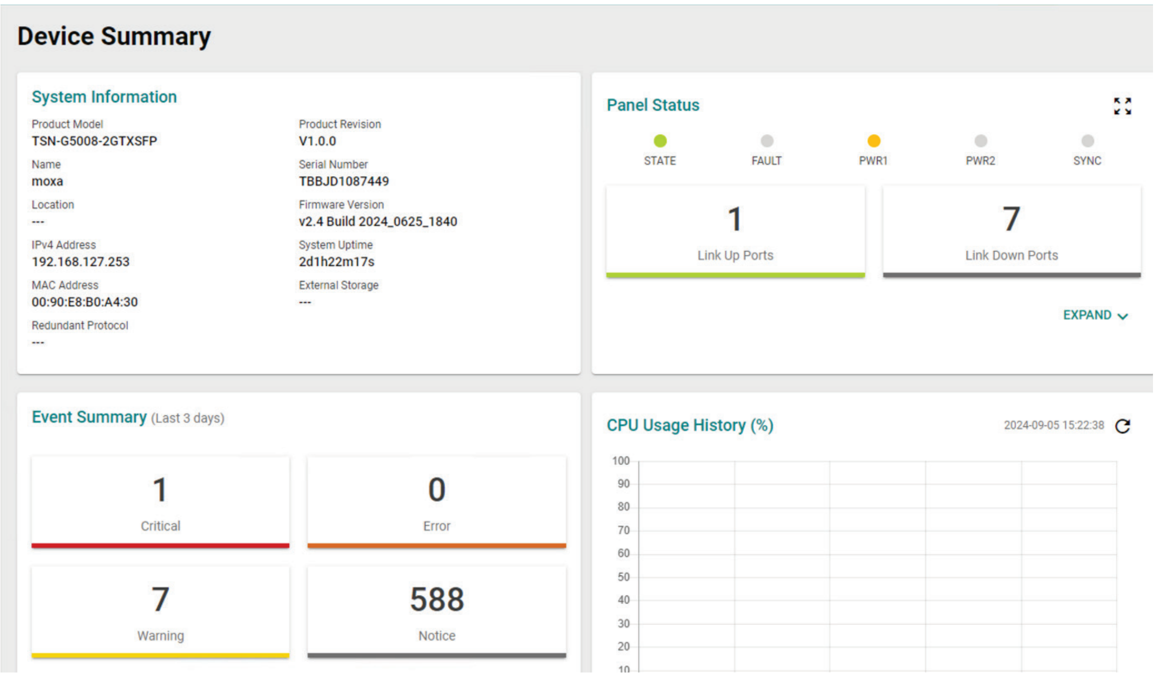
VIEW ALL EVENT LOGS →

CPU Usage History (%) 2023-07-25 17:35:55

1. **Login Name:** It shows the role of the login name.
2. **Configuration Mode**: Two modes are supported: **Standard Mode** and **Advanced Mode.**
   - **Standard Mode:** Some of the features and parameters will be hidden to make the configurations simpler (default).
   - **Advanced Mode:** All features and parameters will be available for users to configure detailed settings.
3. **Search Bar:** Type the name of the function you want to search for in the function menu tree.
4. **Function Menu:** All functions of the switch are shown here. Click the function you want to view or configure.
5. **Device Summary:** All important device and function information will be shown here.

Device Summary

After successfully connecting to the switch, the **Device Summary** will automatically appear. You can view the whole web interface on the screen. If you are in the middle of performing configurations, simply click **Device Summary** from the function menu and you can view the detailed information of the switch.



Device Summary

System Information

Product Model
TSN-G5008-2GTXSFP

Name
moxa

Location

IPv4 Address
192.168.127.253

MAC Address
00:90:E8:B0:A4:30

Redundant Protocol

Product Revision
V1.0.0

Serial Number
TBBJD1087449

Firmware Version
v2.4 Build 2024_0625_1840

System Uptime
2d1h22m17s

External Storage

Panel Status

1
Link Up Ports

7
Link Down Ports

Event Summary (Last 3 days)

1
Critical

0
Error

7
Warning

588
Notice

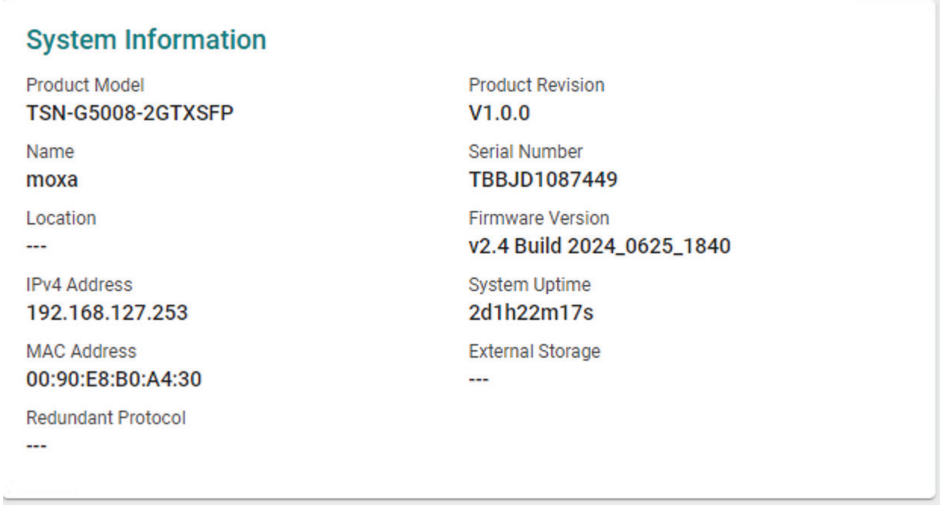
CPU Usage History (%)

2024-09-05 15:22:38

See the following sections for detailed descriptions for the specific items.

System Information

This shows the system information, including the product model name, serial number, firmware version, system uptime, etc.



System Information

Product Model
TSN-G5008-2GTXSFP

Name
moxa

Location

IPv4 Address
192.168.127.253

MAC Address
00:90:E8:B0:A4:30

Redundant Protocol

Product Revision
V1.0.0

Serial Number
TBBJD1087449

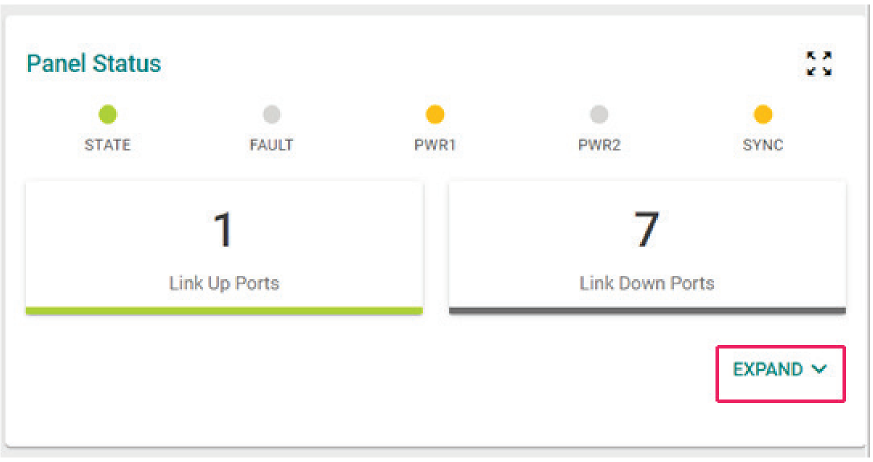
Firmware Version
v2.4 Build 2024_0625_1840

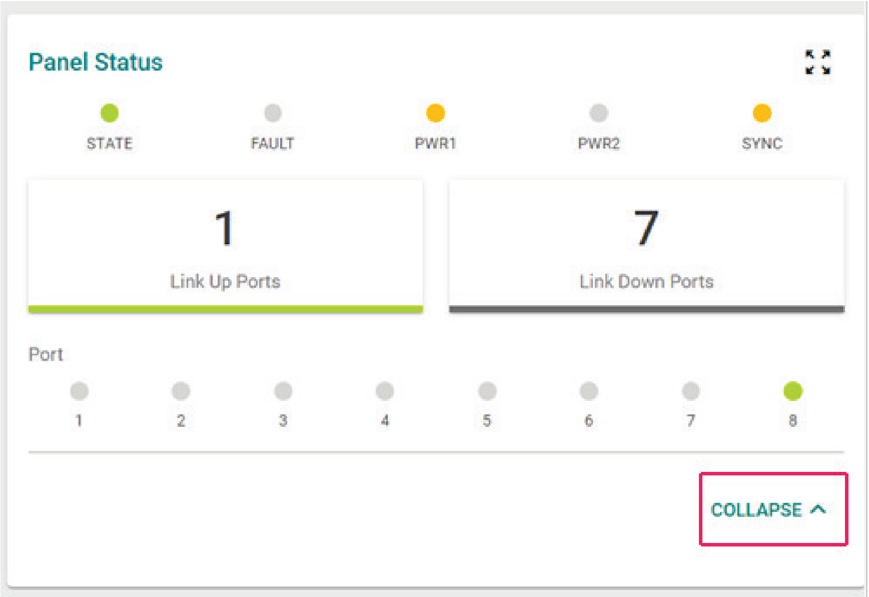
System Uptime
2d1h22m17s

External Storage

Panel Status

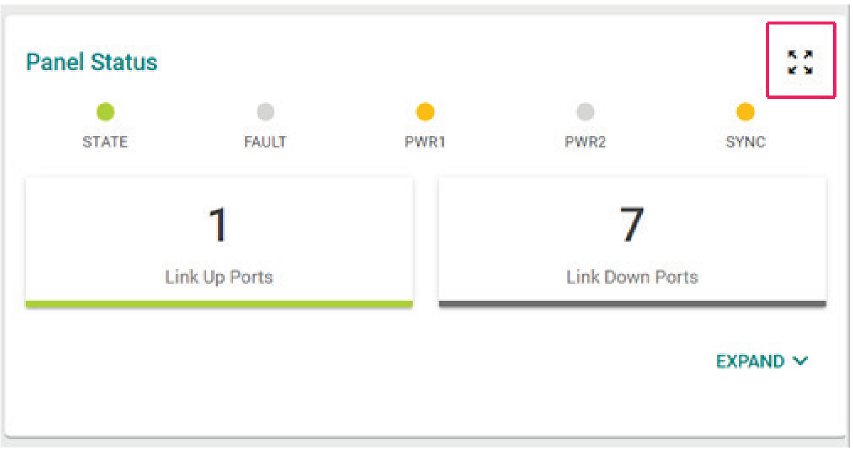
This section illustrates the panel status. For example, the connecting ports will be shown in green, while the disconnected ports will be shown in gray. Click **EXPAND** to view more detailed information on the panel status and click **COLLAPSE** to return.





Panel View

By clicking this icon, ⛶, users can view the device port status through a visual representation of the device. Click the close icon on the upper-right corner to return to the main page.

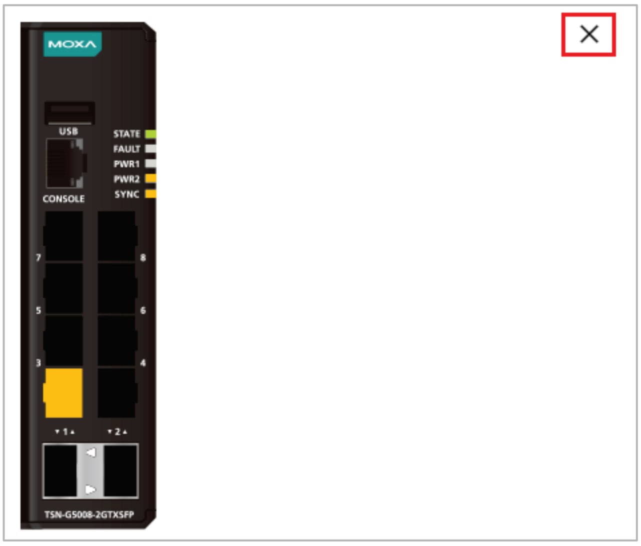


Panel Status

● STATE ● FAULT ● PWR1 ● PWR2 ● SYNC

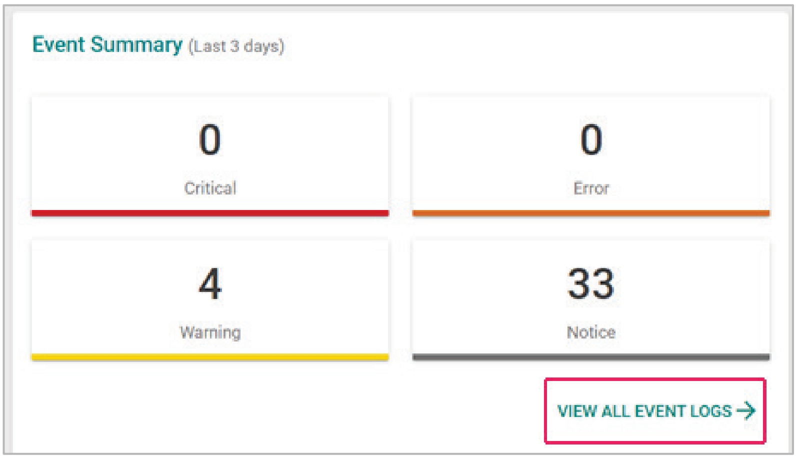
1	7
Link Up Ports	Link Down Ports

The panel image will differ depending on the model used. The following panel view shows the TSN-G5008-2GTXSFP.

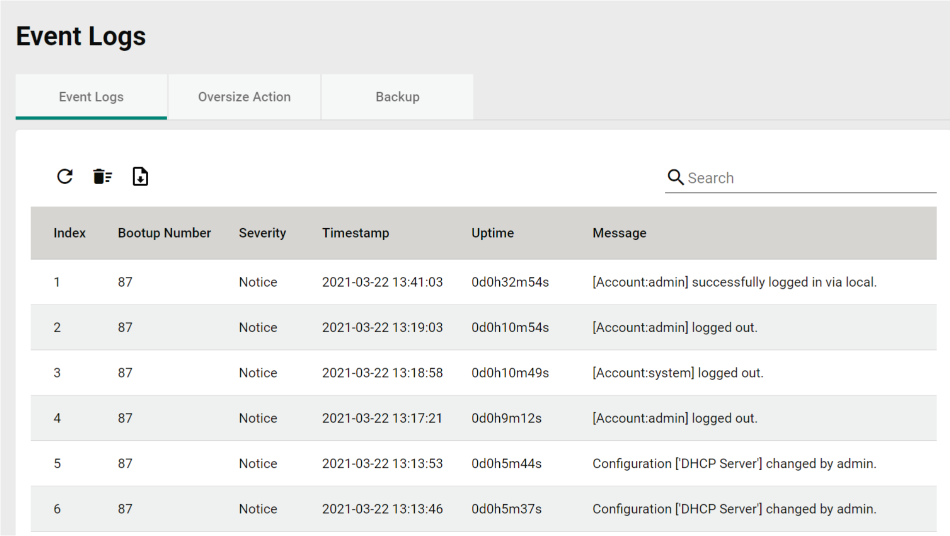


Event Summary (Last 3 Days)

This section shows the event summary for the past three days.



Click **VIEW ALL EVENT LOGs** to go to the Event Logs page, where you can view all event logs.

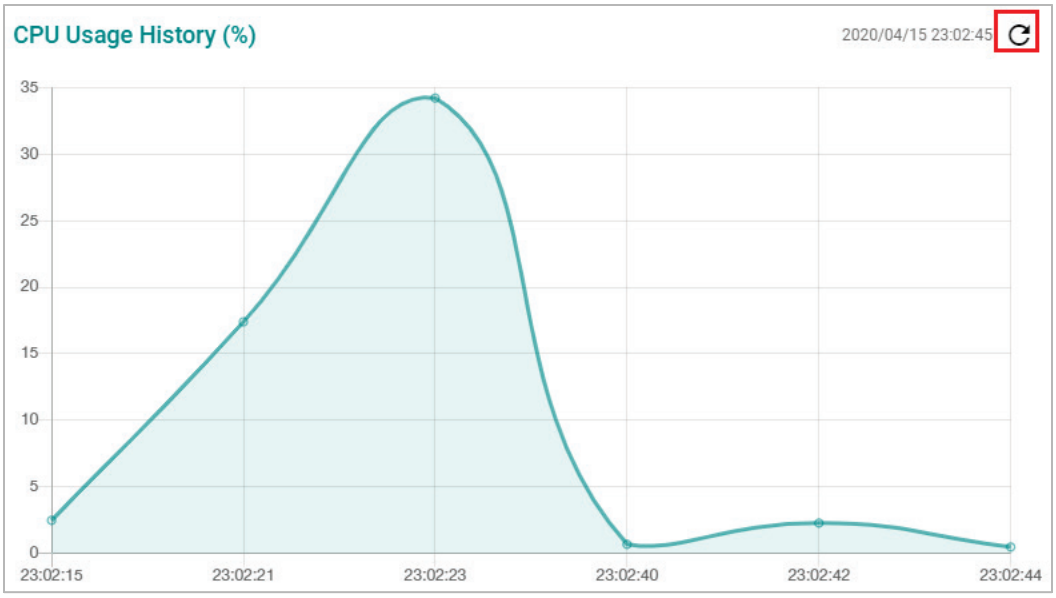


Index	Bootup Number	Severity	Timestamp	Uptime	Message
1	87	Notice	2021-03-22 13:41:03	0d0h32m54s	[Account:admin] successfully logged in via local.
2	87	Notice	2021-03-22 13:19:03	0d0h10m54s	[Account:admin] logged out.
3	87	Notice	2021-03-22 13:18:58	0d0h10m49s	[Account:system] logged out.
4	87	Notice	2021-03-22 13:17:21	0d0h9m12s	[Account:admin] logged out.
5	87	Notice	2021-03-22 13:13:53	0d0h5m44s	Configuration ['DHCP Server'] changed by admin.
6	87	Notice	2021-03-22 13:13:46	0d0h5m37s	Configuration ['DHCP Server'] changed by admin.

For event log settings, refer to the Event Logs section.

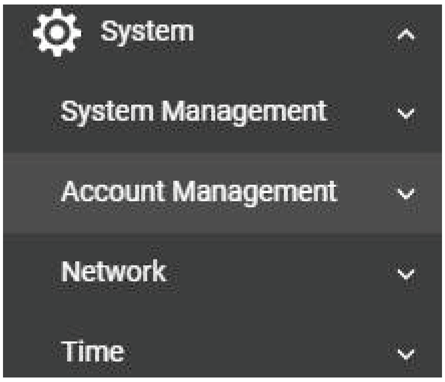
CPU Usage History

This section shows the CPU usage. The data will be shown as a percentage over time. Click the refresh icon on the page to show the latest information.



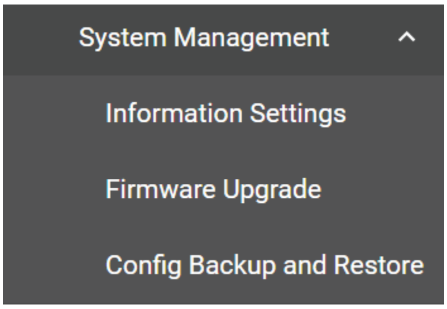
System

From the **System** section in the function menu you can configure **System Management, Account Management, Network,** and **Time** settings.



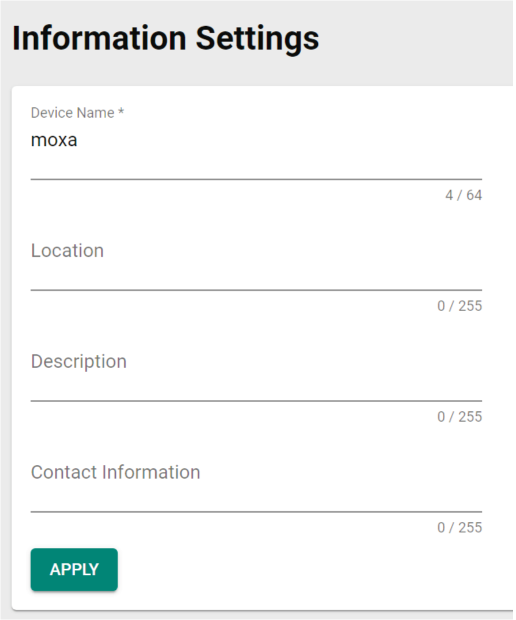
System Management

From the **System Management** section you can configure three functions: **Information Settings, Firmware Upgrade,** and **Config Backup and Restore.**



Information Settings

Define **Information Settings** items to make it easier to identify different switches that are connected to your network.



Information Settings

Device Name *
moxa
4 / 64

Location
0 / 255

Description
0 / 255

Contact Information
0 / 255

Device Name

Setting	Description	Factory Default
1 to 64 characters	This option is useful for differentiating between the roles or applications of different units. Note that the device name cannot be empty.	moxa

NOTE

The device name should not start with –(dash) and should not end with –(dash).

In addition, the device name cannot use the following format:

Port-xxx or Port-xxx-xxxxx

The x is used to denote any number. All other variations are allowed.

Location

Setting	Description	Factory Default
Max. 255 characters	This option is for differentiating between the locations of different switches. Example: production line 1.	None

Description

Setting	Description	Factory Default
Max. 255 characters	This option is for recording a more detailed description of the unit.	None

Contact Information

Setting	Description	Factory Default
Max. 255 characters	Users can input contact information such as email address, or telephone number when problems occur.	None

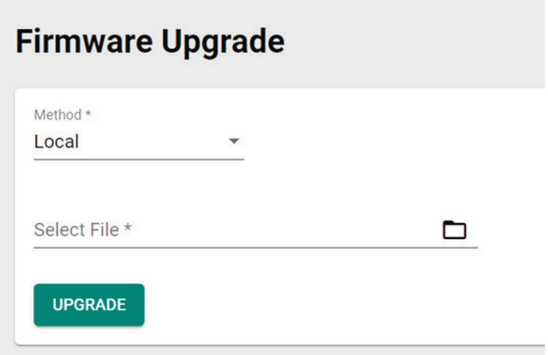
When finished, click **APPLY** to save your changes.

Firmware Upgrade

This section describes how to upgrade your Moxa switch’s firmware.

NOTE

After updating the firmware, refresh or reconnect to the web service to make sure your browser has the latest data.



Firmware Upgrade

Method * Local

Select File *

Method

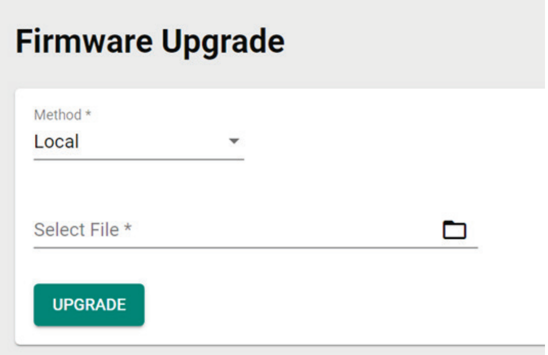
Setting	Description	Factory Default
Select from the drop-down list	Specify whether to update the firmware from a local *.rom file, through a remote SFTP server, a remote TFTP server, a USB, or a microSD device.	Local

Upgrade Locally

Users can upgrade firmware from a local *.rom file. Select **Local** from the drop-down list under **Method**.

NOTE

This method requires users to first download the updated firmware file (.rom) from www.moxa.com.



Firmware Upgrade

Method * Local

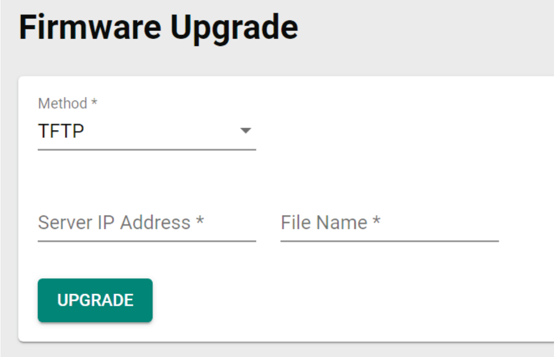
Select File *

Select File

Click the Browse button and navigate to the firmware file on the local machine. With the file selected, click **UPGRADE** to perform the firmware upgrade.

Upgrade Via TFTP

Users can upgrade firmware via a remote TFTP server. Select **TFTP** from the drop-down list under **Method**.



Firmware Upgrade

Method *
TFTP

Server IP Address *

File Name *

Server IP Address

Setting	Description	Factory Default
IP address	Enter the IP address of the TFTP server where the new firmware file (*.rom) is located.	None

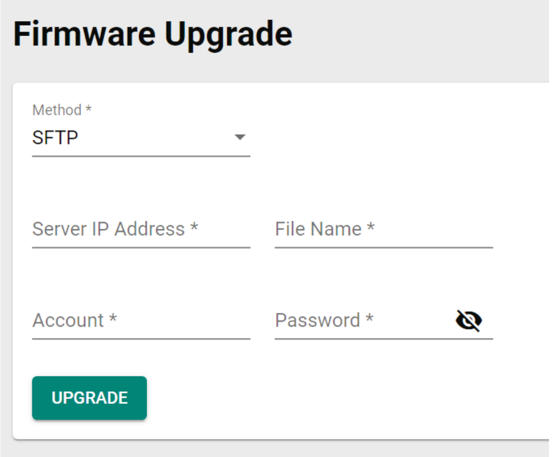
File Name

Setting	Description	Factory Default
Filename	Enter the filename of the new firmware.	None

When finished, click **UPGRADE** to perform the firmware upgrade.

Upgrade Via SFTP

Users can upgrade firmware via a remote SFTP server. Select **SFTP** from the drop-down list under **Method**.



Firmware Upgrade

Method *
SFTP

Server IP Address *

File Name *

Account *

Password *

Server IP Address

Setting	Description	Factory Default
IP address	Enter the IP address of the SFTP server where the new firmware file (*.rom) is located.	None

File Name

Setting	Description	Factory Default
Filename	Enter the filename of the new firmware.	None

Account

Setting	Description	Factory Default
Account name	Enter the SFTP server account name used to authorize the connection to the server.	None

Password

Setting	Description	Factory Default
Password	Enter the SFTP server password used to authorize the connection to the server.	None

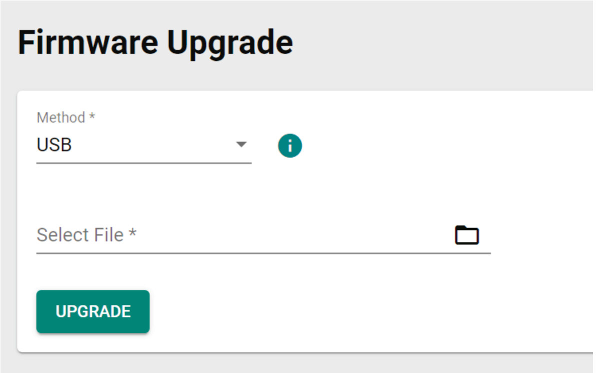
When finished, click **UPGRADE** to perform the firmware upgrade.

Upgrade Via USB

Users can upgrade the firmware via Moxa's USB-based ABC-02 configuration tool. Connect the ABC-02 to the switch and select **USB** from the drop-down list under **Method**.

NOTE

This method requires users to first download the updated firmware file (.rom) from www.moxa.com.


Firmware Upgrade

Method *: USB

Select File *

Select File

Click the Browse button and navigate to the firmware file on the ABC-02 configuration tool. With the file selected, click **UPGRADE** to perform the firmware upgrade.

NOTE

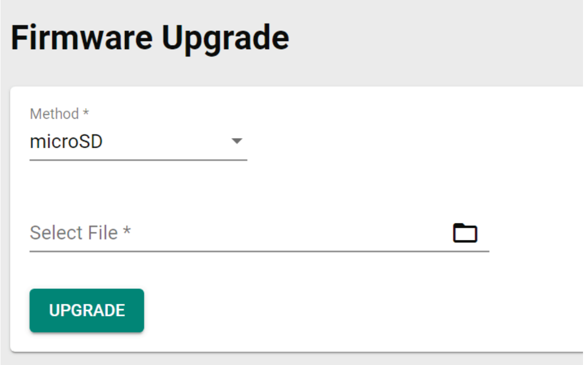
If you encounter issues using the ABC-02 configuration tool, check if the **USB Interface** has been enabled in the Hardware Interfaces section.

Upgrade Via microSD

Users can upgrade the firmware via Moxa's ABC-03-microSD-T configuration tool. Connect the ABC-03-microSD-T to the switch and select **microSD** from the drop-down list under **Method**.

NOTE

This method requires users to first download the updated firmware file (.rom) from www.moxa.com.


Firmware Upgrade

Method *: microSD

Select File *

Select File

Click the Browse button and navigate to the firmware file on the ABC-03 microSD-T configuration tool. With the file selected, click **UPGRADE** to perform the firmware upgrade.

NOTE

If you encounter issues using the ABC-03 configuration tool, check if the **MicroSD Interface** has been enabled in the Hardware Interfaces section.

Backup and Restore

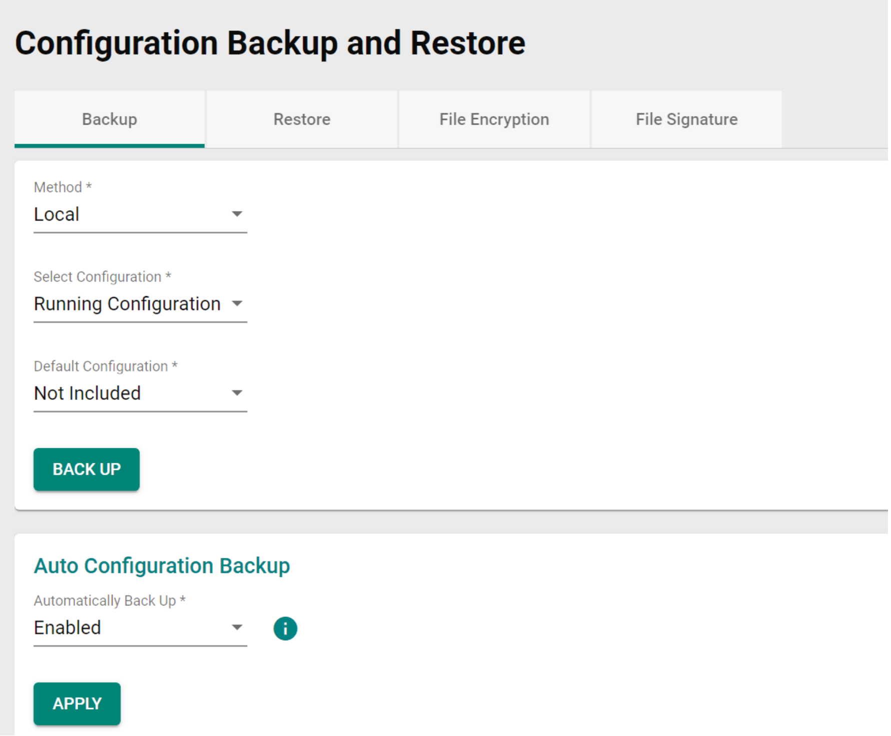
NOTE

This function is only supported on TSN Series models with firmware v2.3 or later.

There are five ways to back up and restore your Moxa switch's configuration: from a local configuration file, by a remote SFTP server, by a remote TFTP server, by an USB, or a microSD. In addition, file encryption and signature are also provided for your safety concern.

Backup

The Backup tab lets you back up the current device configuration. Click **Backup** tab.


Configuration Backup and Restore

Method * Local

Select Configuration * Running Configuration

Default Configuration * Not Included

Auto Configuration Backup

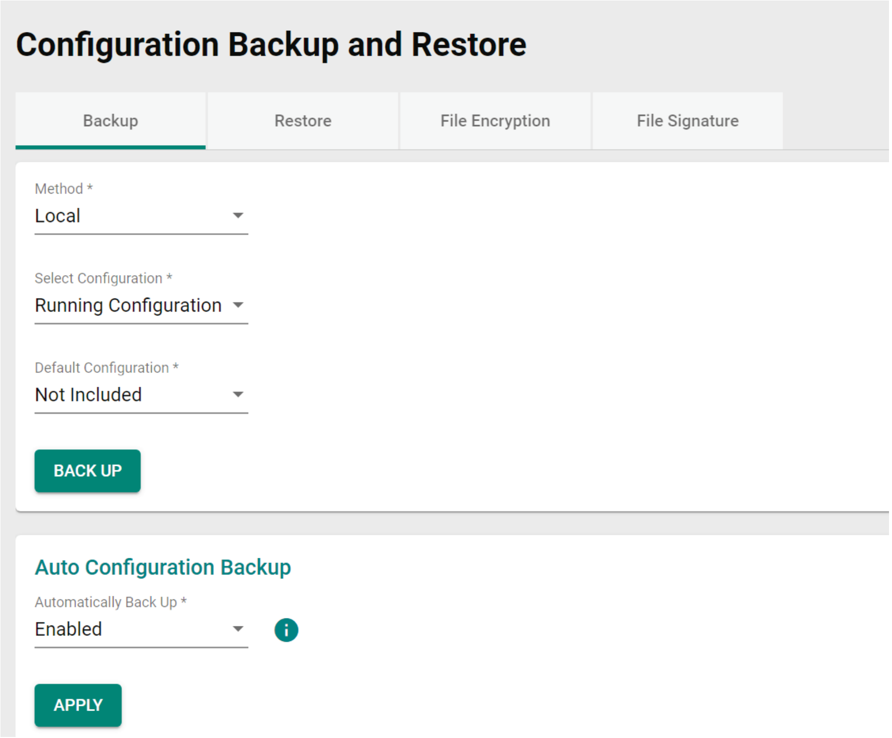
Automatically Back Up * Enabled

Method

Setting	Description	Factory Default
Select from the drop-down list	Specify whether to back up the configuration to a local configuration file, to a remote SFTP server, a remote TFTP server, a USB, or a microSD device.	Local

Back Up Locally

Select **Local** from the drop-down list under **Method**.



Configuration Backup and Restore

Method *: Local

Select Configuration *: Running Configuration

Default Configuration *: Not Included

Auto Configuration Backup

Automatically Back Up *: Enabled

Select Configuration

Setting	Description	Factory Default
Running Configuration	Back up the running configuration.	Running Configuration
Startup Configuration	Back up the start-up configuration.	

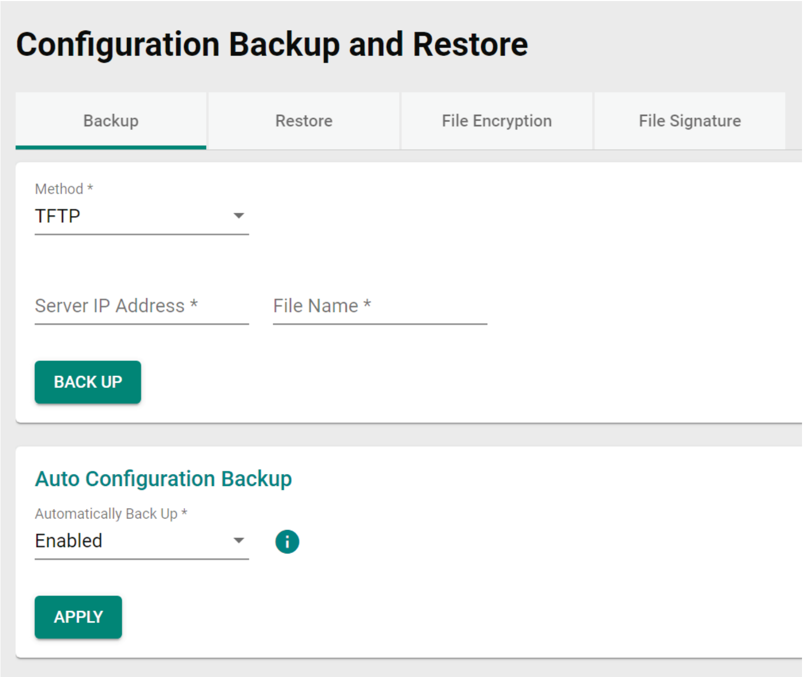
Default Configuration

Setting	Description	Factory Default
Not Included	Back up configuration does not include default settings.	Not Included
Included	Back up configuration includes default settings.	

When finished, click **BACK UP** to back up the system configuration file.

Back Up Via TFTP

Select **TFTP** from the drop-down list under **Method**.



Configuration Backup and Restore

Method * TFTP

Server IP Address *

File Name *

Auto Configuration Backup

Automatically Back Up * Enabled

Server IP Address

Setting	Description	Factory Default
IP address	Enter the IP address of the TFTP server to store the configuration backup file on.	None

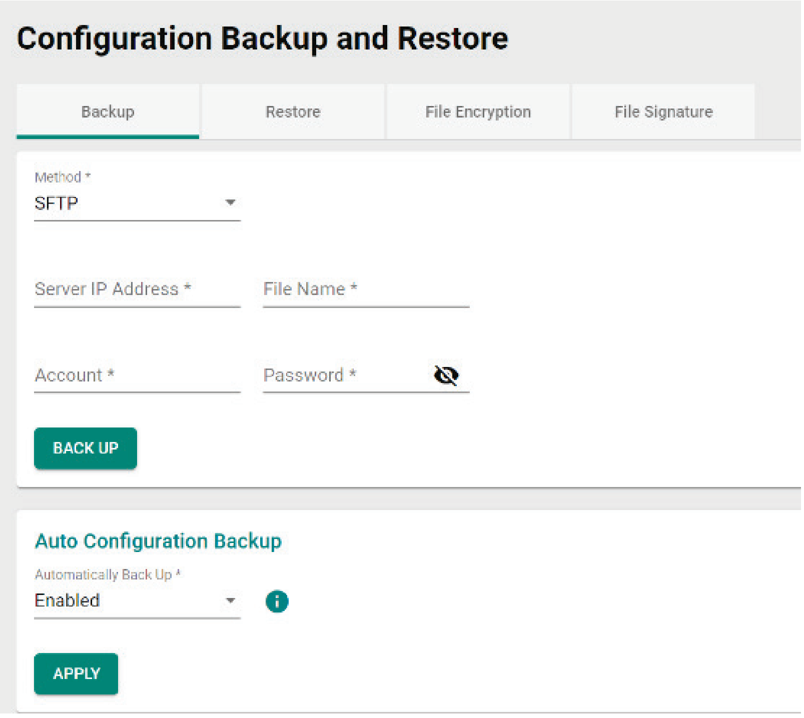
File Name

Setting	Description	Factory Default
Filename	Enter the filename of the configuration backup file, up to 54 characters including the .ini file extension.	None

When finished, click **BACK UP** to back up the system configuration.

Back Up Via SFTP

Select **SFTP** from the drop-down list under **Method**.



Configuration Backup and Restore

Method *: SFTP

Server IP Address *

File Name *

Account *

Password *

Auto Configuration Backup

Automatically Back Up *: Enabled

Server IP Address

Setting	Description	Factory Default
IP address	Enter the IP address of the SFTP server to store the configuration backup file on.	None

File Name

Setting	Description	Factory Default
Filename	Enter the filename of the configuration backup file, up to 54 characters including the .ini file extension.	None

Account

Setting	Description	Factory Default
Account name	Enter the SFTP server account name used to authorize the connection to the server.	None

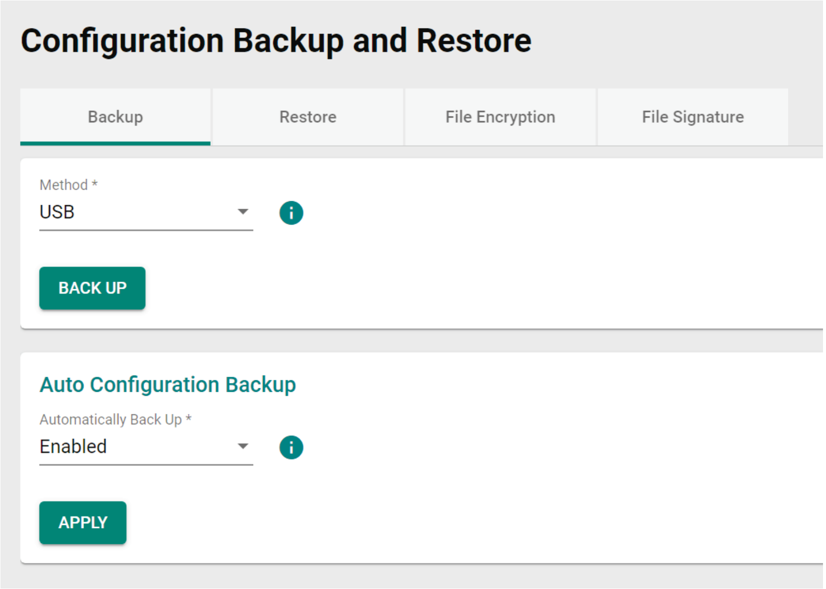
Password

Setting	Description	Factory Default
Password	Enter the SFTP server password used to authorize the connection to the server.	None

When finished, click **BACK UP** to back up the system configuration.

Back Up Via USB

Select **USB** from the drop-down list under **Method**.



Configuration Backup and Restore

Method * USB

Auto Configuration Backup

Automatically Back Up * Enabled

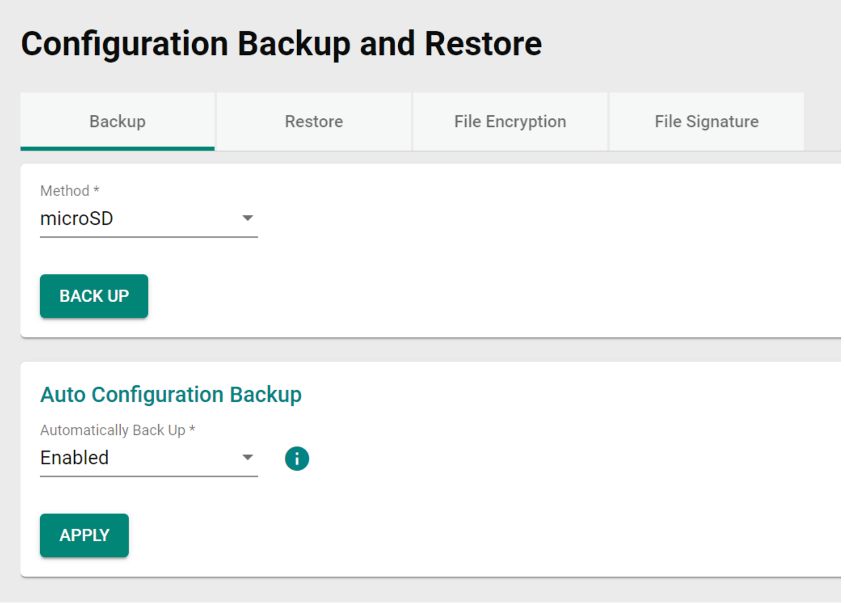
Insert the Moxa ABC-02 USB configuration tool into the USB port of the switch and click **BACK UP** to back up the system configuration file.

NOTE

If you encounter issues using the ABC-02 configuration tool, check if the **USB Interface** has been enabled in the Hardware Interfaces section.

Back Up Via microSD

Select **microSD** from the drop-down list under **Method**.



Configuration Backup and Restore

Method * microSD

Auto Configuration Backup

Automatically Back Up * Enabled

Connect the ABC-03-microSD-T configuration tool to the switch and click **BACK UP** to back up the system configuration file.

NOTE

If you encounter issues using the ABC-03 configuration tool, check if the **MicroSD Interface** has been enabled in the Hardware Interfaces section.

Back Up

The automatic backup function enables the system to automatically back up the device configuration whenever changes are made. The storage location of the backup file depends on the selected backup method.

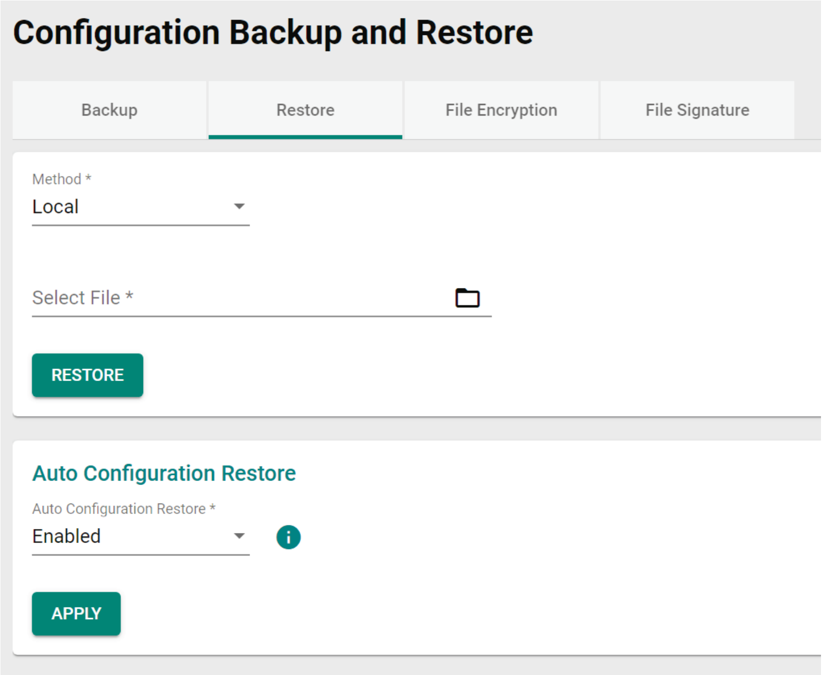
Back Up

Setting	Description	Factory Default
Enabled	Automatically back up to external storage when configurations change.	Enabled
Disabled	Do not automatically back up to external storage when configurations change.	

When finished, click **APPLY** to save your changes.

Restore

The Restore tab lets you restore a previously backed up configuration file. Click the **Restore** tab.



Configuration Backup and Restore

Method * Local

Select File *

Auto Configuration Restore

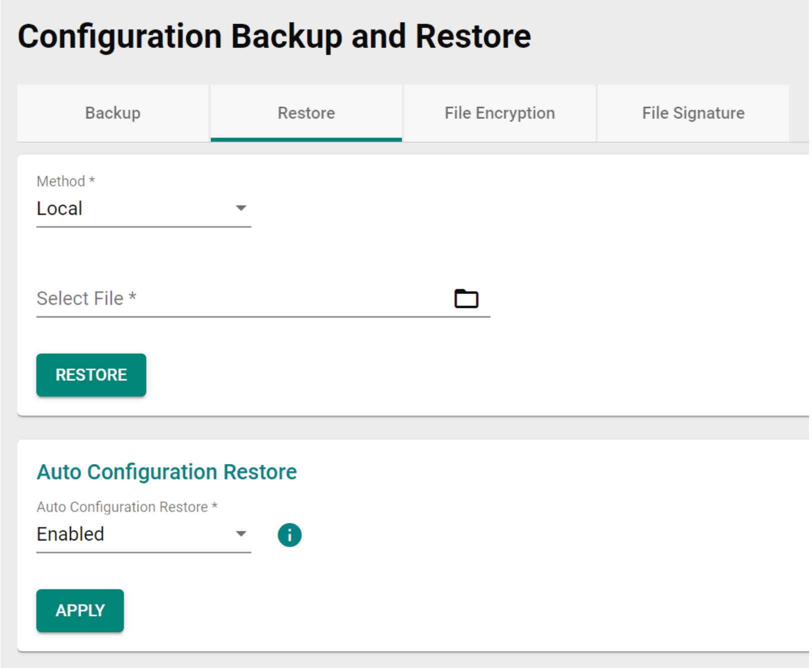
Auto Configuration Restore * Enabled

Method

Setting	Description	Factory Default
Select from the drop-down list	Specify whether to restore the configuration from a local configuration file, through a remote SFTP server, a remote TFTP server, a USB, or a microSD device.	Local

Restore Locally

Select **Local** from the drop-down list under **Method**.



Configuration Backup and Restore

Method *: Local

Select File *

Auto Configuration Restore

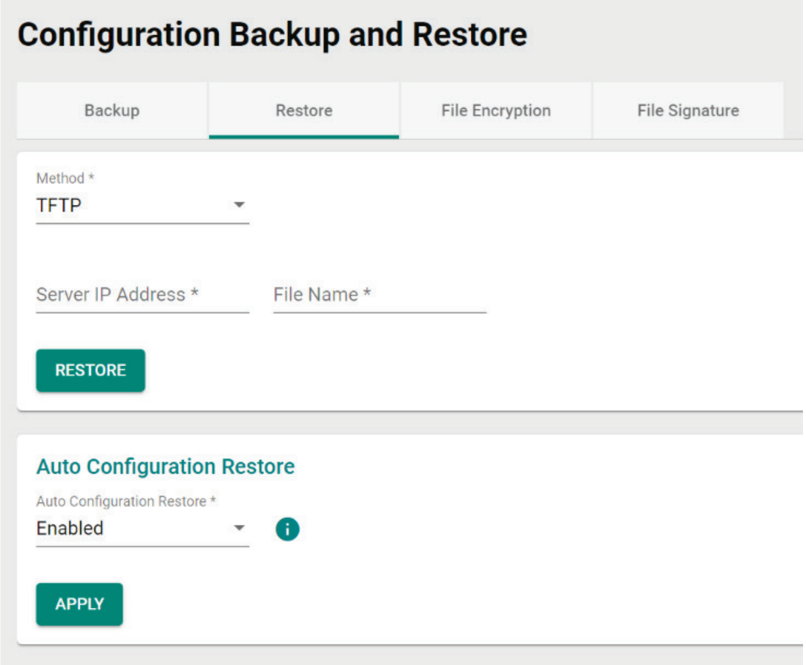
Auto Configuration Restore *: Enabled

Select File

Click the Browse button and navigate to the configuration file on the local machine. With the file selected, click **RESTORE** to restore the device configuration settings.

Restore Via TFTP

Select **TFTP** from the drop-down list under **Method**.



Configuration Backup and Restore

Method *: TFTP

Server IP Address *

File Name *

Auto Configuration Restore

Auto Configuration Restore *: Enabled

Server IP Address

Setting	Description	Factory Default
IP address	Enter the IP address of the TFTP server with the configuration backup file to restore.	None

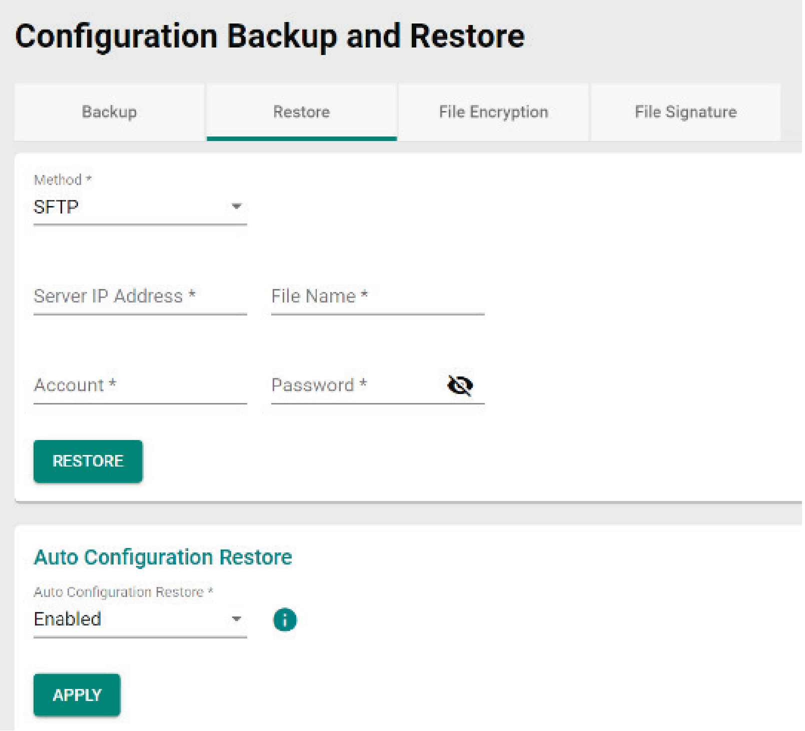
File Name

Setting	Description	Factory Default
Filename	Enter the filename of the configuration backup file to restore, up to 54 characters including the .ini file extension.	None

When finished, click **RESTORE** to restore the device configuration settings.

Restore Via SFTP

Select **SFTP** from the drop-down list under **Method**.



Configuration Backup and Restore

Method *: SFTP

Auto Configuration Restore *: Enabled

Server IP Address

Setting	Description	Factory Default
IP address	Enter the IP address of the SFTP server with the configuration backup file to restore.	None

File Name

Setting	Description	Factory Default
Filename	Enter the filename of the configuration backup file to restore, up to 54 characters including the .ini file extension.	None

Account

Setting	Description	Factory Default
Account name	Enter the SFTP server account name used to authorize the connection to the server.	None

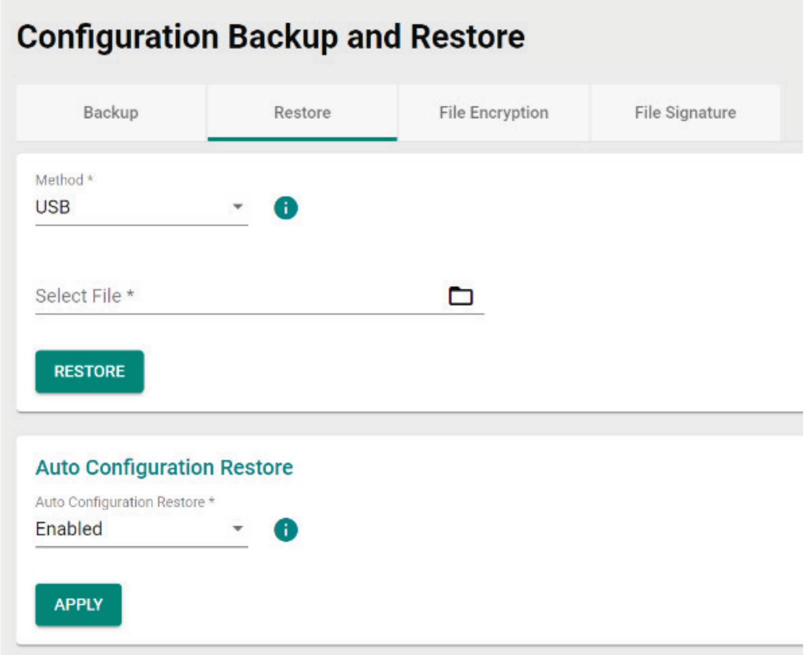
Password

Setting	Description	Factory Default
Password	Enter the SFTP server password used to authorize the connection to the server.	None

When finished, click **RESTORE** to restore the device configuration settings.

Restore Via USB

Insert Moxa's ABC-02 USB-based configuration tool into the USB port of the switch, select **USB** from the drop-down list under **Method**.



Configuration Backup and Restore

Method * USB

Select File *

Auto Configuration Restore

Auto Configuration Restore * Enabled

Select File

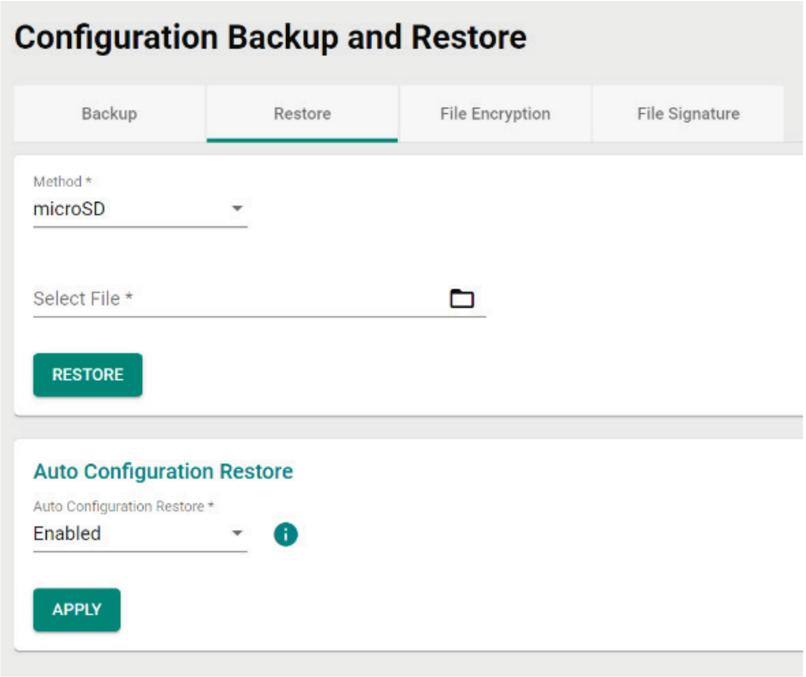
Click the Browse button and navigate to the configuration backup file on the ABC-02 configuration tool. With the file selected, click **RESTORE** to restore the device configuration settings.

NOTE

If you encounter issues using the ABC-02 configuration tool, check if the **USB Interface** has been enabled in the Hardware Interfaces section.

Restore Via microSD

Connect the ABC-03-microSD-T to the switch, Select **microSD** from the drop-down list under **Method**.



Configuration Backup and Restore

Method * microSD

Select File *

Auto Configuration Restore

Auto Configuration Restore * Enabled

Select File

Click the Browse button and navigate to the configuration backup file on the ABC-03 microSD-T configuration tool. With the file selected, click **RESTORE** to restore the device configuration settings.

NOTE

If you encounter issues using the ABC-03 configuration tool, check if the **MicroSD Interface** has been enabled in the the Hardware Interfaces section.

Automatic Restore

The automatic restore function enables the system to automatically restore the device configuration during boot-up. The location of the backup file used to restore the configuration depends on the selected restore method.

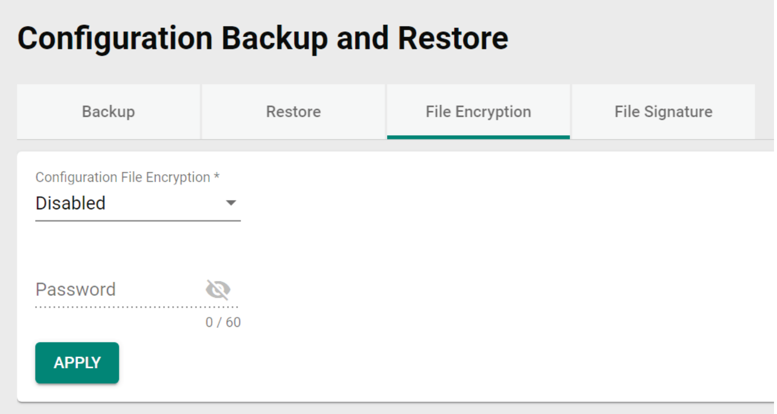
Auto Configuration Restore

Setting	Description	Factory Default
Enabled	Automatically restore the configuration from an external storage device during boot-up.	Enabled
Disabled	Will not automatically restore the configuration from an external storage device during boot-up.	

When finished, click **APPLY** to save your changes.

File Encryption

The File Encryption allows you to enable configuration file encryption. If encrypted, a password will be necessary to decrypt the configuration backup file. Click the **File Encryption** tab.



Configuration File Encryption *
Disabled

Password
0 / 60

Configuration File Encryption

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable configuration file encryption.	Disabled

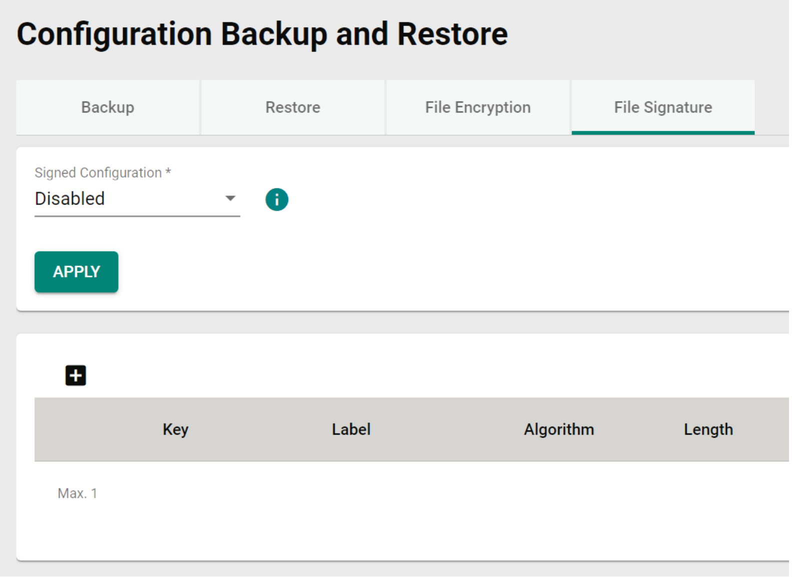
Password

Setting	Description	Factory Default
1 to 60 characters	If Configuration File Encryption is enabled, enter the encryption password.	None

When finished, click **APPLY** to save your changes.

File Signature

Click the **File Signature** tab to configure file signature options, which are used to ensure file integrity and authenticity.



Signed Configuration *
Disabled

Key	Label	Algorithm	Length

Max. 1

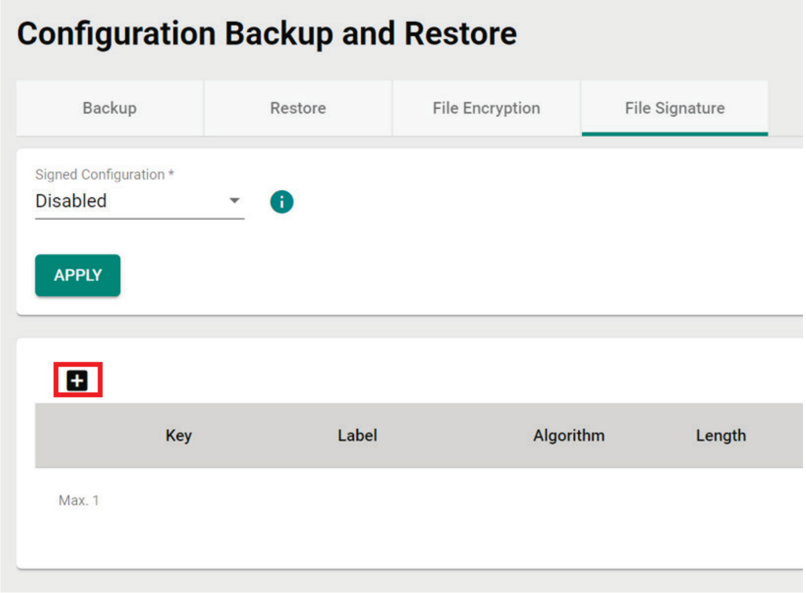
Signed Configuration

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable file signatures. If enabled, a digital signature is added when an administrator backs up or restores the configuration. Requires public an private keys.	Disabled

When finished, click **APPLY** to save your changes.

Adding a Custom Key

To add a custom key, click **+** icon.

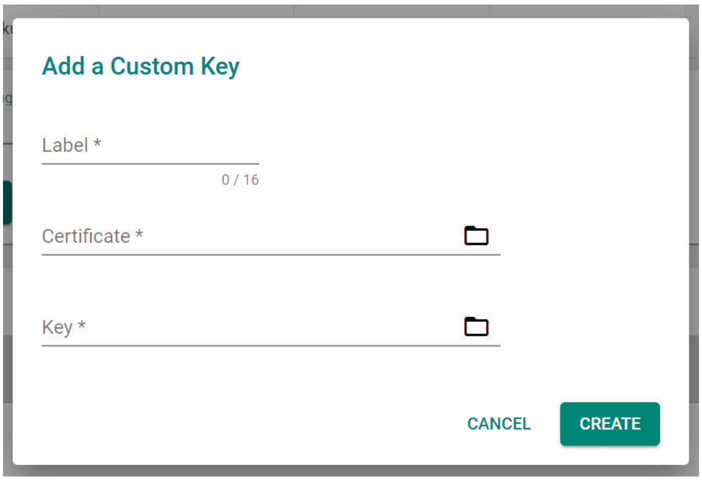


Configuration Backup and Restore

Signed Configuration *
Disabled

Key	Label	Algorithm	Length

Max. 1



Add a Custom Key

Label *
0 / 16

Certificate *

Key *

Label

Setting	Description	Factory Default
1 to 16 characters	Provide the label name for the certificate and the key.	None

Certificate

Setting	Description	Factory Default
Select the file from your computer	Import the certificate file.	None

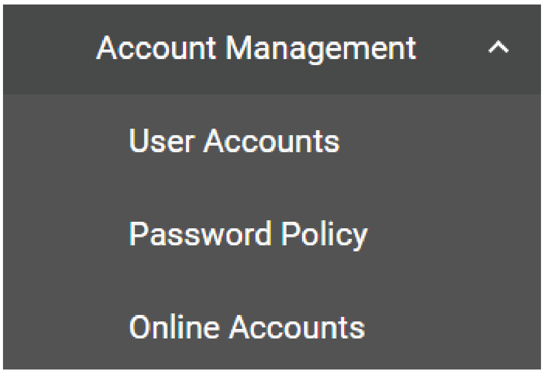
Key

Setting	Description	Factory Default
Select the file from your computer	Import the key file.	None

When finished, click **CREATE** to save your changes.

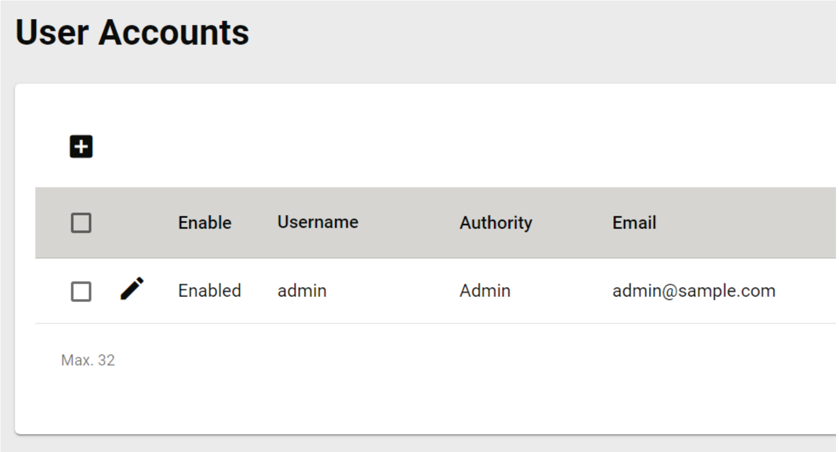
Account Management

The **Account Management** feature allows users to manage the accounts of the switch. You can enable different accounts with different roles to facilitate convenient management and safe access.



User Accounts

This section describes how to manage the existing accounts of the switch. Here, you can add, edit, and delete user accounts for the switch. By default, there is only one account: admin. In order to enhance security, we suggest you create a new account with the user authority.


User Accounts

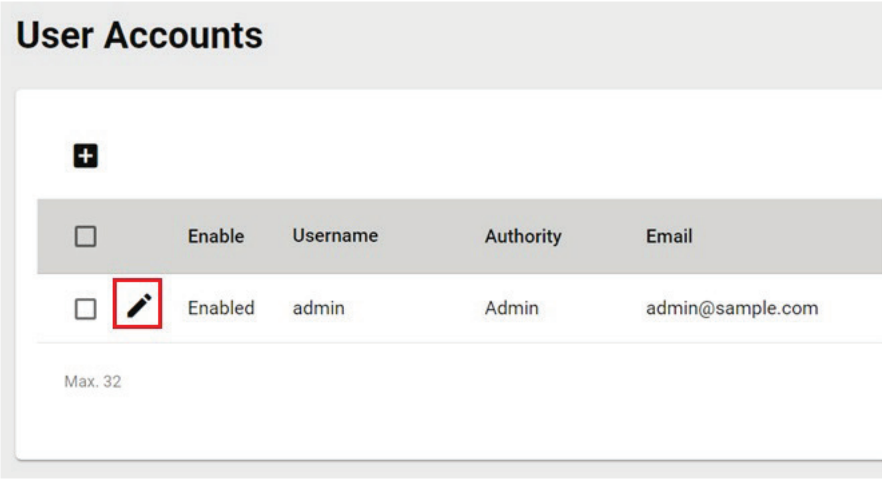
□		Enable	Username	Authority	Email
□	✎	Enabled	admin	Admin	admin@sample.com

Max. 32

Use the search bar in the upper-right corner of the page to quickly search for a user account.

Editing Existing Accounts

Select the account you want to edit and click the edit icon.

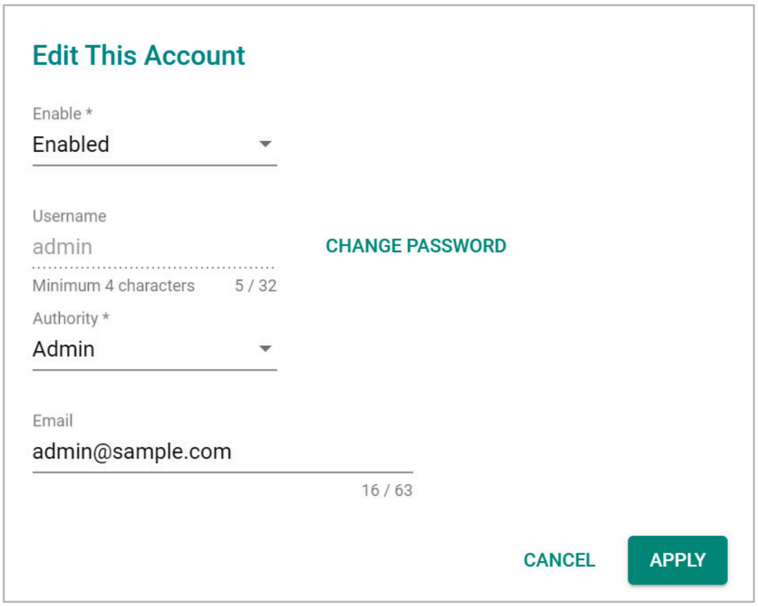


User Accounts

□		Enable	Username	Authority	Email
□	✎	Enabled	admin	Admin	admin@sample.com

Max. 32

Configure the following settings:



Edit This Account

Enable *: Enabled

Username: admin

Minimum 4 characters 5 / 32

Authority *: Admin

Email: admin@sample.com

16 / 63

Enable

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable this user account.	Enabled

Username

Information	Description	Factory Default
Show the username (read only)	It displays the username.	username

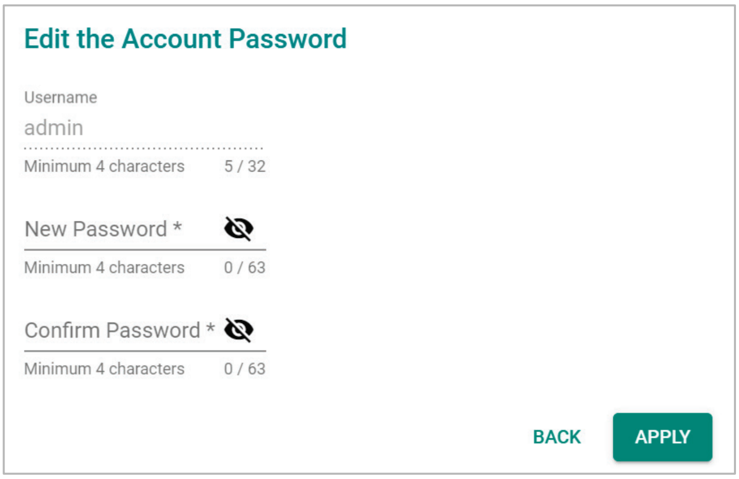
Authority

Setting	Description	Factory Default
admin	This account has read/write access of all configuration parameters.	admin
supervisor	This account has read/write access of some specific configuration parameters.	
user	This account can only view some specific configuration parameters.	

Email

Setting	Description	Factory Default
Email address	Enter an email address for the account.	None

To change the password, click **CHANGE PASSWORD**.



Edit the Account Password

Username
admin
Minimum 4 characters 5 / 32

New Password *
Minimum 4 characters 0 / 63

Confirm Password *
Minimum 4 characters 0 / 63

Username

Information	Description	Factory Default
Show the username (read only)	It displays the username.	admin

New Password

Setting	Description	Factory Default
4 to 63 characters	It allows users to provide a new password for this account.	None

Confirm Password

Setting	Description	Factory Default
4 to 63 characters	Input the same password for confirmation.	None

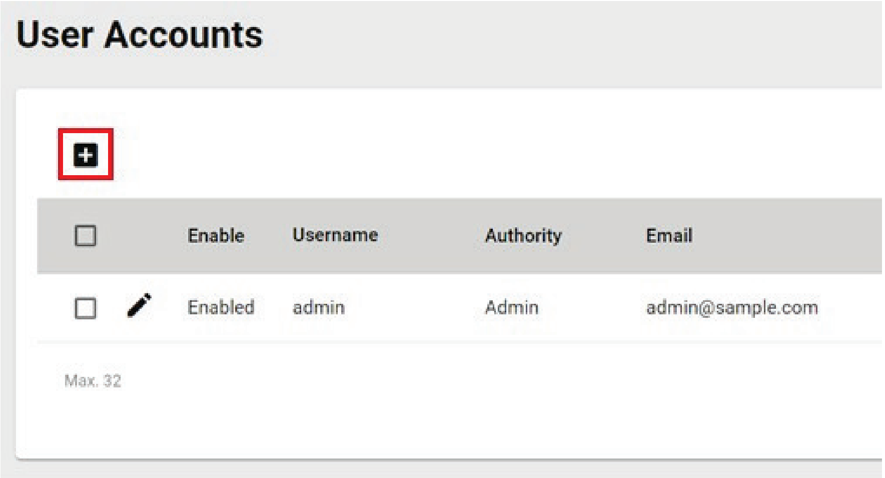
When finished, click **APPLY** to save your changes.

NOTE

Refer to **Appendix A** for detailed descriptions for read/write access privileges for the admin, supervisor, and user authority levels.

Creating a New Account

You can create new account by clicking the **+** icon on the configuration page.

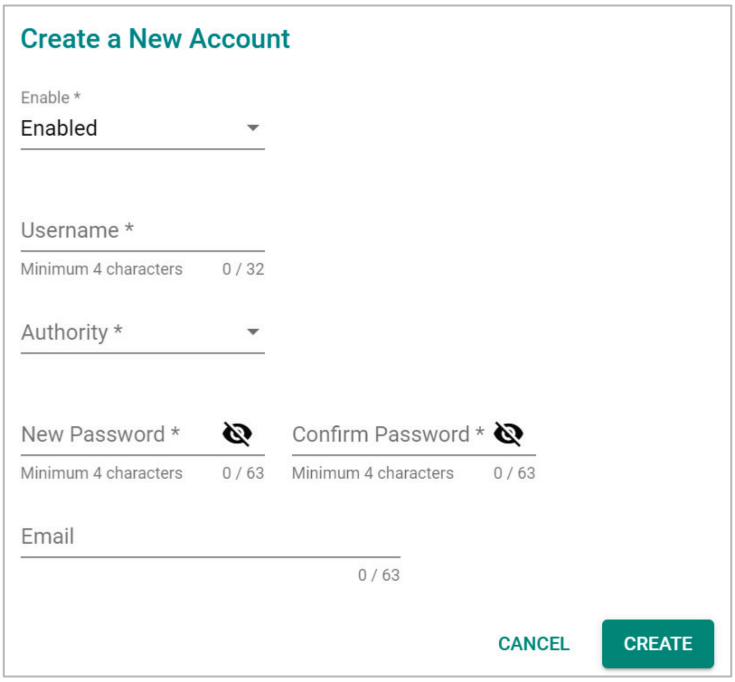


User Accounts

□		Enable	Username	Authority	Email
□		Enabled	admin	Admin	admin@sample.com

Max. 32

Configure the following settings:



Create a New Account

Enable *
Enabled

Username *
Minimum 4 characters 0 / 32

Authority *

New Password * Minimum 4 characters 0 / 63

Confirm Password * Minimum 4 characters 0 / 63

Email 0 / 63

Enable

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable this user account.	Enabled

Username

Setting	Description	Factory Default
4 to 32 characters	Input a new username for this account.	None

Authority

Setting	Description	Factory Default
admin	This account has read/write access of all configuration parameters.	None
supervisor	This account has read/write access for some specific configuration parameters.	
user	This account can only view some specific configuration parameters.	

In order to enhance security, we suggest you create a new account with the user authority.

New Password

Setting	Description	Factory Default
4 to 63 characters	Input a new password for this account.	None

Confirm Password

Setting	Description	Factory Default
4 to 63 characters	Reenter the password to confirm.	None

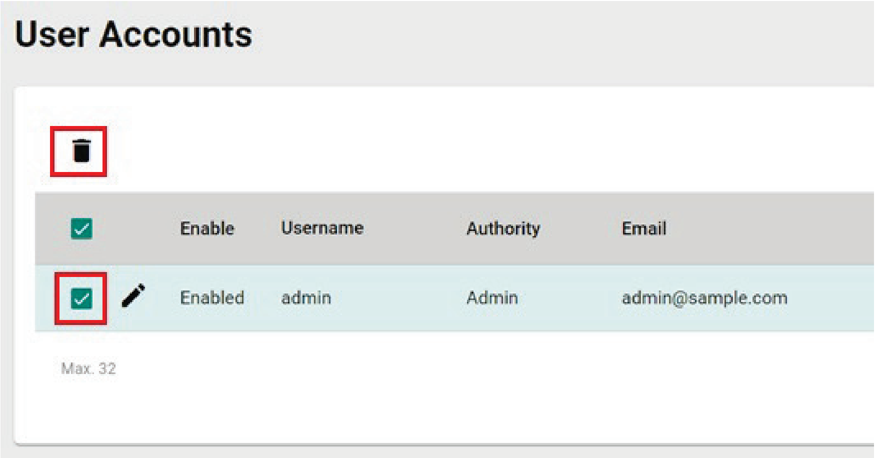
Email

Setting	Description	Factory Default
Email address	Enter an email address for the account if required.	None

When finished, click **CREATE** to complete.

Delete an Existing Account

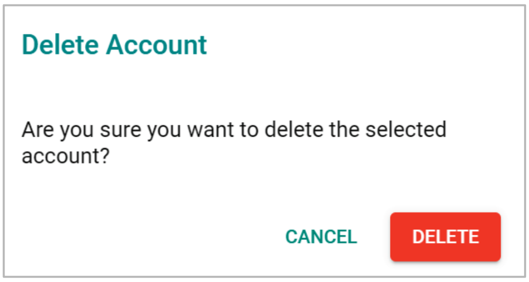
To delete an existing account, simply select the account you want to delete, and then click the delete icon on the configuration page.



User Accounts

☑	Enable	Username	Authority	Email
☑	Enabled	admin	Admin	admin@sample.com

Click **DELETE** to delete the account.

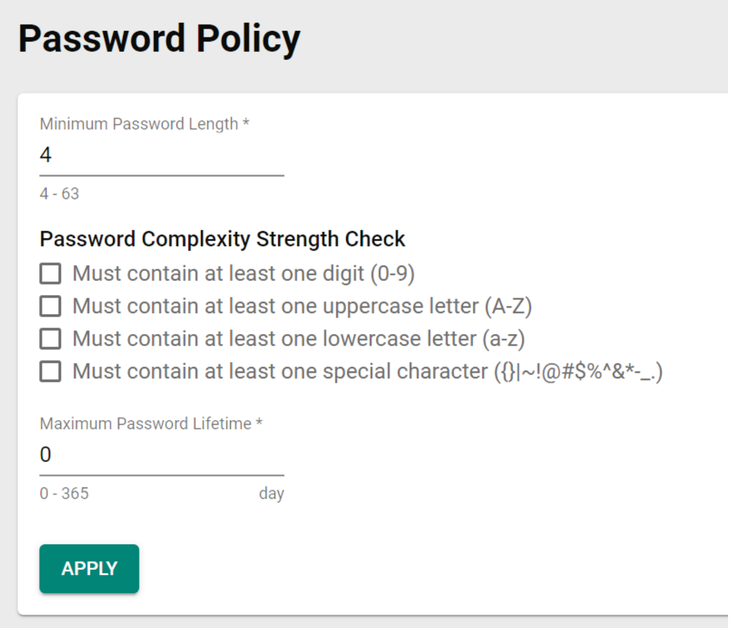


Delete Account

Are you sure you want to delete the selected account?

Password Policy

In order to prevent hackers from cracking weak passwords, a password policy can be set. The password policy can force users to create passwords with a minimum length and complexity and can also set a maximum lifetime for the password to ensure it is changed periodically.



Password Policy

Minimum Password Length *

4

4 - 63

Password Complexity Strength Check

□ Must contain at least one digit (0-9)

□ Must contain at least one uppercase letter (A-Z)

□ Must contain at least one lowercase letter (a-z)

□ Must contain at least one special character ({}|~!@#$%^&*-_.)

Maximum Password Lifetime *

0

0 - 365 day

Minimum Length

Setting	Description	Factory Default
Input from 4 to 63	This sets the minimum length of the password.	4

Password Complexity Strength Check

Setting	Description	Factory Default
digit, letter cases, special characters	These determine the required complexity for the password. Multiple options may be checked.	None

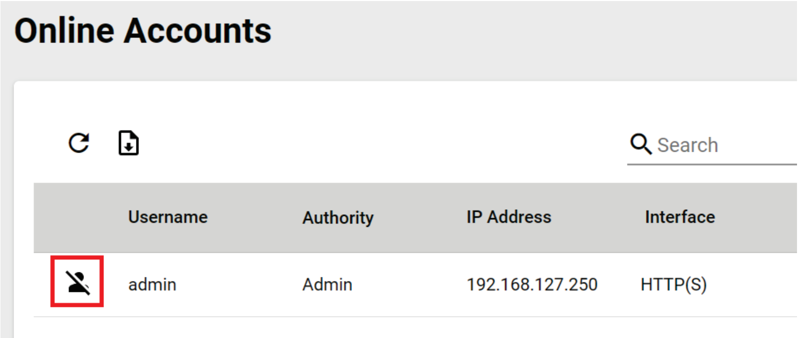
Password Max-life-time (day)

Setting	Description	Factory Default
Input from 0 to 365	This determines how long the password can be used before it must be changed.	0

When finished, click **APPLY** to save your changes.

Online Accounts

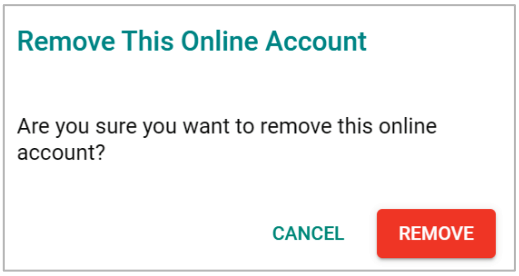
The **Online Accounts** function allows you to view users connected to the device. Deleting an online account will immediately disconnect that user from the device.



Online Accounts

	Username	Authority	IP Address	Interface
	admin	Admin	192.168.127.250	HTTP(S)

Click the remove icon and click **REMOVE** to disconnect the user.

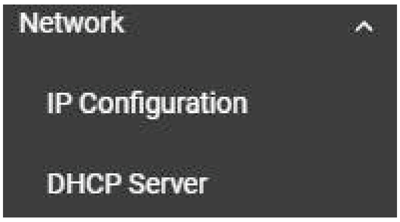


Remove This Online Account

Are you sure you want to remove this online account?

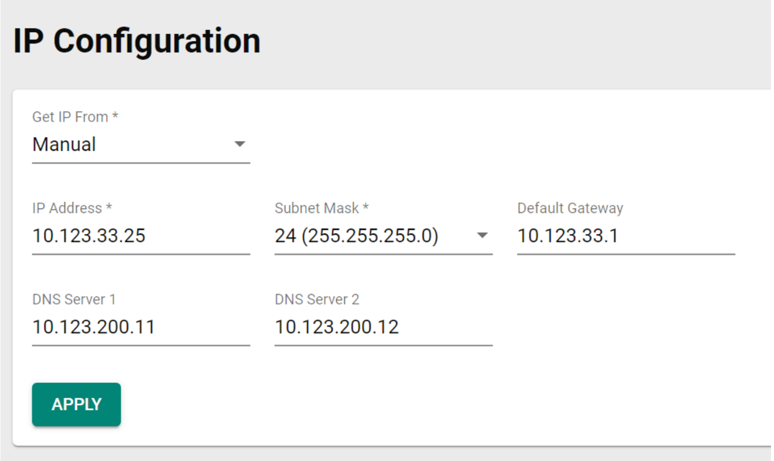
Network

This section describes how to configure the switch’s network settings, including **IP Configuration** and the **DHCP Server**.



IP Configuration

Users can configure the IP settings of the switch.



IP Configuration

Get IP From *: Manual

IP Address *: 10.123.33.25

Subnet Mask *: 24 (255.255.255.0)

Default Gateway: 10.123.33.1

DNS Server 1: 10.123.200.11

DNS Server 2: 10.123.200.12

Get IP From

Setting	Description	Factory Default
Manual	The IP address of the switch must be set manually.	Manual
DHCP	The IP address of the switch will be assigned automatically by the network's DHCP server.	

IP Address

Setting	Description	Factory Default
Input the IP address for the switch	Specify the IP address to use for the switch.	192.168.127.253

Subnet Mask

Setting	Description	Factory Default
Input the subnet mask for the switch	Specify the subnet mask to use for the switch.	24(255.255.255.0)

Default Gateway

Setting	Description	Factory Default
Input the IP address for the gateway	Specify the IP address of the gateway that connects the LAN to a WAN or another network.	None

DNS Server 1

Setting	Description	Factory Default
Input the IP address of the 1st DNS server	Specify the IP address of the 1st DNS server used by your network. After specifying the DNS server's IP address, you can use the switch's URL (e.g., www.mymoxaswitch.com) to open the web console instead of entering the IP address.	None

DNS Server 2

Setting	Description	Factory Default
Input the IP address of the 2nd DNS server	Specify the IP address of the 2nd DNS server used by your network. The switch will use the secondary DNS server if the first DNS server fails to connect.	None

IPv6 Global Unicast Address Prefix (Prefix Length: 64 bits) Default Gateway

Setting	Description	Factory Default
Global Unicast Address Prefix	The prefix value must be formatted according to the RFC 2373 IPv6 Addressing Architecture, using 8 colon-separated 16-bit hexadecimal values. One double colon can be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. Note: This feature is only available in Advanced Mode.	None

IPv6 DNS Server 1

Setting	Description	Factory Default
Input the IPv6 IP address of the 1st DNS server	Specify the IPv6 address of the 1st DNS server used by your network. After specifying the DNS server's IP address, you can use the switch's URL (e.g., www.mymoxaswitch.com) to open the web console instead of entering the IP address. Note: This feature is only available in Advanced Mode.	None

IPv6 DNS Server 2

Setting	Description	Factory Default
Input the IPv6 address of the 2nd DNS server	Specify the IPv6 address of the 2nd DNS server used by your network. The Moxa switch will use the secondary DNS server if the first DNS server fails to connect. Note: This feature is only available in Advanced Mode.	None

IPv6 Global Unicast Address

Setting	Description	Factory Default
None	Displays the IPv6 Global Unicast address. The network portion of the Global Unicast address can be configured by specifying the Global Unicast Prefix and using an EUI-64 interface ID in the low order 64 bits of the address. The host portion of the Global Unicast address is automatically generated using the modified EUI-64 form of the interface identifier (the switch's MAC address). Note: This feature is only available in Advanced Mode.	None

IPv6 Link-Local Address

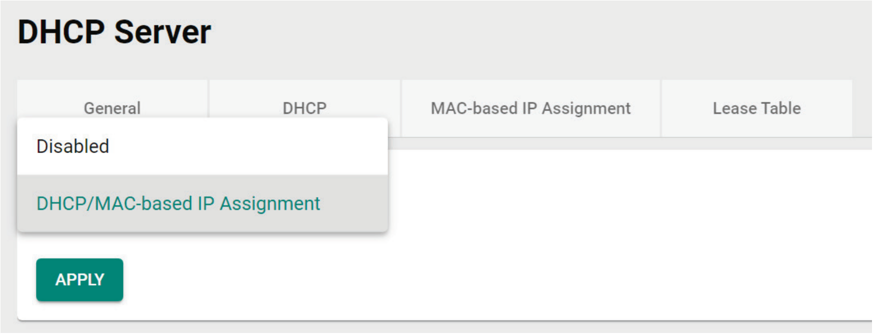
Setting	Description	Factory Default
None	The network portion of the Link-Local address is FE80 and the host portion of the Link-Local address is automatically generated using the modified EUI-64 form of the interface identifier (the switch's MAC address). Note: This feature is only available in Advanced Mode.	None

When finished, click **APPLY** to save your changes.

DHCP Server

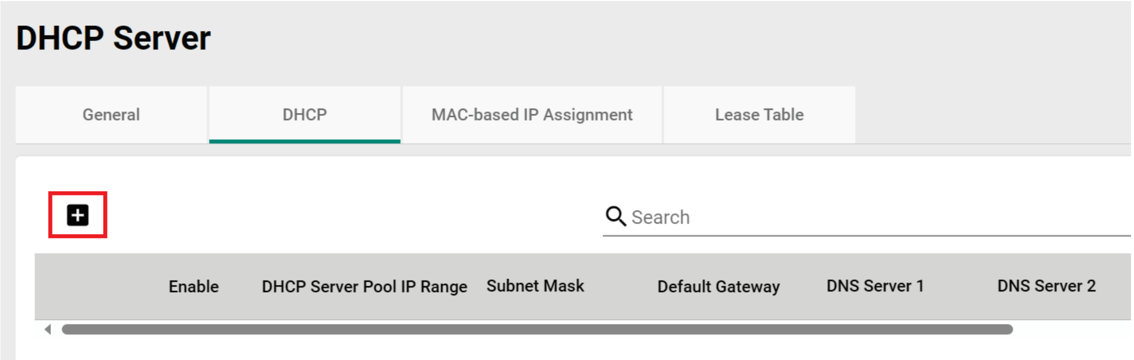
This section describes how to configure the DHCP server settings for Moxa's switch.

To enable the DHCP server, select **DHCP / MAC-based IP Assignment** in the **General** tab and click **APPLY**.



DHCP

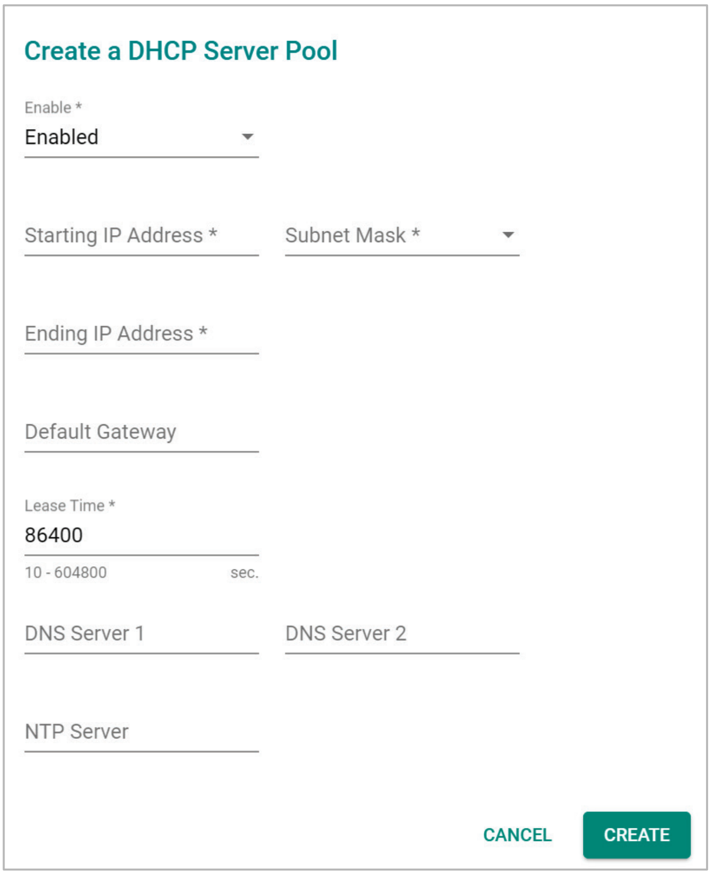
Select the **DHCP** tab and then click the **+** icon on the configuration page to create a new DHCP server pool.



DHCP Server

Enable	DHCP Server Pool IP Range	Subnet Mask	Default Gateway	DNS Server 1	DNS Server 2

Configure the following parameters.



Create a DHCP Server Pool

Enable * Enabled

Starting IP Address *

Subnet Mask *

Ending IP Address *

Default Gateway

Lease Time * 86400

10 - 604800 sec.

DNS Server 1

DNS Server 2

NTP Server

NOTE

Users can only create one IP pool. It can be connected to different network subnets with the Management IP of the switch.

Enable

Setting	Description	Factory Default
Enabled	Enables the DHCP server pool.	Enabled
Disable	Disables the DHCP server pool.	

Start IP Address

Setting	Description	Factory Default
Input the first IP address	Specify the first IP address for the pool.	None

Subnet Mask

Setting	Description	Factory Default
Select from the drop-down list	Specify the subnet mask for the pool.	None

End IP Address

Setting	Description	Factory Default
Input the last IP address	Specify the last IP address for the pool.	None

Default Gateway

Setting	Description	Factory Default
Input the IP address of the default gateway	Specify the default gateway for clients to use.	None

Lease Time (sec.)

Setting	Description	Factory Default
Input the lease time for the DHCP, from 10 to 604,800 seconds (up to 7 days)	Specify the lease time for DHCP IP assignments.	86400

DNS Server 1

Setting	Description	Factory Default
Input the IP address of the 1st DNS server	Specify the IP address of the 1st DNS server for clients to use.	None

DNS Server 2

Setting	Description	Factory Default
Input the IP address of the 2nd DNS server	Specify the IP address of the 2nd DNS server for clients to use.	None

NTP Server

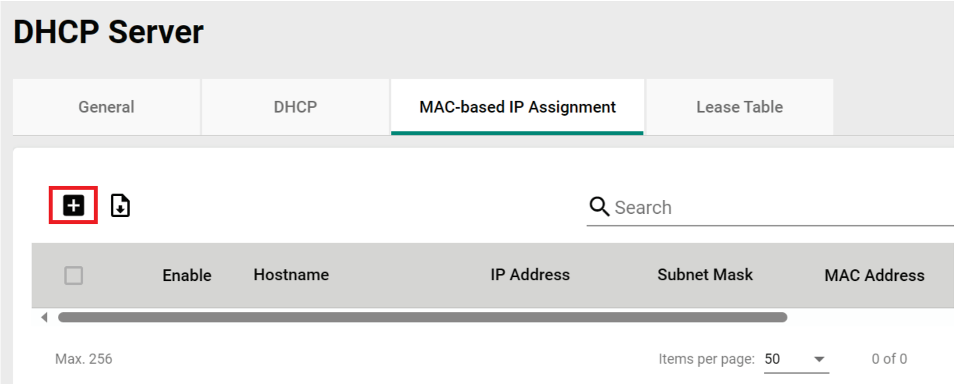
Setting	Description	Factory Default
Input the address of the NTP server	Specify the NTP server clients will use.	None

When finished, click **CREATE**.

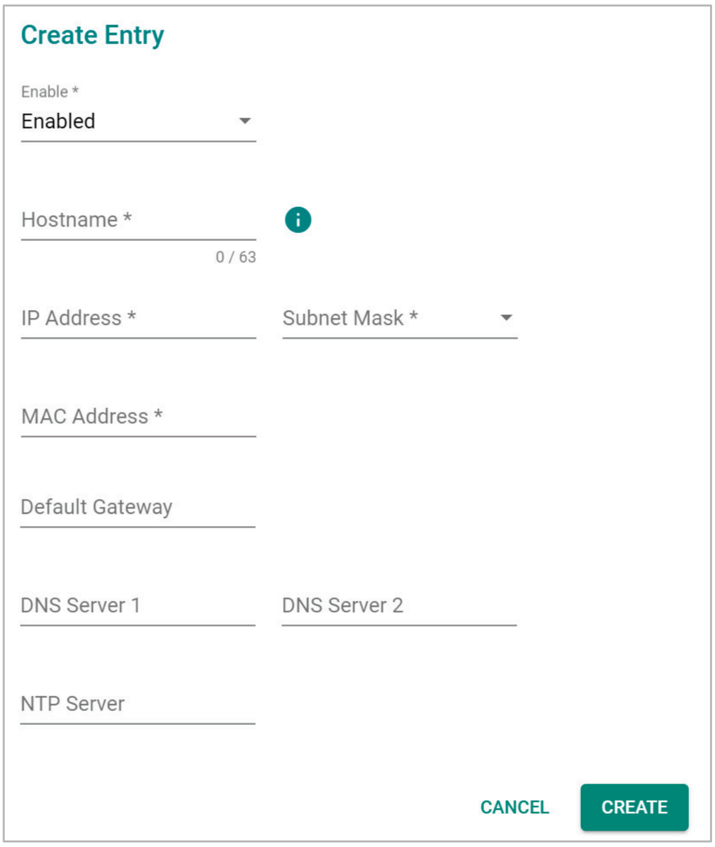
MAC-based IP Assignment

Users can assign an IP address for a specific MAC address. This can be useful if you always want the same IP address to be assigned to a specific device, even if it is reconnected or connected to a different port.

Click the **MAC-based IP Assignment** tab, and then click the **+** icon on the configuration page. Note that the MAC-based IP Assignment has a higher priority than the DHCP server.



Configure the following parameters.



Enable *
Enabled

Enable

Setting	Description	Factory Default
Enabled	Enables the MAC-based IP assignment entry.	Enabled
Disabled	Disables the MAC-based IP assignment entry.	

Hostname

Setting	Description	Factory Default
Enter a hostname between 0 and 63 characters	Specify a hostname to use for the DHCP client.	None

IP Address

Setting	Description	Factory Default
Input the assigned IP address	Specify the IP address to assign to the client.	None

Subnet Mask

Setting	Description	Factory Default
Select from the drop-down list	Specify the subnet mask to use for the client.	None

MAC Address

Setting	Description	Factory Default
Input the assigned MAC address	Specify the MAC address of the device you want to assign an IP address to. Make sure the MAC address is entered in the correct format. Here is an example: 28-d2-44-D3-e3-f2 or 28:d2:44:D3:e3:f2.	None

Default Gateway

Setting	Description	Factory Default
Input the IP address of the default gateway	Specify the default gateway for the client to use.	None

DNS Server 1

Setting	Description	Factory Default
Input the IP address of the 1st DNS server	Specify the IP address of the 1st DNS server for the client to use.	None

DNS Server 2

Setting	Description	Factory Default
Input the IP address of the 2nd DNS server	Specify the IP address of the 2nd DNS server for the client to use.	None

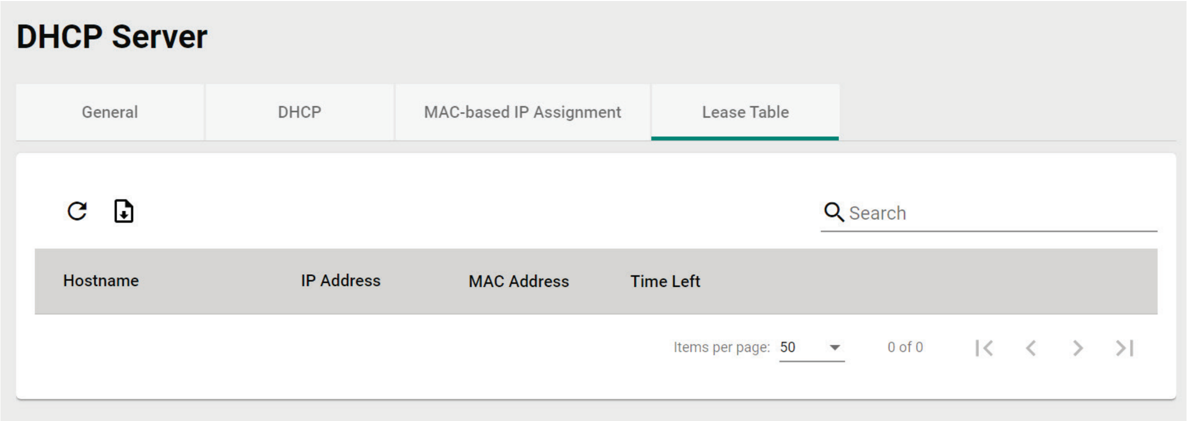
NTP Server

Setting	Description	Factory Default
Input the address of the NTP server	Specify the NTP server the client will use.	None

When finished, click **Create**.

Lease Table

Click **Lease Table** to view detailed information for the hostname, IP address, MAC address, and time left for each port.



DHCP Server

General | DHCP | MAC-based IP Assignment | Lease Table

Search

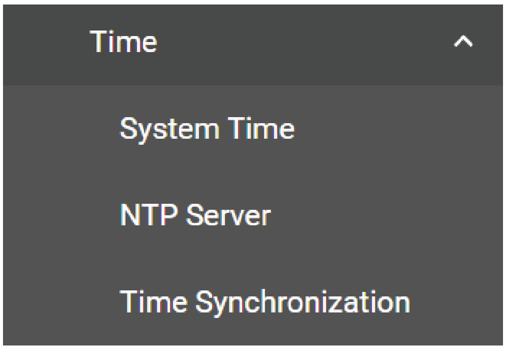
Hostname	IP Address	MAC Address	Time Left

Items per page: 50 0 of 0

Item	Description
Hostname	The hostname of the client.
IP Address	The IP address of the client.
MAC Address	The MAC address of the client.
Time Left	The amount of time left on the DHCP lease for the client.

Time

This section describes how to configure the **System Time**, **NTP Serve**, and **Time Synchronization** settings for the switch. The switch can synchronize the system time with an NTP server, or use a manually specified time and date, allowing functions such as automatic warning emails to include a time and date stamp.



NOTE

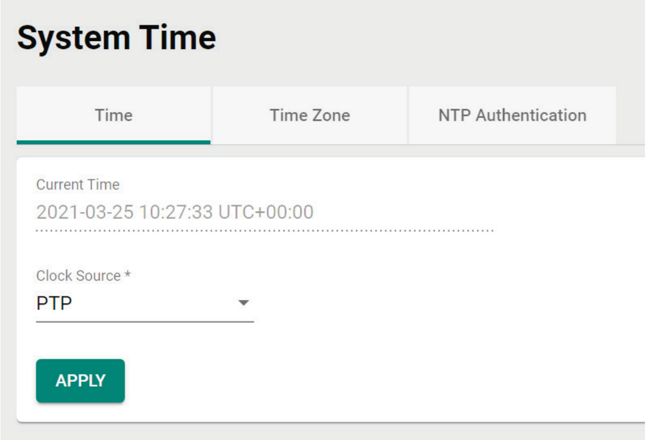
If the switch has been powered off for an extended period of time (e.g., three days), it is recommended to update the Current Time and Current Date, especially if no NTP server is configured or if the switch has no Internet connection.

System Time

This section describes how to configure the **Time, Time Zone** and **NTP Authentication** settings.

Time

The section describes how to configure the system time. Click the **Time** tab.



System Time

Current Time
2021-03-25 10:27:33 UTC+00:00

Clock Source *
PTP

Current Time

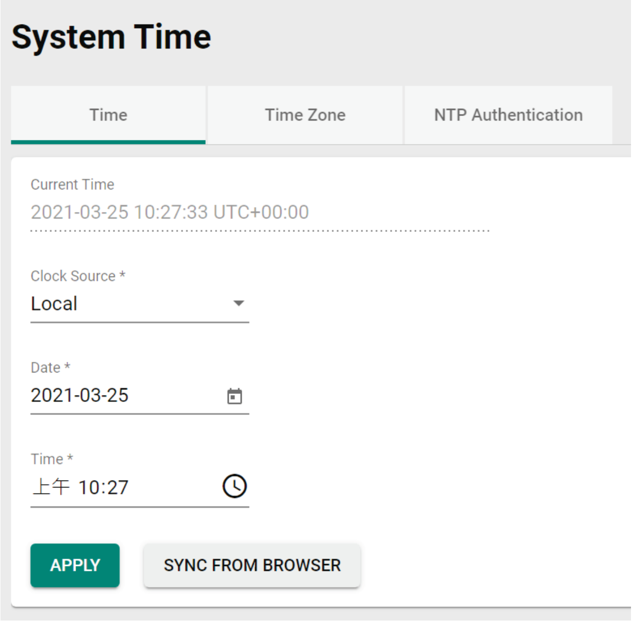
Setting	Description	Factory Default
None	This shows the current time based on the current configuration.	Current time (read only)

Clock Source

Setting	Description	Factory Default
Local, SNTP, NTP, PTP	Specify whether to set the time manually (Local), or via a SNTP server, a NTP server, or PTP.	PTP

Clock Source - Local

To set the time manually, select **Local** from the drop-down list under **Clock Source** and Configure the following settings:



System Time

Current Time
2021-03-25 10:27:33 UTC+00:00

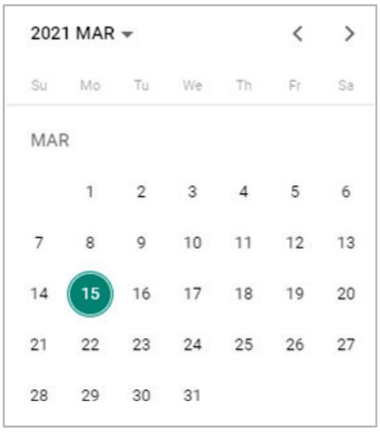
Clock Source *
Local

Date *
2021-03-25

Time *
上午 10:27

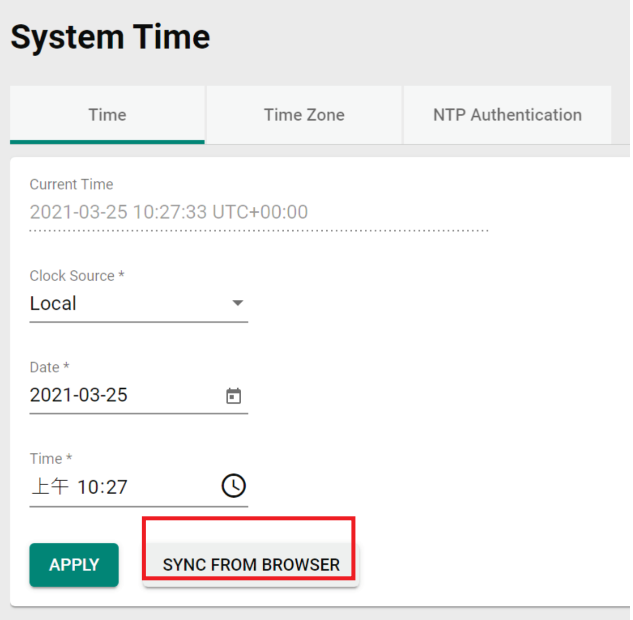
Date

Setting	Description	Factory Default
Date	Select the current date.	None



Time

Setting	Description	Factory Default
Time	Specify the current time. You can manually specify the time, or you can click **SYNC FROM BROWSER** to synchronize the time with your web browser's clock.	None



Current Time
2021-03-25 10:27:33 UTC+00:00

Clock Source *
Local

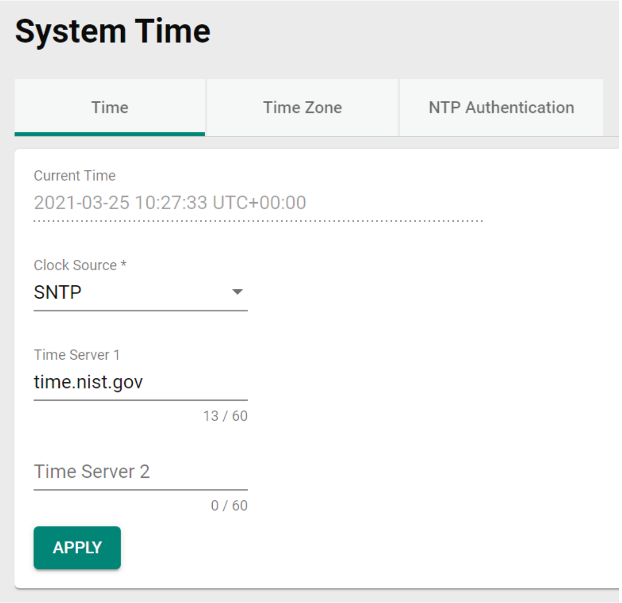
Date *
2021-03-25

Time *
上午 10:27

When finished, click **APPLY** to save your changes.

Clock Source - SNTP

To synchronize the system time with an SNTP server, select **SNTP** from the drop-down list under **Clock Source** and Configure the following settings:



Current Time
2021-03-25 10:27:33 UTC+00:00

Clock Source *
SNTP

Time Server 1
time.nist.gov
13 / 60

Time Server 2
0 / 60

Time Server 1

Setting	Description	Factory Default
IP address or domain name	Specify the IP address or domain name of the primary SNTP server (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	Time.nist.gov

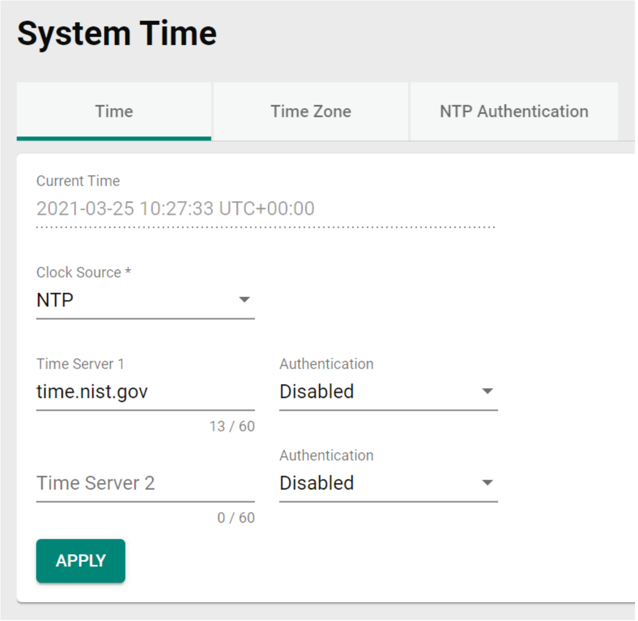
Time Server 2

Setting	Description	Factory Default
IP address or domain name	Specify the IP address or domain name of the secondary SNTP server. If the primary server becomes unavailable, the system will switch to the secondary SNTP server.	None

When finished, click **APPLY** to save your changes.

Clock Source - NTP

To synchronize the system time with a NTP server, select **NTP** from the drop-down list under **Clock Source** and Configure the following settings:



Current Time
2021-03-25 10:27:33 UTC+00:00

Clock Source *
NTP

Time Server 1
time.nist.gov
13 / 60

Authentication
Disabled

Time Server 2
0 / 60

Authentication
Disabled

If the switch is connecting to an NTP server that requires authentication, refer to the NTP Authentication section to configure the NTP key.

Time Server 1

Setting	Description	Factory Default
IP address or domain name	Specify the IP address or domain name of the primary NTP server (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	Time.nist.gov

Authentication

Setting	Description	Factory Default
Disabled	Enable or disable NTP authentication for Time Server 1.	Disabled

Time Server 2

Setting	Description	Factory Default
IP address or domain name	Specify the IP address or domain name of the secondary NTP server. If the primary server becomes unavailable, the system will switch to the secondary SNTP server.	None

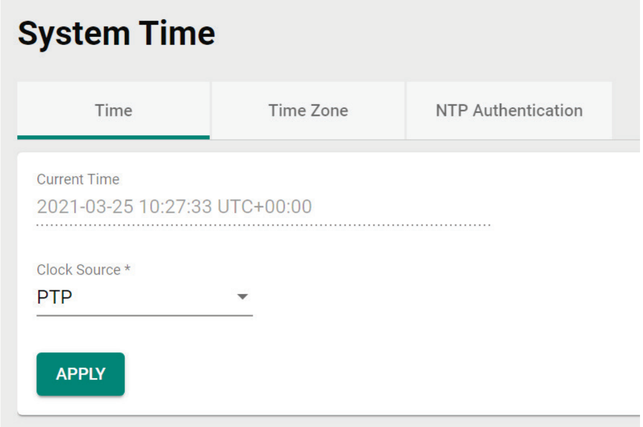
Authentication

Setting	Description	Factory Default
Disabled	Enable or disable NTP Authentication for Time Server 2.	Disabled

When finished, click **APPLY** to save your changes.

Clock Source - PTP

To synchronize the system with the PTP clock, select **PTP** from the drop-down list under **Clock Source** and click **APPLY** to save your change.

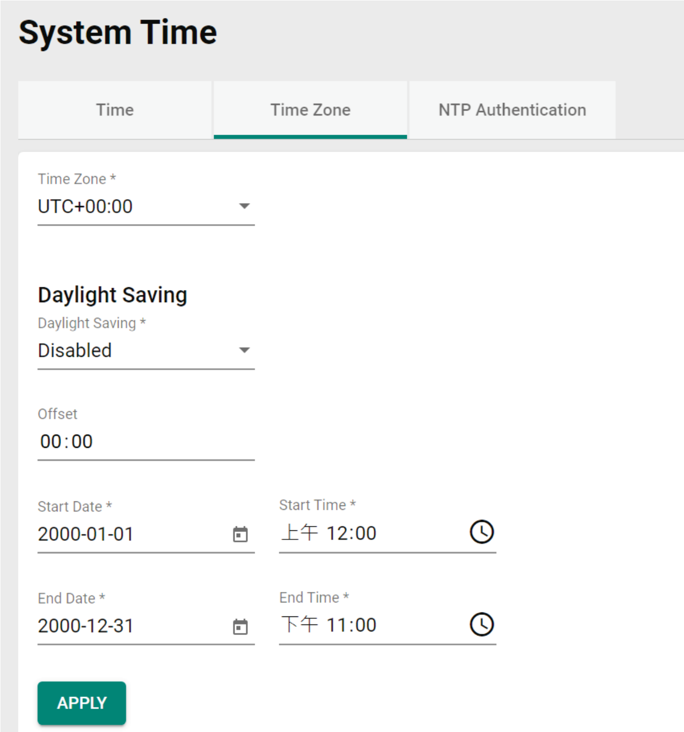


Current Time
2021-03-25 10:27:33 UTC+00:00

Clock Source *
PTP

Time Zone

The section describes how to configure time zone settings. Click the **Time Zone** tab.



Time Zone *
UTC+00:00

Daylight Saving *
Disabled

Offset
00 : 00

Start Date *
2000-01-01

Start Time *
上午 12:00

End Date *
2000-12-31

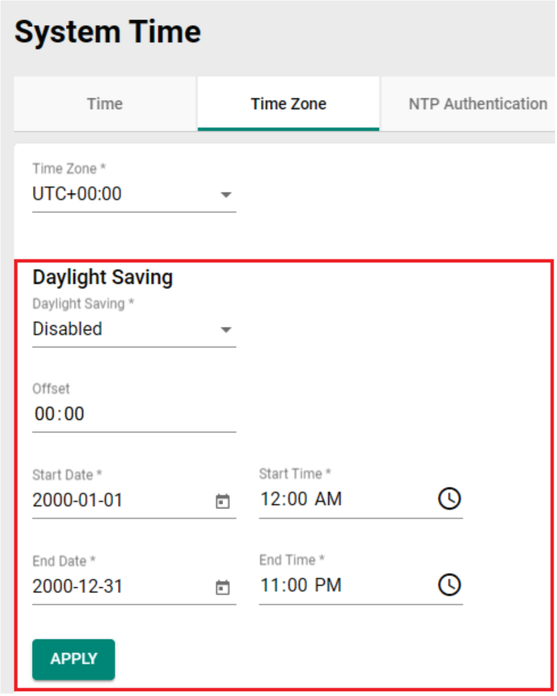
End Time *
下午 11:00

Time Zone

Setting	Description	Factory Default
Select from the drop-down list	Specify the time zone to use for the switch.	GMT (Greenwich Mean Time)

Daylight Saving

The Daylight Saving settings are used to automatically adjust the time according to regional standards.



System Time

Time Zone *
UTC+00:00

Daylight Saving

Daylight Saving *
Disabled

Offset
00:00

Start Date *
2000-01-01

Start Time *
12:00 AM

End Date *
2000-12-31

End Time *
11:00 PM

Configure the following settings:

Daylight Saving

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable Daylight Saving Time.	Disabled

Offset

Setting	Description	Factory Default
User-specified hour	Specify the offset (in HH:MM format) if Daylight Saving Time is enabled.	None

Start Date

Setting	Description	Factory Default
Date	Select the date that Daylight Saving Time begins.	None

Start Time

Setting	Description	Factory Default
Time	Specify the time that Daylight Saving Time begins.	None

End Date

Setting	Description	Factory Default
Date	Select the date that Daylight Saving Time ends.	None

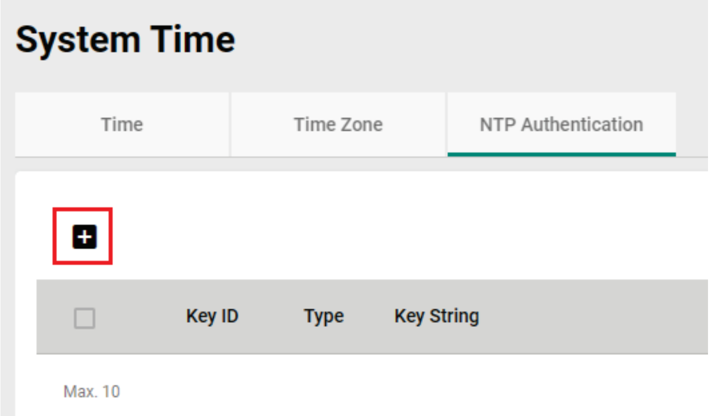
End Time

Setting	Description	Factory Default
Time	Specify the time that Daylight Saving Time ends.	None

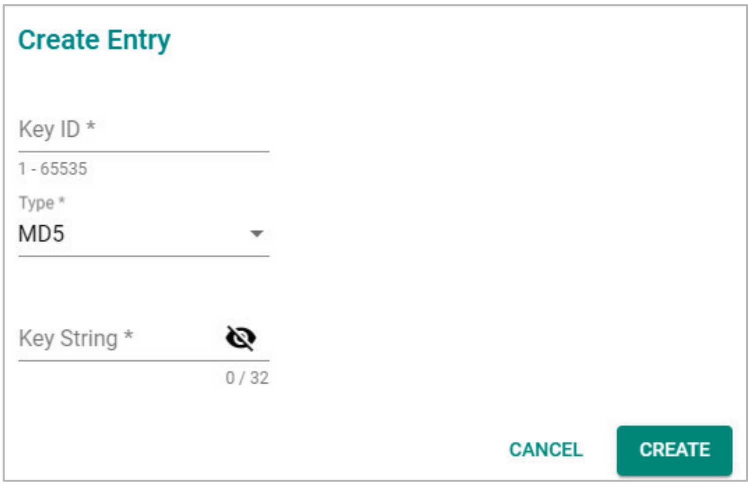
When finished, click **APPLY** save your changes.

NTP Authentication

This section describes how to manage NTP Authentication keys used for NTP servers that require authentication. Click the **NTP Authentication** tab. Click the **+** icon to create a new NTP key entry.



Configure the following settings:



Key ID

Setting	Description	Factory Default
1 to 65535	Specify the Key ID to use for NTP authentication.	None

Type

Setting	Description	Factory Default
Authentication type	Select the authentication type.	MD5

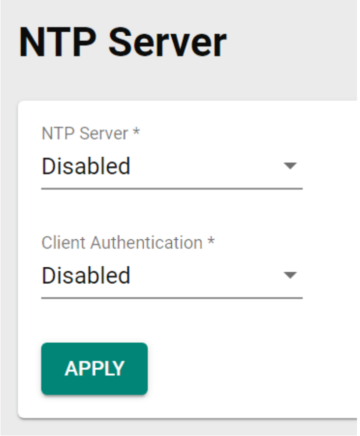
Key String

Setting	Description	Factory Default
0 to 32 characters.	Enter the password to use for the authentication key.	None

When finished, click **CREATE**.

NTP Server

This section describes how to configure the **NTP Server** settings.



NTP Server

NTP Server *
Disabled

Client Authentication *
Disabled

NTP Server

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the NTP server.	Disabled

Client Authentication

Setting	Description	Factory Default
Enabled	Enable or disable NTP authentication.	Disabled

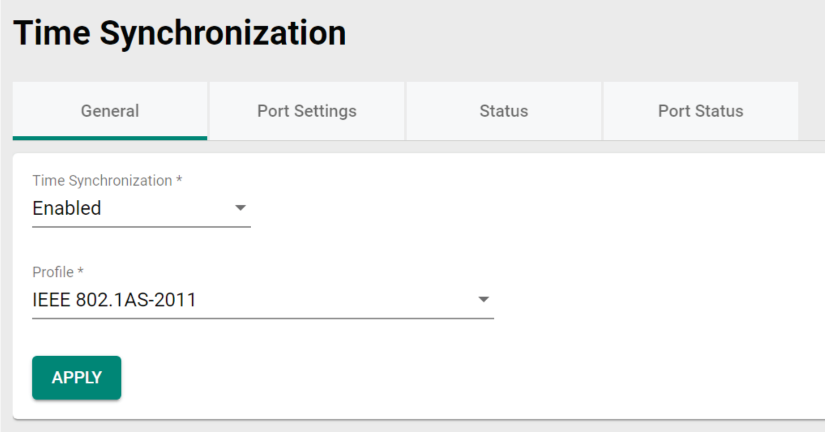
When finished, click **APPLY** to save your changes.

Time Synchronization

This section describes how to configure the time synchronization settings for **802.1AS (gPTP), IEEE 1588v2 (PTP)**, and **Multiple Profiles (802.1AS + 1588v2 Default).**

General Settings

Click **Time Synchronization** from the function menu, and then click **General**.



Time Synchronization

Time Synchronization *
Enabled

Profile *
IEEE 802.1AS-2011

Configure the following settings:

Time Synchronization

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the Time Synchronization function.	Enabled

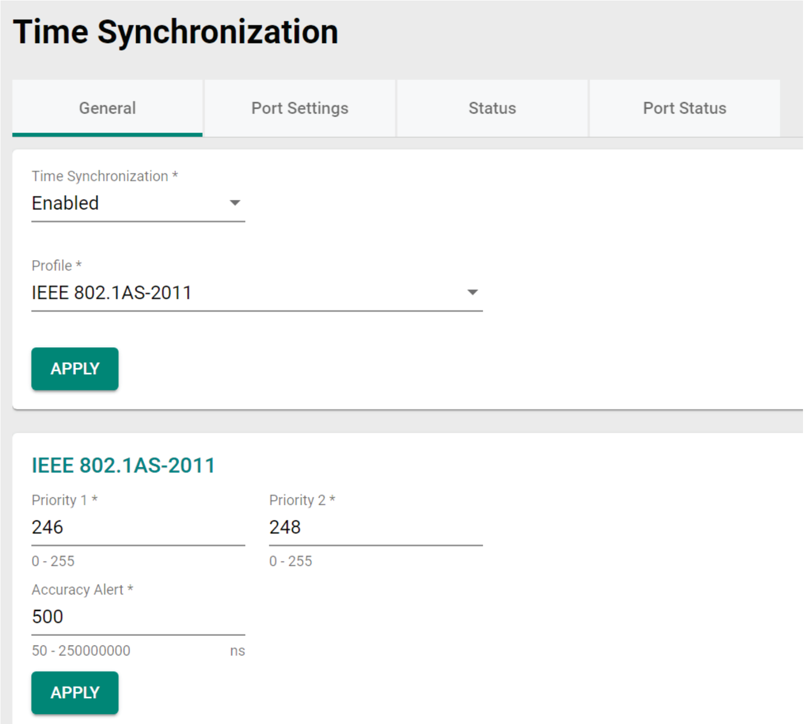
Profile

Setting	Description	Factory Default
IEEE 802.1AS-2011	Use IEEE 802.1AS-2011 (gPTP) as the Time Synchronization profile.	IEEE 802.1AS-2011

Setting	Description	Factory Default
IEEE 1588 Default-2008	Use IEEE 1588 Default-2008 (PTP) as the Time Synchronization profile.	
Multiple Profiles (802.1AS + 1588v2 Default)	Use different profiles (IEEE 802.1AS-2011 or IEEE 1588 Default-2008) on different ports.	

When finished, click **APPLY** to save your changes.

IEEE 802.1AS-2011 Profile Time Synchronization



Time Synchronization

Time Synchronization *: Enabled

Profile *: IEEE 802.1AS-2011

IEEE 802.1AS-2011

Priority 1 *: 246 (0 - 255)

Priority 2 *: 248 (0 - 255)

Accuracy Alert *: 500 (50 - 250000000 ns)

To use the IEEE 802.1AS-2011 (gPTP) as the Time Synchronization profile, select **IEEE 802.1AS-2011** from the drop-down list under **Profile** and Configure the following settings:

Priority 1

Setting	Description	Factory Default
0 to 255	Specify the value for priority 1. Lower values take precedence.	246

Priority 2

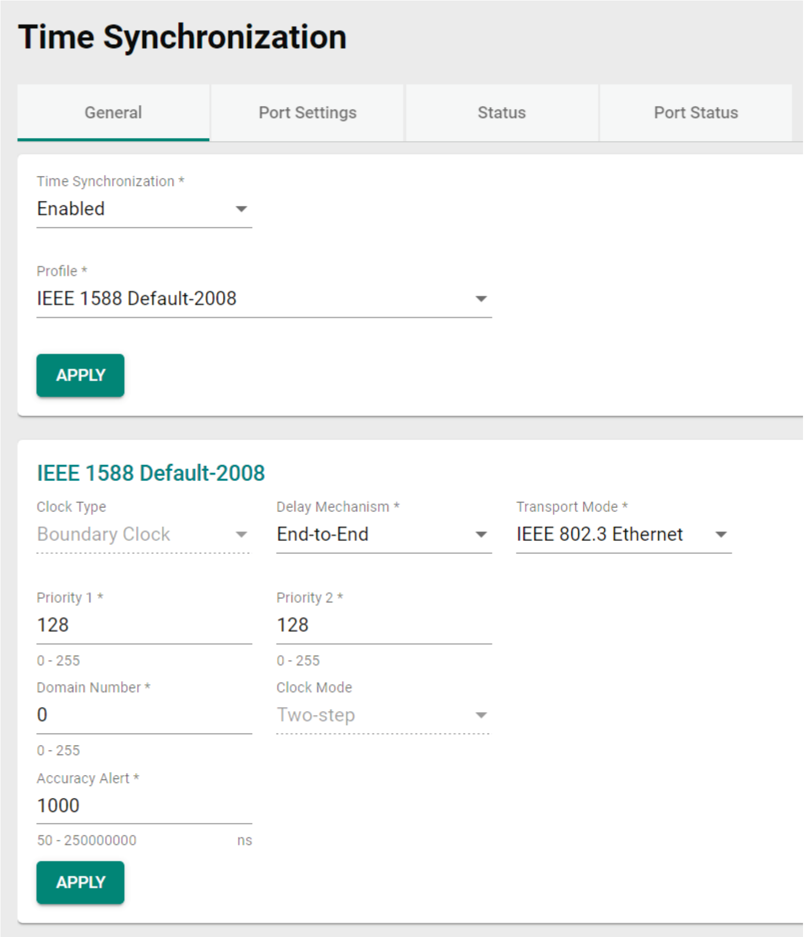
Setting	Description	Factory Default
0 to 255	Specify the value for priority 2. Lower values take precedence.	248

Accuracy Alert

Setting	Description	Factory Default
50 to 250,000,000	Configure the time accuracy threshold (in nanoseconds).	500

When finished, click **APPLY** to save your changes.

IEEE 1588 Default-2008 Profile Time Synchronization



Time Synchronization *
Enabled

Profile *
IEEE 1588 Default-2008

IEEE 1588 Default-2008

Clock Type
Boundary Clock

Delay Mechanism *
End-to-End

Transport Mode *
IEEE 802.3 Ethernet

Priority 1 *
128
0 - 255

Priority 2 *
128
0 - 255

Domain Number *
0
0 - 255

Clock Mode
Two-step

Accuracy Alert *
1000
50 - 250000000 ns

To use the IEEE 1588 Default-2008 (PTP) as the Time Synchronization profile, select **IEEE 1588 Default-2008** from the drop-down list under **Profile** and Configure the following settings:

Clock Type (read only)

Information	Description	Factory Default
Boundary Clock	Operates as an IEEE 1588 PTP boundary clock.	Boundary Clock

Delay Mechanism

Setting	Description	Factory Default
End-to-End	Select End-to-End method as the delay mechanism.	End-to-End
Peer-to-Peer	Select Peer-to-Peer method as the delay mechanism.	

Transport Mode

Setting	Description	Factory Default
IEEE 802.3 Ethernet	Configure PTP implementations using Ethernet format.	IEEE 802.3 Ethernet
UDP IPv4	Configure PTP implementations using UDP/IPv4.	

Priority 1

Setting	Description	Factory Default
0 to 255	Specify the value for priority 1. Lower values take precedence.	128

Priority 2

Setting	Description	Factory Default
0 to 255	Specify the value for priority 2. Lower values take precedence.	128

Domain Number

<table>
<tr><th>Setting</th><th colspan="2">Description</th><th>Factory Default</th></tr>
<tr><td rowspan="8">0 to 255</td><td colspan="2">A domain defines the scope of communication, state, operations, data sets, and timescale of the PTP message.</td><td rowspan="8">0</td></tr>
<tr><td><b>Value (decimal)</b></td><td><b>Definition</b></td></tr>
<tr><td>0</td><td>Default domain</td></tr>
<tr><td>1</td><td>Alternate domain</td></tr>
<tr><td>2</td><td>Alternate domain</td></tr>
<tr><td>3</td><td>Alternate domain</td></tr>
<tr><td>4 to 127</td><td>User-defined domains</td></tr>
<tr><td>128 to 255</td><td>Reserved</td></tr>
</table>

Clock Mode (read only)

Information	Description	Factory Default
Two Step	Set the clock mode to two-step clock.	Two Step

Accuracy Alert

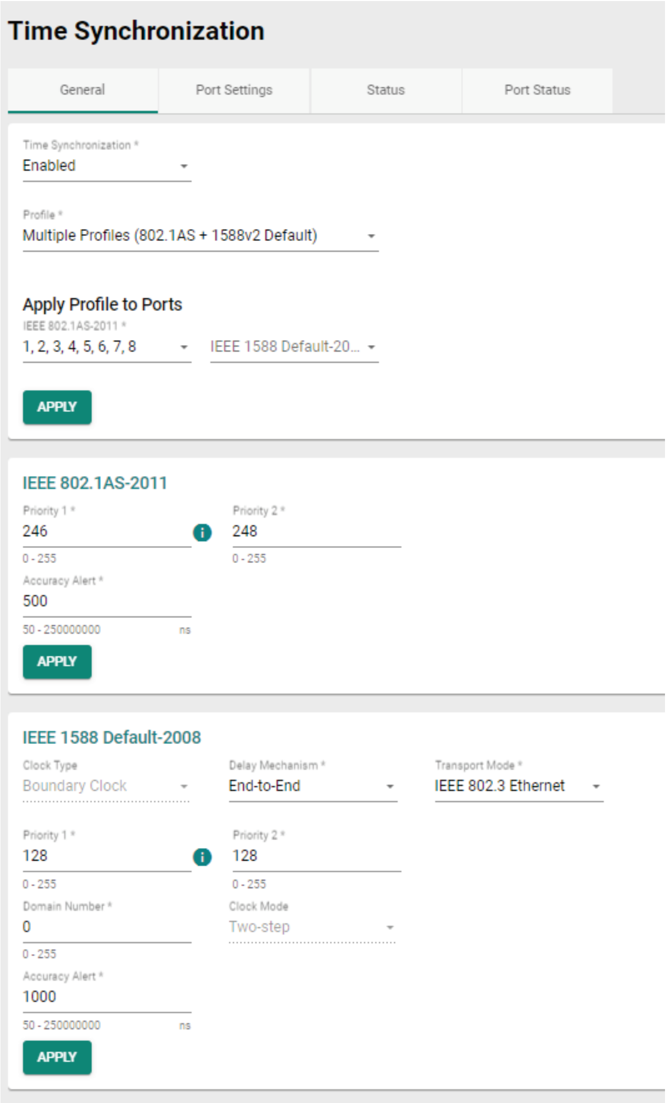
Setting	Description	Factory Default
50 to 250,000,000	Configure the time accuracy threshold (in nanoseconds).	1000

When finished, click **APPLY** to save your changes.

Multiple Profiles (802.1AS + 1588v2 Default) Time Synchronization

NOTE

This function is only supported on TSN Series models with firmware v2.3 or later.



Time Synchronization *
Enabled

Profile *
Multiple Profiles (802.1AS + 1588v2 Default)

Apply Profile to Ports

IEEE 802.1AS-2011 *
1, 2, 3, 4, 5, 6, 7, 8

IEEE 1588 Default-20...

IEEE 802.1AS-2011

Priority 1 *
246
0 - 255

Priority 2 *
248
0 - 255

Accuracy Alert *
500
50 - 250000000 ns

IEEE 1588 Default-2008

Clock Type
Boundary Clock

Delay Mechanism *
End-to-End

Transport Mode *
IEEE 802.3 Ethernet

Priority 1 *
128
0 - 255

Priority 2 *
128
0 - 255

Domain Number *
0
0 - 255

Clock Mode
Two-step

Accuracy Alert *
1000
50 - 250000000 ns

To use different Time Synchronization profiles (IEEE 802.1AS-2011 or IEEE 1588 Default-2008) on different ports, select **Multiple Profiles (802.1AS + 1588v2 Default)** from the drop-down list under **Profile** and Configure the following settings:

Apply Profile to Ports

IEEE 802.1AS-2011

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) to use the IEEE 802.1AS-2011 profile from the drop-down list.	Enabled

IEEE 1588 Default-2008

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) to use the IEEE 1588 Default-2008 profile from the drop-down list.	Enabled

When finished, click **APPLY** to save your changes.

IEEE 802.1AS-2011

Priority 1

Setting	Description	Factory Default
0 to 255	Specify the value for priority 1. Lower values take precedence.	246

Priority 2

Setting	Description	Factory Default
0 to 255	Specify the value for priority 2. Lower values take precedence.	248

Accuracy Alert

Setting	Description	Factory Default
50 to 250,000,000	Configure the time accuracy threshold.	500

When finished, click **APPLY** to save your changes.

IEEE 1588 Default-2008

Clock Type (read only)

Information	Description	Factory Default
Boundary Clock	Operates as an IEEE 1588 PTP boundary clock.	Boundary Clock

Delay Mechanism

Setting	Description	Factory Default
End-to-End	Select End-to-End method as the delay mechanism.	End-to-End
Peer-to-Peer	Select Peer-to-Peer method as the delay mechanism.	

Transport Mode

Setting	Description	Factory Default
IEEE 802.3 Ethernet	Configure PTP implementations using Ethernet format.	IEEE 802.3 Ethernet
UDP IPv4	Configure PTP implementations using UDP/IPv4.	

Priority 1

Setting	Description	Factory Default
0 to 255	Specify the value for priority 1. Lower values take precedence.	128

Priority 2

Setting	Description	Factory Default
0 to 255	Specify the value for priority 2. Lower values take precedence.	128

Domain Number

<table>
<tr><th>Setting</th><th>Description</th><th>Factory Default</th></tr>
<tr><td>0 to 255</td><td>A domain defines the scope of communication, state, operations, data sets, and timescale of the PTP message.
<table>
<tr><th>Value(decimal)</th><th>Definition</th></tr>
<tr><td>0</td><td>Default domain</td></tr>
<tr><td>1</td><td>Alternate domain</td></tr>
<tr><td>2</td><td>Alternate domain</td></tr>
<tr><td>3</td><td>Alternate domain</td></tr>
<tr><td>4 to 127</td><td>User-defined domains</td></tr>
<tr><td>128 to 255</td><td>Reserved</td></tr>
</table></td><td>0</td></tr>
</table>

Clock Mode (read only)

Information	Description	Factory Default
Two Step	Set the clock mode to two-step clock.	Two Step

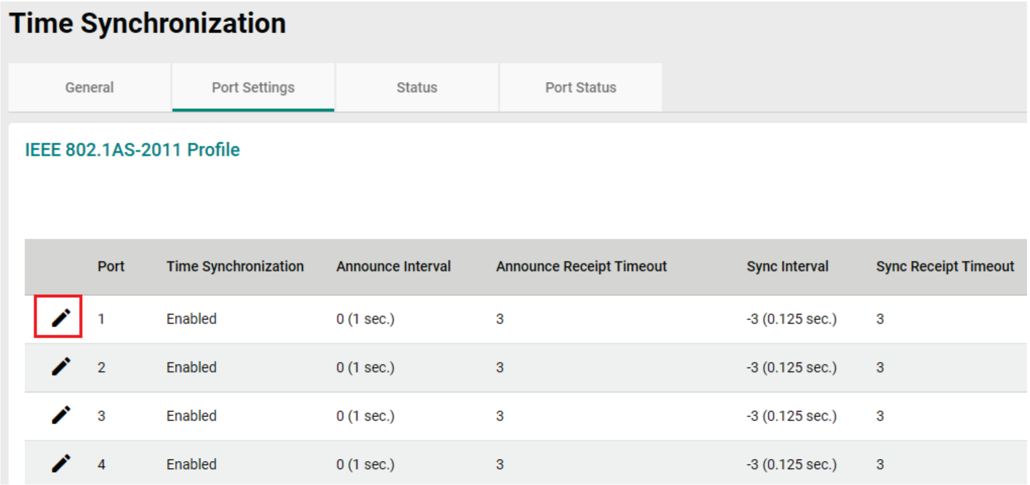
Accuracy Alert

Setting	Description	Factory Default
50 to 250,000,000	Configure the time accuracy threshold (in nanoseconds).	1000

When finished, click **APPLY** to save your changes.

Port Settings for IEEE 802.1AS-2011

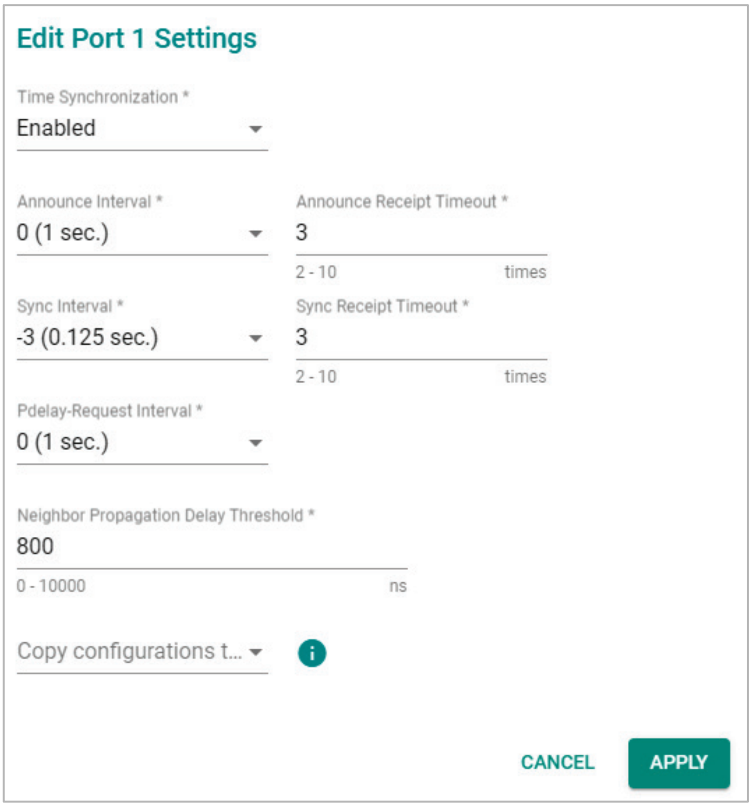
Click the **Port Settings** tab and then select the edit icon for the port you want to configure.



IEEE 802.1AS-2011 Profile

	Port	Time Synchronization	Announce Interval	Announce Receipt Timeout	Sync Interval	Sync Receipt Timeout
✎	1	Enabled	0 (1 sec.)	3	-3 (0.125 sec.)	3
✎	2	Enabled	0 (1 sec.)	3	-3 (0.125 sec.)	3
✎	3	Enabled	0 (1 sec.)	3	-3 (0.125 sec.)	3
✎	4	Enabled	0 (1 sec.)	3	-3 (0.125 sec.)	3

Configure the following settings:



Edit Port 1 Settings

Time Synchronization *
Enabled

Announce Interval *
0 (1 sec.)

Announce Receipt Timeout *
3
2 - 10 times

Sync Interval *
-3 (0.125 sec.)

Sync Receipt Timeout *
3
2 - 10 times

Pdelay-Request Interval *
0 (1 sec.)

Neighbor Propagation Delay Threshold *
800
0 - 10000 ns

Time Synchronization

Setting	Description	Factory Default
Enabled	Enable the Time Synchronization function.	Enabled
Disabled	Disable the Time Synchronization function.	

Announce Interval (sec.)

Setting	Description	Factory Default
0 to 4 (1 sec. to 16 sec.)	Select the announcement interval	0 (1 sec.)

Announce Receipt Timeout (sec.)

Setting	Description	Factory Default
2 to 10	Specify the announcement receipt timeout interval value.	3

Sync Interval

Setting	Description	Factory Default
-3 to 5 (0.125 sec. to 32 sec.)	Select the synchronization interval value.	-3 (0.125 sec.)

Sync Receipt Timeout

Setting	Description	Factory Default
2 to 10	Select the synchronization receipt timeout value.	3

Pdelay-Request Interval

Setting	Description	Factory Default
-3 to 5 (0.25 sec. to 32 sec.)	Select the Pdelay request interval value.	0 (1 sec.)

Neighbor Propagation Delay Threshold (in ns)

Setting	Description	Factory Default
1 to 10000	Specify the value of the neighbor propagation delay threshold. Setting this value to 0 will disable the Neighbor Propagation function, and will leave the port to always be in 1AS mode.	800

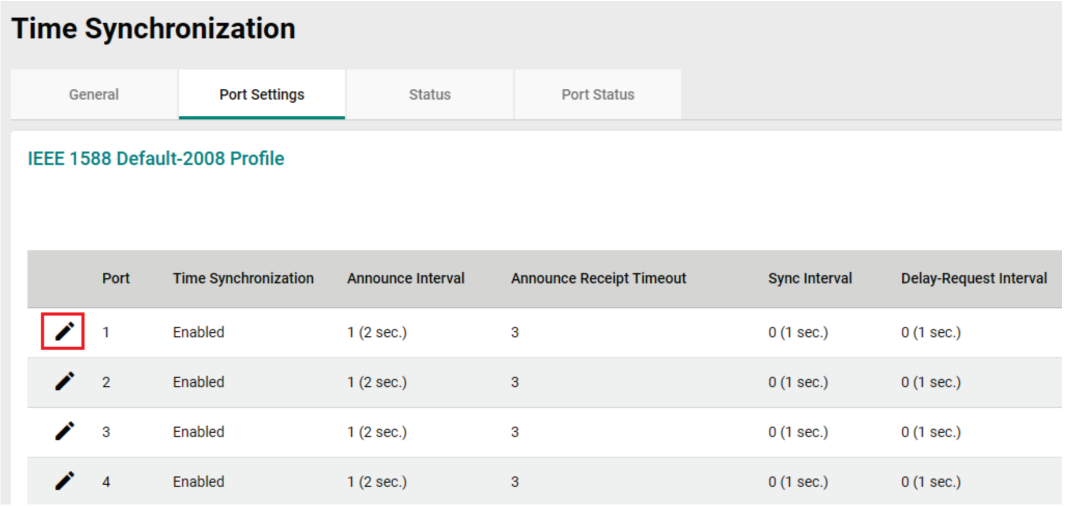
Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configuration to other port(s).	None

When finished, click **APPLY** to save your changes.

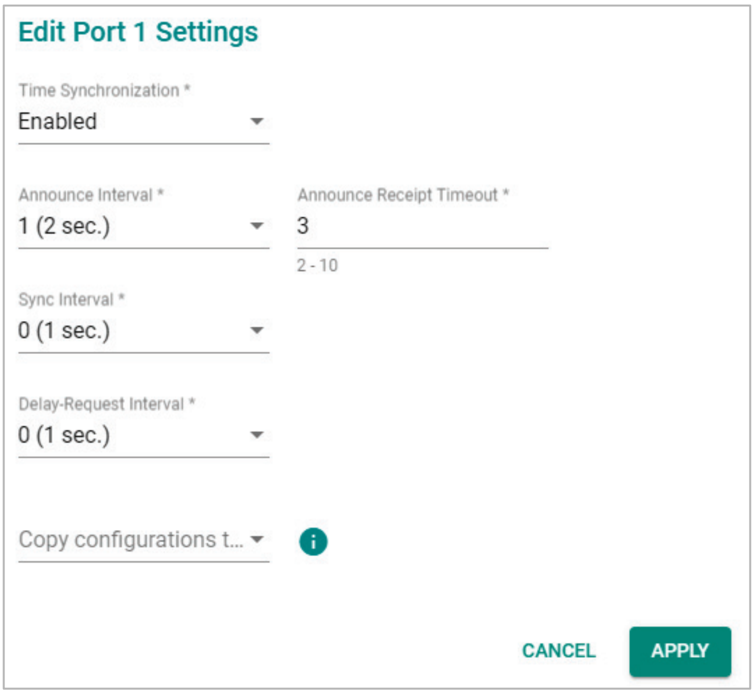
Port Settings for IEEE 1588 Default-2008

Click **Port Settings** tab and then select the edit icon for the port you want to configure.



	Port	Time Synchronization	Announce Interval	Announce Receipt Timeout	Sync Interval	Delay-Request Interval
✎	1	Enabled	1 (2 sec.)	3	0 (1 sec.)	0 (1 sec.)
✎	2	Enabled	1 (2 sec.)	3	0 (1 sec.)	0 (1 sec.)
✎	3	Enabled	1 (2 sec.)	3	0 (1 sec.)	0 (1 sec.)
✎	4	Enabled	1 (2 sec.)	3	0 (1 sec.)	0 (1 sec.)

Configure the following settings:



Edit Port 1 Settings

Time Synchronization *
Enabled

Announce Interval *
1 (2 sec.)

Announce Receipt Timeout *
3
2 - 10

Sync Interval *
0 (1 sec.)

Delay-Request Interval *
0 (1 sec.)

Time Synchronization

Setting	Description	Factory Default
Enabled	Enable the Time Synchronization function.	Enabled
Disabled	Disable the Time Synchronization function.	

Announce Interval (sec.)

Setting	Description	Factory Default
0 to 4 (1 sec. to 16 sec.)	Select the announcement interval value	1 (2 sec.)

Announce Receipt Timeout (sec.)

Setting	Description	Factory Default
2 to 10	Select the announcement receipt timeout interval value.	3

Sync Interval

Setting	Description	Factory Default
-3 to 5 (0.125 sec. to 32 sec.)	Select the synchronization interval value	0 (1 sec.)

Delay-Request Interval

Setting	Description	Factory Default
-3 to 5 (0.25 sec. to 32 sec.)	Select the delay request interval value	0 (1 sec.)

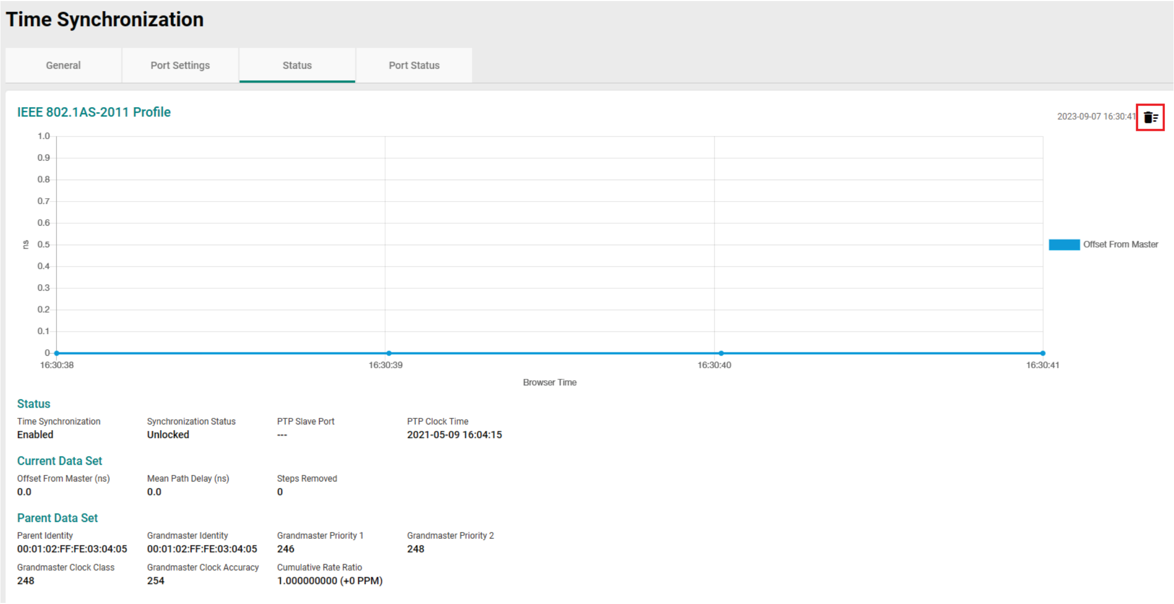
Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configuration to other port(s).	None

When finished, click **APPLY** to save your changes.

Time Synchronization Status

To view the current time synchronization status, click the **Status** tab. You can view the status for IEEE 802.1AS-2011 Profile, IEEE 1588 Default-2008 Profile, or Multiple Profiles (802.1AS + 1588v2 Default). There is a clear graph icon on the upper-right corner of the page. Click the icon to show the latest status. The IEEE 802.1AS-2011 Profile status will appear as shown below.



Status

Time Synchronization Enabled	Synchronization Status Unlocked	PTP Slave Port ---	PTP Clock Time 2021-05-09 16:04:15

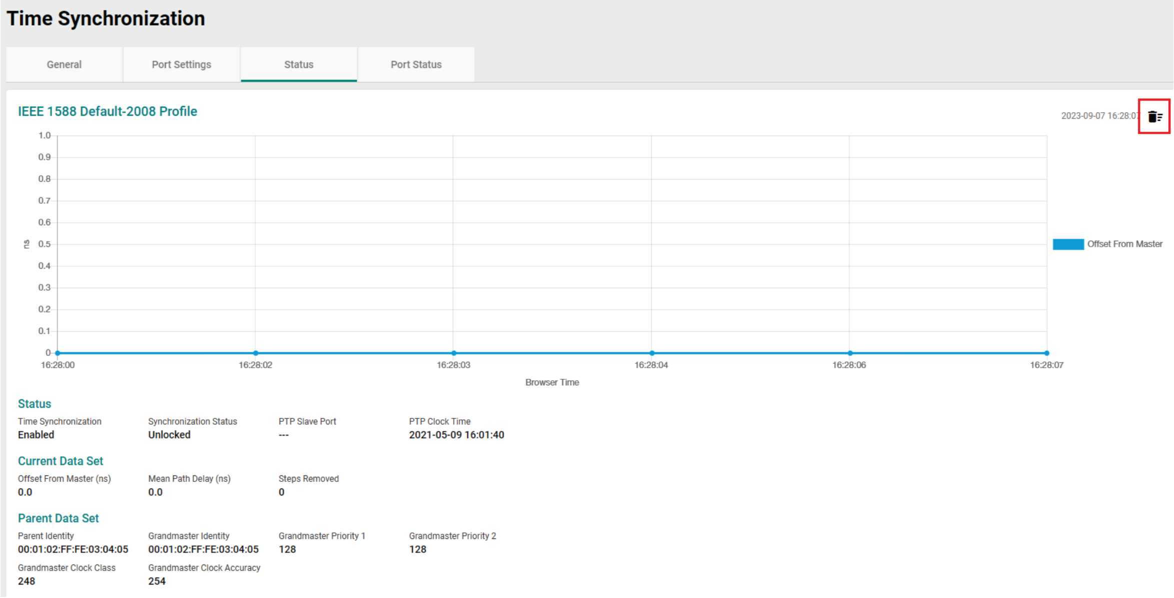
Current Data Set

Offset From Master (ns) 0.0	Mean Path Delay (ns) 0.0	Steps Removed 0

Parent Data Set

Parent Identity 00:01:02:FF:FE:03:04:05	Grandmaster Identity 00:01:02:FF:FE:03:04:05	Grandmaster Priority 1 246	Grandmaster Priority 2 248
Grandmaster Clock Class 248	Grandmaster Clock Accuracy 254	Cumulative Rate Ratio 1.000000000 (+0 PPM)	

The IEEE 1588 Default-2008 Profile Status will appear as shown below.



Status

Time Synchronization Enabled	Synchronization Status Unlocked	PTP Slave Port ---	PTP Clock Time 2021-05-09 16:01:40

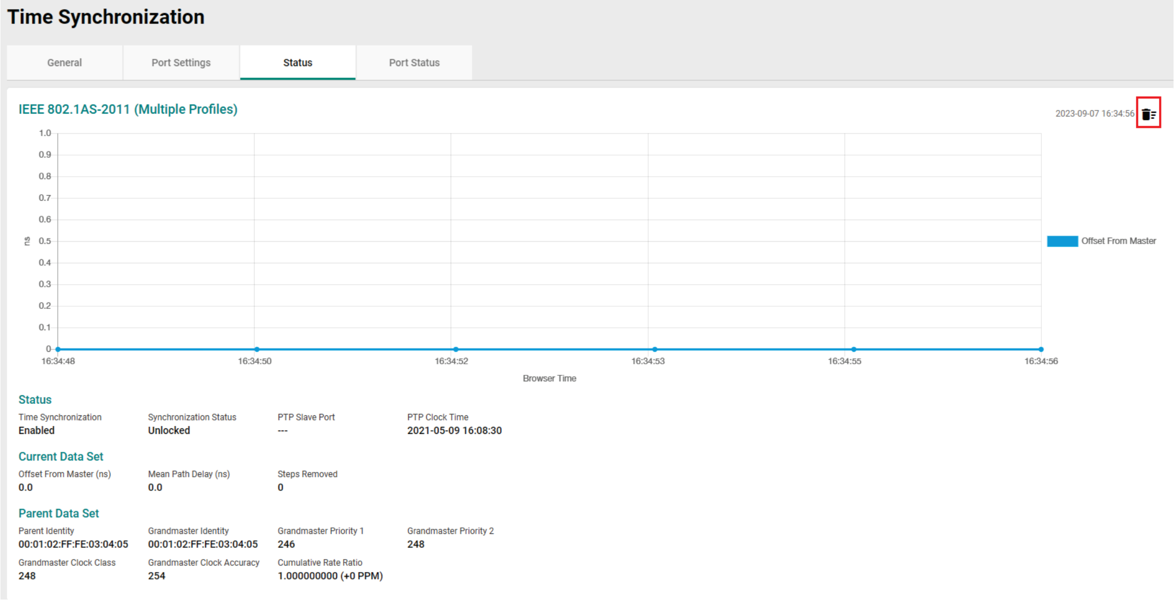
Current Data Set

Offset From Master (ns) 0.0	Mean Path Delay (ns) 0.0	Steps Removed 0

Parent Data Set

Parent Identity 00:01:02:FF:FE:03:04:05	Grandmaster Identity 00:01:02:FF:FE:03:04:05	Grandmaster Priority 1 128	Grandmaster Priority 2 128
Grandmaster Clock Class 248	Grandmaster Clock Accuracy 254		

The IEEE 802.1AS-2011 (Multiple Profiles) Status will appear as shown below.



Status

Time Synchronization: Enabled
Synchronization Status: Unlocked
PTP Slave Port: ---
PTP Clock Time: 2021-05-09 16:08:30

Current Data Set

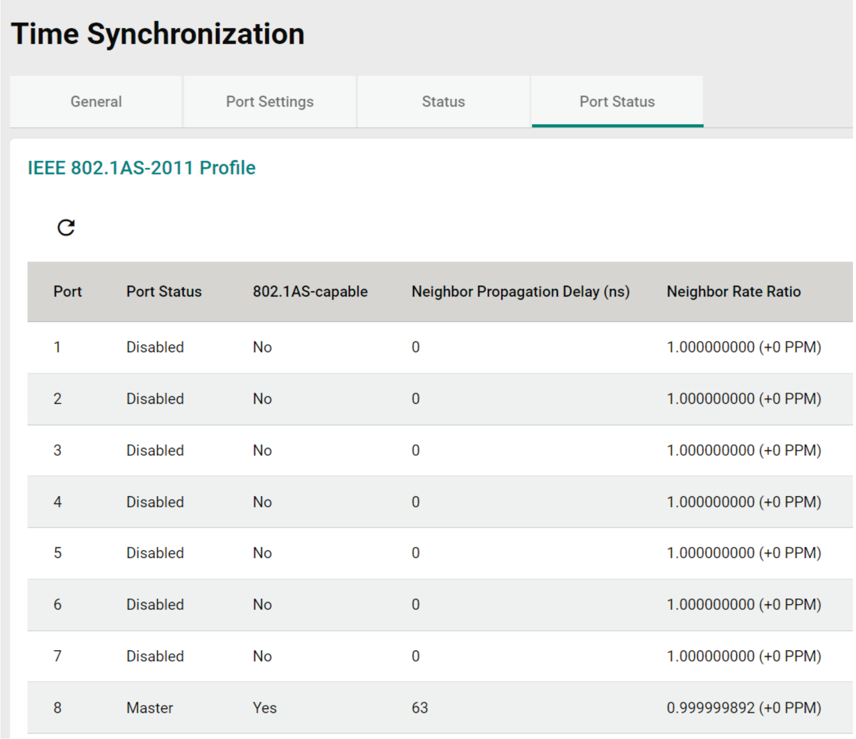
Offset From Master (ns): 0.0
Mean Path Delay (ns): 0.0
Steps Removed: 0

Parent Data Set

Parent Identity: 00:01:02:FF:FE:03:04:05
Grandmaster Identity: 00:01:02:FF:FE:03:04:05
Grandmaster Priority 1: 246
Grandmaster Priority 2: 248
Grandmaster Clock Class: 248
Grandmaster Clock Accuracy: 254
Cumulative Rate Ratio: 1.000000000 (+0 PPM)

Port Status for IEEE 802.1AS-2011 Profile

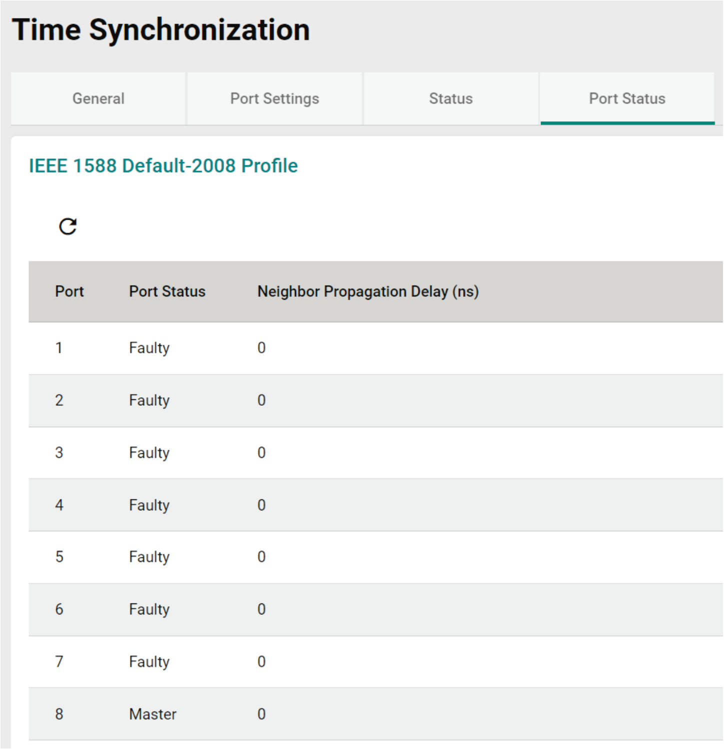
Click the **Port Status** tab to view the port status for IEEE 802.1AS-2011 Profile.



Port	Port Status	802.1AS-capable	Neighbor Propagation Delay (ns)	Neighbor Rate Ratio
1	Disabled	No	0	1.000000000 (+0 PPM)
2	Disabled	No	0	1.000000000 (+0 PPM)
3	Disabled	No	0	1.000000000 (+0 PPM)
4	Disabled	No	0	1.000000000 (+0 PPM)
5	Disabled	No	0	1.000000000 (+0 PPM)
6	Disabled	No	0	1.000000000 (+0 PPM)
7	Disabled	No	0	1.000000000 (+0 PPM)
8	Master	Yes	63	0.999999892 (+0 PPM)

Port Status for IEEE 1588 Default-2008 Profile

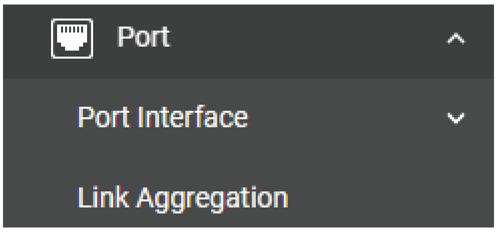
You can view the port status for IEEE 1588 Default-2008 Profile. Click the **Port Status** tab.



Port	Port Status	Neighbor Propagation Delay (ns)
1	Faulty	0
2	Faulty	0
3	Faulty	0
4	Faulty	0
5	Faulty	0
6	Faulty	0
7	Faulty	0
8	Master	0

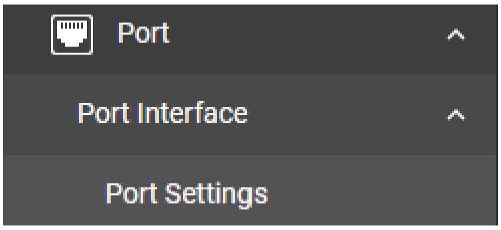
Port

This section describes how to configure the **Port Interface** and **Link Aggregation** functions for the switch.



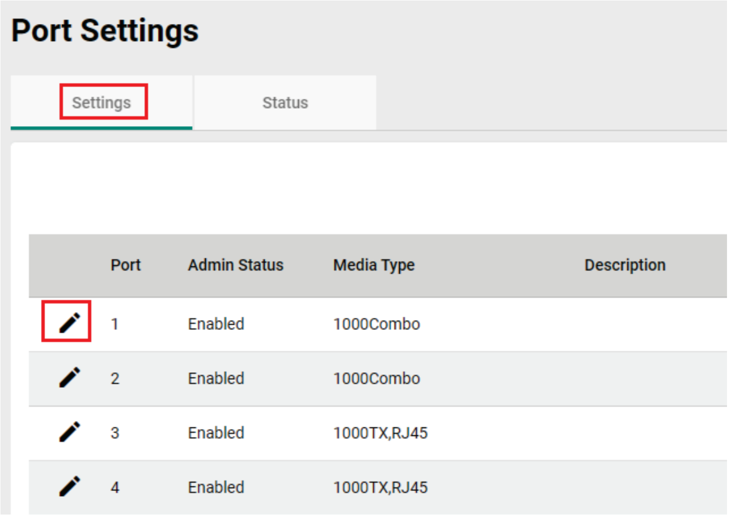
Port Interface

You can configure **Port Settings** in the section.



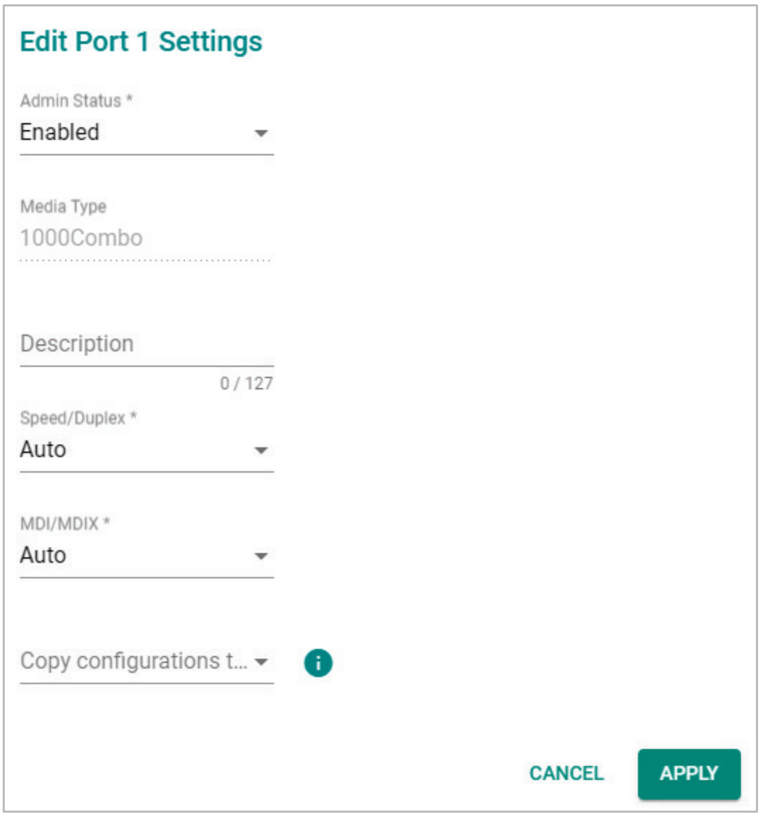
Port Settings

Under **Port Settings**, select the **Settings** tab and then click the edit icon on the port you want to configure.



	Port	Admin Status	Media Type	Description
✎	1	Enabled	1000Combo	
✎	2	Enabled	1000Combo	
✎	3	Enabled	1000TX,RJ45	
✎	4	Enabled	1000TX,RJ45	

Configure the following parameters.


Edit Port 1 Settings

Admin Status *
Enabled

Media Type
1000Combo

Description
0 / 127

Speed/Duplex *
Auto

MDI/MDIX *
Auto

Admin Status

Setting	Description	Factory Default
Enabled	Allows data transmission through this port.	Enabled
Disabled	Disables data transmission through this port.	

Media Type

Setting	Description	Factory Default
Media type	Displays the media type for each module's port (read only).	Port Media Type

Description

Setting	Description	Factory Default
Max. 127 characters	Specify an alias for the port to help differentiate between different ports (e.g., PLC1).	None

Speed/Duplex

Setting	Description	Factory Default
Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection.	Auto
10M Half	Choose a fixed speed option if the connected Ethernet device has trouble auto-negotiating line speed.	
10M Full		
100M Half		
100M Full		

MDI/MDIX

Setting	Description	Factory Default
Auto	Allows the port to auto-detect the port type of the connected Ethernet device, and changes the port type accordingly.	Auto
MDI	Choose MDI or MDIX if the connected Ethernet device has trouble auto-detecting the port type.	
MDIX		

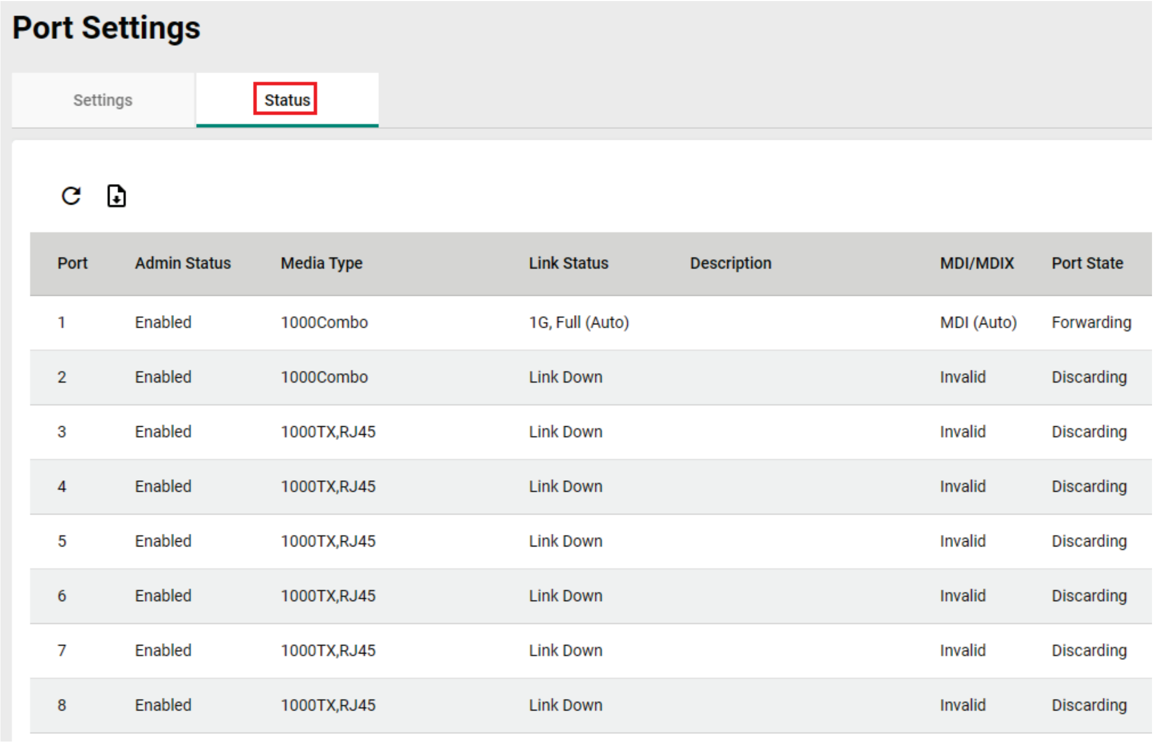
Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configuration to other port(s).	None

When finished, click **APPLY** to save your changes.

Port Status

To view the status of the ports, click the **Status** tab.



Port	Admin Status	Media Type	Link Status	Description	MDI/MDIX	Port State
1	Enabled	1000Combo	1G, Full (Auto)		MDI (Auto)	Forwarding
2	Enabled	1000Combo	Link Down		Invalid	Discarding
3	Enabled	1000TX,RJ45	Link Down		Invalid	Discarding
4	Enabled	1000TX,RJ45	Link Down		Invalid	Discarding
5	Enabled	1000TX,RJ45	Link Down		Invalid	Discarding
6	Enabled	1000TX,RJ45	Link Down		Invalid	Discarding
7	Enabled	1000TX,RJ45	Link Down		Invalid	Discarding
8	Enabled	1000TX,RJ45	Link Down		Invalid	Discarding

Link Aggregation

NOTE

This function is only supported on TSN Series models with firmware v2.3 or later.

This section describes how to configure link aggregation settings for each port. Click **Link Aggregation** from the function menu.

Link Aggregation (Port Channel) Overview

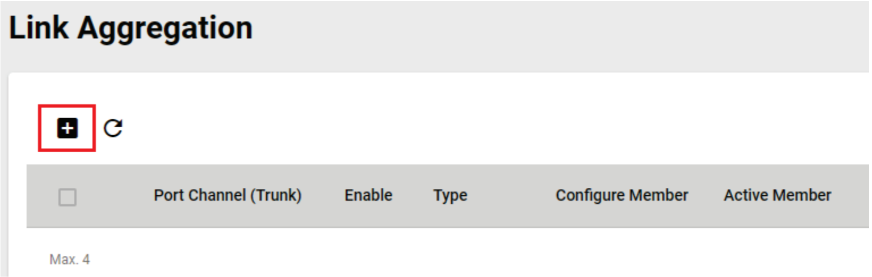
Link Aggregation helps balance, optimize, and facilitate the switch’s throughput. This method can combine multiple network communications in parallel to maximize data throughput, increasing data communication efficiency for each port. In addition, it also acts as a useful method for network redundancy when a link fails. In general, Link Aggregation supports combining multiple physical switch ports into a single, efficient high-bandwidth data communication route. This can improve network load sharing and increase network reliability.

Port Channel

For some networking applications, a situation can arise where traffic from multiple ports is required to be filtered through one port. For example, if there are 30 UHD IP surveillance cameras deployed and connected in a ring, the traffic can stress available bandwidth, causing a surge in traffic that can significantly increase network loading. Hence, the uplink port needs to use the static trunk function to provide more bandwidth and redundancy protection.

Creating a Link Aggregation Group

Click the + icon to create a new link aggregation group.

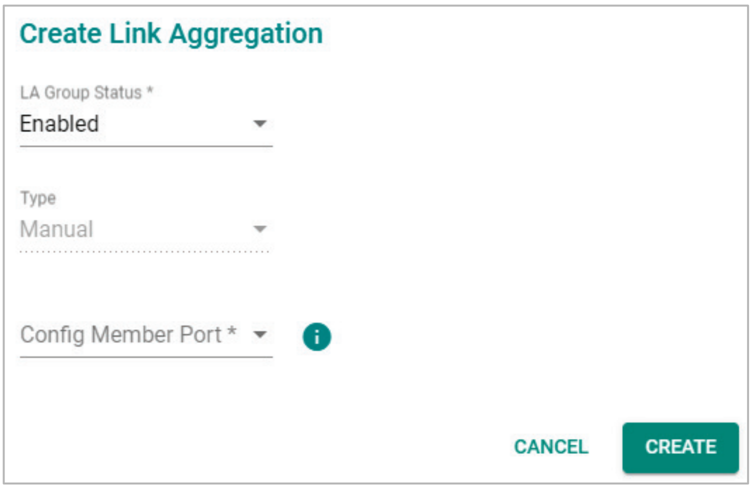


Link Aggregation

□	Port Channel (Trunk)	Enable	Type	Configure Member	Active Member

Max. 4

Configure the following parameters.



Create Link Aggregation

LA Group Status *: Enabled

Type: Manual

Config Member Port *

LA Group Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable link aggregation grouping.	Enabled

Type

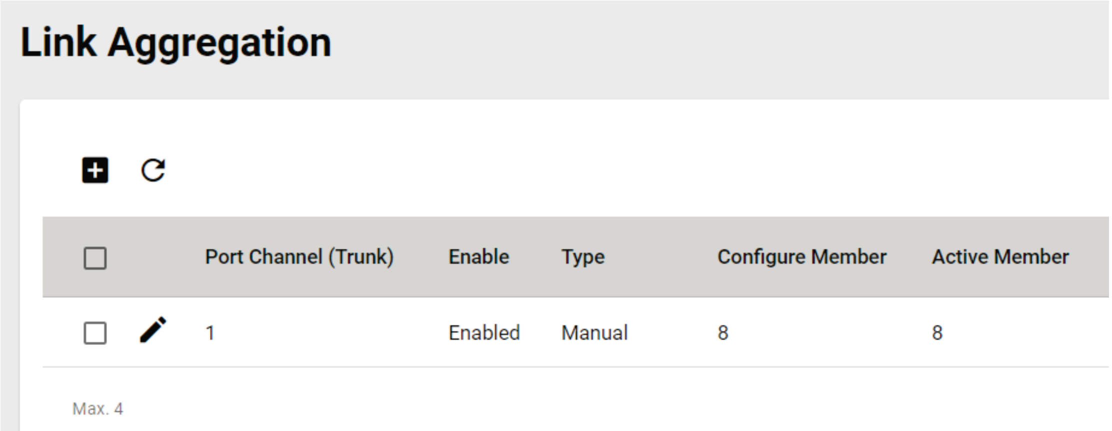
Setting	Description	Factory Default
Manual	Manually configure link aggregation parameters.	Manual

Config Member Port

Setting	Description	Factory Default
Select from the drop-down list	Select the port(s) to add to the link aggregation group.	None

When finished, click **CREATE**.

You can view the current Port Channel (Trunk) status in the table.



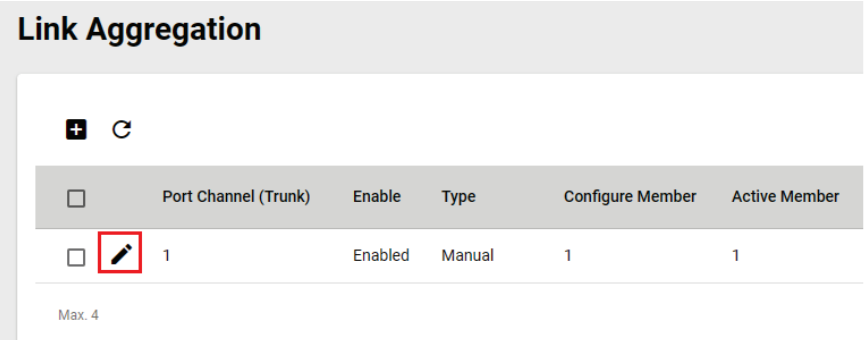
Link Aggregation

□		Port Channel (Trunk)	Enable	Type	Configure Member	Active Member
□	✎	1	Enabled	Manual	8	8

Max. 4

Editing a Link Aggregation Port Channel

To edit a link aggregation port channel, click the edit icon of the port channel you want to modify.

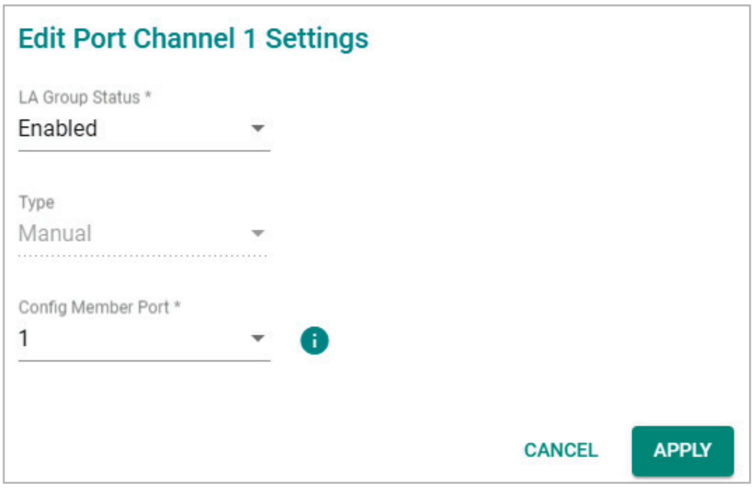


Link Aggregation

□		Port Channel (Trunk)	Enable	Type	Configure Member	Active Member
□	✎	1	Enabled	Manual	1	1

Max. 4

Edit the following port settings.



Edit Port Channel 1 Settings

LA Group Status *: Enabled

Type: Manual

Config Member Port *: 1

LA Group Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable link aggregation grouping.	None

Type

Setting	Description	Factory Default
Manual	Manually configure link aggregation parameters.	Manual

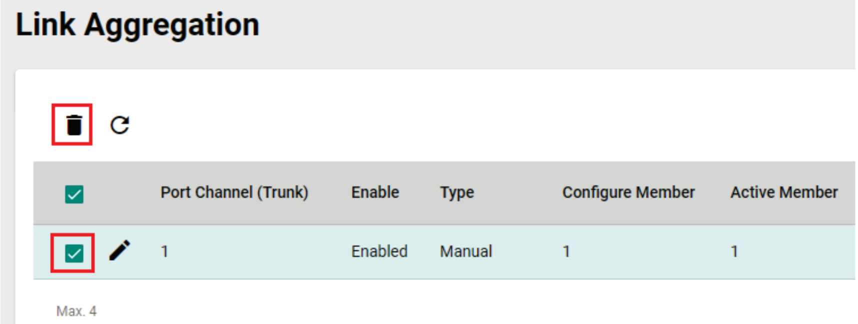
Config Member Port

Setting	Description	Factory Default
Select from the drop-down list	Select the port(s) to add to the link aggregation group.	None

When finished, click **APPLY** to save your changes.

Deleting a Link Aggregation Port Channel

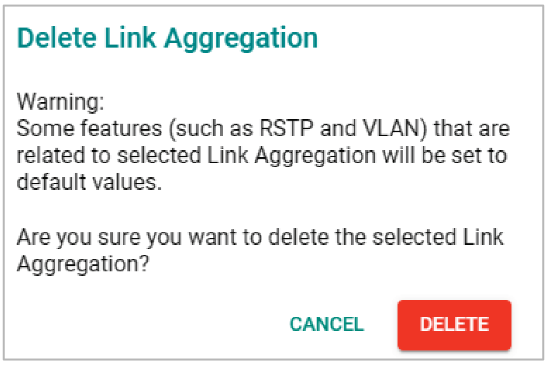
To delete a link aggregation port channel, select the port channel and click the **Delete** icon.



Link Aggregation

☑	Port Channel (Trunk)	Enable	Type	Configure Member	Active Member
☑	1	Enabled	Manual	1	1

Click **DELETE**. Note that some features, such as RSTP and VLAN, will revert to their default values once you delete the Link Aggregation port channel.



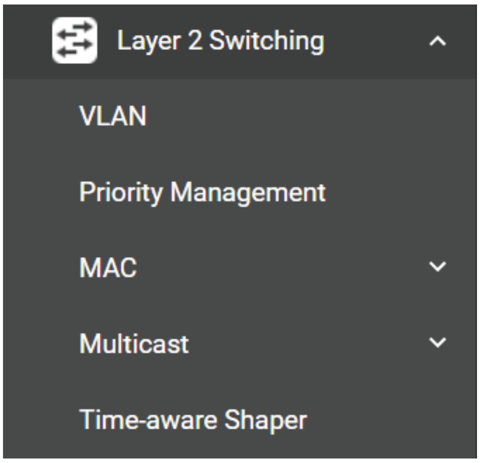
Delete Link Aggregation

Warning:
Some features (such as RSTP and VLAN) that are related to selected Link Aggregation will be set to default values.

Are you sure you want to delete the selected Link Aggregation?

Layer 2 Switching

This section describes how to configure Layer 2 switching functions for the Moxa switch, including **VLAN, Priority Management, MAC, Multicast,** and **Time-aware Shaper**. Click **Layer 2 Switching** from the function menu.



VLAN (IEEE 802.1Q) Overview

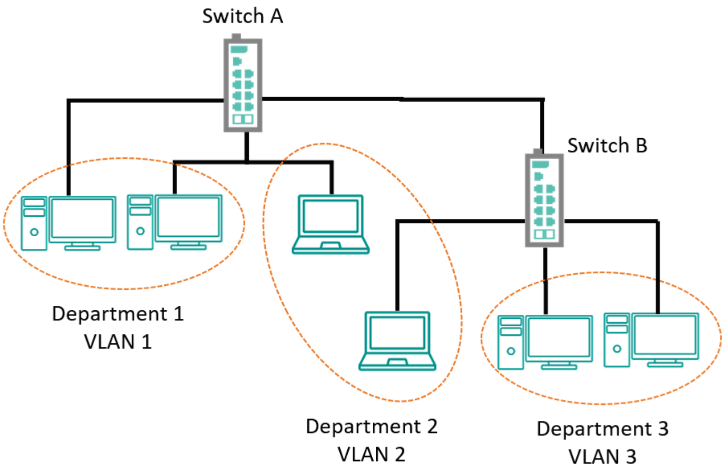
The IEEE 802.1Q is a network communication protocol that falls under the IEEE 802.1 standard regulation, allowing various segments to use a physical network at the same time to block broadcast packets by different segmentations. It specifies the VLAN tagging for Ethernet frames on switches that can control the path process.

How A VLAN Works

What is a VLAN?

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections—a limitation of traditional network design. With VLANs you can segment your network into:

- **Departmental groups—**You could have one VLAN for the marketing department, another for the finance department, and another for the product development department.
- **Hierarchical groups—**You could have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups—**You could have one VLAN for email users and another for multimedia users.



Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

- **VLANs ease the relocation of devices on networks:** With traditional networks, network administrators spend much of their time dealing with changes. If users move to a different subnetwork, the addresses of each host must be updated manually. With a VLAN setup, if a host originally on the Marketing VLAN is moved to a port on another part of the network, and retains its original subnet membership, you only need to specify that the new port is on the Marketing VLAN. You do not need to do any re-cabling.
- **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on the Marketing VLAN needs to communicate with devices on the Finance VLAN, the traffic must pass through a routing device or Layer 3 switch.
- **VLANs help control traffic:** With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether or not they need it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

VLANs and the Moxa switch

Your Moxa switch includes support for VLANs using IEEE Std 802.1Q-2005. This standard allows traffic from multiple VLANs to be carried across one physical link. The IEEE Std 802.1Q-2005 standard allows each port on your Moxa switch to be placed as follows:

- On a single VLAN defined in the switch
- On several VLANs simultaneously using 802.1Q tagging

The standard requires that you define the *802.1Q VLAN ID* for each VLAN on your Moxa switch before the switch can use it to forward traffic:

Managing a VLAN

A new or initialized Moxa switch contains a single VLAN—the Default VLAN. This VLAN has the following definition:

- *VLAN Name*—Management VLAN
- *802.1Q VLAN ID*—1 (if tagging is required)

All the ports are initially placed on this VLAN, and it is the only VLAN that allows you to access the management software of the Moxa switch over the network.

Between VLANs

If devices connected to a VLAN need to communicate with devices on a different VLAN, a router or Layer 3 switching device with connections to both VLANs need to be installed. Communication between VLANs can only take place if they are all connected to a routing or Layer 3 switching device.

VLANs: Tagged and Untagged Membership

Moxa's switch supports 802.1Q VLAN tagging, a system that allows traffic for multiple VLANs to be carried on a single physical link (backbone, trunk). When setting up VLANs you need to understand when to use untagged or tagged membership of VLANs. Simply put, if a port is on a single VLAN it can be an untagged member, but if the port needs to be a member of multiple VLANs, a tagged membership must be defined.

A typical host (e.g., clients) will be an untagged member of one VLAN, defined as an **Access Port** in a Moxa switch, while an inter-switch connection will be a tagged member of all VLANs, defined as a **Trunk Port** in a Moxa switch.

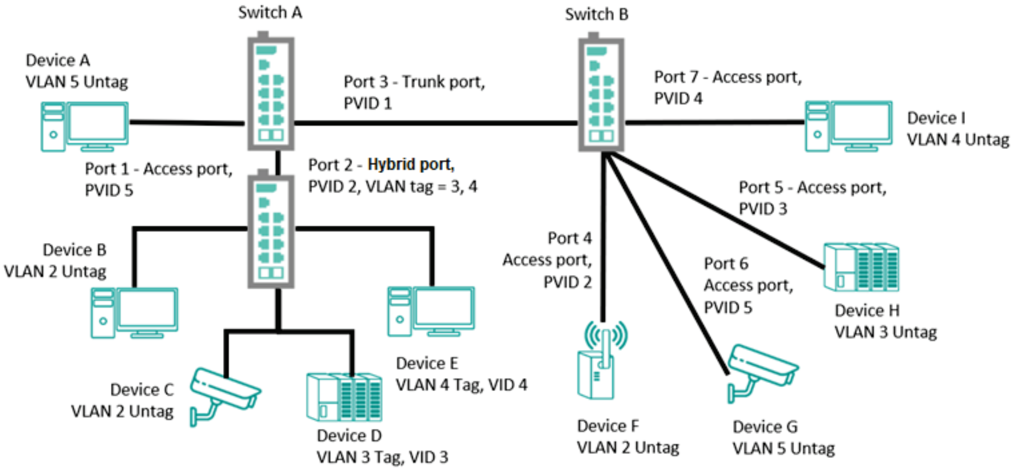
The IEEE Std 802.1Q-2005 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine which VLAN the port belongs to. If a frame is carrying the additional information, it is known as a *tagged* frame.

To carry multiple VLANs across a single physical link (backbone, trunk), each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong to which VLAN. To communicate between VLANs, a router must be used.

Moxa's switch supports three types of VLAN port settings:

- **Access Port:** The port connects to a single device that is not tagged. The user must define the default port PVID that assigns which VLAN the device belongs to. Once the ingress packet of this Access Port egresses to another Trunk Port (the port needs all packets to carry tag information), the switch will insert this PVID into this packet so the next 802.1Q VLAN switch can recognize it.
- **Trunk Port:** The port connects to a LAN that consists of untagged devices, tagged devices, and/or switches and hubs. In general, the traffic of the Trunk Port must have a Tag. Users can also assign a PVID to a Trunk Port. The untagged packet on the Trunk Port will be assigned the default port PVID as its VID.
- **Hybrid Port:** Hybrid ports are similar to Trunk ports, except users can explicitly assign tags to be removed from egress packets.

The following section illustrates how to use these ports to set up different applications.



In this application:

- Port 1 connects a single untagged device and assigns it to VLAN 5. The port should be configured as an **Access Port** with PVID 5.
- Port 2 connects a LAN with two untagged devices belonging to VLAN 2, one tagged device with VID 3 and one tagged device with VID 4. The port should be configured as a **Hybrid** Port with PVID 2 for untagged devices and Fixed VLAN (Tagged) with 3 and 4 for tagged devices. Since each port can only have one unique PVID, all untagged devices on the same port must belong to the same VLAN.
- Port 3 connects with another switch. The port should be configured as a **Trunk Port**. The GVRP protocol will be used through the Trunk Port.
- Port 4 connects a single untagged device and assigns it to VLAN 2. The port should be configured as an **Access Port** with PVID 2.
- Port 5 connects a single untagged device and assigns it to VLAN 3. The port should be configured as an **Access Port** with PVID 3.

- Port 6 connect a single untagged device and assigns it to VLAN 5. The port should be configured as an **Access Port** with PVID 5.
- Port 7 connects a single untagged device and assigns it to VLAN 4. The port should be configured as an **Access Port** with PVID 4.

After the application is properly configured:

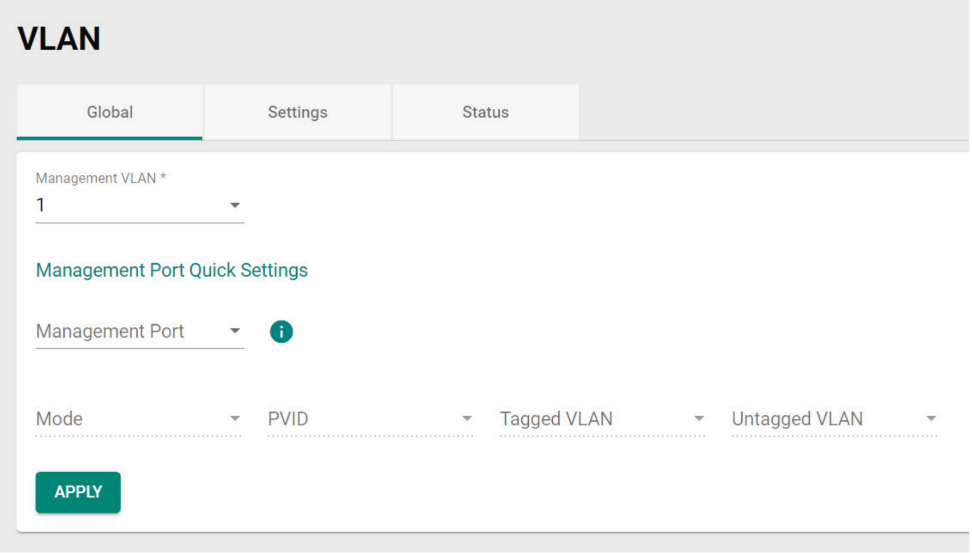
- Packets from Device A will travel through **Trunk Port 3** with tagged VID 5. Switch B will recognize its VLAN, pass it to port 6, and then remove tags received successfully by Device G, and vice versa.
- Packets from Devices B and C will travel through **Hybrid Port** 2 with tagged VID 2. Switch B recognizes its VLAN, passes it to port 4, and then removes tags received successfully by Device F, and vice versa.
- Packets from Device D will travel through **Trunk Port 3** with tagged VID 3. Switch B will recognize its VLAN, pass to port 5, and then remove tags received successfully by Device H. Packets from Device H will travel through **Trunk Port 3** with PVID 3. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by Device D.
- Packets from Device E will travel through **Trunk Port 3** with tagged VID 4. Switch B will recognize its VLAN, pass it to port 7, and then remove tags received successfully by Device I. Packets from Device I will travel through **Trunk Port 3** with tagged VID 4. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by Device E.

VLAN Settings

To configure VLAN settings, click **VLAN** in the function menu, then click the **Global** tab.

VLAN Management Port Quick Setting

You can quickly configure VLAN setting.



Configure the following settings:

Management VLAN

Setting	Description	Factory Default
Select the Management VLAN from the drop-down list	Show the list of selectable VLANs.	1

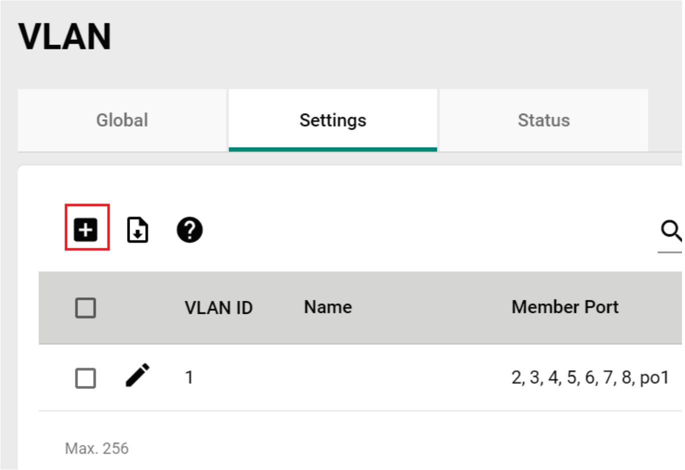
Management Port

Setting	Description	Factory Default
Select the port(s) as the management port(s) from the drop-down list	To select the port(s) to act as the management port(s).	None

When finished, click **APPLY** to save your changes.

Adding a VLAN

On the **VLAN** page, first click the **Settings** tab, and then click the + icon.



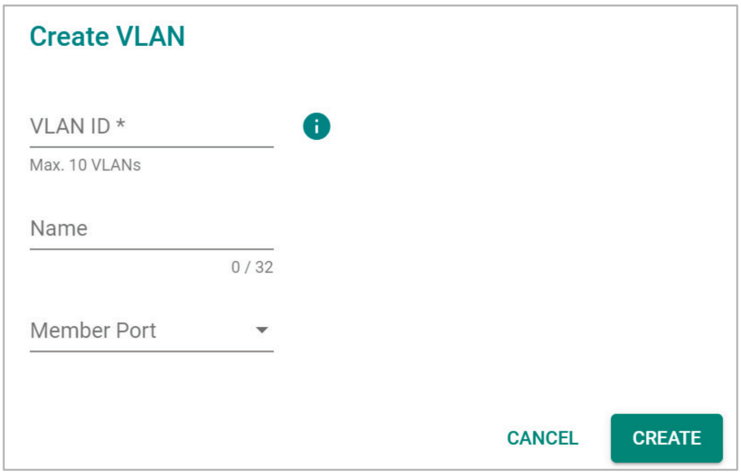
VLAN

Global | Settings | Status

□	VLAN ID	Name	Member Port
□	1		2, 3, 4, 5, 6, 7, 8, po1

Max. 256

Configure the following parameters.



Create VLAN

VLAN ID *

Max. 10 VLANs

Name

0 / 32

Member Port

VLAN ID

Setting	Description	Factory Default
Input a VLAN ID, (10 VLANs max.)	Input a VLAN ID.	None

Name

Setting	Description	Factory Default
Input a name for the VLAN, (32 characters max.)	Specify a name for the VLAN.	None

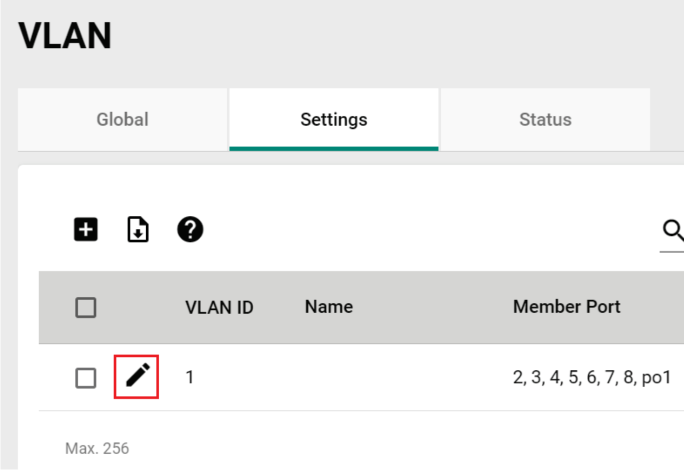
Member Port

Setting	Description	Factory Default
Select the port from the drop-down list.	Specify the ports that are the member ports for the VLAN.	None

When finished, click **CREATE**.

Editing Existing VLAN Settings

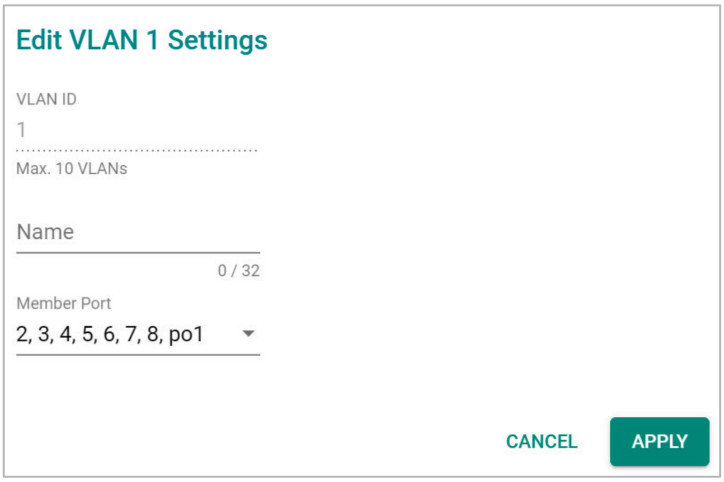
To edit the settings of an existing VLAN, click the edit icon of the VLAN you want to edit.



□		VLAN ID	Name	Member Port
□	✎	1		2, 3, 4, 5, 6, 7, 8, po1

Max. 256

Configure the following settings:


Edit VLAN 1 Settings

VLAN ID: 1

Max. 10 VLANs

Name

0 / 32

Member Port: 2, 3, 4, 5, 6, 7, 8, po1

VLAN ID

Setting	Description	Factory Default
Show the VLAN ID	Display the VLAN ID.	None

Name

Setting	Description	Factory Default
Show the name of the VLAN	Display the VLAN name.	None

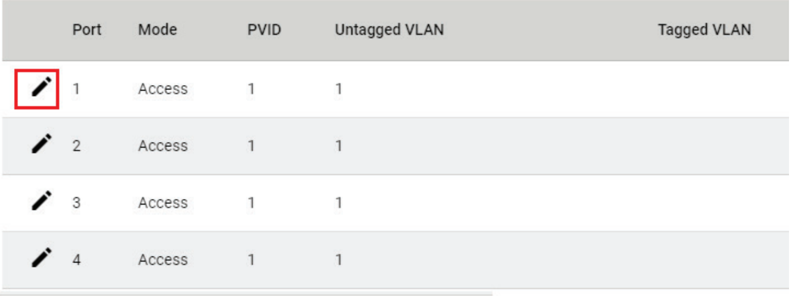
Member Port

Setting	Description	Factory Default
Select the port from the drop-down list	Specify the ports that are member ports for the VLAN.	None

When finished, click **APPLY** to save your changes.

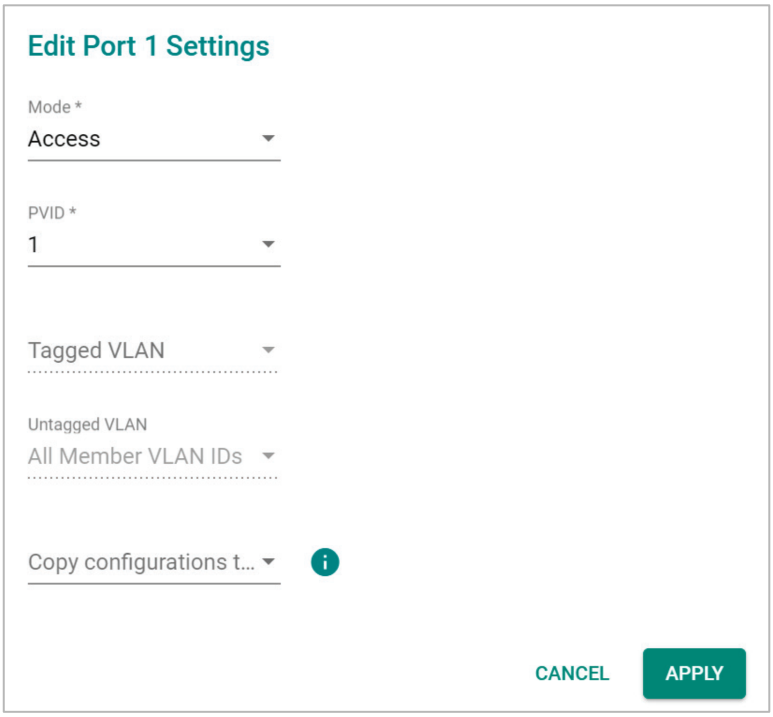
Editing Port Settings

To edit the port settings, click the edit icon off the port you want to configure in the bottom section of the **Settings** page.



	Port	Mode	PVID	Untagged VLAN	Tagged VLAN
✎	1	Access	1	1	
✎	2	Access	1	1	
✎	3	Access	1	1	
✎	4	Access	1	1	

Configure the following settings:



Edit Port 1 Settings

Mode *
Access

PVID *
1

Tagged VLAN

Untagged VLAN
All Member VLAN IDs

Copy configurations t...

Mode

Setting	Description	Factory Default
Access	Configures the port as an access port, used for connecting to a single device, without tags.	Access
Trunk	Configures the port as a trunk port, used for connecting to another 802.1Q VLAN-aware switch.	
Hybrid	Configures the port as a hybrid port, used for connecting to another Access 802.1Q VLAN-aware switch or another LAN that combines tagged and/or untagged devices.	

PVID

Setting	Description	Factory Default
1 to 4094	Sets the default VLAN ID for untagged devices connected to the port.	None

Tagged VLAN

Setting	Description	Factory Default
1 to 4094	This field will be active only when selecting the Trunk type. Set the other VLAN ID for tagged devices that connect to the port. Use commas to separate different VIDs.	Port Name

Untagged VLAN (currently disabled)

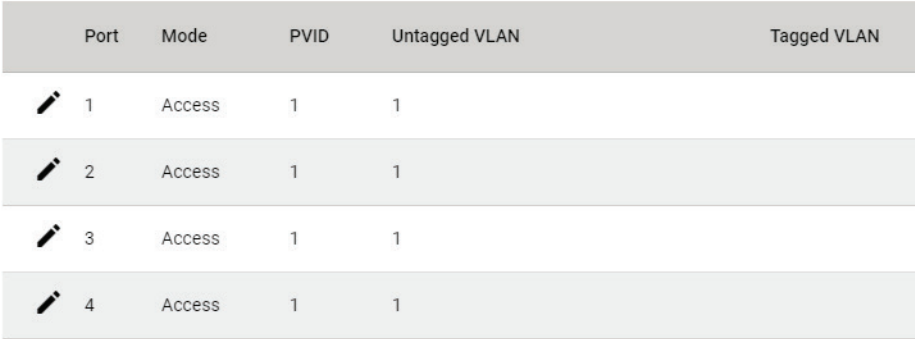
Setting	Description	Factory Default
VID range from 1 to 4094	This field is only active when the Hybrid port type is selected. Set the other VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets. Use commas to separate different VIDs.	Same as the PVID

Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configuration to other port(s).	None

When finished, click **APPLY** to save your changes.

The VLAN table shows an overview of all configured VLANs.



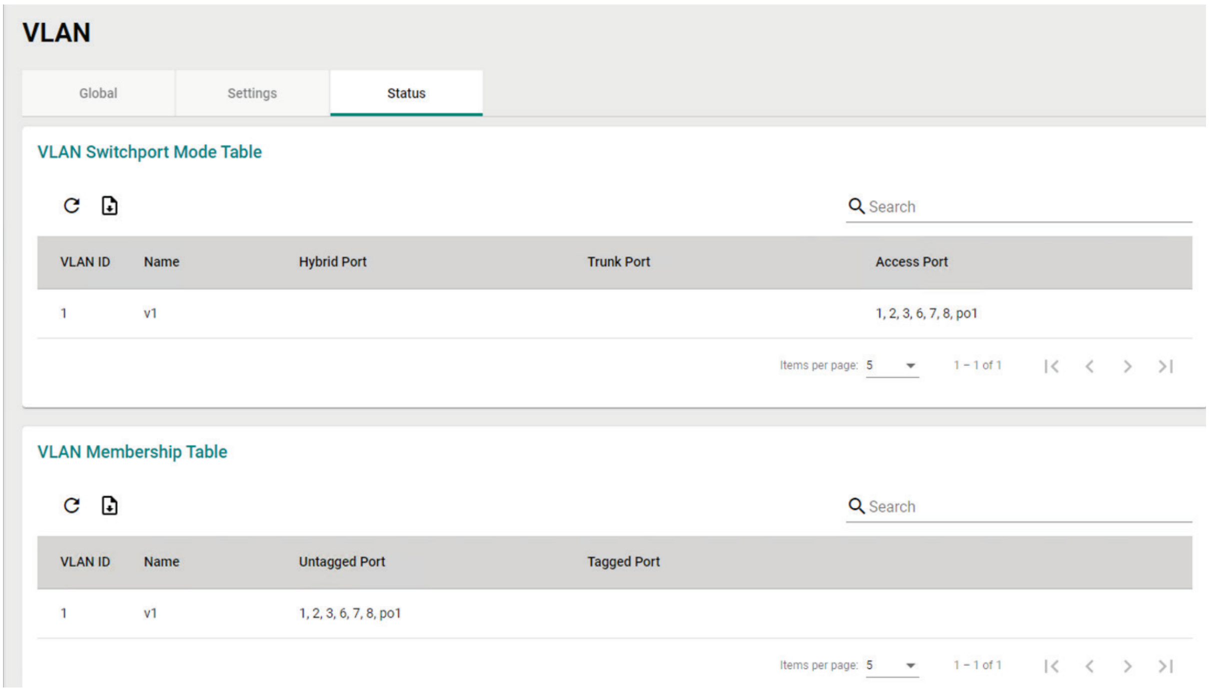
	Port	Mode	PVID	Untagged VLAN	Tagged VLAN
✎	1	Access	1	1	
✎	2	Access	1	1	
✎	3	Access	1	1	
✎	4	Access	1	1	

See the description below for more information.

Port	Mode	PVID	Untagged VLAN	Tagged VLAN
Port number on the switch	VLAN Mode: Access or Trunk	Port default VID of the VLAN	The untagged VLAN list	The tagged VLAN list

VLAN Status

To view VLAN status, click the **Status** tab.



VLAN Switchport Mode Table

VLAN ID	Name	Hybrid Port	Trunk Port	Access Port
1	v1			1, 2, 3, 6, 7, 8, po1

VLAN Membership Table

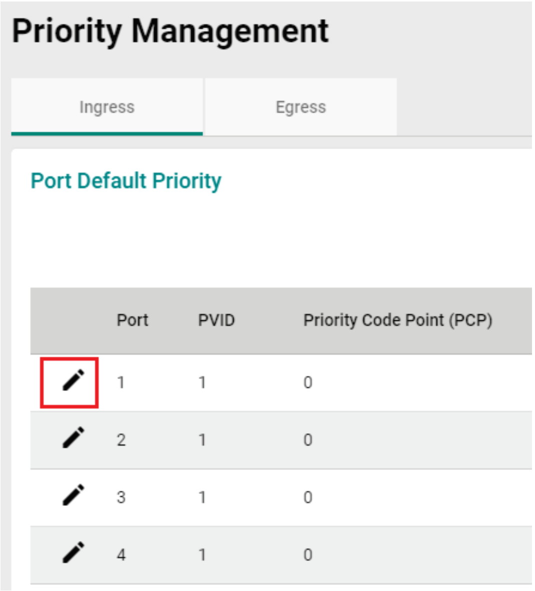
VLAN ID	Name	Untagged Port	Tagged Port
1	v1	1, 2, 3, 6, 7, 8, po1	

Priority Management

This section describes how to configure the ingress and egress priority settings.

Ingress Settings

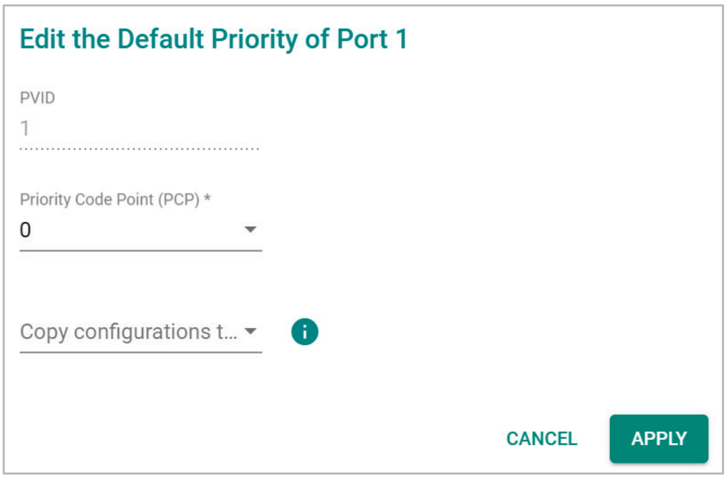
Click the **Ingress** tab and then click the edit icon to configure the default port priority for that port.



Port Default Priority

	Port	PVID	Priority Code Point (PCP)
✎	1	1	0
✎	2	1	0
✎	3	1	0
✎	4	1	0

Configure the following settings:

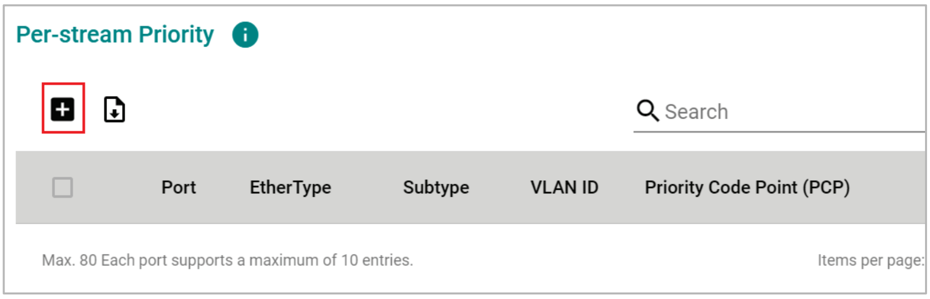

Edit the Default Priority of Port 1

PVID: 1

Priority Code Point (PCP) *: 0

Copy configurations t...

Next, click the + icon to add a Per-stream Priority entry.

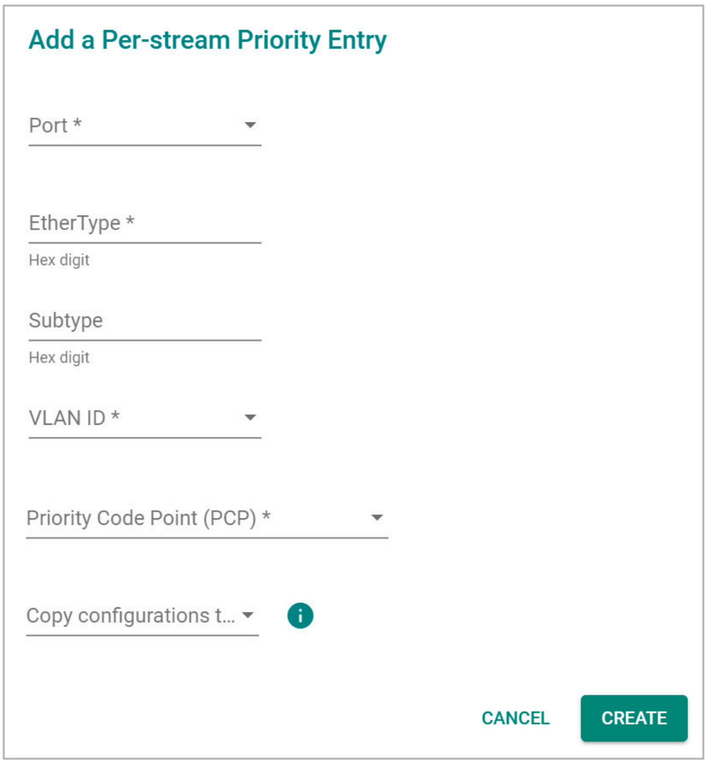

Per-stream Priority

□	Port	EtherType	Subtype	VLAN ID	Priority Code Point (PCP)

Max. 80 Each port supports a maximum of 10 entries.

Items per page:

Configure the following settings:



Add a Per-stream Priority Entry

Port *

EtherType *
Hex digit

Subtype
Hex digit

VLAN ID *

Priority Code Point (PCP) *

Copy configurations t...

Port

Setting	Description	Default
Select port(s) from the list	Select the port(s) to add Per-stream Priority	None

EtherType

Setting	Description	Default
Hex digit	Specify the EtherType hex value for this entry.	None

Subtype

Setting	Description	Default
Hex digit	Specify the Subtype hex value for this entry.	None

VLAN ID

Setting	Description	Default
Select VLAN ID from the drop-down list	Select the VLAN ID for this entry.	None

Priority Code Point (PCP)

Setting	Description	Default
Select the port(s) from the down-down list	Specify the Priority Code Point value in this entry.	None

Copy Configurations to Ports

Setting	Description	Default
Select port(s) from the drop-down list	Copy the configurations to other port(s).	None

When finished, click **CREATE** to complete.

NOTE

The TSN switch will check packets based on the sequence of the entry in the per-stream priority list (from top to bottom) in the per-stream priority table.

For example:

In case 1, packets with EtherType: 0x890F +Subtype:0xC0/0xFF will be treated as compliance with 1st entry rather than 2nd or 3rd entry.

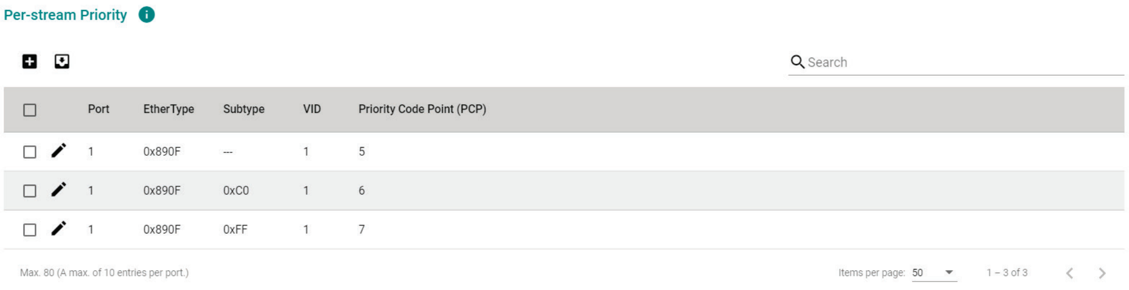
However, in case 2:

Packets with EtherType:0x890F + Subtype:0xC0 will be treated as compliance with 1st entry

Packets with EtherType:0x890F + Subtype:0xFF will be treated as compliance with 2nd entry

Then packets with EtherType:0x890F + Subtype: every will be treated as compliance with 3rd entry

Case 1:

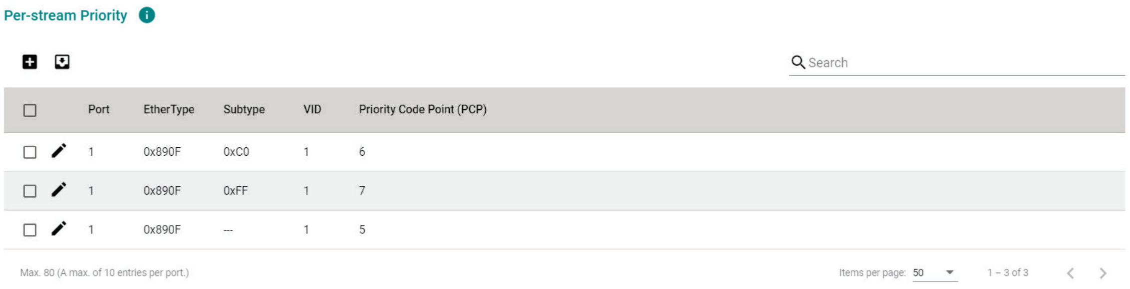


□	Port	EtherType	Subtype	VID	Priority Code Point (PCP)
□	1	0x890F	---	1	5
□	1	0x890F	0xC0	1	6
□	1	0x890F	0xFF	1	7

Max. 80 (A max. of 10 entries per port.)

Items per page: 50 1 – 3 of 3

Case 2:



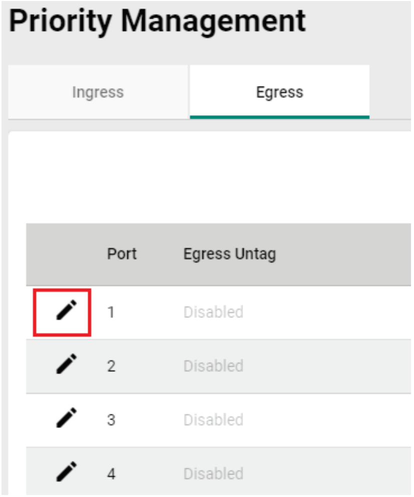
□	Port	EtherType	Subtype	VID	Priority Code Point (PCP)
□	1	0x890F	0xC0	1	6
□	1	0x890F	0xFF	1	7
□	1	0x890F	---	1	5

Max. 80 (A max. of 10 entries per port.)

Items per page: 50 1 – 3 of 3

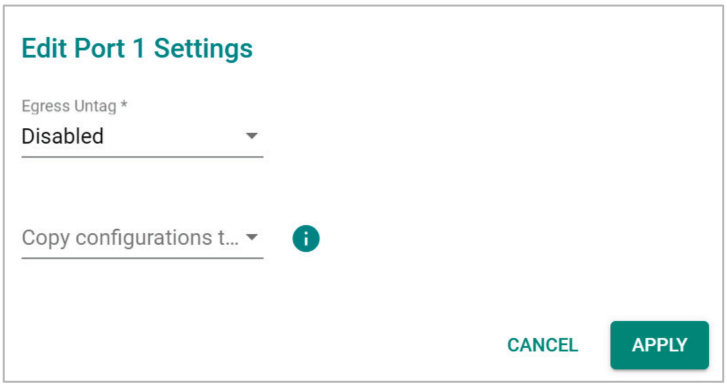
Egress Settings

Click **Egress** tab and click edit icon on the port you want to configure.



Port	Egress Untag
1	Disabled
2	Disabled
3	Disabled
4	Disabled

Configure the following settings:



Egress Untag

Setting	Description	Factory Default
Enabled	Enable Egress Untag.	Disabled
Disabled	Disable Egress Untag.	

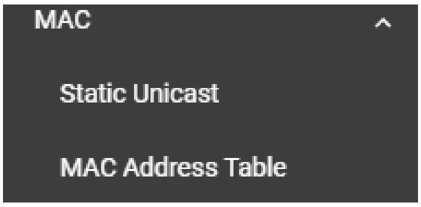
Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configurations to other port(s).	None

When finished, click **APPLY** to save your changes.

MAC

This section explains Independent VLAN learning and describes how to configure **Static Unicast** and the **MAC Address Table**.



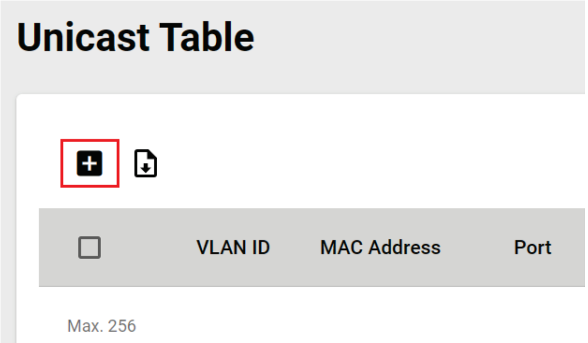
Independent VLAN Learning

Moxa's switch uses the **Independent VLAN Learning (IVL)** mode.

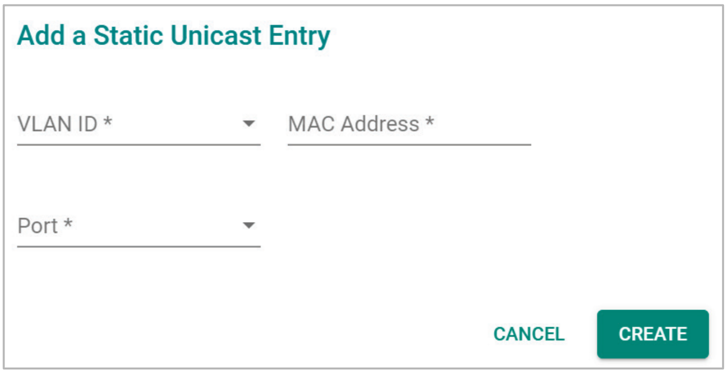
In an **IVL Mode**, a MAC table will be created in each VLAN, which will constitute many MAC tables. However, the same VID record will be selected and put in a table. A MAC table will be stored in the format of MAC + VID, the same MAC will be stored in different tables with different VIDs.

Static Unicast

Click **Static Unicast** from the function menu page and click the **+** icon on the configuration page.



Configure the following settings:


Add a Static Unicast Entry

VLAN ID *

MAC Address *

Port *

VLAN ID

Setting	Description	Factory Default
Input a VLAN ID	Input a VLAN ID.	None

MAC Address

Setting	Description	Factory Default
MAC address of the port	Input the MAC address of the port, for example 00:90:e8:01:01:01.	None

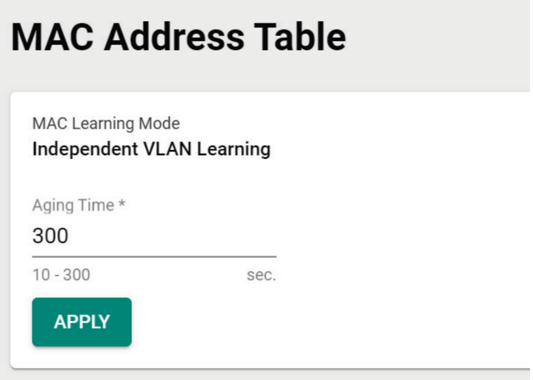
Port

Setting	Description	Factory Default
Select the port from the drop-down list	Specify the port you want to create a VLAN for.	None

When finished, click **CREATE**.

MAC Address Table

Select **MAC Address Table**, and Configure the following settings:



MAC Address Table

MAC Learning Mode
Independent VLAN Learning

Aging Time *
300
10 - 300 sec.

MAC Learning Mode

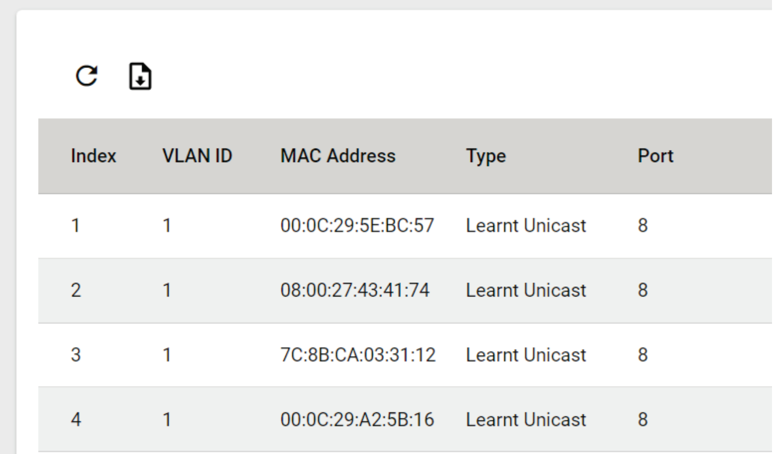
Information	Description	Factory Default
Independent VLAN Learning (read-only)	Show the current MAC Learning Mode.	Independent VLAN Learning

Aging Time

Setting	Description	Factory Default
10 to 300	Define the length of time that a MAC address entry can remain in the switch's MAC table.	None

When finished, click **APPLY** to save your changes.

You can view the current MAC Address Table on the bottom part of the configuration page.

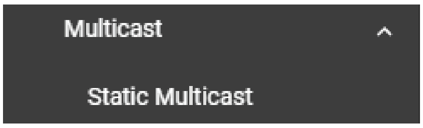


Index	VLAN ID	MAC Address	Type	Port
1	1	00:0C:29:5E:BC:57	Learnt Unicast	8
2	1	08:00:27:43:41:74	Learnt Unicast	8
3	1	7C:8B:CA:03:31:12	Learnt Unicast	8
4	1	00:0C:29:A2:5B:16	Learnt Unicast	8

Item Name	Description
Index	The number of the MAC address.
VLAN ID	The VLAN ID number
MAC Address	The MAC address of this device.
Type	Learnt Unicast, Learnt Multicast, Static Unicast, Static: Multicast
Port	The forwarding port of this MAC address.

Multicast

Multicast filtering improves the performance of networks that carry multicast traffic. This section will explain the **Static Multicast** settings for the Layer 2 Multicast functions.

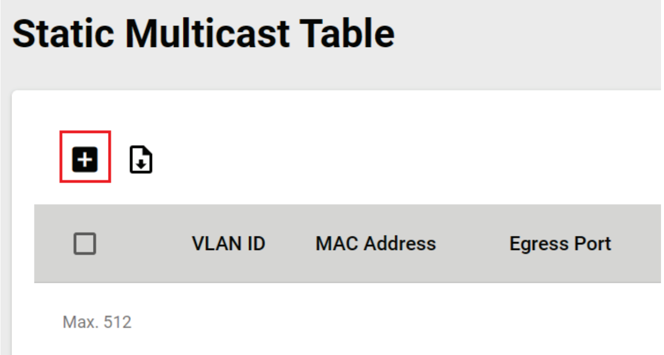


Static Multicast

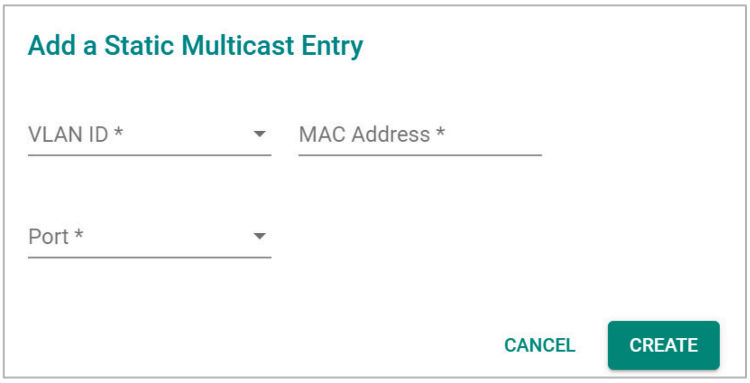
Click **Static Multicast** from the menu to view the current multicast table.

Adding Static Multicast Entry

To add more tables, click the + icon.



Configure the following settings:



VLAN ID

Setting	Description	Factory Default
Select the VLAN ID	Specify the multicast group's associated VLAN ID.	None

MAC Address

Setting	Description	Factory Default
Input the MAC address	Specify the multicast MAC address, for example 01:00:5e:01:01:01.	None

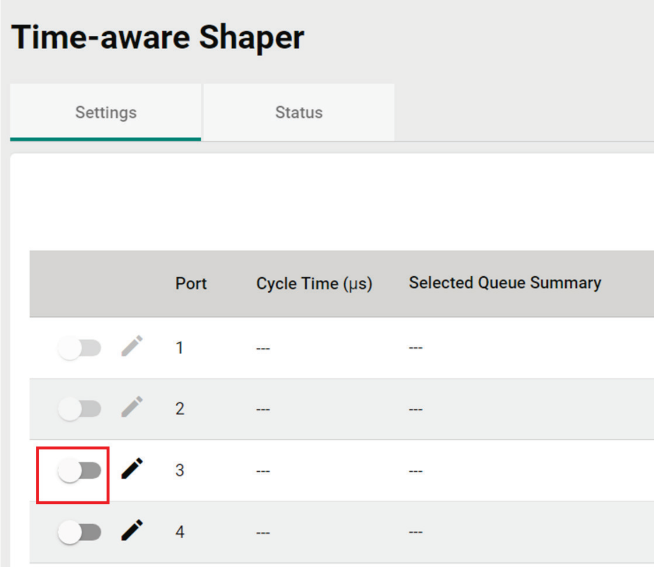
Port

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Set the port(s) as an egress port(s) so that multicast streams can be forwarded to this port.	None

When finished, click **CREATE**.

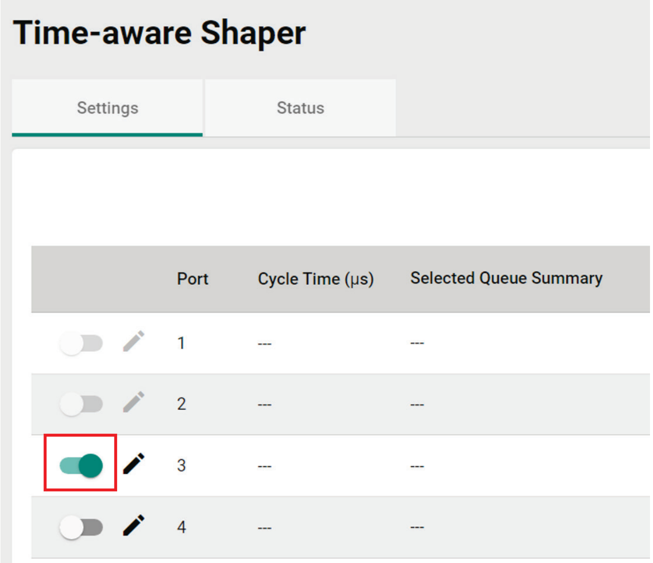
Time-aware Shaper

This section describes how to configure the **Time-aware Shaper** settings. Click **Time-aware Shaper** menu and click the **Settings** tab. To enable the Time-aware Shaper function, use the toggle in front of the respective port.



	Port	Cycle Time (μs)	Selected Queue Summary
	1	---	---
	2	---	---
	3	---	---
	4	---	---

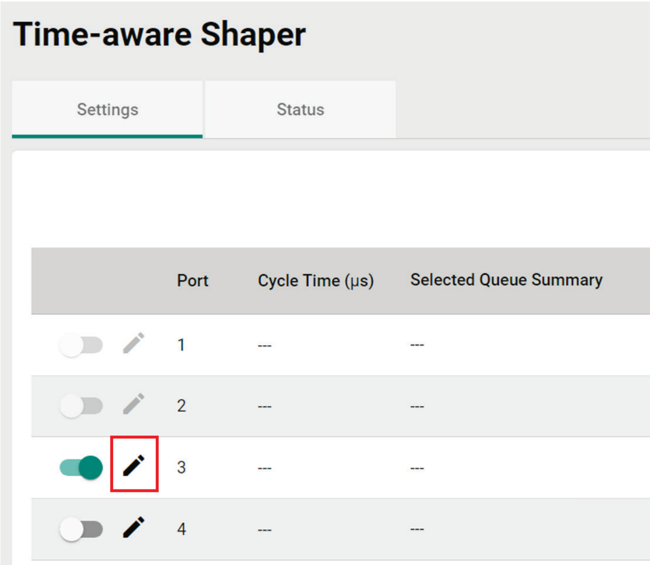
A green toggle indicates the Time-aware Shaper function is enabled for the port.



	Port	Cycle Time (μs)	Selected Queue Summary
	1	---	---
	2	---	---
	3	---	---
	4	---	---

Time-aware Shaper Settings

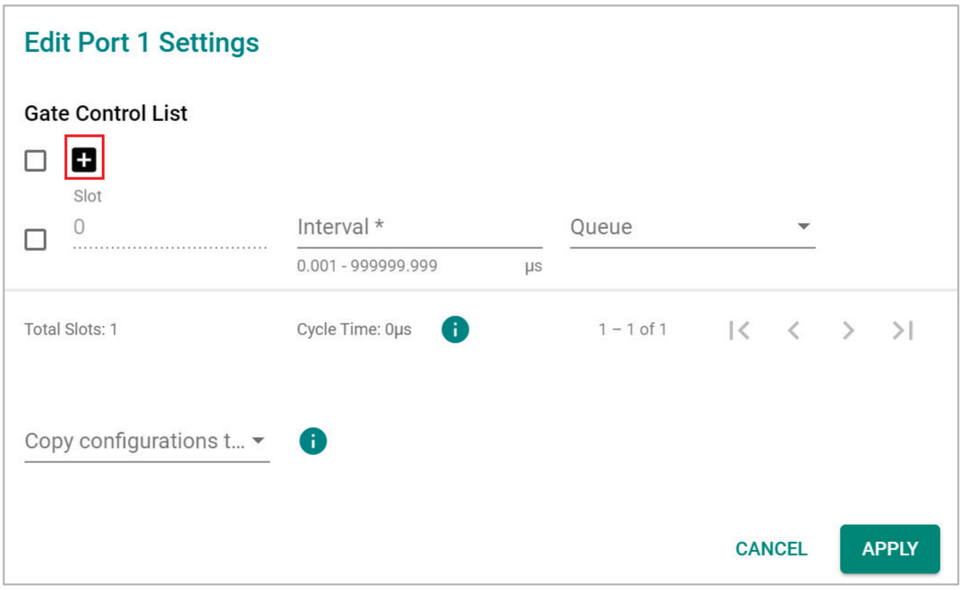
To configure the Time-aware Shaper settings, click the edit icon of the port.



Time-aware Shaper

Port	Cycle Time (µs)	Selected Queue Summary
1	---	---
2	---	---
3	---	---
4	---	---

In the Edit Port Settings window, click the + icon and configure the following settings:



Edit Port 1 Settings

Gate Control List

	Slot	Interval *	Queue
□	0	0.001 - 999999.999 µs	

Total Slots: 1

Cycle Time: 0µs

1 – 1 of 1

Checkbox for Gate Control List

Setting	Description	Factory Default
Checkbox	Select the gate control entry.	Unchecked

Slot

Information	Description	Factory Default
A variable depending on the amount of entries	Display the slot number (read only).	None

Interval (µs)

Setting	Description	Factory Default
0.001 to 999999.999	Select the interval value in µs.	None

Queue

Setting	Description	Factory Default
Q7 to Q0	Select the queue(s) from the list.	None

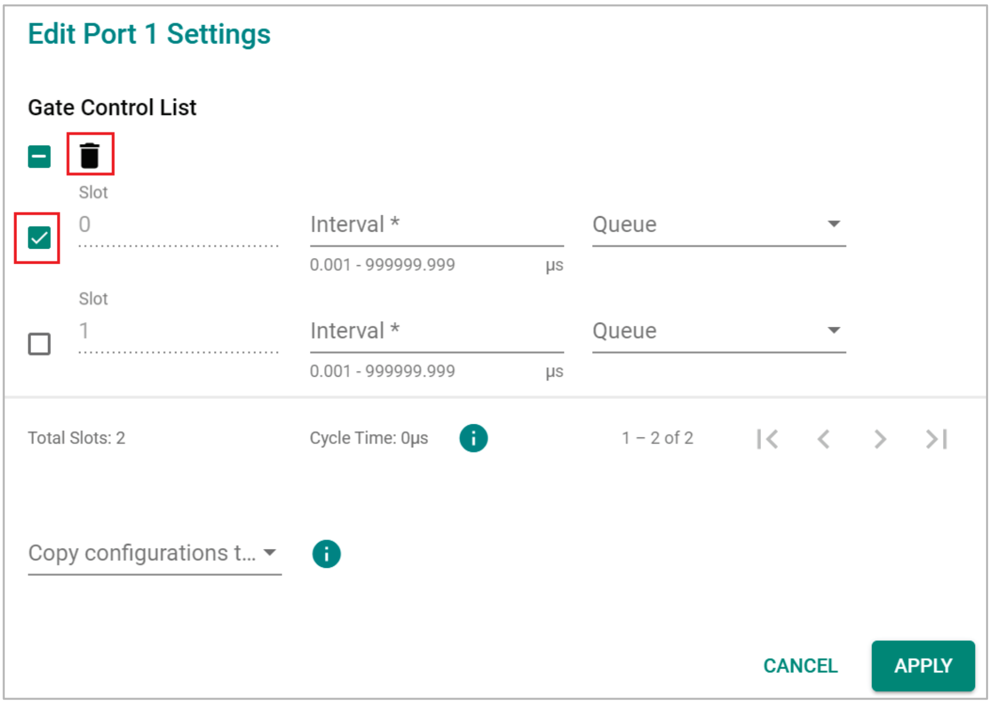
Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configurations to other port(s).	None

When finished, click **APPLY** to save your changes.

Deleting Gate Control List

To delete the Gate Control List, click the delete icon.



Edit Port 1 Settings

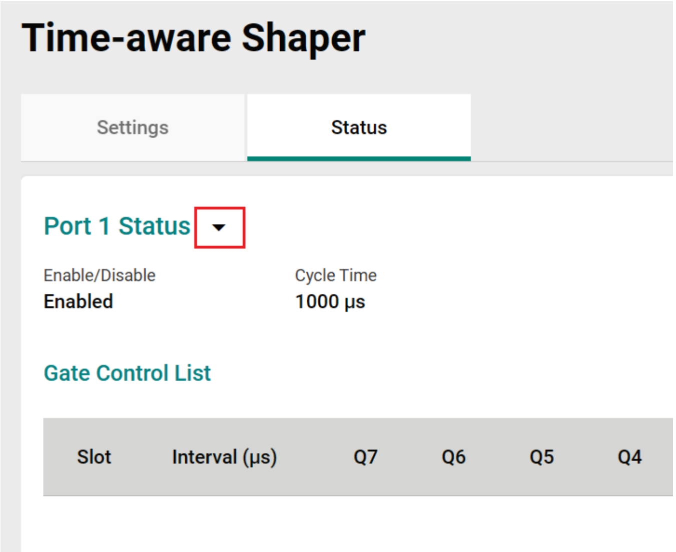
Gate Control List

	Slot	Interval *	Queue
☑	0	0.001 - 999999.999 µs	
□	1	0.001 - 999999.999 µs	

Total Slots: 2 Cycle Time: 0µs 1 – 2 of 2

Time-aware Shaper Status

To view the Time-aware Shaper status, click the **Status** tab, then select the port you want to view from the drop-down list.



Time-aware Shaper

Port 1 Status

Enable/Disable: Enabled

Cycle Time: 1000 µs

Gate Control List

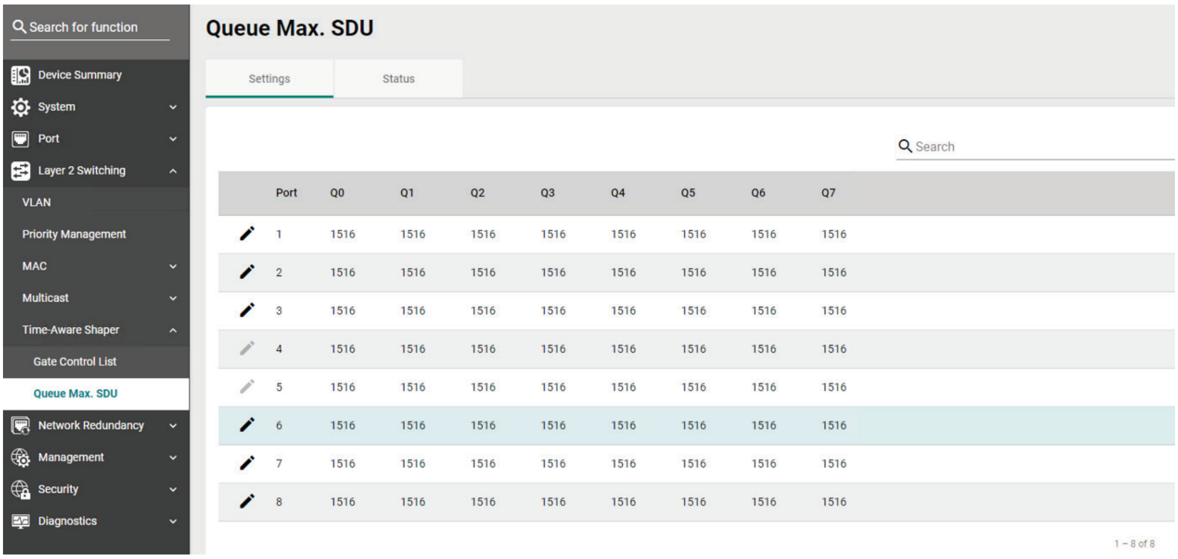
Slot	Interval (µs)	Q7	Q6	Q5	Q4

QBV Queue max. SDU

NOTE

This function is only supported on TSN Series models with firmware v2.4 or later.

This section description how to configure **QBV Queue max. SDU**. This setting specifies the maximum service data unit size for each queue; frames that exceed queue max SDU are discarded. The default value is the maximum-supported SDU size. This setting is effective even 802.1QBV is not enabled

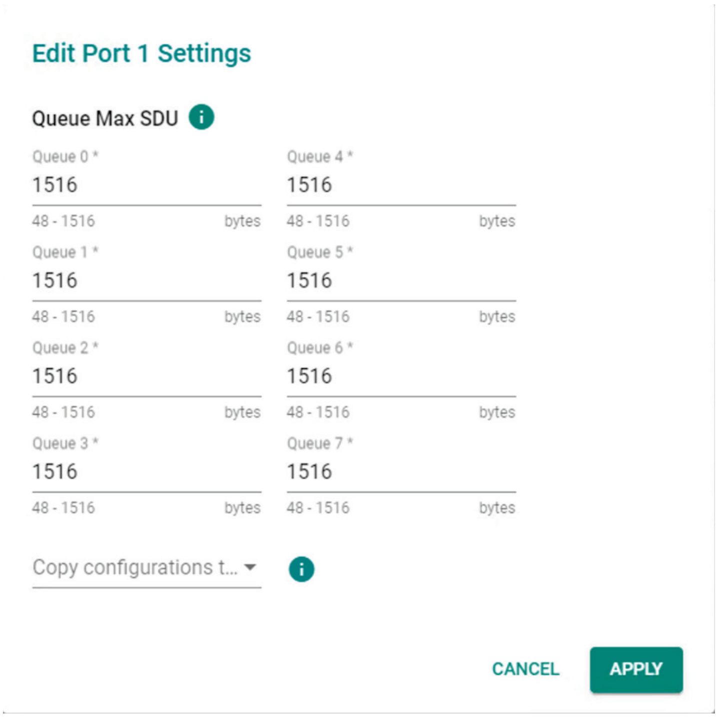


Queue Max. SDU

Port	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	1516	1516	1516	1516	1516	1516	1516	1516
2	1516	1516	1516	1516	1516	1516	1516	1516
3	1516	1516	1516	1516	1516	1516	1516	1516
4	1516	1516	1516	1516	1516	1516	1516	1516
5	1516	1516	1516	1516	1516	1516	1516	1516
6	1516	1516	1516	1516	1516	1516	1516	1516
7	1516	1516	1516	1516	1516	1516	1516	1516
8	1516	1516	1516	1516	1516	1516	1516	1516

1 – 8 of 8

Click the pencil icon to edit port settings.



Edit Port 1 Settings

Queue Max SDU

Queue 0 * 1516 (48 - 1516 bytes)

Queue 1 * 1516 (48 - 1516 bytes)

Queue 2 * 1516 (48 - 1516 bytes)

Queue 3 * 1516 (48 - 1516 bytes)

Queue 4 * 1516 (48 - 1516 bytes)

Queue 5 * 1516 (48 - 1516 bytes)

Queue 6 * 1516 (48 - 1516 bytes)

Queue 7 * 1516 (48 - 1516 bytes)

Queue 0-7

Setting	Description	Factory Default
Queue	Specify the queue value in bytes.	Unchecked

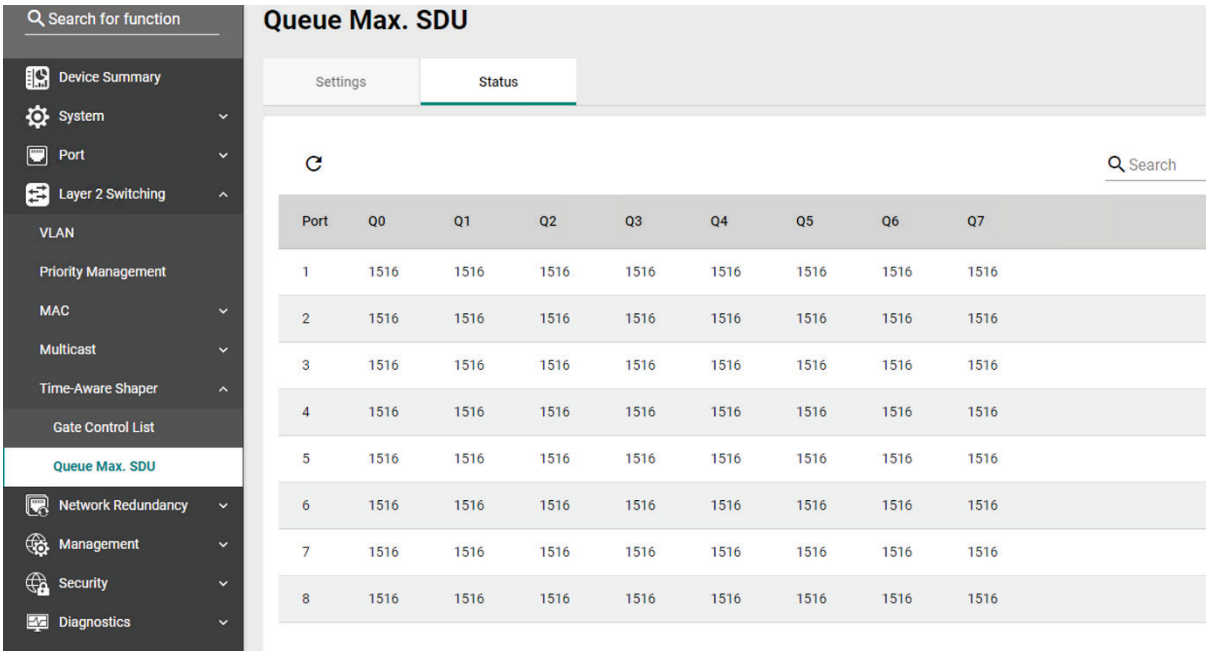
Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configurations to other port(s).	None

When finished, click **APPLY** to save your changes.

Status

To view Queue Max. SDU status, click the **Status** tab.



Port	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	1516	1516	1516	1516	1516	1516	1516	1516
2	1516	1516	1516	1516	1516	1516	1516	1516
3	1516	1516	1516	1516	1516	1516	1516	1516
4	1516	1516	1516	1516	1516	1516	1516	1516
5	1516	1516	1516	1516	1516	1516	1516	1516
6	1516	1516	1516	1516	1516	1516	1516	1516
7	1516	1516	1516	1516	1516	1516	1516	1516
8	1516	1516	1516	1516	1516	1516	1516	1516

Network Redundancy

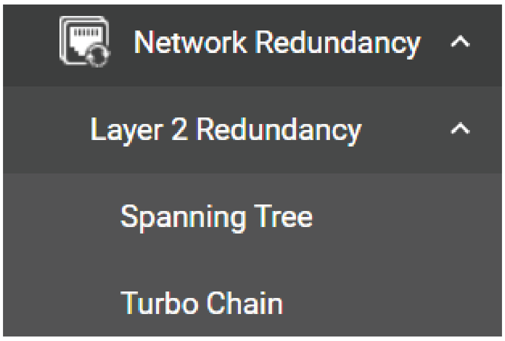
4Setting up the Redundancy Protocol on your network helps protect critical links against failure, protects against network loops, and keeps network downtime to a minimum.

The Redundancy Protocol allows you to set up redundant paths on the network to provide a backup data transmission route in the event that a cable or one of the switches is inadvertently disconnected or damaged. This is a particularly important feature for industrial applications, since it can take several minutes to address the link down port or failed switch. For example, if a Moxa switch is used as a key communications device for a production line, several minutes of downtime can cause a big loss in production and revenue. Moxa switches support the following Redundancy Protocol functions:

- **Spanning Tree**
- **Turbo Chain**

Layer 2 Redundancy

First select **Network Redundancy** from the menu and then click **Layer 2 Redundancy**.



Spanning Tree

Spanning Tree Overview

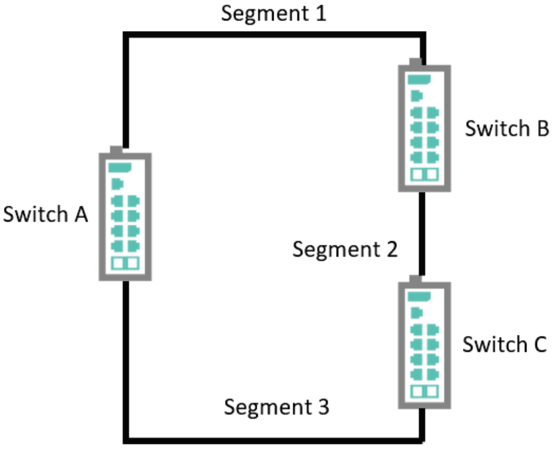
Spanning Tree Protocol (STP) was designed to help construct a loop-free logical typology on an Ethernet network and provide an automatic means of avoiding any network loops. This is particularly important for networks that have a complicated architecture since unintended loops in the network can cause broadcast storms. Moxa switches’ STP feature is disabled by default. To be completely effective, you must enable STP/RSTP on every Moxa switch connected to your network.

STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

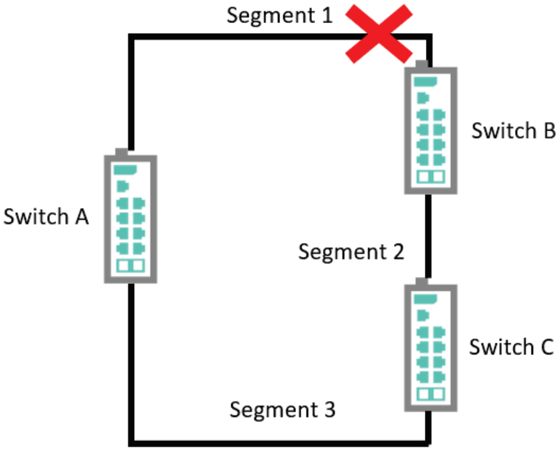
- Locate and then disable less efficient paths (e.g., paths that have lower bandwidth).
- Enable one of the less efficient paths if a more efficient path fails.

How STP Works

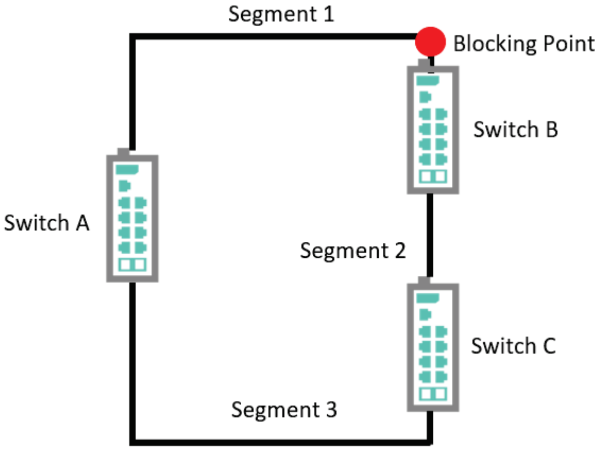
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is not enabled.



If STP is enabled, it will detect duplicate paths or block one of the paths from forwarding traffic. In the following example, STP determined that traffic from LAN segment 2 to LAN segment 1 should flow through switches C and A since this path has become shorter and is therefore more efficient. However, switch B on segment 1 is a blocking port.



What happens if a link failure is detected? As shown in the figure below, STP will change the blocking port to a forwarding state so that traffic from LAN segment 2 flows through switch B.



STP will determine which path between each bridged segment is most efficient, and then assign a specific reference point on the network. When the most efficient path has been identified, the other paths are blocked. In the previous three figures, STP first determined that the path through bridge C was the most efficient, and as a result, blocked the path through bridge B. After the failure of bridge C, STP re-evaluated the situation and opened the path through Bridge B.

Between STP and RSTP

RSTP is similar to STP but includes additional information in the BPDUs that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connected via point-to-point links will be able to enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP.

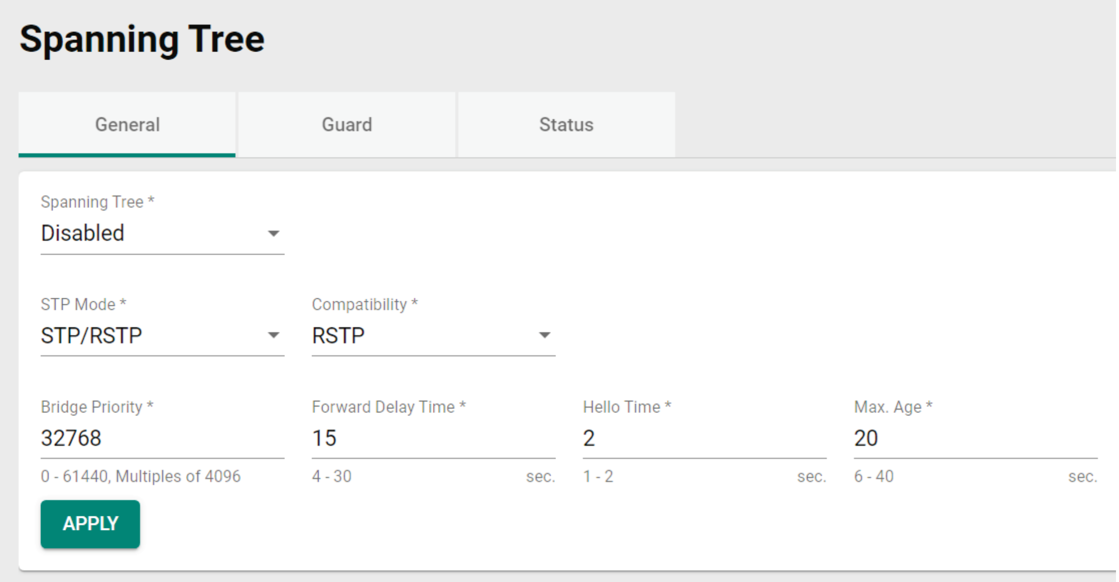
STP and RSTP spanning tree protocols operate without regard to a network's VLAN configuration and maintain one common spanning tree throughout a bridged network. Thus, these protocols map one loop-free, logical topology on a given physical topology.

STP/RSTP Settings and Status

This section describes how to configure Spanning Tree settings.

General

Click **Spanning Tree** from the menu and then select the **General** tab.



Spanning Tree

Spanning Tree * Disabled

STP Mode * STP/RSTP

Compatibility * RSTP

Bridge Priority * 32768
0 - 61440, Multiples of 4096

Forward Delay Time * 15 sec.
4 - 30

Hello Time * 2 sec.
1 - 2

Max. Age * 20 sec.
6 - 40

Configure the following settings:

Spanning Tree

Setting	Description	Factory Default
Enabled	Enable Spanning Tree.	Disabled
Disabled	Disable Spanning Tree.	

STP Mode

Setting	Description	Factory Default
STP/RSTP	Use the STP/RSTP mode as the Spanning Tree protocol.	STP/RSTP

Compatibility

Setting	Description	Factory Default
STP	To be compatible with STP mode only	RSTP
RSTP	To be compatible with RSTP and STP modes	

Bridge Priority

Setting	Description	Factory Default
0 to 61440	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Forwarding Delay Time (sec.)

Setting	Description	Factory Default
4 to 30	The amount of time the device waits before checking to see if it should change to a different state.	15

Hello Time (sec.)

Setting	Description	Factory Default
1 or 2	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. The "hello time" is the amount of time the root waits between sending hello messages.	2

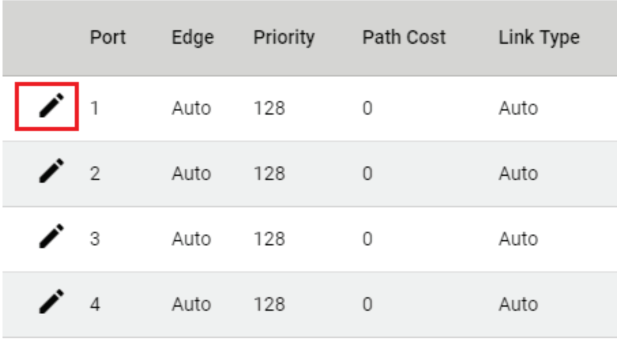
Max Age (sec.)

Setting	Description	Factory Default
6 to 40	If this device is not the root, and it has not received a hello message from the root in the amount of time equal to "Max. Age," then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate a new Spanning Tree topology.	20

When finished, click **APPLY** to save your changes.

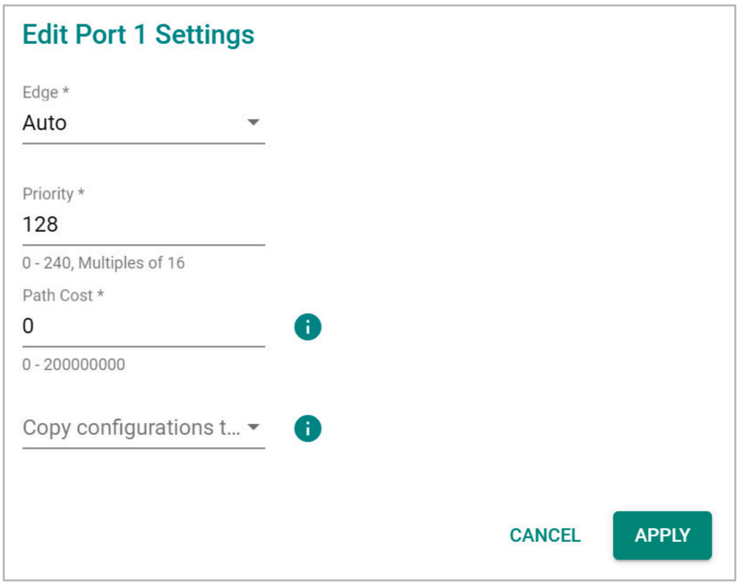
Editing Spanning Tree for a Port

To edit the spanning tree settings for a specific port, click the edit icon on the port you want to configure.



	Port	Edge	Priority	Path Cost	Link Type
✎	1	Auto	128	0	Auto
✎	2	Auto	128	0	Auto
✎	3	Auto	128	0	Auto
✎	4	Auto	128	0	Auto

Configure the following settings:



Edit Port 1 Settings

Edge * Auto

Priority * 128

0 - 240, Multiples of 16

Path Cost * 0

0 - 200000000

Edge

Setting	Description	Factory Default
Auto	Automatically detect and designate the port as an edge port.	Auto
Yes	Designate as the port as an edge port.	
No	Do not designate the port as an edge port.	

Priority

Setting	Description	Factory Default
0 to 240	Increase the priority of a port by selecting a lower number. A port with a higher priority has a greater chance of being a root port.	128

Path Cost

Setting	Description	Factory Default
0 to 20000000	The path cost value will be automatically assigned according to the different port speed if the value is set to zero.	0

Link Type (in Advanced Mode only)

Setting	Description	Factory Default
Point-to-Point	Set to Point-to-Point mode in full-duplex mode. The port should be connected to a single switch at the other end of the link.	Auto
Shared	Set to Shared mode in half-duplex mode. The port should be connected to shared media, such as a hub at the other end of the link.	
Auto	Automatically select Point-to-Point mode or Shared mode.	

Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configurations to other port(s).	None

Click **APPLY** to finish.

PDU Overview

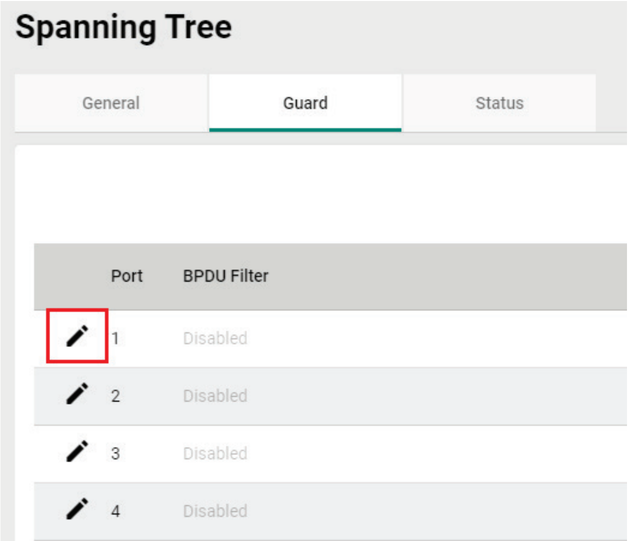
BDPUs (Bridge Protocol Data Units) are the network communication frames used in the STP (Spanning Tree Protocol). When two switches exchange messages, BDPUs are used to calculate the STP topology, and determine the network communication route. A BDPU filter is often used to screen sending or receiving BPDUs on a specific port of the switch.

PDU Filter

BPDU Filter prevents a port from sending and processing BPDUs. A BPDU filter enabled port cannot transmit any BPDUs and drop all received BPDU either.

PDU Filter Settings

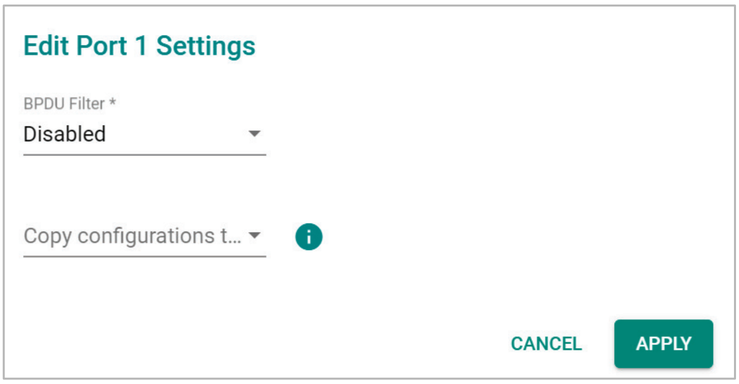
First click **Spanning Tree** from the menu and then select the **Guard** tab. Next, click the edit icon on the port you want to configure.



Spanning Tree

Port	BPDU Filter
1	Disabled
2	Disabled
3	Disabled
4	Disabled

Configure the following settings:



Edit Port 1 Settings

BPDU Filter *: Disabled

NOTE

To set up a redundant port, it is highly recommended that you do not enable the BPDU filter.

DPU Filter

Setting	Description	Factory Default
Enabled	Enable BDPU Filter.	Disabled
Disabled	Disable BDPU Filter.	

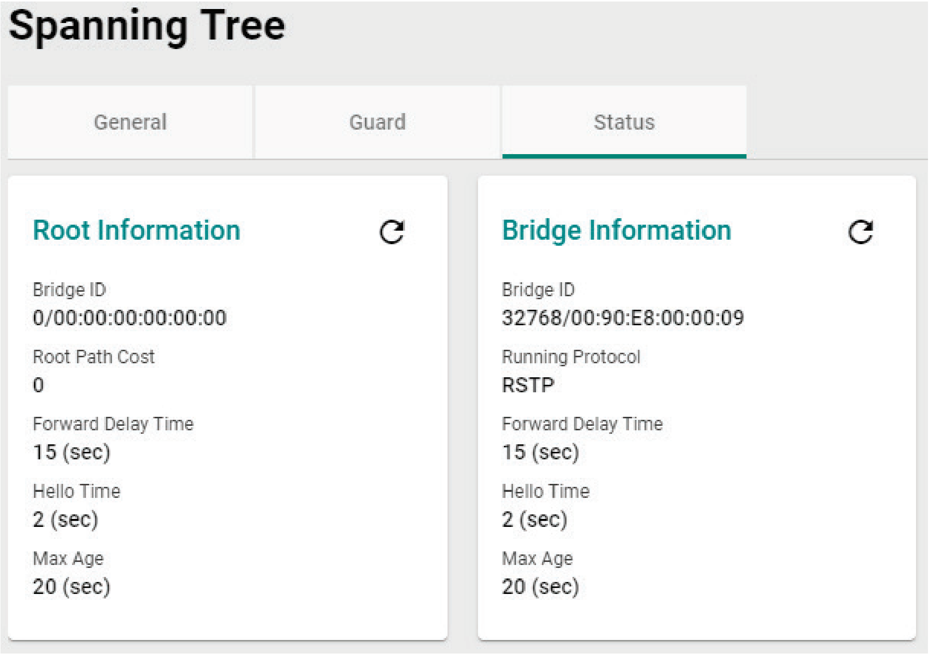
Copy Configurations to Port

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the same settings to other port(s).	None

When finished, click **APPLY** to save your changes.

Viewing the Current Spanning Tree Status

Click the **Status** tab to view the current Spanning Tree status.



Spanning Tree

Root Information

Bridge ID
0/00:00:00:00:00:00

Root Path Cost
0

Forward Delay Time
15 (sec)

Hello Time
2 (sec)

Max Age
20 (sec)

Bridge Information

Bridge ID
32768/00:90:E8:00:00:09

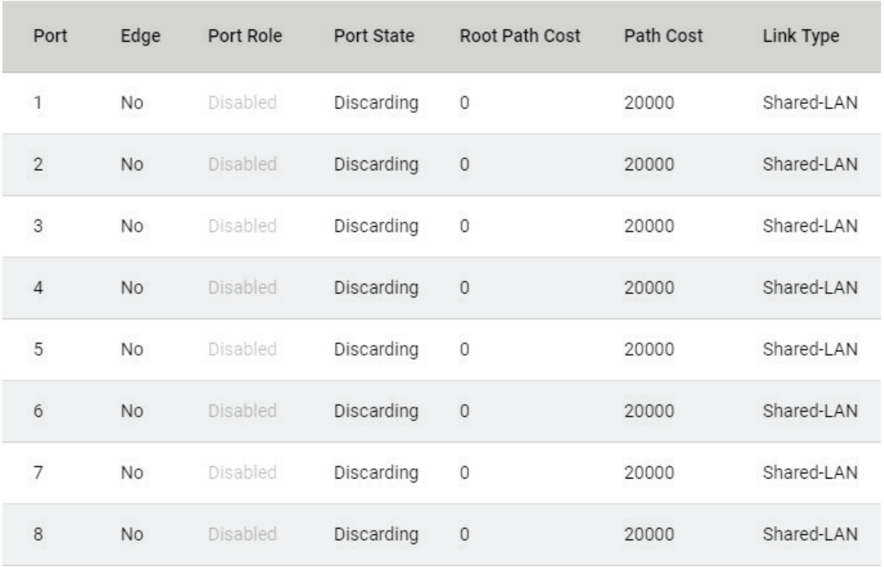
Running Protocol
RSTP

Forward Delay Time
15 (sec)

Hello Time
2 (sec)

Max Age
20 (sec)

In addition, the status for each port will also be shown below.



Port	Edge	Port Role	Port State	Root Path Cost	Path Cost	Link Type
1	No	Disabled	Discarding	0	20000	Shared-LAN
2	No	Disabled	Discarding	0	20000	Shared-LAN
3	No	Disabled	Discarding	0	20000	Shared-LAN
4	No	Disabled	Discarding	0	20000	Shared-LAN
5	No	Disabled	Discarding	0	20000	Shared-LAN
6	No	Disabled	Discarding	0	20000	Shared-LAN
7	No	Disabled	Discarding	0	20000	Shared-LAN
8	No	Disabled	Discarding	0	20000	Shared-LAN

Refer to the following table for detailed description of each item.

Item	Description
Port	The port number on this device.
Edge	Show if this port is connected to an edge device.
Port Rule	Root: The port is connected directly or indirectly to the root device. Designated: The port is designated if it can send the best BPDU on the segment to which it is connected. Alternate: The alternate port receives more useful BPDU from another bridge and is the blocked port. Backup: The backup port receives more useful BPDU from the same bridge and is the blocked port. Disabled: The function is disabled.
Port State	Forwarding: The traffic can be forwarded through this port. Discarding: The traffic will be blocked. Disabled: The function is disabled.
Root Path Cost	The total path cost to the root bridge.
Path Cost	The path cost on this link.

Turbo Chain Overview

NOTE

This function is only supported on TSN Series models with firmware v2.3 or later.

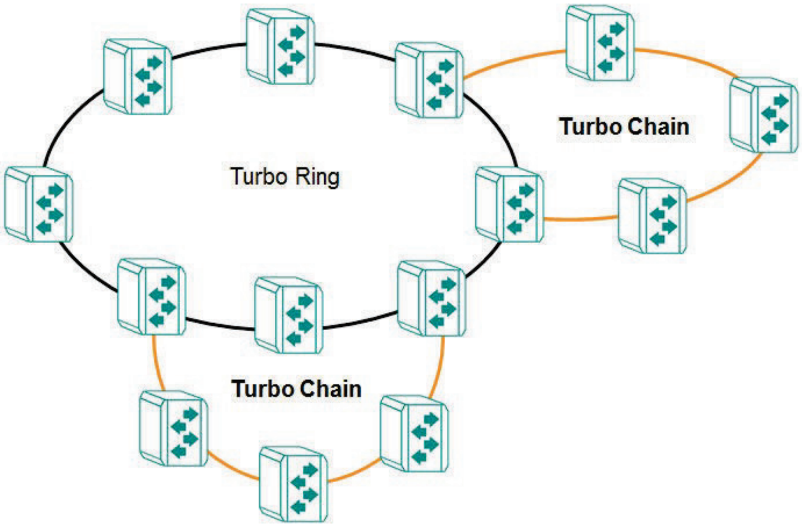
Moxa’s Turbo Chain is an advanced software technology that gives network administrators the flexibility of constructing any type of redundant network topology. In addition, it offers system recovery time under 20 ms for Fast Ethernet (50 ms for copper-cabled Turbo Chain Member ports [non-head/tail]), and 50 ms for Gigabit Ethernet for member port link environments. When using the “chain” concept, you first connect the Ethernet switches in a chain and then simply link the two ends of the chain to an Ethernet network.

Turbo Chain can be used on industrial networks that have a complex topology. If the industrial network uses a multi-ring architecture, Turbo Chain can be used to create flexible and scalable topologies with a fast media-recovery time.

How Turbo Chain Works

Moxa’s Turbo Chain outperforms traditional ring topologies by providing great flexibility, unrestricted expansion, and cost-effective configurations when connecting separate redundant rings together—in a simplified manner. With Turbo Chain, you can create any complex redundant network that correspond to your needs, while still ensuring great reliability and availability for your industrial Ethernet network applications.

With Moxa's Turbo Chain, network engineers have the flexibility to construct any type of redundant topology with minimum effort—by simply linking Turbo Chain to the Ethernet Network. Turbo Chain allows for unrestricted network expansion. Network engineers no longer need to go through the hassle of reconfiguring the existing network, and can simply use Turbo Chain to scale up their redundant networks.

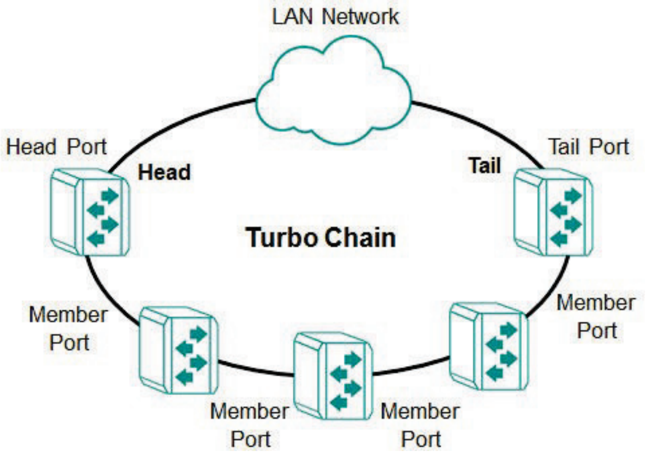

Turbo Ring
Turbo Chain
Turbo Chain

How to Determine the Redundant Path

Here is an example of how to set up Turbo Chain and determine the redundant path.

1. Select the Head switch, Tail switch, and Member switches.
2. Configure one port as the Head port and one port as the Member port in the Head switch, configure one port as the Tail port and one port as the Member port in the Tail switch, and configure two ports as Member ports in each of the Member switches.
3. Connect the Head switch, Tail switch, and Member switches as shown in the diagram below.

The path connecting to the Head port is the main path, and the path connecting to the Tail port is the backup path of Turbo Chain. Under normal conditions, packets are transmitted through the Head Port to the LAN network. If any Turbo Chain path is disconnected, the Tail Port will be activated so that packet transmission can continue.

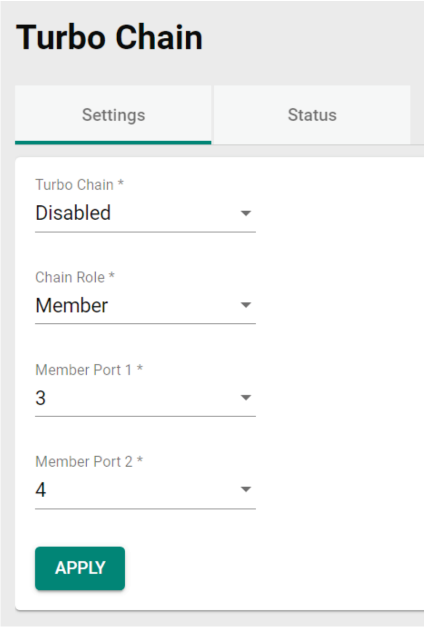


There are two points to note:

4. Two Chain ports must have the same PVID.
5. Chain ports must join the untagged members of PVID VLAN before being assigned to be a Chain port.

Turbo Chain V2 Settings

First select **Turbo Chain** from the menu and then click **Settings**.



Turbo Chain

Turbo Chain *
Disabled

Chain Role *
Member

Member Port 1 *
3

Member Port 2 *
4

Configure the following settings:

Turbo Chain

Setting	Description	Factory Default
Enabled	Enable Turbo Chain.	Disabled
Disabled	Disable Turbo Chain.	

Chain Role

Setting	Description	Factory Default
Head	Designate the switch as the Turbo Chain Head.	Member
Member	Designate the switch as a Turbo Chain Member.	
Tail	Designate the switch as the Turbo Chain Tail.	

Head/Member/Tail Port

Setting	Description	Factory Default
Select the port from the list	Specify the port as the Head/Member/Tail port.	1/1

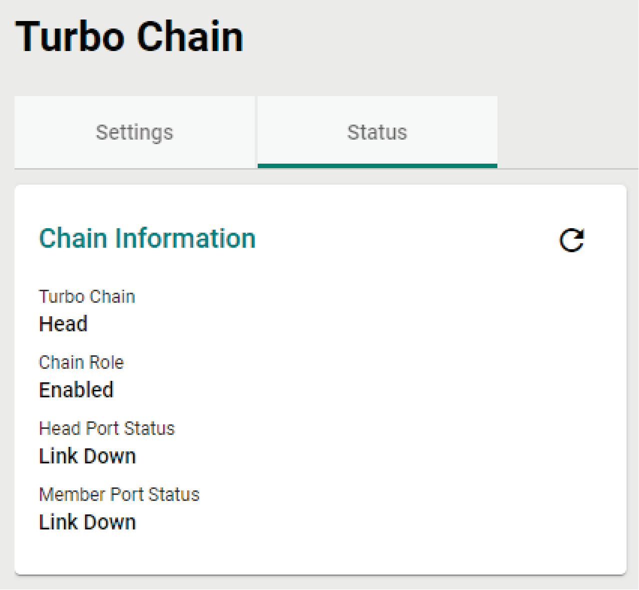
Member Port

Setting	Description	Factory Default
Select the port from the list	Specify the port as the member port.	1/2

When finished, click **APPLY** to save your changes.

Viewing Current Turbo Chain Status

Click the S**tatus t**ab to view the current Turbo Chain status.


Turbo Chain

Chain Information

Turbo Chain
Head

Chain Role
Enabled

Head Port Status
Link Down

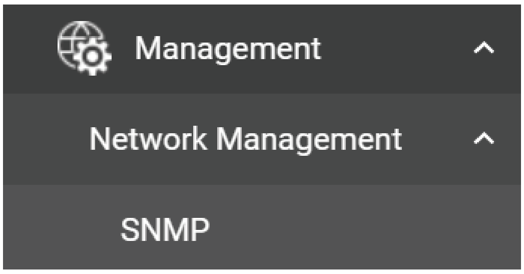
Member Port Status
Link Down

Refer to the following table for a detailed description of each item.

Item	Description
Turbo Chain	Head: The device is the head of this chain. Member: The device is a member of this chain. Tail: The device is the tail of this chain.
Chain Role	Healthy: The Chain and the ports are working properly. Break: The chain or the ports are broken.
Head/Member/Tail (1) Port Status	The status of the (first) Head/Member/Tail port.
Member (2) Port Status	The status of the (second) Member port.

Management

This section describes how to configure **Management** functions.



Management

Network Management

SNMP

Network Management

This section demonstrates how to configure SNMP settings.

SNMP

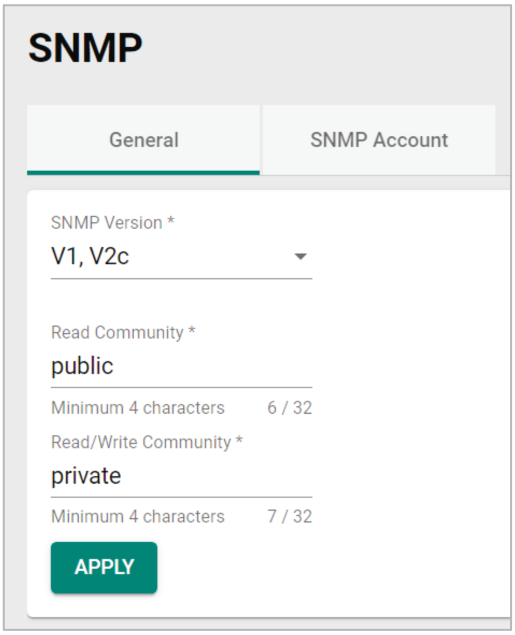
Moxa switches support SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community strings *public* and *private* by default. SNMP V3 requires that you select an authentication level of MD5 or SHA. You can also enable data encryption to enhance data security.

Supported SNMP security modes and levels are shown in the table below. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	UI Setting	Authentication	Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Uses a community string match for authentication.
	V1, V2c Write/Read Community	Community string	No	Uses a community string match for authentication.
SNMP V3	None	No	No	Uses an account with admin or user to access objects.
	MD5 or SHA	Authentication based on MD5 or SHA	Disabled	Uses authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key: DES, AES	Uses authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

General Settings

First click **SNMP** from the menu and then click **General**.



SNMP Version *
V1, V2c

Read Community *
public
Minimum 4 characters 6 / 32

Read/Write Community *
private
Minimum 4 characters 7 / 32

Configure the following settings:

SNMP Version

Setting	Description	Factory Default
V1, V2c, V3	Specify V1, V2c, and V3 as the SNMP version.	V1, V2c
V1, V2c	Specify V1 and V2c as the SNMP version.	
V3 only	Specify V3 as the SNMP version.	

Read Community

Setting	Description	Factory Default
4 to 32 characters	Specifies the community string to authenticate the SNMP agent for read-only access. The SNMP agent will access all objects with read-only permissions using this community string.	public

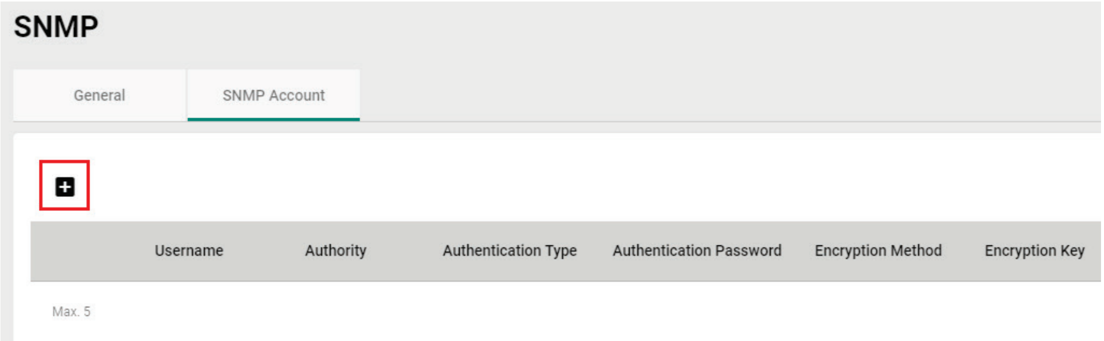
Read/Write Community

Setting	Description	Factory Default
4 to 32 characters	Specifies the community string to authenticate the SNMP agent for read/write access. The SNMP server will access all objects with read/write permissions using this community string.	private

When finished, click **APPLY** to save your changes.

Creating an SNMP Account

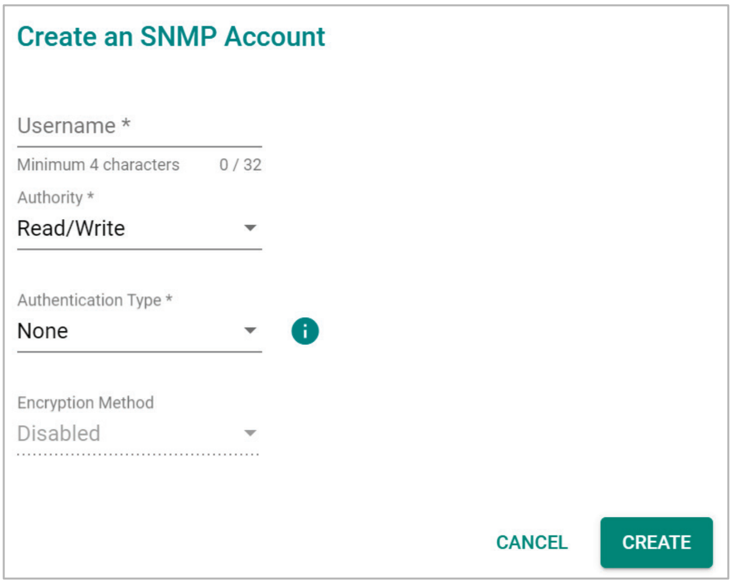
Click **SNMP** from the menu and then click the **SNMP Account**. Next click the **+** icon on the page.



Username	Authority	Authentication Type	Authentication Password	Encryption Method	Encryption Key

Max. 5

Configure the following settings:


Create an SNMP Account

Username *

Minimum 4 characters 0 / 32

Authority *: Read/Write

Authentication Type *: None

Encryption Method: Disabled

Username

Setting	Description	Factory Default
At least 4 characters, (max. 32 characters)	Input a username.	None

Authority

Setting	Description	Factory Default
Read/Write	The user has read/write access.	Read/Write
Read Only	The user only has read access.	

Authentication type

Setting	Description	Factory Default
None	No authentication will be used.	None
MD5	MD5 is the authentication type.	
SHA	SHA is the authentication type.	

Authentication password

Setting	Description	Factory Default
8 to 64 characters	Input the authentication password.	None

Encryption Method

Setting	Description	Factory Default
Disabled	Disable the encryption method.	Disabled
DES	DES is the encryption method.	
AES	AES is the encryption method.	

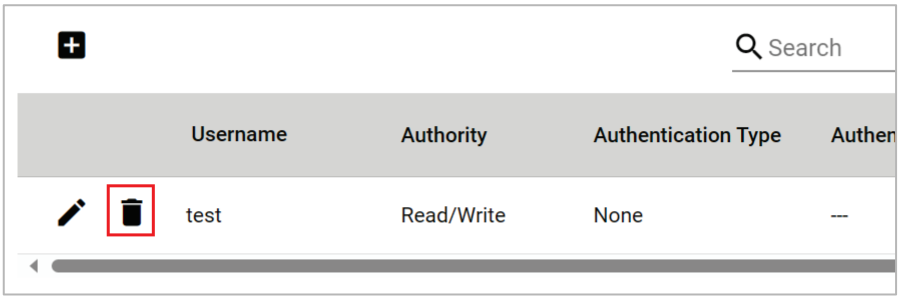
Encryption Key

Setting	Description	Factory Default
8 to 64 characters	Enable data encryption.	None

When finished, click **CREATE**.

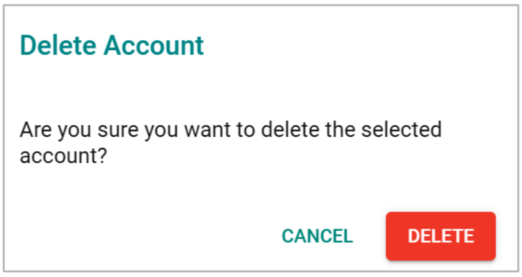
Deleting an Existing SNMP Account

To delete an existing SNMP account, select the delete icon on the account.



	Username	Authority	Authentication Type	Authen
✎ 🗑	test	Read/Write	None	---

Click **DELETE** to delete the SNMP account.

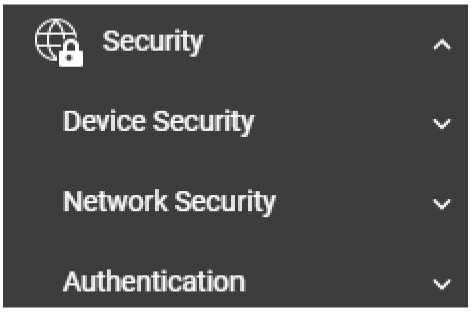


Delete Account

Are you sure you want to delete the selected account?

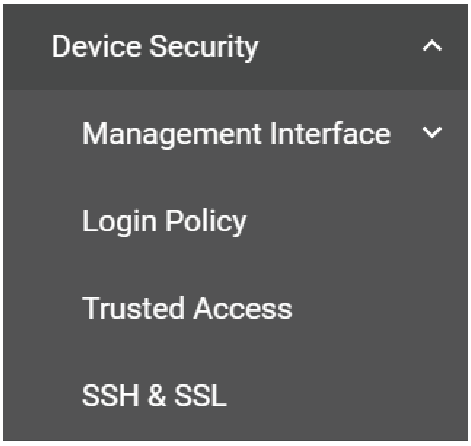
Security

This section describes how to configure **Device Security**, **Network Security**, and **Authentication**.



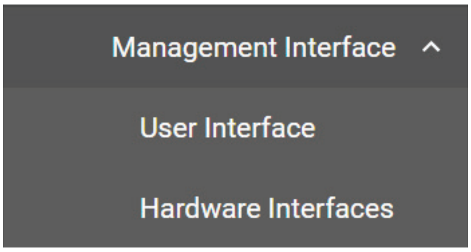
Device Security

This section includes information about the **Management Interface**, **Login Policy**, **Trusted Access**, and **SSH & SSL** configurations.



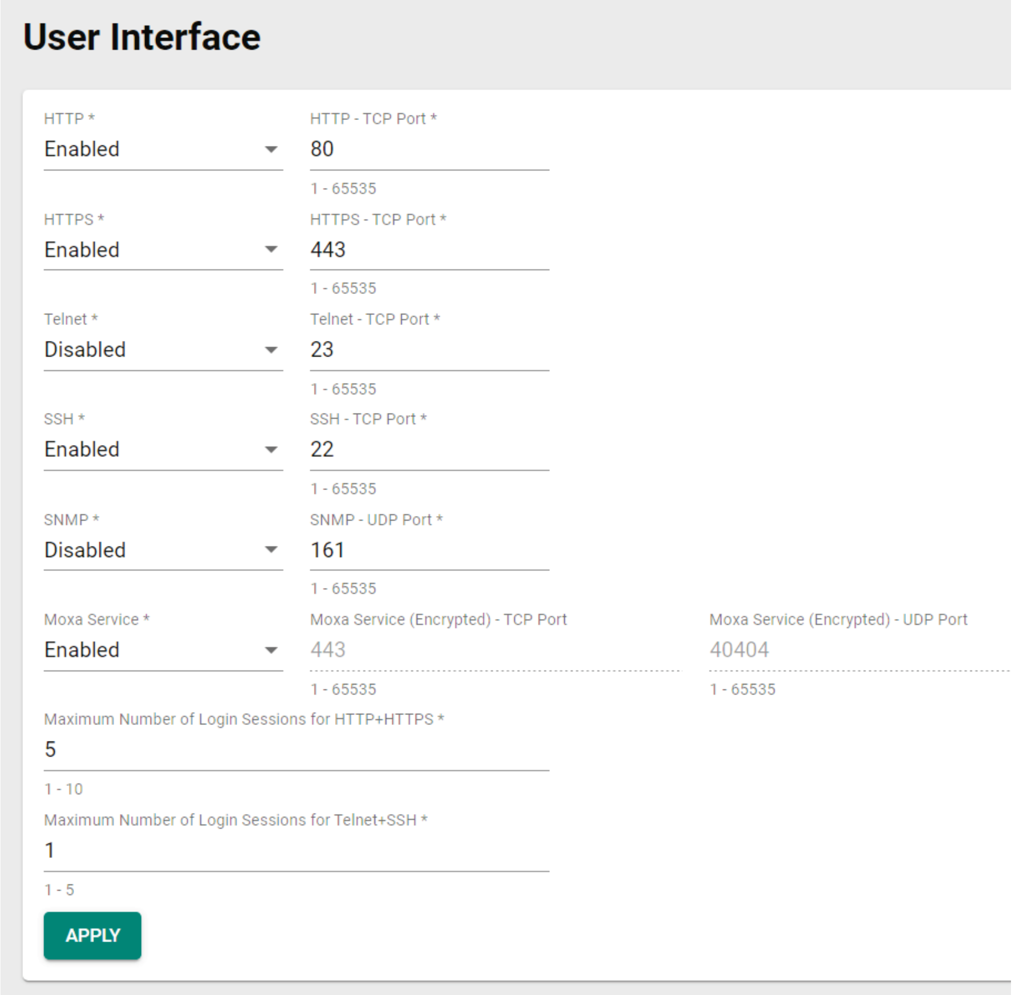
Management Interface

This section includes settings for **User Interface** and **Hardware Interfaces**.



User Interface

From the **Management Interface** menu, click **User Interface**. This section is used to enable, disable, and configure various user interfaces for the device.



User Interface

HTTP * Enabled

HTTP - TCP Port * 80 (1 - 65535)

HTTPS * Enabled

HTTPS - TCP Port * 443 (1 - 65535)

Telnet * Disabled

Telnet - TCP Port * 23 (1 - 65535)

SSH * Enabled

SSH - TCP Port * 22 (1 - 65535)

SNMP * Disabled

SNMP - UDP Port * 161 (1 - 65535)

Moxa Service * Enabled

Moxa Service (Encrypted) - TCP Port 443 (1 - 65535)

Moxa Service (Encrypted) - UDP Port 40404 (1 - 65535)

Maximum Number of Login Sessions for HTTP+HTTPS * 5 (1 - 10)

Maximum Number of Login Sessions for Telnet+SSH * 1 (1 - 5)

Configure the following settings:

HTTP

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the HTTP interface.	Enabled

HTTP – TCP Port

Setting	Description	Factory Default
1 to 65535	Specify the HTTP connection port number.	80

HTTPS

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the HTTPS interface.	Enabled

HTTPS – TCP Port

Setting	Description	Factory Default
1 to 65535	Specify the HTTP connection port number.	443

NOTE

When both the HTTP and HTTPS interfaces are enabled, HTTP connections will be automatically redirected to HTTPS.

Telnet

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the Telnet interface.	Disabled

Telnet – TCP Port

Setting	Description	Factory Default
1 to 65535	Specify the Telnet connection port number.	23

SSH

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the SSH interface.	Enabled

SSH – TCP Port

Setting	Description	Factory Default
1 to 65535	Input the SSH connection port number.	22

SNMP

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the SNMP interface.	Disabled

SNMP – UDP Port

Setting	Description	Factory Default
1 to 65535	Input the SNMP connection port number.	161

Moxa Service (in Advanced Mode)

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable Moxa Service.	Enabled

NOTE

Moxa Service refers to Moxa network management software suites.

Moxa Service (Encrypted) – TCP Port (in Advanced Mode)

Setting	Description	Factory Default
443 (read only)	Enable a Moxa Service TCP port.	443

Moxa Service (Encrypted) – UDP Port (in Advanced Mode)

Setting	Description	Factory Default
40404 (read only)	Enable a Moxa Service UDP port.	40404

Maximum number of Login Sessions for HTTP+HTTPS

Setting	Description	Factory Default
1 to 10	Specify the maximum amount of HTTP+HTTPS login sessions that can happen at the same time.	5

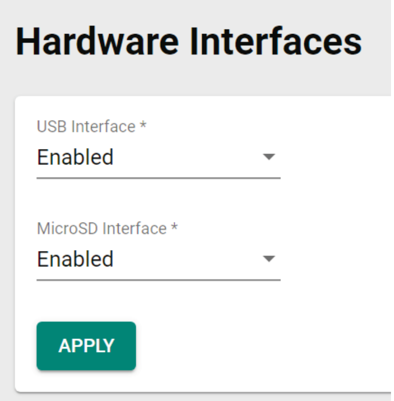
Maximum number of Login Sessions for Telnet+SSH

Setting	Description	Factory Default
1 to 5	Specify the maximum amount of Telnet+SSH login sessions that can happen at the same time.	1

When finished, click **APPLY** to save your changes.

Hardware Interfaces

From the **Management Interface** menu, click **Hardware Interface**. This section is used to enable or disable the USB and MicroSD interfaces on the device.



Hardware Interfaces

USB Interface *
Enabled

MicroSD Interface *
Enabled

Configure the following settings:

Interface

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the USB interface.	Enabled

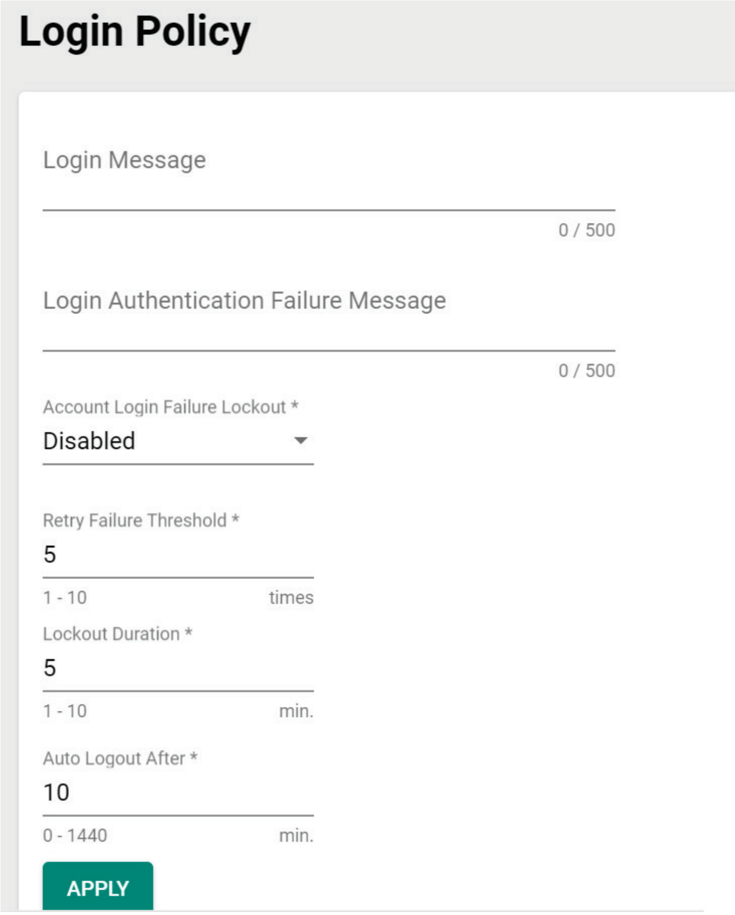
MicroSD Interface

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the MicroSD interface.	Enabled

When finished, click **APPLY** to save your changes.

Login Policy

Click **Login Policy** from the menu.



Login Policy

Login Message

0 / 500

Login Authentication Failure Message

0 / 500

Account Login Failure Lockout *
Disabled

Retry Failure Threshold *
5
1 - 10 times

Lockout Duration *
5
1 - 10 min.

Auto Logout After *
10
0 - 1440 min.

Configure the following settings:

Login Message

Setting	Description	Factory Default
0 to 500 characters	Input the message that will be displayed to users when they log in.	None

Login Authentication Failure Message

Setting	Description	Factory Default
0 to 500 characters	Input the message that will be displayed when users fail to log in.	None

Account Login Failure Lockout

Setting	Description	Factory Default
Enabled	Enable the lockout function when a user fails to log in.	Disabled
Disabled	Disable the lockout function when a user fails to log in.	

Retry Failure Threshold (times)

Setting	Description	Factory Default
1 to 10	Input the maximum number of retry failure times.	5

Lockout Duration (min.)

Setting	Description	Factory Default
1 to 10	Specify the duration a user is locked out from the device before they can try to log in again.	5

Auto Logout After (min.)

Setting	Description	Factory Default
0 to 1440	Specify how long a user can be inactive before getting logged out automatically.	5

When finished, click **APPLY** to save your changes.

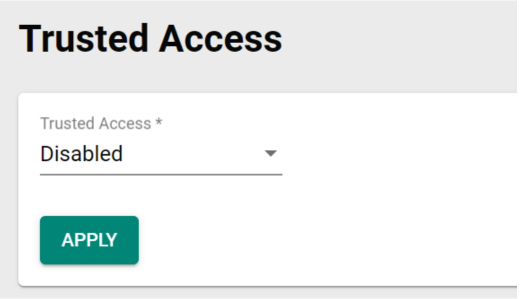
Trusted Access

Trusted Access Overview

Trusted Access is a mechanism that provides a secure connection to Moxa's switch. Users can use this method to allow the connection from the assigned IP address to ensure safe data transmission.

Trusted Access Settings and Status

Click **Trusted Access** from the function menu.


Trusted Access

Trusted Access *
Disabled

Configure the following settings:

Trusted Access

Setting	Description	Factory Default
Enabled	Enable Trusted Access.	Disabled
Disabled	Disable Trusted Access.	

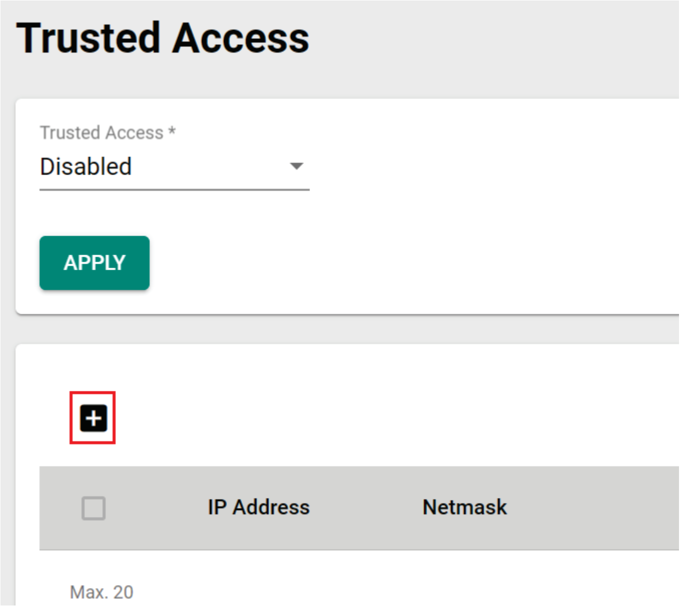
NOTE

1. A Trusted Access entry must be added before Trusted Access can be enabled.
2. In order to avoid being disconnected after you enable Trusted Access, you must first add the current IP subnet to Trusted Access. In order to use this function, you should use an RS-232 console to log in or set the device to factory default.

When finished, click **APPLY** to save your changes.

Creating a Trusted Access Entry

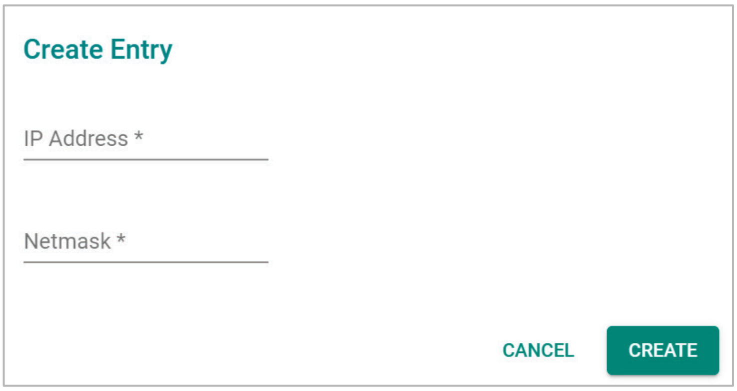
From the **Trusted Access** table, click the **+** icon to add a new entry.



Trusted Access

Trusted Access *: Disabled

Configure the following settings:



Create Entry

IP Address *

Netmask *

IP Address

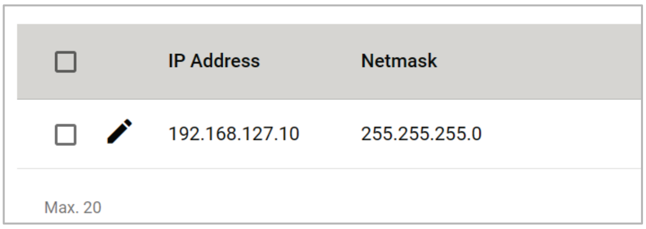
Setting	Description	Factory Default
Input IP address	Specify the IP address that is allowed to connect to Moxa's switch.	None

Netmask

Setting	Description	Factory Default
Input Netmask	Specify the Netmask that is allowed to connect to Moxa's switch.	None

When finished, click **CREATE**.

All created entries will appear in the table.

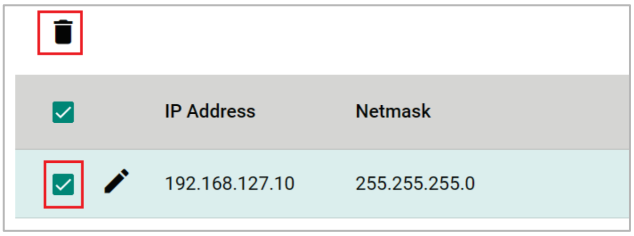


□	IP Address	Netmask
□	192.168.127.10	255.255.255.0

Max. 20

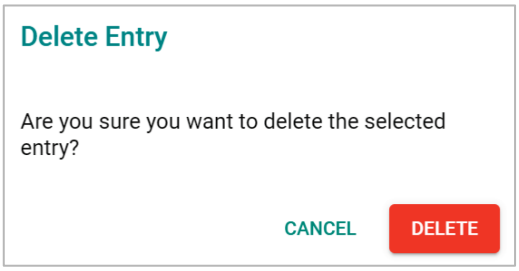
Deleting a Trusted Access entry

To delete an existing Trusted Access entry, select the item and then click the Delete icon at the top of the table.



☑		IP Address	Netmask
☑	✎	192.168.127.10	255.255.255.0

Click **DELETE** to delete the item.



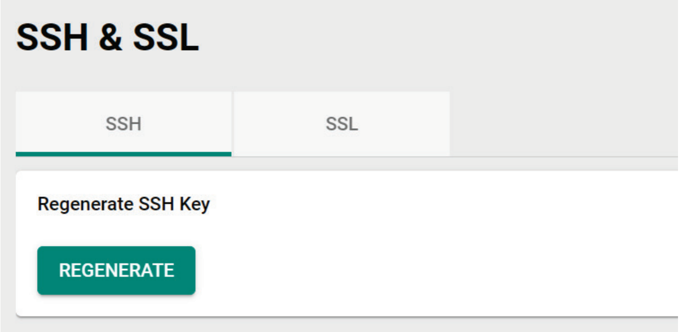
Delete Entry

Are you sure you want to delete the selected entry?

SSH & SSL

SSH Key Regeneration

Click **SSH & SSL** from the menu and then select the **SSH** tab.



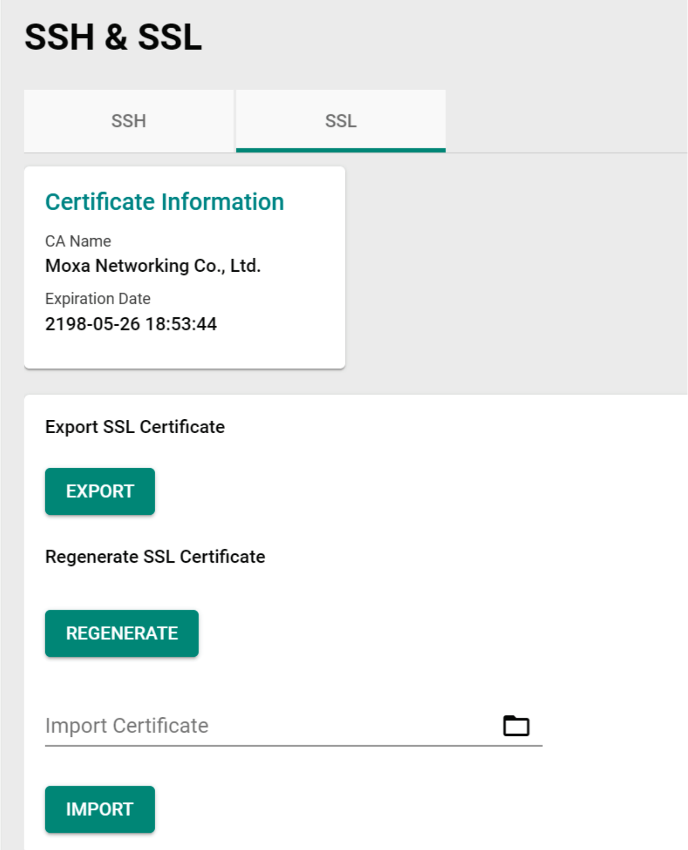
SSH & SSL

Regenerate SSH Key

Click **REGENERATE** to regenerate the key.

SSL Certification Regeneration

Click **SSH & SSL** from the menu and select the **SSL** tab. The Certificate Information is shown on this screen.



SSH & SSL

Certificate Information

CA Name
Moxa Networking Co., Ltd.

Expiration Date
2198-05-26 18:53:44

Export SSL Certificate

Regenerate SSL Certificate

Configure the following settings:

Export SSL Certificate

Setting	Description	Factory Default
Export	Export the SSL certificate to your local computer.	None

Regenerate SSL Certificate

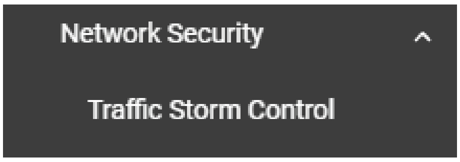
Setting	Description	Factory Default
Regenerate	Regenerate the SSL certificate.	None

Import Certificate

Setting	Description	Factory Default
Select the file	Import the SSL certificate from the location where the SSL certificate is located.	None

Network Security

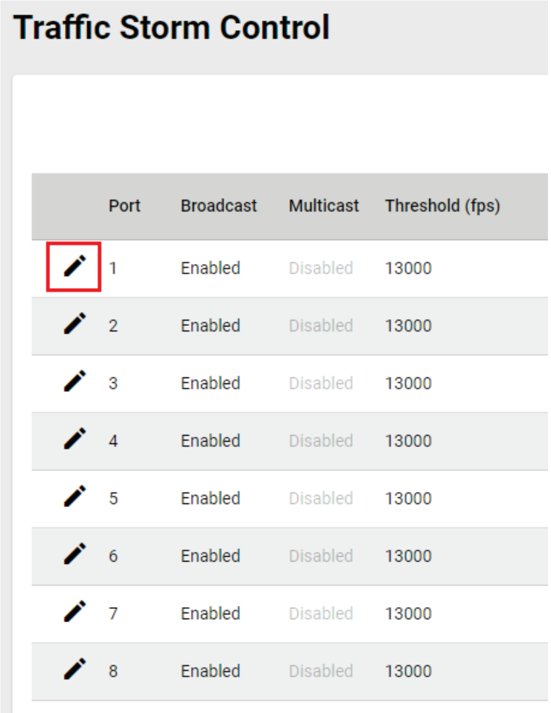
This section demonstrates how to configure network security settings for **Traffic Storm Control**.



Traffic Storm Control

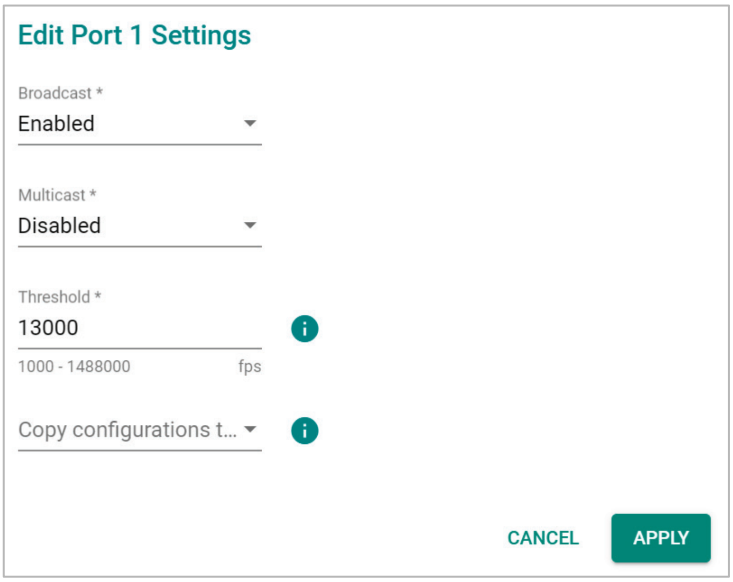
A traffic storm can happen when packets flood the network; this causes excessive traffic and slows down the network performance. To counter this, Traffic Storm Control provides an efficient design to prevent the network from flooding caused by a broadcast, multicast, or unicast traffic storm on a physical network layer. The feature can handle packets from both ingress and egress data.

First click **Traffic Storm Control** from the menu, and then click the edit icon on the specific port you want to configure. Threshold values differ depending on the model. The following reference images are from the TSN-G5004/8 models.



	Port	Broadcast	Multicast	Threshold (fps)
✎	1	Enabled	Disabled	13000
✎	2	Enabled	Disabled	13000
✎	3	Enabled	Disabled	13000
✎	4	Enabled	Disabled	13000
✎	5	Enabled	Disabled	13000
✎	6	Enabled	Disabled	13000
✎	7	Enabled	Disabled	13000
✎	8	Enabled	Disabled	13000

Configure the following settings:



Edit Port 1 Settings

Broadcast *
Enabled

Multicast *
Disabled

Threshold *
13000
1000 - 1488000 fps

There are two methods that can be used for traffic storm control: Broadcast and Multicast.

Broadcast

Setting	Description	Factory Default
Enabled	Enable Broadcast control, limiting broadcast packets during traffic storms.	Enabled
Disabled	Disable Broadcast control, forwarding all broadcast packets during traffic storms.	

Multicast

Setting	Description	Factory Default
Enabled	Enable multicast control, limiting multicast packets during traffic storms.	Disabled
Disabled	Disable multicast control, forwarding all multicast packets during traffic storms.	

Threshold (fps/Mbps)

Due to hardware limitations, the **Traffic Storm Control** calculation is different depending on the model.

TSN-G5004/G5008 models: fps

Setting	Description	Factory Default
1000 to 1488000	Define the threshold for a traffic storm (in fps).	13000

TSN-G5016 models: bps

Setting	Description	Factory Default
1GbE ports: 1 to 850 10GbE ports: 1 to 8500	Define the threshold for a traffic storm (in Mbps).	8

Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configurations to other port(s).	None

When finished, click **APPLY** to save your changes.

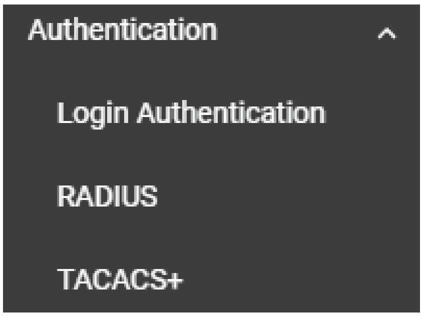
Authentication

This section describes how to configure system authentication including RADIUS and TACACS+. Moxa switches have three different user login authentications: TACACS+ (Terminal Access Controller Access-Control System Plus), RADIUS (Remote Authentication Dial In User Service), and Local. The TACACS+ and RADIUS mechanisms are centralized "AAA" (Authentication, Authorization, and Accounting) systems for connecting to network services. The fundamental purpose of both TACACS+ and RADIUS is to provide an efficient and secure mechanism for user account management.

There are five combinations available for users to choose from:

- **TACACS+, Local:** Check the TACACS+ database first. If checking the TACACS+ database fails, then check the Local database.
- **RADIUS, Local:** Check the RADIUS database first. If checking the RADIUS database fails, then check the Local database.
- **TACACS+:** Only check TACACS+ database.
- **RADIUS:** Only check the RADIUS database.
- **Local:** Only check the Local database.

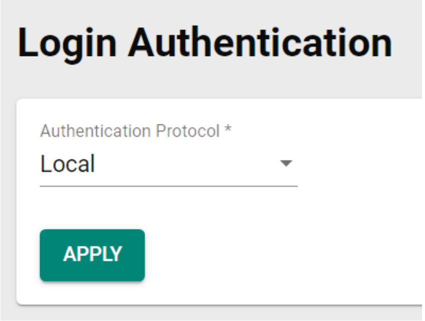
This section includes the configurations for **Login Authentication, RADIUS,** and **TACACS+**.



Login Authentication

This section allows users to select the login authentication protocol.

Select **Login Authentication**.


Login Authentication

Authentication Protocol *: Local

Configure the following settings:

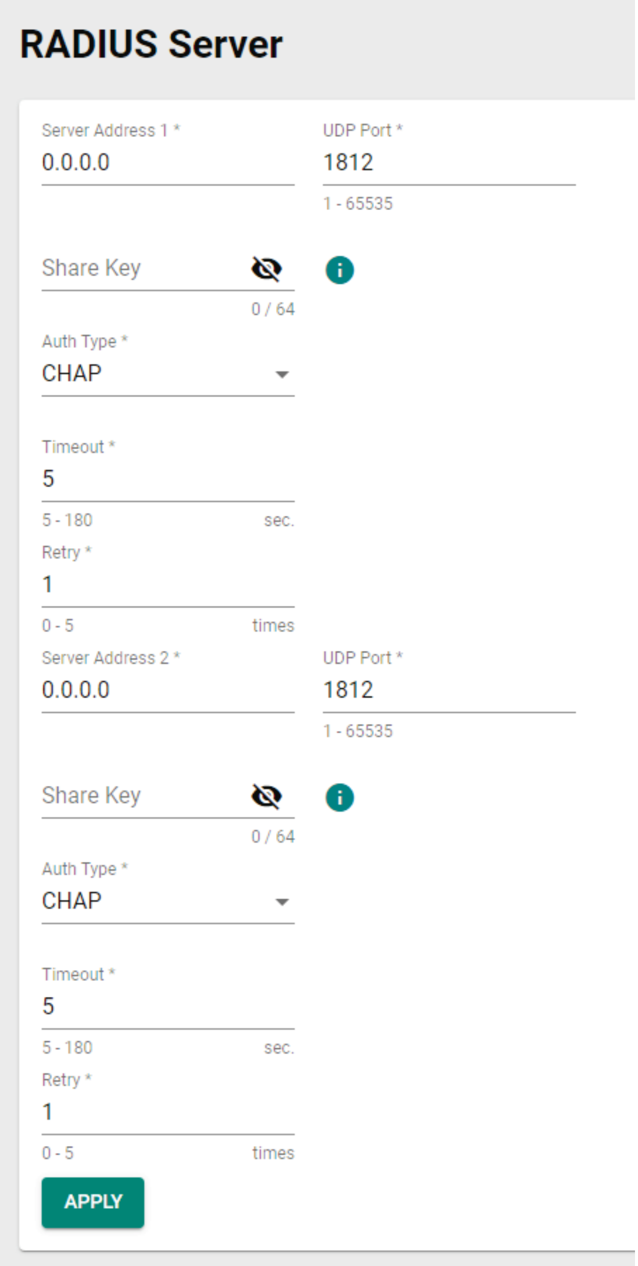
Authentication Protocol

Setting	Description	Factory Default
Local	Select Local as the authentication protocol.	Local
RADIUS	Select RADIUS as the authentication protocol.	
TACACS+	Select TACACS+ as the authentication protocol.	
RADIUS, Local	Select RADIUS and Local as the authentication protocol.	
TACACS+, Local	Select TACACS+ and Local as the authentication protocol.	

When finished, click **APPLY** to save your changes.

RADIUS

Click **RADIUS** from the menu and Configure the following settings:



RADIUS Server

Server Address 1 * 0.0.0.0

UDP Port * 1812

1 - 65535

Share Key

0 / 64

Auth Type * CHAP

Timeout * 5

5 - 180 sec.

Retry * 1

0 - 5 times

Server Address 2 * 0.0.0.0

UDP Port * 1812

1 - 65535

Share Key

0 / 64

Auth Type * CHAP

Timeout * 5

5 - 180 sec.

Retry * 1

0 - 5 times

Server Address 1

Setting	Description	Factory Default
Input the server address	Specify the 1st server address as the authentication database.	0.0.0.0

UDP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	1812

Share Key

Setting	Description	Factory Default
Input the key	Input the share key for 1st server authentication verification.	None

Auth Type

Setting	Description	Factory Default
PAP	Set the authentication type to PAP.	CHAP
CHAP	Set the authentication type to CHAP.	
MS-CHAPv1	Set the authentication type to MS-CHAPv1.	

Timeout (sec.)

Setting	Description	Factory Default
5 to 180	When waiting for a response from the server, set the amount of time before timeout.	5

Retry (sec.)

Setting	Description	Factory Default
0 to 5	Define the retry interval when trying to reconnect to a server.	1

Server Address 2

Setting	Description	Factory Default
Input the server address	Specify the 2nd server address as the authentication database.	0.0.0.0

UDP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	1812

Share Key

Setting	Description	Factory Default
Input the key	Specify the share key for 2nd server authentication verification.	None

Auth Type

Setting	Description	Factory Default
PAP	Set the authentication type to PAP.	CHAP
CHAP	Set the authentication type to CHAP.	
MS-CHAPv1	Set the authentication type to MS-CHAPv1.	

Timeout (sec.)

Setting	Description	Factory Default
5 to 180	When waiting for a response from the server, set the amount of time before the device is timed out.	5

Retry (sec.)

Setting	Description	Factory Default
0 to 5	Set the retry interval when trying to reconnect to a server.	1

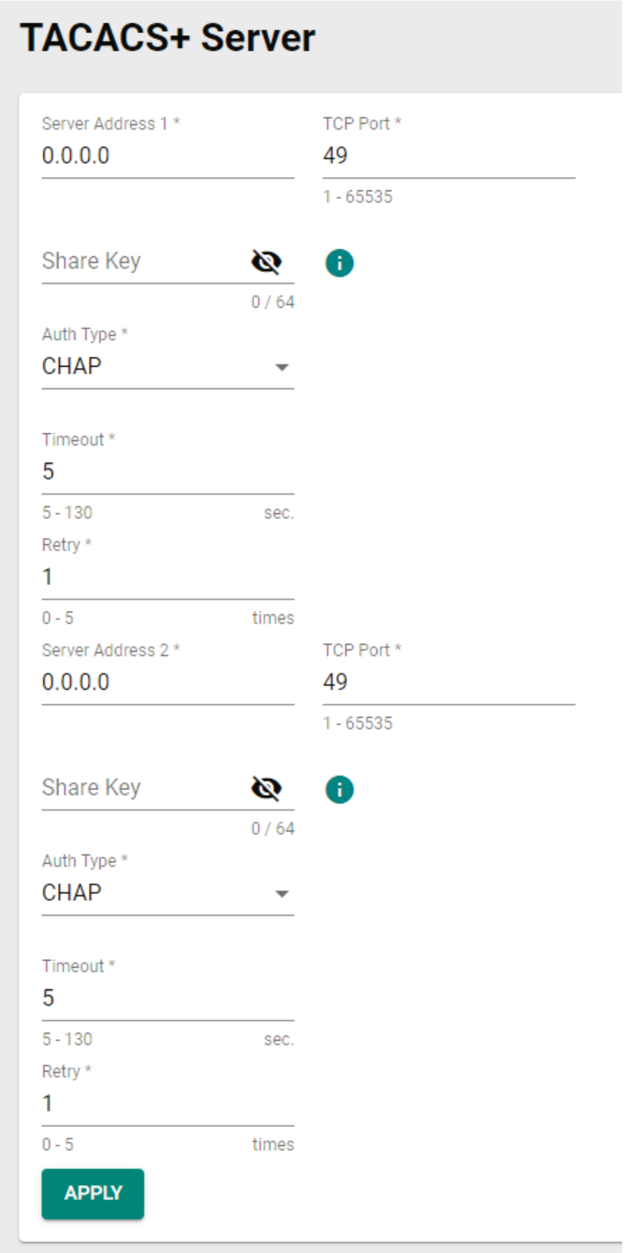
When finished, click **APPLY** to save your changes.

NOTE

RADIUS authentication services will be handled by the primary RADIUS server. If the primary server becomes unavailable, the secondary RADIUS server will take over.

TACACS+

Click **TACACS+** from the menu and then Configure the following settings:



TACACS+ Server

Server Address 1 *: 0.0.0.0

TCP Port *: 49 (1 - 65535)

Share Key (0 / 64)

Auth Type *: CHAP

Timeout *: 5 (5 - 130 sec.)

Retry *: 1 (0 - 5 times)

Server Address 2 *: 0.0.0.0

TCP Port *: 49 (1 - 65535)

Share Key (0 / 64)

Auth Type *: CHAP

Timeout *: 5 (5 - 130 sec.)

Retry *: 1 (0 - 5 times)

APPLY

Server Address 1

Setting	Description	Factory Default
Input the server address	Specify the 1st server address as the authentication database.	0.0.0.0

TCP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	49

Share Key

Setting	Description	Factory Default
Input the key	Specify the share key for 1st server authentication verification.	None

Auth Type

Setting	Description	Factory Default
ASCII	Set the authentication type to ASCII.	CHAP
PAP	Set the authentication type to PAP.	
CHAP	Set the authentication type to CHAP.	

Timeout (sec.)

Setting	Description	Factory Default
Input the value	When waiting for a response from the server, set the amount of time before the device is timed out.	5

Retry

Setting	Description	Factory Default
Input the value	Set the retry interval when trying to reconnect to a server.	1

Server Address 2

Setting	Description	Factory Default
Input the server address	Specify the 2nd server address as the authentication database.	0.0.0.0

TCP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	49

Share Key

Setting	Description	Factory Default
Input the key	Specify the share key for 2nd server authentication verification.	None

Auth Type

Setting	Description	Factory Default
ASCII	Set the authentication type to ASCII.	CHAP
PAP	Set the authentication type to PAP.	
CHAP	Set the authentication type to CHAP.	

Timeout (sec.)

Setting	Description	Factory Default
Input the value	When waiting for a response from the server, set the amount of time before the device is timed out.	5

Retry

Setting	Description	Factory Default
Input the value	Set the retry interval when trying to reconnect to a server.	1

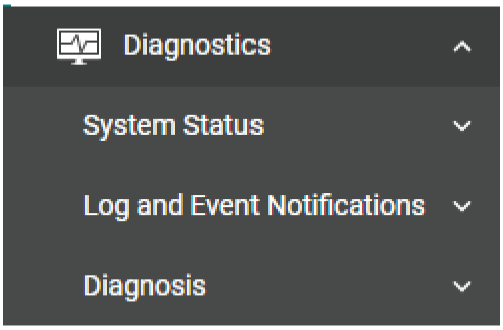
When finished, click **APPLY** to save your changes.

NOTE

TACACS+ authentication services will be handled by the primary TACACS+ server. If the primary server becomes unavailable, the secondary RADIUS server will take over.

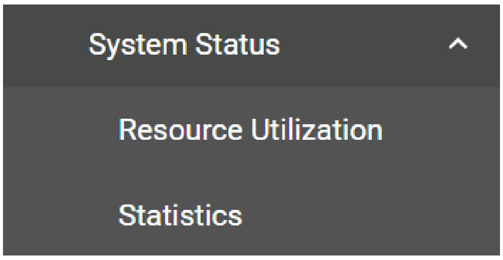
Diagnostics

This section describes the diagnostics functions of Moxa’s switch. Click **Diagnostics** from the function menu.



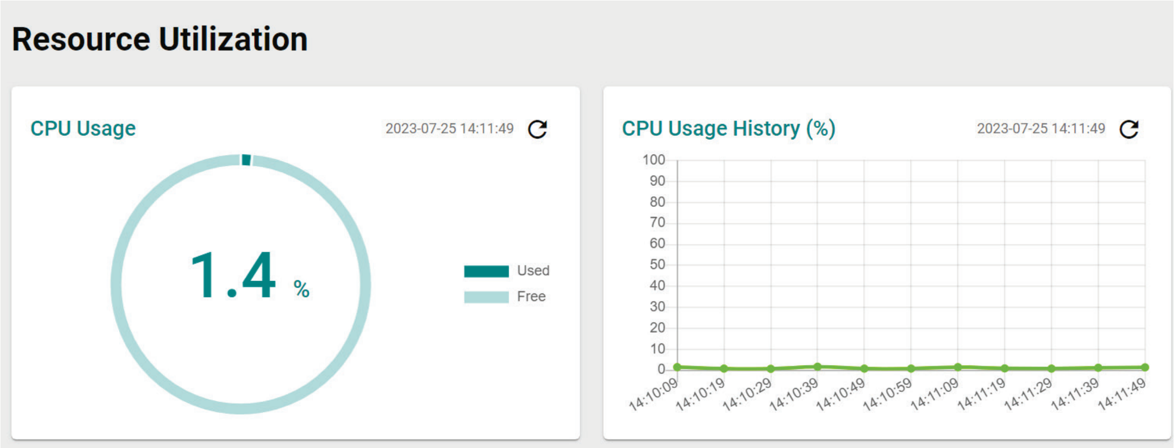
System Status

This section allows users to view the current system status, including **Resource Utilization** and **Statistics**.



Resource Utilization

Click **Resource Utilization** from the function menu to view the current utilization status including CPU utilization, memory history, power consumption, and power history. All of the information is displayed via graphics, making it easier for users to view the system status. In addition, a refresh icon is available on the upper right corner of each figure, which allows users to view the latest status for each function.

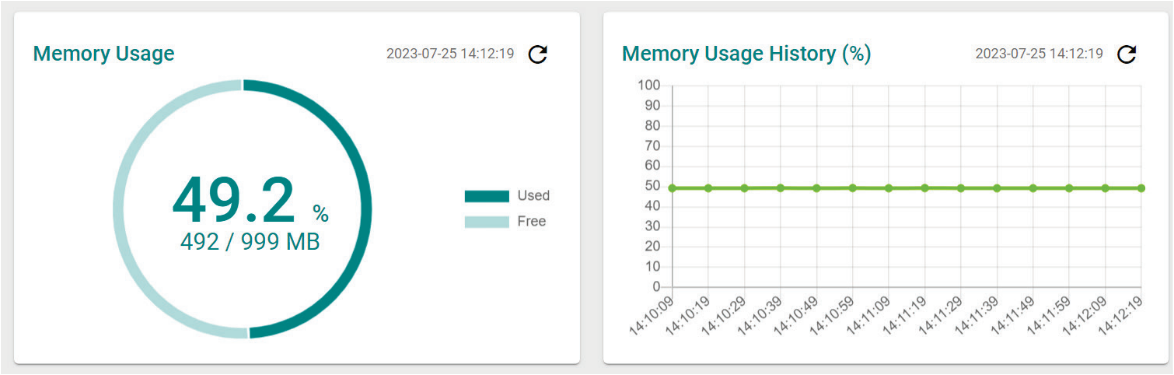


CPU Usage

Setting	Description	Factory Default
Read-only	Displays the current utilization of the CPU.	None

CPU Usage History

Setting	Description	Factory Default
Read-only	Displays the CPU usage history trend in a chart.	None

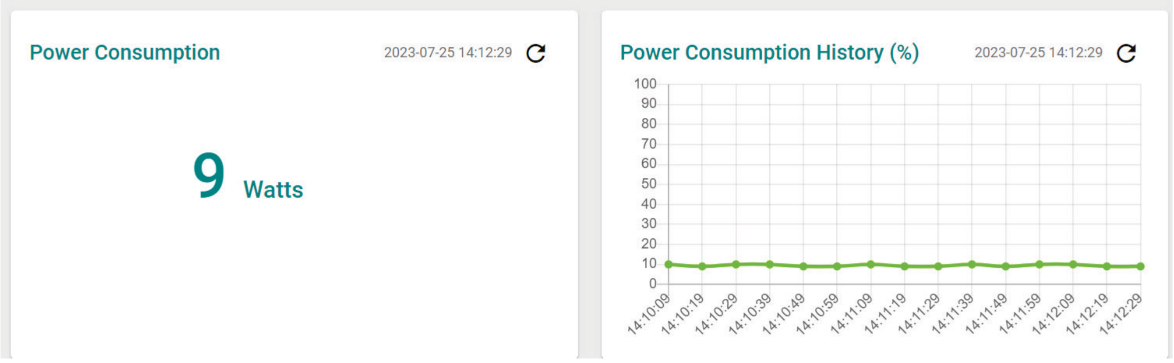


Memory Usage

Setting	Description	Factory Default
Read-only	Displays the memory status.	None

Memory Usage History

Setting	Description	Factory Default
Read-only	Displays the history of the memory usage.	None



Power Consumption

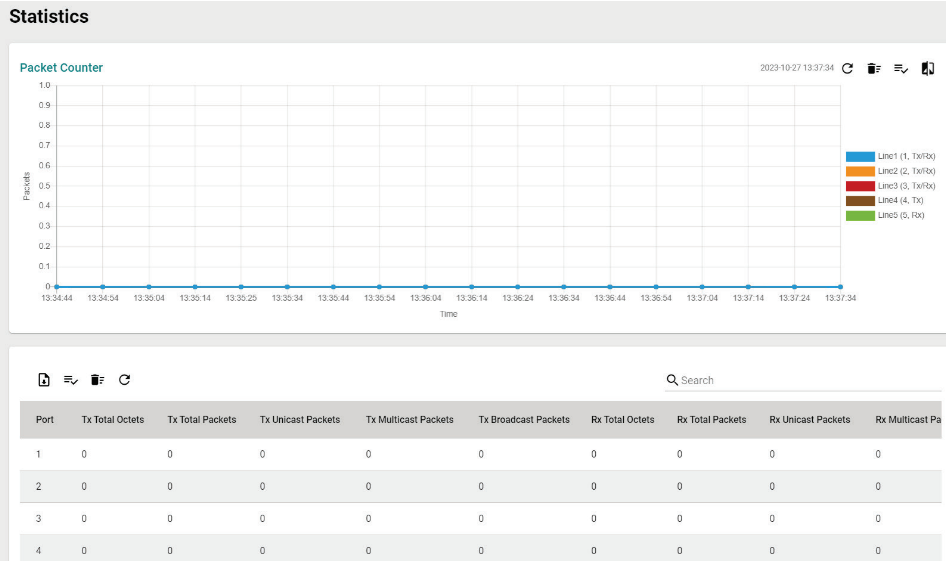
Setting	Description	Factory Default
Read-only	Displays the current power consumption in Watts.	None

Power Consumption History

Setting	Description	Factory Default
Read-only	Displays the history of the power usage.	None

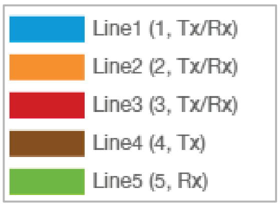
Statistics

Click **Statistics** from the function menu. The first figure shows the packet counter status.



Port	Tx Total Octets	Tx Total Packets	Tx Unicast Packets	Tx Multicast Packets	Tx Broadcast Packets	Rx Total Octets	Rx Total Packets	Rx Unicast Packets	Rx Multicast Pa
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0

The status of the different ports will be shown in different colors. A maximum of five ports will have their information displayed. Detailed port status shown as follows:



🟦 Line1 (1, Tx/Rx)
🟧 Line2 (2, Tx/Rx)
🟥 Line3 (3, Tx/Rx)
🟫 Line4 (4, Tx)
🟩 Line5 (5, Rx)

There are four icons on the upper-right corner of the page. Refer to the table below for a description of each icon.

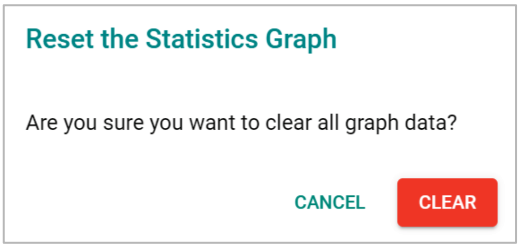
Item	Name	Description
↻	Refresh	Refresh all statistical data.
🗑	Reset	Clear data from the corresponding display.
≡✓	Display Settings	Select the data shown on the corresponding display.
◧	Compare Data	Select the data you want to compare.
⤓	Export	Export CSV or PDF.

Refreshing the Statistics

Click the **Refresh** button immediately refreshed all statistical data.

Resetting the Statistics Graph

Click the **Reset** button and click **CLEAR** to clear the packet counter and reset the graph.

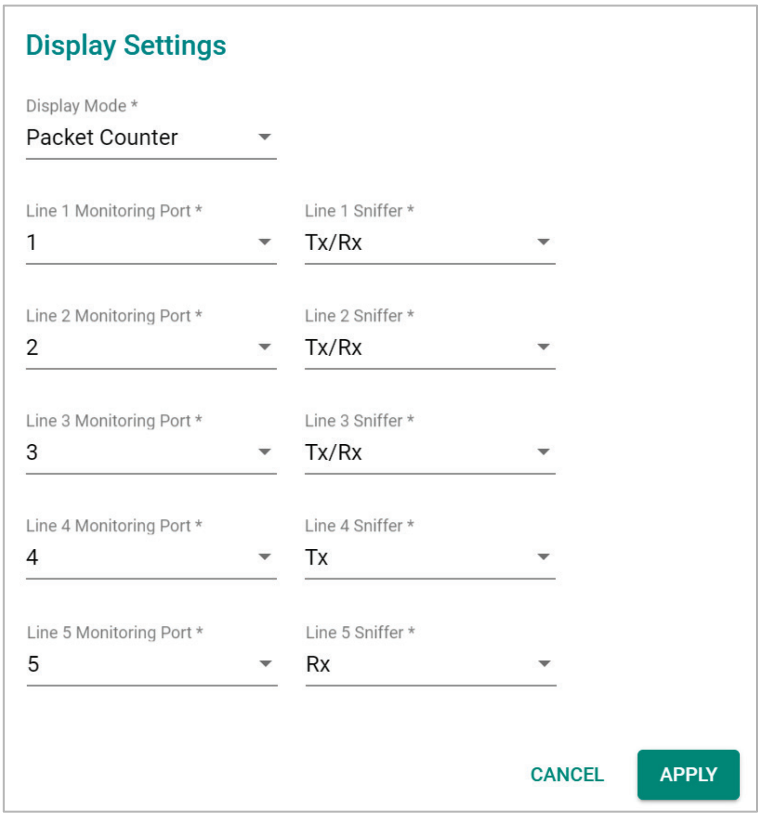


Reset the Statistics Graph

Are you sure you want to clear all graph data?

Display Settings

Click the **Display Settings** icon to configure the data shown on the graph. You can select the display mode from the drop-down list.



Display Settings

Display Mode *: Packet Counter

Line 1 Monitoring Port *: 1 — Line 1 Sniffer *: Tx/Rx

Line 2 Monitoring Port *: 2 — Line 2 Sniffer *: Tx/Rx

Line 3 Monitoring Port *: 3 — Line 3 Sniffer *: Tx/Rx

Line 4 Monitoring Port *: 4 — Line 4 Sniffer *: Tx

Line 5 Monitoring Port *: 5 — Line 5 Sniffer *: Rx

The Monitoring Port is the port you want to view or monitor. The sniffer port is the port that you can choose to view its receiving or transmission status, or both.

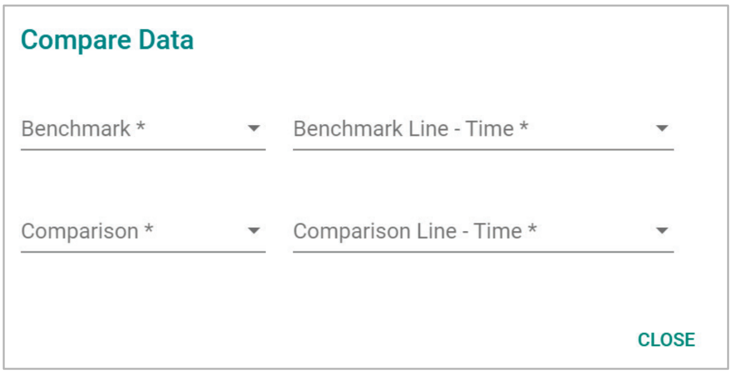
Display Mode

Setting	Description	Factory Default
Packet Counter	The packet statistics will be displayed.	Packet Counter
Bandwidth Usage	The bandwidth statistics will be displayed.	

When finished, click **APPLY** to save your changes.

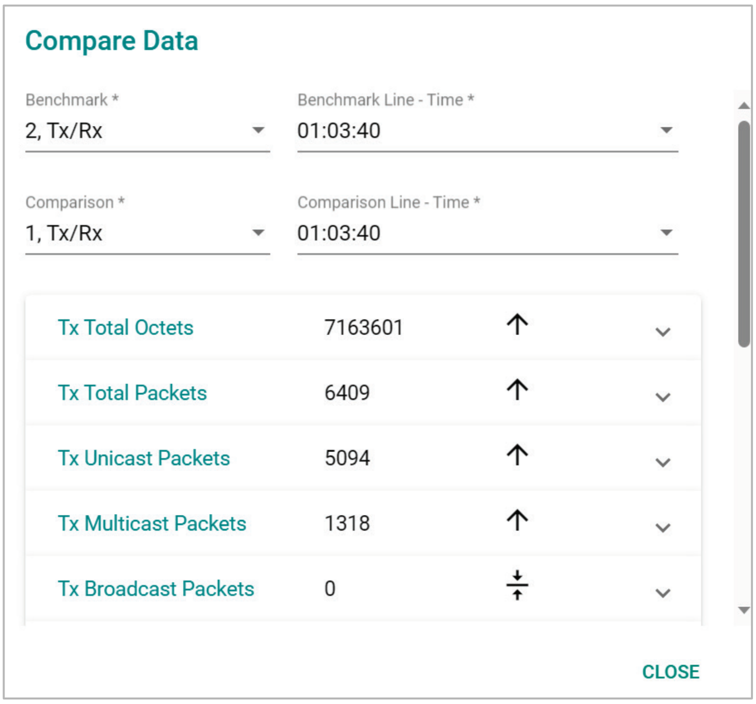
Comparing Data

Click the **Compare Data** icon and then select the items from the relevant fields.



Compare Data

Select the data to compare. When finished, click **Close**.



Compare Data

Benchmark *: 2, Tx/Rx

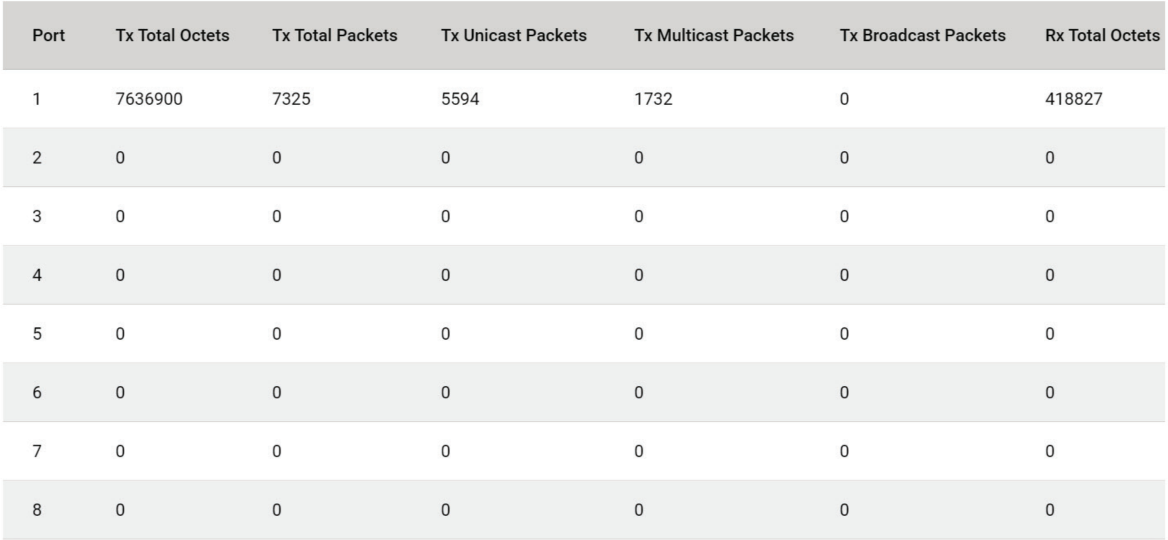
Benchmark Line - Time *: 01:03:40

Comparison *: 1, Tx/Rx

Comparison Line - Time *: 01:03:40

Tx Total Octets	7163601	↑
Tx Total Packets	6409	↑
Tx Unicast Packets	5094	↑
Tx Multicast Packets	1318	↑
Tx Broadcast Packets	0	≑

Transmission activity information for each port will be shown in the table.



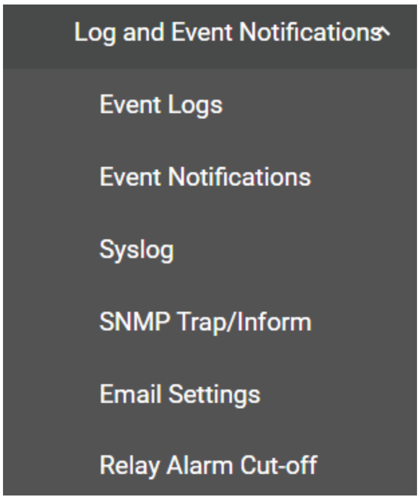
Port	Tx Total Octets	Tx Total Packets	Tx Unicast Packets	Tx Multicast Packets	Tx Broadcast Packets	Rx Total Octets
1	7636900	7325	5594	1732	0	418827
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0

Setting	Description
Port	The port number.
Tx Total Octets	The Number of octets transmitted including bad packets and FCS octets. Framing bits are not included.
Tx Total Packets	The number of packets transmitted.
Tx Unicast Packets	The number of Unicast packets transmitted.
Tx Multicast Packets	The number of Multicast packets transmitted.
Tx Broadcast Packets	The number of good Broadcast packets transmitted. Multicast packets are not included.
Rx Total Octets	The number of octets received, including bad packets and FCS octets. Framing bits are not included.
Rx Total Packets	The number of packets received.
Rx Unicast Packets	The number of Unicast packets received.
Rx Multicast Packets	The number of Multicast packets received.
Rx Broadcast Packets	The number of valid Broadcast packets received. Multicast packets are not included.

Setting	Description
CRC Align Error Packets	The number of CRC and Align errors that have occurred.
Dropped Packets	The number of packets that were dropped.
Undersize	The number of undersized packets (less than 64 octets) received.
Oversized Packets	The number of oversized packets (over 1518 octets) received.

Log and Event Notifications

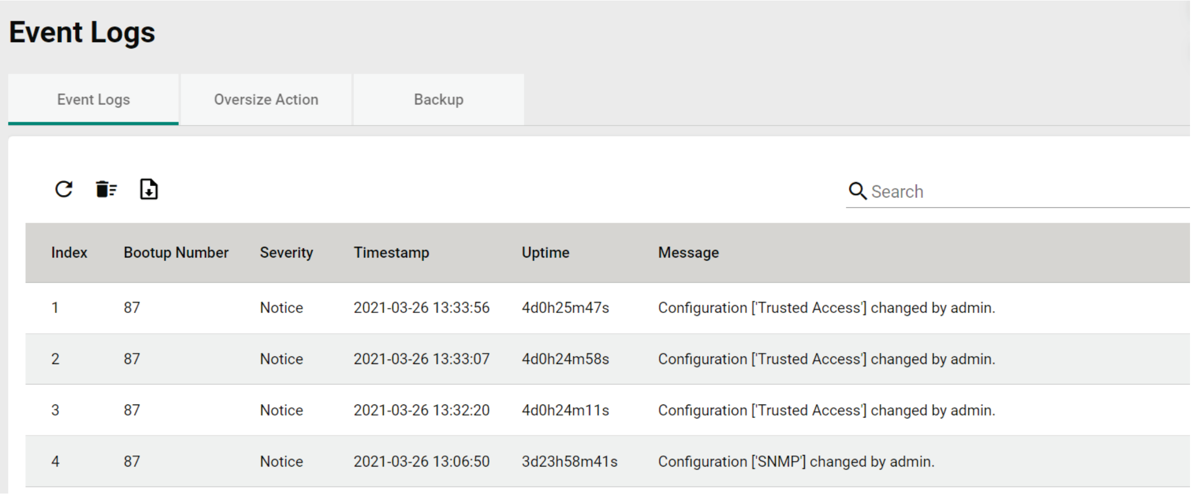
This section includes the information regarding **Event Logs**, **Event Notifications**, **Syslog**, **SNMP Trap/Inform**, **Email Notification**, and **Relay Alarm Cut-off**.



Event Logs

Viewing Event Logs

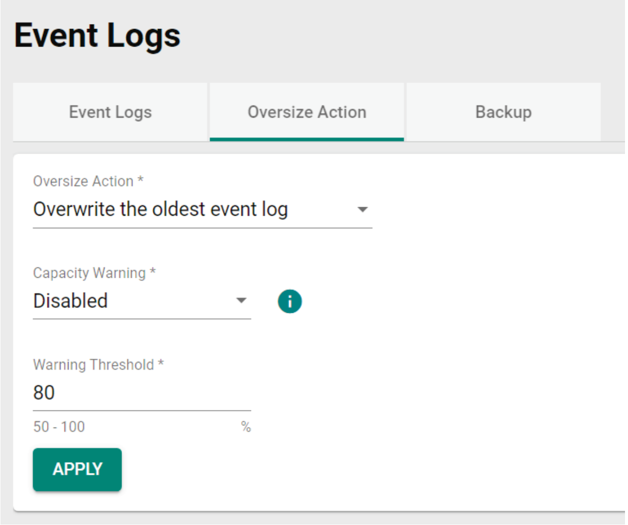
Click the **Event Logs** tab to view information about all recorded events.



Index	Bootup Number	Severity	Timestamp	Uptime	Message
1	87	Notice	2021-03-26 13:33:56	4d0h25m47s	Configuration ['Trusted Access'] changed by admin.
2	87	Notice	2021-03-26 13:33:07	4d0h24m58s	Configuration ['Trusted Access'] changed by admin.
3	87	Notice	2021-03-26 13:32:20	4d0h24m11s	Configuration ['Trusted Access'] changed by admin.
4	87	Notice	2021-03-26 13:06:50	3d23h58m41s	Configuration ['SNMP'] changed by admin.

Configuring the Oversize Action

To edit the event log oversize action, click the **Oversize Action** tab. The oversize action will trigger when the event log reaches maximum capacity.



Event Logs

Oversize Action *
Overwrite the oldest event log

Capacity Warning *
Disabled

Warning Threshold *
80
50 - 100 %

Configure the following settings when the event logs file is full.

Oversize-Action

Setting	Description	Factory Default
Overwrite the oldest event log	If the log capacity is reached, new log entries will overwrite oldest logs first.	Overwrite the oldest event log
Stop recording event logs	If the log capacity is reached, no new event log entries will be recorded.	

The event log supports a capacity warning to alert users when the event log has reached the specified percentage of the maximum log capacity. The event log can record a total of 10,000 event logs.

Capacity Warning

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable event log capacity warnings.	Disabled

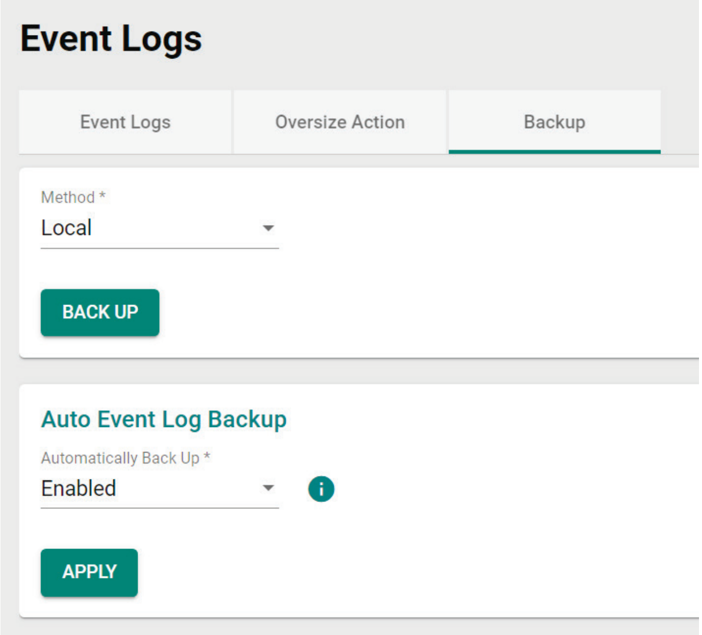
Warning Threshold (%)

Setting	Description	Factory Default
50 to 100	Set the warning threshold as a percentage.	80

When finished, click **APPLY** to save your changes.

Backup Event Logs

To back up the event log, click the **Backup** tab.



Event Logs

Method *
Local

Auto Event Log Backup

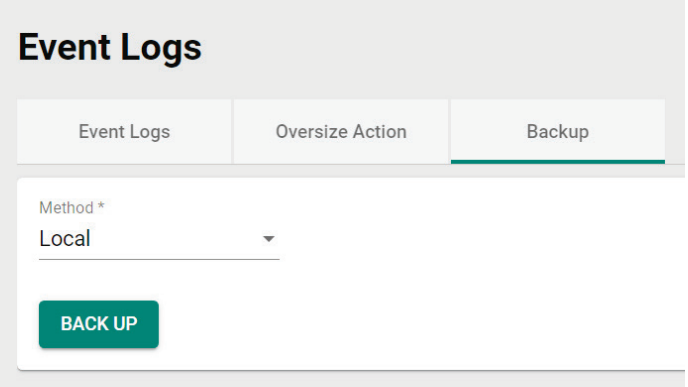
Automatically Back Up *
Enabled

Method

Setting	Description	Factory Default
Select from the drop-down list	Specify whether to back up the event logs from a local drive, by a remote SFTP server, by a remote TFTP server, by a USB, or by a microSD.	Local

Back Up Event Logs Locally

Select **Local** from the drop-down list under Method. This will back up the event log to the local host.



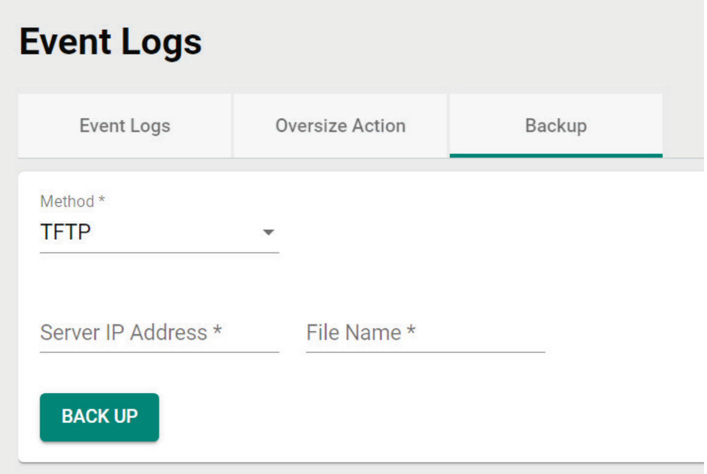
Event Logs

Method *
Local

When finished, click **BACK UP** to back up the event log.

Back Up Event Logs Via TFTP

Select **TFTP** from the drop-down list under **Method**.



Event Logs

Method * TFTP

Server IP Address

Setting	Description	Factory Default
IP address	Enter the IP address of the SFTP server to store the event log backup file on.	None

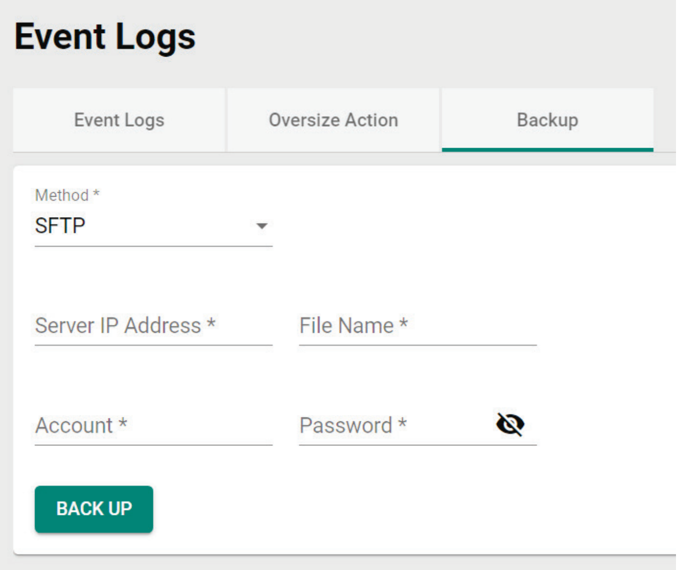
File Name

Setting	Description	Factory Default
Filename	Enter the filename of the event log backup file.	None

When finished, click **BACK UP** to back up the event log.

Back Up Event Logs Via SFTP

Select **SFTP** from the drop-down list under **Method**.



Event Logs

Method * SFTP

Server IP Address

Setting	Description	Factory Default
IP address	Enter the IP address of the SFTP server to store the event log backup file on.	None

File Name

Setting	Description	Factory Default
Filename	Enter the filename of the event log backup file.	None

Account

Setting	Description	Factory Default
Account name	Enter the SFTP server account name used to authorize the connection to the server.	None

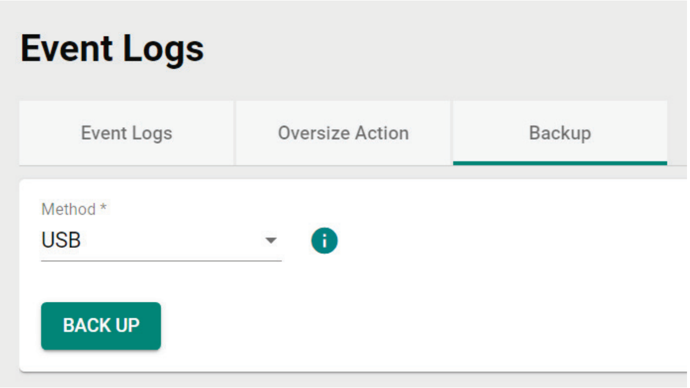
Password

Setting	Description	Factory Default
Password	Enter the SFTP server password used to authorize the connection to the server.	None

When finished, click **BACK UP** to back up the event log.

Back Up Event Logs Via USB

Select **USB** from the drop-down list under **Method**.



Event Logs

Method * USB

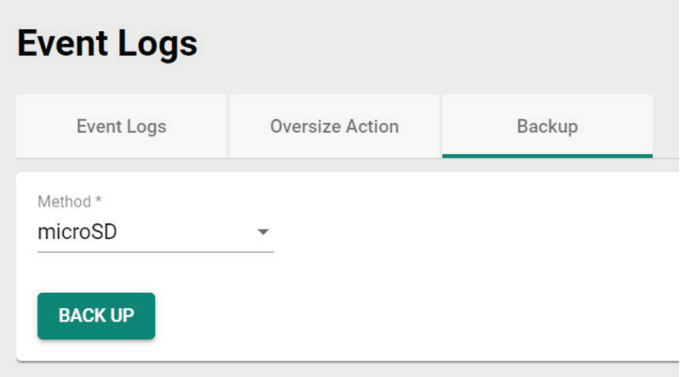
Connect the Moxa ABC-02 USB configuration tool to the switch and click **BACK UP** to back up the event log.

NOTE

If you encounter issues using the ABC-02 configuration tool, check if the **USB Interface** has been enabled in the Hardware Interfaces section.

Back Up Event Logs Via microSD

Select **microSD** from the drop-down list under **Method**.



Event Logs

Method * microSD

Connect the Moxa ABC-03-microSD-T configuration tool to the switch and click **BACK UP** to back up the event log.

NOTE

If you encounter issues using the ABC-03 configuration tool, check if the **MicroSD Interface** has been enabled in the Hardware Interfaces section.

Backup

The automatic backup function enables the system to automatically back up the event log whenever new event logs are recorded. The storage location of the backup file depends on the selected backup method.

Back Up

Setting	Description	Factory Default
Enabled	Automatically back up to external storage when new event logs are recorded.	Enabled
Disabled	Do not automatically back up to external storage when new event logs are recorded.	

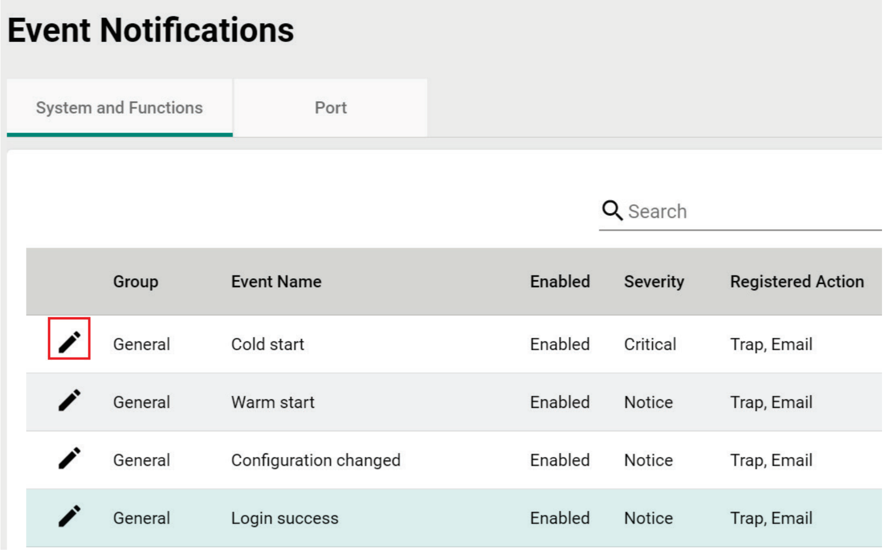
When finished, click **APPLY** to save your changes.

Event Notifications

You can configure notifications for two main types of events: System and functions events, and port events.

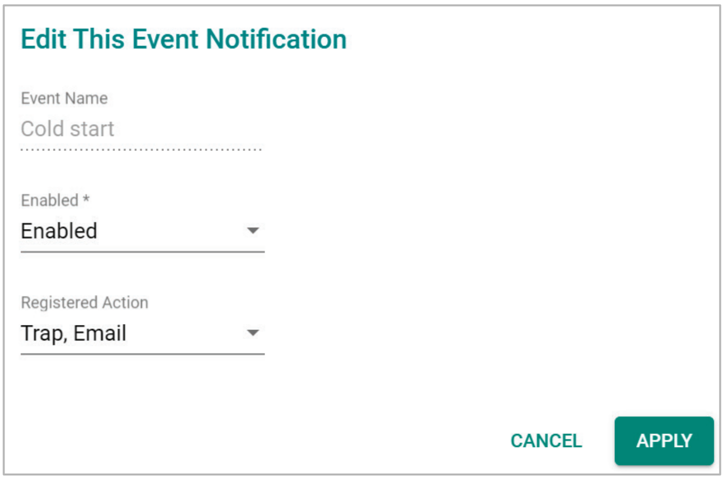
Configuring Notifications for System and Functions Events

On the **Event Notifications** screen, click the **System and Functions** tab. Click the edit icon of the specific event you want to configure.



	Group	Event Name	Enabled	Severity	Registered Action
✎	General	Cold start	Enabled	Critical	Trap, Email
✎	General	Warm start	Enabled	Notice	Trap, Email
✎	General	Configuration changed	Enabled	Notice	Trap, Email
✎	General	Login success	Enabled	Notice	Trap, Email

Configure the following settings:



Event Name: Cold start

Enabled *: Enabled

Registered Action: Trap, Email

Enabled

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable notifications for this event.	Enabled

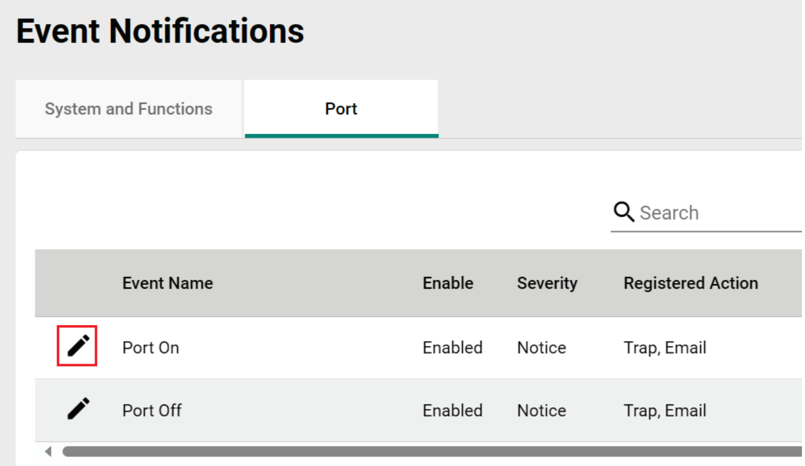
Registered Action

Setting	Description	Factory Default
Trap	Send notifications via SNMP Trap. This requires SNMP Trap/Inform settings to be configured first. Refer to SNMP Trap/Inform.	Trap, Email
Email	Send notifications via email. This requires Email settings to be configured first. Refer to Email Notification.	
Relay	Trigger the relay for notifications. This requires Relay settings to be configured first. Refer to Relay Alarm Cut-off.	

When finished, click **APPLY** to save your changes.

Configuring Notifications for Port Events

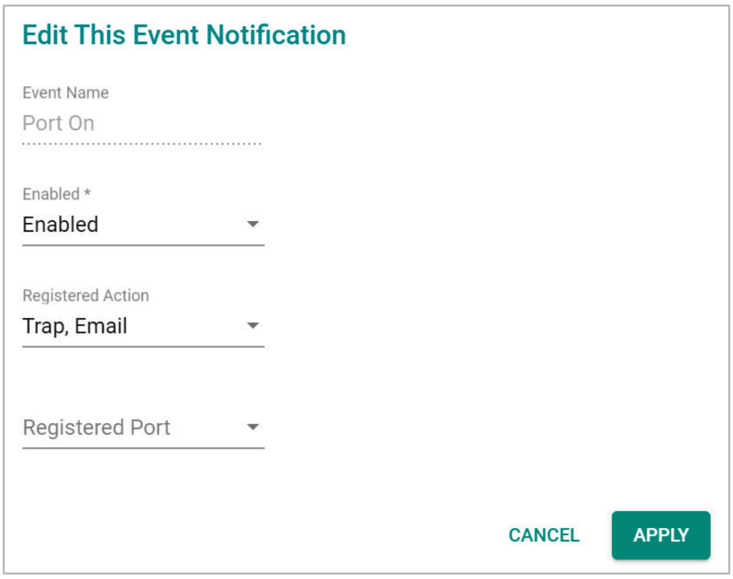
On the **Event Notifications** screen, click the **Port** tab. Click the edit icon of the specific event you want to configure.



Event Notifications

	Event Name	Enable	Severity	Registered Action
	Port On	Enabled	Notice	Trap, Email
	Port Off	Enabled	Notice	Trap, Email

Configure the following settings:



Edit This Event Notification

Event Name: Port On

Enabled *: Enabled

Registered Action: Trap, Email

Registered Port

Enabled

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable notifications for this event.	Enabled

Registered Action

Setting	Description	Factory Default
Trap	Send notifications via SNMP Trap. This requires SNMP Trap/Inform settings to be configured first. Refer to SNMP Trap/Inform.	Trap, Email
Email	Send notifications via email. This requires Email settings to be configured first. Refer to Email Notification.	
Relay	Trigger the relay for notifications. This requires Relay settings to be configured first. Refer to Relay Alarm Cut-off.	

Registered Port

Setting	Description	Factory Default
Select port(s) from the drop-down list	Specify the port(s) that will use the registered action.	None

When finished, click **APPLY** to save your changes.

The same method is used to edit other events such as, port status is off, port shutdown by port security, and port recovery by rate limit.

Event Severity Overview

Check the following table for an overview of the severity of each event..

System & Functions	
Event Name	**Severity**
Cold start	Critical
Warm start	Notice
Configuration changed	Notice
Login success	Notice
Login fail	Warning
Login lockout	Warning
Account setting changed	Notice
Configuration imported	Notice
SSL certification changed	Notice
Log capacity threshold	Warning
Password changed	Notice
PWR Off->On	Notice
PWR On->Off	Notice
DI On	Notice
DI Off	Notice
RSTP topology changed	Warning
LLDP table changed	Information

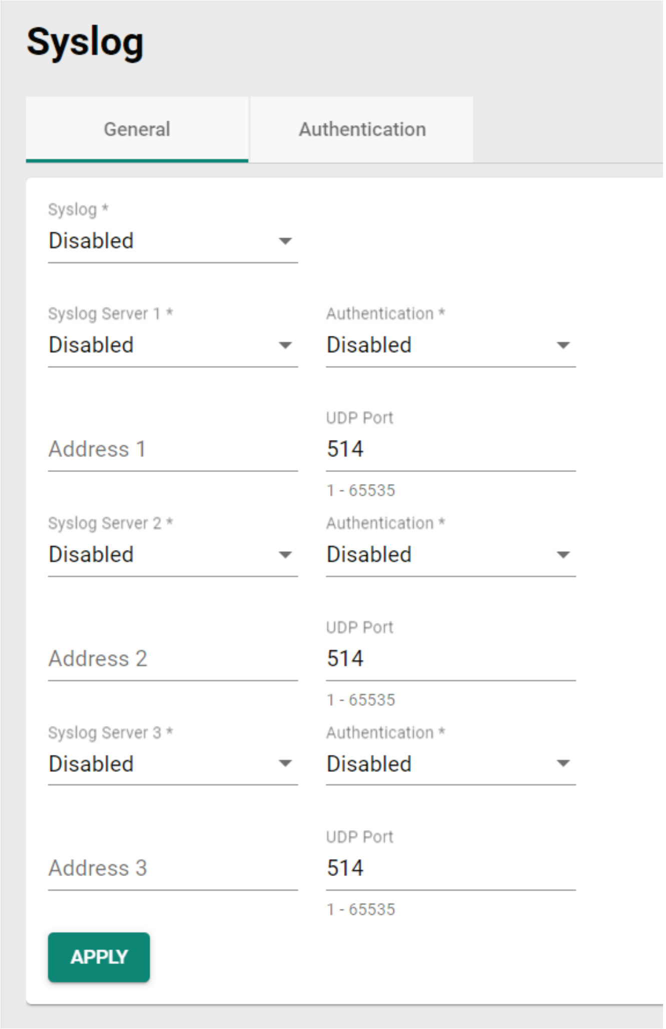
Port	
Event Name	**Severity**
Port On	Notice
Port Off	Notice

Syslog

The **Syslog** section is used to configure the Syslog server parameters and set up the authentication method.

General Settings

Click **Syslog** from the function menu, then click the **General** tab to configure basic syslog server parameters.



Syslog

General | Authentication

Syslog *: Disabled

Syslog Server 1 *: Disabled | Authentication *: Disabled

Address 1 | UDP Port: 514 (1 - 65535)

Syslog Server 2 *: Disabled | Authentication *: Disabled

Address 2 | UDP Port: 514 (1 - 65535)

Syslog Server 3 *: Disabled | Authentication *: Disabled

Address 3 | UDP Port: 514 (1 - 65535)

Configure the following settings:

Syslog

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable syslog functionality.	Disabled

Syslog Server 1/2/3

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the first, second, or third syslog server.	Disabled

Authentication

Setting	Description	Factory Default
Disabled	Disable authentication.	Disabled
TLS	Use a TLS certificate and key to authenticate the syslog server. Refer to Authentication section to create a certificate and key set required for TLS authentication.	

Address 1/2/3

Setting	Description	Factory Default
IP address	Enter IP address of the first, second, or third syslog server.	None

UDP Port

Setting	Description	Factory Default
1 to 65535	Enter the UDP port number of the first, second, or third syslog server.	514

When finished, click A**PPLY t**o save your changes.

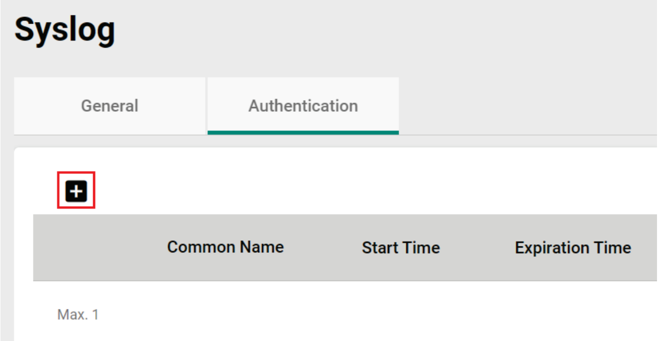
NOTE

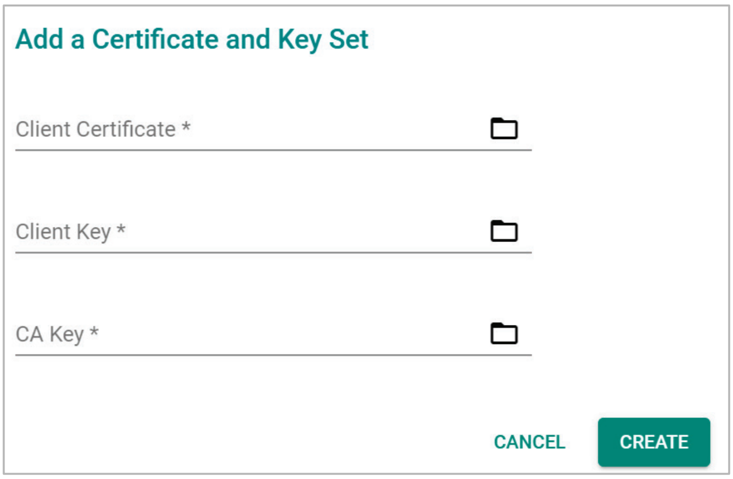
1. If the syslog server cannot receive the previous logs, it is possible that the receiving port of the syslog server is not ready. We recommend enabling the Linkup Delay function to delay the log delivery time.
2. A certificate and key set must be created before enabling TLS. Refer to the Authentication section.

Syslog Authentication

Click **Syslog** from the function menu, then click the **Authentication** tab to manage TLS authentication certificate and keys.

Click the + icon to add a certificate and key set.





Configure the following settings:

Client Certificate

Click the Browse button and navigate to the client certificate file on the local machine.

Client Key

Click the Browse button and navigate to the client key file on the local machine.

CA Key

Click the Browse button and navigate to the CA key file on the local machine.

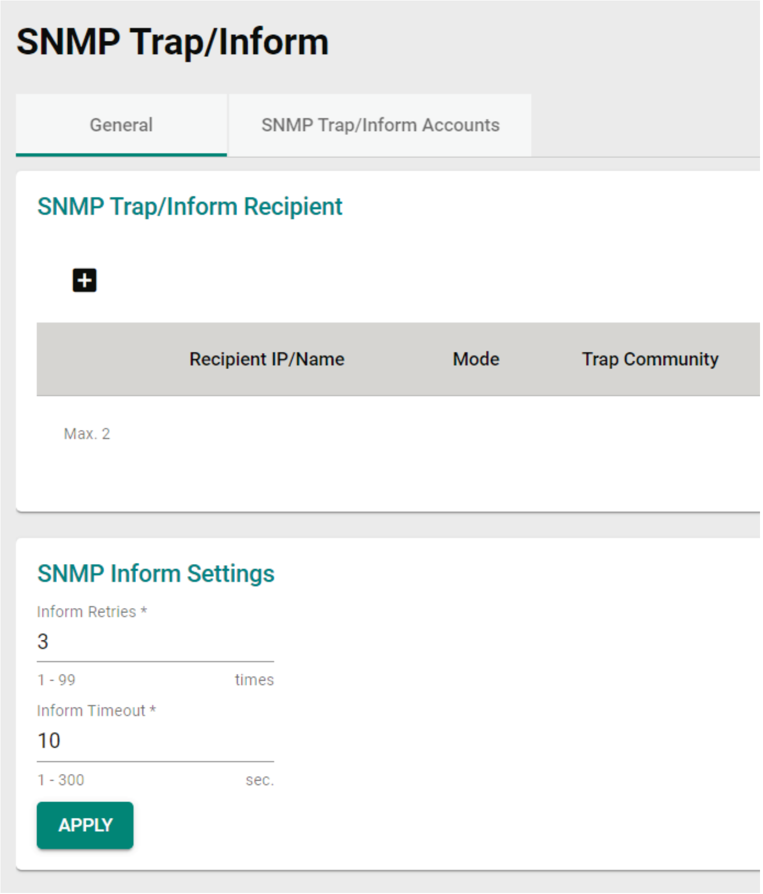
When finished, click **CREATE** to save your changes.

SNMP Trap/Inform

General Settings

Click **SNMP Trap/Inform** from the function menu, then click the **General** tab to manage SNMP Trap/Inform recipients and configure basic SNMP Inform settings.

First select **SNMP Trap/Inform** from the menu and then click the **General** tab.



Recipient IP/Name	Mode	Trap Community

Max. 2

SNMP Inform Settings

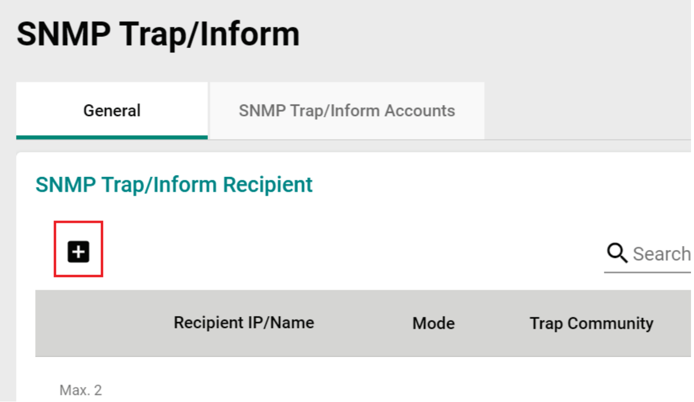
Inform Retries * 3 (1 - 99 times)

Inform Timeout * 10 (1 - 300 sec.)

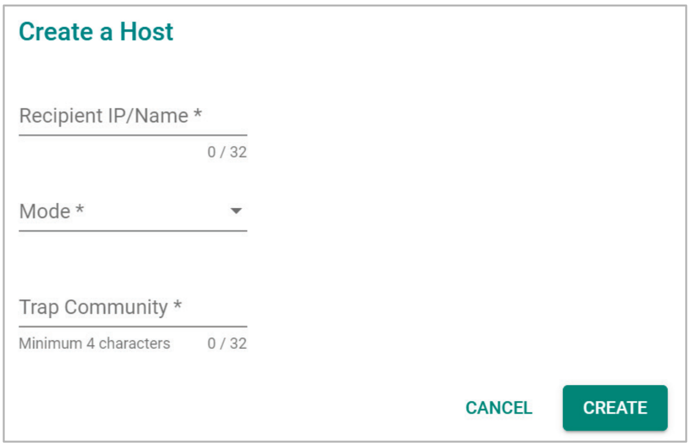
Adding an SNMP Trap/Inform Recipient

SNMP Trap allows an SNMP agent to notify the NMS of a significant event. The switch supports two SNMP modes: **Trap** and **Inform**.

Click the **+** icon to add a Trap/Inform recipient.



Configure the following settings:



Recipient IP/Name

Setting	Description	Factory Default
Max. 32 characters	Specify the recipient IP or hostname.	None

Mode

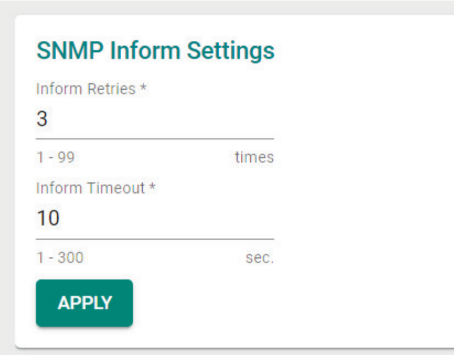
Setting	Description	Factory Default
Trap V1	Set the Trap version to Trap V1.	None
Trap V2c	Set the Trap version to Trap v2c.	
Inform V2c	Set the Inform version to Inform V2c.	
Trap V3	Set the Trap version to Trap V3.	
Inform V3	Set the Inform version to Inform V3.	

Trap Community

Setting	Description	Factory Default
4 to 32 characters	Specify the community string that will be used for authentication.	None

When finished, click **CREATE**.

SNMP Inform Settings


SNMP Inform Settings

Inform Retries *
3
1 - 99 times

Inform Timeout *
10
1 - 300 sec.

Configure the following settings:

Inform Retries (times)

Setting	Description	Factory Default
1 to 99	Specify the number of times the SNMP Inform is sent if no response is received from the SNMP manager.	3

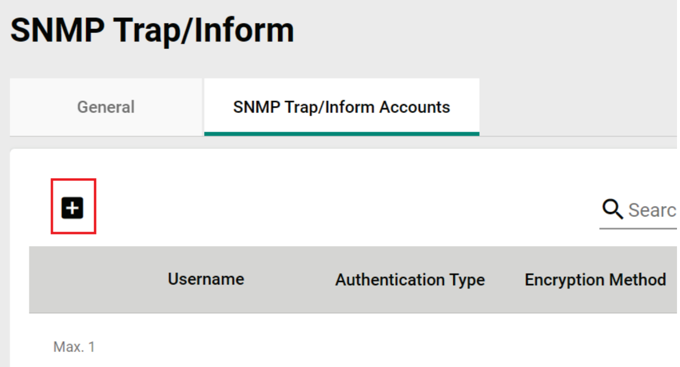
Timeout (sec.)

Setting	Description	Factory Default
1 to 300	Specify the duration (in seconds) the SNMP Inform sender will wait for a response from the SNMP manager before sending the Inform again.	10

When finished, click **APPLY** to save your changes.

Adding an SNMP Trap/Inform Account

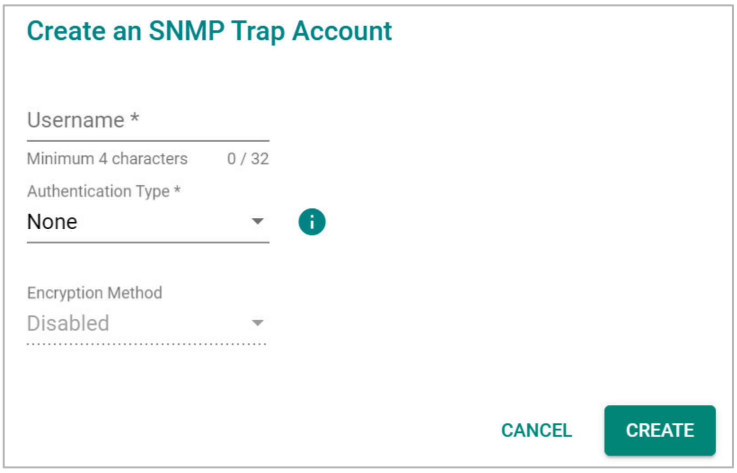
Click the **SNMP Trap/Inform Accounts** tab. Click the **+** icon to add an SNMP Trap account.


SNMP Trap/Inform

Username	Authentication Type	Encryption Method

Max. 1

Configure the following settings:


Create an SNMP Trap Account

Username *
Minimum 4 characters 0 / 32

Authentication Type *
None

Encryption Method
Disabled

Username

Setting	Description	Factory Default
At least 4 characters, (max. 32 characters)	Input a username.	None

Authentication type

Setting	Description	Factory Default
None	Disable authentication.	None
MD5	Use MD5 authentication.	
SHA	Use SHA authentication.	

Authentication Password

Setting	Description	Factory Default
8 to 64 characters	Enter the authentication password.	None

Encryption Method

Setting	Description	Factory Default
Disabled	Disable encryption.	None
DES	Use DES encryption.	
AES	Use AES encryption.	

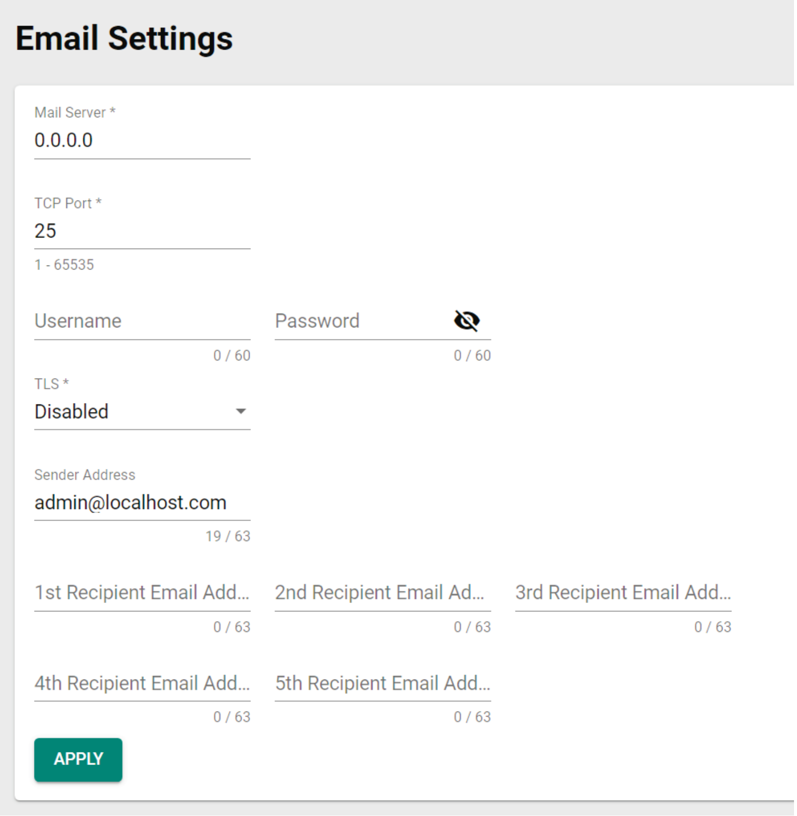
Encryption Key

Setting	Description	Factory Default
8 to 64 characters	If encryption is enabled, enter the data encryption key.	None

When finished, click **CREATE**.

Email Notification

Select **Email Notification** from the function menu and configure the following settings:



Email Settings

Mail Server * 0.0.0.0

TCP Port * 25
1 - 65535

Username 0 / 60

Password 0 / 60

TLS * Disabled

Sender Address admin@localhost.com 19 / 63

1st Recipient Email Add... 0 / 63

2nd Recipient Email Ad... 0 / 63

3rd Recipient Email Add... 0 / 63

4th Recipient Email Add... 0 / 63

5th Recipient Email Add... 0 / 63

Mail Server

Setting	Description	Factory Default
IP address or URL	Specify the IP address or URL of the email server.	0.0.0.0

TCP Port

Setting	Description	Factory Default
1 to 65535	Specify the TCP port number of the email server.	25

Username

Setting	Description	Factory Default
Max. of 60 characters	Enter the email account name.	None

Password

Setting	Description	Factory Default
Max. of 60 characters	Enter the email account password.	None

TLS

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable TLS (Transport Layer Security) authentication.	Disabled

Sender Address

Setting	Description	Factory Default
Max. 63 characters	Specify the sender's email address.	admin@localhost.com

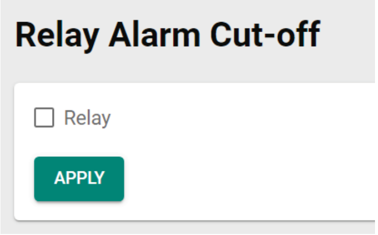
1st to 5th Email Addresses

Setting	Description	Factory Default
Max. of 63 characters	Specify the recipient's email address. A total of 5 recipients can be set up.	None

When finished, click **APPLY** to save your changes.

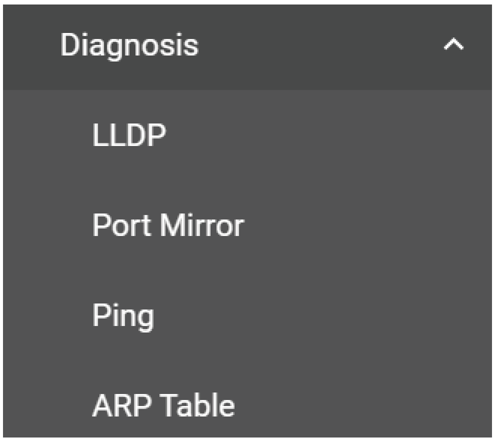
Relay Alarm Cut-off

When a relay warning is triggered by either system or port events, check the **Relay** box and click **APPLY** to cut off the relay alarm and switch from the triggered state back to the power-on state.

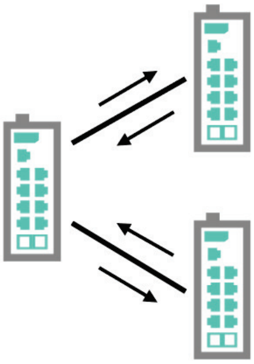


Diagnosis

This section covers system diagnostics functions, including **LLDP**, **Port Mirror**, **Ping**, and **ARP Table**.



LLDP Overview

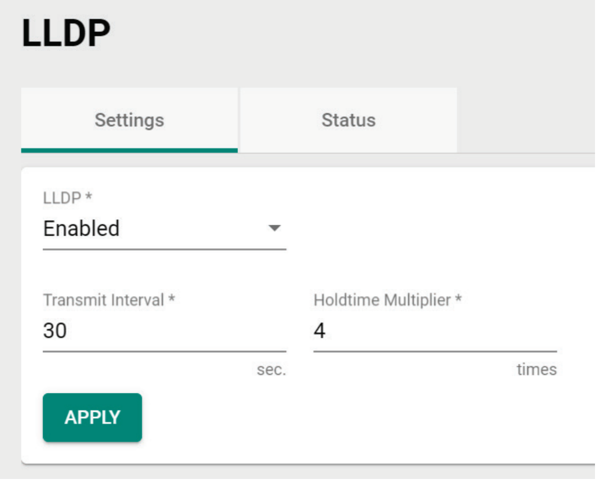


LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device, such as a Moxa managed switch, to periodically send its system and configuration information to its neighbors. Because of this, all LLDP devices are kept informed of each other's status and configurations. With SNMP, this information can be transferred to Moxa's MXview for auto-topology and network visualization.

From the switch's web interface, you can enable or disable LLDP, and set the LLDP transmit interval. In addition, you can view each switch's neighbor-list, which is reported by its network neighbors. Most importantly, enabling the LLDP function allows Moxa's MXview to automatically display the network's topology and system setup details, such as VLAN and Trunking for the entire network.

LLDP Settings and Status

Click **LLDP** from the menu and then select the **Settings** tab to configure the following settings:



LLDP

LLDP * Enabled

Transmit Interval * 30 sec.

Holdtime Multiplier * 4 times

LLDP

Setting	Description	Factory Default
Enabled	Enable LLDP.	Enabled
Disabled	Disable LLDP.	

Transmit Interval (sec.)

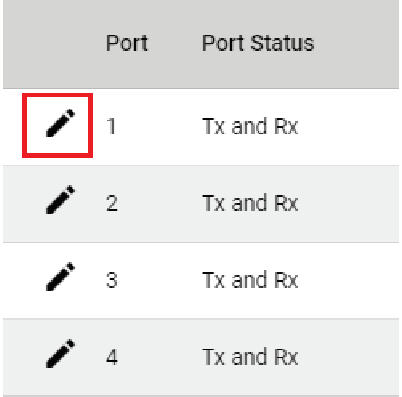
Setting	Description	Factory Default
5 to 32768	Set the transmit interval for LLDP messages.	30

Holdtime Multiplier (times)

Setting	Description	Factory Default
2 to 10	Set the holdtime multiplier value, representing the number of times that the receiving device holds an LLDP packet before discarding it.	4

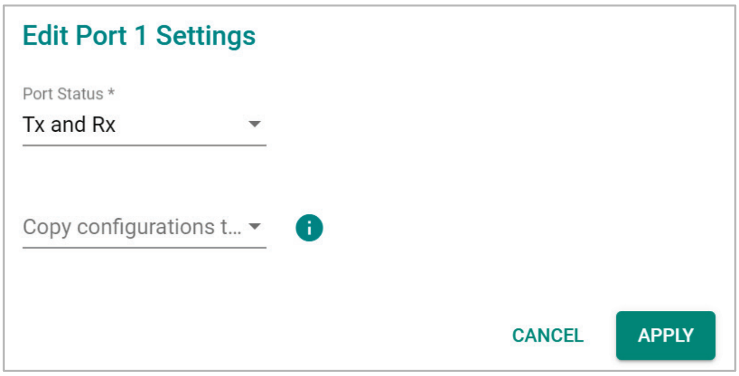
When finished, click **APPLY** to save your changes.

You can configure LLDP settings for each individual port. Click the edit icon of the port you want to configure.



	Port	Port Status
✎	1	Tx and Rx
✎	2	Tx and Rx
✎	3	Tx and Rx
✎	4	Tx and Rx

Configure the following settings:



Edit Port 1 Settings

Port Status *: Tx and Rx

Copy configurations t...

Port Status

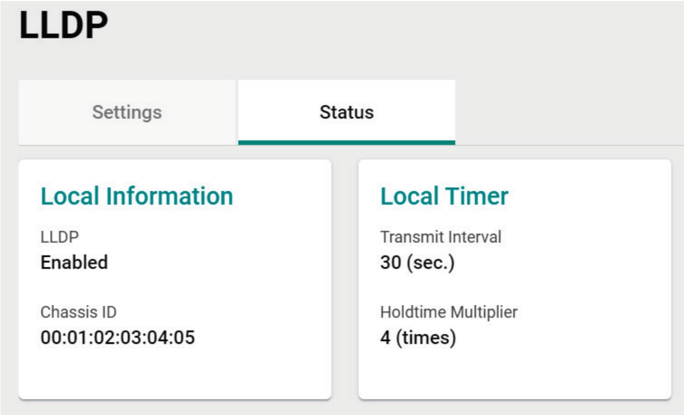
Setting	Description	Factory Default
Tx Only	Only transmit local information to remote.	Tx and Rx
Rx Only	Only receive remote information.	
Tx and Rx	Receive remote and send local information.	
Disabled	Disable information transmission between local and remote.	

Copy Configurations to Port

Setting	Description	Factory Default
Select the port from the list	Copy the same configurations to other port(s).	None

When finished, click **APPLY** to save your changes.

To view the LLDP status, click the **Status** tab on the LLDP page.



LLDP

Local Information

LLDP: Enabled

Chassis ID: 00:01:02:03:04:05

Local Timer

Transmit Interval: 30 (sec.)

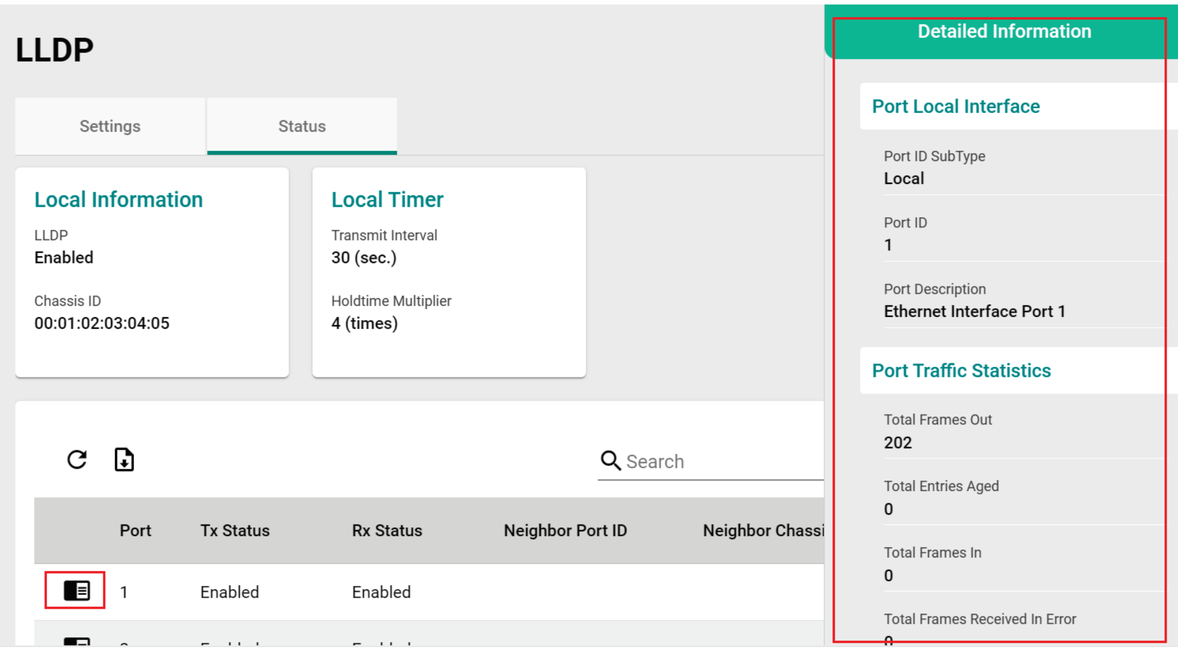
Holdtime Multiplier: 4 (times)

Refer to the following table for the detailed description of each item.

Local Information	
LLDP	Shows if LLDP has been enabled or disabled.
Chassis ID	Shows the chassis ID.

Local Timer	
Transmit Interval (sec.)	The interval between regular LLDP packet transmissions.
Holdtime Multiplier (times)	The number of times that the receiving device holds an LLDP packet before discarding it.

To view the LLDP status for a specific port, click the detailed information icon on the port. All information will be shown on the right side of the page.



Local Information

LLDP
Enabled

Chassis ID
00:01:02:03:04:05

Local Timer

Transmit Interval
30 (sec.)

Holdtime Multiplier
4 (times)

	Port	Tx Status	Rx Status	Neighbor Port ID	Neighbor Chassi
▤	1	Enabled	Enabled		

Port Local Interface

Port ID SubType
Local

Port ID
1

Port Description
Ethernet Interface Port 1

Port Traffic Statistics

Total Frames Out
202

Total Entries Aged
0

Total Frames In
0

Total Frames Received In Error
0

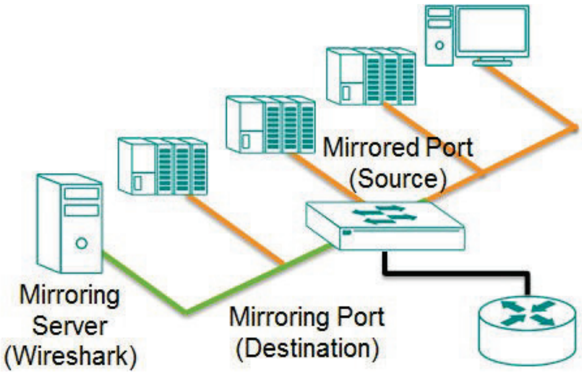
Port Mirror

Port Mirroring Overview

The Port Mirroring function can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the mirror port) to receive the same data being transmitted from, or both to and from, the port under observation. Using a mirror port allows the network administrator to sniff the observed port to keep tabs on network activity.

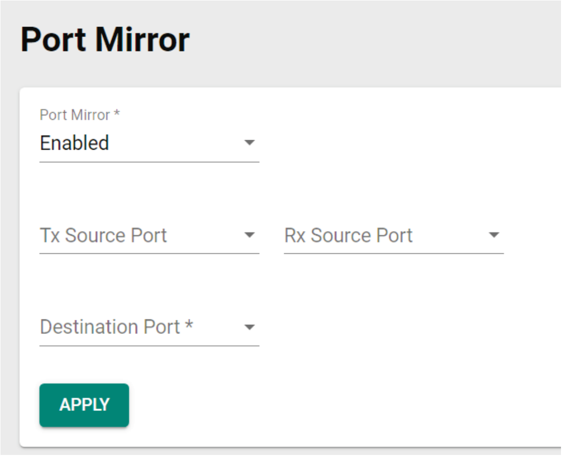
How Port Mirror Works

Port Mirroring can configure to copy one or more packets from various ports to a single port to observe and identify issues on any of these ports. For example, the following figure demonstrates how the packets transmitted through the four mirrored ports (marked in orange) are copied (mirrored) to a single mirroring port (marked in green). These packets will be sent to a monitoring computer which uses specialized to check for problematic packets. Port mirroring is a useful way troubleshoot or debug network data transmission issues.



Port Mirror Settings and Status

Click **Port Mirror** from the function menu.



Port Mirror

Port Mirror *: Enabled

Port Mirror

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable port mirroring for this session.	Disabled

Tx Source Port

Setting	Description	Factory Default
Select the port from the list	Select the port to mirror and monitor the traffic being sent from that port.	None

Rx Source Port

Setting	Description	Factory Default
Select the port from the list	Select the port to mirror and monitor the traffic coming in to that port.	None

Destination Port

Setting	Description	Factory Default
Select the port from the list	Select the destination port for the mirrored traffic.	None

When finished, click **APPLY** to save your changes.

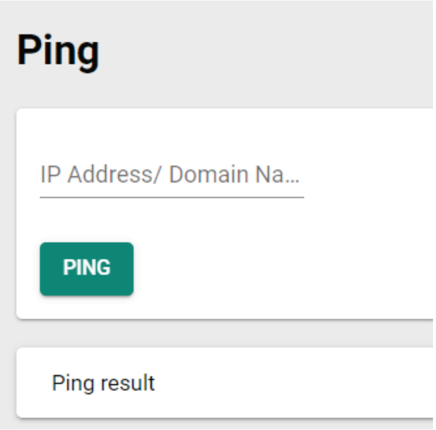
NOTE

The same port cannot be both an RSTP port and Port Mirror destination port.

Ping

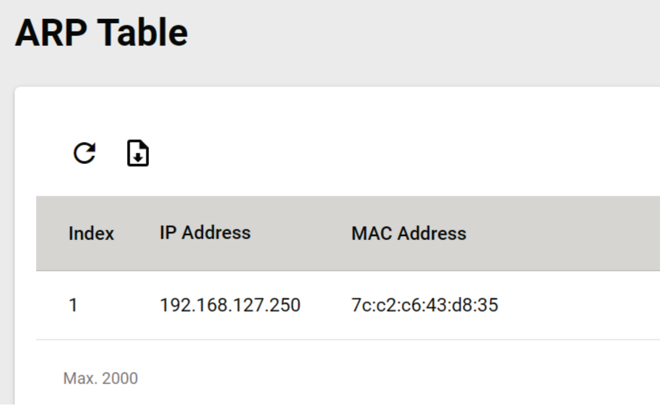
The **Ping** function uses the ping command to give users a simple but powerful tool for troubleshooting network problems. The function most unique feature of the function is that even though the ping command is entered from the user's PC, the actual ping command originates from the Moxa switch itself. This allows the user to essentially sit on top of the Moxa switch and send ping commands out through its ports.

To use the Ping function, click **Ping** from the menu, and enter the IP address or hostname you want to ping. Click **PING** to ping the target host.



ARP Table

To view the ARP Table, select **ARP Table** from the function menu.

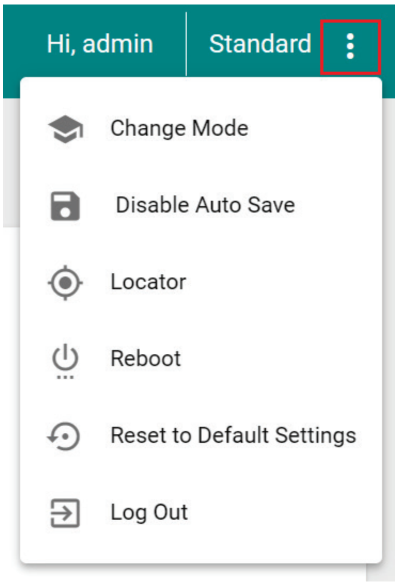

ARP Table

Index	IP Address	MAC Address
1	192.168.127.250	7c:c2:c6:43:d8:35

Max. 2000

Maintenance and Tool

This section explains how to maintain Moxa's switch and the tools that help users operate the switch. Click the icon on the upper right corner of the page.

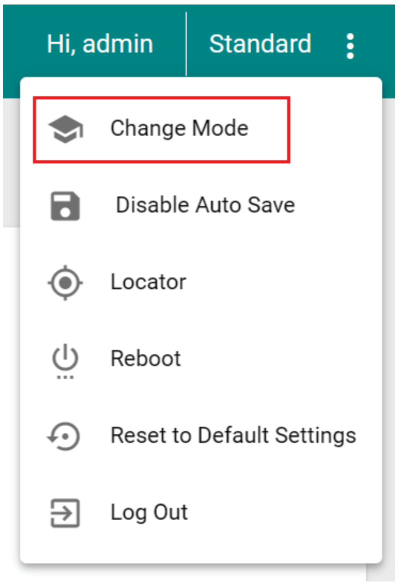


Standard/Advanced Mode

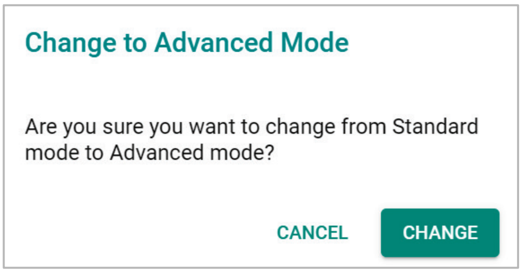
There are two configuration modes available for users: **Standard Mode** and **Advanced Mode**.

1. In **Standard Mode**, some of the features/parameters will be hidden to make it easier to perform configurations (this is the default setting).
2. In **Advanced Mode**, some advanced features/parameters will be available for users to adjust these settings.

To switch to Advanced Mode, click the change mode icon on the upper right corner of the page, and then select **Change Mode**.



Click **CHANGE** to change to **Advanced Mode**.



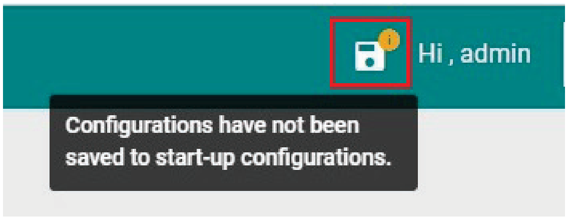
Change to Advanced Mode

Are you sure you want to change from Standard mode to Advanced mode?

Advanced Mode offers more detailed system configurations for specific functions. Use the same process if you want to return to Standard Mode.

Disable Auto Save

Auto Save allows users to save the settings to the start-up configurations; all parameters will be effective when applied immediately, even when the switch has restarted. When users select **Disable Auto Save**, all parameters will be temporarily stored in the running config (memory), and a disk icon will appear on the upper right corner of the page. Users need to save the running-configuration to the startup-configuration when changing any parameters or function after clicking **APPLY**.

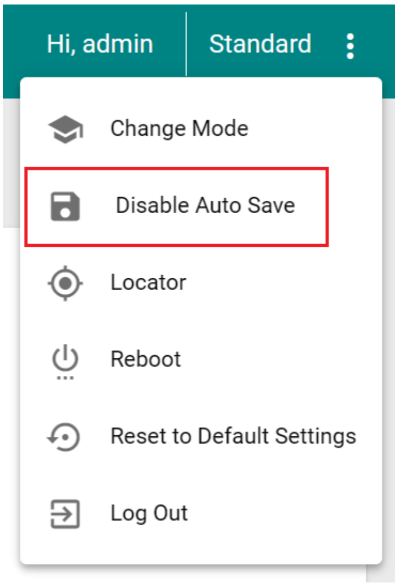


Configurations have not been saved to start-up configurations.

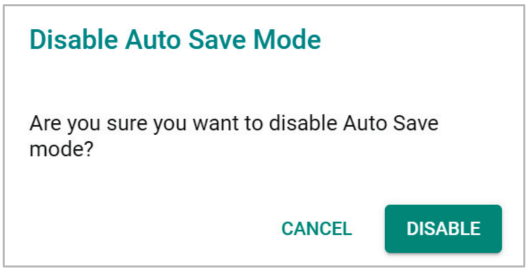
It is highly recommended that you always manually save all configurations by clicking Save Disk icon when **Disable Auto Save** is applied, or all information will have disappeared after the switch has restarted.

When **Disable Auto Save** is applied, only the configurations that are running will be saved; users can unplug the power or perform a warm start to recover the network before manually saving the configurations. When Auto Save is enabled, the start-up configurations will be saved in the switch.

To disable the **Auto Save** function, click **Disable Auto Save** in the menu.



Click **DISABLE**.

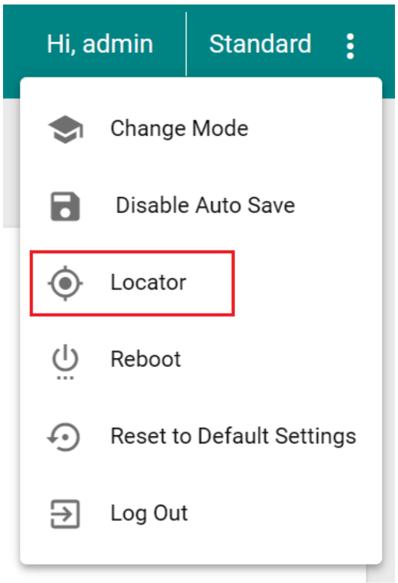


Disable Auto Save Mode

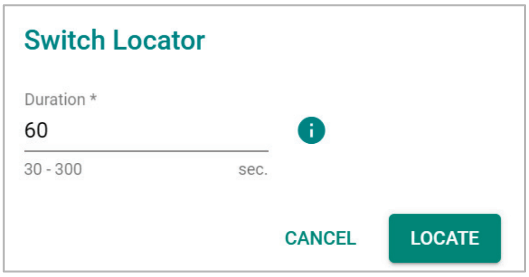
Are you sure you want to disable Auto Save mode?

Locator

Users can trigger the device locator by clicking this icon. This will cause the LED indicators on the switch to flash for one minute. This helps users easily find the location of the switch in a field site.



Configure the following setting:



Switch Locator

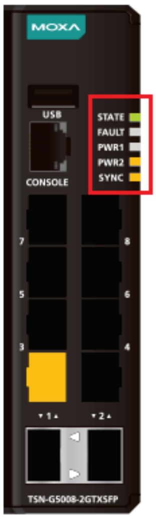
Duration * 60

30 - 300 sec.

Duration (sec.)

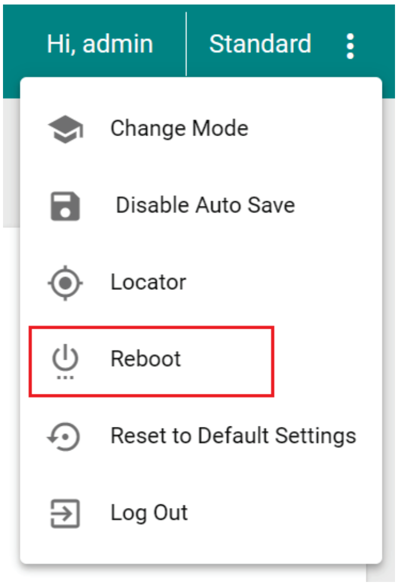
Setting	Description	Factory Default
30 to 300	Specify the duration the indicators will keep flashing.	60

Click **LOCATE** to activate the switch locator. The **STATE**, **FAULT**, and **SYNC** LED indicators will start flashing.

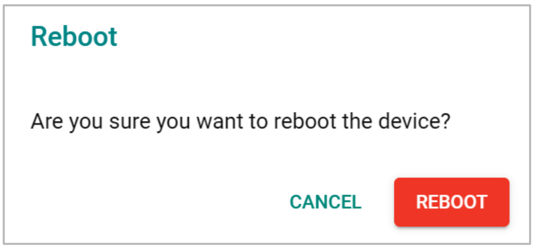


Reboot

To reboot the device, select **Reboot**.



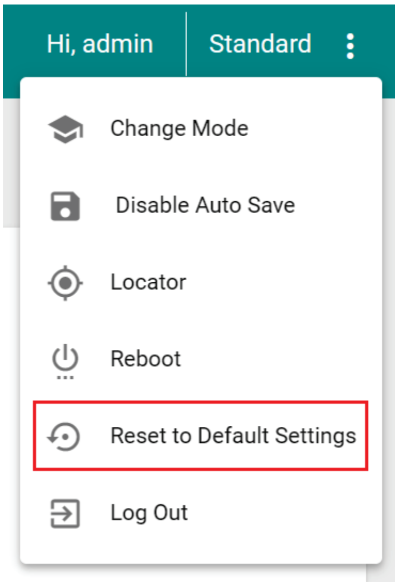
Click **REBOOT** to reboot the device.


Reboot

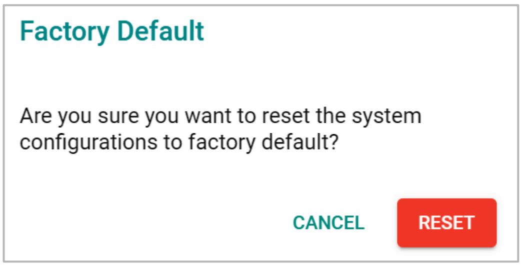
Are you sure you want to reboot the device?

Reset to Default Settings

To reset the switch to the default factory values, select **Reset to Default Settings**.



To return the switch to factory default settings, click **RESET**.

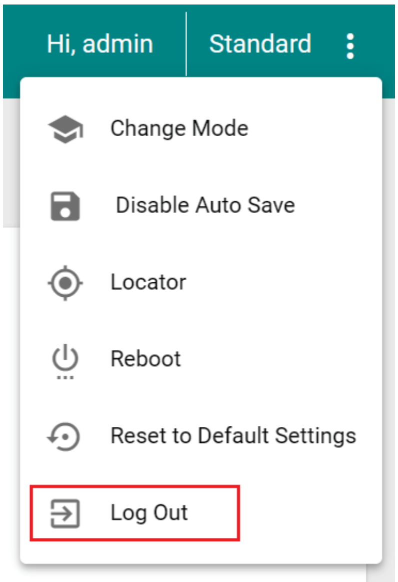


Factory Default

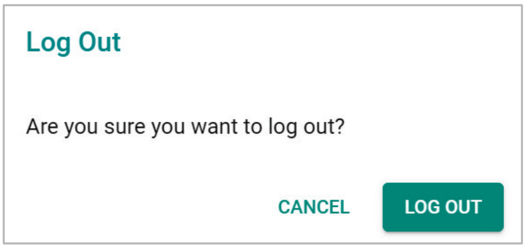
Are you sure you want to reset the system configurations to factory default?

Log Out of the Switch

To log out of the switch, select **Log Out**.



Click **LOG OUT** to log out of the switch.



Log Out

Are you sure you want to log out?

A. Account Privileges List

This appendix describes the read/write access privileges for different accounts on Moxa's Managed Ethernet Series switches.

Account Privileges List

This appendix lists the privileges for different account roles.

Please note, **R** stands for **Read** and **W** stands for **Write**.

Function	Account Privilege		
System	**Admin**	**Supervisor**	**User**
Information Setting	R/W	R/W	R
Firmware Upgrade	Execute	No Access	No Access
Configuration Backup and Restore	Execute	No Access	No Access
Event log backup	Execute	Execute	Execute
User Account	R/W	No Access	No Access
Password Policy	R/W	No Access	No Access
IP Configuration	R/W	R/W	R
DHCP Server	R/W	R/W	R
Time Zone	R/W	R/W	R
System Time	R/W	R/W	R
Time Synchronization	R/W	R/W	R
Port			
Port Setting	R/W	R/W	R
Link Aggregation	R/W	R/W	R
VLAN			
IEEE 802.1Q	R/W	R/W	R
Priority Management	R/W	R/W	R
MAC			
Static Unicast	R/W	R/W	R
MAC Address Table	R/W	R/W	R
Multicast			
Static Multicast	R/W	R/W	R
Time-Aware Shaper	R/W	R/W	R
Layer 2 Redundancy			
Spanning Tree	R/W	R/W	R
Turbo Chain	R/W	R/W	R
Network Management			
SNMP	R/W	No Access	No Access
SNMP Trap/Inform	R/W	No Access	No Access
Security			
Management Interface	R/W	R/W	R
Login Policy	R/W	R	R
Trusted Access	R/W	R	R
SSH & SSL	Execute	Execute	No Access
Traffic Storm Control	R/W	R/W	R
Authentication			
RADIUS	R/W	No Access	No Access
TACACS+	R/W	No Access	No Access
Login Authentication	R/W	No Access	No Access

Function	Account Privilege		
Diagnostics	**Admin**	**Supervisor**	**User**
Event Notification	R/W	R/W	R
Relay Alarm Cut-off	R/W	R/W	R
Email Notification	R/W	R	R
Syslog	R/W	R	R
Event Log	R/W	R/W	R
LLDP	R/W	R/W	R
Ping	Execute	Execute	Execute
ARP Table	R/W	R/W	R
Utilization	R	R	R
Statistics	R	R	R
Maintenance and Tool			
Standard/Advanced Mode	Execute	Execute	Execute
Disable Auto Save	R/W	R/W	R
Locator	R/W	R/W	Execute
Reboot	Execute	Execute	No Access
Reset to default	R/W	No Access	No Access

B. Event Log Description

This appendix describes all of the information for the event logs. When an event occurs, it will be recorded in the event log files. Users can check the event log name and its event log description.

Event Log Description

Event Log Name	Event Log Description
Login success	[Account:{{user_name}}] successfully logged in via {{interface}}.
Login fail	[Account:{{user_name}}] log in failed via {{interface}}.
Login lockout	[Account:{{user_name}}] locked due to {{failed_times}} failed login attempts.
Account setting changed	Account settings of [Account:{{user_name}}] has been updated. Account settings of [Account:{{user_name}}] has been deleted. Account settings of [Account:{{user_name}}] has been created.
SSL certification changed	SSL certificate has been changed. SSL certificate has been regenerated.
Password changed	The password of [Account:{{user_name}}] has been changed.
Cold start	The system has performed a cold start.
Warm start	The system has performed a warm start.
Configuration changed	Configurations {{modules}} have been changed by [Account:{{user_name}}].
Configuration imported	Configuration import {{'successful'/'failed'}} by [Account:{{user_name}}].
Log capacity threshold	The threshold of event log entries {{numbers}} has been reached.
Event log export	Event Log export {{successful /failed}} by {{username}} via {{method}}.
PWR on	Power {{index}} has turned on.
PWR off	Power {{index}} has turned off.
DI on	Digital Input {{index}} has turned on.
DI off	Digital Input {{index}} has turned off.
Port link up	Port {{number}} link up.
Port link down	Port {{number}} link down.
Topology changed (RSTP)	Topology has been changed by RSTP.
Topology changed (Turbo Chain)	Topology has been changed by Turbo Chain.
Log Turbo Chain port restart	Port-Channel {{channel id}} has restarted by Turbo Chain. Port {{number}} has restarted by Turbo Chain.
RSTP topo. changed	Topology has been changed by RSTP.
RSTP root changed	New root has been elected in topology.
RSTP migration	Port {{number}} changed to RSTP Port {{number}} changed to STP.
RSTP invalid BPDU	STP port {{number}} received an invalid BPDU (type:{{type}}, value:{{value}}).
RSTP new port role	STP port {{number}} role changed from {{role}} to {{role}}.
Redundant port health check fail	Redundant port {{number}} health check fail.
LLDP table changed	LLDP remote table changed.
SSH key generate	SSH key has been regenerated.
Configuration export	Configuration export {{successful /failed}} by [{{user_name}}] via {{interface}}.
Firmware upgrade success	Firmware successfully upgraded.
Firmware upgrade failed	Firmware failed to upgrade.
Relay cut off	{relay_name} relay alarm has been cut off.
PTP sync status changed	The PTP sync status has changed from {LOCKED/UNLOCKED} to {UNLOCKED/LOCKED}.
PTP select master clock event	Select local clock as GM

Event Log Name	Event Log Description
PTP select master clock event	Select GM [clockidentity]
802.1as noncapable event	port {{number}}: Path delay > neighborPropDelayThresh, set asCapable to 0
	port {{number}}: Loss 4 pdelay_rsp and pdelay_rsp_fup continuously, set asCapable to 0
	port {{number}}: Receive multiple sequential pdelay_rsp, set asCapable to 0
	port {{number}}: Invalid peer port id, set asCapable to 0
	port {{number}}: asCapable 1->0
802.1as capable event	port {{number}}: asCapable 0->1
PTP port trans event	port {{number}}: port state from {{state}} to {{state}}
PTP lost time event	port {{number}}: pdelay_rsp and pdelay_rsp_fup with sid %u both lost. Lost {{number}} times continuously
PTP send fail event	Port {{number}}: Send pdelay req fail
	Port {{number}}: Send Sync fail
	Port {{number}}: Send pdelay rsp fail
PTP receive timeout event	Port {{number}}: Rx Sync timeout
	Port {{number}}: Rx Announce timeout
	Timed out while polling for tx timestamp

C. SNMP MIB File

This appendix contains the SNMP MIB file for the managed switch.

Standard MIB Installation Order

If you need to import the MIB one-by-one, please install the MIBs in the following order.

1. RFC1213-MIB.mib
2. SNMP-FRAMEWORK-MIB.mib
3. SNMPv2-SMI.mib
4. SNMPv2-TC.mib
5. SNMPv2-CONF.mib
6. SNMPv2-MIB.mib
7. IANAifType-MIB.mib
8. IF-MIB.mib
9. EtherLike-MIB.mib
10. BRIDGE-MIB.mib
11. RMON2-MIB.mib
12. INET-ADDRESS-MIB.mib
13. IEEE8021-TC-MIB.mib
14. IEEE8021-SPANNING-TREE-MIB.mib
15. IANA-ADDRESS-FAMILY-NUMBERS-MIB.mib
16. LLDP-MIB.mib
17. PTPBASE-MIB.mib
18. IEEE8021-AS-MIB.mib
19. IEEE8021-ST-MIB.mib

MIB Tree

Refer to the following content for the MIB Tree structure.

```
iso(1)
 |-std(0)-iso8802(8802)-ieee802dot1(1)-ieee802dot1mibs(1)
     |-ieee8021SpanningTreeMib(3): IEEE8021-SPANNING-TREE-MIB.mib
 |-org(3)
  |-dod(6)-internet(1)
    |-mgmt(2)-mib-2(1): SNMPv2-MIB.mib
              |-system(1): RFC1213-MIB.mib
                  |-interface(2): RFC1213-MIB.mib
              |-at(3): RFC1213-MIB.mib
              |-snmp(11): RFC1213-MIB.mib
              |-dot1dBridge(17): BRIDGE-MIB.mib, Q-BRIDGE-MIB.mib
              |-ifMIB(31): IF-MIB.mib
              |-etherMIB(35): EtherLike-MIB.mib
    |-private(4)-moxa(8691)
              |-product(600): mxGeneralInfo.mib, mxProductInfo.mib,
              |-general(602): mxGeneral.mib, mxDeviceIo.mib, mxDhcpSvr.mib, mxEmailC.mib,
                           mxEventLog.mib,
                          :mxGene.mib, mxLocator.mib, mxManagementIp.mib,
                           mxPorte.mib,
                          : mxRelayC.mib, mxSnmp.mib, mxSwe.mib, mxSysLoginPolicySvr.mib,
                          : mxSyslogSvr.mib, mxSysPasswordPolicySvr.mib, mxSystemInfo.mib,
                          : mxSysTrustAccessSvr.mib, mxSysUtilSvr.mib, mxTimeSetting.mib,
                          : mxTimeZone.mib, mxTrapC.mib, mxUiServiceMgmt.mib
               |-switching(603): mxSwitching.mib
                   |- portInterfacce : mxLa.mib
                   |- basicLayer2: mxQos, mxStreamAdapter.mib
                   |- layer2Redundancy: mxRstp.mib, mxTc.mib
                   |- layer2Security: mxStcl.mib
                   |- layer2Diagnosic: mxLldp.mib, mxPortMirror.mib
                   |- layer3Diagnosic
                   |- layer2Multicast
                   |- layer3Multicast
    |-snmpV2(6)-snmpModules(3)
                   |-snmpFrameworkMIB(10): SNMP-FRAMEWORK.mib
 |-ieee(111)-standards-association-numbers-series-standards(2)-lan-man-stds(802)-ieee802dot1(1)-
      ieee802dot1mibs(1)-ieee8021SpanningTreeMib(3): IEEE8021-SPANNING-TREE-MIB.mib
```