MX-NOS Rail Version V2

Version 1.0

January 2026

Table of Contents

Chapter 1

Overview

Introduction

Welcome to the MX-NOS Rail Version user manual. This comprehensive guide is designed to help you understand and navigate the UI features, technical concepts, and tasks you may encounter while using your device. Our goal is to simplify your experience and make the setup process easier.

About MX-NOS and MX-NOS Rail Version

MX-NOS

Moxa's next-generation Ethernet switches are powered by MX-NOS, a tailored firmware platform that seamlessly integrates with your Moxa devices. This unlocks their full potential, transforming your switches into powerful tools with consistent functionality and a user-friendly interface.

How does Moxa achieve this? By providing a platform-based management OS, Moxa offers several key advantages, including:

- **Streamlined software management with regular updates:** Moxa keeps your switches up-to-date with the latest technologies throughout their lifetime. Continuous bug fixes and vulnerability synchronization ensure high software quality and improved network security.
- **Robust security by design**: Moxa adheres to IEC 62443-4-1 for software development lifecycles. As a result, MX-NOS provides a solid foundation for the switches running on it to build security features based on IEC 62443-4-2.
- **Consistent user experience:** MX-NOS features an intuitive UI that provides a consistent user experience across different browsing devices, minimizing training time and maximizing efficiency.

MX-NOS is more than just a firmware platform; it's a significant leap towards a superior user experience.

MX-NOS Rail Version

Built on the robust foundation of MX-NOS, MX-NOS Rail Version caters specifically to the unique needs and demands of onboard railway networks. It addresses the growing demand for reliable communications and faster response times.

MX-NOS Rail Version offers a comprehensive suite of features that prioritize unwavering reliability to achieve smooth operation of critical railway systems such as TCMS. Furthermore, MX-NOS Rail Version simplifies network design, installation, and maintenance with features designed for onboard networks. This significantly reduces deployment time and ongoing management costs, which translates to a streamlined workflow for railway personnel, allowing them to focus on core operational tasks.

In essence, MX-NOS Rail Version represents a game-changer for onboard railway communications. Its innovative approach streamlines network management and fosters a more agile and responsive railway ecosystem.

What's in This Document

This document includes the following sections:

- **Overview**: This section introduces this document and how to use it.
- **Quick Start**: This section tells you how to connect to your device so you can start using and configuring it.
- **UI Reference**: This section goes through the web user interface (UI) of your device to help you quickly understand what settings are available. This section also shows you the valid ranges and defaults for settings, and any limitations there may be when configuring your device.
- **Appendix**: This section provides additional reference information for your device.

Supported Series and Firmware Versions

Moxa Switch Series	Firmware Version
TN-4500B Series	v2.0

Note

We are continually improving and developing our software. Check regularly to see if there is an updated version of the software that provides you with additional benefits. You can find information and software downloads on the Moxa product pages at https://www.moxa.com/en/support/product-support/software-and-documentation.

Product Series Feature Comparison Table

Refer to the table below for a full overview of the supported features for each product series model covered by this manual.

- **YES:** Supported
- **PARTIAL:** Partially supported
- **–**: Unsupported

For more details on partially supported features, refer to their respective sections in this manual.

Options Menu

Settings	TN-4500B Series
Locator	YES
Reboot	YES
Reset to Default Settings	YES
Save Custom Default	YES
Auto-save to startup	YES
Advanced Mode	YES
Log Out	YES

System

Settings	TN-4500B Series
System Management	**YES**

Settings	TN-4500B Series
Information Settings	YES
Firmware Upgrade	YES
Config Backup and Restore	YES
Account Management	**YES**
User Accounts	YES
Online Accounts	YES
Password Policy	YES
Management Interface	**YES**
User Interface	YES
Hardware Interfaces	YES
SNMP	YES
Time	**YES**
System Time	YES
NTP Server	YES

Provisioning

Settings	TN-4500B Series
Auto Configuration	**YES**

Port

Settings	TN-4500B Series
Port Interface	**YES**
Port Settings	YES
Linkup Delay	YES
Link Aggregation	**YES**
PoE **(for PoE models)**	**YES**

Layer 2 Switching

Settings	TN-4500B Series
VLAN	**YES**
GARP	**YES**
MAC	**YES**
Static Unicast	YES
MAC Address Table	YES
QoS	**YES**
Classification	YES
Ingress Rate Limit	YES
Scheduler	YES
Egress Shaper	YES
Multicast	**YES**
IGMP Snooping	YES

Settings	TN-4500B Series
GMRP	YES
Static Multicast	YES

IP Configuration

Settings	TN-4500B Series
IP Configuration	**YES**

Redundancy

Settings	TN-4500B Series
Layer 2 Redundancy	**YES**
Spanning Tree	YES
Turbo Ring v2	YES
MRP	YES

Network Service

Settings	TN-4500B Series
DHCP Server	**YES**
DHCP Relay Agent	**YES**
DNS Server	**YES**
mDNS Responder	**YES**

Security

Settings	TN-4500B Series
Device Security	**YES**
Login Policy	YES
Trusted Access	YES
SSH & SSL	YES
Network Security	**YES**
IEEE 802.1X	YES
MAC Authentication Bypass	YES
MACsec	YES
Port Security	YES
Traffic Storm Control	YES
Access Control List	YES
Network Loop Protection	YES
Binding Database	YES
DHCP Snooping	YES
IP Source Guard	YES
Dynamic ARP Inspection	YES
Authentication	**YES**
Login Authentication	YES
RADIUS	YES
TACACS+	YES

Diagnostics

Settings	TN-4500B Series
System Status	**YES**
Resource Utilization	YES
Network Status	**YES**
Network Statistics	YES
LLDP	YES
ARP Table	YES
Tools	**YES**
Port Mirroring	YES
Ping	YES
Event Logs and Notifications	**YES**
Event Logs	YES
Event Notifications	YES
Syslog	YES
SNMP Trap/Inform	YES
Email Settings	YES

Icons Used in the Web Interface

This table shows various icons used in the web interface and their corresponding meanings.

You can also hover your mouse over an icon to show an explanatory mouseover tip.

Symbols	Meanings
 **To be updated**	Add
	Read detailed information
	Column selection
	Refresh
	Enable/Disable Auto Save When Auto Save is disabled, users need to click this icon to save changes to the startup configuration. Refer to Configuration Types for more information.
	Export
	Edit
	Auto Refresh enabled
	Auto Refresh disabled
	Delete
 **To be updated**	

Symbols	Meanings
	Clear all
	Panel view
	Expand
	Collapse
	Hint information
To be updated	Menu icon
	Change mode
	Locator
	Reboot
	Reset to default
	Log out
	Data comparison
	Increase
	Decrease
	Equal

Symbols	Meanings
	Menu
	Search
	Copy
	Warning
	Reorder
	Reorder priority
	Set up related event notifications
	Show text
	Hide text
	Remove
 **To be updated**	
	Select a file
	Change language
	Sync to the latest state or reauthenticate
	View list

Symbols	Meanings
	Remove the account
	Relay alarm cut-off
	How to set up

Chapter 2

Quick Start

Using a Web Browser to Configure the Industrial Ethernet Switch

The device's web interface provides a convenient way to modify the switch’s configuration and access the built-in monitoring and network administration functions.

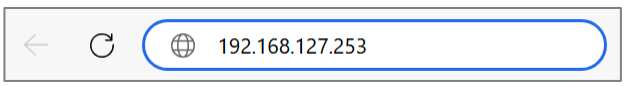
Note

When using the device's web interface, we recommend using the following browsers and versions. Please note that Internet Explorer (IE) is not supported.

- Chrome: 2 most recent versions
- Firefox: Latest version and the Extended Support Release (ESR)
- Edge: 2 most recent major versions
- Safari: 2 most recent major versions
- iOS: 2 most recent major versions
- Android: 2 most recent major versions

Perform the following steps to access the device's web interface:

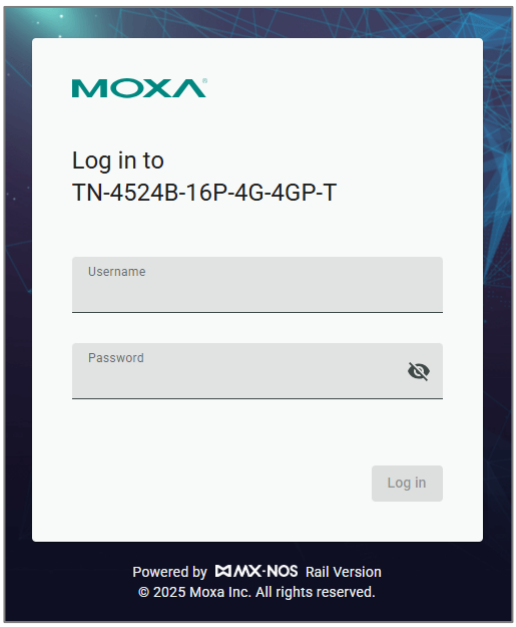
1. Make sure your PC host is connected to your device's LAN port, and is on the same subnet as your device.
2. Open a web browser and type the device’s LAN IP address (**192.168.127.253** by default) into the address bar and press Enter.



3. The web login page will open. Enter the username (**admin** or **user**) and password (the same as the Console password) and click **LOG IN** to continue.

Note

The default username is admin and the default password is moxa. We strongly recommend changing the password as soon as possible to ensure the security of your device.



You may need to wait a few moments for the web interface to appear.

4. After successfully connecting to the switch, the **Device Summary** screen will automatically appear. Use the menu tree on the left side of the window to open the function pages to access each of the switch's functions.

Chapter 3

UI Reference

UI Reference Overview

This section provides you with a quick reference to the different settings and options of your device.

To help you understand how to use the user interface, the following sections are included:

- The MX-NOS Rail Version User Interface
- Options Menu

The rest of this section follows the order of the menu areas in the user interface:

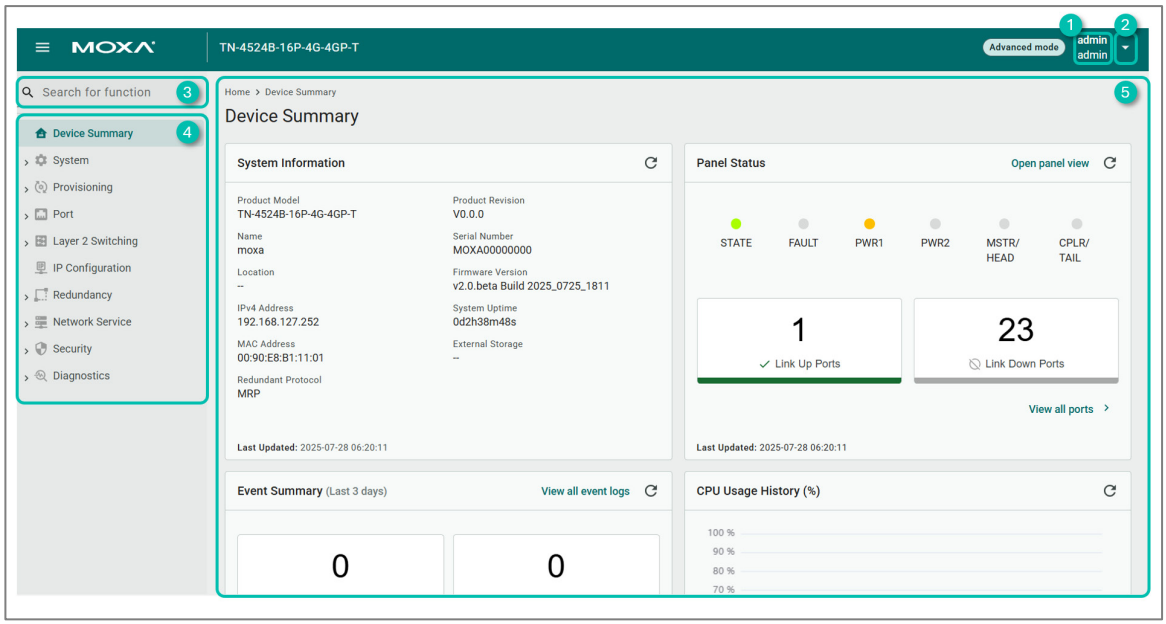
- Device Summary
- System
- Provisioning
- Port
- Layer 2 Switching
- Network Interface
- IP Configuration
- Redundancy
- Network Service
- Security
- Diagnostics

The MX-NOS Rail Version User Interface

Moxa's managed switches offer a user-friendly web interface for easy configuration, reducing system maintenance and configuration effort.

This section describes how the web interface is laid out to make it easier for you to find and access the different function pages.

Here is an overview of the MX-NOS Rail Version user interface:

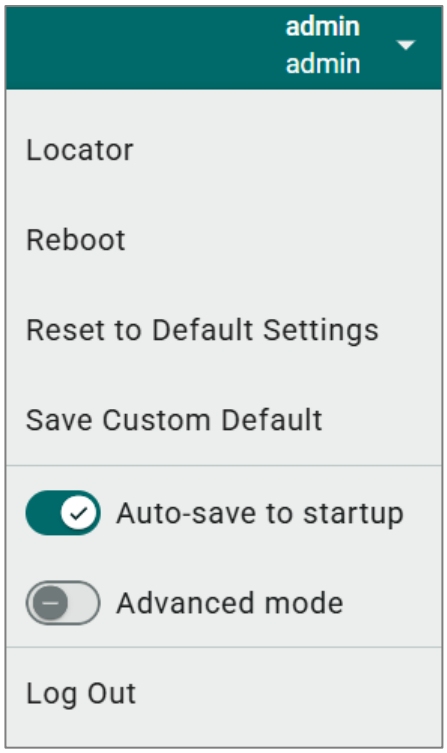


1. **Login Name:** Indicates the current user's account privilege at the top and their account name at the bottom.
2. **Options Menu:** Allows the user to perform various operations, including the locator function, resetting the device to its default configuration, and modifying the configuration mode, etc.
    - **Configuration Mode:** Shows which configuration mode is being used:
        - **Standard Mode:** Some features and parameters will be hidden to make configuration simpler (enabled by default).
        - **Advanced Mode:** More features and parameters will be shown to allow for more detailed configuration.
3. **Search Bar:** Type in a function name to filter to the function menu.

4. **Function Menu:** All functions of the switch are shown here. Click the function you want to view or configure.
5. **Device Summary:** Shows device information and settings for the selected function.

Options Menu

Clicking the **Options (▾)** icon in the upper-right corner of the page will open the options menu.



Options Menu - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to System > Account Management > User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Locator	R/W	R/W	R/W
Reboot	R/W	R/W	-
Reset to Default Settings	R/W	-	-
Save Custom Default	R/W	-	-

Settings	Admin	Supervisor	User
Auto-save to startup	R/W	R/W	-
Advanced mode	R/W	R/W	R/W
Log Out	R/W	R/W	R/W

Change Mode

There are two configuration modes available for users: **Standard Mode** and **Advanced Mode**.

- In **Standard Mode**, some of the features/parameters will be hidden to make it easier to perform configurations. This is the default setting.
- In **Advanced Mode**, advanced features/parameters will be available for users to adjust these settings.

To switch between modes, click the **Options (⋮)** icon in the upper-right corner of the page, and switch on/off the **Advanced mode** button.

Auto-save to Startup

Auto-save to Startup allows users to save all changes to the device's running configuration to the startup configuration immediately and automatically, so all changes will persist even after the device has restarted. Refer to Configuration Types for more information about the different configurations your device uses.

> **Note**
> Auto-save to Startup is enabled by default.

To enable or disable auto-saving to the startup configuration, click the **Options (▾)** icon in the upper-right corner of the page, and toggle **Auto-save to startup**.

When auto-saving is disabled, you can save configuration changes to the startup configuration by clicking the **Save (💾)** icon.

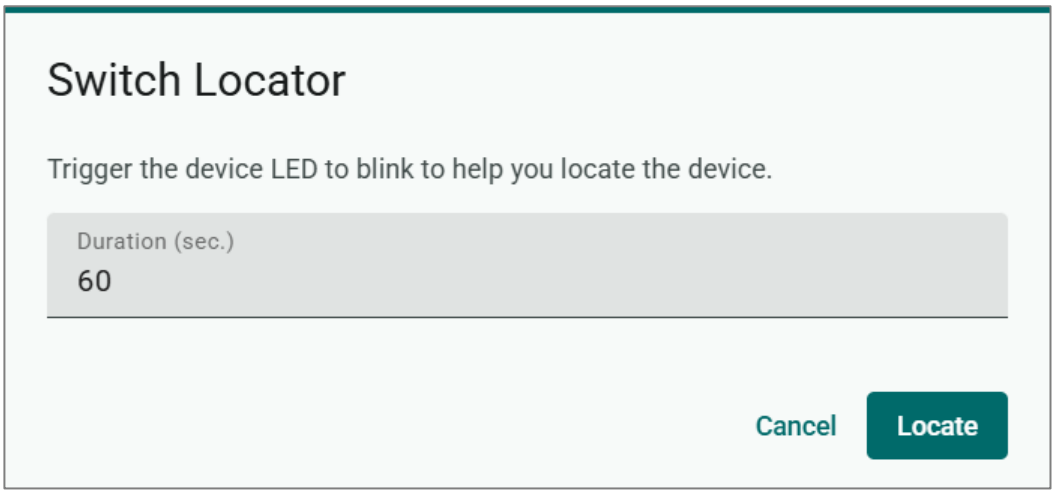
Note

When auto-saving is disabled, if changes have not been saved and the device is restarted, all changes will be lost and the device will revert to its startup configuration.

Locator

The Locator feature will cause the LED indicators on the device to flash, making it easier to locate and identify the specific device when installed at a field site.

To trigger the device locator, click the **Options (⋮)** icon in the upper-right corner of the page, and select **Locator**. Select how long in seconds the LEDs should flash for, then click **Locate**.



Reboot

To manually reboot the device, click the **Options (⋮)** icon in the upper-right corner of the page, and select **Reboot**.

Reset to Default Settings

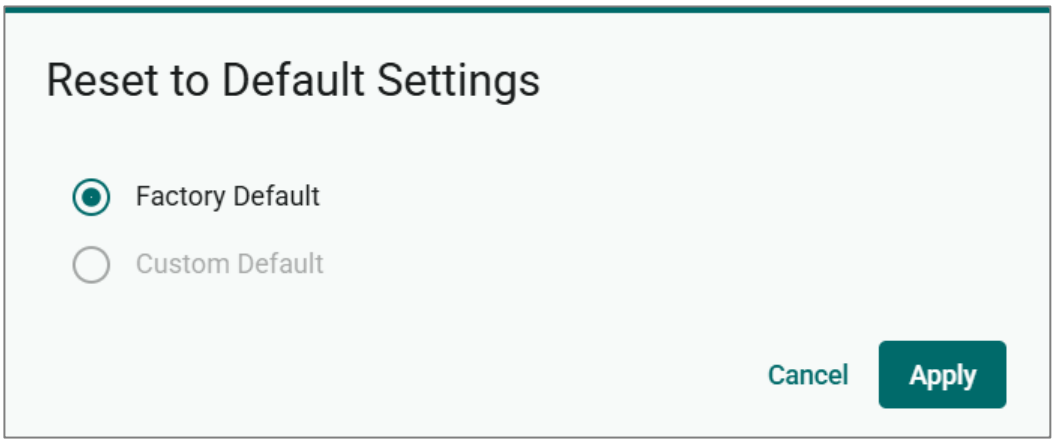
To reset the device to its default settings, click the **Options (▾)** icon in the upper-right corner of the page, and select **Reset to Default Settings**.

Select whether to reset to **Factory Default** settings, or the saved **Custom Default** settings, then click **Apply**.

Refer to Save Custom Default for more information about custom default settings.

> **Note**
> Custom Default can only be selected if custom default settings have been saved on the device.

> **Warning**
> When resetting your device to the factory default settings, all your current configuration settings will be permanently deleted.



Save Custom Default

You can save a custom default configuration for your device. This allows you to reset the device to a trusted configuration without uploading a configuration file to restore from.

After saving a custom default, the custom default configuration will become part of the startup configuration and can be backed up and restored with the startup configuration.

Refer to Reset to Default Settings for more information.

Note

- Ensure that the current startup configuration works as expected and that the user account settings are correct before saving the configuration as a custom default.
- The configuration name can be modified on the Config Backup and Restore page. We recommend using a unique name when backing up a configuration to differentiate it for easy identification and management.
- Each device can only have one set of custom default settings.
- Custom default settings can only save and restore configuration settings. They do not include other uploaded files, such as SSL certificate files, SSH keys, etc.
- Refer to Configuration Types for more information about the different configurations your device uses.

To save the current startup configuration as a custom default, click the **Options (⋮)** icon in the upper-right corner of the page, and select **Save Custom Default**.

Log Out

To log out of the device, click the **Options (⋮)** icon in the upper-right corner of the page, and select **Log Out**.

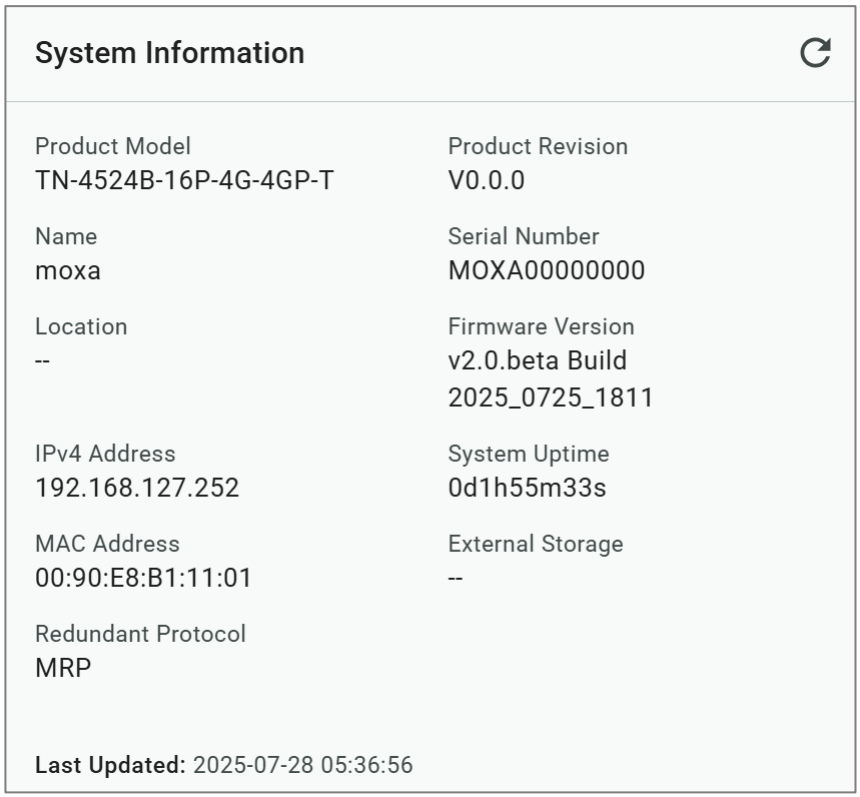
Device Summary

Menu Path: Device Summary

This page lets you see the current status of your device through a variety of display panels.

System Information

This display shows basic information about your device and its current status.

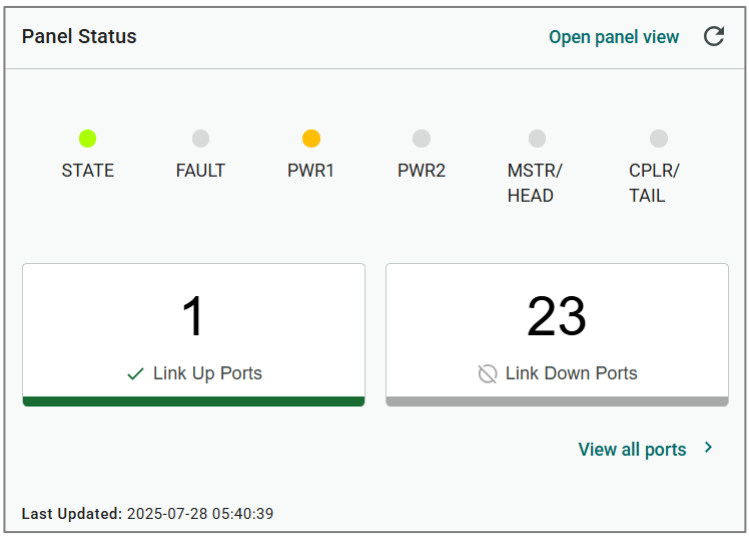


UI Setting	Description
Product Model	Shows the product model of the device.
Name	Shows the name of the device. Refer to System > System Management > Information Settings for more information.

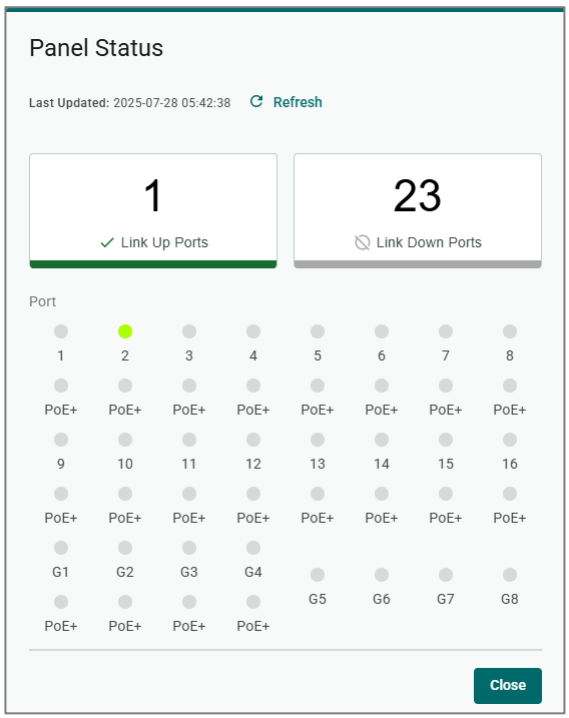
UI Setting	Description
Location	Shows the location of the device. Refer to System > System Management > Information Settings for more information.
IPv4 Address	Shows the IPv4 address of the device.
MAC Address	Shows the MAC address of your device.
Redundant Protocol	Shows the current redundancy protocol for this switch.
Product Revision	Shows the product revision of the device.
Serial Number	Shows the serial number of your device.
Firmware Version	Shows the firmware version of your device.
System Uptime	Shows the amount of time your device has been continuously running for.
External Storage	Shows the external storage device currently connected to your device, if applicable.

Panel Status

This display reflects the current status of the physical LEDs on your device, and shows how many ports currently have a link up or link down status. Grey is used to indicate an LED is off. For more information about status LEDs and their behavior, please refer to the QIG.



Click **View all ports** to view more detailed information, or click **Close** to return to the compact view.



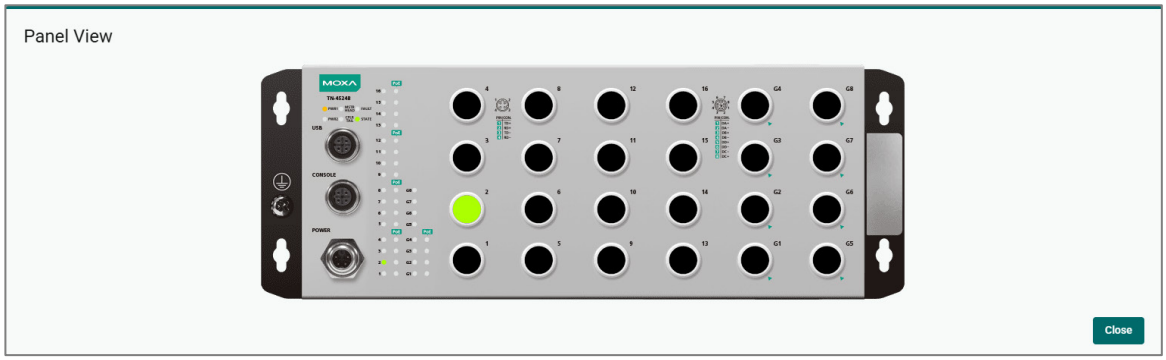
Panel View

By clicking **Open panel view** in **Panel Status**, you can see a visual representation of your device's ports.

Green ports have an active link. You can move your cursor over a port to show a mouseover with more information about that port.

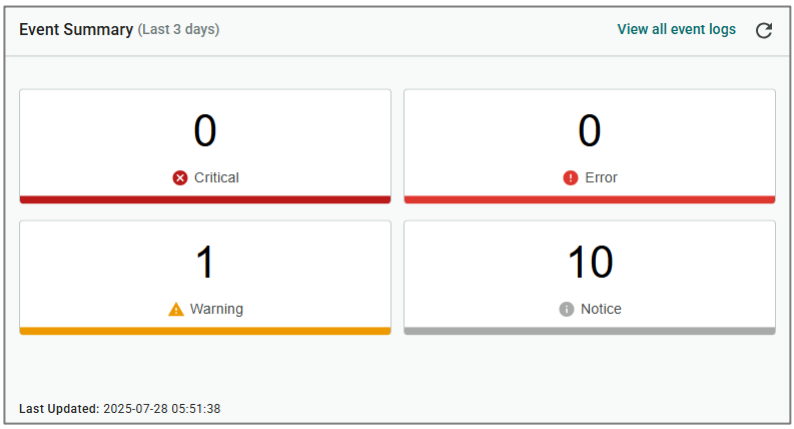
Click **Close** to close the **Panel View** and show the **Panel Status** again.

> **Note**
> The Panel View figure may vary depending on the device and the modules installed in it.



Event Summary (Last 3 days)

This display shows an event summary for the past three days. Click **View all event logs** to go to the Diagnostics > Event Logs and Notifications > Event Logs page to view more detailed information.



CPU Usage History (%)

This display shows the device's CPU usage shown as a percentage over time. Click the **Refresh (↻)** icon to refresh the graph.

System

Menu Path: System

This section lets you adjust various system settings.

This section includes these pages:

- System Management
- Account Management
- Management Interface
- Time

System - User Privileges

Privileges to System settings are granted to the different authority levels as follows. Refer to System > Account Management > User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Device Summary	R	R	R
System Management			
Information Settings	R/W	R/W	R
Firmware Upgrade	R/W	-	-
Config Backup and Restore	R/W	-	-
Account Management			
User Accounts	R/W	-	-
Online Accounts	R/W	-	-
Password Policy	R/W	-	-
Management Interface			

Settings	Admin	Supervisor	User
User Interface	R/W	R	R
Hardware Interfaces	R/W	R/W	R
SNMP	R/W	-	-
RMON1 (Only in CLI)	R/W	R/W	R
Time			
System Time	R/W	R/W	R
NTP Server	R/W	R/W	-

System Management

Menu Path: System > System Management

This section lets you adjust various system management related settings.

This section includes these pages:

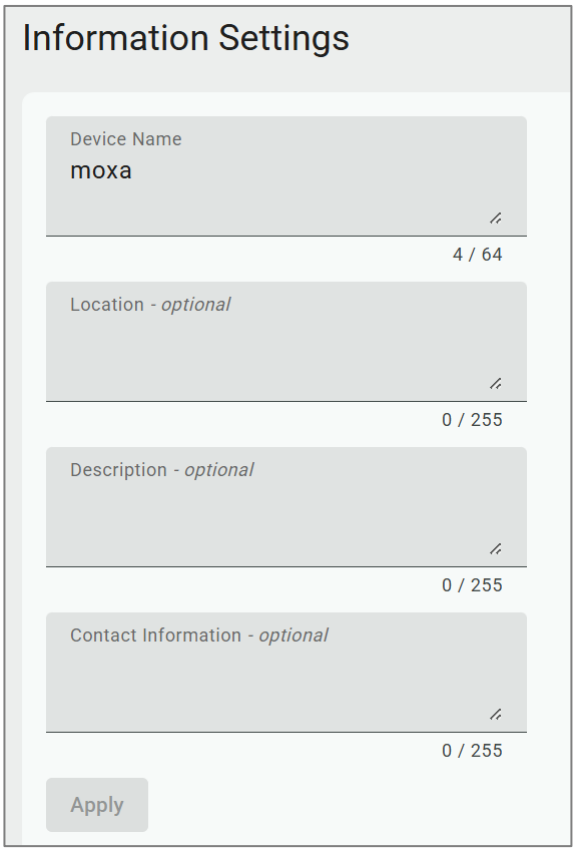
- Information Settings
- Firmware Upgrade
- Config Backup and Restore

Information Settings

Menu Path: System > System Management > Information Settings

This page lets you add additional information about the device to make it easier to identify different switches that are connected to your network.

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



UI Setting	Description	Valid Range	Default Value
Device Name	Specify a name for the device. This helps you differentiate between the roles or applications of different devices.	1 to 64 characters • characters: a-z, A-Z, 0-9 • special characters: .- • The device name cannot start with– (dash) and cannot end with–(dash).	moxa
Location	Specify a location for the device. This helps you differentiate between different locations or sites for different devices.	0 to 255 characters • characters: a-z, A-Z, 0-9 • special characters: ~ ! @ # $ % ^ & * ( ) { } [ ] < > _ + - = \ : ; , . /	N/A
Description	Specify a description for the device. This helps you keep a more detailed description of the device.	0 to 255 characters	N/A

UI Setting	Description	Valid Range	Default Value
Contact Information	Specify the contact information of the person in charge of the device. You can enter information such as an email address or telephone number for a person to contact if problems occur.	0 to 255 characters	N/A

Firmware Upgrade

Menu Path: System > System Management > Firmware Upgrade

This section lets you upgrade the firmware through the following methods:

- Local
- TFTP
- SFTP
- USB

Note

It is highly recommended that you back up your device's configuration before upgrading the firmware. Refer to System > System Management > Configuration Backup and Restore for more information.

Note

If it is necessary to verify the integrity and signature of the application when the system is running, the administrator can use the show integrity check CLI command.

Warning

Upgrading the firmware should be only be done by qualified personnel, as it is possible to render the device inoperable if the upgrade is not done properly. If you are not familiar with the process, please request the assistance of qualified personnel. You can also consult with Moxa support and we will provide you with the necessary assistance.

Before performing a firmware upgrade, make sure you take the following precautions:

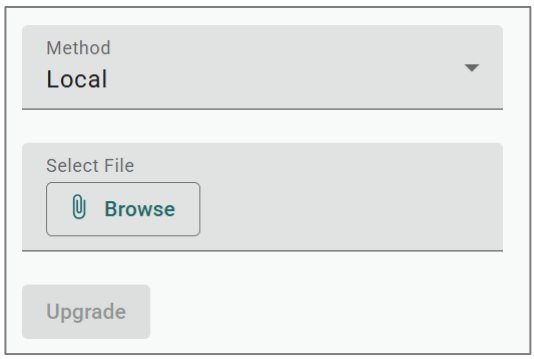
- Back up your configuration before upgrading the firmware
- Ensure that the device has power during the entire process
- Ensure that your computer stays connected to the device you are upgrading the firmware on
- Make sure the connection to the firmware source is not interrupted during the upgrade process

Firmware Upgrade - Local

If you select **Local** as your **Method**, these settings will appear. The Local method lets you upload firmware directly from local storage on the host device.

Note

Before performing a firmware upgrade, download the updated firmware (*.rom) file first from Moxa's website (www.moxa.com).

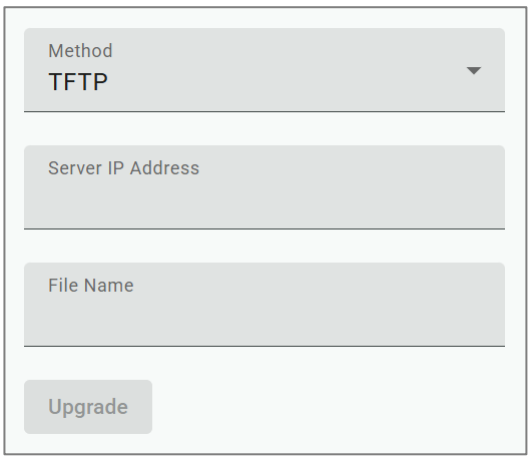


UI Setting	Description	Valid Range	Default Value
Select File	Select the new firmware file (*.rom) to use from your computer.	Select a file from your computer	N/A

Firmware Upgrade - TFTP

If you select **TFTP** as your **Method**, these settings will appear. The TFTP method lets you upload and install firmware stored on a remote TFTP server.

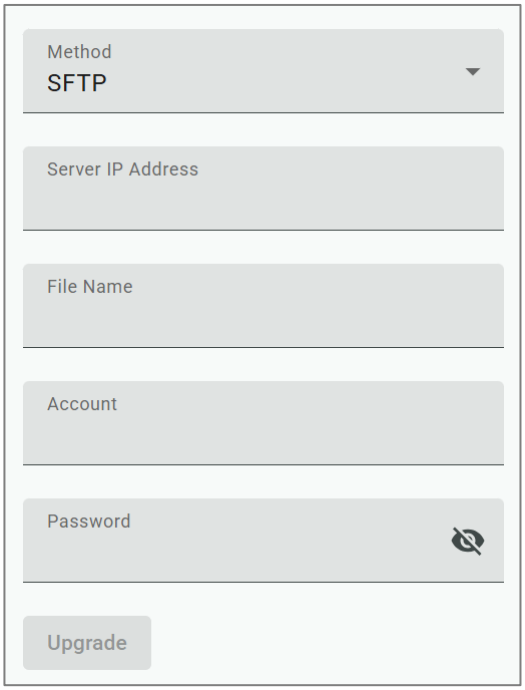
> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.



UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the TFTP server where the new firmware file (*.rom) is located.	Valid IP address	N/A
File Name	Specify the filename of the new firmware, including its full path on the server. Example: /path_to_firmware_file/firmware_file.rom **Note** If a path is not specified, the default folder for the server will be used.	File name	N/A

Firmware Upgrade - SFTP

If you select **SFTP** as your **Method**, these settings will appear. The SFTP method lets you upload and install firmware stored on a remote SFTP server.



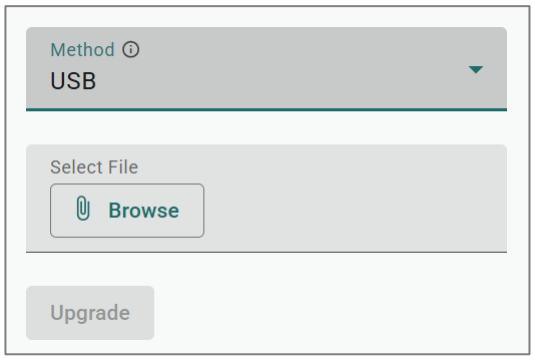
UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the SFTP server where the new firmware file (*.rom) is located.	Valid IP address	N/A
File Name	Specify the filename of the new firmware, including its full path on the server. Example: /path_to_firmware_file/firmware_file.rom **Note** If a path is not specified, the default folder for the server will be used.	File name can only contain A-Z, a-z, 0-9 or the symbols -._().	N/A
Account	Enter the SFTP server account name to use to connect to the SFTP server.	Account	N/A
Password	Enter the SFTP server account password to use to connect to the SFTP server.	Password	N/A

Firmware Upgrade - USB

If you select **USB** as your **Method**, these settings will appear. The USB method allows you to upgrade the firmware via Moxa's USB-based ABC-02 configuration tool.

Note

To use this feature, USB Function must be enabled in System > Management Interface > Hardware Interface.



UI Setting	Description	Valid Range	Default Value
Select File	Select the new firmware file (*.rom) to use from your USB device.	Select a file from the USB device	N/A

Creating a Configuration Backup

Backup known-good configurations to restore devices to secure states.

- Make sure all device has been configured to known-good, known-secure settings. Refer to the Security Hardening Guide for more information.
- Configure **File Signature** and **Import Custom Key** to help reduce the risk of tampering.
- Configure **File Encryption** to help avoid exposing sensitive information in the event of coconfiguration backup compromise.

1. Sign in to the device with administrator credentials.
2. Go to **System** > **System Management** > **Config Backup and Restore** > **Backup**.
3. **Optional:** Specify **Configuration Name** and then select **Apply**.

Note

The configuration name alone cannot ensure the integrity and consistency of the configuration file. You can have multiple backups with the same configuration name, but the settings in the configuration files may be different.

4. For **Method**, select an option for backup.

Option	Description
Local	Backs up configuration to local host. For **Select Configuration**, select **Running Configuration** or **Startup Configuration**. For **Default Configuration**, select **Not Included** or **Included**.
TFTP	Uses a remote TFTP server. Specify **Server IP Address** and **File Name**. **Note** Specify a path as part of File Name in the format /path_to_configuration_file/configuration_file.conf. If a path is not specified, the default folder for the server will be used.
SFTP	As TFTP, with the addition of **Account** and **Password** for authentication.
USB	Uses a Moxa ABC-02 configuration tool connected to the device. **Note** Requires enabling USB Function under System > Management Interface > Hardware.

The configuration backup begins.

Note

Configure Auto Configuration Backup to automatically backup to USB whenever the configuration changes.

Specify Configuration Name and then select **Apply**.

Restoring a Configuration Backup

Restore previously-backed up configurations to recover devices to known-good, secure states.

If your backup has been configured with **File Signature** or **File Encryption**, make sure that the proper keys or passwords are configured before proceeding.

1. Sign in to the device with administrator credentials.
2. Go to **System** > **System Management** > **Config Backup and Restore** > **Restore**.
3. Choose whether to enable **Configuration Firmware Version Checking**.

This can help prevent restoration of configuration files that might not be backward or forward compatible.

4. For **Method**, select an option for restoration.

Method	Description
Local	Restores a configuration from a file on the local host. To choose a file, select **Browse**.
TFTP	Uses a remote TFTP server. Specify **Server IP Address** and **File Name**.**Important:** Specify a path as part of **File Name** in the format `/path_to_configuration_file/configuration_file.conf`. If a path is not specified, the default folder for the server will be used.
SFTP	As TFTP, with the addition of **Account** and **Password** for authentication.
USB	Uses a Moxa ABC-02 configuration tool connected to the device.**Note:** Requires enabling **USB Function** under **System** > **Management Interface** > **Hardware**.

4. Select **Restore** to start the restoration process.

The restoration process begins.

> **Note**
> Configure Auto Configuration Restore to automatically restore from USB whenever the device restarts.

Config Backup and Restore

Menu Path: System > System Management > Config Backup and Restore

This page helps you back up and restore your device configuration.

This page includes these tabs:

- Backup
- Restore
- File Encryption
- File Signature

Config Backup and Restore - Backup

Menu Path: System > System Management > Config Backup and Restore - Backup

This section lets you create a backup of the current device configuration.

There are multiple methods of backing up the device configuration:

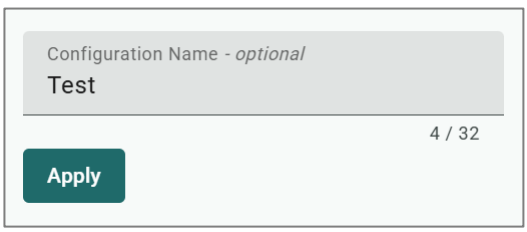
- Local
- TFTP
- SFTP
- USB

> **Note**
> For security reasons, we strongly recommend that you back up the system configuration to a secure storage location periodically.

Configuration Name

You can specify a configuration name to easily identify the configuration during backup or restore.

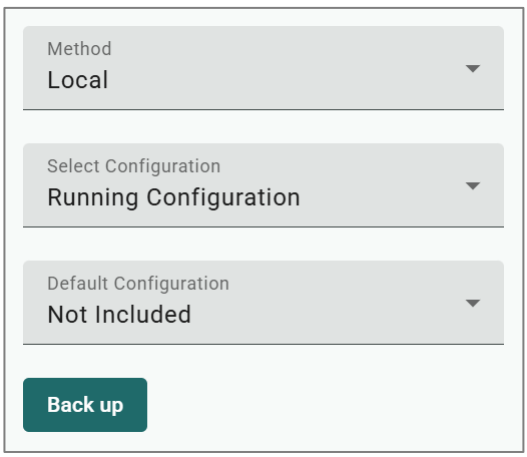
> **Note**
> The configuration name alone cannot ensure the integrity and consistency of the configuration file. You can have multiple backups with the same configuration name, but the settings in the configuration files may be different.



UI Setting	Description	Valid Range	Default Value
Configuration Name	Specify the configuration name to use for the backup.	1 to 32 characters	N/A

Configuration Backup - Local

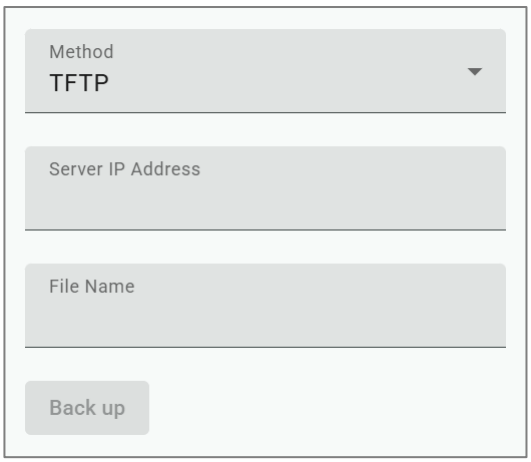
If you select **Local** as your **Method**, these settings will appear. The Local method will export the configuration backup file to the local host.



UI Setting	Description	Valid Range	Default Value
Select Configuration	Select whether to back up the running configuration or the startup configuration of the switch. Refer to Auto-save to Startup for more information. **Note** To export custom default settings to a local host, select Startup Configuration when exporting the configuration, as custom default settings are part of the startup configuration.	Running Configuration / Startup Configuration	Running Configuration
Default Configuration	Choose to back up the configuration with or without default settings.	Not Included / Included	Not Included

Configuration Backup - TFTP

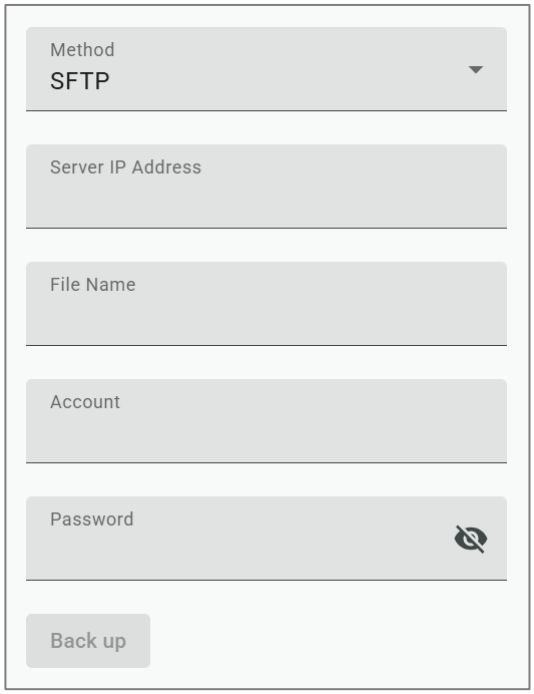
If you select **TFTP** as your **Method**, these settings will appear. The TFTP method lets you back up the startup configuration to a remote TFTP server.



UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the TFTP server to upload the backup of the startup configuration to.	Valid IP address	N/A
File Name	Specify a filename for the backup, including its full path on the server. Example: /path_to_configuration_file/configuration_file.conf **Note** If a path is not specified, the default folder for the server will be used.	N/A	N/A

Configuration Backup - SFTP

If you select **SFTP** as your **Method**, these settings will appear. The SFTP method lets you back up the startup configuration to a remote SFTP server.



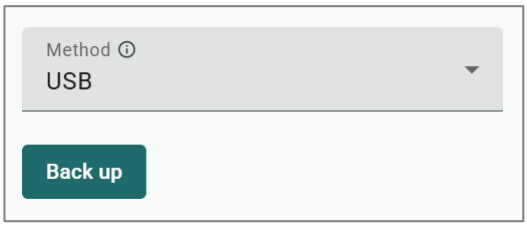
UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the SFTP server to upload the backup of the startup configuration to.	Valid IP address	N/A
File Name	Specify a filename for the backup, including its full path on the server. Example: /path_to_configuration_file/configuration_file.conf **Note** If a path is not specified, the default folder for the server will be used.	File name can only contain A-Z, a-z, 0-9 or the symbols -._().	N/A
Account	Enter the SFTP server account name to use to connect to the SFTP server.	N/A	N/A
Password	Enter the SFTP server account password to use to connect to the SFTP server.	N/A	N/A

Configuration Backup - USB

If you select **USB** as your **Method,** these settings will appear. The USB method allows you to back up the startup configuration to a Moxa ABC-02 configuration tool connected to the device.

Insert a Moxa ABC-02 configuration tool into the USB port of the switch, then click **Back up** to back up the startup configuration.

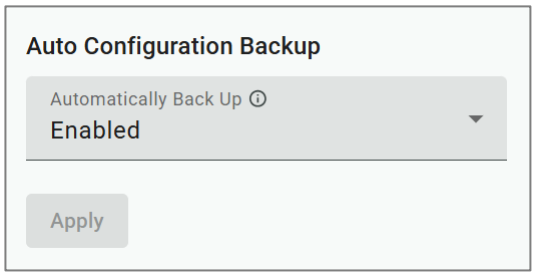
> **Note**
>
> To use this feature, USB Function must be enabled in System > Management Interface > Hardware Interface.



Auto Configuration Backup

Auto configuration backup lets you automatically back up the startup configuration to an ABC-02 configuration tool whenever the startup configuration changes.

To enable automatic backup, select **Enabled** from the drop-down list, then click **Apply.**



UI Setting	Description	Valid Range	Default Value
Automatically Back Up	When enabled, this will back up the startup configuration to an inserted ABC-02 configuration tool whenever the startup configuration changes. **Note** To use an ABC-02 configuration tool, USB Function must be enabled in System > Management Interface > Hardware Interface.	Enabled / Disabled	Enabled

Config Backup and Restore - Restore

Menu Path: System > System Management > Config Backup and Restore - Restore

This page lets you restore a previously backed up configuration. When restoring from a file that contains a startup configuration, any custom default settings in the startup configuration will also be restored. Refer to Save Custom Default for more information.

Note

Configurations are restored to the running configuration.

If Auto-save to Startup is disabled, the restored configuration will not be saved to the startup configuration, and the device will revert to its current startup configuration if the device is rebooted.

To save the restored configuration to the startup configuration, click the Save ( ) icon or enable Auto-save to Startup.

Refer to Auto-save to Startup for more information.

Note

To ensure that configuration files can be imported successfully, do not modify the configuration files manually.

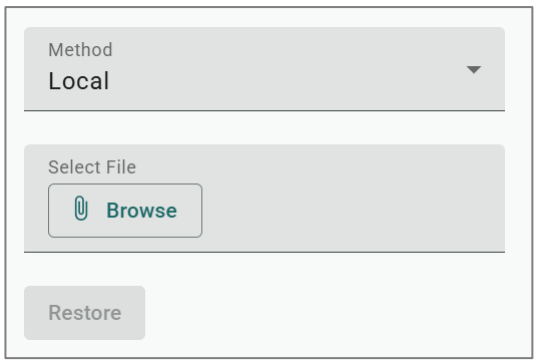
There are multiple methods of restoring the device configuration:

- Local
- TFTP

- SFTP
- USB

Configuration Restore - Local

If you select **Local** as your **Method**, these settings will appear. The Local method will restore from a configuration file on the local host.

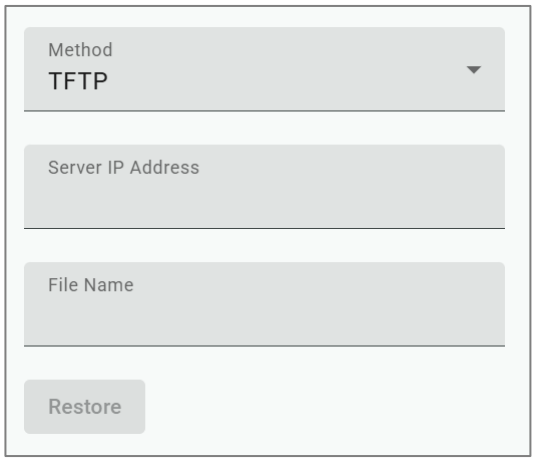


UI Setting	Description	Valid Range	Default Value
Select File	Select the configuration file to use from your computer.	Select a file from your computer	N/A

Configuration Restore - TFTP

If you select **TFTP** as your **Method**, these settings will appear. The TFTP method lets you download and install a configuration stored on a remote TFTP server.

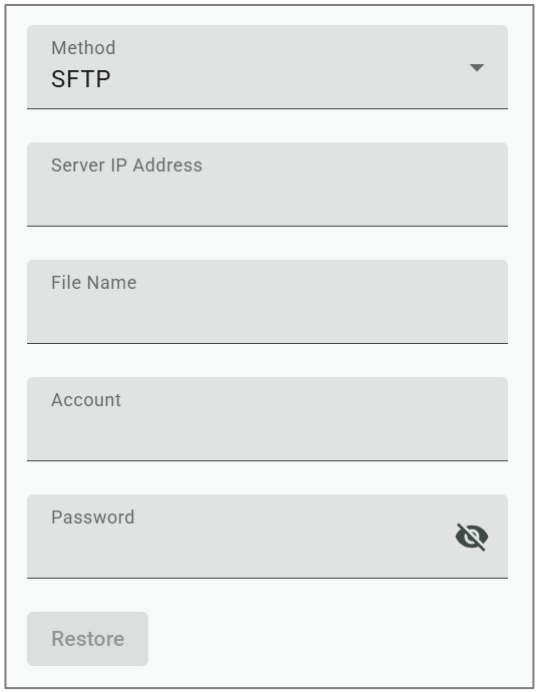
> **Note**
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.



UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the TFTP server.	Valid IP address	N/A
File Name	Specify the file name of the configuration file to restore from, including its full path on the server. Example: /path_to_configuration_file/configuration_file.conf **Note** If a path is not specified, the default folder for the server will be used.	Up to 54 characters, including file extension. File name can only contain the characters A-Z, a-z, 0-9, and special characters -._().	N/A

Configuration Restore - SFTP

If you select **SFTP** as your **Method**, these settings will appear. The SFTP method lets you download and install a configuration stored on a remote SFTP server.



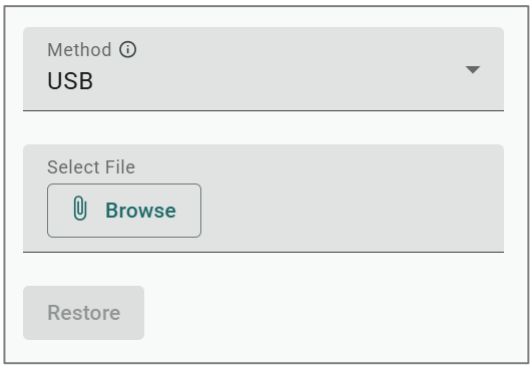
UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the SFTP server where the configuration file is stored.	Valid IP address	N/A
File Name	Specify the file name of the configuration file to restore from, including its full path on the server. Example: /path_to_configuration_file/configuration_file.conf **Note** If a path is not specified, the default folder for the server will be used.	File name can only contain the characters A-Z, a-z, 0-9, and special characters -._().	N/A
Account	Enter the SFTP server account name to use to connect to the SFTP server.	Account	N/A
Password	Enter the SFTP server account password to use to connect to the SFTP server.	Password	N/A

Configuration Restore - USB

If you select USB as your **Method**, these settings will appear. The USB method allows you to restore the configuration from a file via Moxa's USB-based ABC-02 configuration tool.

Note

To use this feature, USB Function must be enabled in System > Management Interface > Hardware Interface.

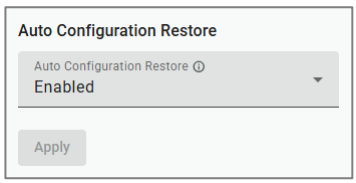


UI Setting	Description	Valid Range	Default Value
Select File	Select the configuration file to use from your USB device.	Select a file from the USB device	N/A

Auto Configuration Restore

Auto configuration restore lets you restore the device's configuration from an inserted ABC-02 configuration tool whenever the device is rebooted.

To enable automatic restore, select **Enabled** from the drop-down list, then click **Apply**.

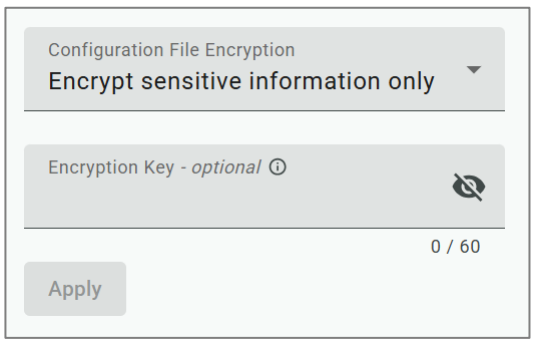


UI Setting	Description	Valid Range	Default Value
Automatically Restore	When enabled, this will restore the device's configuration from an inserted ABC-02 configuration tool whenever the device is rebooted. **Note** To use an ABC-02 configuration tool, USB Function must be enabled in System > Management Interface > Hardware Interface.	Enabled / Disabled	Enabled

Config Backup and Restore - File Encryption

Menu Path: System > System Management > Config Backup and Restore - File Encryption

This page lets you configure data encryption settings for exported configuration files.



UI Setting	Description	Valid Range	Default Value
Configuration File Encryption	Select which file encryption mode to use. **Encrypt sensitive information only:** Only sensitive information will be encrypted in the configuration file. **Encrypt the entire file:** The entire configuration file will be encrypted. **Note** Sensitive information includes passwords used for authentication and the encryption key used to encrypt data.	Encrypt sensitive information only / Encrypt whole file	Encrypt sensitive information only
Encryption Key	Specify an encryption key to use for configuration files. **Note** If no encryption key is specified, then the Moxa encryption key will be used.	0 to 60 characters	Blank (the Moxa encryption key will be used)

File Signature

Menu Path: System > System Management > Config Backup and Restore - File Signature

This page lets you enable use of file signatures to help ensure the file integrity and authenticity of your configuration files.

Note

Before enabling file signatures, you will need to add a private/public key to the table on this page.

Limitations

You can add up to 1 key to use for file signatures.

Signed Configuration

UI Setting	Description	Valid Range	Default Value
Signed Configuration	Enables or disables the use of a digital signature to check the integrity of configuration files. **Note** To enable this feature, a private/public key must be installed first. Refer to Adding a Custom Key for more information.	Enabled / Disabled	Disabled

File Signature Key List

UI Setting	Description
Label	Shows the label used to help identify the key.
Algorithm	Shows the algorithm used for the key, such as RSA or ECDSA.

UI Setting	Description
Length	Shows the length of the key in bits.

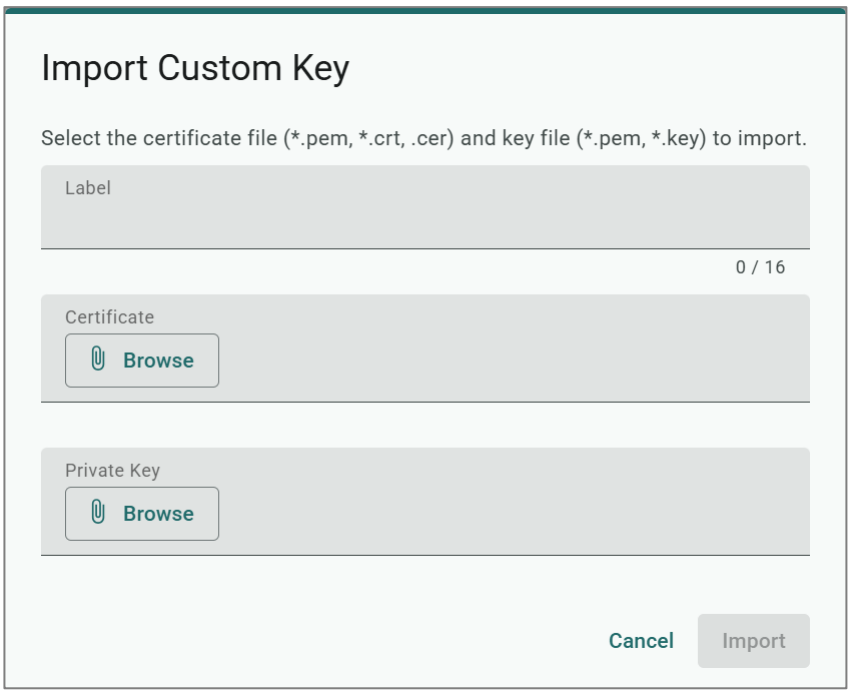
Import Custom Key

Menu Path: System > System Management > Config Backup and Restore - File Signature

Clicking the **Import Custom Key** button on the **System > System Management > Config Backup and Restore - File Signature** page will open this dialog box. This dialog lets you add a custom key to use for file signatures.

Click **Import Custom Key** to save your changes and add the new key.

Once the File Signature Key is imported, you can click the **Manage** button to: edit the label, import a new custom key, or delete the current key.



UI Setting	Description	Valid Range	Default Value
Label	Specify a label to help describe the certificate and the key.	0 to 16 characters	N/A

UI Setting	Description	Valid Range	Default Value
Certificate	Select a certificate file to import from your computer.	Select a certificate file from your computer	N/A
Key	Select a key file to import from your computer.	Select a key file from your computer	N/A

Account Management

Menu Path: System > Account Management

This section lets you manage user accounts for your device. You can enable different accounts with different roles to facilitate convenient management and safe access.

This section includes these pages:

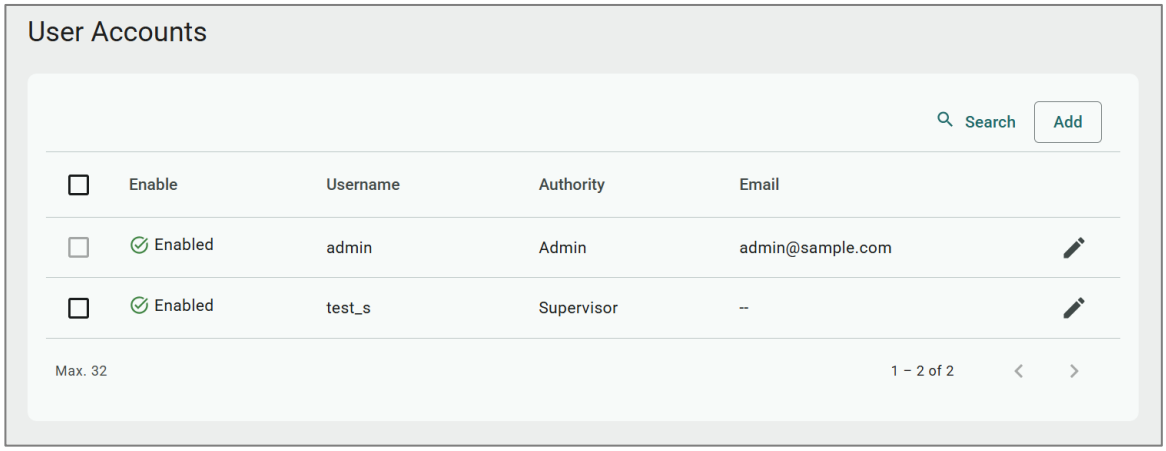
- User Accounts
- Online Accounts
- Password Policy

User Accounts

Menu Path: System > Account Management > User Accounts

This page lets you manage the user accounts for your device.

> **Note**
> By default, there is only one account: admin



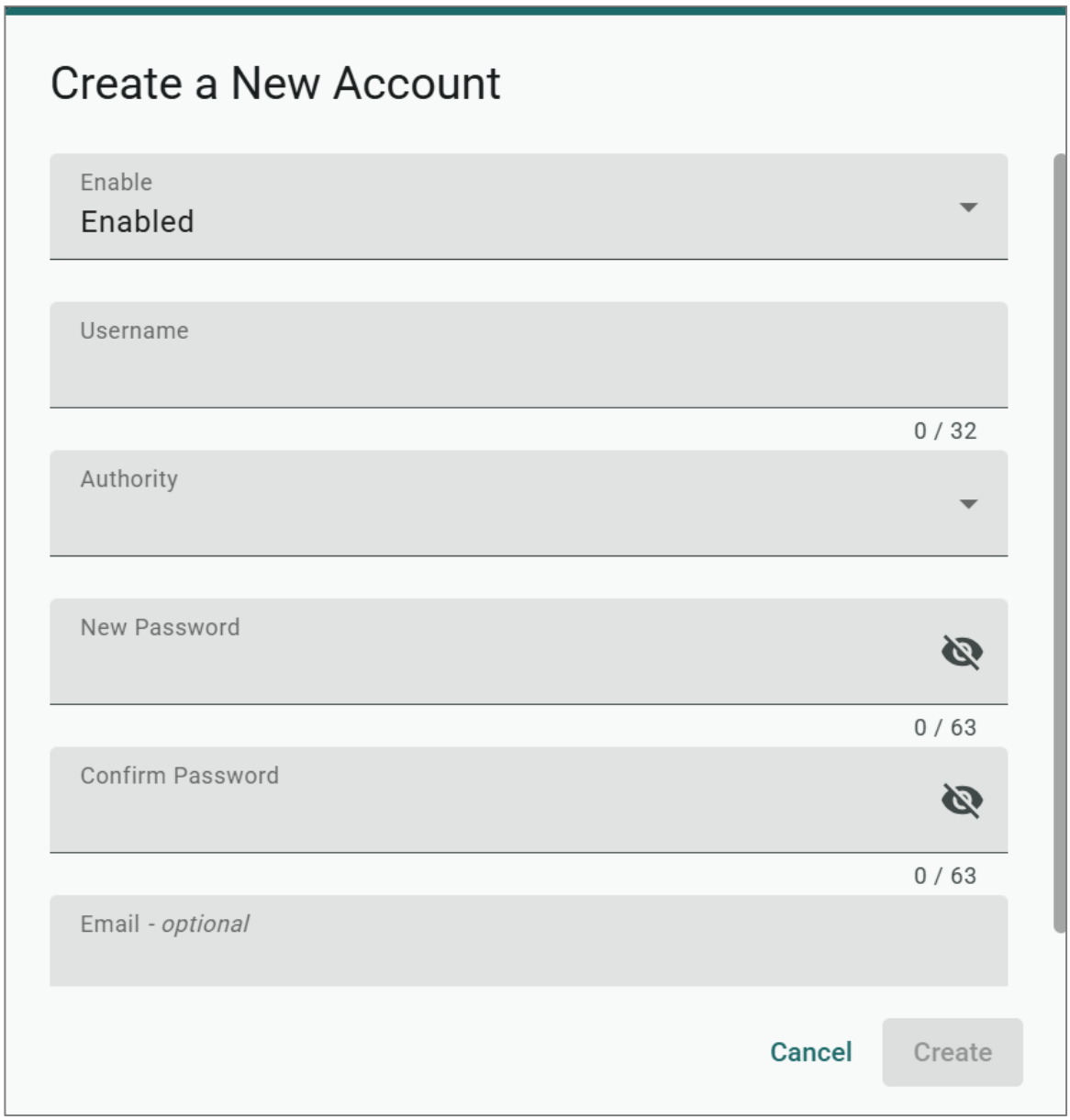
UI Setting	Description
Enable	Shows whether the account is enabled or disabled.
Username	Shows the username of the account.
Authority	Shows the authority level of the account.
Email	Shows the email address of the account.

User Accounts - Create a New Account

Menu Path: System > Account Management > User Accounts

Clicking the **Create** button on the page will open this dialog box. This dialog lets you create a new user account.

Click **Create** to save your changes and add the new account.



UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable the user account.	Enabled / Disabled	Enabled
Username	Specify a username for this account.	4 to 32 characters	N/A

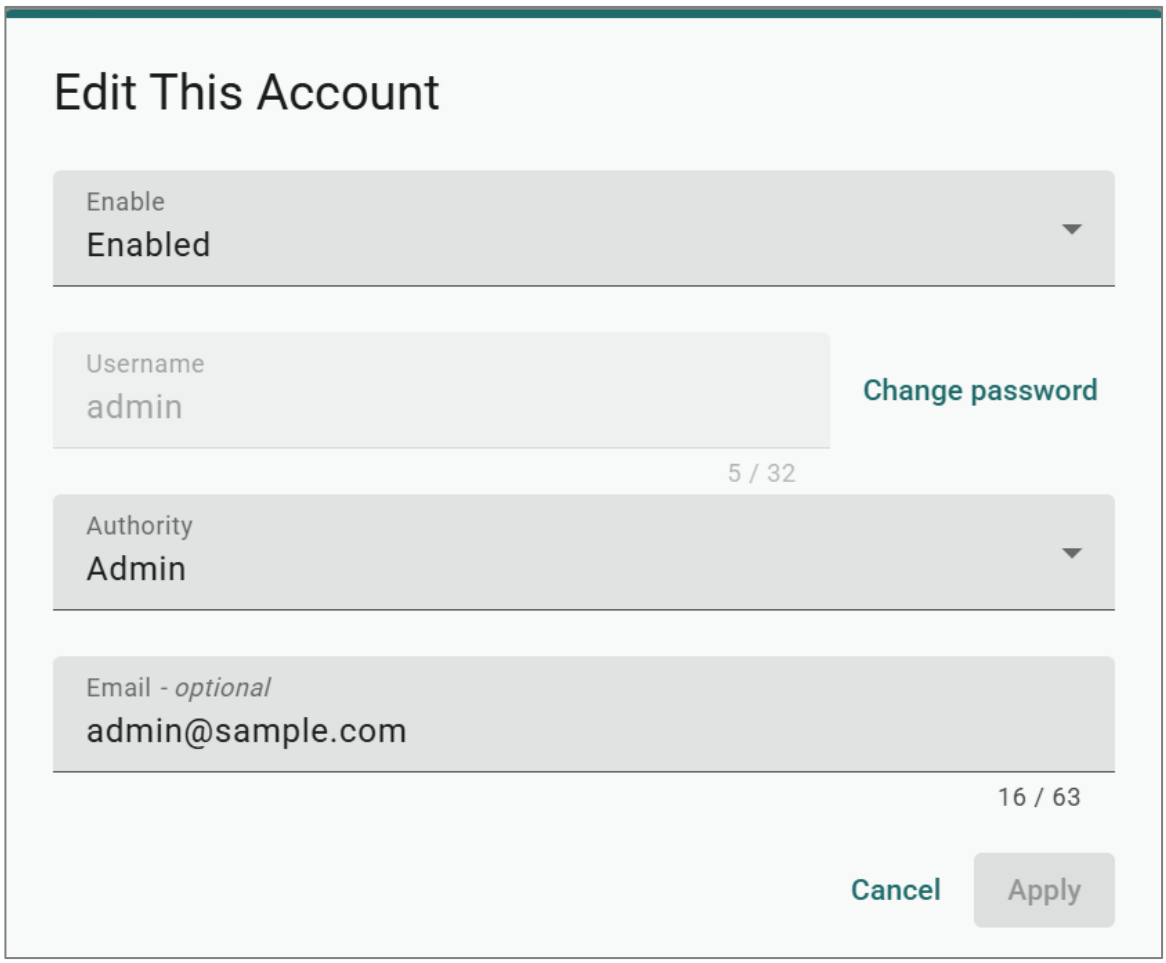
UI Setting	Description	Valid Range	Default Value
Authority	Specify the authority level of the account. Refer to the Account Privileges List for a list of what read/write access privileges are granted for the different authority levels. • **Admin**: This account has read/write access of all configuration parameters. • **Supervisor**: This account has read/write access for a limited set of configuration parameters. • **User**: This account can only view a limited set of configuration parameters. **Note** In order to enhance security, we suggest you create a new account with the User authority.	Admin / Supervisor / User	N/A
New Password	Specify the new password for this account.	4 to 63 characters, additional requirements are based on settings in **System > Account Management > Password Policy**	N/A
Confirm Password	Reenter the password to confirm.	4 to 63 characters, must match **New Password**	N/A
Email	Specify an email address for the account (optional).	Valid email address, 0 to 63 characters	N/A

User Accounts - Edit This Account

Menu Path: System > Account Management > User Accounts

Clicking the **Edit (✎)** icon for an account on the **System > Account Management > User Accounts** page will open this dialog box. This dialog lets you edit an existing user account.

Click **Apply** to save your changes.

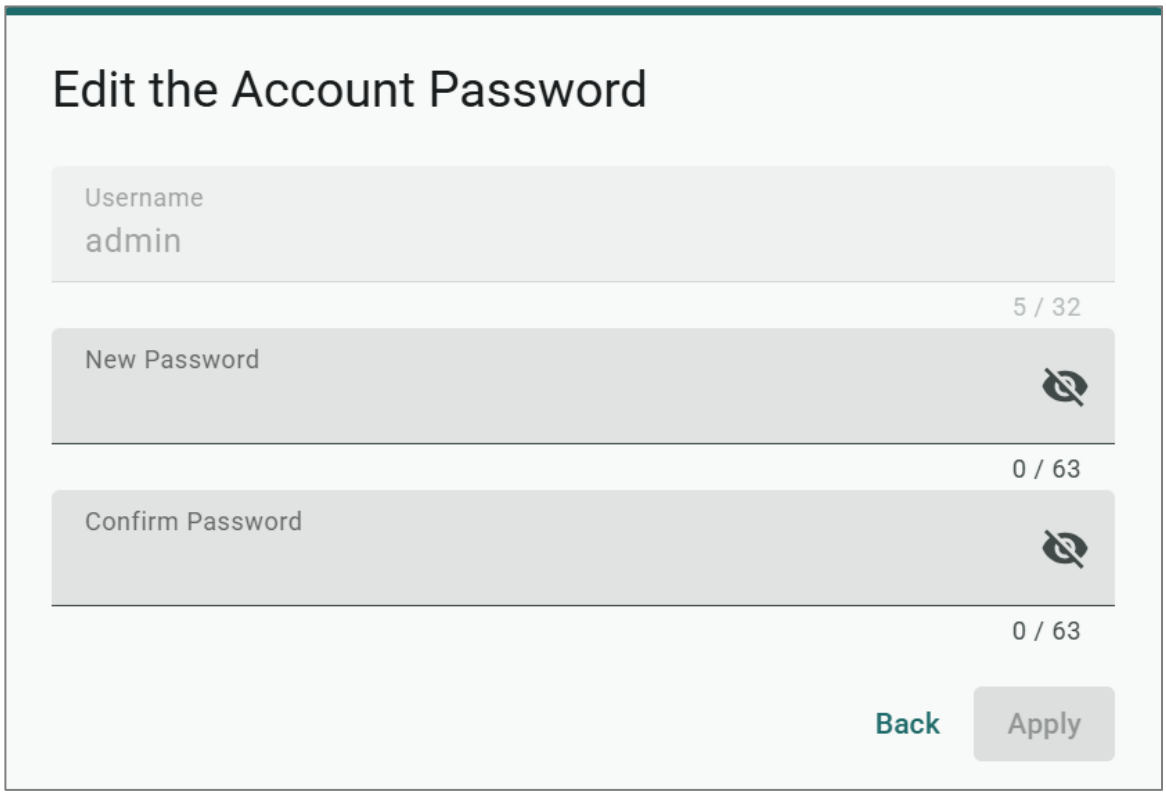


UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable the user account.	Enabled / Disabled	Enabled
Username	Shows the username of the account. **Note** The username cannot be edited after creating an account.	N/A	N/A
Change Password	Click **Change password** to change the account password. Refer to Edit the Account Password for more information.	N/A	N/A

UI Setting	Description	Valid Range	Default Value
Authority	Specify the authority level of the account. Refer to the Account Privileges List for a list of what read/write access privileges are granted for the different authority levels. • **Admin**: This account has read/write access of all configuration parameters. • **Supervisor**: This account has read/write access for a limited set of configuration parameters. • **User**: This account can only view a limited set of configuration parameters.	Admin / Supervisor / User	N/A
Email	Specify an email address for the account (optional).	Valid email address, 0 to 63 characters	N/A

Edit the Account Password

Clicking **Change password** in the **Edit This Account** dialog will open this dialog box. This dialog lets you change the password for an account. Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Username	Shows the username of the account. **Note** The username cannot be edited after creating an account.	N/A	N/A
New Password	Specify the new password for this account.	4 to 63 characters, additional requirements are based on settings in **System > Account Management > Password Policy**	N/A
Confirm Password	Reenter the password to confirm.	4 to 63 characters, must match **New Password**	N/A

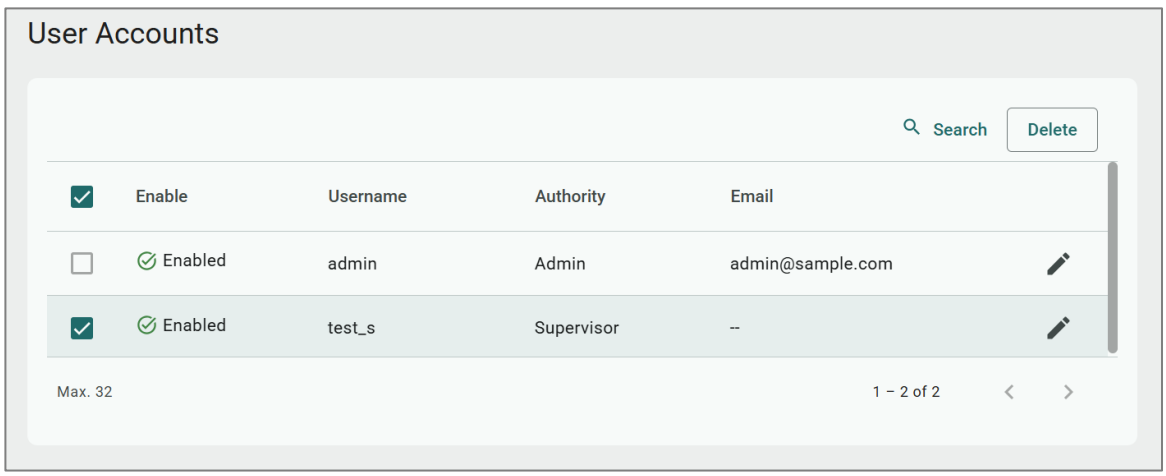
User Accounts - Delete Account

Menu Path: System > Account Management > User Accounts

You can delete an account by using the checkboxes to select the entries you want to delete, then clicking the **Delete** button.

Note

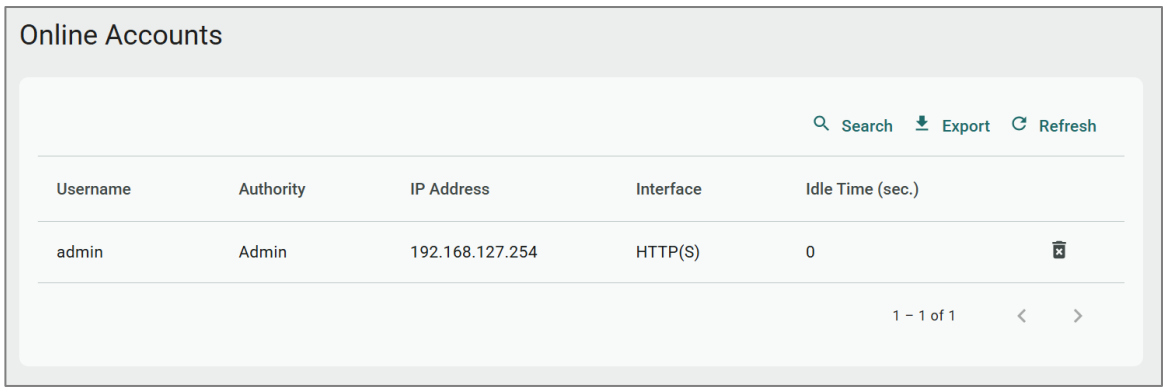
The "admin" account cannot be removed, but can be disabled if not in use.



Online Accounts

Menu Path: System > Account Management > Online Accounts

This page lets you view a list of connected user and also lets you disconnect users.

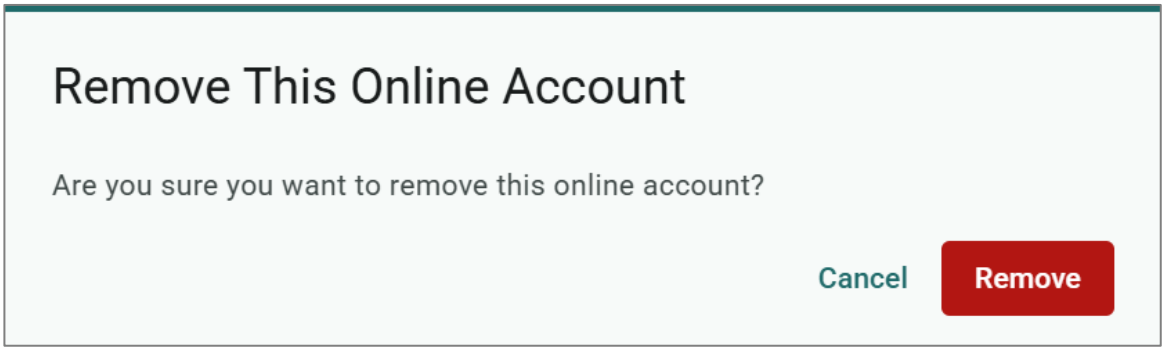


UI Setting	Description
Username	Shows the username of the online account.
Authority	Shows the authority level of the online account.
IP Address	Shows the IP address of the online account.
Interface	Shows the interface that the online account is using.
Idle Time (sec.)	Show the idle time in seconds for the online account.

Online Accounts - Remove This Online Account

Menu Path: System > Account Management > Online Accounts

You can disconnect a user by clicking its **Remove (** **)** icon. Click **Remove** to save your changes and remove the online account.



Password Policy

Menu Path: System > Account Management > Password Policy

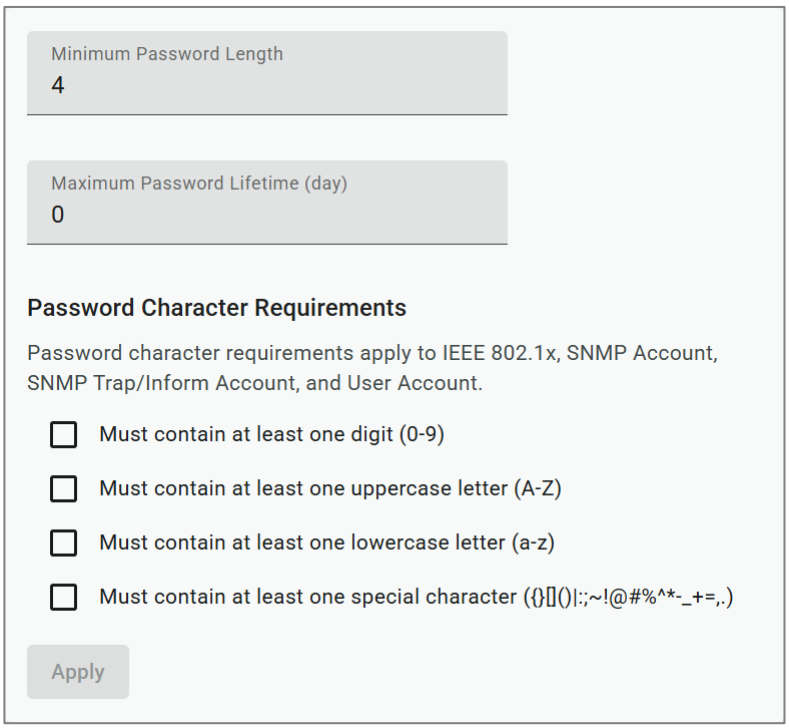
This page lets you create a robust password policy to safeguard your system against hackers. By enforcing minimum length and complexity requirements, you can empower users to choose strong passwords that are difficult to crack. Additionally, you can set a maximum password lifetime to ensure regular password changes, further enhancing security.

Click **Apply** to save your changes.

Note

To improve the security of your device and network, we recommend that you:

- Set the Minimum Length for passwords to 8
- Set a Maximum Password Lifetime to ensure that users change their password regularly
- Enable all the Password Character Requirements to ensure a minimum level of complexity



UI Setting	Description	Valid Range	Default Value
Minimum Password Length	Specify the minimum required password length.	4 to 16 characters	4
Maximum Password Lifetime (day)	Specify how long in days passwords will be valid for. When the password expires, the system will require the user to change their password. If this is set to 0, passwords will not expire.	0 to 365 days	0

UI Setting	Description	Valid Range	Default Value
Password Character Requirements	Select the complexity requirements that will apply to new passwords. **Note** 1. Password character requirements apply to IEEE 802.1x, SNMP Account, SNMP Trap/Inform Account, and User Account. 2. New requirements will only apply when creating or changing a password. They will not apply to existing passwords.	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 ({}[]()|:;~!@#%^*-_+=,.)	N/A

Management Interface

Menu Path: System > Management Interface

This section lets you configure the interfaces used to manage the device.

This section includes these pages:

- User Interface
- Hardware Interfaces
- SNMP

User Interface

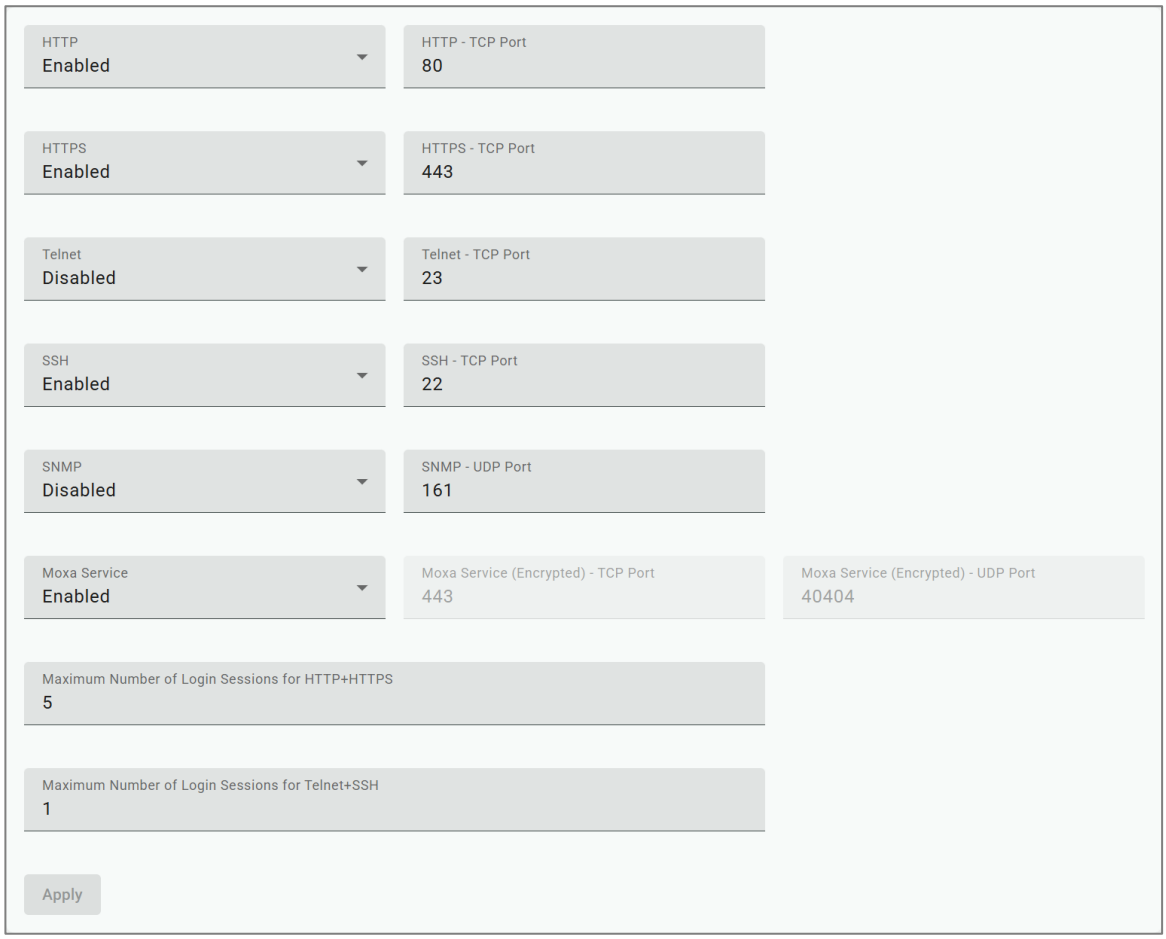
Menu Path: System > Management Interface > User Interface

This page lets you configure which interfaces can be used to access the device.

Click **Apply** to save your changes.

Note

For security reasons, users should access the device using secure HTTPS and SSH interfaces.



UI Setting	Description	Valid Range	Default Value
HTTP	Enable or disable HTTP connections.	Enabled / Disabled	Enabled
HTTP - TCP Port	Specify the TCP port to use for HTTP connections.	80, 1024 to 65535	80

UI Setting	Description	Valid Range	Default Value
HTTPS	Enable or disable HTTPS connections. **Note** The administrator can manually import a self-signed certificate (in .p12 format) for web server (HTTPS) services. However, the administrator should check the root certificate and validity of the signature before importing, according to the organization's security procedures and requirements. After importing a certificate, the administrator should check if the certificate has been revoked and if so, the certificate must be replaced. When a browser verifies the signature and accesses the device, it will return a subject name which the administrator can use to confirm the connected device is authorized. **Note** The encryption algorithm of keys should be selected based on internationally recognized and proven security practices and recommendations. The lifetime of certificates generated for web server (HTTPS) services should be short and in accordance with the organization's security procedures and requirements.	Enabled / Disabled	Enabled
HTTPS - TCP Port	Specify the TCP port to use for HTTPS connections.	443, 1024 to 65535	443
Telnet	Enable or disable Telnet connections.	Enabled / Disabled	Disabled
Telnet - TCP Port	Specify the TCP port to use for Telnet connections.	23, 1024 to 65535	23
SSH	Enable or disable SSH connections.	Enabled / Disabled	Enabled
SSH - TCP Port	Specify the TCP port to use for SSH connections.	22, 1024 to 65535	22
SNMP	Enable or disable SNMP connections.	Enabled / Disabled	Disabled
SNMP - UDP Port	Specify the UDP port to use for SNMP connections.	161, 1024 - 65535	161

UI Setting	Description	Valid Range	Default Value
Moxa Service **(Only in Advanced Mode)**	Enable or disable Moxa Service connectivity. **Note** Moxa Service is only used for Moxa network management software, and is only available for user accounts with admin privileges.	Enabled / Disabled	Enabled
Moxa Service (Encrypted) - TCP Port **(Only in Advanced Mode)**	Shows the TCP port used for Moxa Service. This setting cannot be changed.	N/A	443
Moxa Service (Encrypted) - UDP Port **(Only in Advanced Mode)**	Shows the UDP port used for Moxa Service. This setting cannot be changed.	N/A	40404
Maximum Number of Login Sessions for HTTP+HTTPS	Specify the maximum combined number of users that can be logged in using HTTP and HTTPS.	1 to 10	5
Maximum Number of Login Sessions for Telnet+SSH	Specify the maximum combined number of users that can be logged in using Telnet and SSH.	1 to 5	1

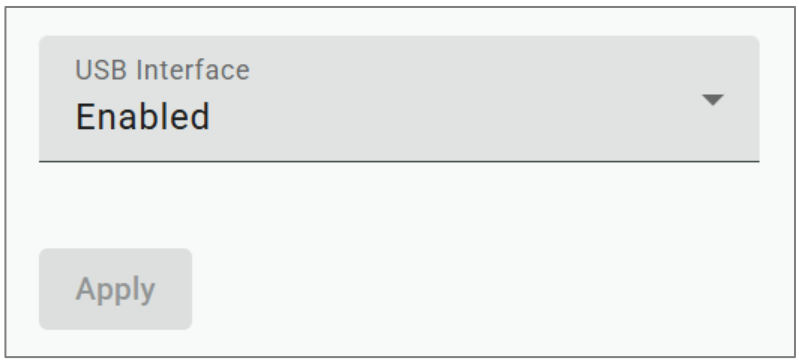
Hardware Interfaces

Menu Path: System > Management Interface > Hardware Interfaces

This page lets you enable or disable the USB interface on the device for use with an ABC-02 backup configurator tool.

Click **Apply** to save your changes.

Hardware Interfaces Settings



UI Setting	Description	Valid Range	Default Value
USB Interface	Enable or disable the USB interface on the device.	Enabled / Disabled	Enabled

Configuring Simple Network Management Protocol

Simple Network Management Protocol (SNMP) be used to manage and monitor network devices.

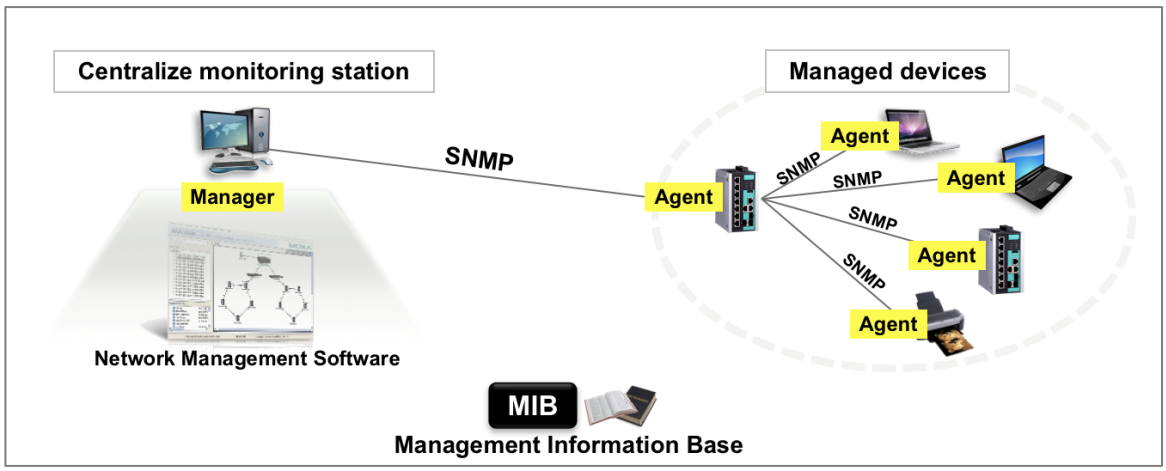
It is an application-layer protocol that allows administrators to manage network performance, diagnose network problems, and gather information about network devices such as routers, switches, servers, printers, and other network equipment. SNMP works by using agents installed on network devices, which provide information to a central management system known as an SNMP manager. The manager sends requests to the agent to retrieve information about the device, such as CPU utilization, memory usage, network traffic, and other metrics.

About SNMP

An SNMP deployment consists of Managers, Agents, and Management Information Bases (MIBs).

- **Management Information Base (MIB):** A database of information about network devices and their performance metrics. The MIB is organized hierarchically and uses a tree-like structure.

- **SNMP Manager:** The central management system that monitors and manages network devices. It sends requests to the SNMP agents to gather information and configure network devices.
- **SNMP Agent:** A software module installed on network devices that provides information about the device to the SNMP manager. The agent responds to requests from the manager and sends notifications to the manager when certain events occur, such as a device failure.



SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as configuration changes, through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. SNMP itself does not define which variables a managed system should offer. Rather, SNMP uses an extensible design that allows applications to define their own hierarchies. These hierarchies are described as a management information base (MIB). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that can be read or set via SNMP.

Creating an SNMP Account

You must configure an SNMP account on each of your devices to manage them.

Some account settings are contingent on SNMP account settings. Protocol versions earlier than v3 do not support authentication or encryption, and require shared community keys. Go to **System** > **Management Interface** > **SNMP**, click **General**, and choose an SNMP Version. For insecure versions, also specify community strings.

Note

SNMP versions earlier than v3 do not support authentication or encryption, and provide no security. It is strongly recommended to choose V3 Only unless compatibility absolutely requires earlier versions and security risks have been thoroughly evaluated.

To configure SNMP accounts:

1. Sign in to the device using administrator credentials.
2. Go to **System** > **Management Interface** > **SNMP**, and then click **SNMP Account**.
3. Click ***[Add]***.

   The Create an SNMP Account screen appears.
4. Specify all of the following, and then click **Create**:

Option	Value
Username	Specify a username for the account with up to 32 characters
Authority	Choose from: • **Read/Write** • **Read**
Authentication Type	Choose from: • **None** • **MD5** • **SHA** • **SHA-256** • **SHA-512** **Note** Authentication requires SNMP v3.
Authentication Password	If an authentication type has been specified, specify a password for the account between 8 and 64 characters long.

Option	Value
Encryption Key	• **Disabled** • **DES** • **AES** **Note** Encryption requires SNMP v3.
Encryption Key	If an encryption method has been chosen, specify an Encryption Key between 8 and 64 characters long.

The account appears in the **SNMP Account** table.

You can Edit or Delete from the list by clicking the corredponing **[Edit]** or **[Delete]**.

SNMP

Menu Path: System > Management Interface > SNMP

This page lets you configure SNMP settings for your device.

This page includes these tabs:

- General
- SNMP Account

SNMP - General

Menu Path: System > Management Interface > SNMP - General

This page lets you specify the SNMP versions used to manage your device.

Click **Apply** to save your changes.

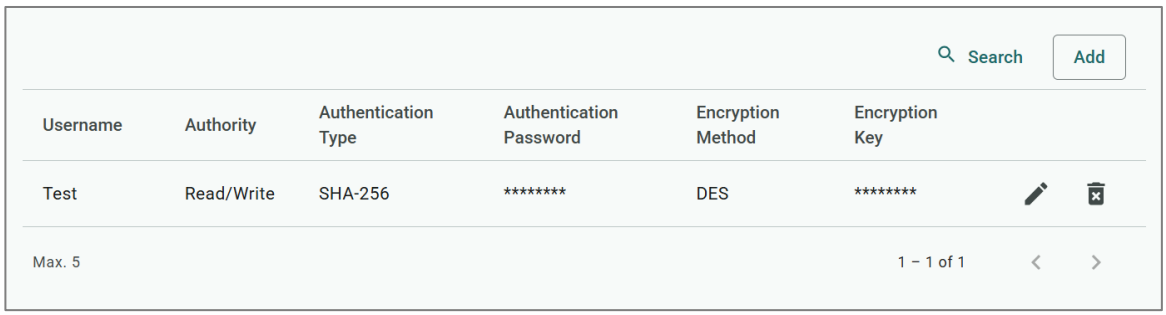
UI Setting	Description	Valid Range	Default Value
SNMP Version	Specify the SNMP protocol version used to manage your device. • **V1, V2c, V3**: Enable SNMP V1, V2c, and V3. • **V1, V2c**: Enable SNMP V1 and V2c only. • **V3 only**: Enable SNMP V3 only.	V1, V2c, V3 / V1, V2c / V3 only	V1, V2C
Read Community	Specify a string name for the SNMP Read Community.	4 to 32 characters	public
Read/Write Community	Specify a string name for the SNMP Read/Write Community.	4 to 32 characters	private

SNMP Account

Menu Path: System > Management Interface > SNMP - SNMP Account

This page lets you configure the SNMP management accounts for the device. SNMP management accounts are provided for Admin and User-level authority.

SNMP Account List



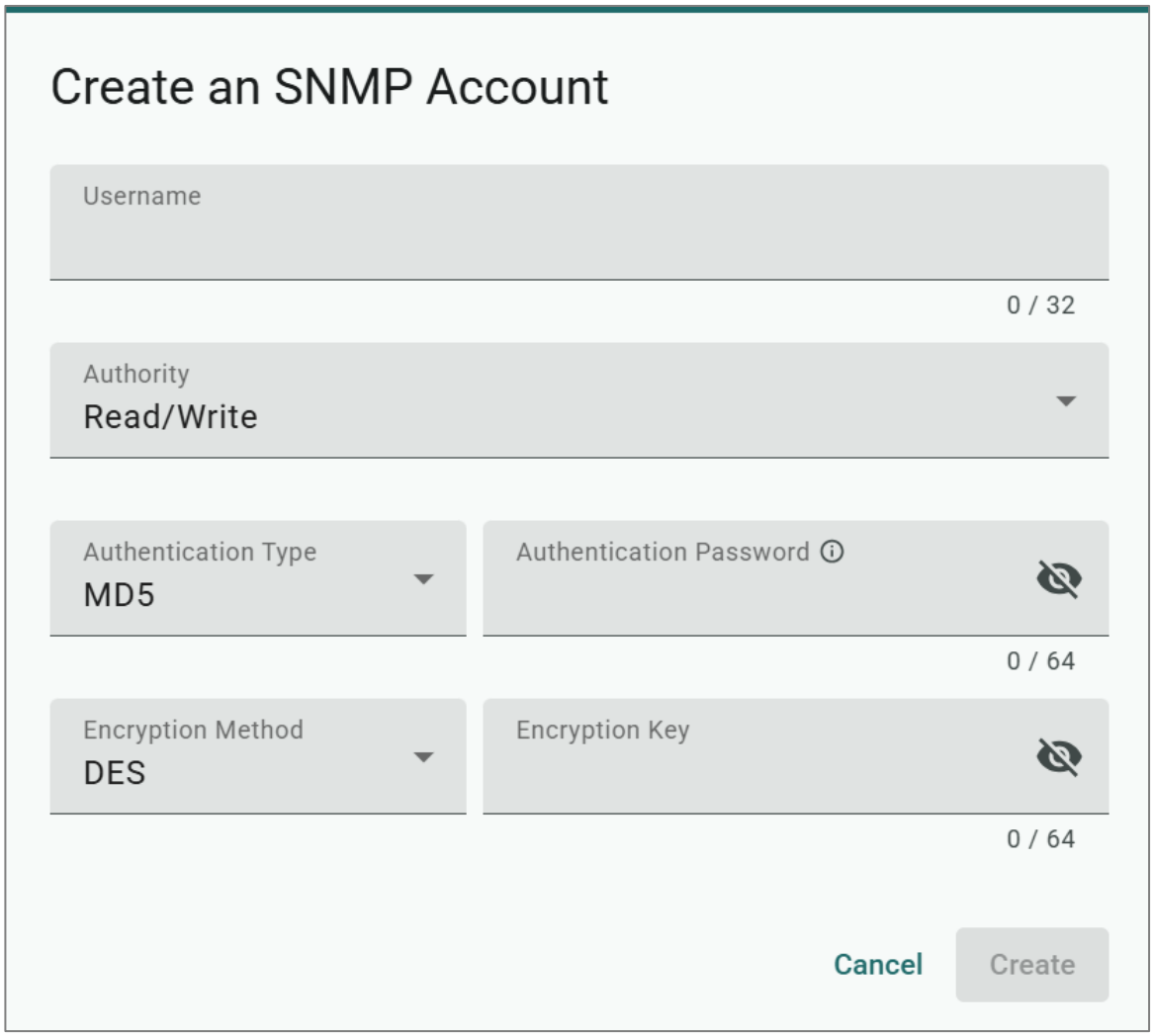
UI Setting	Description
Username	Shows the username of the SNMP account.
Authority	Shows the authority level of the management account.
Authentication Type	Shows the authentication type used for the account.
Authentication Password	Shows ******** if there is an authentication password for the account.
Encryption Method	Shows the encryption method used for the account.
Encryption Key	Shows ******** if there is an encryption key for the account.

Creating an SNMP Account

Menu Path: System > Management Interface > SNMP - SNMP Account

Clicking the **Create** button on the **System > Management Interface > SNMP - SNMP Account** page will open this dialog box. This dialog lets you create an SNMP account.

Click **Create** to save your changes and add the new account.



UI Setting	Description	Valid Range	Default Value
Username	Specify a username for the SNMP account.	1 to 32 characters • Valid characters: a-z, A-Z, 0-9 • Valid special characters: ._-	N/A
Authority	Specify the authority level of the management account. • **Read/Write**: Can read and write configuration settings • **Read**: Can only read configuration settings	Read/Write / Read	Read/Write
Authentication Type	Specify the authentication type to use for the account.	None / MD5 / SHA / SHA-256 / SHA-512	N/A

UI Setting	Description	Valid Range	Default Value
Authentication Password **(If Authentication Type is not None)**	Specify the authentication password for the account.	8 to 64 characters • Valid characters: a-z, A-Z, 0-9 • Valid special characters: . , - _ + = | : ; @ ! ~ # % ^ * ( ) [ ] { }	N/A
Encryption Method **(If Authentication Type is not None)**	Specify the encryption method to use for the account.	Disabled / DES / AES	Disabled
Encryption Key **(If Encryption Method is not Disabled)**	Specify the encryption key for the account.	8 to 64 characters • Valid characters: a-z, A-Z, 0-9 • Valid special characters: . , - _ + = | : ; @ ! ~ # % ^ * ( ) [ ] { }	N/A

Editing an SNMP Account

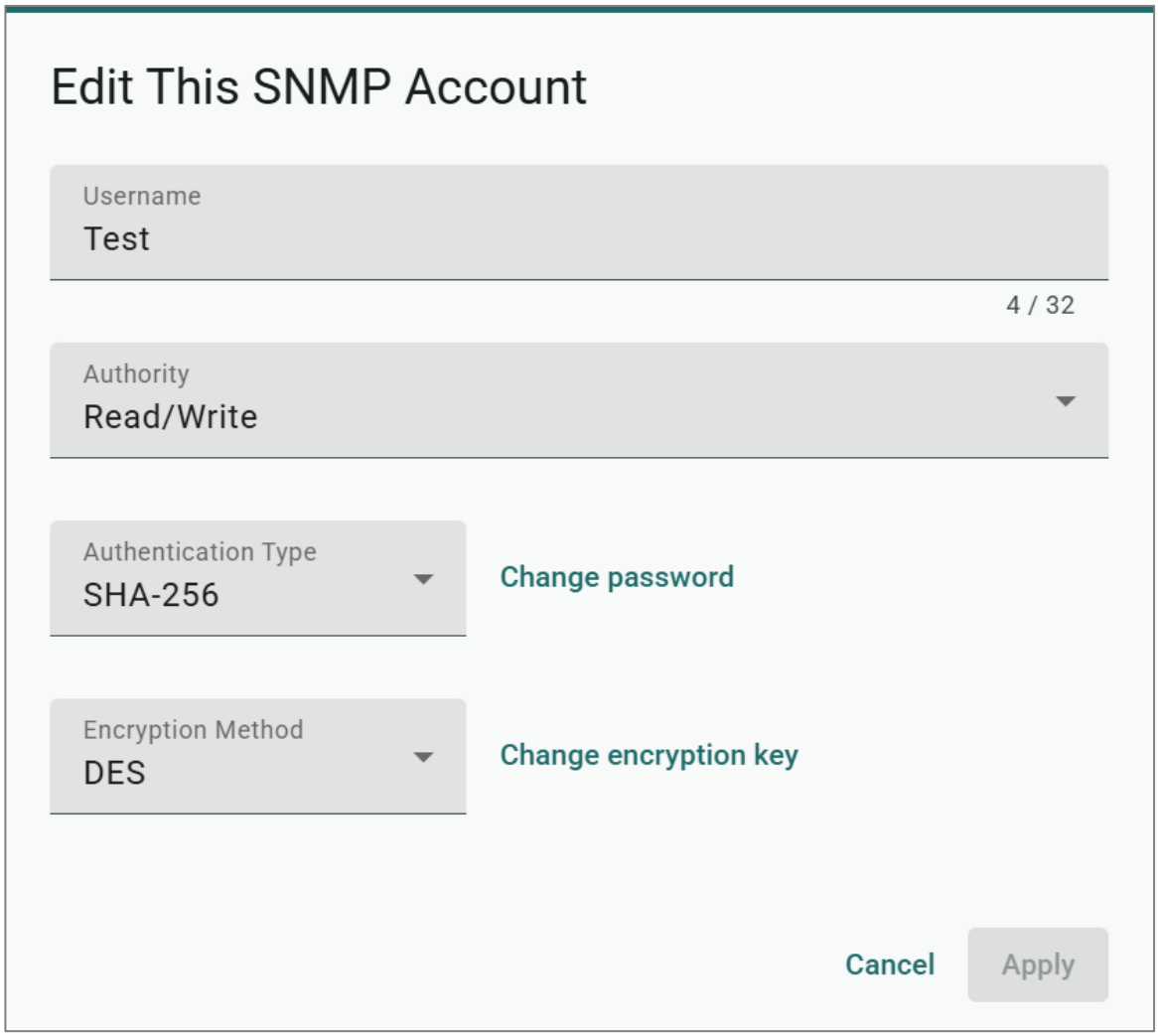
Menu Path: System > Management Interface > SNMP - SNMP Account

Clicking the **Edit (✎)** icon for an account on the **System > Management Interface > SNMP - SNMP Account** page will open this dialog box. This dialog lets you edit an existing account.

Click **Apply** to save your changes.

Click **Change password** to change the authentication password for the account.

Click **Change encryption key** to change the encryption key for the account.



UI Setting	Description	Valid Range	Default Value
Username	Specify a username for the SNMP account.	1 to 32 characters • Valid characters: a-z, A-Z, 0-9 • Valid special characters: ._-	N/A
Authority	Select the authority level of the management account. • **Read/Write**: Can read and write configuration settings • **Read**: Can only read configuration settings	Read/Write / Read	Read/Write
Authentication Type	Select the authentication type to use for the account.	None / MD5 / SHA / SHA-256 / SHA-512	N/A

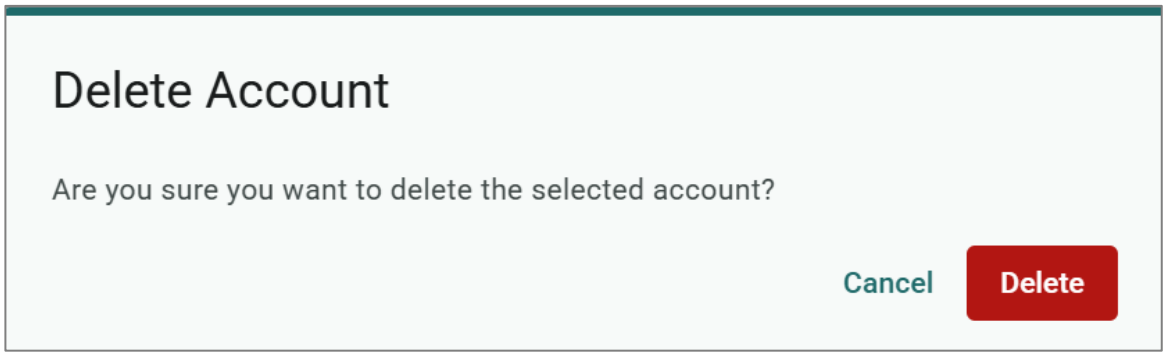
UI Setting	Description	Valid Range	Default Value
Encryption Method **(If Authentication Type is not None)**	Select the encryption method to use for the account.	Disabled / DES / AES	Disabled

Deleting an SNMP Account

Menu Path: System > Management Interface > SNMP - SNMP Account

Clicking the **Delete ( )** icon for an account on the **System > Management Interface > SNMP - SNMP Account** page will open this dialog box. This dialog lets you delete an existing account.

Click **Delete** to save your changes.



Time

Menu Path: System > Time

This page lets you configure the time related settings.

This page includes these tabs:

- System Time
- NTP Server

About System Time

Correct system time is required for automatic warning emails to include a time and date stamp.

> **Note**
>
> Make sure to update the Current Time and Current Date after the switch has been powered off for three days or more. This is particularly important when no NTP server or Internet connection are available.

This section describes how to configure the **System Time** and **NTP Server** settings for the switch. The switch has a time calibration function based on information from an NTP server or a user-specified time and date, allowing functions such as automatic warning emails to include a time and date stamp.

Configuring System Time

To configure System Time, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **System** > **Time** > **System Time**, and then click on the **Time** tab.
3. Set **Clock Source** to **Enabled**.
4. Configure the **Date**, **Time**, and **Time Zone**. Specify **Daylight Savings** details if appropriate for your region.
5. Click **Apply** to save your settings.

System Time

Menu Path: System > Time > System Time

This page lets you configure the system time.

This page includes these tabs:

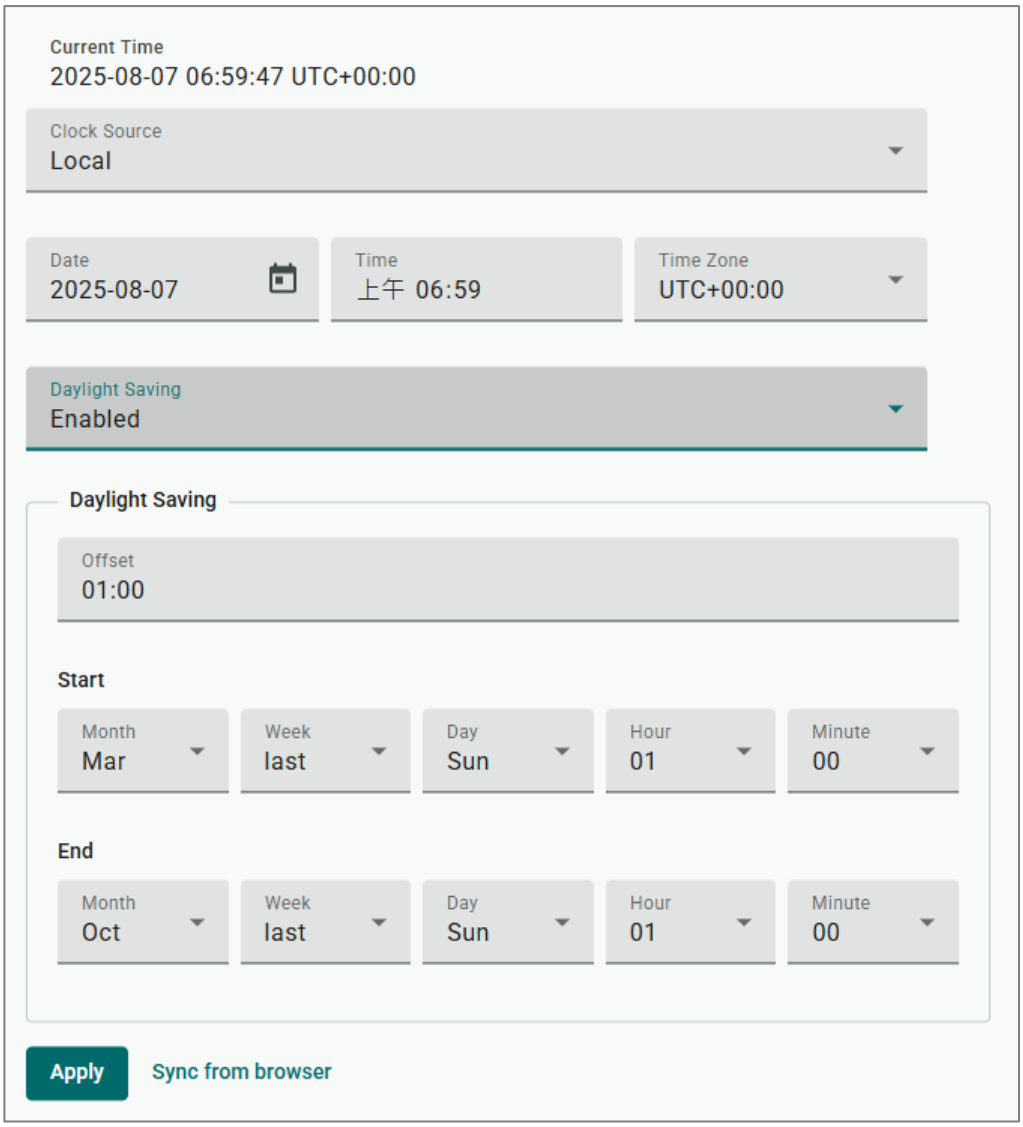
- Time
- NTP Authentication

System Time - Time

Menu Path: System > Time > System Time - Time

This page allows you to configure your device's system time by selecting a clock source or by synchronizing with your browser.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Current Time	Show the current time according to your local default settings.	N/A	N/A
Clock Source	Specify whether to set the time manually (Local), from an SNTP server, or from an NTP server.	Local / SNTP / NTP	Local
Date **(If Clock Source is Local)**	Select the current date from the calendar.	Calendar	Local Date
Time **(If Clock Source is Local)**	Specify the current time. You can manually input the time, or you can click **SYNC FROM BROWSER** to set the time based on the time used by your web browser.	Timestamp	N/A
Time Zone	Specify the time zone used for the device.	Drop-down list of time zones	UTC+00:00
1st Time Server: IP Address/Domain Name **(If Clock Source is SNTP or NTP)**	Specify the IP or domain address of the 1st SNTP/NTP server to use (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	Valid IP address or domain name	time.nist.gov
2nd Time Server: IP Address/Domain Name **(If Clock Source is SNTP or NTP)**	Specify the IP or domain address of the 2nd SNTP/NTP server to use if the first SNTP/NTP server fails to connect.	Valid IP address or domain name	N/A
Query Interval **(If Clock Source is SNTP)**	Specify the query interval time.	Drop-down list of intervals	9 (512 sec.)
Authentication **(If Clock Source is NTP)**	Select an NTP authentication key to use, or disable authentication for the time server. **Note** To use authentication, you need to create an NTP authentication entry first. Refer to NTP Authentication for more information.	Disabled / Drop-down list of NTP key IDs	Disabled

Daylight Saving

UI Setting	Description	Valid Range	Default Value
Daylight Saving	Enable or disable use of daylight saving time adjustment.	Enabled / Disabled	Disabled
Offset	Specify the number of hours and minutes to add during the daylight saving time period.	00:30 / 01:00	01:00
Start **Month/Week/Day/Hour/Minute**	Specify the start time for the daylight seaving period.	Month: Drop-down list of months Week: 1st / 2nd / 3rd / 4th / last Day: Drop-down list of days of the week Hour: Drop-down list of hours Minute: Drop-down list of minutes	Mar/last/Sun/01/00
End **Month/Week/Day/Hour/Minute**	Specify the end time of the daylight saving period.	Month: Drop-down list of months Week: 1st / 2nd / 3rd / 4th / last Day: Drop-down list of days of the week Hour: Drop-down list of hours Minute: Drop-down list of minutes	Oct/last/Sun/01/00

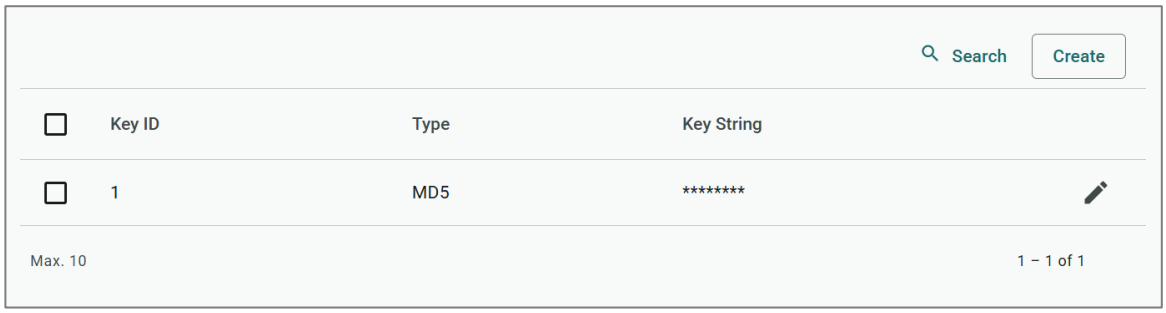
NTP Authentication

Menu Path: System > Time > System Time - NTP Authentication

This page lets you configure NTP authentication for when the device is acting as an NTP client. This helps ensure that received NTP responses are from the NTP server and have not been modified in transit.

Limitations

You can create up to 10 NTP authentication entries.



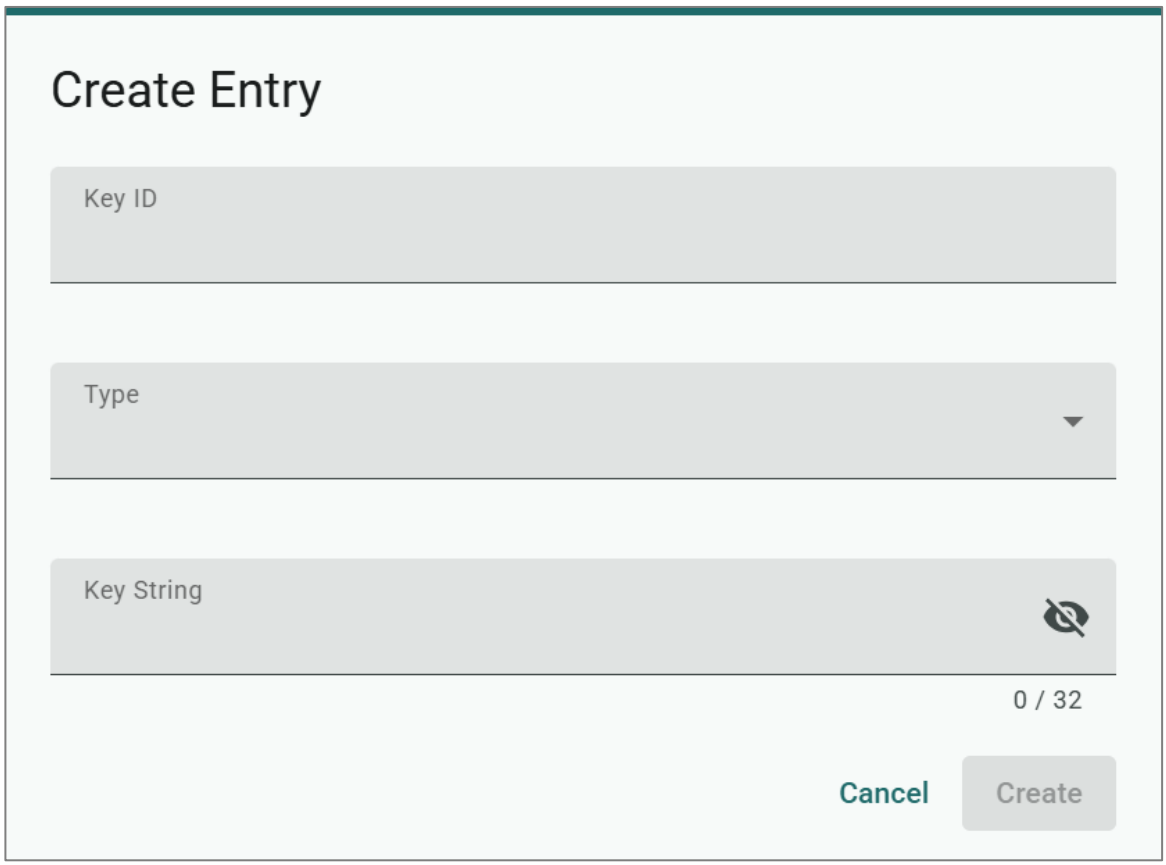
UI Setting	Description
Key ID	Shows the key ID for NTP authentication.
Type	Shows the authentication type.
Key String	Shows the password used for authentication.

Creating an NTP Authentication Entry

Menu Path: System > Time > System Time - NTP Authentication

Clicking the **Create** button on the **System > Time > System Time - NTP Authentication** page will open this dialog box. This dialog lets you create an NTP authentication entry.

Click **Create** to save your changes and add the new account.



UI Setting	Description	Valid Range	Default Value
Key ID	Specify the Key ID to use for NTP authentication.	1 to 65535	N/A
Type	Specify the authentication type.	MD5 / AES128CMAC	N/A
Key String	Specify the password to use for the authentication key.	0 to 32 characters	N/A

About NTP Server

Network Time Protocol (NTP) is used to synchronize the clocks of computers and other devices on a network, and is widely used on the Internet and in local networks to ensure accurate timekeeping. NTP operates by exchanging time information between servers and clients.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

NTP Server In Depth

Typically, there are several hierarchical strata of NTP servers.

- **Stratum 1 servers** are directly connected to highly accurate time sources, such as atomic clocks or GPS receivers.
- **Stratum 2 servers** synchronize their time with Stratum 1 servers.
- **Client devices** synchronize their clocks with NTP servers, which helps maintain accurate time across the network.

You can configure your device to act as an NTP client to sync the system time with a specified NTP server.

You can also configure your device to act as an NTP server to provide time sync service to end devices on the network. When enabling the NTP server function, the device will answer the NTP queries sent from NTP client and provide the device's time to the client.

Configuring NTP Server

Moxa devices can serve as network time protocol (NTP) servers to allow other devices to synchronize their clocks over the network.

NTP operates by exchanging time information between servers and clients.

Typically, there are several hierarchical strata of NTP servers. Stratum 1 servers are directly connected to highly accurate time sources, such as atomic clocks or GPS receivers. Stratum 2 servers synchronize their time with Stratum 1 servers, and so on. Client devices synchronize their clocks with NTP servers, which helps maintain accurate time across the network.

NTP is widely used on the internet and in local networks to ensure accurate timekeeping, and it has been a critical component of network infrastructure for decades.

Our switch can act as NTP client to sync the system time with the configured NTP server (Stratum 1). Our switch can also act as an NTP server (Stratum 2) to propagate the synchronized time to other clients on the network.

Enabling NTP Server

1. Sign in to the device using administrator credentials.
2. Go to **System** > **Time** > **NTP Server**.
3. Set **NTP Server** to **Enabled**.
4. To Enable Client Authentication and create keys, do the following:
5. Set **Client Authentication** to **Enabled**.
6. Go to **System** > **Time** > **System Time** > **NTP Authentication**, and then click **Add**.

   The **Create Entry** screen appears.
7. Key ID Type Key String Configure all of the following, and then click **Create**:

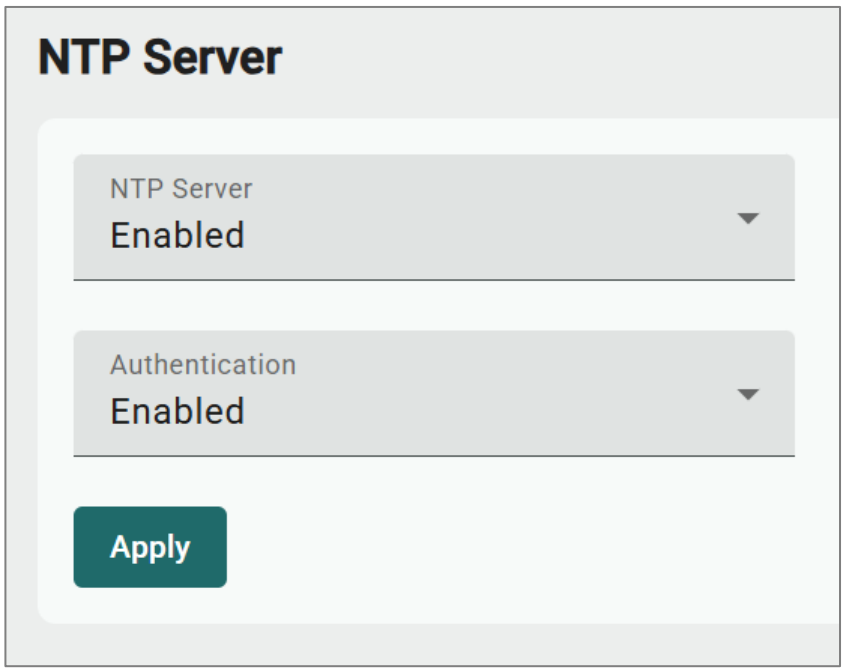
Option	Value
Key ID	Specify a number to identify the key
Type	Specify the authentication type.
Key String	Specify a key at least one character long.

NTP Server

Menu Path: System > Time > NTP Server

This page lets you configure your device to act as an NTP server.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
NTP Server	Enable or disable the NTP server.	Enabled / Disabled	Disabled
Authentication	Enable or disable NTP client authentication.	Enabled / Disabled	Disabled

Provisioning

Menu Path: Provisioning

This section lets you manage provisioning for your device.

This section includes these pages:

- Auto Configuration

Provisioning - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to System > Account Management > User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Auto Configuration	R/W	R/W	R

About Auto Configuration

This is a Moxa-proprietary feature that enables zero-touch deployment and configuration management for network devices. It leverages the Dynamic Host Configuration Protocol (DHCP) service to automate the provisioning process during device boot-up.

Benefits of Auto Configuration include:

- **Reduced Manual Work:** Eliminates the need to manually configure each device individually, saving significant time and effort.
- **Faster Deployment:** Streamlines the configuration process for quicker network setup, especially for large deployments.

Auto Configuration In Depth

Auto Configuration can be broken down into several distinct stages. Here's a breakdown of the key stages.

Stage 1: Device Initialization

- The device boots up and acquires an IP address from the DHCP server.

Stage 2: DHCP Server Guidance

- The DHCP server transmits crucial information to the device using DHCP options:
    - **Option 66:** Specifies the address of the file server where the configuration files are stored.
    - **Option 67:** Identifies the specific configuration file on the file server that the device should download.

Stage 3: Retrieving and Applying the Configuration

- Based on the information received from the DHCP options, the device contacts the file server to request the specified configuration file.
- If a matching configuration file is found, the device downloads it from the file server and automatically applies the settings.

Once the configuration is imported, Auto Configuration is complete.

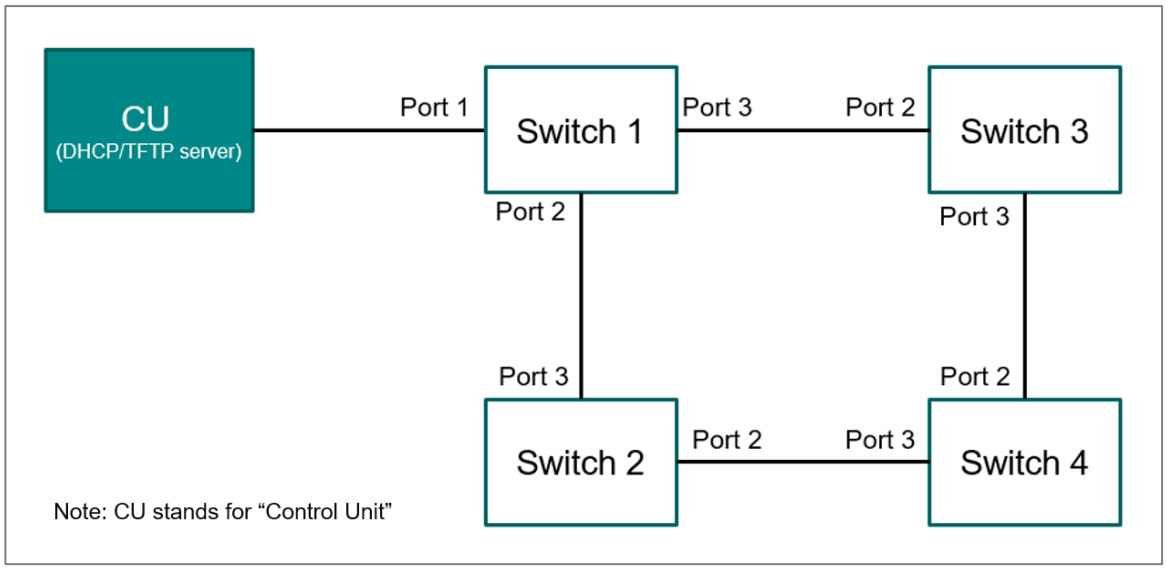
> **Note**
>
> The process of Auto Configuration uses DHCP Option 61 Client-Identifier and LLDP information to determine who should offer the IP and related configuration. The device sends DHCP discover/request packets with Option 61 only through the control unit port connected to the DHCP/file server. DHCP discover/request packets sent through other ports will not contain Option 61.

With Auto Configuration, you can set up larger networks with multiple switches, connect the server to a ring network, and have the switches get the corresponding configuration and be automatically configured one by one.

Here is an example of 4 switches connected in a ring and 1 server with DHCP and file transfer functionality.

Note

Please make sure the initial network is loop-free by opening a ring or using a configuration with ring protocol enabled. Here, we suggest using Turbo Ring v2 as a redundant protocol. Refer to Redundancy for more information.



Step 1: Auto Configuration on Switch 1

- After device initialization, switch 1 will follow the auto configuration stages to retrieve and apply the corresponding configuration file.

Step 2: Auto Configuration on Switch 2 and 3

- After Switch 1 applies the configuration successfully, the switch can be configured as a DHCP server to give Switch 2 and Switch 3 offers.
- Switch 2 and 3 will follow the Auto Configuration stages to retrieve and apply the configuration.

Note

Currently, setting up a DHCP server with Option 66 and 67 is not supported on MX-NOS switches. They will automatically propagate the Option 66 value from the server and use an offered IP address as Option 67. Therefore, please make sure the configuration filenames for the switches match and are stored in the corresponding file server.

Step 3: Auto Configuration on Switch 4

- After Switch 2 finishes, it can be configured as a DHCP server to provide an offer to Switch 4.

Here are tips for network design and configuration preparation for Moxa network devices:

1. To have a better zero-touch and massive deployment, using a **custom default** configuration is useful. With a custom default, the switches can have the same default configuration with Auto Configuration enabled, and with the same redundant protocol and VLAN settings. Once the switches reboot, the devices will start get the configuration automatically. Please refer to Deploying Multiple Devices Using Auto Configuration or Maintenance and Tools for more information.
2. There can be multiple file servers in a network for faster file transfers and load balancing.
3. To avoid conflicting offers, please make sure each device will only get their offer from a single source. Please refer to the DHCP server settings for port-based offers.
4. The amount of time needed for the Auto Configuration process depends on the size of the network, file transfer time, and LLDP/DHCP timer.

Auto Configuration

Menu Path: Provisioning > Auto Configuration

This page lets you manage the Auto Configuration feature for your device.

This page includes these tabs:

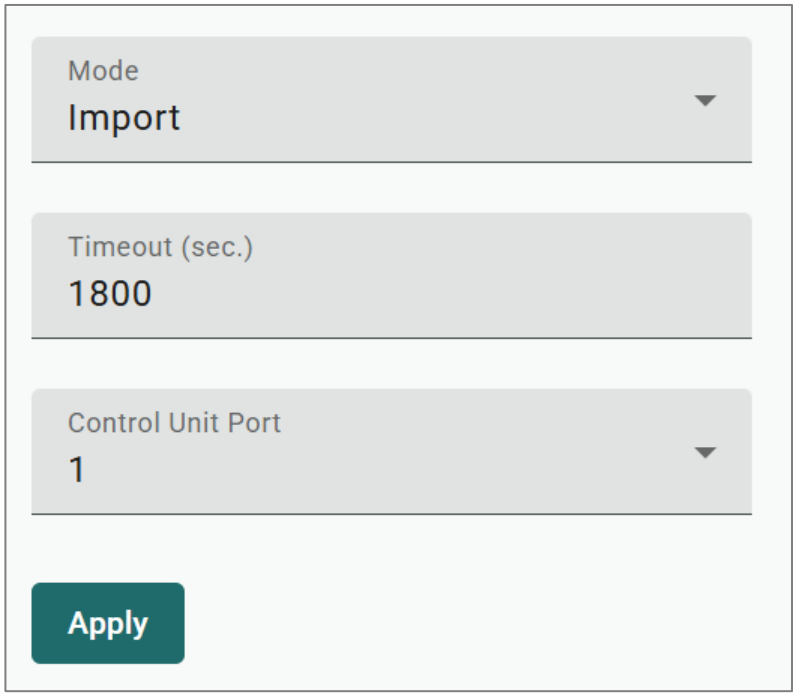
- Settings
- Status

Auto Configuration Settings

Menu Path: Provisioning > Auto Configuration - Settings

This page lets you configure your device's Auto Configuration settings.

Click **Apply** to save your changes.

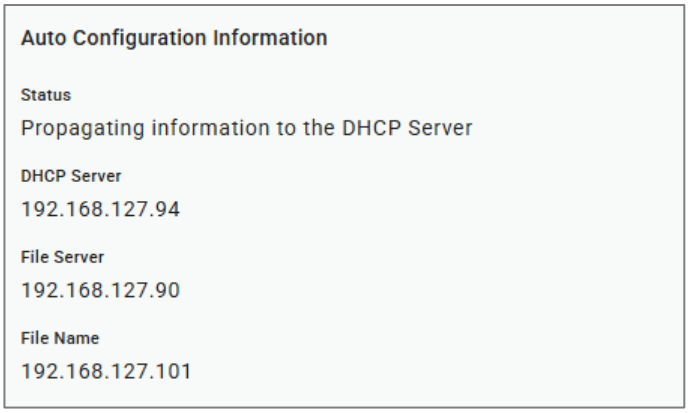


UI Setting	Description	Valid Range	Default Value
Mode	Select the operational mode to use. **Disabled**: Auto Configuration will be disabled. **Import**: In this mode, Auto Configuration only sends Option 61 packets over the control unit port. This requires DHCP Client to be enabled, and the boot file and client ID must be preconfigured in IP Configuration. **Propagate**: In this mode, the DHCP server assigns IP addresses based on LLDP information. This requires IP Configuration to be set to manual and LLDP to be enabled.	Disabled / Import / Propagate	Disabled
Timeout **(If Mode is Import)**	Specify the Auto Configuration timeout value in seconds. This parameter defines the maximum time (in seconds) your device will wait for a DHCP offer during the bootup process. If the device fails to receive a DHCP offer within the specified timeout period, the Automatic Configuration process ceases. A log message is recorded to indicate this event for troubleshooting purposes. **Note** The overall duration of the Auto Configuration process can be influenced by various factors, including the network size, file transfer times, and other network-related conditions.	1 - 3600	1800 sec.
Control Unit Port	Select the control unit port from the drop-down list. This is the port that connects to the DHCP/file server.	Drop-down list of ports	1

Auto Configuration Status

Menu Path: Provisioning > Auto Configuration - Settings

This page lets you view your device's auto configuration status.



UI Setting	Description
Status	Shows the current status of Auto Configuration. The status may be one of the following: • Auto Configuration process started • Received IP address • Downloaded the configuration • Imported the configuration • Propagating information to the DHCP Server • Auto Configuration is disabled • Insufficient information to propagate • Auto Configuration timed out • Failed to download the configuration • Failed to import the configuration • Auto Configuration will be triggered after the reboot
DHCP Server	Shows the server information if the device successfully receives an offer from a DHCP server.
File Server	Shows the file server information retrieved from a DHCP Option 66 offer.
File Name	Shows the file name information retrieved from a DHCP Option 67 offer.

Port

Menu Path: Port

This section lets you configure various port-specific functions for the switch.

This section includes these pages:

- Port Interface
- Link Aggregation
- PoE

Port - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to System > Account Management > User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Port Interface			
Port Settings	R/W	R/W	R
Linkup Delay	R/W	R/W	R
Link Aggregation	R/W	R/W	R
PoE	R/W	R/W	R

Port Interface

Menu Path: Port > Port Interface

This section lets you configure the port interface functions.

This section includes these pages:

- Port Settings

- Linkup Delay

About Port Settings

Port Settings allows you to manage and configure the various parameters of your device's individual network ports. By letting you adjust settings such as speed, duplex, and flow control, it helps you optimize the performance of your network connections.

Port Settings

Menu Path: Port > Port Interface > Port Settings

This page lets you configure the port settings.

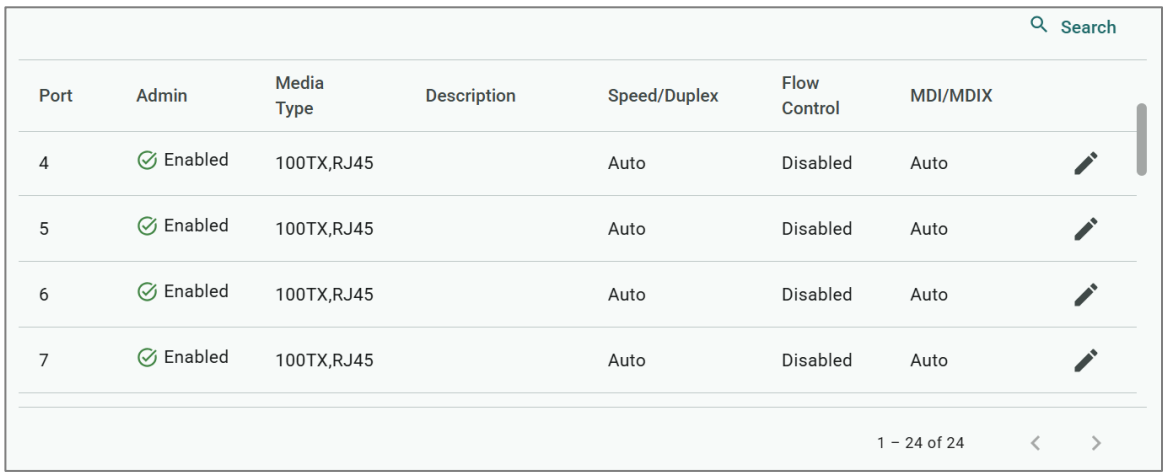
This page includes these tabs:

- Settings
- Status

Port Settings - Settings

Menu Path: Port > Port Interface > Port Settings - Settings

This page lets you configure basic port settings.



UI Setting	Description
Port	Shows which port the entry describes.

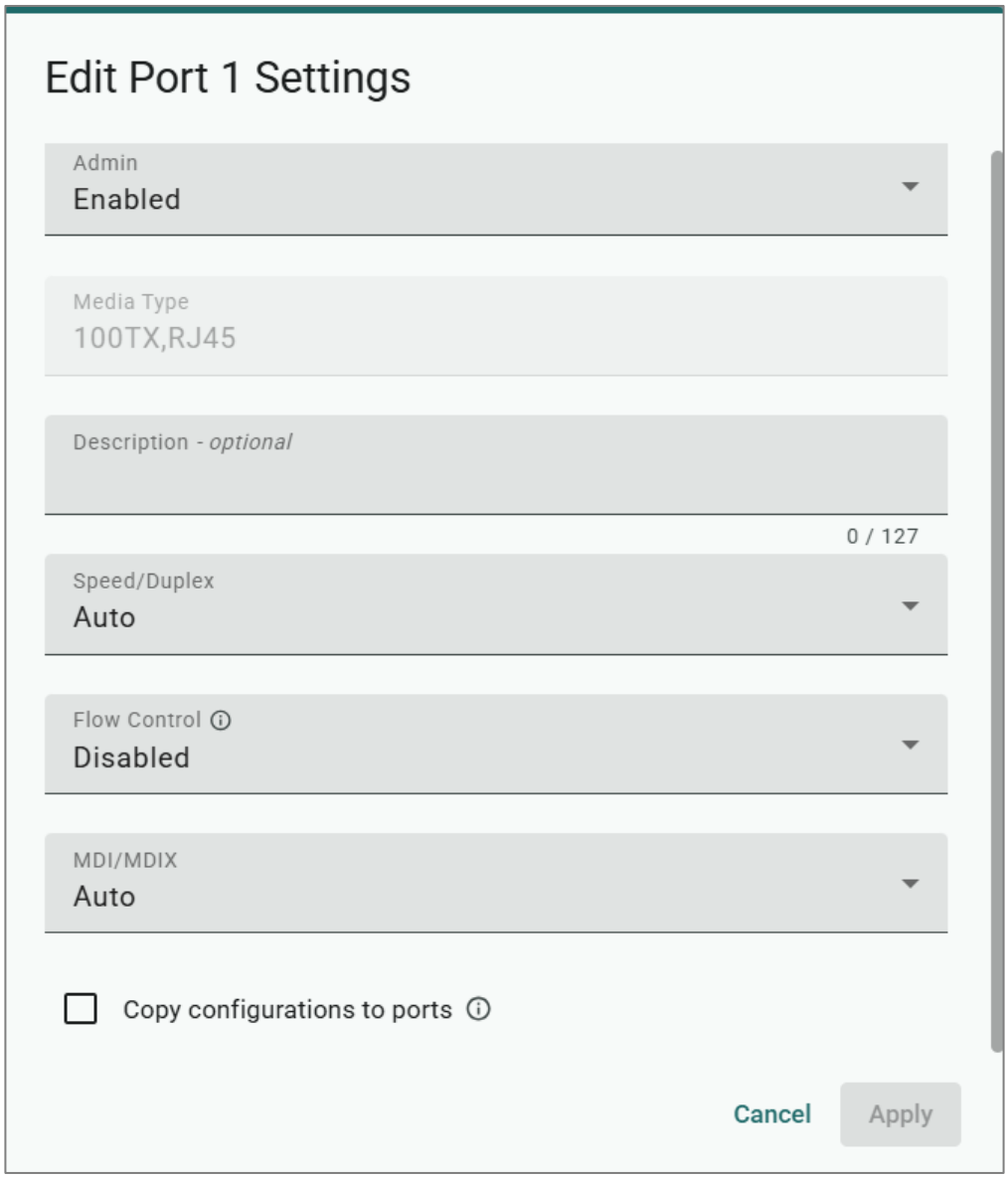
UI Setting	Description
Admin Status	Shows whether admin status is enabled for data transmission through the port.
Media Type	Shows the detected media type for the port.
Description	Shows the description used to help identify the port.
Speed/Duplex	Shows the port speed and duplex option selected for the port.
Flow Control	Shows whether flow control is enabled for the port.
MDI/MDIX	Shows the MDI/MDIX option used for the port.

Editing Port Settings

Menu Path: Port > Port Interface > Port Settings - Settings

Clicking the **Edit (✎)** icon for the desired port on the **Port > Port Interface > Port Settings - Settings** page will open this dialog box. This dialog lets you configure the port settings parameters.

Click **Apply** to save your changes.



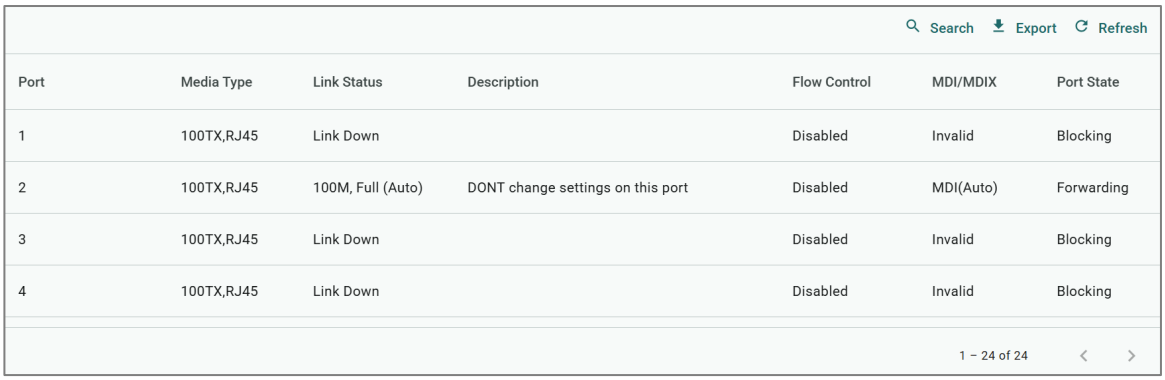
UI Setting	Description	Valid Range	Default Value
Admin	Enable or disable data transmission through the port.	Enabled / Disabled	Enabled
Media Type	Displays the detected media type for each port. This setting cannot be changed.	Detected media type	N/A
Description	Specify a description to help identify the port.	0 to 127 characters	N/A

UI Setting	Description	Valid Range	Default Value
Speed/Duplex	Select the speed/duplex mode to use for the port. Select **Auto** to enable the port to negotiate the optimal speed using the IEEE 802.3u protocol with connected devices. The port and connected devices will determine the most suitable speed for the connection. Alternatively, choose a fixed speed and duplex option if the connected Ethernet device has trouble with auto-negotiation. This can be useful for connecting legacy devices without auto-negotiation support. **Note** Speed/Duplex cannot be set for fiber ports.	Auto / 10M Half / 10M Full / 100M Half / 100M Full	Auto
Flow Control	Enable or disable flow control for the port. **Note** The switch and connected device will automatically determine the final result. **Note** Flow control can be enabled/disabled, but it is only effective at full duplex. Back pressure can be enabled/disabled, but it is only effective at half duplex.	Enabled / Disabled	Disabled
MDI/MDIX	Select the MDI/MDIX mode to use for the port. Select **Auto** to allow the port to auto-detect the port type of the connected Ethernet device, and change the port type accordingly. Alternatively, manually select **MDI** or **MDIX** if the device has trouble auto-detecting the port type. **Note** MDI/MDIX cannot be set for fiber ports.	Auto / MDI / MDIX	Auto
Copy configurations to ports	Select the ports you want to copy this configuration to. **Note** The copy configuration feature cannot be used with fiber ports.	Drop-down list of ports	N/A

Port Settings - Status

Menu Path: Port > Port Interface > Port Settings - Status

This page lets you view the status and configuration of the device's ports.



UI Setting	Description
Port	Shows the port index.
Media Type	Shows the detected media type for the port.
Link Status	Shows the port's link status. **Link Down** will be shown If the link is down. Otherwise, the port's speed and duplex will be shown.
Description	Shows the description used to help identify the port.
Flow Control	Shows whether flow control is enabled for the port.
MDI/MDIX	Shows the MDI/MDIX option used for the port.
Port State	Shows whether the port status is blocking or forwarding.

About Linkup Delay

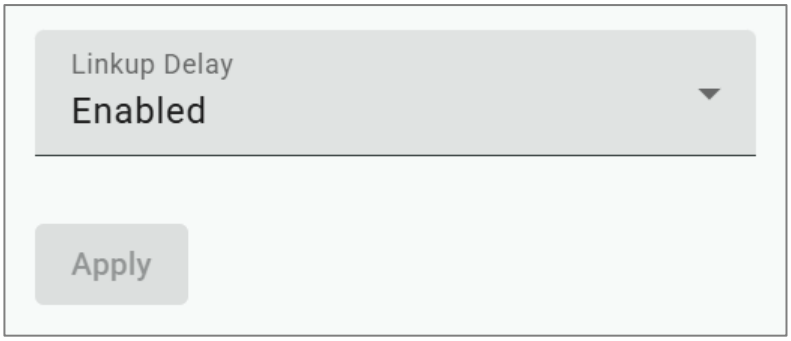
Linkup delay, also known as link flap prevention, is used to prevent a port alternating between link up and link down statuses, and is useful when a link connection is unstable. An unstable connection might be caused by situations such as a faulty cable, faulty fiber transceiver, duplex mismatch, etc. Linkup delay helps you mitigate the risk of an unstable network, particularly when the topology changes frequently.

Linkup Delay

Menu Path: Port > Port Interface > Linkup Delay

This page lets you configure the linkup delay for device's ports.

Linkup Delay Settings



UI Setting	Description	Valid Range	Default Value
Linkup Delay	Enable or disable the linkup delay feature for the device. **Note** After enabling linkup delay, you will still need to configure and enable linkup delay for each port you want to use it on. Refer to Linkup Delay - Edit Port Settings for more information.	Enabled / Disabled	Enabled

Linkup Delay - Port List

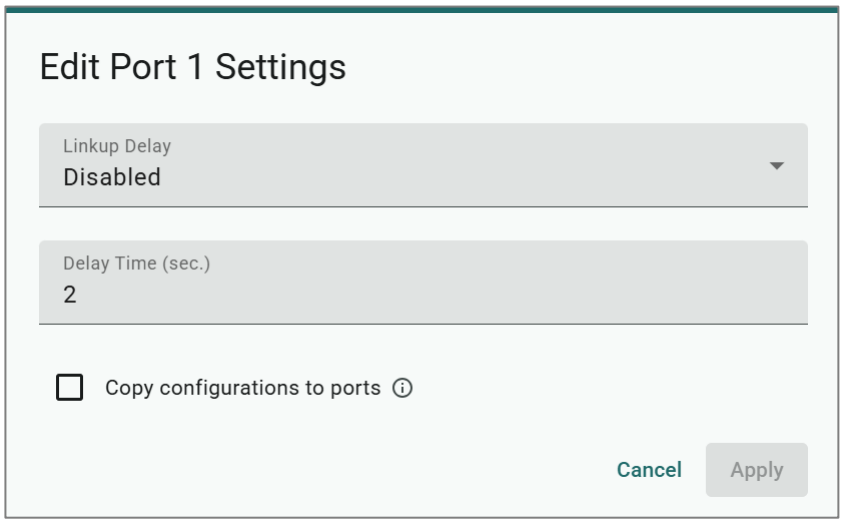
UI Setting	Description
Port	Shows the port index.
Status	Shows whether linkup delay is enabled or disabled for the port. **Note** To enable linkup delay for a port, both the linkup delay setting for the port and the global linkup delay setting must be enabled. Refer to Linkup Delay Settings for more information.
Delay Time	Shows the delay time in seconds for the port.
Remaining Time	Shows the remaining time in seconds for the port to alternate between link up and link down.

Linkup Delay - Edit Port Settings

Menu Path: Port > Port Interface > Linkup Delay

To configure linkup delay for a port, click the **Edit (✎)** icon on the desired port on the **Port > Port Interface > Linkup Delay** page will open this dialog box. This dialog lets you configure the linkup delay parameters for the port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Linkup Delay	Enable or disable linkup delay for the port. **Note** To enable linkup delay for a port, both the linkup delay setting for the port and the global linkup delay setting must be enabled. Refer to Linkup Delay Settings for more information.	Enabled / Disabled	Disabled
Delay Time	Specify the delay time in seconds before the port alternates between link up and link down.	1 to 1000	2
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

About Link Aggregation

Link aggregation, also known as port channels or port trunking, helps balance, optimize, and facilitate a device's throughput. This method combines multiple network communication interfaces 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, bandwidth-efficient data communication route. This can improve network load sharing and increase network reliability.

Static Trunk

For some networking applications, a situation can arise where traffic from multiple ports is required to be filtered through a single port. For example, if there are 30 UHD IP surveillance cameras deployed and connected in a ring, traffic can reach up to 1 Gbps, causing a surge in traffic that can increase network loading by up to 50%. Hence, the uplink port needs to use static trunking to provide additional bandwidth and redundancy protection.

LACP

Link Aggregation Control Protocol (LACP) is a protocol defined by IEEE 802.3ad that allows a network device to negotiate automatic bundling of several ports by sending LACP packets to the peer, a directly connected device that also uses LACP.

Link Aggregation Algorithms

In link aggregation, three load-sharing hash algorithms can be used to optimize packet forwarding:

- **SMAC:** Source MAC (SMAC) uses the source MAC address for a packet to optimize packet forwarding to ensure that packets from the same source address follow the same path consistently to optimize connection stability and reduce the chance of out-of-order packet delivery.
- **DMAC:** Destination MAC (DMAC) uses the destination MAC address for a packet to optimize packet forwarding to ensure that packets being sent to the same destination address are consistently sent over the same link to optimize connection stability and traffic distribution.
- **SMAC + DMAC:** SMAC and DMAC can be used together for more complex hash algorithms, but tends to be used only when a network has few clients and servers.

Link Aggregation Settings

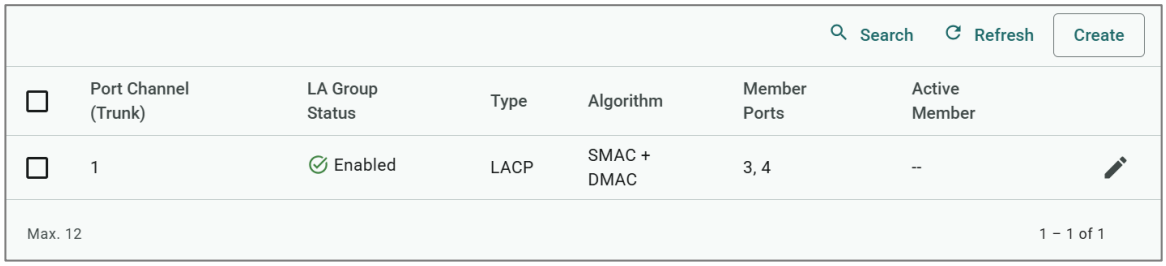
Menu Path: Port > Link Aggregation

This page lets you configure link aggregation groups for each port. A link aggregation group combines multiple physical ports into a single logical link.

Limitations

The maximum number of Link Aggregation groups is half of the device's total number of ports. For example, users can create up to 12 link aggregation groups on the 24-port model.

Link Aggregation List



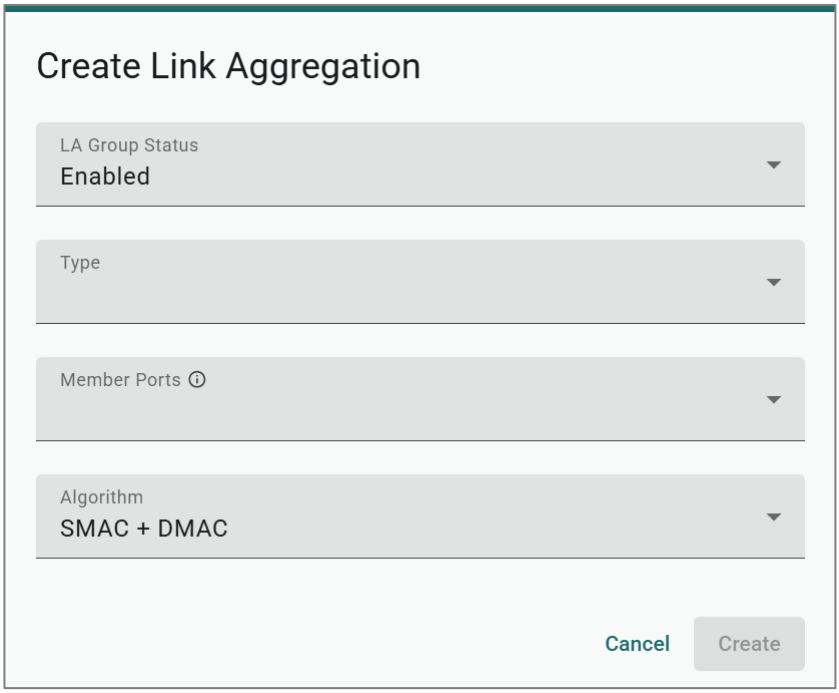
UI Setting	Description
Port Channel (Trunk)	Shows the Port Channel (Trunk) number of the link aggregation group.
LA Group Status	Shows whether the link aggregation group is enabled.
Type	Shows the method for configuring the link aggregation group.
Algorithm **(Only in Advanced Mode)**	Shows the load-sharing hash algorithms being used for the link aggregation group.
Member Ports	Shows the configured member ports in the link aggregation group.
Active Member	Shows the active member ports in the link aggregation group.

Creating a Link Aggregation Group

Menu Path: Port > Link Aggregation

Clicking the **Create** button on the **Port > Link Aggregation** page will open this dialog box. This dialog lets you create a link aggregation group.

Click **Create** to save your changes and add the new link aggregation group.



UI Setting	Description	Valid Range	Default Value
LA Group Status	Enable or disable the link aggregation group.	Enabled / Disabled	Enabled
Type	Select the method to use for configuring the link aggregation group. **Manual**: This allows you to specify the ports to be included in the LA Group. **LACP**: LACP protocol will be used to automatically negotiate link aggregation configuration between devices.	Manual / LACP	N/A
Member Ports	Select the ports to add to the link aggregation group. **Note** A port cannot be assigned to multiple link aggregation groups. This is because each port can only be a member of a single link aggregation group at a time. A link aggregation group (Port-channel) cannot be created when selected ports are operating at different speeds.	Drop-down list of ports	N/A

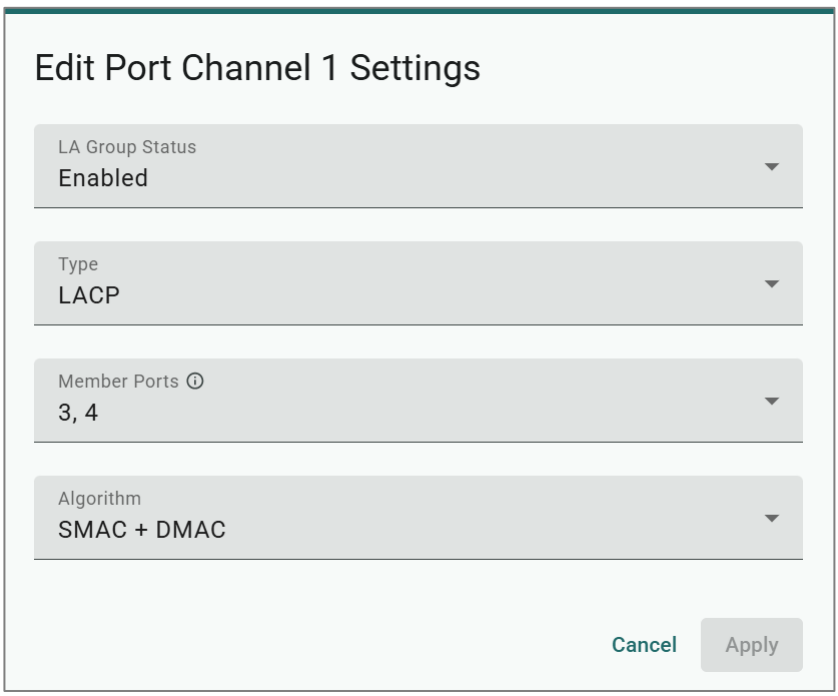
UI Setting	Description	Valid Range	Default Value
Algorithm **(Only in Advanced Mode)**	Select the load-sharing hash algorithms to be used for configuring link aggregation.	SMAC / DMAC / SMAC+DMAC	SMAC+DMAC

Editing a Link Aggregation Group

Menu Path: Port > Link Aggregation

Clicking the **Edit (✎)** icon for an entry in the Link Aggregation List on the **Port > Link Aggregation** page will open this dialog box. This dialog lets you edit Link Aggregation group settings.

Click **Apply** to save your changes.



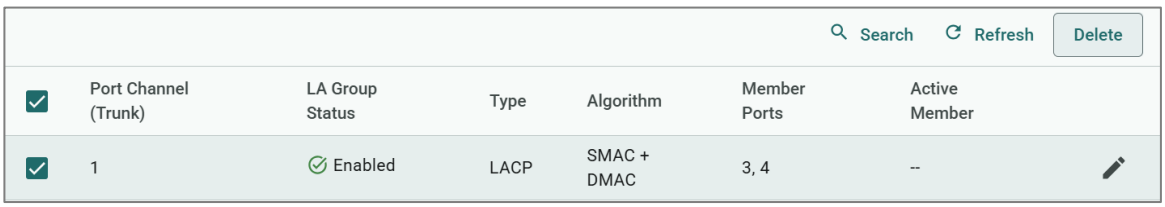
UI Setting	Description	Valid Range	Default Value
LA Group Status	Enable or disable the link aggregation group.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Type	Select the method to use for configuring the link aggregation group. **Manual**: This allows you to specify the ports to be included in the LA Group. **LACP**: LACP protocol will be used to automatically negotiate link aggregation configuration between devices.	Manual / LACP	N/A
Member Ports	Select the ports to add to the link aggregation group. **Note** A port cannot be assigned to multiple link aggregation groups. This is because each port can only be a member of a single link aggregation group at a time. A link aggregation group (Port-channel) cannot be created when selected ports are operating at different speeds.	Drop-down list of ports	N/A
Algorithm **(Only in Advanced Mode)**	Select the load-sharing hash algorithms to be used for configuring link aggregation.	SMAC / DMAC / SMAC+DMAC	SMAC+DMAC

Deleting a Link Aggregation Group (Port Channel)

Menu Path: Port > Link Aggregation

You can delete a link aggregation group by using the checkboxes to select the entries you want to delete, then clicking the **Delete** button.



Link Aggregation Port List

This table lets you see the LACP settings for each port.

Note

This appears only in Advanced Mode.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

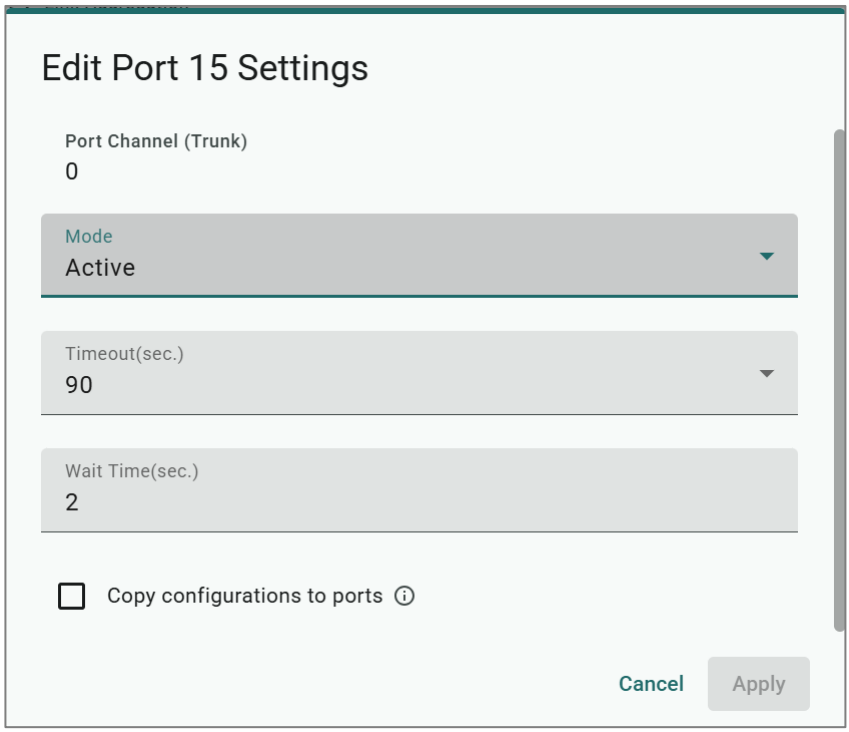
UI Setting	Description
Port	Shows which port the entry describes.
Mode	Shows the LACP mode for the port.
Timeout (sec.)	Shows the LACP inactivity timeout in seconds for the port.
Wait Time (sec.)	Shows the LACP wait time in seconds for the port.
Port Channel (Trunk)	Shows the link aggregation group (Port channel) number for the port.

Editing LACP Port Settings

Menu Path: Port > Link Aggregation

Clicking the **Edit (✎)** icon by a port on the **Port > Link Aggregation** page will open this dialog box. This dialog lets you edit the port settings for LACP parameters if your link aggregation type is set to LACP.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Port Channel (Trunk)	Shows the link aggregation group (Port channel) number of the port. This setting cannot be changed.	Port Channel Number	N/A
Mode	Select the LACP mode to decide how the ports establish LACP links. • **Active**: Ports will actively query link partners for LACP by sending LACP PDUs. If the partner is also LACP-enabled, the ports will establish an LACP link. • **Passive**: Ports can respond to LACP queries from active ports and passively establish LACP links. They will not initiate any LACP negotiation on their own. **Note** For LACP to establish a link, at least one port for the link must use active mode. If both ports are passive, no LACP PDUs will be sent, and no link will be established.	Active / Passive	Active

UI Setting	Description	Valid Range	Default Value
Timeout	Specify the LACP inactivity timeout in seconds. This is the amount of time that must elapse without receiving any LACP PDUs before a link is considered to have failed.	3 / 90	90
Wait Time	Specify the LACP wait time in seconds. This is the amount of time that must elapse after a LACP link comes up before it is added to the link aggregation group.	0 to 10	2
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

PoE

Power over Ethernet (PoE) provides power along with network connectivity to PoE network devices (PDs), allowing them to be powered and connected to the network using a single network cable. This can greatly simplify installation, maintenance, and troubleshooting of these PoE devices, especially when they are installed in areas that are difficult to reach or do not have power outlets nearby.

PoE is frequently used with a variety of devices:

- Surveillance cameras
- Security I/O sensors
- Industrial wireless access points
- Emergency IP phones

Moxa devices also support the high-power PoE+ standard and advanced PoE management functions such as PD failure check, legacy PD detection, and auto power cutting. These work together to provide critical security systems with a convenient and reliable Ethernet network that is easier to manage.

PoE Settings

Menu Path: Port > PoE

This page lets you configure your device's Power over Ethernet (PoE) settings. PoE allows your Moxa device to power other connected PoE Ethernet devices—such as security cameras, wireless access points, and sensors—through the Ethernet cable.

This page includes these tabs:

- General
- PD Failure Check
- Scheduling
- Status

Note

PoE functionality is only available on specific PoE-enabled Moxa device models. Connected PoE devices must support the IEEE 802.3af/at standard in order to use this feature.

Limitations

Only PoE Type 1 (802.3af) and Type 2 (802.3at) are supported, with a maximum of Class 4 and 30 W per port.

PoE - General

Menu Path: Port > PoE - General

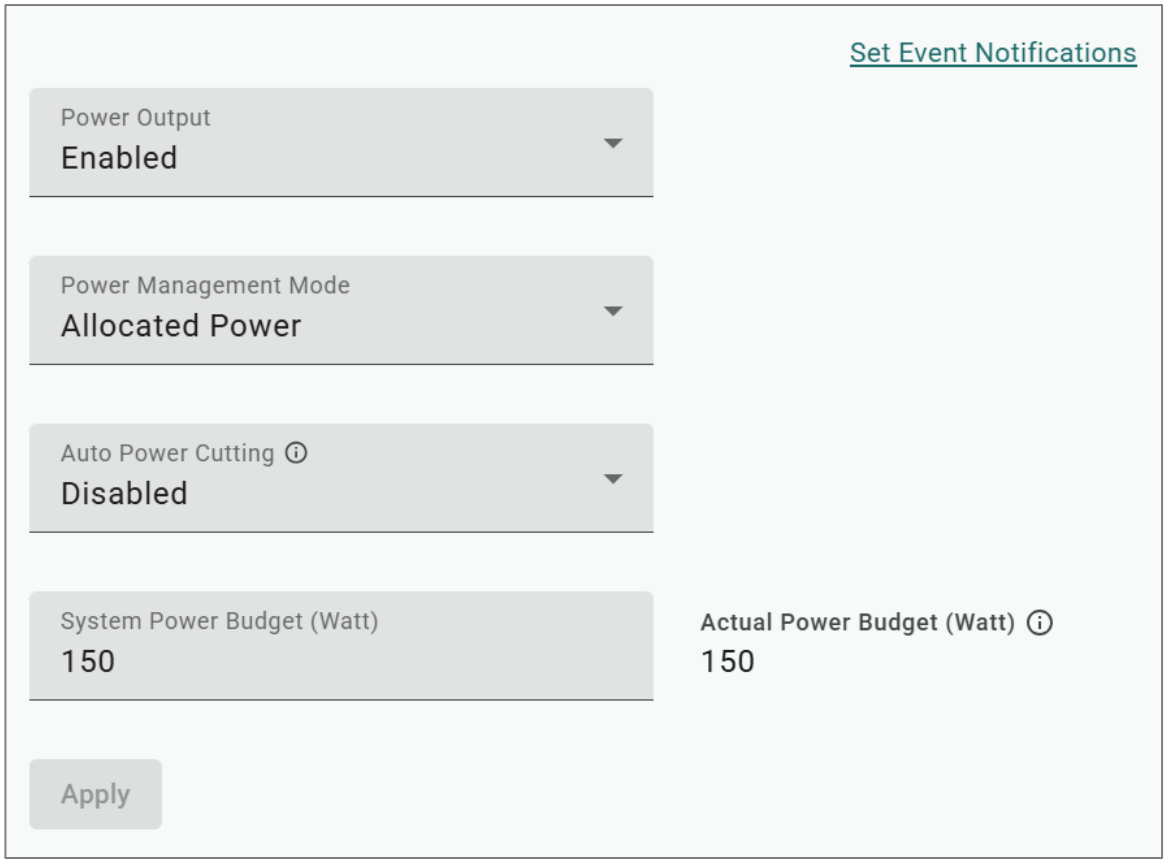
This page lets you enable PoE power output and configure system-level PoE settings.

Note

When the PoE function is activated, PoE-enabled ports should only be connected to standard/legacy powered devices.

If there is a need to connect non-powered devices to a PoE-enabled port, it is recommended to disable PoE for the port to prevent unnecessary PoE detection behavior.

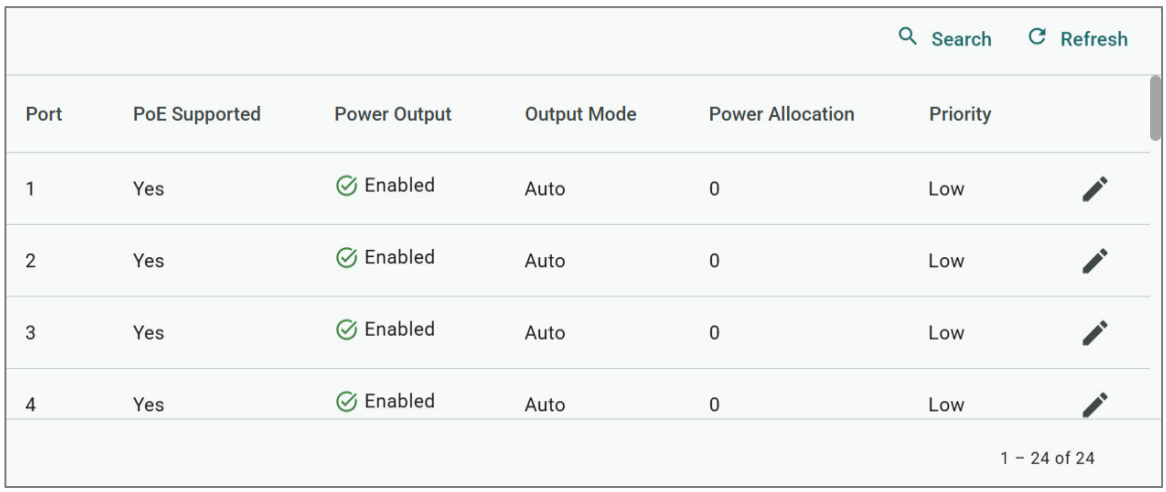
PoE Settings



UI Setting	Description	Valid Range	Default Value
Power Output	Enable or disable PoE.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Power Management Mode	Specify whether the power budget for all ports should be calculated. • **Allocated Power**: This calculates the power budget based on the Power Allocation settings of all ports. For more information on per-port power allocation, refer to PoE - Edit Port Settings. • **Consumed Power**: This calculates the power budget based on actual power consumed by all ports.	Allocated Power / Consumed Power	Allocated Power
Auto Power Cutting	Enable or disable auto power cutting, which allows PoE to be disabled for ports when total power consumption exceeds the system power budget threshold. Ports with lower priority will be disabled before ports with higher priority.	Enabled / Disabled	Disabled
System Power Budget	Specify the "total measured power" limit in watts to use for all PoE ports combined.	*(Depends on your device model)*	*(Depends on your device model)*
Actual Power Budget	Shows the system power budget in watts. This setting cannot be changed.	N/A	*(Depends on your device model)*

PoE - Port List



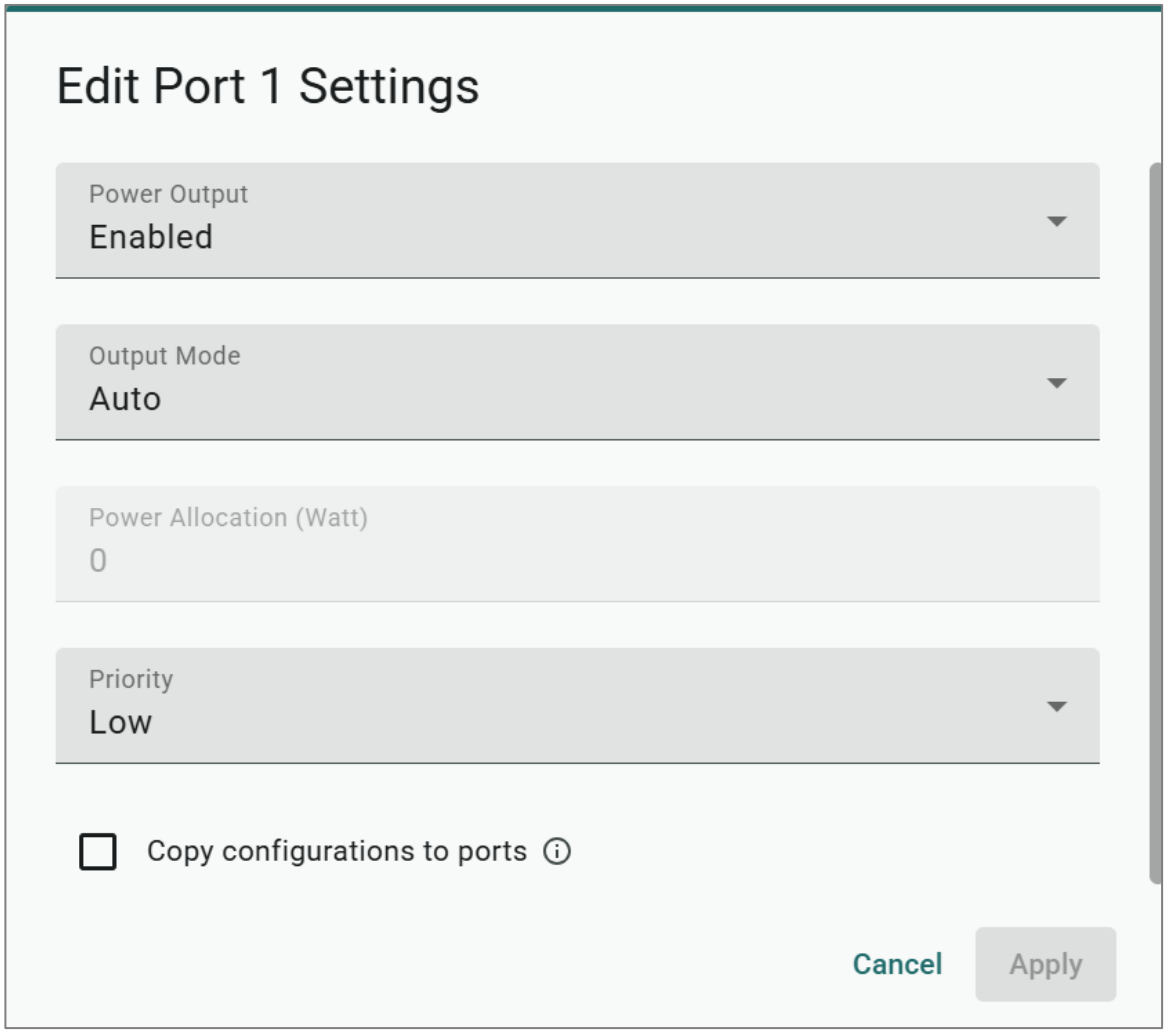
UI Setting	Description
Port	Shows which port the entry describes.
PoE Supported	Shows whether the port supports PoE.
Power Output	Shows whether PoE is enabled for the port.
Output Mode	Shows the output mode for the port. **Note** For the TN-4500B PSE chip, when Output Mode is Auto: • Devices will be classified as a Standard PD if both their resistance is 17 to 29 kΩ and their capacitance is 0 to 1 µF. • Devices will be classified as a Legacy PD if their resistance is 0.86 to 17 kΩ or 29 to 100 kΩ, or if their capacitance is 1 to 12 µF.
Power Allocation	Shows the power allocation value for the port. When the output mode is **Auto**, this value is fixed as 0.
Priority	Shows the port priority: Critical (highest) / High / Low.

PoE - Edit Port Settings

Menu Path: Port > PoE - General

Clicking the **Edit (✎)** icon for a port on the **Port > PoE - General** page will open this dialog box. This dialog lets you edit PoE settings for the port.

Click **Apply** to save your changes.



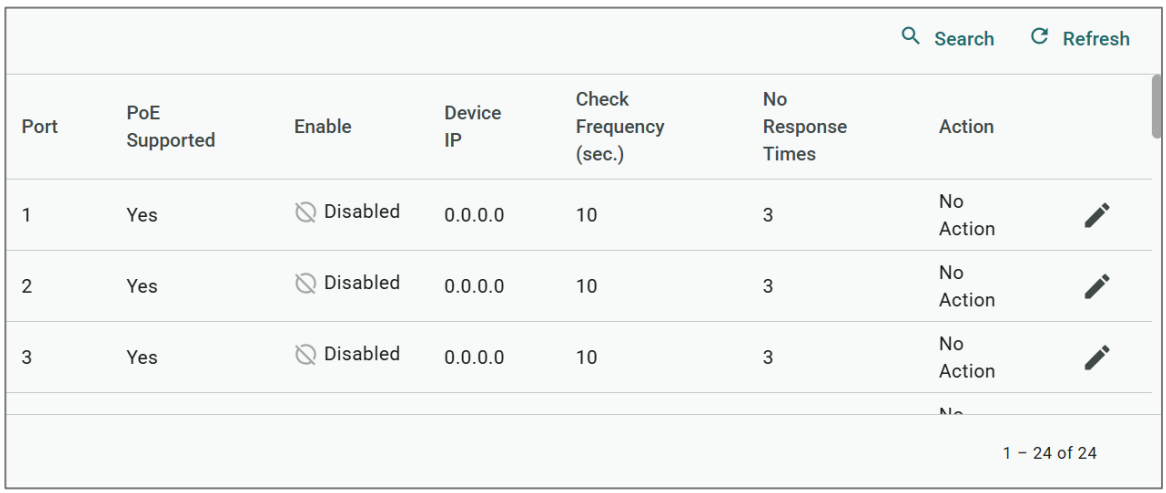
UI Setting	Description	Valid Range	Default Value
Power Output	Enable or disable PoE for this port.	Enabled / Disabled	Enabled
Output Mode	Specify whether to set the PoE output mode to Auto or Force. **Auto**: Power output will be determined by using 802.3at auto-detection. **Force**: Power output will be determined by the **Power Allocation** setting for the port. This may be necessary for PDs that do not follow 802.3af/at standards.	Auto / Force	Auto
Power Allocation (Watt)	Specify the power in watts to allocate to a connected PD when the **Output Mode** is set to **Force**. • When the output mode is **Auto**, the value is fixed as 0. • When the output mode is set to **Force**, input a value from 0 to 30.	0 to 30	N/A

UI Setting	Description	Valid Range	Default Value
Priority	Specify the priority of the port to use with the **Auto Power Cutting** feature. If Auto Power Cutting is enabled, PoE will be disabled for ports with lower priority when total power consumption exceeds the system power budget threshold. Ports with lower priority will be disabled before ports with higher priority. Refer to PoE - General for more information.	Critical / High / Low	Low
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

PD Failure Check

Menu Path: Port > PoE - PD Failure Check

This tab lets you monitor the status of a powered device (PD) through its IP address. If the PD fails, the switch will not receive a PD response after the defined period, and the PoE powering process will be restarted. This function is extremely useful for ensuring network reliability and simplifying management.



UI Setting	Description
Port	Shows which port this row describes.
PoE Supported	Shows whether the port supports PoE.
Enable	Shows whether PD failure checking is enabled or disabled for the port.

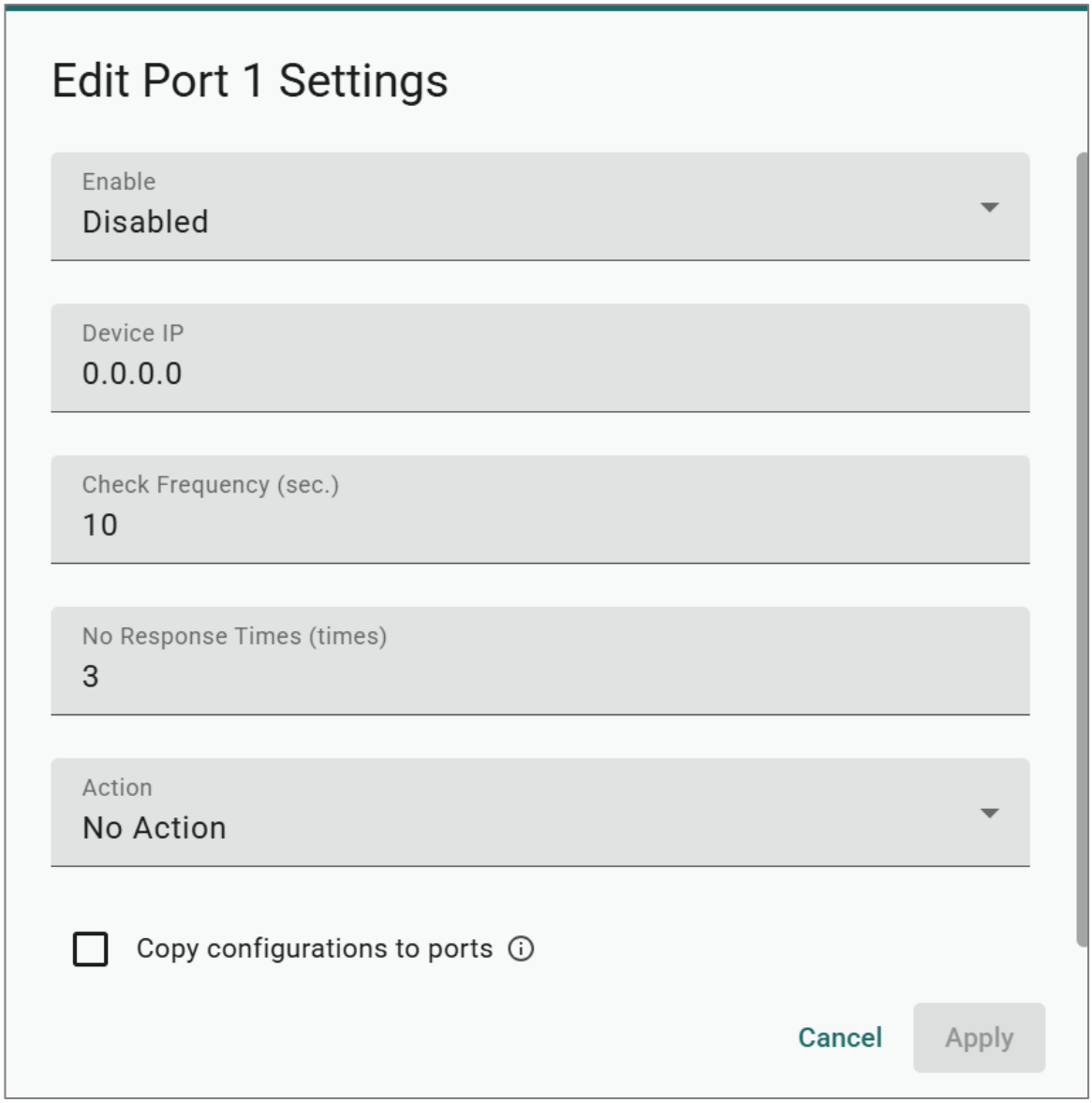
UI Setting	Description
Device IP	Shows what IP will be monitored for PD failure checking for the port.
Check Frequency (sec.)	Shows how often PD failure checks will be performed for the port.
No Response Times	Shows how many IP checking cycles will be tried before determining a PD is not responding.
Action	Shows what action will be taken if a PD failure is detected for the port.

PD Failure Check - Edit Port Settings

Menu Path: Port > PoE - PD Failure Check

Clicking the **Edit (✎)** icon for a port on the **Port > PoE - PD Failure Check** page will open this dialog box. This dialog lets you configure the PD failure check settings for the port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable PD failure checks for the port to check the status of PDs via ICMP.	Enabled / Disabled	Disabled
Device IP	Specify the IP address of the PD connected to the port to send ping packets to check for PD connection failure.	Valid IP address	0.0.0.0
Check Frequency (sec.)	Specify how frequently in seconds ping packets will be sent to to the **Device IP**. If there is no reply, a "no response" will be detected.	5 to 300	10

UI Setting	Description	Valid Range	Default Value
No Response Times (times)	Specify the number of consecutive "no response" events required to detect a PD connection failure and execute the specified **Action**.	1 to 10	3
Action	Specify the action to take when the number of **No Response Times** is reached. • **No Action**: No action will be taken. • **Restart PD**: PoE power to the PD will be stopped, then started again to restart the PD. • **Shut Down PD**: PoE power to the PD will be stopped.	No Action / Restart PD / Shut Down PD	No Action
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

PoE - Scheduling

Menu Path: Port > PoE - Scheduling

This page lets you create PoE scheduling rules that can be applied to individual ports or multiple ports.

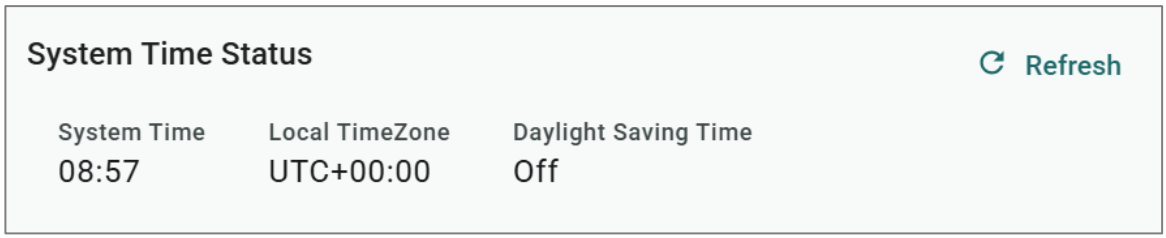
Note

This appears only in Advanced Mode.

Limitations

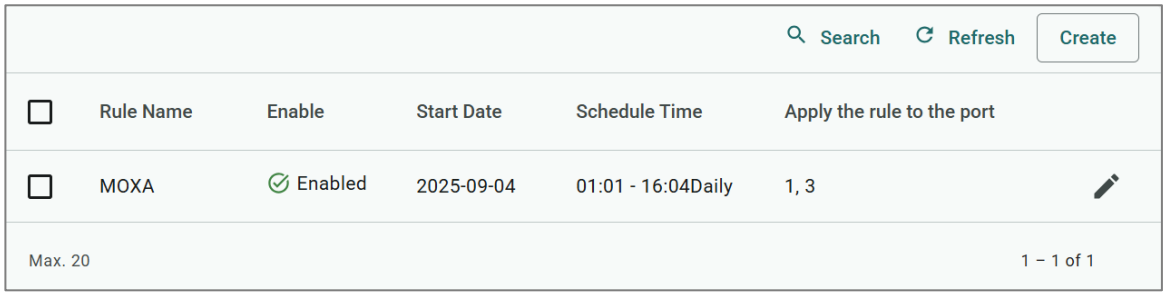
You can create up to 20 PoE scheduling rules.

PoE - System Time Status



UI Setting	Description
System Time	Shows the current system time of the device.
Local Time Zone	Shows the time zone of the device.
Daylight Saving Time	Shows whether the daylight saving time is on.

PoE Scheduling - Rule List



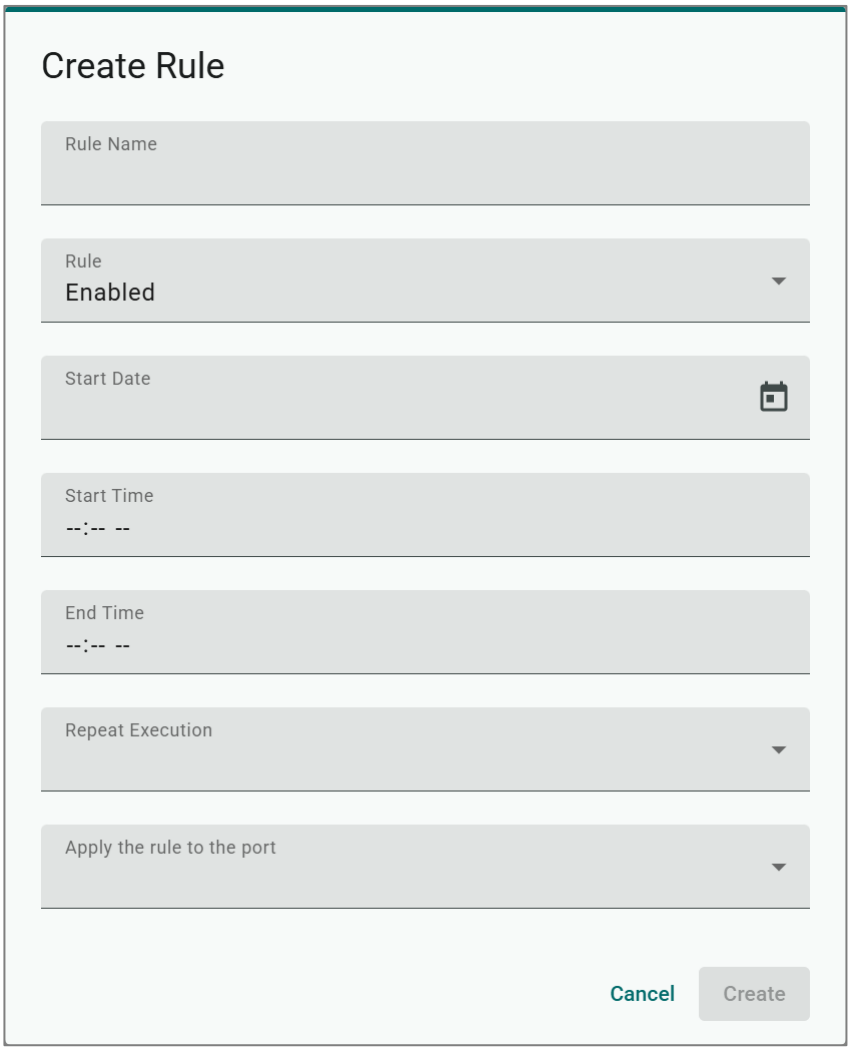
UI Setting	Description
Rule Name	Shows the name of the scheduling rule.
Enable	Shows whether the rule is enabled or disabled.
Start Date	Shows when this rule will become active.
Schedule Time	Shows when the PoE will supply power for the specified ports. The system will not supply PoE power outside the scheduled time.
Apply the rule to the port	Shows which ports will use this rule.

PoE Scheduling - Create Rule

Menu Path: Port > PoE - Scheduling

Clicking the **Create** button on the **Port > PoE - Scheduling** page will open this dialog box. This dialog lets you create a PoE scheduling rule.

Click **Create** to save your changes.



UI Setting	Description	Valid Range	Default Value
Rule Name	Specify a name for the scheduling rule.	1 to 63 characters	N/A
Rule	Enable or disable the scheduling rule.	Enabled / Disabled	Enabled
Start Date	Specify a start date for the rule to become active.	yyyy/mm/dd	N/A
Start Time	Specify a start time to enable PoE.	AM/PM hh/mm	N/A
End Time	Specify an end time to disable PoE.	AM/PM hh/mm	N/A
Repeat Execution	Specify whether to repeat execution of the rule on a daily or weekly basis.	None / Daily / Weekly	N/A

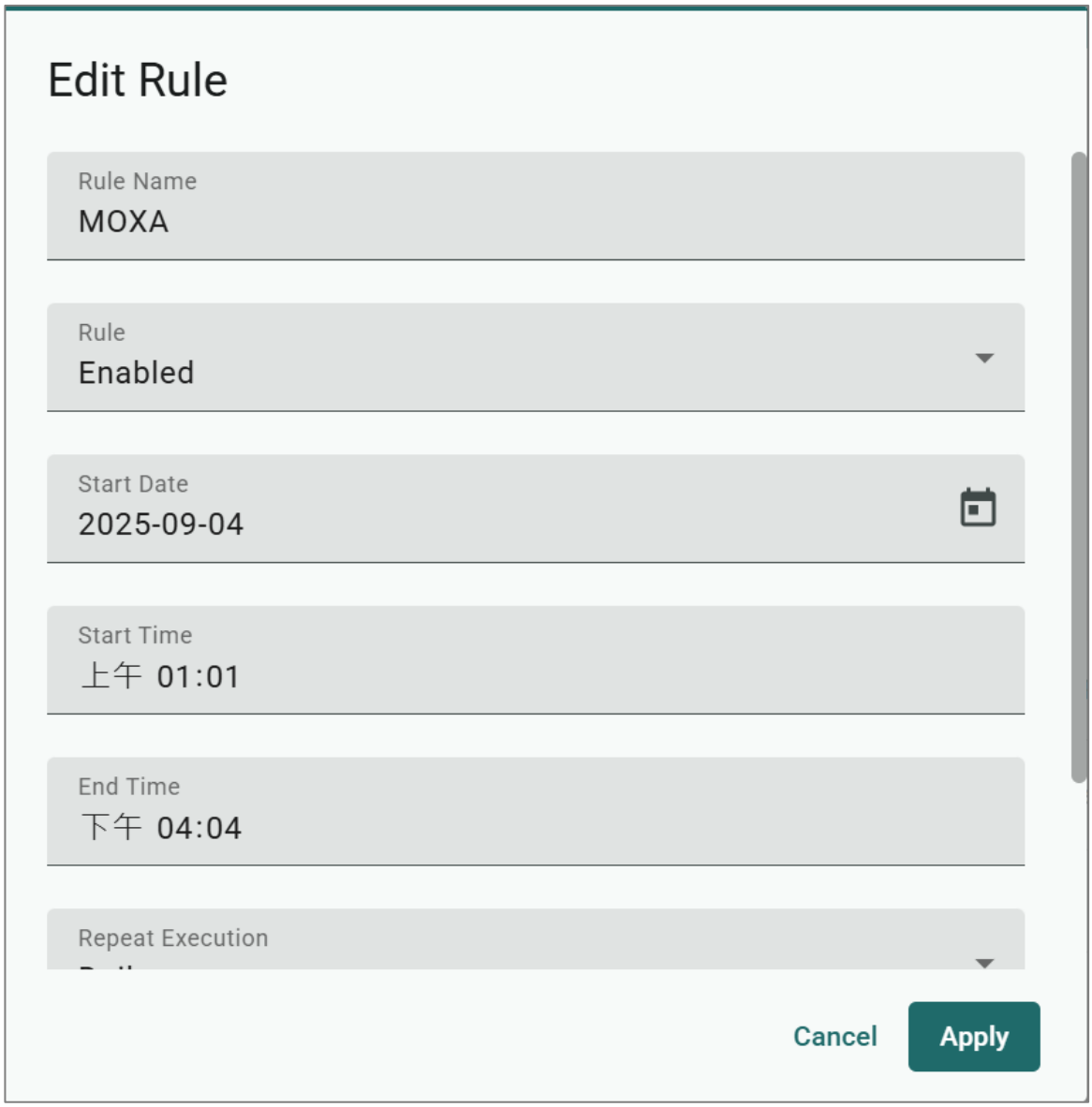
UI Setting	Description	Valid Range	Default Value
Apply the rule to the port	Specify which ports should use this rule.	Select port(s) from the drop-down list	N/A

PoE Scheduling - Edit Rule

Menu Path: Port > PoE - Scheduling

Clicking the **Edit (✎)** icon for a rule on the **Port > PoE - Scheduling** page will open this dialog box. This dialog lets you edit an existing PoE scheduling rule.

Click **Apply** to save your changes.



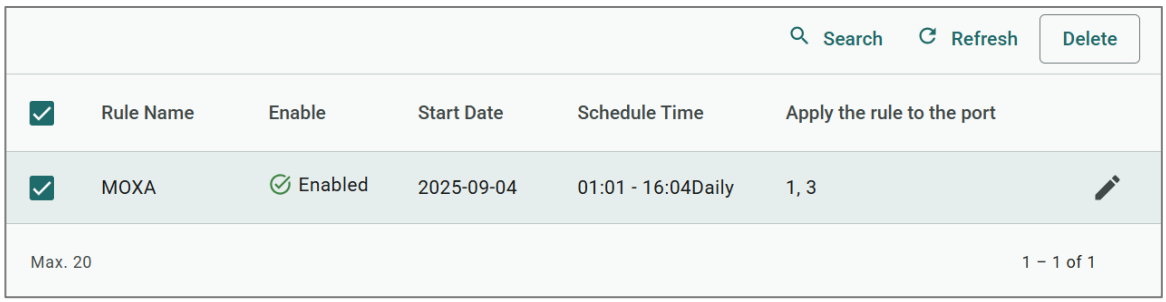
UI Setting	Description	Valid Range	Default Value
Rule Name	Specify a name for the scheduling rule.	1 to 63 characters	N/A
Rule	Enable or disable the scheduling rule.	Enabled / Disabled	Enabled
Start Date	Specify a start date for the rule to become active.	yyyy/mm/dd	N/A
Start Time	Specify a start time to enable PoE.	AM/PM hh/mm	N/A
End Time	Specify an end time to disable PoE.	AM/PM hh/mm	N/A

UI Setting	Description	Valid Range	Default Value
Repeat Execution	Specify whether to repeat execution of the rule on a daily or weekly basis.	None / Daily / Weekly	N/A
Apply the rule to the port	Specify which ports should use this rule.	Select port(s) from the drop-down list	N/A

PoE Scheduling - Delete Rule

Menu Path: Port > PoE - Scheduling

You can delete a rule by using the checkboxes to select the entries you want to delete, then clicking the **Delete** button.

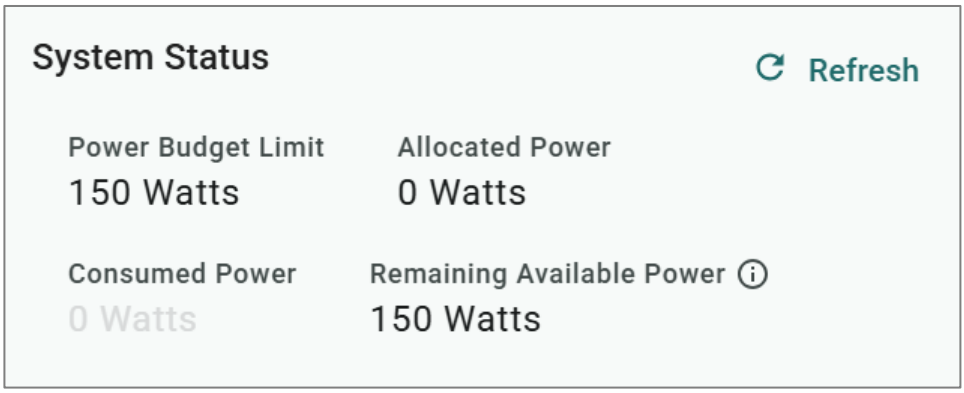


PoE - Status

Menu Path: Port > PoE - Status

This page lets you view PoE system and port status.

PoE - System Status

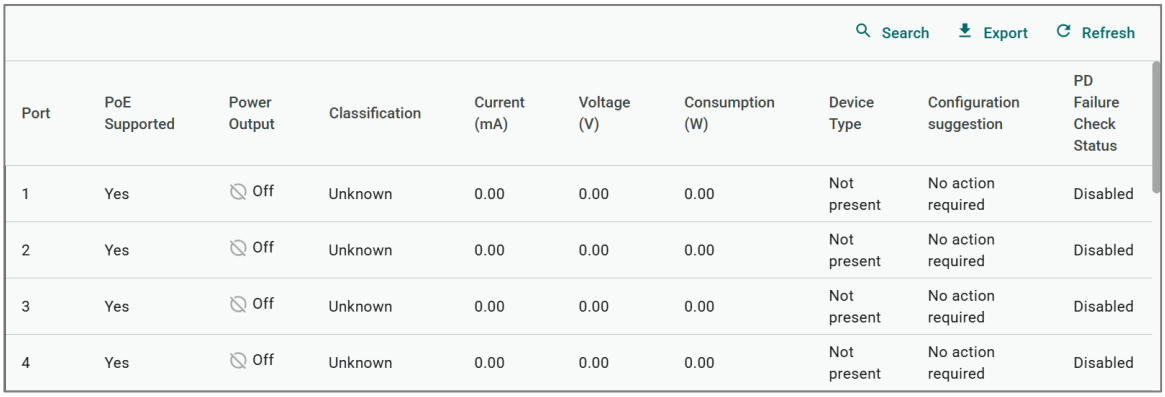


UI Setting	Description
Power Budget Limit	Shows the PoE power budget limit.
Allocated Power	Shows the total allocated PoE power.
Consumed Power	Shows the total consumed PoE power.
Remaining Available Power	Shows the remaining power available for the device. **Note** Remaining Available Power is Maximum Input Power minus Allocated Power.

PoE Status - Port List

Note

When a higher-power 802.3bt (Class 5~8) PD is connected to a lower-power 802.3at or 802.3af PSE, the PD will simply operate at a lower power state, which is known as downgrading. In this situation, the classification and device type of the PD will appear as Class 4 and 802.3at because of inherent device limitations.



UI Setting	Description
Port	Shows the number of the PoE port.
PoE Supported	Shows whether the port supports PoE.
Power Output	Shows whether PoE power output is on or off for the port.
Classification	Shows the PoE power classification of the port. Each PoE power classification has a different maximum power (in watts) by PSE output as follows: • **0**: 15.4 watts • **1**: 4 watts • **2**: 7 watts • **3**: 15.4 watts • **4**: 30 watts
Current (mA)	Shows the amount of current (in mA) being supplied to the port.
Voltage (V)	Shows the voltage (in V) being used for the port.
Consumption (W)	Shows the power consumption (in W) of the device connected to the port.
Device Type	Shows the device type of the device currently connected to the port. • **Not Present**: There are no active connections to the port. • **Legacy PoE Device**: A legacy PD is connected to the port, and the device has detected that the voltage is too low or high, or the PD's detected capacitance is too high. • **802.3at**: An IEEE 802.3at PD is connected to the port. • **802.3af**: An IEEE 802.3af PD is connected to the port. • **NIC**: A NIC is connected to the port. • **Unknown**: An unknown PD is connected to the port. • **N/A**: The PoE function is disabled.

UI Setting	Description
Configuration Suggestion	Shows configuration suggestions based on detected conditions. • **Disable PoE power output**: A NIC or unknown PD was detected; you may want to disable PoE power output for the port. • **Select Force Mode**: A higher/lower resistance or higher capacitance was detected; you may want to select **Force Mode** for the port. • **Select high power output**: An unknown classification was detected; you may want to select **High Power** output. • **Raise the external power supply voltage to greater than 46 VDC**: When the external supply voltage is detected at less than 46 V, the system suggests raising the voltage. • **Enable PoE function for detection**: The system suggests enabling the PoE function. • **Select IEEE 802.3at auto mode**: When detecting an IEEE 802.3at PD, the system suggests selecting 802.3at Auto mode. • **Select IEEE 802.3af auto mode**: When detecting an IEEE 802.3af PD, the system suggests selecting 802.3af Auto mode.
PD Failure Check Status	Shows the results of the last PD failure check, if checking is enabled. Refer to PD Failure Check for more information. • **Disable**: PD failure checking is not enabled for the port. • **Alive**: The port is alive, and passed the last PD failure check. • **Not Alive**: The port is not alive, and failed the last PD failure check.

Layer 2 Switching

Menu Path: Layer 2 Switching

This section lets you configure your device's Layer 2 switching features.

This section includes these pages:

- VLAN
- GARP
- MAC
- QoS
- Multicast

Layer 2 Switching - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to System > Account Management > User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
VLAN	R/W	R/W	R
GARP	R/W	R/W	R
MAC			
Static Unicast	R/W	R/W	R
MAC Address Table	R/W	R/W	R
QoS			
Classification	R/W	R/W	R
Ingress Rate Limit	R/W	R/W	R
Scheduler	R/W	R/W	R

Settings	Admin	Supervisor	User
Egress Shaper	R/W	R/W	R
Multicast			
IGMP Snooping	R/W	R/W	R
GMRP	R/W	R/W	R
Static Multicast	R/W	R/W	R

About VLAN

A VLAN, or Virtual Local Area Network, is a logical grouping of devices on a network.

Assigning VLANs to Ports

VLANs must be assigned to ports to route traffic correctly. Now that you've created the VLANs, they need to be assigned to ports so that traffic from those ports will be routed over the correct VLAN. A similar procedure must be performed on each switch or router on the network.

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching→VLAN→Settings.**
3. To assign the newly created VLAN ID to a port, find the port on the **Port Table** on the lower part of the page, and the click ***[Edit]***.
   Result: The **Edit Port Settings** panel appears.
4. Specify the **Mode** and **PVID** that will be assigned to the port, and then click **Apply**.

Tutorial Info:

Access mode is used when connecting single devices without tags. These are usually end-user devices that belong to a single VLAN, and do not need to communicate with devices in other VLANs.

Trunk mode allows a port to carry traffic for multiple VLANs over a single physical connection. This is useful for linking switches together that may have many different VLANs.

Hybrid mode is similar to a Trunk port, except users can explicitly assign tags to be removed from egress packets.

> **Note**
>
> The port VID (PVID) setting will apply a VLAN tag only for untagged traffic coming through that port. If traffic going through the port has already been tagged with a VLAN ID, the PVID setting will not change the existing tag.

Result: The **Port Table** will show the new port configuration.

Creating VLANs

Create VLANs in preparation for assigning them to ports.

To create a VLAN, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching > VLAN > Settings**.
3. To add a VLAN ID, click ***[Add]***.
   Result: The **Create VLAN** screen appears.
4. Specify the VLAN to create in the **VID**, and then click **Create**.
   Optionally:
   - Type a human-readable identifier in the **Name** field
   - Assign the VLAN to a **Member Port**. You also assign VLANs to ports later.

   Result: The VLAN will appear on the VLAN table at the top of the page.
5. Repeat this process to create VLANs needed for the network topology.

What to do next: After you have created the VLANs needed for your topology, you can assign VLANs to ports if you have not done so already.

Note

You can delete VLANs by choosing a VLAN ID from the VLAN table at the top of the page, clicking the checkbox, and then clicking [Delete].

VLANs in Depth

This technology allows network administrators to divide a large network into smaller, more manageable segments without the need for additional physical hardware. Devices within a VLAN can be located anywhere on the network but communicate as though they are on the same physical segment. This facilitates traffic management, as administrators can ensure traffic is directed only to devices within the same VLAN by assigning a VLAN tag to each Ethernet frame. Consequently, VLANs provide a means to segment a network beyond the constraints of physical connections, a limitation inherent in traditional network design. VLANs can be utilized to segment your network into various groups, such as:

- **Departmental groups**—One VLAN for the R&D department, another for Office Automation, etc.
- **Hierarchical groups**—One VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—One VLAN for email users and another for multimedia users.

VLAN Standards and Implementation

The functioning of VLANs is guided by IEEE 802.1Q, often referred to as Dot1q. This standard outlines the protocol for VLAN tagging on Ethernet frames within an IEEE 802.3 Ethernet network. During the transmission of data between switches, VLAN tags identify the VLAN ownership of frames. Networking equipment reads these tags and ensures that tagged frames are delivered to devices within that VLAN, maintaining the network's logical segmentation.

A VLAN tag is a specific piece of data embedded in the header of an Ethernet frame. It comprises a 4-byte field carrying key information, such as the VLAN ID (VID) and priority level. The VID is a numerical identifier that uniquely links the frame to a specific VLAN. The priority field within the tag plays a critical role in prioritizing certain types of traffic within a VLAN. This structure contributes to effective network traffic management by giving precedence to certain data when necessary.

Benefits of VLANs

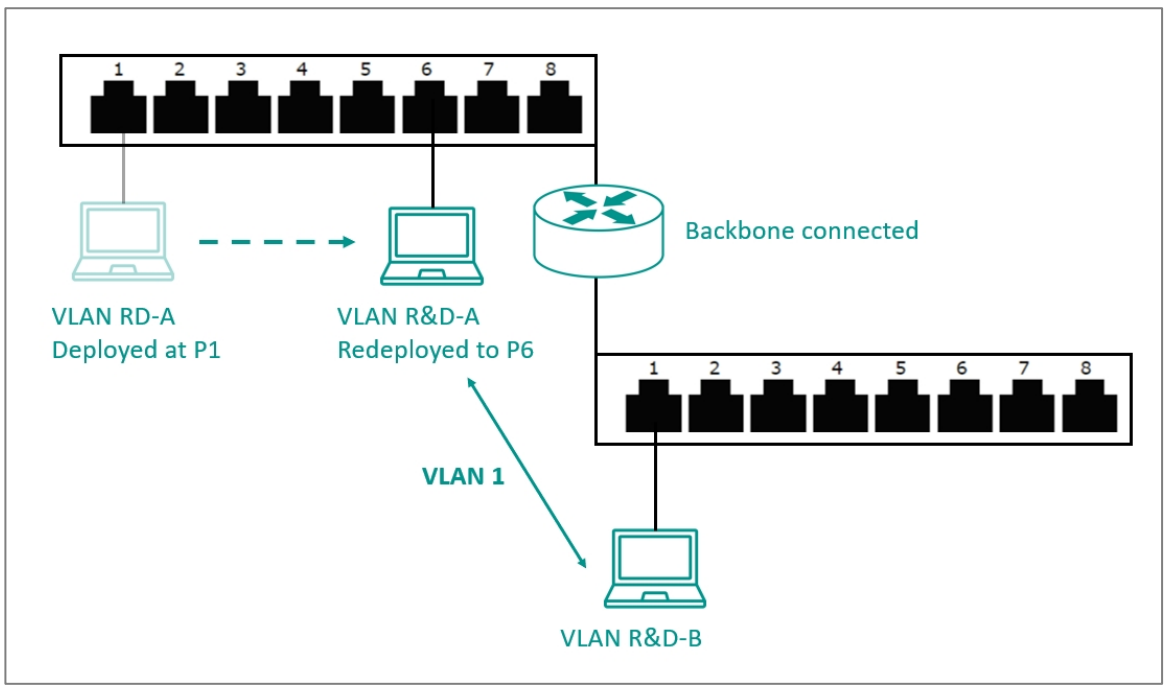
The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

VLANs 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.

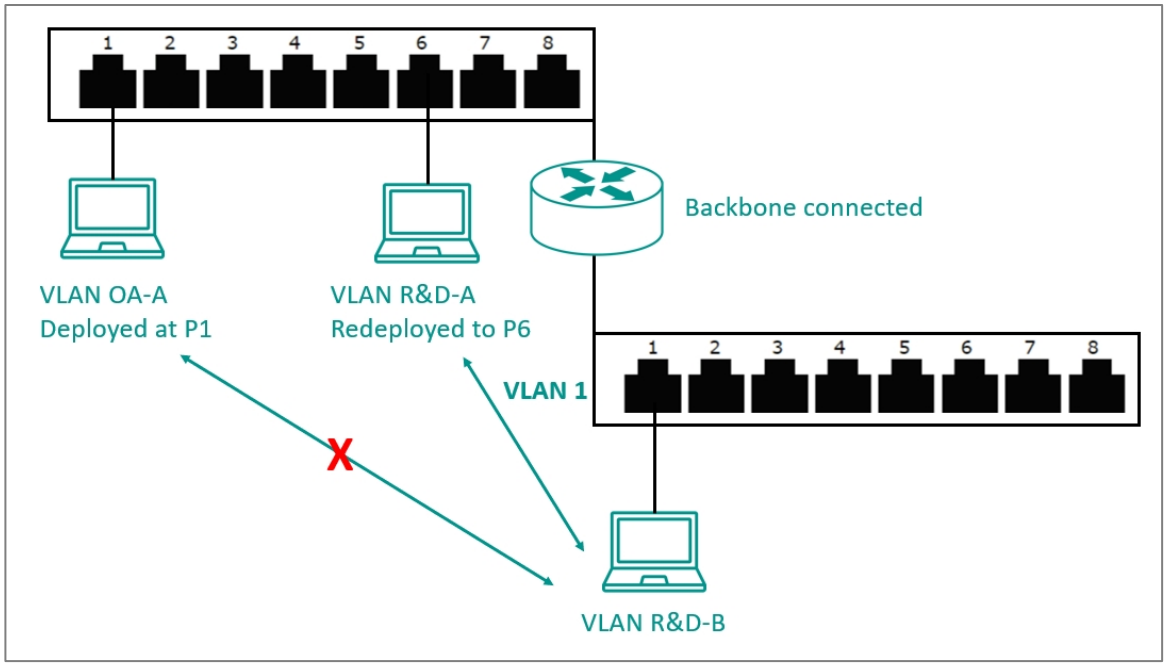
VLANs simplify device relocation

In traditional networks, administrators spend significant time managing moves and changes, requiring manual updates of host addresses when users switch sub-networks. In contrast, VLANs simplify this process. For example, when relocating a host from Port 1 to Port 6 in a different network section, simply assign Port 6 to the relevant VLAN (e.g., VLAN R&D A). This enables seamless communication between VLANs, eliminating the need for re-cabling.



VLANs provide extra security

Devices within each VLAN can only communicate with other devices on the same VLAN. If VLAN R&D B needs to communicate with VLAN OA(Office Automation) A, the traffic must pass through a routing device or Layer 3 switch.



Note

Network segmentation is not a substitute for network security. While network segmentation can provide a degree of isolation that contributes to the overall security environment, the primary benefit of VLANs is improved performance by ensuring minimal crosstalk between unrelated systems. Network segmentation should be complimented with network security procedures.

About VLAN Unaware

VLAN Unaware allows the device to operate in a VLAN-segmented LAN by processing packets based on inbound rules. It forwards data packets without modification, acting as a transparent bridge.

Enabling this mode disables standard VLAN settings, and the device prioritizes packets based on the data packet's information. Tagged packets are transmitted as tagged, and untagged packets as untagged.

Note

To enable VLAN Unaware, the following conditions must be met:

- Only one VLAN can exist: VLAN 1.
- All ports must be configured as access ports.
- All ports must have a Port VLAN ID (PVID) of VLAN 1.
- The management VLAN must be set to VLAN 1.

When VLAN Unaware mode is enabled, GVRP, RSPAN, MSTP, and MRP cannot be activated. This is because these features necessitate the creation of additional VLANs or the use of multiple VLANs.

VLAN Settings

Menu Path: Layer 2 Switching > VLAN

This page lets you view and configure your device's VLAN settings.

This page includes these tabs:

- Global
- Settings
- Status

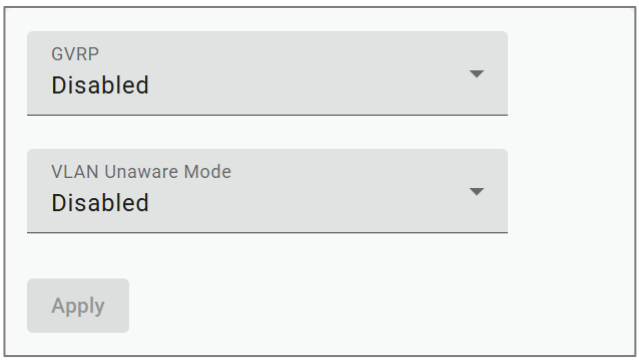
VLAN - Global

Menu Path: Layer 2 Switching > VLAN - Global

This page lets you configure the global VLAN settings.

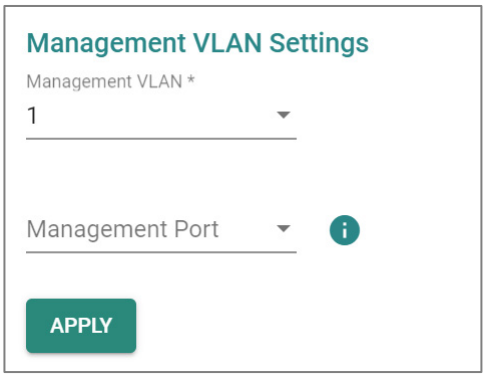
Click **Apply** to save your changes.

VLAN Global Settings



UI Setting	Description	Valid Range	Default Value
GVRP	Enable or disable GVRP for the device. **Note** MSTP and GVRP are both VLAN-related functions. When VLAN changes dynamically, MSTP needs to re-converge, which can make the system unstable due to running complex operations. When both MSTP and GVRP are used together, this can result in network instability. Therefore, it is recommended that network administrators avoid enabling both MSTP and GVRP.	Enabled / Disabled	Disabled
VLAN Unaware	Enable or disable VLAN Unaware mode for the device. **Note** To enable VLAN Unaware, the following conditions must be met: • Only one VLAN can exist: VLAN 1. • All ports must be configured as access ports. • All ports must have a Port VLAN ID (PVID) of VLAN 1. • The management VLAN must be set to VLAN 1. When VLAN Unaware mode is enabled, GVRP, RSPAN, MSTP, and MRP cannot be activated. This is because these features necessitate the creation of additional VLANs or the use of multiple VLANs.	Enabled / Disabled	Disabled

Management VLAN Settings



UI Setting	Description	Valid Range	Default Value
Management VLAN	Specify the management VLAN.	Drop-down list of VLANs	1
Management Port	Specify a management port for this device to allow for quick and easy configuration of VLAN settings. **⚠ Warning** Make sure the computer you are using to configure the device is connected to the selected management port, or you may become disconnected from your device.	Drop-down list of ports	N/A

VLAN - Settings

Menu Path: Layer 2 Switching > VLAN - Settings

This page lets you configure VLANs and which ports they include.

Limitations

You can create up to 256 VLAN IDs.

VLAN List

UI Setting	Description
VLAN ID	Shows the ID of the VLAN.
Name	Shows the name of the VLAN.
Member Port	Shows the member port(s) of the VLAN.
Forbidden Port **(Only in Advanced Mode)**	Shows the forbidden port(s) of the VLAN.

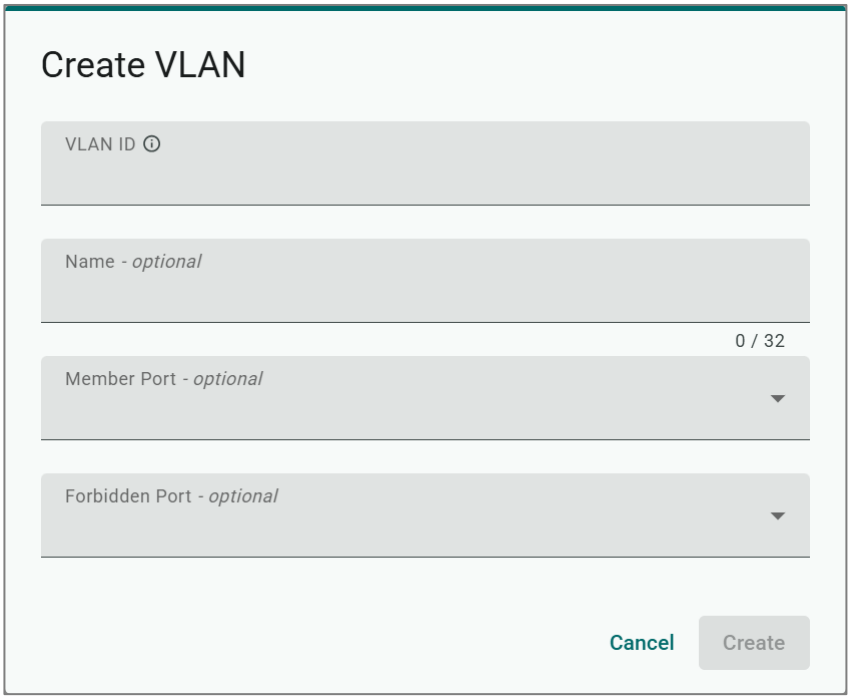
VLAN - Create VLAN

Menu Path: Layer 2 Switching > VLAN - Settings

Clicking **Create** on the **Layer 2 Switching > VLAN - Settings** page will open this dialog box. This dialog lets you create a VLAN.

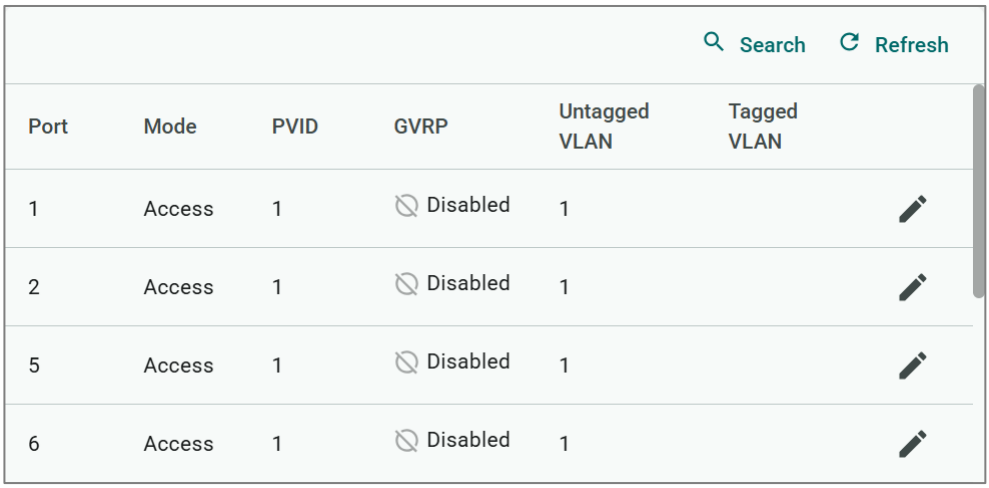
Click **Create** to save your changes.

Create VLAN



UI Setting	Description	Valid Range	Default Value
VLAN ID	Specify the VLAN ID.	1 to 4094	N/A
Name	Specify the name of the VLAN.	0 to 32 characters	N/A
Member Port	Specify the member port(s) of the specific VLAN.	Drop-down list of ports	N/A
Forbidden Port **(Only in Advanced Mode)**	Specify the forbidden port(s) of the specific VLAN.	Drop-down list of ports	N/A

VLAN Port List



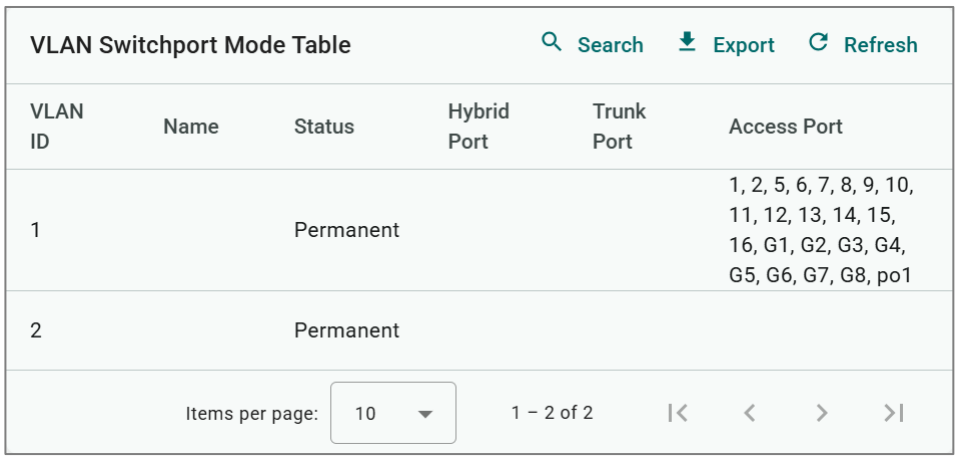
UI Setting	Description
Port	Shows the port number.
Mode	Shows the mode of the port. • **Access**: The port is connected to a single device, without tags. • **Trunk**: The port is connected to another 802.1Q VLAN aware switch. • **Hybrid**: The port is connected to another Access 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices.
PVID	Shows the default VLAN ID for untagged devices connected to the port. The PVID will be added for ingress traffic, and will be removed for egress traffic for the access port only.
GVRP	Shows whether GVRP is enabled for the port.
Untagged VLAN	When the port is using **Hybrid** VLAN mode, this shows all VLAN IDs that will be removed from egress packets.
Tagged VLAN	When the port is using **Trunk** or **Hybrid** VLAN mode, this shows all VLAN IDs will be carried to connected devices.

VLAN - Status

Menu Path: Layer 2 Switching > VLAN - Status

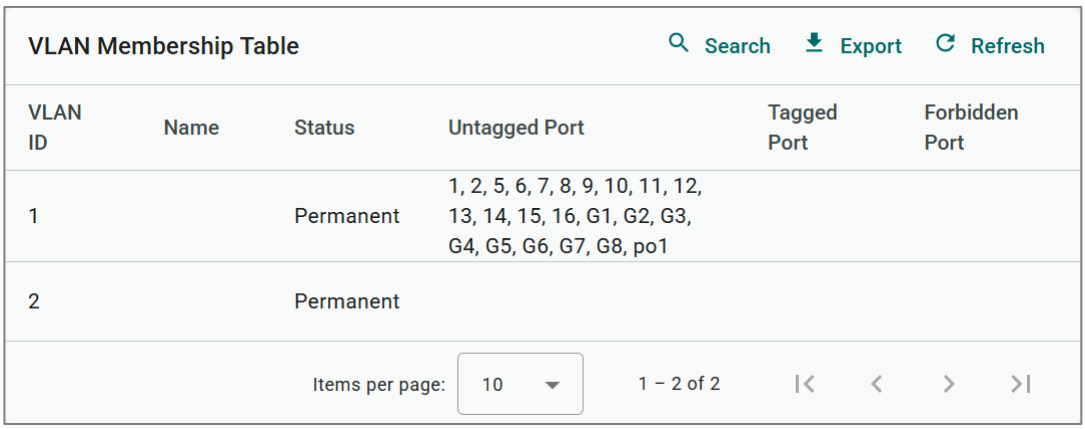
This page lets you monitor the status of the VLANs on your device.

VLAN Switchport Mode Table



UI Setting	Description
VLAN ID	Shows the ID of the VLAN.
Name	Shows the name of the VLAN.
Status	Shows the status of the VLAN.
Hybrid Port	Shows ports acting as a Hybrid Port for the VLAN.
Trunk Port	Shows ports acting as a Trunk Port for the VLAN.
Access Port	Shows ports acting as an Access Port for the VLAN.

VLAN Membership Table



UI Setting	Description
VLAN ID	Shows the ID of the VLAN.
Name	Shows the name of the VLAN.
Status	Shows the status of the VLAN.
Untagged Port	Shows the untagged port(s) for the VLAN.
Tagged Port	Shows the tagged port(s) for the VLAN.
Forbidden Port **(Only in Advanced Mode)**	Shows the forbidden port(s) for the VLAN.

GARP

Generic Attribute Registration Protocol (GARP) is a communication protocol defined by IEEE 802.1 that offers a generic framework for bridges to register and de-register an attribute value.

In a VLAN structure, two GARP applications can be applied:

- **GARP VLAN Registration Protocol (GVRP)** is used to register VLAN trunking between multilayer switches.
- **GARP Multicast Registration Protocol (GMRP)** provides a constrained multicast flooding facility.

Note

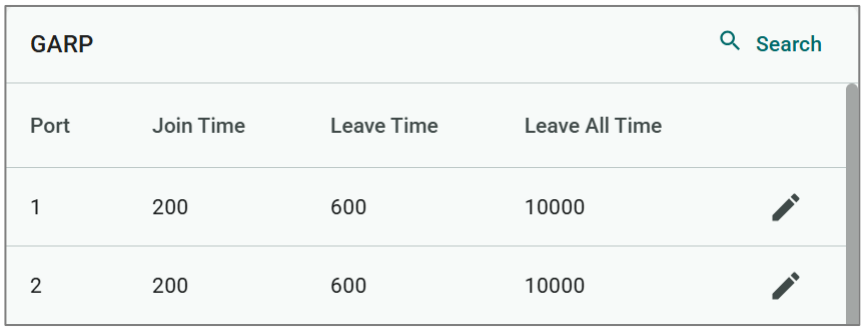
This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

GARP Settings

Menu Path: Layer 2 Switching > GARP

This page lets you configure GARP settings for each port.

GARP List



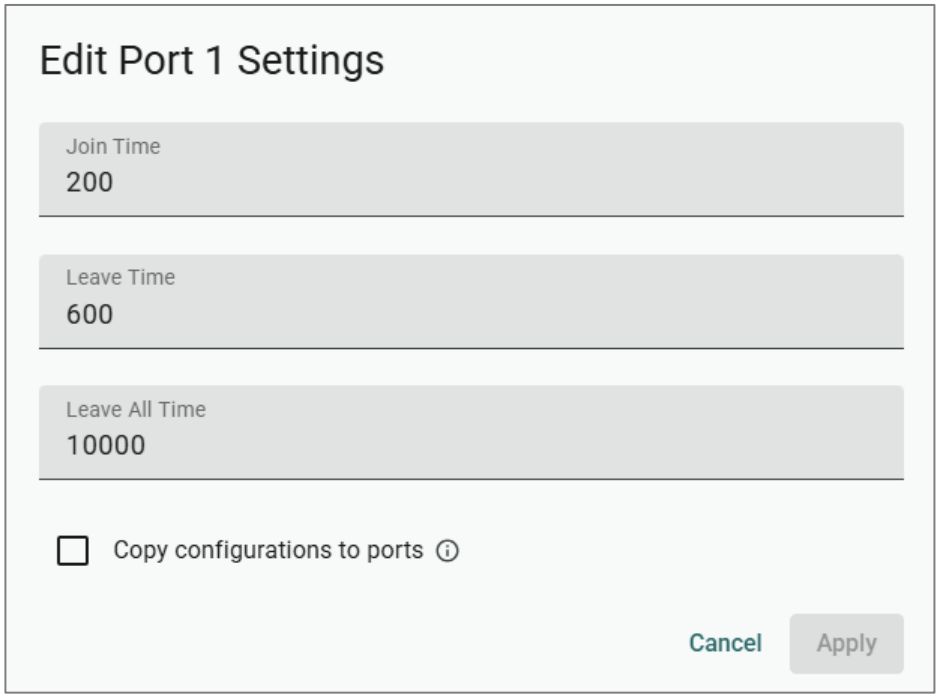
UI Setting	Description
Port	Shows which port the entry is for.
Join Time (sec.)	Shows the join time in seconds for the port.
Leave Time (sec.)	Shows the leave time in seconds for the port.
Leave All time (sec.)	Shows the leave all time in seconds for the port.

GARP - Edit Port Settings

Menu Path: Layer 2 Switching > GARP

Clicking the **Edit (✎)** icon for a port on the **Layer 2 Switching > GARP** page will open this dialog box. This dialog lets you configure the GARP parameters for each port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Join Time (sec.)	Specify the join time in seconds.	10 to 499999980	200
Leave Time (sec.)	Specify the leave time in seconds.	30 to 499999980	600
Leave All time (sec.)	Specify the leave all time in seconds.	30 to 499999990	10000
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

MAC

Menu Path: Layer 2 Switching > MAC

This section lets you manage MAC related switching features of your device.

This section includes these pages:

- Static Unicast
- MAC Address Table

About Static Unicast

Static Unicast lets you manually define specific forwarding paths for data packets destined for particular devices on the network.

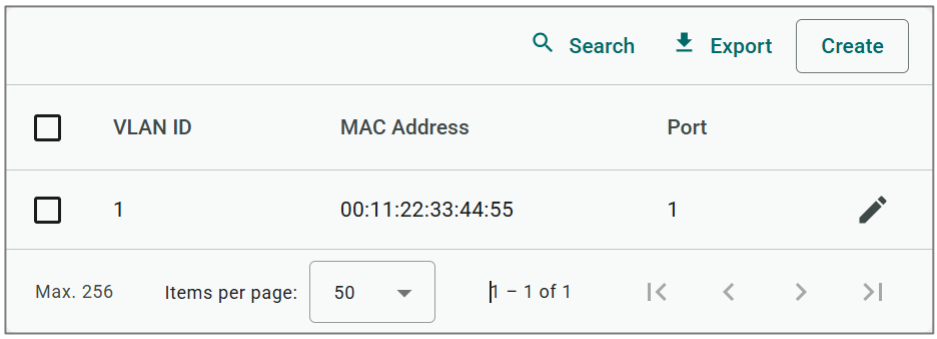
Static Unicast

Menu Path: Layer 2 Switching > MAC > Static Unicast

This page lets you manage your device's static unicast entries.

> **Limitations**
> You can create up to 256 static unicast entries.

Unicast Table



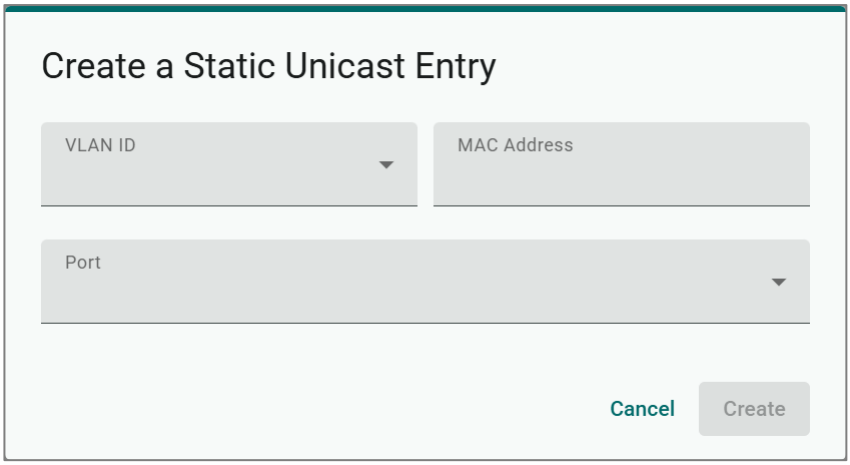
UI Setting	Description
VLAN ID	Shows the VLAN ID used for the static unicast entry.
MAC Address	Shows the MAC address used for the static unicast entry.
Port	Shows which ports are included for the static unicast entry.

Add a Static Unicast Entry

Menu Path: Layer 2 Switching > MAC > Static Unicast

Clicking **Create** on the **Layer 2 Switching > MAC > Static Unicast** page will open this dialog box. This dialog lets you add a new static unicast entry.

Click **Create** to save your changes and add the new entry.



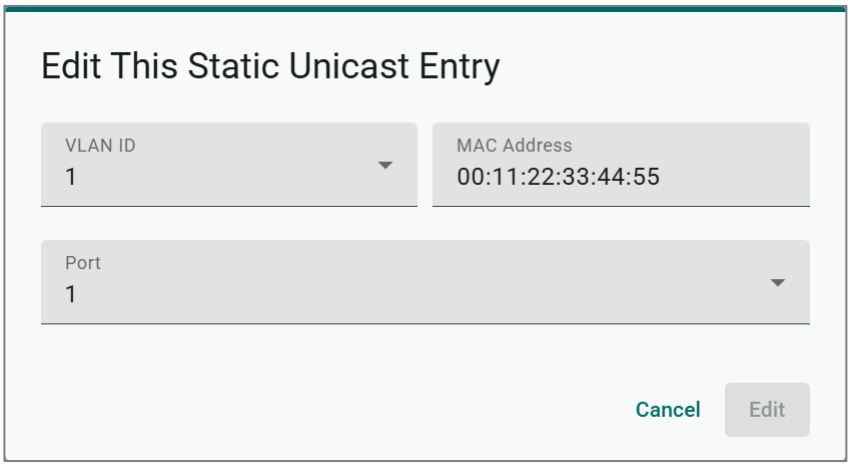
UI Setting	Description	Valid Range	Default Value
VLAN ID	Specify the VLAN ID.	Drop-down list of VLAN IDs	N/A
MAC Address	Specify the static unicast MAC address of the port.	Valid unicast MAC address	N/A
Port	Specify which ports you want to include in the static unicast group	Drop-down list of ports	N/A

Edit a Static Unicast Entry

Menu Path: Layer 2 Switching > MAC > Static Unicast

Clicking the **Edit (✎)** icon for an entry on the **Layer 2 Switching > MAC > Static Unicast** page will open this dialog box. This dialog lets you edit the static unicast entry.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
VLAN ID	Specify the VLAN ID.	Drop-down list of VLAN IDs	N/A
MAC Address	Specify the static unicast MAC address of the port.	Valid unicast MAC address	N/A
Port	Specify which ports you want to include in the static unicast group	Drop-down list of ports	N/A

About MAC Address Tables

The MAC address table is a database maintained on your device that acts like a directory to keep track of all the devices currently connected to the network. Each entry in the table includes a device's unique identifier, known as its Media Access Control (MAC) address, and the specific switch port it is connected to.

Note

Moxa devices manage MAC address learning for VLANs using IVL (Independent VLAN Learning), which uses separate MAC address tables for each VLAN so that MAC address learning for different VLANs do not interfere with each other.

A MAC table will be stored in the format of MAC + VID. This allows the same MAC address to be used in multiple VLANs without causing forwarding issues.

This may lead to a larger MAC address table size, as each VLAN maintains its own individual address table, and the number of MAC address entries will increase based on the number of VLAN member ports used.

MAC Address Table

Menu Path: Layer 2 Switching > MAC > MAC Address Table

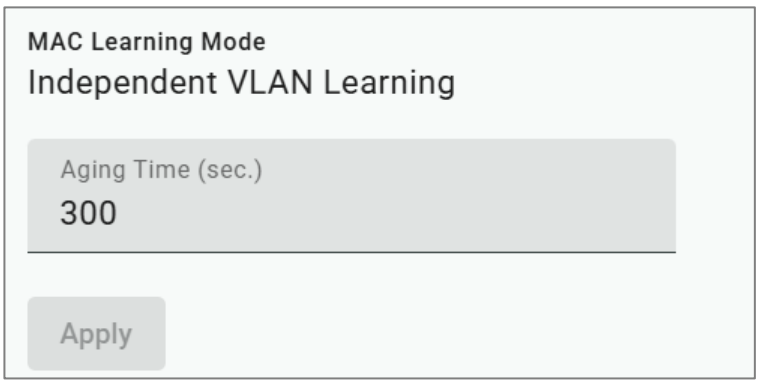
This page lets you view your device's MAC address table and set the aging time for MAC address entries.

Click **Apply** to save your changes.

Limitations

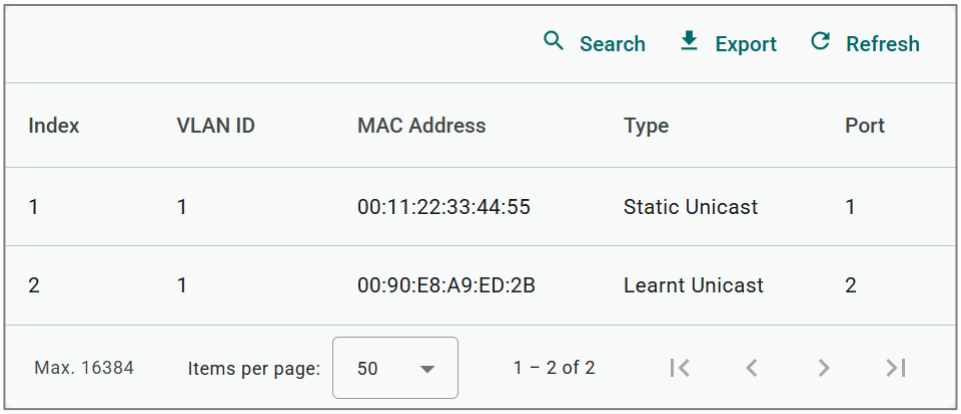
The MAC address table can hold up to 16384 entries.

MAC Address Settings



UI Setting	Description	Valid Range	Default Value
MAC Learning Mode	Shows the current MAC learning mode.	N/A	Independent VLAN Learning
Aging Time	Specify the aging time for MAC address entries in seconds. The aging time determines how long entries will be kept in the MAC address table in the device's memory before expiring.	10 to 300	300

MAC Address Table List



UI Setting	Description
Index	Shows the index number of the MAC address.
VLAN ID	Shows which VLAN ID is being used for the MAC address.
MAC Address	Shows the MAC address of the device.
Type	Shows what kind of MAC address entry this is: **Learnt Unicast**: Used for all learnt unicast MAC addresses. **Learnt Multicast**: Used for all learnt multicast MAC addresses. **Static Unicast**: Used for all static unicast MAC addresses. **Static Multicast**: Used for all static multicast MAC addresses.
Port	Shows which port on the device the MAC address is connected to.

About QoS

Quality of Service (QoS) is a set of techniques and mechanisms used in computer networks to prioritize certain types of traffic to ensure reliable delivery of data and optimize network performance. QoS mechanisms allow network administrators to define policies and rules for managing network resources and controlling the flow of traffic based on factors such as traffic type and application requirements.

This device has the following QoS features:

- Classification

- Ingress Rate Limit
- Scheduler
- Egress Shaper

QoS In Depth

This device provides Quality of Service (QoS) for your network by classifying and prioritizing traffic to make data delivery more reliable. Traffic can be classified by applying IEEE 802.1p/1Q Layer 2 CoS (Class of Service) tags or Layer 3 DSCP (Differentiated Services Code Point) information. The device can use these together with a set of rules that specify how each type of traffic should be treated as it passes through the device. This allows delivery of traffic to be prioritized to ensure that high-priority data is transmitted with minimum delay. Refer to Classification for more information about traffic classification.

Network administrators can use Strict Priority and Weighted Round Robin scheduling algorithms—as well as a mix of the two—to choose the most suitable method for packet transmission in their field applications. Refer to Scheduler for more information.

In addition to packet classification for incoming packets and scheduling for outgoing packets, users can also establish a rate threshold for incoming data. When this limit is exceeded, they can choose to either drop or remark the packet. Refer to Ingress Rate Limit for more information.

The egress shaper helps optimize outbound traffic, maintain network stability, and ensure efficient utilization of available bandwidth resources. Refer to Egress Shaper for more information.

QoS

Menu Path: Layer 2 Switching > QoS

This section lets you enable and configure your device's QoS settings.

This section includes these pages:

- Classification
- Ingress Rate Limit
- Scheduler

- Egress Shaper

> **Note**
>
> For MX-NOS platform devices, QoS behavior will be consistent as long as the chipset solutions are the same. Therefore, TN devices will exhibit identical QoS behavior.

Classification

Traffic classification and prioritization allows you to classify data for prioritization so that time-sensitive and system-critical data can be transferred smoothly and with minimal delay over a network.

Benefits of using traffic classification and prioritization include:

- Improving network performance by controlling a wide variety of traffic types and managing congestion
- Assigning priorities to different categories of traffic, such as setting higher priorities for time-critical or mission-critical applications
- Providing predictable throughput to improve the performance of multimedia applications–such as video conferencing or voice over IP–to minimize traffic delay and jitter
- Optimizing network utilization depending on application usage and usage needs, allowing the amount of traffic to increase without requiring increases in backbone bandwidth

Traffic classification and prioritization uses eight traffic queues to ensure that higher priority traffic can be forwarded separately from lower priority traffic to help guarantee quality of service (QoS) for your network.

Traffic classification and prioritization for your Moxa device is based on two standards:

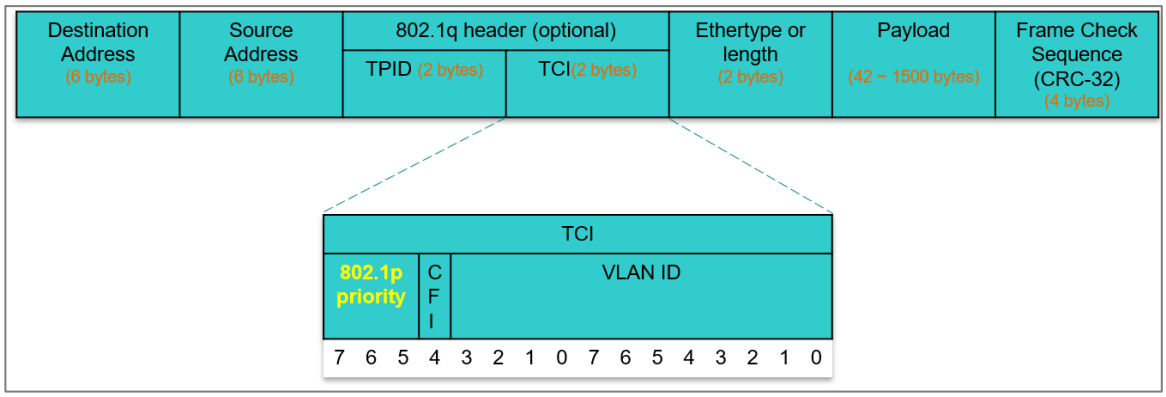
- **IEEE 802.1p Class of Service**: A Layer 2 QoS marking scheme
- **Differentiated Services (DiffServ) Traffic Marking:** A Layer 3 QoS marking scheme

IEEE 802.1p Class of Service (CoS) In Depth

The IEEE Std 802.1D 2005 Edition marking scheme, which is an enhancement to IEEE Std 802.1D, enables Quality of Service on a LAN. Traffic service levels are defined in the

IEEE 802.1Q 4-byte tag, which is used to carry VLAN identification as well as IEEE 802.1p priority information. If the 802.1q header presents and the Tag Protocol Identifier (TPID) value is 0x8100, then it means the frame is tagged. The TPID is followed by a 2-byte field Tag Control Information (TCI) which contains a 3-bit 802.1p priority field as shown in below figure.

The IEEE Std 802.1D 2005 Edition priority marking scheme assigns an IEEE 802.1p priority level between 0 and 7 to each frame, which specifies the level of service that the associated packets shall be handled.



The table below shows an example of how different traffic types can be mapped to the eight IEEE 802.1p priority levels.

IEEE 802.1p Priority (decimal)	IEEE 802.1p Priority (binary)	IEEE 802.1D Traffic Type
0	0 0 0	Best Effort
1	0 0 1	Background (lowest priority)
2	0 1 0	Reserved
3	0 1 1	Excellent Effort (business critical)
4	1 0 0	Controlled Load (streaming multimedia)
5	1 0 1	Video (interactive media)
6	1 1 0	Voice (interactive voice)
7	1 1 1	Network Control Reserved traffic

Even though the IEEE 802.1p standard is the most widely used prioritization scheme for LAN environments, it still has some restrictions:

- It requires an additional 4-byte tag in the frame, which is normally optional for Ethernet networks. Without this tag, the scheme cannot work.
- The tag is part of the IEEE 802.1Q header, so to implement QoS at Layer 2, the entire network must implement IEEE 802.1Q VLAN tagging.
- It is only supported within a LAN and does not cross the WAN boundaries, since the IEEE 802.1Q tags will be removed when the packets pass through a router.

Differentiated Services (DiffServ) Traffic Marking In Depth

DiffServ is a Layer 3 marking scheme that uses the DiffServ Code Point (DSCP) field in the IP header to specify the packet priority. DSCP is an intelligent method of traffic marking that allows you to choose how your network prioritizes different types of traffic. The DSCP field can be set from 0 to 63 to map to user-defined service levels, enabling users to regulate and categorize traffic by application and assign different service levels.

Advantages of DiffServ over IEEE 802.1Q

- You can prioritize and assign different traffic with appropriate latency, throughput, or reliability for each port.
- No extra tags are required.
- The DSCP priority tags are carried in the IP header, which can pass through WAN boundaries and through the Internet.
- DSCP is backwards compatible with IPv4 ToS (Type of Service), which allows operation with legacy devices that use IPv4 Layer 3.

Default Mapping of DSCP and CoS Values

DSCP values	Mapped CoS value
0 to 7	0
8 to 15	1
16 to 23	2

DSCP values	Mapped CoS value
24 to 31	3
32 to 39	4
40 to 47	5
48 to 55	6
56 to 63	7

Traffic Prioritization In Depth

Moxa switches classify traffic based on Layer 2 of the OSI 7 layer model, and prioritize outbound traffic according to the priority information defined in received packets. Incoming traffic is classified based on the IEEE 802.1p service level field and is assigned to the appropriate egress priority queue.

Traffic flows through the switch as follows:

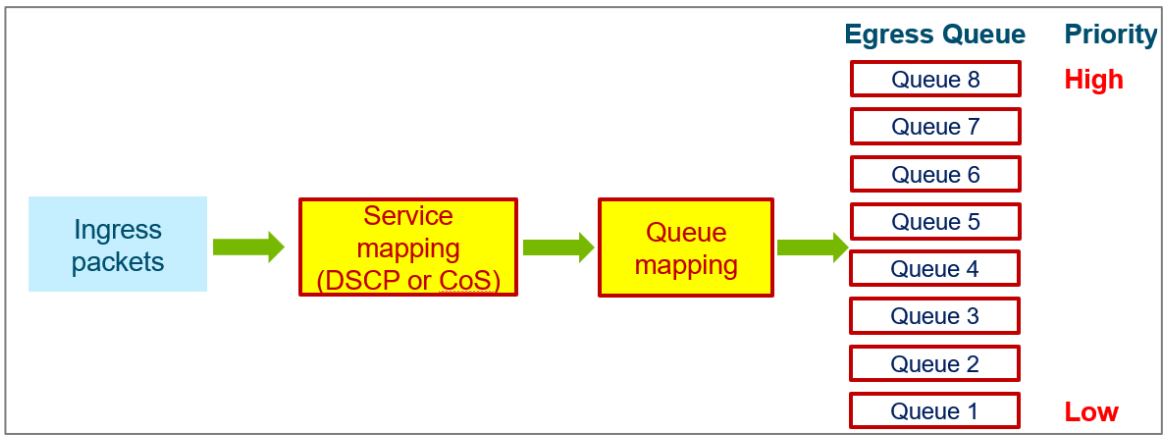
- A received packet may or may not have an 802.1p tag associated with it. If it does not, then it is given a default CoS value according to the port settings in the Classification section.
- Each egress queue has associated 802.1p priority levels that can be defined by users. Packets will be placed in the appropriate priority queue. When the packet reaches the head of its queue and is about to be transmitted, the device determines whether or not the egress port belongs to the VLAN group. If it is, then the new 802.1p tag is used in the extended 802.1D header.

Please be aware that the priority of redundancy protocol control packets is determined by the switch and is not influenced by user-specified QoS settings. The prioritization of traffic is determined by the QoS policies configured on network devices, and remains consistent regardless of whether the interface used is a single port or a trunk port.

Traffic Queues In Depth

Moxa switches have eight different traffic queues that allow packet prioritization to occur. The priority of these queues ranges from 1 (lowest priority) to 8 (highest priority). Higher priority traffic can pass through the switch without being delayed by lower priority traffic.

Ingress packets containing DSCP or CoS fields require classification and mapping to a priority queue. Incoming packets with a specified DSCP value at Layer 3 are remapped to a CoS value at Layer 2 before being directed to an egress queue. The corresponding mapping of DSCP to CoS and the CoS to the egress queue priority is preconfigured on a Moxa switch. As each packet arrives at the switch, it undergoes ingress processing (which includes classification, marking/re-marking), and is then sorted into the appropriate egress queue.



Packets lacking DSCP or CoS values will be directed to the appropriate egress queue based on the settings of Untag Default Priority configured in Port Settings. Refer to Port Classification - Edit Port Setting for more information.

Classification

Menu Path: Layer 2 Switching > QoS > Classification

This page lets you configure your device's QoS classifications.

This page includes these tabs:

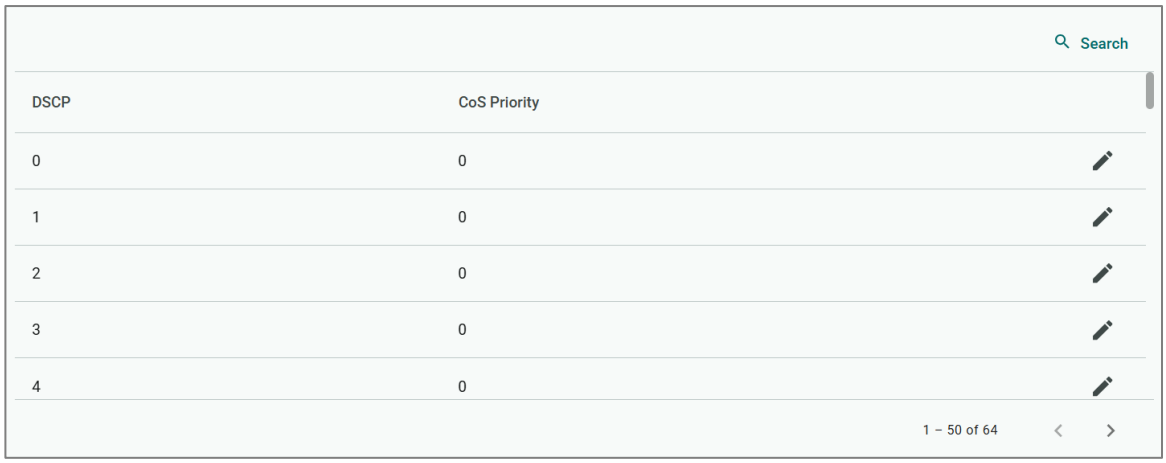
- DSCP Mapping
- CoS Mapping
- Port Settings

DSCP Mapping

Menu Path: Layer 2 Switching > QoS > Classification - DSCP Mapping

This page lets you view and edit your DSCP CoS mappings.

DSCP Mapping List



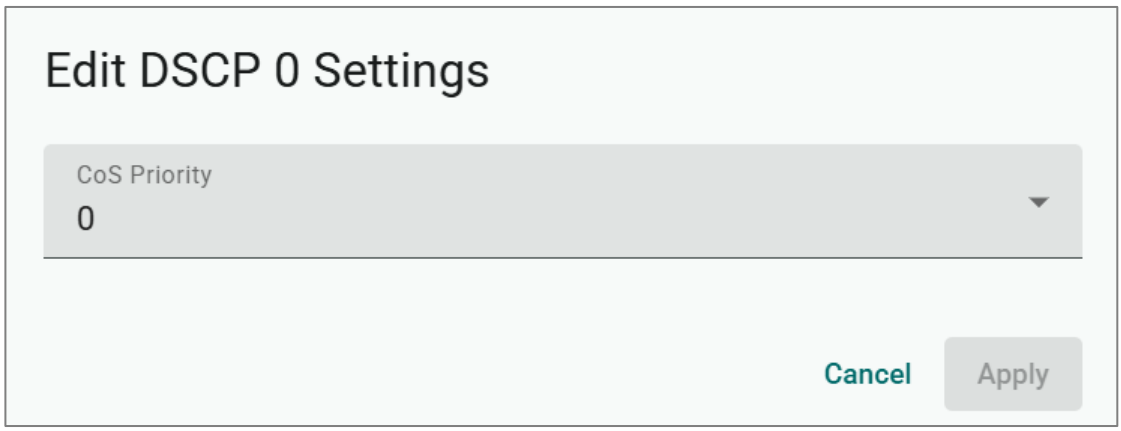
UI Setting	Description
DSCP	Shows the DSCP value for the entry.
CoS Priority	Shows the CoS priority mapped to the DSCP value.

Edit DSCP Settings

Menu Path: Layer 2 Switching > QoS > Classification - DSCP Mapping

Clicking the **Edit (✎)** icon for an entry on the **Layer 2 Switching > QoS > Classification - DSCP Mapping** page will open this dialog box. This dialog lets you edit CoS priority for a DSCP value.

Click **Apply** to save your changes.



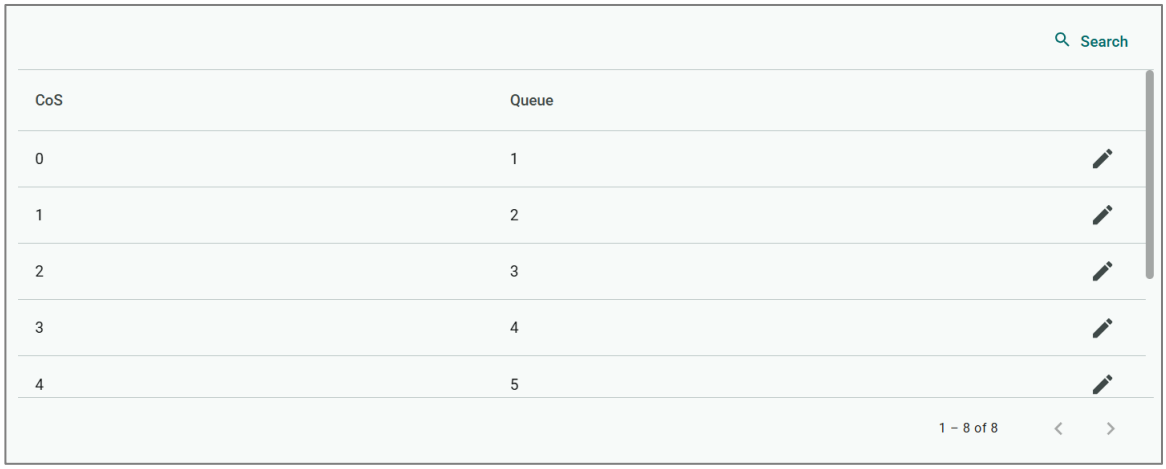
UI Setting	Description	Valid Range	Default Value
CoS Priority	Specify the CoS priority to assign to the DSCP value. Higher numbers have higher priority.	0 to 7	DSCP 0 to 7: 0 DSCP 8 to 15: 1 DSCP 16 to 23: 2 DSCP 24 to 31: 3 DSCP 32 to 39: 4 DSCP 40 to 47: 5 DSCP 48 to 55: 6 DSCP 56 to 63: 7

CoS Mapping

Menu Path: Layer 2 Switching > QoS > Classification - CoS Mapping

This page lets you view and edit your CoS Queue mappings.

CoS Mapping List



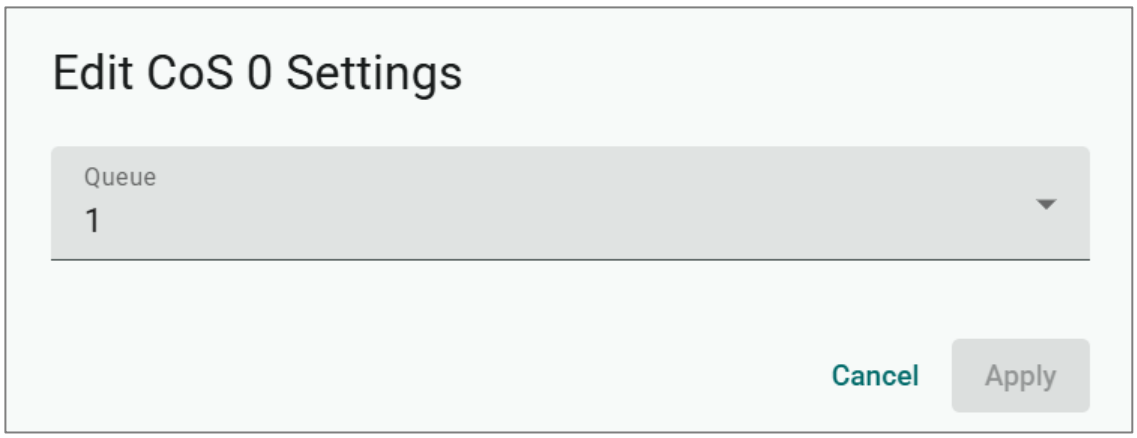
UI Setting	Description
CoS	Shows the CoS value for the entry.
Queue	Shows the queue mapped to the CoS value.

Edit CoS Settings

Menu Path: Layer 2 Switching > QoS > Classification - CoS Mapping

Clicking the **Edit (✎)** icon for a CoS value on the **Layer 2 Switching > QoS > Classification - CoS Mapping** page will open this dialog box. This dialog lets you map a queue to a CoS value.

Click **Apply** to save your changes.



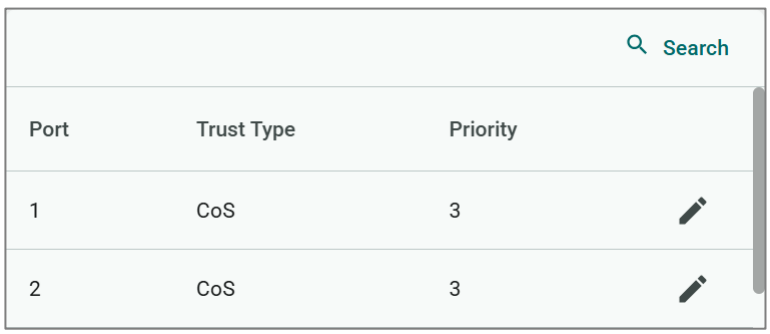
UI Setting	Description	Valid Range	Default Value
Queue	Select a queue to map to the CoS value. Queues with higher numbers have higher priority.	1 to 8	CoS 0: 1 CoS 1: 2 CoS 2: 3 CoS 3: 4 CoS 4: 5 CoS 5: 6 CoS 6: 7 CoS 7: 8

QoS - Port Settings

Menu Path: Layer 2 Switching > QoS > Classification - Port Settings

This page lets you manage the trust type and CoS value for untagged packets on a per-port basis.

Port Settings List



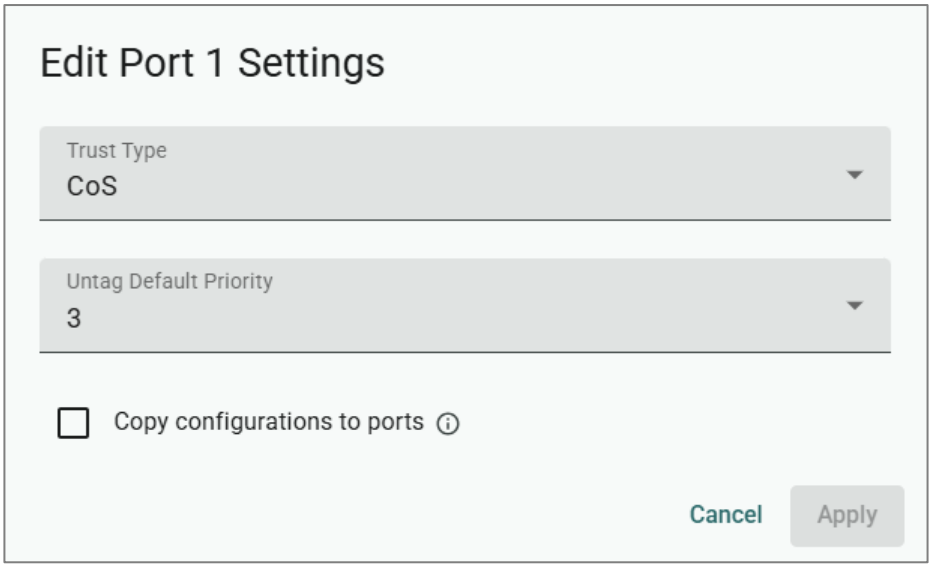
UI Setting	Description
Port	Shows the port number for the entry.
Trust Type	Shows the trust type used to classify traffic for the port.
Priority	Shows the CoS value to use for untagged packets for the port.

QoS - Edit Port Settings

Menu Path: Layer 2 Switching > QoS > Classification - Port Settings

Clicking the **Edit (✎)** icon for a port on the **Layer 2 Switching > QoS > Classification - Port Settings** page will open this dialog box. This dialog lets you edit the trust type and priority for a specific port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Trust Type	Select the trust type used to classify traffic for the port.	CoS / DSCP	CoS
Untag Default Priority	Specify a CoS value to use for untagged packets for the port. Higher values will have higher priority.	0 to 7	3
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

About Ingress Rate Limits

Ingress rate limits drop—or "mark"—network traffic when it exceeds user-defined thresholds.

Ingress Rate Limits In-depth

There are two elements to this process:

- Meter - An algorithm in the switch that monitors and limits traffic by applying QoS markers to data packets or dropping them entirely
- Marker - The DSCP/802.1p field of data packets is assigned a value or "marked" by the QoS policies, determining their handling in the network

Meter algorithms include simple token bucket and SrTCM (Single Rate Three Color Marker) (RFC2697).

In addition to ingress rate management, the switch also offers an option for the administrators to configure the shutdown of an Ethernet port that may be under attack from an excess of incoming packets, such as a Denial-of-Service attack.

About Port Shutdown

Ports can be shutdown to avoid broadcast storms.

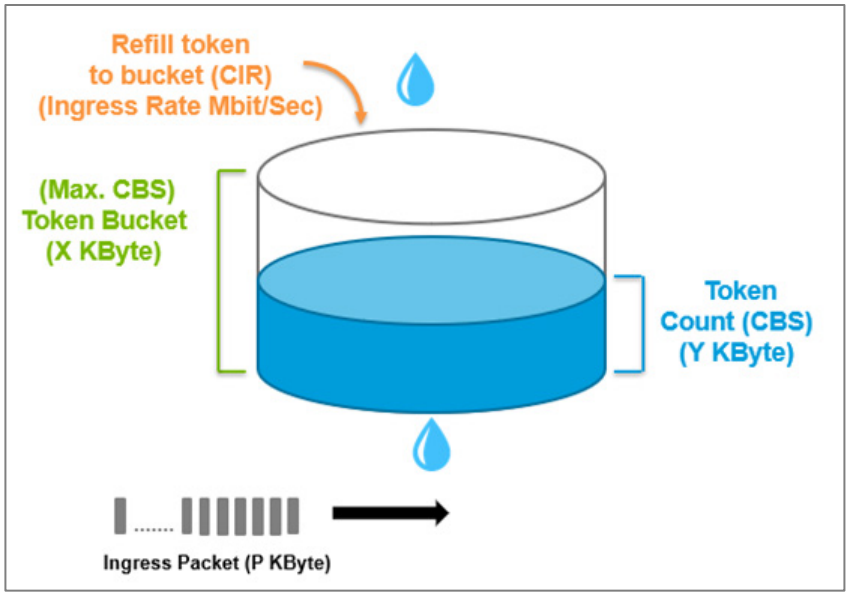
In general, any user shall not consume unlimited bandwidth and influence others' access. One particular scenario is that a malfunctioning switch or mis-configured network might cause "broadcast storms". Moxa industrial Ethernet switches not only prevent broadcast storms, but can also regulate ingress packet rates, giving administrators full control of their limited bandwidth to prevent undesirable effects caused by unpredictable faults.

The network administrator has the option to establish a maximum throughput threshold (in Mbps) for incoming packets on a designated port and activate this function. If unexpected ingress packets are detected on that port, the physical Ethernet port will be disabled, preventing further packet transmission. Re-activation of the port can be done manually or left to occur automatically after the pre-defined release interval, specified in minutes, has elapsed.

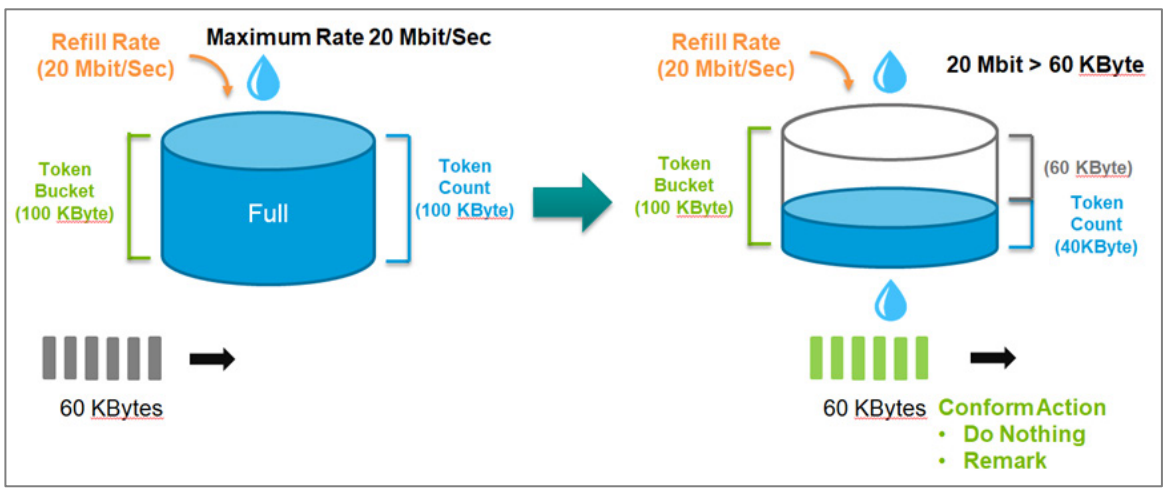
About Token Buckets

Token Bucket is an algorithm used to achieve an efficient network flow control and manage bandwidth. This algorithm is based on a token bucket that allows for a traffic surge for short periods. When a token is unavailable, no burst of packets can be sent. Under this concept, the number of tokens will be refilled in the bucket at specific

intervals. Users need to configure these settings so that the tokens in the bucket are always available to ensure packets can be sent when necessary.



CAR (Committed Access Rate) is a traffic control mechanism used to ensure that packets meet the network rules before they enter the network. CAR can guarantee the traffic flow is under user-defined control; the packets exceeding the rule will be either dropped or remarked and transmitted again. When network traffic is jammed, these packets will be dropped first.



Token Bucket is an algorithm that is demonstrated as a container in the image below. The token can be seen as a marker to mark a packet that is allowed to be transmitted through this switch. When the token is flowing into the bucket, the length of the bucket

will be consumed as the volume of the bucket is limited. When the volume of the bucket is insufficient, some packets will be dropped or remarked and transmitted again. This algorithm can control the speed of the traffic flow by consuming the speed of the token in the bucket.

About Single Rate Three Color Markers

Single Rate Three Color Markers (SrTCM) is a policing scheme for ingress rate limits. Traffic marking is based on a Committed Information Rate (CIR) and two associated burst sizes:

- Committed Burst Size (CBS)
- Excess Burst Size (EBS)

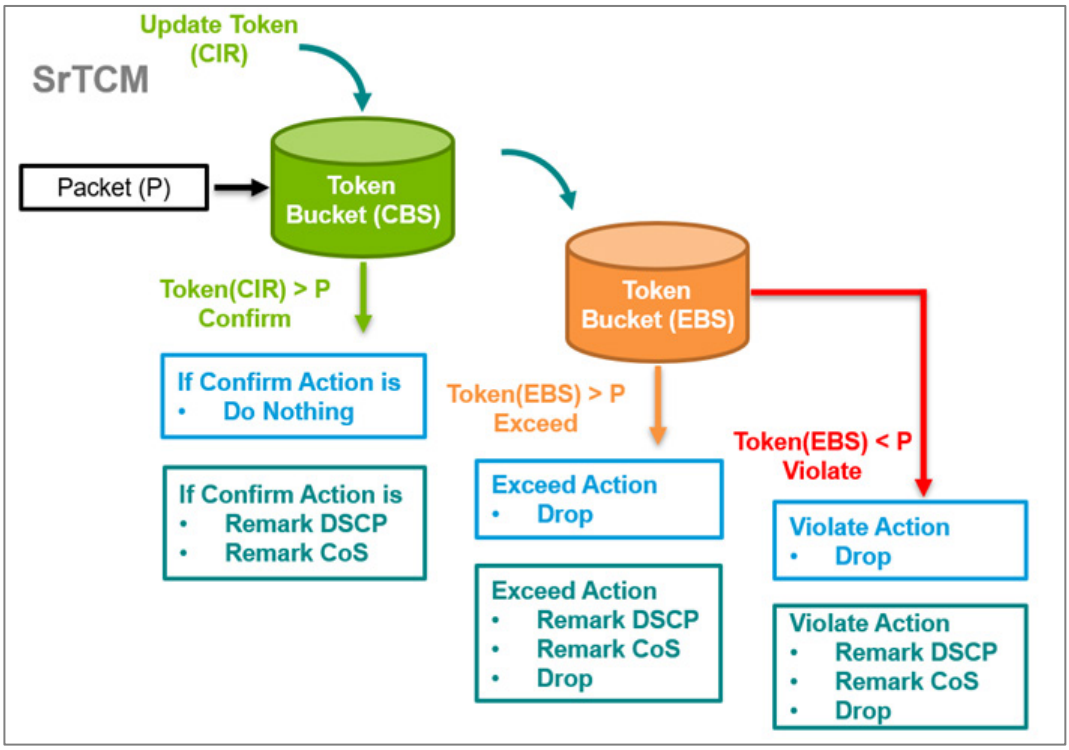
A packet is marked green if it does not exceed the CBS, yellow if it does exceed the CBS, but not the EBS, and red otherwise.

SrTCM will categorize the ingress packet by its length, and mark it as one of three colors:

- **Green:** performs the "conform" action. It could be "Do nothing", "Remark DSCP" or "Remark CoS". The Token Bucket (CBS) will deduct corresponding tokens.
- **Yellow:** performs the "exceed" action. It could be "Drop", "Remark DSCP" or "Remark CoS". The Token Bucket (EBS) will deduct corresponding tokens.
- **Red:** performs the "violate" action. It could be "Drop", "Remark DSCP" or "Remark CoS".

If you select "Do nothing" as the conform action, then "Drop" will be the only action when it enters the Exceed or Violate state.

The SrTCM is useful for ingress policing of a service, where only the length, not the peak rate, of the burst determines service eligibility.



Dropping Limit-exceeding Incoming Packets

You can setup the ingress rate limits that will automatically drop packets exceeding limits you specify.

In this example, we will prevent the switch from being overwhelmed by unexpected large amount of ingress packets through port 1, set an ingress rate limit of 5 Mbps on port 1. Then, verify that the device connected to port 2 receives packets at no more than 5 Mbps.

Before you begin:

- Change the configuration mode to **Advanced** mode by selecting the mode in the upper right corner of the UI.
- Create a new **VLAN ID** with a value of **10**
- Configure Port 1 with a **PVID** of 10 and with **Access mode** enabled
- Configure Port 2 with a **PVID** of 10 and with **Access mode** enabled

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching→QoS→Ingress Rate Limit→General**.

3. Click ***[Edit]*** corresponding to **Port 1**.
   Result: The **Edit Port Settings** dialogue appears.
4. In the **Ingress Rate (CIR)** field, specify 5 Mbps, and then click **Apply**.
   Result: The new Ingress Rate (CIR) will appear in the table.

Results:

When a device connected to port 1 sends out a large number of packets (for example, at a rate exceeding 10 Mbps), the switch will throttle the incoming packets to match the configured limit (5 Mbps in this example) before forwarding them to port 2.

Remarking Limit-exceeding Incoming Packets

Abstract:

Short Description: You can setup the ingress rate limits that will automatically remark packets exceeding limits you specify.

In this example, we will limit incoming packets to 5 Mbps on Port 1—maintaining a consistent ingress rate. To avoid dropping data caused by a sudden influx of packets from Port 1, the outgoing packets will be remarked with a DSCP value (0x07) before sending over Port 2.

Before you begin:

- Change the configuration mode to **Advanced** mode by selecting the mode in the upper right corner of the UI.
- Create a new **VLAN ID** with a value of **10**
- Configure Port 1 with a **PVID** of 10 and with **Access mode** enabled
- Configure Port 2 with a **PVID** of 10 and with **Access mode** enabled

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching→QoS→Ingress Rate Limit→General**.
3. Click ***[Edit]*** corresponding to **Port 1**.
   Result: The **Edit Port Settings** dialogue appears.
4. Specify the following:

Value	Option
Type	**Simple Token Bucket**
Ingress Rate (CIR)	5 Mbps
Conform Action	**Remark DSCP**
Conform Action > Remark Value	**0**
Violate Action	**Remark DSCP**
Violate Action > Remark Value	**7**

5. Click **Apply** to save changes.

Results:

When a device connected to port 1 sends out a large number of packets (for example, at a rate exceeding 10 Mbps), the switch will throttle the incoming packets to match the configured limit (5 Mbps in this example) and remark DSCP value (0x07) without dropping the packets. This ensures the timely transmission of data to the device connected on port 2.

Ingress Rate Limit

Menu Path: Layer 2 Switching > QoS > Ingress Rate Limit

This page lets you configure your device's QoS ingress rate limit.

This page includes these tabs:

- General
- Port Shutdown

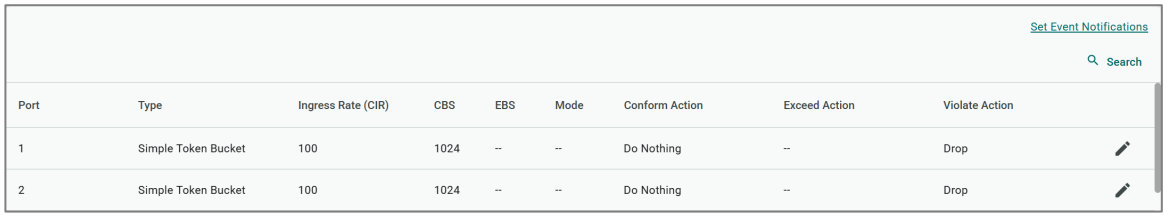
Ingress Rate Limit - General

Menu Path: Layer 2 Switching > QoS > Ingress Rate Limit - General

This page lets you view and edit the ingress rate limit for each port.

Ingress Rate Limit List

> **Note**
> Some fields are only visible when using Advanced Mode.



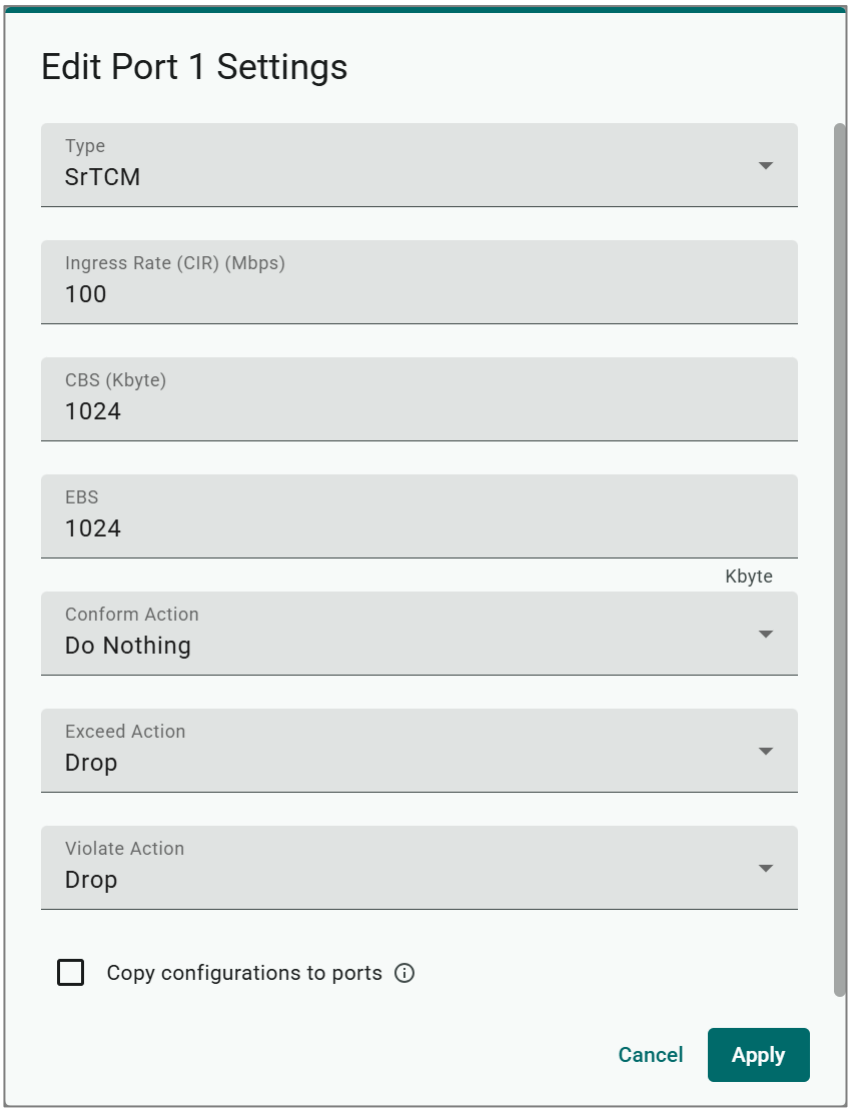
UI Setting	Description
Port	Shows the port number for the entry.
Type **(Only in Advanced Mode)**	Shows the ingress limit type for the port.
Ingress Rate (CIR)	Shows the ingress Committed Information Rate (CIR) value for the port.
CBS **(Only in Advanced Mode)**	Shows the ingress Committed Burst Size (CBS) value for the port.
EBS **(Only in Advanced Mode)**	Shows the ingress Excess Burst Size (EBS) value for the port.
Mode **(Only in Advanced Mode)**	Shows the meter mode for the port.
Conform Action **(Only in Advanced Mode)**	Shows the conform action for the port.
Exceed Action **(Only in Advanced Mode)**	Shows the exceed action for the port.
Violate Action	Shows the violate action for the port.

Ingress Rate Limit - Edit Port Settings

Menu Path: Layer 2 Switching > QoS > Ingress Rate Limit - General

Clicking the **Edit (✎)** icon for a port on the **Layer 2 Switching > QoS > Ingress Rate Limit - General** page will open this dialog box. This dialog lets you select the traffic policy and configure associated actions for specific conditions on a per-port basis.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Type **(Only in Advanced Mode)**	Specify the ingress limit type to use.	Simple Token Bucket / SrTCM	Simple Token Bucket
Ingress Rate (CIR)	Specify the maximum bandwidth allowed for ingress through the port in Mbps.	1 to 1000	100 for Fast Ethernet ports, 1000 for Gigabit Ethernet ports
CBS (Committed Burst Size) **(Only in Advanced Mode)**	Specify the data buffer size in KB for the port that can be used when the data rate exceeds the CIR rate. Data that exceeds the CIR rate will be saved in this buffer, and will be sent when bandwidth is available.	10 to 10240	1024
EBS (Excess Burst Size) **(Only in Advanced Mode, if Type is SrTCM)**	Specify the data buffer size in KB for the port when the data rate exceeds the CIR rate. Data that exceeds the CIR rate will be saved in the CBS buffer, and if the CBS buffer is full, data will be stored in the EBS buffer and will be sent when bandwidth is available.	10 to 10240	1024
Conform Action **(Only in Advanced Mode)**	Select a conform action for the port to take. If **Remark CoS** or **Remark DSCP** is selected, an additional input field will appear where a Remark value must be specified.	Do Nothing / Remark CoS / Remark DSCP	Do Nothing
Exceed Action **(Only in Advanced Mode, if Type is SrTCM)**	Select an action to take if the amount of data exceeds both the CBS and EBS buffers. • **Drop**: Packets marked as yellow will be dropped. • **Remark CoS**: Specify a CoS Remark value to use if a packet is marked as yellow. This is only available if **Remark CoS** is selected for the **Conform Action**. • **Remark DSCP**: Specify a DSCP Remark value to use if a packet is marked as yellow. This is only available if **Remark DSCP** is selected for the **Conform Action**.	Drop / Remark CoS / Remark DSCP	Drop

UI Setting	Description	Valid Range	Default Value
Violate Action	Select an action to take if a packet violates CIR and CBS. • **Drop:** Packets marked as violated will be dropped. • **Remark CoS**: Specify a CoS Remark value to use if a packet is marked as violated. This is only available if **Remark CoS** is selected for the **Conform Action**. • **Remark DSCP**: Specify a DSCP Remark value to use if a packet is marked as violated. This is only available if **Remark DSCP** is selected for the **Conform Action**.	Drop / Remark CoS / Remark DSCP	Drop
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

Port Shutdown

Menu Path: Layer 2 Switching > QoS > Ingress Rate Limit - Port Shutdown

This page lets you enable the port shutdown feature and configure its settings for each port.

Port Shutdown Settings

UI Setting	Description	Valid Range	Default Value
Port Shutdown	Enable or disable the port shutdown feature for the device. **Note** After enabling this, you will still need to configure port shutdown for each port you want to use the feature with.	Enabled / Disabled	Disabled
Release Interval	Specify how long in minutes to wait before a shut down port is enabled again. 0 means if this port is shut down, it will remain shut down until manually enabled.	0 to 10080	60

Port Shutdown List

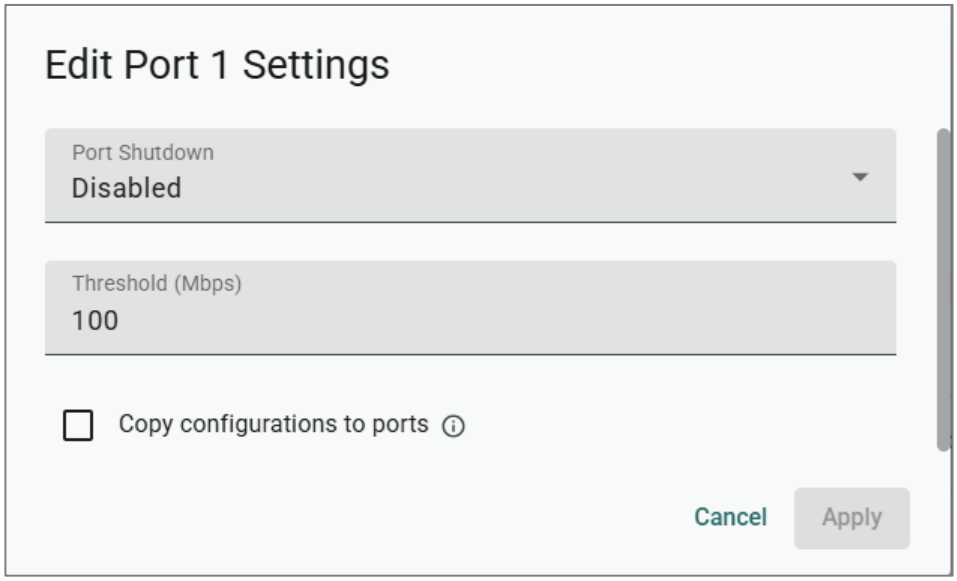
UI Setting	Description
Port	Shows the port number for the entry.
Port Shutdown	Shows whether port shutdown is enabled or disabled for the port.
Threshold (Mbps)	Shows the threshold in Mbps required to trigger port shutdown for the port.

Port Shutdown - Edit Port Settings

Menu Path: Layer 2 Switching > QoS > Ingress Rate Limit - Port Shutdown

Clicking the **Edit (✎)** icon for a port on the **Layer 2 Switching > QoS > Ingress Rate Limit - Port Shutdown** page will open this dialog box. This dialog lets you configure the threshold to trigger port shutdown.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Port Shutdown	Enable or disable port shutdown for this port.	Enabled / Disabled	Disabled
Threshold	Specify the threshold (Mbps) required to trigger a port shutdown.	Fast Ethernet ports: 1 to 100 Gigabit Ethernet ports: 1 to 1000	Fast Ethernet ports: 100 Gigabit Ethernet ports: 1000
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

About Scheduler

The Scheduler functions as an arbiter within the switching forwarding paths, prioritizing traffic flows based on user-defined criteria. This mechanism enhances data transmission efficiency and ensures that critical packets are transmitted with priority. Moxa devices support below scheduling algorithms: Strict Priority, Weighted Round Robin and mix of both.

- **Weighted Round Robin:** The Weighted Round Robin type allows users to give priority to specific packets in the higher weighted queue to ensure those packets will be sent first. Moxa switches now have 8 queues, and the weights from highest to lowest are 8:8:4:4:2:2:1:1.

- **Strict Priority:** The Strict Priority type allows users to determine to transmit packets in the highest priority queue first, while packets with lower priority will be transmitted later. This guarantees that traffic with the highest level of priority for data transmission will go first.
- **Strict Priority and Weighted Round Robin:** Supports one Strict Priority with seven Weighted Round Robin or two Strict Priority with six Weighted Round Robin.

Moxa network devices are equipped with multiple traffic queues that enable packet prioritization. This allows higher-priority traffic to pass through the network devices without being delayed by lower-priority traffic. As each packet enters the network devices, it undergoes ingress processing, including classification and marking/re-marking, before being placed into the appropriate egress queue. The network device then forwards packets based on their assigned queue.

Scenario: Configuring 3 Devices with Strict Priority

In this scenario, we will configure three attached devices on the network device with strict priority.

Specifically, we will focus on how packets are managed as they leave (egress) the network device on a particular port. In this case, the setup involves three devices:

- **Device A**: Connected to port 1 on the network device.
- **Device B**: Connected to port 2 on the network device.
- **Device C**: Connected to port 3 on the network device.

Objective

The goal is to configure a "Strict Priority" scheduler on port 3 of the switch. This scheduler will control how packets are prioritized when they exit the switch from this port (which is connected to Device C).

Key Components

1. **DSCP (Differentiated Services Code Point) Value**:
    - This is a field in the IP header that indicates the level of priority a packet should have.

- In this scenario, packets from Device A have a DSCP value of `0x48`, which signifies they should be treated with higher priority.

2. **Egress Queues**:
    - Network switches typically have multiple egress queues per port. Each queue can be assigned different levels of priority.
    - In this case, queue 7 is configured as a high-priority queue, while queue 1 is a lower-priority queue.

Configuration Details

- **Device A (port 1)** is sending packets with a DSCP value of `0x48`. These packets are mapped to egress queue 7 on port 3. Queue 7 is given a higher priority.
- **Device B (port 2)** is sending normal packets without any special DSCP value, so these packets are mapped to egress queue 1 on port 3. Queue 1 has a lower priority.

"Strict Priority" Scheduler

- **Strict Priority Scheduling** is a mechanism used to determine how packets are sent out when multiple queues have packets waiting to be transmitted.
- In a strict priority setup, the switch will always service higher-priority queues first. This means that as long as there are packets in queue 7 (the high-priority queue), they will be sent out before any packets in queue 1 (the lower-priority queue) are even considered.

Expected Behavior

- When **Device A and Device B** both send packets to **Device C** at the same time:
    - Packets from **Device A** (with DSCP `0x48`) will be placed in the high-priority egress queue 7 and will be transmitted first.
    - Packets from **Device B** will be placed in the low-priority egress queue 1. These packets will only be transmitted once queue 7 is empty.
- As a result, packets from **Device A** will reach **Device C** quickly, without being delayed by the packets from **Device B**.

Summary

By configuring the scheduler with "Strict Priority" on port 3, we're ensuring that high-priority traffic (from Device A) is not delayed by lower-priority traffic (from Device B). This setup is crucial in scenarios where certain types of data, such as real-time communications or critical control signals, must be delivered promptly without delay.

Example: Configuring A Sample Environment for Strict Priority Scheduler (TN_Series)

The QoS scheduler example relies on this configuration.

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching** > **VLAN** > **Settings**, and then click ***[Add]***.

   The Create VLAN screen appears.
3. In **VLAN**, type `10`, and then click **Create**.

   The specified VLAN appears in the list.
4. In the table on the second half of the page, find **1** and click **[Edit].**

   The Edit Port Settings screen appears.
5. Specify **Mode** as **Access**, and then specify a **PVID** of **10**.
6. Under **Copy configurations to ports**, choose ports **2** and **3**, and then click **Apply** to save changes.
7. Go to **Layer 2 Switching** > **QoS** > **Classification**, and under **DSCP Mapping**, locate **DSCP** 48 and verify that it is set to **6**.

   If the value is different, click **[Edit]**, set **CoS Priority** to **6**, and then click **Apply**.
8. Click **CoS Mapping** at the top of the screen, locate **CoS 6**, and verify that **Queue** is set to **7**.

   If the value is different, click **[Edit]**, set **Queue** to **7**, and then click **Apply**.

The device on Port **3** needs to be configured to set its outgoing packets with a QoS DSCP value of `0x48`.

Example: Configuring Scheduler for Strict Priority (TN Series)

Strict Priority switching ensures that higher priority packets always preempt loc

This example assumes the following configuration, outlined in the preceding section:

- VLAN of 10
- Ports **1**, **2**, and **3** in **Access** mode assigned to **PVID** 10
- **DSCP** 48 set to **6**
- **CoS 6** with a **Queue** of **7**

Additionally, the device on Port **3** needs to be configured to set its outgoing packets with a QoS DSCP value of 0x48.

If your environment does not match the above configuration, the example may not function properly.

1. Sign in to the devices using administrator credentials.
2. Go to **Layer 2 Switching** > **QoS** > **Scheduler**.
3. Locate Port **3**, and then click **[Edit]**.

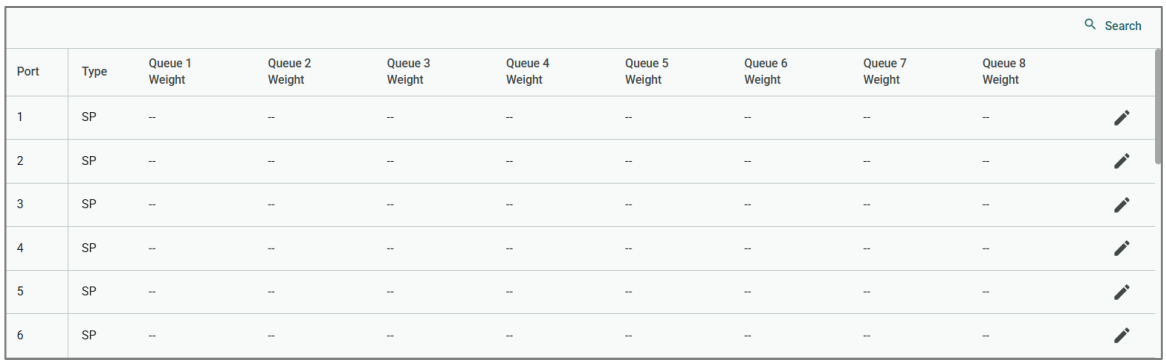
   The Edit Port Settings screen appears.
4. Make sure **Type** is set to **Strict Priority**, and then click **Apply**.

Scheduler

Menu Path: Layer 2 Switching > QoS > Scheduler

This page lets you configure your device's QoS scheduler on a per-port basis.

Scheduler List



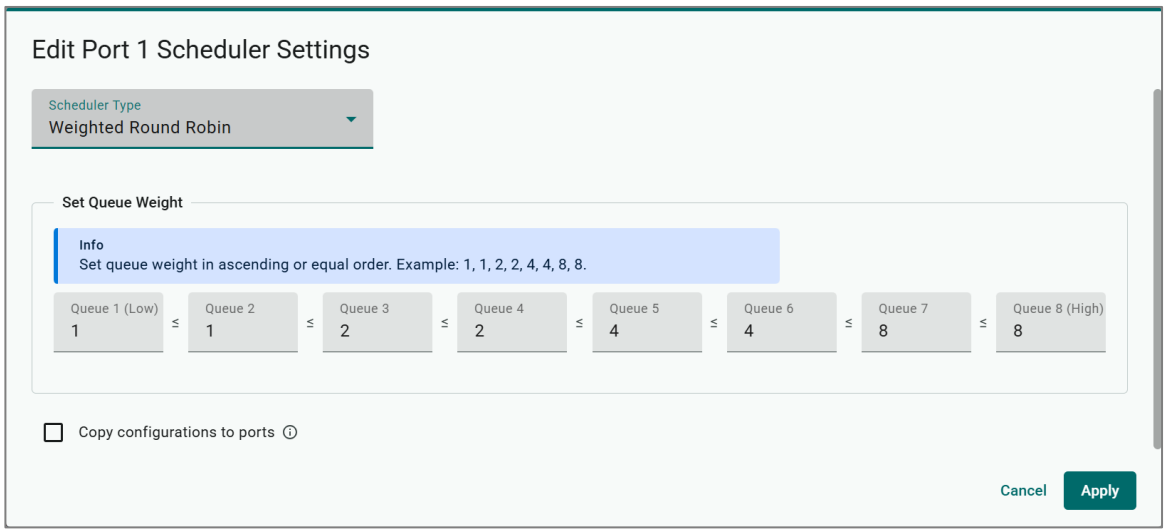
UI Setting	Description
Port	Shows the port number for the entry.
Type	Shows the scheduling algorithm selected for the port.
Queue 1 - 8 Weight	Shows the weight associated with the queue. SP indicates the queue uses strict priority.

Scheduler - Edit Port Settings

Menu Path: Layer 2 Switching > QoS > Scheduler

Clicking the **Edit (✎)** icon for a port on the **Layer 2 Switching > QoS > Scheduler** page will open this dialog box. This dialog lets you select the scheduling algorithm for the port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Scheduler Type	Select the scheduler algorithm to use for the port. • **Strict Priority**: Strict priority will be used. • **Weighted Round Robin**: Queued packets will be forwarded based on their associated weight. • **1SP7WRR**: Queue 8 will use Strict Priority and the packets in other queues will be forwarded based on their associated weight. • **2SP6WRR**: Queues 7 and 8 will use Strict Priority and the packets in other queues will be forwarded based on their associated weight.	Strict Priority / Weighted Round Robin / 1SP7WRR / 2SP6WRR	Strict Priority
Queue 1 - 8	Specify the weight for packets forwarded in each queue. **Note** If Scheduler Type is 1SP7WRR, Queue 8 will be fixed to strict priority (SP). If Scheduler Type is 2SP6WRR, Queues 7 and 8 will be fixed to strict priority (SP).	1 to 8 Subsequent queue weights must be equal or higher than the previous one.	1,1,2,2,4,4,8,8
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

Scenario: Configuring 3 Devices with Strict Priority and Weighted Round Robin(2SP6WRR)

In this scenario, we will configure three attached devices on the network device with strict priority and weighted round robin.

Specifically, we will focus on how packets are managed as they leave (egress) the network device on a particular port. In this case, the setup involves three devices:

- **Device A**: Connected to port 1 on the network device.
- **Device B**: Connected to port 2 on the network device.
- **Device C**: Connected to port 3 on the network device.

Objective

The goal is to configure two "Strict Priority" and "Weighted Round Robin" scheduler on port 3 of the switch. This scheduler will control how packets are prioritized when they exit the switch from this port (which is connected to Device C).

Key Components

1. **CoS (Class of Services) Value**:
    - This is a field in the Ethernet frame header for 802.1Q VLAN tagged frames that indicates the level of priority a packet should have.
    - In this scenario, you want to make sure GOOSE and SMV packets from Device A and Devices B to be treated with highest priority and some user-defined packets have the corresponding traffic bandwidth.
2. **Egress Queues**:
    - Network switches typically have eight egress queues per port. Each queue can be assigned different levels of priority.
    - In this case, queue 7 and queue 8 are reserved as high-priority queues(strict priority), while queue 1 to queue 6 are lower-priority queues(weighted round robin) and you can configured the egress weighted bandwidth for them.

Configuration Details

- **Device A (port 1) & Device B (port 2)**

    - You can remark CoS value of GOOSE and SMV packets as 6 and 7 in ACL MAC rule by configuring Rule Type as Permit, Ether Type as GOOSE and SMV, CoS set as 6 and 7. Then the GOOSE and SMV packets will be mapped to egress queue 7 and queue 8 on port 3.
    - You can specify some user-defined packets with certain Ether Type for CoS value 0-5 using ACL MAC rule mentioned above. These packets will be mapped to egress queue 1~6 depends on the CoS value you set.
- **Device C (port 3)**
    - You can configure Scheduler Type in Scheduler Setting as 2SP6WRR. SP stands for Strict Priority and 2SP are queue 7 and queue 8. WRR stands for Weighted Round Robin, 6WRR are queue 1~queue 6, and you can specify the weighted bandwidth for queue 1~6.

"Strict Priority" Scheduler

- **Strict Priority Scheduling** is a mechanism used to determine how packets are sent out when multiple queues have packets waiting to be transmitted.
- In a strict priority setup, the switch will always service higher-priority queues first. This means that as long as there are packets in queue 7 (the high-priority queue), they will be sent out before any packets in queue 1 (the lower-priority queue) are even considered.

"Strict Priority" and "Weighted Round Robin" Scheduler (under construction)

- **Strict Priority and Weighted Round Robin Scheduling** are mechanism used to determine how packets are sent out when multiple queues have packets waiting to be transmitted.
- In a strict priority setup, the switch will always service higher-priority queues first. This means that as long as there are packets in queue 7 (the high-priority queue), they will be sent out before any packets in queue 1 (the lower-priority queue) are even considered.
- In weighted round robin Scheduling setup, the packets will be sent out after strict priority queue empty and receive the bandwidth according to the weighted you configures for WRR queue.

Expected Behavior

- When **Device A and Device B** both send packets to **Device C** at the same time:

- GOOSE and SMV Packets from **Device A** and **Devices B** will be placed in the high-priority egress queue 7 and 8 , and will be transmitted first.
- Other Packets from **Device A** and **Device B** will be placed in the low-priority egress queue 1~queue 6. These packets will only be transmitted once queue 7 is empty and the transmitted bandwidth are based on the weighted you configure for queue 1~6.

- As a result, GOOSE and SMV packets from **Device A** and **Devices** B will reach **Device C** quickly, without being delayed by the other packets.

Summary

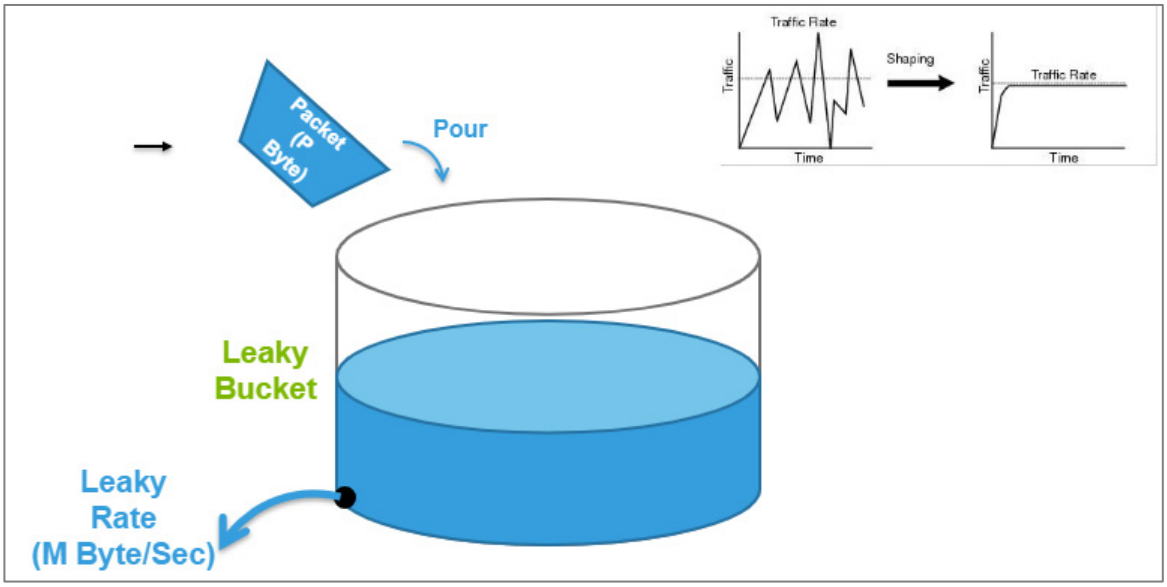
By configuring remark CoS for the scheduler with "Strict Priority" and "Weighted Round Robin" on port 3, we're ensuring that high-priority traffic is not delayed by lower-priority traffic and the lower-priority packets still transmitted based on the bandwidth you specify for them. This setup is crucial in scenarios where certain types of data, such as real-time communications or critical control signals, must be delivered promptly without delay.

Configuring Egress Shaper

A shaper for egress traffic buffers or queses excess traffic to hold packets and shape traffic flow when source data rates are higher than expected.

About Egress Shaper

The Egress Shaper uses a meter algorithm known as a leaky bucket. Like its physical counterpart, the leaky bucket collects incoming traffic up to a maximum capacity. Data stored in the bucket is released at a steady rate. When the bucket is empty, the flow stops.



If incoming packets would exceed the capacity the bucket, those packets would be non-conforming, and are not added to the bucket (dropped). Data will be added to the bucket as space becomes available for conforming packets. To setup Egress Shaper on a specific port, you will need to provide CIR (Committed Information Rate) and CBS (Committed Burst Rate) values.

Configuring Rate Limits for Outgoing Traffic

You can use egress rate limits to ensure steady flow of traffic to ports you specify. In this scenario, we have 3 devices:

- Device A, connected to the switch at Port 1
- Device B, connected to the switch at Port 2
- Device C, connected to the switch at Port 3

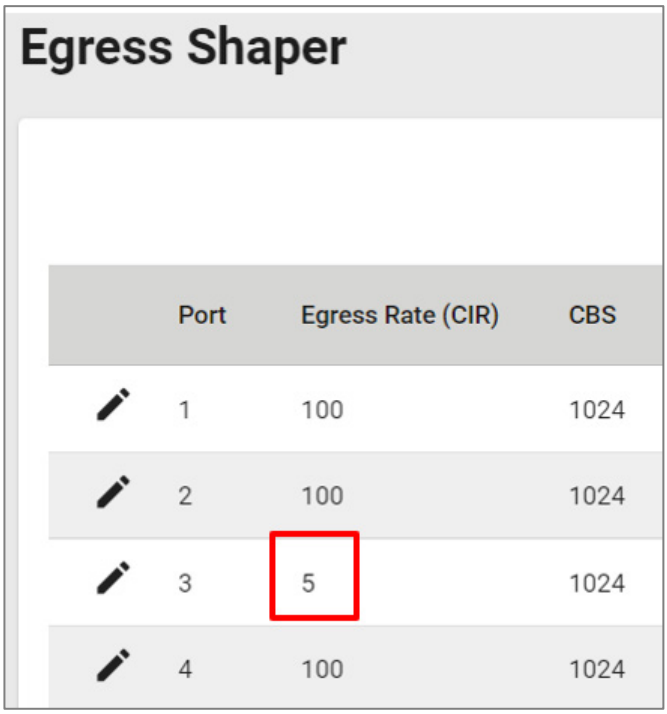
When both Device A and Device B send packets simultaneously to Device C, and there are no rate limits set on ports 1 and 2, Configuring the Committed Information Rate (CIR) to 5 Mbps on port 3 ensures that the outgoing packets maintain a steady packet rate to reach Device C as expected.

Before you begin:

- Change the configuration mode to **Advanced** mode by selecting the mode in the upper right corner of the UI.
- Create a new **VLAN ID** with a value of **10**

- Configure Port 1 with a **PVID** of 10 and with **Access mode** enabled
- Configure Port 2 with a **PVID** of 10 and with **Access mode** enabled
- Configure Port 3 with a **PVID** of 10 and with **Access mode** enabled

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching > QoS > Egress Shaper**.
3. Click ***[Edit]*** corresponding to **Port 3**.
   Result: The **Edit Port Settings** dialogue appears.
4. In the **CIR** field, specify 5 Mbps, and then click **Apply**.
   Result: The new Egress Rate (CIR) will appear in the table.



Egress Shaper

Menu Path: Layer 2 Switching > QoS > Egress Shaper

This page lets you configure QoS egress shaper settings on a per-port basis.

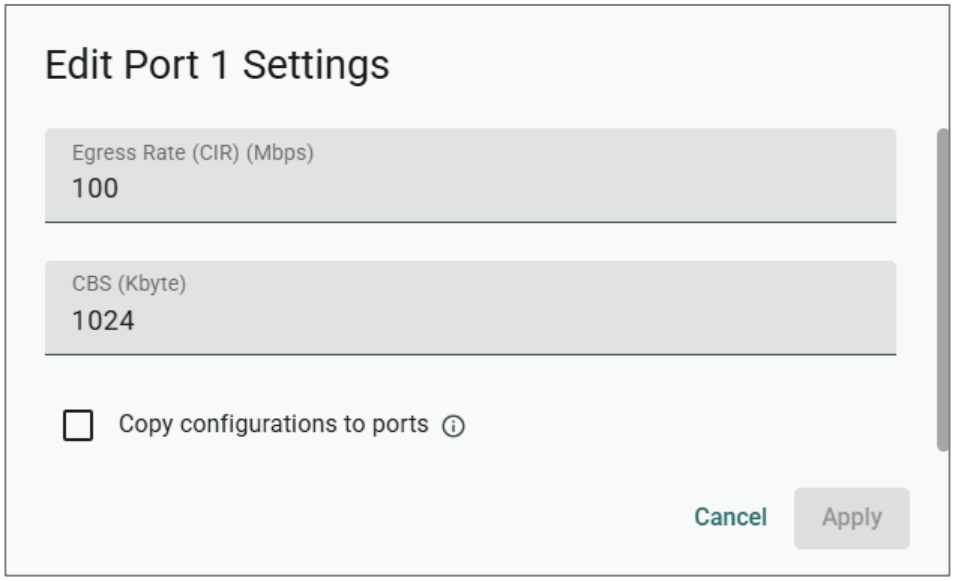
UI Setting	Description
Port	Shows the port number the entry is for.
Egress Rate (CIR)	Shows the egress Committed Information Rate (CIR) value for the port.
CBS **(Only in Advanced Mode)**	Shows the egress Committed Burst Size (CBS) value for the port.

Egress Shaper - Edit Port Settings

Menu Path: Layer 2 Switching > QoS > Egress Shaper

Clicking the **Edit (✎)** icon for a port on the **Layer 2 Switching > QoS > Egress Shaper** page will open this dialog box. This dialog lets you configure the egress shaping settings for the port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Egress Rate (CIR)	Specify the egress Committed Information Rate (CIR) in Mbps.	Fast Ethernet ports: 1 to 100 Gigabit Ethernet ports: 1 to 1000	Fast Ethernet ports: 100 Gigabit Ethernet ports: 1000
CBS **(Only in Advanced Mode)**	Specify the Committed Burst Size (CBS) in KB. This is the maximum amount of data allowed to be transmitted in a burst, even if it would cause the CIR rate to be exceeded.	10 to 10240	1024
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

Multicast

Multicast is a one-to-many communication method that sends data to a specific group of receivers. Those who wish to receive multicast packets must register for the multicast service; unregistered recipients will not receive the packets. Multicast is an "on-demand" service typically used for audio and video applications. For example, IP cameras (commonly used in CCTV systems) may need to transmit video streams to three different

security guard rooms in a building simultaneously. Multicast is also used for protocol exchanges, as L3 protocols (VRRP, OSPF, RIP, etc) communicate with each other using multicast.

Benefits of Multicast:

- **Efficient bandwidth utilization:** Multicast reduces network congestion by sending data to only interested recipients.
- **Reduced server load:** Multicast servers only need to send data once, rather than multiple times for individual recipients.
- **Scalability:** Multicast can effectively handle large groups of receivers without affecting network performance.

Overall, multicast is a valuable tool for efficient and scalable one-to-many communication, particularly in applications involving audio, video, and protocol exchanges.

Multicast In Depth

As mentioned, multicast is a network communication method designed for efficient one-to-many data transmission. Imagine you have a presentation you want to deliver to a specific group of people in a large conference hall. Instead of emailing it to everyone individually, multicast allows you to send it to a single "group" that only the intended recipients can access.

Here's a breakdown of how it works:

- **Groups and Membership:**
    - Devices interested in receiving the same data stream form a multicast group identified by a unique multicast address.
    - Devices join or leave the group dynamically using protocols like IGMP (Internet Group Management Protocol).
- **Source and Data:**
    - A single source device transmits the data (e.g., a video stream, a software update).
    - The data is encapsulated with the specific multicast address of the target group.

- **Network Routing:**
    - Network switches and routers play a crucial role in directing the data.
    - They recognize the multicast address and replicate the data packet only for the ports connected to devices that are members of the target group.
    - Devices not in the group will not receive the data, reducing unnecessary network traffic.

There are three primary methods for controlling multicast traffic on a switch:

- **Static multicast** is for configuring the multicast forwarding entries in the switch in a manual or predetermined manner. (e.g., forward 01:00:5E:05:06:07 to ports 1, 2, and 3). This method suits static networks where you want to control all the multicast flow. Another scenario is that the end device cannot communicate with IGMP protocol.
- **GMRP** allows bridges and the devices at the edge of the network to perform dynamic group membership information registration with the MAC bridges connected to the same LAN section. This method lets bridges communicate with each other to register the static multicast table dynamically.
- **IGMP snooping** allows a device to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the device maintains an association mapping table between port(s) and multicast groups. This method suits dynamic networks where end devices use IGMP to register the multicast group.

In summary, here are key considerations when selecting a multicast traffic control method:

- For static networks with predetermined multicast destinations, **static multicast** offers a simple solution.
- If you have a network with multiple bridges and static multicast tables on edge devices, **GMRP** can help maintain consistency.
- In dynamic networks where end devices use IGMP, **IGMP snooping** provides efficient management of multicast traffic.

Multicast

Menu Path: Layer 2 Switching > Multicast

This section lets you configure the Multicast settings.

This section includes these pages:

- IGMP Snooping
- GMRP
- Static Multicast

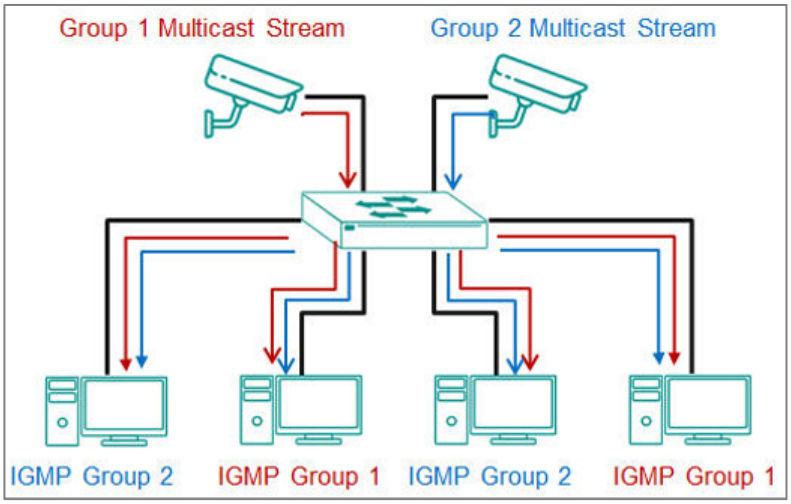
About IGMP Snooping

IGMP snooping allows switches to reduce the amount of unwanted multicast traffic on a network by maintaining maps of multicast group members, ensuring that multicast packets are only delivered to devices that have explicitly asked to receive them. Internet Group Management Protocol (IGMP) is a network protocol that hosts nearby routers on networks to construct multicast group memberships. IGMP snooping allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains an association mapping table between port(s) and multicast group.

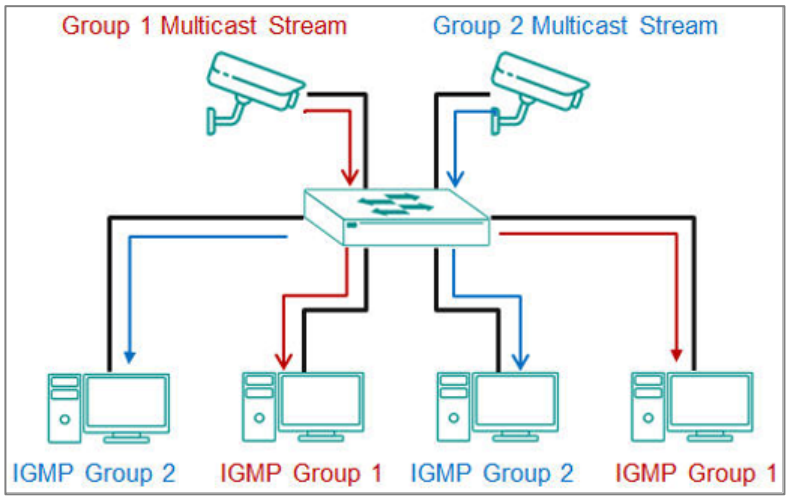
How IGMP Snooping Works

Without IGMP snooping, a switch will flood multicast traffic to all other non-ingress ports within a broadcast domain (or VLAN). This can cause unnecessary loading for host devices by requiring them to process packets they have not solicited. IGMP snooping can help prevent host devices on a local network from receiving traffic for a multicast group they have not explicitly joined. It provides switches with a mechanism to forward multicast traffic to specific ports that receive IGMP hosts, resulting in more efficient network bandwidth utilization.

Without IGMP Snooping:



With IGMP Snooping:



Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

Enabling IGMP Snooping

IGMP Snooping must be enabled before it can be configured on specific interfaces.

To enable IGMP snooping, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching** > **Multicast** > **IGMP Snooping** and click **General**.

3. Set **IGMP Snooping** to **Enabled**.
4. Click **Apply**.

IGMP snooping is now enabled. Existing IGMP snooping configurations will now be active.

Configuring IGMP Snooping

IGMP snooping is configured at the VLAN level.

- VLAN IDs must be created and assigned before IGMP snooping can be configured.
- IGMP Snooping must be enabled before it can be configured on specific interfaces.

To configure IGMP snooping, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching** > **Multicast** > **IGMP Snooping**, and click **VLAN Settings**.

   The **IGMP Snooping** list of **VLAN IDs** appears.

3. Click **[Edit]** corresponding to the VLANs on which to configure IGMP snooping.

   Note: If you do not see the VLANs you expect, make sure they are correctly assigned.

   The Edit VLAN Settings screen appears.

4. Configure all of the following:

Option	Value
IGMP Snooping	**Enabled**
Version	Choose a version corresponding to device support and feature needs.
Query Interval	125
Static Router Port	This is optional.
Config Role	**Querier**

5. Click **Apply**.

About IGMP Versions

IGMP protocols regulate the communication mechanism between querier and listener.

For IGMP-related settings, ensure that you have chosen the correct protocol version. Consult the table below for guidelines on choosing a version.

IGMP Version	Features	Reference
v1	Features: • **Multicast Group Membership:** Host devices can join multicast groups, but there is no explicit leave message. The host will simply stop responding to membership queries. • **Membership Query:** Network devices periodically send membership queries to determine if any host devices are still interested in receiving multicast traffic. • **Membership Report:** When a host device wants to join a multicast group, it sends a membership report. If no reports are received for a multicast group, the network device assumes there are no interested hosts and stops forwarding traffic to that group. Limitations: No Leave Group Message: Hosts cannot explicitly leave a multicast group, which can lead to inefficient use of resources as routers have to rely on timeouts to determine if there are no more members.	RFC-1112
v2	Additional features: • **Leave Group Message:** Host devices can send a leave group message to notify the network device they are no longer interested in a multicast group, improving the efficiency of multicast traffic management. • **Group-Specific Queries:** Network devices can send group-specific queries to confirm if any members of a particular multicast group still exist, reducing overall network traffic compared to general queries. • **Query Election:** Introduces a mechanism to elect a single query router on a subnet to avoid redundant queries, thereby optimizing network bandwidth.	RFC-2236
v3	Additional Features: • **Source-Specific Multicast (SSM):** Supports source filtering, allowing host devices to specify from which sources they receive multicast traffic. This is useful for applications that need to filter out unwanted traffic from certain sources. • **Include/Exclude Mode:** Host devices can explicitly include or exclude traffic from specified sources, providing more granular control over multicast group membership. • **Membership Report Enhancements:** The membership report format is enhanced to support the new source filtering capabilities.	RFC-3376

> **Note**
>
> Although most modern devices should support v3, there may be regulatory concerns or legacy deployments to consider.

IGMP Snooping

Menu Path: Layer 2 Switching > Multicast > IGMP Snooping

This page lets you configure IGMP snooping for your device.

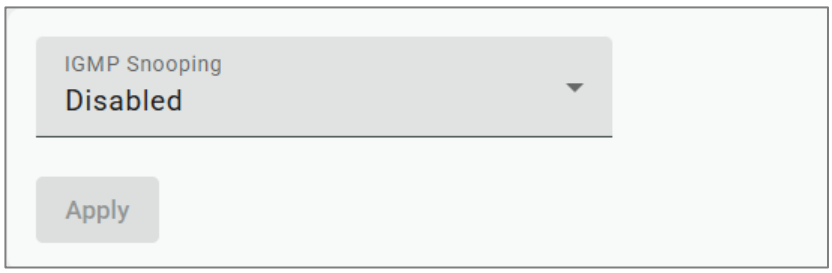
This page includes these tabs:

- General
- VLAN Settings
- Group Table
- Forwarding Table

IGMP Snooping - General

Menu Path: Layer 2 Switching > Multicast > IGMP Snooping - General

This page lets you configure IGMP snooping general settings.

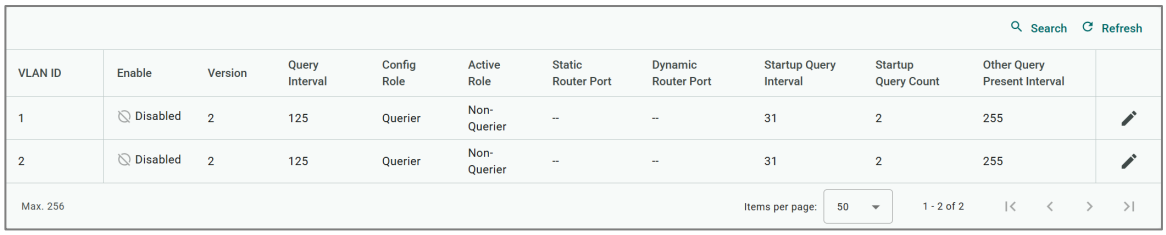


UI Setting	Description	Valid Range	Default Value
IGMP Snooping	Enable or disable IGMP snooping for the device. **Note** IGMP Snooping cannot be enabled when GMRP is enabled.	Enabled / Disabled	Disabled

IGMP Snooping - VLAN Settings

Menu Path: Layer 2 Switching > Multicast > IGMP Snooping - VLAN Settings

This page lets you configure IGMP snooping VLAN settings.



UI Setting	Description
VLAN ID	Shows the ID of the VLAN ID the entry is for.
Enable	Shows whether IGMP snooping is enabled for the VLAN.
Version	Shows the IGMP version of the packets the VLAN will listen to and send queries for.
Query Interval	Shows the query interval for the Querier function globally for the VLAN, if the Querier is enabled.
Config Role	Shows the config role of the VLAN.
Active Role	Shows the active role of the VLAN.
Static Router Port	Shows the static router port for the VLAN. This is the port that connects to the upper level router (or IGMP querier), or to the upper level router of downstream multicast streams. All received IGMP signaling packets and multicast streams will be forwarded to the static router ports.
Dynamic Router Port	Shows the dynamic router port for the VLAN.
Startup Query Interval **(Only in Advanced Mode)**	
Startup Query Count **(Only in Advanced Mode)**	

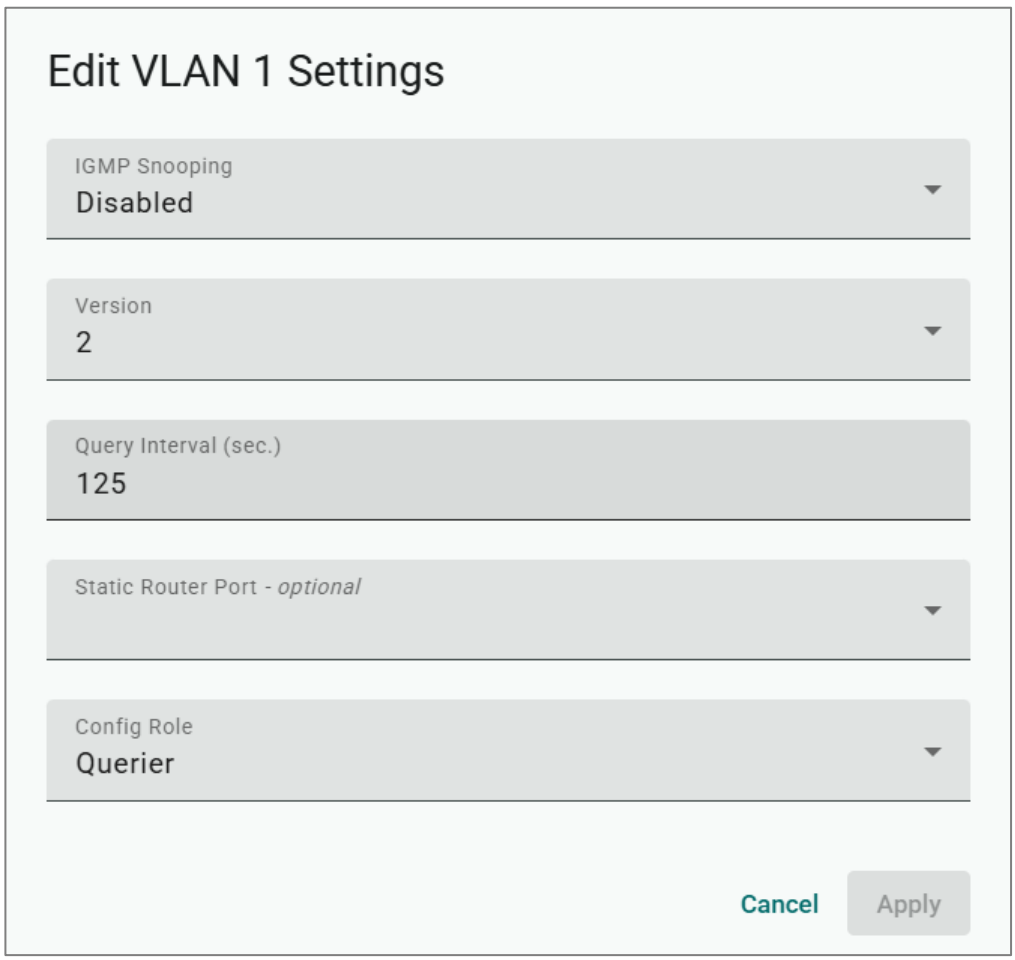
UI Setting	Description
Other Query Present Interval **(Only in Advanced Mode)**	

IGMP Snooping - Edit VLAN Settings

Menu Path: Layer 2 Switching > Multicast > IGMP Snooping - VLAN Settings

Clicking the **Edit (✎)** icon for a VLAN on the **Layer 2 Switching > Multicast > IGMP Snooping - VLAN Settings** page will open this dialog box. This dialog lets you edit the IGMP snooping settings for the VLAN.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
IGMP Snooping	Enable or disable IGMP snooping for the VLAN.	Enabled / Disabled	Disabled
Version	Specify the IGMP version of the packets to listen to and send queries for.	1 / 2 / 3	2
Query Interval	Specify the query interval for the VLAN, if the Querier is enabled.	20 to 600 sec.	125 sec.
Static Router Port	Select a static router port for the VLAN. This is the port that connects to the upper level router (or IGMP querier), or to the upper level router of downstream multicast streams. All received IGMP signaling packets and multicast streams will be forwarded to the static router ports.	Drop-down list of ports	N/A
Config Role	Select the config role for the VLAN.	Querier / Non-Querier	Querier

Group Table

Menu Path: Layer 2 Switching > Multicast > IGMP Snooping - Group Table

This page lets you view the IGMP snooping group table.

Limitations

There can be up to 1024 IGMP snooping group table entries.

Item	Description
VLAN	Shows the ID of the VLAN the entry is for.

Item	Description
Group Address	Shows the registered multicast group address for the VLAN.
Filter Mode	Shows the filter mode for the VLAN. This is only applicable for IGMPv3. • **Include**: Source-specific multicast address group • **Exclude**: Source-specific exclusive multicast address group
Port	Shows the forwarding port for the VLAN.
Source Address	Shows the source address for the VLAN. This is only applicable for IGMPv3.

IGMP Snooping - Forwarding Table

Menu Path: Layer 2 Switching > Multicast > IGMP Snooping - Forwarding Table

This page lets you view the IGMP snooping forwarding table.

Limitations

There can be up to 1024 IGMP snooping forwarding table entries.

Item	Description
VLAN	Shows the ID of the VLAN the entry is for.
Group Address	Shows the associated multicast group address for streaming data for the VLAN.
Source Address	Shows the source address for streaming data for the VLAN.
Port	Shows the forwarding port of the VLAN.

About GMRP

GMRP stands for GARP Multicast Registration Protocol, which is a Generic Attribute Registration Protocol (GARP) application that can be used to prevent multicast from data flooding.

Both GMRP and GARP are defined by IEEE 802.1P, and widely used as a standard protocol in various industrial-related applications. GMRP allows bridges and the devices at the edge of the network to perform a dynamic group membership information registration with the MAC bridges connected to the same LAN section. The information can be transmitted among all bridges in the Bridge LAN that is implemented with extended filtering features. To operate GMRP, the GARP service must be established first.

GARP stands for **Generic Attribute Registration Protocol**, which is a communication protocol defined by IEEE 802.1, offering a generic framework for bridges to register and de-register an attribute value. In a LAN structure, two applications can be applied: **GARP VLAN Registration Protocol (GVRP)** is used to register VLAN trunking between multilayer switches, and **GARP Multicast Registration Protocol (GMRP)** for providing a constrained multicast flooding facility.

L2 switches exchange GMRP packets with each other to know the multicast entries on other switches so that it can also register the multicast entry on its own table. After exchanging the information, the multicast traffic will only be forwarded to the corresponding ports.

Configuring GMRP

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching** > **Multicast** > **GMRP**.
3. Set **GMRP** to **Enabled**, and then click **Apply**.
4. Locate the port on which you want to enable GMRP, and then click the corresponding **[Edit]** button.

   The Edit Port Settings screen appears.
5. Set **GMRP** to **Enabled**, and then click **Apply** to save your settings.

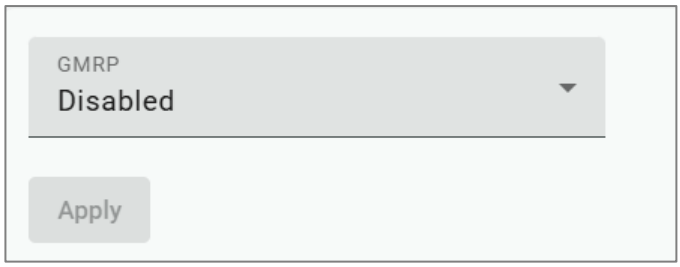
GMRP is now enabled.

GMRP

Menu Path: Layer 2 Switching > Multicast > GMRP

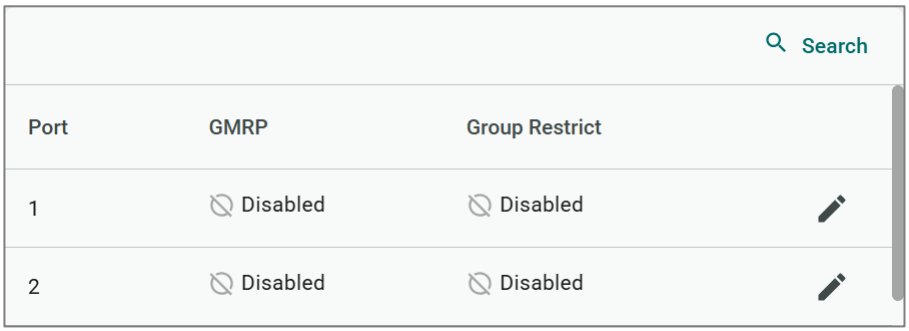
This page lets you configure the GMRP settings of your device.

GMRP Settings



UI Setting	Description	Valid Range	Default Value
GMRP	Enable or disable GMRP for the device. **Note** GMRP cannot be enabled when IGMP Snooping is enabled.	Enabled / Disabled	Disabled

GMRP Port List



UI Setting	Description
Port	Shows the port number the entry is for.
GMRP	Shows whether GMRP is enabled for the port.

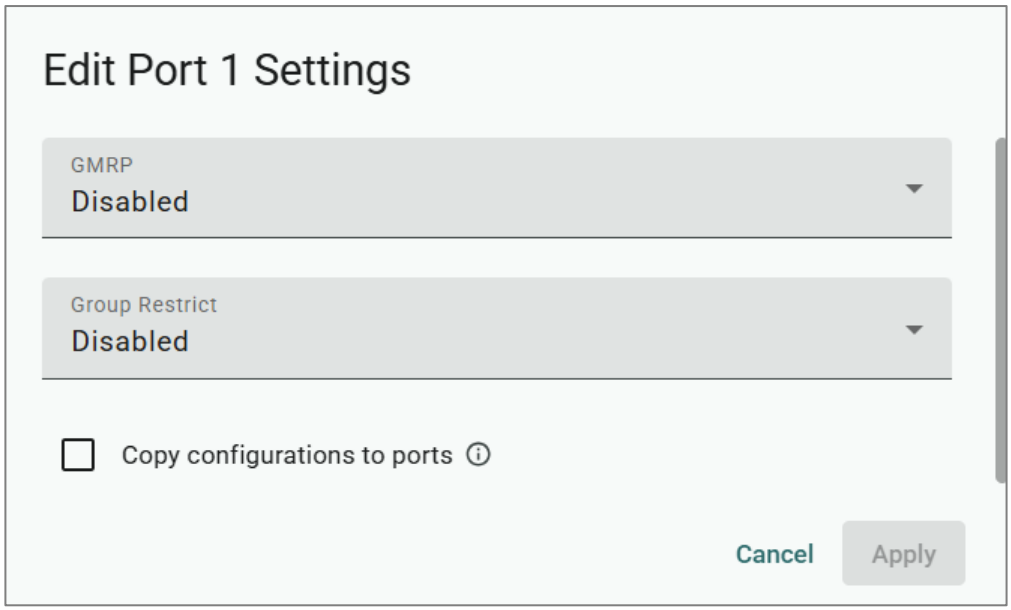
UI Setting	Description
Group Restrict	Shows whether group restrict is enabled for the port.

GMRP - Edit Port Settings

Menu Path: Layer 2 Switching > Multicast > GMRP

Clicking the **Edit (✎)** icon for a port on the **Layer 2 Switching > Multicast > GMRP** page will open this dialog box. This dialog lets you edit the GMRP settings for the port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
GMRP	Enable or disable GMRP for the port.	Enabled / Disabled	Disabled
Group Restrict	Enable or disable group restrict for the port.	Enabled / Disabled	Disabled
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

About Static Multicast

Static multicast is for configuring the multicast forwarding entries in the switch in a manual or predetermined manner.

In multicast networking, data packets are sent from one sender to multiple receivers efficiently, rather than sending individual packets to each receiver separately, as in unicast communication.

Network administrators manually configure the multicast forwarding entries in the device's multicast forwarding table. This involves specifying the multicast group addresses and the corresponding outbound interfaces or ports through which multicast traffic should be forwarded.

Benefits:

1. **Predictable Behavior**: Static multicast provides predictable behavior, as the forwarding paths for multicast traffic are predetermined by the administrator. This can be advantageous in certain network environments where stability and control are prioritized over flexibility and adaptability.
2. **Resource Efficiency**: Since static multicast entries are manually configured and do not involve the overhead of dynamic routing protocols, they can be more resource-efficient in terms of processing power and network bandwidth, especially in small-scale deployments with relatively stable multicast group memberships.

How Static Multicast works

If the user wants to restrict some of the multicast groups to be forwarded to specific ports for devices that don't support IGMP, users can use static multicast setting.

Users can manually register the multicast forwarding entries, including multicast MAC address and forwarding/forbidden port on the table, and the switch will forward the multicast traffic following the table rather than flooding.

Configuring Static Multicast Tables

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching** > **Multicast** > **Static Multicast**
3. To add a static multicast entry, click the ***[Add]***.

4. Configure the following, and then click **Create**:

Option	Value
VLAN ID	Specify the VLAN ID
MAC Address	Specify the multicast MAC address. • IPv4 Multicast Range: 01:00:5E:00:00:00 to 01:00:5E:7F:FF (last 23 bits used for the multicast group address) • IPv6 Multicast Range: 33:33:00:00:00:00 to 33:33:FF:FF:FF (last 32 bits used for multicast group address)
Port	Choose one or more egress ports.
Forbidden Ports	Specify a device port that will never forward multicast packets, even if it would otherwise be covered.

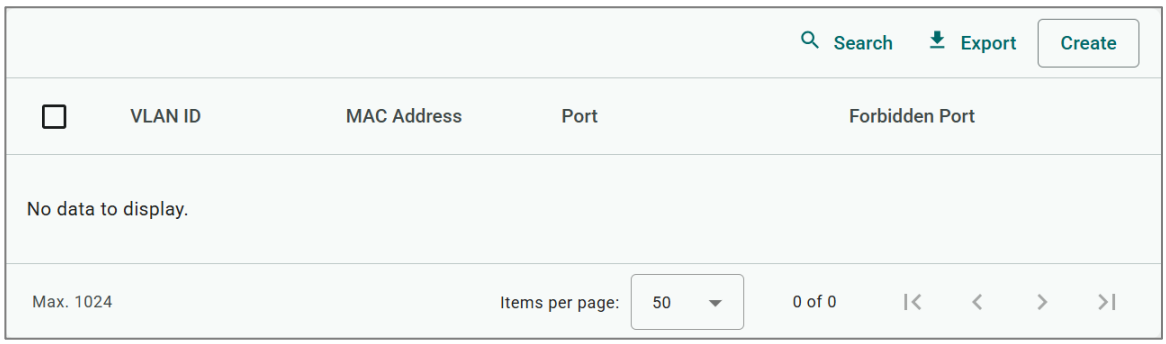
Static Multicast

Menu Path: Layer 2 Switching > Multicast > Static Multicast

This page lets you view and manage your device's static multicast table.

Limitations

You can create up to 1024 static multicast entries.



UI Setting	Description
VLAN ID	Shows the ID of the VLAN used for the multicast group entry.

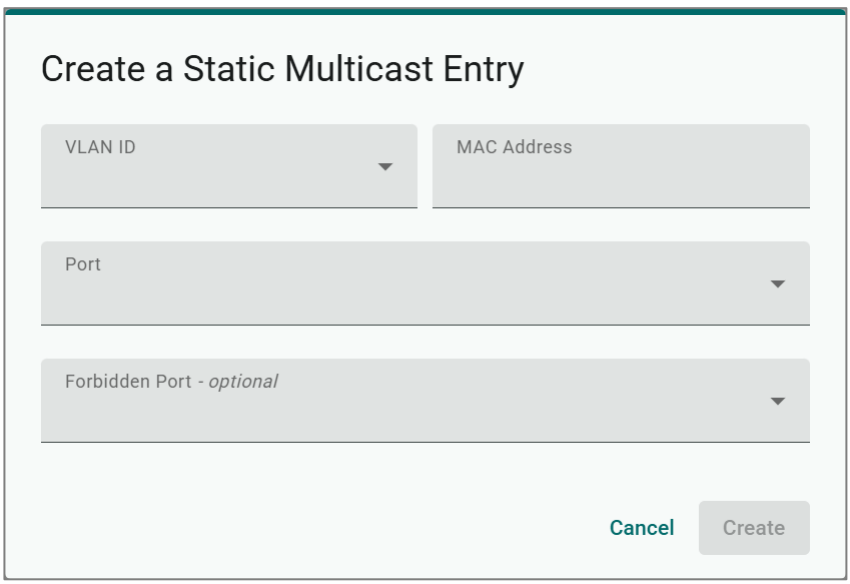
UI Setting	Description
MAC Address	Shows the MAC address for the multicast group entry.
Port	Shows the egress ports that multicast streams will forward to for the multicast group entry.
Forbidden Port **(Only in Advanced Mode)**	Show the forbidden ports that packets will not be forwarded to for the multicast group entry.

Create a Static Multicast Entry

Menu Path: Layer 2 Switching > Multicast > Static Multicast

Clicking **Create** on the **Layer 2 Switching > Multicast > Static Multicast** page will open this dialog box. This dialog lets you add a static multicast entry.

Click **Create** to save your changes and add the new entry.



UI Setting	Description	Valid Range	Default Value
VLAN ID	Select a VLAN ID for the multicast entry.	Drop-down list of VLAN IDs	N/A
MAC Address	Specify the MAC address for the multicast entry.	Valid multicast MAC address	N/A

UI Setting	Description	Valid Range	Default Value
Port	Select the ports to use as egress ports for multicast streams to be forwarded to.	Drop-down list of ports	N/A
Forbidden Port **(Only in Advanced Mode)**	Select which ports are forbidden so packets cannot be forwarded to them.	Drop-down list of ports	N/A

About IP Configuration

The IP Configuration feature allows you to assign an IP address and related settings to the device itself. This essentially gives the device its own unique identity on the network, enabling it to communicate and manage other network devices, be accessible remotely, and facilitate specific functions such as DHCP Relay Agent.

The IP address can be set manually to a static IP address, using user-entered values, or automatically obtained from an external DHCP server.

IP Configuration

Menu Path: IP Configuration

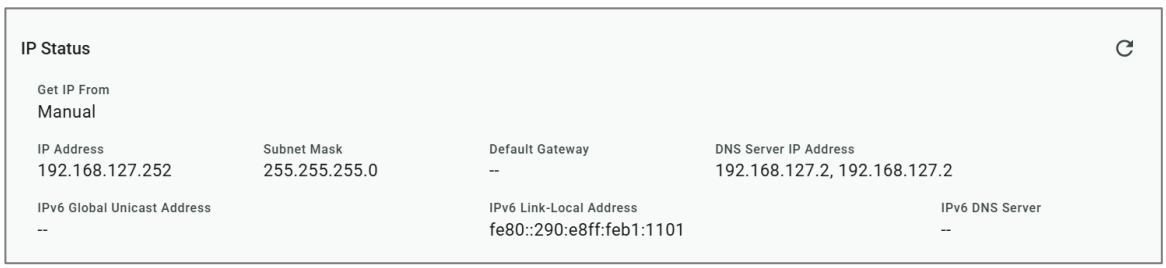
This page lets you view and manage the device's IP address.

IP Configuration - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to System > Account Management > User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Auto Configuration	R/W	R/W	R

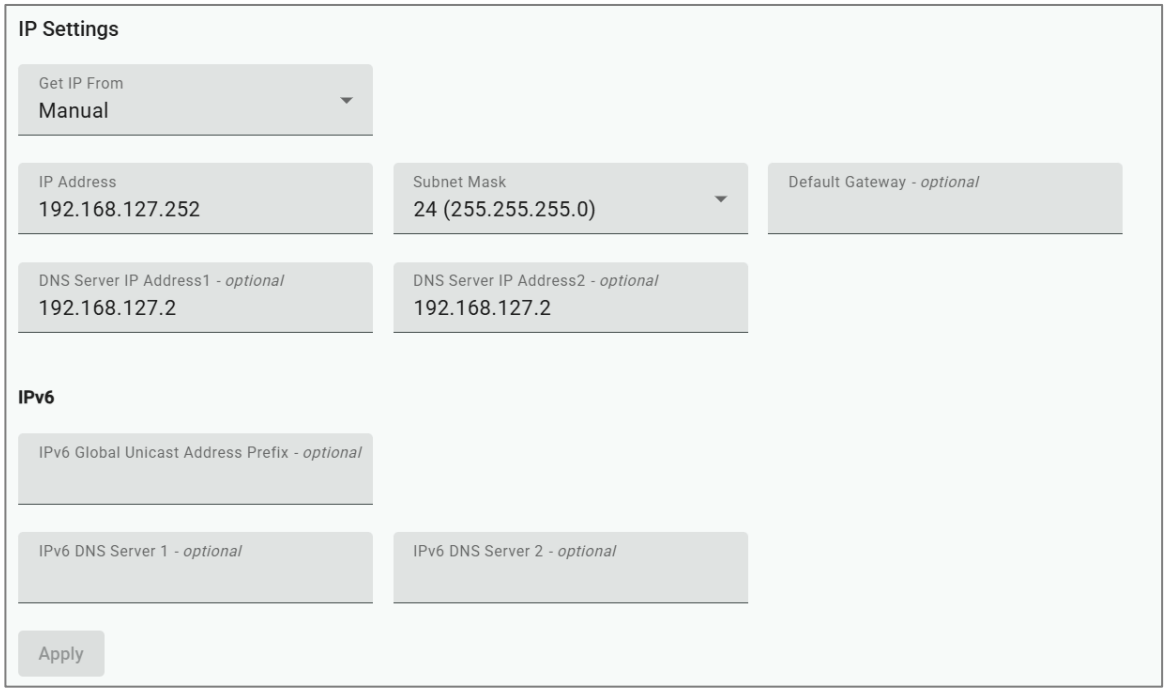
IP Status



UI Setting	Description
Get IP From	Shows where the device gets its IP address from. **Manual** means that the IP address is manually assigned.
IP Address	Shows the IP address for the device.
Subnet Mask	Shows the subnet mask used for the device.
Default Gateway	Shows the IP address of the gateway that connects the LAN to a WAN or another network.
DNS Server IP Address	Shows the IP address of the DNS server to use for connected devices.
IPv6 Global Unicast Address **(Only in Advanced Mode)**	Shows the IPv6 global unicast address to use for connected devices.
IPv6 Link-Local Address **(Only in Advanced Mode)**	Shows the IPv6 link-local address to use for connected devices.
IPv6 DNS Server **(Only in Advanced Mode)**	Shows the IP address of the IPv6 DNS server to use for connected devices.

IP Settings - Manual

If **Get IP From** is set to **Manual**, the following settings will appear.



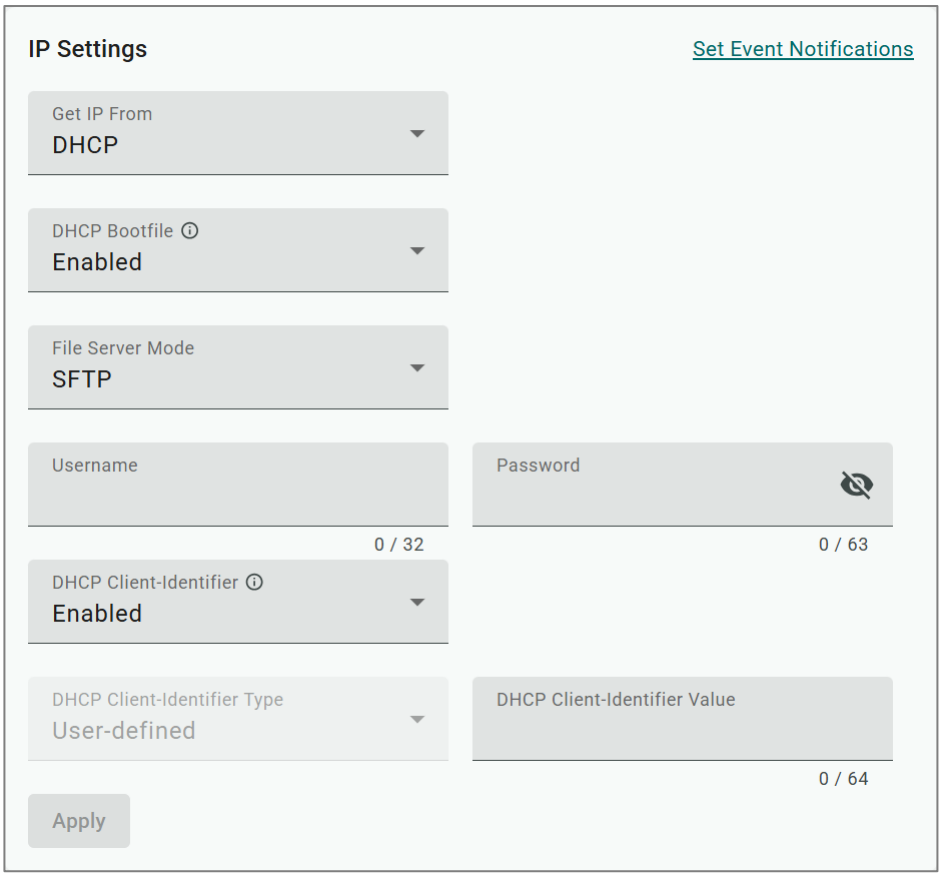
UI Setting	Description	Valid Range	Default Value
Get IP From	Specify where the device will get its IP from. • **Manual**: Set the IP address manually. • **DHCP**: Assign the IP address automatically through a DHCP server.	Manual / DHCP	Manual
IP Address	Specify the IP address to use for the device.	Valid IP address	192.168.127.252
Subnet Mask	Select the subnet mask to use for the device.	Drop-down list of subnet masks	24(255.255.255.0)
Default Gateway	Specify the IP address of the gateway that connects the LAN to a WAN or another network.	Valid IP address	N/A
DNS Server IP Address 1/2	Specify the IP address of the 1st and 2nd DNS server used by your network.	Valid IP address	N/A
IPv6 Global Unicast Address Prefix **(Only in Advanced Mode)**	Specify the IPv6 global unicast address prefix to use for your network.	Valid IPv6 address	N/A

UI Setting	Description	Valid Range	Default Value
IPv6 DNS Server 1/2 **(Only in Advanced Mode)**	Specify the IP address of the 1st and 2nd IPv6 DNS server used by your network.	Valid IPv6 address	N/A

IP Settings - DHCP

If **Get IP From** is set to **DHCP**, the following settings will appear.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.



UI Setting	Description	Valid Range	Default Value
Get IP From	Specify where the device will get its IP from. • **Manual**: Set the IP address manually. • **DHCP**: Assign the IP address automatically through a DHCP server.	Manual / DHCP	Manual
DHCP Bootfile	Enable or disable use of a DHCP bootfile. If enabled, the system will automatically download and restore the configuration settings of the bootfile described in Option 67 and from the server described in Option 66.	Enabled / Disabled	Enabled
File Server Mode **(If DHCP Bootfile is Enabled)**	Specify which file server mode to use to get the DHCP bootfile.	TFTP / SFTP	TFTP
Username **(If File Server Mode is SFTP)**	Specify the username for the SFTP server to get the DHCP bootfile from.	0 to 32 characters	N/A
Password **(If File Server Mode is SFTP)**	Specify the password for the SFTP server to get the DHCP bootfile from.	0 to 63 characters	N/A
DHCP Client-Identifier	Enable or disable use of a DHCP client-identifier. If enabled, the system will send DHCP client messages with an Option 61 tag including a client ID. The DHCP server will assign the IP address associated with the client ID value, if available.	Enabled / Disabled	Disabled
DHCP Client-Identifier Type **(If DHCP Client-Identifier is Enabled)**	Shows the DHCP Client-Identifier Type. **Note** This is fixed to User-defined and cannot be changed.	User-defined	User-defined
DHCP Client-Identifier Value **(If DHCP Client-Identifier is Enabled)**	Specify the DHCP client-identifier value to use.	1 to 64 characters	N/A

Redundancy

Menu Path: Redundancy

This section lets you configure the redundancy settings for your device.

This section includes these pages:

- Layer 2 Redundancy

Redundancy - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to System > Account Management > User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Layer 2 Redundancy			
Spanning Tree	R/W	R/W	R
Turbo Ring v2	R/W	R/W	R
MRP	R/W	R/W	R

Layer 2 Redundancy

Menu Path: Redundancy > Layer 2 Redundancy

This section lets you manage the Layer 2 redundancy features of your device.

This section includes these pages:

- Spanning Tree
- Turbo Ring V2
- MRP

About Spanning Tree

The 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.

Rapid Spanning Tree Protocol (RSTP) is an IEEE 802.1w network protocol that enhances the speed and stability of the Spanning Tree Protocol (STP). RSTP promotes high availability and a "loop-free" topology, similar to STP, but more quickly within Ethernet networks. It provides faster convergence and is backward compatible with STP. While STP takes 30-50 seconds to converge, RSTP can achieve sub-second convergence.

For applications that require redundancy, but require use of only open-standard protocols and no proprietary protocols, RSTP is a good choice.

Difference 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.

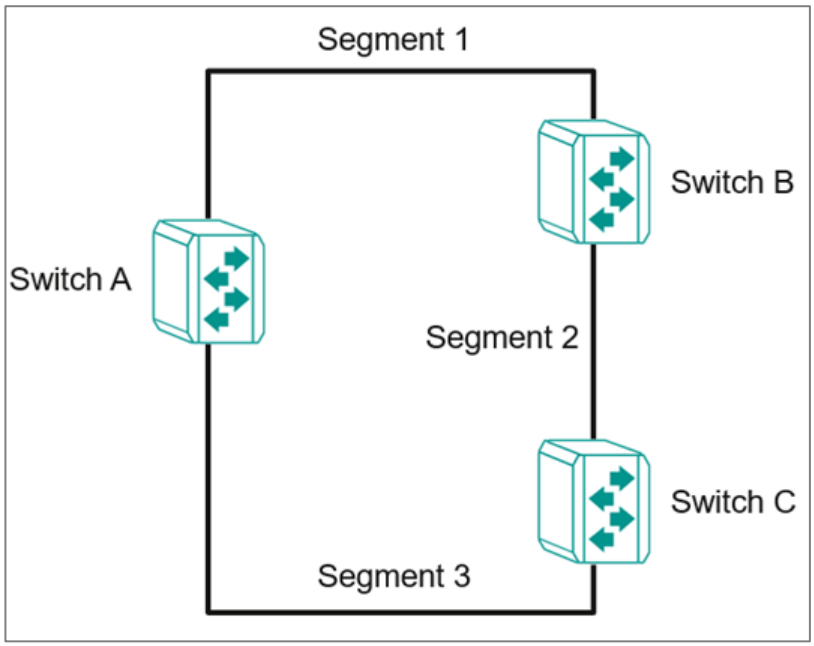
STP and RSTP spanning tree protocols operate without regard to a network's VLAN configuration and maintain one common spanning tree throughout a bridged network. Thus, these protocols map one loop-free, logical topology on a given physical topology.

Note

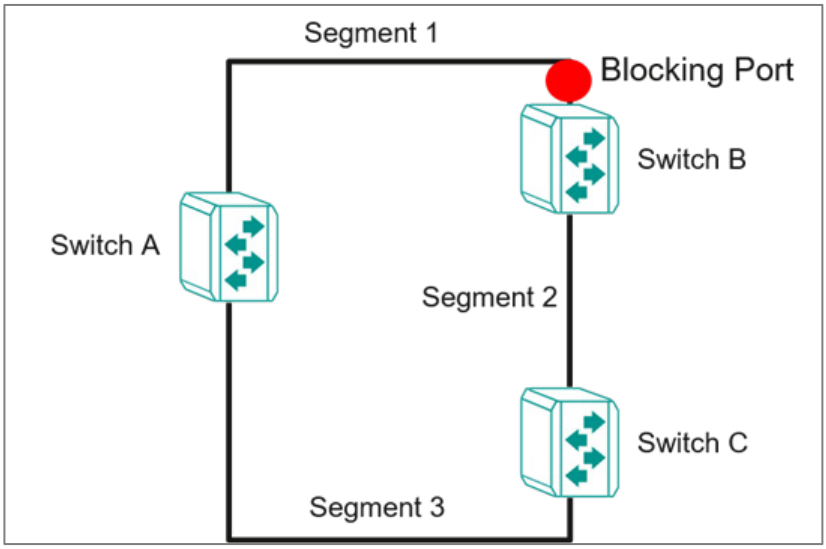
This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

About STP Operations

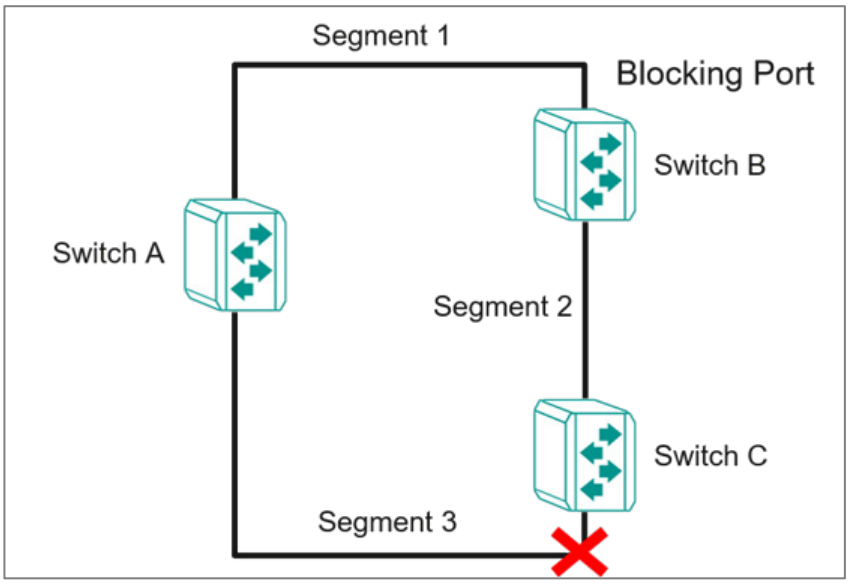
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is not enabled.



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 segment 2 to segment 1 flows through switches C and A since this path is in a forwarding state and is processing BPDUs. However, switch B on segment 1 is in a blocking state.



What happens if a link failure is detected? As shown in the figure below, the STP will change the blocking state to a forwarding state so that traffic from segment 2 flows through switch B to segment 1 through a redundant path.



STP will determine which path between each 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 switch C was the most efficient, and as a result, blocked the path through switch B. After the failure of switch C, STP re-evaluated the situation and opened the path through switch B.

About RSTP

Rapid Spanning Tree Protocol (RSTP) is an enhancement of the original Spanning Tree Protocol (STP) designed to speed up network convergence and improve overall network performance. RSTP ensures there is only one active path between devices in a network, with backup paths ready to activate if the primary path fails.

Each port is assigned a cost that indicates the efficiency of its link. Typically, this cost is determined by the link's bandwidth, with less efficient links assigned a higher cost.

The RSTP path cost default was originally calculated after detecting the bandwidth as follows.

Link Speed	RSTP/MSTP cost
100 Mbit/s	200,000
1 Gbit/s	20,000
10 Gbit/s	2,000

This can be overwritten from the UI.

Key Features of RSTP

- **Faster Convergence:** RSTP reduces the time required to detect and respond to network topology changes compared to STP. It eliminates the lengthy listening and learning states of STP, allowing for quicker transitions to active states.
- **Localized Decision-Making:** Unlike STP, where decisions are made network-wide, RSTP enables switches to make local configuration decisions. This allows for faster automatic configuration and quicker restoration of network links.
- **Simplified Port Roles:** RSTP uses only three primary port roles—Root Port, Designated Port, and Alternate Port—streamlining the network’s operation and improving convergence speed.
- **Proposal/Agreement Mechanism:** RSTP introduces the Proposal/Agreement process to quickly determine designated ports during topology changes, further accelerating convergence.

How RSTP Works

RSTP operates in the following sequence:

1. **Root Bridge Selection:** The switch with the lowest bridge priority or MAC address is designated as the root bridge, forming the base of the spanning tree.
2. **Root Port Selection:** Non-root switches select their root port, which provides the best path to the root bridge based on path cost.
3. **Designated Ports Assignment:** Each network segment designates a port to forward traffic, ensuring optimal paths are used.
4. **Blocking State:** Non-designated or non-root ports remain in a blocking state, preventing loops.

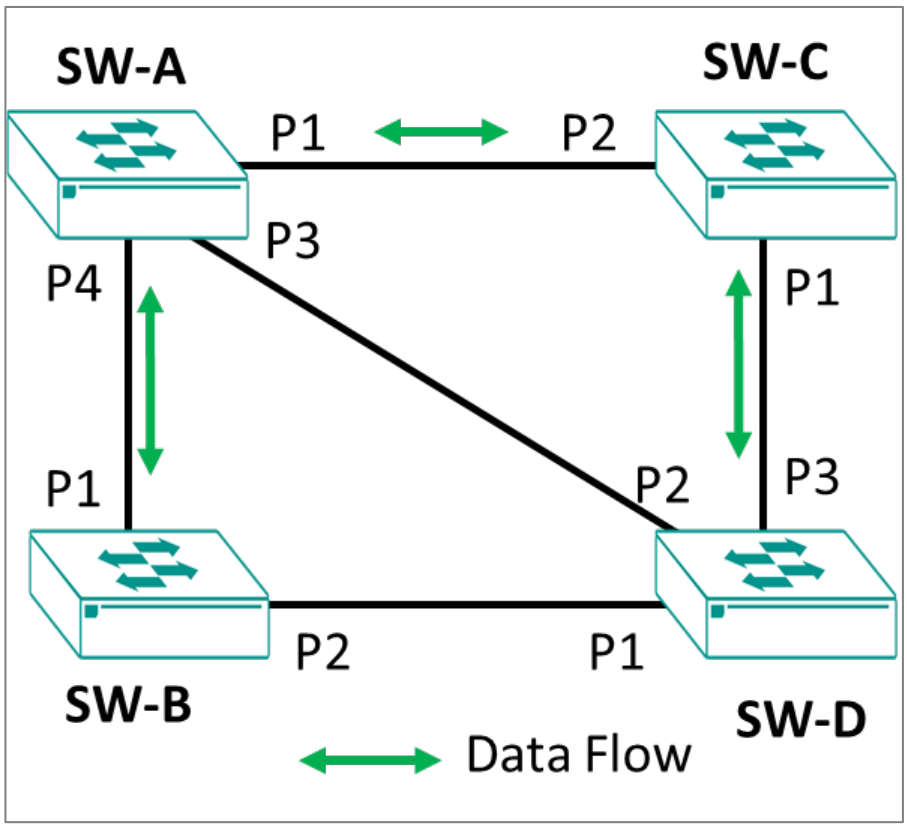
Benefits of RSTP

- **Improved Network Stability:** RSTP's fast convergence mechanisms reduce the risk of network outages by adapting quickly to changes in the network topology.
- **Backward Compatibility:** RSTP is fully compatible with STP, allowing a smooth transition in mixed networks where some devices still use the older protocol.

Overall, RSTP offers significant improvements over STP, making networks more resilient and responsive to changes, thereby enhancing overall reliability and performance.

Scenario: Configuring 4 Devices with RSTP

A user wants to configure 4 network devices in an RSTP topology.



Ordinarily, data will flow from SW-A directly to SW-B and SW-C. SW-D data will transit SW-D. However, if something happens that breaks links, data flow can be rerouted without administrator intervention. Follow the subsequent examples to configure each switch.

Example: Configuring RSTP on SW-A

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Spanning Tree**, and then click **General**.
3. Under **STP Mode**, select **STP/RSTP** from the drop-down list.

If this option was previously **Disabled**, numerous new features will appear.

4. Under **Compatibility**, select **RSTP**.
5. Set **Bridge Priority** to 28672.

This most be lower than other switches on the network to establish SW-A as the root of the topology.

6. Click **Apply** to save your changes.

The list of ports becomes available.

7. Find Port **1** on the list of ports, and then click the corresponding **[Edit]**.

The Edit Port Settings screen appears.

8. Under **Enable**, choose **Enabled** from the drop-down menu.
9. Click **Apply** to save your changes.
10. Find Port **3** on the list of ports, and then click the corresponding **[Edit]**.

The Edit Port Settings screen appears.

11. Under **Enable**, choose **Enabled** from the drop-down menu.
12. Click **Apply** to save your changes.
13. Find Port **3** on the list of ports, and then click the corresponding **[Edit]**.

The Edit Port Settings screen appears.

14. Under **Enable**, choose **Enabled** from the drop-down menu.
15. Click **Apply** to save your changes.
16. Find Port **4** on the list of ports, and then click the corresponding **[Edit]**.

The Edit Port Settings screen appears.

17. Under **Enable**, choose **Enabled** from the drop-down menu.
18. Click **Apply** to save your changes.

SW-A has been configured. You can now move on to configuring SW-B.

Example: Configuring RSTP on SW-B

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Spanning Tree**, and then click **General**.
3. Under **STP Mode**, select **STP/RSTP** from the drop-down list.

If this option was previously **Disabled**, numerous new features will appear.

4. Under **Compatibility**, select **RSTP**.
5. Click **Apply** to save your changes.

The list of ports becomes available.

6. Find Port **1** on the list of ports, and then click the corresponding **[Edit]**.

The Edit Port Settings screen appears.

7. Under **Enable**, choose **Enabled** from the drop-down menu.
8. Find Port **2** on the list of ports, and then click the corresponding **[Edit]**.

The Edit Port Settings screen appears.

9. Under **Enable**, choose **Enabled** from the drop-down menu.
10. Click **Apply** to save your changes.

SW-B has been configured. You can now move on to configuring SW-C.

Example: Configuring RSTP on SW-C

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Spanning Tree**, and then click **General**.
3. Under **STP Mode**, select **STP/RSTP** from the drop-down list.

If this option was previously **Disabled**, numerous new features will appear.

4. Under **Compatibility**, select **RSTP**.
5. Click **Apply** to save your changes.

The list of ports becomes available.

6. Find Port **1** on the list of ports, and then click the corresponding **[Edit]**.
7. Under **Enable**, choose **Enabled** from the drop-down menu.
8. Find Port **2** on the list of ports, and then click the corresponding **[Edit]**.

The Edit Port Settings screen appears.

9. Under **Enable**, choose **Enabled** from the drop-down menu.
10. Click **Apply** to save your changes.

SW-C has been configured. You can now move on to configuring SW-D.

Example: Configuring RSTP on SW-D

SW-D requires specific configuration to ensure that the correct paths are followed.

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Spanning Tree**, and then click **General**.
3. Under **STP Mode**, select **STP/RSTP** from the drop-down list.

If this option was previously **Disabled**, numerous new features will appear.

4. Under **Compatibility**, select **RSTP**.
5. Click **Apply** to save your changes.

The list of ports becomes available.

6. Find Port **1** on the list of ports, and then click the corresponding **[Edit]**.

The Edit Port Settings screen appears.

7. Under **Enable**, choose **Enabled** from the drop-down menu.
8. Verify that there is a value in the **Path Cost** field. If there is no value, enter a tentative value of `20,000`.
9. Click **Apply** to save your changes.

10. Find Port **4** on the list of ports, and then click the corresponding **[Edit]**.

The Edit Port Settings screen appears.

11. Under **Enable**, choose **Enabled** from the drop-down menu.
12. Verify that there is a value in the **Path Cost** field. If there is no value, enter a tentative value of `20,000`.
13. Click **Apply** to save your changes.

14. Find Port **4** on the list of ports, and then click the corresponding **[Edit]**.
15. Under **Enable**, choose **Enabled** from the drop-down menu.
16. Set **Path Cost** to `0`.
17. Click **Apply** to save your changes.

With SW-D completed, all devices in the topology are complete.

Spanning Tree Settings

Menu Path: Redundancy > Spanning Tree

This page lets you configure the spanning tree settings of your device.

This page includes these tabs:

- General
- Status

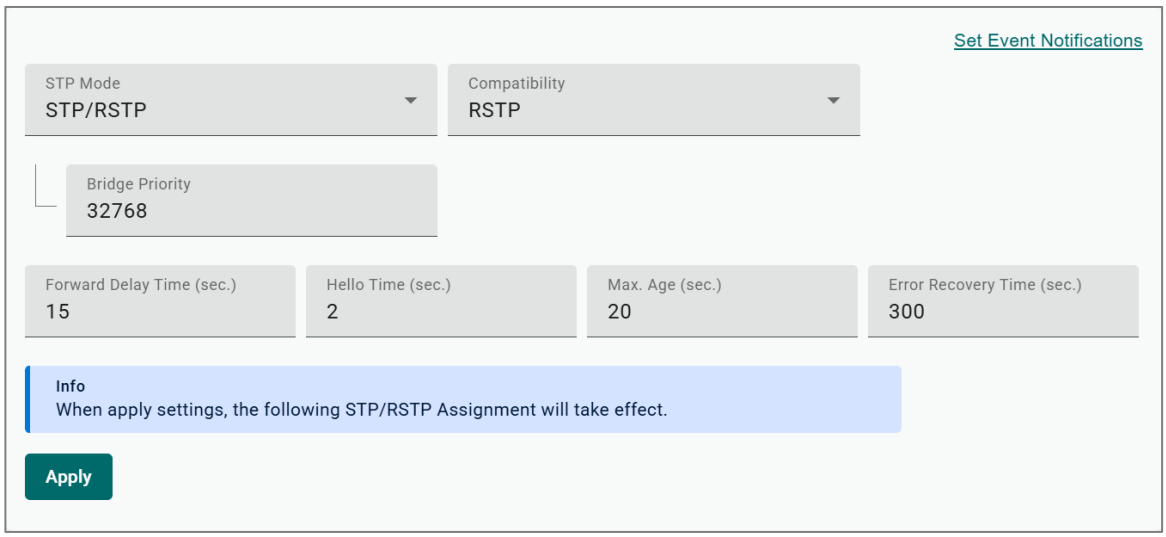
Spanning Tree - General

Menu Path: Redundancy > Spanning Tree - General

This page lets you configure the STP mode and its related settings.

Spanning Tree Settings - STP/RSTP

If **STP Mode** is set to **STP/RSTP**, the following settings will appear.

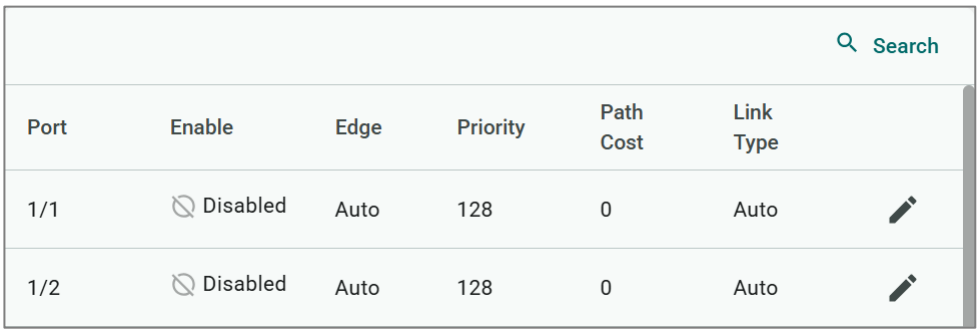


UI Setting	Description	Valid Range	Default Value
STP Mode	Specify the spanning tree protocol (STP) to use. **Note** MSTP and GVRP are both VLAN-related functions. When VLAN changes dynamically, MSTP needs to re-converge, which can make the system unstable due to running complex operations. When both MSTP and GVRP are used together, this can result in network instability. Therefore, it is recommended that network administrators avoid enabling both MSTP and GVRP.	Disabled / STP/RSTP/ MSTP	Disabled
Compatibility	Specify the compatibility mode to use.	STP / RSTP	RSTP
Bridge Priority	Specify the bridge priority number, which must be a multiple of 4096. Lower numbers have higher priority. A device with a higher bridge priority (e.g., a lower value) has a greater chance of being established as the root of the spanning tree topology.	Multiples of 4096 from 0 to 61440	32768
Forward Delay Time	Specify the amount of time in seconds the device waits before checking to see if it should change to a different state.	4 to 30	15
Hello Time	Specify the hello time in seconds. This is the amount of time the root waits between sending hello messages. 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.	1 to 2	2

UI Setting	Description	Valid Range	Default Value
Max. Age	Specify the max age in seconds. If this device is not the root, and it has not received a hello message from the root for longer than the max age time, 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.	6 to 40	20
Error Recovery Time	Specify the error recovery time in seconds. If BPDU guard is triggered on a port, it will automatically recover to the normal state after the error recovery time.	30 to 65535	300

STP/RSTP - Port Table

If **STP Mode** is set to **STP/RSTP**, this table will appear.



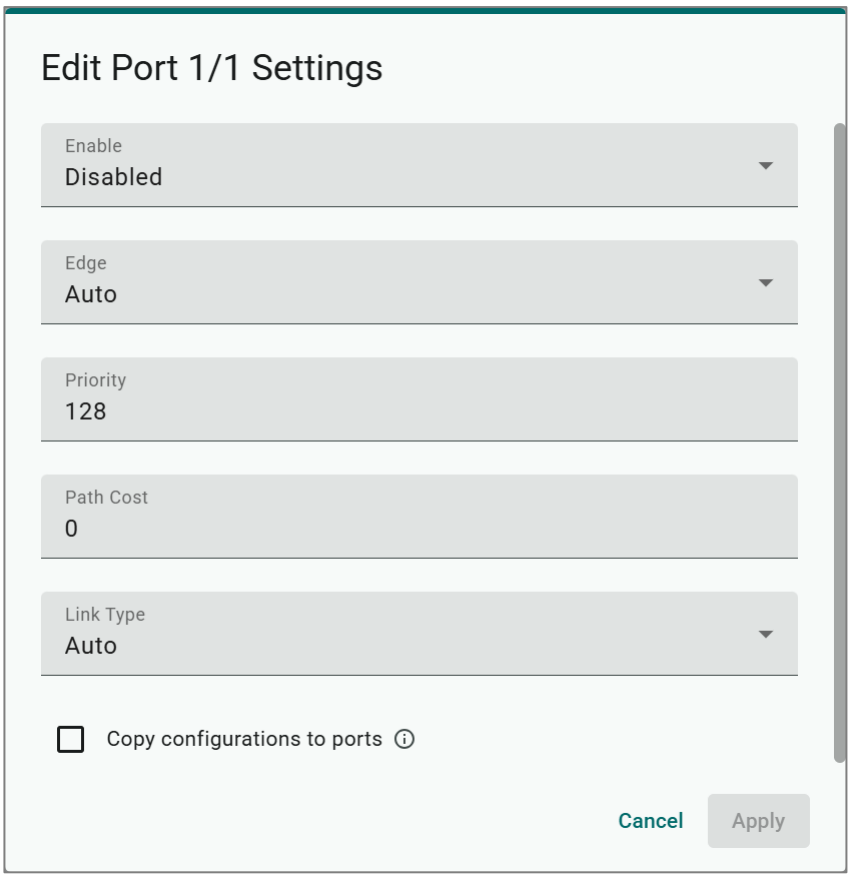
UI Setting	Description
Port	Shows the port number the entry is for.
Enable	Shows whether the spanning tree protocol is enabled for the port.
Edge	Shows the current edge port configuration for the port.
Priority	Show the bridge priority number for the port.
Path Cost	Show the path cost value for the port.
Link Type **(Only in Advanced Mode)**	Show the link type configuration for the port.

STP/RSTP Port Table - Edit Port Settings

Menu Path: Redundancy > Spanning Tree - General

Clicking the **Edit (✎)** icon for a port on the **Redundancy > Spanning Tree - General** page will open this dialog box. This dialog lets you edit the STP/RSTP settings for the port.

Click **Apply** to save your changes.

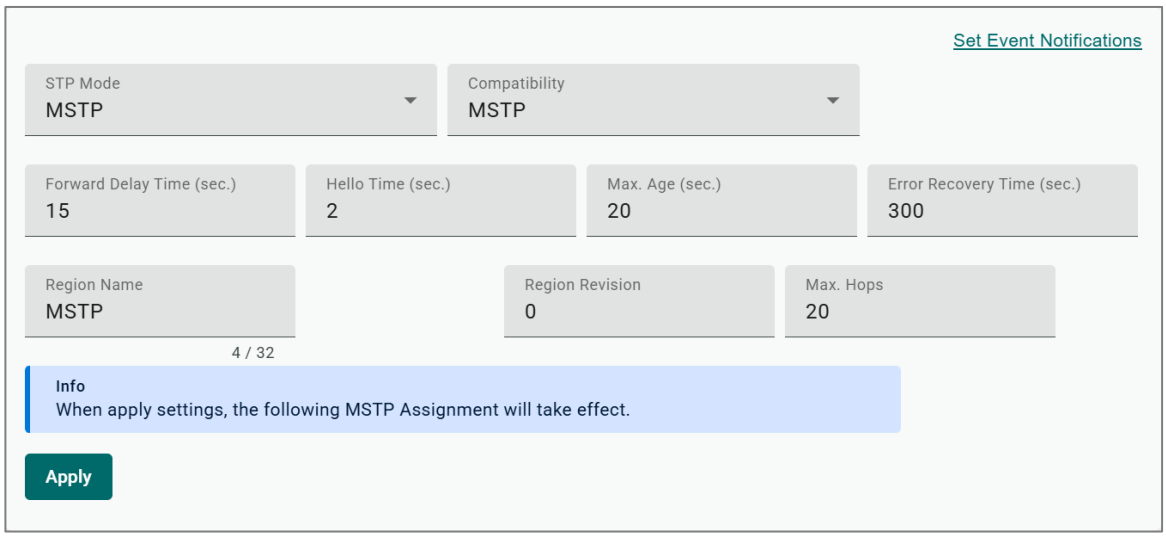


UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable spanning tree protocol for the port.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Edge	Select the edge port configuration for the port. • **Auto**: Auto-detect whether to configure the port as an edge port. • **Yes**: The port will be configured as an edge port. • **No**: The port will not be configured as an edge port.	Auto / Yes / No	Auto
Priority	Specify the priority of the port as a multiple of 16. Lower numbers have higher priority. A port with a higher priority (e.g., a lower value) has a greater chance of being a root port.	Multiples of 16 from 0 to 240	128
Path Cost	Specify the path cost value. If this is set to 0, the path cost value will be automatically assigned according to the port speed.	0 to 20000000	0
Link Type **(Only in Advanced Mode)**	Select the link type for the port. • **Point-to-point**: Use this when the port is operating in full-duplex mode. • **Shared**: Use this when the port is operating in half-duplex mode. • **Auto**: Auto-detect which mode to use for the port.	Point-to-point / Shared / Auto	Auto
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

Spanning Tree Settings - MSTP

If **STP Mode** is set to **MSTP**, the following settings will appear.

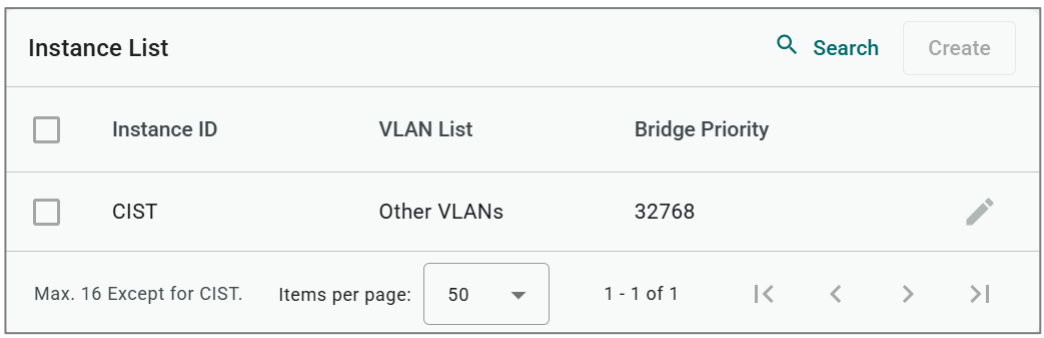


UI Setting	Description	Valid Range	Default Value
STP Mode	Specify the spanning tree protocol (STP) to use. **Note** MSTP and GVRP are both VLAN-related functions. When VLAN changes dynamically, MSTP needs to re-converge, which can make the system unstable due to running complex operations. When both MSTP and GVRP are used together, this can result in network instability. Therefore, it is recommended that network administrators avoid enabling both MSTP and GVRP.	Disabled / STP/RSTP/ MSTP	Disabled
Compatibility	Specify the compatibility mode to use.	RSTP / STP / MSTP	MSTP
Forward Delay Time	Specify the amount of time in seconds the device waits before checking to see if it should change to a different state.	4 to 30	15
Hello Time	Specify the hello time in seconds. This is the amount of time the root waits between sending hello messages. 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.	1 to 2	2
Max. Age	Specify the max age in seconds. If this device is not the root, and it has not received a hello message from the root for longer than the max age time, 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.	6 to 40	20

UI Setting	Description	Valid Range	Default Value
Error Recovery Time	Specify the error recovery time in seconds. If BPDU guard is triggered on a port, it will automatically recover to the normal state after the error recovery time.	30 to 65535	300
Region Name	Specify the MSTP region name.	0 to 32 characters	MSTP
Region Revision	Specify the MSTP region revision.	0 to 65535	0
Max. Hops	Specify the maximum number of hops allowed.	6 to 40	20

MSTP - Instance List

If **STP Mode** is set to **MSTP**, the following table will appear.



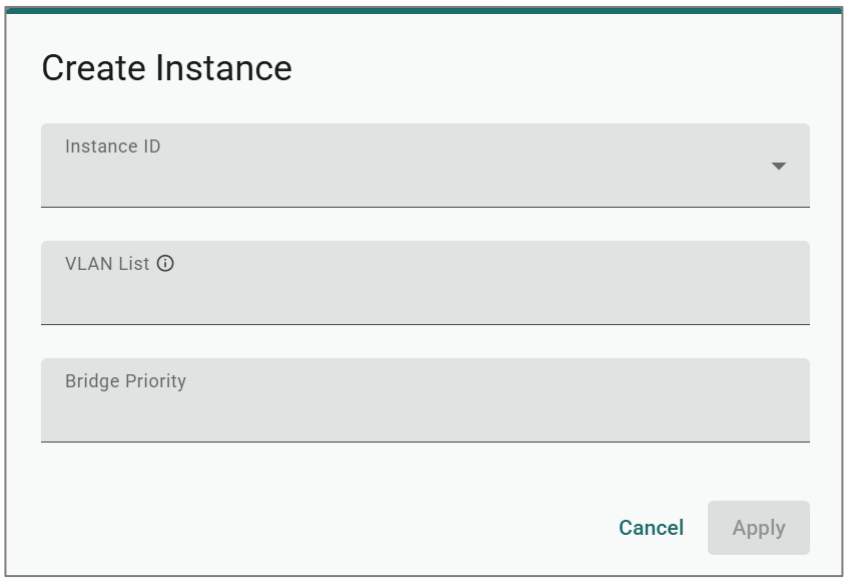
UI Setting	Description
Instance ID	Shows the of the instance the entry is for.
VLAN List	Show the VLAN list configured for the instance.
Bridge Priority	Show the bridge priority value for the instance.

Instance List - Create Instance

Menu Path: Redundancy > Spanning Tree - General

Clicking **Create** on the **Redundancy > Spanning Tree - General** page will open this dialog box. This dialog lets you create an MSTP instance.

Click **Create** to save your changes.



UI Setting	Description	Valid Range	Default Value
Instance ID	Select an ID for the instance.	Drop-down list of ID numbers.	N/A
VLAN List	Specify the VLAN IDs to use for the instance. You can enter multiple VLAN IDs by separating them with commas or by using ranges (e.g., 2, 4-8, 10-13).	Valid VLAN IDs	N/A
Bridge Priority	Specify the bridge priority value for the instance as a multiple of 4096. Lower values have higher priority.	Multiples of 4096 from 0 - 61440	N/A

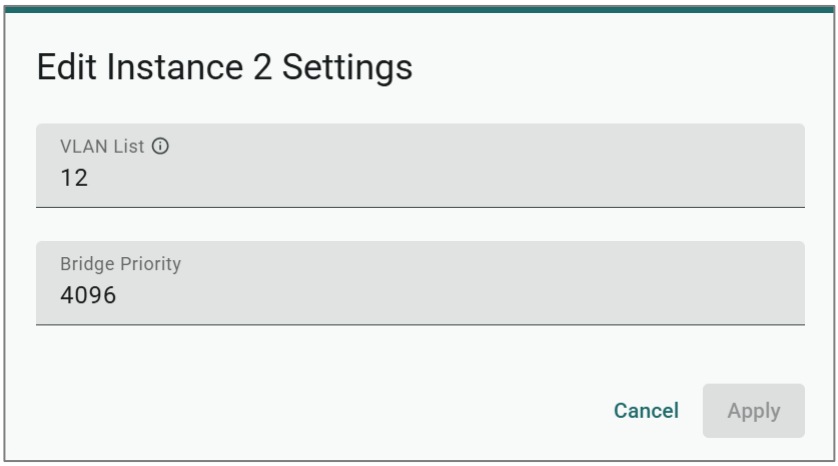
Instance List - Edit Settings

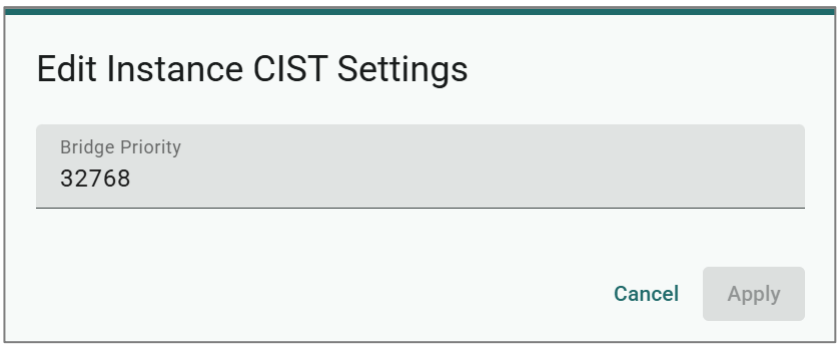
Menu Path: Redundancy > Spanning Tree - General

Clicking the **Edit (✎)** icon for an instance on the **Redundancy > Spanning Tree - General** page will open this dialog box. This dialog lets you edit the instance settings.

Click **Apply** to save your changes.

The dialog shown will be different when editing the CIST instance.

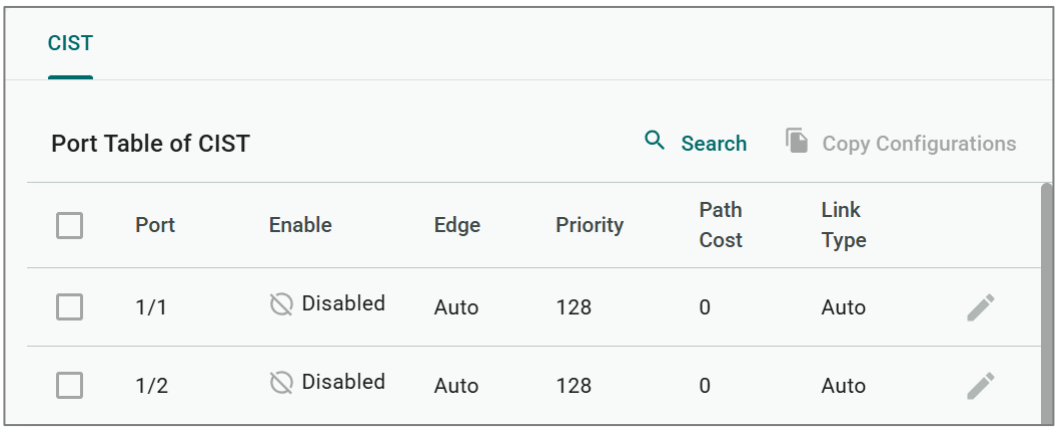




UI Setting	Description	Valid Range	Default Value
VLAN List	Specify the VLAN IDs to use for the instance. You can enter multiple VLAN IDs by separating them with commas or by using ranges (e.g., 2, 4-8, 10-13). **Note** This setting is not available for the CIST instance.	N/A	N/A
Bridge Priority	Specify the bridge priority value for the instance as a multiple of 4096. Lower values have higher priority.	Multiples of 4096 from 0 - 61440	32768 for CIST N/A for other instances

MSTP - Port Table

If **STP Mode** is set to **MSTP**, the following table will appear. Clicking on the drop-down list at the top left will let you select which instance's port table you want to view.



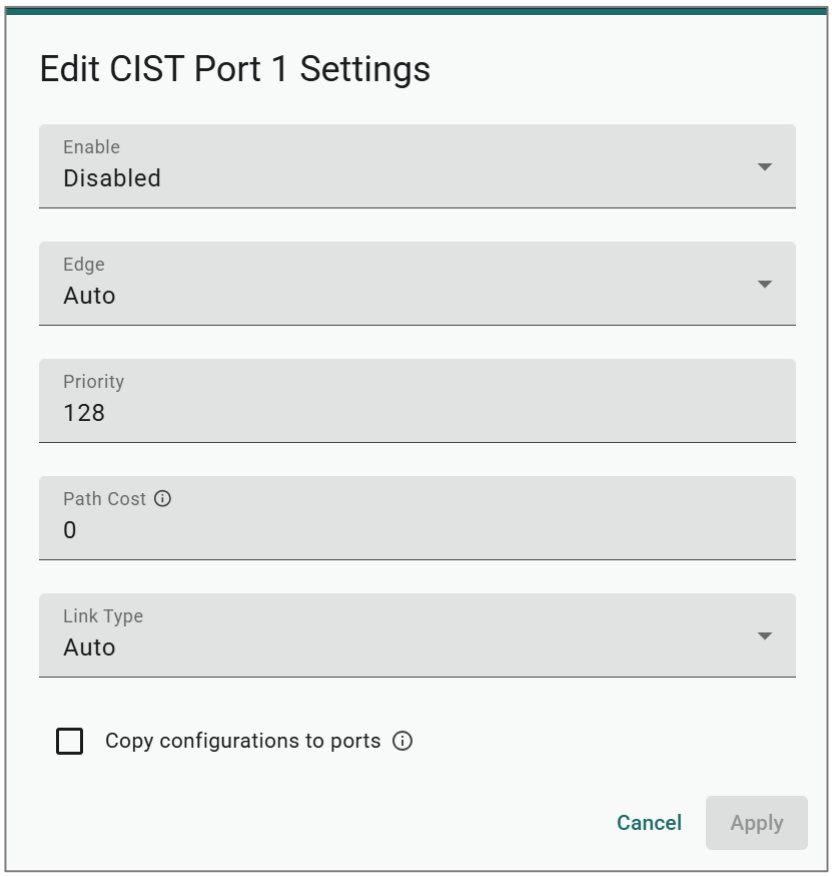
UI Setting	Description
Port	Shows the port number the entry is for.
Enable	Shows whether the spanning tree protocol is enabled for the port.
Edge	Shows the current edge port configuration for the port.
Priority	Show the bridge priority number for the port.
Path Cost	Show the path cost value for the port.
Link Type **(Only in Advanced Mode)**	Show the link type configuration for the port.

MSTP Port Table - Edit Port Settings

Menu Path: Redundancy > Spanning Tree - General

Clicking the **Edit (✎)** icon for a port on the **Redundancy > Spanning Tree - General** page will open this dialog box. This dialog lets you edit the port's settings for the selected instance.

Click **Apply** to save your changes.



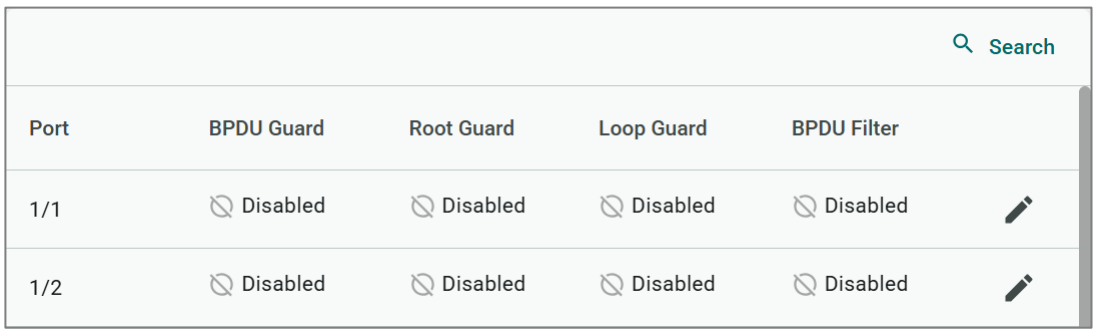
UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable spanning tree protocol for the port.	Enabled / Disabled	Disabled
Edge	Select the edge port configuration for the port. • **Auto**: Auto-detect whether to configure the port as an edge port. • **Yes**: The port will be configured as an edge port. • **No**: The port will not be configured as an edge port.	Auto / Yes / No	Auto
Priority	Specify the priority of the port as a multiple of 16. Lower numbers have higher priority. A port with a higher priority (e.g., a lower value) has a greater chance of being a root port.	Multiples of 16 from 0 to 240	128
Path Cost	Specify the path cost value. If this is set to 0, the path cost value will be automatically assigned according to the port speed.	0 to 20000000	0

UI Setting	Description	Valid Range	Default Value
Link Type **(Only in Advanced Mode)**	Select the link type for the port. • **Point-to-point**: Use this when the port is operating in full-duplex mode. • **Shared**: Use this when the port is operating in half-duplex mode. • **Auto**: Auto-detect which mode to use for the port.	Point-to-point / Shared / Auto	Auto
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

Spanning Tree - Guard

Menu Path: Redundancy > Spanning Tree - Guard

This page lets you configure BPDU Guard by port.



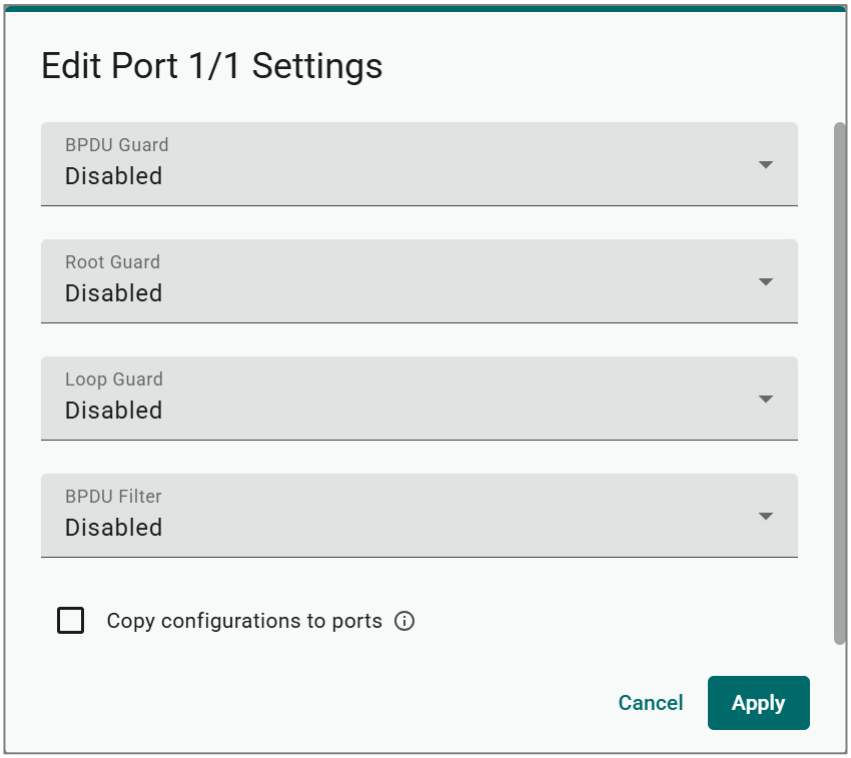
UI Setting	Description
Port	Shows the port number the entry is for.
BPDU Guard	Shows whether BPDU Guard is enabled for the port.
Root Guard **(Only in Advanced Mode)**	Shows whether Root Guard is enabled for the port.
Loop Guard **(Only in Advanced Mode)**	Shows whether Loop Guard is enabled for the port.
BPDU Filter	Shows whether the BPDU Filter is enabled for the port.

Spanning Tree Guard - Edit Port Settings

Menu Path: Redundancy > Spanning Tree - Guard

Clicking the **Edit (✎)** icon for a port on the **Redundancy > Spanning Tree - Guard** page will open this dialog box. This dialog lets you edit the BPDU settings for the port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
BDPU Guard	Enable/disable BPDU Guard on the port.	Enabled / Disabled	Disabled
Root Guard **(Only in Advanced Mode)**	Enable/disable Root Guard on the port.	Enabled / Disabled	Disabled
Loop Guard **(Only in Advanced Mode)**	Enable/disable Loop Guard on the port.	Enabled / Disabled	Disabled
BDPU Filter	Enable/disable BPDU Filter on the port.	Enabled / Disabled	Disabled
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

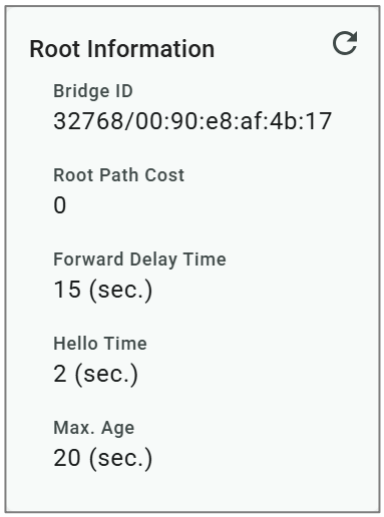
Spanning Tree - Status

Menu Path: Redundancy > Spanning Tree - Status

This page lets you view the current spanning tree status of your device.

Root Information

If **STP Mode** is set to **STP/RSTP**, this display will appear.



UI Setting	Description
Bridge ID	Shows the bridge ID.
Root Path Cost	Shows the root path cost.
Forward Delay Time	Shows the forward delay time in seconds.
Hello Time	Shows the hello time in seconds.
Max. Age	Shows the max. age time in seconds.

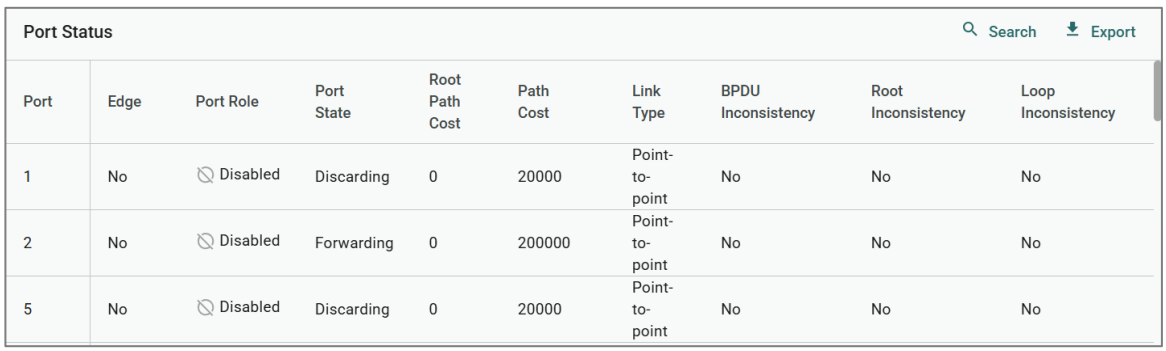
Bridge Information

If **STP Mode** is set to **STP/RSTP**, this display will appear.

UI Setting	Description
Bridge ID	Shows the bridge ID.
Running Protocol	Shows the current configured spanning tree protocol.
Forward Delay Time	Shows the forward delay time in seconds.
Hello Time	Shows the hello time in seconds.
Max. Age	Shows the max. age time in seconds.

Spanning Tree - Port Status

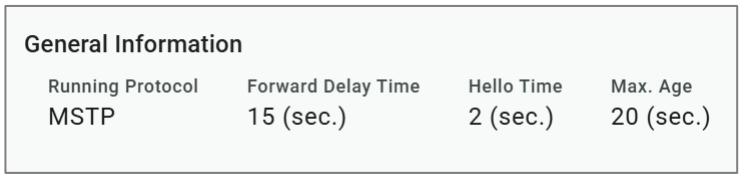
If **STP Mode** is set to **STP/RSTP**, the following table will appear.



UI Setting	Description
Port	Shows the port number the entry is for.
Edge	Shows whether this port is connected to an edge device.
Port Role	Shows the role for the port. • **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 a blocked port. • **Backup**: The backup port receives more useful BPDU from the same bridge and is a blocked port. • **Disabled**: The port is disabled.
Port State	Show the port state. • **Forwarding**: Traffic can be forwarded through this port. • **Blocked**: Traffic will be blocked. • **Disabled**: The port is disabled.
Root Path Cost	Shows the total path cost to the root bridge for the port.
Path Cost	Shows the path cost for the port.
Link Type	Show the link type for the port. • **Edge Port**: The port is connected to an edge device. • **Point-to-point**: The port is connected to another bridge and is full duplex. • **Shared**: The port is connected to another bridge and is half duplex.
BPDU Inconsistency	Shows whether BPDU inconsistency was detected for the port.
Root Inconsistency **(Only in Advanced Mode)**	Shows whether root inconsistency was detected for the port.
Loop Inconsistency **(Only in Advanced Mode)**	Shows whether loop inconsistency was detected for the port.

General Information

If **STP Mode** is set to **MSTP**, this display will appear.

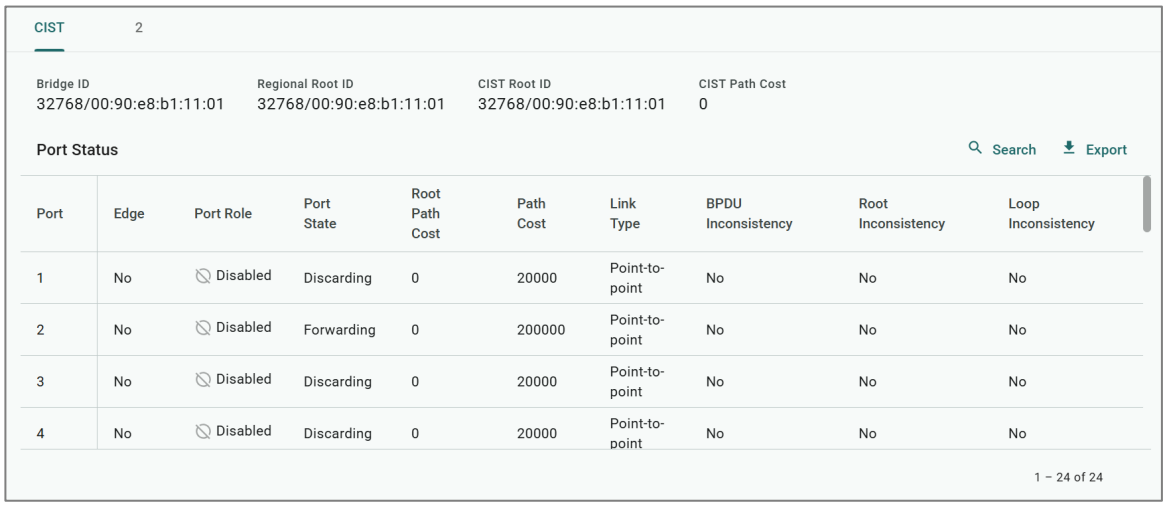


UI Setting	Description
Running Protocol	Shows the current configured spanning tree protocol.
Forward Delay Time	Shows the forward delay time in seconds.
Hello Time	Shows the hello time in seconds.
Max. Age	Shows the max. age time in seconds.

Spanning Tree - Port Status

If **STP Mode** is set to **MSTP**, the following table will appear.

You can use the drop-down list at the top-left to select which instance's status you want to view.



Information of Instance

When viewing the CIST instance, this information will appear:

UI Setting	Description
Bridge ID	Shows the bridge ID for the CIST instance.
Regional Root ID	Shows the regional root ID for the CIST instance.
CIST Root ID	Shows the bridge ID for the CIST instance.
CIST Path Cost	Shows the bridge ID for the CIST instance.

When viewing an instance other than the CIST instance, this information will appear:

UI Setting	Description
Bridge ID	Shows the bridge ID for the instance.
VLAN List	Shows the VLAN IDs for the instance.
Designated Root ID	Shows the designated root ID for the instance.
Root Path Cost	Shows the root path cost for the instance.

Port Status

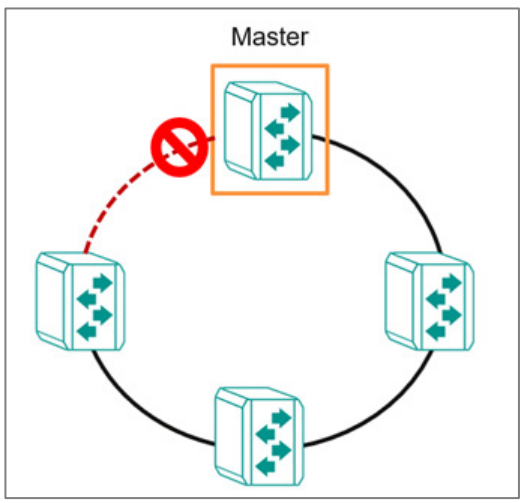
UI Setting	Description
Port	Shows the port number the entry is for.
Edge	Shows whether this port is connected to an edge device.
Port Role	Shows the role for the port. • **Root**: The port is connected directly or indirectly to the root device. • **Designated**: The port is designated if it can send the best BPDU on the segment to which it is connected. • **Alternate**: The alternate port receives more useful BPDU from another bridge and is a blocked port. • **Backup**: The backup port receives more useful BPDU from the same bridge and is a blocked port. • **Disabled**: MSTP is disabled for the port.
Port State	Show the port state. • **Forwarding**: Traffic can be forwarded through this port. • **Blocked**: Traffic will be blocked. • **Disabled**: The port is disabled.

UI Setting	Description
Root Path Cost	Shows the total path cost to the root bridge for the port.
Path Cost	Shows the path cost for the port.
Link Type	Show the link type for the port. • **Edge Port**: The port is connected to an edge device. • **Point-to-point**: The port is connected to another bridge and is full duplex. • **Shared**: The port is connected to another bridge and is half duplex.
BPDU Inconsistency	Shows whether BPDU is received on a port enabled by a BPDU guard.
Root Inconsistency	Shows whether the port is changed to a root port when enabled by a loop guard.
Loop Inconsistency	Shows whether a loop is detected on this port by a loop guard.

About Turbo Ring v2

Turbo Ring v2 is a high-performance, redundant network topology developed by Moxa for configuring network devices in redundant loops.

In the event of a link failure, the network can automatically reconfigure itself to maintain uninterrupted communication. Recovery times are within 20 ms for Fast Ethernet and 50 ms for Gigabit Ethernet on a network of up to 250 nodes.



Turbo Ring v2 allows connected network devices to elect a "master" switch, which blocks packets from traveling through any of the network's redundant loops and manages the network. If a section breaks, the protocol adjusts the ring so that the disconnected parts of the network establish contact. This enables continuous network operations, even when there is a fault in the network.

Furthermore, the election mechanism is redundant. If the "master" device itself fails, the network devices detect the failure and automatically elect another. The process occurs quickly, ensuring no interruption.

Turbo Ring v2 supports a backup segment connected to the redundant port (secondary port) on the ring "master". In this case, the backup path is easily identifiable for troubleshooting and replacement.

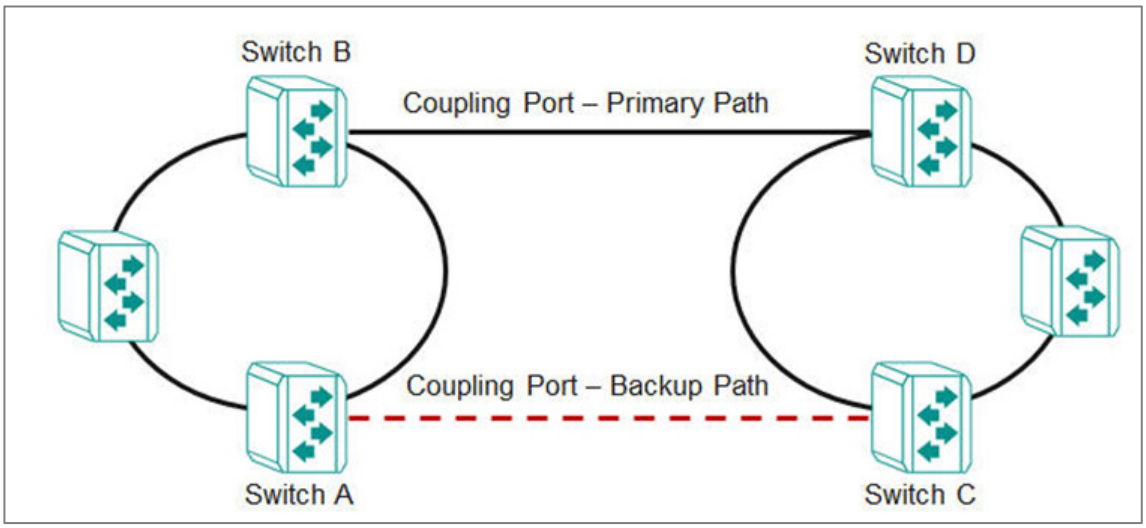
Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

About Ring Coupling

Ring Coupling refers to the practice of coupling two rings together.

This may be useful when creating a large redundant ring is inconvenient or impractical, such as for devices in remote areas. Smaller redundant rings can be coupled together for inter-ring communication while still maintaining redundancy of constituent rings and couplings.



Ring coupling uses extra ports on each pair of coupled switches. In this example, that means:

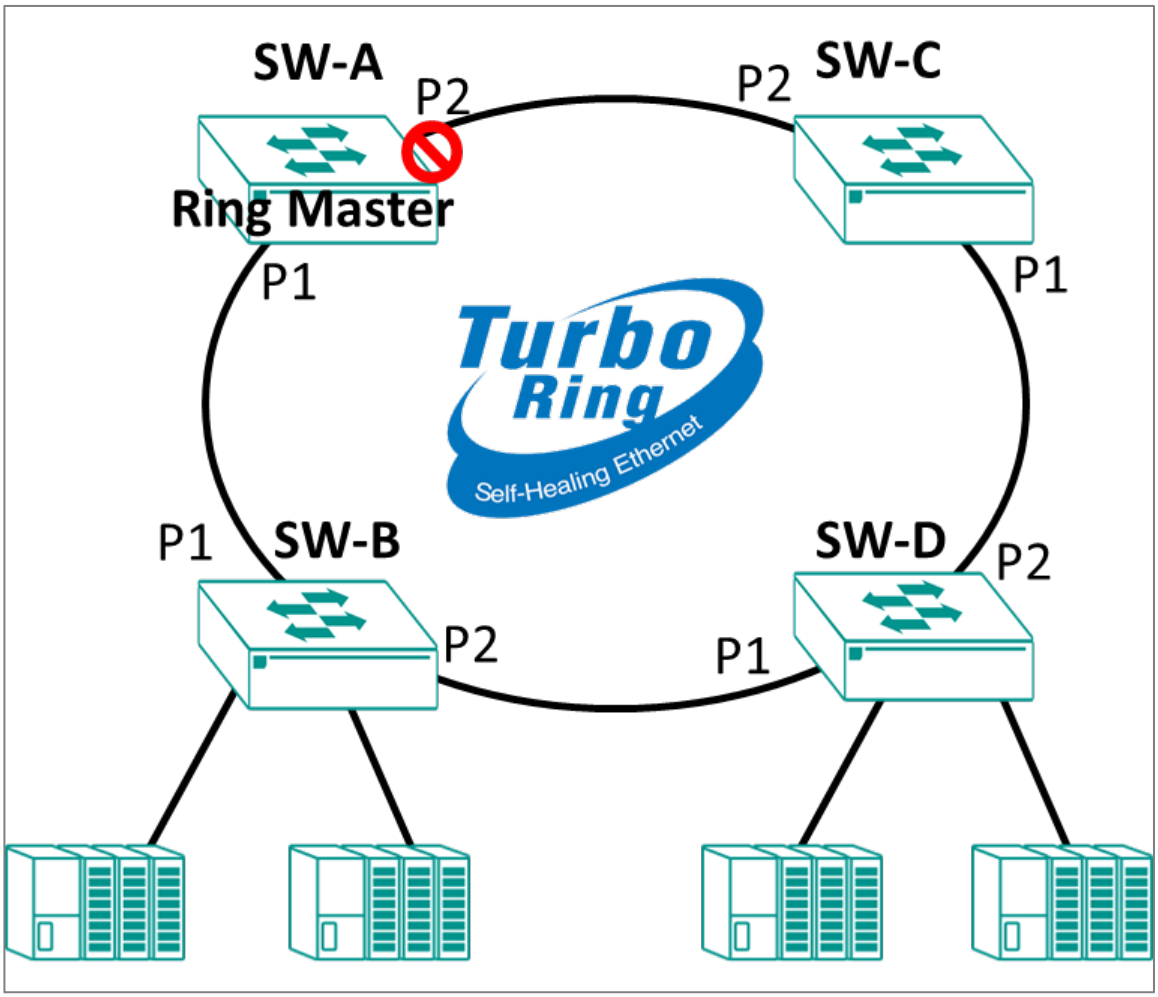
- The (Primary) coupling port on Switch B monitors the main path and connects directly to the port on Switch D.
- The (Backup) coupling port on Switch A monitors the main path and connects directly to the port on Switch C.

> **Note**
> There can be only one coupling (primary + backup) per ring pair.

Scenario: Using Turbo Ring in a Manufacturing Plant

In this scenario, we describe a factory using a simple ring topology.

A manufacturing plant has a complex network of machines and devices that communicate with each other to keep the production line running smoothly. To ensure that the network remains stable and reliable, the plant needs to use Turbo Ring v2 to create a fault-tolerant network by forming a ring topology.



Set up Turbo Ring v2 to connect multiple networks of machines and devices to create a fault-tolerant network and achieve continuous operations.

Ensure that switches are installed and powered. Wait to connect them until the end.

To configure this scenario, do the following:

1. Configure the settings each network device for Turbo Ring v2.

   See the subsequent sections for details about how to configure each device.

2. Connect the network devices in a ring topology, using ports 1 and 2 for ring segments.

If the master network device fails, the other devices in the ring will automatically detect the problem and initiate a new election process to select a new master switch, ensuring that there is no significant interruption in communication.

Example: Configuring the Master for Turbo Ring v2 in a Manufacturing Plant

Configure the device labeled SW-A for Turbo Ring v2 in our factory example.

Make sure you have NOT connected the ring ports until after you configure Turbo Ring v2 settings. Our examples use ports **1** and **2** as ring ports.

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **Settings**.
3. Set **Turbo Ring V2** to **Enabled**.
4. Under Ring Settings, next to **Ring 1**, click **[Edit].**

The Ring 1 Settings screen appears.

5. Configure all of the following:

Option	Value
Enabled	**Enabled**
Master	**Enabled**
Ring Port 1	**1**
Ring Port 2	**2**

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
Multiple devices set to Enabled	Ring election based on MAC addresses of **Enabled** devices
No devices set to Enabled	Ring election based on MAC addresses of all devices
Single device set to Enabled	**Enabled** device always master, failure of **Enabled** device results in ring election

6. Click **Apply** to save your changes.

Repeat this step on devices SW-B, SW-C, and SW-D, but with the **Master** setting set to **Disabled**. This process is outlined in the subsequent section.

Example: Configuring Non-Master Network Devices for Turbo Ring v2 in a Manufacturing Plant

Follow these steps to configure devices SW-B through SW-D in our scenario.

Make sure you have NOT connected the ring ports until after you configure Turbo Ring v2 settings. Our examples use ports **1** and **2** as ring ports.

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **Settings**.
3. Set **Turbo Ring V2** to **Enabled**.
4. Under Ring Settings, next to **Ring 1**, click **[Edit].**

   The Ring 1 Settings screen appears.
5. Configure all of the following:

Option	Value
Enabled	**Enabled**
Master	**Disabled**
Ring Port 1	**1**
Ring Port 2	**2**

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
Multiple devices set to Enabled	Ring election based on MAC addresses of **Enabled** devices
No devices set to Enabled	Ring election based on MAC addresses of all devices
Single device set to Enabled	**Enabled** device always master, failure of **Enabled** device results in ring election

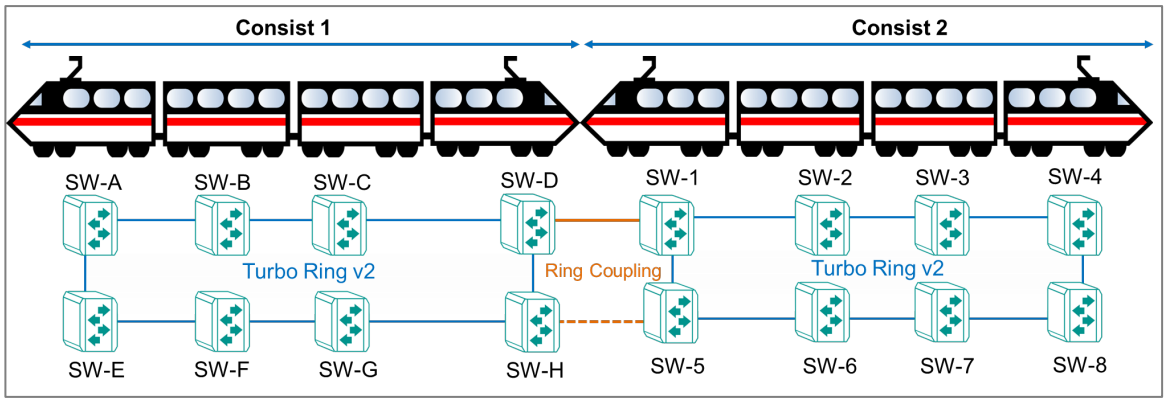
6. Click **Apply** to save your changes.

Once all devices in the ring are configured and enabled, you can connect the ring ports.

Scenario: Using Turbo Ring in an On-board Train Application

In this scenario, we describe setting up Turbo Ring v2 with ring coupling between train consists.

A railway vehicle manufacturer needs to plan a new on-board network with redundancy and flexible inter-consist communication. The customer plans a ring network with Turbo Ring v2 between multiple vehicles to form one ring per consist. Multiple consists will then use ring coupling for inter-consist communication.



This structure allows for easy administration as consists are coupled and uncoupled.

To configure this scenario, do the following:

1. Configure the settings each network device for Turbo Ring v2.
   See the subsequent sections for details about how to configure each device.
2. Connect the network devices SW-A through SW-H in a ring topology, using ports 1 and 2 for segments of the ring. Do the same for SW-1 through SW-8. Do not connect the ring coupling yet.
3. Configure the Primary Coupling Path path on SW-D.
   See the subsequent sections for details about how to configure ring coupling.
4. Configure the Backup Ring Coupling on SW-H.
   See the subsequent sections for details about how to configure ring coupling.

Once all devices have been configured, you can connect the ring ports and coupling ports.

Example: Configuring the Master for Turbo Ring v2 in an On-board Rail Application

Make sure you have NOT connected the ring ports until after you configure Turbo Ring v2 settings. Our examples use ports **1** and **2** as ring ports.

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **Settings**.
3. Set **Turbo Ring V2** to **Enabled**.
4. Under Ring Settings, next to **Ring 1** , click **[Edit].**

   The Ring 1 Settings screen appears.
5. Configure all of the following:

Option	Value
Enabled	**Enabled**
Master	**Enabled**
Ring Port 1	**1**
Ring Port 2	**2**

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
Multiple devices set to Enabled	Ring election based on MAC addresses of **Enabled** devices
No devices set to Enabled	Ring election based on MAC addresses of all devices
Single device set to Enabled	**Enabled** device always master, failure of **Enabled** device results in ring election

6. Click **Apply** to save your changes.

Once all devices in the ring are configured and enabled, you can connect the ring ports.

Continue to the next section to see how to configure ring coupling. Do not connect coupling ports until network devices have been configured.

Example: Configuring non-Master devices for Turbo Ring v2 in an On-board Rail Application

Make sure you have NOT connected the ring ports until after you configure Turbo Ring v2 settings. Our examples use ports **1** and **2** as ring ports.

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **Settings**.
3. Set **Turbo Ring V2** to **Enabled**.
4. Under Ring Settings, next to **Ring 1** , click **[Edit].**

   The Ring 1 Settings screen appears.
5. Configure all of the following:

Option	Value
Enabled	**Enabled**
Master	**Disabled**
Ring Port 1	**1**
Ring Port 2	**2**

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
Multiple devices set to Enabled	Ring election based on MAC addresses of **Enabled** devices
No devices set to Enabled	Ring election based on MAC addresses of all devices
Single device set to Enabled	**Enabled** device always master, failure of **Enabled** device results in ring election

6. Click **Apply** to save your changes.

Once all devices in the ring are configured and enabled, you can connect the ring ports. Once all

Continue to the next section to see how to configure ring coupling. Do not connect coupling ports until network devices have been configured.

Example: Configuring the Primary Ring Coupling Between Consists

Both network devices that make up the ring coupling must be configured as coupling devices.

- Make sure that you have configured both rings in the scenario.
- Do not connect the coupling ports until completing setup on both devices. Our scenario assumes port **5** will serve as coupling port.
- Couplers should only be configured on one ring. Our example uses SW-D as the primary and SW-H as the backup. Do not configure SW-1 or SW-5 as couplers.

To configure SW-D as the primary ring coupler:

The procedure on each device is identical. To configure each device, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **Settings**.
3. Under Ring Coupling Settings, click **[Edit].**

   The Ring Coupling Settings screen appears.
4. Configure all of the following:

Option	Value
Enabled	**Enabled**
Coupling Mode	**Coupling Primary Path**
Coupling Port	**5**

5. Click **Apply** to save your changes.

The device has been configured as a primary ring coupling.

Connect the ring coupling ports. Once both devices are connected, you can move on to configuring the backup coupling.

Example: Configuring the Backup Ring Coupling Between Consists

Both network devices that make up the backup ring coupling must be configured as coupling devices.

- Make sure that you have configured both rings in the scenario.
- Do not connect the coupling ports until completing setup on both devices. Our scenario assumes port **5** will serve as coupling port.
- Couplers should only be configured on one ring. Our example uses SW-D as the primary and SW-H as the backup. Do not configure SW-1 or SW-5 as couplers.

To configure SW-H as the backup coupler:

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **Settings**.
3. Under Ring Coupling Settings, click **[Edit]**.

   The Ring Coupling Settings screen appears.
4. Configure all of the following:

Option	Value
Enabled	**Enabled**
Coupling Mode	**Coupling Backup Path**
Coupling Port	**5**

5. Click **Apply** to save your changes.

The device has been configured as a backup ring coupling.

Once the device has been configured, connect the ring coupling ports. Your coupling configuration will be complete.

Turbo Ring V2

Menu Path: Redundancy > Turbo Ring V2

This page lets you set up and configure Turbo Ring v2 redundancy for your device.

This page includes these tabs:

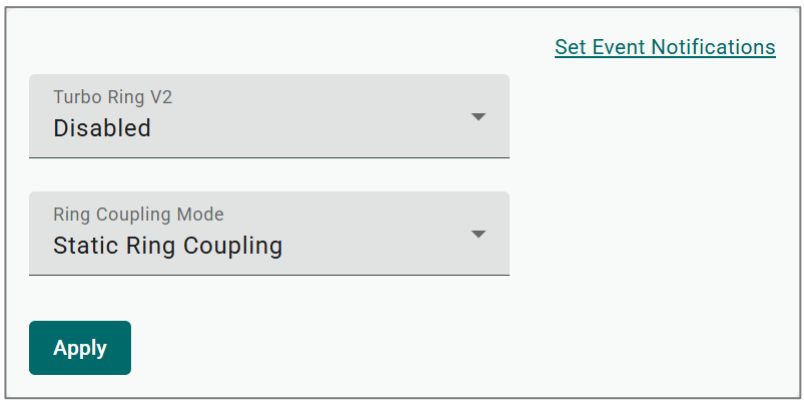
- Settings
- Status

Turbo Ring V2 - Settings

Menu Path: Redundancy > Turbo Ring V2 - Settings

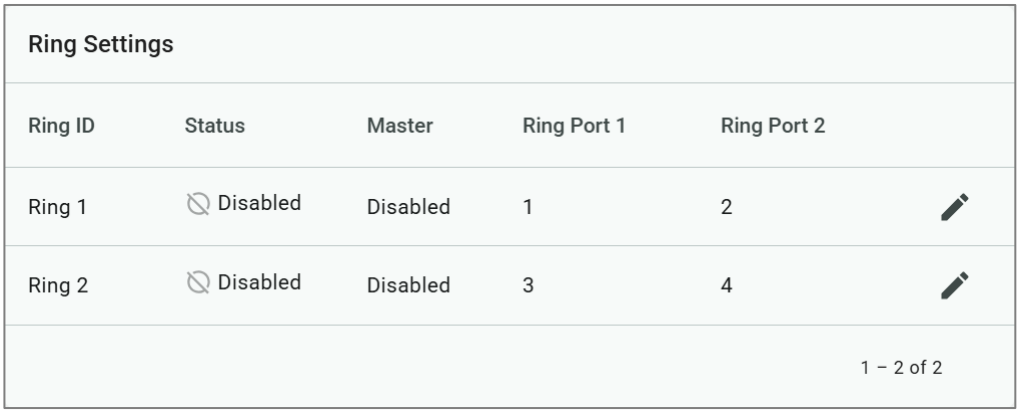
This page lets you configure the Turbo Ring V2 settings.

Turbo Ring V2 Settings



UI Setting	Description	Valid Range	Default Value
Turbo Ring V2	Enable or disable Turbo Ring V2 for the device.	Enabled / Disabled	Disabled
Ring Coupling Mode	Select the ring coupling mode to use for the device. • **Static Ring Coupling**: Manually configure the ring coupling port and coupling mode (primary path or backup path). • **Dynamic Ring Coupling**: Dynamically adjust ring coupling configurations. This allows the active coupler switch for each train consist to be automatically assigned when train consist sequences are changed, added, or removed.	Static Ring Coupling / Dynamic Ring Coupling	Static Ring Coupling

Ring Settings



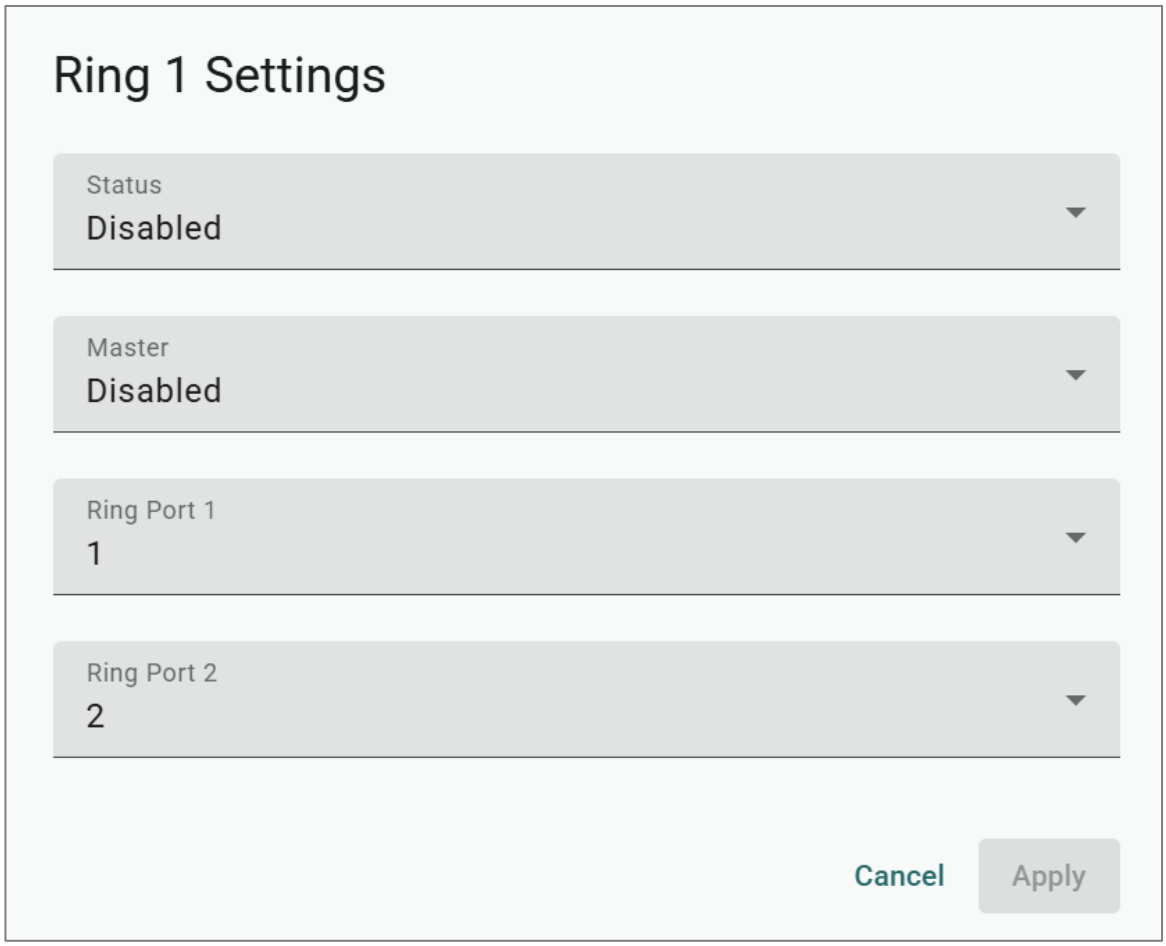
UI Setting	Description
Ring ID	Shows the ID of the ring the entry is for. **Note** When using dynamic ring coupling, only Ring 1 settings will be shown because dynamic ring coupling only operates on Ring 1.
Status	Shows whether Turbo Ring V2 is enabled for the ring.
Master	Shows whether the device is designated as the master for the ring.
Ring Port 1	Shows which port will act as ring port 1. If this device is designated as the master for the ring, this will be the primary ring connection.
Ring Port 2	Shows which port will act as ring port 2. If this device is designated as the master for the ring, this will be the backup ring connection and will be blocked normally.

Edit Ring Settings

Menu Path: Redundancy > Turbo Ring V2 - Settings

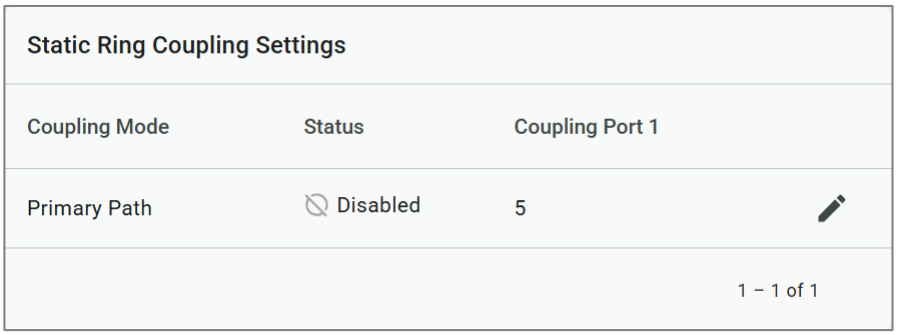
Clicking the **Edit (✎)** icon for a ring on the **Redundancy > Turbo Ring V2 - Settings** page will open this dialog box. This dialog lets you edit the Turbo Ring V2 settings for the ring.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable Turbo Ring V2 for the ring.	Enabled / Disabled	Disabled
Master	Enable or disable whether the device will be designated as the master for the ring.	Enabled / Disabled	Disabled
Ring Port 1	Specify which port will act as ring port 1. If this device is designated as the master for the ring, this will be the primary ring connection.	Drop-down list of ports	1
Ring Port 2	Specify which port will act as ring port 2. If this device is designated as the master for the ring, this will be the backup ring connection and will be blocked normally.	Drop-down list of ports	2

Static Ring Coupling Settings



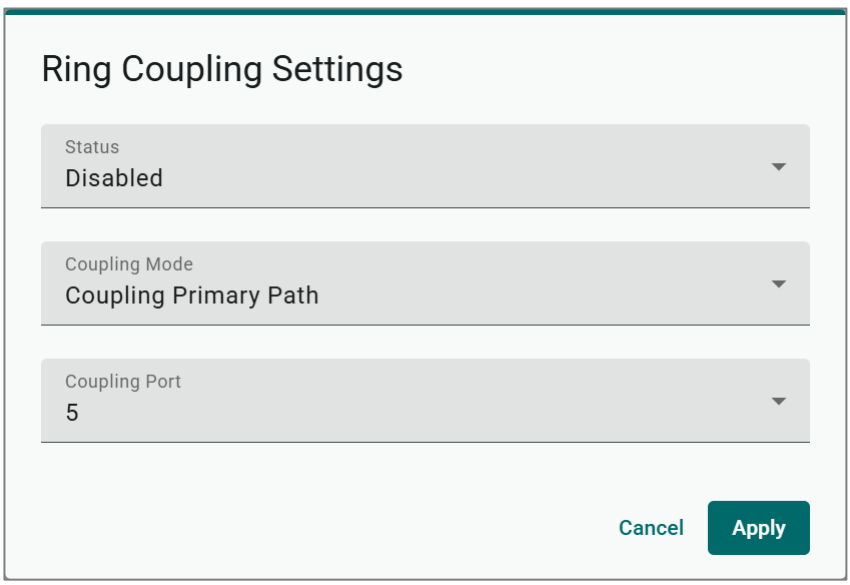
UI Setting	Description
Coupling Mode	Shows which coupling mode the entry is for.
Status	Shows whether ring coupling is enabled or disabled.
Coupling Port	Shows the port used for ring coupling.

Edit Static Ring Coupling Settings

Menu Path: Redundancy > Turbo Ring V2 - Settings

Clicking the **Edit (✎)** icon for an entry in the Static Ring Coupling Settings list on the **Redundancy > Turbo Ring V2 - Settings** page will open this dialog box. This dialog lets you edit the ring coupling settings for the entry.

Click **Apply** to save your changes.

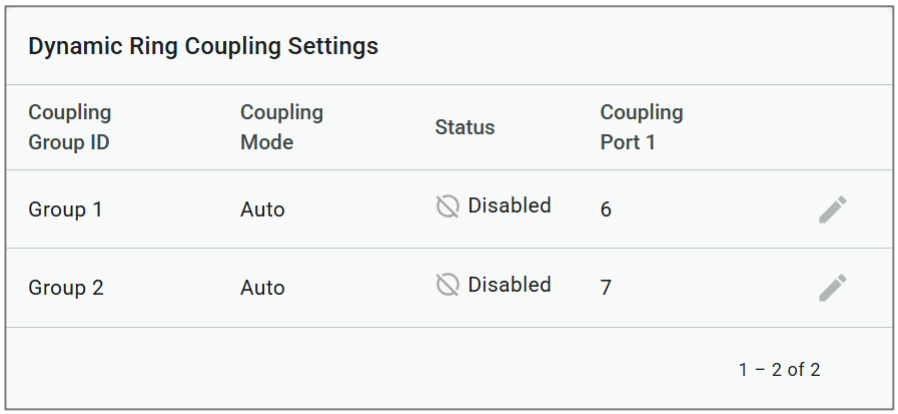


UI Setting	Description	Valid Range	Default Value
Status	Enable or disable ring coupling for the device.	Enabled / Disabled	Disabled
Coupling Mode	Specify whether this device will be designated as primary or backup path for ring coupling.	Coupling Primary Path / Coupling Backup Path	Coupling Primary Path
Coupling Port	Specify the port to use for ring coupling.	Drop-down list of ports	5

Dynamic Ring Coupling Settings

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.



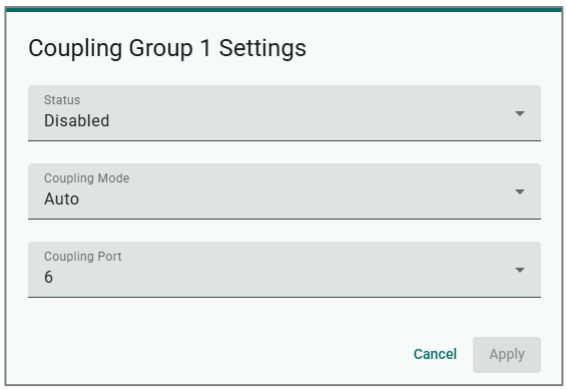
UI Setting	Description
Coupling Group ID	Shows the ID of the coupling group the entry is for.
Coupling Mode	Shows the coupling mode used for the group.
Status	Shows whether the ring coupling group is enabled or disabled.
Coupling Port	Shows which port is the coupling port for the group.

Edit Dynamic Ring Coupling Settings

Menu Path: Redundancy > Turbo Ring V2 - Settings

Clicking the **Edit (✎)** icon for an entry in the Dynamic Ring Coupling Settings list on the **Redundancy > Turbo Ring V2 - Settings** page will open this dialog box. This dialog lets you edit the ring coupling settings for the entry.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the dynamic ring coupling group.	Enabled / Disabled	Disabled
Coupling Mode	Specify the mode used to determine the coupling mode for the group. • **Coupling Backup Path**: This group will act as the backup path. • **Coupling Primary Path**: This group will act as the primary path. • **Auto**: The ring master will collect packets from all ring coupling switches to determine whether the group will act as the primary or backup path. **Note** If both ports in the same group have the same role, the port with the smaller MAC address will be the backup port, and the other port will be the primary port.	Coupling Backup Path / Coupling Primary Path / Auto	Auto
Coupling Port	Specify which port will act as the coupling port for the group.	Drop-down list of ports	Group 1: 6 Group 2: 7

Turbo Ring V2 - Status

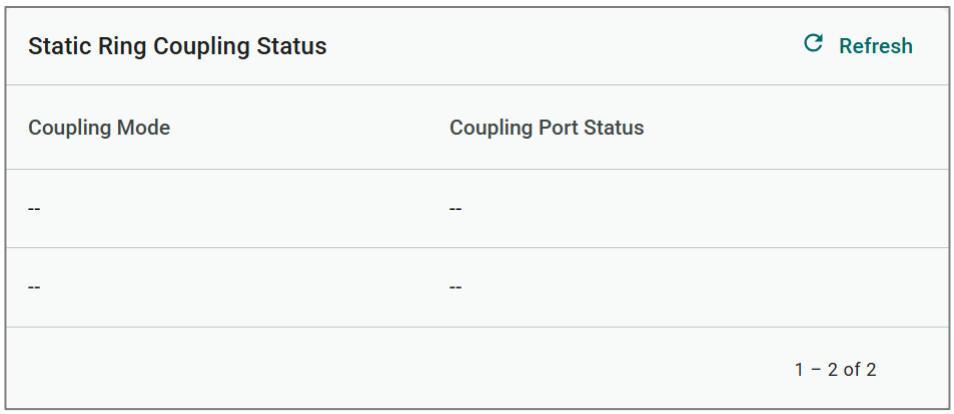
Menu Path: Redundancy > Turbo Ring V2 - Status

This page lets you view the Turbo Ring V2 ring and ring coupling status.

Ring Status

UI Setting	Description
Ring ID	Shows the ID of the ring the entry is for. **Note** When using dynamic ring coupling, only Ring 1 will be shown because dynamic ring coupling only operates on Ring 1.
Master ID	Shows the MAC address of the ring master.
Status	Shows the status of the ring. • **Healthy**: The ring and the ports are working properly. • **Break**: One or more rings are currently broken. • **Disabled**: The ring is disabled.
Role	Shows whether the device is configured as a master or slave for the ring.
Ring Port 1	Shows which port will act as ring port 1. If this device is designated as the master for the ring, this will be the primary ring connection.
Ring Port 2	Shows which port will act as ring port 2. If this device is designated as the master for the ring, this will be the backup ring connection and will be blocked normally.

Static Ring Coupling Status



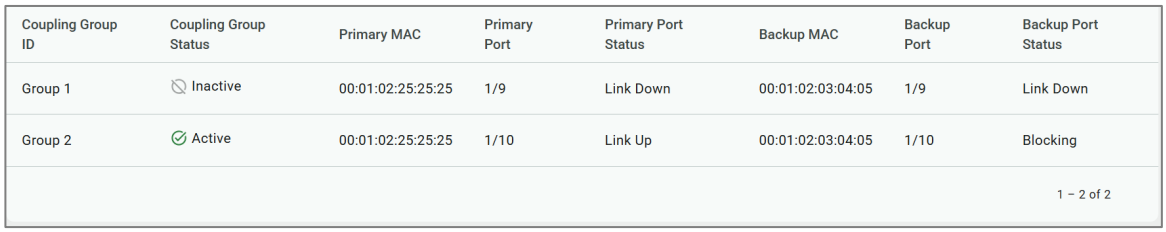
UI Setting	Description
Coupling Mode	Shows whether the device is the primary or backup path for ring coupling.
Coupling Port Status	Shows the status of the port used for ring coupling.

Dynamic Ring Coupling Status

UI Setting	Description
Role	Shows the device role for Turbo Ring V2.
Ring Index	Shows the ring index for dynamic ring coupling. This allows the device to determine its order within the dymamic ring coupling mechanism.
Total Ring Number	Shows the the total ring number for dynamic ring coupling. This allows the device to determine its order within the dymamic ring coupling mechanism.

Dynamic Ring Coupling Status List - Master

If the device role is **Master,** this table will appear.



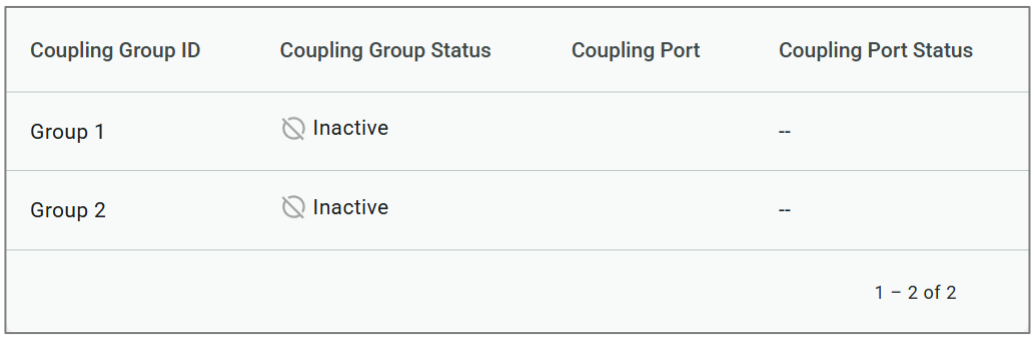
Coupling Group ID	Coupling Group Status	Primary MAC	Primary Port	Primary Port Status	Backup MAC	Backup Port	Backup Port Status
Group 1	Inactive	00:01:02:25:25:25	1/9	Link Down	00:01:02:03:04:05	1/9	Link Down
Group 2	Active	00:01:02:25:25:25	1/10	Link Up	00:01:02:03:04:05	1/10	Blocking

1 – 2 of 2

UI Setting	Description
Coupling Group ID	Shows the ID of the coupling group which the entry is for.
Coupling Group Status	Shows whether the group is active or inactive.
Primary MAC	Shows the MAC address of the primary port used for the group.
Primary Port	Shows the primary port used for the group.
Primary Port Status	Shows the status of the primary port used for the group. • **Remote coupler switch**: Shows the status of the coupling port as **Link Up** or **Link Down**. • **Local coupling port**: Shows the status of the coupling port as **Link Down, Forwarding,** or **Blocking**.
Backup MAC	Shows the MAC address of the backup port used for the group.
Backup Port	Shows the backup port used for the group.
Backup Port Status	Shows the status of the backup port used for the group. • **Remote coupler switch**: Shows the status of the coupling port as **Link Up** or **Link Down**. • **Local coupling port**: Shows the status of the coupling port as **Link Down, Forwarding,** or **Blocking**.

Dynamic Ring Coupling Status List - Slave

If the device role is **Slave,** this table will appear.



Coupling Group ID	Coupling Group Status	Coupling Port	Coupling Port Status
Group 1	Inactive		--
Group 2	Inactive		--

1 – 2 of 2

UI Setting	Description
Coupling Group ID	Shows the ID of the coupling group which the entry is for.
Coupling Group Status	Shows whether the group is active or inactive.
Coupling Port	Shows the coupling port used for the group.
Coupling Port Status	Shows the status of the local coupling port used for the group as **Link Down**, **Forwarding**, or **Blocking**.

About MRP (Media Redundancy Protocol)

MRP (Media Redundancy Protocol) is a network protocol based on the IEC 62439-2 that allows users to create a redundant ring system. With a recovery time of less than 200 ms, it can support up to 50 devices in each ring.

MRP includes the following roles:

MRM (Media Redundancy Manager)

MRM, also known as the Ring Manager, is a node in the network topology that manages and monitors the health of the entire ring. There is only one MRM in the network. In the event of a Link Down scenario, the MRM diagnoses the issue and notifies all MRCs (Media Redundancy Clients) to flush their MAC address table and relearn the path. Additionally, the MRM changes the port status of the primary port from blocking to forwarding to restore connectivity.

MRC (Media Redundancy Client)

MRC, also known as the Ring Client, is a node in the network topology that is monitored by the MRM (Media Redundancy Manager). However, the MRCs do not solely rely on the MRM to detect the health of the ring, they also automatically notify the MRM in the event of a Link Down or Recovery situation. The MRC flushes its MAC address table and relearns the path when requested by the MRM.

MIM (Media Redundancy Interconnection Manager)

The function of the MIM is to observe and to control the redundant interconnection topology in order to react on interconnection faults. To cover a maximum of applications, two detection methods are provided by this international standard. The MIM can observe the interconnection topology by either:

- **LC-mode (Link check mode)**: The MRP interconnection manager can observe the interconnection topology by reacting directly on interconnection port link change notification messages
- **RC-mode (Ring check mode)**: The MRP interconnection manager can observe the interconnection topology by sending test frames on the interconnection port over the connected rings and receiving them over its ring ports, checking in both directions

MIC (Media Redundancy Interconnection Client)

The other three nodes in the interconnection topology have the role of media redundancy interconnection clients (MIC), in addition to the role of a MRC or MRM. The MIC reacts on received reconfiguration frames from the MIM, it can detect and signal link changes of its interconnection port, and it can issue link change notification messages.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

Configuring Ring Managers and Clients

MRP Managers and Clients must be configured before the rings can be used.

- Determine which devices will be the Manager and the Clients. There can only be a single manager.
- Do not connect any of the devices until configuration of all devices is complete.
- Do not use any of the ring ports until configuration is completed. Do not use these ports for administration, as applying the chain configuration to these ports will disconnect you from the web GUI.

Choose a device to configure and do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **MRP**, and then click **Settings**.
3. Under Media Redundancy Protocol, choose **Enabled** from the drop-down menu.
4. Specify the following based on the **Role**:

Ring Manager Option	Ring Manager Value
Role	**Ring Manager**
VLAN ID	Specify the VLAN ID for the ring
Domain UUID	Choose either **Default** or **PROFITNET (Siemens)** according to your network configuration
React on Link Change	It is recommended to set this to **Enabled**. This setting allows the Ring Manager to quickly respond to topology changes, both when a link goes down and when the original topology is restored.
Ring Port 1	Specify the first redundant ring port
Ring Port 2	Specify the second redundant ring port

Ring Client Option	Ring Client Value
Role	**Ring Client**
VLAN ID	Specify the VLAN ID for the ring
Domain UUID	Choose either **Default** or **PROFITNET (Siemens)** according to your network configuration
Ring Port 1	Specify the first redundant ring port

Ring Client Option	Ring Client Value
Ring Port 2	Specify the second redundant ring port

5. Click **Apply** to save your changes.

Once all devices are configured, you can connect the ring ports.

MRP

Menu Path: Redundancy > MRP

This page lets you configure the MRP parameters of the switch and view the MRP protocol operation status of the switch.

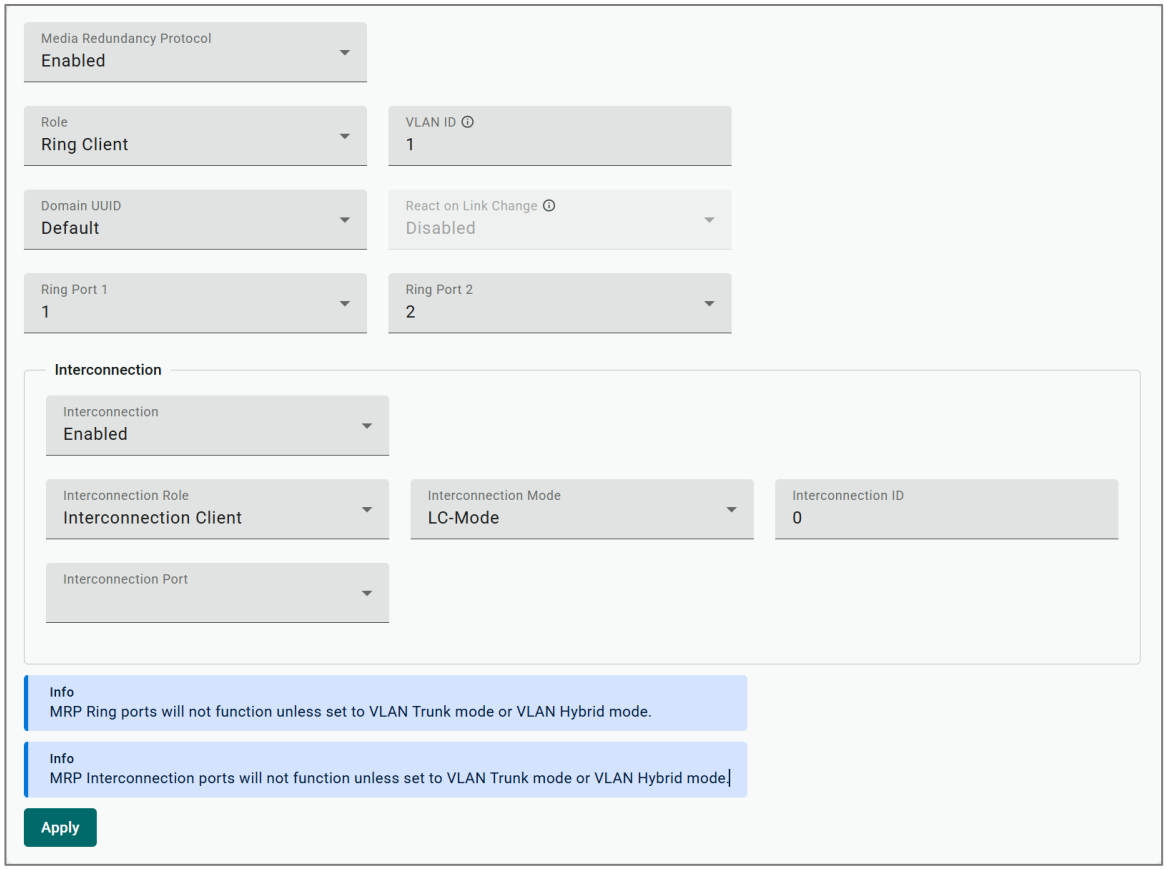
This page includes these tabs:

- Settings
- Status

MRP - Settings

Menu Path: Redundancy > MRP - Settings

This page lets you enable and configure MRP for your device.



UI Setting	Description	Valid Range	Default Value
Media Redundancy Protocol	Enable or disable Media Redundancy Protocol (MRP) for the device.	Enabled / Disabled	Disabled
Role	Specify the role for the device. • **Ring Client**: The device will act as a ring client. • **Ring Manager**: The device will act as a ring manager, and can manage and monitor the ring's health status.	Ring Client / Ring Manager	Ring Client
VLAN ID	Specify the VLAN ID to use for MRP. **Note** The VLAN ID should align with the ring port settings.	1 to 4094	1
Domain UUID	Select whether to use a default or PROFINET domain UUID.	Default / PROFINET	Default

UI Setting	Description	Valid Range	Default Value
React on Link Change **(If Role is Ring Manager)**	Enable or disable reacting on link change. Enable reaction on link change for faster recovery speeds.	Enabled / Disabled	Enabled
Ring Port 1	Specify the port to use as the 1st redundant port. **Note** Only select the port in VLAN Trunk/Hybrid mode.	Drop-down list of ports	N/A
Ring Port 2	Specify the port to use as the 2nd redundant port. **Note** Only select the port in VLAN Trunk/Hybrid mode.	Drop-down list of ports	N/A

Interconnection

UI Setting	Description	Valid Range	Default Value
Interconnection	Enable or disable MRP interconnection for the device.	Enabled / Disabled	Disabled
Interconnection Role	Select the interconnection role for the device.	Interconnection Manager / Interconnection Client	Interconnection Client
Interconnection Mode	Select the interconnection mode to use for the device. **Note** The Interconnection Manager and all Interconnection Clients in the same MRP interconnection topology must use the same interconnection mode.	LC-Mode / RC-Mode	LC-Mode
Interconnection ID	Specify an ID for the interconnection.	0 to 65535	0

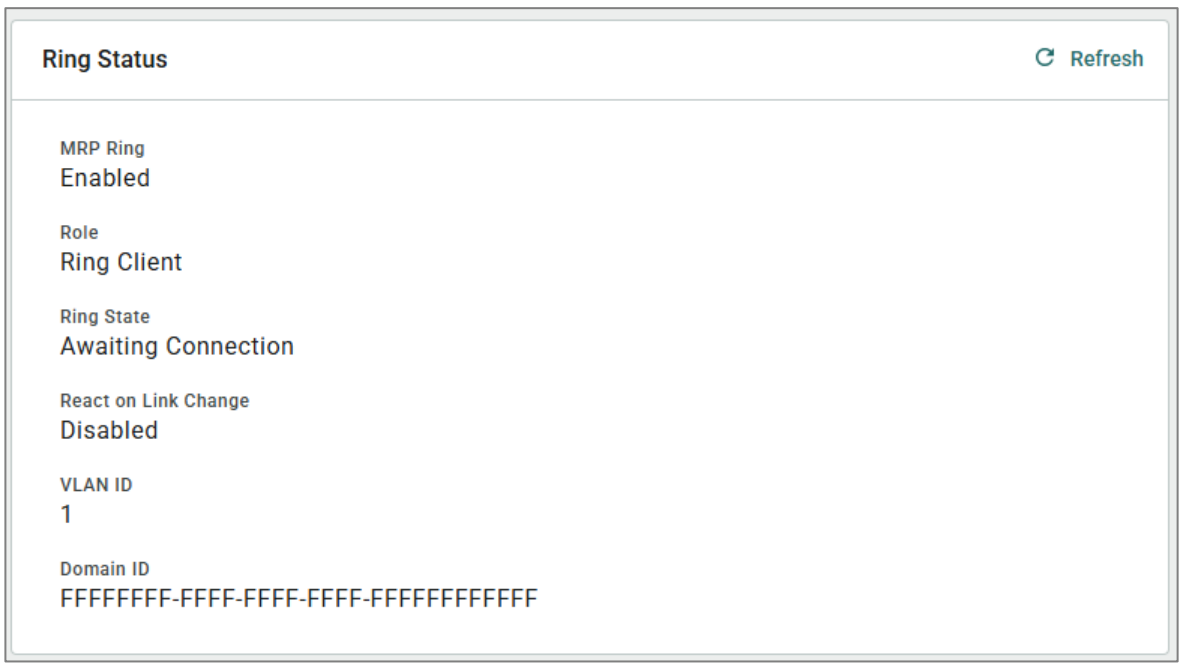
UI Setting	Description	Valid Range	Default Value
Interconnection Port	Select a port to use for the interconnection. **Note** For MRP Interconnection to perform properly, only select a port using VLAN Trunk/Hybrid mode.	Drop-down list of ports	3

MRP - Status

Menu Path: Redundancy > MRP - Status

This page lets you view the overall status of the MRP ring and ring ports.

Ring Status



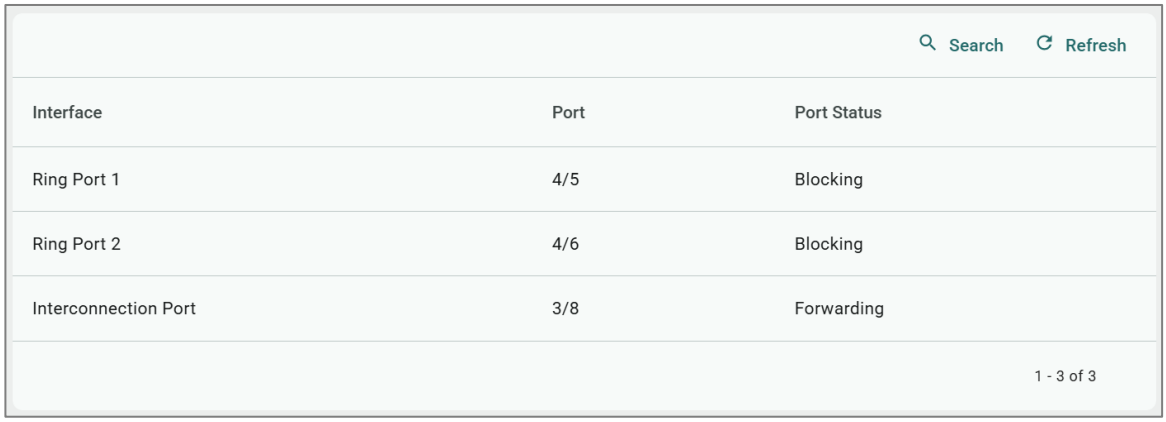
UI Setting	Description
MRP Ring	Shows whether the MRP ring is enabled.
Role	Shows the role of the device.
Ring State	Shows the current ring state.

UI Setting	Description
React on Link Change	Shows whether reaction on link change is enabled.
VLAN ID	Shows the VLAN ID for the ring.
Domain ID	Shows the domain UUID for the ring.

Interconnection Status

UI Setting	Description
Interconnection	Shows whether MRP Interconnection is enabled.
Interconnection Role	Shows the Interconnection role of the device.
Interconnection State	Shows the current Interconnection state.
Interconnection Mode	Shows the current Interconnection mode.
Interconnection ID	Shows the Interconnection ID for the ring.

MRP Port Status List



UI Setting	Description
Interface	Shows the interface the entry is for.
Port	Shows the port used for the interface.
Port Status	Shows the port status of the interface.

Network Service

Menu Path: Network Service

This section lets you configure your device's network services.

This section includes these pages:

- DHCP Server
- DHCP Relay Agent
- DNS Server
- mDNS Responder

Network Service - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to System > Account Management > User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
DHCP Server	R/W	R/W	R
DHCP Relay Agent	R/W	R/W	R
DNS Server	R/W	R/W	R
mDNS Responder	R/W	R/W	R

Configuring DHCP Server Functions

Moxa routers and L2 switches support DHCP server functionality, allowing auto-assignment of IP configurations.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

Introduction to DHCP

The Dynamic Host Configuration Protocol (DHCP) automatically provides an Internet Protocol (IP) host with an IP configuration. This can include IP address, subnet mask, DNS Configuration, and default gateway. among others.

This ensures that connected clients do not need manual IP configuration, saving time and increasing flexibility in deployments.

Overview of DHCP Server Configuration

The integrated DHCP server of the device can operate in one of three modes.

DHCP Pool

This mode automatically assigns IP addresses to connected devices from a user-configured IP address pool.

MAC-based IP Assignment (Static IP)

MAC-based IP assignment, also known as static IP assignment, assigns specified IP addresses to MAC addresses of network devices. This ensures that devices maintain the same IP address, regardless of factors like connection order or lease duration. By configuring a DHCP server with table of MAC addresses and corresponding IP addresses, administrators can have more control over IP allocation, and by extension, device management and security.

Note

DHCP Pool and MAC-based IP Assignment can be active at the same time.

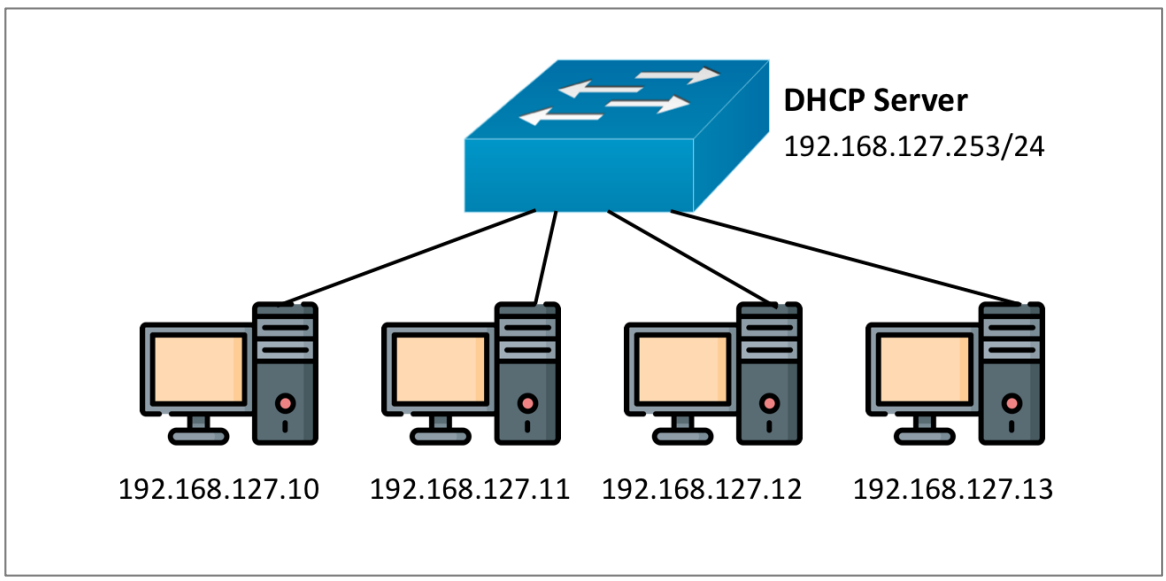
Port-based IP Assignment

Port-based IP assignment allocates IP addresses by the physical port on the device (Port 1, 2 etc.). This allows pre-assignment based on port, ensuring the device connected to each port will always have the same IP address.

Configuring Dynamic IP Address Assignment (DHCP Server Pool)

In this example, we configure a sample scenario with a pool of automatically-assigned IP addresses.

This scenario explains how automatically assign IP addresses to four PC clients on a subnet. We configure a switch act as DHCP server to automatically assign addresses, in In this scenario, the switch acts as a DHCP server for the 192.168.127.xxx IP subnet and PCs are DHCP clients.



1. Sign in to the device using administrator credentials.
2. Go to **Network Service** > **DHCP Server** > **General**.
3. Under **Mode**, make sure **DHCP/MAC-based IP Assignment** is selected.

4. Under **DHCP Pool Settings**, select **Enabled** from the drop-down list.

The IP Address Pool configuration options appear.

5. Configure all of the following:

Option	Value
Starting IP Address	192.168.127.10
Subnet Mask	**24 (255.255.255.0)**
Ending IP Address	192.168.127.20
Default Gateway	192.168.127.253
Lease Time	1440
DNS Server IP Address 1	8.8.8.8
DNS Server IP Address 2	8.8.8.4
NTP Server IP Address	8.8.8.10

6. Click **Apply** to save your settings.

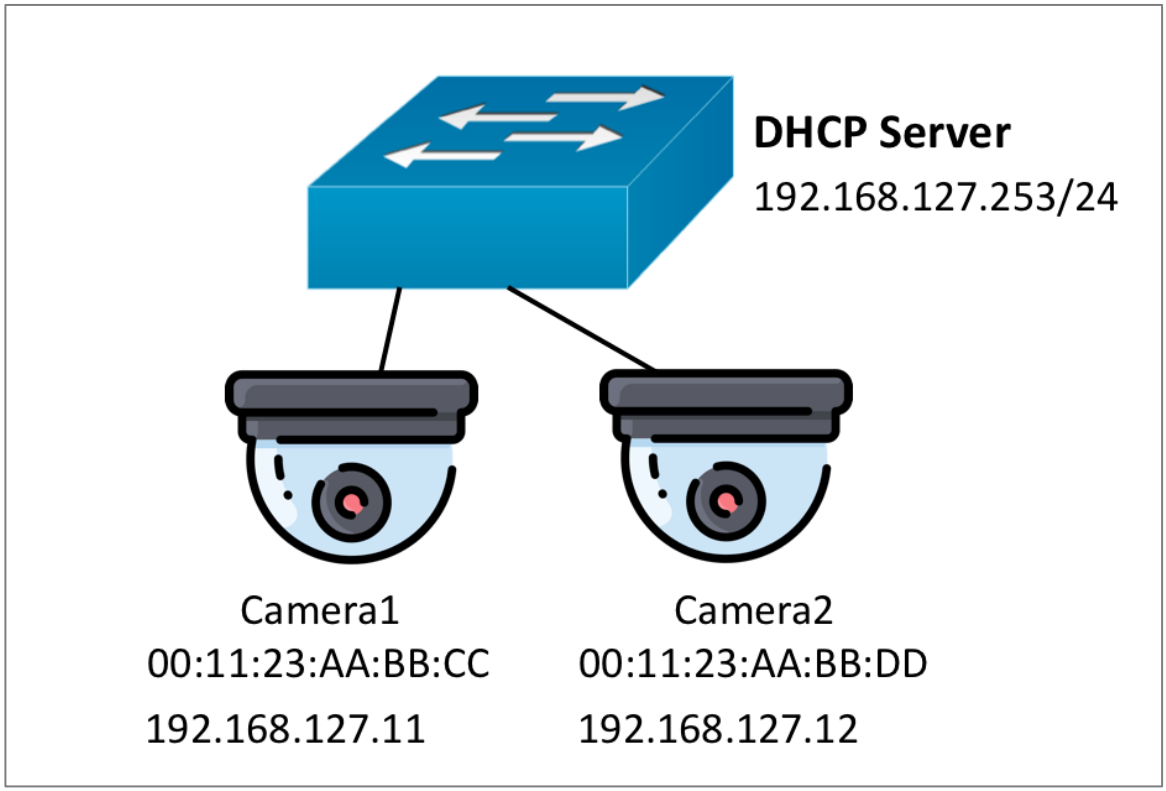
Note

You can delete entries by going to Network Service > DHCP Server > General, and then under DHCP Pool Settings, choose Disabled from the drop-down menu.

Reserving IP Addresses for Specific Devices (MAC-based IP Assignment)

This scenario outlines how to reserve and automatically assign IP addresses for two cameras, ensuring that each camera always receives the same address.

We will configure the switch using MAC-based IP reservation and assignment.



1. Sign in to the device using administrator credentials.
2. Go to **Network Service** > **DHCP Server** > **General**.
3. Under **Mode**, choose **DHCP/MAC-based IP Assignment** from the drop-down list, and then click **Apply**.
4. In the table below **Mode**, click ***[Add]***.

The Create Entry screen appears.

5. Configure all of the following:

Option	Value
Enable	**Enabled**
Hostname	Camera1
IP Address	192.168.127.11
Subnet Mask	**24 (255.255.255.0)**

Option	Value
MAC Address	00:11:23:AA:BB:CC
Default Gateway	192.168.127.253
Lease Time	1440
DNS Server IP Address1	8.8.8.8
DNS Server IP Address1	8.8.8.4
NTP Server IP Address	8.8.8.10

The entry will appear in the table.

6. Repeat this process for the second camera, with the following settings:

Option	Value
Enable	**Enabled**
Hostname	Camera2
IP Address	192.168.127.12
Subnet Mask	**24 (255.255.255.0)**
MAC Address	00:11:23:AA:BB:CC
Default Gateway	192.168.127.253
Lease Time	1440
DNS Server IP Address1	8.8.8.8
DNS Server IP Address1	8.8.8.4
NTP Server IP Address	8.8.8.10

The entry will appear in the table.

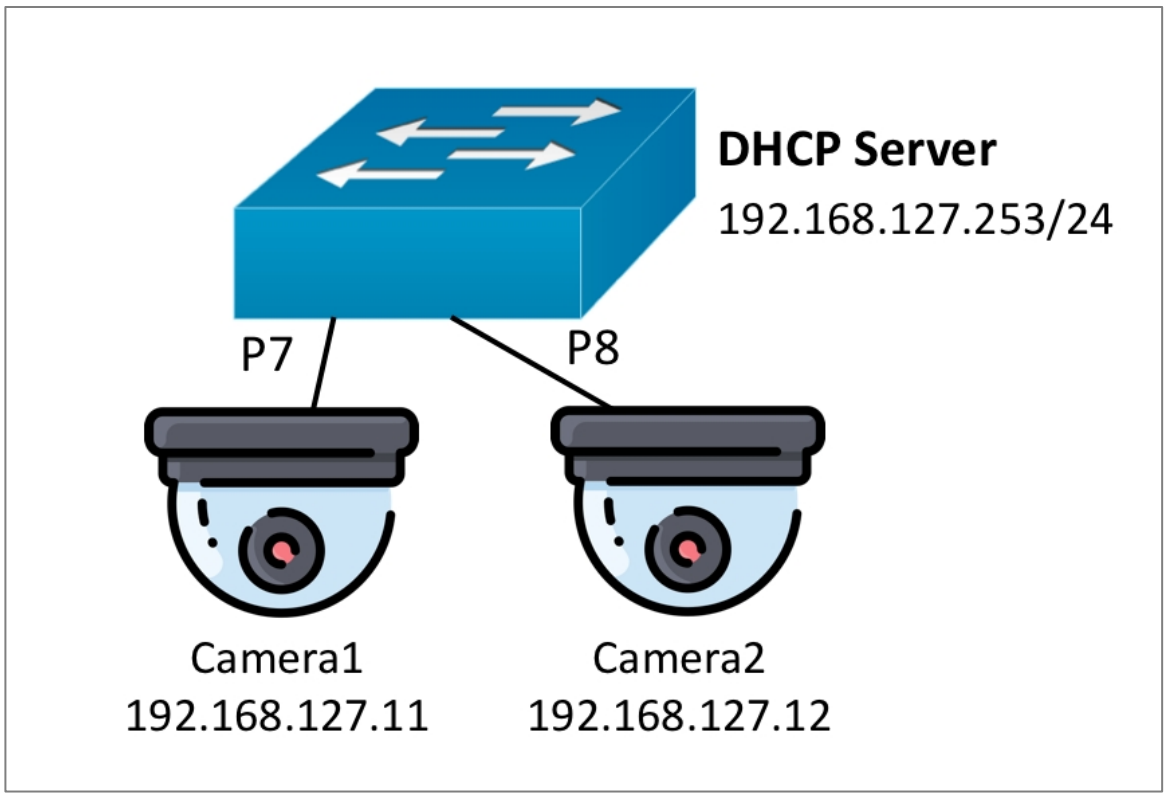
Note

You can delete entries by going to Network Service > DHCP Server > General, and then in the table at the bottom of the page, selecting one or more entries by clicking the corresponding checkbox, and then clicking [Delete].

Configuring Port-based IP Assignment

This scenario assigns IP addresses to cameras based on their port of connection.

We will configure the switch as a DHCP server that uses port index-based IP assignments for each of the cameras. All ports will always assign the same IP addresses.



1. Sign in to the device using administrator credentials.
2. Go to **Network Service** > **DHCP Server** > **General**.
3. Under **Mode**, choose **Port-based IP Assignment** from the drop-down list, and then click **Apply**.
4. In the table below **Mode**, click ***[Add]***.

5. Configure all of the following:

Option	Value
Enable	**Enabled**
Port	**7**
IP Address	192.168.127.11
Subnet Mask	**24 (255.255.255.0)**
Default Gateway	192.168.127.253
Lease Time	1440
DNS Server IP Address1	8.8.8.8
DNS Server IP Address1	8.8.8.4
NTP Server IP Address	8.8.8.10
Hostname	Camera1

The entry will appear in the table.

6. Repeat this process for the second camera, with the following settings:

Option	Value
Enable	**Enabled**
MAC Address	00:11:23:AA:BB:CC
IP Address	192.168.127.12
Subnet Mask	**24 (255.255.255.0)**
Default Gateway	192.168.127.253
Lease Time	1440
DNS Server IP Address1	8.8.8.8

Option	Value
DNS Server IP Address1	8.8.8.4
NTP Server IP Address	8.8.8.10
Hostname	Camera2

The entry will appear in the table.

Note

You can delete ports from the list at the bottom of the page by clicking the corresponding checkbox, and then clicking [Delete].

Note

You can delete ports from the list by clicking on Port-based IP Assignment, clicking the corresponding checkbox, and then clicking [Delete].

DHCP Server

Menu Path: Network Service > DHCP Server

This page lets you configure the DHCP server settings.

This page includes these tabs:

- General
- Lease Table
- Classless Static Route Table

Note

MX-NOS Rail V1.0 supports the following options:

- DHCP Client option 1/3/6/53/55/61/66/67/255
- DHCP Server option 1/3/6/7/12/15/42/51/53/54/*55/66/67/121/255
    - *55: The DHCP server will not include option 55 in its outgoing packets, but it will process option 55 if it is received from a DHCP client.

DHCP Server - General

Menu Path: Network Service > DHCP Server - General

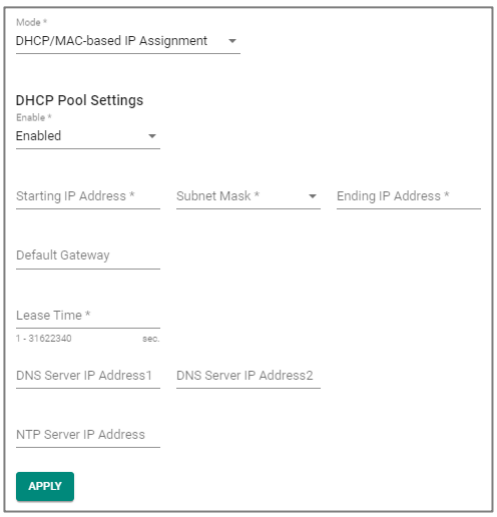
This page lets you configure the DHCP server mode and port settings.

Limitations

You can create up to 256 DHCP/MAC-based IP assignments.

DHCP Server Settings - DHCP/MAC-based IP Assignment

If **Mode** is set to **DHCP/MAC-based IP Assignment**, and **DHCP Pool Settings** is **Enabled**, these settings will appear.

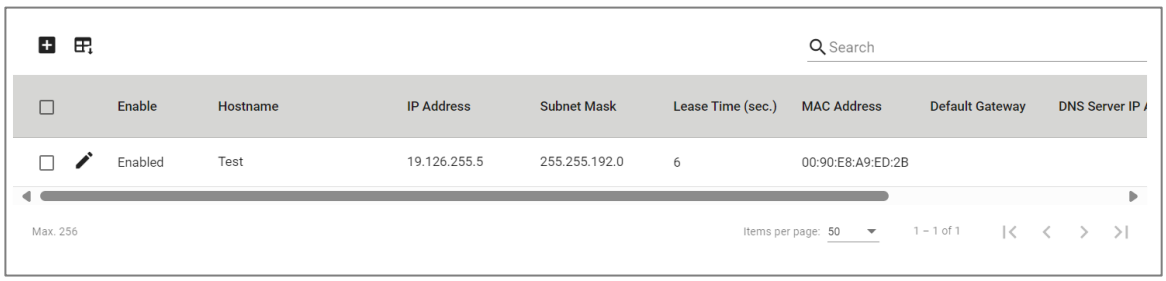


UI Setting	Description	Valid Range	Default Value
Mode	Select a DHCP server mode.	Disabled / DHCP/MAC-based IP Assignment / Port-based IP Assignment	Disabled

UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable use of a DHCP pool.	Enabled / Disabled	Disabled
Starting IP Address	Specify the starting IP address of the DHCP IP pool.	Valid unicast IP address	N/A
Subnet Mask	Specify the subnet mask for DHCP clients in the pool.	Valid subnet mask	N/A
Ending IP Address	Specify the ending IP address of the DHCP IP pool.	Valid unicast IP address	N/A
Default Gateway	Specify the default gateway to use for DHCP clients in the pool.	Valid IP address	N/A
Lease Time	Specify how long in seconds a device can keep the assigned IP address before it needs to renew the lease with the DHCP server.	1 to 31622340	N/A
DNS Server IP Address1	Specify the IP address of the first DNS server to use for DHCP clients in the pool.	Valid IP address	N/A
DNS Server IP Address2	Specify the IP address of the second DNS server to use for DHCP clients in the pool.	Valid IP address	N/A
NTP Server IP Address	Specify the IP address of the NTP server to use for DHCP clients in the pool.	Valid IP address	N/A

DHCP Server List - DHCP/MAC-based Assignment

If **DHCP Server Mode** is set to **DHCP/MAC-based IP Assignment**, this table will appear.



UI Setting	Description
Enable	Shows whether MAC-based IP assignment is enabled for the MAC address.

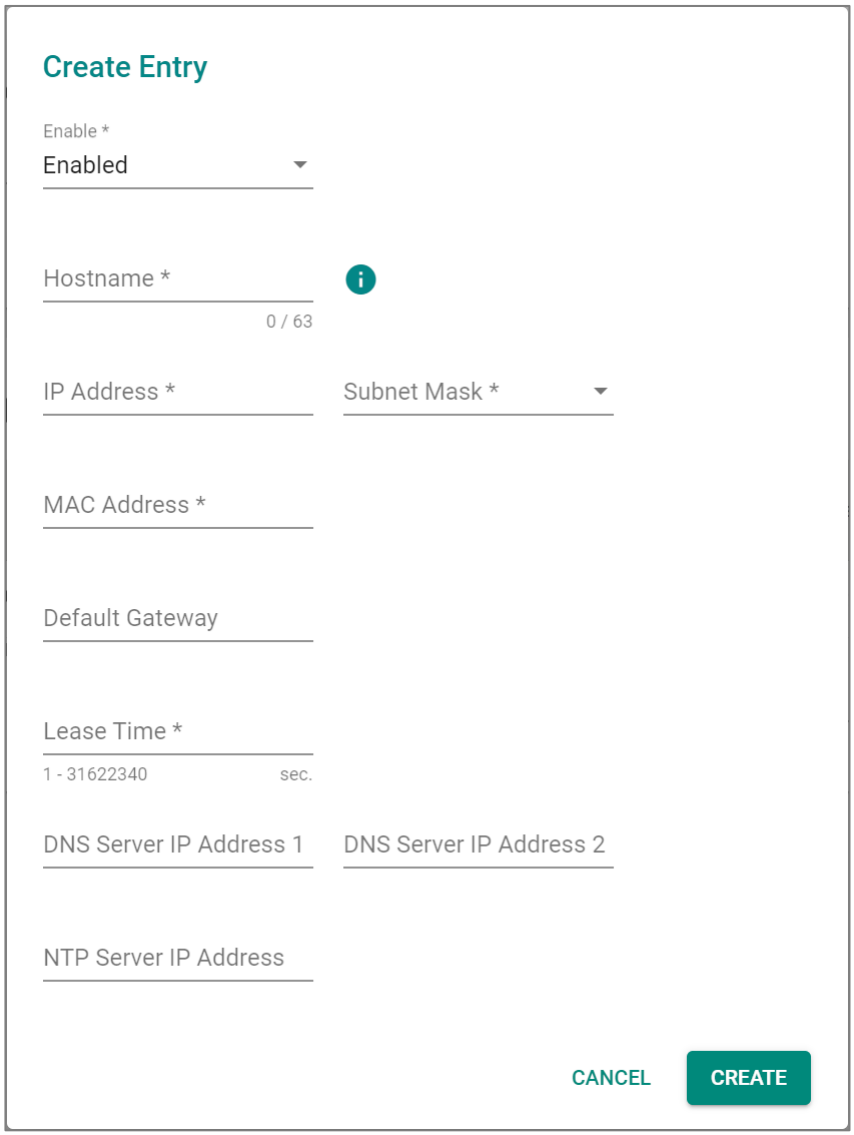
UI Setting	Description
Hostname	Shows the hostname to use for clients that connect to the MAC address.
IP Address	Shows the IP address assigned to clients that connect to the MAC address.
Subnet Mask	Shows the subnet mask assigned to clients that connect to the MAC address.
Lease Time (sec.)	Shows the lease time in seconds for IP assignments through the MAC address.
MAC Address	Shows the MAC address of the MAC-based IP assignment.
Default Gateway	Shows the default gateway for clients that connect to the MAC address.
DNS Server IP Address 1	Shows the IP address of the first DNS server to use for clients that connect to the MAC address.
DNS Server IP Address 2	Shows the IP address of the second DNS server to use for clients that connect to the MAC address.
NTP Server IP Address	Shows the NTP server to use for clients that connect to the MAC address.

MAC-based IP Assignment - Creating a DHCP Server Entry

Menu Path: Network Service > DHCP Server - General

Clicking **Create** on the **Network Service > DHCP Server - General** page when **Mode** is set to **DHCP/MAC-based IP Assignment** will open this dialog box. This dialog lets you create a new entry.

Click **Create** to save your changes and add the new entry.

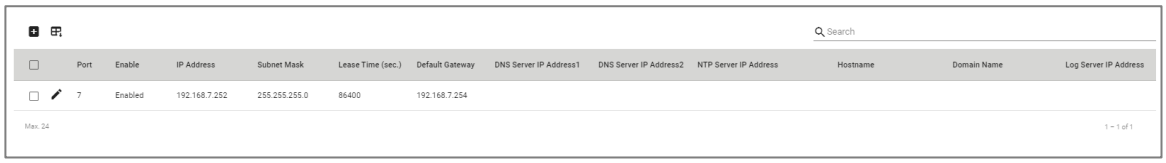


UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable the MAC-based IP assignment entry.	Enabled / Disabled	Enabled
Hostname	Specify a hostname for the IP assignment.	Drop-down list of ports	N/A
IP Address	Specify the IP address for the IP assignment.	Valid IP address	N/A
Subnet Mask	Select the subnet mask for the IP assignment.	Drop-down list of subnet masks	N/A
MAC Address	Specify the MAC address that this IP assignment will apply to.	Valid MAC address	

UI Setting	Description	Valid Range	Default Value
Default Gateway	Specify the default gateway for the IP assignment.	Valid IP address	N/A
Lease Time	Specify the lease time in seconds for the IP assignment.	1 to 31622340	
DNS Server IP Address1	Specify the IP address of the first DNS server to use for the IP assignment.	Valid IP address	N/A
DNS Server IP Address2	Specify the IP address of the second DNS server to use for the IP assignment.	Valid IP address	N/A
NTP Server IP Address	Specify the NTP server to use for the IP assignment.	Valid IP address	N/A

DHCP Server List - Port-based Assignment

If **DHCP Server Mode** is set to **Port-based IP Assignment**, this table will appear.



UI Setting	Description
Port	Shows the port number the entry is for.
Enable	Shows whether port-based IP assignment is enabled for the port.
IP Address	Shows the IP address assigned to clients that connect to the port.
Subnet Mask	Shows the subnet mask assigned to clients that connect to the port.
Lease Time (sec.)	Shows the lease time in seconds for IP assignments through the port.
Default Gateway	Shows the default gateway for clients that connect to the port.
DNS Server IP Address 1	Shows the IP address of the first DNS server to use for clients that connect to the port.
DNS Server IP Address 2	Shows the IP address of the second DNS server to use for clients that connect to the port.

UI Setting	Description
NTP Server IP Address	Shows the NTP server to use for clients that connect to the port.
Hostname	Shows the hostname to use for clients that connect to the port.
Domain Name	Shows the domain name to use for clients that connect to the port.
Log Server IP Address	Shows the IP address of the log server to use for clients that connect to the port.

Port-based Assignment - Creating a DHCP Server Entry

Menu Path: Network Service > DHCP Server - General

Clicking **Create** on the **Network Service > DHCP Server - General** page when **Mode** is set to **Port-based IP Assignment** will open this dialog box. This dialog lets you create a new entry.

Click **Create** to save your changes and add the new entry.

UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable the port-based IP assignment entry.	Enabled / Disabled	Enabled

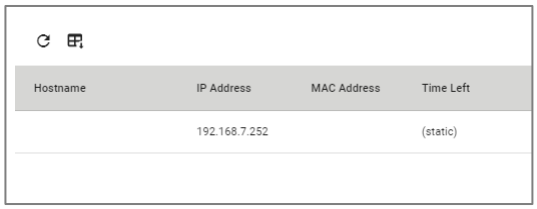
UI Setting	Description	Valid Range	Default Value
Port	Select which port the DHCP server will assign an IP address for.	Drop-down list of ports	N/A
IP Address	Specify the IP address assigned to clients that connect to the port.	Valid IP address	N/A
Subnet Mask	Select the subnet mask assigned to clients that connect to the port.	Drop-down list of subnet masks	N/A
Lease Time	Specify the lease time in seconds for IP assignments through the port.	1 to 31622340	N/A
Default Gateway	Specify the default gateway for clients that connect to the port.	Valid IP address	N/A
DNS Server IP Address1	Specify the IP address of the first DNS server to use for clients that connect to the port.	Valid IP address	N/A
DNS Server IP Address2	Specify the IP address of the second DNS server to use for clients that connect to the port.	Valid IP address	N/A
NTP Server IP Address	Specify the NTP server to use for clients that connect to the port.	Valid IP address	N/A
Hostname	Specify the hostname to use for clients that connect to the port.	Up to 63 characters	N/A
Domain Name	Specify the domain name to use for clients that connect to the port.	Up to 63 characters	N/A
Log Server IP Address	Specify the IP address of the log server to use for clients that connect to the port.	Valid IP address	N/A

Lease Table

Menu Path: Network Service > DHCP Server - Lease Table

This page lets you view the IP address lease table.

Lease Table



UI Setting	Description
Hostname	Shows the hostname of the client.
IP Address	Shows the IP address leased to the client.
MAC Address	Shows the MAC address of the client.
Time left	Shows the amount of time left in seconds on the DHCP lease for the client. **(static)** means the IP address is statically assigned.

Classless Static Route Table

Menu Path: Network Service > DHCP Server - Classless Static Route Table

This page lets you view the classless static route table and configure related settings.

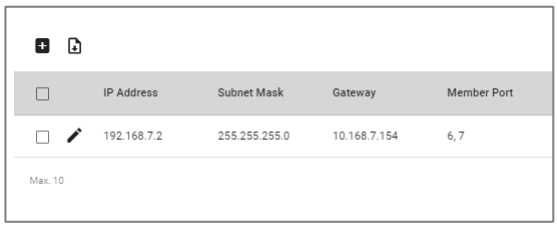
Limitations

You can create up to 10 classless static routes.

Classless Static Route Table Settings

UI Setting	Description	Valid Range	Default Value
Mode	Select the mode to use for classless static routing.	Disabled / Port-based IP Assignment	Disabled
Default Gateway **(If Mode is Port-based IP Assignment)**	Enable or disable use of a default gateway for classless static routes. When enabled, routes will use the default gateway address for the relevant port defined in the **General** tab.	Enabled / Disabled	Disabled

Classless Static Route Table



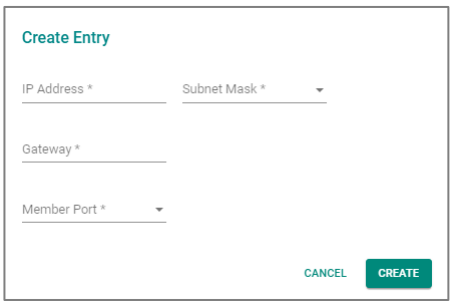
UI Setting	Description
IP Address	Shows the IP address of the packet's final destination for the route.
Subnet Mask	Shows the subnet mask of the destination address for the route.
Gateway	Shows the next hop or the neighboring device's IP address to which the packet is forwarded for the route.
Member Port	Shows the member ports that are using the route.

Creating a Classless Static Route Entry

Menu Path: Network Service > DHCP Server - Classless Static Route Table

Clicking **Create** on the **Network Service > DHCP Server - Classless Static Route Table** page when **Mode** is set to **Port-based IP Assignment** will open this dialog box. This dialog lets you create a new entry.

Click **Create** to save your changes and add the new entry.



UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address of the packet's final destination.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask of the destination address.	Drop-down list of subnet masks	N/A
Gateway	Specify the next hop or the neighboring device's IP address to which the packet is forwarded.	Valid Gateway	N/A
Member Port	Specify the ports that are using the port-based IP assignment.	Drop-down list of ports	N/A

Configuring DHCP Relay Agent

DHCP Relays can help reduce broadcast DHCP requests by relaying DHCP requests between networks.

Note

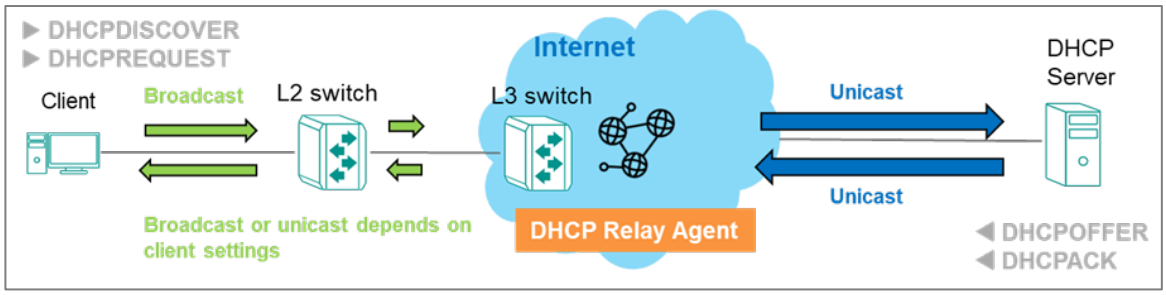
This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

About DHCP Relay Agents

DHCP relay agents can provide a bridge for DHCP communication across network segments.

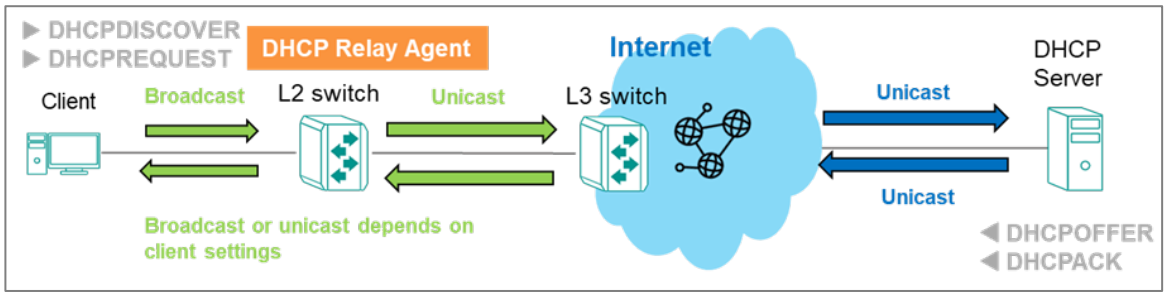
DHCP Relays on L3 Switches

A DHCP Relay Agent on an L3 switch converts broadcast DHCP packets to unicast packets, and then routes them to the DHCP server.



DHCP Relays on L2 Switches

On an L2 switch, the switch would convert DHCP broadcast packets to DHCP unicast packets, forward them to an L3 switch, which would then route them the DHCP server.



Configuring DHCP Relay Agent

You can configure your switch to serve as a DHCP relay agent.

1. Sign in to the device using administrator credentials.
2. Go to **Network Service** > **DHCP Relay Agent** > **General**.
3. Under **DHCP Relay Agent**, choose **Enabled** from the drop-down menu.
4. Specify up to 4 addresses in the **DHCP Server Address** field, and then click **Apply** to save changes.

Note

If DHCP Server Address is left blank, DHCP servers will be unable to reply to packets sent from connected clients.

5. To configure a **Port**, click the corresponding **[Edit]** button.

The **Edit Port** screen appears.

6. Specify all of the following:

Option	Value
Relay	To enable the relay, choose **Enabled**. To disable the relay while retaining settings, choose **Disabled**.
Status	To accept incoming DHCP packets from DHCP servers, choose **Trusted** from the drop-down menu.

7. Click **Apply** to save your changes.

Note

You can copy your settings to other ports by selecting them from the drop-down menu.

Configuring Option 82

Option 82 provides additional information in relayed packets that can make DHCP server address allocation more effective. If your DHCP server supports it, it can provide additional information that can facilitate context-aware address allocation, as well as more flexible tracking and management.

To configure Option 82:

1. Sign in to the device using administrator credentials.
2. Go to **Network Service** > **DHCP Relay Agent** > **General**, and then click **Option 82**.
3. Specify the ID that will be sent to the relay by clicking **Remote ID Type**, and then choosing an option from the drop-down menu.

For the **Other** option, you can specify a static value of up to 64 characters.

4. To enable **Option 82** on a given **Port**, click **[Edit]** next to the corresponding **Port**.

> **Note**
> The Edit Port screen appears.

5. Click **Option 82** and choose **Enable** from the drop-down menu.
6. Click **Apply** to save your settings.

DHCP Relay Agent

Menu Path: Network Service > DHCP Relay Agent

This page lets you manage the DHCP Relay Agent feature of your device.

This page includes these tabs:

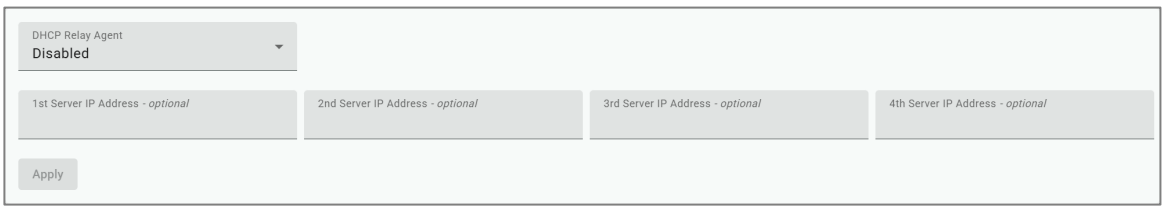
- General
- Option 82

DHCP Relay Agent - General

Menu Path: Network Service > DHCP Relay Agent - General

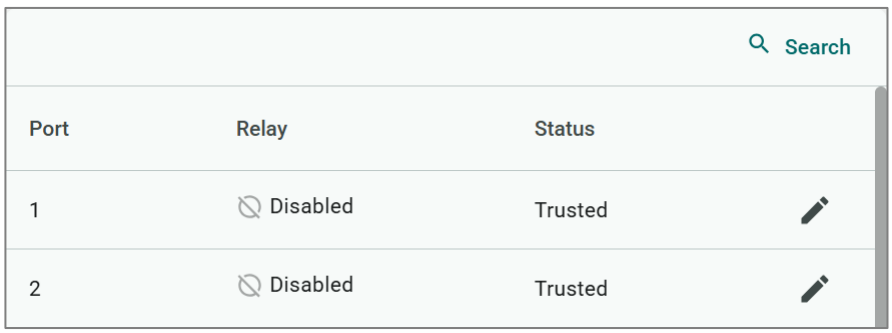
This page lets you enable the DHCP Relay Agent feature and configure its related settings.

DHCP Relay Agent Settings



UI Setting	Description	Valid Range	Default Value
DHCP Relay Agent	Enable or disable the DHCP Relay Agent feature on your device.	Enabled / Disabled	Disabled
1st/2nd/3rd/4th Server IP Address	Specify the 1st, 2nd, 3rd, and 4th server IP address.	Valid IP address	N/A

DHCP Relay Agent - Port List



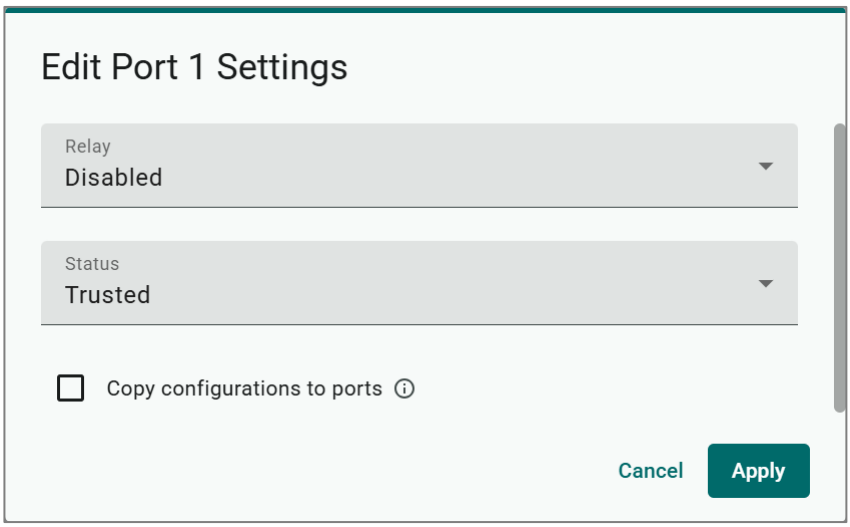
UI Setting	Description
Port	Shows the port number the entry is for.
Relay	Shows whether the relay function is enabled for the port.
Status	Shows the status of the relay on the port.

DHCP Relay Agent - Edit Port Settings

Menu Path: Network Service > DHCP Relay Agent - General

Clicking the **Edit (✎)** icon for a port on the **Network Service > DHCP Relay Agent - General** page will open this dialog box. This dialog lets you manage DHCP relay settings for the port.

Click **Apply** to save your changes.



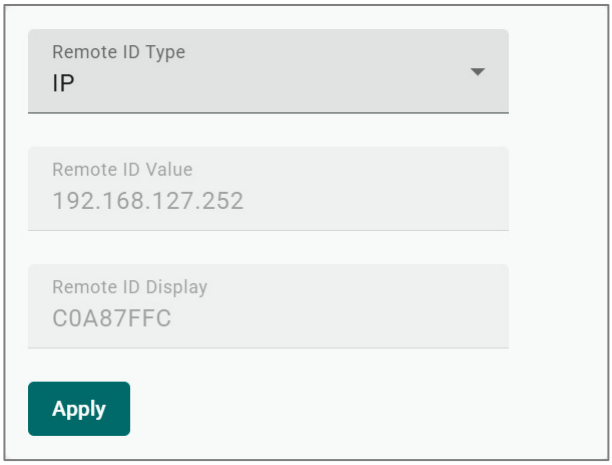
UI Setting	Description	Valid Range	Default Value
Relay	Enable or disable the relay function for the port.	Enabled / Disabled	Disabled
Status	Specify the relay status for the port. • **Trusted**: DHCP packets with Option 82 or with a non-zero gateway IP address (GIADDR) will be accepted. • **Untrusted**: DHCP packets with Option 82 or with a non-zero gateway IP address (GIADDR) will be discarded.	Trusted / Untrusted	Trusted
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

Option 82

Menu Path: Network Service > DHCP Relay Agent - Option 82

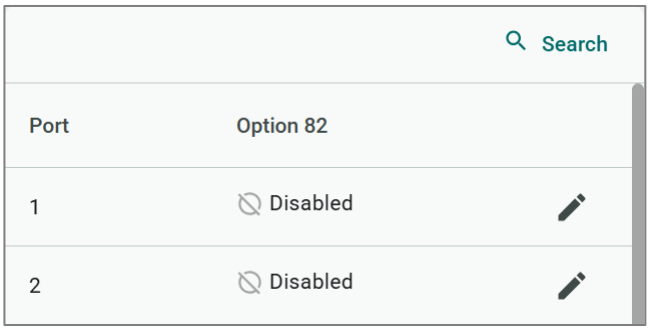
This page lets you manage Option 82 and its related settings.

Option 82 Settings



UI Setting	Description	Valid Range	Default Value
Remote ID Type	Specify the remote ID type.	IP / MAC / Client ID / Other	IP
Remote ID Value	If the **Remote ID Type** is **Other**, specify the remote ID value to use. For all other types, this shows the remote ID value for the selected remote ID type and cannot be edited.	Other: 1 to 64 characters All other settings: N/A	IP: • For L2 devices: Device system IP • For L3 devices: First IP in the system MAC: MAC address of the device Client ID: moxa Other: moxa-dhcp-relay
Remote ID Display	Shows the remote ID generated from the Remote ID Value. This field is read-only and cannot be changed.	N/A	N/A

Option 82 - Port List



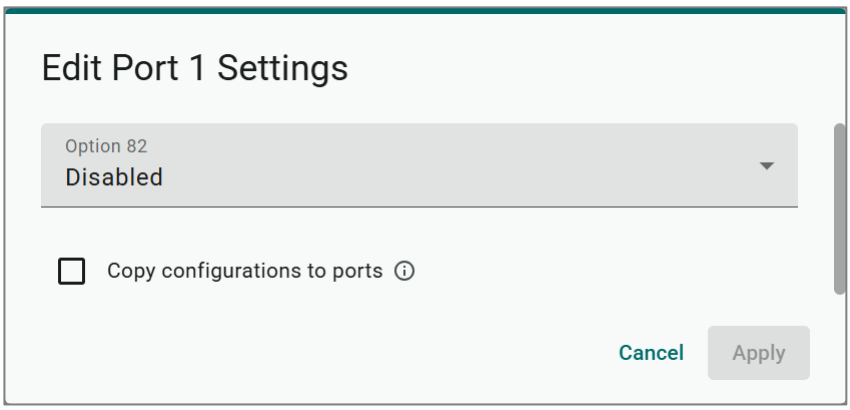
UI Setting	Description
Port	Shows the port number the entry is for.
Option 82	Shows whether Option 82 is enabled for the port.

Option 82 - Edit Port Settings

Menu Path: Network Service > DHCP Relay Agent - Option 82

Clicking the **Edit (✎)** icon for a port on the **Network Service > DHCP Relay Agent - Option 82** page will open this dialog box. This dialog lets you enable or disable Option 82 for the port.

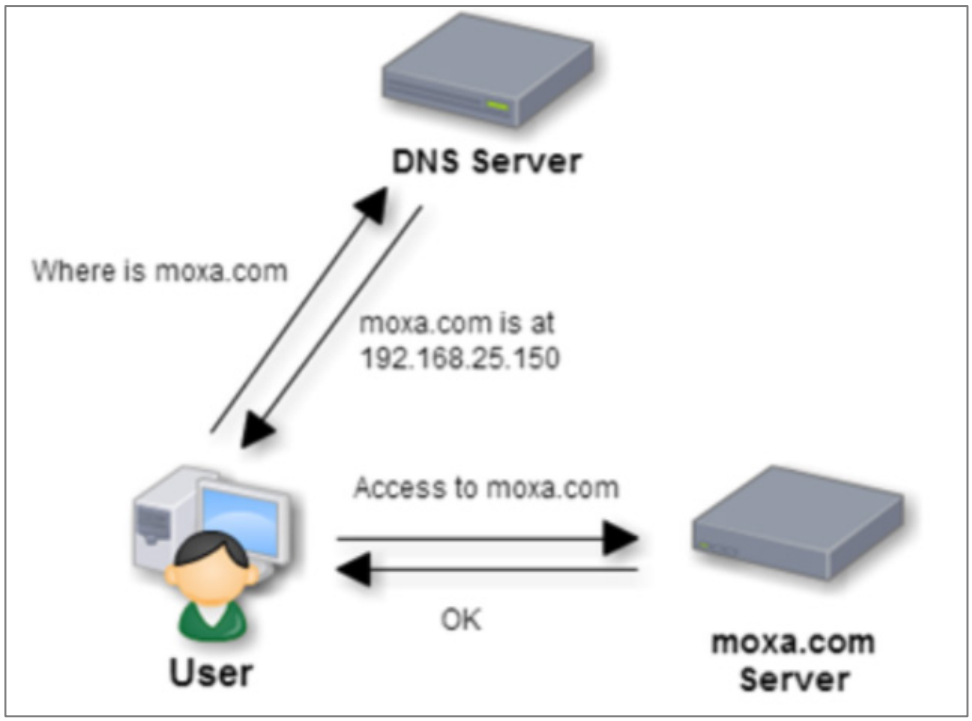
Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Option 82	Enable or disable Option 82 for the port.	Enabled / Disabled	Disabled
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

About DNS Server

DNS (Domain Name System) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network.It translates domain names, which are human-readable identifiers for resources, into IP addresses, which are numerical identifiers used to locate and communicate with these resources. For example, http://www.moxa.com is easier to remember than http://92.115.213.11.



While the DNS lookup translates domain names to IP addresses, **DNS Reverse Lookup** performs the opposite. It is a feature that allows the switch to identify the hostname (device name) associated with a known IP address on the network. Imagine you have an IP address on your network, like 192.168.1.100, but you don't know the corresponding

device name (hostname). This is where DNS Reverse Lookup comes in. By querying a DNS server configured for reverse lookups, you can retrieve the hostname associated with that IP address. For instance, a reverse lookup for 192.168.1.100 might reveal the hostname "printer-server". This helps with network manageability by making it easier to recognize devices by their names instead of just IP addresses.

Components of DNS

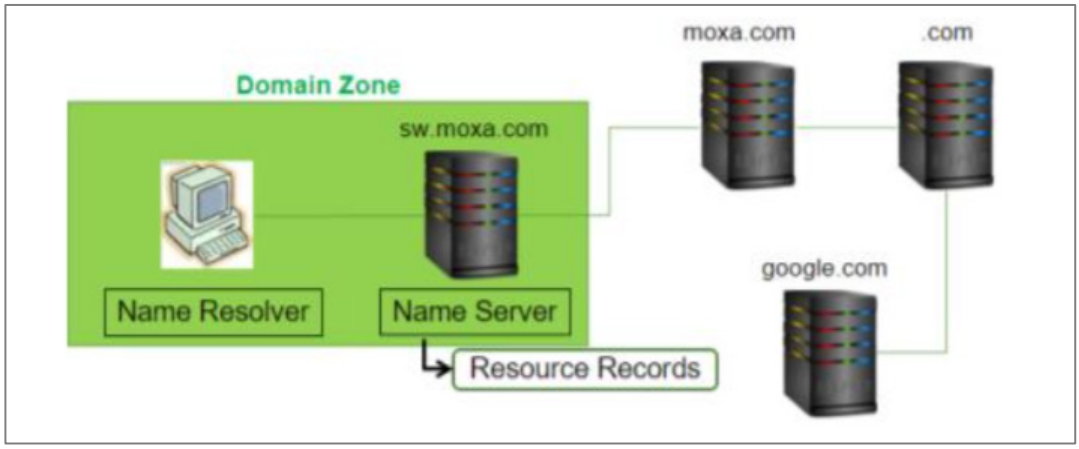
DNS has three major components:

1. **Domain Name Space and Resource Records:** A resource record is basically a single mapping between a resource and a name. These can map a domain name to an IP address; define the name servers for the domain, etc.
2. **Name Servers:** A name server is a device designated to translate domain names into IP addresses. These servers do most of the work in the DNS system. Since the total number of domain translations is too much for any one server, each server may redirect request to other name servers or delegate responsibility for a subset of sub-domains they are responsible for.
3. **Resolvers:** Programs that extract information from name servers in response to client requests

For a Moxa "DNS Server" device feature, we will focus on the name server, the following section will further describe the name server and how it works.

Name Servers in Depth

Name servers are the repositories of information that make up the domain database. The database is divided up into sections called **zones**, which are distributed among the name servers. While name servers can have several optional functions and sources of data, the essential task of a name server is to answer queries using data in its zones. As earlier mentioned, the database in name server is divided up into sections called zones. Each zone will be described by many different types of resource records (RRs). The DNS specifies a set of various types of resource records, which are the basic information elements of the domain name system.

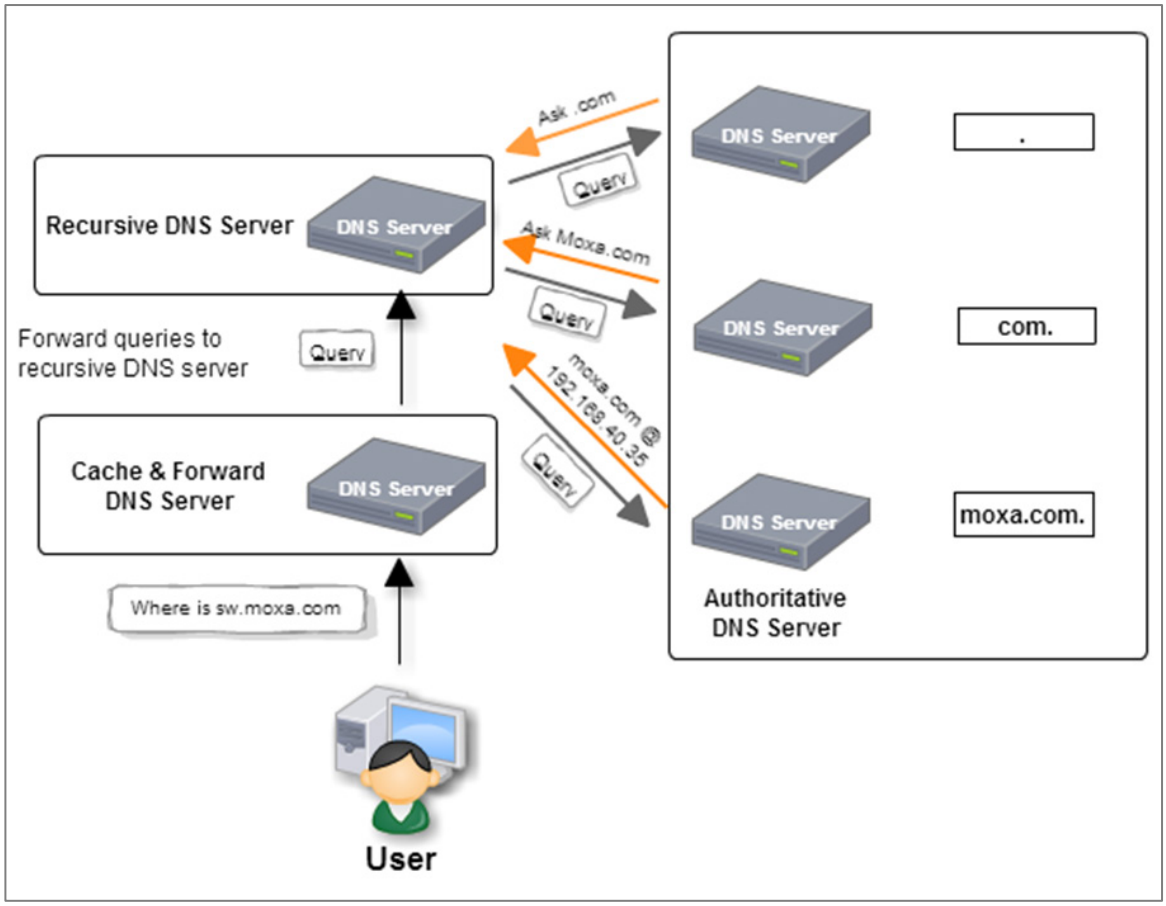


A domain name identifies a node. Each node has a set of resource information, which may be empty. The set of resource information associated with a particular name is composed of separate RRs. The order of RRs in a set is not significant, and need not be preserved by name servers, resolvers, or other parts of the DNS. The basic RR formats are defined in RFC 1034.

There are three types of name servers:

- **Authoritative Name Server:** Authoritative name servers are assigned to be responsible for their supported domains, returns answers only to queries about domain names that have been specifically configured by the administrator. An authoritative name server can either be a master server or a slave server. A master server is a server that stores the original (master) copies of all zone records. A slave server uses an automatic updating mechanism of the DNS protocol in communication with its master to maintain an identical copy of the master records. The zone records can be distributed to all authoritative name servers in the same zone by many ways, the preferred method is the zone transfer of the DNS protocol.
- **Caching & Forwarding Name Server:** Caching & forwarding name server forwards queries to other authoritative or recursive name server when user queries a domain which is out of the authority of this name server. It caches the response from other DNS server to improve the efficiency of the DNS by reducing DNS traffic across the Internet, and by reducing load on authoritative name-servers, particularly root name-servers.
- **Recursive Name Server:** If the DNS queries cannot reply from either the authoritative or caching DNS information in name servers, queries might be

forward to recursive DNS server. Recursive DNS server queries the root DNS server from the TLD of the domain you are trying to reach. The root DNS servers then send the information about the authoritative DNS server back to recursive server. The operation will repeat many times if needed, until the queried domain name is found.



How the Root DNS Server Knows the Location of the ".com" DNS Server

In the Domain Name System (DNS), each domain is managed by its parent domain. For instance, the ".com" domain is delegated by the root DNS server, represented as ".". When ".com" is delegated, the root DNS server adds ".com" as an authoritative server in its database. This ensures that when a query for a ".com" domain is received, the root DNS server can direct it to the appropriate ".com" authoritative DNS server.

Delegation Process

- **Parent to Child Delegation:** The root DNS server must have up-to-date records of which DNS servers are authoritative for each sub-domain. Whenever new DNS servers are added to a child domain like ".com," they must be registered with the parent domain (in this case, the root DNS server).
- **Maintaining Delegation:** Keeping this delegation accurate and up-to-date manually can be challenging. It requires that any changes in the child domain's authoritative servers are promptly reflected in the parent domain's records.

A stub zone can be a useful tool in some scenarios. It helps automate the update process for the authoritative zone data, ensuring that the delegation information between parent and child domains remains current without requiring constant manual updates.

DNS Server for Layer 2 Switch in Railway Field

Generally, the DNS is the hierarchical and decentralized naming system used to identify computers reachable through the Internet or other Internet Protocol (IP) networks. The resource records contained in the DNS server in corresponding zone can provide necessary information for DNS queries.

In railway field, the DNS is a nonhierarchical and centralized naming system, and the L2 switch DNS server acts as a local authoritative DNS server. It contains a statically configured database of IP addresses and their associated hostnames, and it translates the FQDN to an IP address for DNS clients. The IP address could be either a multicast IP (may represents a service) or a unicast IP (device IP address). For example, it can translate ""ext.door.consist" to "225.1.32.170", and "ext.door.train1" to "10.1.34.170".

Obviously, it is much simpler to remember a word like "door1" instead of a series of numbers. With DNS server, customers will be much easier to manage IP address allocation during the process of the communication system construction.

Example: Configuring DNS Server for a Consist Door

In this procedure, we will create a Zone and a corresponding domain name, and then configure mapping between hostnames and IP addresses.

Zones allow you to create private analogues to top level domains. They allow you to reuse the same hostname without creating conflicts, for example:

- Zone 1 is named `moxa1`

- Zone 2 is named `moxa2`

Let's further suppose that you have one door on each consist in a train setup:

- `consist1.door` in Zone 1 `moxa1` with an IP address of `192.168.1.10`
- `consist1.door` in Zone 2 `moxa2` with an IP address of `192.168.2.10`

The resulting mapping will be

- `consist1.door.moxa1` resolves to `192.168.1.10`
- `consist1.door.moxa1` resolves to `192.168.2.10`

To configure the device as a DNS server, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Network Service** > **DNS Server** and then click **Global**.
3. Under **DNS Server**, choose **Enabled** from the dropdown menu, and then click **Apply**.
4. Create a Zone by clicking the **Settings** settings tab, and then under Zone Table, click ***[Create]***.

   The Create a Zone screen appears.
5. Under **Index**, specify a Zone from the list. Type a **Domain Name** for the domain you choose, and then click **Create**.

> **Note**
> Each Zone must have a unique domain name.

   This Zone will mapped to the domain name, and **DNS Table for –** will be updated with the Zone index you selected, such as **DNS Table for ZONE-1**. If multiple zones have been created, you can choose the correct zone by choosing from the drop-down menu.
6. To create a DNS host entry: First, add a new zone to configure the hostname-to-IP address mappings. Next, under the DNS Table for ZONE, click ***[Create]***.

   The **Create Resource Record for ZONE** screen appears.
7. Specify the **Hostname** and corresponding **IP Address**, and then click **Create**.

   If we specify a **Hostname** of `consist1.door` and an IP of **192.168.1.10.**

   The record appears in the DNS Table.

DNS Server

Menu Path: Network Service > DNS Server

This page lets you configure the DNS server settings.

This page includes these tabs:

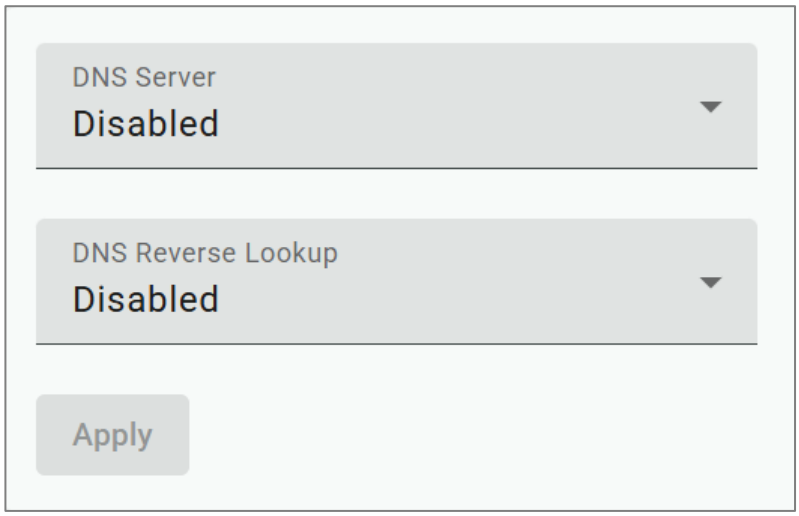
- Global
- Settings
- Status

DNS Server - Global

Menu Path: Network Service > DNS Server - Global

This page lets you configure the DNS server settings for your device.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
DNS Server	Enable or disable the DNS server for your device.	Enabled / Disabled	Disabled
DNS Reverse Lookup	Enable or disable DNS reverse lookup for your device. DNS reverse lookup allows the switch to identify the hostname (device name) associated with a known IP address on the network.	Enabled / Disabled	Disabled

DNS Server - Settings

Menu Path: Network Service > DNS Server - Settings

This page lets you configure the DNS server zone settings.

Limitations

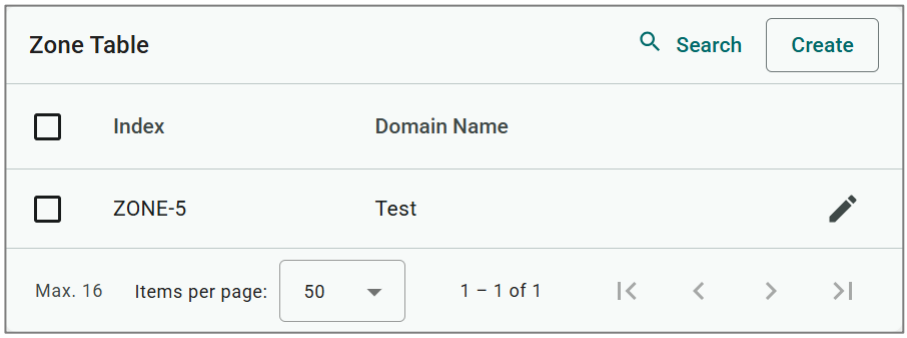
You can create up to 16 DNS zones.

Limitations

You can create up to 256 resource records for each zone.

Zone Table

Zones provide a structured way to manage and organize DNS records for a domain. They allow administrators to group related records together and apply consistent configurations across the domain.



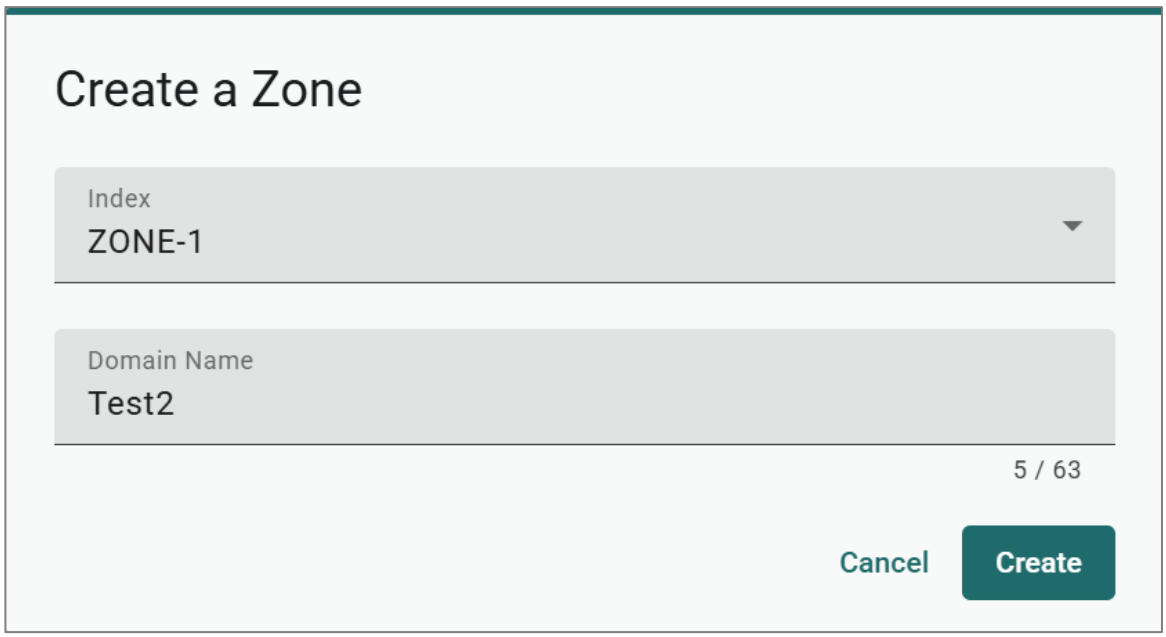
UI Setting	Description
Index	Shows the zone the entry is for.
Domain Name	Shows the domain name of the zone.

Create a Zone

Menu Path: Network Service > DNS Server - Settings

Clicking the **Create** button in **Zone Table** on the **Network Service > DNS Server - Settings** page will open this dialog box. This dialog lets you create a zone for the DNS server.

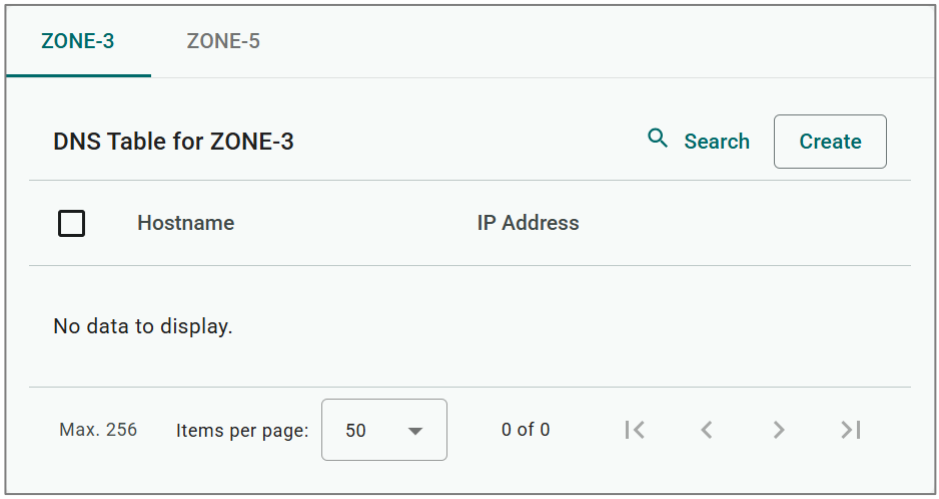
Click **Create** to save your changes and add the new zone.



UI Setting	Description	Valid Range	Default Value
Index	Select a zone to create.	Drop-down list of zones	N/A
Domain Name	Specify a domain name for the zone.	Up to 63 characters, only a-z, A-Z, 0-9 or . - are allowed	N/A

DNS Table

Select a zone name to view that zone's DNS table.



UI Setting	Description
Hostname	Shows the hostname of the resource record.
IP Address	Shows the IP address of the resource record.

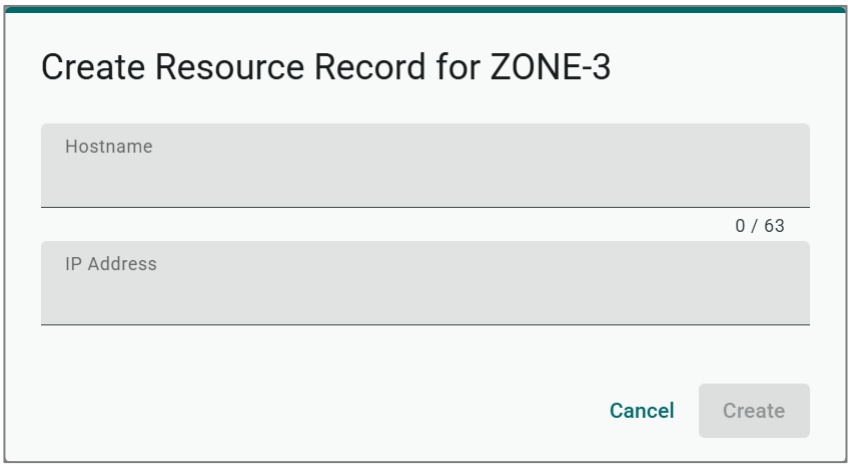
Create a Resource Record

Menu Path: Network Service > DNS Server - Settings

Clicking the **Create** button in a DNS table on the **Network Service > DNS Server - Settings** page will open this dialog box. This dialog lets you create a resource record for the displayed zone.

Click **Create** to save your changes and add the resource record for the displayed zone.

> **Note**
> Resource records cannot be created for a zone until the corresponding zone has been created.



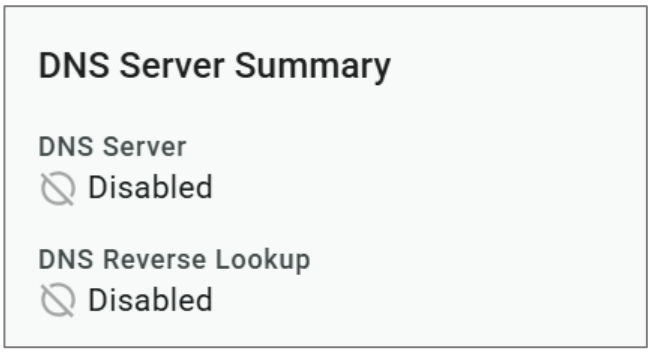
UI Setting	Description	Valid Range	Default Value
Hostname	Specify the hostname for the resource record.	1 to 63 characters, only a-z, A-Z, 0-9 or . - are allowed	N/A
IP Address	Specify the IP address for the resource record.	Valid IP address	N/A

DNS Server - Status

Menu Path: Network Service > DNS Server - Status

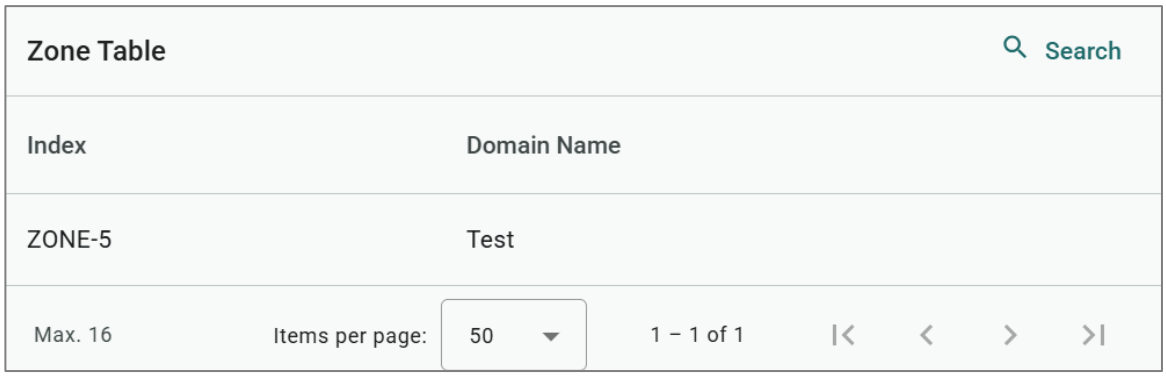
This page lets you see the DNS server's overall status.

DNS Server Summary



UI Setting	Description
DNS Server	Shows whether the DNS server is enabled for the device.
DNS Reverse Lookup	Shows whether DNS reverse lookup is enabled for the device

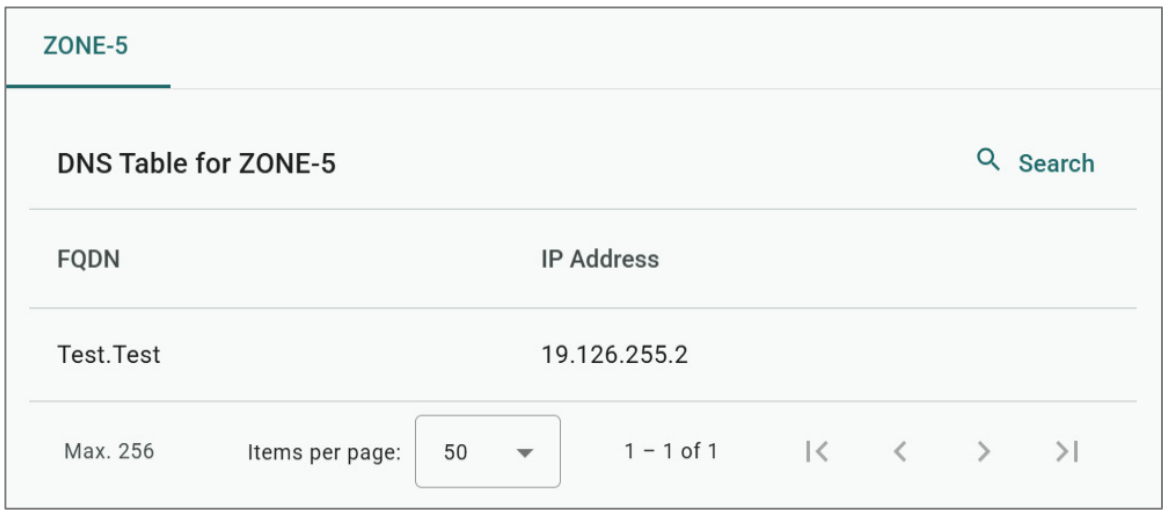
Status - Zone Table



UI Setting	Description
Index	Shows the zone the entry is for.
Domain Name	Shows the domain name of the zone.

Status - DNS Table

Select a zone name to view that zone's DNS table.



UI Setting	Description
FQDN	Shows the fully qualified domain name (FQDN) of the resource record in the format "`Hostname.Domain Name`". For example, if the hostname is "`door1`" and the domain name for the zone is "`train1`", the FQDN will be "`door1.train1`".
IP Address	Shows the IP address of the resource record.

About mDNS Responder

The **mDNS responder** allows a device to announce its presence and available services on a local network using **Multicast DNS (mDNS)** and **DNS-Based Service Discovery (DNS-SD)** protocols. This enables users to easily discover Moxa devices, as the devices will respond to mDNS queries with a `_moxa._tcp` service advertisement. This automates device discovery on local networks.

- **Multicast DNS (mDNS)**: This protocol provides DNS-like capabilities on a local link, even without a conventional Unicast DNS server. Devices use link-local Multicast DNS hostnames, typically in the format "hostname.local," within local networks. This reduces reliance on global DNS namespaces like ".com."
- **DNS-Based Service Discovery (DNS-SD)**: Given a specific service type and a domain, this mechanism enables clients to discover a list of named instances for that service using standard DNS queries.

This feature can be **applied to ITxPT services**. The TN-4500B Series is **ITxPT certified** and supports the **"Module Inventory Service"** specification (defined in ITxPT S02P01). The primary goal of the Module Inventory Service is to automatically inventory modules installed on a vehicle. When a DNS Module Inventory query is received, the device provides a corresponding DNS reply containing inventory data as defined by the specification.

About ITxPT

ITxPT is a collaborative agreement among various public transport stakeholders aimed at enabling the digitalization and integration of mobility services. It provides a framework for designing hardware and software, allowing modules to be integrated into a coherent

architecture. This simplifies market access for IT suppliers and offers purchasers the flexibility to select services and components from diverse providers.

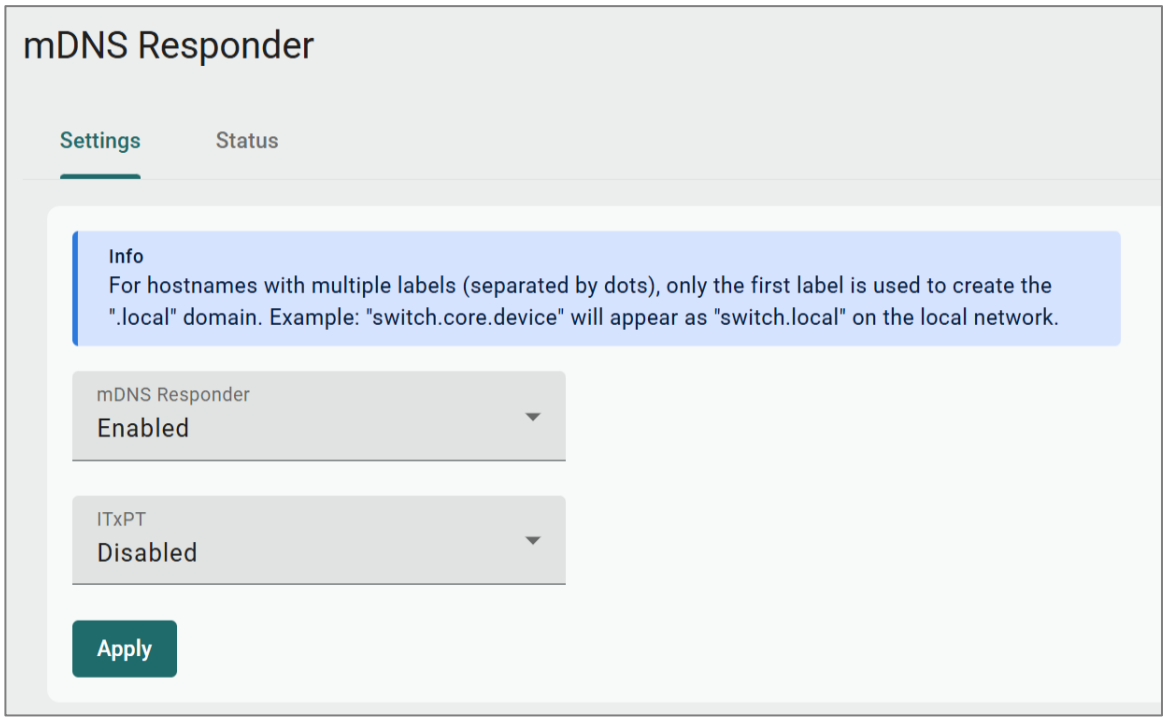
mDNS Responder - Settings

Menu Path: Network Service > mDNS Responder - Settings

This page lets you configure the mDNS Responder feature for your device.

Click **Apply** to save your changes.

mDNS Responder Settings



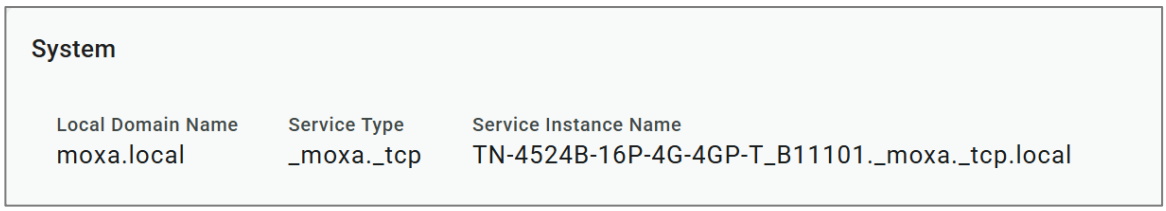
Note: current UI's parameter name is wrong, i'll update the correct one once ready

UI Setting	Description	Valid Range	Default Value
mDNS Responder	Enable/disable the mDNS feature. When mDNS Responder is enabled, device shall identify query by query's domain name include "_moxa._tcp".	Enabled / Disabled	Enabled
ITxPT Service	Enable/disable the ITxPT services. When ITxPT service is enabled, device shall identify 'Module Inventory Service' query by query's domain name include "_itxpt_socket._tcp".	Enabled / Disabled	Disabled

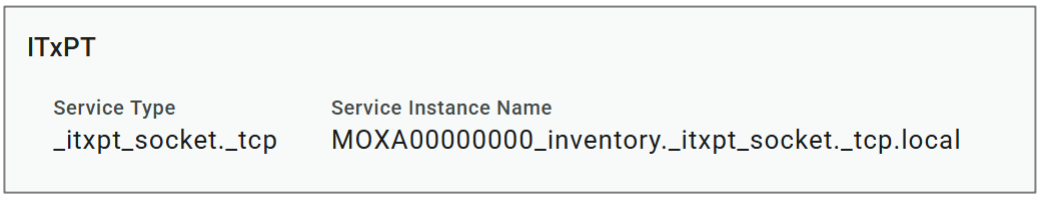
mDNS Responder - Status

Menu Path: Network Service > mDNS Responder - Status

This page lets you view the status and configuration of the device's ports.



UI Setting	Description
Local Domain Name	Shows the system local domain name derived from the device's hostname by appending the .local suffix. • If the hostname does not contain any dots, the System Local Domain Name shall be <hostname>.local. • If the hostname does contain one or more dots (e.g., `foo.bar`), only the first label (`foo`) shall be used. The resulting System Local Domain Name in this case shall be: foo.local.
Service Type	Shows the system service type.
Service Instance Name	Shows the service instance name. • *<Device's model name>_<Last 3 bytes of MAC>*._moxa._tcp.local



UI Setting	Description
Service Type	Shows the ITxPT service type.
Service Instance Name	Shows the ITxPT service instance name. The format follows RFC: • *<UniqueIdentifier>_<Name>._<Type>._<Protocol>.<Domain>*

Security

Menu Path: Security

This section lets you configure the security settings of your device.

This section includes these pages:

- Device Security
- Network Security
- Authentication

Security - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to System > Account Management > User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Device Security			
Login Policy	R/W	R	R
Trusted Access	R/W	R	R
SSH & SSL	R/W	R/W	-
Network Security			
IEEE 802.1X	R/W	R/W	R
MAC Authentication Bypass	R/W	R/W	R
MACsec	R/W	R/W	R
Port Security	R/W	R/W	R
Traffic Storm Control	R/W	R/W	R
Access Control List	R/W	R/W	R

Settings	Admin	Supervisor	User
Network Loop Protection	R/W	R/W	R
Binding Database	R/W	R/W	R
DHCP Snooping	R/W	R/W	R
IP Source Guard	R/W	R/W	R
Dynamic ARP Inspection	R/W	R/W	R
Authentication			
Login Authentication	R/W	-	-
RADIUS	R/W	-	-
TACACS+	R/W	-	-

Device Security

Menu Path: Security > Device Security

This section lets you configure the device-level security settings of your device.

This section includes these pages:

- Login Policy
- Trusted Access
- SSH & SSL

About Login Policy

Login Policy lets you define and enforce login restrictions to improve the security of your device and protect it from unauthorized access from brute force attacks.

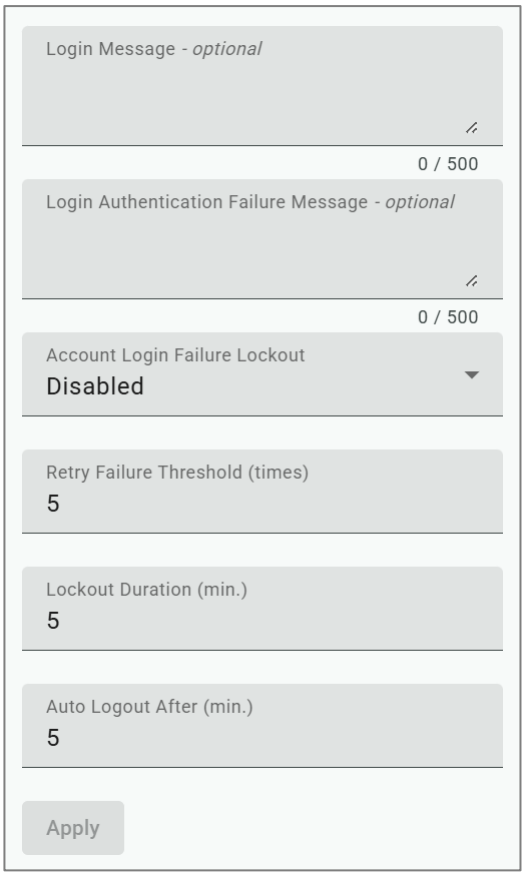
Login Policy

Menu Path: Security > Device Security > Login Policy

This page lets you configure the login policies for your device.

Click **Apply** to save your changes.

Login Policy Settings



UI Setting	Description	Valid Range	Default Value
Login Message	Specify the welcome message to display when users log in to the device.	0 to 500 characters	N/A

UI Setting	Description	Valid Range	Default Value
Login Authentication Failure Message	Specify the message to display if the user fails to log in. **⚠ Warning** The Login Authentication Failure Message should not include information about passwords or other sensitive information.	0 to 500 characters	N/A
Account Login Failure Lockout	Enable or disable the lockout function, which will temporarily prevent users from logging in for the **Lockout Duration** after the **Retry Failure Threshold** is exceeded. This can be useful for preventing brute force attacks.	Enabled / Disabled	Disabled
Retry Failure Threshold (times)	Specify the number of login retry attempts allowed before the user is locked out for the **Lockout Duration**.	1 to 10	5
Lockout Duration (min.)	Specify the lockout duration in minutes during which a locked-out user will be unable to log in.	1 to 10	5
Auto Logout After (min.)	Specify the amount of time in minutes a user can be idle before they will be automatically logged out from the device.	0 to 1440	5

About Trusted Access

Trusted Access is a feature that allows device management only from trusted IP addresses that you specify.

Trusted access is a crucial mechanism for maintaining the security and integrity of your network infrastructure. It ensures that only authorized devices can connect to sensitive network resources, reducing the risk of unauthorized access and potential security breaches.

Why Trusted Access Matters

- **Security:** By allowlisting IP addresses, administrators ensure that only devices with approved IP addresses can access the network configuration, helping to prevent unauthorized connections.
- **Access Control:** Trusted access enables administrators to define which IP addresses can connect to sensitive resources, ensuring that only trusted devices interact with critical areas of the network.

How Trusted Access Works

Enabling trusted access on a device involves configuring IP allowlists. Once an IP address is allowlisted, the device treats it as trusted, allowing access to device management functions. Devices not on the allowlist are denied access, helping to maintain a secure and controlled network environment.

Example: Configuring and Enabling Trusted Access

Enable trusted IP address settings to only allow users to access network device management features from IP addresses you choose. Only IPv4 addresses are supported.

Make sure you add all management devices to the allowlist before enabled Trusted Access, otherwise you may lose access to the management console.

To configure trusted access, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Security** > **Device Security** > **Trusted Access**, and then click ***[Create]***.

   The Create Entry screen appears.
3. Specify the **IP Address** and **Subnet Mask** of the device to add the device IP to the allowlist, and then click **Create**.

   The specified **IP Address** and **Netmask** appear on the Trusted Access list.
4. Once you have created entries for all devices, under **Trusted Access**, choose **Enabled**, and then click **Apply**.

   Trusted access will now be enabled, and only devices on the allowlist will be able to access management features.

Trusted Access

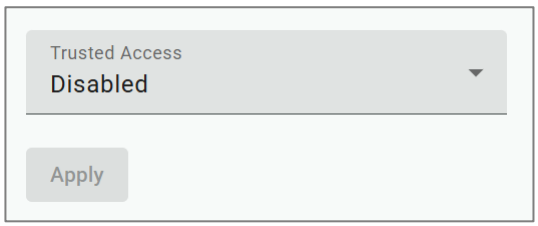
Menu Path: Security > Device Security > Trusted Access

This page lets you limit access to the device to trusted IP addresses you specify. You can also limit access to the device to LAN connections only.

Limitations

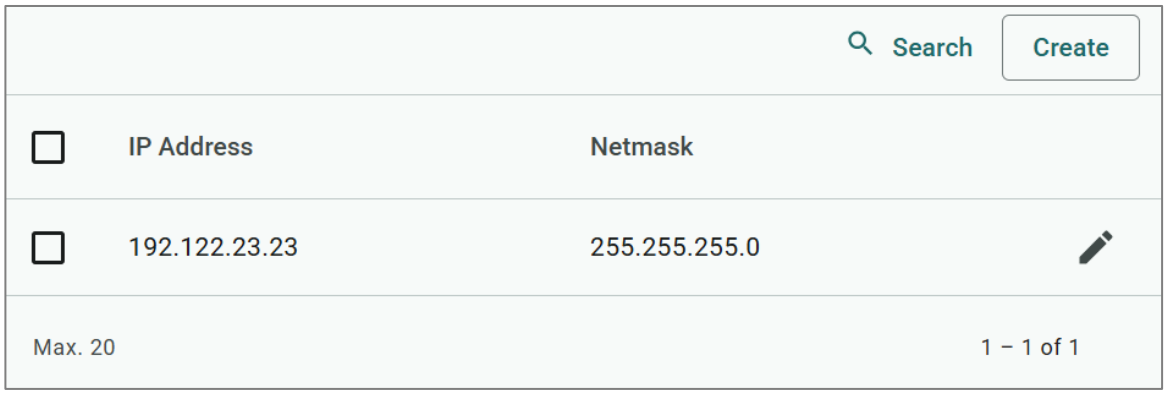
You can create up to 20 trusted IP entries.

Trusted Access Settings



UI Setting	Description	Valid Range	Default Value
Trusted Access	Enable or disable the Trusted IP List. **Enabled:** Only IP addresses in the Trusted IP List can access the device. **Disabled:** Any IP address can access the device. **Note** Trusted Access cannot be enabled if there are no entries in the Trusted Access List. **Warning** Depending on the features you enable, you may lose access to your device if the computer you are using to configure the device is not in the Trusted Access List or connected through a LAN connection.	Enabled / Disabled	Disabled

Trusted Access List



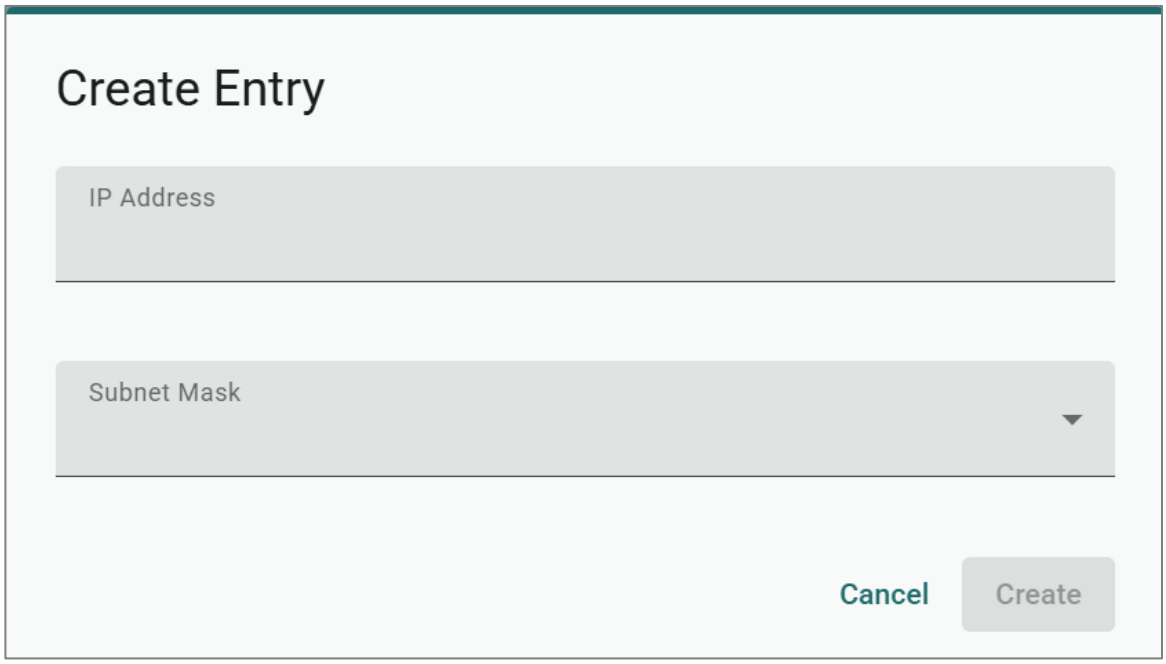
UI Setting	Description
IP Address	Shows the IP address of the Trusted IP entry.
Subnet Mask	Shows the netmask of the Trusted IP entry.

Trusted Access - Create Entry

Menu Path: Security > Device Security > Trusted Access

Clicking the **Create** button on the **Security > Device Security > Trusted Access** page will open this dialog box. This dialog lets you create a trusted IP entry.

Click **Create** to save your changes and add the new entry.



UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address of the trusted host(s).	Valid IP address	N/A
Subnet Mask	Select a netmask for the trusted host(s).	Drop-down list of subnet masks	N/A

About SSH & SSL

SSH and SSL are security protocols.

- **Secure Shell (SSH):** SSH is the recommended protocol for secure command-line access. This protocol encrypts the communication channel between a user and a device's management interface. This helps ensure that any data exchanged–like usernames, passwords, or configuration commands–remains hidden from eavesdroppers on the network.
- **Secure Sockets Layer (SSL):** While functionally similar to SSH, SSL is often used for web-based applications. Though The term "Secure Sockets Layer (SSL)" is still commonly used, it's important to note that it's been deprecated in favor of the more secure Transport Layer Security (TLS) protocol. In the context of Ethernet switches, some may offer a web interface for management tasks. Moxa switches support TLS versions 1.2 and 1.3. TLS encrypts the communication

channel between a user's web browser and a device's web interface. This ensures the security of sensitive data during remote configuration tasks performed through the web interface.

Note

Certificates: Self-signed vs. Trusted

There are two main types of certificates used for TLS connections: self-signed certificates and trusted certificates.

- Self-signed certificates: These certificates are issued by the device itself and are not verified by a third-party Certificate Authority (CA). While they provide basic encryption, they may generate warnings in web browsers due to the lack of trust verification.
- Trusted certificates: These certificates are issued by a trusted CA and are generally considered more secure. Web browsers readily accept connections secured with trusted certificates.

The choice between self-signed and trusted certificates depends on your specific security requirements.

SSH & SSL

Menu Path: Security > Device Security > SSH & SSL

This page lets you manage your SSH key and SSL certificate.

This page includes these tabs:

- SSH
- SSL

SSH

Menu Path: Security > Device Security > SSH & SSL - SSH

This page lets you manage your device's SSH key.

Note

Regenerating your SSH key regularly strengthens SSH security by invalidating potentially compromised keys and adding another layer of defense against unauthorized access. There's no one-size-fits-all answer for how often to regenerate keys; it depends on security risk factors like server importance, access frequency, and potential exposure. Consider regenerating them every few months or every year, especially for critical servers.

Regenerate SSH Key

UI Setting	Description	Valid Range	Default Value
Regenerate SSH Key	Click **Regenerate** to regenerate the SSH key. **Warning** Regenerating the SSH key will restart the device's system services and will make the device temporarily unavailable.	N/A	N/A

SSL

Menu Path: Security > Device Security > SSH & SSL - SSL

This page lets you manage your device's SSL certificate.

Certificate Information

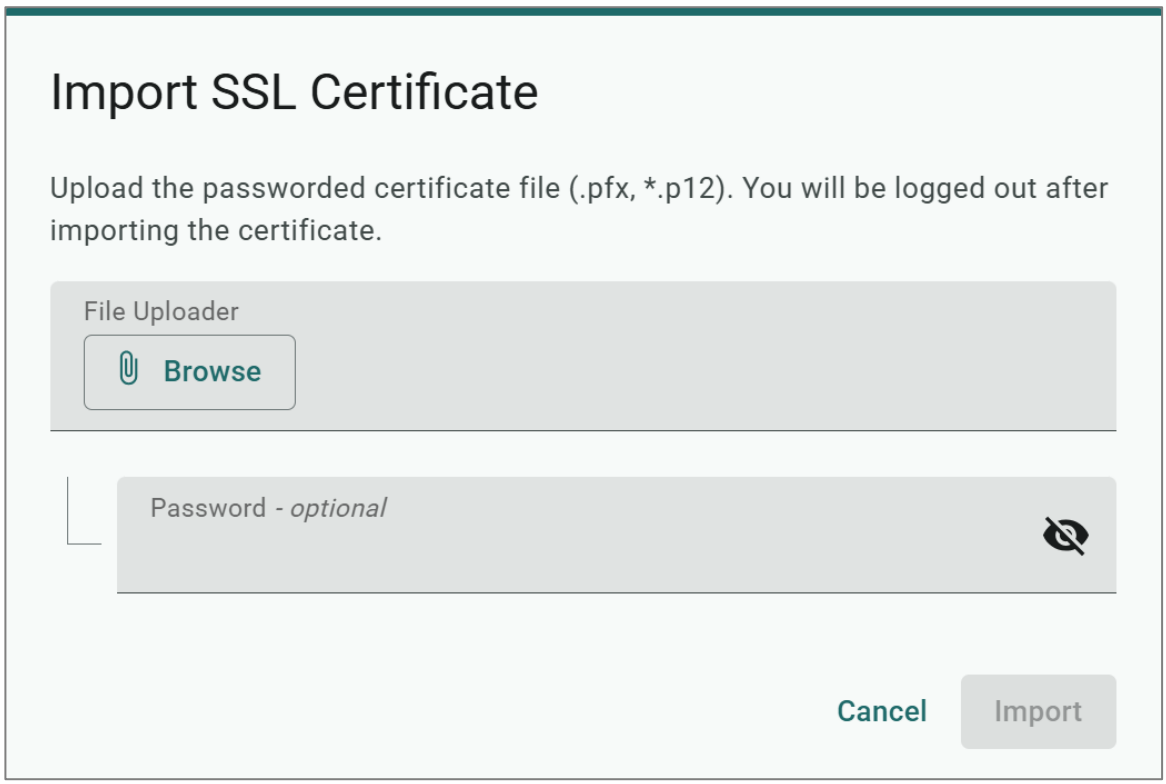
UI Setting	Description
CA Name	Shows the CA name of the SSL certificate.
Expiration Date	Shows when the current certificate will expire.

Import SSL Certificate

Menu Path: Security > Device Security > SSH & SSL - SSL

Clicking the **Manage** button on the **Security > Device Security > SSH & SSL - SSL** page and selecting **Import SSL Certificate** will open this dialog box. This dialog lets you import a SSL certificate.

Click **Import** to save your changes and add the new SSL certificate.



UI Setting	Description	Valid Range	Default Value
File Uploader	Select and upload an SSL certificate file (.pfx, *.p12) from your computer.	N/A	N/A

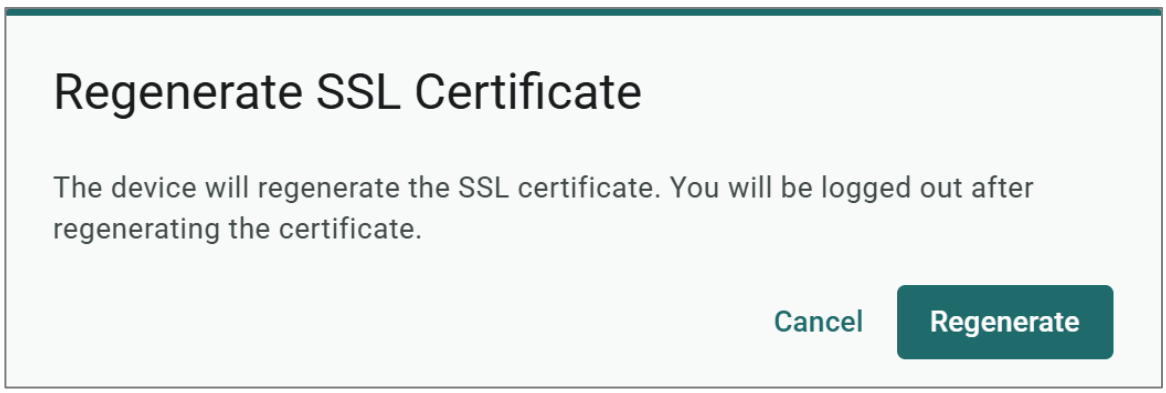
UI Setting	Description	Valid Range	Default Value
Password	Specify the password for the selected SSL certificate, if applicable.	N/A	N/A

Regenerate SSL Certificate

Menu Path: Security > Device Security > SSH & SSL - SSL

Clicking the **Manage** button on the **Security > Device Security > SSH & SSL - SSL** page and selecting **Regenerate SSL Certificate** will open this dialog box. This dialog lets you regenerate the SSL certificate.

Click **Regenerate** to regenerate the SSL certificate. You will be logged out after regenerating the certificate.



Network Security

Menu Path: Security > Network Security

This section lets you configure the network-level security settings of your device.

This section includes these pages:

- IEEE 802.1X
- MAC Authentication Bypass
- Port Security
- Traffic Storm Control
- Access Control List

- Network Loop Protection
- Binding Database
- DHCP Snooping
- IP Source Guard
- Dynamic ARP Inspection

About IEEE 802.1X

IEEE 802.1X is a standard for managing access control, ensuring that devices seeking to access network resources are what they claim to be.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

About IEEE 802.1X

802.1X is a standard for port-based Network Access Control (NAC) that provides an authentication framework for devices trying to connect to a network.

Part of the IEEE 802.1 group of networking protocols, the primary purpose of 802.1X is to enhance the security of wired and wireless networks by requiring users and devices to authenticate themselves before gaining access to network resources.

Topology

An 802.1X topology has three roles:

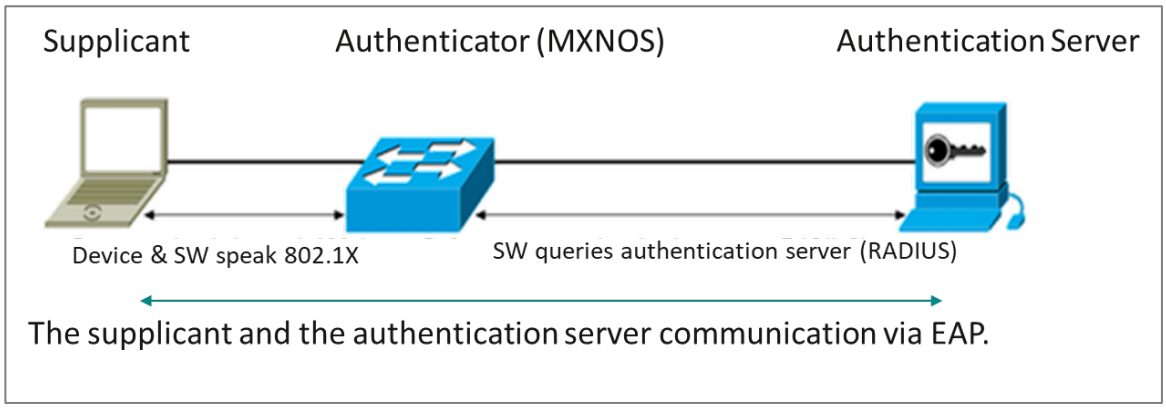
- Supplicant: The client device (e.g., laptop, smartphone) seeking network access.
- Authenticator: The network device (e.g., switch, wireless access point) that controls access to the network ports.
- Authentication Server: A server that performs the actual authentication of the supplicant. It could be a RADIUS (Remote Authentication Dial-In User Service) server or another centralized authentication service.

Note

In an 802.1X environment, Moxa switches primarily function as authenticators. However, they can also be optionally configured to act as authentication servers.

In an 802.1X authentication system, the supplicant (client), authenticator device (Switch or Wi-Fi AP), and authentication server exchange information using the Extensible Authentication Protocol (EAP).

A supplicant and an authenticator exchange EAPOL (Extensible Authentication Protocol over LAN) frames with each other. We can either use an external RADIUS server as the authentication server or implement the authentication server in the Moxa switch by using a Local User Database as the authentication look-up table. When using an external RADIUS server as the authentication server, the authenticator and the authentication server exchange EAP frames.

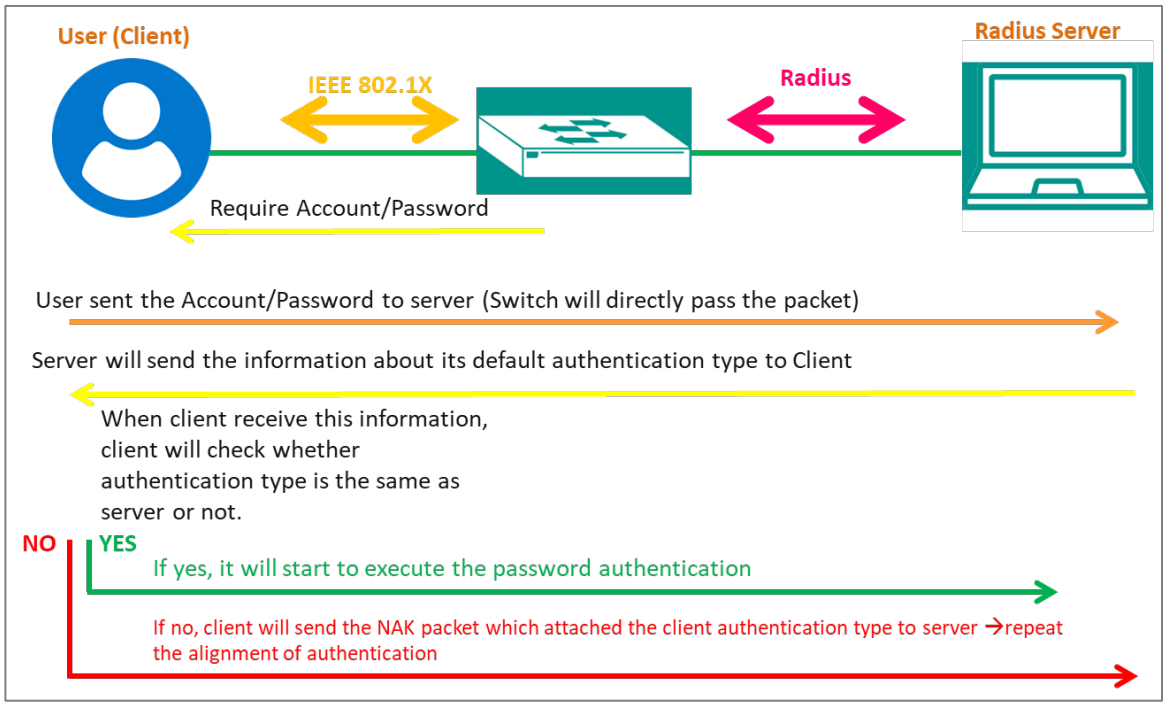


Note

It is possible to use 802.1X authentication without a separate authentication server using local authentication. The Authenticator can be configured to determine client access rights.

Authentication Process

When a device connects to a network port configured for 802.1X, the following process occurs:

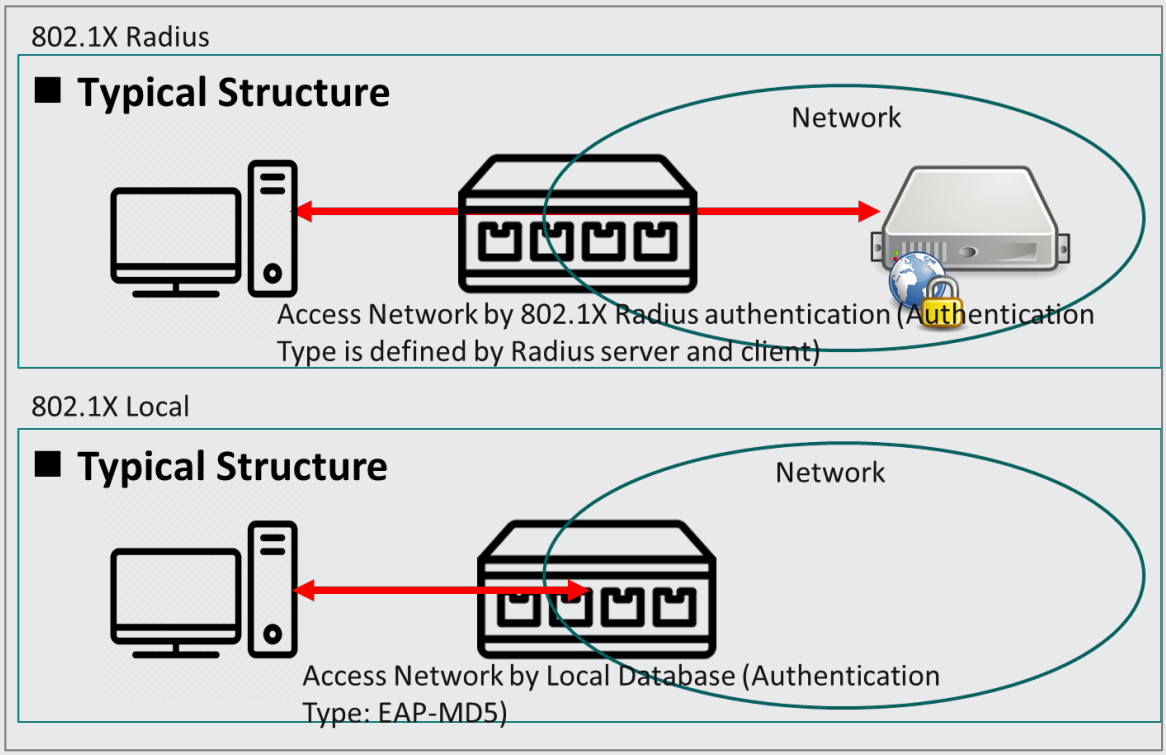


1. Initialization: The supplicant sends an EAPOL (Extensible Authentication Protocol Over LAN) start message to the authenticator.
2. Authentication Request: The authenticator replies with an EAP Request/Identity message, prompting the supplicant to provide its identity.
3. Identity Response: The supplicant responds with its identity, typically a username.
4. Authentication Exchange: The authenticator relays the identity to the authentication server, which then initiates an authentication exchange with the supplicant using EAP (Extensible Authentication Protocol).
5. Authentication Result: Based on the outcome of the authentication process (which could involve methods like username/password, digital certificates, or other credentials), the authentication server sends an Accept or Reject message to the authenticator.
6. Access Granted/Denied: If authentication is successful, the authenticator allows the supplicant access to the network. If authentication fails, access is denied.

802.1X provides a robust mechanism for controlling network access, ensuring that only authorized users and devices can connect to the network. It's widely used in enterprise environments to enforce security policies and protect against unauthorized access. The following diagram illustrates the process of a client establishing 802.1X communication with the authentication server through the MXNOS switch.

Note

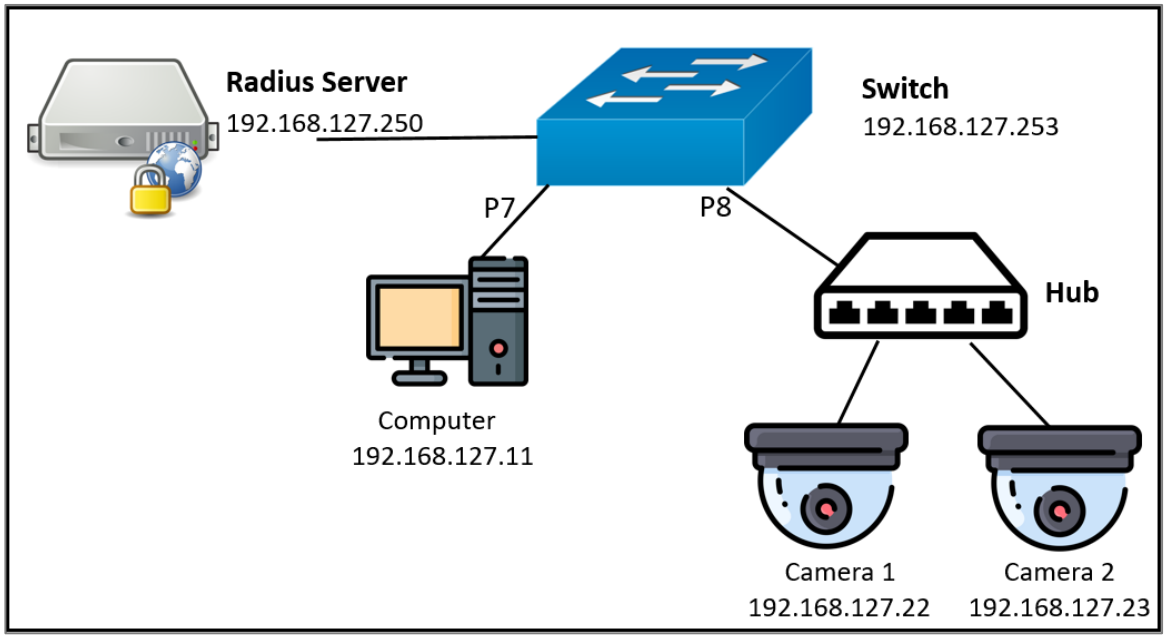
Authentication can also be initiated by the authenticator. Ordinarily, supplicants initiate the authentication process, with an EAPOL-Start frame sent to the authenticator. When the authenticator initiates the authentication process (either on its own, or on receipt of an EAPOL-Start frame), it sends an EAP Request/Identity frame to ask for the username of the supplicant.



Example: Configuring a Switch as an Authenticator

In this example, we configure a Moxa switch as an authenticator, connecting supplicant devices (2 cameras and a computer) to a RADIUS server.

Our sample topology should look like the following:



The topology uses the following roles:

- Supplicants:
  - Cameras 1 and 2, connected to the switch with a hub on port 8
  - Computer, connected on Port 7
- Authenticator: Switch
- Server: RADIUS server

Before you begin: This task uses sample values and assumes that a RADIUS server is already configured.

To configure the switch as an authenticator, do the following:

1. Sign in to the device using administrator credentials.
2. Got to **Security > Network Security > IEEE 802.1X→General**.
3. Click **IEEE 802.1X** and choose **Enabled** from the drop-down menu.
4. Click **Authentication Mode**, choose **RADIUS** from the drop-down menu, and then click **Apply** to save your settings.
5. To configure the example computer, click ***[Edit]*** corresponding to **Port 7**.
   Result: The **Port Settings** screen appears.
6. Configure the following:

7.

Option	Value
Enabled	**Enabled**
Port Control	**Auto**
Authentication Session Type	**Port-Based**
Max. Request	**2**
Quiet Period	**60**
Reauthentication	**Disabled**

8. Click **Apply**.
9. To configure the example cameras, click ***[Edit]*** corresponding to **Port 8**.
   Result: The **Port Settings** screen appears.
10. Configure the following:

Option	Value
Enabled	Enabled
Port Control	Auto
Authentication Session Type	MAC-based
Max. Request	2
Quiet Period	60
Reauthentication	Disabled

11. Click **Apply**.

What to do next: You must configure RADIUS server settings before the switch can function as an authenticator.

Example: Configuring RADIUS Server Settings

The switch must be configured with the RADIUS server settings before it can serve as an authenticator.

1. Sign in to the device using administrator credentials.
2. Go to **Security > Network Security > IEEE 802.1X > RADIUS**.
3. Specify all of the following:

Option	Value
Server IP Address 1	192.168.127.11
Auth Port	1812
Share Key	Type your key here
Timeout	**5**
Retransmit	**5**

4. Click **Apply** to save changes.

What to do next: Once configured, status information will be available under **Security > Network Security > IEEE 802.1X > Status**.

IEEE 802.1X

Menu Path: Security > Network Security > IEEE 802.1X

This page lets you manage your device's IEEE 802.1X authentication feature.

This page includes these tabs:

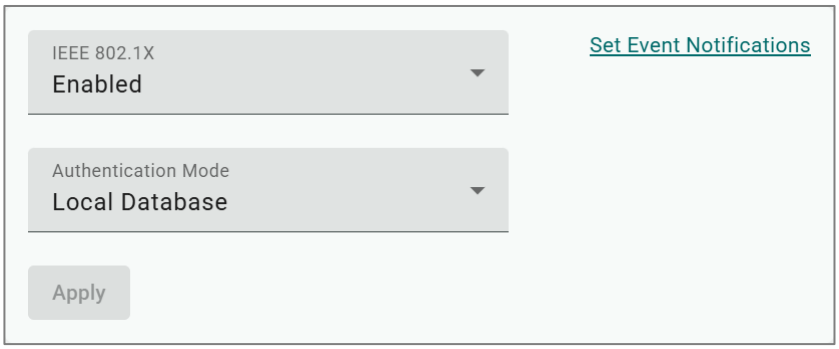
- General
- RADIUS
- Local Database

IEEE 802.1X - General

Menu Path: Security > Network Security > IEEE 802.1X - General

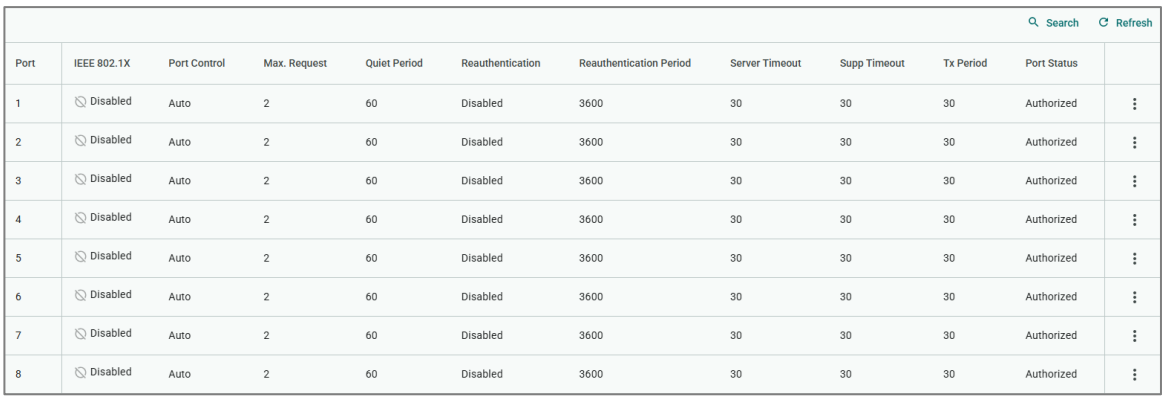
This page lets you configure your device's IEEE 802.1X settings.

IEEE 802.1X Settings



UI Setting	Description	Valid Range	Default Value
IEEE 802.1X	Enable or disable IEEE 802.1X authentication. **Note** Enabling IEEE 802.1X allows VLAN assignment through a RADIUS server, but the VLAN must already exist.	Enabled / Disabled	Disabled
Authentication Mode	Specify the authentication mode to use. • **RADIUS**: Use a RADIUS server for authentication. • **Local Database**: Use the local database for authentication.	RADIUS / Local Database	Local Database

IEEE 802.1X List



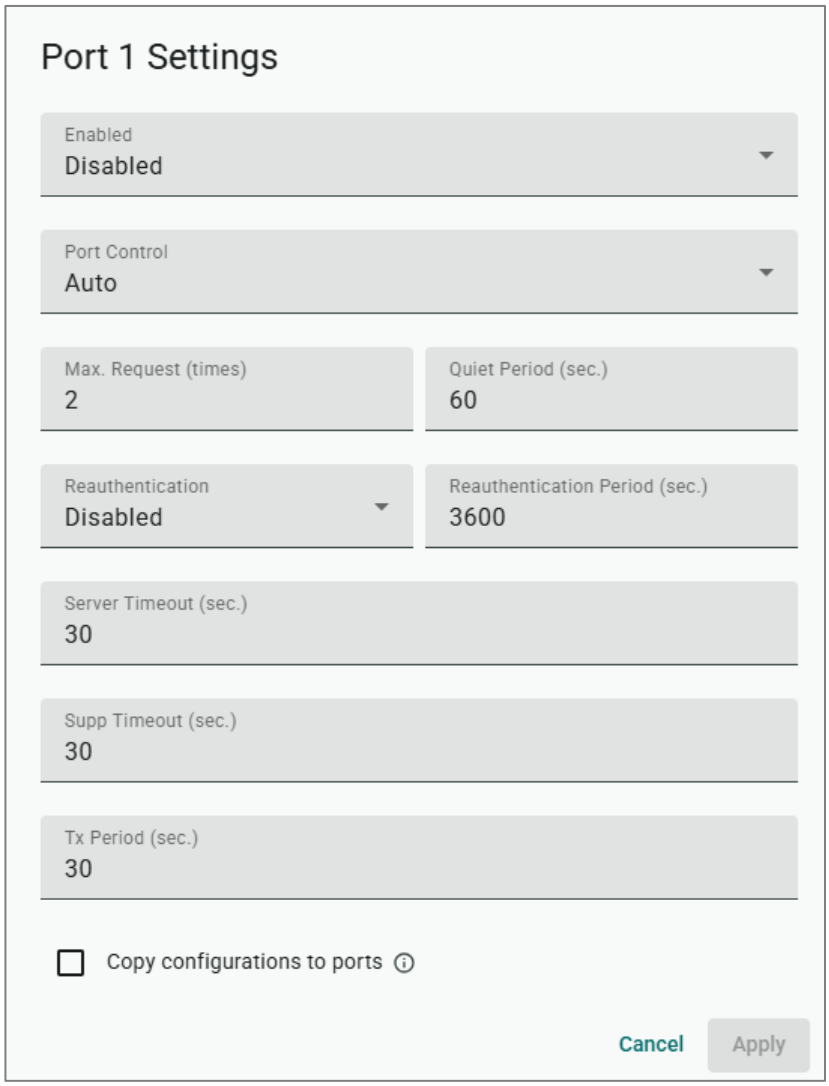
UI Setting	Description
Port	Shows the port number the entry is for.
IEEE 802.1X	Shows whether IEEE 802.1X is enabled for the port.
Port Control	Shows the port control method used for the port.
Max. Request	Shows the maximum number of re-authentication requests allowed for the port.
Quiet Period	Shows the amount of time in seconds the device will remain in a quiet state following a failed authentication exchange with a client through the port.
Reauthentication	Shows whether IEEE 802.1X reauthentication is enabled for the port.
Reauthentication Period **(Only in Advanced Mode)**	Shows the amount of time in seconds to wait in between reauthentication attempts for the port.
Server Timeout **(Only in Advanced Mode)**	Shows the amount of time in seconds the device will try to retransmit packets to an authentication server.
Supp Timeout **(Only in Advanced Mode)**	Shows the amount of time in seconds the device will try to retransmit packets to a supplicant, such as a client PC.
Tx Period **(Only in Advanced Mode)**	Shows the amount of time in seconds the device will try to retransmit the data to a client.
Port Status	Shows the current authorization status of the port.

IEEE 802.1X - Edit Port Settings

Menu Path: Security > Network Security > IEEE 802.1X - General

Clicking the **Actions (⋮)** icon then **Edit** for a port on the **Security > Network Security > IEEE 802.1X - General** page will open this dialog box. This dialog lets you edit the IEEE 802.1X settings for the port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Enabled	Enable or disable IEEE 802.1X authentication for the port.	Enabled / Disabled	Disabled
Port Control	Select the port control method to use for the port. • **Force Unauthorized**: The controlled port will stay in the unauthorized state. • **Auto**: The controlled port will be set to the authorized or unauthorized state based on the outcome of an authentication exchange between the supplicant and the authentication server. • **Force Authorized**: The controlled port will stay in the authorized state.	Force Unauthorized / Auto / Force Authorized	Auto

UI Setting	Description	Valid Range	Default Value
Max. Request	Specify how many times to attempt reauthentication for the port.	1 to 10	2
Quiet Period	Specify the amount of time in seconds the device will remain in a quiet state following a failed authentication exchange with a client through the port.	0 to 65535	60
Reauthentication	Enable/disable IEEE 802.1X reauthentication for the port.	Enabled / Disabled	Disabled
Reauthentication Period **(Only in Advanced Mode)**	Specify the amount of time in seconds to wait in between reauthentication attempts for the port.	1 to 65535	3600
Server Timeout **(Only in Advanced Mode)**	Specify the amount of time in seconds the device will try to retransmit packets to an authentication server.	1 to 65535	30
Supp Timeout **(Only in Advanced Mode)**	Specify the amount of time in seconds the device will try to retransmit packets to a supplicant, such as a client PC.	1 to 65535	30
Tx Period **(Only in Advanced Mode)**	Specify the amount of time in seconds the device will try to retransmit the data to a client.	1 to 65535	30
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

IEEE 802.1X - Reauthenticate Port Settings

Menu Path: Security > Network Security > IEEE 802.1X - General

Clicking the **Actions (⋮)** icon then **Reauthenticate** for a port on the **Security > Network Security > IEEE 802.1X - General** page will open this dialog box. This dialog lets you reauthenticate the IEEE 802.1X settings for the port.

Click **Apply** to save your changes.

IEEE 802.1X - RADIUS

Menu Path: Security > Network Security > IEEE 802.1X - RADIUS

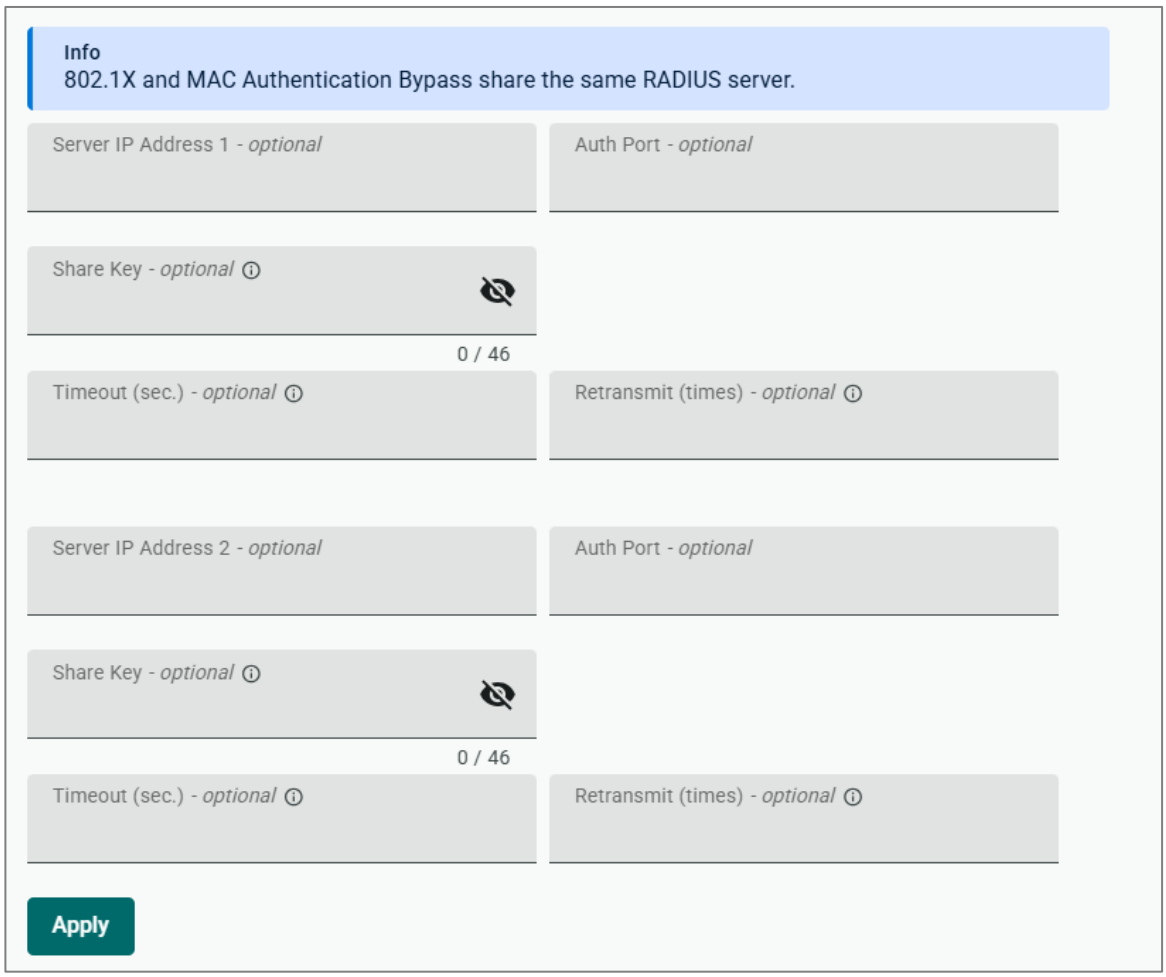
This page lets you specify a RADIUS server to use for IEEE 802.1X authentication. Click **Apply** to save your changes.

> **Note**
>
> The system will use the primary RADIUS server by default. If the primary RADIUS server is unavailable, it will use the secondary RADIUS server.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

IEEE 802.1X RADIUS Settings

> **Note**
>
> 802.1X and MAC authentication bypass share the same RADIUS server settings; changes made here will also affect the other feature.



UI Setting	Description	Valid Range	Default Value
Server IP Address 1/2	Specify the IP address of the 1st/2nd server.	Valid IP address	N/A
Auth Port	Specify the authentication port number for the RADIUS server.	1 to 65535	N/A
Share Key	Specify the share key for the server.	0 to 46 characters	N/A
Timeout	Specify how long to wait in seconds before a device is logged out.	1 to 120	N/A
Retransmit	Specify how many times to retry data transmission.	1 to 254	N/A

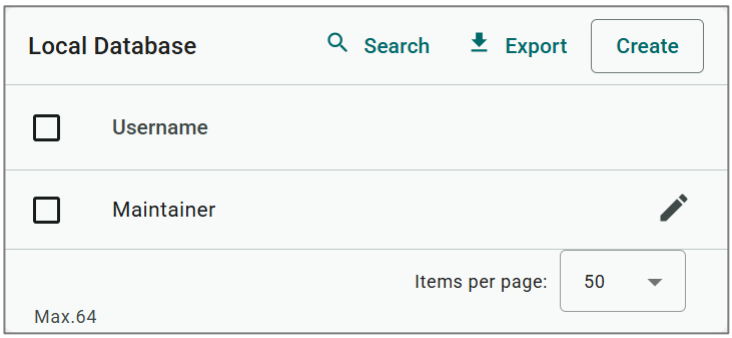
IEEE 802.1X - Local Database

Menu Path: Security > Network Security > IEEE 802.1X - Local Database

This page lets you create local database user accounts to use with IEEE 802.1X authentication.

Limitations

You can create up to 64 IEEE 802.1X local database accounts.



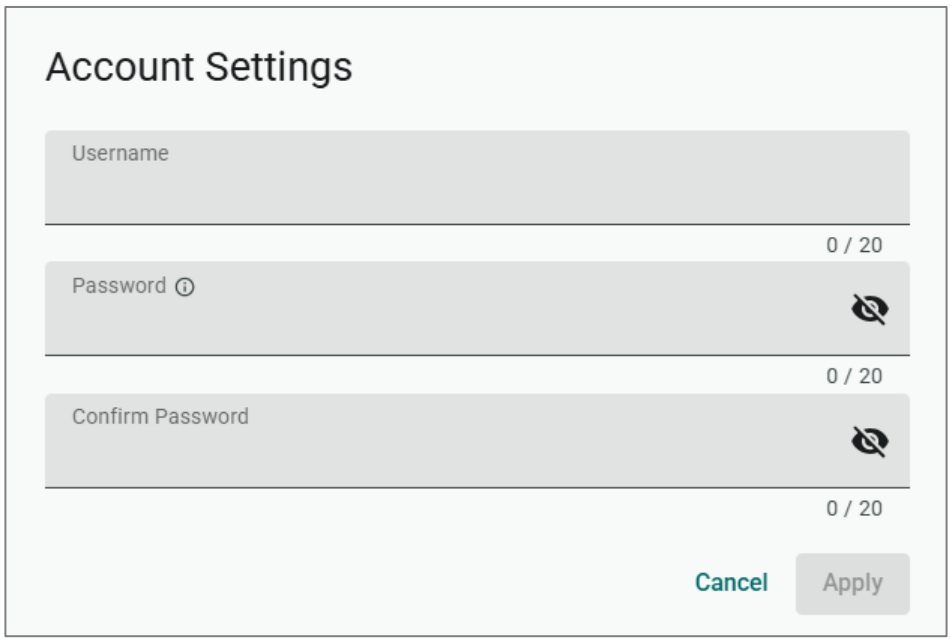
UI Setting	Description
Username	Shows the username of the account.

IEEE 802.1X - Local Database - Account Settings

Menu Path: Security > Network Security > IEEE 802.1X - Local Database

Clicking **Create** on the **Security > Network Security > IEEE 802.1X - Local Database** page will open this dialog box. This dialog lets you create a new user account for IEEE 802.1X authentication.

Click **Create** to save your changes and add the new account.



UI Setting	Description	Valid Range	Default Value
Username	Specify the username for this account.	1 to 20 characters	N/A
Password	Specify the password for this user account.	4 to 20 characters	N/A
Confirm Password	Re-enter the password for this user account.	4 to 20 characters	N/A

About MAC Authentication Bypass

MAC Authentication Bypass (MAB) allows network access based on a device's Media Access Control (MAC) address, bypassing traditional username/password authentication methods like 802.1X. This feature is particularly useful for granting access to devices that cannot support more advanced authentication protocols.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

How MAC Authentication Bypass Works

MAB operates like a VIP list for your network. When a device connects, the network checks its MAC address against an approved list. If the MAC address is recognized, the device is granted access without needing additional authentication. If the MAC address isn't on the list, access is denied.

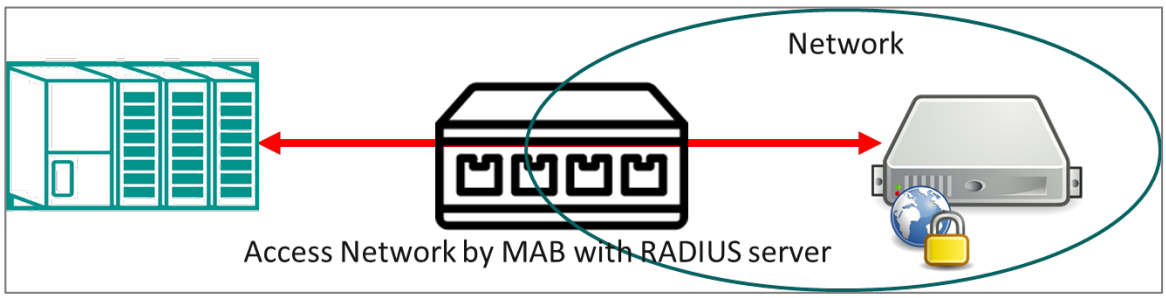
When to Use MAB

- **Legacy Devices:** Some older devices may not support advanced authentication methods like 802.1X. MAB provides a way to allow these devices to connect using their MAC address.

While MAB is convenient, it’s important to note that MAC addresses can be spoofed, making this method less secure compared to more robust authentication techniques. Therefore, MAB should be used in scenarios where ease of access is prioritized over stringent security measures.

Configuring MAC Authentication Bypass

To add a device to MAC Authentication Bypass, first add the MAC address of the bypass device to the **Local Database**, then enable **MAC Authentication Bypass** on the Port the bypass device is attached to.



This procedure assumes that devices on your network are authenticated using either a RADIUS server or a local database.

Note

MAC addresses are easily spoofed, and are not generally accepted as adequete means of authentication without other forms of security. Make sure that you have fully evaluated the security risks associated with this feature before use in a sensitive environment.

To configure MAC Authentication Bypass, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Security** > **Network Security** > **MAC Authentication Bypass**, click on the **Local Database** tab, and then click ***[Add]***.

   The Create Entry screen appears.
3. Specify the **MAC Address** of the device to be added to the local database, and then click **Create**.

   The MAC address appears in the table.
4. Click the **General** tab at the top of the screen, and verify that **MAC Authentication Bypass** is **Enabled**.
5. Locate the port the bypass device is attached to, and then click the corresponding **[Edit]** button.

   The Edit Port Settings screen appears.
6. Set **MAC Authentication Bypass** to **Enabled**, and then click **Apply**.

The bypass device will now be authenticated for network access.

MAC Authentication Bypass

Menu Path: Security > Network Security > MAC Authentication Bypass

This page lets you configure the MAC Authentication Bypass settings.

This page includes these tabs:

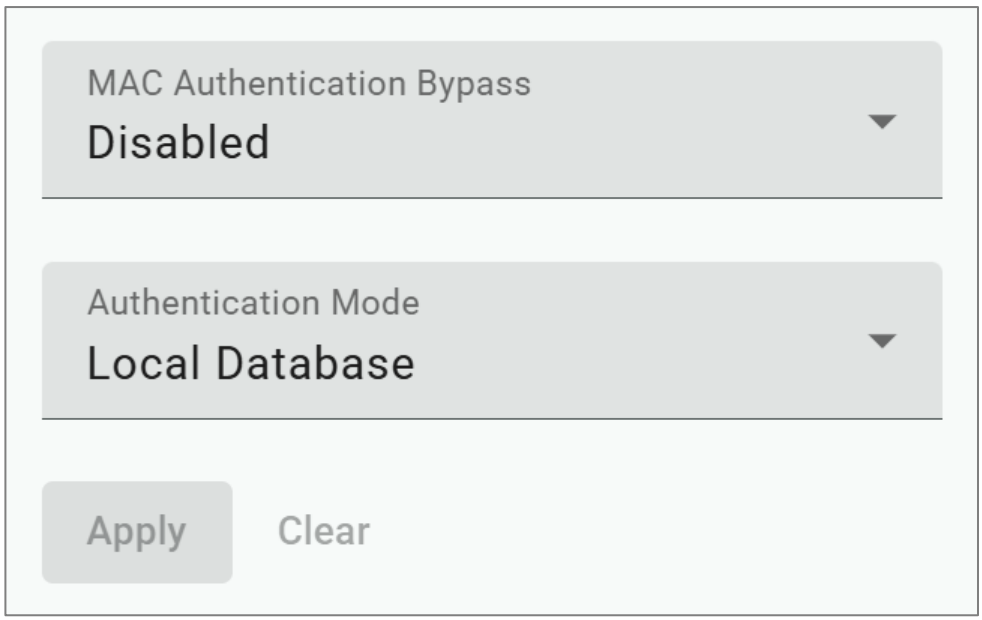
- General
- RADIUS
- Local Database

MAC Authentication Bypass - General

Menu Path: Security > Network Security > MAC Authentication Bypass - General

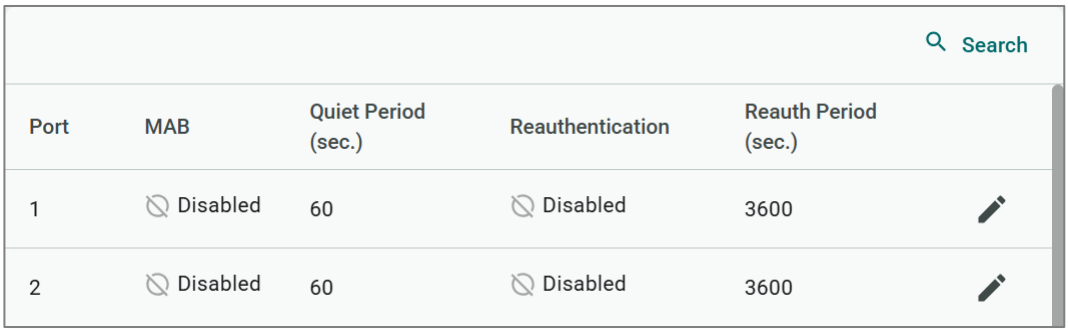
This page lets you configure general settings for MAC authentication bypass.

MAC Authentication Bypass Settings



UI Setting	Description	Valid Range	Default Value
MAC Authentication Bypass	Enable or disable MAC authentication bypass (MAB). **Note** If the static MAC address limit is reached, you can re-enable MAC Authentication Bypass to clear all MAC addresses gathered through MAC Authentication Bypass.	Enabled / Disabled	Disabled
Authentication Mode	Specify the authentication mode for MAC authentication bypass. **Note** When MAC Authentication Bypass is set to the Local Database authentication mode, it does not support a quiet period. If you require MAB with a quiet period, please use RADIUS authentication.	RADIUS / Local Database	Local Database

MAC Authentication Bypass List



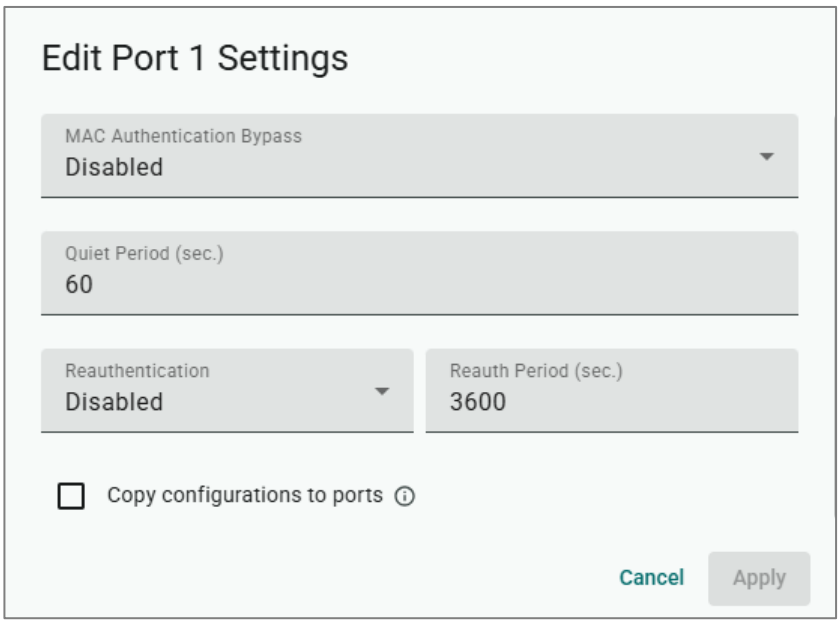
UI Setting	Description
Port	Shows the port number the entry is for.
MAB	Shows whether MAC Authentication Bypass is enabled for the port.
Quiet Period	Show the amount of time in seconds the device will remain in a quiet state following a failed authentication exchange with a client through the port.
Reauthentication	Shows whether IEEE 802.1X reauthentication is enabled for the port.
Reauthentication Period	Shows the amount of time in seconds to wait in between reauthentication attempts for the port.

MAC Authentication Bypass - Edit Port Settings

Menu Path: Security > Network Security > MAC Authentication Bypass - General

Clicking the **Edit (✎)** icon for a port on the **Security > Network Security > MAC Authentication Bypass - General** page will open this dialog box. This dialog lets you edit the MAC Authentication Bypass settings for the port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
MAC Authentication Bypass	Enable or disable MAC Authentication Bypass for the port.	Enabled / Disabled	Disabled
Quiet Period	Specify the amount of time in seconds the device will remain in a quiet state following a failed authentication exchange with a client through the port.	5 to 300	60 sec.
Reauthentication	Enable or disable IEEE 802.1X reauthentication for the port.	Enabled / Disabled	Disabled
Reauthentication Period	Specify the amount of time in seconds to wait in between reauthentication attempts for the port.	60 to 65535	3600 sec.
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

MAC Authentication Bypass - RADIUS

Menu Path: Security > Network Security > MAC Authentication Bypass - RADIUS

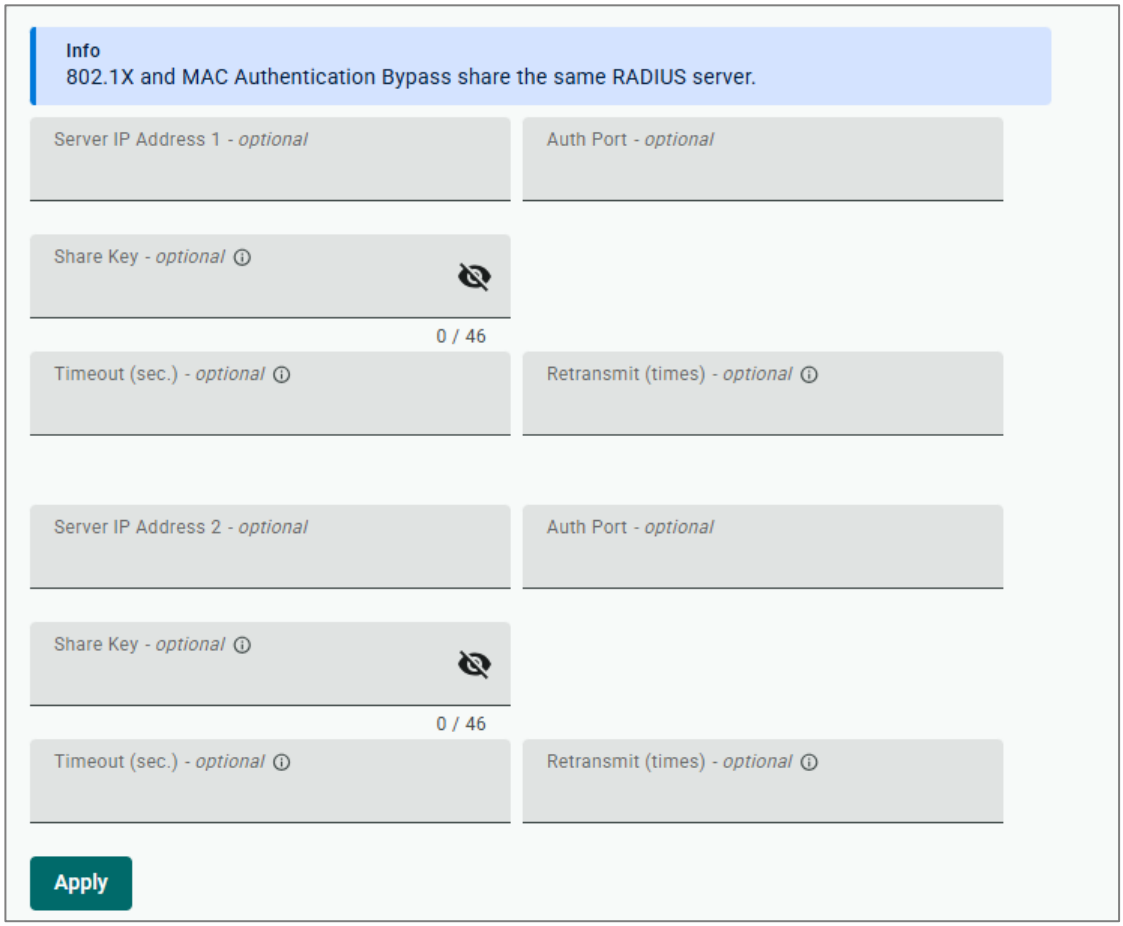
This page lets you configure the RADIUS settings for MAC authentication bypass.

Note

Enabling MAC Authentication Bypass allows VLAN assignment through a RADIUS server, but the VLAN must already exist.

Note

802.1X and MAC authentication bypass share the same RADIUS server settings; changes made here will also affect the other feature.



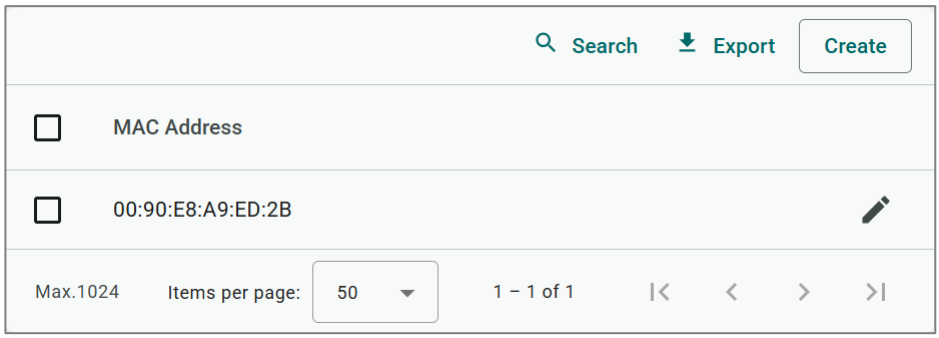
UI Setting	Description	Valid Range	Default Value
Server IP Address 1/2	Specify the IP address of the 1st/2nd server.	Valid IP address	N/A
Auth Port	Specify the authentication port number for the RADIUS server.	1 to 65535	N/A

UI Setting	Description	Valid Range	Default Value
Share Key	Specify the share key for the server.	0 to 46 characters	N/A
Timeout	Specify how long to wait in seconds before a device is logged out.	1 to 120	N/A
Retransmit	Specify how many times to retry data transmission.	1 to 254	N/A

MAC Authentication Bypass - Local Database

Menu Path: Security > Network Security > MAC Authentication Bypass - Local Database

This page lets you manage local database entries for MAC authentication bypass.



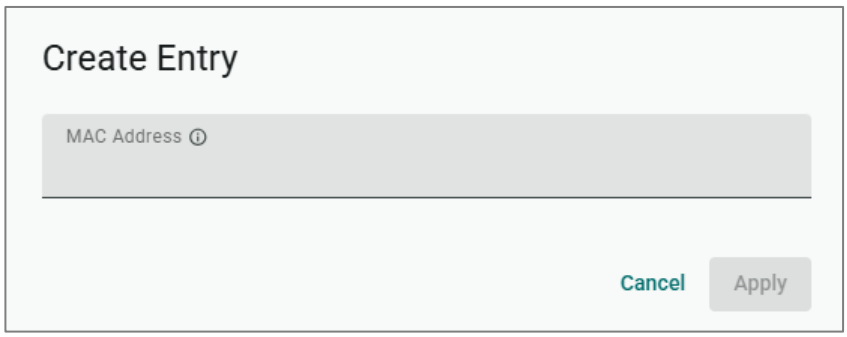
UI Setting	Description
MAC Address	Shows the MAC address used for MAC authentication bypass.

MAC Authentication Bypass - Local Database - Create Entry

Menu Path: Security > Network Security > MAC Authentication Bypass - Local Database

Clicking **Create** on the **Security > Network Security > MAC Authentication Bypass - Local Database** page will open this dialog box. This dialog lets you create a new MAC authentication bypass entry.

Click **Create** to save your changes and add the new entry.



UI Setting	Description	Valid Range	Default Value
MAC Address	Specify the MAC address to use for MAC authentication bypass.	Valid unicast MAC address	N/A

About MAC Security

Media Access Control Security (MAC security) is defined in IEEE802.1AE and 802.1X, specifying how to secure data communication over a Local Area Network (LAN). MAC security ensures data is securely sent and received at the MAC layer by providing data integrity checks, data origin authentication, and confidentiality.

MAC security cryptographically protects frames on a hop-by-hop basis at Layer 2 on LAN and can be enabled as in combination with other end-to-end Layer 3 security technologies such as IPsec, Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Secure Shell Protocol (SSH).

MAC Security In-Depth

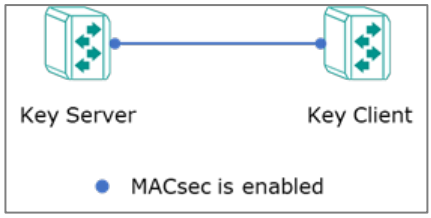
For data exchanged between devices in a LAN, MAC security ensures transmission security using cryptographic technology in the MAC layer.

MAC security involves two standards: IEEE802.1AE and 802.1X. The frame format for data encapsulation, encryption, and authentication is defined in IEEE802.1AE. MACsec Key Agreement (MKA), a key management protocol, is defined in IEEE 802.1X-2010. MKA provides agreement for MAC security policy and key generation mechanisms to extend and optimize the original 802.1X protocol.

MAC security operation starts by using a Pre-shared Key (PSK) to authenticate a peer switch. One switch is designated as the Key Server and the other switch as the Key Client. The Key Server and Key Client share the same user-specified connectivity

Association Key Name (CKN) and Connectivity Association Key (CAK). The Key Server uses the CAK to generate a Secure Association Key (SAK) and distribute it to the Key Client to form a secure association. Data exchanged between the peer switches in the path will then be encrypted.

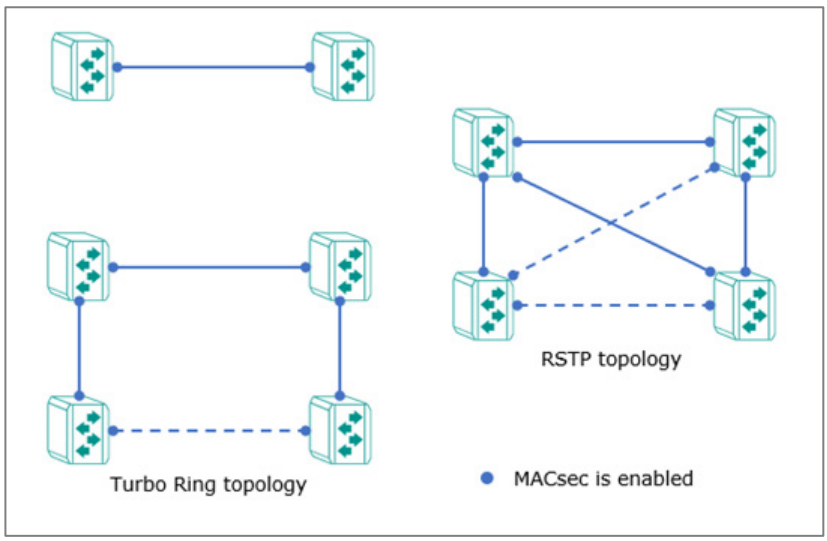
To ensure data traffic is transmitted securely, all data traffic ports must enable MAC security.



MAC Security with Redundancy Protocols

When running MAC security with Redundancy Protocols, make sure of the following:

- For Turbo Ring topologies, all ring ports must enable MAC security.
- For RSTP topologies, all redundant ports must enable MAC security.



Configuring MAC Security

MAC security must be configured on each relevant port and device to protect data.

To configure MAC security, do the following:

1. Sign in to the device with administrator credentials.
2. **Security** > **Network Security** > **MAC security**, and then click **Settings**.
3. To enable **MAC security**, under **MAC security** choose **Enabled** from the dropdown menu, and then click **Apply**.
4. To configure MAC security on a given port, click the corresponding ***[Edit]*** and then configure all of the following:

Option	Value
Status	**Enabled**
Participant CKN	Specify a Connectivity association Key Name of 1-16 characters.
Participant CAK	Specify a Connectivity association Key of 1-16 characters.
Key Server	• **Enabled:** The port is a key server. • **Disabled:** The port is a key client.

Note

- The CKN/CAK must match the connected port on the peer switch.
- One CKN and one CAK per port.
- CKNs/CAKs should not be reused on the same device.
- Valid CKN/CAK characters: a-z, A-Z, numbers 0-9, special characters @%^*()-_+={}[]:.,~$`, and do not permit whitespaces.
- CKNs/CAKs must be configured in pairs, and cannot be partially configured (such as configuring one, but not the other).
- Deleting a CKN/CAK may also delete its corresponding CAK/CKN.

5. Click **Apply** to save your changes.

Make sure to enable MAC security on all relevant devices and ports.

MAC Security (MACsec)

Menu Path: Security > Network Security > MACsec

This page lets you manage MAC security for your device.

This page includes these tabs:

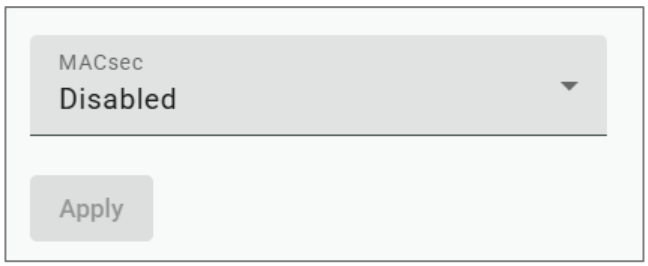
- General
- MKA Status

MACsec - General

Menu Path: Security > Network Security > MACsec - General

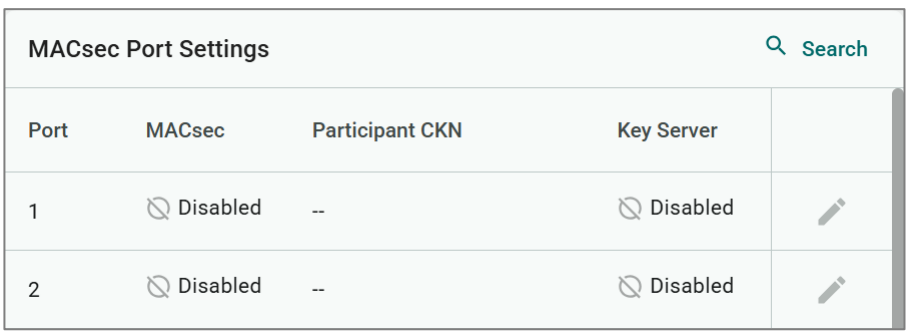
This section lets you configure MAC security for your device.

MACsec Settings



UI Setting	Description	Valid Range	Default Value
MACsec	Enable or disable MAC security (MACsec) for your device.	Enabled / Disabled	Disabled

MACsec Port Settings



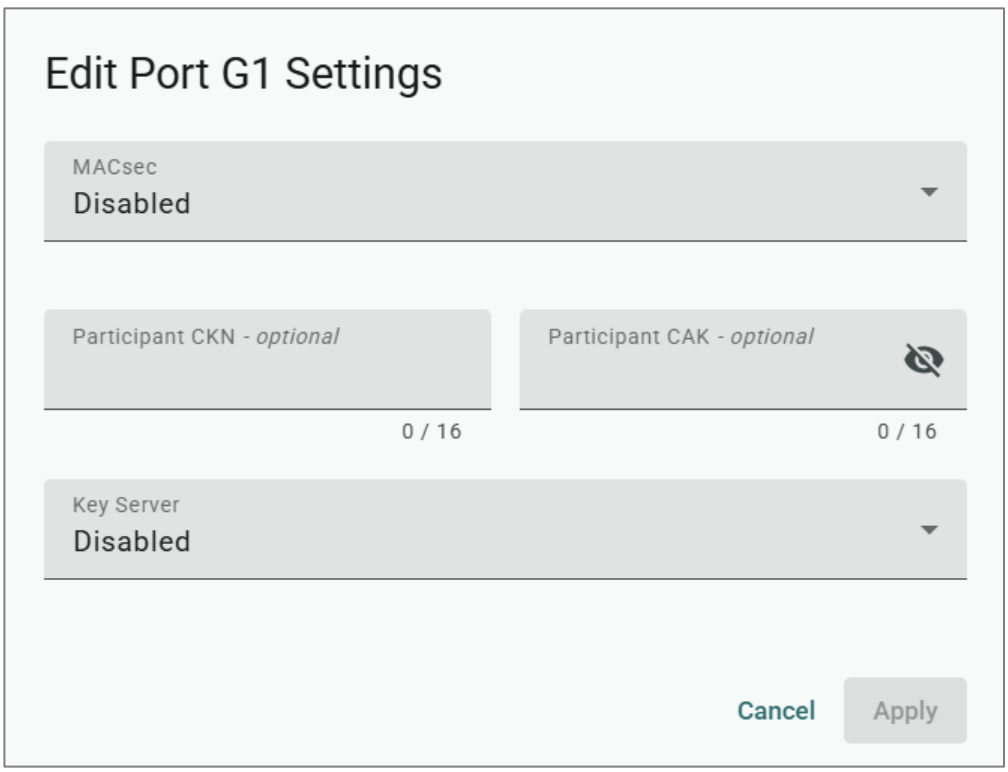
UI Setting	Description
Port	Shows the port this entry is for.
Status	Shows whether MAC security is enabled for the port.
Participant CKN	Shows the Connectivity association Key Name (CKN) configured for the port as the pre-shared key.
Key Server	Shows whether the port is a key server or a key client. • **Enabled:** The port is a key server. • **Disabled:** The port is a key client.

Editing a MACsec Port

Menu Path: Security > Network Security > MACsec - General

Clicking the **Edit** (✎) icon for a port on the **Security > Network Security > MACsec - General** page will open this dialog box. This dialog lets you edit the port's MAC security settings.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable MAC security for this port.	Enabled / Disabled	Disabled
Participant CKN	Specify the Connectivity association Key Name (CKN) to use for the port. **Note** • The CKN configured for this port should be the same as the connected port on the peer switch to enable MACsec for data exchange. • Multiple CKNs are not allowed for a single port. • Different CKNs on a device should be unique. • A CKN can only contain the letters a-z, A-Z, numbers 0-9, special characters @%^*()-_+={}[]:.,~$`, and cannot have any spaces. • CKNs and CAKs must be configured in pairs, and cannot be partially configured (such as configuring one, but not the other). • Deleting a CKN may also delete its corresponding CAK.	1 to 16 characters	N/A
Participant CAK	Specify the Connectivity Association Key (CAK) to use for the port. **Note** • The CAK configured for this port should be the same as the connected port on the peer switch to enable MACsec for data exchange. • Multiple CAKs are not allowed for a single port. • Different CAKs on a device should be unique. • A CAK can only contain the letters a-z, A-Z, numbers 0-9, special characters @%^*()-_+={}[]:.,~$`, and cannot have any spaces. • CKNs and CAKs must be configured in pairs, and cannot be partially configured (such as configuring one, but not the other). • Deleting a CAK may also delete its corresponding CKN.	1 to 16 characters	N/A

UI Setting	Description	Valid Range	Default Value
Key Server	Enable or disable specifying the port as a key server. • **Enabled:** The port is a key server. • **Disabled:** The port is a key client. **Note** • The column for the two connected switches are disabled is not allowed. • If you enable Key Server for a port, Key Server should be disabled for the connected port of the other switch. • If you disable Key Server for a port, Key Server should be enabled for the connected port of the other switch.	Enabled / Disabled	Disabled

MAC Security - MKA Status

Menu Path: Security > Network Security > MACsec - MKA Status

This page lets you view the current MAC security status for your device.

MKA Status Port List

UI Setting	Description
Port	Shows the port this entry is for.
Peer List Member Identifier (MI)	Shows the member identifier of the connected switch.

UI Setting	Description
Peer List Message Number (MN)	Shows the message number received from the connected switch.
Secure Channel ID (SCI)	Shows the session ID for the channel to the other switch.
Peer List Type	Shows the peer list type. • **Potential Peer List**: The MI from the sender cannot be recognized by the receiver. • **Live Peer List**: The MI from the sender can be recognized by the receiver, and the MN from the sender is larger than the MN recorded in the receiver.

Port Security

Menu Path: Security > Network Security > Port Security

This page lets you enable and configure a port security mode for your device.

This page includes these tabs:

- General
- Static Port Lock (if **Static Port Lock** is selected for **Port Security Mode**)
- MAC Sticky (if **MAC Sticky** is selected for **Port Security Mode**)

Port Security - General

Menu Path: Security > Network Security > Port Security - General

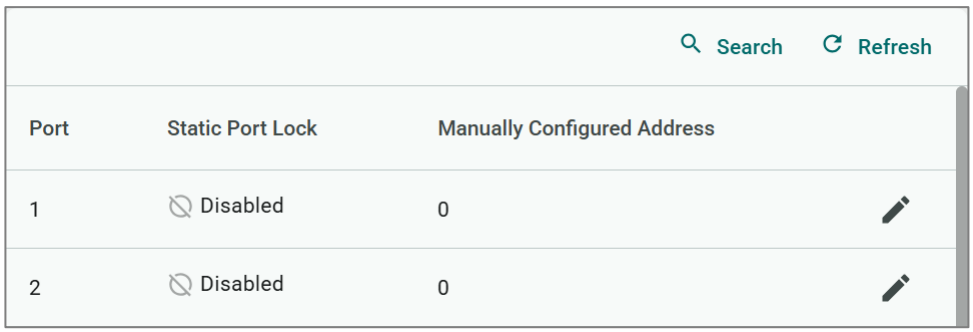
This page lets you enable port security and select a port security mode.

Port Security Settings

UI Setting	Description	Valid Range	Default Value
Port Security	Enable or disable port security.	Enabled / Disabled	Enabled
Port Security Mode	Select a port security mode. **⚠ Warning** When changing the port security mode, all configured port security entries in the Static Port Lock/MAC Sticky tab will be deleted.	Static Port Lock / MAC Sticky	Static Port Lock

Port Security List - Static Port Lock

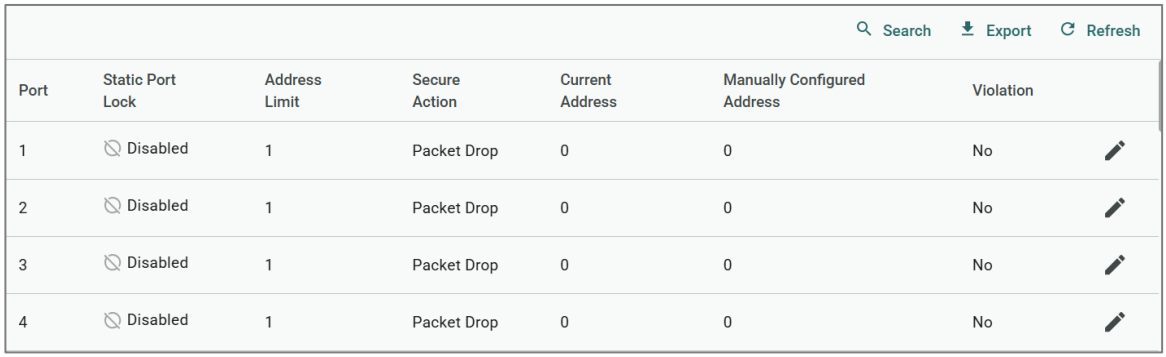
If **Port Security Mode** is set to **Static Port Lock**, the following table will appear.



UI Setting	Description
Port	Shows the port number the entry is for.
Static Port Lock	Shows whether static port lock is enabled for the port.
Manually Configured Address	Shows the number of MAC addresses manually configured for the port.

Port Security List - MAC Sticky

If **Port Security Mode** is set to **MAC Sticky**, the following table will appear.



UI Setting	Description
Port	Shows the port number the entry is for.
MAC Sticky	Shows whether MAC Sticky mode is enabled for the port.
Address Limit	Shows the maximum number of MAC addresses to learn for the port.
Secure Action	Shows the action the device will take when the number of MAC addresses exceeds the address limit.
Current Address	Shows the current number of MAC addresses learned for the port.
Manually Configured Address	Shows the number of manually configured MAC addresses for the port.
Violation	Shows whether there have been any violations for the port.

Port Security - Edit Port Settings

Menu Path: Security > Network Security > Port Security - General

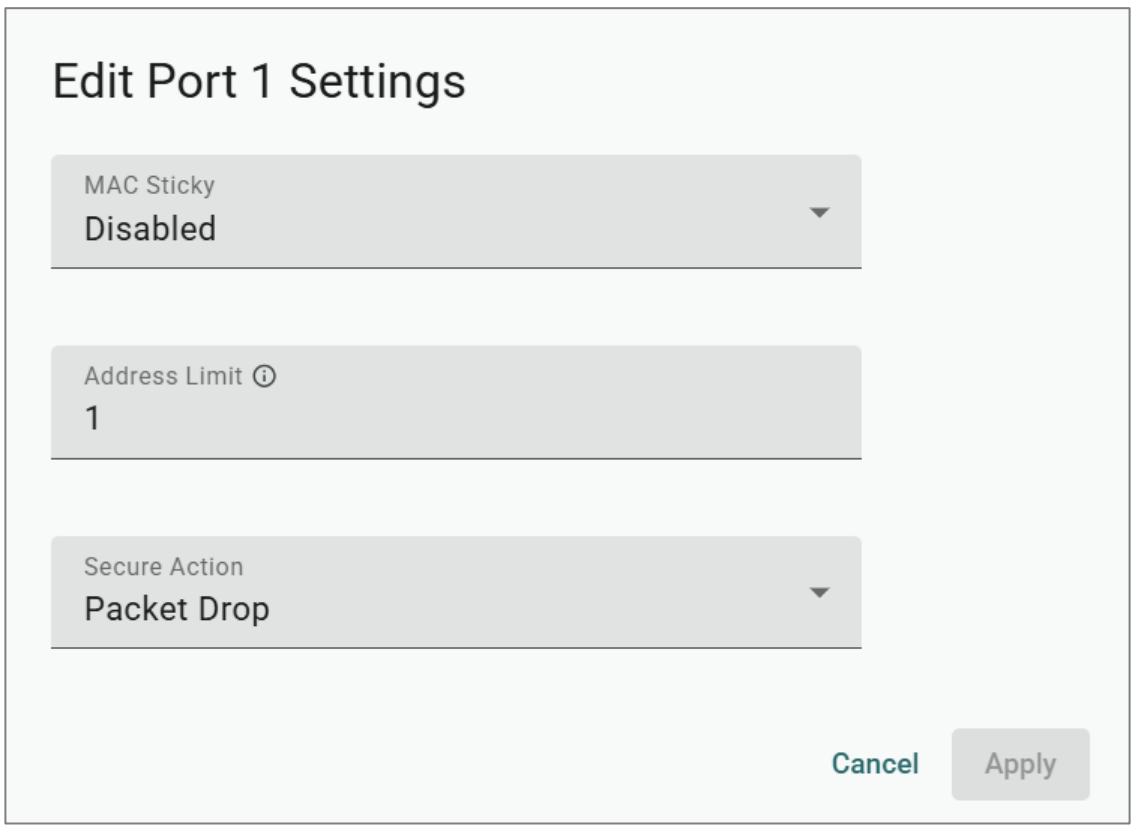
Clicking the **Edit (✎)** icon for a port on the **Security > Network Security > Port Security - General** page will open this dialog box. This dialog lets you configure port security settings for the port.

Click **Apply** to save your changes.

If **Port Security Mode** is set to **Static Port Lock**, the following dialog will appear when editing port security settings.

UI Setting	Description	Valid Range	Default Value
Static Port Lock	Enable or disable Static Port Lock for the port.	Enabled / Disabled	Disabled

If **Port Security Mode** is set to **MAC Sticky**, the following dialog will appear when editing port security settings.



UI Setting	Description	Valid Range	Default Value
MAC Sticky	Enable or disable MAC Sticky for the port.	Enabled / Disabled	Disabled
Address Limit	Specify the maximum number of the learned and configured MAC addresses allowed for the port. **Note** Changing the address limit will clear all currently configured MAC addresses for the port.	1 to 1001	1
Secure Action	Specify the action to take when a violation occurs. • **Port Shutdown**: The port will be shut down. • **Packet Drop**: Packets for the additional MAC addresses will be dropped.	Port Shutdown / Packet Drop	Packet Drop

About Static Port Lock

Static Port Lock provides port-based security by letting you specify which device MAC addresses are allowed to access the network through a specific port. Packets sent from unknown devices or from configured devices with mismatching ports will be dropped. In other words, only packets from devices with allowed MAC addresses can be sent to the specific port, helping secure network data transmissions.

Static Port Lock

Menu Path: Security > Network Security > Port Security - Static Port Lock

This page lets you configure Static Port Lock.

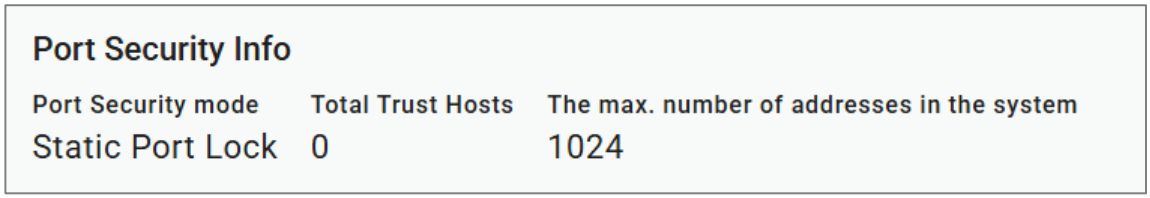
Note

This tab will only appear when Port Security Mode is set to Static Port Lock.

Limitations

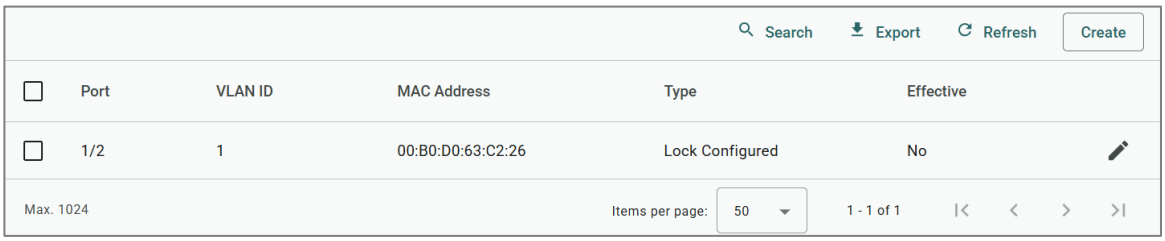
You can create up to 1024 static port lock entries.

Static Port Lock - Port Security Info



UI Setting	Description
Port Security mode	Shows the port security mode being used.
Total Trust Hosts	Shows the number of trusted hosts allowed to access the network.
The max. number of address in the system	Show the maximum number of MAC addresses allowed to be learned or specified for port security.

Static Port Lock - Port List



UI Setting	Description
Port	Shows the port number the entry is for.
VLAN ID	Shows the VLAN applied to the port.
MAC Address	Shows the MAC address of the device which is used as a reliable source for network access.
Type	Shows how the entry was created.

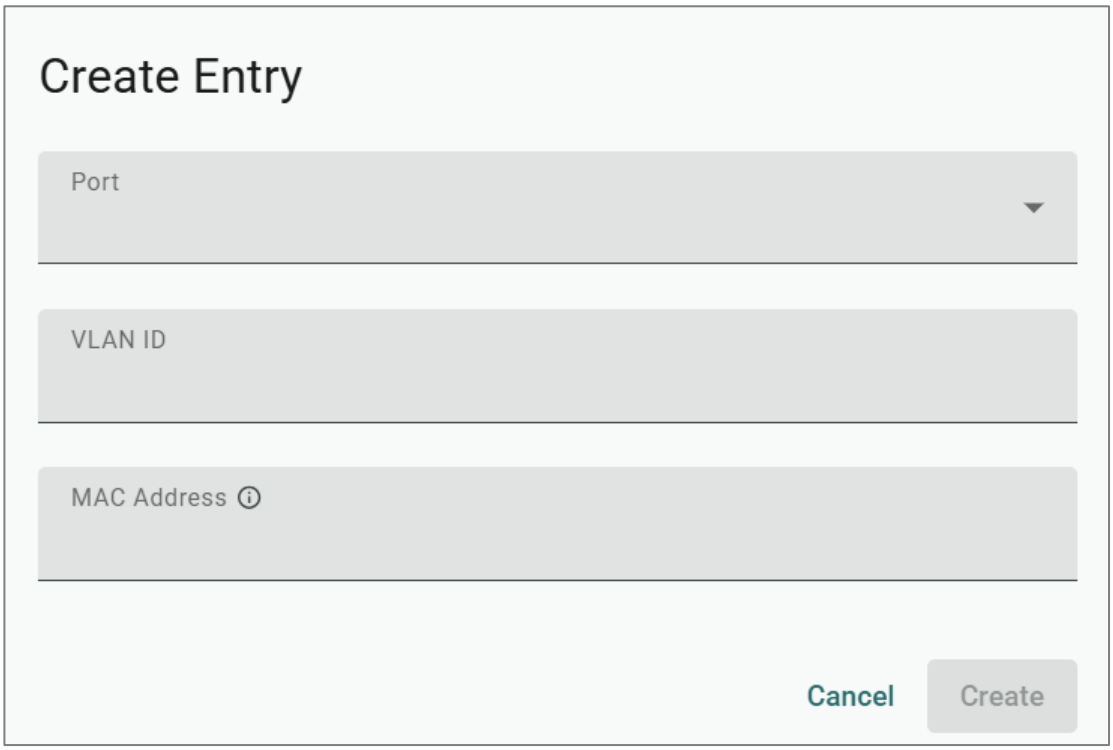
UI Setting	Description
Effective	Shows whether the entry is effective. **Note** If an entry is not effective, it may have an invalid interface set for it.

Static Port Lock - Create Entry

Menu Path: Security > Network Security > Port Security - Static Port Lock

Clicking **Create** on the **Security > Network Security > Port Security - Static Port Lock** page will open this dialog box. This dialog lets you configure static port lock settings for a port.

Click **Create** to save your changes and add the new entry.



UI Setting	Description	Valid Range	Default Value
Port	Select the port to add an entry for.	Drop-down list of ports	N/A
VLAN ID	Specify the VLAN ID to use with the port.	Valid VLAN ID	N/A

UI Setting	Description	Valid Range	Default Value
MAC Address	Specify the MAC address of the device that will be used as the reliable source for network access.	Valid unicast MAC address	N/A

About MAC Sticky

MAC Sticky is a function that allows you to configure the maximum number of MAC addresses that a port can "learn." You can also configure what action should be taken when a new MAC address tries to access a port after the maximum number of MAC addresses have already been learned.

How MAC Sticky Works

In MAC Sticky mode, you can set a proper limit number and then configure trusted devices manually, or let the device configure trusted devices automatically. Aside from dropping packets as a response to any violations, you can also configure ports to enter "port shutdown" and achieve a strict security guarantee. When a violation is registered on a port, the port will shut down and an administrator will receive a notification to perform a check.

MAC Sticky

Menu Path: Security > Network Security > Port Security - MAC Sticky

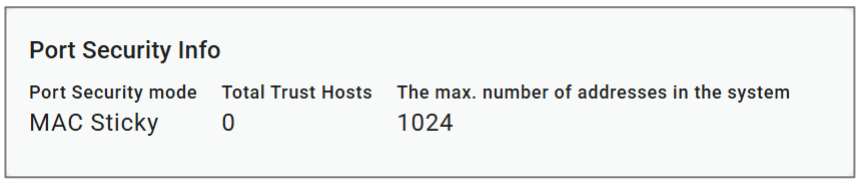
This page lets you configure MAC Sticky.

> **Note**
> This tab will only appear when Port Security Mode is set to MAC Sticky.

Limitations

You can create up to 1024 MAC Sticky entries.

MAC Sticky - Port Security Info



UI Setting	Description
Port Security mode	Shows the port security mode being used.
Total Trust Hosts	Shows the number of trusted hosts allowed to access the network.
The max. number of address in the system	Show the maximum number of MAC addresses allowed to be learned or specified for port security.

MAC Sticky - Port List

UI Setting	Description
Port	Shows the port number the entry is for.
VLAN ID	Shows the VLAN applied to the port.
MAC Address	Shows the MAC address of the device which is used as a reliable source for network access.
Type	Shows how the entry was created.

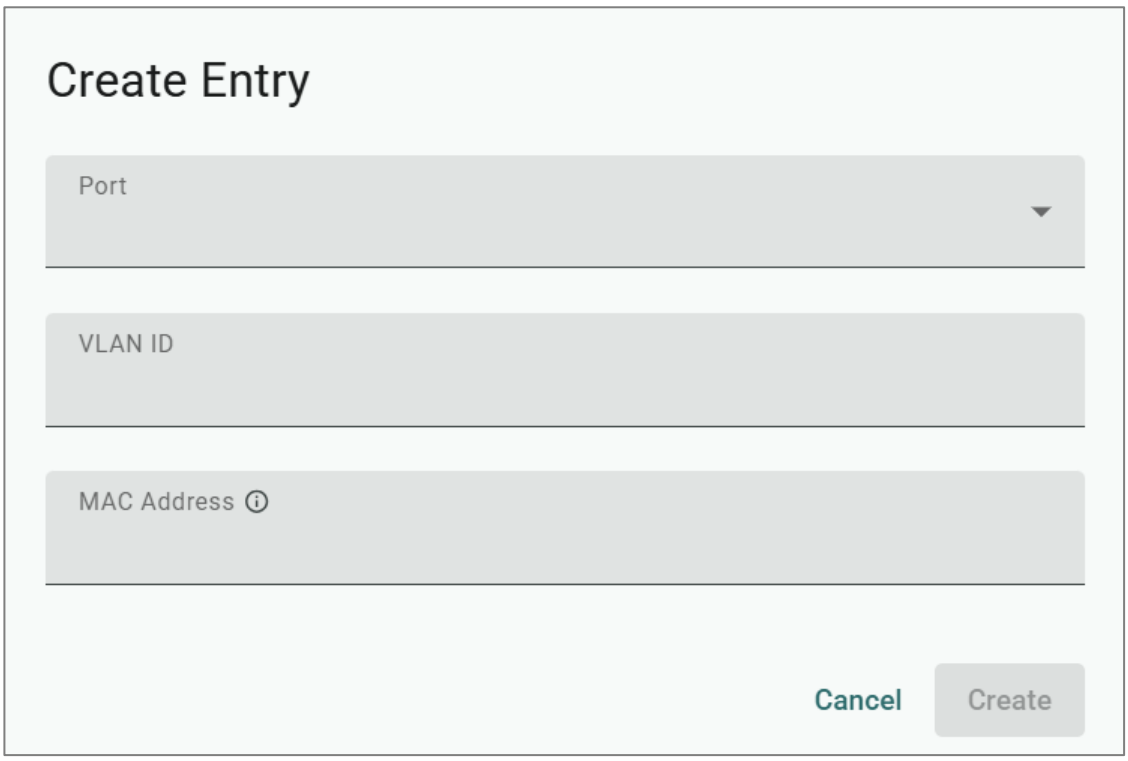
UI Setting	Description
Effective	Shows whether the entry is effective. **Note** If an entry is not effective, it may have an invalid interface set for it.

MAC Sticky - Create Entry

Menu Path: Security > Network Security > Port Security - MAC Sticky

Clicking **Create** on the **Security > Network Security > Port Security - MAC Sticky** page will open this dialog box. This dialog lets you configure MAC Sticky settings for a port.

Click **Create** to save your changes and add the new entry.



UI Setting	Description	Valid Range	Default Value
Port	Select the port to add an entry for.	Drop-down list of ports	N/A
VLAN ID	Specify the VLAN ID to use with the port.	Valid VLAN ID	N/A

UI Setting	Description	Valid Range	Default Value
MAC Address	Specify the MAC address of the device that will be used as the reliable source for network access.	Valid unicast MAC address	N/A

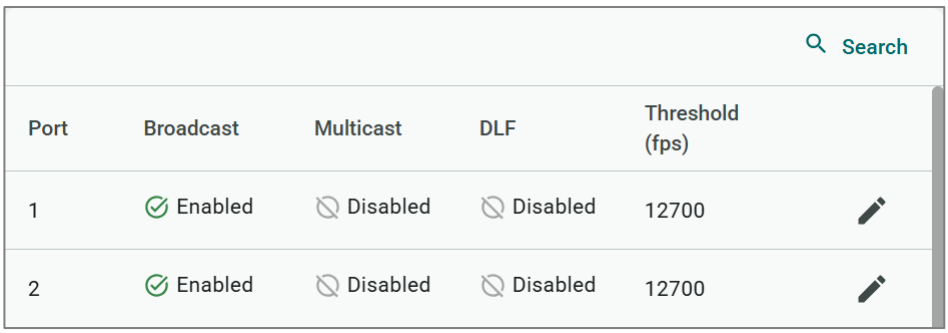
About Traffic Storm Control

A traffic storm can happen when packets flood the network and cause excessive traffic, slowing down 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. Traffic Storm Control can handle packets from both ingress and egress data.

Traffic Storm Control

Menu Path: Security > Network Security > Traffic Storm Control

This page lets you configure traffic storm control for each port.



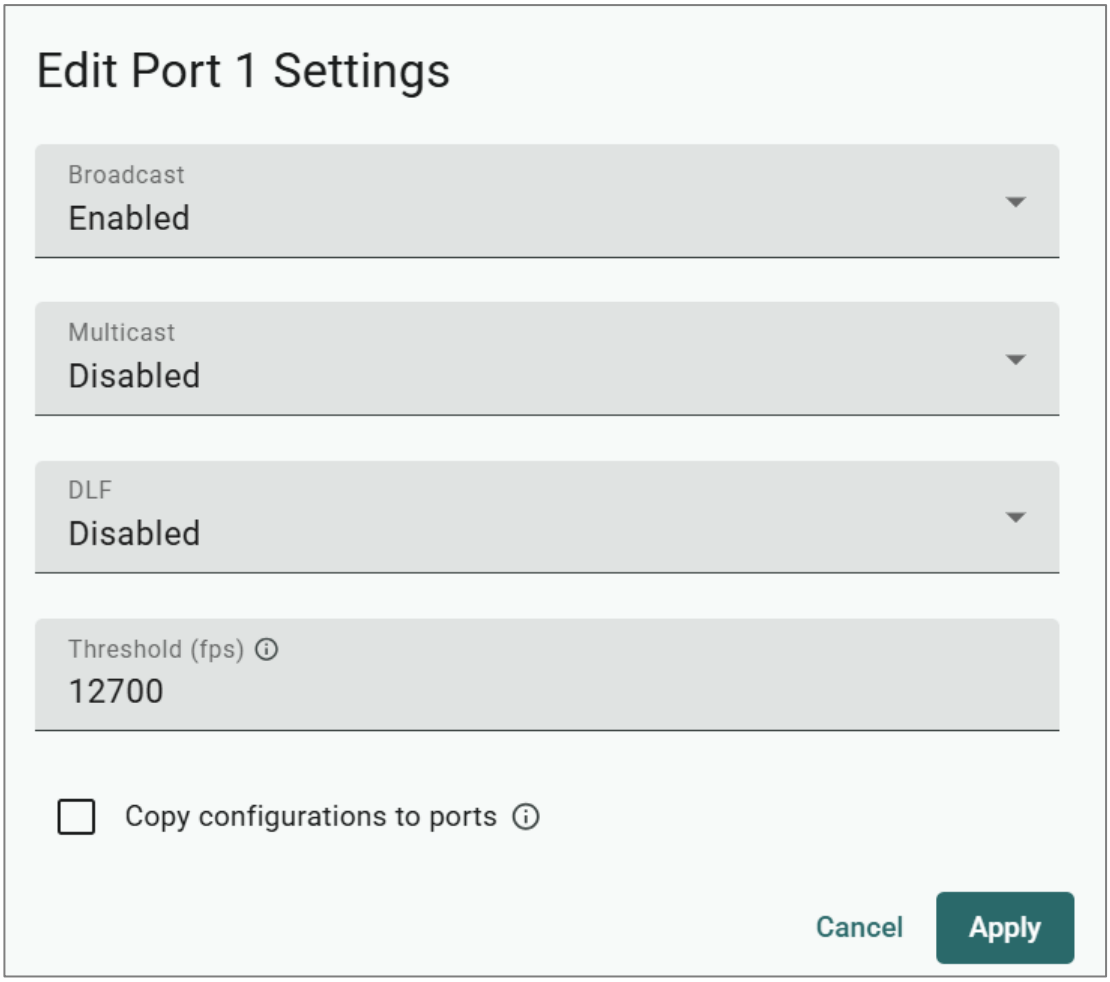
UI Setting	Description
Port	Shows the port number the entry is for.
Broadcast	Shows whether traffic storm control is enabled for broadcast packets for the port.
Multicast	Shows whether traffic storm control is enabled for multicast packets for the port.
DLF	Shows whether traffic storm control is enabled for DLF packets for the port.
Threshold	Shows the traffic storm threshold value in frames per second for the port.

Traffic Storm Control - Edit Port Settings

Menu Path: Security > Network Security > Traffic Storm Control

Clicking the **Edit (✎)** icon for a port on the **Security > Network Security > Traffic Storm Control** page will open this dialog box. This dialog lets you configure traffic storm control for the port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Broadcast	Enable or disable traffic storm control for broadcast packets for the port.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Multicast	Enable or disable traffic storm control for multicast packets for the port.	Enabled / Disabled	Disabled
DLF	Enable or disable traffic storm control for DLF packets for the port.	Enabled / Disabled	Disabled
Threshold	Specify the threshold in frames per second to reach before detecting a traffic storm for the port.	625 to 14881000	12700 fps
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

About Access Control Lists

Access Control Lists (ACLs) help you control network traffic based on specific criteria.

Here's an overview of some different kinds of ACLs:

- **Security:** ACLs provide a means to control access to network resources based on specific criteria such as source or destination IP addresses, MAC addresses, protocols, or port numbers. By implementing ACLs, you can enforce security policies and restrict unauthorized access to sensitive resources.
- **Traffic Management:** ACLs allow you to manage network traffic by selectively permitting or denying certain types of traffic. This helps optimize network performance by prioritizing critical traffic and controlling bandwidth usage.
- **Compliance:** In many industries, organizations are required to comply with security regulations and standards that mandate access control measures. By enabling ACLs, you can implement and demonstrate compliance with these requirements and mitigate security risks.
- **Protection Against Attacks:** ACLs can help protect networks against various types of attacks by blocking malicious traffic before it reaches its intended destination.
- **Preventing Unauthorized Access:** By implementing ACLs, you can prevent unauthorized users or devices from accessing network resources, reducing the risk of data breaches and unauthorized activities.

Overall, enabling ACLs enhances network security, improves traffic management, helps ensure compliance with regulations, and protects against various threats and attacks.

Access Control Lists In Depth

In an Ethernet switch, Access Control Lists (ACLs) work by examining incoming or outgoing packets and making decisions based on predefined rules. Each access list is a filter. When a packet enters into or exits from a switch, ACL will compare the packet to the rules in the access lists, starting from the first rule. If a packet is rejected or accepted by the first rule, the switch will drop or pass this packet directly without checking the rest of the lower-priority rules.

Here's how it typically works:

1. **Packet Inspection:** When a packet arrives at a switch port, the switch inspects the packet headers, including source and destination MAC addresses, IP addresses, and port numbers.
2. **ACL Lookup:** The switch compares the packet's header information against the ACL rules configured on the switch. These rules define which types of traffic are allowed or denied based on specific criteria such as MAC addresses, IP addresses, protocols, or port numbers.
3. **Decision Making:** Based on the ACL rules, the switch decides whether to permit or deny the packet. If the packet matches an ACL rule that permits the traffic, it is forwarded according to the switch's normal forwarding behavior. If the packet matches an ACL rule that denies the traffic, it is either dropped or forwarded to a specified destination, depending on the ACL configuration.
4. **Logging and Statistics:** Some switches may also provide logging and statistical features for ACLs, allowing administrators to monitor and analyze network traffic and ACL rule matches.

Overall, ACLs in Ethernet switches provide a mechanism for controlling access to network resources based on specific criteria, helping to enforce security policies and manage network traffic.

Access Control List

Menu Path: Security > Network Security > Access Control List

This page lets you configure the access control list and its related settings.

This page includes these tabs:

- Settings
- Status

Access Control List - Settings

Menu Path: Security > Network Security > Access Control List - Settings

This page lets you configure your device's access control lists.

> **Limitations**
> You can create up to 32 access lists.

Access Control List

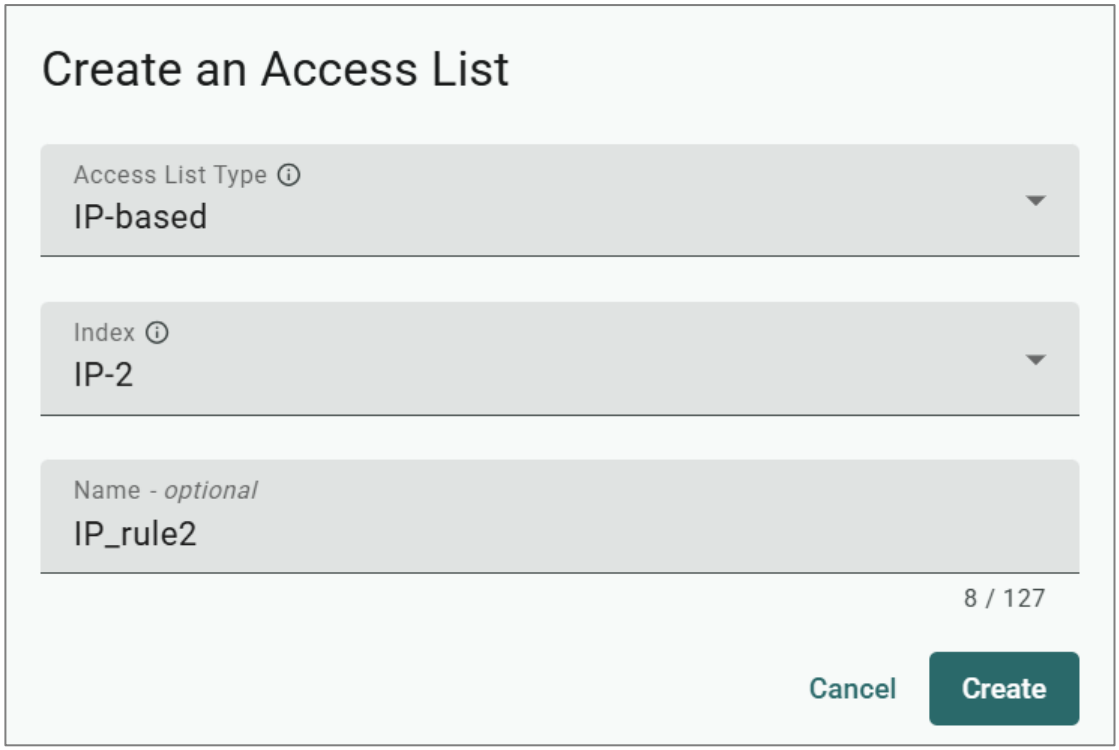
UI Setting	Description
Index	Shows the access list type and its index value.
Name	Shows the name of the access list.

Create an Access List

Menu Path: Security > Network Security > Access Control List - Settings

Clicking **Create** on the **Security > Network Security > Access Control List - Settings** page will open this dialog box. This dialog lets you create an access list.

Click **Create** to save your changes and add the new list.



UI Setting	Description	Valid Range	Default Value
Access List Type	Specify the access list type to determine how it should control access.	IP-based / MAC-based	N/A
Index	Specify an index value for the access list. **Note** Priority is determined by two factors: index value and address type. Lower index values indicate higher priority. In cases where entries share the same index, MAC addresses take precedence over IP addresses.	Drop-down list of index values	N/A
Name	Specify a name for the access list.	0 to 127 characters	N/A

ACL Table Settings

You can switch to another ACL table by clicking on its name.

UI Setting	Description	Valid Range	Default Value
Active Interface Type	Specify the active interface type for the ACL.	Port-based / VLAN-based	Port-based
Active Ingress Ports	Specify the active ingress ports for the ACL.	Drop-down list of ports	N/A
Active Egress Ports	Specify the active egress ports for the ACL.	Drop-down list of ports	N/A

ACL Rule List (MAC-based)

If the currently displayed ACL table is **MAC-based**, the following table will appear.

UI Setting	Description
Index	Shows the index number for the ACL rule.

UI Setting	Description
ACL Rule	Shows whether the ACL rule is enabled.
Rule Type	Shows the rule type.
EtherType	Shows the EtherType for the ACL rule.
Source	Shows the source MAC address with mask for the ACL rule.
Destination	Shows the destination MAC address with mask for the ACL rule.
VLAN ID	Shows the VLAN ID for the ACL rule.
CoS	Shows the CoS value used to prioritize packets for the ACL rule.
Action	Shows whether the redirect action or CoS remark are enabled for the ACL rule. If enabled, their respective configuration settings will be shown.

ACL Rule List (IP-based)

If the currently displayed ACL table is **IP-based**, the following table will appear.

UI Setting	Description
Index	Shows the index number for the ACL rule.
ACL Rule	Shows whether the ACL rule is enabled.
Rule Type	Shows the rule type.
Protocol	Show the protocol used for the ACL rule.
Source	Shows the source IP address with subnet mask for the ACL rule.
Destination	Shows the destination IP address with subnet mask for the ACL rule.
DSCP	Shows the DSCP value used to prioritize packets for the ACL rule.

UI Setting	Description
Optional Parameter	Show the relevant parameters for the selected protocol.
Action	Show whether the redirect action or DSCP remark are enabled. If enabled, their respective configuration settings will be shown.

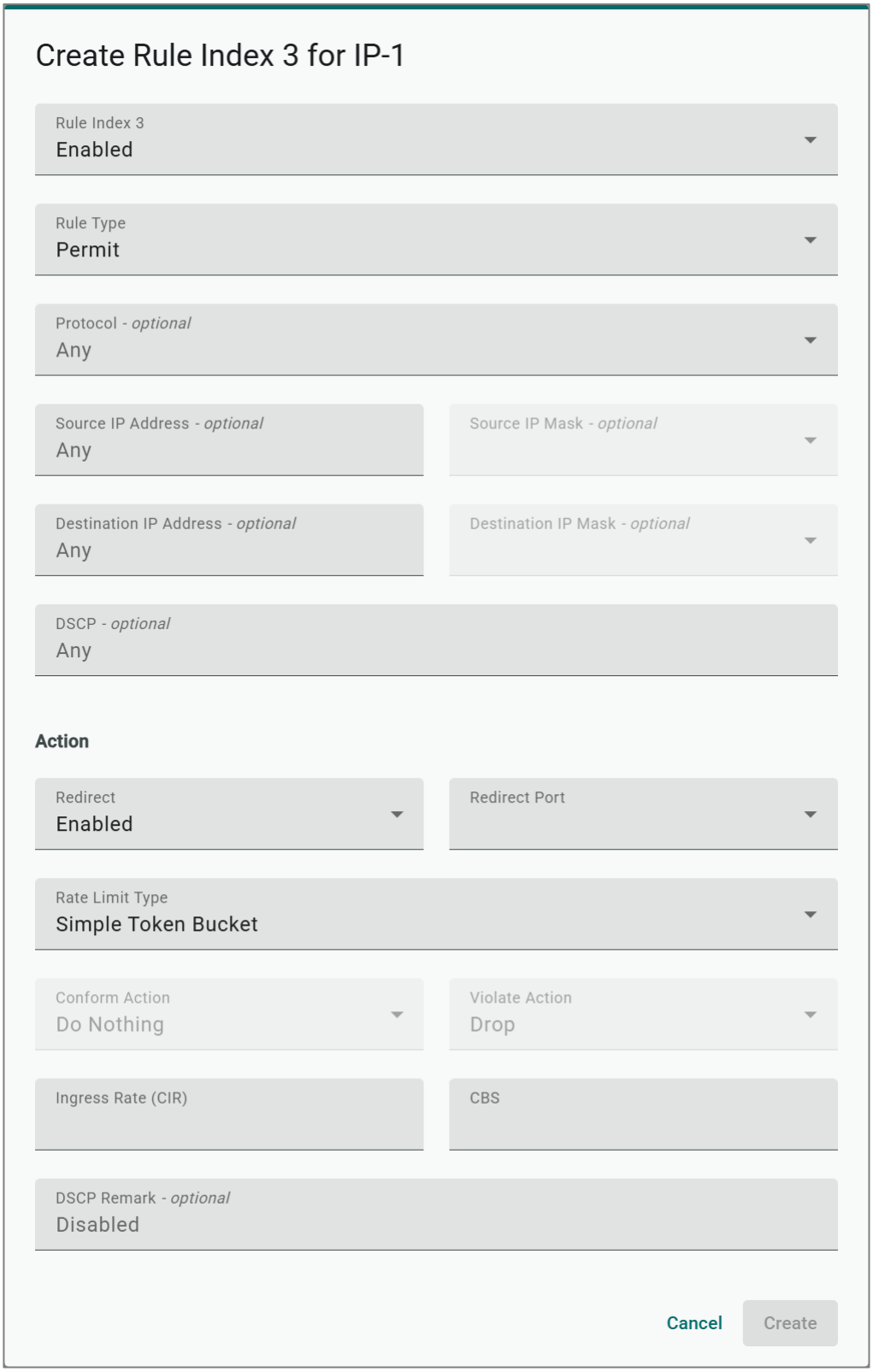
ACL Rule List - Create Rule

Menu Path: Security > Network Security > Access Control List - Settings

Clicking **Create** for an ACL table on the **Security > Network Security > Access Control List - Settings** page will open this dialog box. This dialog lets you create a rule for the displayed ACL table.

Click **Create** to save your changes and add the new rule.

If the currently displayed ACL table is **IP-based**, the following table will appear.


Create Rule Index 3 for IP-1
Rule Index 3
Enabled
Rule Type
Permit
Protocol - optional
Any
Source IP Address - optional
Any
Source IP Mask - optional
Destination IP Address - optional
Any
Destination IP Mask - optional
DSCP - optional
Any
Action
Redirect
Enabled
Redirect Port
Rate Limit Type
Simple Token Bucket
Conform Action
Do Nothing
Violate Action
Drop
Ingress Rate (CIR)
CBS
DSCP Remark - optional
Disabled
Cancel
Create

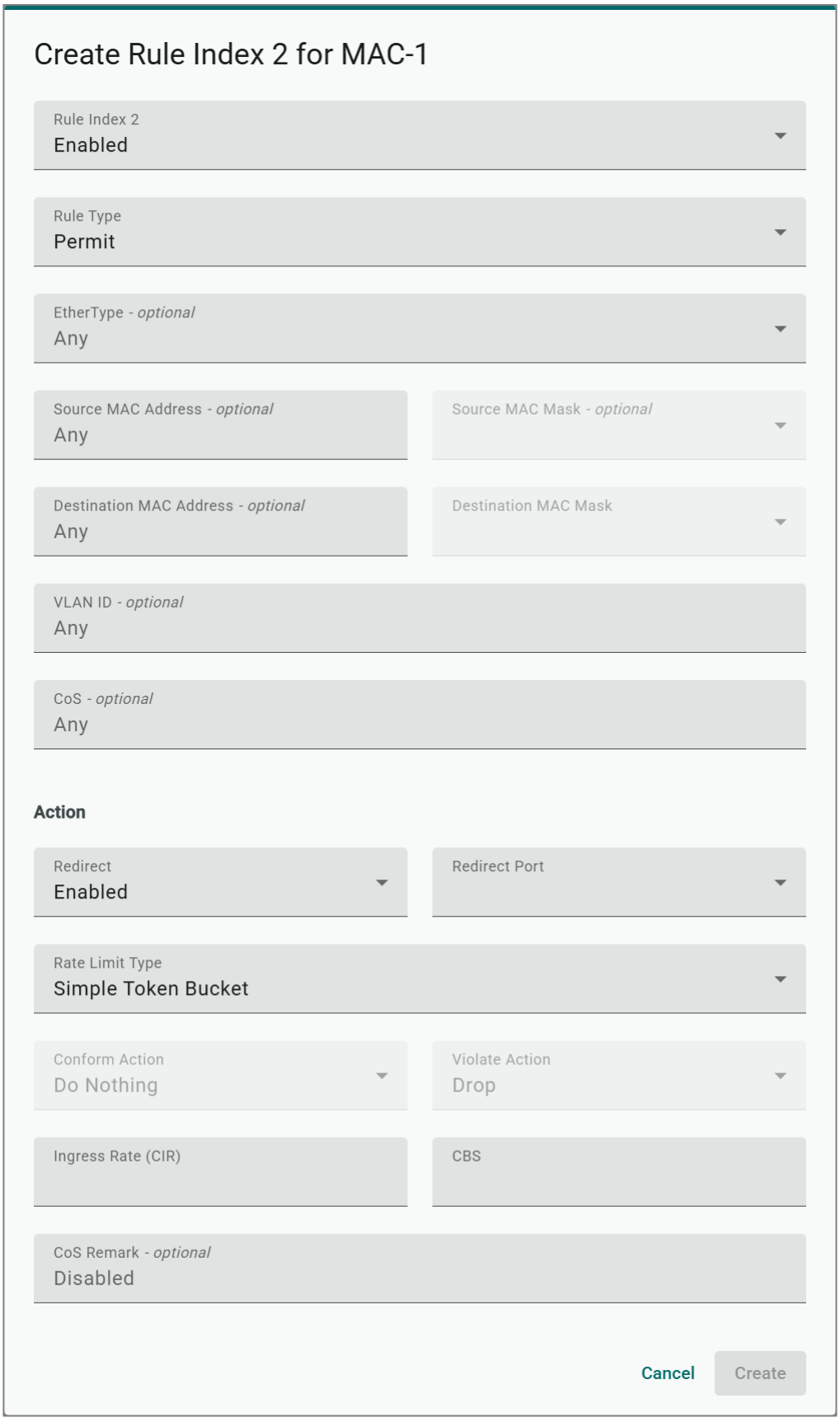
UI Setting	Description	Valid Range	Default Value
Rule Index	Enable or disable the rule.	Enabled / Disabled	Enabled
Rule Type	Specify the rule type.	Permit / Deny	N/A
Protocol	Specify the protocol for the ACL rule.	TCP / UDP / ICMP / IGMP / OSPF / User-defined	Any
ICMP Type **(If Protocol is ICMP)**	Specify the ICMP type for the rule. If this is blank, any type will apply.	0 to 255	Any
ICMP Code **(If Protocol is ICMP)**	Specify the ICMP code for the rule. If this is blank, any code will apply.	0 to 15	Any
IGMP Type **(If Protocol is IGMP)**	Specify the IGMP type for the rule. If this is blank, any type will apply.	0 to 255	Any
Protocol Number **(If Protocol is User-defined)**	Specify the protocol number for this rule.	0 to 255	N/A
Source IP Address	Specify the source IP address.	Valid IP address	Any
Source IP Mask	Specify the source IP subnet mask.	Drop-down list of subnet masks	N/A
Destination IP Address	Specify the destination IP address.	Valid IP address	Any
Destination IP Mask	Specify the destination IP subnet mask.	Drop-down list of subnet masks	N/A
DSCP	Specify a DSCP value to prioritize packets for the ACL rule.	0 to 63	Any

Action

These settings will appear if **Rule Type** is **Permit.**

UI Setting	Description	Valid Range	Default Value
Redirect	Enable or disable redirects.	Enabled / Disabled	Disabled
Redirect port **(If Redirect is Enabled)**	Specify the port to redirect packets to.		N/A
Rate Limit Type **(Only in Advanced Mode)**	Specify whether to enable rate limiting. Moxa switches provide Simple Token Bucket as a rate limit algorithm.	None / Simple Token Bucket	None
Conform Action **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	Shows the action to take for packets within the allowed average rate (CIR) and burst tolerance (CBS). This is fixed to Do Nothing.	Do Nothing	Do Nothing
Violate Action **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	Shows the action to take for packets that exceed the allowed average rate (CIR) and burst tolerance (CBS). This is fixed to Drop.	Drop	Drop
Ingress Rate(CIR) **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	1024 EBS (Excess Burst Size) (If Type is SrTCM) Specify the data buffer size in KB for the port when the data rate exceeds the CIR rate. Data that exceeds the CIR rate will be saved in the CBS buffer, and if the CBS buffer is full, data will be stored in the EBS buffer and will be sent when bandwidth is available.	1 to 1000	None
CBS **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	Specify the CBS (Committed Burst Size) data buffer size in KB for the port that can be used when the data rate exceeds the CIR rate. Data that exceeds the CIR rate will be saved in this buffer, and will be sent when bandwidth is available.	10 to 10240	None
DSCP Remark	Enable adding a DSCP remark by specifying a DSCP Remark value. To disable it, leave this blank.	0 to 63	Disabled

If the displayed ACL table is **MAC-based**, the following dialog will appear.


Create Rule Index 2 for MAC-1
Rule Index 2
Enabled
Rule Type
Permit
EtherType - optional
Any
Source MAC Address - optional
Any
Source MAC Mask - optional
Destination MAC Address - optional
Any
Destination MAC Mask
VLAN ID - optional
Any
CoS - optional
Any
Action
Redirect
Enabled
Redirect Port
Rate Limit Type
Simple Token Bucket
Conform Action
Do Nothing
Violate Action
Drop
Ingress Rate (CIR)
CBS
CoS Remark - optional
Disabled
Cancel
Create

UI Setting	Description	Valid Range	Default Value
Rule Index	Enable or disable the rule.	Enabled / Disabled	Enabled
Rule Type	Specify the rule type.	Permit / Deny	N/A
EtherType	Specify the EtherType for the ACL rule.	GOOSE / SMV / User-defined	Any
Source MAC Address	Specify a source MAC address.	Valid MAC address	Any
Source MAC Mask	Select a source MAC mask.	Drop-down list of MAC masks	N/A
Destination MAC Address	Specify a destination MAC address.	Valid MAC address	Any
Destination MAC Mask	Specify a destination MAC mask.	Drop-down list of MAC masks	N/A
VLAN ID	Specify the VLAN ID for the ACL rule.	1 to 4094	Any
CoS	Specify a CoS value to prioritize packets for the ACL rule.	0 to 7	Any

Action

These settings will appear if **Rule Type** is **Permit.**

UI Setting	Description	Valid Range	Default Value
Redirect	Enable or disable redirects.	Enabled / Disabled	Disabled
Redirect port **(If Redirect is Enabled)**	Specify the port to redirect packets to.		N/A
Rate Limit Type **(Only in Advanced Mode)**	Specify whether to enable rate limiting. Moxa switches provide Simple Token Bucket as a rate limit algorithm.	None / Simple Token Bucket	None

UI Setting	Description	Valid Range	Default Value
Conform Action **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	Shows the action to take for packets within the allowed average rate (CIR) and burst tolerance (CBS). This is fixed to Do Nothing.	Do Nothing	Do Nothing
Violate Action **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	Shows the action to take for packets that exceed the allowed average rate (CIR) and burst tolerance (CBS). This is fixed to Drop.	Drop	Drop
Ingress Rate(CIR) **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	1024 EBS (Excess Burst Size) (If Type is SrTCM) Specify the data buffer size in KB for the port when the data rate exceeds the CIR rate. Data that exceeds the CIR rate will be saved in the CBS buffer, and if the CBS buffer is full, data will be stored in the EBS buffer and will be sent when bandwidth is available.	1 to 1000	None
CBS **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	Specify the CBS (Committed Burst Size) data buffer size in KB for the port that can be used when the data rate exceeds the CIR rate. Data that exceeds the CIR rate will be saved in this buffer, and will be sent when bandwidth is available.	10 to 10240	None
DSCP Remark	Enable adding a DSCP remark by specifying a DSCP Remark value. To disable it, leave this blank.	0 to 63	Disabled

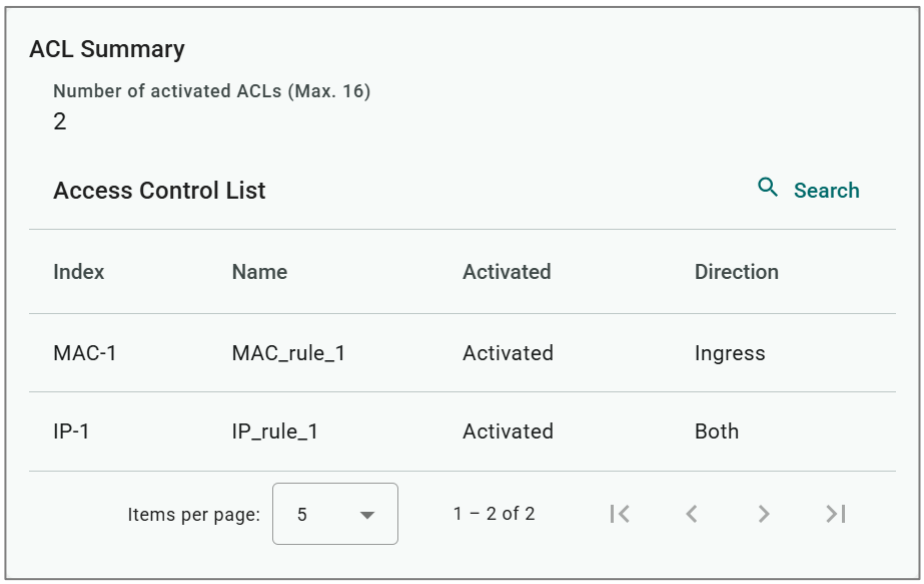
Access Control List - Status

Menu Path: Security > Network Security > Access Control List - Status

This page lets you view ACL status information for your device.

ACL Summary

When **View by ACL** is selected from the drop-down list, this information will appear.

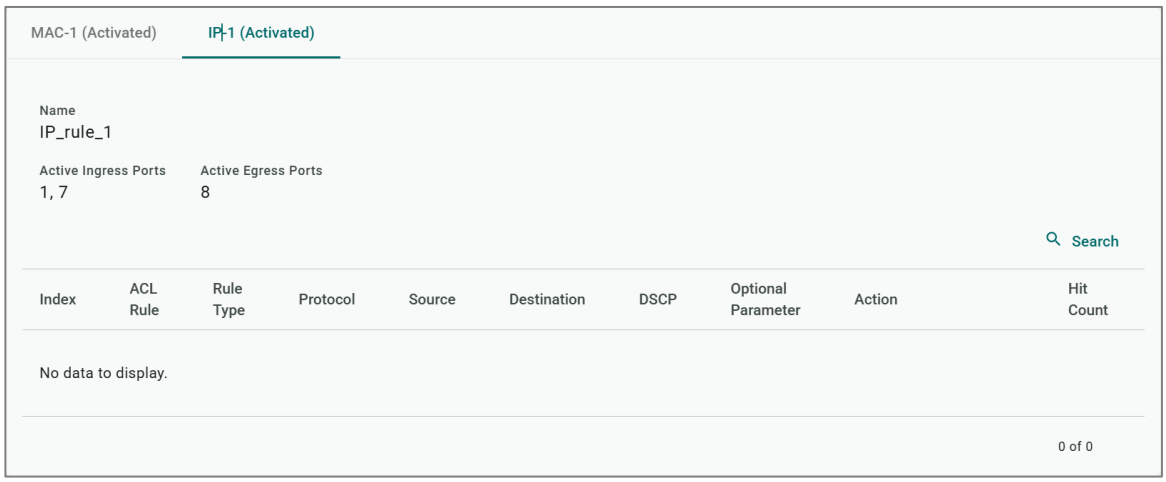


UI Setting	Description
Number of activated ACLs (Max. 16)	Shows the number of activated ACLs.
Index	Shows the ACL type and its index value.
Name	Shows the name of the ACL.
Activated	Shows whether the ACL is enabled.
Direction	Shows the direction of the ACL.

ACL Rule Status (by ACL, IP-based)

When **View by ACL** is selected from the drop-down list and the selected ACL is **IP-based**, the following table will appear.

You can view ACL rules for a different ACL by clicking on the ACL's name.



UI Setting	Description
Name	Shows the name of the access list.
Active Ingress Portss	Shows the active ingress ports configured for the ACL.
Active Egress Port	Shows the active egress ports configured for the ACL.
Index	Shows the index of the ACL rule.
ACL Rule	Shows whether the ACL rule is enabled.
Rule Type	Shows the rule type.
Protocol	Shows the protocol used for the ACL rule.
Source	Shows the source IP address with its subnet mask.
Destination	Shows the destination IP address with its subnet mask.
DSCP	Shows the DSCP value specified to differentiate the prioritization of IP packets.
Optional Parameter	Shows the relevant parameters for the selected protocol.
Action	Shows the redirect actions to take for this rule.
Hit Count	Shows the hit count of the ACL rule.

ACL Rule Status (by ACL, MAC-based)

When **View by ACL** is selected from the drop-down list and the selected ACL is **MAC-based**, the following table will appear.

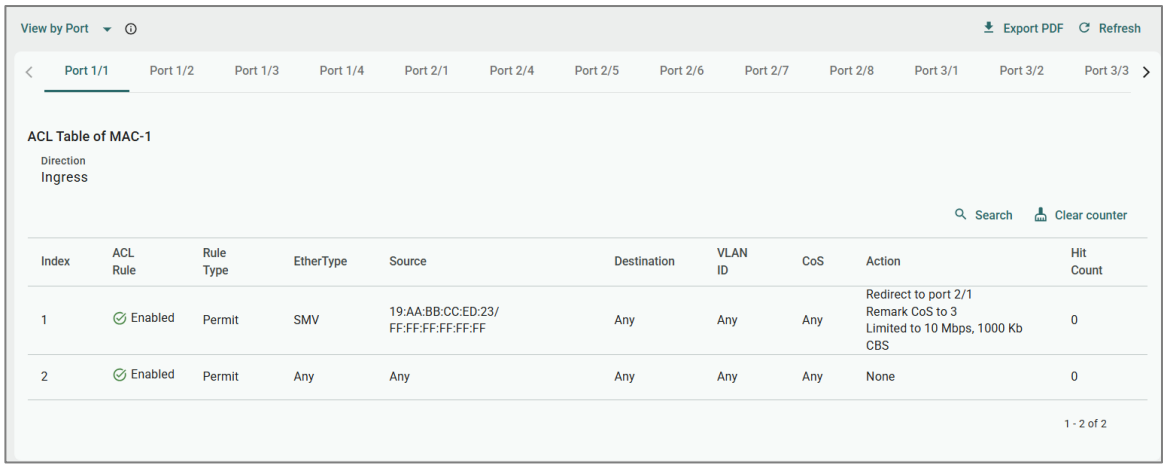
You can view ACL rules for a different ACL by clicking on the ACL's name.

UI Setting	Description
Name	Shows the name of the access list.
Active Ingress Ports	Shows the active ingress ports configured for the ACL.
Active Egress Ports	Shows the active egress ports configured for the ACL.
Index	Shows the index of the ACL rule.
ACL Rule	Shows whether the ACL rule is enabled.
Rule Type	Shows the rule type.
EtherType	Shows the EtherType used for the ACL rule.
Source	Shows the source MAC address with its mask.
Destination	Shows the destination MAC address with its mask.
VLAN ID	Shows the VLAN ID.
CoS	Shows the CoS value specified to differentiate the prioritization of packets.
Action	Shows the redirect actions to take for this rule.
Hit Count	Shows the hit count of the ACL rule.

ACL Rule Status (by Port)

When **View by Port** is selected from the drop-down list, the following information will appear.

You can view ACL rules for a specific port by clicking on the port's name.



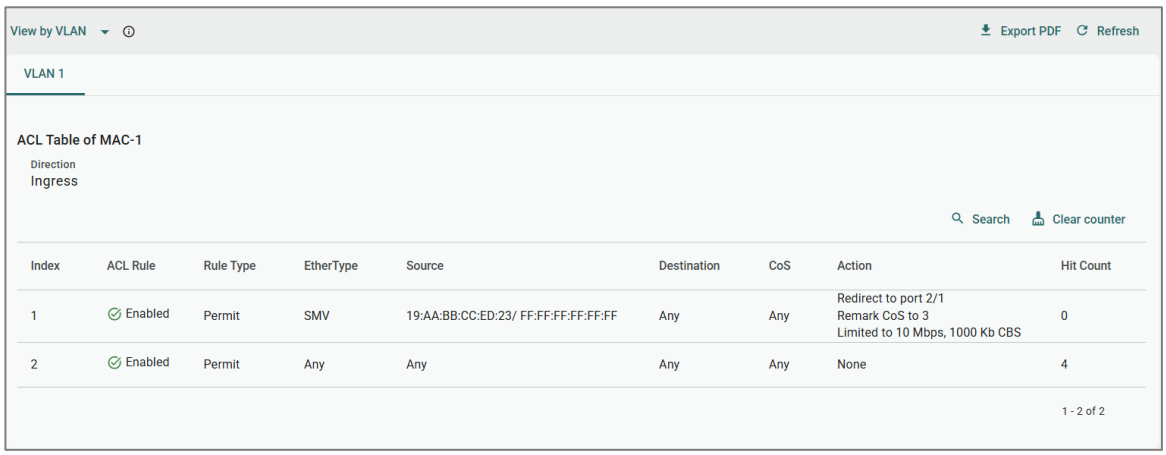
UI Setting	Description
Direction	Shows the direction of the relevant ACL for this port.
Index	Shows the index of the ACL rule.
ACL Rule	Shows whether the ACL rule is enabled.
Rule Type	Shows the rule type.
EtherType **(If relevant ACL is MAC-based)**	Shows the EtherType used for the ACL rule.
Protocol **(If relevant ACL is IP-based)**	Shows the Protocol used for the ACL rule.
Source	Shows the source IP or MAC address with its mask.
Destination	Shows the destination IP or MAC address with its mask.

UI Setting	Description
VLAN ID **(If relevant ACL is MAC-based)**	Shows the VLAN ID.
CoS **(If relevant ACL is MAC-based)**	Shows the CoS value specified to differentiate the prioritization of packets.
DSCP **(If relevant ACL is IP-based)**	Shows the DSCP value specified to differentiate the prioritization of packets.
Optional Parameter **(If relevant ACL is IP-based)**	Shows the relevant parameters for the selected EtherType/Protocol.
Action	Shows the actions to take for the ACL rule.
Hit Count	Shows the hit count of the ACL rule.

ACL Rule Status (by VLAN)

When **View by VLAN** is selected from the drop-down list, the following information will appear.

You can view ACL rules for a specific VLAN by clicking on the VLAN's name.



UI Setting	Description
Direction	Shows the direction of the relevant ACL for this VLAN.
Index	Shows the index of the ACL rule.
ACL Rule	Shows whether the ACL rule is enabled.
Rule Type	Shows the rule type.
EtherType **(If relevant ACL is MAC-based)**	Shows the EtherType used for the ACL rule.
Protocol **(If relevant ACL is IP-based)**	Shows the Protocol used for the ACL rule.
Source	Shows the source IP or MAC address with its mask.
Destination	Shows the destination IP or MAC address with its mask.
VLAN ID **(If relevant ACL is MAC-based)**	Shows the VLAN ID.
CoS **(If relevant ACL is MAC-based)**	Shows the CoS value specified to differentiate the prioritization of packets.
DSCP **(If relevant ACL is IP-based)**	Shows the DSCP value specified to differentiate the prioritization of packets.
Optional Parameter **(If relevant ACL is IP-based)**	Shows the relevant parameters for the selected EtherType/Protocol.
Action	Shows the actions to take for the ACL rule.
Hit Count	Shows the hit count of the ACL rule.

About Network Loop Protection

Network Loop Protection helps avoid network loops by disabling ports when looping is detected in the network topology. This is designed for devices that do not support

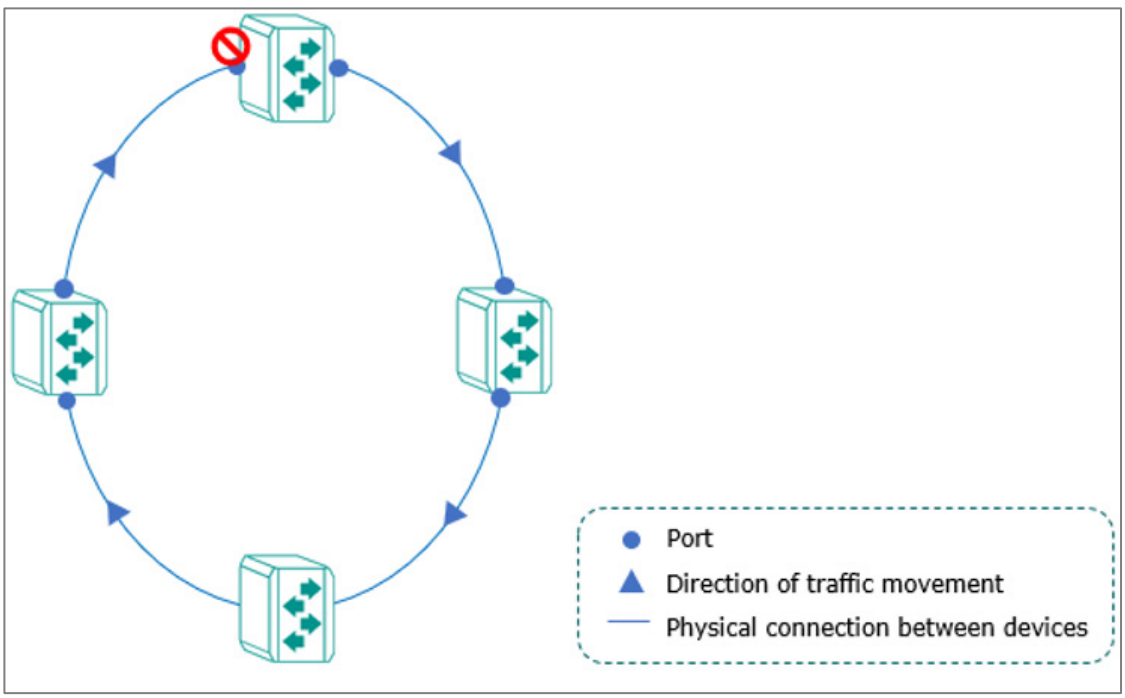
redundant protocols, when redundant protocols are not configured, or if the redundant protocol fails.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

Network Loop Protection In Depth

Network Loop Protection prevents looping by sending detection packets through the network topology to all ports. After receiving a packet, a port will check if the packet was sent by the device itself. If so, the receiving port will be disabled to prevent looping.

Network loop protection features cannot prevent ports from activating redundancy protocols–such as STP, RSTP, MSTP, Turbo Ring, Ring Coupling, Turbo Chain, Dual Homing, or Link Aggregation–from looping, as these ports do not process detection packets sent by the Network Loop Protection features.



Network Loop Protection

Menu Path: Security > Network Security > Network Loop Protection

This page lets you manage network loop protection for your device.

This page includes these tabs:

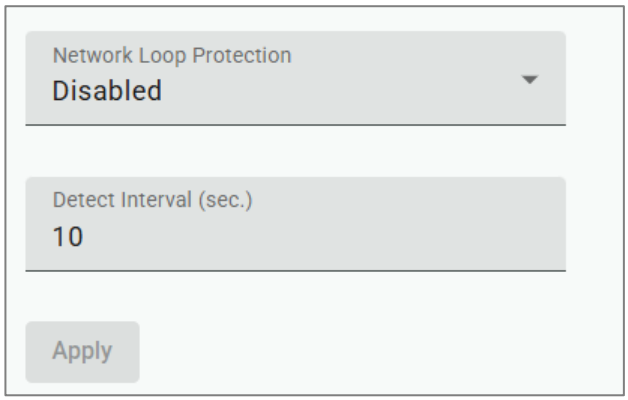
- Settings
- Status

Network Loop Protection - Settings

Menu Path: Security > Network Security > Network Loop Protection - Settings

This page lets you enable network loop protection settings.

Network Loop Protection Settings



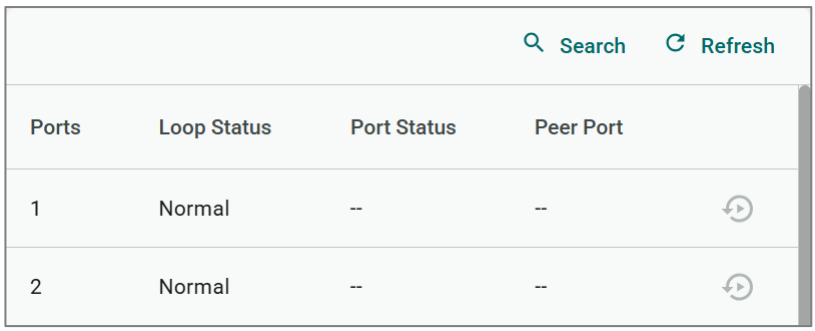
UI Setting	Description	Valid Range	Default Value
Network Loop Protection	Enable or disable the network loop protection.	Enabled / Disabled	Disabled
Detect Interval	Specify the detect interval in seconds.	1 to 30	10

Network Loop Protection - Status

Menu Path: Security > Network Security > Network Loop Protection - Status

This page lets you view the status of network loop protection.

Network Loop Protection - Port List



UI Setting	Description
Ports	Shows the port number the entry is for.
Loop Status	Shows the loop status of the port. • **Normal**: The port is not looping. • **Looping**: The port is looping.
Port Status	Shows the port status of the port. • **Disabled**: The port is disabled due to a port shutdown or detected loop.
Peer Port	Shows the port where the looping frames are from when detecting a loop.

About Binding Databases

A binding database acts as an allowlist for IP Source Guard and Dynamic ARP Inspection to help protect against unauthorized traffic.

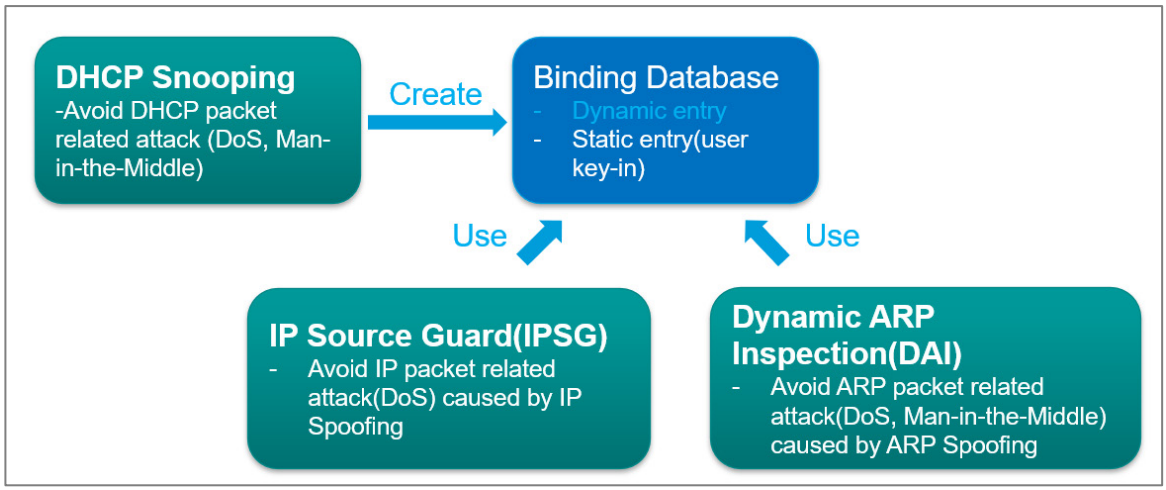
Binding Databases In Depth

A binding database consists of dynamic entries and static entries.

- **Dynamic Entries**: Generated automatically after a DHCP client successfully obtains an IP while DHCP snooping is enabled. The entry will be released after exceeding the IP lease time or upon disabling DHCP snooping.

- **Static Entries**: User-generated/edited entry. The entry will be released only when a user deletes it.

Binding database entries consist of VLAN IDs, MAC addresses, ports, and IP addresses. This information forms an allowlist used by IP Source Guard to filter IP packets, and for Dynamic ARP Inspection to filter ARP packets. This helps prevent spoofing attacks such as man-in-the-middle and denial-of-service attacks.



Configuring Binding Database

Binding Database is the base for IP Source Guard and Dynamic ARP Inspection, there are two ways to populate Binding Database entries, including entries automatically created after enabling DHCP Snooping or manually entries created by users.

Before you begin:

- Determine which kind of Binding Database Entries to use: Static, or Dynamic. See above for guidelines to make this determination.

Configuring Dynamic Binding Database Entries

To configure a Dynamic Binding Database entry:

1. Go to **Security > Network Security > DHCP Snooping.**
2. Click DHCP Snooping and then select Enable, optionally specify a VLAN ID, and then click Apply.

3. Under Port Settings, click **Edit (✎)**to configure the corresponding port binding settings.
4. Configure the following:
   ● **Status● Copy configurations to ports**
5. Click **Apply**

Results: The Binding Database entries will be created upon a successful DHCP transaction on DHCP Snooping-enabled Untrusted ports. You can view the binding database entries by going to **Security > Network Security > Binding Database > Binding Status.**

Configuring Static Binding Database Entries

To configure a Static Binding Database Entry:

1. Go to **Security > Network Security > Binding Database.> Binding Setting.**
2. Click (Add), and then specify all of the following:
   ● **VLAN ID● MAC Address● Port● IP Address**
3. Click **Create** to add the entry to the database.

Results: The Binding Database entries will be created upon a successful DHCP transaction on DHCP Snooping-enabled Untrusted ports. You can view the binding database entries by going to **Security > Network Security > Binding Database > Binding Status.**

Binding Database

Menu Path: Security > Network Security > Binding Database

This page lets you view and manage the binding database, which can be used for an allowlist for IP Source Guard or Dynamic ARP Inspection.

This page includes these tabs:

- Binding Settings
- Binding Status

Limitations

You can create up to 32 binding database entries, including dynamic and static entries. Entries will stop being generated or being user-addable when the this limit is reached. More entries can only be added when existing entries are released, bringing the total number below 32.

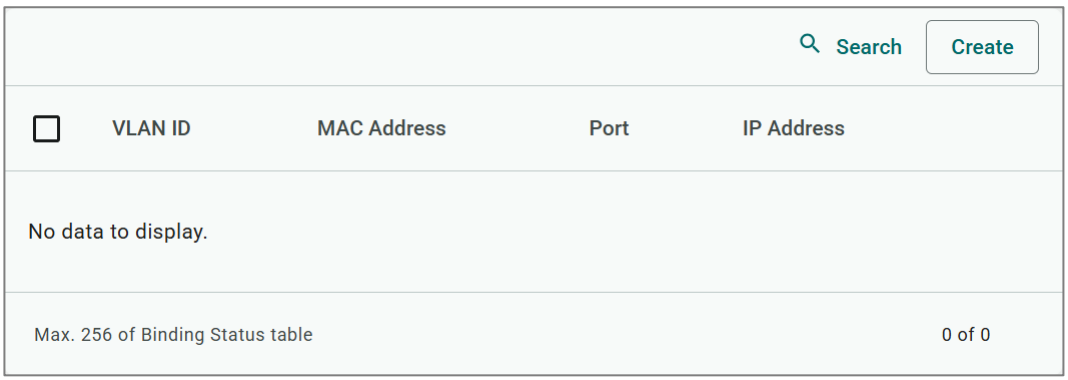
Binding Settings

Menu Path: Security > Network Security > Binding Database - Binding Settings

This page lets you manage the static entries you want to use for an allowlist.

Binding Database Static Entry List

This list shows the user-configured static entries for the binding database. These entries can be used as an allowlist base for IP Source Guard and Dynamic IP Inspection.



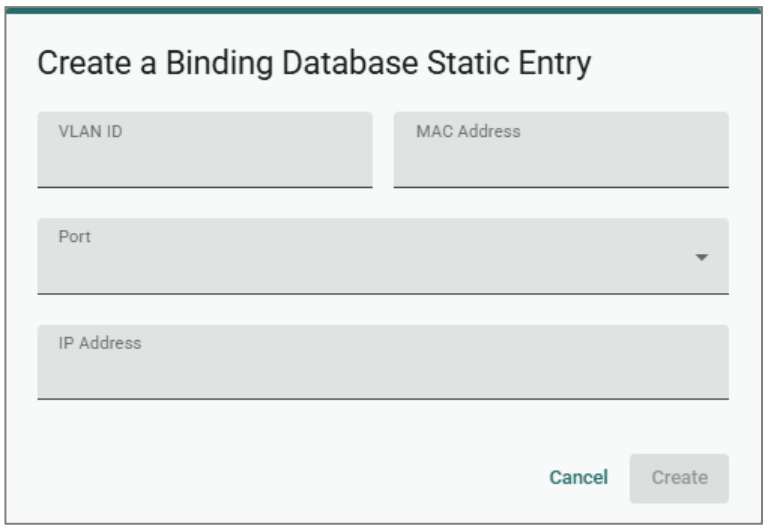
UI Setting	Description
VLAN ID	Shows the VLAN ID for the static entry.
MAC Address	Shows the MAC address for the static entry.
Port	Shows the port for the static entry.
IP Address	Shows the IP address for the static entry.

Create a Binding Database Static Entry

Menu Path: Security > Network Security > Binding Database - Binding Settings

Clicking **Create** on the **Security > Network Security > Binding Database - Binding Settings** page will open this dialog box. This dialog lets you add a new static entry to be an allowlist base for IP Source Guard or Dynamic ARP Inspection.

Click **Create** to save your changes and add the new entry.



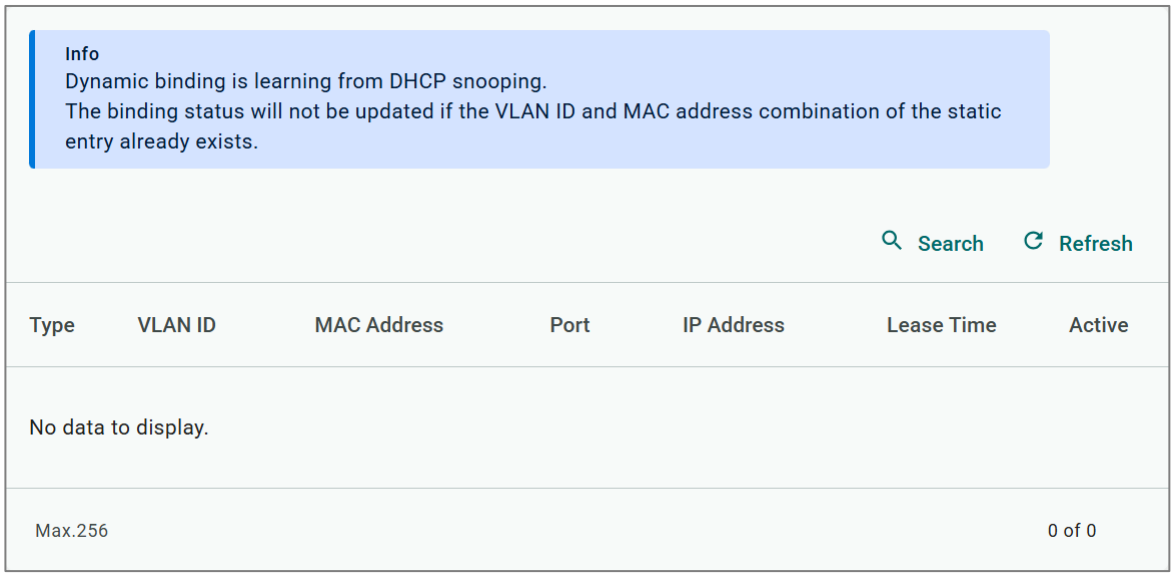
UI Setting	Description	Valid Range	Default Value
VLAN ID	Specify the VLAN ID to allowlist for the static entry.	1 to 4094	N/A
MAC Address	Specify the MAC address to allowlist for the static entry.	Valid MAC address	N/A
Port	Specify the port to allowlist for the static entry.	Drop-down list of ports	N/A
IP Address	Specify the IP address to allowlist for the static entry.	Valid IP address	N/A

Binding Status

Menu Path: Security > Network Security > Binding Database - Binding Status

This page lets you view the current binding database entries of your device.

Binding Status List



UI Setting	Description
Type	Shows the type of entry.
VLAN ID	Shows the VLAN ID for a successful DHCP packet transaction on an untrusted port, or the specified VLAN ID for a user-created static entry.
MAC Address	Shows the MAC address for a successful DHCP packet transaction on an untrusted port, or the specified MAC address for a user-created static entry.
Port	Shows the untrusted port for a successful DHCP packet transaction, or the specified port for a user-created static entry.
IP Address	Shows the IP address for a successful DHCP packet transaction on an untrusted port, or the specified IP address for a user-created static entry.
Lease Time	Shows the lease time for the entry to be active. The lease time is infinite for user-created static entries.
Active	Shows whether the entry is active for use with IP Source Guard, Dynamic ARP Inspection, or both.

About DHCP Snooping

DHCP Snooping is a VLAN-specific security feature for DHCP operations. You can configure untrusted hosts and trusted DHCP servers for corresponding ports on your

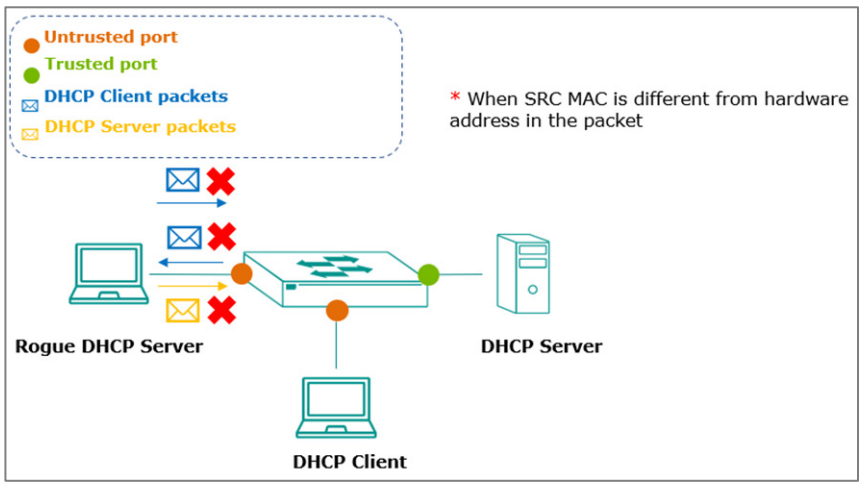
device, and then the feature will act like a firewall to validate DHCP messages received from untrusted sources and filter out invalid messages to exclude rogue DHCP servers and remove malicious DHCP traffic. This helps guarantee that clients obtain a legal address from the DHCP server you designate.

Enabling DHCP snooping will also set up a binding database, which will act as an allowlist for IP Source Guard and Dynamic ARP Inspection.

DHCP Snooping In Depth

By configuring the designated ports connected to DHCP server ports as trusted ports, and ports connected to clients/hosts as untrusted ports:

- Trusted ports will allow all DHCP packets.
- Untrusted ports will handle DHCP packets as follows:
    a. Pass ingress DHCP client packets and egress DHCP server packets to complete normal DHCP transactions.
    b. Drop egress DHCP client packets and ingress DHCP server packets to avoid rogue DHCP server attacks.
    c. Drop DHCP client packets with a different source MAC address and hardware address to avoid malicious DHCP client attacks.



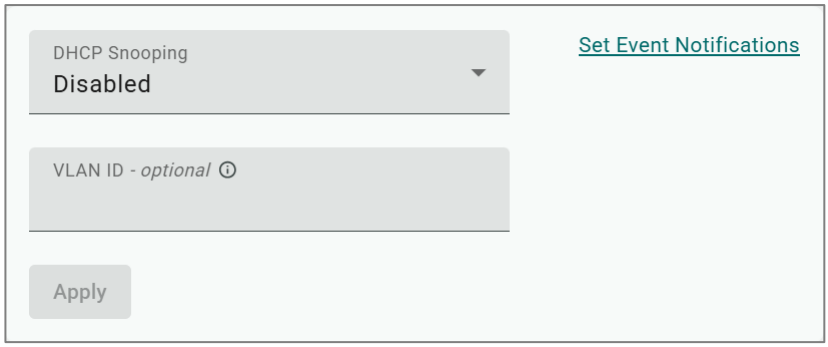
Successful DHCP transactions with DHCP snooping enabled will create and update the binding database. The binding database contains VLAN IDs, MAC addresses, untrusted ports of DHCP clients, and IP addresses. The binding database can also be used for other security functions such as IP Source Guard and Dynamic ARP Inspection.

DHCP Snooping

Menu Path: Security > Network Security > DHCP Snooping

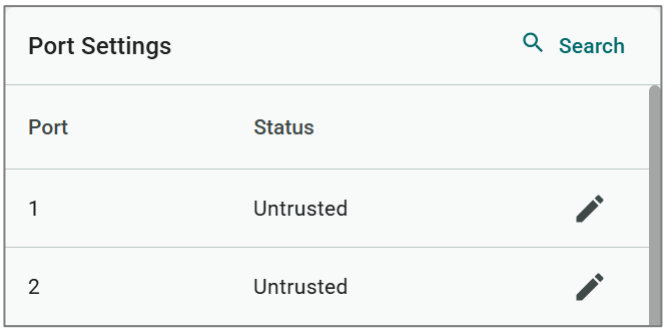
This page lets you manage DHCP Snooping for your device.

DHCP Snooping Settings



UI Setting	Description	Valid Range	Default Value
DHCP Snooping	Enable or disable DHCP snooping.	Enabled / Disabled	Disabled
VLAN ID	Specify the VLAN IDs to use for DHCP snooping. You can enter multiple VLAN IDs by separating them with commas or by using ranges (e.g., 2, 4-8, 10-13).	1 to 4094	N/A

DHCP Snooping - Port Settings



UI Setting	Description
Port	Shows the port number the entry is for.

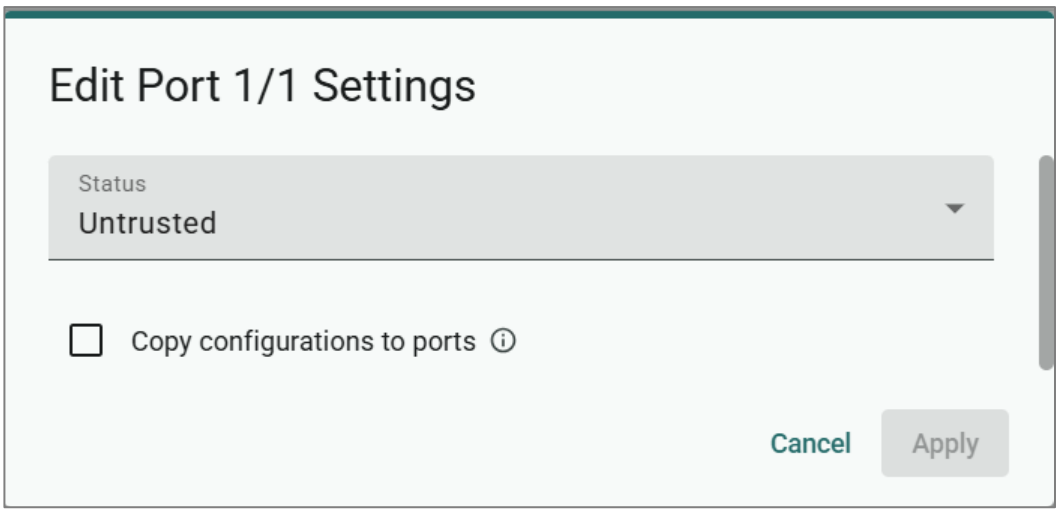
UI Setting	Description
Status	Shows whether the port is trusted or untrusted.

DHCP Snooping - Edit Port Settings

Menu Path: Security > Network Security > DHCP Snooping

Clicking the **Edit (✎)** icon for a port on the **Security > Network Security > DHCP Snooping** page will open this dialog box. This dialog lets you configure the port as trusted or untrusted for DHCP snooping.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Specify the port as untrusted or trusted.	Untrusted / Trusted	Untrusted
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

About IP Source Guard

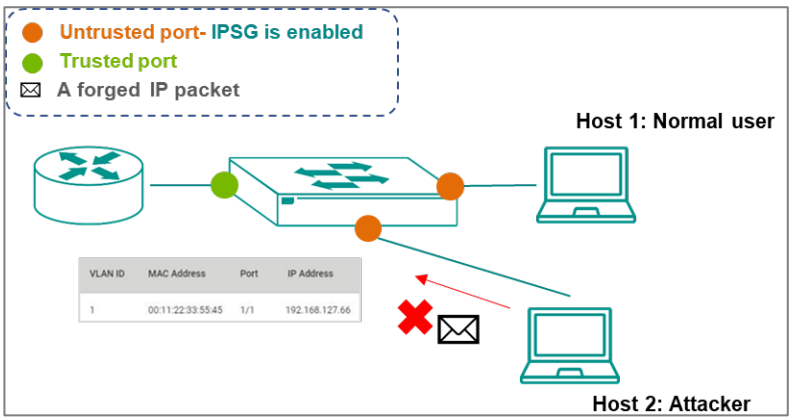
IP Source Guard (IPSG) is an IP data packet filtering security feature that works on Layer 2 interfaces. It works together with DHCP Snooping and the Binding Database to filter IP

data packets to defend against attacks such as denial-of-service (DoS) that are caused by forging/spoofing source IP addresses.

IP Source Guard In Depth

IPSG checks all traffic to make sure its host IP address, MAC address, VLAN, and port match a valid entry in the binding database. If the host does not match a valid entry in the binding database, the traffic will not be forwarded.

> **Note**
>
> IP Source Guard (IPSG) works with DHCP snooping, so DHCP snooping must be enabled to create binding database entries before enabling IPSG
>
> IPSG can only be used on ports specified as "untrusted" for DHCP snooping.

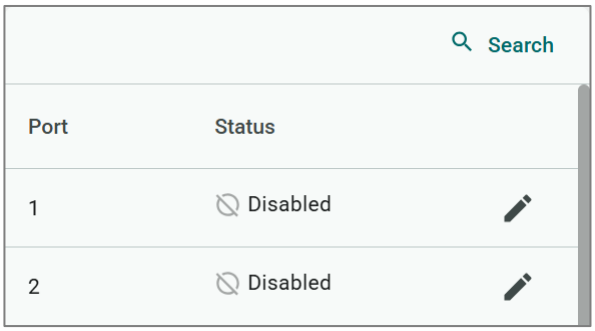


IP Source Guard

Menu Path: Security > Network Security > IP Source Guard

This page lets you enable or disable IP Source Guard for each port.

IP Source Guard Port List



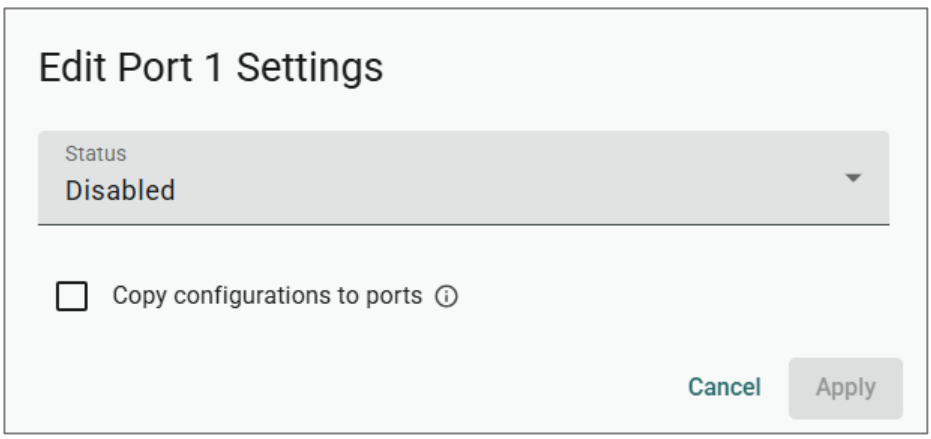
UI Setting	Description
Port	Shows the port number the entry is for.
Status	Shows whether IP Source Guard is enabled for the port.

IP Source Guard - Edit Port Settings

Menu Path: Security > Network Security > IP Source Guard

Clicking the **Edit (✎)** icon for a port on the **Security > Network Security > IP Source Guard** page will open this dialog box. This dialog lets you enable or disable IP Source Guard for the port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable IP Source Guard for the port. When enabled, only traffic with packet headers that have a source IP and MAC address that match a valid entry in the Binding Database will be forwarded. **Note** IP Source Guard can only be enabled on ports specified as untrusted in DHCP snooping.	Enabled / Disabled	Disabled
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

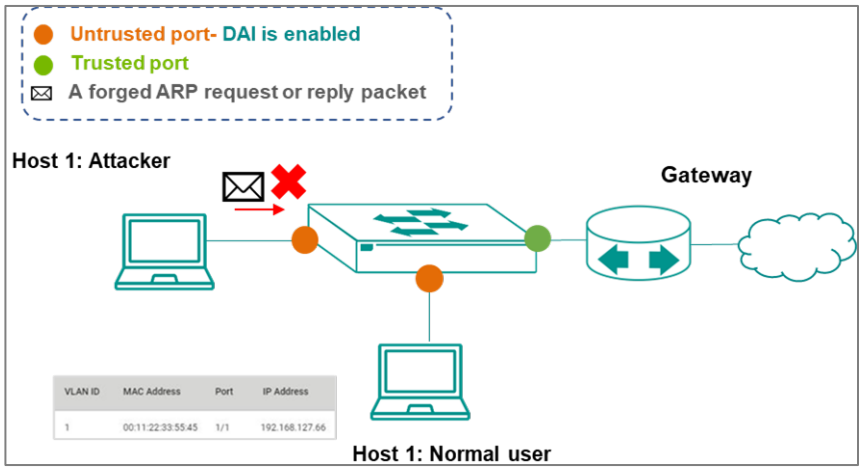
About Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is an ARP packet filtering security feature that works on Layer 2 interfaces. It works together with DHCP snooping and the binding database to help defend against attacks such as man-in-the-middle or denial-of-service (DoS) attacks caused by ARP packet spoofing (also known as ARP poisoning or ARP cache poisoning).

Dynamic ARP Inspection In Depth

Dynamic ARP Inspection (DAI) works with DHCP Snooping. Users must enable DHCP snooping to create Binding Database entries before enabling DAI, and DAI can only be used on ports specified as untrusted DHCP Snooping.

DAI inspects each ARP packet sent from a host attached to an untrusted port on the switch. The IP address, MAC address, VLAN, and port associated with the host are checked against entries stored in the Binding Database. If the host information does not match a valid entry in the Binding Database, the ARP packet will not be forwarded.

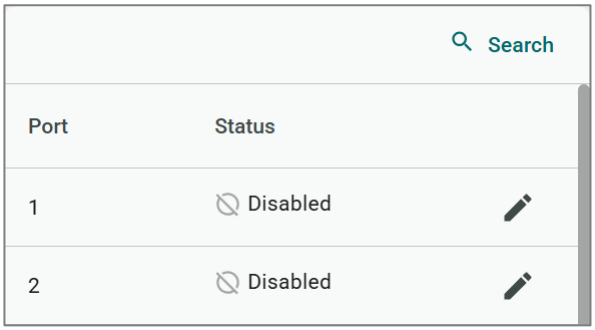


Dynamic ARP Inspection

Menu Path: Security > Network Security > Dynamic ARP Inspection

This page lets you enable or disable Dynamic ARP Inspection for each port.

Dynamic ARP Inspection List



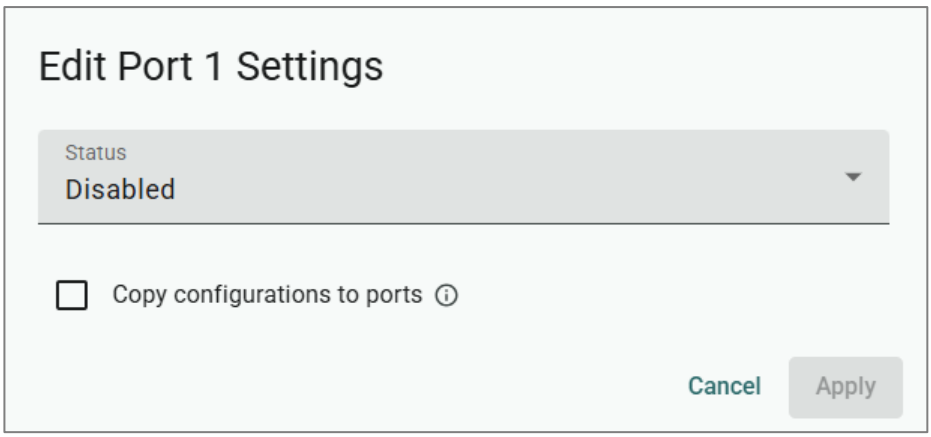
UI Setting	Description
Port	Shows the port number the entry is for.
Status	Shows whether Dynamic ARP Inspection is enabled for the port. **Note** Dynamic ARP Inspection can only be enabled on ports specified as untrusted in DHCP snooping.

Dynamic ARP Inspection - Edit Port Settings

Menu Path: Security > Network Security > Dynamic ARP Inspection

Clicking the **Edit (✎)** icon for a port on the **Security > Network Security > Dynamic ARP Inspection** page will open this dialog box. This dialog lets you enable or disable Dynamic ARP Inspection for the port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable Dynamic ARP Inspection for the port. When enabled, ARP packets are inspected, and only ARP packets that have a source IP and MAC address that match a valid entry in the Binding Database will be forwarded. ✎ **Note** Dynamic ARP Inspection can only be enabled on ports specified as untrusted in DHCP snooping.	Enabled / Disabled	Disabled
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

Authentication

Menu Path: Security > Authentication

This section lets you manage the authentication features of your device.

This section includes these pages:

- Login Authentication
- RADIUS
- TACACS+

About Login Authentication

Your device can authenticate user logins to protect against unauthorized access to your device.

How Login Authentication Works

Your device has three different methods of authenticating user logins:

- TACACS+ (Terminal Access Controller Access-Control System Plus)
- RADIUS (Remote Authentication Dial In User Service)
- Local database

TACACS+ and RADIUS are centralized "AAA" (Authentication, Authorization, and Accounting) systems for connecting to network services. The fundamental purpose of these is to provide an efficient and secure mechanism for user account management.

You can use different combinations of these authentication methods:

1. **TACACS+, Local:** Check the TACACS+ database first. If checking the TACACS+ database fails, then check the local database.
2. **RADIUS, Local:** Check the RADIUS database first. If checking the RADIUS database fails, then check the local database.
3. **TACACS+:** Only check the TACACS+ database.
4. **RADIUS:** Only check the RADIUS database.
5. **Local:** Only check the local database.

Login Authentication

Menu Path: Security > Authentication > Login Authentication

This page lets you select the login authentication protocol for your device.

Login Authentication Settings

Note

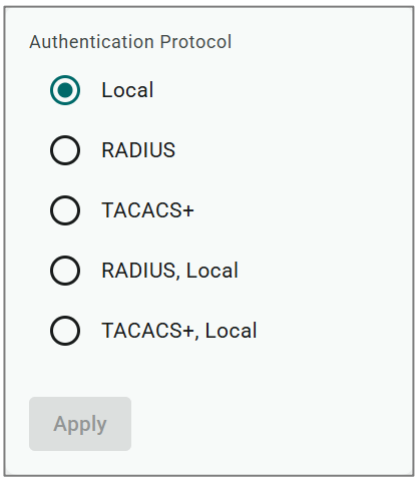
The account privilege level will be granted based on the service type setting for the user for RADIUS authentication, and the privilege level for the user for TACACS+ authentication.

RADIUS Service Type

- 6: Administrator
- 3: Supervisor
- All other values (1, 2, 4, 5, 7, 8, 9, 10, 11): User

TACACS+ Privilege Level

- 15: Administrator
- 12: Supervisor
- 1: User



UI Setting	Description	Valid Range	Default Value
Authentication Protocol	Select the login authentication protocol to use for your device. • **Local:** Only the local database will be checked for login authentication. • **RADIUS:** Only the RADIUS database will be checked for login authentication. • **TACACS+**: Only the TACACS+ database will be checked for login authentication. • **RADIUS, Local**: The RADIUS database will be checked first for login authentication. If checking the RADIUS database fails, then the local database will be checked. • **TACACS+, Local**: The TACACS+ database will be checked first for login authentication. If checking the TACACS+ database fails, then the local database will be checked.	Local / RADIUS / TACACS+ / RADIUS, Local / TACACS+, Local	Local

RADIUS

RADIUS, or Remote Authentication Dial-In User Service, acts like a central security checkpoint for your network. It verifies the identities of users and devices trying to connect, ensuring only authorized ones gain access. Imagine it as a doorman for your switch – RADIUS checks credentials and grants permission to enter the network, enhancing overall security. This centralized approach simplifies user management and eliminates the need for individual security configurations on each device. RADIUS is particularly useful for businesses with many users, devices, or remote access needs.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

RADIUS

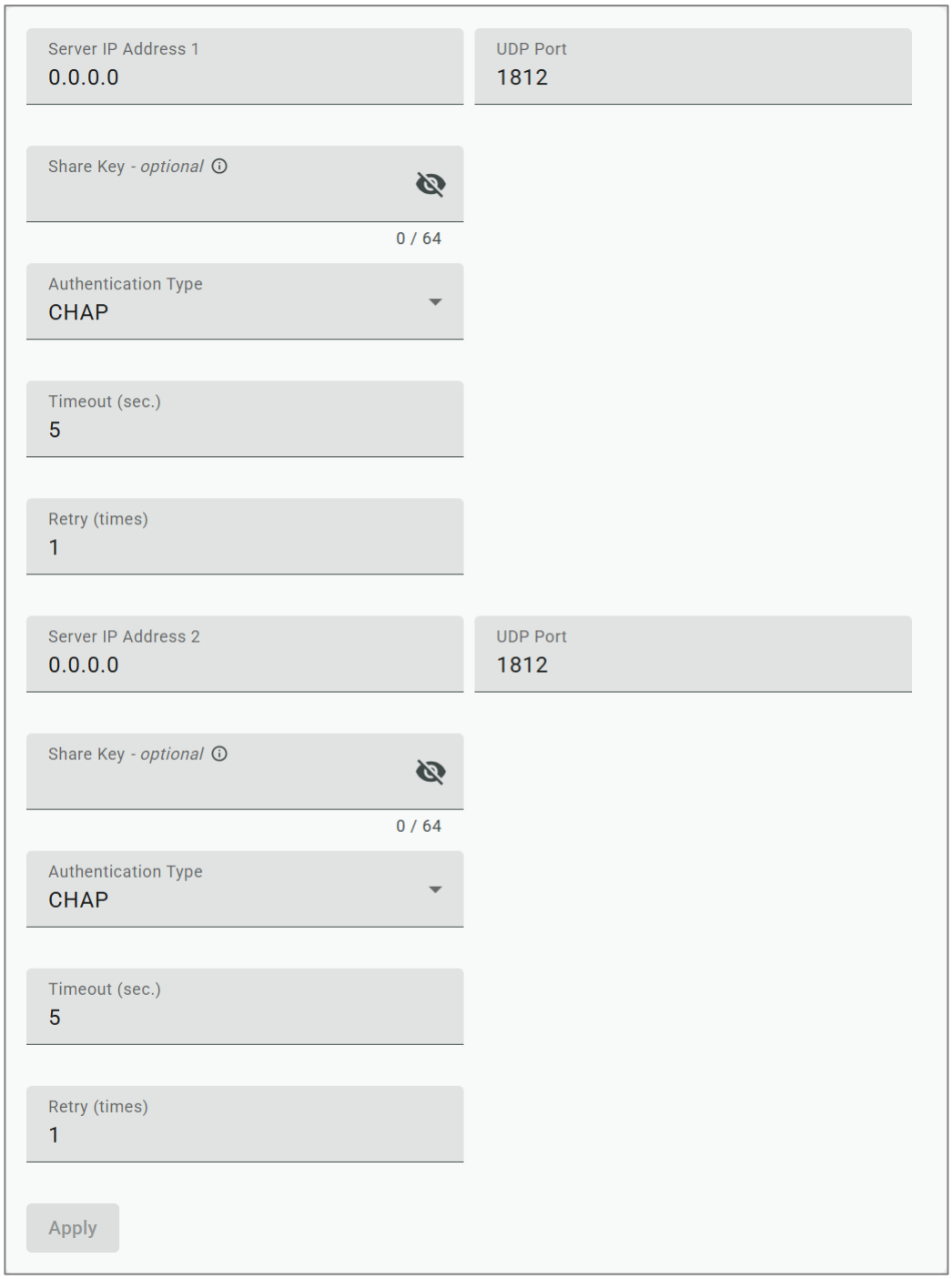
Menu Path: Security > Authentication > RADIUS

This page lets you configure the RADIUS settings for your device.

RADIUS Server Settings

Note

After leaving this page or refreshing, the Share Key fields will automatically be cleared to enhance security.



UI Setting	Description	Valid Range	Default Value
Server Address 1/2	Specify the address of the first/second RADIUS server.	Valid IP address	0.0.0.0
UDP Port	Specify the UDP port for the RADIUS server.	1 to 65535	1812
Share Key	Specify the share key for server authentication verification.	0 to 64 characters	N/A
Authentication Type	Select the authentication type to use for the RADIUS server.	PAP / CHAP / MS-CHAPv1 / MS-CHAPv2	CHAP
Timeout (sec.)	Specify how long in seconds to wait for a response from the RADIUS server before timing out.	5 to 180	5
Retry (sec.)	Specify how many times to try reconnecting to the RADIUS server.	0 to 5	1

TACACS+

Terminal Access Controller Access Control System Plus (TACACS+) helps provide network access control by verifying users, authorizing their actions (like read, write, or configure), and keeping a detailed log of activity. This granular control allows you to restrict what users can do on specific network devices, ensuring security and compliance. TACACS+ is especially beneficial for network administrators who need to manage user access privileges and track activity across multiple devices.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

TACACS+

Menu Path: Security > Authentication > TACACS+ Server

This page lets you configure the TACACS+ settings for your device.

Note

The TACACS+ service will be operated using the 1st server specified. If it fails, it will run on the 2nd server specified.

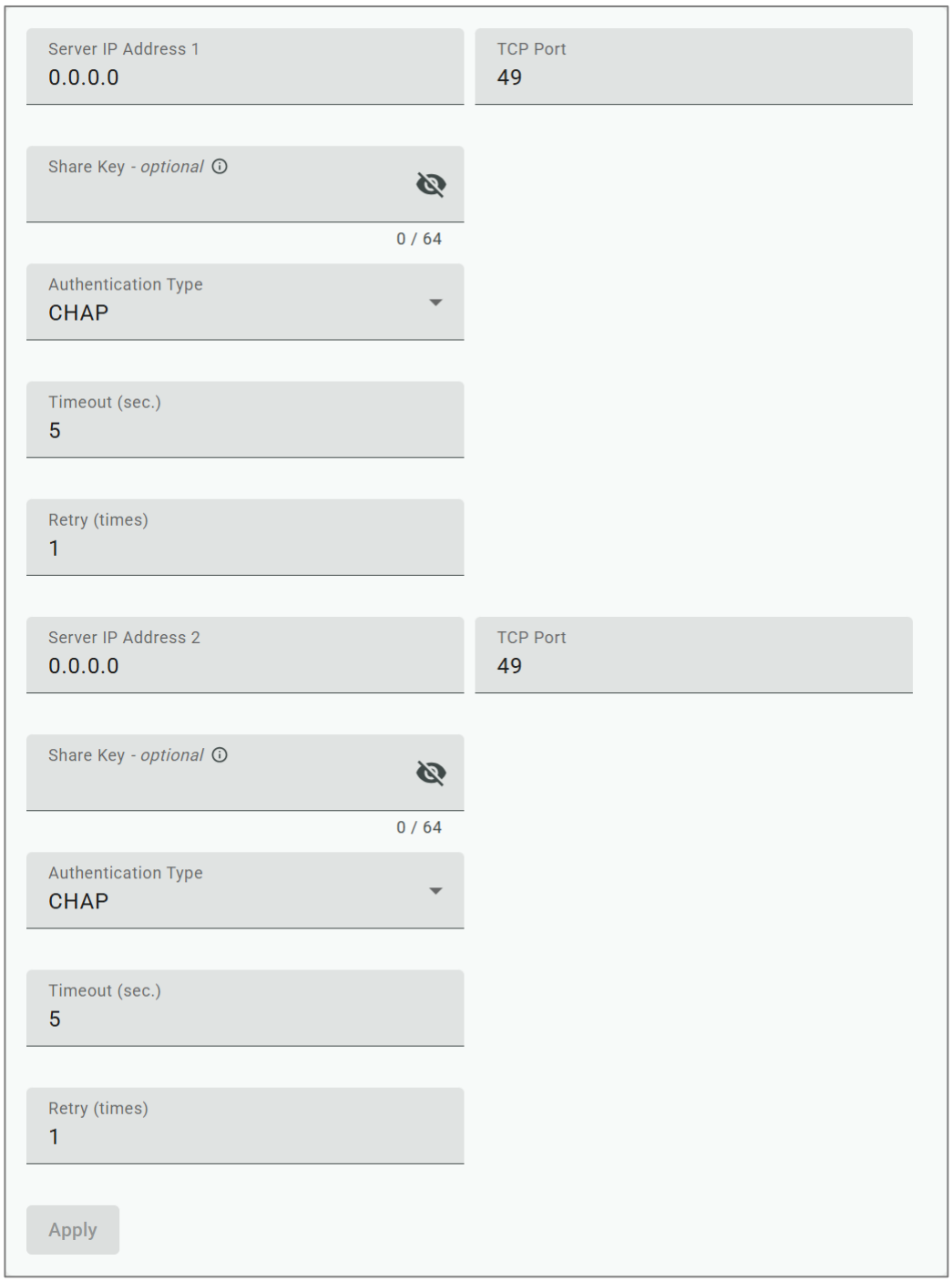
Note

Users created with the TACACS+ server will be granted Admin privileges.

TACACS+ Server Settings

Note

After leaving this page or refreshing, the Share Key fields will automatically be cleared to enhance security.



UI Setting	Description	Valid Range	Default Value
Server Address 1/2	Specify the address of the first/second TACACS+ server.	Valid IP address	0.0.0.0
TCP Port	Specify the TCP port for the TACACS+ server.	1 to 65535	49

UI Setting	Description	Valid Range	Default Value
Share Key	Specify the share key for server authentication verification.	0 to 64 characters	N/A
Authentication Type	Select the authentication type to use for the TACACS+ server.	ASCII / PAP / CHAP	CHAP
Timeout (sec.)	Specify how long in seconds to wait for a response from the TACACS+ server before timing out.	5 to 180	5
Retry	Specify how many times to try reconnecting to the TACACS+ server.	0 to 5	1

Diagnostics

Menu Path: Diagnostics

This section lets you configure the diagnostics settings.

This section includes these pages:

- System Status
- Network Status
- Tools
- Event Logs and Notifications

Diagnostics - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to System > Account Management > User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
System Status			
Resource Utilization	R	R	R
Network Status			
Network Statistics	R	R	R
LLDP	R/W	R/W	R
ARP Table	R	R	R
Tools			
Port Mirroring	R/W	R/W	R
Ping	R/W	R/W	R/W
Event Logs and Notifications			

Settings	Admin	Supervisor	User
Event Logs	R/W	R/W	R
Event Notifications	R/W	R/W	R
Syslog	R/W	R/W	-
SNMP Trap/Inform	R/W	-	-
Email Settings	R/W	R	R

System Status

Menu Path: Diagnostics > System Status

This section lets you view the current system status.

This section includes these pages:

- Resource Utilization

About Resource Utilization

Resource Utilization provides a set of monitoring tools to give you insights into the switch's current and historical resource usage.

These tools typically include:

- **CPU Utilization:** Percentage of CPU processing power currently being used by the device.
- **Memory History:** Historical trend of memory usage over time.
- **Power Consumption:** Current power consumption of the device.
- **Power History:** Historical trend of power consumption over time.

Resource Utilization

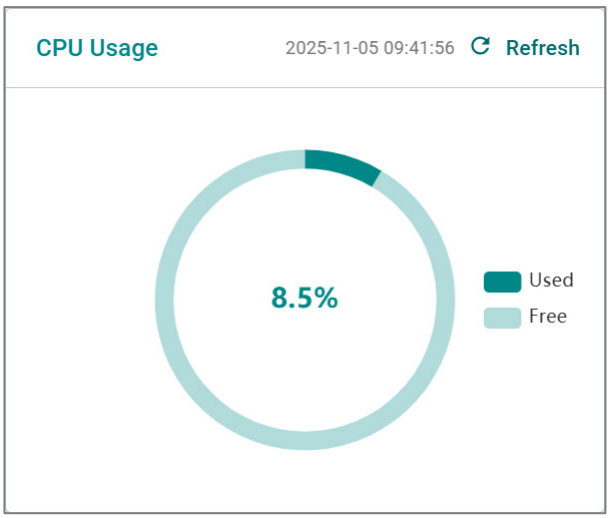
Menu Path: Diagnostics > System Status > Resource Utilization

This page lets you monitor current and historical system resource utilization.

CPU Usage

This display shows the device's CPU usage.

Click the **Refresh (↻)** icon to refresh the graph.



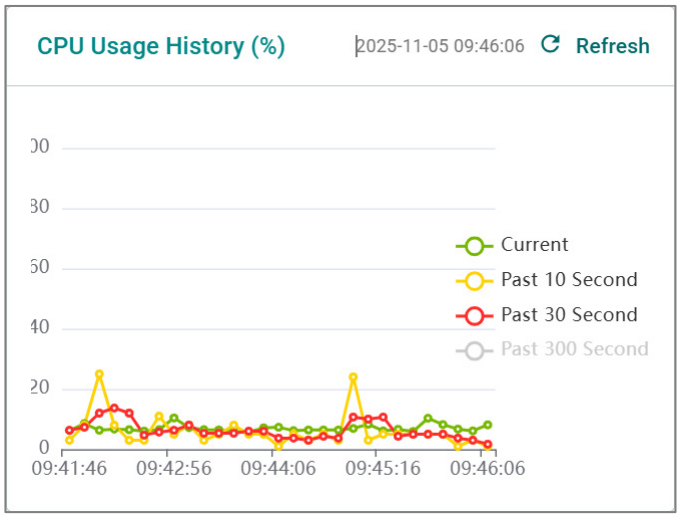
UI Setting	Description
CPU Usage	Displays the current utilization of the CPU.

CPU Usage History (%)

The device's CPU usage will be shown as a percentage based on a time interval. For example, a point on the **Past 10 Second** line shows the average CPU usage for the past 10 seconds at that time.

Click the **Refresh (↻)** icon to refresh the graph.

Click the names on the right side to toggle display of that data.

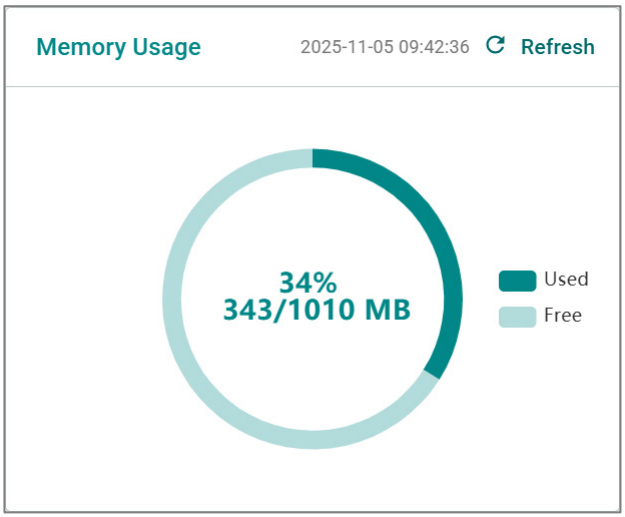


UI Setting	Description
CPU Usage History (%)	Displays the CPU usage history trend in a chart.

Memory Usage

This display shows the device's memory usage.

Click the **Refresh (↻)** icon to refresh the graph.

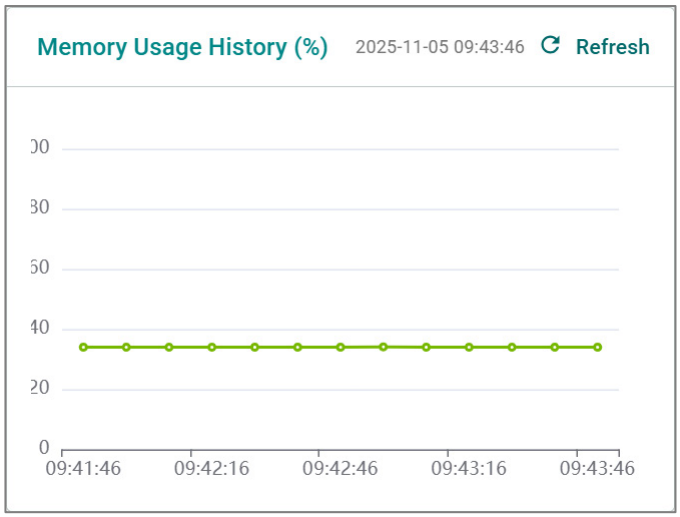


UI Setting	Description
Memory Usage	Displays the memory utilization status.

Memory Usage History

The device's memory usage will be shown as a percentage over time.

Click the **Refresh (↻)** icon to refresh the graph.



UI Setting	Description
Memory Usage History (%)	Displays the history of the memory usage.

Network Status

Menu Path: Diagnostics > Network Status

This section lets you view the network status.

This section includes these pages:

- Network Statistics
- LLDP

About Network Statistics

Network Statistics provides monitoring tools that give you a real-time view of traffic flowing through the device.

This information typically includes:

- **Packet Counter:** The number of data packets being transmitted and received within a specific period of time, providing a crucial metric for assessing the activity and load on a network's infrastructure.
- **Bandwidth Utilization:** The percentage of the total bandwidth currently being used for data transmission.

Network Statistics

Menu Path: Diagnostics > Network Status > Network Statistics

This page lets you see the real-time packet and bandwidth status for your device.

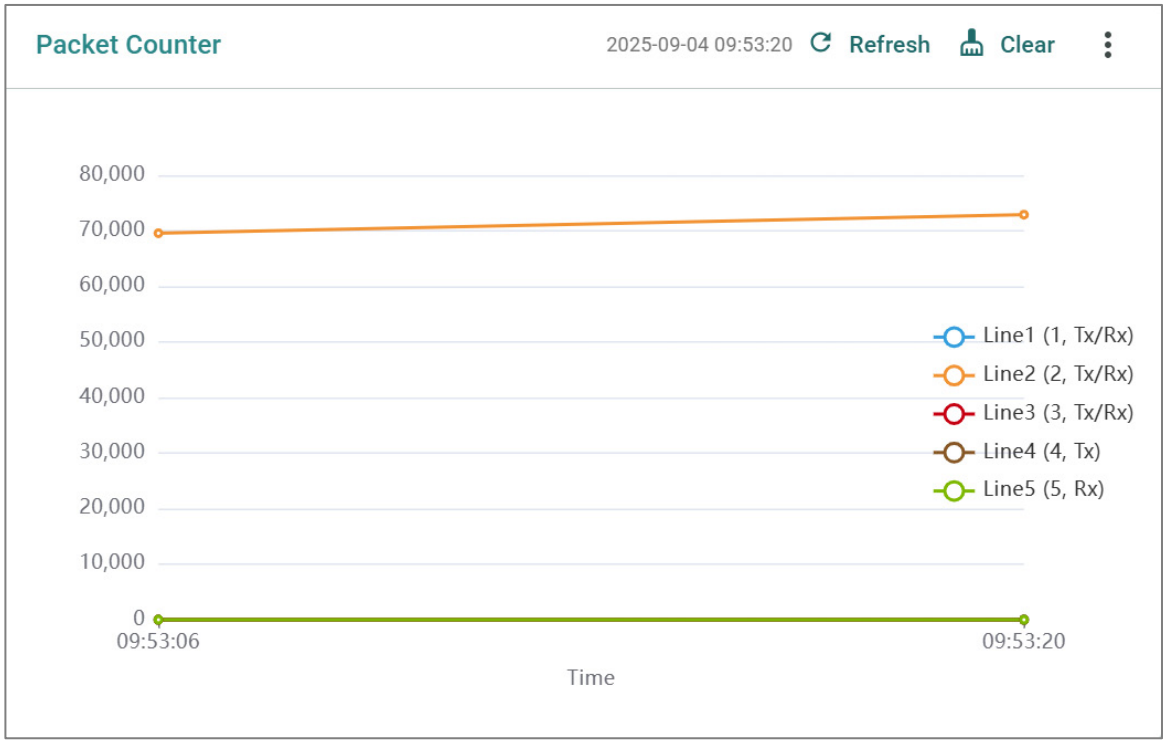
Network Status Display

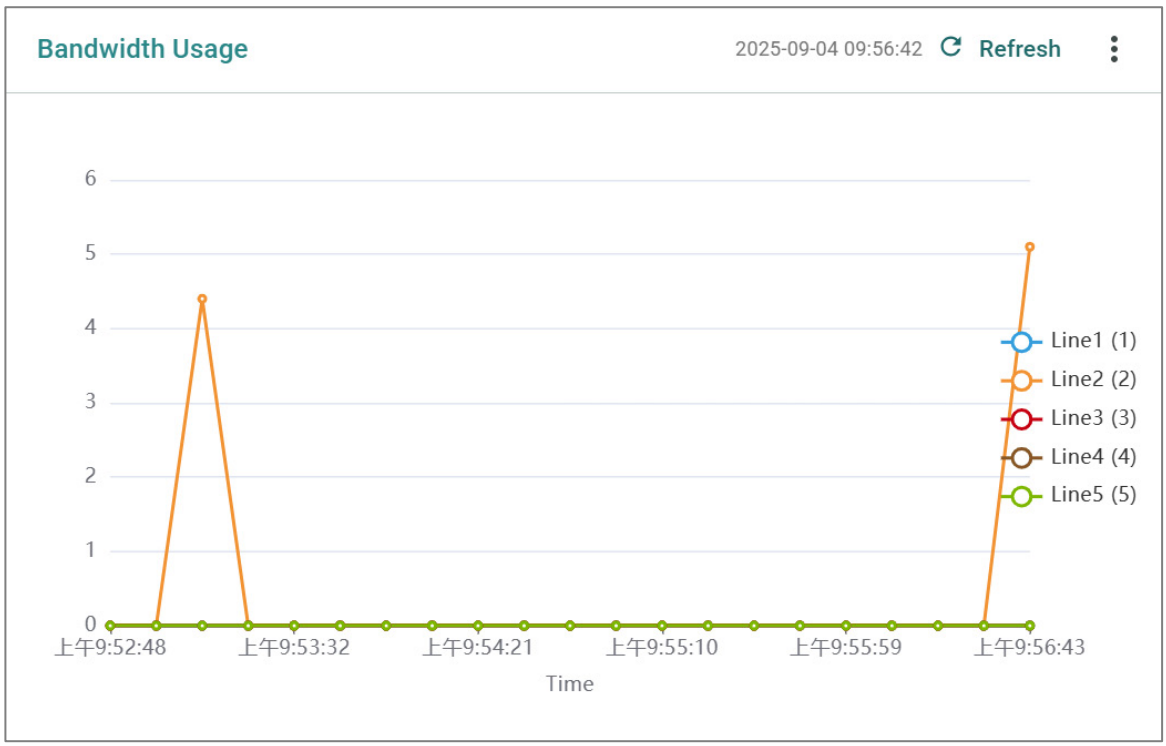
Click the **Options (⋮)** icon and select **Display Settings** to switch between **Packet Counter** and **Bandwidth Utilization** views and configure them.

- **Packet Counter**: This view shows how many packets are being handled over time. This view updates every 5 seconds.
- **Bandwidth Utilization**: This view shows bandwidth utilization over time. This view updates every 3 seconds.

Click the **Refresh (↻)** icon to refresh the graph.

Click the **Clear (🧹)** icon to clear all graph data.



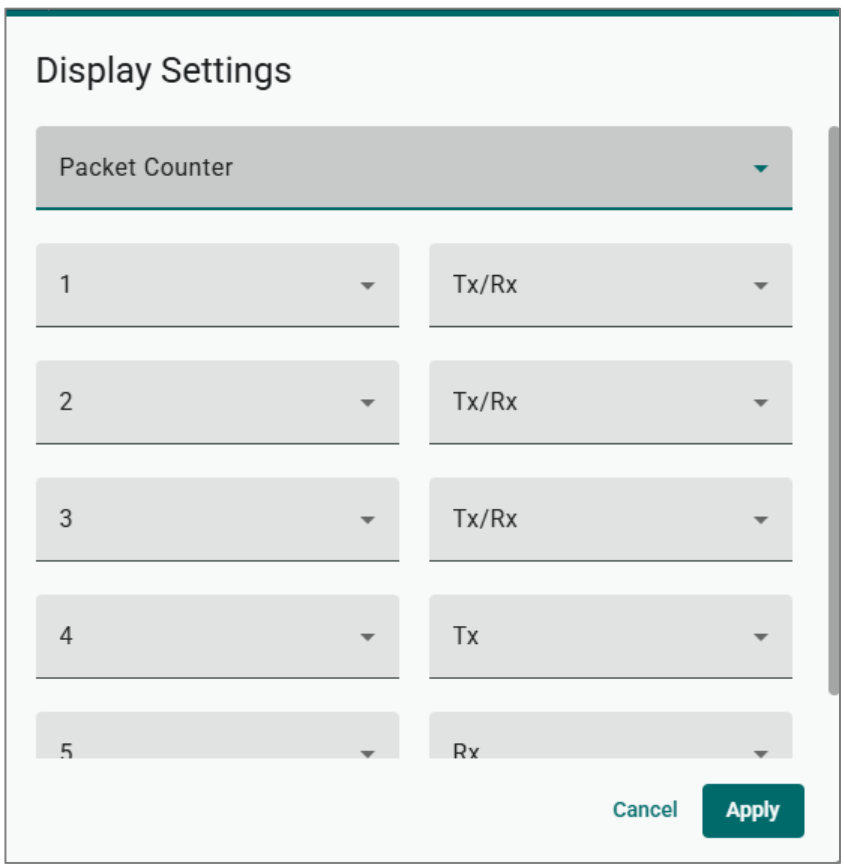


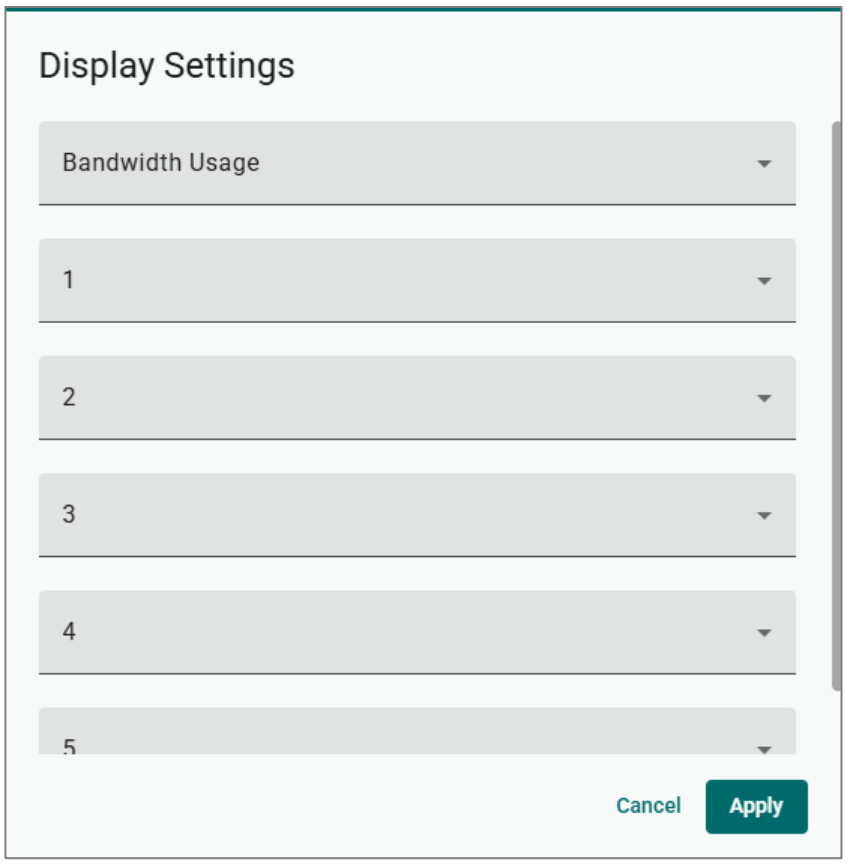
UI Setting	Description
Refresh ( )	Updates statistics immediately without waiting for the refresh interval.

UI Setting	Description
Clear **(For Packet Counter display only)**	Clears the display and resets display settings back to defaults.
Options (⋮)	Opens a drop-down menu with additional options. • **Display Settings**: Opens **Display Settings**, which allows you to switch between **Packet Counter** and **Bandwidth Usage** view, and add lines based on user-defined criteria. • **Compare Data**: Compare data by selecting a benchmark line and time and a comparison line and time. This is only available for the **Packet Counter** view.

Display Settings

If you click the **Options (⋮)** icon on the **Diagnostics > System Status > Resource Utilization** page and select **Display Settings**, this dialog will appear.





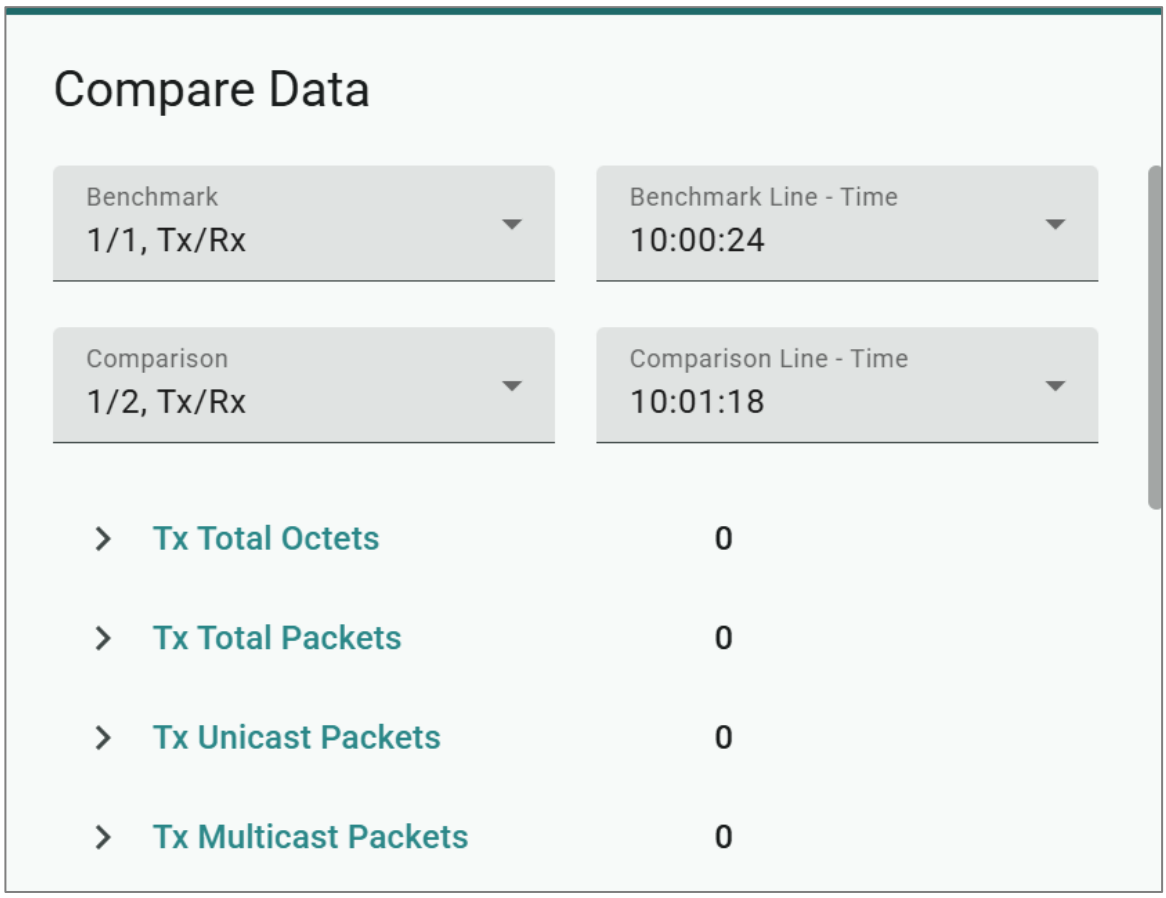
UI Setting	Description	Valid Range	Default Value
Display Mode	Select whether to show the **Packet Counter** or the **Bandwidth Usage** display.	Packet Counter / Bandwidth Usage	Packet Counter
Line 1-5 Sniffer **(If Display Mode is Packet Counter)**	Select which type of traffic to monitor for the line. • **Tx/Rx**: Monitor both transmit and receive traffic. • **Tx**: Only monitor transmit traffic. • **Rx**: Only monitor receive traffic.	Tx/Rx / Tx / Rx	Line 1: Tx/Rx Line 2: Tx/Rx Line 3: Tx/Rx Line 4: Tx Line 5: Rx
Line 1-5 Monitoring Port **(If Display Mode is Bandwidth Usage)**	Select which port to monitor for the line.	Drop-down list of ports	Line 1: 1 Line 2: 2 Line 3: 3 Line 4: 4 Line 5: 5

Compare Data Settings

If you click the **Options (⋮)** icon on the **Diagnostics > System Status > Resource Utilization** page for the **Packet Counter** display and select **Compare Data**, this dialog will appear.

After making your selections, a table will appear that compares various packet statistics between the benchmark and comparison data.

- ↑ : Shows that the benchmark line number is **higher** than the comparison line.
- ± : Shows that the benchmark line number is **equal** to the comparison line.
- ↓ : Shows that the benchmark line number is **lower** than the comparison line.



UI Setting	Description	Valid Range	Default Value
Benchmark	Specify which line to use as the benchmark.	Drop-down list of monitored port and sniffer combinations	N/A

UI Setting	Description	Valid Range	Default Value
Benchmark Line - Time	Select a timestamp to determine which benchmark data to use.	Drop-down list of timestamps	N/A
Comparison	Specify which line to use as the comparison.	Drop-down list of monitored port and sniffer combinations	N/A
Comparison Line - Time	Select a timestamp to determine which comparison data to use.	Drop-down list of timestamps	N/A

Network Statistics Table

This table shows various packet statistics for each port.

The table shows the total number of octets and packets since the last boot for the following items:

- 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 Packets
- Rx Broadcast Packets
- Rx Pause Packets
- Collision Packets
- Late Collision Packets
- Excessive Collision Packets
- CRC Align Error Packets
- Dropped Packets

- Undersize Packets

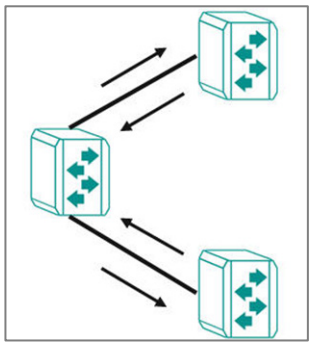
Search Export Edit Columns Clear Counters Refresh

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 Packets	Rx Broadcast Packets	Rx Pause Packets	Collision Packets	Late Collision Packets	Excessive Collision Packets	CRC Align Error Packets	Dropped Packets	Undersize Packets
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	49214170	40786	37585	3199	2	3146012	22863	19687	3174	2	0	0	0	0	0	0	0

About LLDP

Link Layer Discovery Protocol (LLDP) is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device 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 One for auto-topology and network visualization.

From the device'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 One to automatically display the network’s topology and system setup details, such as VLAN and Trunking for the entire network.



Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

LLDP

Menu Path: Diagnostics > Network Status > LLDP

This page lets you configure Link Layer Discovery Protocol (LLDP) for your device.

This page includes these tabs:

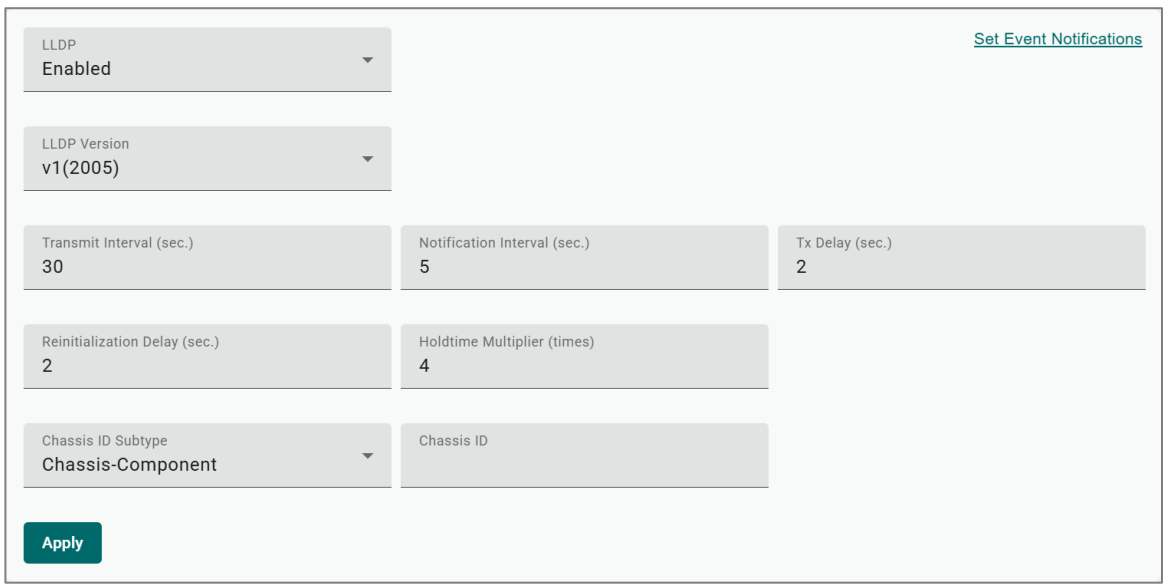
- Settings
- Status

LLDP - Settings

Menu Path: Diagnostics > Network Status > LLDP - Settings

This page lets you configure Link Layer Discovery Protocol (LLDP) settings.

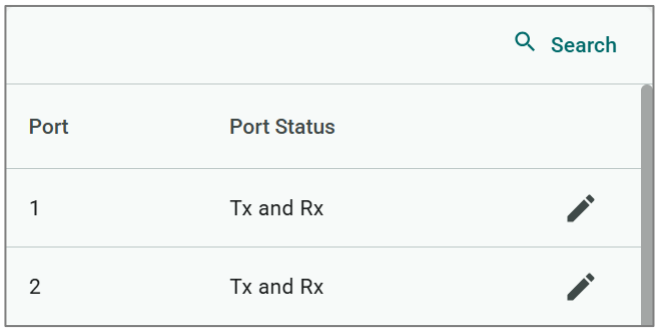
LLDP - Settings



UI Setting	Description	Valid Range	Default Value
LLDP	Enable or disable Link Layer Discovery Protocol (LLDP).	Enabled / Disabled	Enabled
LLDP Version	Shows the LLDP version.	v1(2005)	v1(2005)

UI Setting	Description	Valid Range	Default Value
Transmit Interval (sec.)	Specify how long in seconds the interval will be in between sending LLDP messages.	5 to 32768	30
Notification Interval (sec.)	Specify how long in seconds the interval will be in between sending notifications.	5 to 3600	5
Tx Delay (sec.)	Specify how long in seconds the interval will be in between successive LLDP frame transmissions initiated by changes.	1 to 8192	2
Reinitialization Delay (sec.)	Specify how long in seconds the delay will be before reinitializing an LLDP packet transmission.	1 to 10	2
Holdtime Multiplier (sec.)	Specify how long in seconds the receiving device will hold an LLDP packet before discarding it.	2 to 10	4
Chassis ID Subtype	Specify the Chassis ID subtype of the device.	Chassis-Component / If-Alias / Port-Component / MAC-Address / Network-Address / If-Name / Local	MAC-Address
Chassis ID **(If Chassis ID Subtype is Chassis-Component, Port-Component, or Local)**	Specify the Chassis ID. **Note** The MAC address of the default VLAN is often used for the Chassis ID.	1 to 255 characters	N/A

LLDP Port List



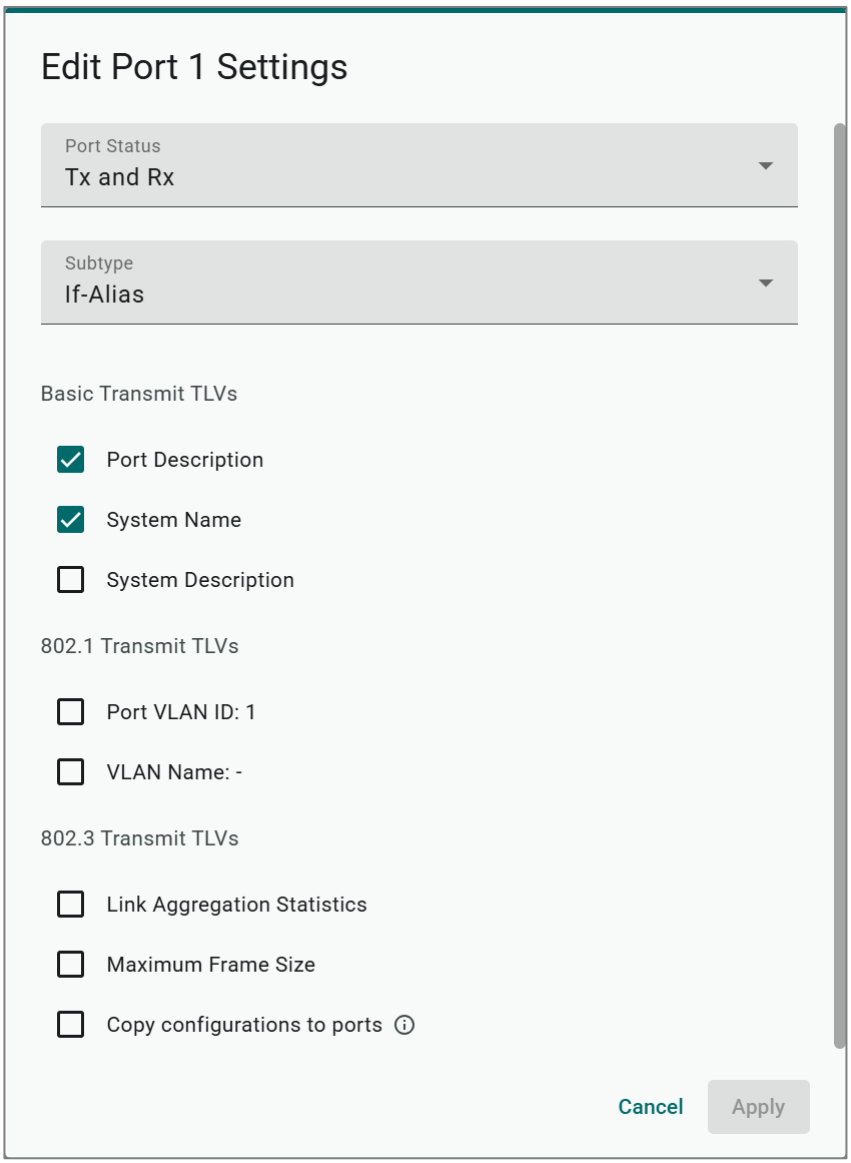
UI Setting	Description
Port	Shows the port number the entry is for.
Port Status	Show the status of what data is being transmitted for the port.

LLDP - Edit Port Settings

Menu Path: Diagnostics > Network Status > LLDP - Settings

Clicking the **Edit (✎)** icon for a port on the **Diagnostics > Network Status > LLDP - Settings** page will open this dialog box. This dialog lets you configure the LLDP settings for the port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Port Status	Specify the port status for transmitting data.	Tx and Rx / Tx Only / Rx Only	Tx and Rx
Subtype	Specify the Chassis ID subtype for the port.	Chassis-Component / If-Alias / Port-Component / MAC-Address / Network-Address / If-Name / Local	If-Alias

UI Setting	Description	Valid Range	Default Value
Port Component Description **(If Subtype is Port-Component or Local)**	Specify a port component description (optional).	0 to 255 characters	N/A
Basic Transmit TLVs	Select the basic information to use for the TLV. You can select multiple options.	Port Description / System Name / System Description	Port Description, System Name
802.1 Transmit TLVs	Select the 802.1 information to use for the TLV. You can select multiple options.	Port VLAN ID / VLAN Name	N/A
802.3 Transmit TLVs	Select the 802.3 information to use for the TLV. You can select multiple options.	Link Aggregation Statistics / Maximum Frame Size	N/A
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

LLDP - Status

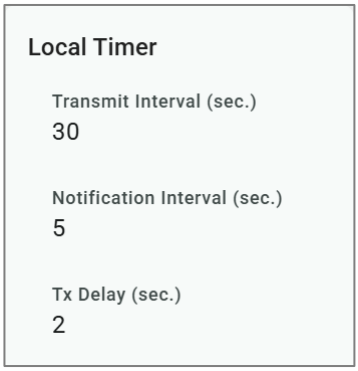
Menu Path: Diagnostics > Network Status > LLDP - Status

This page lets you see the status of LLDP on your device.

Local Information

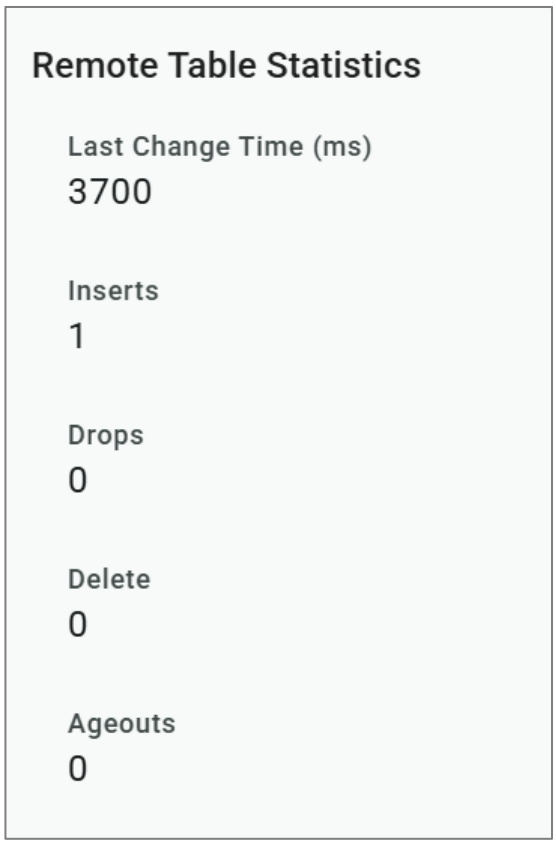
UI Setting	Description
LLDP	Shows whether LLDP is enabled.
LLDP Version	Shows the LLDP version.
Chassis ID Subtype	Shows the chassis ID subtype.
Chassis ID	Shows the chassis ID.

Local Timer



UI Setting	Description
Transmit Interval	Shows the interval between regular LLDP packet transmissions.
Notification Interval	Shows the interval between sending notifications.
Tx Delay	Shows the delay period between successive LLDP frame transmissions initiated by changes.

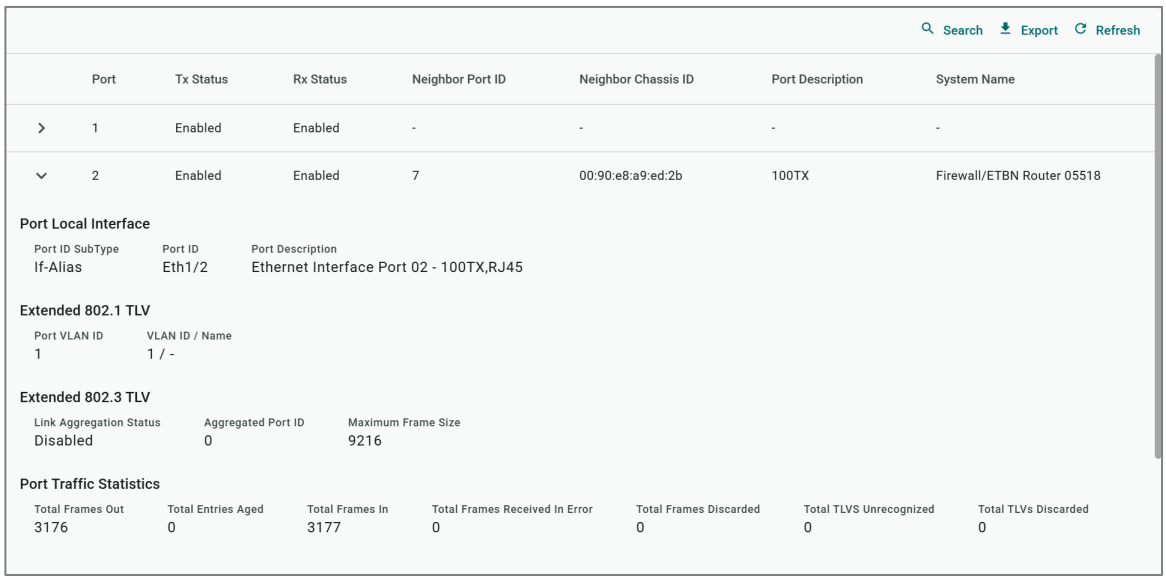
Remote Table Statistics



UI Setting	Description
Last Change Time (ms)	Shows how long ago in milliseconds the remote table was last changed.
Inserts	Shows how many inserts have occurred since the last change.
Drops	Shows how many drops have occurred since the last change.
Delete	Shows how many deletes have occurred since the last change.
Ageouts	Shows how many ageouts have occurred since the last change.

LLDP Port Status

To view the detailed LLDP status for a specific port, click the **detailed information (›)** icon for the port.



UI Setting	Description
Port	Shows the port number the entry is for.
Tx Status	Shows whether LLDP is enabled for transmit traffic.
Rx Status	Shows whether LLDP is enabled for receive traffic.
Neighbor Port ID	Shows the port number of the connected neighbor device's interface that is used to connect to this device.
Neighbor Chassis ID	Shows the unique ID (typically the MAC address) that identifies the neighbor device.
Port Description	Shows the port description of the connected neighbor device's interface that is used to connect to this device.
System Name	Shows the hostname of the neighbor device.

About ARP Tables

The **ARP Table (Address Resolution Protocol Table)** is a database maintained by Ethernet switches. It acts like a translator that maps Media Access Control (MAC) addresses to their corresponding IP addresses. Network devices communicate using MAC addresses, which are unique hardware identifiers. However, routing between devices often relies on IP addresses, so ARP tables are used to bridge this gap.

ARP Table

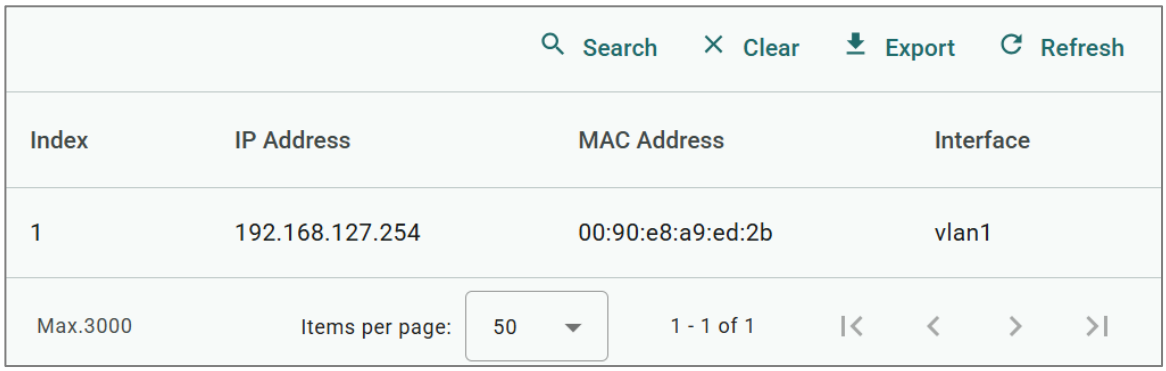
Menu Path: Diagnostics > Network Status > ARP Table

This page lets you see the device's Address Resolution Protocol (ARP) table.

Limitations

The ARP table can show up to 2000 entries.

ARP Table



UI Setting	Description
Index	Shows the index of the device entry.
IP Address	Shows the IP address used for the device.
MAC Address	Shows the MAC address of the device.
Interface	Shows the interface the device is connecting through.

Tools

Menu Path: Diagnostics > Tools

This page lets you use various tools to help troubleshoot network issues.

This page includes these tabs:

- Port Mirroring
- Ping

About Port Mirroring

Port Mirroring is used to monitor data being transmitted through specific ports. This is done by setting up mirror ports to receive the same data being transmitted to, from, or both to and from the ports being monitored. Using mirror ports allows network administrators to sniff the observed ports to keep tabs on network activity.

Port Mirroring In Depth

There are two ways to use Port Mirroring on this device:

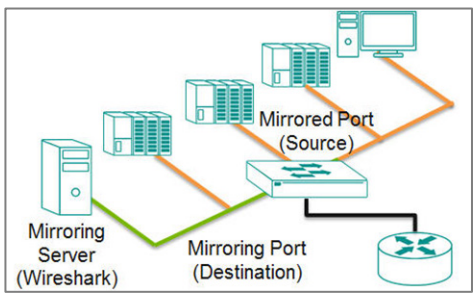
- **SPAN (Switched Port Analyzer):** Mirrors data from monitored ports to multiple terminal ports on the same switch.
- **RSPAN (Remote Switched Port Analyzer):** Mirrors data from monitored ports on one switch to multiple terminal ports on other switches.

> **Note**
>
> Whether Port Mirroring and VLAN Mirroring can be enabled at the same time depends on the product model.

SPAN Port Mirroring

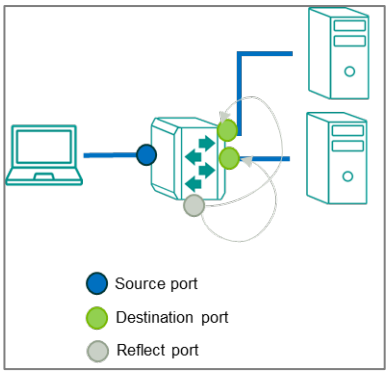
SPAN can be configured to copy packets from various ports to a single port or multiple ports, so that users can check if there are problems occurring in these ports.

For example, the following figure demonstrates how 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 where software is used to check for issues with the packets. This is useful for troubleshooting or monitoring network data transmissions for debugging or security purposes.



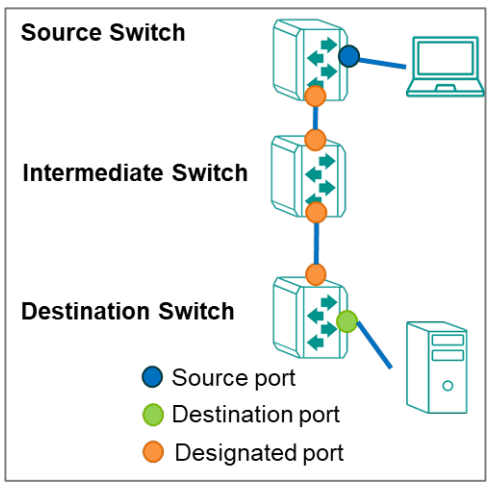
Ingress, egress, or both ingress and egress traffic can be mirrored one or more destination ports.

If you want to mirror traffic to multiple destination ports, than a reflect port needs to be assigned and the destination ports need to be in the same VLAN as the reflect port.



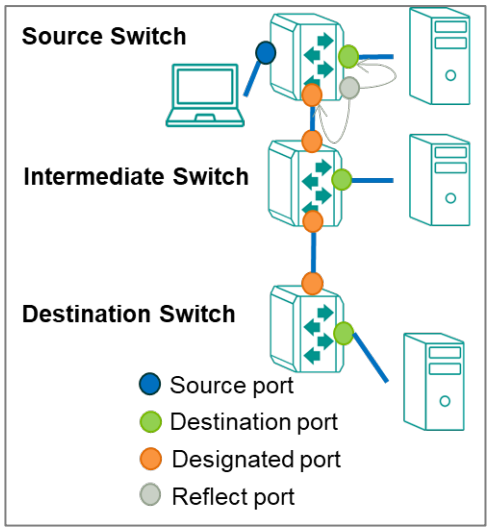
RSPAN Port Mirroring

RSPAN can be configured to copy packets from one or more ports from one or more source switches through intermediate switches to one or more ports on destination switches. The PC or monitoring server can be connected to destination ports on the destination switch to receive a copy of the original traffic being monitored. For example, the following figure demonstrates how packets transmitted to a source port (marked in blue) are copied (mirrored) through an intermediate switch to one or more destination ports (marked in green). Source traffic can be copied through multiple intermediate switches to single or multiple destination switches.



Ingress, egress, or both ingress and egress traffic of the source port(s) can be mirrored to one or more destination ports on destination switches.

If you want to mirror traffic to destination ports on the source switch, a reflect port needs to be assigned. Destination ports in source switch, intermediate switch(es), and destination switch(es) need to be in the same VLAN as the reflect port.



- You can set source ports to be from one or more RSPAN source switches. If one of the destination ports is on a source switch, a reflect port needs to be assigned.
- You can configure an RSPAN VLAN for monitored traffic to be labeled with a RSPAN VLAN tag and send monitored traffic to an RSPAN destination switch via trunk ports.
- You can configure ports to join an RSPAN VLAN, these ports will be destination ports to receive monitored traffic.
- You can connect a monitoring computer to a destination port to receive monitoring traffic for software analysis or diagnostics.

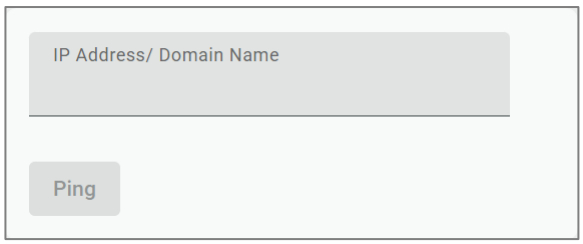
About Ping

Ping lets you use the ping command through the device for a simple, but powerful tool for troubleshooting network problems. The unique feature of this is that even though the ping command is entered in your browser window, the actual ping command will be sent from the Moxa device itself.

Ping

Menu Path: Diagnostics > Tools > Ping

This page lets you use the ping function, which is useful for troubleshooting network problems.



UI Setting	Description	Valid Range	Default Value
IP Address/Domain Name	Specify the IP address or domain name you want to ping, then click the **Ping** button to ping the address and display the results.	Valid IP address or domain name up to 50 characters	N/A

Event Logs and Notifications

Menu Path: Diagnostics > Event Logs and Notifications

This section lets you set up and view your device's event logs and notifications.

This section includes these pages:

- Event Logs
- Event Notifications
- Syslog
- SNMP Trap/Inform
- Email Settings

About Event Logs

Event logs automatically record important events that happen on the network connected to a switch. They are useful when troubleshooting network issues.

These events can include:

- **Changes in connection status:** This could be a cable being plugged in or unplugged, a device joining or leaving the network, or a port going up or down.
- **Errors:** The switch might detect issues like data corruption, excessive traffic, or problems with specific ports.
- **Security events:** Some switches can log attempts to access the switch itself or suspicious activity on the network.

Event Logs

Menu Path: Diagnostics > Event Logs and Notifications > Event Logs

This page lets you browse and export your device's various event logs.

This page includes these tabs:

- Event Logs
- Oversize Action
- Backup

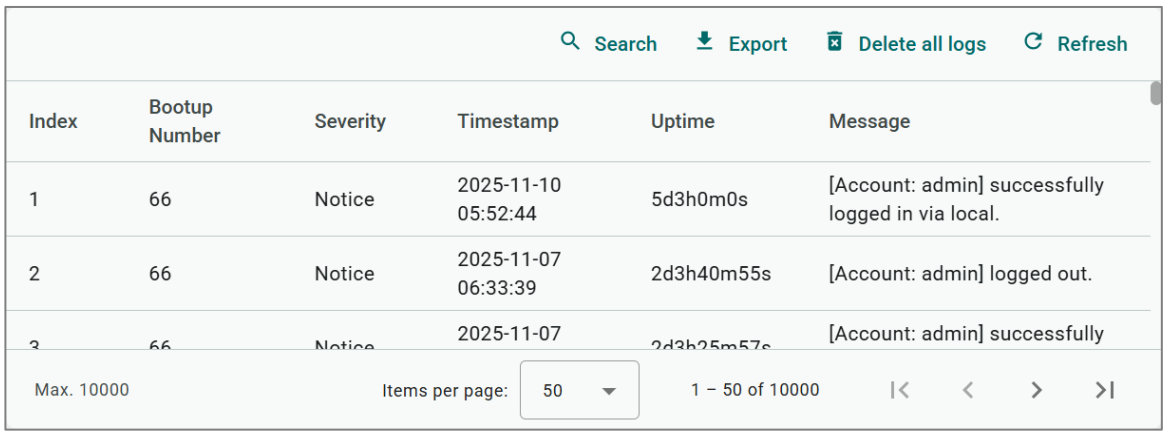
Event Logs - Event Logs

Menu Path: Diagnostics > Event Logs and Notifications > Event Logs - Event Logs

This page lets you view your device's event logs.

> **Limitations**
> The system log can record up to 10000 events.

- Click the **Export icon ( )** to export all logs to a file.
- Click the **Delete all logs icon ( )** to delete all logs.
- Click the **Refresh icon ( )** to refresh the logs.



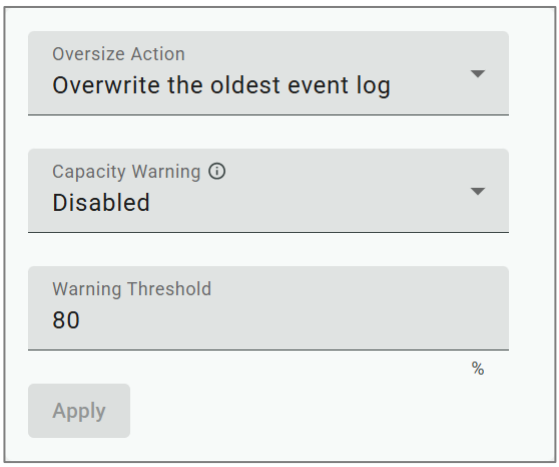
UI Setting	Description
Index	Shows the index of the event.
Bootup Number	Shows the total number of times the device has been powered on. The number increases by 1 every time the device is powered on.
Severity	Shows the severity categorization of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Uptime	Shows the uptime of the device after it is powered on.
Message	Shows additional information about the event, based on the type of event. The username of the account will also be recorded for the following events: **Login Success, Login Fail**, **User Logout**.

Event Logs - Oversize Action

Menu Path: Diagnostics > Event Logs and Notifications > Event Logs - Oversize Action

This page lets you configure the system's oversize action when the event log reaches its maximum number of entries.

Oversize Action



UI Setting	Description	Valid Range	Default Value
Oversize Action	Select the action to take when the event log reaches its maximum number of entries. • **Overwrite the oldest event log**: New events will overwrite the oldest events. • **Stop recording event logs**: No new events will be recorded. This will also disable port monitoring.	Overwrite the oldest event log / Stop recording event logs	Overwrite the oldest event log
Capacity Warning	Enable or disable capacity warnings. **Note** The registered action can be configured for individual events on the Event Notifications page.	Enabled / Disabled	Disabled
Warning Threshold	Set the warning threshold as a percentage. When **Capacity Warning** is enabled, a warning event log will be triggered when the event log reaches this threshold.	50 to 100	80

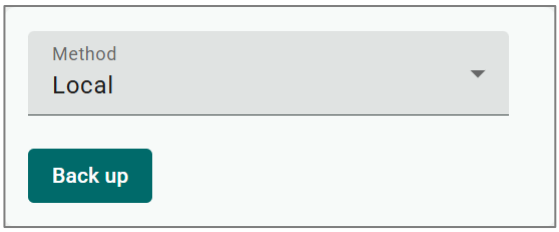
Event Logs - Backup

Menu Path: Diagnostics > Event Logs and Notifications > Event Logs - Backup

This page lets you back up the event logs through various methods.

Event Logs - Backup Settings - Local

If **Method** is set to **Local**, these settings will appear. Click **Back up** to save the event logs to your local computer.

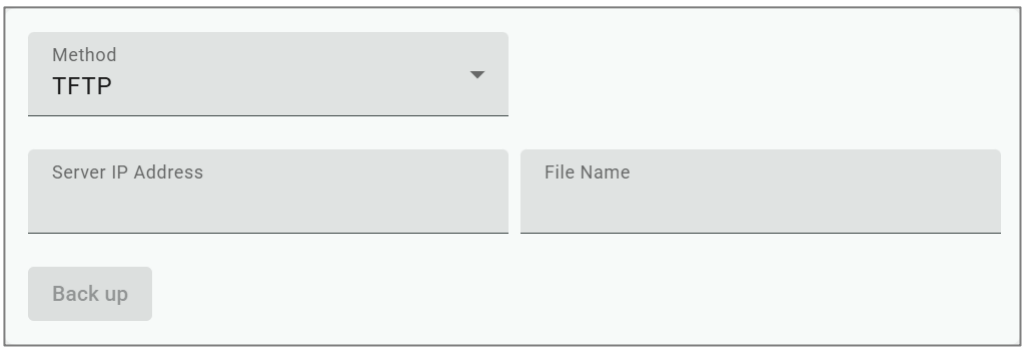


UI Setting	Description	Valid Range	Default Value
Method	Select a method for backing up event logs.	Local / TFTP / SFTP / USB	Local

Event Logs - Backup Settings - TFTP

If **Method** is set to **TFTP**, these settings will appear. Click **Back up** to save the event log to the specified TFTP server.

> **Note**
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

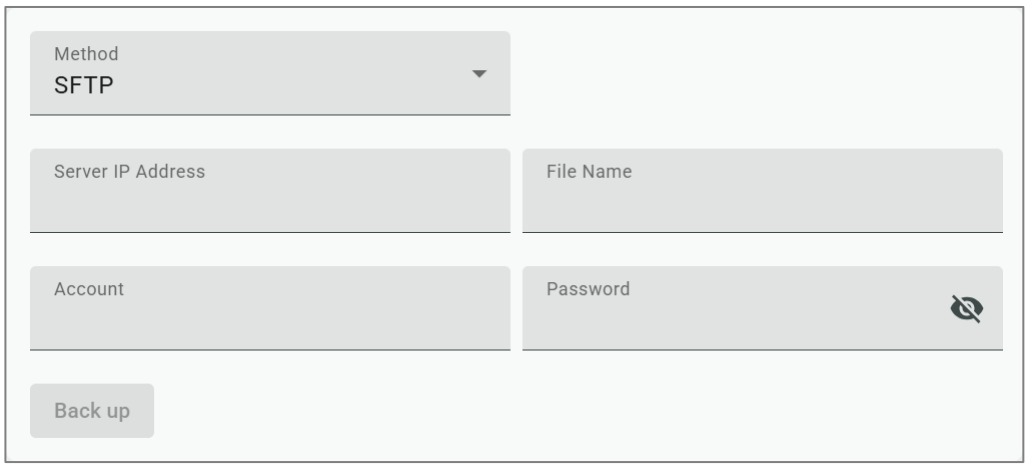


UI Setting	Description	Valid Range	Default Value
Method	Select a method for backing up event logs.	Local / TFTP / SFTP / USB	Local

UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the TFTP server to upload the event logs to.	Valid IP address	N/A
File Name	Specify a file name to use for the event logs file.	File name can only contain A-Z, a-z, 0-9 or the symbols -._().	N/A

Event Logs - Backup Settings - SFTP

If **Method** is set to **SFTP**, these settings will appear. Click **Back up** to save the event log to the specified SFTP server.

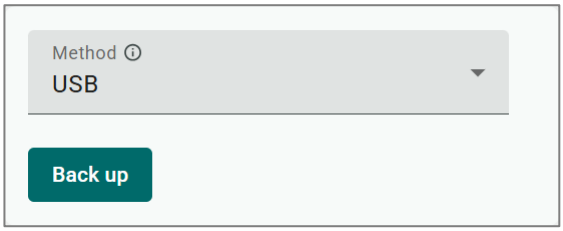


UI Setting	Description	Valid Range	Default Value
Method	Select a method for backing up event logs.	Local / TFTP / SFTP / USB	Local
Server IP Address	Specify the IP address of the SFTP server to upload the event logs to.	Valid IP address	N/A
File Name	Specify a file name to use for the event logs file.	File name can only contain A-Z, a-z, 0-9 or the symbols -._().	N/A
Account	Enter the SFTP server account name to use to connect to the SFTP server.	N/A	N/A
Password	Enter the SFTP server account password to use to connect to the SFTP server.	N/A	N/A

Event Logs - Backup Settings - USB

If **Method** is set to **USB,** these settings will appear. Click **Back up** to save the event log to an ABC-02 configuration tool connected to your device's USB port.

> **Note**
> To use this feature, USB Function must be enabled in System > Management Interface > Hardware Interface.

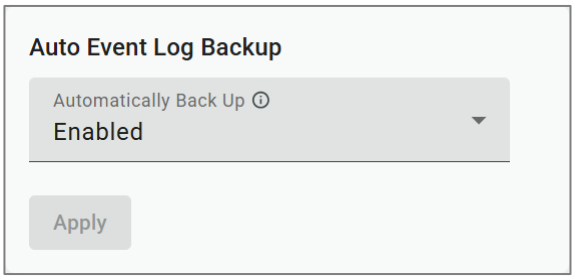


UI Setting	Description	Valid Range	Default Value
Method	Select a method for backing up event logs.	Local / TFTP / SFTP / USB	Local

Auto Event Log Backup

When **Automatically Back Up** is enabled, when the event log is full, the oldest 1000 event logs will be backed up to an inserted ABC-02 configuration tool and then deleted from the device to make space for new logs.

> **Note**
> To use an ABC-02 configuration tool, USB Function must be enabled in System > Management Interface > Hardware Interface.



UI Setting	Description	Valid Range	Default Value
Automatically Back Up	Enable or disable automatic backup of your event logs.	Enabled / Disabled	Enabled

About Event Notifications

Event Notifications act like an alert system for the network. They allow you to be proactively notified when important events occur on the device or for other network devices connected to it.

Event Notifications

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications

This page lets you configure notifications for various kinds of events.

This page includes these tabs:

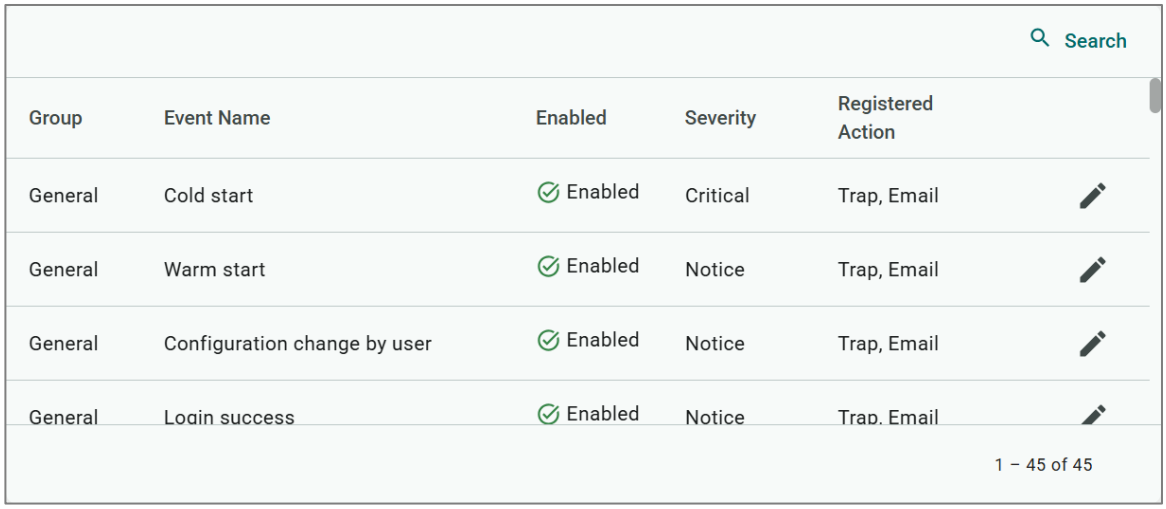
- System and Functions
- Port

Event Notifications - System and Functions

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - System and Functions

This page lets you configure notification settings for various system events related to the overall functions of the device. Each event can be configured independently with different warning methods and severity classifications.

Event Notifications List



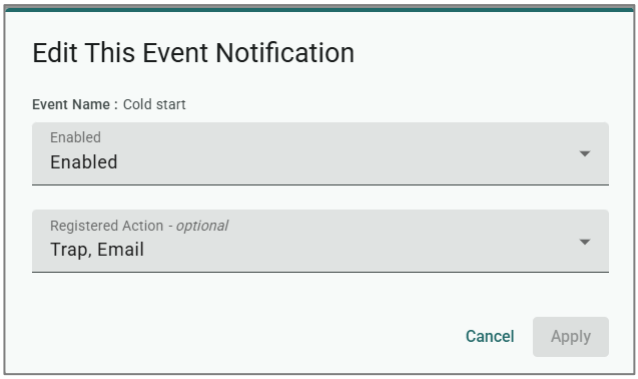
UI Setting	Description
Group	Shows which group this event belongs to.
Event Name	Shows the name of the event. Refer to Event Log Descriptions for more details.
Enabled	Shows whether event notifications are enabled for this kind of event.
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
Registered Action	Shows which action will be taken for this kind of event. • **Trap**: A notification is sent to the Trap server when the event is triggered. • **Email**: A notification is sent to the email server defined in the Email Settings section. **Note** This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions. **Note** The types of actions available may vary depending on the event type and the device model.

Editing an Event Notification

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - System and Functions

Clicking the **Edit (✎)** icon for an entry on the **Diagnostics > Event Logs and Notifications > Event Notifications - System and Functions** page will open this dialog box. This dialog lets you change the notification settings for the selected event.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Event Name (View-only)	Shows the name of the event. Refer to Event Log Descriptions for more information.	(Fixed)	(Fixed)
Enabled	Enable or disable notifications for this event.	Enabled / Disabled	Enabled
Registered Action	Select which actions to take when the event occurs. Multiple actions may be selected. • **Trap**: A notification will be sent to the Trap server. • **Email**: A notification email will be sent to the email server defined in the Email Settings section.	Trap / Email / Relay	Trap, Email

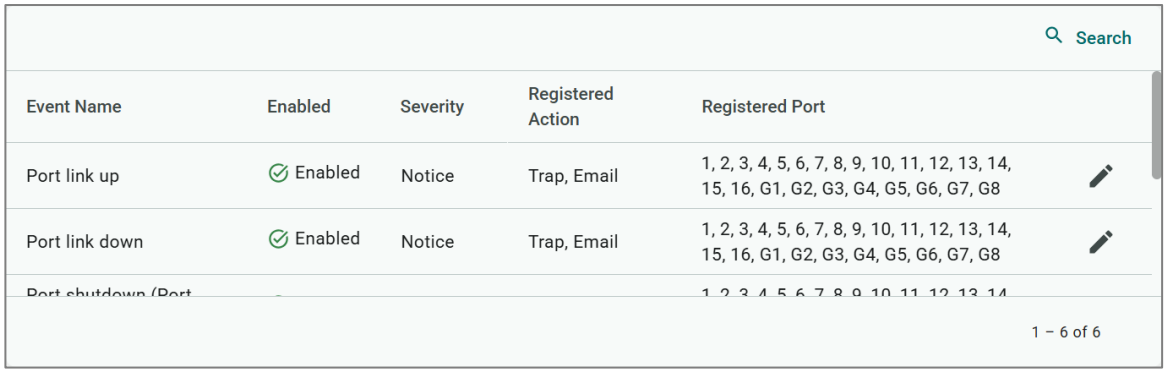
Event Notifications - Port

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - Port

This page lets you configure notification settings for various events related to your device's physical ports. Each port can be configured independently with different warning methods and severity classifications.

When a port event is triggered, the FAULT LED on your device will also light up if your device has one.

Port Event List



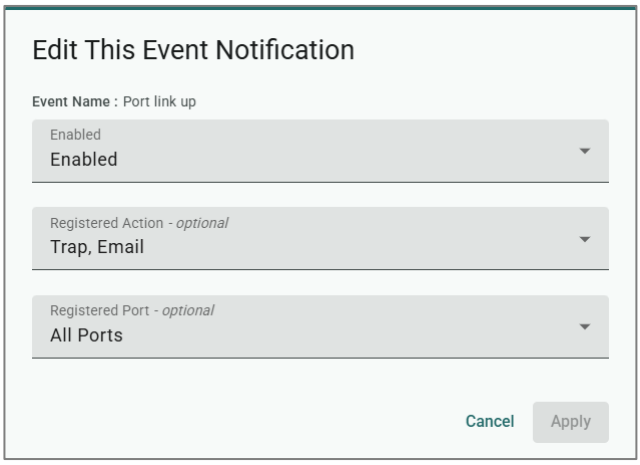
UI Setting	Description
Event Name	Shows the name of the port event.
Enabled	Shows whether event notifications are enabled for this kind of event.
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
Registered Action	Shows which action will be taken for this kind of event. **Trap**: A notification is sent to the Trap server when the event is triggered. **Email**: A notification is sent to the email server defined in the Email Settings section. **Syslog**: An event log is recorded to the Syslog server defined in the Syslog section.
Registered Port	Shows the ports that use the registered action.

Editing a Port Event Notification

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - Port

Clicking the **Edit (✎)** icon for a port on the **Diagnostics > Event Logs and Notifications > Event Notifications - Port** page will open this dialog box. This dialog lets you change the notification settings for the selected port.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Event Name (View-only)	Shows the name of the port event.	(Fixed)	(Fixed)
Enabled	Enable or disable notifications for this event.	Enabled / Disabled	Enabled
Registered Action	Select which actions to take when the event occurs. Multiple actions may be selected. • **Trap**: A notification will be sent to the Trap server. • **Email**: A notification email will be sent to the email server defined in the Email Settings section.	Trap / Email / Relay	Trap, Email
Registered Port	Specify the ports that will use the registered action.	Drop-down list of ports	All Ports

About Syslog

Syslog allows you to centralize event logs on a dedicated server. This provides a more comprehensive record of network activity compared to the limited storage on an individual device, aiding in troubleshooting and security analysis.

When an event occurs, an event notification can be sent as a syslog UDP packet to specified syslog servers. Each syslog server can be enabled individually.

Administrators can manually import self-signed certificates for syslog client services. However, they should check the root certificate and validity of the signature before importing, according to the organization's security procedures and requirements. After importing a certificate, the administrator should check if the certificate has been revoked

and if so, the certificate must be replaced. When the device sends an imported certificate to the syslog server, the syslog server will attempt to verify the certificate against the approved certificate pool on the server.

Syslog Formats

This device supports different syslog formats.

RFC 3164

Also known as BSD syslog format, RFC 3164 syslog messages contain information to form a header followed by a message:

`<PRIORITY>TIMESTAMP HOSTNAME TAGS: MESSAGE`

PRIORITY	Indicates the syslog priority of the event.
TIMESTAMP	Indicates the date and time of the event. The following date format is used: `Mmm dd hh:mm:ss`
HOSTNAME	Indicates the host device that originally sent the syslog message.
TAGS	Additional information tags about the event. This device uses: `CLASSIFICATION: [boot=COUNT][uptime=VALUE]` Moxa devices use the classification of the relevant feature, according to the device's web UI.
MESSAGE	The event message, which may be in legacy or CEF message format. Refer to Message Formats for more information.

Example RFC 3164 message using legacy message format:

```
<156> Jan  8 23:58:37 moxa Redundancy: [boot=3079][uptime=21d22h4m40s]
Topology change detected on Ring 1 of Turbo Ring v2.
```

Example RFC 3164 message using CEF message format:

```
<156> Jan  8 23:59:13 moxa CEF:0|MOXA|TN-4520B-12P-4GP-4GBP-T|v2.0 Build
2025_0917_1811|1073742862|Topology change (Turbo Ring)|5|dvchost=moxa
dvc=192.168.127.106 index=1
```

RFC 5424

RFC 5424 defines an updated syslog format that includes additional fields:

`<PRIORITY>VERSION TIMESTAMP HOSTNAME APP-NAME PROCID MSGID STRUCTURED-DATA MESSAGE`

PRIORITY	Indicates the syslog priority of the event.
VERSION	Indicates the syslog protocol specification version used for the syslog message.
TIMESTAMP	Indicates the date and time of the event. ISO-8601 date format is used.
HOSTNAME	Indicates the host device that originally sent the syslog message.
APP-NAME	Indicates the device or application that originated the message. Moxa devices use the classification of the relevant feature, according to the device's web UI.
PROCID	This device does not use this field, so a `-` is used as a placeholder.
MSGID	Indicates the ID of the message type. Refer to Event Log Descriptions for the event IDs used by this device.
STRUCTURED-DATA	This device does not use this field, so a `-` is used as a placeholder.
MESSAGE	The event message, which may be in legacy or CEF message format. Refer to Message Formats for more information.

Example RFC 5424 message using legacy message format:

```
<156>1 2026-01-09T01:23:24+00:00 moxa Redundancy - 1073742862 - Topology change detected on Ring 1 of Turbo Ring v2.
```

Example RFC 5424 message using CEF message format:

```
<156>1 2026-01-09T01:23:49+00:00 moxa Redundancy - 1073742862 - CEF:0|MOXA|TN-4520B-12P-4GP-4GBP-T|v2.0 Build 2025_0917_1811|1073742862|Topology change (Turbo Ring)|5|dvchost=moxa dvc=192.168.127.106 index=1
```

Message Formats

This device supports both legacy and CEF message formats for syslog logging.

Refer to Event Log Descriptions for more details on messages used for specific events.

Legacy Message Format

The legacy message format uses a simple event description.

Example legacy message:

```
Topology change detected on Ring 1 of Turbo Ring v2
```

CEF Message Format

The Common Event Format (CEF) is a standardized, text-based format for logging security-related events from various sources. Built on the syslog format, CEF provides a structured and consistent way to log events, making it a crucial component for effective security information and event management (SIEM) solutions.

By using a standardized logging format, CEF simplifies managing and analyzing security logs, making it easier to:

- Collect and aggregate log data from diverse systems and applications
- Analyze and troubleshoot issues efficiently
- Automate the analysis of logs to reduce manual effort
- Identify security threats, patterns, and trends across the network

Example CEF message:

```
CEF:0|Moxa|RKS-G4028-L3-4GS-HV-T|v6.0 Build 2025_1201_1045|0x4000040e|Topology change (Turbo Ring)|5|index=1
```

Refer to CEF Message Format for Event Logs for more information.

Syslog

Menu Path: Diagnostics > Event Logs and Notifications > Syslog

This page lets you manage your device's Syslog.

This page includes these tabs:

- General
- Authentication

Note

In order to ensure the security of your network, we recommend the following:

- The encryption algorithm of keys should be selected based on internationally recognized and proven security practices and recommendations.
- The lifetime of certificates generated for syslog client services should be short and in accordance with the organization's security procedures and requirements.
- For security reasons, it is recommended to send event logs to a centralized syslog server for continuous network event monitoring.

Syslog - General

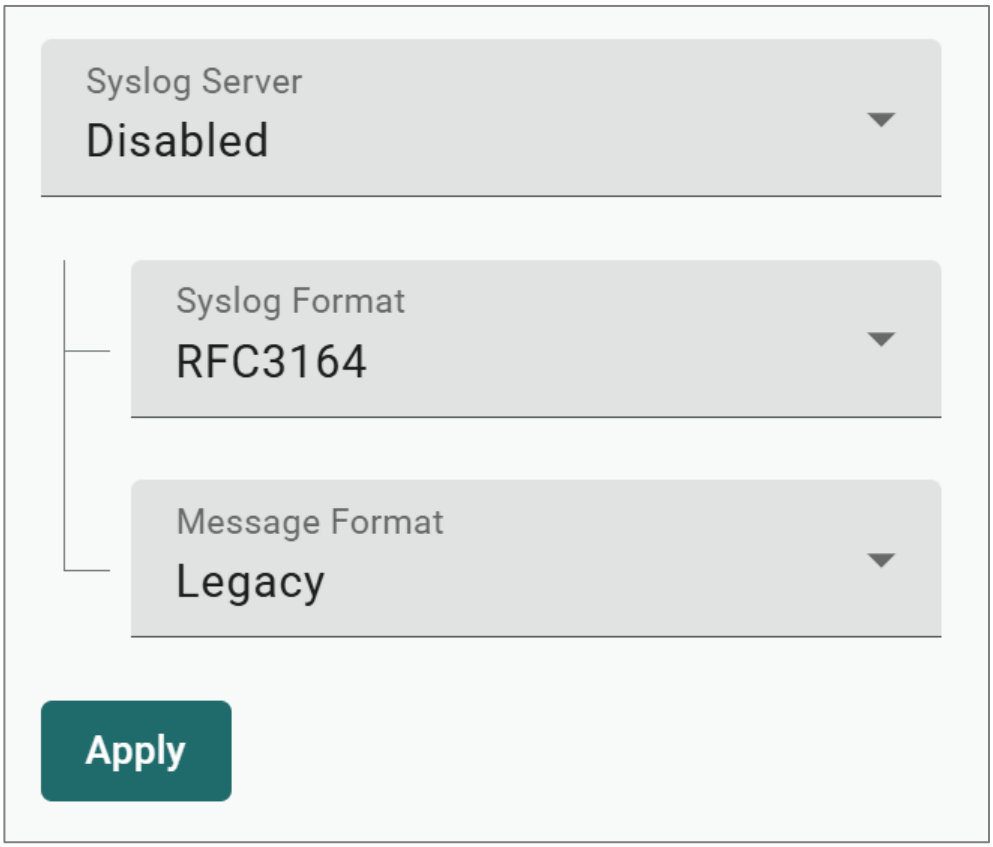
Menu Path: Diagnostics > Event Logs and Notifications > Syslog - General

This page lets you configure the Syslog server settings.

Syslog Settings

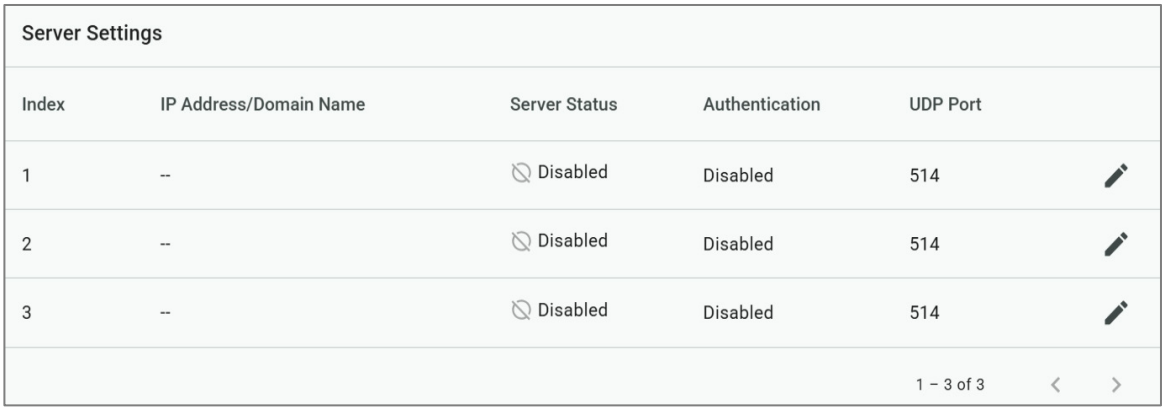
Note

If the syslog server cannot receive previous logs, it is possible that the receiving port of the syslog server is not ready. We suggest you enable the Linkup Delay function to delay the log delivery time.



UI Setting	Description	Valid Range	Default Value
Syslog	Enable or disable syslog logging for your device.	Enabled / Disabled	Disabled
Syslog Format	Specify the syslog format to use.	RFC3164 / RFC5424	RFC3164
Message Format	Specify the message format to use.	Legacy / CEF (Common Event Format)	Legacy

Syslog Server Settings List



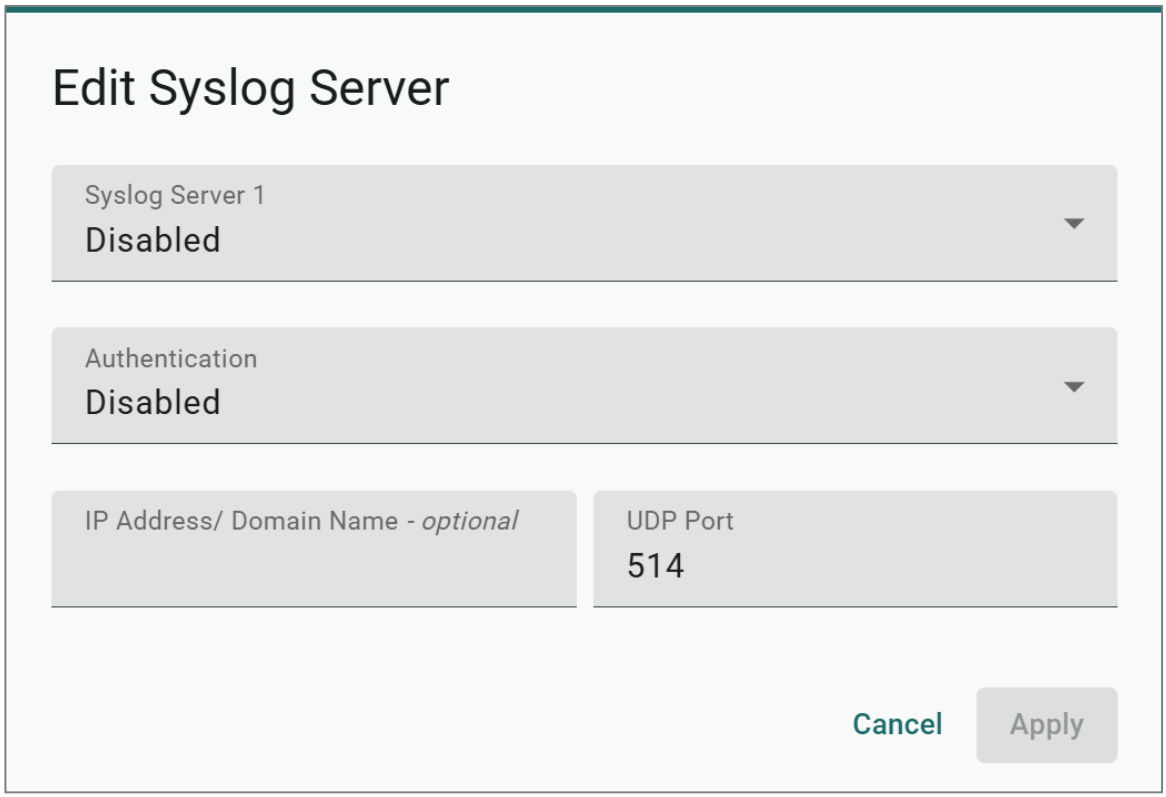
UI Setting	Description
Index	Shows the index of the syslog server.
IP Address/Domain Name	Shows the IP address or domain name of the syslog server.
Server Status	Shows whether the syslog server is enabled.
Authentication	Shows whether authentication via TLS is enabled for the syslog server.
UDP Port	Shows the UDP port of the syslog server.

Editing a Syslog Server

Menu Path: Diagnostics > Event Logs and Notifications > Syslog - General

This page lets you edit the syslog server settings.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Syslog Server 1/2/3	Enable or disable the specified syslog server.	Enabled / Disabled	Disabled
Authentication	Select whether to authenticate via TLS or disable authentication. **Note** To enable TLS, a certificate and key set must be created first on the "Authentication" tab.	Disabled / TLS	Disabled
IP Address/ Domain Name	Enter the IP address or domain name of the related syslog server.	Valid IP address or domain name	N/A
UDP Port	Specify the UDP port of the related syslog server.	1 to 65535	514

Syslog - Authentication

Menu Path: Diagnostics > Event Logs and Notifications > Syslog - Authentication

This page lets you manually import self-signed certificates for syslog client services.

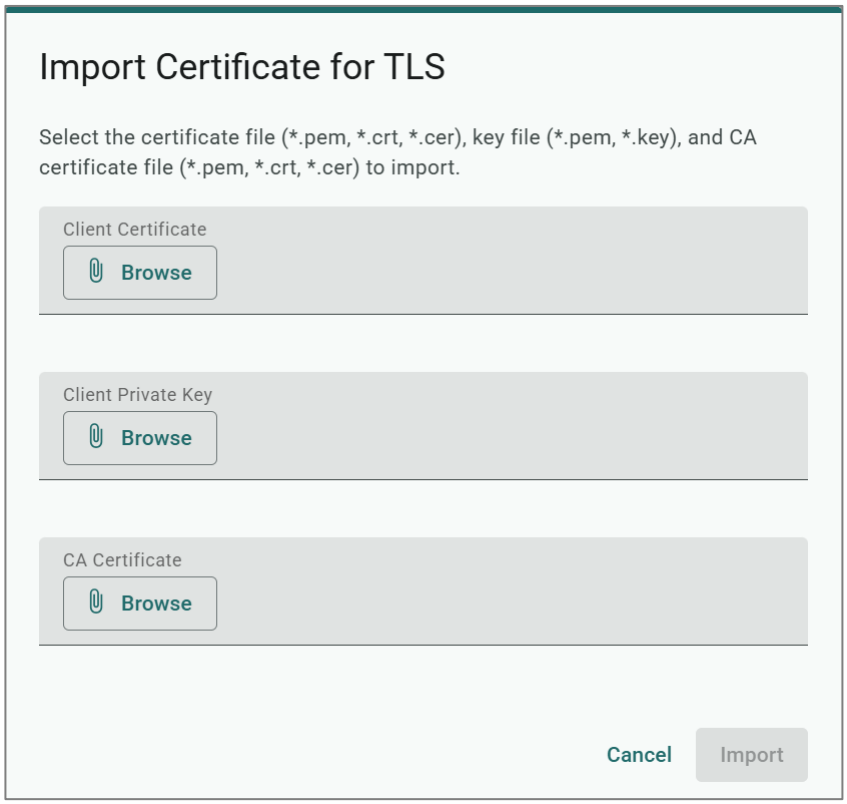
UI Setting	Description
Common Name	Shows the name of the imported certificate and keys.
Start Time	Shows the start time of the imported certificate and keys.
Expiration Time	Shows the expiration time of the imported certificate and keys.

Adding a Syslog Certificate and Key Set

Menu Path: Diagnostics > Event Logs and Notifications > Syslog - Authentication

To import a client certificate and key for syslog authentication over TLS, click **Manage** on the **Diagnostics > Event Logs and Notifications > Syslog - Authentication** page and select **Import Certificate**. This dialog will let you import a TLS certificate and its related keys.

Click **Import** to save your changes.



UI Setting	Description	Valid Range	Default Value
Client Certificate	Click the **Browse** button and select a client certificate file from your computer to import.	N/A	N/A
Client Private Key	Click the **Browse** button and select a client private key file from your computer to import.	N/A	N/A
CA Key	Click the **Browse** button and select a CA certificate file from your computer to import.	N/A	N/A

About SNMP Trap/Inform

SNMP Trap allows an SNMP agent to notify the NMS of a significant event.

Your device supports two SNMP modes: **Trap** mode and **Inform** mode.

SNMP Trap/Inform allows your switch to actively send real-time notifications about critical events to network management systems. This proactive alerting can help identify and address network issues faster, improving overall network health and uptime.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

SNMP Trap/Inform

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform

This page lets you configure the SNMP Trap/Inform notification feature.

This page includes these tabs:

- General
- SNMP Trap/Inform Accounts

SNMP Trap/Inform - General

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - General

This page lets you configure the SNMP Trap/Inform settings of your device.

Click **Apply** to save your changes.

SNMP Trap/Inform Recipients

UI Setting	Description
Recipient IP Address/ Domain Name	Shows the IP address or domain name of the recipient trap server that will receive notifications.

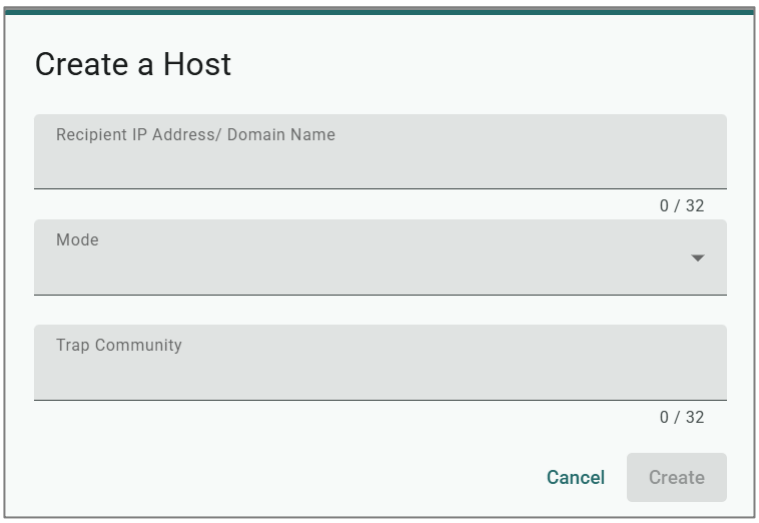
UI Setting	Description
Mode	Shows the mode used for SNMP notifications.
Trap Community	Shows the community string used for authentication.

Creating an SNMP Trap/Inform Host

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - General

Clicking the **Create** on the **Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - General** page will open this dialog box. This dialog lets you add an SNMP Trap/Inform server.

Click **Create** to save your changes and add the new server.



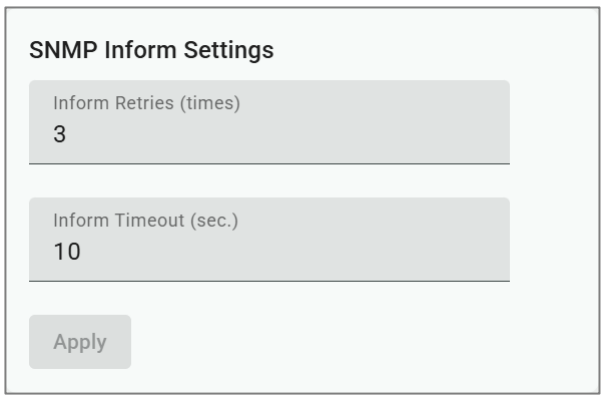
UI Setting	Description	Valid Range	Default Value
Recipient IP Address/ Domain Name	Specify the IP address or the name of the recipient trap server that will receive notifications.	Valid IP address or domain name, 0 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
Mode	Select a mode to use for SNMP notifications. Trap notifications are sent without requesting an acknowledgement from the recipient. Inform notifications will request an acknowledgement from the recipient, and will retry sending the notification if the acknowledgement is not received. • **Trap V1**: Use Trap V1 for SNMP notifications. • **Trap V2c**: Use Trap V2 for SNMP notifications. • **Inform V2c**: Use Inform V2 for SNMP notifications. • **Trap V3**: Use Trap V3 for SNMP notifications. • **Inform V3**: Use Inform V3 for SNMP notifications.	Trap V1 / Trap V2 / Inform V2 / Trap V3 / Inform V3	N/A
Trap Community	Specify the community string that will be used for authentication.	4 to 32 characters	N/A

SNMP Inform Settings

Note

These settings only apply to SNMP Trap/Inform entries that have Trap Mode set to Inform V2c or Inform V3.



UI Setting	Description	Valid Range	Default Value
Inform Retries	Specify the number of times to retry sending an inform notification.	1 to 99	3

UI Setting	Description	Valid Range	Default Value
Inform Timeout	Specify the amount of time in seconds to wait to wait for an acknowledgement before trying to resend an inform notification.	1 to 300	10

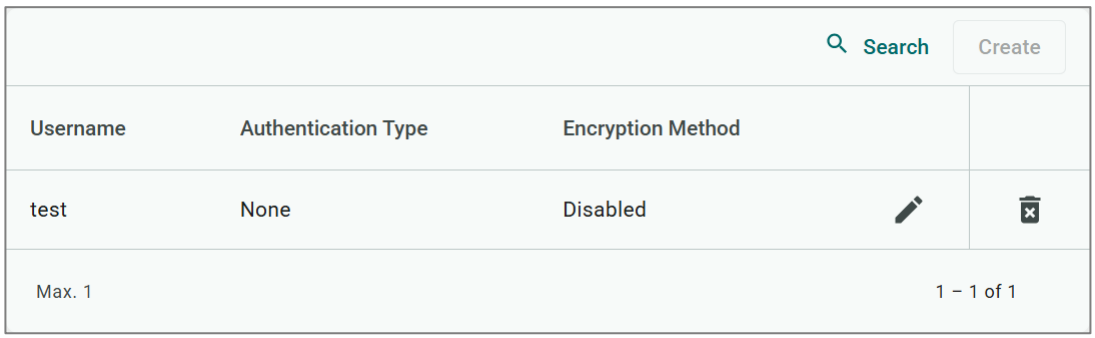
SNMP Trap/Inform Accounts

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Trap/Inform Accounts

This page lets you configure an SNMP trap account for your device.

Limitations

You can configure up to 1 SNMP trap account.



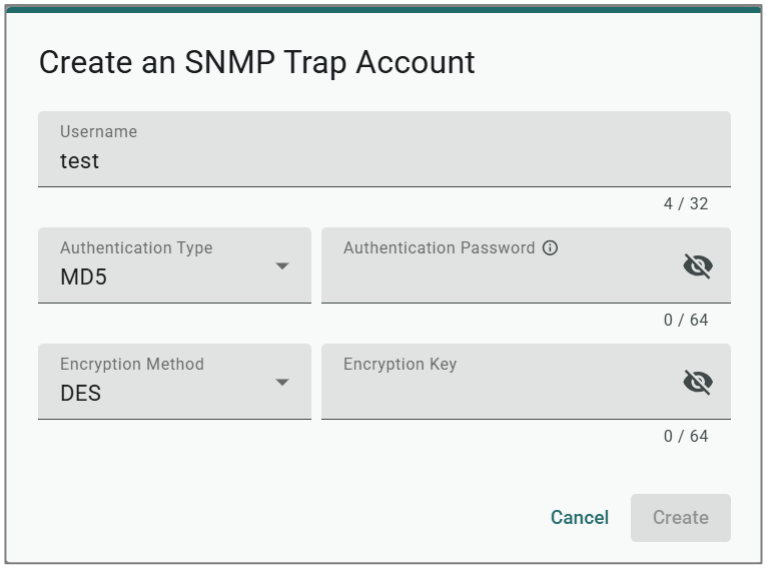
UI Setting	Description
Username	Shows the username for the SNMP trap account.
Authentication Type	Shows which authentication method is used for the account.
Encryption Method	Shows which encryption method is used for the account.

Creating an SNMP Trap Account

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Trap/Inform Accounts

Clicking the **Create** on the **Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Trap/Inform Accounts** page will open this dialog box. This dialog lets you add an SNMP trap account for your device.

Click **Create** to save your changes and add the new account.



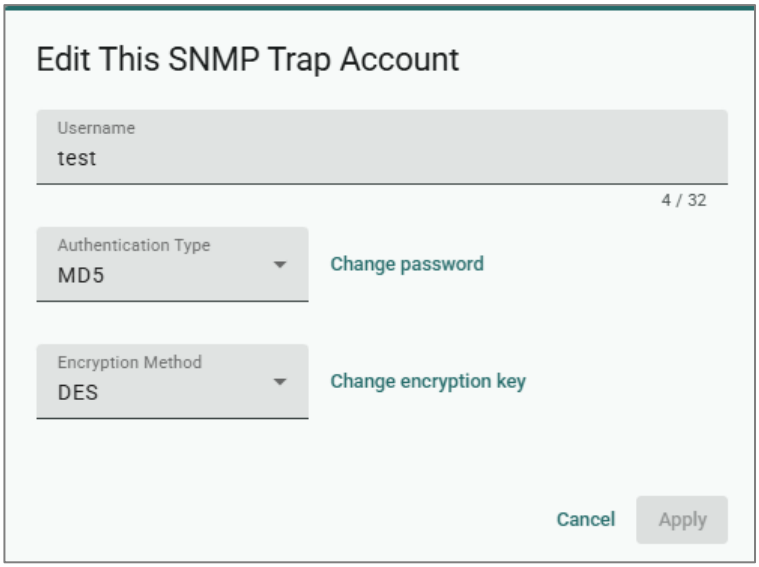
UI Setting	Description	Valid Range	Default Value
Username	Specify a username for the SNMP trap account.	4 to 32 characters	N/A
Authentication Type	Select which authentication method to use for the account.	None / MD5 / SHA / SHA-256 / SHA-512	None
Authentication Key **(if Authentication Type is not None)**	Specify an authentication key to use for the account.	8 to 64 characters	N/A
Encryption Method	Disable encryption or select which encryption method to use for the account.	Disabled / DES / AES	Disabled
Encryption Key **(if Encryption Method is not Disabled)**	Specify an encryption password for the account.	8 to 64 characters	N/A

Editing an SNMP Trap Account

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Trap/Inform Accounts

Clicking the **Edit (✎)** icon for an account on the **Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Trap/Inform Accounts** page will open this dialog box. This dialog lets you edit the account's settings.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Username	Specify a username for the SNMP trap account.	4 to 32 characters	N/A
Authentication Type	Select which authentication method to use for the account. Click **Change password** to specify a new authentication password for the account.	None / MD5 / SHA / SHA-256 / SHA-512	None
Encryption Method	Disable encryption or select which encryption method to use for the account. Click **Change encryption key** to specify a new encryption key for the account.	Disabled / DES / AES	Disabled

Deleting an SNMP Trap Account

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Trap/Inform Accounts

You can delete an account by clicking its **Delete ( )** icon.

About Email Settings

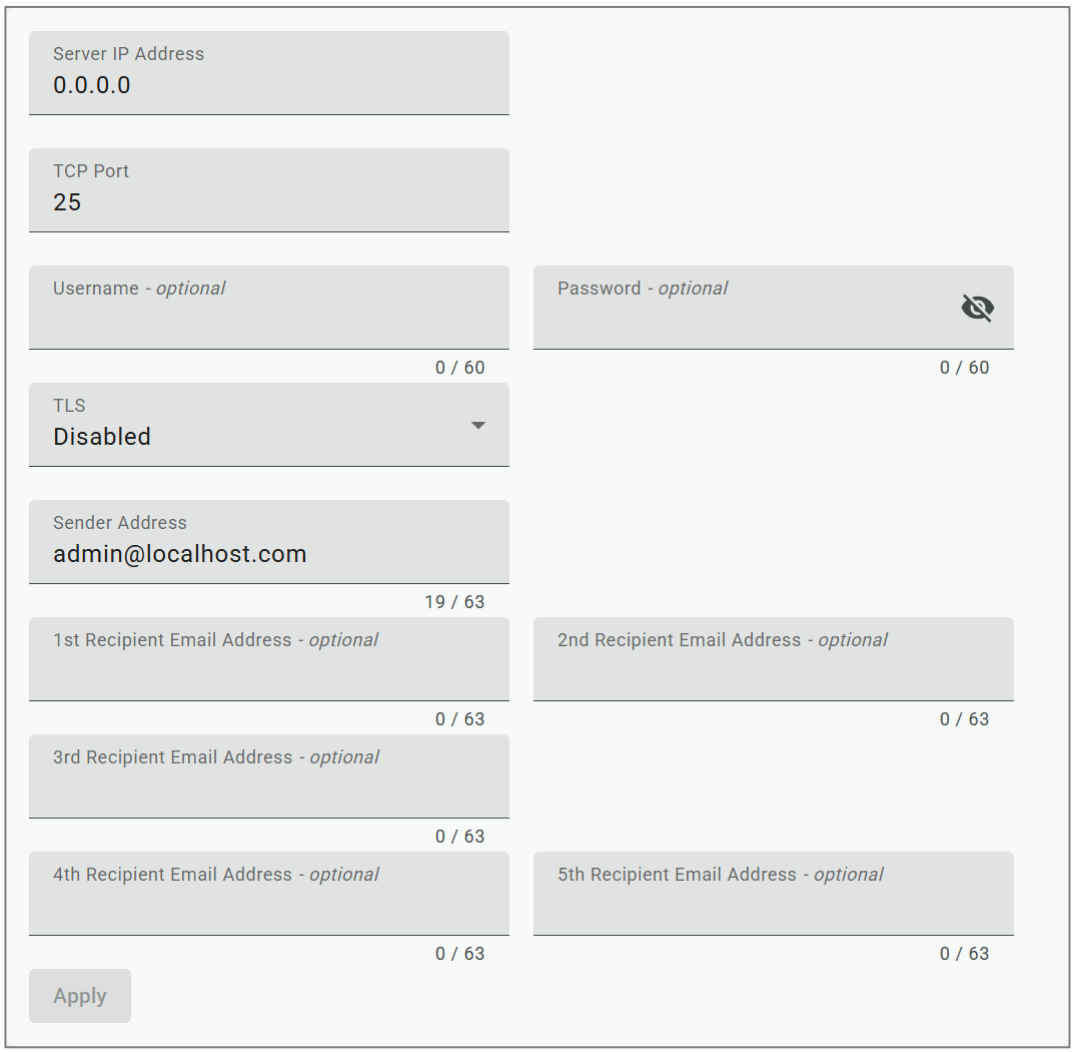
Email Settings lets you configure email notifications for important events. This lets you receive alerts directly in your inbox, providing a convenient way to stay informed about critical network issues.

Email Settings

Menu Path: Diagnostics > Event Logs and Notifications > Email Settings

This page lets you configure your device's email notification settings. You can specify which mail server and account to use, and which email addresses to send email notifications to.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the email server.	Valid IP address	N/A
TCP Port	Specify the TCP port of the email server.	1 to 65535	25
Username	Specify the username used to log in to the email server.	0 to 60 characters	N/A
Password	Specify the password used to log in to the email server.	0 to 60 characters	N/A
TLS	Enable or disable TLS (Transport Layer Security).	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Sender Address	Specify the sender email address to use for email notifications.	Valid email address up to 63 characters	N/A
1st/2nd/3rd/4th/5th Recipient Email Address	Enter an email address to send email notifications to. You can set up to 5 email addresses to send email notifications to.	Valid email address up to 63 characters	N/A

Chapter 4

Security Hardening Guide

This chapter provides an overview of security strategy, standards, and recommended best practices to improve the security landscape.

The threat landscape is constantly evolving, and no security guide can ever provide 100% protection. This chapter is constantly being expanded, and is not exhaustive.

Security Best Practices

Product Security

This section provides essential information on the installation of your product.

Account Management Guidelines

Manage user accounts, set passwords, and restrict access to authorized personnel only.

- Assign the appropriate account privileges.

  Limit the number of users with admin privileges to only those who need to perform device configuration or modifications. For other users, read-only access is sufficient. Moxa devices supports both local account authentication and remote centralized mechanisms, including Radius and TACACS+. This allows for flexible and secure access control options.

- Implement good password practices.

  Good password practices include:

  - Enabling and configuring a Password Policy to ensure your password meets specified requirements.
  - Setting the minimum password length to at least eight characters.
  - Require passwords to have at least one uppercase and lowercase letter, a digit, and a special character.
  - Set password expiration.
  - Replacing all default passwords and secure default accounts.
  - Use unique passwords.
  - Update passwords regularly.
  - Never share passwords.

Note

Based on trends in cybersecurity regulations, we recommend users increase the complexity of their passwords to the highest level to further strengthen password security.

- Verify and manage account activity.
    - Enable event logging and periodically check for login failures or irregular activity.
    - Consider centralized management or automation of log details.
    - Consider enabling account lockout. After too many sign-in attempts, the account can be deactivated or the source IP blocked. Evaluate operational impacts of account or IP blocks to ensure the right balance of security and continuous operation.
- Do not include sensitive information in user-configurable feedback.

Some messages can be configured, such as showing an error message after a failed login. Do not include any sensitive information in these messages, or any other information that might give an attacker an advantage. Possible sensitive information might include:

- Hints about accounts or passwords
- Unessary information about password requirements that might help an attacker narrow down brute force candidates.
- Detailed contact information for administrators that could be used in spearphishing attacks.

Physical Installation Guidelines

Physical protection of devices is vital to network security.With physical access to devices, prospective attackers can physically bypass security mechanisms, alter network conditions, or plant additional malicious devices in networks. Follow these tips to help reduce the risk of tampering with networking devices by unauthorized personnel.

- Install the device in an access-controlled area.

To further protect your device from potential physical attacks, it is important to conduct a risk analysis and implement appropriate physical security measures. Consider physical security like installation within a locked cabinet, surveillance,

security guards, and access control systems, among other measures. The specific measures you choose should be based on your environment and the level of risk you face.

- Install a Layer 2 switch within the security perimeter.

This perimeter can be established by setting up a firewall at the border, as the switch is not designed to be directly connected to the Internet. Note that the switch should not be classified as zone or boundary equipment. Avoid connecting the device directly to the Internet, as this can leave your network vulnerable to security breaches.

- Follow the Quick Installation Guide included in the package of your device.

It contains step-by-step instructions that are easy to follow and will help you set up the device quickly and efficiently.

- Examine and monitor anti-tamper labels applied to the device enclosures.

These labels provide a quick and easy way for administrators to determine if the device has been tampered with.

- Protect or deactivate any ports that are not currently in use.

Fewer active ports mean fewer avenues of attack. Refer to the Port Interface section in the User Manual.

- Protect reset buttons and other physical controls.

An attacker could bypass software/firmware security by forcing a reset and restoring default device credentials. Ensure that management interfaces, reset buttons, and other physical access routes are protect. For example, a device in a locked cabinet could still be vulnerable to being reset using a probe through a vent. Ensure that access to the locked cabinet is controlled, and that the reset button itself is covered or inaccessible from vents.

Protecting Vulnerable Network Ports

Understand security risks and mitigate them by configuring network ports correctly.

- Changing port numbers for active, including TCP port numbers for HTTP, HTTPS, Telnet, and SSH.
- Disable any ports that are not in use, as they could pose an unacceptable security risk.

- Use encrypted communication protocols wherever available.

Consider the following alternatives

  - HTTPS instead of HTTP
  - SSH instead of Telnet
  - SFTP instead of TFTP
  - SNMPv3 instead of SNMPv1/v2c
  - 802.1x with EAP-PEAP instead of MAC Authentication Bypass Refer to Network Interfaces for more information.

- Enable encryption for encryption-optional protocols.

Encryption-optional protocols (encryption) include:

  - 802.1x (EAP-PEAP authentication)
  - SNMPv3 (authentication and encryption)
  - Syslogs (TLS)

- Avoid using Ping Tracking to external devices (e.g. over the internet).
- Disable Loop Protection when no longer needed.
- Configure automatic session locking or idle timeouts so that idle sessions cannot be hijacked.
- Generate new SSL certificates and SSH keys for devices prior to using HTTPS or SSH applications.

Refer to SSH & SSL for more information.

Device Access Control Best Practices

Device access control is an essential aspect of network security that helps protect against unauthorized access to network resources.Unauthorized access can occur through various means, including physical access to network devices, hacking, or social engineering. Without proper access control measures in place, networks are vulnerable to security breaches, data theft, and other malicious activities.

Device access control is particularly important for organizations that handle sensitive data, such as financial institutions, healthcare providers, and government agencies. By

implementing device access control, these organizations can limit access to sensitive information and prevent security breaches. Below are some ways to ensure device access control:

- Adopt the **Principle of Least Privilege**.

This principle involves granting users, applications, or systems the minimum level of access or permissions they need to perform their specific tasks and nothing more. Requests for additional access, such as HTTPS, SSH, or Moxa services for administration, should be carefully evaluated before being approved.

- Use strong passwords.

Passwords should be complex and unique for each device. Passwords should also be changed regularly to maintain security.

- Implement allowlists.

Allowlists are authorized devices or users allowed to access a particular network resource. Allowlists can be managed at the device, network, or application levels. Network administrators can use allowlists to ensure that only authorized devices or users can access sensitive resources. The key feature of an allowlist is that anything not on the allowlist is automatically blocked, ensuring only authorized devices, uses, or services can operate freely in a network environment.

- Implement Traffic Storm Control
  Limits excessive broadcast traffic to maintain network performance. Broadcast storms can occur accidentally when devices are misconfigured, but they can also be a tool used in denial-of-service attacks.

About Device Integrity and Authenticity

Integrity and authenticity are vital elements of trust within a network.

Device integrity refers to the state of a device being complete, unaltered, and free from any unauthorized changes or modifications.

Authenticity refers to the assurance that the device is genuine and comes from a trusted source.

Both integrity and authenticity are critical aspects of device security. Methods to sustain these aspects include:

- Configuration Backup & Encryption

- Secure Boot

Configuration Backup and Encryption

Configuration backup and encryption protects a device's sensitive data and configuration by created an encrypted copy storing it securely. In the event of unauthorized device changes, correct configuration information can be quickly and securely restored.

The process involves creating a backup of the device's configuration and then encrypting it using a strong encryption algorithm. The encrypted backup is then stored securely to prevent unauthorized access. This process is particularly important for devices that store sensitive information, such as network equipment, servers, and other critical infrastructure. Encrypting the configuration backup ensures that the data remains protected even if the backup location is compromised.

Refer to Configuration Backup and Restore for more information.

Secure Boot

Secure Boot is a security mechanism designed to ensure that devices boot using only software that is verified as trusted. The primary function of Secure Boot is to prevent unauthorized software from running during the boot process. It achieves this by verifying the integrity and authenticity of the bootloader and firmware.

A bootloader refers to the initial software that runs when a device is powered on. Its primary role is to load the device's operating system. Firmware is software embedded within the device that manages and controls the device's hardware functions.

Moxa hardware makes use of cryptographic modules embedded in devices to support verification processes. The device's ROM (read-only memory) contains approved bootloaders and associated digital certificates, which are used to verify the integrity of the firmware.

When the device boots, the first thing to run is the bootloader. Secure boot checks the digital signature against the certificate stored in ROM. If the signatures match, the boot process continues. If they do not match, or there is evidence of tampering, the boot process halts to prevent potential security breaches.

Securing USB Interfaces on Network Devices

- Disable USB ports when not in use.

USB ports should be disabled by default to prevent unauthorized or accidental use.

- Limit rights to enable or configure USB ports to a minimum number of authorized users.

Use role-based access control (RBAC) or require multi-factor authentication (MFA) to enable USB ports.

- Standardize procedures and rigorously observe them.

Your procedures should cover:

  - When and why USB interfaces can be used
  - The type and number of USB devices permitted
  - How data on those devices must be secured. Ensure that all employees and users understand and observe these procedures

Device Resource Management and Monitoring

Moxa devices provide a number of features to help customers manage device resources efficiently and monitor security.

About Device Resource Monitoring

Network device resource management is essential for network reliability and security. By monitoring use of network resources, administrators can verify that network guidelines are being followed and devices are operating efficiently and effectively.

Proactive monitoring and management of device resources such as CPU utilization, memory utilization, and network traffic allows administrators to identify potential security breaches early, and help avoid network downtime and disruption. For example, abnormal spikes in network traffic or CPU utilization could be indicative of a malware infection or a denial-of-service attack.

Examples of activities to monitor include:

- Connected ports

- CPU usage
- Memory usage

Refer to Device Summary for more information.

About Event Logs for Monitoring

In addition to real-time monitoring and management, Moxa devices provide advanced logging options to help identify security events. Chosen event types can also generate notifications to notify administrators of unusual events where attention is needed, or to feed into larger security monitoring systems.

You can leverage system logs to monitor events, such as failed logins or access attempts from unauthorized accounts. Event logs respond the same way to the same events, providing comprehensive visibility into security events.

Refer to Event Log for more information about Event Logs.

Refer to Event Notifications for more information about Event Notifications.

Refer to SNMP - General for more information about SNMP configuration.

About Port Mirroring for Monitoring

Port Mirroring duplicates data transmitted over a port for analysis.

You can use port mirroing to mirror the trafic of an Ethernet port connected to untrusted networks to allow for monitoring and analysis of trafic that would otherwise be uncontrolled.

Refer to Port Mirroring for more information.

Recommended Settings for Services and Features

When prioritizing device security, the first point of assessment is often the network interfaces and services.By deactivating unneeded interfaces and services, one can reduce potential vulnerabilities and associated security threats. Additionally, activating the appropriate security features enhances early anomaly detection and bolsters the device's defense against cyber attacks.

Note

Factory defaults are described in each feature section.

Common Protocols and Ports

Service Name	Default Port	Default Setting	Security Suggestions
HTTP	TCP 80	Enabled	Disable if possible to avoid leaks from unencrypted traffic.
HTTPS	TCP 443	Enabled	
Telnet	TCP 23	Enabled	Disable if possible to avoid leaks from unencrypted traffic.
SSH	TCP 22	Enabled	
NTP/SNTP	UDP 123	Disabled	Use SNTP to synchronize system time if possible. Enable NTP authentication if possible.
SNMP	UDP 161 UDP 162 TCP 10161 TCP 10162	Disabled	For V1 & V2c, change default community string names, i.e. public & private, to other unique names. For V3, enable SNMP admin account authentication.
Syslog	UDP 514	Disabled	Enabling Syslog is recommended to avoid missing critical logs due to limited local storage. This sends logs to an external syslog server, where they can be securely stored and retained. The syslog server is responsible for keeping these logs for a minimum period required by local regulations, ensuring critical incidents are properly documented and accessible when needed.
RADIUS	UDP 1812	Disabled	Enabling RADIUS authentication can help administrators manage password changes more efficiently.
Moxa Services	TCP 443 UDP 40404	Enabled	These 2 ports are only used by the Moxa management software. Disable it if you don’t use Moxa management software.

Security-Related Functions

Function	Default Setting	Security Suggestions
Password Policy	Disable	Enable password policy to comply enterprise security policies.
Login policy	Disable	Enable a login policy to heighten resistance against brute force attacks and terminating any inactive login sessions.
Malformed Packets Filtering	Disable	The "Malformed Packets Filtering" feature logs events at a user-defined severity level whenever the system discards malformed packets. Depending on the protocols active in your network, you can choose to enable this feature or leave it disabled.
DoS Policy	None	Select a DoS policy according to your network traffic to increase network robustness.
Session control	None	Configure session control policies appropriate for your traffic to improve network reliability.
802.1X over ports	Disable	Enable 802.1X port authentication to block unauthorized LAN access.
Traffic Storm Control	Enable	Enable Traffic Storm Control to manage the amount of unknown traffic on the network.
Trusted Access	Enabled	By default, the device permits all connections from the LAN attempting to access it. For enhanced security, block all LAN connections attempting to access the device. Then, use a trusted IP list to specify which trusted IPs are allowed access to the device.
Static Port Lock	Disable	Static port lock, also known as MAC Table or MAC Sticky, is a port security feature that remembers the first MAC address used, and will not initiate links with other MAC addresses.

Caution

The following are known to have security flaws:

Use alternatives or take extra precautions

Protocols/Services with Weak Authentication/Encryption

Some protocols and services support weaker authentication or encryption, and may not be secure over untrusted networks.

Choose secure alternatives or take precautions to mitigate possible threats.

Services

- TACACS+
- RADIUS
- 802.1x
- MAB
- NTP server
- NTP/SNTP client
- PTP
- DHCP relay
- mDNS
- Tracking
- Email notification
- TFTP
- SNMP v1/v2
- GVRP/GMRP
- DNS client

- DNS server
- DHCP client
- DHCP server
- LACP
- Loop protection
- LLDP
- IGMP snooping

Redundant Protocols

- MRP
- TruboRing v2
- TurboChain
- RSTP/MSTP

Industrial Protocols

- MMS server
- Ethernet/IP
- Modbus TCP
- Profinet
- GOOSE check

L3 protocols

- RIP (NOS v6.0)
- BFD (NOS v6.0)
- VRRP
- PIM-DM
- PIM-SM

Common Threats and Countermeasures

These are examples of common known threats, and suggestions for mitigation.

Incident Category	Detailed Description	Mitigation Suggestions
Tampering & Information Disclosure	An attacker can read or modify data transmitted over HTTP data flow.	Disable HTTP, and replace HTTP transmission with HTTPS.
Tampering & Information Disclosure	An attacker can read or modify data transmitted over Telnet data flow.	Disable Telnet, and replace HTTP transmission by SSH.
Information Disclosure	Data flowing across TFTP may be sniffed by an attacker.	Use SFTP instead of FTP.
Denial of Service	SNMP Server crashes, halts, stops or runs slowly by excessive quires.	Enable rate limit to stop excessive SNMP requests.
Denial of Service	RADIUS Server crashes, halts, stops or runs slowly by excessive quires.	Enable rate limit to stop excessive RADIUS requests.
Repudiation	Devices fail to synchronize a system time with a trusted NTP/SNTP server.	Enable NTP authentication to verify a connection with the trusted NTP/SNTP server.

Note

Create an incident response plan and follow it carefully. Ensure your procedures allow for user reporting and admin response to those reports. Many threats manifest themselves as irregular device behavior – such as device inability to provide basic services like routing or firewall functions, which in turn lead to interruptions or unauthorized access. Create a plan that allows admins to prepare, reboot, and monitor devices with abnormal behavior.

Recommended Operational Roles and Duties

Adhering to the principle of least privilege reduces risks by ensuring users operate at the minimum privilege required to complete their tasks.

Instead of individual allocation, privilege levels should be tied to specific job functions. For optimized device security, we recommend three distinct privilege levels, each tailored for different management needs.

Note

Customize user roles based on your organization needs, and eliminate unneeded roles.

Administrator

Designated for system management, this privilege level permits:

- Creation and deletion of configuration objects, files, and user accounts.
- Monitoring system status and resources.
- Modifying parameter values.
- Reviewing stored data within the device.

Administrator Responsibilities:

- Reset and periodically change the default administrator password.
- Ensure password complexity aligns with enterprise security policies.
- Manage and authorize individuals with appropriate access privileges.
- Disable non-essential interfaces or network services.
- Enable secure communication protocols to guard against data breaches.
- Regularly update firmware to address potential vulnerabilities.

Supervisor

Tailored for network experts or operators, this privilege grants:

- Monitoring of system status and resources.
- Adjusting values in configuration objects or files.
- Access to review data stored in the device.

Supervisor Responsibilities:

- Continuously monitor system status and resources to maintain device functionality.
- Routinely verify the integrity of device configuration objects and files.
- Manage trusted devices through IP and MAC allowlisting.

- Oversee and respond to system alerts to preempt device failures and security threats.

Auditor

Reserved for audit-focused personnel, this level allows:

- Monitoring of system status and resources.
- Reviewing data stored within the device.

Auditor Responsibilities:

- Regularly inspect logs to identify and assess incidents and their associated risks.

Moxa devices provide three user privilege categories: admin, supervisor, and user. We advise aligning the admin role for administrator users, the supervisor role for supervisor users, and the user role for auditor users.

Recommended Patching and Backup Practices

Moxa's guidance on ensuring device security through regular firmware upgrades and configuration backups.

Configuration Backup

For network operators and system administrators, it is essential to regularly back up device configurations. This precaution allows for quick recovery in unforeseen scenarios, such as cyber attacks.

> **Note**
>
> Prioritize use of secure transfer protocols – such as SFTP – for file transfers to protect the configuration maintenance process.

Recommendations for Vulnerability Management

As the adoption of the Industrial IoT (IIoT) continues to grow rapidly, security becomes an increasingly high priority.

The Moxa Product Security Incidence Response Team (PSIRT) takes a proactive approach to protect our products from security vulnerabilities and help our customers better manage security risks.

To report vulnerabilities for Moxa products, please submit your findings on the following web page: https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability.

For the most up-to-date Moxa security information, please visit our security advisory page: https://www.moxa.com/en/support/product-support/security-advisory

Recommendations for Decommissioning

To avoid any sensitive information such as account passwords or network configurations from disclosure, always delete all imported certificates and reset devices to factory default before you decommission your devices.

Note

Things to keep in mind when decommissioning or re-purposing devices:

- Device data can be cleared using the Factory Reset options. When reseting devices, make sure to confirm the operation and allow it sufficient time to complete.
- Delete all logs, and verify deletion.
- After all reset processes are complete, verify that all sensitive data has been cleared.

Security Standards and Concepts

Introduction to Defense in Depth

The Defense-in-Depth strategy is used to protect systems from various types of attacks by using multiple independent defense mechanisms.This involves incorporating multiple layers of security to protect the product against potential attacks and vulnerabilities at various stages of its design, development, and use.

It is crucial to understand that no single protection can guarantee complete security. That's why the Defense-in-Depth approach makes it difficult for attackers to leverage one weakness to attack the product or network as a whole. This approach requires attackers to overcome multiple obstacles undetected, increasing the difficulty level. By leveraging multiple security features and layers of protection in a product, vulnerabilities in any one layer can be mitigated.

About AAA - Authentication, Authorization, and Accounting

Authentication, **A**uthorization, and **A**ccounting (AAA) is a user-based access control paradigm.AAA coexists with other security practices. While product security and network security focus on device or process security, AAA focuses on users.

AAA comprises a set of functions for an administrator to determine which users can access a network device, which services are available to authorized users, and collect information about user activities for audits or charging purposes if required. When implemented well, AAA can provide an extra layer of security across different aspects.

Authentication

Authentication provides a method of identifying a user before access to the network device is granted, typically by having the user enter a valid username and password and/or provide a physical token or digital certificate. Additional policies such as a password complexity check or login failure lockout can also increase access security.

Authorization

After authentication is successful, a user can be authorized to use specific resources on the device or perform specific operations. For instance, a normal user with limited permissions may only view the device's system settings, whereas an administrator would have full control to view or edit all system settings.

Accounting

Accounting keeps track of user activities on the device. It monitors the resources a user consumes during network access. This can include the amount of data sent and received through an Ethernet port or the number of user login failures.

About Authentication Types

Handle authentication with the local device exclusively, or with a remote server using local accounts only as a fallback.

It is important to choose the right authentication method, or combination of authentication methods for your network environment and use case. Moxa devices offer the following authentication options.

Local Authentication

Local authentication uses the accounts and settings stored on the local network device to identify users (authentication), determine which services they can use (authorization), and track basic user activities such as amount of data transferred or number of login failures (accounting).

Remote Authentication

Remote authentication uses accounts configured on a RADIUS server - allowing AAA to be configured from a single, centralized location. However, it is important to note that local authentication is retained as a fallback mechanism to ensure the device can be configured if the RADIUS server becomes inaccessible. Additionally, Moxa products support backup RADIUS servers if the primary becomes inaccessible. Due consideration should be given to the configuration and maintenance of backup servers for redundancy.

Features	Local	Remote
Configuration location	Local device	Remote RADIUS server, local as fallback
Number of accounts	Few	Many
Password security requirements	Limited	Many
Allowed services	Specified locally	Determined by server
Authority types	Admin, User, Supervisor	Admin, User
User feedback on failed login	Custom prompt	Server-defined
Setup effort	Low	High
***Allowed services are usually dependent on authority types.**		

Example: Creating a Local User

Local accounts are authenticated and managed by the local device, and function even when remote RADIUS servers are unavailable.

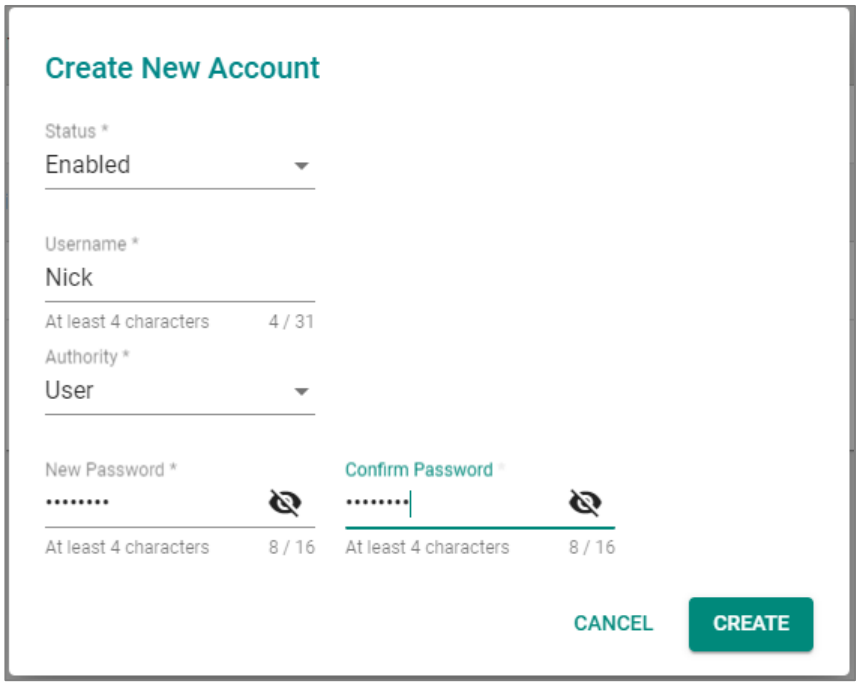
Make sure you have an account with **Admin** authority.

In this example, create a local user with simple **User** level authority to fill the Authentication of the AAA tripod. Once the user has been created, add additional access controls.

1. Sign in to the device with admin credentials.
2. Go to **System** > **Account Management** > **User Accounts**, and then click ***[Add]***.

   The Create New Account panel appears.
3. Set **Status** to **Enabled**.
4. In the **Username** field, type `Nick`.
5. Set **Authority** as **User**.
6. In the **New Password** field, type `1qaz!@#$`, and then type again to confirm.
7. Click **Create**.

By creating the user **Nick**, Authorization and Accounting details can now be configured.



Now that a user account has been created, add account controls. Account controls allow setting a warning for incorrect passwords, account lockouts, and automatic logout.

Example: Configuring Account Controls for Local Users

Login Failure Account Lockout and Auto Logout increase the security of local accounts.

Make sure you have set **Authentication Protocol** as **Local** or **RADIUS, Local** to ensure that local accounts can be used to **Security** > **Authentication** > **Login Authentication**.

Enabling additional account controls can increase resistance to brute-force attacks as well as enable troubleshooting. This example demonstrates how to set account lockouts after failed login attempts and manage idle users.

1. Sign in to the device with administrator credentials.
2. Go to **Security** > **Device Security** > **Login Policy**.

   The Login Policy panel appears.

3. In the **Login Authentication Failure Message** field, type the following:
   `Warning! The account will be temporarily locked if there are too many consecutive login failures.`

Note

Do not configure the message with any information that might help an attacker guess a password or conduct phishing operations, such as password hints or staff contact information.

4. Set **Login Failure Account Lockout** to **Enabled**.
5. In the **Login Failure Retry Threshold** field, type `3`.

   This is the number of failed attempts before the user account will be temporarily blocked.

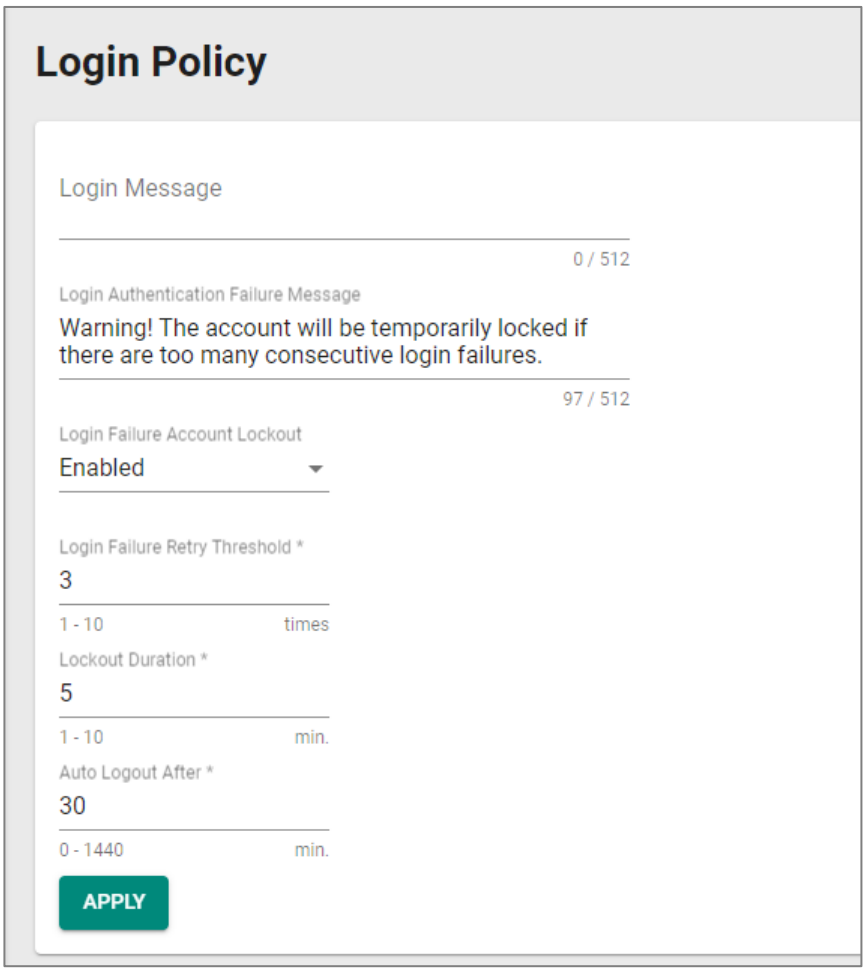
   Temporary can bans help prevent password guessing and brute force attacks by preventing attackers from rapidly guessing many passwords.
6. In the **Lockout Duration** field, type `5`.

   This specifies the number of minutes the account will be locked.
7. In the **Auto Lockout After** field, type `30`.

   This is the amount of time in minutes before inactive accounts automatically log out.

This configuration:

- Displays a warning message on failed login attempts, enabling troubleshooting
- Blocks accounts for five minutes after three unsuccessful login attempts, limiting the effectiveness of credential guessing
- Automatically logs out inactive user accounts after thirty minutes, reducing risks of unauthorized access through idle consoles



Optionally, configure allowed access protocols.

Example: Configuring a Remote RADIUS Server

In this example, the RADIUS server handles all Authentication, Authorization, and Accounting.

Make sure you have a working RADIUS server and corresponding configuration information. In our example, we use a server that has the following settings:

- PAP authentication protocol
- An address of `192.168.127.1`
- UDP port 1812
- A preconfigured shared key

Remote Authentication Dial-In User Service (RADIUS) servers may make it easier to manage large numbers of users from a central location.

1. Sign in to the device with admin credentials
2. Go to **Security** > **Authentication** > **Login Authentication**, and then set **Authentication Protocol** to **RADIUS, Local**.

This setting will use the remote RADIUS server as the primary authentication source, and use local authentication as a fallback if the RADIUS server is unavailable.

> **Note**
> Enabling a RADIUS authentication will not remove local accounts. Make sure local accounts have a strong, unique password. Local accounts are still required both for RADIUS server configuration as well as for local fallback if the RADIUS server is not reachable. Go to Security > Authentication > RADIUS.

3. The RADIUS Server will appear.
4. Configure all of the following:

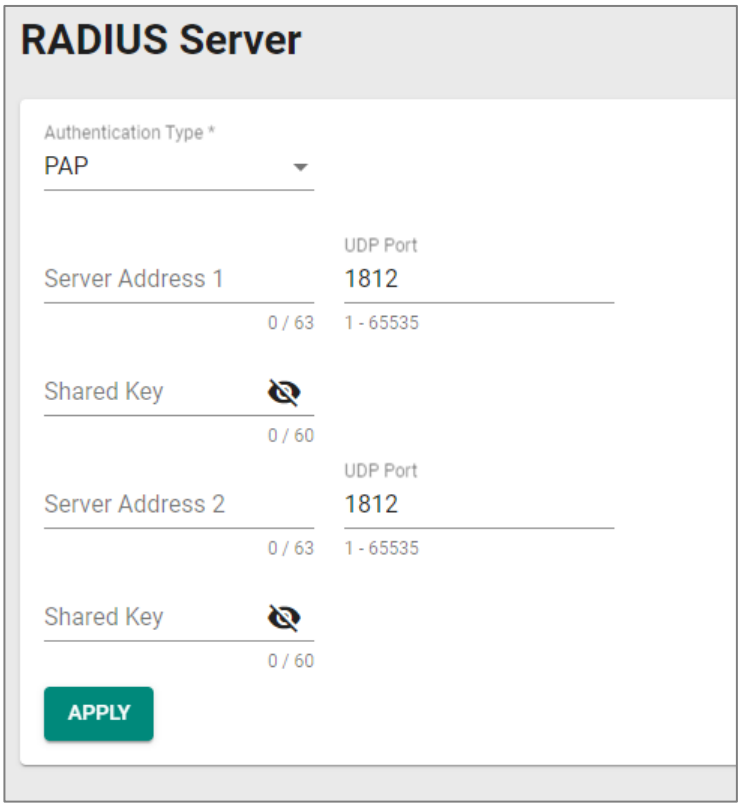
Field	Setting
Authentication Type	**PAP**
Server Address 1	192.168.127.1
UDP Port	1812
Shared Key	Enter your Shared Key here.

These configuration options are provided as an example only, and will need to match your network environment.

5. Click **Apply**.

By configuring a remote authentication, the network device will redirect user login requests to the RADIUS server. When logging in with remote user `Peter`, the RADIUS server will process the authentication request and determine whether to grant access to the device. If `Peter` does not match RADIUS or Local information, access will be denied.

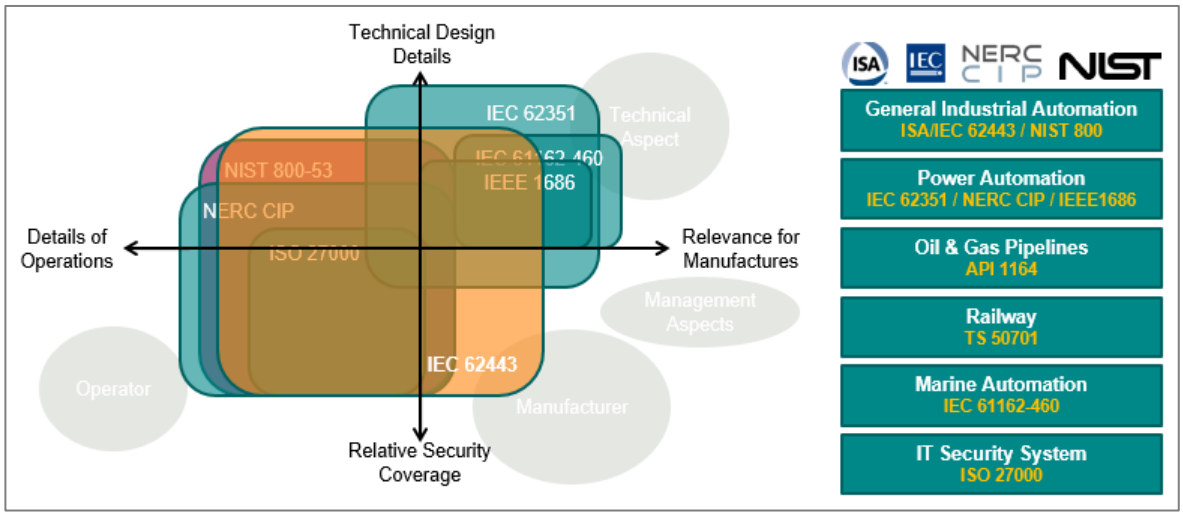
In situations where the RADIUS server is not reachable or unavailable, users such as `Nick` or other existing local users can still access the network device using their local passwords.



ISA/IEC 62443 Standards and Architecture

Security Reference Standards

In the field, large networks are connected through switches and routers. These devices manage all data traffic and serve as the main bridge between devices. However, if these switches and routers are compromised, the repercussions can cascade to all connected devices. To help mitigate this risk, Moxa implements the ISA/IEC 62443-4-2 standard into our network device designs.



Industries such as electricity, oil and gas, rail transportation, and maritime have established their own standards for security. These standards include guidelines and regulations designed to address each industry's unique concerns. Among these standards,62443 is the most comprehensive, covering a wide range of industries and security concerns, making it an excellent choice for organizations that prioritize security in their operations.

ISA/IEC 62443 Standards and Architecture

The ISA/IEC 62443 standard is a set of guidelines and best practices designed to help organizations secure their industrial automation and control systems (IACS) against cyber threats. The framework helps assess risks to IACS and implement appropriate security measures to protect against cyber attacks and malware. The standard consists of multiple parts, with each covering different aspects of industrial cybersecurity.

Parts of ISA/IEC 62443	Scope	Sections
ISA/IEC 62443-1	General	Part 1-1: Terminology, concepts, and models Part 1-2: Master glossary of terms and abbreviations Part 1-3: System security compliance metrics Part 1-4: IACS security lifecycle and use-cases

Parts of ISA/IEC 62443	Scope	Sections
ISA/IEC 62443-2	Process and Program requirements	Part 2-1: Establishing an industrial automation and control system security program Part 2-2: Implementation guidance for an IACS security management system Part 2-3: Patch management in the IACS environment Part 2-4: Security program requirements for IACS service providers
ISA/IEC 62443-3	Systems	Part 3-1: Security technologies for industrial automation and control systems Part 3-2: Security risk assessment and system design Part 3-3: System security requirements and security levels
ISA/IEC 62443-4	Components	Part 4-1: Secure product development lifecycle requirements Part 4-2: Technical security requirements for IACS components

Product suppliers adhere to the ISA/IEC 62443 standard to provide components for Industrial Automation and Control System \(IACS\) solutions. These components can be:

- Individual items
- Combined products forming a system or subsystem

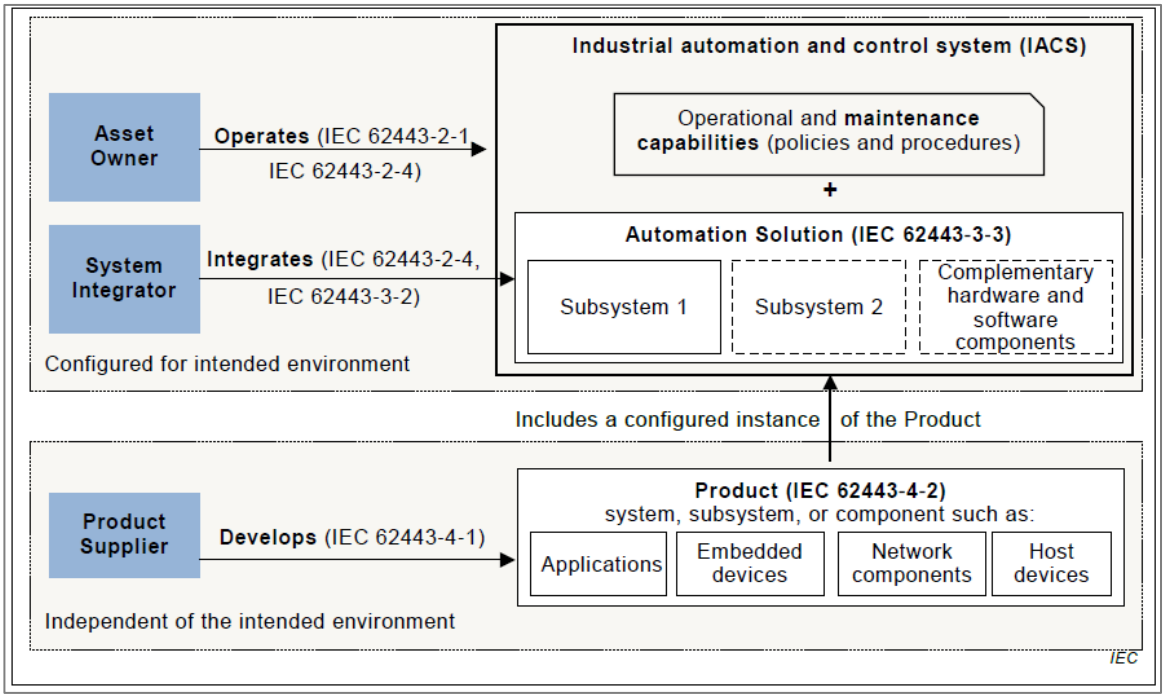
Additionally, system integrators use the following sections of the ISA/IEC 62443 standard:

- IEC 62443-2-1
- IEC 62443-2-4
- IEC 62443-3-2
- IEC 62443-3-3

These standards help integrators:

- Determine security zones
- Specify security capability levels for each zone
- Integrate products into an Automation Solution

General ISA/IEC 62443-1	ISA-/IEC 62443-1-1 Foundational Requirements (FR)
System **ISA/IEC 62443-3**	ISA-/IEC 62443-3-3 System Requirements (SR)
Component **ISA/IEC 62443-4**	ISA-/IEC 62443-4-2 Component Requirements (CR)



Establishing Foundational Requirements

FR 1	Identification and Authentication Control
FR 2	User Control
FR 3	System Integrity
FR 4	Data Confidentiality
FR 5	Restricted Data Flow

FR 1	Identification and Authentication Control
FR 6	Timely Response to Events
FR 7	Resource Availability

Once an organization settles on target security levels, foundational requirements can help further specify requirements based on the seven foundational security functions \(FRs\). The ISA/IEC 62443 framework includes:

- **System Requirements (SRs)**: Detailed in Part 3-3, these are guidelines for those shaping the system's overall architecture.
- **Component Requirements (CRs)**: Outlined in Part 4-2, they cater to designers focusing on individual components.

Both system and component designers reference these standards, ensuring the final product's security aligns with what the asset owner's requirements. This methodology not only bolsters the product's defense against specific threat levels but also optimizes resource utilization among stakeholders. As a side note, every FR from Part 1-1 is paired with four distinct security levels, which trace back to standards set in Parts 3-3 and 4-2. For simplicity in cross-referencing, CRs are numerically aligned with their corresponding SRs.

Component Requirements

Part 4-2 extends the SRs from Part 3-3 by introducing CRs tailored for a variety of IACS components. These components fall under four broad categories.

Generic	Specific
Component Requirements (CR)	Software Applications
Embedded Devices	
Host Devices	
Network Devices	

While a majority of Part 4-2's criteria are generic and apply uniformly across categories, there are exceptions. Unique, component-specific stipulations are clearly signposted, with

exhaustive details available in dedicated clauses. For details, consult the original standards.

Requirement Enhancements

CRs may contain one or more requirement enhancements (RE). REs are additional requirements attached to CRs that add additional conditions to accommodate higher security levels.

Applying FR 1: User Identification and Authentication

FR 1 codifies the principle that all users—humans, software processes, or devices—must first be identified and authenticated before accessing systems or assets.

Recognizing the need to verify different kinds of users, FR 1 uses the following CRs:

- **CR 1.1** focuses on human users.
- **CR 1.2** addresses software processes and devices.

Identification vs. Authentication: Consider a person's ID card. While the card identifies its owner, can someone else misuse it? Certainly. Here, the distinction between 'identifying' (matching a person to an ID card) and 'authenticating' (confirming the card holder's authenticity) becomes crucial. Each process has distinct methods and requirements.

Understanding CR and RE in Determining Security Levels: CR represents foundational requirements, whereas RE (related entity) accounts for advanced needs. Together, they define the security capacity of a component. Each component's security level, according to FR, ranges from 0 (no requirements) to 4.

For instance:

- **Security Level 1**: Implementing basic identification and authentication for all human users.
- **Security Level 2**: Incorporates RE1 - uniquely identify and authenticate users, like using ID cards for employees.
- **Security Level 3**: Engages RE2 - multifactor authentication.

Multifactor Authentication Unraveled: Typically, this methodology hinges on:

1. **Knowledge**: Passwords or PINs.

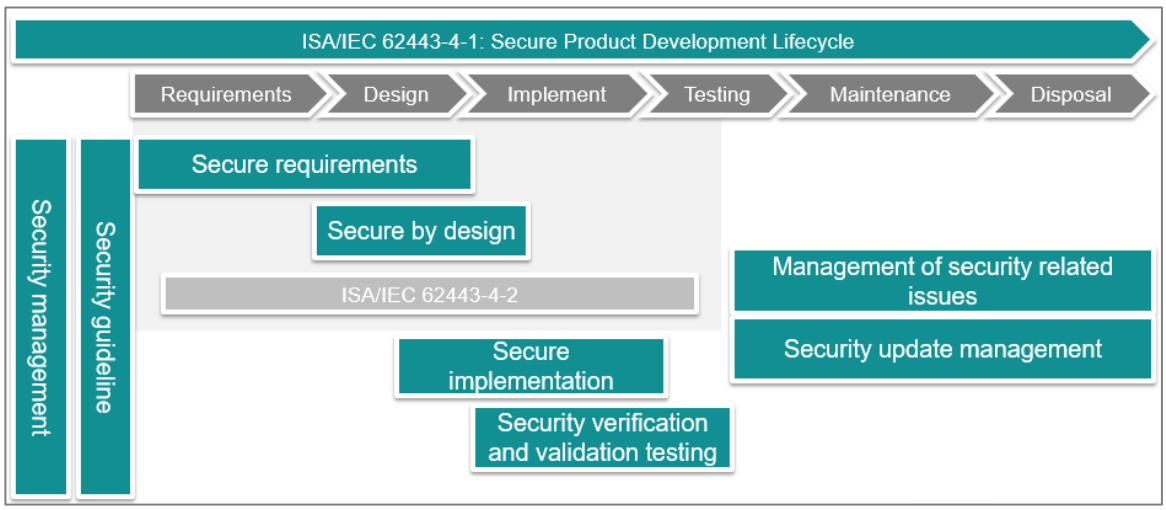
2. **Possession**: Devices like smartphones or security keys.
3. **Inherence**: Biometrics such as fingerprints.

To achieve Level 3, a combination of at least two of these factors is essential.

Security Level	Attack Type				
	Example Threat Actor	Violation Type	Means	Resource Level	Motivation
SL-1	• Ordinary user	Coincidental	N/A	N/A	N/A
SL-2	• Entry-level hacker	Intentional	Simple	Low	Low
SL-3	• Terrorist Organization • Organized crime	Intentional	Sophisticated	Moderate	Moderate
SL-4	• Nation state	Intentional	Sophisticated	Extended	High

Product Lifecycle and Security

Component security plays a role throughout the product lifecycle



How Moxa applies ISA/IEC 62443-4-1

Our commitment to security includes to adhering to the ISA/IEC 62443-4-1 standard, considering security at each stage of the product's lifecycle. This includes the safeguarding of our corporate network, keys, secure design and implementation

proficiencies, testing processes, and post-sales services. Our approach involves extensive training and certification of all team members associated with product design, execution, and assistance. Moreover, we offer robust support mechanisms like vulnerability handling and patch management.

Component Security with IEC 62443-4-2

IEC 62443-4-2 serves as a guide for product suppliers, helping us decipher the specific security capability benchmarks for control system components. This standard not only clarifies which requirements should be assigned but also pinpoints those that must be integral to the components. The fusion of these component requirements with their enhancement requirements defines the component's target security level.

Chapter 5

Appendix

Advanced Mode Settings

This table shows settings that are only available in **Advanced Mode**.

Location in UI	Advanced Mode Items
System > Management Interface > User Interface	• Moxa Service settings
Port > Link Aggregation	• Link Algorithm setting • Link Aggregation Port List
Port > PoE - Scheduling	• PoE - Scheduling tab
Layer 2 Switching > VLAN - Settings **Layer 2 Switching > VLAN - Status**	• Forbidden Port setting
Layer 2 Switching > QoS > Ingress Rate Limit	• Type setting • CBS setting • EBS setting • Mode setting • Conform Action setting • Exceed Action setting
Layer 2 Switching > QoS > Egress Shaper	• CBS setting
Layer 2 Switching > Multicast > IGMP Snooping - VLAN Settings	• Startup Query Interval information • Startup Query Count information • Other Query Present Interval information
Layer 2 Switching > Multicast > Static Multicast	• Forbidden Port setting
IP Configuration	• IPv6 settings
Redundancy > Spanning Tree - General	If **STP Mode** is **STP/RSTP**: • Link Type setting
Redundancy > Spanning Tree - Guard	• Root Guard setting • Loop Guard setting
Redundancy > Spanning Tree - Status	• Root Inconsistency information • Loop Inconsistency information

Location in UI	Advanced Mode Items
Security > Network Security > IEEE 802.1X - General	• Reauthentication Period setting • Server Timeout setting • Supp Timeout setting • Tx Period setting
Security > Network Security > Access Control List - Settings	If **Rule Type** is **Permit**: • Rate Limit Type settings

CEF Message Format for Event Logs

The CEF message format for Moxa switch event logs contains the following information:

`CEF: Version|Device Vendor|Device Product|Device Version|CEF Event ID|Event Name|Severity|Extension (Key + Value)`

Example CEF message:

`CEF:0|Moxa|RKS-G4028-L3-4GS-HV-T|v6.0 Build 2025_1201_1045|0x4000040e|Topology change (Turbo Ring)|5|index=1`

Version

This indicates the CEF Specification version used for the message.

Device Vendor

This shows the vendor of the device the message comes from, e.g., `MOXA`.

Device Product

This shows the product name of the device the message comes from, e.g., `MDS-G4028`, `TN-4500B`.

Device Version

This shows the version number of the device the message comes from, e.g., `v5.0 Build 2023_1206_1706`.

CEF Event ID

The CEF event ID definition has a length of 8 bytes, with different bytes used to carry specific information.

To see which event corresponds with a specific CEF Event ID, refer to Event Log Descriptions.

Bytes 0-1: OS Identification

The first two bits are used for OS encoding:

- `01` = MX-NOS
- `10` and `11` = reserved
- The remaining 6 bits are currently undefined and reserved.

For example, MX-NOS would be `01` (MX-NOS) + `000000` (reserved bits) = `01000000`

Converting this binary code to hexadecimal will result in **0x40**.

Bytes 2-3: Revision

This field indicates the revision number. The first version is **0x00**. This field should be incremented if there are changes to the event's severity or name.

Bytes 4-5: Classification System (Feature ID)

This field contains the Feature ID.

Menu Tree Title	Feature ID
System	0x00
Port	0x01
Layer 2 Switching	0x02
IP Configuration	0x03
Redundancy	0x04
Network Service	0x05
Security	0x06
Diagnostics	0x07

Menu Tree Title	Feature ID
Provisioning	0x09

Bytes 6-7: Sequence Number

This field contains the sequential number for the event. The first ID is **0x00**.

Event Name

This field refers to the name of the event.

Severity

This field describes the severity of the event, with higher numbers indicating higher severity.

Standard syslog severity levels are mapped to the Common Event Format (CEF) severity levels as follows:

Syslog Severity	CEF Severity	Description
0	10	Emergency
1	8	Alert
2	7	Critical
3	6	Error
4	5	Warning
5	4	Notice
6	1	Informational
7	0	Debug

Extension (Key + Value)

This contains additional information that follows the **Extension (Key + Value)** format, based on Chapter 2 of *Micro Focus Security ArcSight Common Event Format Version 25*.

For parameters that do not have a proper key name in the above document, the Moxa defined CEF key names are as follows:

CEF Key Name	Full Name	Data Type	Length	Meaning
dportIndex	destinationPortIndex	String	7	The index of target (destination) ports: the index of a port or port-channel.
dportType	destinationPortType	String	15	The type of target (destination) ports: Port or port-channel.
drole	destinationRole	String	31	The role of the target ports or device in the protocol,. e.g., for RSTP, the port roles include root port, destination port, alternate port, backup port, and disabled port.
dstate	destinationState	String	15	The state of the targeting systems/ports/functions. One state example for interfaces is up or down.
index	indexValue	Integer	N/A	The alphabetical list of names, subjects, etc. related to the pages on which they are mentioned. e.g., Index of module, index of power input, index of port
intfIp	interfaceIP	IPv4 Address	N/A	The interface IP address. In Layer 3 switches, each interface has its own IP address.
intfName	interfaceName	String	15	The interface name used to identify an L3 interface. e.g., vlan1, vlan10
intVlan	interfaceVlan	Integer	N/A	The interface VLAN. In Layer 3 switches, each interface has its own VLAN ID.
method	method	String	15	The media used for file operations such as backup, restore or firmware upgrade. e.g., HTTP/HTTPS, SFTP , TFTP, ABC-02, ABC-03
moduleType	TypeOfModule	String	7	The type of module responsible for generating the event. e.g., Management module(MGMT)/Power Module(PWR1 or PWR2)
netAddr	networkAddress	String	31	The range of an IP network.

CEF Key Name	Full Name	Data Type	Length	Meaning
nodeType	IreRemNodeType	String	15	Doubly Attached Node (DAN) type used in PRP/HSR, as indicated in the received supervision frame.
sportIndex	sourcePortIndex	String	7	The index of ports responsible for generating the event: the index of a port or port-channel.
sportType	sourcePortType	String	15	The type of ports responsible for generating the event: Port or port-channel.
srole	sourceRole	String	31	The role of the ports or device in the protocol responsible for generating the event. e.g., for RSTP, the port roles include root port, destination port, alternate port, backup port, and disabled port.
sstate	sourceState	String	15	The state of the systems/ports/functions responsible for generating the event. One state example for interfaces is up or down.
threshold	thresholdValue	Floating Point	N/A	The threshold value that must be reached to trigger an action.
value	valueOrNumber	Floating Point		A number value. e.g., power value, number of packets, priority value
vlanId	vlanID	Integer	N/A	The ID of the VLAN.

Configuration Types

This table describes the different types of configurations that your device uses.

Configuration Type	Description
Startup Config	The configuration that is loaded when the device boots up. These settings persist even when the device is powered off.
Running Config	The configuration that is currently in use by the device. • **If auto-save is enabled**, all changes will be saved to the startup config, and will be retained when the device powers off. • **If auto-save is disabled**, any unsaved changes will be lost when the device powers off. Refer to Disable/Enable Auto Save for more information.
Factory Default Config	The pre-defined factory default configuration of your device. This configuration cannot be changed.
Custom Default Config	A user-defined default configuration saved on the device. • Users can define a custom default configuration by saving the current startup configuration as a custom default. Refer to Save Custom Default for more information.

Event Log Descriptions

This section details the different events that can be recorded in the event log files.

Events are organized by classification.

Event log descriptions include the following information:

Severity	Severity of the event.
Event Description	Event description used for the legacy message format and the event name in the CEF message format. Double braces {{ }} indicate placeholders for event-specific text that will be provided by the device.
Classification	Classification of the event, which follows the menu tree structure in the device's web UI.
CEF Event ID (Hexadecimal)	8-byte CEF event ID for the event.
CEF Event ID (Decimal)	Decima CEF event ID for the event. This is the CEF Event ID that appears in Moxa CEF messages.
Arg1 - Arg6	Additional information for the event that appears in the Extension (Key + Value) part of the CEF message format.

System

Cold start

Severity	Critical
Event Description	System has performed a cold start.
Classification	System
CEF Event ID (Hexadecimal)	0x40000000
CEF Event ID (Decimal)	1073741824
Arg1	-
Arg2	-
Arg3	-
Arg4	-

Arg5	-
Arg6	-

Warm start

Severity	Notice
Event Description	System has performed a warm start.
Classification	System
CEF Event ID (Hexadecimal)	0x40000001
CEF Event ID (Decimal)	1073741825
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Configuration change by user

Severity	Notice
Event Description	Configuration {{modules}} changed by user {{username}}. If user configure through SNMPv3: Configuration {{modules}} changed by {{username}} via snmp service.
Classification	System
CEF Event ID (Hexadecimal)	0x40000002
CEF Event ID (Decimal)	1073741826
Arg1	sourceServiceName
Arg2	suser
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Login success

Severity	Notice
Event Description	[Account: {{user_name}}] successfully logged in via {{interface}}.
Classification	System
CEF Event ID (Hexadecimal)	0x40000003
CEF Event ID (Decimal)	1073741827
Arg1	suser
Arg2	app
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Login failure

Severity	Warning
Event Description	[Account: {{user_name}}] failed to log in via {{interface}}.
Classification	System
CEF Event ID (Hexadecimal)	0x40000004
CEF Event ID (Decimal)	1073741828
Arg1	suser
Arg2	app
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Login lockout

Severity	Warning
Event Description	[Account: {{user_name}}] locked due to {{failed_times}} failed login attempts.

Classification	System
CEF Event ID (Hexadecimal)	0x40000005
CEF Event ID (Decimal)	1073741829
Arg1	suser
Arg2	cnt
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Account settings change

Severity	Notice
Event Description	Account settings updated for [Account: {{user_name}}]. Account settings deleted for [Account: {{user_name}}]. Account settings created for [Account: {{user_name}}].
Classification	System
CEF Event ID (Hexadecimal)	0x40000006
CEF Event ID (Decimal)	1073741830
Arg1	reason
Arg2	suser
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Configuration import

Severity	Notice
Event Description	Configuration import by {{username}} via {{method}} {{succeeded /failed}}.
Classification	System
CEF Event ID (Hexadecimal)	0x40000007

CEF Event ID (Decimal)	1073741831
Arg1	suser
Arg2	method
Arg3	outcome
Arg4	-
Arg5	-
Arg6	-

Configuration export

Severity	Notice
Event Description	Configuration export by {{username}} via {{method}} {{succeeded /failed}}.
Classification	System
CEF Event ID (Hexadecimal)	0x40000008
CEF Event ID (Decimal)	1073741832
Arg1	suser
Arg2	method
Arg3	outcome
Arg4	-
Arg5	-
Arg6	-

Password change

Severity	Notice
Event Description	Password changed for [Account: {{user_name}}].
Classification	System
CEF Event ID (Hexadecimal)	0x40000009
CEF Event ID (Decimal)	1073741833
Arg1	suser
Arg2	-

Arg3	-
Arg4	-
Arg5	-
Arg6	-

Power Off->On

Severity	Notice
Event Description	Power {{index}} turned on.
Classification	System
CEF Event ID (Hexadecimal)	0x4000000a
CEF Event ID (Decimal)	1073741834
Arg1	index
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Power On->Off

Severity	Notice
Event Description	Power {{index}} turned off.
Classification	System
CEF Event ID (Hexadecimal)	0x4000000b
CEF Event ID (Decimal)	1073741835
Arg1	index
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

ABC-02 insertion/removal

Severity	Notice
Event Description	ABC-02 was {{inserted/removed}}.
Classification	System
CEF Event ID (Hexadecimal)	0x40000013
CEF Event ID (Decimal)	1073741843
Arg1	reason
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Firmware upgrade success

Severity	Notice
Event Description	Firmware successfully upgraded by {{username}}.
Classification	System
CEF Event ID (Hexadecimal)	0x4000001d
CEF Event ID (Decimal)	1073741853
Arg1	suser
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Firmware upgrade failure

Severity	Warning
Event Description	Firmware upgrade failed by {{username}}.

Classification	System
CEF Event ID (Hexadecimal)	0x4000001e
CEF Event ID (Decimal)	1073741854
Arg1	suser
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Account log out

Severity	Notice
Event Description	[Account: {{user_name}}] logged out.
Classification	System
CEF Event ID (Hexadecimal)	0x4000001f
CEF Event ID (Decimal)	1073741855
Arg1	suser
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Account removal

Severity	Notice
Event Description	[Account: {{user_name}}] removed by admin.
Classification	System
CEF Event ID (Hexadecimal)	0x40000020
CEF Event ID (Decimal)	1073741856
Arg1	suser

Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Self-healing system reboot (main function)

Severity	Info
Event Description	The system performed a self-healing reboot to resolve abnormal main function behavior.
Classification	System
CEF Event ID (Hexadecimal)	0x40000025
CEF Event ID (Decimal)	1073741861
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Self-healing system reboot (framework)

Severity	Info
Event Description	The system performed a self-healing reboot to resolve abnormal framework behavior.
Classification	System
CEF Event ID (Hexadecimal)	0x40000026
CEF Event ID (Decimal)	1073741862
Arg1	-
Arg2	-
Arg3	-

Arg4	-
Arg5	-
Arg6	-

Port

Port link up

Severity	Notice
Event Description	Port {{index}}/{{number}} status changed to link up.
Classification	Port
CEF Event ID (Hexadecimal)	0x40000100
CEF Event ID (Decimal)	1073742080
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Port link down

Severity	Notice
Event Description	Port {{index}}/{{number}} status changed to link down.
Classification	Port
CEF Event ID (Hexadecimal)	0x40000101
CEF Event ID (Decimal)	1073742081
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-

Arg5	-
Arg6	-

PD power on

Severity	Notice
Event Description	Port {{number}} PD power on.
Classification	Port
CEF Event ID (Hexadecimal)	0x40000103
CEF Event ID (Decimal)	1073742083
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

PD power off

Severity	Notice
Event Description	Port {{number}} PD power off.
Classification	Port
CEF Event ID (Hexadecimal)	0x40000104
CEF Event ID (Decimal)	1073742084
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	--

Low input voltage

Severity	Warning
Event Description	The input voltage of the power supply dropped below 46 VDC. Adjust the voltage to between 46 and 57 VDC to meet PoE voltage requirements.
Classification	Port
CEF Event ID (Hexadecimal)	0x40000105
CEF Event ID (Decimal)	1073742085
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

PD overcurrent

Severity	Error
Event Description	The current of port {{number}} exceeded the safety limit. Check the device status.
Classification	Port
CEF Event ID (Hexadecimal)	0x40000106
CEF Event ID (Decimal)	1073742086
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

PD no response

Severity	Error
Event Description	Port {{number}} device is not responding to the PD failure check. Please check the device status.
Classification	Port
CEF Event ID (Hexadecimal)	0x40000107
CEF Event ID (Decimal)	1073742087
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Power budget overrun

Severity	Warning
Event Description	The consumed power {{power_value}} of all the PDs exceeded the maximum input power {{input_power_value}}.
Classification	Port
CEF Event ID (Hexadecimal)	0x40000108
CEF Event ID (Decimal)	1073742088
Arg1	value
Arg2	threshold
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Power detection failure

Severity	Warning

Event Description	Port {{number}} device is {{Not present/Legacy PD/802.3 af/802.3 at/Non-PD or PD short circuit/Unknown/Not applicable/802.3 bt SS/802.3 bt DS}}. {{No action required./Please enable PoE power output./Please disable PoE power output./Please select PoE output mode to Auto./Please select PoE output mode to High power./Please select PoE output mode to Force./Please enable legacy PD detection./Please raise external power supply voltage greater than 44 VDC./Please raise external power supply voltage greater than 46 VDC.}}.
Classification	Port
CEF Event ID (Hexadecimal)	0x40000109
CEF Event ID (Decimal)	1073742089
Arg1	sportIndex
Arg2	reason
Arg3	msg
Arg4	-
Arg5	-
Arg6	-

Port link up (port channel)

Severity	Notice
Event Description	Port channel {{Channel id}} changed to link up.
Classification	Port
CEF Event ID (Hexadecimal)	0x4000010a
CEF Event ID (Decimal)	1073742090
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Port link down (port channel)

Severity	Notice

Event Description	Port channel {{Channel id}} changed to link down.
Classification	Port
CEF Event ID (Hexadecimal)	0x4000010b
CEF Event ID (Decimal)	1073742091
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Non-PD or PD short circuit

Severity	Warning
Event Description	The device connected to Port {{number}} detected as a non-PD or the PD short circuited. Check device status.
Classification	Port
CEF Event ID (Hexadecimal)	0x4000010e
CEF Event ID (Decimal)	1073742094
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

L2

Port shutdown (Rate Limit)

Severity	Warning

Event Description	Port {{index}}/{{number}} shut down due to traffic overload.
Classification	L2
CEF Event ID (Hexadecimal)	0x40000200
CEF Event ID (Decimal)	1073742336
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Port recovery (Rate Limit)

Severity	Warning
Event Description	Port {{index}}/{{number}} recovered by Rate Limit.
Classification	L2
CEF Event ID (Hexadecimal)	0x40000201
CEF Event ID (Decimal)	1073742337
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

IP Configuration

DHCP Bootfile Failed

Severity	Notice

Event Description	The TFTP server name is not a valid IPv4 address or domain name. The bootfile name is invalid. The TFTP request has timed out.
Classification	IP Configuration
CEF Event ID (Hexadecimal)	0x40000300
CEF Event ID (Decimal)	1073742592
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Redundancy

Topology change (MRP)

Severity	Warning
Event Description	Topology change detected, MRP {{strMRMState}}.
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x40000400
CEF Event ID (Decimal)	1073742848
Arg1	reason
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Redundant port health check failure

Severity	Error
Event Description	Redundant port {{index}}/{{number}} health check failed.
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x40000402
CEF Event ID (Decimal)	1073742850
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Topology change (MSTP)

Severity	Warning
Event Description	Topology (MST{{Index}}) changed by MSTP.
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x40000404
CEF Event ID (Decimal)	1073742852
Arg1	index
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

MSTP root change

Severity	Warning
Event Description	MSTP (MST{{Index}}) new root was elected in topology.

Classification	Redundancy
CEF Event ID (Hexadecimal)	0x40000405
CEF Event ID (Decimal)	1073742853
Arg1	index
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

MSTP new port role

Severity	Warning
Event Description	MSTP (MST{{Index}}) port {{number}} role changed from {{role}} to {{role}}.
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x40000406
CEF Event ID (Decimal)	1073742854
Arg1	index
Arg2	sportIndex
Arg3	srole
Arg4	drole
Arg5	-
Arg6	-

Topology change (RSTP)

Severity	Warning
Event Description	Topology changed by RSTP.
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x40000407
CEF Event ID (Decimal)	1073742855

Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

RSTP invalid BPDU

Severity	Warning
Event Description	RSTP Port-Channel {{channel id}} received an invalid BPDU (type:{{type}}, value:{{value}}). RSTP port {{index}}/{{number}} received an invalid BPDU (type:{{type}}, value:{{value}}).
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x40000408
CEF Event ID (Decimal)	1073742856
Arg1	sportType
Arg2	sportIndex
Arg3	moduleType
Arg4	value
Arg5	-
Arg6	-

RSTP migration

Severity	Warning
Event Description	Port-Channel {{channel id}} changed to {{rstp/stp}}. Port {{index}}/{{number}} changed to {{rstp/stp}}.
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x40000409
CEF Event ID (Decimal)	1073742857
Arg1	sportType

Arg2	sportIndex
Arg3	sourceServiceName
Arg4	-
Arg5	-
Arg6	-

RSTP root change

Severity	Warning
Event Description	New RSTP root was elected in the topology.
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x4000040a
CEF Event ID (Decimal)	1073742858
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

RSTP new port role

Severity	Warning
Event Description	RSTP Port-Channel {{channel id}} role changed from {{role}} to {{role}}. RSTP port {{index}}/{{number}} role changed from {{role}} to {{role}}.
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x4000040b
CEF Event ID (Decimal)	1073742859
Arg1	sportType
Arg2	sportIndex
Arg3	srole

Arg4	drole
Arg5	-
Arg6	-

Topology change (Turbo Ring)

Severity	Warning
Event Description	Topology change detected on Ring {{RingIndex}} of Turbo Ring v2.
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x4000040e
CEF Event ID (Decimal)	1073742862
Arg1	index
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Master mismatch

Severity	Warning
Event Description	Ring {{Index}} Master settings mismatch detected.
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x4000040f
CEF Event ID (Decimal)	1073742863
Arg1	index
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Master change

Severity	Warning
Event Description	The Master of Ring {{Index}} changed.
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x40000410
CEF Event ID (Decimal)	1073742864
Arg1	index
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Coupling change

Severity	Warning
Event Description	The Turbo Ring v2 coupling path status changed
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x40000411
CEF Event ID (Decimal)	1073742865
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

MRP multi managers

Severity	Warning
Event Description	MRP multi managers: {{mac addr}}.

Classification	Redundancy
CEF Event ID (Hexadecimal)	0x40000414
CEF Event ID (Decimal)	1073742868
Arg1	smac
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

DRC edge status changed

Severity	Warning
Event Description	The Dynamic Ring Coupling edge status changed.
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x40000419
CEF Event ID (Decimal)	1073742873
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Topology change (MRP Interconnection)

Severity	Warning
Event Description	Topology change detected, MRP interconnection {{strMIMState}}.
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x4000041a
CEF Event ID (Decimal)	1073742874
Arg1	reason

Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

MRP Ring-Open

Severity	Warning
Event Description	MRP MRM port 2 changed from blocking to forwarding due to Ring-Open state.
Classification	Redundancy
CEF Event ID (Hexadecimal)	0x4000041c
CEF Event ID (Decimal)	1073742876
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

Security

SSH key regeneration

Severity	Notice
Event Description	The SSH key was regenerated.
Classification	Security
CEF Event ID (Hexadecimal)	0x40000600
CEF Event ID (Decimal)	1073743360
Arg1	-

Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

SSL certification change

Severity	Notice
Event Description	SSL certificate changed. SSL certificate was regenerated.
Classification	Security
CEF Event ID (Hexadecimal)	0x40000601
CEF Event ID (Decimal)	1073743361
Arg1	reason
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

DHCP client ingress packet drop

Severity	Warning
Event Description	VLAN <vlan-id> dropped DHCP client ingress packets due to a DHCP Snooping rule violation. Total packets discarded: <number>.
Classification	Security
CEF Event ID (Hexadecimal)	0x40000602
CEF Event ID (Decimal)	1073743362
Arg1	vlanId
Arg2	value
Arg3	-

Arg4	-
Arg5	-
Arg6	-

DHCP server packet drop

Severity	Warning
Event Description	VLAN <vlan-id> dropped DHCP server packets due to a DHCP Snooping rule violation. Total packets discarded: <number>.
Classification	Security
CEF Event ID (Hexadecimal)	0x40000603
CEF Event ID (Decimal)	1073743363
Arg1	vlanId
Arg2	value
Arg3	-
Arg4	-
Arg5	-
Arg6	-

DHCPSNP static entry overwrite failure

Severity	Warning
Event Description	Static entry: VLAN: {{Vlan Id}}, MAC: {{mac addr}} already exists.
Classification	Security
CEF Event ID (Hexadecimal)	0x40000604
CEF Event ID (Decimal)	1073743364
Arg1	vlanId
Arg2	smac
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Port shutdown (Network Loop Protection)

Severity	Critical
Event Description	Port {{index}}/{{number}} shut down due to looping.
Classification	Security
CEF Event ID (Hexadecimal)	0x40000605
CEF Event ID (Decimal)	1073743365
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

MACsec MKA expiration

Severity	Warning
Event Description	The secure MKA session on port {{index}}/{{number}} expired.
Classification	Security
CEF Event ID (Hexadecimal)	0x40000606
CEF Event ID (Decimal)	1073743366
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

802.1X Auth Fail

Severity	Warning
Event Description	802.1x authentication failed on port {{index}}/{{number}} with {{buffer}}

Classification	Security
CEF Event ID (Hexadecimal)	0x40000607
CEF Event ID (Decimal)	1073743367
Arg1	sportIndex
Arg2	smac
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Port shutdown (Port Security)

Severity	Warning
Event Description	Port {{index}}/{{number}} shut down due to a Port Security rule violation.
Classification	Security
CEF Event ID (Hexadecimal)	0x40000608
CEF Event ID (Decimal)	1073743368
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Packet dropped by Port Security

Severity	Warning
Event Description	Port {{index}}/{{number}} dropped packets due to violation of Port Security rule.
Classification	Security
CEF Event ID (Hexadecimal)	0x40000609

CEF Event ID (Decimal)	1073743369
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Trust host moved from one port to another port (Port Security)

Severity	Warning
Event Description	A trust host, MAC is {{mac address}} with VLAN {{Vlan Id}}, moved from port {{index}}/{{number}} to port {{index}}/{{number}}.
Classification	Security
CEF Event ID (Hexadecimal)	0x4000060a
CEF Event ID (Decimal)	1073743370
Arg1	smac
Arg2	vlanId
Arg3	sportIndex
Arg4	dportIndex
Arg5	-
Arg6	-

Integrity check failure

Severity	Warning
Event Description	Event log integrity check failed.
Classification	Security
CEF Event ID (Hexadecimal)	0x4000060b
CEF Event ID (Decimal)	1073743371

Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Integrity is missing

Severity	Warning
Event Description	The log integrity information is missing.
Classification	Security
CEF Event ID (Hexadecimal)	0x4000060c
CEF Event ID (Decimal)	1073743372
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

VLAN Assignment check port mode

Severity	Error
Event Description	VLAN Assignment: Port {{index}}/{{number}} is not in Access mode.
Classification	Security
CEF Event ID (Hexadecimal)	0x4000060d
CEF Event ID (Decimal)	1073743373
Arg1	sportIndex
Arg2	-
Arg3	-
Arg4	-

Arg5	-
Arg6	-

VLAN Assignment check vlan

Severity	Info
Event Description	VLAN Assignment: VLAN ID {{Vlan Id}} does not exist.
Classification	Security
CEF Event ID (Hexadecimal)	0x4000060e
CEF Event ID (Decimal)	1073743374
Arg1	vlanId
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Event Logs Cleared

Severity	Notice
Event Description	Event logs have been cleared by {{account}}.
Classification	Security
CEF Event ID (Hexadecimal)	0x4000060f
CEF Event ID (Decimal)	1073743375
Arg1	account
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Configuration integrity check failure

Severity	Warning
Event Description	Configuration integrity check failed.
Classification	Security
CEF Event ID (Hexadecimal)	0x40000610
CEF Event ID (Decimal)	#NUM!
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Diagnostics

Event log export

Severity	Notice
Event Description	Event Log export {{successful /failed}} by {{username}} via {{method}}.
Classification	Diagnostics
CEF Event ID (Hexadecimal)	0x40000700
CEF Event ID (Decimal)	1073743616
Arg1	outcome
Arg2	suser
Arg3	method
Arg4	-
Arg5	-
Arg6	-

Resource log export

Severity	Notice
Event Description	Resource Log export {{successful /failed}} by {{username}} via {{method}}.
Classification	Diagnostics
CEF Event ID (Hexadecimal)	0x40000701
CEF Event ID (Decimal)	1073743617
Arg1	outcome
Arg2	suser
Arg3	method
Arg4	-
Arg5	-
Arg6	-

Log capacity threshold warning

Severity	Warning
Event Description	Event log entry threshold {{logEntryNum}} reached.
Classification	Diagnostics
CEF Event ID (Hexadecimal)	0x40000702
CEF Event ID (Decimal)	1073743618
Arg1	threshold
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

LLDP table change

Severity	Info

Event Description	LLDP remote table changed LLDP remote table changed.
Classification	Diagnostics
CEF Event ID (Hexadecimal)	0x40000703
CEF Event ID (Decimal)	1073743619
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Module initialization failure

Severity	Error
Event Description	Failed to initialize module {{index}}.
Classification	Diagnostics
CEF Event ID (Hexadecimal)	0x40000704
CEF Event ID (Decimal)	1073743620
Arg1	index
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

RMON raising alarm

Severity	Warning
Event Description	{{user defined}}.
Classification	Diagnostics
CEF Event ID (Hexadecimal)	0x40000705

CEF Event ID (Decimal)	1073743621
Arg1	msg
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

RMON falling alarm

Severity	Warning
Event Description	{{user defined}}.
Classification	Diagnostics
CEF Event ID (Hexadecimal)	0x40000706
CEF Event ID (Decimal)	1073743622
Arg1	msg
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Relay cut-off

Severity	Notice
Event Description	{{relay_name}} relay alarm was cut off.
Classification	Diagnostics
CEF Event ID (Hexadecimal)	0x4000070a
CEF Event ID (Decimal)	1073743626
Arg1	moduleType
Arg2	-
Arg3	-

Arg4	-
Arg5	-
Arg6	-

Moxa tech support login

Severity	Notice
Event Description	Moxa technical support logged in to the device for troubleshooting.
Classification	Diagnostics
CEF Event ID (Hexadecimal)	0x4000070d
CEF Event ID (Decimal)	1073743629
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Moxa tech support logout

Severity	Notice
Event Description	Moxa technical support logged out of the device.
Classification	Diagnostics
CEF Event ID (Hexadecimal)	0x4000070e
CEF Event ID (Decimal)	1073743630
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Moxa tech support function activation

Severity	Notice
Event Description	The Moxa technical support function activated.
Classification	Diagnostics
CEF Event ID (Hexadecimal)	0x4000070f
CEF Event ID (Decimal)	1073743631
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Moxa tech support function deactivation

Severity	Notice
Event Description	The Moxa technical support function deactivated.
Classification	Diagnostics
CEF Event ID (Hexadecimal)	0x40000710
CEF Event ID (Decimal)	1073743632
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Provisioning

Auto Config Notice

Severity	Notice
Event Description	Auto Configuration process started. Received IP address. Downloaded the configuration. Propagating information to the DHCP Server. Auto Configuration is disabled. Auto Configuration will be triggered after the reboot.
Classification	Provisioning
CEF Event ID (Hexadecimal)	0x40000900
CEF Event ID (Decimal)	1073744128
Arg1	-
Arg2	-
Arg3	-
Arg4	-
Arg5	-
Arg6	-

Auto Config Warning

Severity	Warning
Event Description	Insufficient information to propagate. Auto Configuration timed out. Failed to download the configuration. Failed to import the configuration.
Classification	Provisioning
CEF Event ID (Hexadecimal)	0x40000901
CEF Event ID (Decimal)	1073744129
Arg1	-
Arg2	-

Arg3	-
Arg4	-
Arg5	-
Arg6	-

Severity Level List

This is a list of severity levels and descriptions, which are based on CVSS vulnerability classifications.

Syslog Severity	CEF Severity	Severity Name	Description
0	10	Emergency	System is unusable
1	8	Alert	Action must be taken immediately
2	7	Critical	Critical conditions
3	6	Error	Error conditions
4	5	Warning	Warning conditions
5	4	Notice	Normal but significant condition
6	1	Infomational	Informational messages
7	0	Debug	Debug-level messages

SNMP MIB Files

This appendix contains the SNMP MIB file for the managed switch.

You can download the MIB file via the product site. Please note the MIB file varies by model.

Structure of the Moxa MIB group package

Moxa support standard MIB and properties MIB. Below are all of folder and related MIB files. Please note that the applicable MIB files may vary across different models.

<Package File Lists>

EX. MOXA_MIB_XXX-XXXX_v1.0_YYYY_MMDD_HHMM.zip //XXX-XXXX means model name

```
├──   Private    // MOXA properties MIB
│       │
│       ├── General    // General group
│       │   ├── mx1588.mib
│       │   ├── mxDeviceIo.mib
│       │   ├── mxDhcpRelay.mib
│       │   ├── mxDhcpSvr.mib
│       │   ├── mxEip.mib
│       │   ├── mxEmailC.mib
│       │   ├── mxEventLog.mib
│       │   ├── mxGene.mib
│       │   ├── mxGeneral.mib
│       │   ├── mxIec6185093Profile.mib
│       │   ├── mxIeeeC37238Profile.mib
│       │   ├── mxLocator.mib
│       │   ├── mxManagementIp.mib
│       │   ├── mxMms.mib
│       │   ├── mxModbusTcp.mib
│       │   ├── mxPoee.mib
│       │   ├── mxPorte.mib
│       │   ├── mxProfinet.mib
```

```
|       |   ├── mxPtp.mib
|       |   ├── mxRelayC.mib
|       |   ├── mxSnmp.mib
|       |   ├── mxSwe.mib
|       |   ├── mxSysLoginPolicySvr.mib
|       |   ├── mxSyslogSvr.mib
|       |   ├── mxSysPasswordPolicySvr.mib
|       |   ├── mxSystemInfo.mib
|       |   ├── mxSysTrustAccessSvr.mib
|       |   ├── mxSysUtilSvr.mib
|       |   ├── mxTimeSetting.mib
|       |   ├── mxTimeZone.mib
|       |   ├── mxTrackinge.mib
|       |   ├── mxTrapC.mib
|       |   └── mxUiServiceMgmt.mib
|       ├── PoE     // PoE group
|       |   ├── mxPoe.mib
|       |   └── mxPoeBt.mib
|       ├── Product_Information        // Product group
|       |   ├── mxGeneralInfo.mib
|       |   └── mxProductInfo.mib
|       ├── Switching    // Switching group
|       |   ├── mxDai.mib
|       |   ├── mxDhcpSnp.mib
|       |   ├── mxDot1x.mib
|       |   ├── mxDualHoming.mib
|       |   ├── mxFiberCheck.mib
|       |   ├── mxIgmpSnp.mib
|       |   ├── mxIpsg.mib
|       |   ├── mxLa.mib
|       |   ├── mxLhc.mib
|       |   ├── mxLldp.mib
|       |   ├── mxLp.mib
|       |   ├── mxMab.mib
|       |   ├── mxMacsec.mib
|       |   ├── mxPort.mib
```

```
│       │   ├── mxPortMirror.mib
│       │   ├── mxPsms.mib
│       │   ├── mxPssp.mib
│       │   ├── mxQos.mib
│       │   ├── mxRadius.mib
│       │   ├── mxRlps.mib
│       │   ├── mxRmon.mib
│       │   ├── mxRstp.mib
│       │   ├── mxStcl.mib
│       │   ├── mxSwitching.mib
│       │   ├── mxTc.mib
│       │   ├── mxTcst.mib
│       │   ├── mxTrv2.mib
│       │   └── mxVlan.mib
│       ├── Routing    // Routing group
│           ├── mxArp.mib
│           ├── mxIpIf.mib
│           ├── mxMulticastRouting.mib
│           ├── mxOspf.mib
│           ├── mxPimSm.mib
│           ├── mxRte.mib
│           ├── mxStaticRoute.mib
│           ├── mxUnicastRoutingTable.mib
│           └── mxVrrp.mib
│
├── Standard     // Standard MIB
│   ├── BRIDGE-MIB.mib
│   ├── EtherLike-MIB.mib
│   ├── IANA-ADDRESS-FAMILY-NUMBERS.mib
│   ├── IANAifType-MIB.mib
│   ├── IEC-62439-2.mib
│   ├── IEEE8021-PAE-MIB.mib
│   ├── IEEE8021-SPANNING-TREE-MIB.mib
│   ├── IEEE8021-TC-MIB.mib
│   ├── IEEE8023-LAG-MIB.mib
│   ├── IEEE8023-MSTP-MIB.mib
```

```
│   ├── IF-MIB.mib
│   ├── INET-ADDRESS-MIB.mib
│   ├── LLDP-EXT-DOT1-MIB.mib
│   ├── LLDP-EXT-DOT3-MIB.mib
│   ├── LLDP-EXT-ODVA-MIB.mib
│   ├── LLDP-MIB.mib
│   ├── P-BRIDGE-MIB.mib
│   ├── Q-BRIDGE-MIB.mib
│   ├── RFC1213-MIB.mib
│   ├── RFC1271-MIB.mib
│   ├── RMON2-MIB.mib
│   ├── RMON-MIB.mib
│   ├── SNMP-FRAMEWORK-MIB.mib
│   ├── SNMPv2-CONF.mib
│   ├── SNMPv2-MIB.mib
│   ├── SNMPv2-SMI.mib
│   ├── SNMPv2-TC.mib
│   ├── OSPF-MIB.mib
│   ├── PTPBASE-MIB.mib
│   └── TOKEN-RING-RMON-MIB.mib
│   └── IEEE8021-AS-MIB.mib
│   └── IEEE8021-BRIDGE-MIB.mib
│   └── IEEE8021-Q-BRIDGE-MIB.mib
│   └── IEEE8021-ST-MIB.mib
├── README.txt      // this file
```

Standard MIB Installation Order

If your tool need to import MIB one-by-one, please refer to the Standard MIBs Installation 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.IEEE8023-LAG-MIB.mib
9.IF-MIB.mib
10.EtherLike-MIB.mib
11.IEEE8021-PAE-MIB.mib
12.BRIDGE-MIB.mib
13.P-BRIDGE-MIB.mib
14.RFC1271-MIB.mib
15.RMON-MIB.mib
16.TOKEN-RING-RMON-MIB.mib
17.RMON2-MIB.mib
18.Q-BRIDGE-MIB.mib
19.INET-ADDRESS-MIB.mib
20.IEEE8021-TC-MIB.mib
21.IEEE8021-SPANNING-TREE-MIB.mib
22.IEEE8021-MSTP-MIB.mib
23.IANA-ADDRESS-FAMILY-NUMBERS-MIB.mib
24.LLDP-MIB.mib
25.LLDP-EXT-DOT1-MIB.mib
26.LLDP-EXT-DOT3-MIB.mib
27.LLDP-EXT-ODVA-MIB.mib
28.OSPF-MIB.mib
29.PTPBASE-MIB.mib
30.IEEE8021-AS-MIB.mib
31.IEEE8021-BRIDGE-MIB.mib
32.IEEE8021-ST-MIB.mib
33.IEEE8021-Q-BRIDGE-MIB.mib

MIB Tree

iso(1)
|-std(0)-iso8802(8802)-ieee802dot1(1)-ieee802dot1mibs(1)
| |-ieee8021paeMIB(1) : IEEE8021-PAE-MIB.mib
| |-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
   |      |      |-ospf(14)                   : OSPF-MIB.mib
   |      |      |-rmon(16)                   : RMON-MIB.mib
   |      |      |-dot1dBridge(17)            : BRIDGE-MIB.mib, P-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,
mxDhcpRelay.mib, mxDhcpSvr.mib, mxEmailC.mib,
   |      |      |                            : mxEventLog.mib, mxGene.mib,
mxLocator.mib, mxManagementIp.mib, mxPoee.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, mxRte.mib, mxMms.mib,
   |      |      |                            : mxPtp.mib, mx1588.mib,
mxIec6185093Profile.mib, mxIeeeC37238Profile.mib mxModbusTcp.mib,
   |      |      |                            : mxEip.mib, mxProfinet.mib, mxTrackinge.mib
   |      |      |-switching(603)             : mxSwitching.mib
   |      |      |      |- portInterfacce     : mxPort.mib, mxLa.mib
   |      |      |      |- basicLayer2        : mxLhc.mib, mxQos, mxVlan.mib
   |      |      |      |- layer2Redundancy   : mxRstp.mib, mxTrv2.mib,
mxTurboChain.mib, mxDualHoming.mib
   |      |      |      |- layer2Security     : mxStcl.mib, mxRlps.mib, mxPssp.mib,
```

mxPsms.mib, mxDot1x.mib, mxRadius.mib, mxLp.mib, mxDhcpSnp.mib, mxIpsg.mib, mxMab.mib, mxDai.mib, mxMacsec.mib

| | | |- layer2Diagnosic : mxLldp.mib, mxTcst.mib, mxPortMirror.mib, mxRmon.mib, mxFiberCheck.mib, mxTracking.mib

| | | |- layer3Diagnosic

| | | |- layer2Multicast : mxIgmpSnp.mib

| | | |- layer3Multicast

| | |-routing(605)

| | | |- l3Genral : mxIpIf.mib, mxArp.mib

| | | |- unicastRouting : mxUnicastRoutingTable.mib, mxStaticRoute.mib, mxOspf.mib

| | | |- multicastRouting : mxMulticastRouting.mib, mxPimSm.mib

| | | |- l3Redundant : mxVrrp.mib

| | |-poe(608) : mxPoe.mib

| |-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

User Role Privileges

This page shows the privilege levels granted to the different authority levels: Admin, Supervisor, and User on Moxa's Managed Ethernet Series switches. Refer to System > Account Management > User Accounts for more information on user accounts.

Privileges are indicated as follows:

- **R/W**: Read and write access granted for the relevant settings.
- **R**: Read-only access granted for the relevant settings.
- **-**: No access granted for the relevant settings.

> **Note**
> Available settings and options will vary depending on the product model.

Options Menu

Settings	Admin	Supervisor	User
Locator	R/W	R/W	R/W
Reboot	R/W	R/W	-
Reset to Default Settings	R/W	-	-
Save Custom Default	R/W	-	-
Auto-save to startup	R/W	R/W	-
Advanced mode	R/W	R/W	R/W
Log Out	R/W	R/W	R/W

System

Settings	Admin	Supervisor	User
Device Summary	R	R	R
System Management			
Information Settings	R/W	R/W	R
Firmware Upgrade	R/W	-	-
Config Backup and Restore	R/W	-	-
Account Management			
User Accounts	R/W	-	-
Online Accounts	R/W	-	-
Password Policy	R/W	-	-
Management Interface			
User Interface	R/W	R	R
Hardware Interfaces	R/W	R/W	R
SNMP	R/W	-	-
RMON1 (Only in CLI)	R/W	R/W	R
Time			
System Time	R/W	R/W	R
NTP Server	R/W	R/W	-

Provisioning

Settings	Admin	Supervisor	User
Auto Configuration	R/W	R/W	R

Port

Settings	Admin	Supervisor	User
Port Interface			
Port Settings	R/W	R/W	R
Linkup Delay	R/W	R/W	R
Link Aggregation	R/W	R/W	R
PoE	R/W	R/W	R

Layer 2 Switching

Settings	Admin	Supervisor	User
VLAN	R/W	R/W	R
GARP	R/W	R/W	R
MAC			
Static Unicast	R/W	R/W	R
MAC Address Table	R/W	R/W	R
QoS			
Classification	R/W	R/W	R
Ingress Rate Limit	R/W	R/W	R

Settings	Admin	Supervisor	User
Scheduler	R/W	R/W	R
Egress Shaper	R/W	R/W	R
Multicast			
IGMP Snooping	R/W	R/W	R
GMRP	R/W	R/W	R
Static Multicast	R/W	R/W	R

IP Configuration

Settings	Admin	Supervisor	User
IP Configuration	R/W	R/W	R

Redundancy

Settings	Admin	Supervisor	User
Layer 2 Redundancy			
Spanning Tree	R/W	R/W	R
Turbo Ring v2	R/W	R/W	R
MRP	R/W	R/W	R

Network Service

Settings	Admin	Supervisor	User
DHCP Server	R/W	R/W	R

Settings	Admin	Supervisor	User
DHCP Relay Agent	R/W	R/W	R
DNS Server	R/W	R/W	R
mDNS Responder	R/W	R/W	R

Security

Settings	Admin	Supervisor	User
Device Security			
Login Policy	R/W	R	R
Trusted Access	R/W	R	R
SSH & SSL	R/W	R/W	-
Network Security			
IEEE 802.1X	R/W	R/W	R
MAC Authentication Bypass	R/W	R/W	R
MACsec	R/W	R/W	R
Port Security	R/W	R/W	R
Traffic Storm Control	R/W	R/W	R
Access Control List	R/W	R/W	R
Network Loop Protection	R/W	R/W	R
Binding Database	R/W	R/W	R
DHCP Snooping	R/W	R/W	R
IP Source Guard	R/W	R/W	R

Settings	Admin	Supervisor	User
Dynamic ARP Inspection	R/W	R/W	R
Authentication			
Login Authentication	R/W	-	-
RADIUS	R/W	-	-
TACACS+	R/W	-	-

Diagnostics

Settings	Admin	Supervisor	User
System Status			
Resource Utilization	R	R	R
Network Status			
Network Statistics	R	R	R
LLDP	R/W	R/W	R
ARP Table	R	R	R
Tools			
Port Mirroring	R/W	R/W	R
Ping	R/W	R/W	R/W
Event Logs and Notifications			
Event Logs	R/W	R/W	R
Event Notifications	R/W	R/W	R
Syslog	R/W	R/W	-
SNMP Trap/Inform	R/W	-	-

Settings	Admin	Supervisor	User
Email Settings	R/W	R	R

Moxa Inc.

www.moxa.com/products