www.moxa.com/products

MX-ROS V3 User Manual

Version 1.0

August 2023

Table of Contents

Chapter 1

Overview

Overview

Introduction

Welcome to the Moxa RouterOS (MX-ROS) 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 MX-ROS device. The goal is to simplify your experience and make the setup process easier.

Supported Series and Firmware Versions

This manual has been updated for the following products and firmware versions.

Moxa Router Series	Firmware Version
TN-4900 Series	v3.0
EDR-G9010 Series	v3.0

The information in this document is applicable to other products and firmwares that use MX-ROS V3, but the appearance and availability of features and settings may vary.

MX-ROS support will expand to other products in the future; please check the Moxa website for the latest information.

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.

Other Features: This section helps you understand features for your device that may not have a related user interface.

Security: This section gives you an overview of industrial network security and the related product features and best practices needed to help you better secure your application.

Appendix: This section provides additional reference information for your device.

Who This Document Is For

We want you to get the most out of your Moxa device, so we designed this document with these audiences in mind:

OT engineers learning how to configure OT network devices: For frontline personnel operating in OT environments, keeping your MX-ROS configuration up-to-date is crucial. We created the **Security** section to help you better understand how you can use this device effectively for your application.

Experienced OT network engineers integrating Moxa devices into OT network infrastructure: For those who already have a solid understanding of networking concepts, the **UI Reference** section is designed to give you a quick reference for all the device settings, options, default settings, and limitations. You may also find the **Security** section useful for learning how to get more out of your Moxa device and to optimize your application.

Document Conventions

This document uses the following formatting conventions:

Convention/Format	Description
Bold	Used for UI elements you see on-screen, including page name, tab name, field labels, dropdown options, menu path, etc.
Italics	Used to highlight important information in a paragraph or a table, such as indicating that a UI setting is only shown under certain conditions.
Code/commands/CLI	Used for code snippets, blocks, commands, and CLI output.

Chapter 2

Quick Start

Quick Start

This section provides you with information on how to connect to your device to access its configuration interface.

Using a Web Browser to Configure the Industrial Secure Router

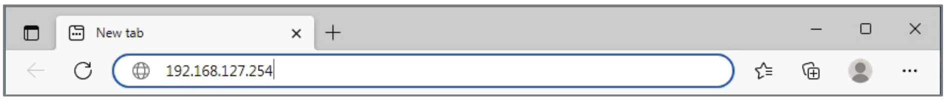
The device's web browser interface provides a convenient way to modify the router’s configuration and access the built-in monitoring and network administration functions.

To use the device’s management and monitoring functions from a PC host connected to the same LAN as the device, you must make sure that the PC host and the device are connected to the same logical subnet.

Before accessing the device’s web browser, first connect one of the device's Ethernet LAN ports to your Ethernet LAN, or directly to an Ethernet port on your PC. You can use either a straight-through or cross-over Ethernet cable.

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

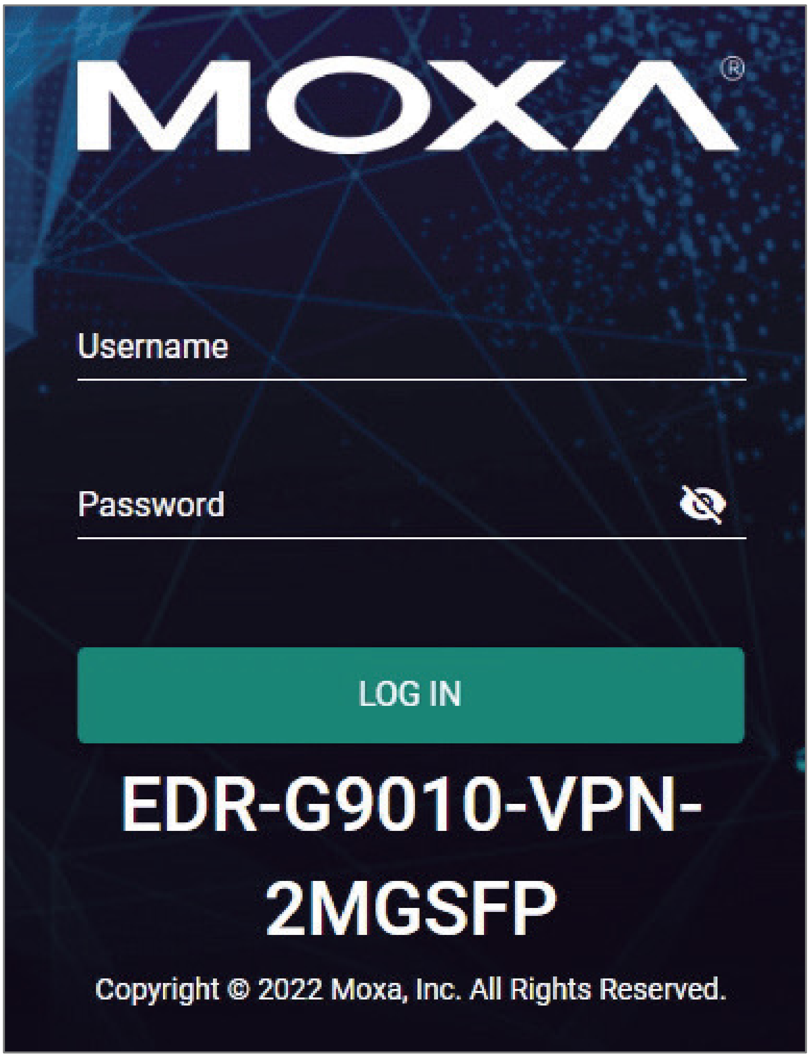
1. Open a web browser and type the device’s LAN IP address (**192.168.127.254** by default) into the address bar and press Enter.



2. 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

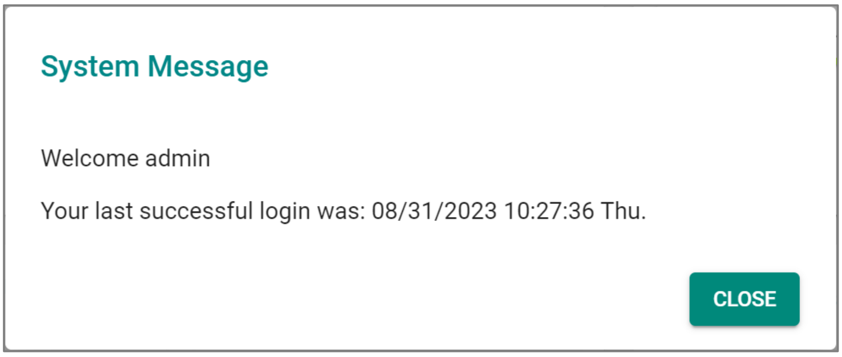
The default username is **admin** and the default password is **moxa**. We strongly recommend changing the password as soon as possible to ensure the security of your device.



EDR-G9010-VPN-2MGSFP

Copyright © 2022 Moxa, Inc. All Rights Reserved.

You may need to wait a few moments for the web interface to appear. If you have logged in before, a system message will appear showing the details of the last successful login. Click **CLOSE** to close this message.

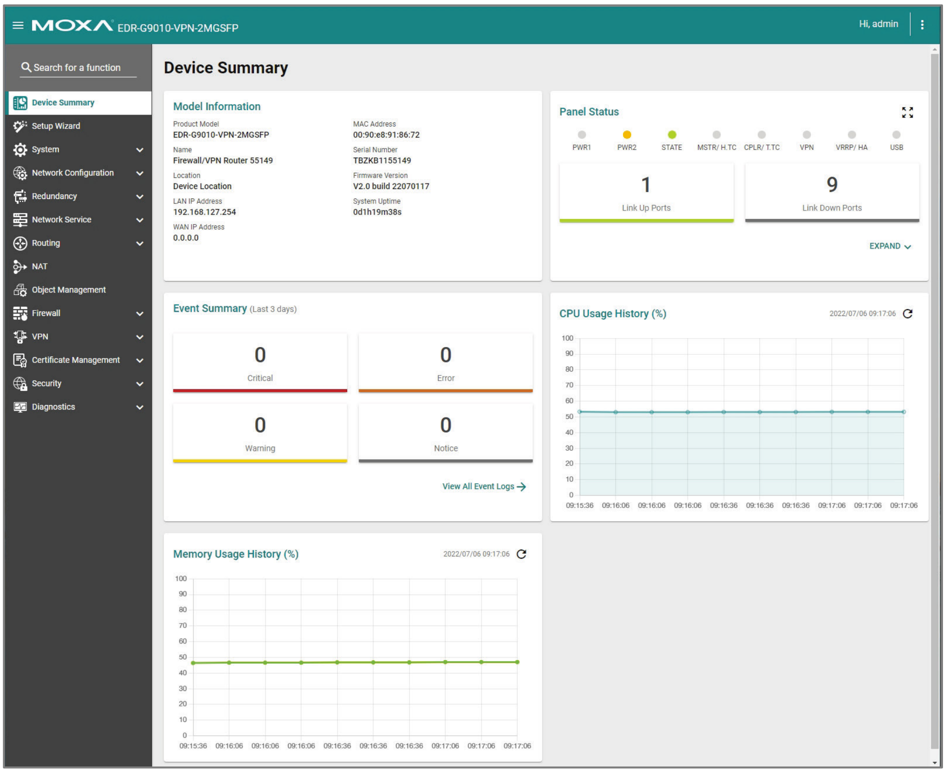


System Message

Welcome admin

Your last successful login was: 08/31/2023 10:27:36 Thu.

After successfully connecting to the router, 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 router’s functions.



Device Summary

Model Information

Product Model: EDR-G9010-VPN-2MGSFP
MAC Address: 00:90:e8:91:86:72
Name: Firewall/VPN Router 55149
Serial Number: TBZKB1155149
Location: Device Location
Firmware Version: V2.0 build 22070117
LAN IP Address: 192.168.127.254
System Uptime: 0d1h19m38s
WAN IP Address: 0.0.0.0

Panel Status

1 Link Up Ports
9 Link Down Ports

Event Summary (Last 3 days)

0 Critical
0 Error
0 Warning
0 Notice

CPU Usage History (%) 2022/07/06 09:17:06

Memory Usage History (%) 2022/07/06 09:17:06

Chapter 3

UI Reference

UI Reference

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:

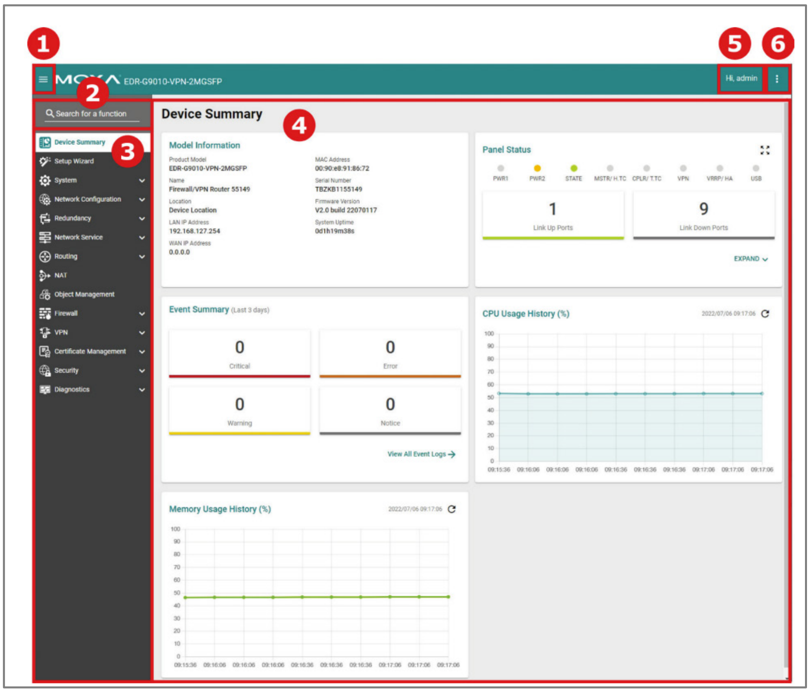
- The MX-ROS User Interface

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

- Device Summary
- Setup Wizard
- System
- Network Configuration
- Redundancy
- Network Service
- Routing
- NAT
- Object Management
- Firewall
- VPN
- Certificate Management
- Security
- Diagnostics

The MX-ROS User Interface

Here is an overview of the MX-ROS user interface.



Device Summary

Model Information

Product Model
EDR-G9010-VPN-2MGSFP

MAC Address
00:90:e8:91:86:72

Name
Firewall/VPN Router 55149

Serial Number
TBZKB1155149

Location
Device Location

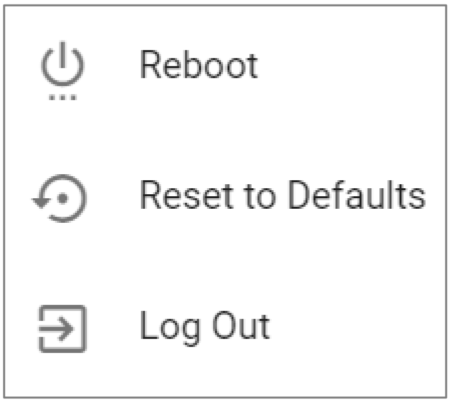
Firmware Version
V2.0 build 22070117

LAN IP Address
192.168.127.254

System Uptime
0d1h19m38s

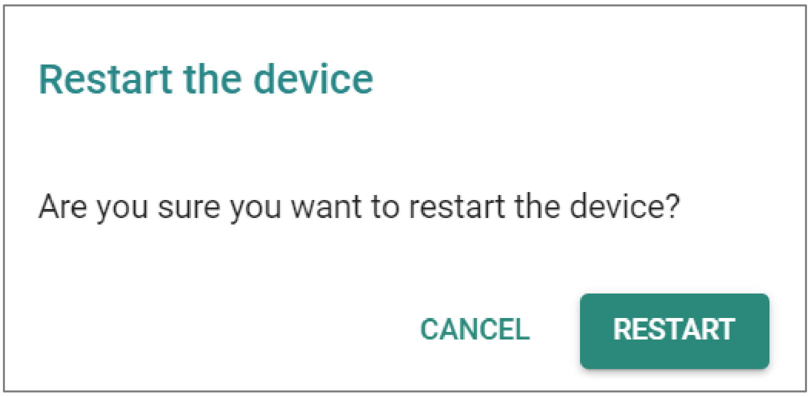
WAN IP Address
0.0.0.0

1. Clicking ☰ in the top-left will toggle display of the function menu.
2. Enter the name of a function in the **Search Bar** to quickly find a specific function page.
3. Click on a page name in the **Function Menu** on the left-hand side to go to its function page.
4. All the configuration options and information of the selected function page will be shown here.
5. The name of the currently logged-in user is shown here.
6. Clicking ⋮ in the top-right will expand the drop-down menu shown below.



Reboot

Click **RESTART** to reboot your Moxa device.


Restart the device

Are you sure you want to restart the device?

Reset to Defaults

The Reset to Defaults option gives users a quick way to restore their device's settings back to their factory default values. This function is available in both the console utility (serial or Telnet) and the web browser interface. Click **RESET** to reset your device to the factory default settings.

Warning

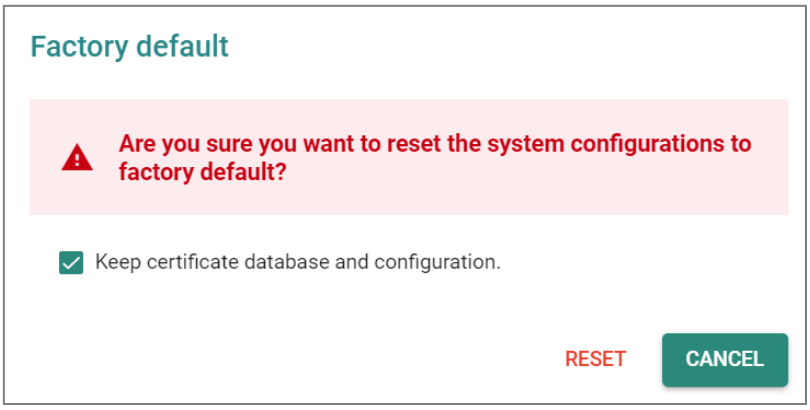
When resetting your device to the factory default settings, all your current configuration settings will be permanently deleted.

Check the **Keep certificate database and configuration** option to keep the certificate database and configuration information. Leaving this option unchecked will **delete all information** on the device and reset everything to its factory default value.

After resetting to default, the Network Security Package will be reset to the built-in version. If you have installed a newer version of the package, remember to reinstall your desired version of the Network Security Package if needed.

After resetting the device, you will need to use the default network settings to re-establish a web-browser or Telnet connection to your Moxa device.

For security reasons, before decommisioning the device, the device should be reset to factory default settings and all stored data should be erased.



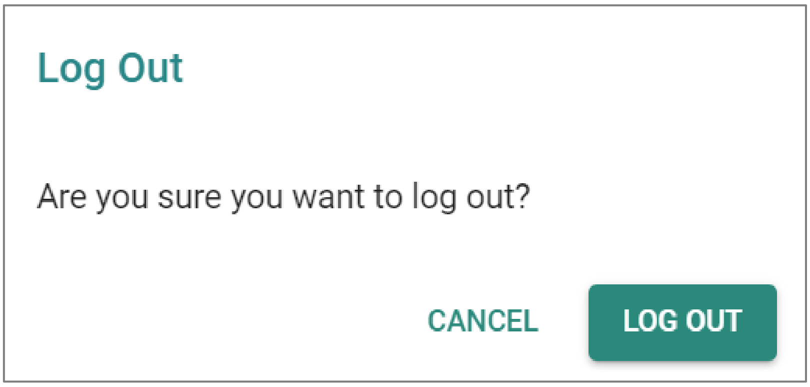
Factory default

Are you sure you want to reset the system configurations to factory default?

☑ Keep certificate database and configuration.

Log Out

Click **LOG OUT** to log out of your device.



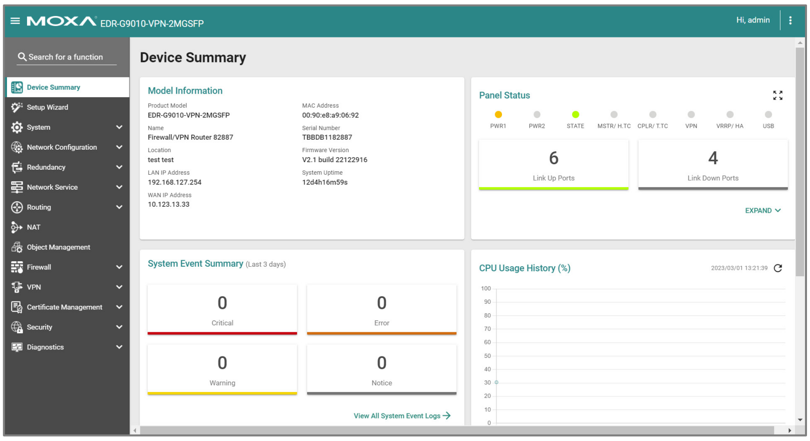
Log Out

Are you sure you want to log out?

Device Summary

Menu Path: Device Summary

This page lets you see displays with information about your device and current status.



Device Summary

Model Information

Product Model: EDR-G9010-VPN-2MGSFP
Name: Firewall/VPN Router 82887
Location: test test
LAN IP Address: 192.168.127.254
WAN IP Address: 10.123.13.33
MAC Address: 00:90:e8:a9:06:92
Serial Number: TBBDB1182887
Firmware Version: V2.1 build 22122916
System Uptime: 12d4h16m59s

Panel Status

6 Link Up Ports
4 Link Down Ports

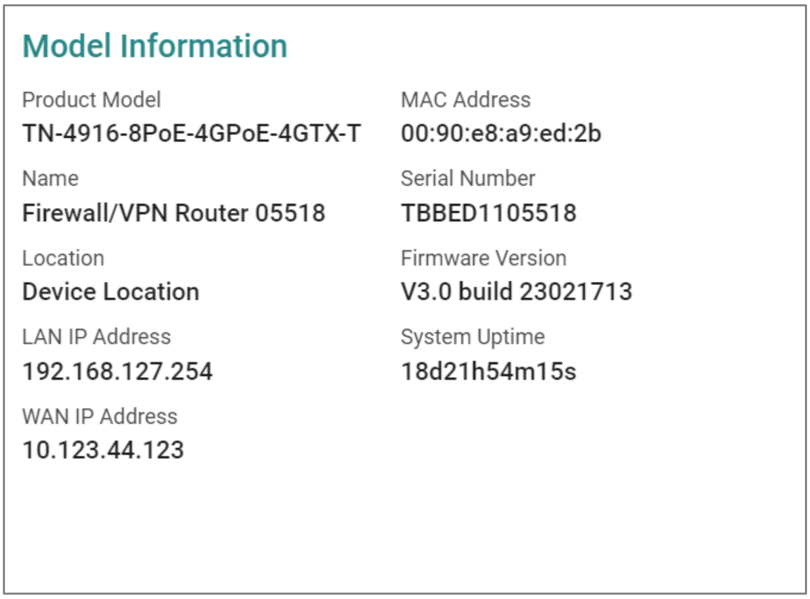
System Event Summary (Last 3 days)

0 Critical
0 Error
0 Warning
0 Notice

CPU Usage History (%) 2023/03/01 13:21:39

Model Information

This display shows basic information about your device.



Model Information

Product Model
TN-4916-8PoE-4GPoE-4GTX-T

Name
Firewall/VPN Router 05518

Location
Device Location

LAN IP Address
192.168.127.254

WAN IP Address
10.123.44.123

MAC Address
00:90:e8:a9:ed:2b

Serial Number
TBBED1105518

Firmware Version
V3.0 build 23021713

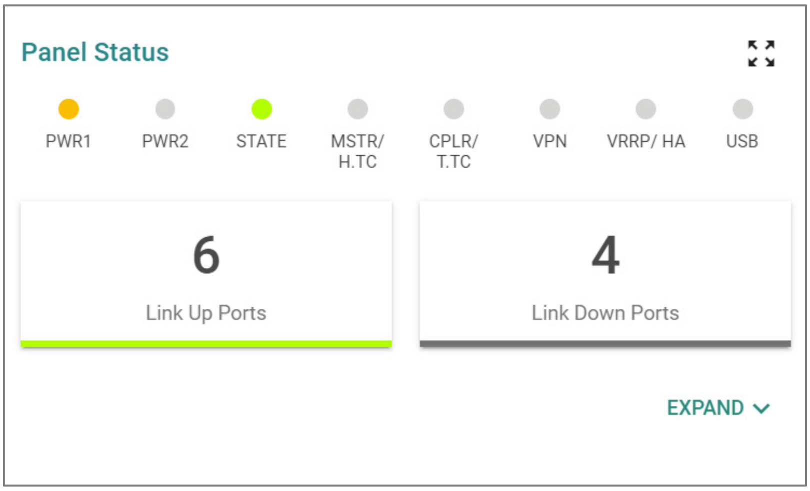
System Uptime
18d21h54m15s

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.
Location	Shows the location of the device. Refer to System > System Management > Information Settings for more information.
LAN IP Address	Shows the LAN IP address of the device. This can be configured in the Setup Wizard.
WAN IP Address	Shows the WAN IP address of your device. This can be configured in the Setup Wizard.
MAC Address	Shows the MAC address of your 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.

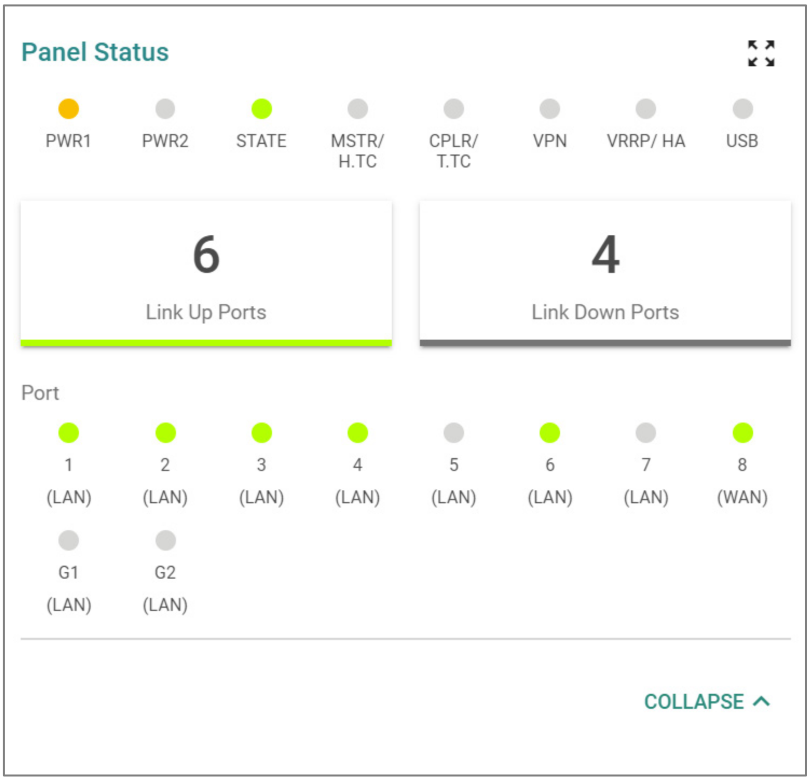
Panel Status

This display shows the status LEDs of your device. For example, connected ports will be shown in green, while disconnected ports will be shown in gray.

Click **EXPAND** to view more detailed information.



Click **COLLAPSE** to hide the details.

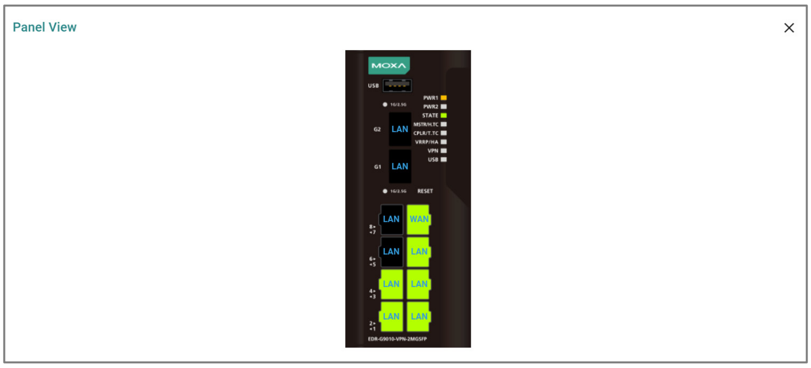


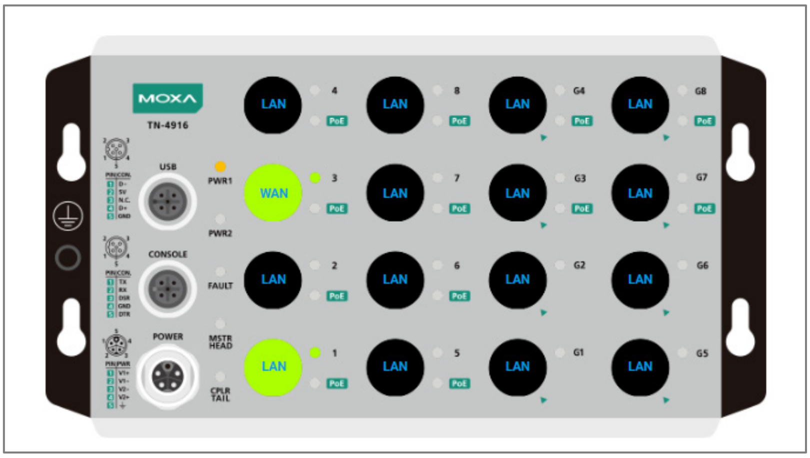
Panel View

Clicking the **Expand (⤢)** icon in the **Panel Status** display will show your device's port status on a representative image of the device. This image will vary depending on your device. Click the **Close (×)** icon in the upper-right corner to close the **Panel View**.

Note

Available LEDs may vary across different versions of devices.



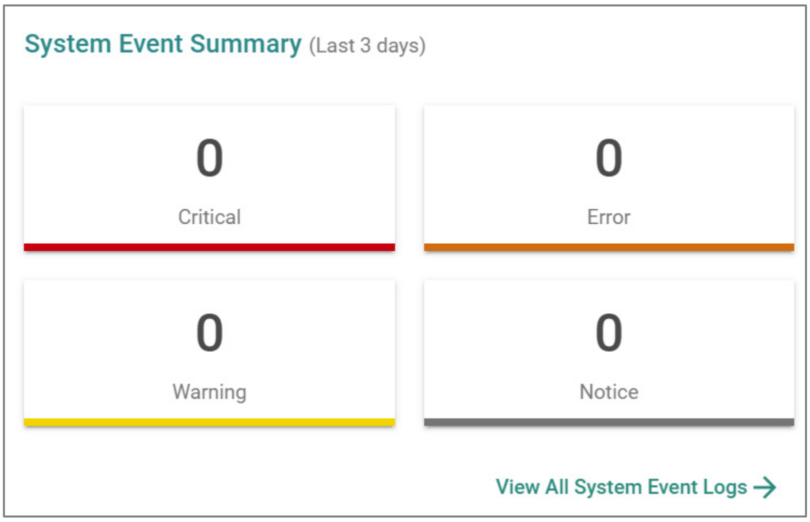


UI Setting	Description
PWR	Shows the power status of the device. **Amber:** Power is being supplied to the designated power input. **Gray**: Power is not being supplied to designated power input.
STATE	Shows the self-diagnosis status of the device. **Solid green**: The system passed the self-diagnosis test on boot-up and is ready to run. **Blinking green**: A device reset is in progress. **Solid red**: The system failed the self-diagnosis test on boot-up.
FAULT	Shows whether corresponding PORT alarm is enabled, and the FAULT LED will turn on while the Port event is triggered in Event Notification. **Red:** When the corresponding PORT alarm is enabled, and a user-configured event is triggered. **Gray:** When the corresponding PORT alarm is enabled and a user-configured event is not triggered, or when the corresponding PORT alarm is disabled.
MSTR/ H.TC	Lights up when the device is the Master/Head of a Turbo Ring/Turbo Chain. This can be configured in Redundancy > Layer 2 Redundancy > Turbo Ring V2. **Solid green**: The device is set as the Master of the Turbo Ring, or as the Head of the Turbo Chain. **Blinking green**: The Turbo Ring or the Turbo Chain is down. **Gray**: The device is not set as the Master of this Turbo Ring or is set as a Member of the Turbo Chain.
CPLR/ T.TC	Lights up when the device is enabling the coupling or tail role of Turbo Chain. **Solid green**: The device's coupling function is enabled to form a backup path, or the device is set as the Tail of the Turbo Chain. **Blinking green**: When Turbo Chain is down. **Gray**: The device’s coupling function is disabled, or the device is set as a Member of the Turbo Chain.
VPN	Lights up when there are active VPN connections. Refer to VPN for more information. **Solid green**: All VPN tunnels are working normally. **Amber**: Only parts of the VPN tunnels are working normally. **Gray**: No active VPN connections.
VRRP/ HA	Lights up when the device is a Master for VRRP or HA. Refer to Redundancy > Layer 3 Redundancy > VRRP for more information. **Solid Green**: The device is set as the Master of the VRRP or HA. **Gray**: The device is not set as the Master of the VRRP or HA.
USB	Lights up when a USB drive is connected. **Solid green**: USB drive successfully connected. **Blinking green**: USB data is being transmitted. **Red:** USB dongle malfunction. **Gray**: USB drive is not connected.

UI Setting	Description
PoE Ports	Lights up when the power is being supplied to a Powered Device (PD). **Amber:** Power is being supplied to a Powered Device (PD). **Gray**: Power is not being supplied to a Powered Device (PD).

System Event Summary (Last 3 days)

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



System Event Summary (Last 3 days)

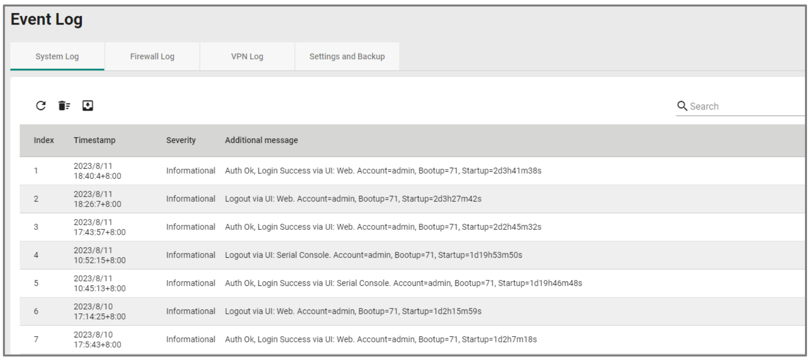
0 Critical

0 Error

0 Warning

0 Notice

Click **View All System Event Logs** to go to the Event Log page to view event logs in more detail.



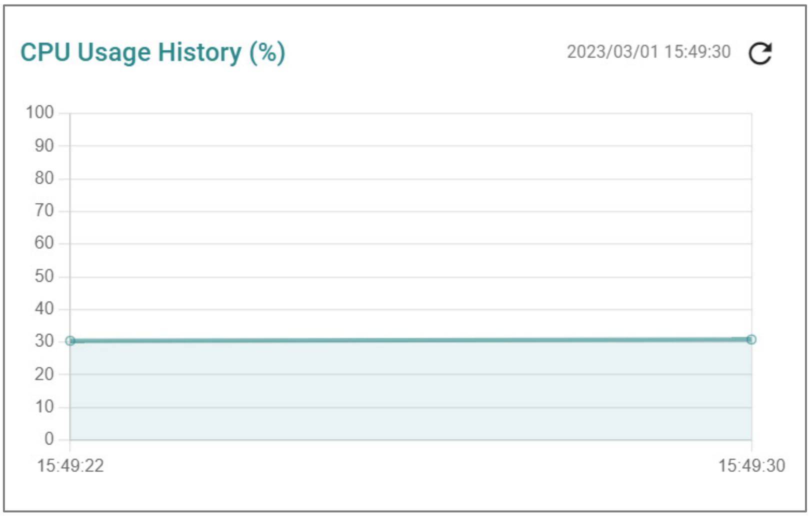
Event Log

Index	Timestamp	Severity	Additional message
1	2023/8/11 18:40:4+8:00	Informational	Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=2d3h41m38s
2	2023/8/11 18:26:7+8:00	Informational	Logout via UI: Web. Account=admin, Bootup=71, Startup=2d3h27m42s
3	2023/8/11 17:43:57+8:00	Informational	Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=2d2h45m32s
4	2023/8/11 10:52:15+8:00	Informational	Logout via UI: Serial Console. Account=admin, Bootup=71, Startup=1d19h53m50s
5	2023/8/11 10:45:13+8:00	Informational	Auth Ok, Login Success via UI: Serial Console. Account=admin, Bootup=71, Startup=1d19h46m48s
6	2023/8/10 17:14:25+8:00	Informational	Logout via UI: Web. Account=admin, Bootup=71, Startup=1d2h15m59s
7	2023/8/10 17:5:43+8:00	Informational	Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=1d2h7m18s

Refer to Diagnostics > Event Logs and Notifications > Event Log for more information.

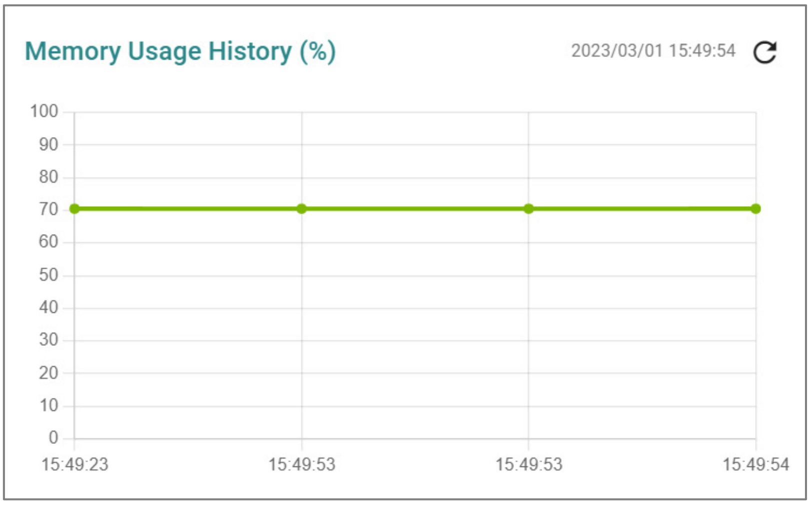
CPU Usage History (%)

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



Memory Usage History (%)

This display shows the device’s memory usage. The data will be shown as a percentage over time. Click the **Refresh (**↻**)** icon to refresh the graph.



Setup Wizard

Menu Path: Setup Wizard

The Setup Wizard helps guide you through basic setup of your device through four steps:

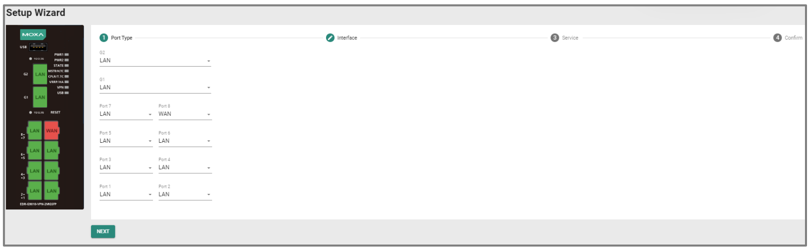
- Port Type
- Interface
- Service
- Confirm

Note

Available settings will vary depending on your product model.

Port Type

In this step, you can set each port of your device to act as a LAN, WAN, or Bridge port.



G2: LAN

G1: LAN

Port 7: LAN

Port 8: WAN

Port 5: LAN

Port 6: LAN

Port 3: LAN

Port 4: LAN

Port 1: LAN

Port 2: LAN

UI Setting	Description	Valid Range	Default Value
G1 / G2	Select whether to use this fiber port as a LAN, WAN, or Bridge port.	LAN / WAN / Bridge	LAN
Port 1 / 2 / 3 / 4 / 5 / 6 / 7 / 8	Select whether to use this Ethernet port as a LAN, WAN, or Bridge port.	LAN / WAN / Bridge	LAN

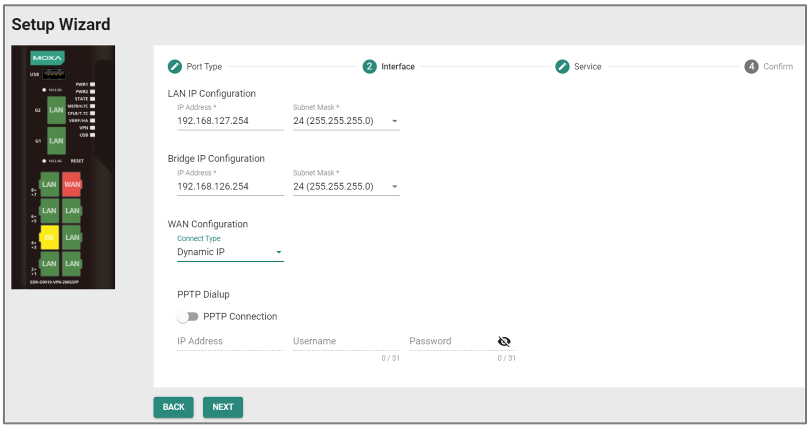
Interface

In this step, you can set up the connection interfaces for your device:

- LAN IP Configuration
- Bridge IP Configuration
- WAN Configuration

Note

Some of these settings may not appear if there are no ports set to **LAN**, **WAN**, or **Bridge**.



LAN IP Configuration

IP Address * 192.168.127.254

Subnet Mask * 24 (255.255.255.0)

Bridge IP Configuration

IP Address * 192.168.126.254

Subnet Mask * 24 (255.255.255.0)

WAN Configuration

Connect Type: Dynamic IP

PPTP Dialup

PPTP Connection

IP Address

Username 0 / 31

Password 0 / 31

LAN IP Configuration

Set the LAN connection details for your device. If you're not familiar with your LAN interface, seek assistance from the network administrator. Network administrator usually determind the LAN interface configuration.

UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address for your LAN port. **Note** The IP Address should be input as a unicast IP address.	Valid IP address	192.168.127.245
Subnet Mask	Specify the subnet mask for your LAN port.	Valid subnet mask	255.255.255.0

WAN IP Configuration

Set the WAN connection details for your device. If you're not familiar with your WAN interface, seek assistance from the network administrator. Network administrator usually determind the WAN interface configuration.

UI Setting	Description	Valid Range	Default Value
Connect Type	Select the connection type to use for your WAN port.	Dynamic IP / Static IP / PPPoE	Dynamic IP

If you choose **Static IP** as your **Connection Type**, these settings will also appear:

UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address for your WAN port.	Valid IP address	N/A
Gateway	Specify the gateway for your WAN port.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask for your WAN port.	Valid subnet mask	N/A

PPTP Dialup

Set the PPTP Dialup connection details for your device. This section only appears if **Static IP** or **Dynamic IP** is set for **WAN Configuration > Connect Type**.

Note

Availability of this feature may vary depending on your product model and version.

UI Setting	Description	Valid Range	Default Value
PPTP Connection	Enable or disable using a PPTP connection.	Enabled / Disabled	Disabled
IP Address	Specify the IP address of your PPTP connection.	Valid IP address	N/A
Username	Specify the username for your PPTP connection.	1 to 31 characters	N/A
Password	Specify the password for your PPTP connection.	1 to 31 characters	N/A

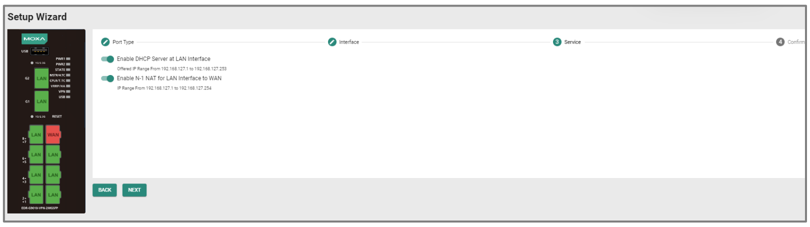
PPPoE Dialup

Set the PPPoE Dialup connection details for your device. This section only appears if **PPPoE** is set for **WAN Configuration > Connect Type**.

UI Setting	Description	Valid Range	Default Value
Username	Specify the username for your PPPoE connection.	1 to 31 characters	N/A
Password	Specify the password for your PPTP connection.	1 to 31 characters	N/A
Host Name	Specify the host name for your PPPoE connection.	1 to 31 characters	N/A

Service

In this step, you can enable or disable services for your device.

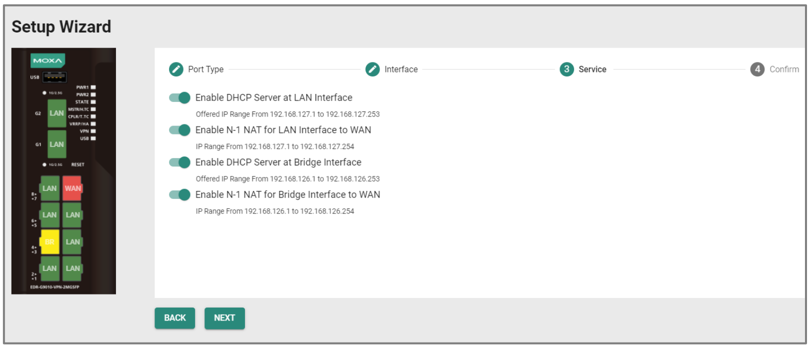


Enable DHCP Server at LAN Interface

Offered IP Range From 192.168.127.1 to 192.168.127.253

Enable N-1 NAT for LAN Interface to WAN

IP Range From 192.168.127.1 to 192.168.127.254



Enable DHCP Server at LAN Interface

Offered IP Range From 192.168.127.1 to 192.168.127.253

Enable N-1 NAT for LAN Interface to WAN

IP Range From 192.168.127.1 to 192.168.127.254

Enable DHCP Server at Bridge Interface

Offered IP Range From 192.168.126.1 to 192.168.126.253

Enable N-1 NAT for Bridge Interface to WAN

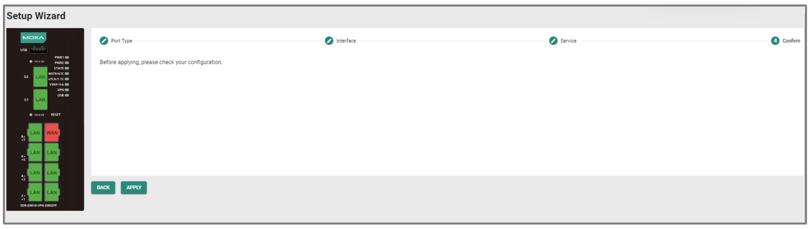
IP Range From 192.168.126.1 to 192.168.126.254

UI Setting	Description	Valid Range	Default Value
Enable DHCP Server at LAN Interface	Enable or disable using a DHCP server for the LAN interface.	Enable / Disable	Enable
Enable N-1 NAT for LAN Interface to WAN	Enable or disable using N-1 NAT for LAN interfaces to WAN.	Enable / Disable	Enable
Enable DHCP Server at Bridge Interface **(if Bridge Mode is Port)**	Enable or disable using a DHCP server for bridge interfaces.	Enable / Disable	Enable

UI Setting	Description	Valid Range	Default Value
Enable N-1 NAT for Bridge Interface to WAN **(if Bridge Mode is Port)**	Enable or disable using N-1 NAT for bridge interfaces to WAN.	Enable / Disable	Enable

Confirm

Confirm your settings, then click **APPLY** to save and apply your changes.



Before applying, please check your configuration.

System

Menu Path: System

The System settings area lets you configure the main system settings for your device.

This settings area includes these sections:

- System Management
- Account Management
- License Management
- Management Interface
- Time
- Setting Check

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
System Management			
Information Settings	R/W	R/W	R
Firmware Upgrade	R/W	-	-
Software Package Management	R/W	-	-
Configuration Backup and Restore	R/W	-	-
Account Management			
User Account	R/W	-	-
Password Policy	R/W	-	-
License Management	R/W	R	R
Management Interface			
User Interface	R/W	R/W	R
Hardware Interface	R/W	R/W	R
SNMP	R/W	-	-
MXsecurity	R/W	R/W	-
Time			
System Time	R/W	R/W	R
NTP/SNTP Server	R/W	R/W	R
Setting Check	R/W	R/W	R
Power Management	R/W	R/W	R
SMS	R/W	R/W	R
GNSS	R/W	R/W	R

System Management

Menu Path: System > System Management

This section lets you manage your device's identification, firmware, and configuration backup settings.

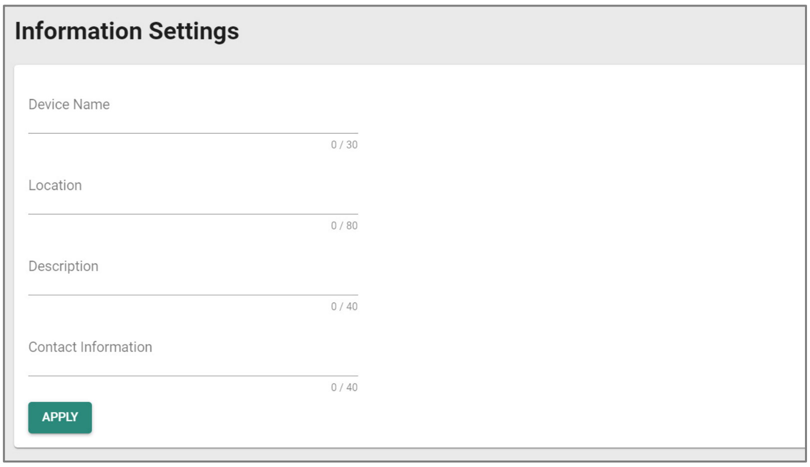
This section includes these pages:

- Information Settings
- Firmware Upgrade
- Software Package Management
- Configuration 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 on the network.



Information Settings

Device Name 0 / 30

Location 0 / 80

Description 0 / 40

Contact Information 0 / 40

UI Setting	Description	Valid Range	Default Value
Device Name	Enter a name for the device.	1 to 30 characters	Firewall/VPN Router-xxxxx (where xxxxx is the last 5 characters of the device's serial number)
Location	Enter a location for the device.	1 to 80 characters	Device Location
Description	Enter a description for the device.	1 to 40 characters	N/A
Contact Information	Enter the contact information of the person in charge of the device.	1 to 40 characters	N/A

Firmware Upgrade

Menu Path: System > System Management > Firmware Upgrade

This page lets you upgrade the firmware of your device.

You can upgrade the firmware through the following methods:

- Local
- TFTP
- USB
- SCP
- SFTP

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.

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.

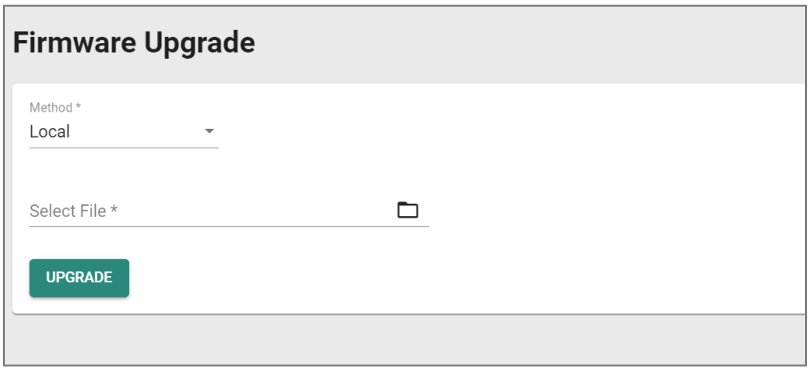
Upgrading the firmware should be only be done by qualified personnel, as it is possible to render the device inoperable if the upgrade is not done properly. If you are not familiar with the process, please request the assistance of qualified personnel. You can also consult with Moxa support and we will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

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.



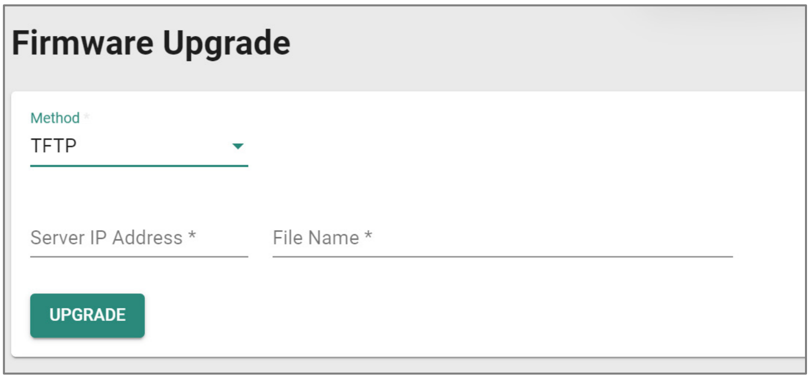
Firmware Upgrade

Method *
Local

UI Setting	Description	Valid Range	Default Value
Select File	Navigate to and upload the firmware file from the local host device.	N/A	N/A

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.



Firmware Upgrade

Method
TFTP

Server IP Address *

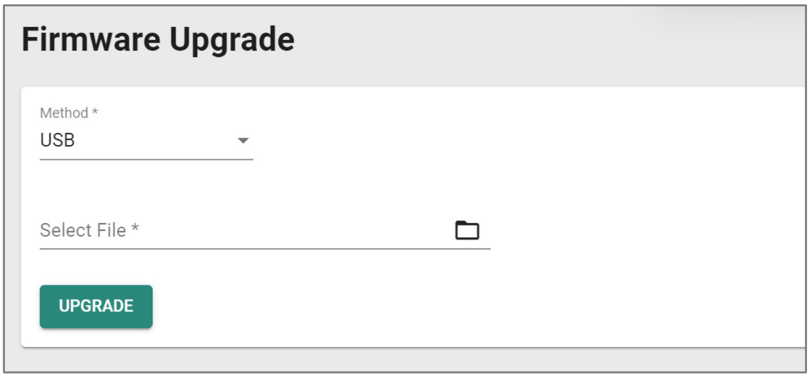
File Name *

UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the TFTP server.	IP address	N/A
File Name	Specify the filename of the firmware file.	File name	N/A

USB

If you select **USB** as your **Method**, these settings will appear. The USB method allows you to install firmware directly from a USB drive attached to your device.

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



Firmware Upgrade

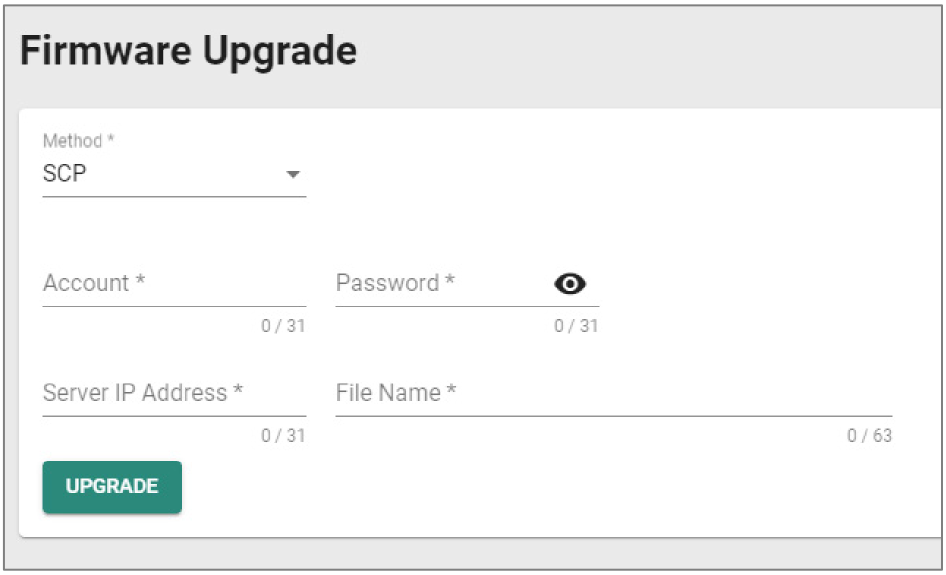
Method *
USB

Select File *

UI Setting	Description	Valid Range	Default Value
Select File	Select the firmware file on the USB device.	N/A	N/A

SCP

If you select **SCP** as your **Method**, these settings will appear. The SCP (secure copy protocol) method lets you upload and install firmware from a remote system.



Firmware Upgrade

Method *
SCP

Account * 0 / 31

Password * 0 / 31

Server IP Address * 0 / 31

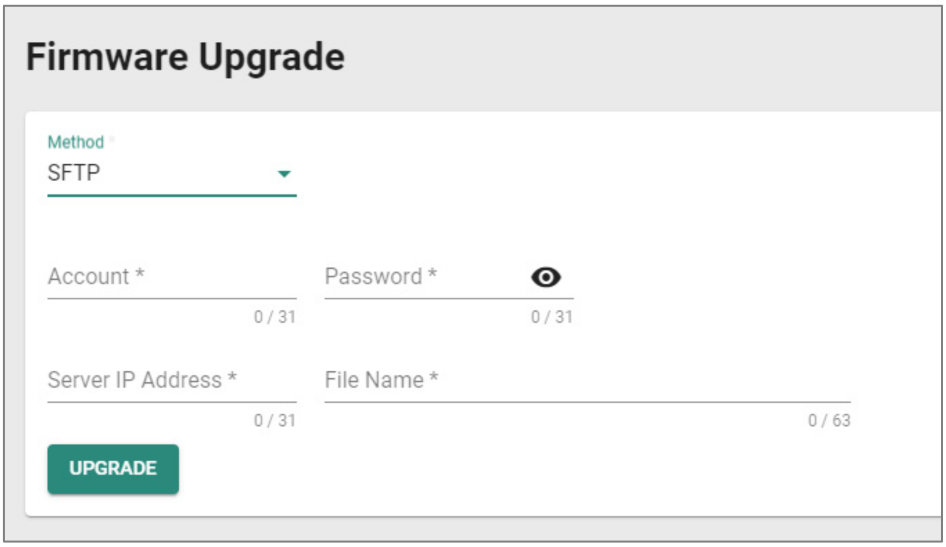
File Name * 0 / 63

UI Setting	Description	Valid Range	Default Value
Account	Enter the remote system account name.	1 to 31 characters	N/A

UI Setting	Description	Valid Range	Default Value
Password	Enter the remote system account password.	1 to 31 characters	N/A
Server IP Address	Specify the IP address of the remote system.	IP address	N/A
File Name	Specify the filename of the firmware file.	1 to 63 characters	N/A

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.



Firmware Upgrade

Method: SFTP

UI Setting	Description	Valid Range	Default Value
Account	Enter the SFTP server account name.	1 to 31 characters	N/A
Password	Enter the SFTP server account password.	1 to 31 characters	N/A
Server IP Address	Specify the IP address of the SFTP server.	IP address	N/A
File Name	Specify the filename of the firmware file.	1 to 63 characters	N/A

Software Package Management

Menu Path: System > System Management > Software Package Management

This page lets you upgrade your Network Security Package and MXsecurity Agent Package, enhancing your device's security capabilities. To upgrade a software package, you can either use the package included with the currently installed firmware, or you can download the latest version from the resource section on the Moxa website at www.moxa.com.

Note

Keeping your software packages updated is critical to keep your device and network secure against the latest cyberattacks.

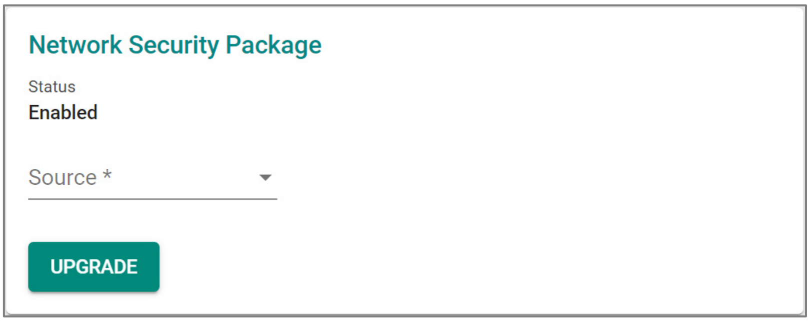
- **Network Security Package**: Helps your protect your device and network with IPS (Intrusion Prevention System) patterns and a DPI (Deep Packet Inspection) engine.

Note

Products that do not support a firewall will not be compatible with the Network Security Package. Most Moxa routers support firewall functionality, except for products with model names that include **'-ETBN-'** but do not include **'-F-'**, such as the **TN-4908-ETBN-4GTX-4GTXBP-WV-CT-T**.

- **MXsecurity Agent Package**: Provides centralized visibility and security management to streamline management of your device. It helps you monitor and identify cyberthreats, and also helps prevent security misconfigurations to create a robust threat defense.

Network Security Package


Network Security Package

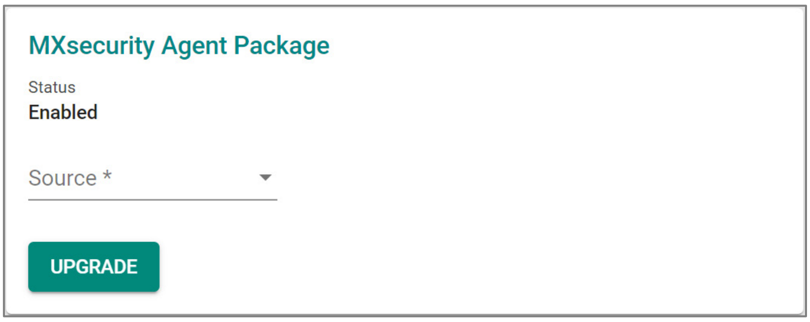
Status

Enabled

Source *

UI Setting	Description	Valid Range	Default Value
Source	Select a source to use to upgrade the software package. **Local**: Use a file stored on the local host. **Firmware**: Use the package included with the current firmware.	Local / Firmware	N/A
Select File **(if Local is set for Source)**	Select network secruity package downloaded from Moxa's website. Moxa will periodically release new security packages on the Moxa official website. Users can download the latest security package and then import it into their device.	N/A	N/A
Package Version **(if Firmware is set for Source)**	Shows the included package version of the current firmware.	N/A	Current Package Version

MXsecurity Agent Package


MXsecurity Agent Package

Status

Enabled

Source *

UI Setting	Description	Valid Range	Default Value
Source	Select a source to use to upgrade the software package. **Local**: Use a file stored on the local host. **Note** The **Local** option is not commonly used in standard environments. However, if you experience issues with your device and MXsecurity, please reach out to Moxa Technical Support. They can utilize the **Local** option as a troubleshooting interface. **Firmware**: Use the package included with the current firmware.	Local / Firmware	N/A
Select File **(if Source is Local)**	This is a troubleshooting interface in case you encounter issues with your device and MXsecurity.	N/A	N/A
Package Version **(if Source is Firmware)**	This shows the included package version of the current firmware.	N/A	Current Package Version

Configuration Backup and Restore

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

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

This page includes these tabs:

- Backup
- Restore
- File Encryption

Configuration Backup and Restore - Backup

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

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

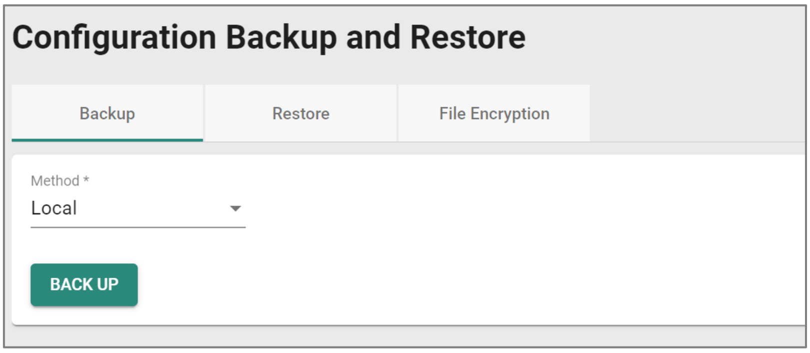
There are multiple methods of backing up the device configuration:

- Local
- TFTP
- USB
- SCP
- SFTP

For security reasons, we strongly recommend the administrator to back up the system configuration to a secure storage location periodically.

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.

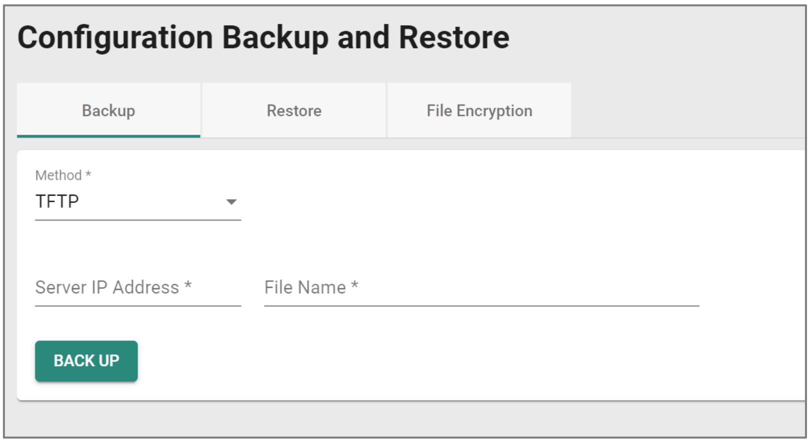


Configuration Backup and Restore

Method * Local

TFTP

If you select **TFTP** as your **Method**, these settings will appear. The TFTP method lets you upload the configuration backup file to a remote TFTP server.



Configuration Backup and Restore

Method * TFTP

Server IP Address *

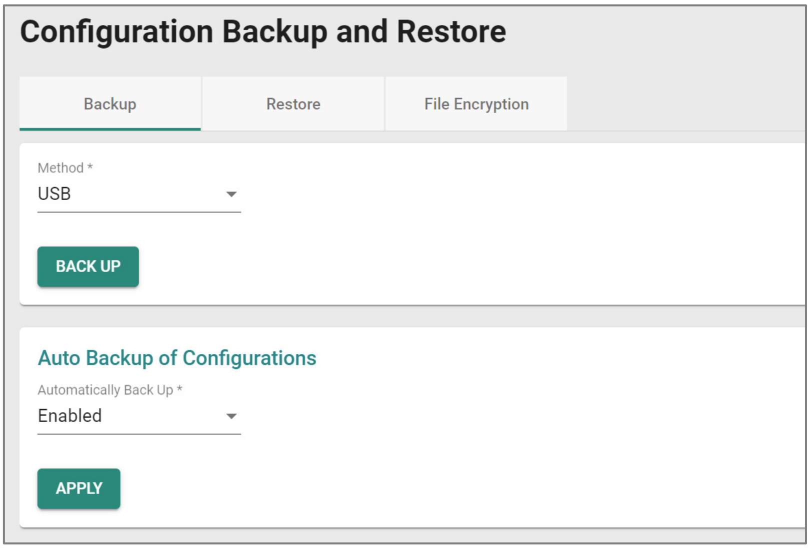
File Name *

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 backup file.	1 to 63 characters	N/A

USB

If you select **USB** as your **Method**, these settings will appear. The USB method allows you to export the configuration backup file to a USB drive connected to the device. You can also enable automatic backups, which will export a configuration file to a USB drive whenever the configuration is changed.

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



Configuration Backup and Restore

Method *: USB

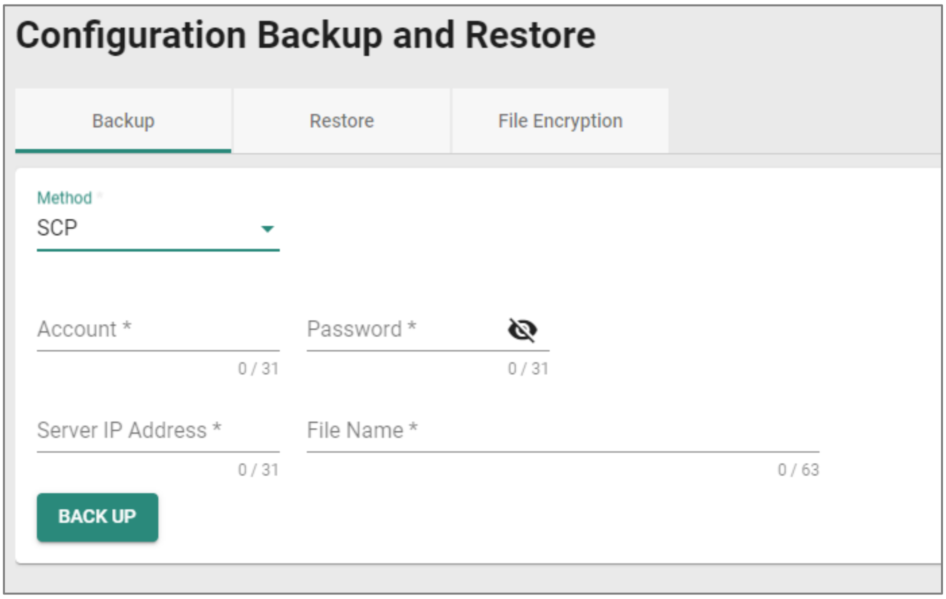
Auto Backup of Configurations

Automatically Back Up *: Enabled

UI Setting	Description	Valid Range	Default Value
Automatically Back Up	Enable or disable automatic backups.	Enabled / Disabled	Disabled

SCP

If you select **SCP** as your **Method**, these settings will appear. The SCP (secure copy protocol) method lets you upload the configuration backup file to a remote system.



Configuration Backup and Restore

Method: SCP

Account * 0 / 31

Password * 0 / 31

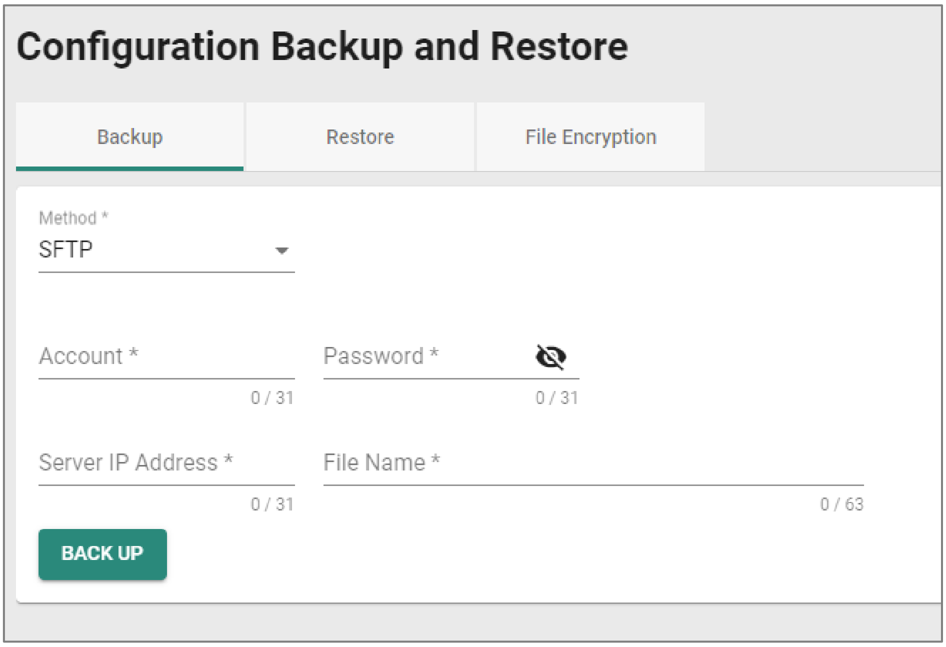
Server IP Address * 0 / 31

File Name * 0 / 63

UI Setting	Description	Valid Range	Default Value
Account	Enter the remote system account name.	1 to 31 characters	N/A
Password	Enter the remote system account password.	1 to 31 characters	N/A
Server IP Address	Specify the IP address of the remote system.	Valid IP address	N/A
File Name	Specify the file name of the configuration backup file.	1 to 63 characters	N/A

SFTP

If you select **SFTP** as your **Method**, these settings will appear. The SFTP method lets you upload the configuration backup file to a remote SFTP server.



Configuration Backup and Restore

Method *
SFTP

Account * 0 / 31

Password * 0 / 31

Server IP Address * 0 / 31

File Name * 0 / 63

UI Setting	Description	Valid Range	Default Value
Account	Enter the SFTP server account name.	1 to 31 characters	N/A
Password	Enter the SFTP server account password.	1 to 31 characters	N/A
Server IP Address	Specify the IP address of the SFTP server.	Valid IP address	N/A
File Name	Specify the file name of the configuration backup file.	1 to 63 characters	N/A

Configuration Backup and Restore - Restore

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

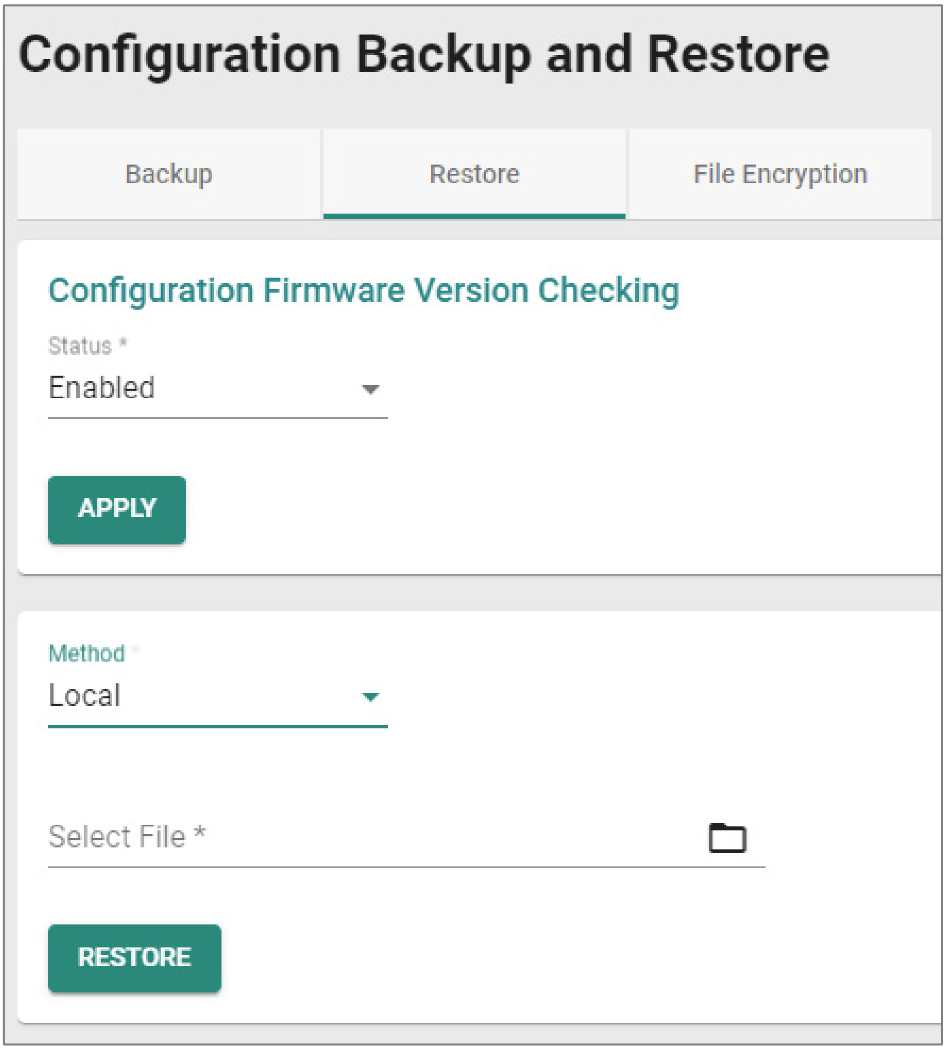
This page lets you restore a previously backed up configuration.

There are multiple methods of restoring the device configuration:

- Local
- TFTP
- USB
- SCP
- SFTP

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.



Configuration Backup and Restore

Configuration Firmware Version Checking

Status * Enabled

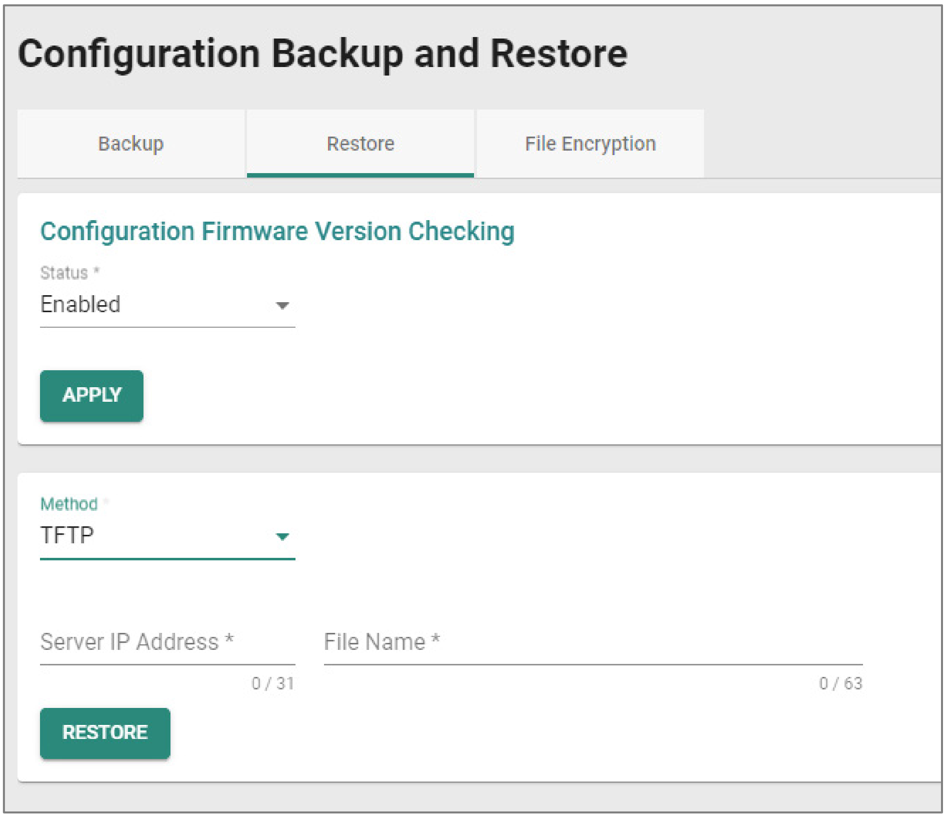
Method Local

Select File *

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable configuration firmware version checking. This checks whether your current firmware version matches the one the configuration file is for.	Enabled / Disabled	Disabled
Select File	Select the configuration file to restore from.	N/A	N/A

TFTP Server

If you select **TFTP** as your **Method**, these settings will appear. The TFTP method lets you restore from a configuration file on a remote TFTP server.


Configuration Backup and Restore

Configuration Firmware Version Checking

Status *
Enabled

Method *
TFTP

Server IP Address *
0 / 31

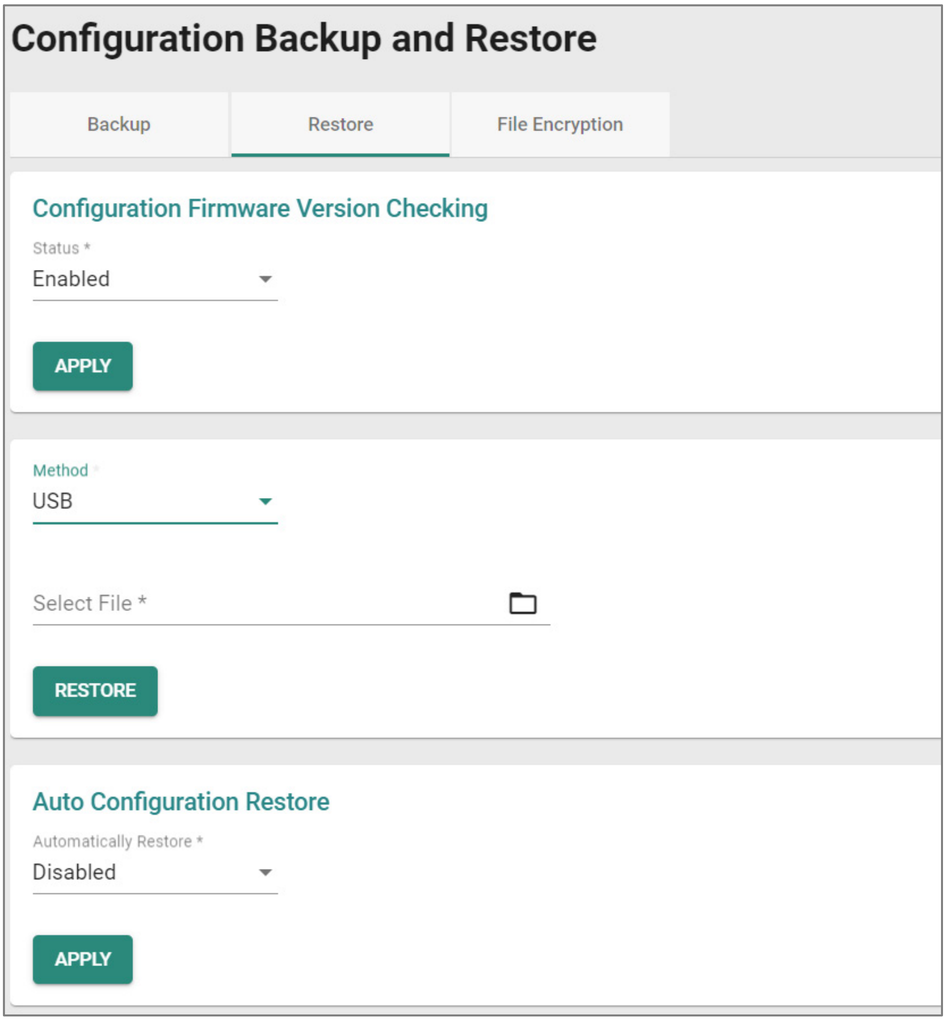
File Name *
0 / 63

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable configuration firmware version checking. This checks whether your current firmware version matches the one the configuration file is for.	Enabled / Disabled	Disabled
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.	N/A	N/A

USB

If you select **USB** as your **Method**, these settings will appear. The USB method allows you to restore from a configuration file on a USB drive connected to the device.

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



Configuration Backup and Restore

Configuration Firmware Version Checking

Status *: Enabled

Method: USB

Select File *

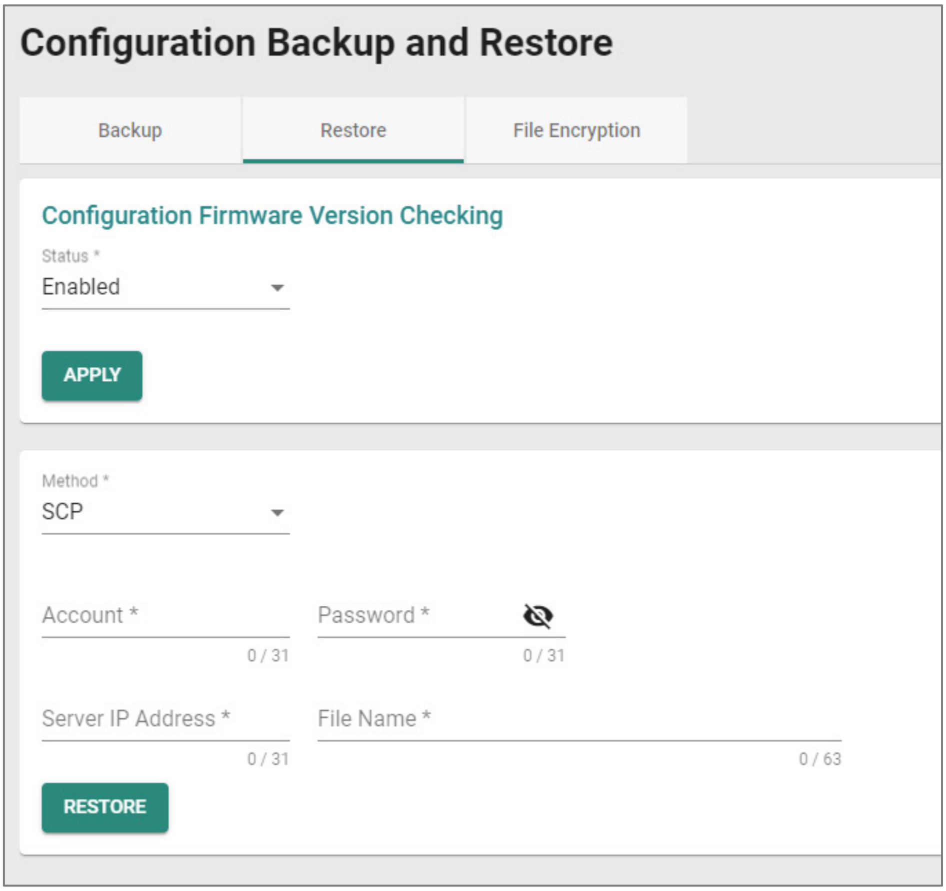
Auto Configuration Restore

Automatically Restore *: Disabled

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable configuration firmware version checking. This checks whether your current firmware version matches the one the configuration file is for.	Enabled / Disabled	Disabled
Select File	Select file for restore.	N/A	N/A
Automatically Restore **(Only when Method is USB)**	Enable or disable auto restore of the device configuration. If this function is enabled, The ABC-02 will automatically export configuration once there is any change.	Enabled / Disabled	Disabled

SCP

If you select **SCP** as your **Method**, these settings will appear. The SCP (secure copy protocol) method allows you to restore from a configuration file on a remote system.



Configuration Backup and Restore

Configuration Firmware Version Checking

Status * Enabled

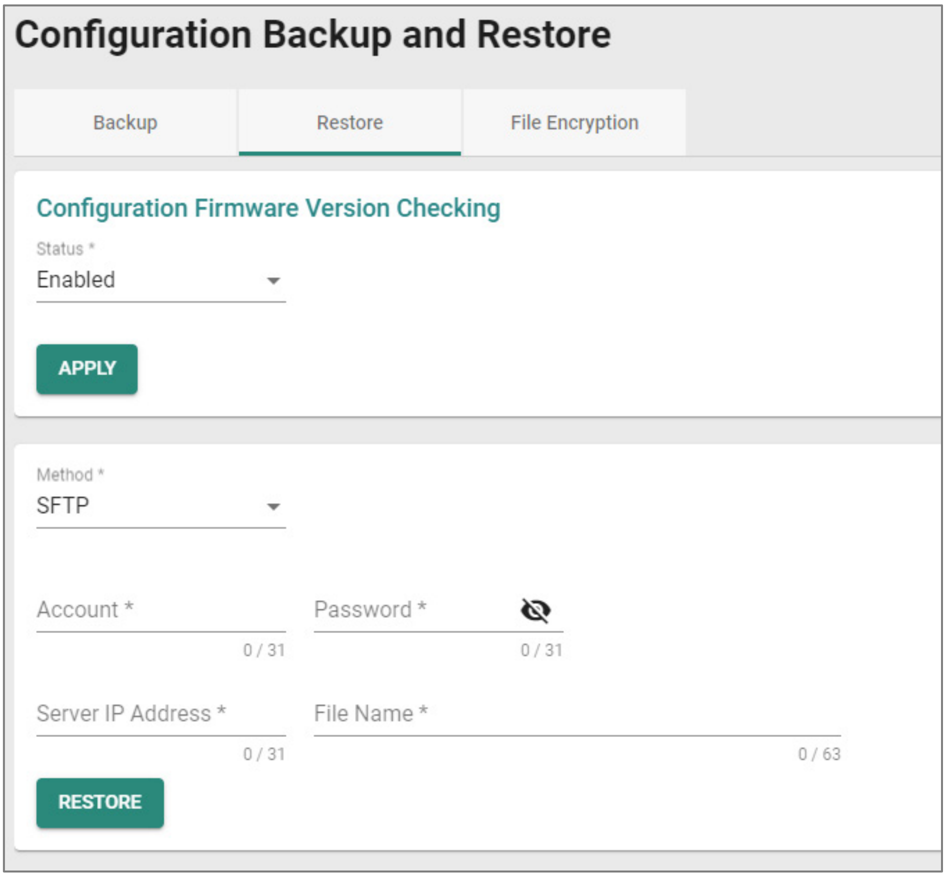
Method * SCP

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable configuration firmware version checking. This checks whether your current firmware version matches the one the configuration file is for.	Enabled / Disabled	Disabled
Account	Enter the remote system account name.	1 to 31 characters	N/A
Password	Enter the remote system account password.	1 to 31 characters	N/A

UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the remote system.	Valid IP address	N/A
File Name	Specify the file name of the configuration file to restore from.	N/A	N/A

SFTP

If you select **SFTP** as your **Method**, these settings will appear. The SFTP method allows you to restore from a configuration file on a remote SFTP server.


Configuration Backup and Restore

Configuration Firmware Version Checking

Status *: Enabled

Method *: SFTP

Account * 0 / 31

Password * 0 / 31

Server IP Address * 0 / 31

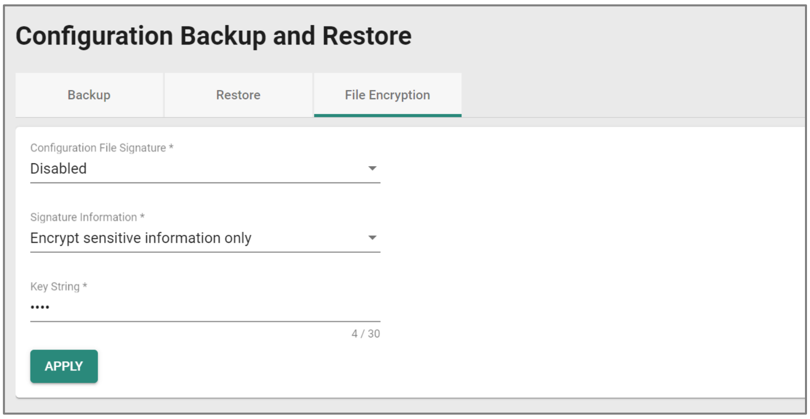
File Name * 0 / 63

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable configuration firmware version checking. This checks whether your current firmware version matches the one the configuration file is for.	Enabled / Disabled	Disabled
Account	Enter the remote system account name.	1 to 31 characters	N/A
Password	Enter the remote system account password.	1 to 31 characters	N/A
Server IP Address	Specify the IP address of the remote system.	Valid IP address	N/A
File Name	Specify the file name of the configuration file to restore from.	N/A	N/A

Configuration Backup and Restore - File Encryption

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

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



Configuration File Signature *
Disabled

Signature Information *
Encrypt sensitive information only

Key String *
••••
4 / 30

UI Setting	Description	Valid Range	Default Value
Configuration File Signature	Enables or disables the use of a digital signature for checking the integrity of a configuration file.	Enabled / Disabled	Disabled
Signature Information	Select the type of data to encrypt. **Encrypt sensitive information only**: Only encrypt password-related sensitive information in the exported configuration file. **Encrypt all information**: Encrypt all information in the exported configuration file.	Encrypt sensitive information only / Encrypt all information	Encrypt sensitive information only
Key String	Specify an encryption key string. The key string is used to decrypt encrypted configuration files.	1 to 30 characters	moxa

Account Management

Menu Path: System > Account Management

This section lets you manage the user accounts used to access the device.

This section includes these pages:

- User Accounts
- Password Policy

User Accounts

Menu Path: System > Account Management > User Accounts

This page allows you create, manage, modify, and remove user accounts.

Note

- We strongly recommend changing the default password for the admin account after logging in for the first time.
- The default admin account cannot be deleted and is enabled by default.
- Only admin accounts may change the password for supervisor and user accounts.
- For security reasons, it is recommended for the administrator to keep a record of the account list and associated users.

Due to the constraints of the IEC 62443-4-2 integrity verification standard, User Accounts will be reset to Factory Default under certain conditions. Specifically, all non-Factory Default user accounts will be entirely removed by the system when the following conditions are all met:

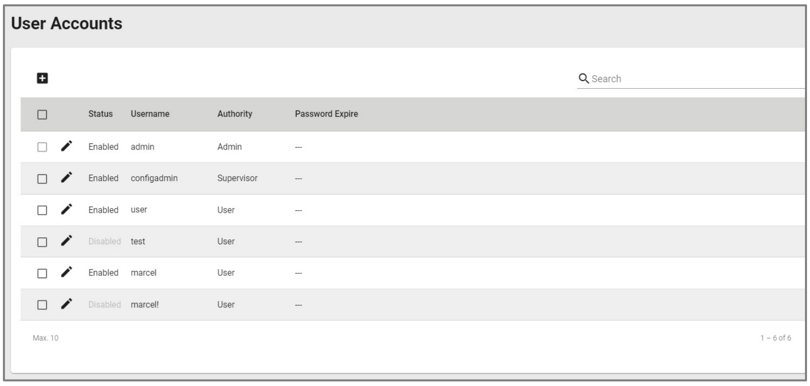
- The original firmware version of the user device is V.3.0 or higher.
- The user downgrades the firmware below to V.3.0 and performs any action on this firmware.
- The firmware version is subsequently upgraded back to V.3.0 or higher.

In cases where all these conditions are satisfied, all user-created non-factory default accounts will be removed.

However, if a user's original firmware version was below V.3.0 and they later upgrade to V.3.0 or subsequent versions, this issue will not arise.

Limitations

You can create up to 10 user accounts.



User Accounts

□		Status	Username	Authority	Password Expire
□	✎	Enabled	admin	Admin	---
□	✎	Enabled	configadmin	Supervisor	---
□	✎	Enabled	user	User	---
□	✎	Disabled	test	User	---
□	✎	Enabled	marcel	User	---
□	✎	Disabled	marcel!	User	---

Max. 10

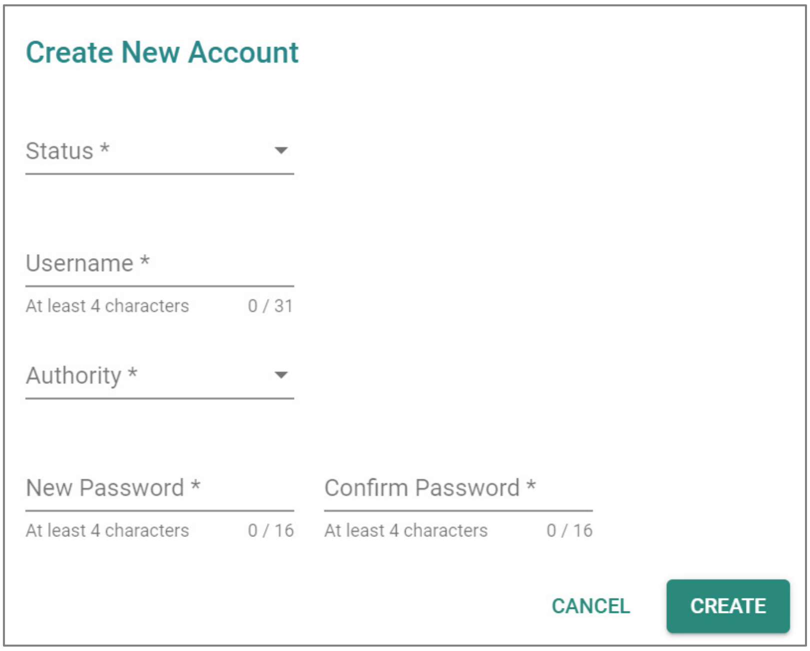
1 – 6 of 6

UI Setting	Description
Status	Shows if the account is enabled or disabled.
Username	Shows the username of the account.
Authority	Shows the authority level of the account.
Password Expire	Shows the number of days left before the password expires for the account. A **-** means the password will not expire. The password expiration time is determined by the **Password Max-life-time** setting on the **Password Policy** page. Refer to System > Account Management > Password Policy for more information.

Create New Account

Menu Path: Menu Path: System > Account Management > User Accounts - Create New Account

Clicking the **Add (** ⊞ **)** icon on the **System > Account Management > User Accounts** 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
Status	Enable or disable this user account.	Enabled / Disabled	N/A
Username	Enter a user name for this account.	4 to 31 characters	N/A
Authority	Select an authority role for this account. **Admin**: The account will have read/write access to all configuration parameters. **Supervisor**: The account will have read/write access to all configuration parameters except create, delete, and modify accounts. **User**: The account can only view configurations and cannot make any modifications. **Note** Refer to User Role Privileges for a list of what read/write access privileges are granted for the different authority levels.	Admin / Supervisor / User	N/A

UI Setting	Description	Valid Range	Default Value
New Password	Enter a password for this account. **Note** The new password must follow any requirements set on the **System > Account Management > Password Policy** page.	4 to 16 characters, additional requirements are based on settings in **System > Account Management > Password Policy**	N/A
Confirm Password	Enter the password again to confirm.	4 to 16 characters	N/A

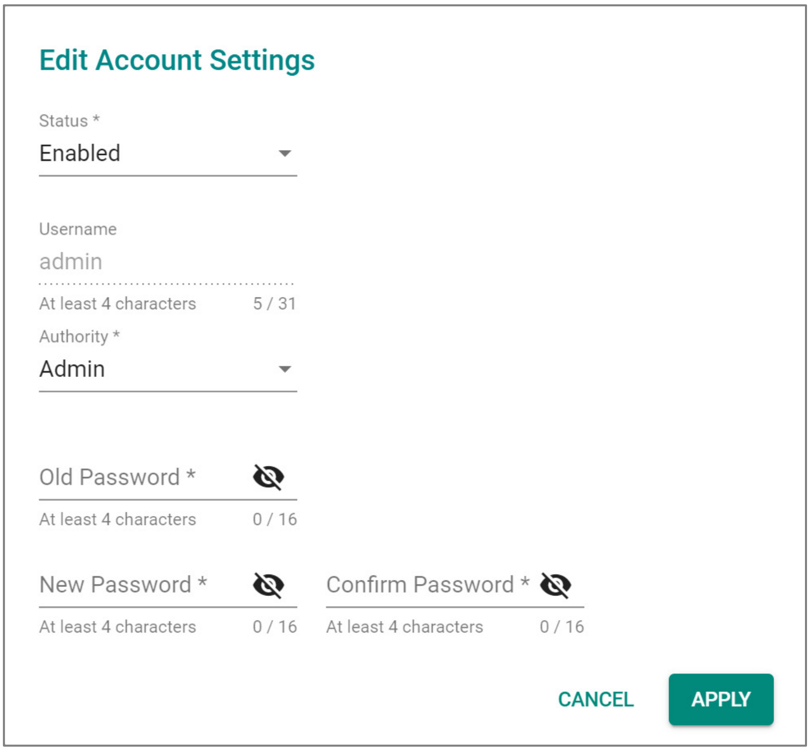
Edit Account Settings

Menu Path: System > Account Management > User Accounts - Edit Account Settings

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.

Note

All account parameters can be modified, except for the username. To modify the username, you must create a new user account.



Edit Account Settings

Status *
Enabled

Username
admin
At least 4 characters 5 / 31

Authority *
Admin

Old Password *
At least 4 characters 0 / 16

New Password *
At least 4 characters 0 / 16

Confirm Password *
At least 4 characters 0 / 16

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this user account.	Enabled / Disabled	N/A
Username	Shows the username for this account. The username cannot be changed.	N/A	N/A

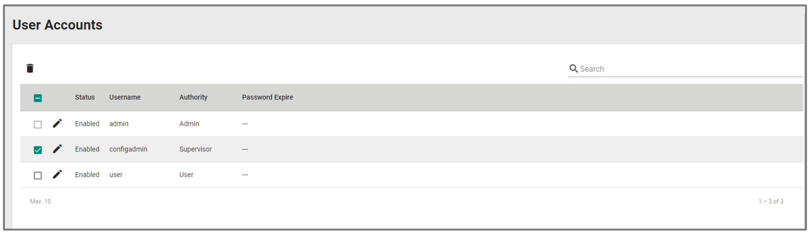
UI Setting	Description	Valid Range	Default Value
Authority	Select an authority role for this account. **Admin**: The account will have read/write access to all configuration parameters. **Supervisor**: The account will have read/write access to all configuration parameters except create, delete, and modify accounts. **User**: The account can only view configurations and cannot make any modifications. **Note** Refer to User Role Privileges for a list of what read/write access privileges are granted for the different authority levels.	Admin / Supervisor / User	N/A
Old Password	Enter the old password for this account.	4 to 16 characters	N/A
New Password	Enter the new password for this account. **Note** The new password must follow any requirements set on the **System > Account Management > Password Policy** page.	4 to 16 characters, additional requirements are based on settings in **System > Account Management > Password Policy**	N/A
Confirm Password	Enter the password again to confirm.	4 to 16 characters, additional requirements are based on settings in **System > Account Management > Password Policy**	N/A

Delete User Account

Menu Path: System > Account Management > User Accounts

You can delete user accounts by using the checkboxes to select the accounts you want to delete, then clicking the **Delete (🗑)** icon.

The default **admin** account is enabled by default and cannot be deleted.



User Accounts

☐		Status	Username	Authority	Password Expire
☐	✎	Enabled	admin	Admin	---
☑	✎	Enabled	configadmin	Supervisor	---
☐	✎	Enabled	user	User	---

Max. 10

1 – 3 of 3

Password Policy

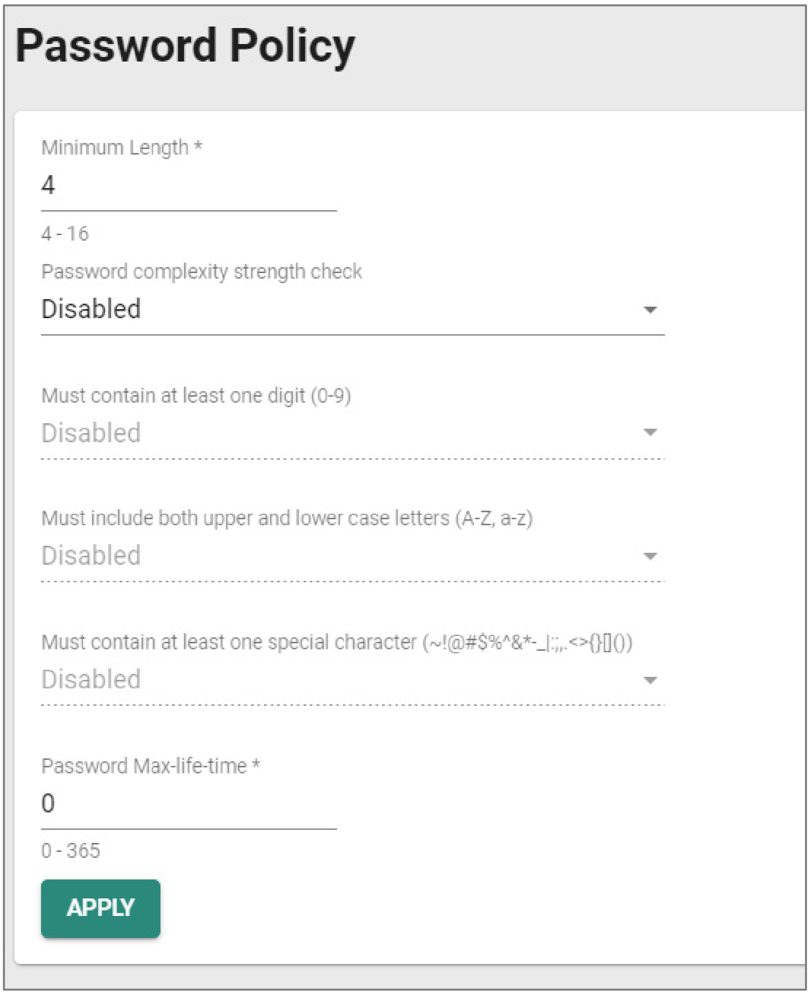
Menu Path: System > Account Management > Password Policy

This page allows you to set password complexity rules for user accounts to improve 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 16.
- Enable the **Password complexity strength check** and enable all the requirement options.
- Set a **Password Max-life-time** to ensure that users change their password regularly.



Password Policy

Minimum Length *

4

4 - 16

Password complexity strength check

Disabled

Must contain at least one digit (0-9)

Disabled

Must include both upper and lower case letters (A-Z, a-z)

Disabled

Must contain at least one special character (~!@#$%^&*-_|;:,.<>{}[]())

Disabled

Password Max-life-time *

0

0 - 365

UI Setting	Description	Valid Range	Default Value
Minimum Length	Set the minimum required password length.	4 to 16 characters	4
Password complexity strength check	Enable or disable the password complexity strength check.	Enabled / Disabled	Disabled
Must contain at least one digit (0-9) **(if Password complexity strength check is Enabled)**	Enable or disable requiring the password to contain at least one digit.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Must include both upper and lower case letters (A-Z, a-z) **(if Password complexity strength check is Enabled)**	Enable or disable requiring the password to include both uppercase and lowercase letters.	Enabled / Disabled	Disabled
Must contain at least one special character (~!@#$%^&*-|:;,.<>{}[]()) **(if Password complexity strength check is Enabled)**	Enable or disable requiring the password to contain at least one special character.	Enabled / Disabled	Disabled
Password Max-life-time	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	0

License Management

Menu Path: System > License Management

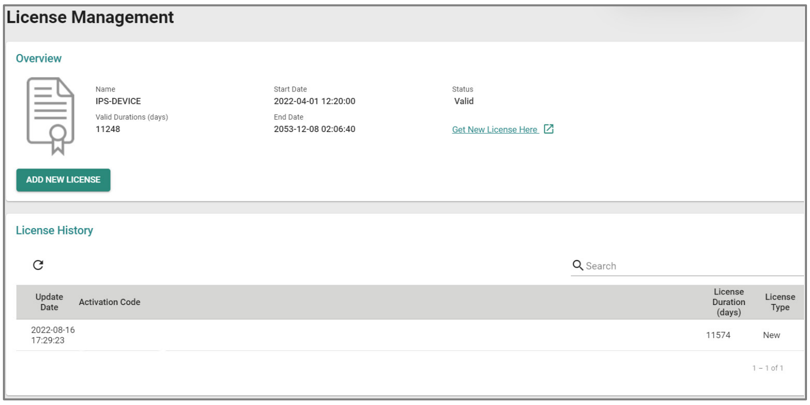
This page lets you add new licenses and view details about existing ones.

This page includes these sections:

- Overview
- License History

Overview

This section lets you view details about your current license, and lets you add or get a new license. To add or get a new license, click on **ADD NEW LICENSE**, which will guide you through the process.



License Management

Overview

Name
IPS-DEVICE

Valid Durations (days)
11248

Start Date
2022-04-01 12:20:00

End Date
2053-12-08 02:06:40

Status
Valid

Get New License Here

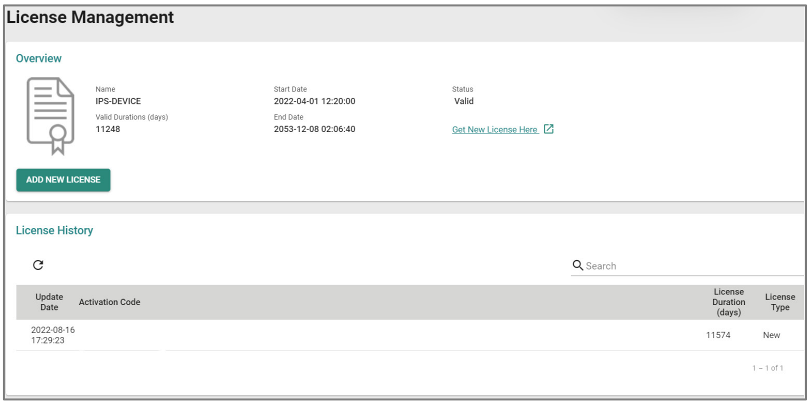
License History

Update Date	Activation Code	License Duration (days)	License Type
2022-08-16 17:29:23		11574	New

1 – 1 of 1

License History

This area lets you see details about previously installed licenses.



License Management

Overview

Name
IPS-DEVICE

Valid Durations (days)
11248

Start Date
2022-04-01 12:20:00

End Date
2053-12-08 02:06:40

Status
Valid

Get New License Here

ADD NEW LICENSE

License History

Search

Update Date | Activation Code | License Duration (days) | License Type
2022-08-16 17:29:23 | | 11574 | New

1 – 1 of 1

UI Setting	Description
Update Date	Shows date the license was updated.
Activation Code	Shows the activation code of the license.
License Duration (days)	Shows the remaining duration of the license in days.
License Type	Shows the type of license.

Adding a New License

Goal

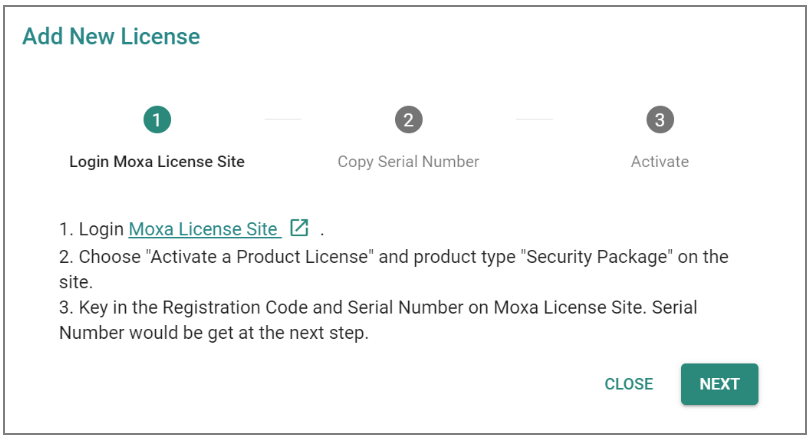
This section provides step-by-step instructions on how to add a new license for your Moxa device.

Prerequisites

- You will need the registration code for your license. You should have received this by email after purchasing the license.

Procedure

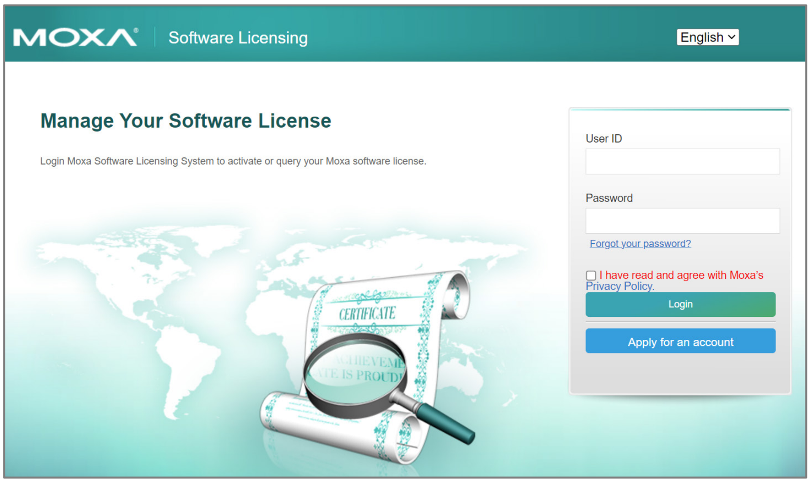
1. In **System > License Management**, click on the **Add New License** button. A new page with instructions will appear.



Add New License

1. Login Moxa License Site .
2. Choose "Activate a Product License" and product type "Security Package" on the site.
3. Key in the Registration Code and Serial Number on Moxa License Site. Serial Number would be get at the next step.

2. Click on the **Moxa License Site** link to open a new browser window for the Moxa Software Licensing site and log in.

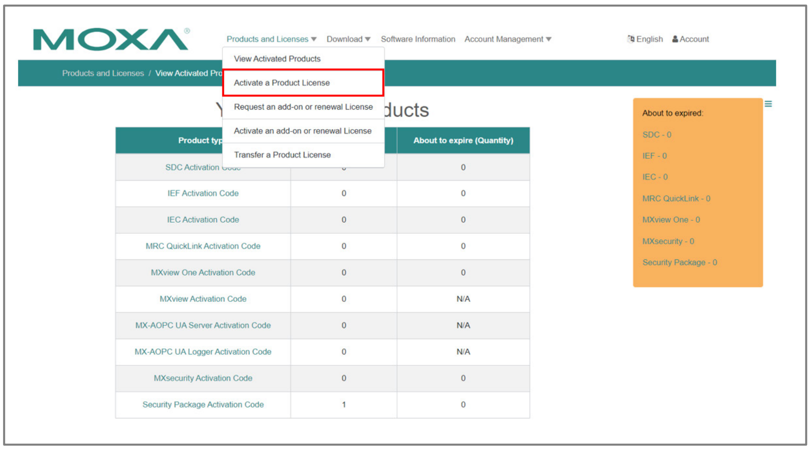


Manage Your Software License

Login Moxa Software Licensing System to activate or query your Moxa software license.

☐ I have read and agree with Moxa's Privacy Policy.

3. Click on the **Products and Licenses** category at the top of the page to expand it, and then select **Activate a Product License**.



MOXA
Products and Licenses ▾
Download ▾
Software Information
Account Management ▾
English
Account
Products and Licenses / View Activated Pro
View Activated Products
Activate a Product License
Request an add-on or renewal License
Activate an add-on or renewal License
Transfer a Product License
Y
ducts

Product typ		About to expire (Quantity)
SDC Activation Code	0	0
IEF Activation Code	0	0
IEC Activation Code	0	0
MRC QuickLink Activation Code	0	0
MXview One Activation Code	0	0
MXview Activation Code	0	N/A
MX-AOPC UA Server Activation Code	0	N/A
MX-AOPC UA Logger Activation Code	0	N/A
MXsecurity Activation Code	0	0
Security Package Activation Code	1	0

About to expired:

SDC - 0

IEF - 0

IEC - 0

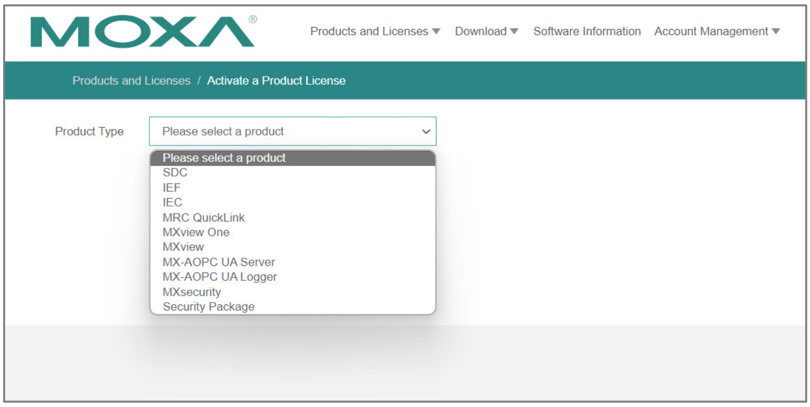
MRC QuickLink - 0

MXview One - 0

MXsecurity - 0

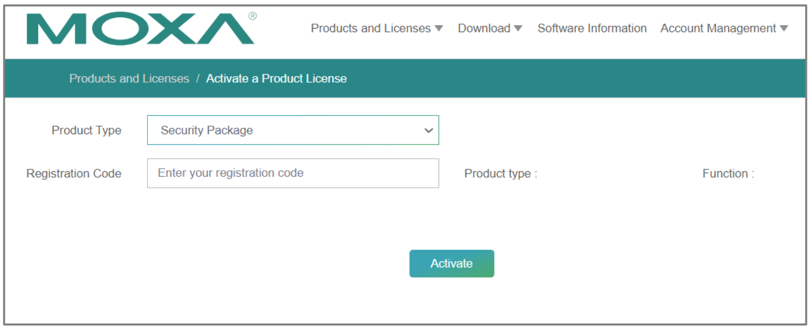
Security Package - 0

4. Choose the product type for which you want to add a license. In this example, we will be adding a **Security Package**.



Product Type: Please select a product

5. Enter the Registration Code and click **Activate**.



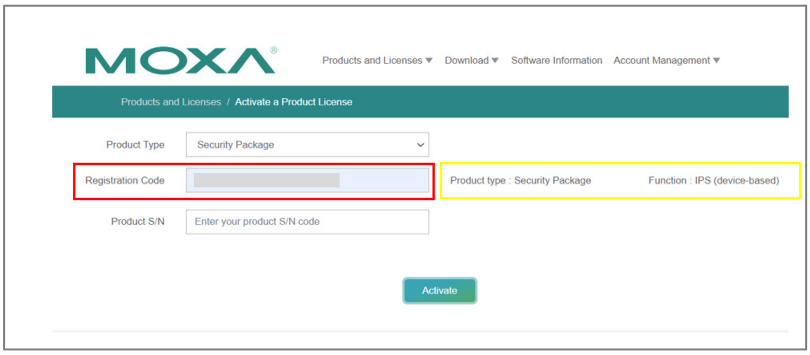
Product Type: Security Package

Registration Code: Enter your registration code

Product type :

Function :

6. Once you click **Activate**, the **Product S/N** (Serial Number) will be displayed, and additional information will appear on the right side of the page.



Product Type: Security Package

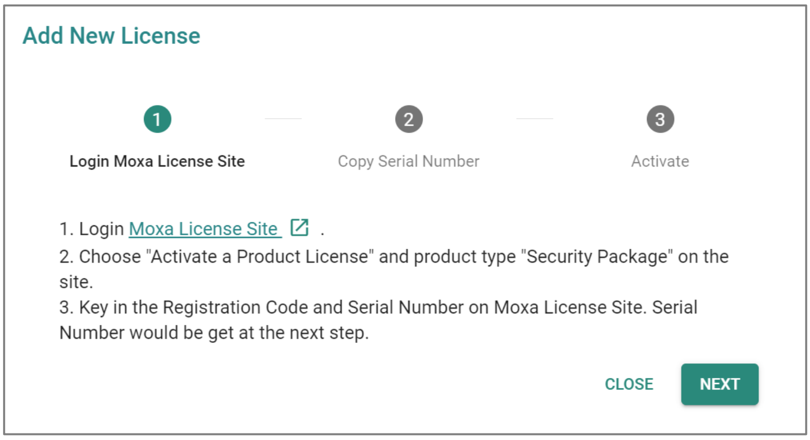
Registration Code: [redacted]

Product type : Security Package

Function : IPS (device-based)

Product S/N: Enter your product S/N code

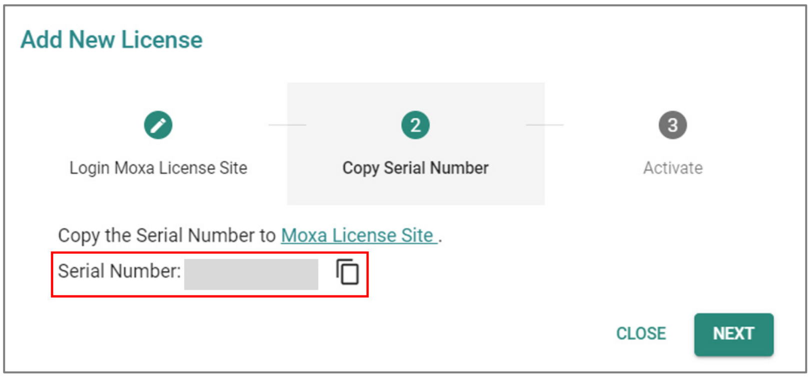
7. Back in the Add New License window for your Moxa device, click **NEXT**.



Add New License

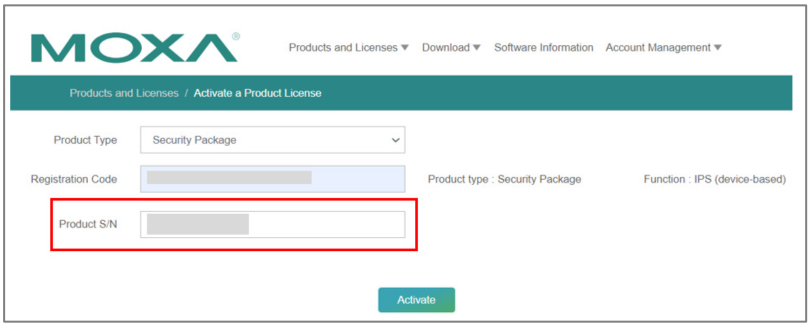
1. Login Moxa License Site .
2. Choose "Activate a Product License" and product type "Security Package" on the site.
3. Key in the Registration Code and Serial Number on Moxa License Site. Serial Number would be get at the next step.

8. Copy the serial number from the Moxa device UI window and paste it in the **Product S/N** field in the Software Licensing window, then click **ACTIVATE**.



Copy the Serial Number to Moxa License Site .

Serial Number:



Product Type: Security Package

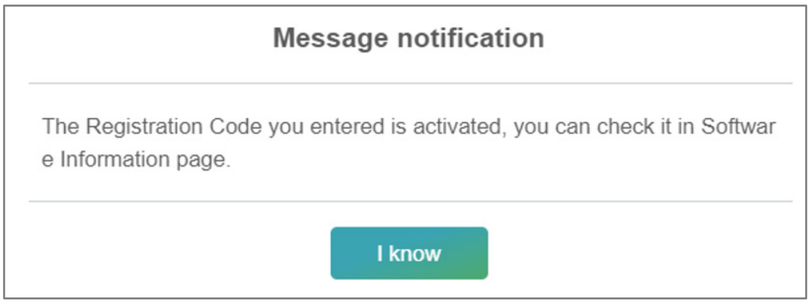
Registration Code

Product type : Security Package

Function : IPS (device-based)

Product S/N

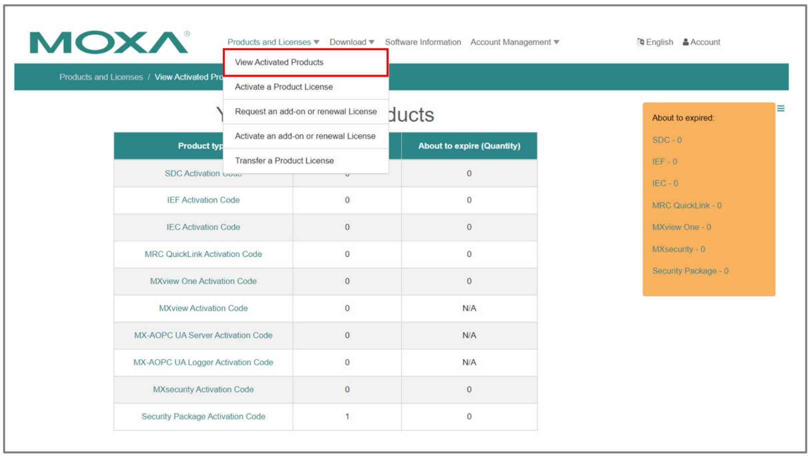
9. A message notification page will appear to confirm that your registration code was successfully activated.



Message notification

The Registration Code you entered is activated, you can check it in Software Information page.

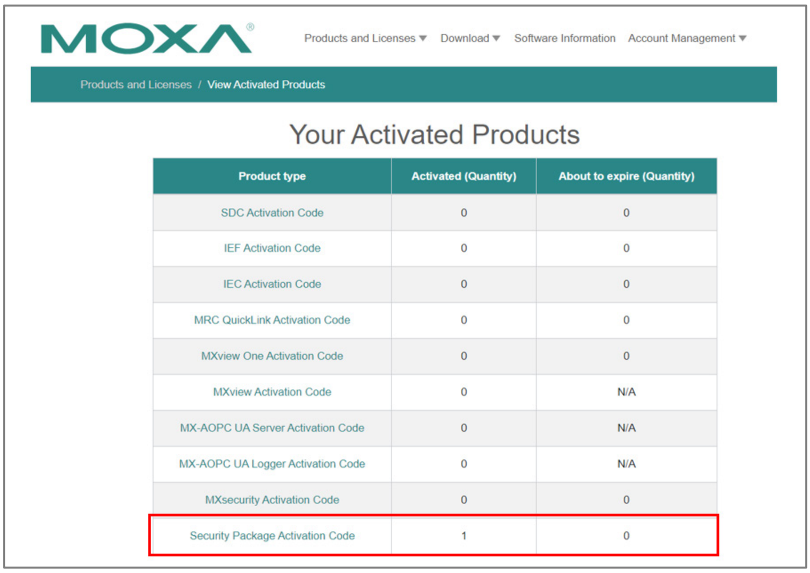
10. In the Software Licensing window, click on **Products and Licenses** to expand it, then select **View Activated Products**.



Y ducts

Product typ		About to expire (Quantity)
SDC Activation Code	0	0
IEF Activation Code	0	0
IEC Activation Code	0	0
MRC QuickLink Activation Code	0	0
MXview One Activation Code	0	0
MXview Activation Code	0	N/A
MX-AOPC UA Server Activation Code	0	N/A
MX-AOPC UA Logger Activation Code	0	N/A
MXsecurity Activation Code	0	0
Security Package Activation Code	1	0

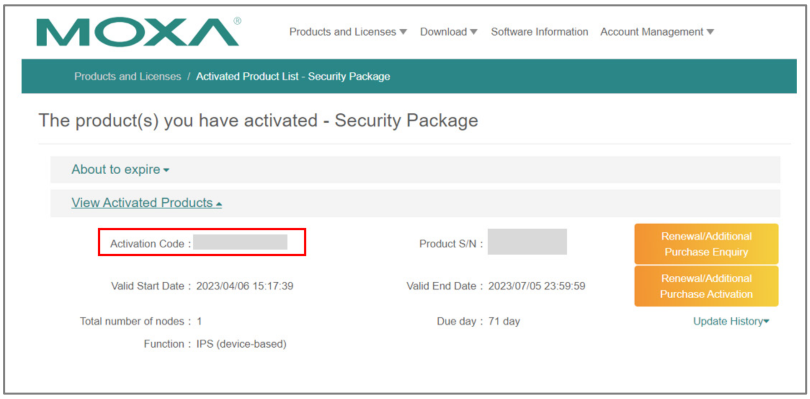
11. Click on the name of the product you just activated. For this example, we need to click on **Security Package Activation Code**.



Your Activated Products

Product type	Activated (Quantity)	About to expire (Quantity)
SDC Activation Code	0	0
IEF Activation Code	0	0
IEC Activation Code	0	0
MRC QuickLink Activation Code	0	0
MXview One Activation Code	0	0
MXview Activation Code	0	N/A
MX-AOPC UA Server Activation Code	0	N/A
MX-AOPC UA Logger Activation Code	0	N/A
MXsecurity Activation Code	0	0
Security Package Activation Code	1	0

12. Click on **View Activated Products** and then click on the **Activation Code**.


MOXA
Products and Licenses ▾ Download ▾ Software Information Account Management ▾
Products and Licenses / Activated Product List - Security Package

The product(s) you have activated - Security Package

About to expire ▾

View Activated Products ▴

Activation Code : [redacted]

Product S/N : [redacted]

Renewal/Additional Purchase Enquiry
Renewal/Additional Purchase Activation

Valid Start Date : 2023/04/06 15:17:39

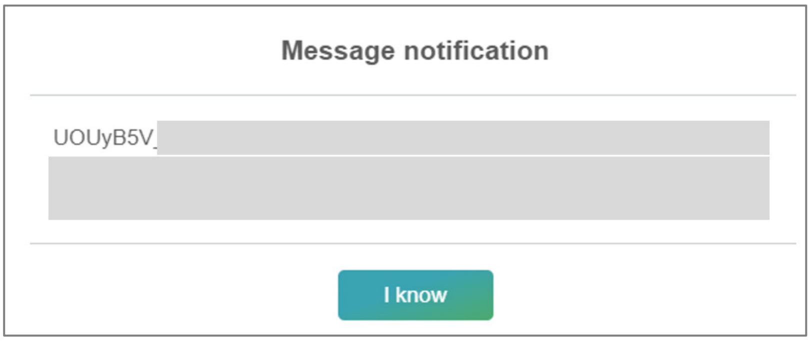
Valid End Date : 2023/07/05 23:59:59

Total number of nodes : 1

Due day : 71 day

Function : IPS (device-based)

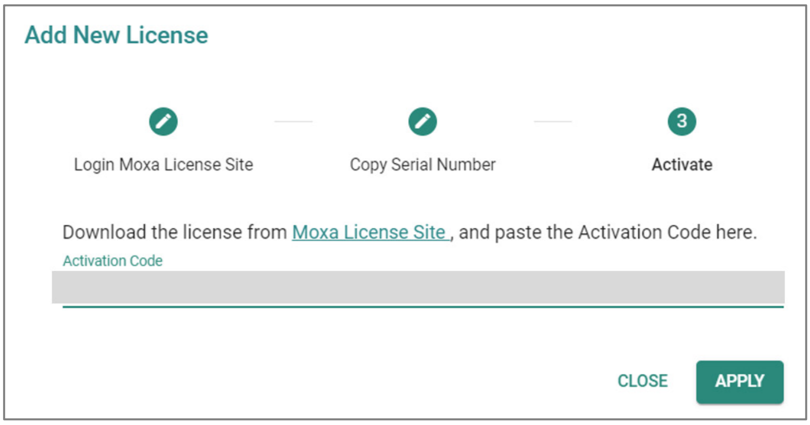
13. Copy the activation code that appears in the pop-up notification.



Message notification

UOUyB5V[redacted]

14. In the device UI window, click **NEXT** and paste in your activation code, then click **APPLY**.



Add New License

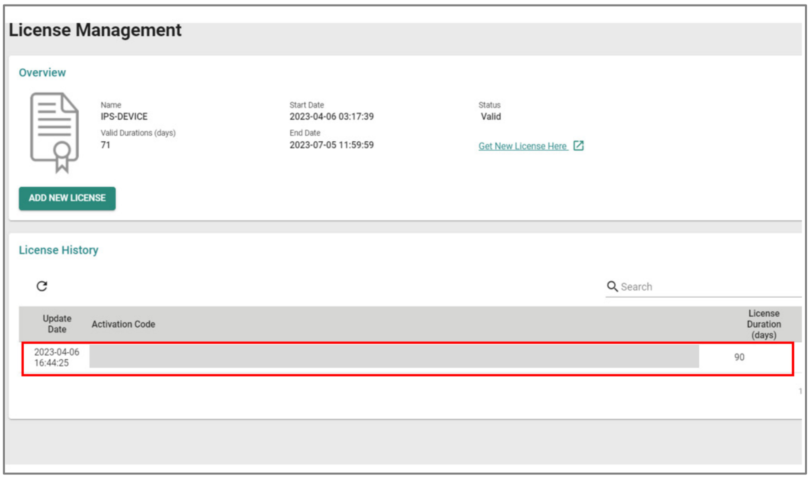
Download the license from Moxa License Site , and paste the Activation Code here.

Activation Code

[redacted]

End Result

You will now see the new license in the **License History** section.



License Management

Overview

Name: IPS-DEVICE
Valid Durations (days): 71
Start Date: 2023-04-06 03:17:39
End Date: 2023-07-05 11:59:59
Status: Valid

License History

Update Date	Activation Code	License Duration (days)
2023-04-06 16:44:25		90

Management Interface

Menu Path: System > Management Interface

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

This section includes these pages:

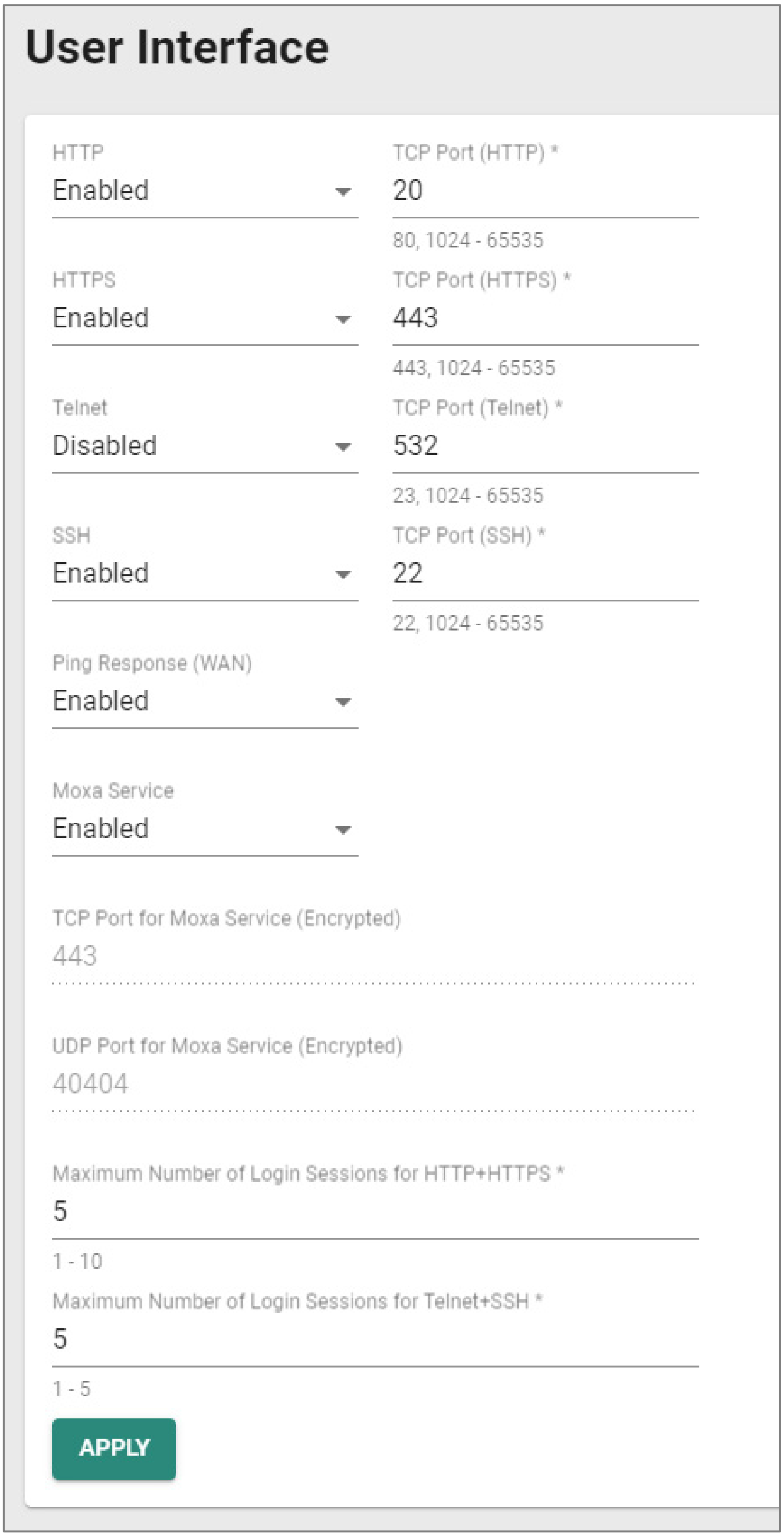
- User Interface
- Hardware Interface
- SNMP
- MXsecurity

User Interface

Menu Path: System > Management Interface > User Interface

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

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



User Interface

HTTP: Enabled

TCP Port (HTTP) *: 20

80, 1024 - 65535

HTTPS: Enabled

TCP Port (HTTPS) *: 443

443, 1024 - 65535

Telnet: Disabled

TCP Port (Telnet) *: 532

23, 1024 - 65535

SSH: Enabled

TCP Port (SSH) *: 22

22, 1024 - 65535

Ping Response (WAN): Enabled

Moxa Service: Enabled

TCP Port for Moxa Service (Encrypted): 443

UDP Port for Moxa Service (Encrypted): 40404

Maximum Number of Login Sessions for HTTP+HTTPS *: 5

1 - 10

Maximum Number of Login Sessions for Telnet+SSH *: 5

1 - 5

UI Setting	Description	Valid Range	Default Value
HTTP	Enable or disable HTTP connections.	Enabled / Disabled	Enabled
TCP Port (HTTP)	Set the TCP port number for HTTP.	80, 1024 to 65535	80
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 the browser verifies the signature and accesses the device, it will return the 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
TCP Port (HTTPS)	Set the TCP port number for HTTPS.	443, 1024 to 65535	443
Telnet	Enable or disable HTTPS connections.	Enabled / Disabled	Enabled
TCP Port (Telnet)	Set the TCP port number for Telnet.	23, 1024 to 65535	23
SSH	Enable or disable HTTPS connections.	Enabled / Disabled	Enabled
TCP Port (SSH)	Set the TCP port number for SSH.	22, 1024 to 65535	22

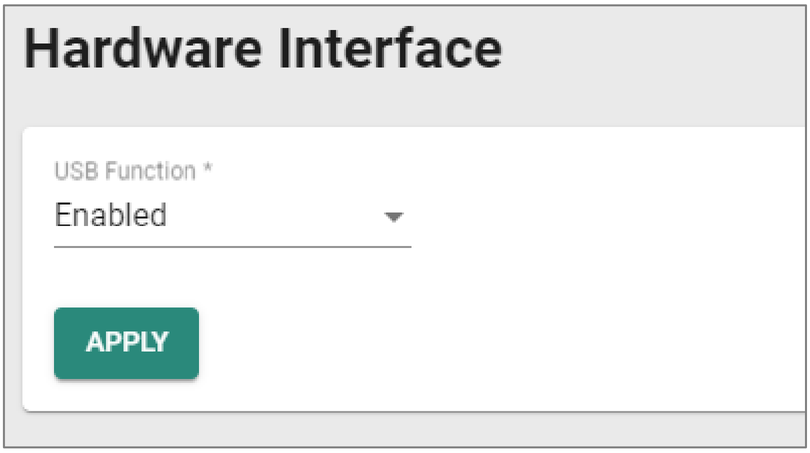
UI Setting	Description	Valid Range	Default Value
Ping Response (WAN)	Enable or disable to have the WAN port respond to ping requests. **Note** To ping the WAN port, make sure the **Ping Response (WAN)** function is enabled, and that the ping sender IP is in the Trusted Access list or the **Accept All LAN Port Connections** option is enabled in **Trusted Access**.	Enabled / Disabled	Disabled
MOXA Service	Enable or disable the MOXA Service. **Note** Moxa Service is only used for Moxa network management software. Moxa Service is only available for user accounts with admin privileges.	Enabled / Disabled	Enabled
TCP Port for Moxa Service (Encrypted)	The TCP port number for Moxa Service. This setting cannot be changed.	443	443
UDP Port for Moxa Service (Encrypted)	The UDP port number for Moxa Service. This setting cannot be changed.	40404	40404
Maximum Number of Login Sessions for HTTP+HTTTPS	Set the maximum combined number of users that can be logged in to the Moxa Router using HTTP and HTTPS.	1 to 10	5
Maximum Number of Login Sessions for Telnet+SSH	Set the maximum combined number of users that can be logged in to the Moxa Router using Telnet and SSH.	1 to 5	5

Hardware Interface

Menu Path: System > Management Interface > Hardware Interface

This page allows you to enable or disable the USB interface on the device for use with a USB drive.

To ensure compatibility, we recommend using an ABC-02 Series backup configurator tool.


Hardware Interface

USB Function *

Enabled

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

SNMP

Menu Path: System > Management Interface > SNMP

This section lets you configure SNMP settings for your device.

There are two tabs in this section:

- General
- SNMP Account

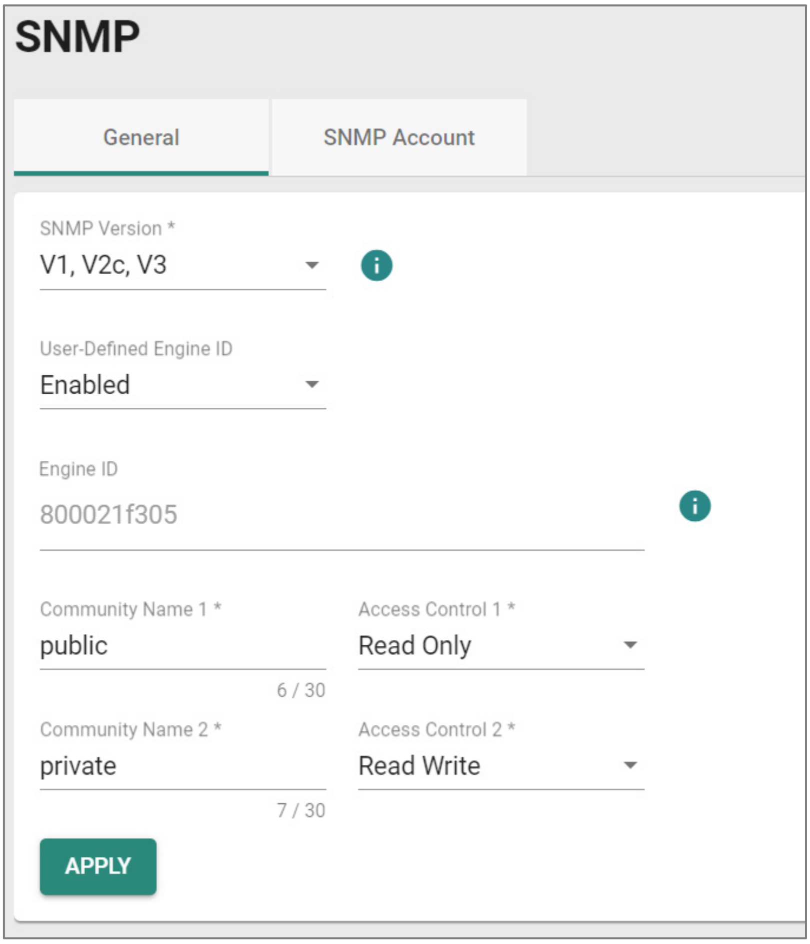
SNMP - General

Menu Path: System > Management Interface > SNMP - General

This page lets you enable or disable SNMP. SNMP versions V1, V2c, and V3 are supported.

Limitations

You can set up to two community names with corresponding access controls.



SNMP Version *: V1, V2c, V3

User-Defined Engine ID: Enabled

Engine ID: 800021f305

Community Name 1 *: public (6 / 30)

Access Control 1 *: Read Only

Community Name 2 *: private (7 / 30)

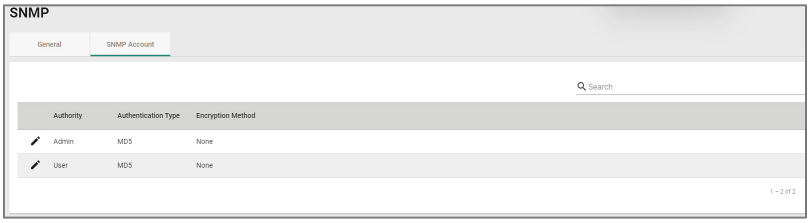
Access Control 2 *: Read Write

UI Setting	Description	Valid Range	Default Value
SNMP Version	Set the SNMP protocol version used to manage your device. **Disabled**: Disable SNMP. **V1, V2c, V3**: Enable SNMP V1, V2c, and V3. **V1, V2c**: Enable SNMP V1, V2c only. **V3 only**: Enable SNMP V3 only.	Disabled / V1, V2c, V3 / V1, V2c / V3 only	Disabled
User-Defined Engine ID **(Only for SNMP Verison is V1, V2c, V3 or V3 only)**	Enable or disable user-defined engine ID. If disabled, the system will use the default engine ID.	Disabled / Enabled	Disabled
Engine ID	Set an engine ID to manage your Moxa Router. If the user-defined engine ID is set to 'disabled', the engine ID will be view-only.	2 to 54 hexadecimal string. The String length must to be even.	800021f305
Community Name 1	Set a community string name match to use for authentication.	1 to 30 characters	public
Community Name 2	Set a community string name match to use for authentication.	1 to 30 characters	private
Access Control 1	Set the access control type to use when Community String 1 is matched.	Read Write / Read only / No Access	Read Only
Access Control 2	Set the access control type to use when Community String 2 is matched.	Read Write / Read only / No Access	Read Write

SNMP - 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

	Authority	Authentication Type	Encryption Method
✎	Admin	MD5	None
✎	User	MD5	None

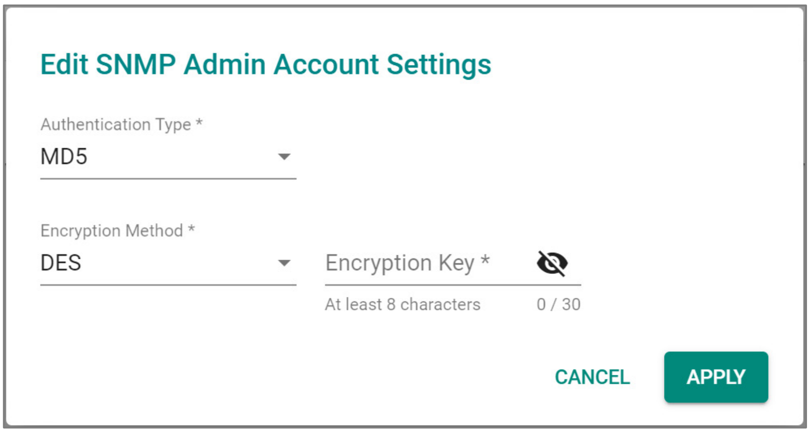
1 – 2 of 2

UI Setting	Description
Authority	Shows authority level of the management account. **admin**: Can read/write configuration settings. **user**: Can only read configuration settings.
Authentication Type	Shows the authentication type used for the account.
Encryption Method	Shows the encryption method used for the account.

Edit SNMP Account Settings

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 modify the selected account. Click **APPLY** to save your changes.



Edit SNMP Admin Account Settings

Authentication Type *: MD5

Encryption Method *: DES

Encryption Key *

At least 8 characters 0 / 30

UI Setting	Description	Valid Range	Default Value
Authentication Type	Select which authentication method to use for the account. **None**: No authentication will be used. **MD5**: Use MD5 authentication. **SHA**: Use SHA authentication.	None / MD5 / SHA	None
Encryption Method	Select which encryption method to use for the account.	None / DES / AES	None
Encryption Key **(if Encryption Method is DES or AES)**	Specify an encryption password for the account.	8 to 30 characters	N/A

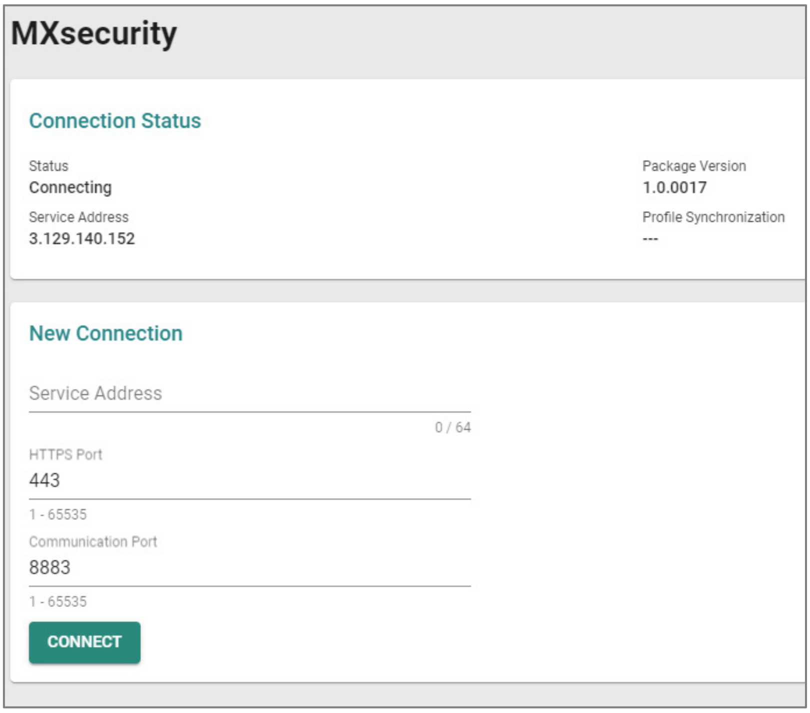
MXsecurity

Menu Path: System > Management Interface > MXsecurity

This page lets you establish a connection to an MXsecurity instance to monitor and manage the device.

After configuring the connection parameters, click **CONNECT** to establish the connection.

To manage your the device through MXsecurity, the MXsecurity Agent Package must be installed and enabled first. Refer to the Software Package Management section for more information and instructions.



MXsecurity

Connection Status

Status
Connecting

Service Address
3.129.140.152

Package Version
1.0.0017

Profile Synchronization

New Connection

Service Address
0 / 64

HTTPS Port
443
1 - 65535

Communication Port
8883
1 - 65535

UI Setting	Description	Valid Range	Default Value
Service Address	Set the MXsecurity server IP address or domain name.	Valid IP address or domain name	N/A
HTTPS Port	Specify the HTTPS port number for MXsecurity.	1 to 65535	443
Communication Port	Specify the communication port number for MXsecurity.	1 to 65535	8833

Time

Menu Path: System > Time

This section lets you configure the system time settings for your device.

This section includes these pages:

- System Time
- NTP/SNTP Server

System Time

Menu Path: System > Time > System Time

This section lets you set up time settings for the device itself.

This page includes these tabs:

- Time
- Time Zone
- NTP Authentication

This device does not include a real-time clock. If there is no NTP/SNTP server on the network or if the device is not connected to the Internet, the Current Time and Current Date must be manually reconfigured after each reboot.

System Time - Time

Menu Path: System > System Time - Time

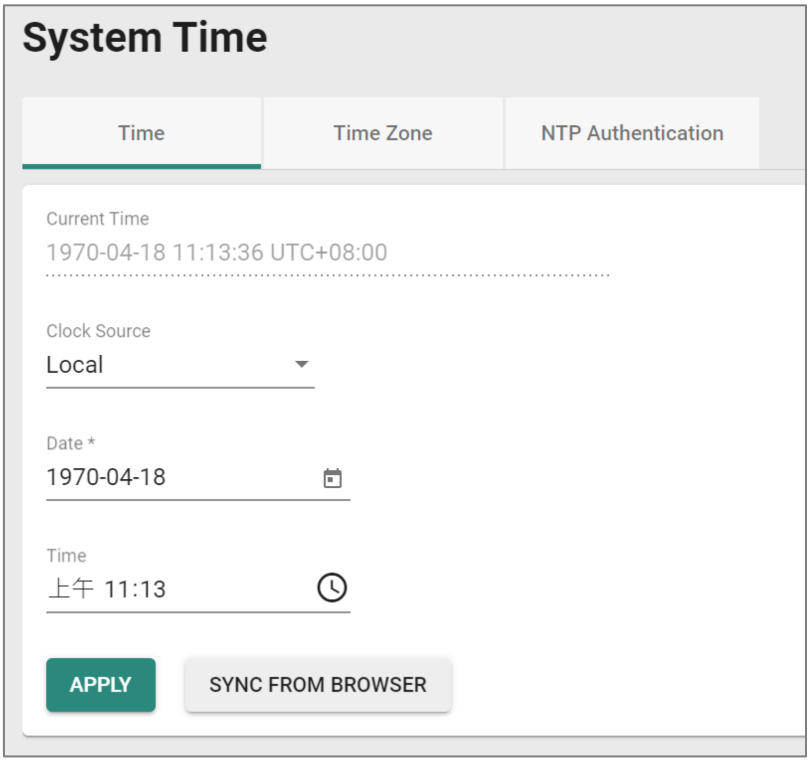
This page lets you set the system time and date.

You can set your system time using these clock sources:

- Local
- SNTP Time
- NTP Time

Local Time

If you select **Local** as your **Clock Source**, these settings will appear. Local lets you set your device's system time manually, or you can copy the time from your local host by clicking **SYNC FROM BROWSER**. Click **APPLY** to save your changes.



Current Time
1970-04-18 11:13:36 UTC+08:00

Clock Source
Local

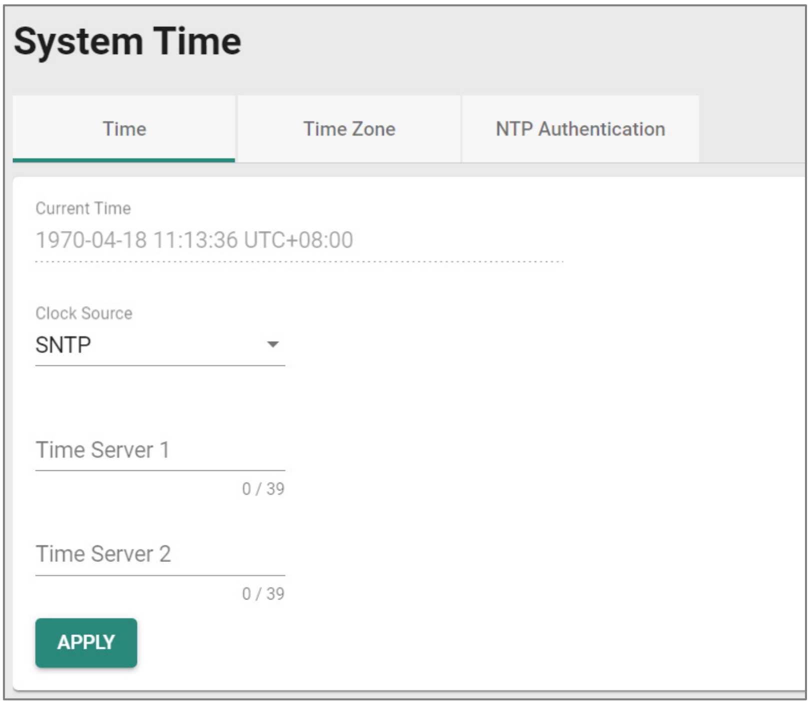
Date *
1970-04-18

Time
上午 11:13

UI Setting	Description	Valid Range	Default Value
Current Time	This shows the device's current system date, time, and time zone.	N/A	N/A
Date	Specify the date manually in YYYY-MM-DD format.	YYYY-MM-DD	Current date
Time	Specify the time manually in HH:MM AM/PM format.	HH:MM AM/PM	Current time

SNTP Time

If you select **SNTP** as your **Clock Source**, these settings will appear. SNTP allows your device to update its system time from a Simplified Network Time Protocol (SNTP) time server. Click **APPLY** to save your changes.



System Time

Current Time
1970-04-18 11:13:36 UTC+08:00

Clock Source
SNTP

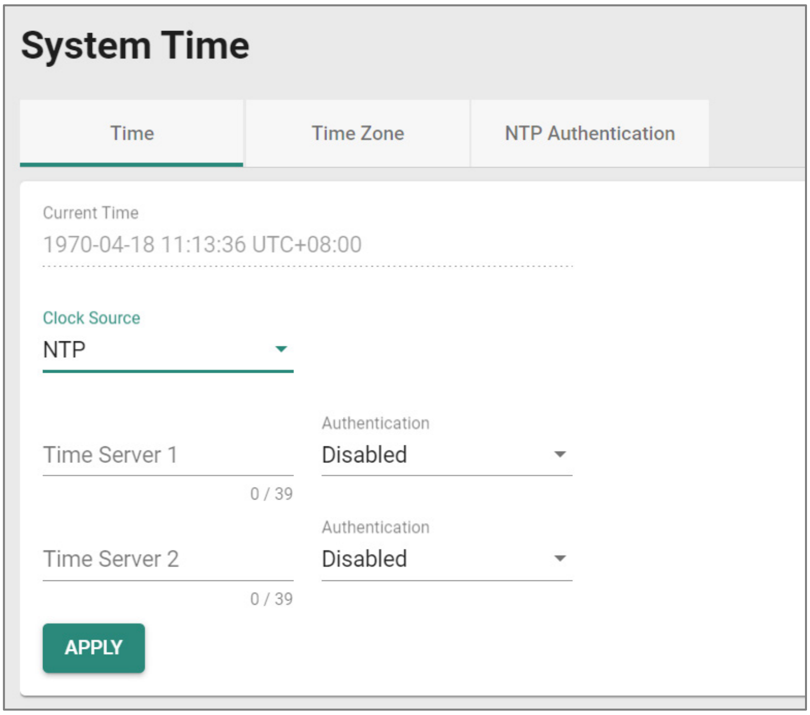
Time Server 1
0 / 39

Time Server 2
0 / 39

UI Setting	Description	Valid Range	Default Value
Current Time	This shows the device's current system date, time, and time zone.	N/A	N/A
Time Server 1	Set the IP or domain address of the primary time server (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	IP address or domain, 1 to 39 characters	N/A
Time Server 2	Set the IP or domain address of the secondary time server. This will be used by the device if it cannot connect to the primary time server.	IP address or domain, 1 to 39 characters	N/A

NTP Time

If you select **NTP** as your **Clock Source**, these settings will appear. NTP allows your device to update its system time from a Network Time Protocol (NTP) server. Click **APPLY** to save your changes.



System Time

Current Time
1970-04-18 11:13:36 UTC+08:00

Clock Source
NTP

Time Server 1
0 / 39

Authentication
Disabled

Time Server 2
0 / 39

Authentication
Disabled

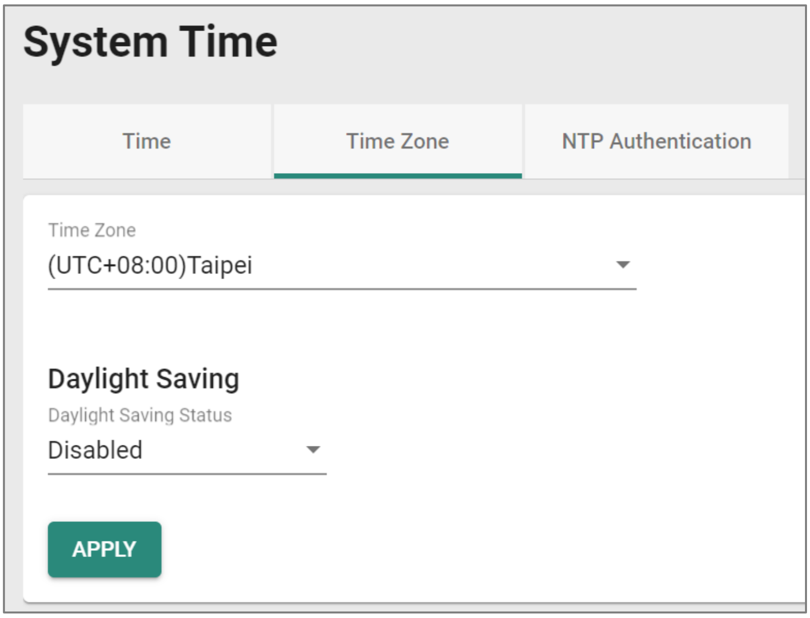
UI Setting	Description	Valid Range	Default Value
Current Time	This shows the device's current system date, time, and time zone.	N/A	N/A
Time Server 1	Set the IP or domain address of the primary time server (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	IP address or domain, 1 to 39 characters	N/A
Time Server 2	Set the IP or domain address of the secondary time server. This will be used by the device if it cannot connect to the primary time server.	IP address or domain, 1 to 39 characters	N/A
Authentication	Specify whether to disable or use a key ID for NTP server authentication. To use authentication, set up the Key ID value in the **NTP Authentication** tab first. After setting it up, it will become available in the **Authentication** drop-down.	Disabled / Key IDs created in the **NTP Authentication** tab	Disabled

System Time - Time Zone

Menu Path: System > System Time - Time Zone

This page lets you set the time zone settings of your device. Click **APPLY** to save your changes.

Changing the time zone will automatically adjust the device's system time. Be sure to set the time zone before setting the system time.



Time Zone: (UTC+08:00)Taipei

Daylight Saving

Daylight Saving Status: Disabled

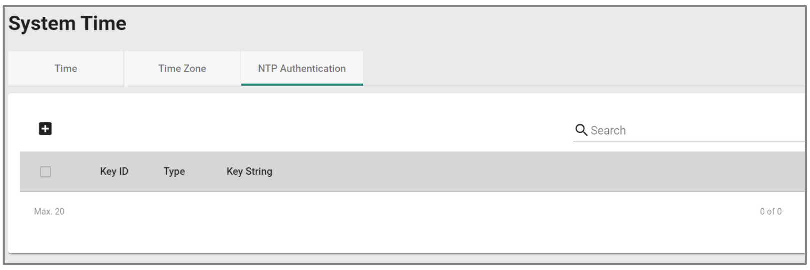
UI Setting	Description	Valid Range	Default Value
Time Zone	Select a time zone from the list of UTC (Coordinated Universal Time) time zones.	N/A	N/A
Daylight Saving Status	Enable or disable Daylight Saving time adjustment.	Enabled / Disabled	Disabled
Offset (if Daylight Saving Status is Enabled)	Set the offset (in hours) to add to the time when Daylight Saving time is active.	0 to 12	0
Month (if Daylight Saving Status is Enabled)	Set the month Daylight Saving time begins/ends.	User-specified month	N/A

UI Setting	Description	Valid Range	Default Value
Week (if Daylight Saving Status is Enabled)	Set the week Daylight Saving time begins/ends.	User-specified week	N/A
Day (if Daylight Saving Status is Enabled)	Set the day of the week Daylight Saving time begins/ends.	User-specified day	N/A
Hour (if Daylight Saving Status is Enabled)	Set the hour Daylight Saving time begins/ends.	User-specified hour	00
Minutes (if Daylight Saving Status is Enabled)	Set the minute Daylight Saving time begins/ends.	User-specified minute(s)	00

System Time - NTP Authentication

Menu Path: System > System Time - NTP Authentication

This section describes how to configure NTP Authentication. After creating a key, it will be available for use in the **Time** tab. Click **APPLY** to save your changes.

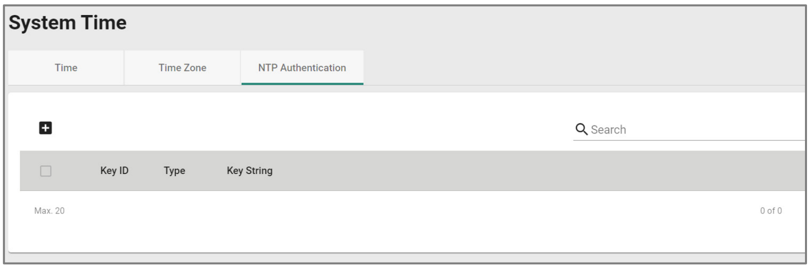


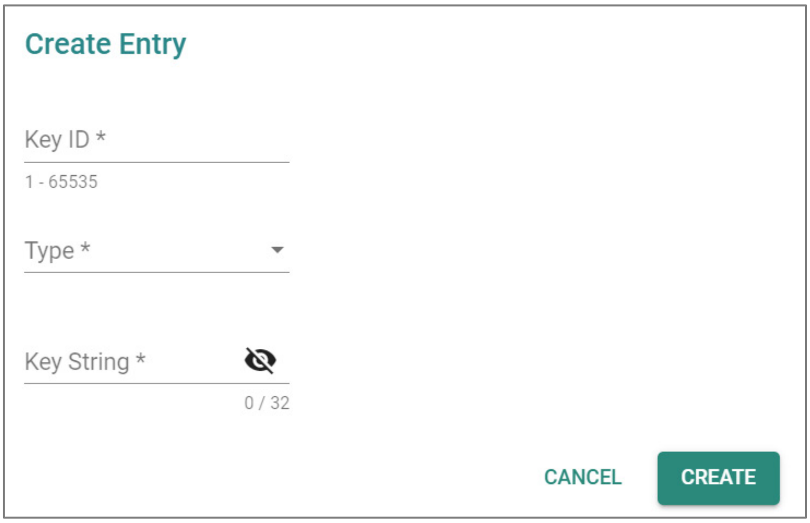
UI Setting	Description
Key ID	Shows the key ID for the authentication key.
Type	Shows the type of NTP authentication the key uses. **MD5**: Uses authentication based on MD5 algorithms. **SHA**: Uses authentication based on SHA-512 algorithms.
Key String	Shows the key string used by the authentication key.

Create Entry

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

Clicking the **Add (** ⊞ **)** icon on the **System > System Time - NTP Authentication** page will open this dialog box. This dialog lets you create a new NTP authentication key. Click **CREATE** to save your settings and create the new authentication key.





UI Setting	Description	Valid Range	Default Value
Key ID	Specify the key ID to use for the authentication key.	1 to 65535 characters	N/A

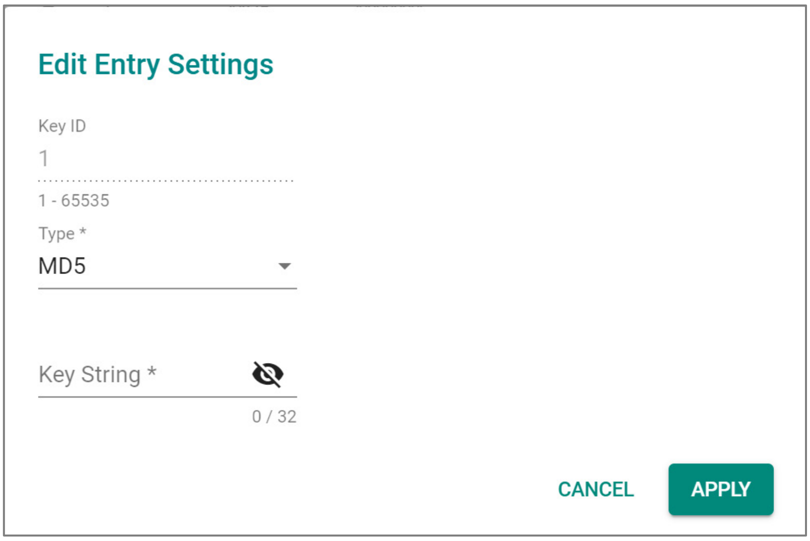
UI Setting	Description	Valid Range	Default Value
Type	Specify the type of NTP authentication the key should use. **MD5**: Sets authentication based on MD5 algorithms. **SHA**: Sets authentication based on SHA-512 algorithms.	MD5 / SHA-512	N/A
Key String	Specify the key string to use for the authentication key.	1 to 32 characters	N/A

Edit Entry

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

Clicking the **Edit (✎)** icon for a key on the **System > System Time - NTP Authentication** page will open this dialog box. This dialog lets you edit an existing authentication key. Click **APPLY** to save your settings.

All key parameters can be modified, except for the key ID. To modify the key ID, you must create a new authentication key.



Edit Entry Settings

Key ID: 1 (1 - 65535)

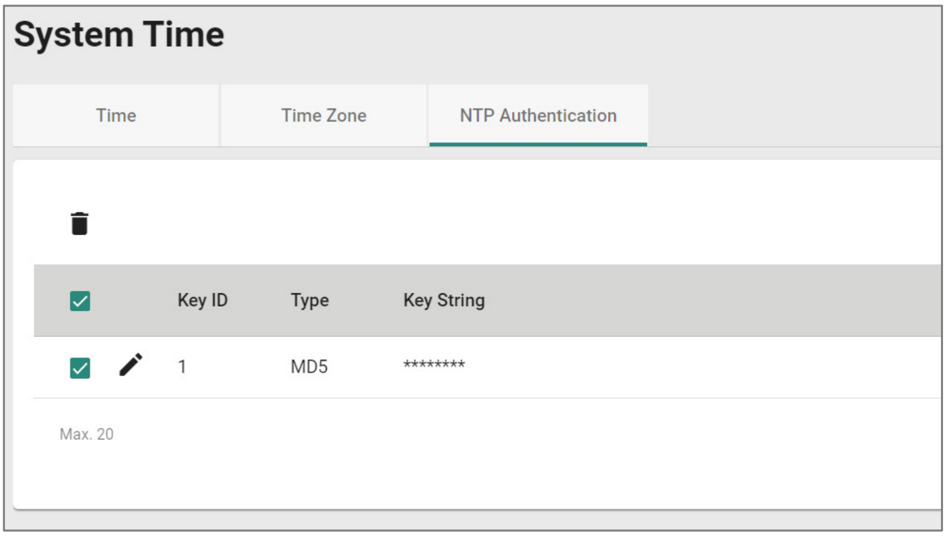
Type *: MD5

Key String *: (0 / 32)

UI Setting	Description	Valid Range	Default Value
Key ID	Shows the key ID for this authentication key. The key ID cannot be changed.	N/A	Current key ID
Type	Specify the type of NTP authentication the key should use. **MD5**: Sets authentication based on MD5 algorithms. **SHA**: Sets authentication based on SHA-512 algorithms.	MD5 / SHA	N/A
Key String	Specify the key string to use for the authentication key.	1 to 32 characters	N/A

Delete Entry

You can delete authentication keys by using the checkboxes to select the keys you want to delete, then clicking the **Delete (🗑)** icon.



System Time

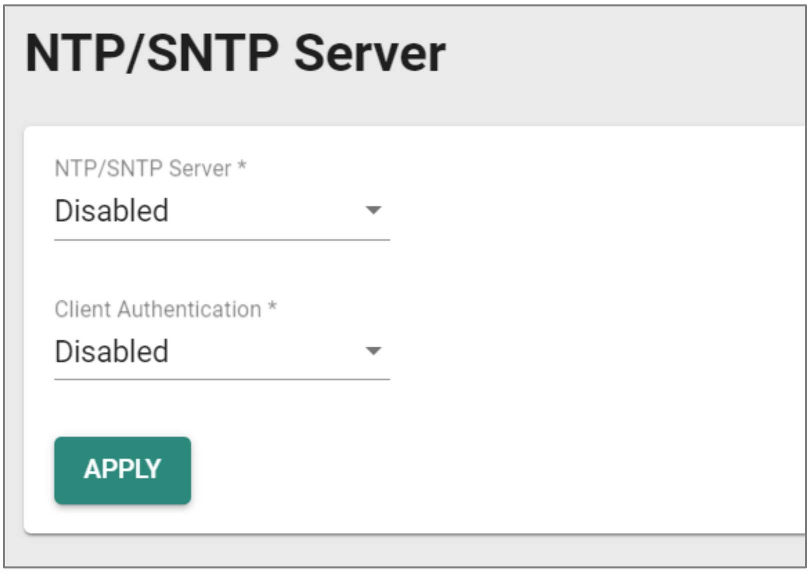
☑		Key ID	Type	Key String
☑	✎	1	MD5	********

Max. 20

NTP/SNTP Server

Menu Path: System > Time > NTP/SNTP Server

NTP/SNTP server allows you to set up: **NTP/SNTP Server, Client Authentication**. While finished, Click **APPLY** to save the settings.



NTP/SNTP Server

NTP/SNTP Server *
Disabled

Client Authentication *
Disabled

UI Setting	Description	Valid Range	Default Value
NTP/SNTP Server	Enable or disable NTP/SNTP server functionality for clients: **Enabled**: Enable NTP/SNTP server functionality for clients. **Disabled**: Disabled NTP/SNTP server functionality for clients.	**Enabled / Disabled**	**Disabled**
Client Authentication	Enable or disable client authentication of NTP/SNTP server: **Enabled**: Enable Client Authentication functionality for clients. **Note** Before enabling Client Authentication, you will need to create NTP authentication keys first. Refer to System > Time > System Time - NTP Authentication for more information. **Disabled**: Disable Client Authentication functionality for clients.	**Enabled / Disabled**	**Disabled**

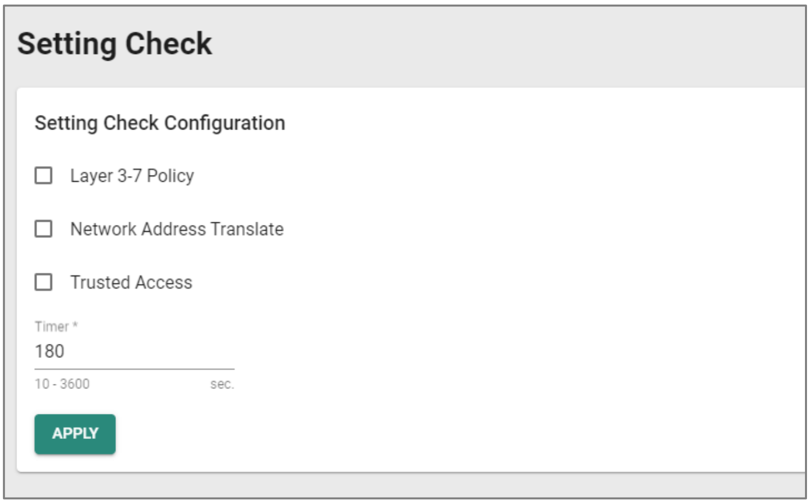
Setting Check

Menu Path: System > Setting Check

This page provides a double confirmation mechanism that allows you to verify configuration changes made by remote users before they are applied.

Setting Check is available for the following configuration settings:

- Layer 3 -7 Policy
- Network Address Translate
- Trusted Access



Setting Check

Setting Check Configuration

□ Layer 3-7 Policy

□ Network Address Translate

□ Trusted Access

Timer *
180
10 - 3600 sec.

UI Setting	Description	Valid Range	Default Value
Layer 3-7 Policy	Enable or disable Setting Check for Layer 3 - 7 policy changes.	Enabled / Disabled	Disabled
Network Address Translate	Enable or disable Setting Check for NAT policy changes.	Enabled / Disabled	Disabled
Trusted Access	Enable or disable Setting Check for Trusted IP address changes.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Timer	Set the time (in seconds) the user has to confirm the changes. **Note** If the user does not confirm the changes within the specified time period, the system will automatically undo the changes.	10 to 3600	180

Network Configuration

Menu Path: Network Configuration

The Network Configuration settings area lets you configure settings related to your device's networking ports.

This settings area includes these sections:

- Ports
- Layer 2 Switching
- Network Interfaces

Network Configuration - User Privileges

Privileges to Network Configuration 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			
Port Settings	R/W	R/W	R
Link Aggregation	R/W	R/W	R

Settings	Admin	Supervisor	User
Layer 2 Switching			
VLAN	R/W	R/W	R
MAC Address Table	R/W	R/W	R
QoS	R/W	R/W	R
Rate Limit	R/W	R/W	R
Multicast	R/W	R/W	R
Network Interface	R/W	R/W	R

Ports

Menu Path: Network Configuration > Ports

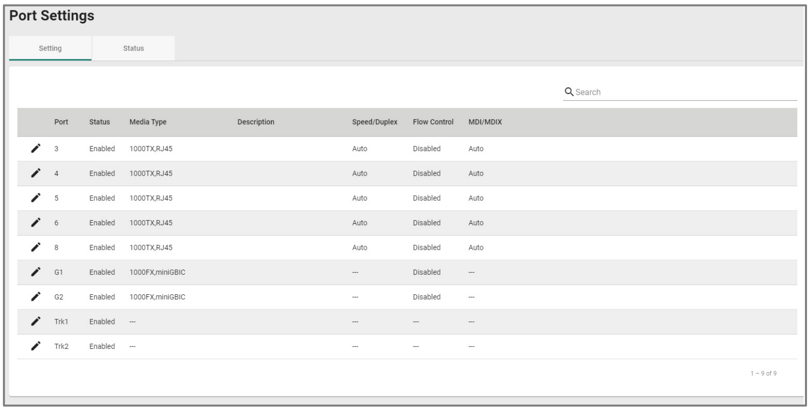
This section includes these pages:

- Port Settings
- Link Aggregation

Port Settings - Settings

Menu Path: Network Configuration > Ports > Port Settings - Settings

This tab lets you view and adjust the settings for each port.



	Port	Status	Media Type	Description	Speed/Duplex	Flow Control	MDI/MDIX
✎	3	Enabled	1000TX,RJ45		Auto	Disabled	Auto
✎	4	Enabled	1000TX,RJ45		Auto	Disabled	Auto
✎	5	Enabled	1000TX,RJ45		Auto	Disabled	Auto
✎	6	Enabled	1000TX,RJ45		Auto	Disabled	Auto
✎	8	Enabled	1000TX,RJ45		Auto	Disabled	Auto
✎	G1	Enabled	1000FX,miniGBIC		---	Disabled	---
✎	G2	Enabled	1000FX,miniGBIC		---	Disabled	---
✎	Trk1	Enabled	---		---	---	---
✎	Trk2	Enabled	---		---	---	---

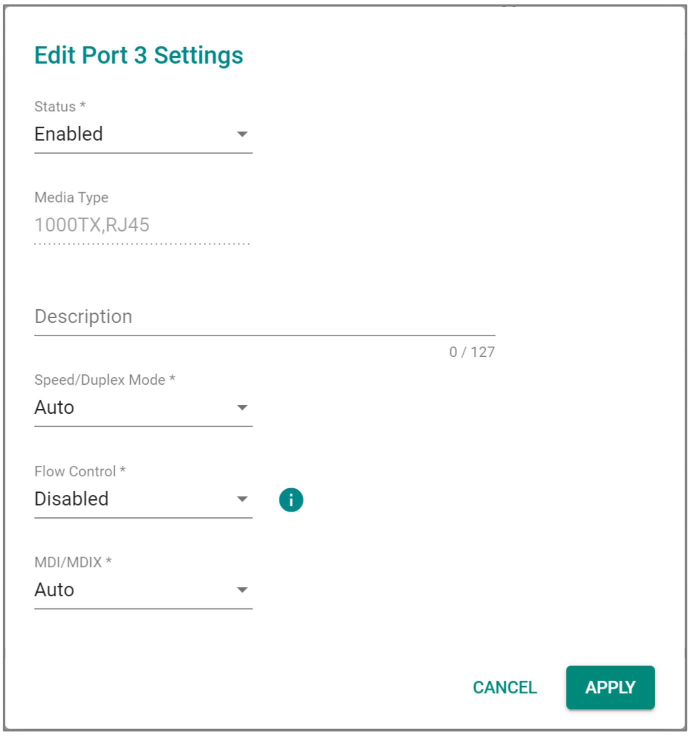
1 – 9 of 9

UI Setting	Description
Port	Shows which port this row describes.
Status	Shows the status of the port.
Media Type	Shows the port’s media type.
Description	Shows the description for the port.
Speed / Duplex	Shows the speed and duplex mode for the port.
Flow Control	Shows the whether flow control is enabled or disabled for the port.
MDI / MDIX	Shows the MDI/MDIX setting for the port.

Edit Port Settings

Menu Path: Network Configuration > Ports > Port Settings - Settings - Edit Port Settings

Clicking the **Edit (✎)** icon for a port on the **Network Configuration > Ports > Port Settings - Settings** page will open this dialog box. This dialog lets you change the settings for a port. Click **APPLY** to save your changes.



Edit Port 3 Settings

Status *
Enabled

Media Type
1000TX,RJ45

Description
0 / 127

Speed/Duplex Mode *
Auto

Flow Control *
Disabled

MDI/MDIX *
Auto

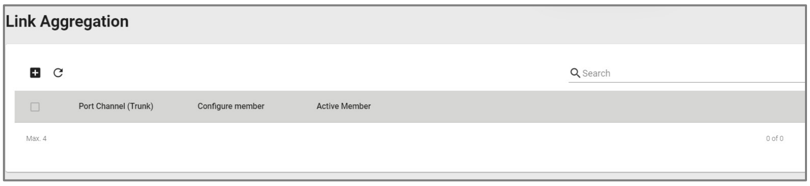
UI Setting	Description	Valid Range	Default Value
Status	Enable or Disable the port.	Enabled / Disabled	Enabled
Media Type	Displays the port's media type. This setting cannot be changed.	N/A	Port's media type
Description	Enter a description for the port to make it easier to identify.	1 to 127 characters	N/A
Speed / Duplex	Select the speed and duplex mode for the port. **Auto**: Allows the port to use IEEE 802.3u protocol to negotiate the best port speed and duplex mode to use for the connected device. **100M-Full**: This will force the port to connect using 100 Mbps at full-duplex. **100M-Half**: This will force the port to connect using 100 Mbps at half-duplex. **10M-Full**: This will force the port to connect using 10 Mbps at full-duplex. **10M-Half**: This will force the port to connect using 10 Mbps at half-duplex.	Auto / 100M-Full /100M-Half /10M-Full / 10M-Half	Auto

UI Setting	Description	Valid Range	Default Value
Flow Control	Enable or disable flow control for this port when the port's **Speed/Duplex** setting is set to **Auto**. Flow control helps manage the data transfer rate between the device and the connected Ethernet devices. **Note** If **Speed/Duplex** is set to something other than **Auto**, **Flow Control** will be disabled.	Enabled / Disabled	Disabled
MDI / MDIX	Select whether the port should use MDI or MDIX. The correct setting depends on both the connected device and the cabling used to connect to the device. **Auto**: Allow the port to auto-detect whether to use MDI or MDIX for connected devices. **MDI**: Force the port to use MDI (also known as "straight-through"). **MDIX**: Force the port to use MDIX (also known as "crossover"). **Note** Only choose MDI or MDIX if your connected Ethernet device has trouble auto-negotiating the correct port type.	Auto / MDI / MDIX	Auto

Link Aggregation Settings

Menu Path: Network Configuration > Ports > Link Aggregation

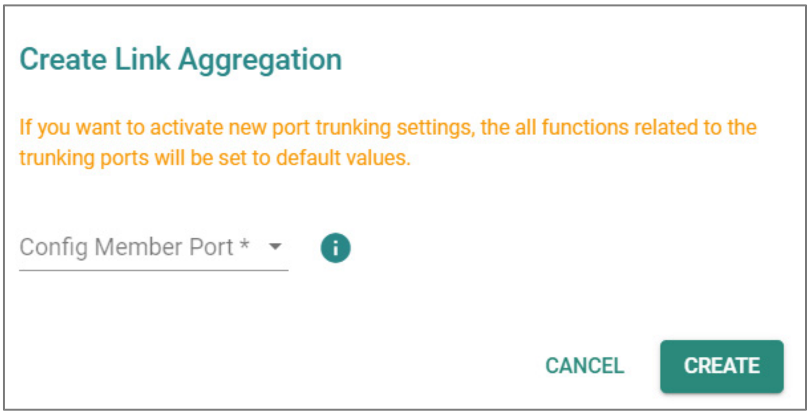
This page lets you configure link aggregation for your device. Link aggregation (or port trunking) is the process of combining multiple physical network links into a single logical link to increase bandwidth, improve redundancy and availability, and provide load balancing across links.



Create Link Aggregation

Menu Path: Network Configuration > Ports > Link Aggregation - Create Link Aggregation

Clicking the **Add (** ⊞ **)** icon on the **Network Configuration > Ports > Link Aggregation** page will open this dialog box. This dialog lets you create a new link aggregation with member ports.



If you want to activate new port trunking settings, the all functions related to the trunking ports will be set to default values.

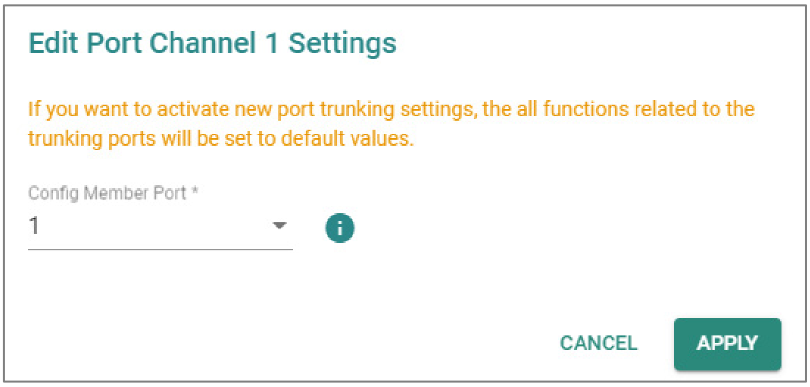
UI Setting	Description	Valid Range	Default Value
Config Member Port	Select the ports you want to include in the link aggregation group.	Port drop-down menu	N/A

Edit Link Aggregation

Menu Path: Network Configuration > Ports > Link Aggregation - Edit Link Aggregation

Clicking the **Edit (** ✎ **)** icon for a link aggregation on the **Network Configuration >**

Ports > Link Aggregation page will open this dialog box. This dialog lets you edit an existing link aggregation with member ports.



Edit Port Channel 1 Settings

If you want to activate new port trunking settings, the all functions related to the trunking ports will be set to default values.

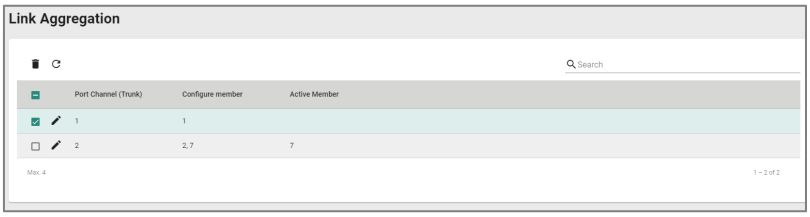
Config Member Port *: 1

UI Setting	Description	Valid Range	Default Value
Config Member Port	Select the ports you want to include in the link aggregation group.	Port drop-down menu	N/A

Delete Link Aggregation

Menu Path: Network Configuration > Ports > Link Aggregation

You can delete link aggregations by using the checkboxes to select the link aggregations you want to delete, then clicking the **Delete (🗑)** icon.



Link Aggregation

	Port Channel (Trunk)	Configure member	Active Member
☑	1	1	
□	2	2, 7	7

Max. 4

1 – 2 of 2

Layer 2 Switching

Menu Path: Network Configuration > Layer 2 Switching

This section lets you configure the Layer 2 switching settings for your device.

This section includes these pages:

- VLAN
- MAC Address
- QoS
- Rate Limit
- Multicast

VLAN

This page lets you configure global VLAN settings so you can partition your network into separate VLANs.

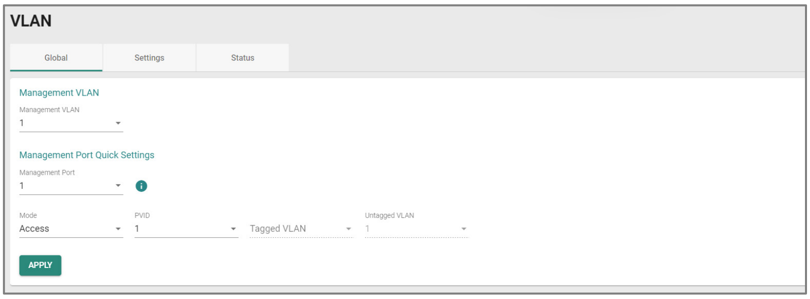
This page includes these tabs:

- Global
- Settings
- Status

VLAN Settings - Global

Menu Path: Network Configuration > Layer 2 Switching > VLAN - Global

This tab lets you configure the settings for the management VLAN and management port. Click **APPLY** to save your changes.



Management VLAN: 1

Management Port: 1

Mode: Access

PVID: 1

Tagged VLAN

Untagged VLAN: 1

UI Setting	Description	Valid Range	Default Value
Management VLAN	Specify the management VLAN ID from the drop-down menu.	1 to 4093	1
Management Port	Specify a management port for this device to allow for quick and easy configuration of VLAN settings for multiple ports.	(Depends on your device model)	N/A

The following settings will appear after selecting a **Management Port**:

UI Setting	Description	Valid Range	Default Value
Mode	Specify which VLAN mode the port should use: **Access**: Define the port as an Access port. This is used when connecting to single devices without tags. **Trunk**: Define the port as a Trunk port. This is used when connecting to another 802.1Q VLAN-aware router. **Hybrid**: Define the port as a Hybrid port. This is used when connecting to another 802.1Q VLAN-aware router, or another LAN that combines tagged and/or untagged devices and/or other routers or hubs.	Access / Trunk / Hybrid	Access
PVID	Set the default VLAN ID to use for traffic from untagged devices that connect to the port.	1 to 4093	1
Tagged VLAN	If the **Mode** is set to **Trunk** or **Hybrid**, you can specify what VLAN IDs tagged devices that connect to the port will use. Use commas to separate different VIDs.	All Member VIDs / 1 to 4093	Access mode: N/A Trunk or Hybrid mode: 1

UI Setting	Description	Valid Range	Default Value
Untagged VLAN	If the **Mode** is set to **Access**, assign a VLAN ID for untagged devices that connect to the port and remove tags upon egress. Use commas to separate different VLAN IDs.	All Member VIDs / 1 to 4093	Access mode: 1 Trunk or Hybrid mode: N/A

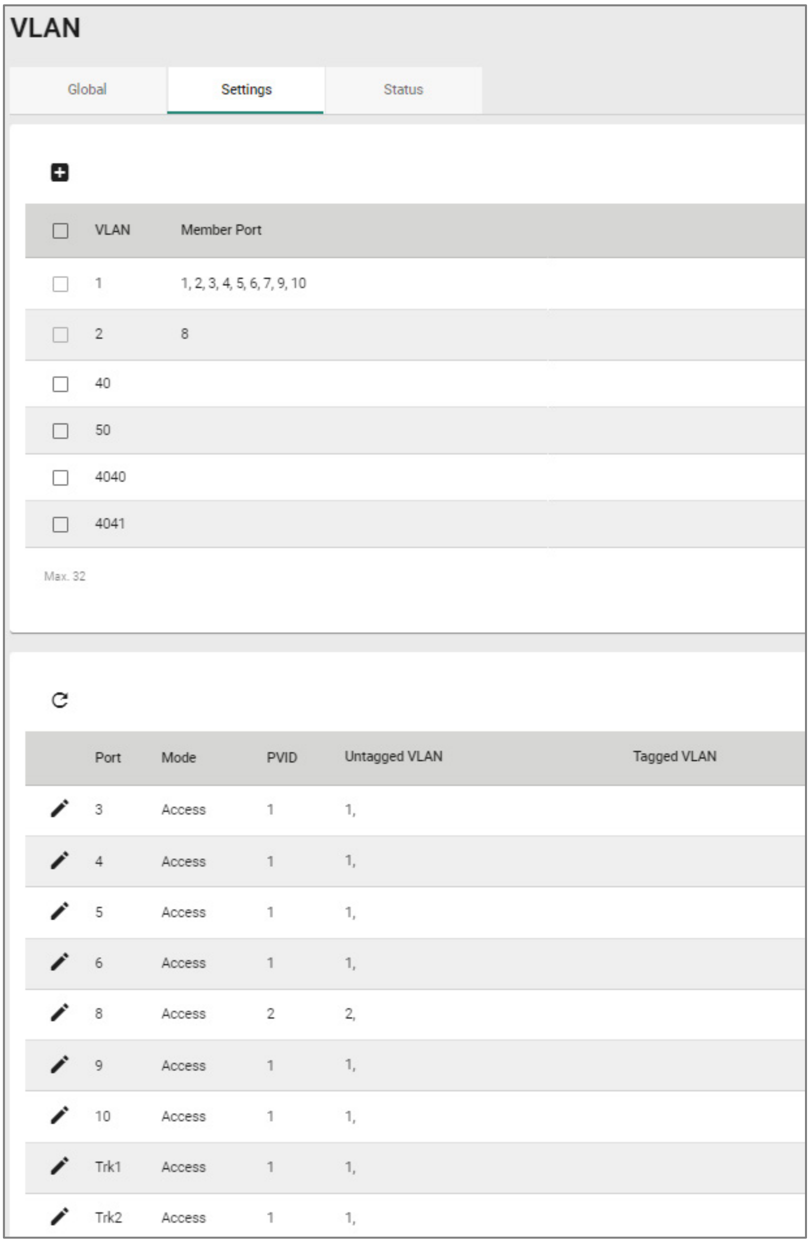
VLAN - Settings

Menu Path: Network Configuration > Layer 2 Switching > VLAN - Settings

This tab lets you configure management VLAN and port settings. Click **APPLY** to save your changes.

Limitations

You can create up to 32 VLANs.



□	VLAN	Member Port
□	1	1, 2, 3, 4, 5, 6, 7, 9, 10
□	2	8
□	40	
□	50	
□	4040	
□	4041	

Max. 32

	Port	Mode	PVID	Untagged VLAN	Tagged VLAN
✎	3	Access	1	1,	
✎	4	Access	1	1,	
✎	5	Access	1	1,	
✎	6	Access	1	1,	
✎	8	Access	2	2,	
✎	9	Access	1	1,	
✎	10	Access	1	1,	
✎	Trk1	Access	1	1,	
✎	Trk2	Access	1	1,	

Please note that port numbers will vary depending on the product model.

The top table shows a list of VLANs.

UI Setting	Description
VLAN	Shows the VID for the VLAN.

UI Setting	Description
Member Port	Shows which ports are in the VLAN.

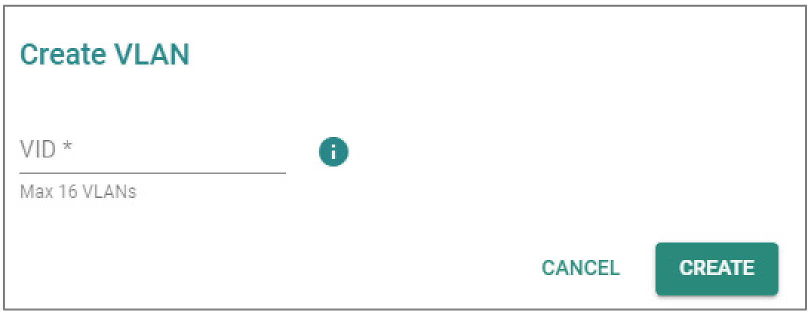
The bottom table shows a list of the device's ports and their VLAN settings.

UI Setting	Description
Port	Shows which port this row describes.
Mode	Shows the VLAN mode for the port.
PVID	Shows the PVID for the port.
Untagged VLAN	Shows the Untagged VLAN.
Tagged VLAN	Shows the Tagged VLAN.

VLAN - Settings - Create VLAN

Menu Path: Network Configuration > Layer 2 Switching > VLAN - Settings

Clicking the **Add (⊞)** icon on the **Network Configuration > Layer 2 Switching > PoE - Scheduling** page will open this dialog box. This dialog lets you create a VLAN. Click **CREATE** to save your changes and add the new VLAN.



Create VLAN

VID *

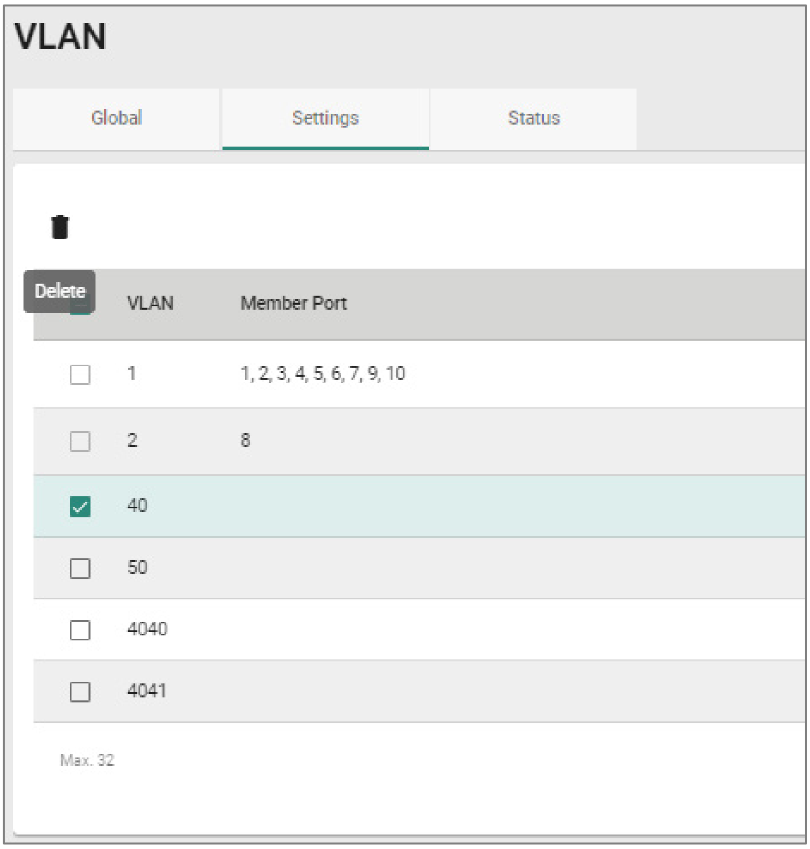
Max 16 VLANs

UI Setting	Description	Valid Range	Default Value
VID	Specify the VID to use for the VLAN. You can create multiple VLANs at once by entering single VIDs or VID ranges separated by commas, such as 2, 4-8, 10-13.	1 to 4094. You can enter multiple VIDs and/or VID ranges, separated by commas.	N/A

VLAN - Settings - Delete VLAN

Menu Path: Network Configuration > Layer 2 Switching > VLAN - Settings

You can delete VLANs by using the checkboxes to select the VLANs you want to delete, then clicking the **Delete (🗑)** icon.



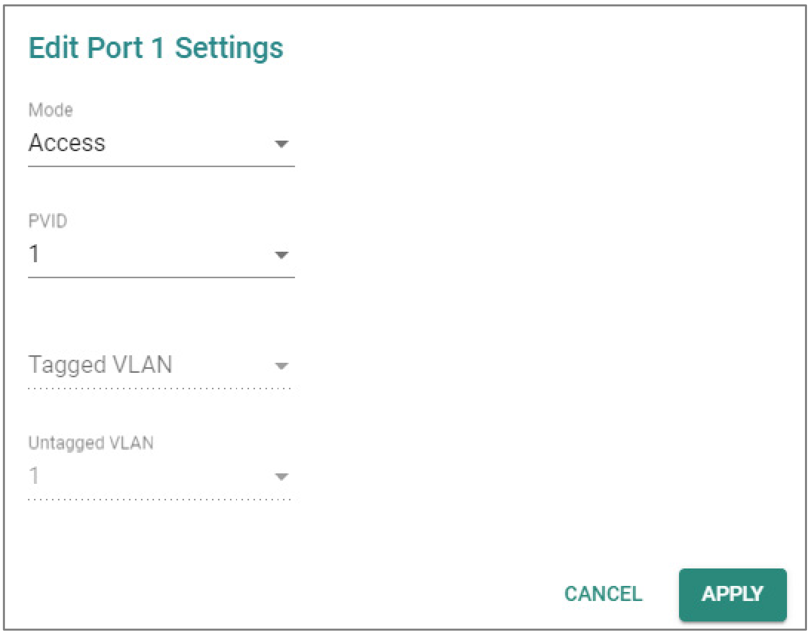
	VLAN	Member Port
☐	1	1, 2, 3, 4, 5, 6, 7, 9, 10
☐	2	8
☑	40	
☐	50	
☐	4040	
☐	4041	

Max. 32

VLAN - Settings - Edit Port Settings

Menu Path: Network Configuration > Layer 2 Switching > VLAN - Settings

Clicking the **Edit (✎)** icon for a port on the **Network Configuration > Layer 2 Switching > VLAN - Settings** page will open this dialog box. This dialog lets you edit the VLAN settings for a port. Click **APPLY** to save your changes.



Edit Port 1 Settings

Mode: Access

PVID: 1

Tagged VLAN

Untagged VLAN: 1

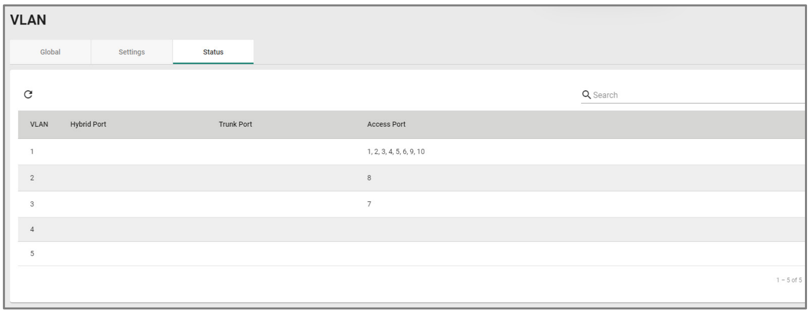
UI Setting	Description	Valid Range	Default Value
Mode	Specify which VLAN mode the port should use: **Access**: Define the port as an Access port. This is used when connecting to single devices without tags. **Trunk**: Define the port as a Trunk port. This is used when connecting to another 802.1Q VLAN-aware router. **Hybrid**: Define the port as a Hybrid port. This is used when connecting to another 802.1Q VLAN-aware router, or another LAN that combines tagged and/or untagged devices and/or other routers or hubs.	Access / Trunk / Hybrid	Access
PVID	Set the default VLAN ID to use for traffic from untagged devices that connect to the port.	1 to 4094	1

UI Setting	Description	Valid Range	Default Value
Tagged VLAN **(when editing settings for the Management Port)**	If the **Mode** is set to **Trunk** or **Hybrid**, you can specify what VLAN IDs tagged devices that connect to the port will use. Use commas to separate different VIDs.	All Member VIDs / 1 to 4094	N/A
Untagged VLAN **(when editing settings for the Management Port)**	If the **Mode** is set to **Access**, assign a VLAN ID for untagged devices that connect to the port and remove tags upon egress. Use commas to separate different VLAN IDs.	All Member VIDs / 1 to 4094	N/A

VLAN - Status

Menu Path: Network Configuration > Layer 2 Switching > VLAN - Status

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



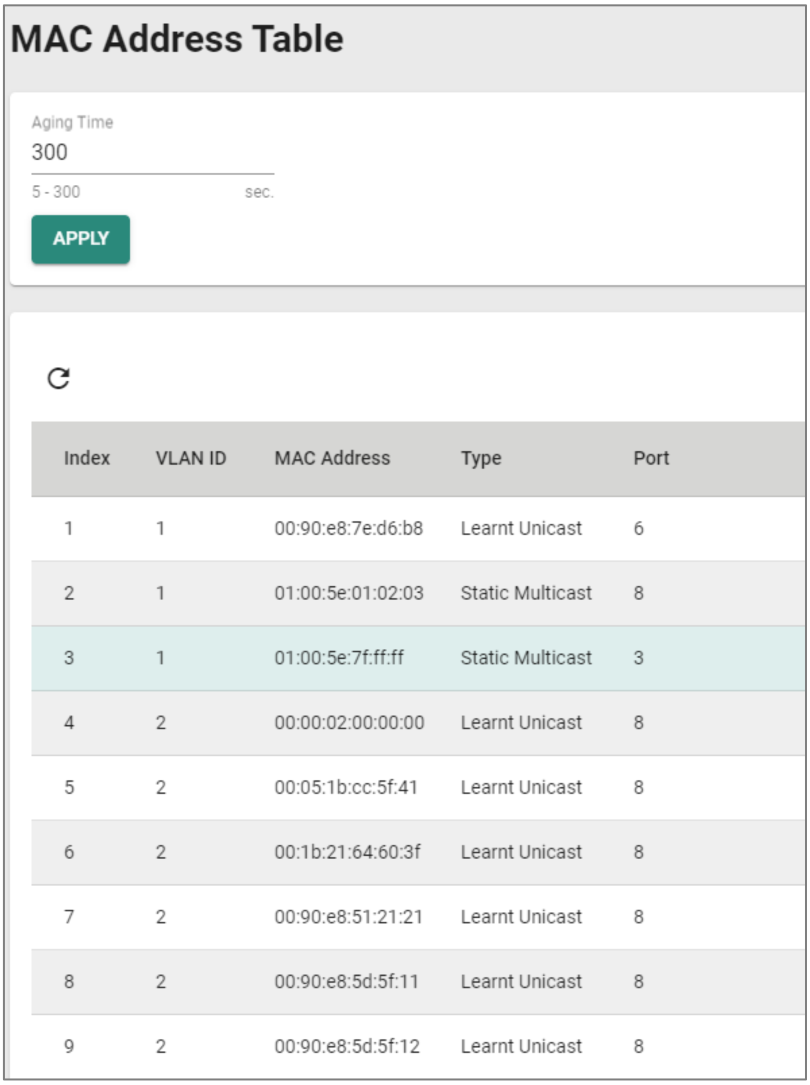
VLAN	Hybrid Port	Trunk Port	Access Port
1			1, 2, 3, 4, 5, 6, 9, 10
2			8
3			7
4			
5			

UI Setting	Description
VLAN	Shows the VID 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.

MAC Address Table Settings

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

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



MAC Address Table

Aging Time: 300 (5 - 300 sec.)

Index	VLAN ID	MAC Address	Type	Port
1	1	00:90:e8:7e:d6:b8	Learnt Unicast	6
2	1	01:00:5e:01:02:03	Static Multicast	8
3	1	01:00:5e:7f:ff:ff	Static Multicast	3
4	2	00:00:02:00:00:00	Learnt Unicast	8
5	2	00:05:1b:cc:5f:41	Learnt Unicast	8
6	2	00:1b:21:64:60:3f	Learnt Unicast	8
7	2	00:90:e8:51:21:21	Learnt Unicast	8
8	2	00:90:e8:5d:5f:11	Learnt Unicast	8
9	2	00:90:e8:5d:5f:12	Learnt Unicast	8

UI Setting	Description	Valid Range	Default Value
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.	5 to 300	300

The MAC address table shows the following information:

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.
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.

QoS

Menu Path: Network Configuration > Layer 2 Switching > QoS

This page lets you configure QoS settings to control network traffic prioritization.

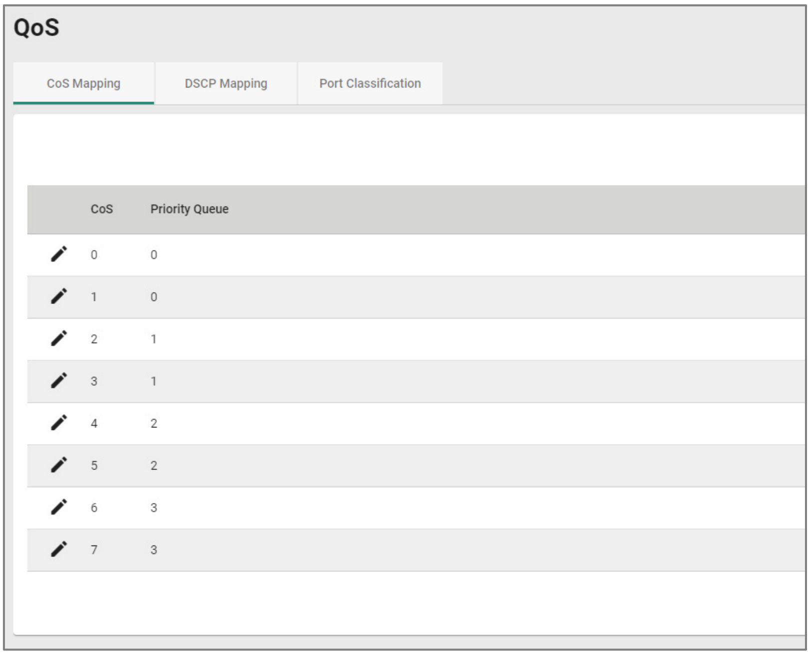
This page includes these tabs:

- CoS Mapping
- DSCP Mapping
- Port Classification

CoS Mapping

Menu Path: Network Configuration > Layer 2 Switching > QoS - CoS Mapping

This tab lets you configure CoS Mapping, which allows you to map 802.1p/1Q Layer 2 CoS tags to priority queues on the device.



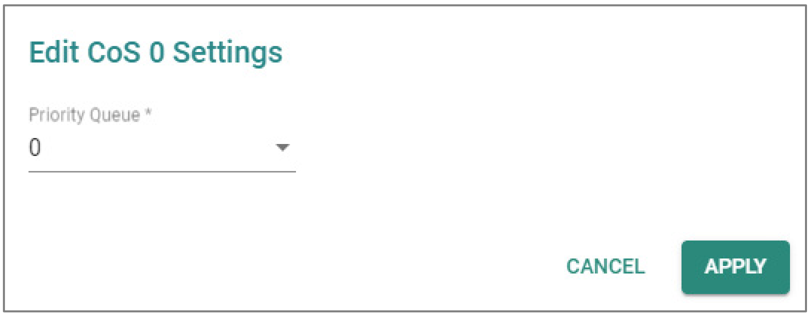
	CoS	Priority Queue
✎	0	0
✎	1	0
✎	2	1
✎	3	1
✎	4	2
✎	5	2
✎	6	3
✎	7	3

UI Setting	Description
CoS	Shows the CoS level. Higher numbers indicate higher priority.
Level	Shows the priority queue. Higher numbers indicate higher priority.

CoS Mapping - Edit a CoS Mapping

Menu Path: Network Configuration > Layer 2 Switching > QoS - CoS Mapping

Clicking the **Edit (✎)** icon for an CoS level on the **Network Configuration > Layer 2 Switching > QoS - CoS Mapping** tab will open this dialog box. This dialog lets you map CoS levels to priority queues. Click **APPLY** to save your changes.



Edit CoS 0 Settings

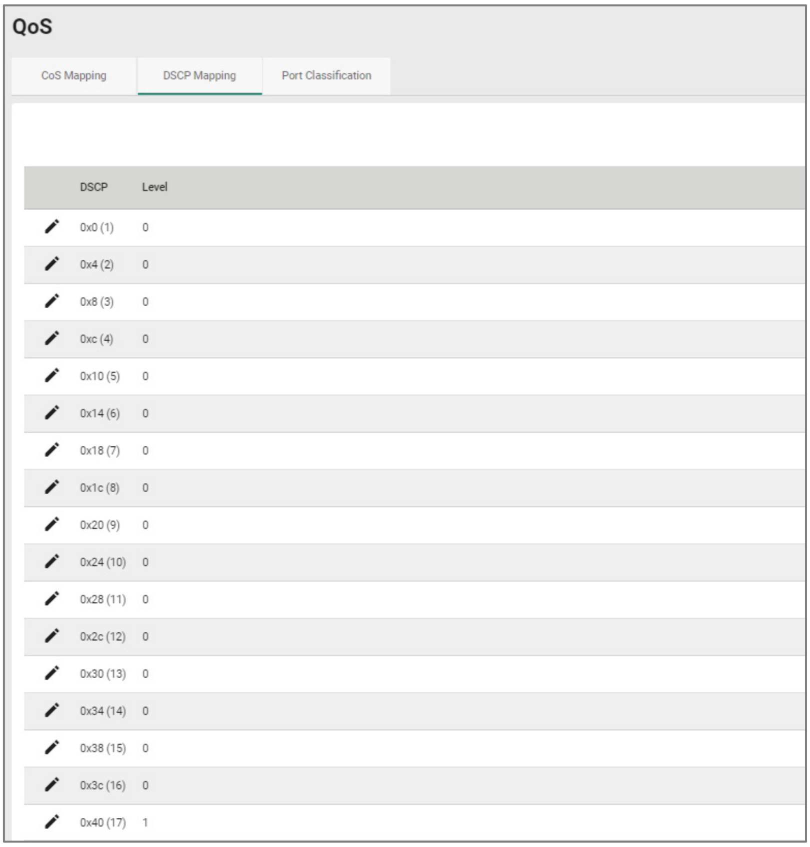
Priority Queue * 0

UI Setting	Description	Valid Range	Default Value
Priority Queue	Specify the priority queue to use for the CoS level. Higher numbers indicate higher priority.	0 to 3 (Depends on your device model)	0

DSCP Mapping

Menu Path: Network Configuration > Layer 2 Switching > QoS - DSCP Mapping

This tab lets you map Layer 3 DSCP levels to priority queues on the device.



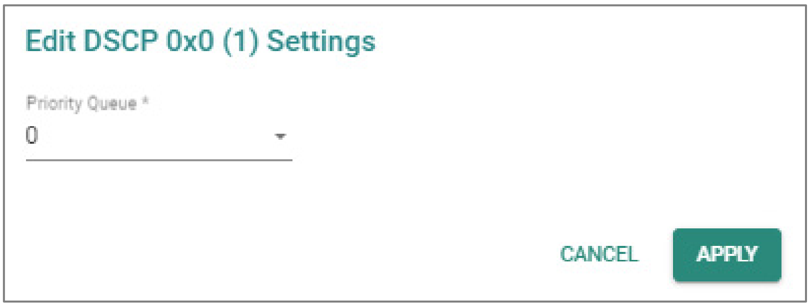
DSCP	Level
0x0 (1)	0
0x4 (2)	0
0x8 (3)	0
0xc (4)	0
0x10 (5)	0
0x14 (6)	0
0x18 (7)	0
0x1c (8)	0
0x20 (9)	0
0x24 (10)	0
0x28 (11)	0
0x2c (12)	0
0x30 (13)	0
0x34 (14)	0
0x38 (15)	0
0x3c (16)	0
0x40 (17)	1

UI Setting	Description
DSCP	Shows the DSCP level. Higher numbers indicate higher priority.
Level	Shows the priority queue. Higher numbers indicate higher priority.

DSCP Mapping - Edit a DSCP Mapping

Menu Path: Network Configuration > Layer 2 Switching > QoS - DSCP Mapping

Clicking the **Edit (✎)** icon for an DSCP mapping on the **Network Configuration > Layer 2 Switching > QoS - DSCP Mapping** page will open this dialog box. This dialog lets you map DSCP levels to priority queues. Click **APPLY** to save your changes.



Edit DSCP 0x0 (1) Settings

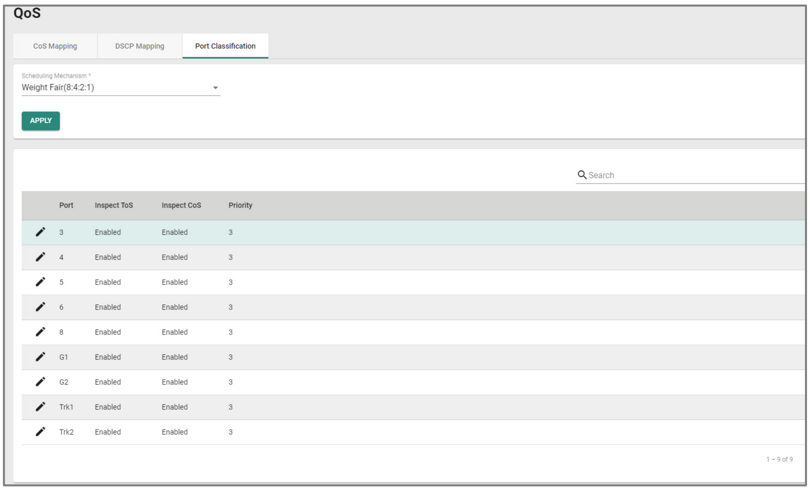
Priority Queue *
0

UI Setting	Description	Valid Range	Default Value
Priority Queue	Specify the priority queue to use for the DSCP level. Higher numbers indicate higher priority.	0 to 3 (Depends on your device model)	0

Port Classification

Menu Path: Network Configuration > Layer 2 Switching > QoS - Port Classification

This tab lets you set up QoS queueing mechanisms.



QoS

Scheduling Mechanism *
Weight Fair(8:4:2:1)

Port	Inspect ToS	Inspect CoS	Priority
3	Enabled	Enabled	3
4	Enabled	Enabled	3
5	Enabled	Enabled	3
6	Enabled	Enabled	3
8	Enabled	Enabled	3
G1	Enabled	Enabled	3
G2	Enabled	Enabled	3
Trk1	Enabled	Enabled	3
Trk2	Enabled	Enabled	3

1 – 9 of 9

UI Setting	Description	Valid Range	Default Value
Scheduling Mechanism	Specify the scheduling mechanism to use for your device: **Weight Fair(8:4:2:1)**: In the weight fair scheme, an 8, 4, 2, 1 weighting is applied to the four priority levels on the device. This approach prevents lower priority frames from being starved of opportunities for transmission with only a slight delay to higher priority frames. **Strict(High Priority First Always)**: In the strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunities for transmitting any frames, but ensures that all high priority frames will egress the switch as soon as possible.	Weight Fair(8:4:2:1) / Strict(High Priority First Always)	Weight Fair(8:4:2:1)

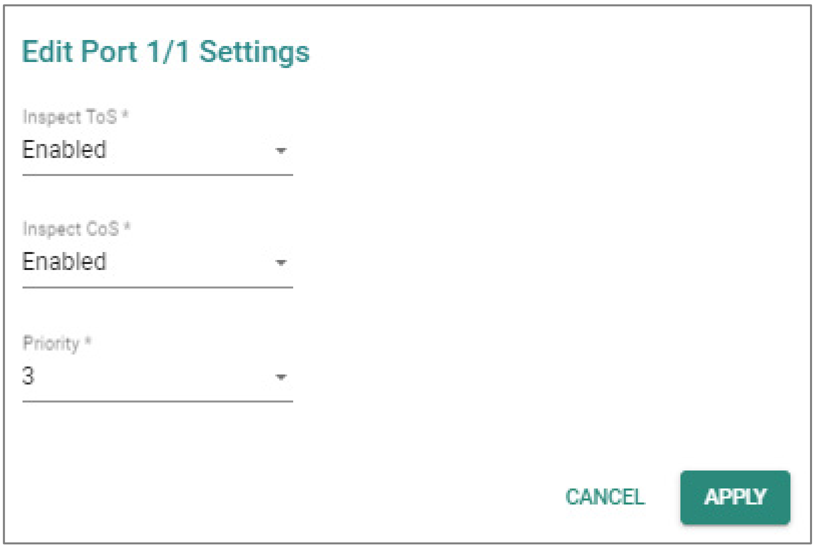
The port classification table shows the following information:

UI Setting	Description
Port	Shows which port this row describes.
Inspect ToS	Shows whether ToS is enabled or disabled for the port.
Inspect CoS	Shows whether CoS inspection is enabled or disabled for the port.
Priority	Shows the priority for the port. Higher numbers indicate higher priority.

Port Classification - Edit Port Setting

Menu Path: Network Configuration > Layer 2 Switching > QoS - Port Classification

Clicking the **Edit (✎)** icon for a port on the **Network Configuration > Layer 2 Switching > QoS - Port Classification** page will open this dialog box. This dialog lets you adjust the QoS classification settings for each port. Click **APPLY** to save your changes.



Edit Port 1/1 Settings

Inspect ToS *: Enabled

Inspect CoS *: Enabled

Priority *: 3

UI Setting	Description	Valid Range	Default Value
Inspect ToS	Enable or disable inspection of Type of Service (ToS) bits in the IPV4 frame to determine the priority of each frame.	Enabled or Disabled	Enabled
Inspect CoS	Enable or disable inspection of 802.1p CoS tags in the MAC frame to determine the priority of each frame.	Enabled or Disabled	Enabled
Priority	Specify the priority of the port. Higher numbers indicate higher priority.	0 to 7	3

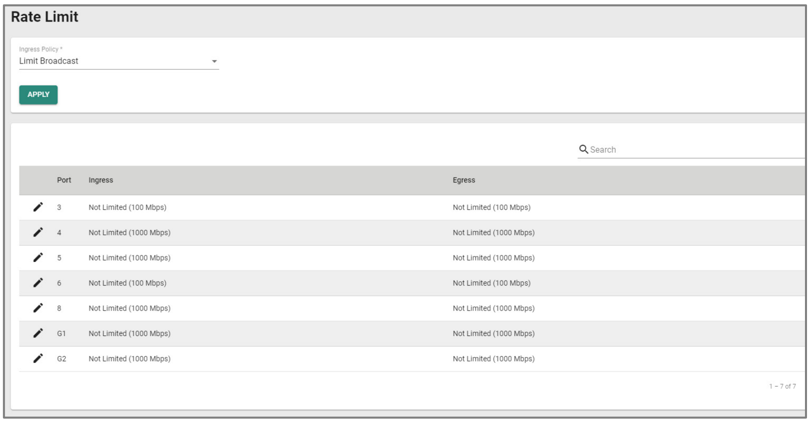
Rate Limit Settings

Menu Path: Network Configuration > Layer 2 Switching > Rate Limit

This page lets you control the bandwidth of ingress (incoming) and egress (outgoing) traffic through the device to protect end-devices that may not have the capability to handle large amounts of traffic.

Note

Please note that available options may vary depending on the product model.

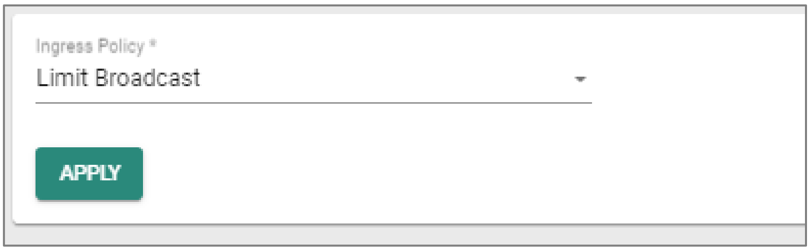

Rate Limit

Ingress Policy *
Limit Broadcast

Port	Ingress	Egress
3	Not Limited (100 Mbps)	Not Limited (100 Mbps)
4	Not Limited (1000 Mbps)	Not Limited (1000 Mbps)
5	Not Limited (1000 Mbps)	Not Limited (1000 Mbps)
6	Not Limited (100 Mbps)	Not Limited (100 Mbps)
8	Not Limited (1000 Mbps)	Not Limited (1000 Mbps)
G1	Not Limited (1000 Mbps)	Not Limited (1000 Mbps)
G2	Not Limited (1000 Mbps)	Not Limited (1000 Mbps)

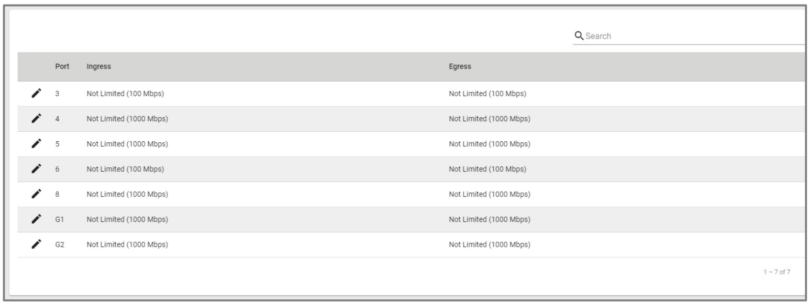
1 – 7 of 7

Rate Limit Settings


Ingress Policy *
Limit Broadcast

UI Setting	Description	Valid Range	Default Value
Ingress Policy	Select which kind of traffic ingress rate limiting will be applied to. **Limit All**: Rate limiting will be applied to all traffic. **Limit Broadcast, Multicast and Flooded Unicast**: Rate limiting will be applied to broadcast, multicast, and flooded unicast traffic only. **Limit Broadcast, Multicast**: Rate limiting will be applied to broadcast and multicast traffic only. **Limit Broadcast**: Rate limiting will be applied to broadcast traffic only.	Limit All / Limit Broadcast, Multicast and Flooded Unicast / Limit Broadcast, Multicast / Limit Broadcast	Limit Broadcast

Rate Limit Port List



Search

	Port	Ingress	Egress
✎	3	Not Limited (100 Mbps)	Not Limited (100 Mbps)
✎	4	Not Limited (1000 Mbps)	Not Limited (1000 Mbps)
✎	5	Not Limited (1000 Mbps)	Not Limited (1000 Mbps)
✎	6	Not Limited (100 Mbps)	Not Limited (100 Mbps)
✎	8	Not Limited (1000 Mbps)	Not Limited (1000 Mbps)
✎	G1	Not Limited (1000 Mbps)	Not Limited (1000 Mbps)
✎	G2	Not Limited (1000 Mbps)	Not Limited (1000 Mbps)

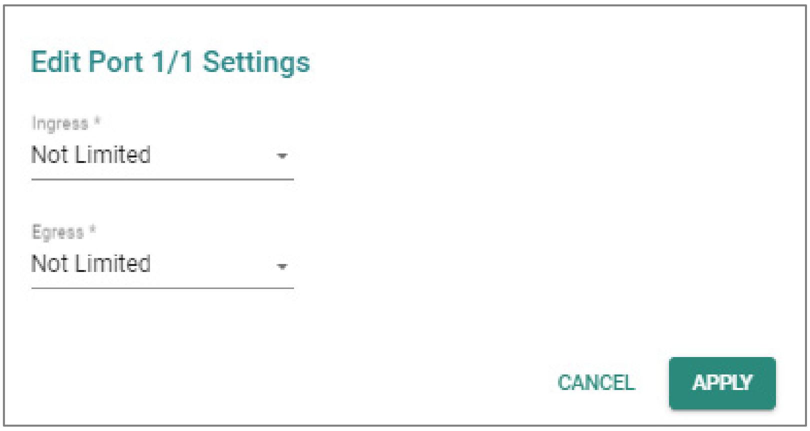
1 – 7 of 7

UI Setting	Description
Port	Shows which port this row describes.
Ingress	Shows the ingress bandwidth rate limit method and bandwidth.
Engress	Shows the egress bandwidth rate limit method and bandwidth.

Rate Limit - Edit Port Settings

Menu Path: Network Configuration > Layer 2 Switching > Rate Limit

Clicking the **Edit (✎)** icon for a port on the **Network Configuration > Layer 2 Switching > Rate Limit** page will open this dialog box. This dialog lets you configure rate limit settings for each port. Click **APPLY** to save your changes.



Edit Port 1/1 Settings

Ingress *
Not Limited

Egress *
Not Limited

UI Setting	Description	Valid Range	Default Value
Ingress	Select the ingress rate limit (% of max. throughput) for all packets.	Not Limited / 3% / 5% / 10% /15% / 25% / 35% / 50% / 65% / 85%	Not Limited
Egress	Select the egress rate limit (% of max. throughput) for all packets.	Not Limited / 3% / 5% / 10% /15% / 25% / 35% / 50% / 65% / 85%	Not Limited

Multicast

Menu Path: Network Configuration > Layer 2 Switching > Multicast

This section lets you adjust various settings for handling multicast traffic.

This section includes these pages:

- IGMP Snooping
- Static Multicast Table

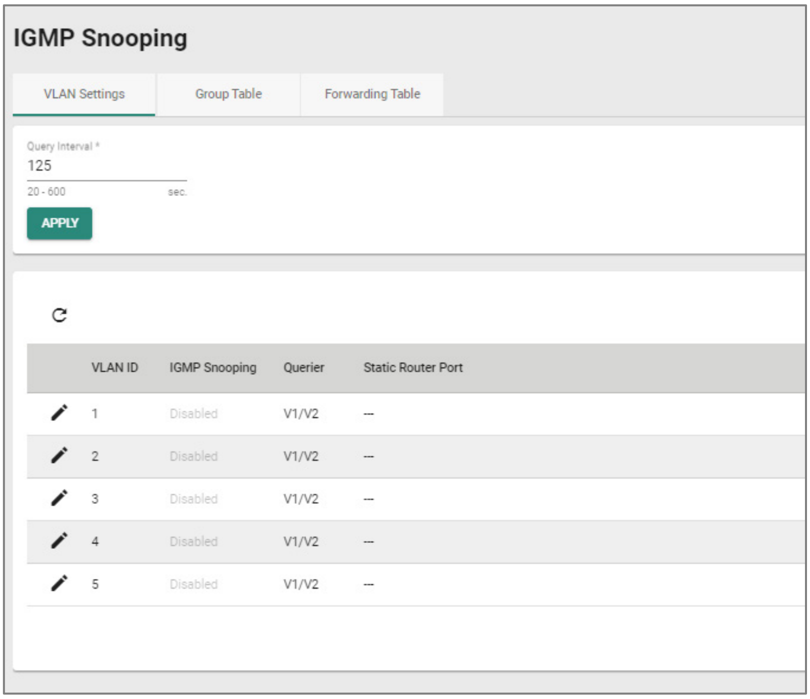
IGMP Snooping

Menu Path: Network Configuration > Layer 2 Switching > Multicast > IGMP Snooping

This page lets you configure IGMP snooping, which enables intelligent forwarding of multicast traffic in local area networks (LANs). By listening to IGMP messages sent between hosts and multicast routers, IGMP snooping can learn which multicast groups are active on the network and maintain a database of multicast group membership.

This page includes these tabs:

- VLAN Settings
- Group Table
- Forwarding Table



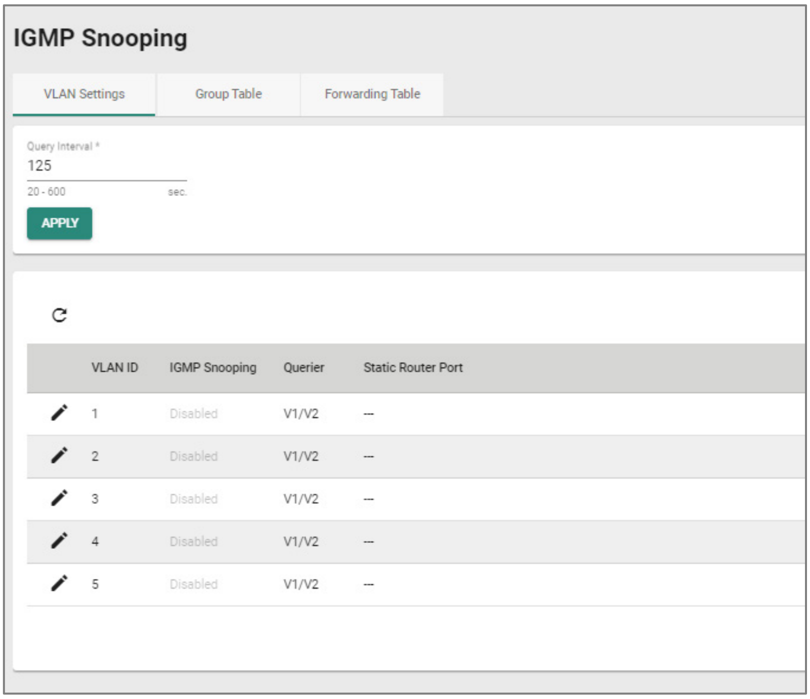
Query Interval *
125
20 - 600 sec.

	VLAN ID	IGMP Snooping	Querier	Static Router Port
✎	1	Disabled	V1/V2	--
✎	2	Disabled	V1/V2	--
✎	3	Disabled	V1/V2	--
✎	4	Disabled	V1/V2	--
✎	5	Disabled	V1/V2	--

VLAN Settings

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

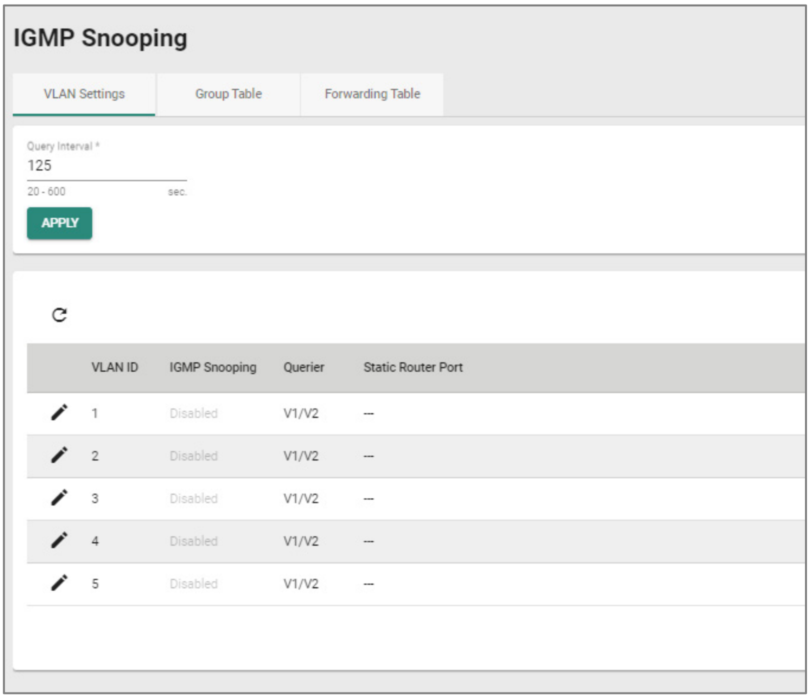
This tab lets you configure IGMP snooping settings for each VLAN.



Query Interval *
125
20 - 600 sec.

	VLAN ID	IGMP Snooping	Querier	Static Router Port
✎	1	Disabled	V1/V2	--
✎	2	Disabled	V1/V2	--
✎	3	Disabled	V1/V2	--
✎	4	Disabled	V1/V2	--
✎	5	Disabled	V1/V2	--

IGMP VLAN Settings

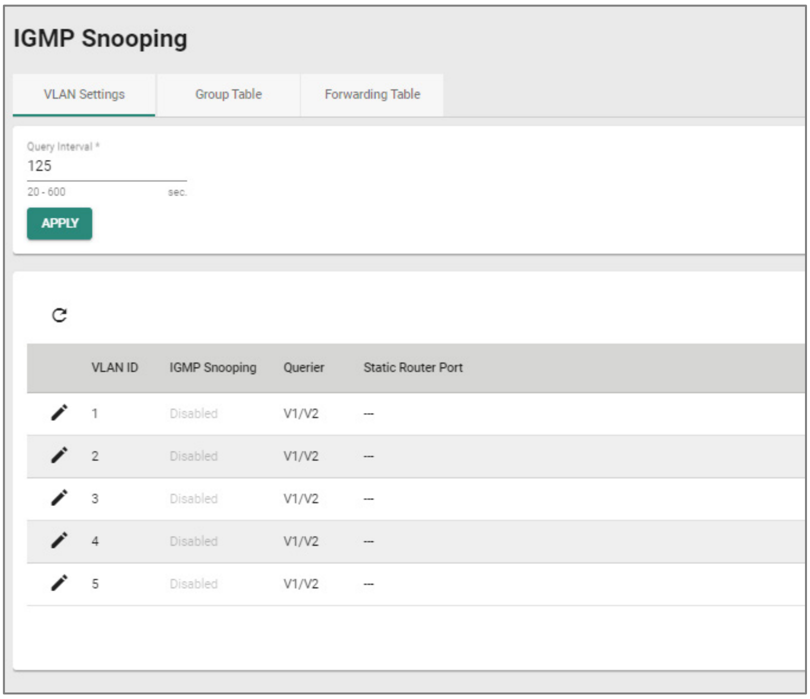


Query Interval *
125
20 - 600 sec.

	VLAN ID	IGMP Snooping	Querier	Static Router Port
✎	1	Disabled	V1/V2	--
✎	2	Disabled	V1/V2	--
✎	3	Disabled	V1/V2	--
✎	4	Disabled	V1/V2	--
✎	5	Disabled	V1/V2	--

UI Setting	Description	Valid Range	Default Value
Query Interval	Specify the query interval of the querier function globally.	20 to 600 seconds	125 seconds

IGMP VLAN List



IGMP Snooping

Query Interval * 125 (20 - 600 sec.)

	VLAN ID	IGMP Snooping	Querier	Static Router Port
✎	1	Disabled	V1/V2	---
✎	2	Disabled	V1/V2	---
✎	3	Disabled	V1/V2	---
✎	4	Disabled	V1/V2	---
✎	5	Disabled	V1/V2	---

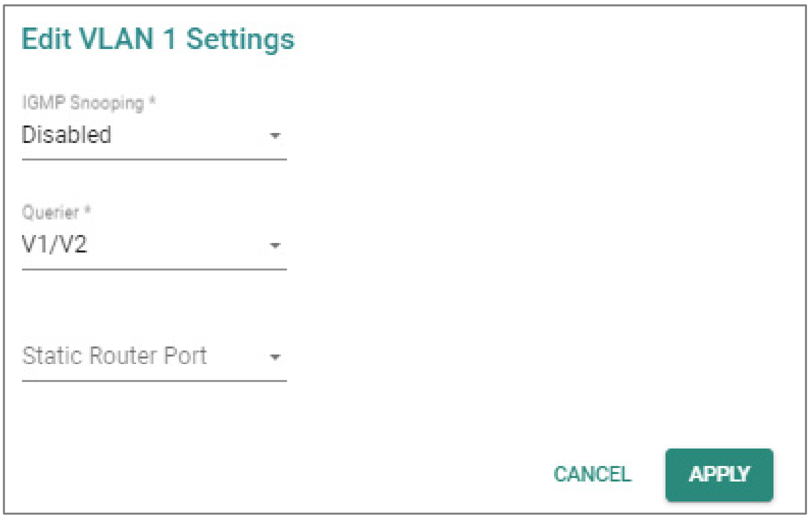
UI Setting	Description
VLAN ID	Shows which VLAN ID this row describes.
IGMP Snooping	Shows whether IGMP snooping is enabled or disabled for the VLAN.
Querier	Shows which version of IGMP snooping the VLAN will use.
Static Router Port	Shows the static router port the VLAN will use to connect to the multicast router for IGMP snooping.

VLAN Settings - Edit VLAN Settings

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

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

Click **APPLY** to save your changes.



Edit VLAN 1 Settings

IGMP Snooping *: Disabled

Querier *: V1/V2

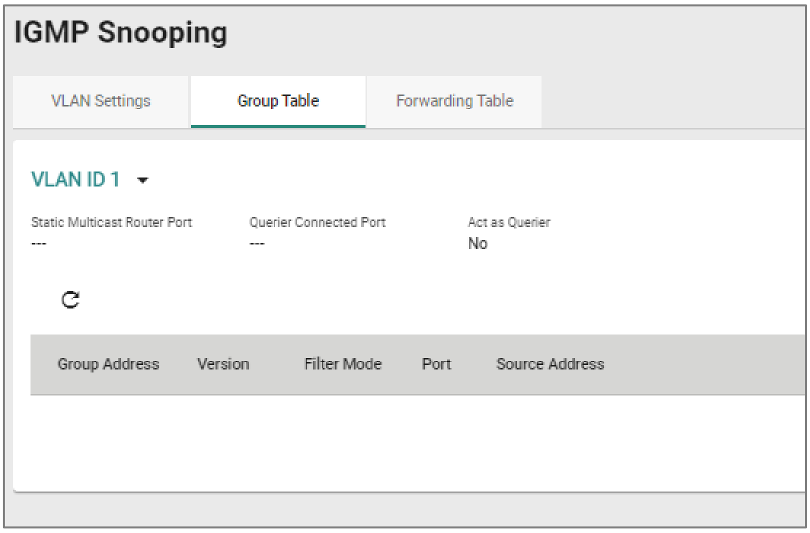
Static Router Port

UI Setting	Description	Valid Range	Default Value
IGMP Snooping	Enable or disable IGMP Snooping function for the VLAN.	Enabled / Disabled	Disabled
Version	Specify which version of IGMP snooping to use: **V1/V2**: Enable the Moxa device to send IGMP snooping version 1 and 2 queries. **V3**: Enable the Moxa device to send IGMP snooping version 3 queries.	V1/V2 / V3	V1/V2
Static Router Port	Select which ports will be used to connect to multicast routers for IGMP Snooping. The device will receive all multicast packets from the selected ports. ✎ **Note** If a router or Layer 3 switch is connected to the network, it will act as the querier, and the querier function will be disabled on all Moxa Layer 2 switches. If all switches on the network are Moxa Layer 2 switches, then only one Layer 2 switch will act as the querier.	1/1 / 1/2 / 1/3 / 1/4 / 1/5 / 1/6 / 1/7 / 1/8 / 1/9 / 1/10	N/A

Group Table

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

This tab lets you see all currently active IGMP groups that were detected for each VLAN.



IGMP Snooping

Static Multicast Router Port: ---

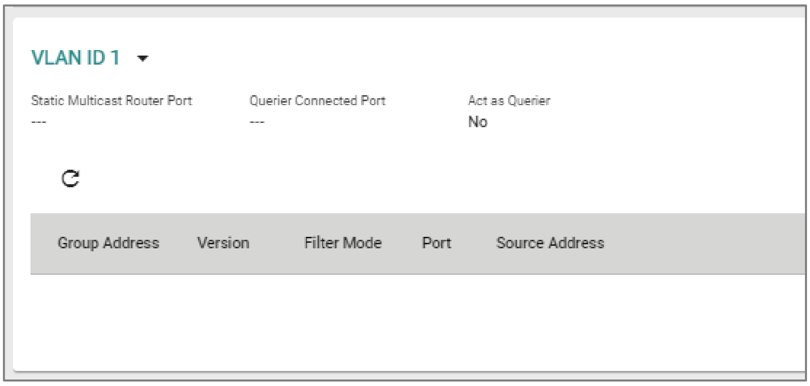
Querier Connected Port: ---

Act as Querier: No

Group Address	Version	Filter Mode	Port	Source Address

VLAN Group Table List

You can use the VLAN drop-down to select which VLAN's group table is displayed.



Static Multicast Router Port: ---

Querier Connected Port: ---

Act as Querier: No

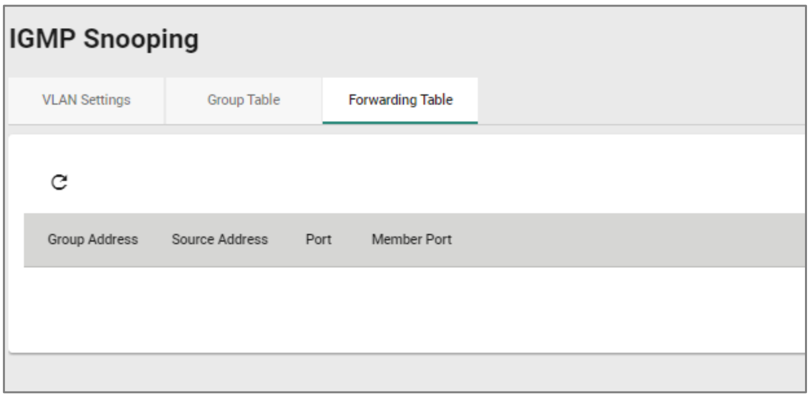
Group Address	Version	Filter Mode	Port	Source Address

UI Setting	Description
Static Multicast Router Port	Shows the static multicast querier port(s) for the VLAN.
Querier Connected Port	Shows the port which is connected to the querier for the VLAN.
Act as a Querier	Shows whether or not this VLAN has been selected to act as a querier.
Group Address	Shows the multicast group addresses for the VLAN.
Version	Shows the IGMP snooping version for the group address.
Filter Mode	If IGMP v3 is enabled for the VLAN ID, this shows whether the group address is Included or Excluded.
Port	Shows which ports are members of the group address.
Source Address	When IGMP v3 is enabled, this shows the multicast source address for the group address.

Forwarding Table

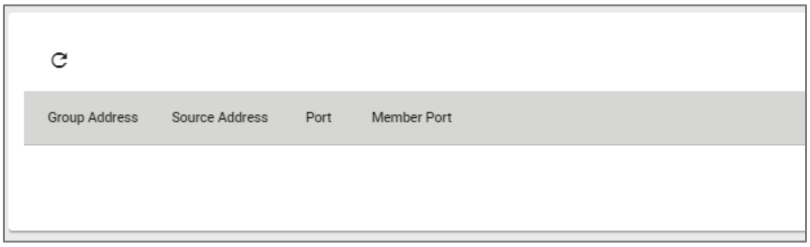
Menu Path: Network Configuration > Layer 2 Switching > Multicast > IGMP Snooping - Forwarding Table

This page lets you see the multicast stream forwarding status for each VLAN.



Group Address	Source Address	Port	Member Port

Forwarding Table



UI Setting	Description
Group Address	Shows the multicast group IP address.
Source Address	Shows the IP address the multicast group will receive multicast streams from.
Port	Shows the port receiving the multicast stream.
Member Port	Shows the port the multicast stream is forwarded to.

Static Multicast Table

Menu Path: Network Configuration > Layer 2 Switching > Multicast > Static Multicast Table

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

Note

Please note that settings and available options will vary depending on the product model.

Note

Moxa's Router Series 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. This allows the same MAC address to be used in multiple VLANs without causing forwarding issues.

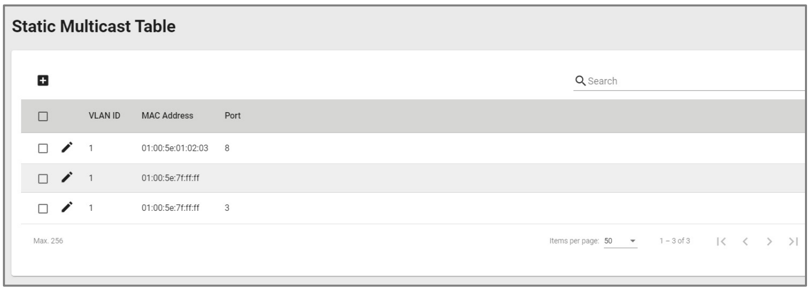
This may lead to a larger MAC address table size, as each VLAN maintains its own individual address table, and the number of MAC address entries will increase based on the number of VLAN member ports used.

Limitations

You can add up to 256 static multicast entries.

The number of entries is calculated as follows: **number of MAC address entries * the number of VLAN IDs**

For example, if the static multicast table contains 30 MAC addresses and is connected to 4 VLAN IDs, then the number of MAC address entries would be 30 MAC addresses * 4 VLAN IDs = 120 static multicast entries.


Static Multicast Table

□	VLAN ID	MAC Address	Port
□	1	01:00:5e:01:02:03	8
□	1	01:00:5e:7f:ff:ff	
□	1	01:00:5e:7f:ff:ff	3

Max. 256

Items per page: 50

1 – 3 of 3

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

Static Multicast Table - Create Static Multicast

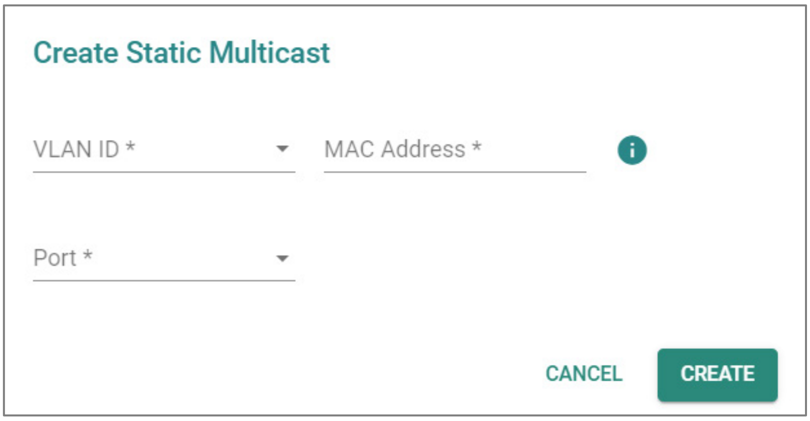
Menu Path: Network Configuration > Layer 2 Switching > Multicast > Static

Multicast Table

Clicking the **Add (⊞)** icon on the **Network Configuration > Layer 2 Switching > Multicast > Static Multicast Table** 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 static multicast entry.

Note

01:00:5E:XX:XX:XX on this page is the IP multicast MAC address, please activate IGMP Snooping for automatic classification.

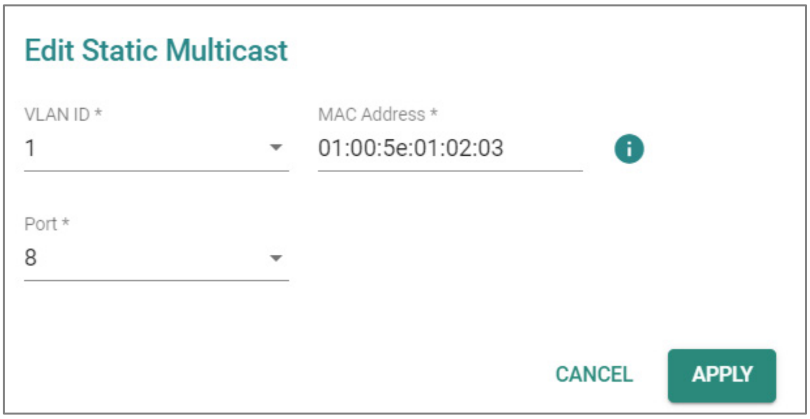


UI Setting	Description	Valid Range	Default Value
VLAN ID	Specify the VLAN ID.	Drop-down list of VLAN ID	N/A
MAC Address	Specify the static multicast MAC address.	Valid multicast MAC address	N/A
Port	Specify which ports you want to include in the static multicast group.	Drop-down list of ports	N/A

Static Multicast Table - Edit Static Multicast

Menu Path: Network Configuration > Layer 2 Switching > Multicast > Static Multicast Table

Clicking the **Edit (✎)** icon for an account on the **Network Configuration > Layer 2 Switching > Multicast > Static Multicast Table** page will open this dialog box. This dialog lets you edit an existing static multicast entry. Click **APPLY** to save your changes.



Edit Static Multicast

VLAN ID * 1

MAC Address * 01:00:5e:01:02:03

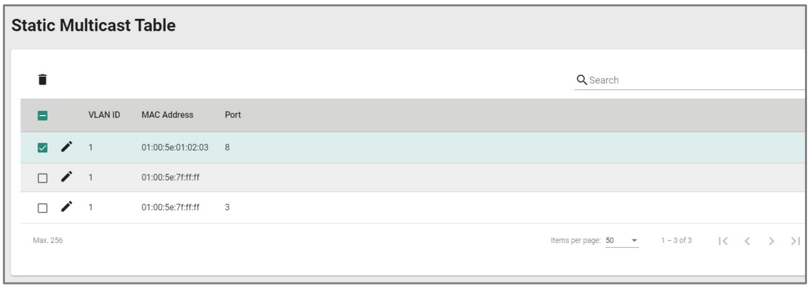
Port * 8

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

Static Multicast Table - Delete Static Multicast

Menu Path: Network Configuration > Layer 2 Switching > Multicast > Static Multicast Table

You can delete user accounts by using the checkboxes to select the accounts you want to delete, then clicking the **Delete (🗑)** icon.



Static Multicast Table

☐		VLAN ID	MAC Address	Port
☑	✎	1	01:00:5e:01:02:03	8
☐	✎	1	01:00:5e:7f:ff:ff	
☐	✎	1	01:00:5e:7f:ff:ff	3

Max. 256

Items per page: 50   1 – 3 of 3

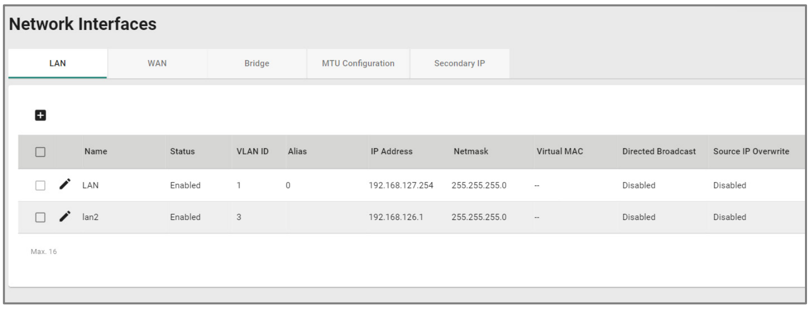
Network Interfaces

Menu Path: Network Configuration > Network Interfaces

This page lets you configure the settings for the various interfaces of your device.

This page includes these tabs:

- LAN
- WAN
- Bridge
- MTU Configuration
- Secondary IP



Network Interfaces

☐		Name	Status	VLAN ID	Alias	IP Address	Netmask	Virtual MAC	Directed Broadcast	Source IP Overwrite
☐	✎	LAN	Enabled	1	0	192.168.127.254	255.255.255.0	--	Disabled	Disabled
☐	✎	lan2	Enabled	3		192.168.126.1	255.255.255.0	--	Disabled	Disabled

Max. 16

LAN

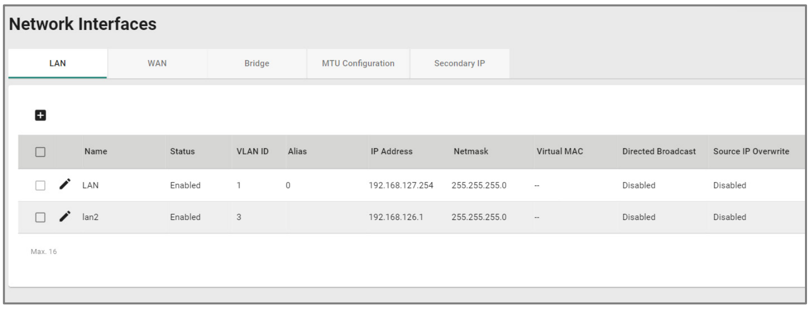
Menu Path: Network Configuration > Network Interfaces - LAN

This tab lets you manage your LAN interfaces.

Limitations

You can create up to 16 LAN interfaces by configuring each port with unique VLAN ID numbers.

Network Interfaces List



Network Interfaces

		Name	Status	VLAN ID	Alias	IP Address	Netmask	Virtual MAC	Directed Broadcast	Source IP Overwrite
□	✎	LAN	Enabled	1	0	192.168.127.254	255.255.255.0	--	Disabled	Disabled
□	✎	lan2	Enabled	3		192.168.126.1	255.255.255.0	--	Disabled	Disabled

Max. 16

UI Setting	Description
Name	Shows the name of the interface.
Status	Shows the status of the interface.
VLAN ID	Shows the VLAN ID used for the interface.
Alias	Shows the alias for the interface.
IP Address	Shows the IP address of the interface.
Netmask	Shows the subnet mask of the interface.
Virtual MAC	Shows the virtual MAC address of the interface.
Directed Broadcast	Shows whether directed broadcast is enabled for the interface.
Source IP Overwrite	Shows whether source IP overwrite is enabled for the interface.

LAN - Create LAN Interface Entry

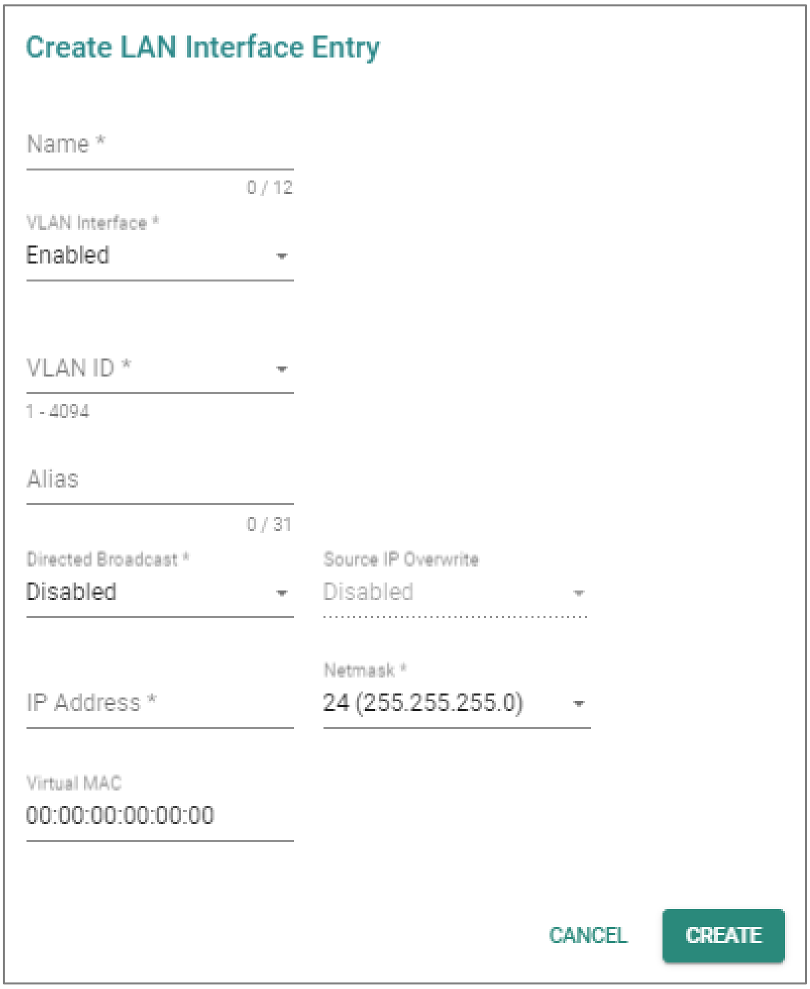
Menu Path: Network Configuration > Network Interfaces - LAN

Clicking the **Add (⊞)** icon on the **Network Configuration > Network Interfaces - LAN** page will open this dialog box. This dialog lets you create new LAN interface entries for your device. Click **CREATE** to save your changes and add the new interface.

Limitations

You can create up to 16 LAN interfaces by configuring each port with unique VLAN ID numbers.

The VLAN ID of the first LAN interface configured will be set as the management VLAN ID.



Create LAN Interface Entry

Name * 0 / 12

VLAN Interface * Enabled

VLAN ID * 1 - 4094

Alias 0 / 31

Directed Broadcast * Disabled

Source IP Overwrite Disabled

IP Address *

Netmask * 24 (255.255.255.0)

Virtual MAC 00:00:00:00:00:00

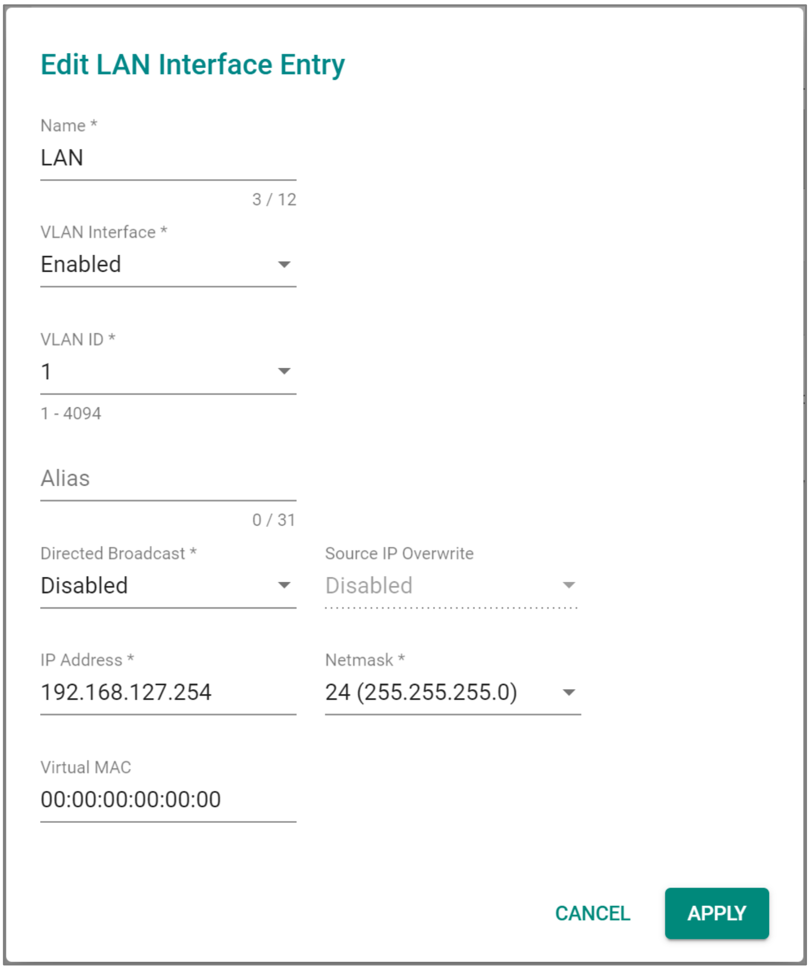
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the interface.	1 to 12 characters	N/A
VLAN Interface	Enable or disable the VLAN interface.	Enabled / Disabled	Enabled
VLAN ID	Specify the VLAN ID.	1 to 4094	N/A
Alias	Specify an alias for the VLAN interface.	1 to 31 characters	N/A
Directed Broadcast	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
Source IP Overwrite	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address of the interface.	Valid IP address	N/A
Netmask	Specify the subnet mask of the interface.	Valid subnet mask	24 (255.255.255.0)
Virtual MAC	Specify the virtual MAC address of the interface.	Valid MAC address	00:00:00:00:00:00

LAN - Edit LAN Interface Entry

Menu Path: Network Configuration > Network Interfaces - LAN

Clicking the **Edit (✎)** icon on the **Network Configuration > Network Interfaces - LAN** page will open this dialog box. This dialog lets you edit an existing LAN interface entry for your device. Click **SAVE** to save your changes.



Edit LAN Interface Entry

Name *
LAN
3 / 12

VLAN Interface *
Enabled

VLAN ID *
1
1 - 4094

Alias
0 / 31

Directed Broadcast *
Disabled

Source IP Overwrite
Disabled

IP Address *
192.168.127.254

Netmask *
24 (255.255.255.0)

Virtual MAC
00:00:00:00:00:00

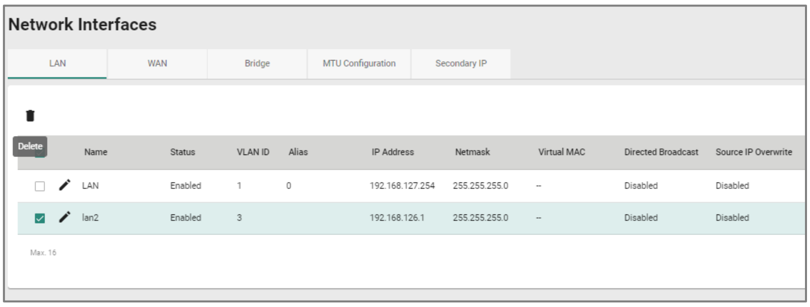
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the interface.	1 to 12 characters	N/A
VLAN Interface	Enable or disable the VLAN interface.	Enabled / Disabled	Enabled
VLAN ID	Specify the VLAN ID.	1 to 4094	N/A
Alias	Specify an alias for the VLAN interface.	1 to 31 characters	N/A
Directed Broadcast	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
Source IP Overwrite	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address of the interface.	Valid IP address	N/A
Netmask	Specify the subnet mask of the interface.	Valid subnet mask	24 (255.255.255.0)
Virtual MAC	Specify the virtual MAC address of the interface.	Valid MAC address	00:00:00:00:00:00

Delete LAN Interface Entry

Menu Path: Network Configuration > Network Interfaces - LAN

You can delete interfaces by using the checkboxes to select the interfaces you want to delete, then clicking the **Delete (🗑)** icon.



Network Interfaces

		Name	Status	VLAN ID	Alias	IP Address	Netmask	Virtual MAC	Directed Broadcast	Source IP Overwrite
□	✎	LAN	Enabled	1	0	192.168.127.254	255.255.255.0	--	Disabled	Disabled
☑	✎	lan2	Enabled	3		192.168.126.1	255.255.255.0	--	Disabled	Disabled

Max. 16

WAN

Menu Path: Network Configuration > Network Interfaces - WAN

This page lets you configure the settings for the WAN interfaces of your device. WAN interface is VLAN-based; when WAN is enabled for a VLAN ID, all ports associated with that VLAN ID will act as a single WAN interface.

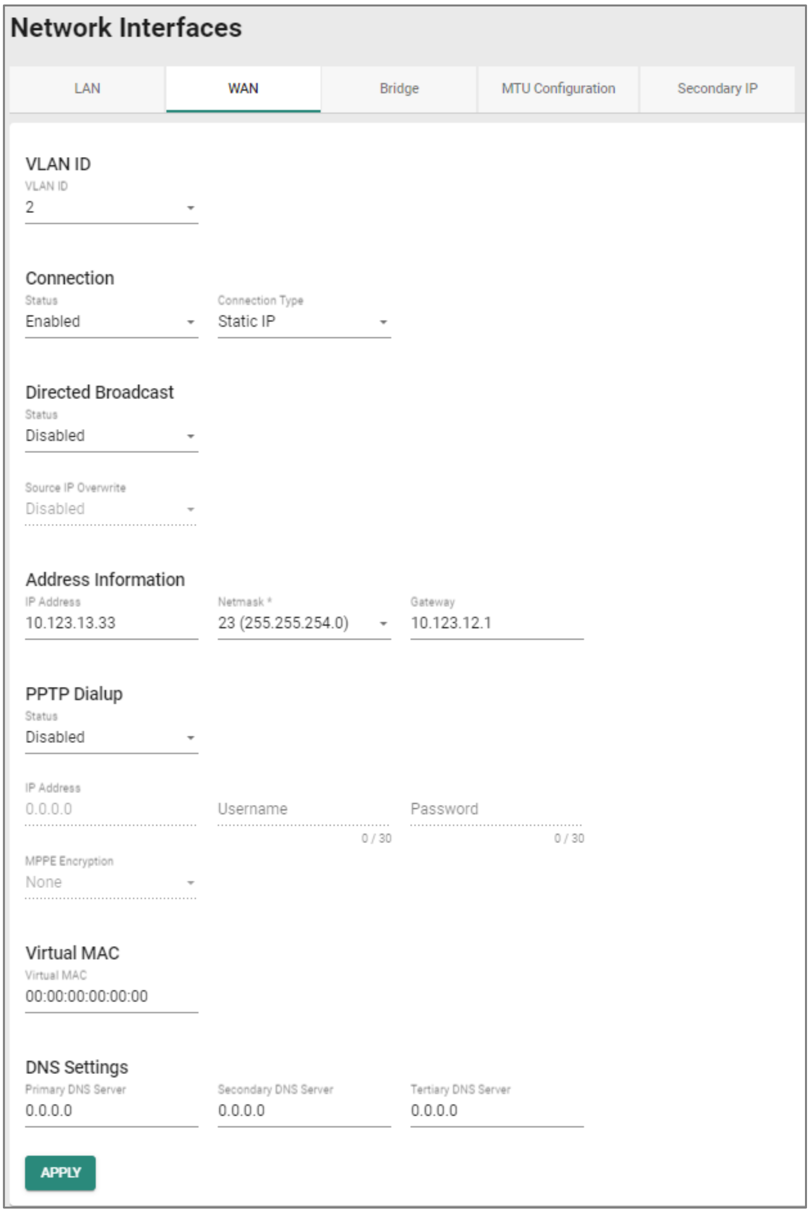
There are multiple types of WAN you can select for your **Connection Type**:

- Static IP

- Dynamic IP
- PPPoE

Static IP

If you select **Static IP** as your **Connection Type**, these settings will appear.



Network Interfaces

VLAN ID

VLAN ID: 2

Connection

Status: Enabled

Connection Type: Static IP

Directed Broadcast

Status: Disabled

Source IP Overwrite: Disabled

Address Information

IP Address: 10.123.13.33

Netmask *: 23 (255.255.254.0)

Gateway: 10.123.12.1

PPTP Dialup

Status: Disabled

IP Address: 0.0.0.0

Username 0 / 30

Password 0 / 30

MPPE Encryption: None

Virtual MAC

Virtual MAC: 00:00:00:00:00:00

DNS Settings

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Tertiary DNS Server: 0.0.0.0

VLAN ID

UI Setting	Description	Valid Range	Default Value
VLAN ID	Select a VLAN ID to use for the WAN interface.	VLAN ID	N/A

Connection

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the WAN interface.	Enabled / Disabled	Enabled
Connection Type	Specify the connection type to use for the connection.	Static IP / Dynamic IP / PPPoE	Dynamic IP

Directed Broadcast

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
Source IP Overwrite	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled

Address Information

UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address for the interface.	Valid IP address	0.0.0.0
Netmask	Specify the subnet mask for the interface.	Valid subnet mask	N/A
Gateway	Specify the gateway address for the interface.	Valid IP address	0.0.0.0

PPTP Dialup

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable PPTP connection for the interface.	Enabled / Disabled	Disabled
IP Address	Specify the PPTP service IP address.	Valid IP address	0.0.0.0
User Name	Enter the username to use for dialing in to the PPTP service.	1 to 30 characters	N/A
Password	Enter the password to use for dialing in to the PPTP service.	1 to 30 characters	N/A
MPPE Encrytion	Enable or disable MPPE encryption.	None / Encrypt	None

Virtual MAC

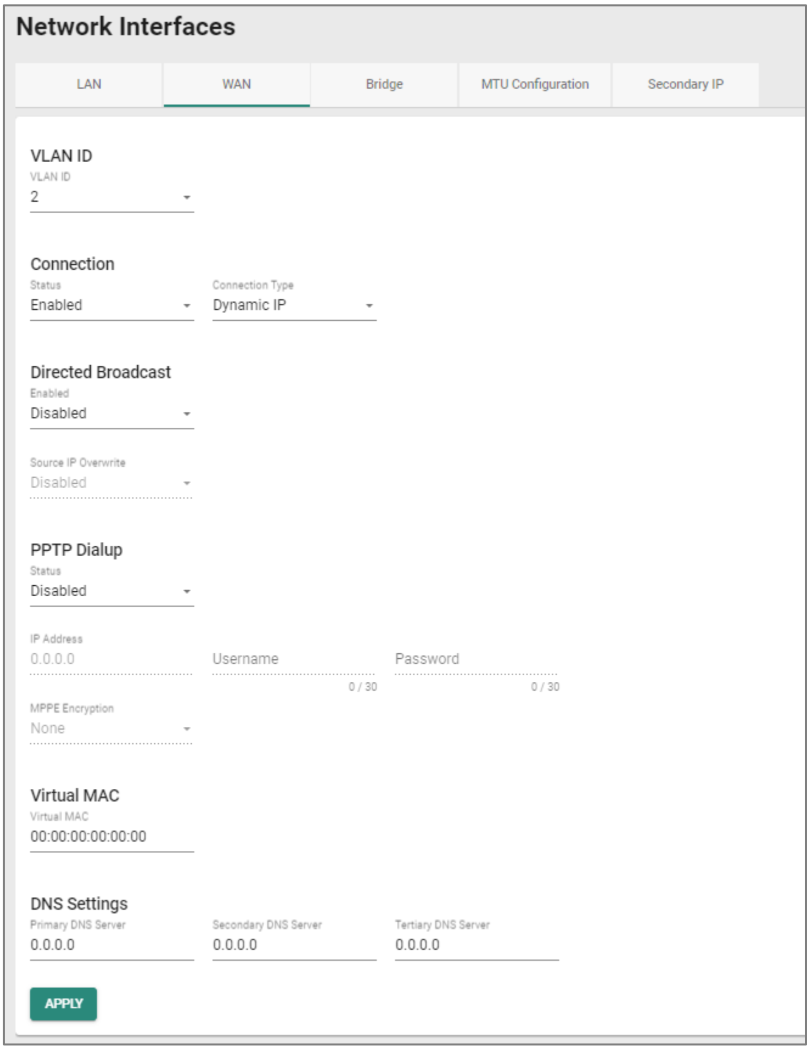
UI Setting	Description	Valid Range	Default Value
Virtual MAC	Specify the virtual MAC address for the interface.	Valid MAC address	00.00.00.00.00.00

DNS Settings

UI Setting	Description	Valid Range	Default Value
Primary DNS Server	Specify the primary DNS IP address.	IP Address	0.0.0.0
Secondary DNS Server	Specify the secondary DNS IP address.	IP Address	0.0.0.0
Tertiary DNS Server	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

Dynamic IP

If you select **Dynamic IP** as your **Connection Type**, these settings will appear.



Network Interfaces

VLAN ID
VLAN ID: 2

Connection
Status: Enabled
Connection Type: Dynamic IP

Directed Broadcast
Enabled: Disabled
Source IP Overwrite: Disabled

PPTP Dialup
Status: Disabled
IP Address: 0.0.0.0
Username 0 / 30
Password 0 / 30
MPPE Encryption: None

Virtual MAC
Virtual MAC: 00:00:00:00:00:00

DNS Settings
Primary DNS Server: 0.0.0.0
Secondary DNS Server: 0.0.0.0
Tertiary DNS Server: 0.0.0.0

VLAN ID

UI Setting	Description	Valid Range	Default Value
VLAN ID	Select a VLAN ID to use for the WAN interface.	VLAN ID	N/A

Connection

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the WAN interface.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Connection Type	Specify the connection type to use for the connection.	Static IP / Dynamic IP / PPPoE	Dynamic IP

Directed Broadcast

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
Source IP Overwrite	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled

PPTP Dialup

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable PPTP connection for the interface.	Enabled / Disabled	Disabled
IP Address	Specify the PPTP service IP address.	Valid IP address	0.0.0.0
User Name	Enter the username to use for dialing in to the PPTP service.	1 to 30 characters	N/A
Password	Enter the password to use for dialing in to the PPTP service.	1 to 30 characters	N/A
MPPE Encrytion	Enable or disable MPPE encryption.	None / Encrypt	None

Virtual MAC

UI Setting	Description	Valid Range	Default Value
Virtual MAC	Specify the virtual MAC address for the interface.	Valid MAC address	00.00.00.00.00.00

DNS Settings

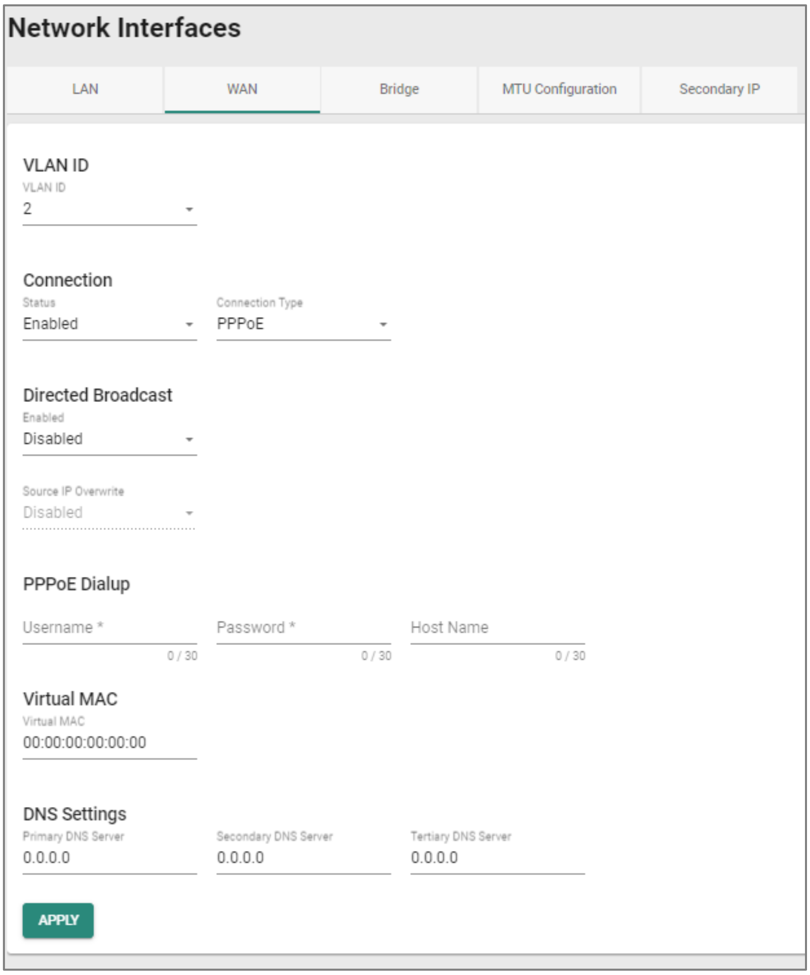
Note

When using Dynamic IP, you can manually configure DNS servers here. Manually configured DNS servers will have a higher priority than DNS servers coming from the DHCP server.

UI Setting	Description	Valid Range	Default Value
Primary DNS Server	Specify the primary DNS IP address.	IP Address	0.0.0.0
Secondary DNS Server	Specify the secondary DNS IP address.	IP Address	0.0.0.0
Tertiary DNS Server	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

PPPoE

If you select **PPPoE** as your **Connection Type**, these settings will appear.



Network Interfaces

VLAN ID
VLAN ID: 2

Connection
Status: Enabled
Connection Type: PPPoE

Directed Broadcast
Enabled: Disabled
Source IP Overwrite: Disabled

PPPoE Dialup
Username * 0 / 30
Password * 0 / 30
Host Name 0 / 30

Virtual MAC
Virtual MAC: 00:00:00:00:00:00

DNS Settings
Primary DNS Server: 0.0.0.0
Secondary DNS Server: 0.0.0.0
Tertiary DNS Server: 0.0.0.0

VLAN ID

UI Setting	Description	Valid Range	Default Value
VLAN ID	Select a VLAN ID to use for the WAN interface.	VLAN ID	N/A

Connection

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the WAN interface.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Connection Type	Specify the connection type to use for the connection.	Static IP / Dynamic IP / PPPoE	Dynamic IP

Directed Broadcast

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
Source IP Overwrite	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled

PPPoE Dialup

UI Setting	Description	Valid Range	Default Value
User Name	Specify the username used to connect to the PPPoE service.	1 to 30 characters	N/A
Password	Specify the password used to connect to the PPPoE service.	1 to 30 characters	N/A
Host Name	Specify the hostname of the PPPoE server.	1 to 30 characters	N/A

Virtual MAC

UI Setting	Description	Valid Range	Default Value
Virtual MAC	Specify the virtual MAC address for the interface.	Valid MAC address	00.00.00.00.00.00

DNS Settings

Note

When using PPPoE, you can manually configure DNS servers here. Manually configured DNS servers will have a higher priority than DNS servers coming from the PPPoE server.

UI Setting	Description	Valid Range	Default Value
Primary DNS Server	Specify the primary DNS IP address.	IP Address	0.0.0.0
Secondary DNS Server	Specify the secondary DNS IP address.	IP Address	0.0.0.0
Tertiary DNS Server	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

Bridge

Menu Path: Network Configuration > Network Interfaces - Bridge

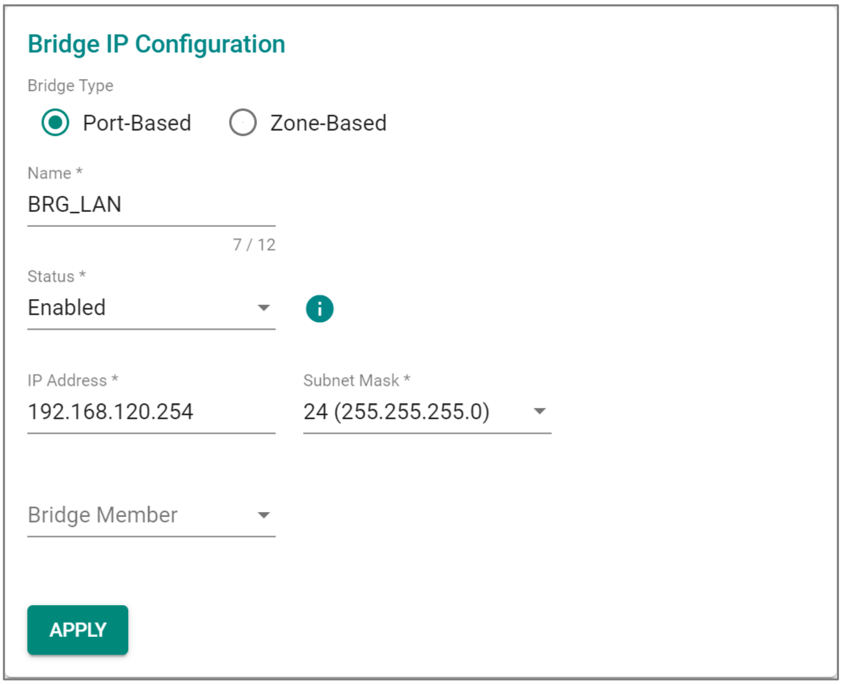
This page lets you configure a bridge for your device.

You can set up these kinds of bridges:

- Port-based
- Zone-based

Port-Based

If you select **Port-Based** as your **Bridge Type**, these settings will appear. Port-based bridges allow the device's firewall to filter traffic moving between bridge member ports.



Bridge IP Configuration

Bridge Type

● Port-Based ○ Zone-Based

Name *
BRG_LAN
7 / 12

Status *
Enabled

IP Address *
192.168.120.254

Subnet Mask *
24 (255.255.255.0)

Bridge Member

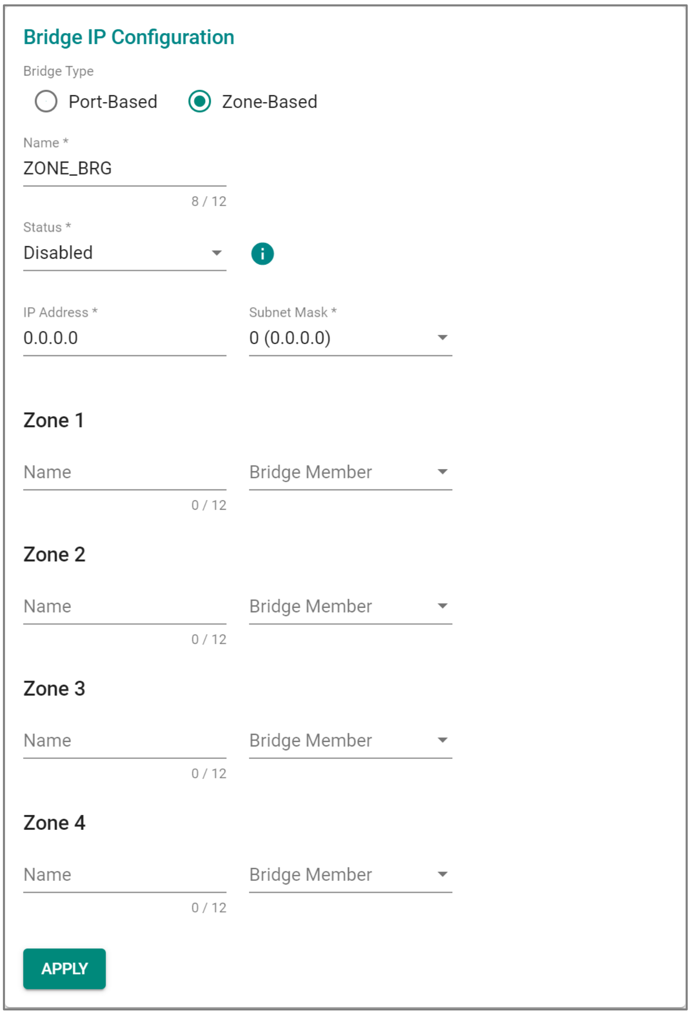
UI Setting	Description	Valid Range	Default Value
Bridge Type	Select which bridge type you want to use.	Port-Based / Zone-Based	N/A
Name	Specify a name for the bridge.	1 to 12 characters	BRG_LAN
Status	Enable or disable the bridge.	Enabled / Disabled	Disabled
IP Address	Specify an IP address for the bridge.	Valid IP address	192.168.126.254
Subnet Mask	Specify a subnet mask for the bridge.	Valid subnet mask	24(255.255.255.0)
Bridge Member	Select which ports will be members of the bridge.	Drop-down list of ports	N/A

Zone-Based

If you select **Zone-Based** as your **Bridge Type**, these settings will appear. Zone-based bridges allow you to create zones based on VLANs. The device's firewall can then filter traffic moving between all ports in a zone.

Limitations

You can create up to 4 different bridge zones.



Bridge IP Configuration

Bridge Type

○ Port-Based ● Zone-Based

Name *

ZONE_BRG

8 / 12

Status *

Disabled

IP Address *

0.0.0.0

Subnet Mask *

0 (0.0.0.0)

Zone 1

Name

0 / 12

Bridge Member

Zone 2

Name

0 / 12

Bridge Member

Zone 3

Name

0 / 12

Bridge Member

Zone 4

Name

0 / 12

Bridge Member

UI Setting	Description	Valid Range	Default Value
Bridge Type	Select which bridge type you want to use.	Port-Based / Zone-Based	N/A
Name	Specify a name for the bridge.	1 to 12 characters	ZONE_BRG
Status	Enable or disable the bridge.	Enabled / Disabled	Disabled
IP Address	Specify an IP address for the bridge.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Subnet Mask	Specify a subnet mask for the bridge.	Valid subnet mask	0 (0.0.0.0)

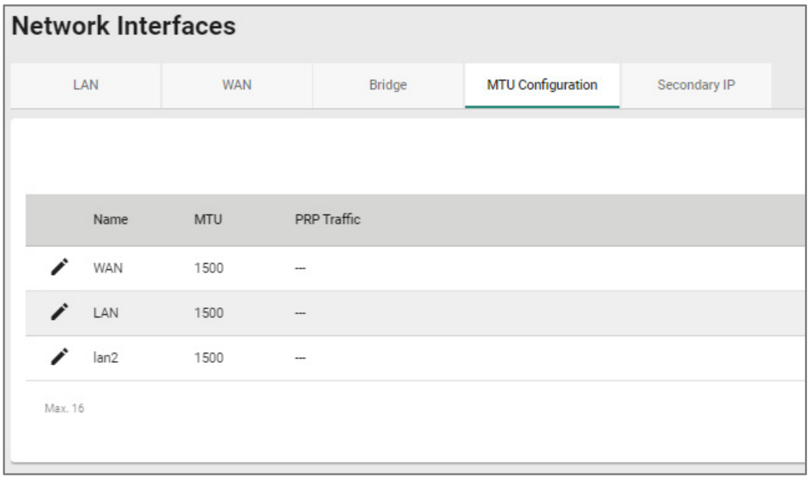
Each zone has the following settings:

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the bridge zone.	1 to 12 characters	N/A
Bridge Member	Select which VLAN will determine the members of this zone.	Drop-down list of VLANs	N/A

MTU Configuration

Menu Path: Network Configuration > Network Interfaces - MTU

This page lets you configure the MTU settings for your interfaces.



	Name	MTU	PRP Traffic
✎	WAN	1500	--
✎	LAN	1500	--
✎	lan2	1500	--

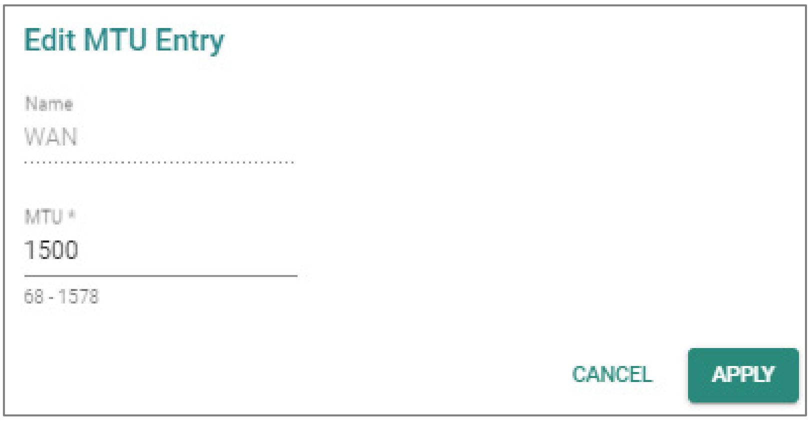
Max. 16

UI Setting	Description
Name	Shows the name of the interface.
MTU	Shows the MTU size used for the interface.
PRP Traffic	Shows the PRP traffic status for the interface.

MTU Configuration - Edit MTU Entry

Menu Path: Network Configuration > Network Interfaces - MTU Configuration

Clicking the **Edit (✎)** icon for an interface on the **Network Configuration > Network Interfaces - MTU Configuration** page will open this dialog box. This dialog lets you edit the MTU settings for an interface. Click **APPLY** to save your changes.



Edit MTU Entry

Name
WAN

MTU *
1500
68 - 1578

UI Setting	Description	Valid Range	Default Value
Name	Shows the name of of this interface. This setting cannot be changed here.	N/A	Name of interface
MTU	Specify the MTU size to use for the interface.	68 to 1578	1500

Secondary IP

Menu Path: Network Configuration > Network Interfaces - Secondary IP

This page lets you create secondary IPs for your interfaces. The Layer 3 interface can act as a secondary IP for a network interface, allowing a single interface to communicate with multiple networks, increasing network flexibility and availability.

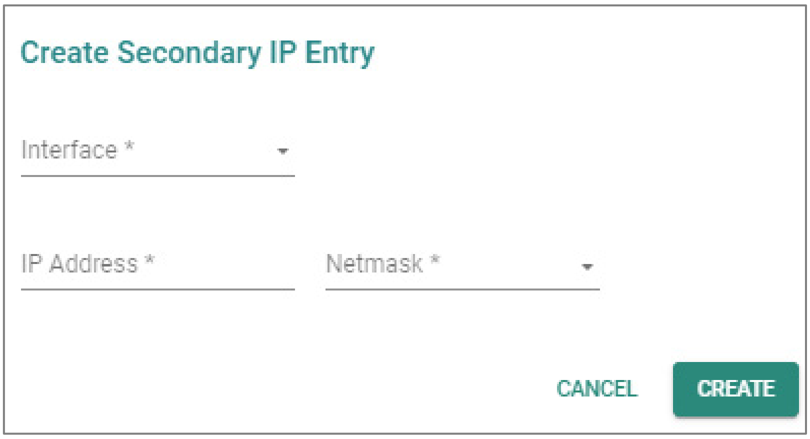
Secondary IP - Create Secondary IP Entry

Menu Path: Network Configuration > Network Interfaces - Secondary IP

Clicking the **Add (⊞)** icon on the **Network Configuration > Network Interfaces - Secondary IP** page will open this dialog box. This dialog lets you create a secondary IP for an interface. Click **CREATE** to save your changes and add the new secondary IP.

Limitations

You can create up to 640 secondary IPs.



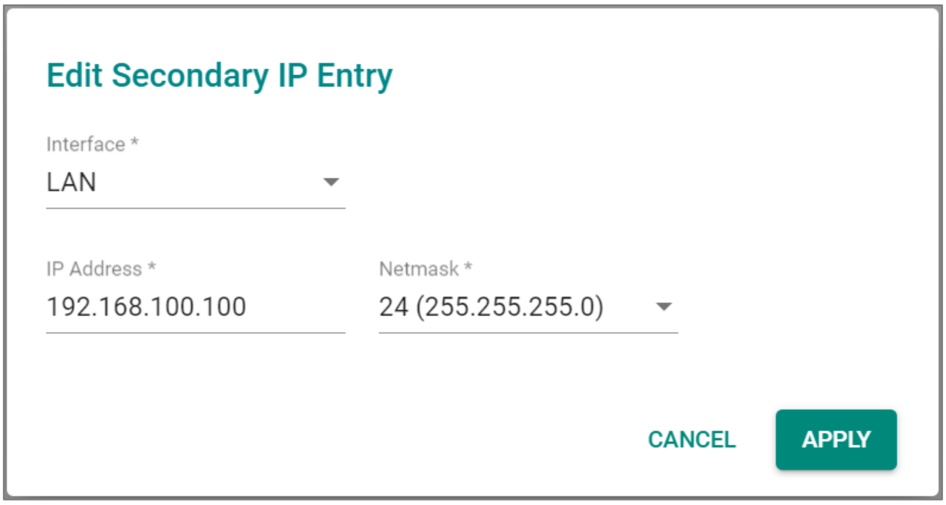
Create Secondary IP Entry

UI Setting	Description	Valid Range	Default Value
Interface	Select which interface the secondary IP is for.	Drop-down list of interfaces	N/A
IP Address	Specify the IP address of the secondary interface.	Valid IP address	N/A
Netmask	Specify the subnet mask of the secondary interface.	Valid netmask	N/A

Secondary IP - Edit Secondary IP Entry

Menu Path: Network Configuration > Network Interfaces - Secondary IP

Clicking the **Edit (✎)** icon on the **Network Configuration > Network Interfaces - LAN** page will open this dialog box. This dialog lets you edit an existing secondary IP entry. Click **SAVE** to save your changes.



Edit Secondary IP Entry

Interface *
LAN

IP Address *
192.168.100.100

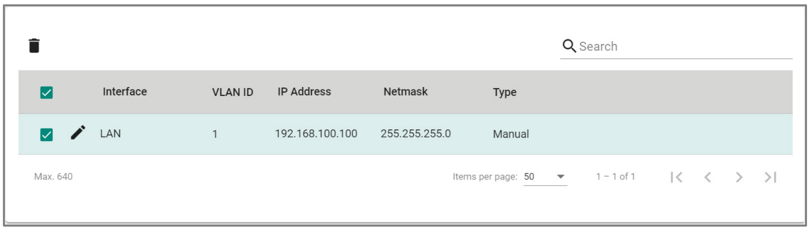
Netmask *
24 (255.255.255.0)

UI Setting	Description	Valid Range	Default Value
Interface	Select which interface the secondary IP is for.	Drop-down list of interfaces	N/A
IP Address	Specify the IP address of the secondary interface.	Valid IP address	N/A
Netmask	Specify the subnet mask of the secondary interface.	Valid netmask	N/A

Delete Secondary IP

Menu Path: Network Configuration > Network Interfaces - Secondary IP

You can delete secondary IP entries by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.



☑	Interface	VLAN ID	IP Address	Netmask	Type
☑	LAN	1	192.168.100.100	255.255.255.0	Manual

Redundancy

Menu Path: Main > Redundancy

The Redundancy settings area lets you configure redundancy settings to help you ensure network availability.

This settings area includes these sections:

- Layer 2 Redundancy
- Layer 3 Redundancy
- VRRP

Redundancy - User Privileges

Privileges to Redundancy settings are granted to the different authority levels as follows. Refer to 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
Layer 3 Redundancy			
VRRP	R/W	R/W	R

Layer 2 Redundancy

Menu Path: Redundancy > Layer 2 Redundancy

This section lets you manage various Layer 2 redundancy features for your device.

This section includes these pages:

- Spanning Tree
- Turbo Ring V2

Spanning Tree

Menu Path: Redundancy > Layer 2 Redundancy > Spanning Tree

This page lets you configure Spanning Tree Protocol (STP) settings for redundancy.

This page includes these tabs:

- General
- Status

Note

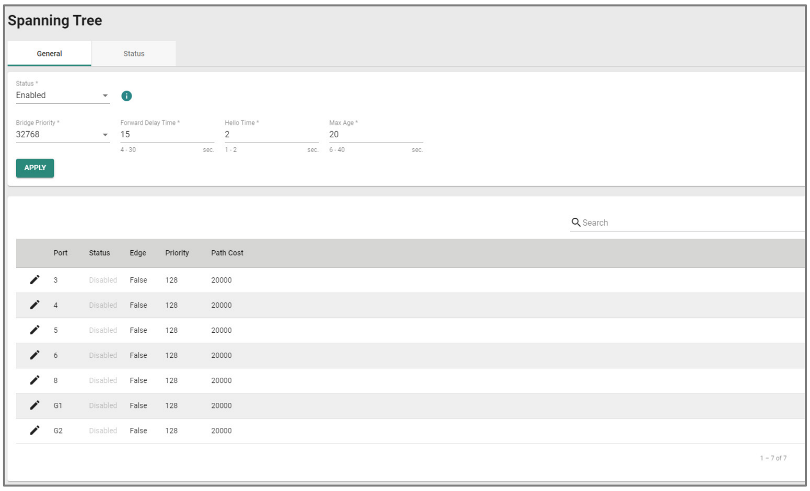
Spanning Tree can only run on the Management VLAN.

Spanning Tree - General

Menu Path: Redundancy > Layer 2 Redundancy > Spanning Tree - General

This page lets you configure spanning tree settings for your device.

Spanning Tree Settings



Spanning Tree

Status *: Enabled

Bridge Priority *: 32768

Forward Delay Time *: 15 (4 - 30 sec.)

Hello Time *: 2 (1 - 2 sec.)

Max Age *: 20 (6 - 40 sec.)

	Port	Status	Edge	Priority	Path Cost
✎	3	Disabled	False	128	20000
✎	4	Disabled	False	128	20000
✎	5	Disabled	False	128	20000
✎	6	Disabled	False	128	20000
✎	8	Disabled	False	128	20000
✎	G1	Disabled	False	128	20000
✎	G2	Disabled	False	128	20000

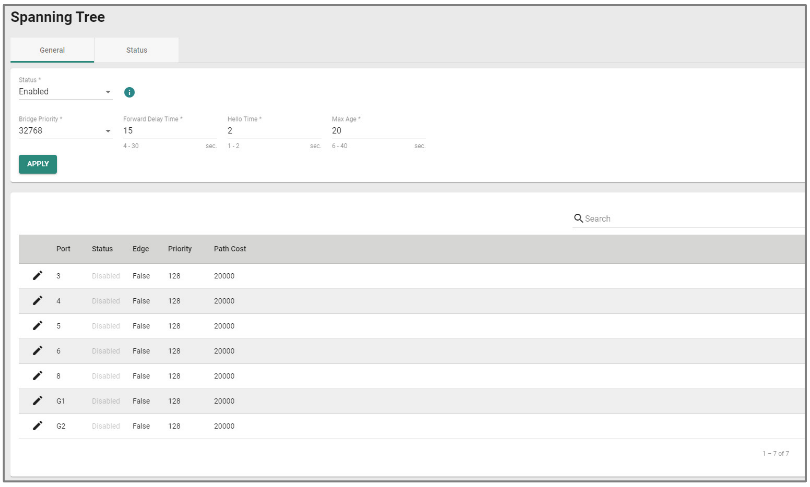
1 – 7 of 7

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable Spanning Tree Protocol for the device.	Enabled / Disabled	Enabled
Bridge Priority	Specify the bridge priority. Lower numbers represent higher priority. A device with a higher bridge priority has a greater chance of being established as the root of the spanning tree topology.	0 to 61440, in multiples of 4096	32768
Forward Delay Time	Specify the forwarding delay time. This is the amount of time this device will wait before checking to see if it should change to a different state.	4 to 30 seconds	15
Hello Time	Specify the interval at which the device, if it is currently the root of the spanning tree topology, will send out periodic “Hello” messages to other devices on the network to check if the topology is healthy.	1 to 2 seconds	2
Max Age	Specify the maximum age duration to wait for a "Hello" message from the root of the spanning tree topology before the device will reconfigure itself as root. If two or more devices on the network are recognized as a root, the devices will negotiate to determine which will act as the new root.	6 to 40 seconds	20

Spanning Tree List

✎ **Note**

We recommend that you disable Spanning Tree Protocol on a port if it is connected to a device (such as a PLC or RTU) instead of network equipment, as this may cause unnecessary negotiation.



Spanning Tree

Status * Enabled

Bridge Priority * 32768

Forward Delay Time * 15 (4 - 30 sec.)

Hello Time * 2 (1 - 2 sec.)

Max Age * 20 (6 - 40 sec.)

Port	Status	Edge	Priority	Path Cost
3	Disabled	False	128	20000
4	Disabled	False	128	20000
5	Disabled	False	128	20000
6	Disabled	False	128	20000
8	Disabled	False	128	20000
G1	Disabled	False	128	20000
G2	Disabled	False	128	20000

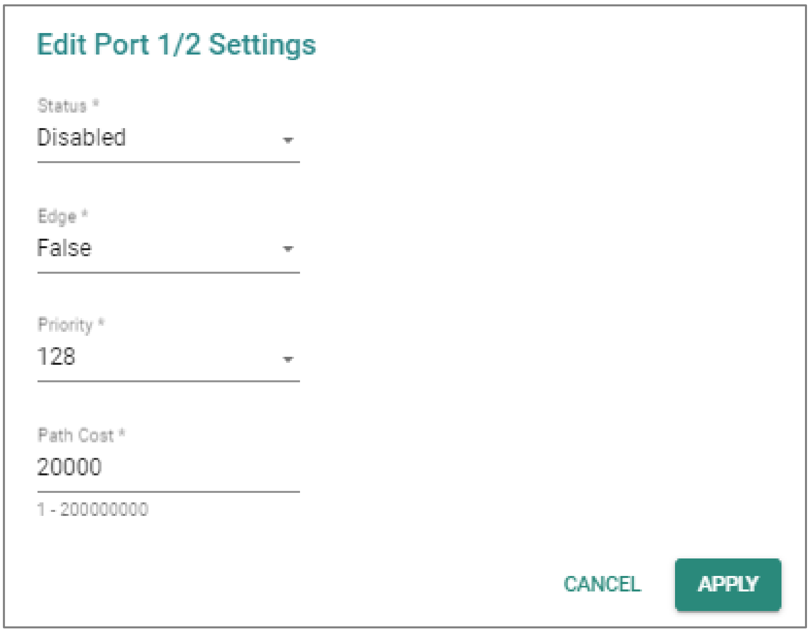
1 – 7 of 7

UI Setting	Description
Port	Shows the port number.
Status	Shows the status of the port as a node in the spanning tree topology.
Edge	Shows whether the port is an edge port or not. **Force Edge**: The port is fixed as an edge port and will always be in the forwarding state. **False**: The port is not an edge port.
Priority	Shows the priority of the port. Lower numbers indicate higher priority.
Path Cost	Shows the path cost for the port. Higher path costs indicate that this port is less suitable as a node for the spanning tree topology. If set to 0, the path cost will be automatically calculated based on different port speeds.

Spanning Tree - Edit Port Settings

Menu Path: Redundancy > Layer 2 Redundancy > Spanning Tree - General

Clicking the **Edit (✎)** icon for an port on the **Redundancy > Layer 2 Redundancy > Spanning Tree - General** page will open this dialog box. This dialog lets you configure the spanning tree settings for a port. Click **APPLY** to save your changes.



Edit Port 1/2 Settings

Status *
Disabled

Edge *
False

Priority *
128

Path Cost *
20000
1 - 200000000

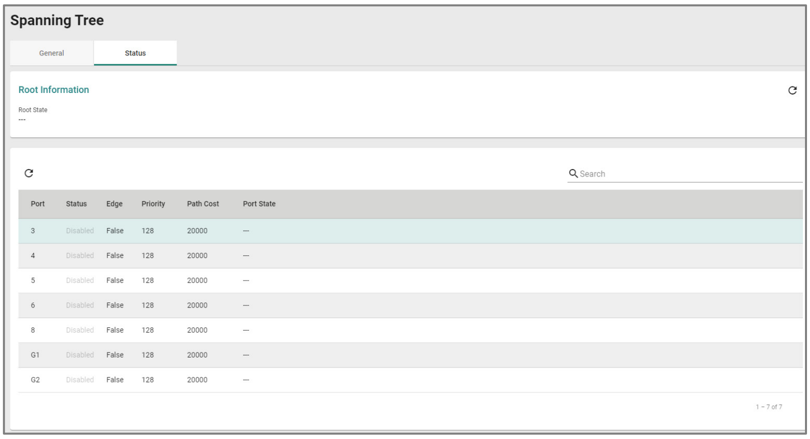
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the port as a node in the spanning tree topology.	Enabled / Disabled	Disabled
Edge	Specify whether the port is an edge port or not. **Force Edge**: The port is fixed as an edge port and will always be in the forwarding state. **False**: The port is not an edge port.	Force Edge / False	False
Priortiy	Specify the priority of the port. Lower numbers indicate higher priority.	0 to 240, in multiples of 16	128
Path Cost	Specify the path cost for the port. Higher path costs indicate that this port is less suitable as a node for the spanning tree topology. If set to 0, the path cost will be automatically calculated based on different port speeds.	1 to 200000000	20000

Spanning Tree - Status

Menu Path: Redundancy > Layer 2 Redundancy > Spanning Tree - Status

This page lets you see the current spanning tree status of your device and its ports.

Root Information



Spanning Tree

Root Information

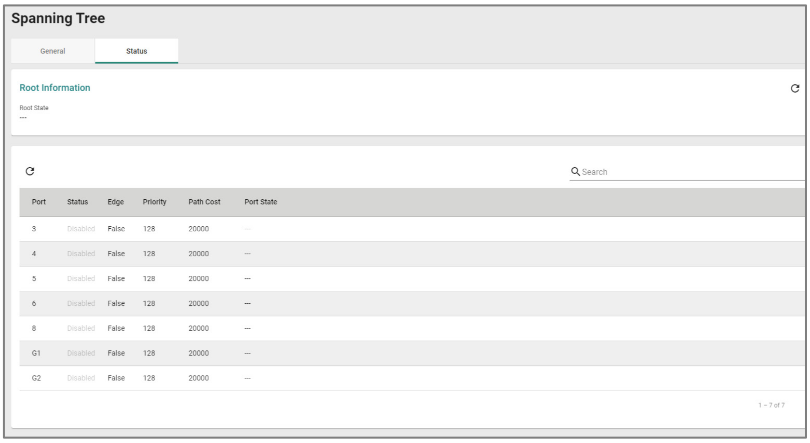
Root State

Port	Status	Edge	Priority	Path Cost	Port State
3	Disabled	False	128	20000	---
4	Disabled	False	128	20000	---
5	Disabled	False	128	20000	---
6	Disabled	False	128	20000	---
8	Disabled	False	128	20000	---
G1	Disabled	False	128	20000	---
G2	Disabled	False	128	20000	---

1 – 7 of 7

UI Setting	Description
Root State	Shows whether the device is currently acting as the root of the spanning tree topology.

Spanning Tree Port List



Spanning Tree

Root Information

Root State

Port	Status	Edge	Priority	Path Cost	Port State
3	Disabled	False	128	20000	---
4	Disabled	False	128	20000	---
5	Disabled	False	128	20000	---
6	Disabled	False	128	20000	---
8	Disabled	False	128	20000	---
G1	Disabled	False	128	20000	---
G2	Disabled	False	128	20000	---

1 – 7 of 7

UI Setting	Description
Port	Shows the port number.
Enable	Shows whether Spanning Tree Protocol is enabled for the port.
Edge	Shows whether the port is an edge port or not. Force Edge: The port is fixed as an edge port and will always be in the forwarding state. **True**: The port is currently designated as an edge port. False: The port is not an edge port.
Priority	Shows the priority of the port. Lower numbers indicate higher priority.
Path Cost	Shows the path cost for the port. Higher path costs indicate that this port is less suitable as a node for the spanning tree topology. If set to 0, the path cost will be automatically calculated based on different port speeds.
Port State	Shows the current spanning tree status of the port. **Forwarding**: Indicates the port is allowing transmissions normally. **Blocking**: Indicates the port is blocking transmissions.

Turbo Ring V2

This page lets you manage the Turbo Ring V2 redundancy feature for your device.

This page includes these tabs:

- General
- Status

Note

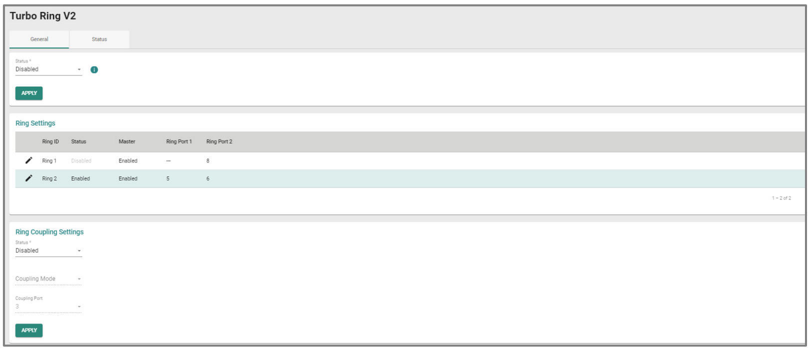
Turbo Ring V2 can only run on the Management VLAN.

Turbo Ring V2 - General

Menu Path: Redundancy > Layer 2 Redundancy > Turbo Ring V2 - General

This page lets you configure the Turbo Ring settings for your device.

Turbo Ring Settings


Turbo Ring V2

Status *: Disabled

Ring Settings

	Ring ID	Status	Master	Ring Port 1	Ring Port 2
✎	Ring 1	Disabled	Enabled	--	8
✎	Ring 2	Enabled	Enabled	5	6

1 – 2 of 2

Ring Coupling Settings

Status *: Disabled

Coupling Mode

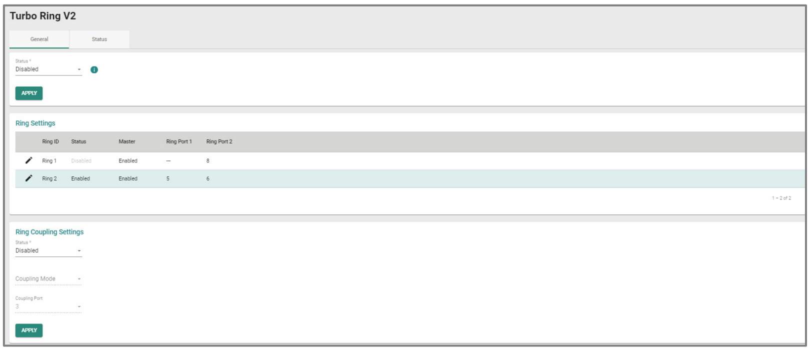
Coupling Port: 3

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable Turbo Ring V2 for the device.	Enabled / Disabled	Disabled

Ring Settings

Note

To set up a Dual-Ring architecture, you must enable both Ring 1 and Ring 2.


Turbo Ring V2

Status *: Disabled

Ring Settings

	Ring ID	Status	Master	Ring Port 1	Ring Port 2
✎	Ring 1	Disabled	Enabled	--	8
✎	Ring 2	Enabled	Enabled	5	6

1 – 2 of 2

Ring Coupling Settings

Status *: Disabled

Coupling Mode

Coupling Port: 3

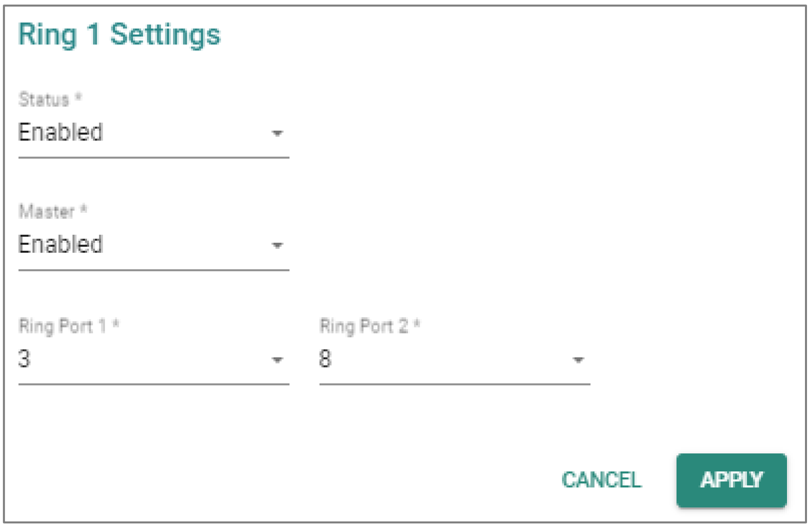
UI Setting	Description
Ring ID	Shows the ring ID.
Status	Shows the status of the ring.

UI Setting	Description
Master	Shows whether this 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.

Turbo Ring V2 - Ring Settings

Menu Path: Redundancy > Layer 2 Redundancy > Turbo Ring V2 - General

Clicking the **Edit (✎)** icon for a ring on the **Redundancy > Layer 2 Redundancy > Turbo Ring V2 - General** page will open this dialog box. This dialog lets you adjust your device's settings for the ring. Click **APPLY** to save your changes.



Ring 1 Settings

Status *
Enabled

Master *
Enabled

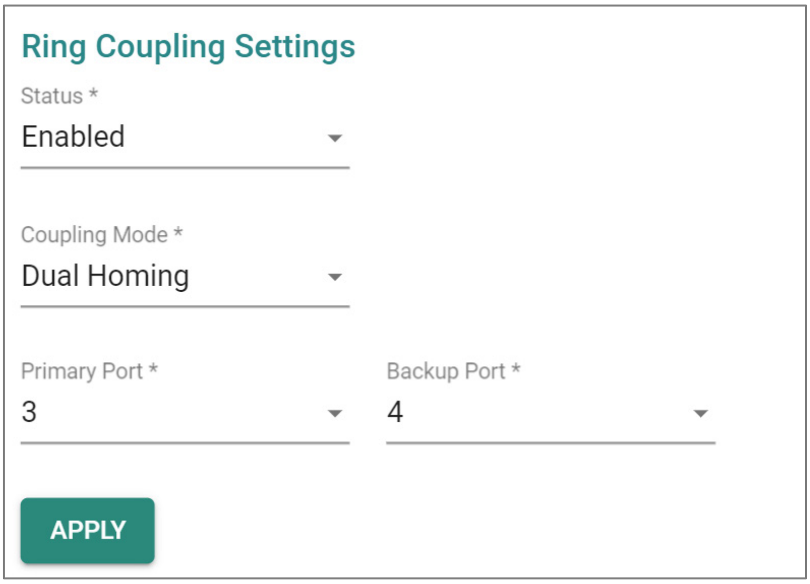
Ring Port 1 *
3

Ring Port 2 *
8

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable Turbo Ring V2 for the device.	Enabled / Disabled	Disabled
Master	Enable or disable whether this device will be designated as the master for the ring.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
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.	Select a port from the drop-down menu	7
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.	Select a port from the drop-down menu	8

Ring Coupling Settings


Ring Coupling Settings

Status *
Enabled

Coupling Mode *
Dual Homing

Primary Port *
3

Backup Port *
4

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable ring coupling for the device.	Enabled / Disabled	Disabled
Coupling Mode **(if Status is Enabled)**	Specify the coupling mode for the device. **Dual Homing**: This device will handle both the primary path and backup path for ring coupling. **Backup Path**: This device only handles the backup path for ring coupling; the primary path will be handled by another device. **Primary Path**: This device only handles the primary path for ring coupling; the backup path will be handled by another device.	Dual Homing / Backup Path / Primary Path	N/A

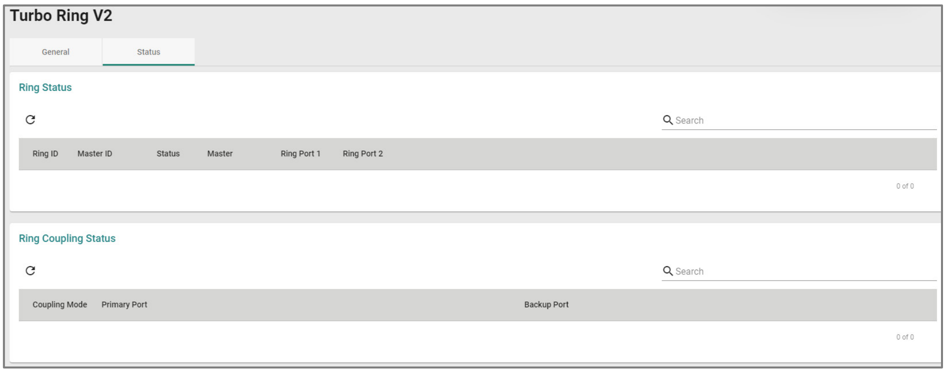
UI Setting	Description	Valid Range	Default Value
Primary Port **(if Coupling Mode is Dual Homing)**	Specify the port that connects to the primary path for ring coupling.	Select a port from the drop-down menu	3
Backup Port **(if Coupling Mode is Dual Homing)**	Specify the port that connects to the backup path for ring coupling.	Select a port from the drop-down menu	N/A
Coupling Port **(if Coupling Mode is Primary Path or Backup Path)**	Specify the prot that connects to primary path or backup path for ring coupling.	Select a port from the drop-down menu	3

Turbo Ring V2 - Status

Menu Path: Redundancy > Layer 2 Redundancy > Turbo Ring V2 - Status

This page lets you see the current status of your rings and ring couplings.

Ring Status



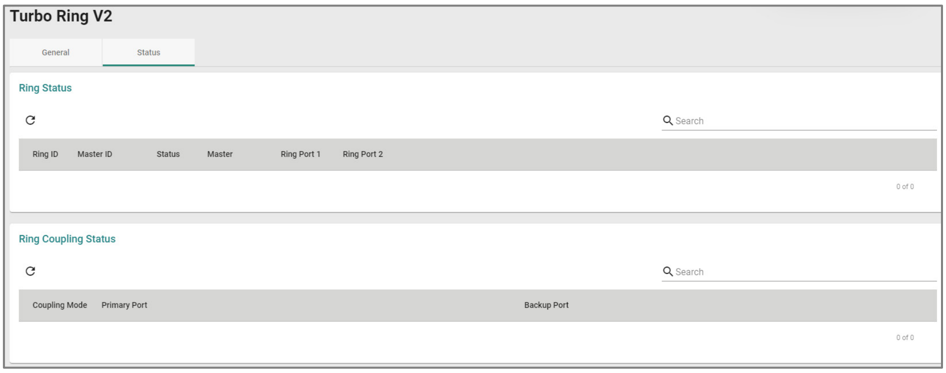
Ring ID	Master ID	Status	Master	Ring Port 1	Ring Port 2

Coupling Mode	Primary Port	Backup Port

UI Setting	Description
Ring ID	Shows the ID number of the ring.
Master ID	Shows the MAC address of the ring master.

UI Setting	Description
Status	Shows the current status of the ring. **Healthy**: The ring and its related ports are working properly. **Break**: One or more rings are broken.
Master	Shows whether this device is acting as a master or slave in the ring.
Ring Port 1	Shows which port is acting as the first ring port.
Ring Port 2	Shows which port is acting as the second ring port.

Ring Coupling Status



Ring Status

Ring ID	Master ID	Status	Master	Ring Port 1	Ring Port 2

0 of 0

Ring Coupling Status

Coupling Mode	Primary Port	Backup Port

0 of 0

UI Setting	Description
Coupling Mode	Shows the mode being used for the ring coupling.
Primary Port	Shows the primary port for the ring coupling.
Backup Port	Shows the backup port for the ring coupling.

Layer 3 Redundancy

Menu Path: Redundancy > Layer 3 Redundancy

This section lets you configure the Layer 3 redundancy features of your device.

This section includes these pages:

- VRRP

VRRP

Menu Path: Redundancy > Layer 3 Redundancy > VRRP

This page lets you configure the VRRP settings for your device.

This page includes these tabs:

- Settings
- Status

VRRP - Settings

Menu Path: Redundancy > Layer 3 Redundancy > VRRP - Settings

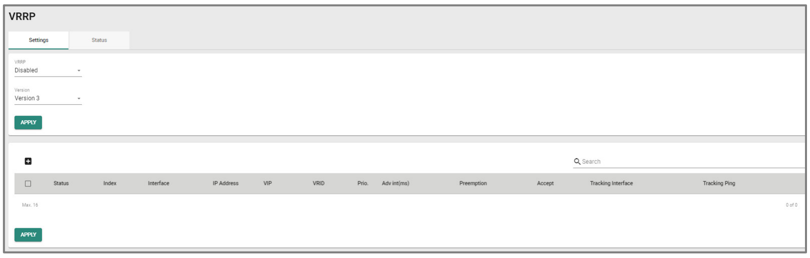
This page lets you configure the VRRP settings for your device.

Virtual Router Redundancy Protocol (VRRP) helps solve some problems with static configurations. VRRP enables a group of routers to form a single virtual router with a virtual IP address. The LAN clients can then be configured with the virtual router's virtual IP address as their default gateway. This virtual router consisting of a group of routers is also known as a VRRP group.

Limitations

You can create up to 16 virtual routers.

VRRP Settings

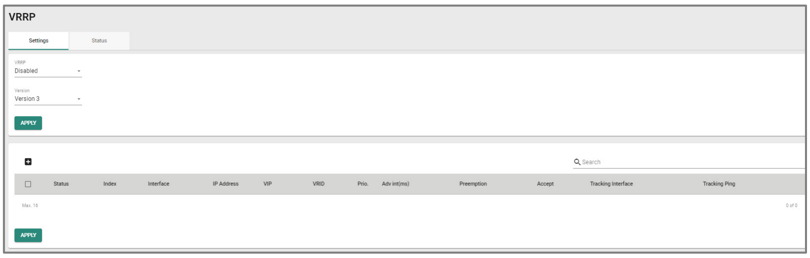


VRRP: Disabled

Version: Version 3

UI Setting	Description	Valid Range	Default Value
VRRP	Enable or disable VRRP for the device.	Enabled / Disabled	Disabled
Version	Select the VRRP version to use.	Version 2 / Version 3	Version 3

VRRP List



VRRP: Disabled

Version: Version 3

UI Setting	Description
Status	Shows the status of the VRRP interface.
Index	Shows the index number used to identify the VRRP interface.
Interface	Shows which network interface is used for the VRRP interface.
IP Address	Shows the IP address of the VRRP interface.
VIP	Shows the virtual router IP address for the VRRP interface.
VRID	Shows the virtual router ID for the VRRP interface, which is used to assign the virtual router to a VRRP group.
Prio.	Shows the priority of the VRRP interface. Higher numbers indicate higher priority, with 254 being the highest.

UI Setting	Description
Adv int(ms)	Shows the advertisement interval for the VRRP interface in milliseconds.
Preemption	Shows the preemption status of the VRRP interface.
Accept	Shows whether Accept Mode is enabled for the VRRP interface. When enabled, the virtual router designated as the master will allow others to access its own virtual IP address.
Tracking Interface	Shows whether Native Interface Tracking is enabled for the VRRP interface.
Tracking Ping	Shows the tracking ping status of the VRRP interface.

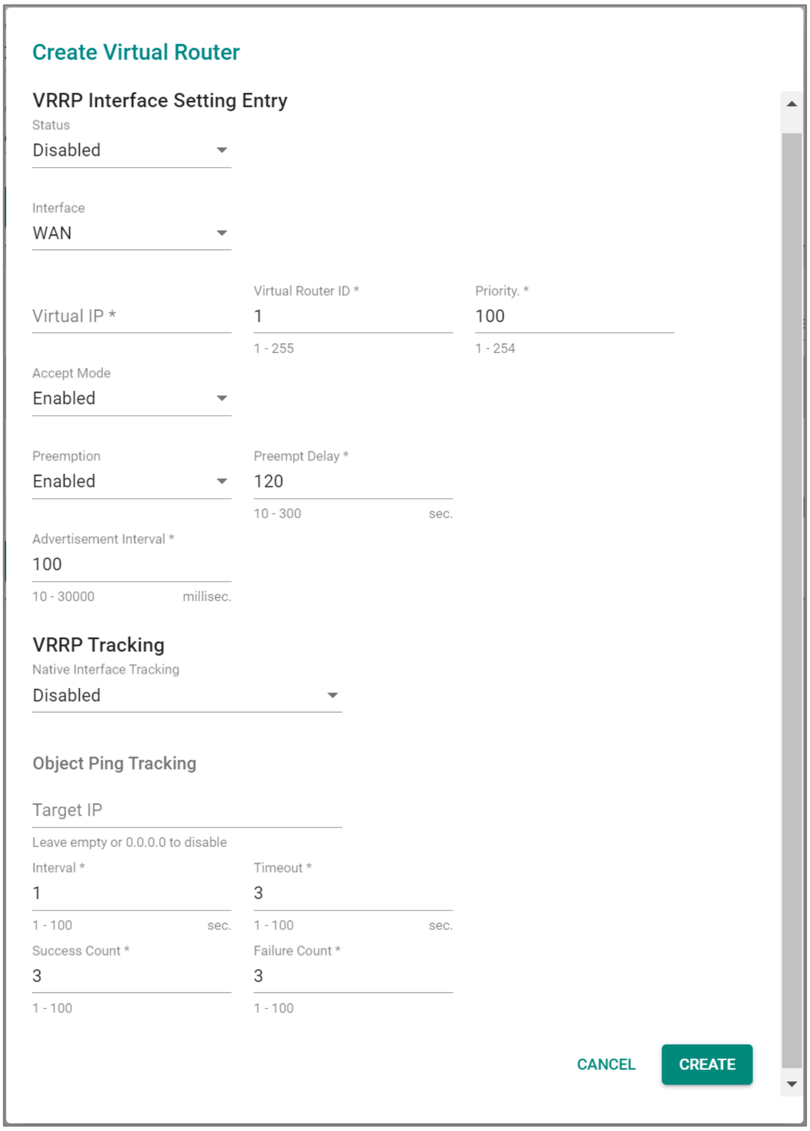
VRRP - Create Virtual Router

Menu Path: Redundancy > Layer 3 Redundancy > VRRP - Settings

Clicking the **Add (**⊞**)** icon on the **Redundancy > Layer 3 Redundancy > VRRP - Settings** page will open this dialog box. This dialog lets you create a new virtual router for your device. Click **CREATE** to save your changes and add the new account.

Limitations

You can create up to 16 virtual routers.



Create Virtual Router

VRRP Interface Setting Entry

Status: Disabled

Interface: WAN

Virtual IP *

Virtual Router ID *: 1 (1 - 255)

Priority. *: 100 (1 - 254)

Accept Mode: Enabled

Preemption: Enabled

Preempt Delay *: 120 (10 - 300 sec.)

Advertisement Interval *: 100 (10 - 30000 millisec.)

VRRP Tracking

Native Interface Tracking: Disabled

Object Ping Tracking

Target IP (Leave empty or 0.0.0.0 to disable)

Interval *: 1 (1 - 100 sec.)

Timeout *: 3 (1 - 100 sec.)

Success Count *: 3 (1 - 100)

Failure Count *: 3 (1 - 100)

VRRP Interface Setting Entry

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the VRRP interface.	Enabled / Disabled	Disabled
Interface	Specify which network interface to use for the VRRP interface.	Drop-down list of interfaces	

UI Setting	Description	Valid Range	Default Value
Virtual IP	Specify the virtual router IP address for the VRRP interface. ✎ **Note** Devices in the same VRRP group must be in the same subnet.	Valid IP address	N/A
Virtual Router ID	Specify the virtual router ID to use for the VRRP interface. The virtual router ID is used to assign the virtual router to a VRRP group. ✎ **Note** Devices that operate as master/backup should have the same ID. Each interface supports one virtual router ID.	1-255	1
Priority	Specify the priority of the VRRP interface. Higher numbers indicate higher priority, with 254 being the highest. ✎ **Note** If multiple devices have the same priority, the device with the highest IP address will have priority.	1-254	100
Accept Mode	Enable or disable Accept Mode for the VRRP interface. When enabled, the virtual router designated as the master will allow others to access its own virtual IP address.	Enabled / Disabled	Enabled
Preemption	Enable or disable preemption for the VRRP interface. When enabled, preemption will decide if the master will retake authority or not after being unavailable.	Enabled / Disabled	Enabled
Preempt Delay **(if Preemption is Enabled)**	Specify the preemption delay in seconds to use for the VRRP interface. The preempt delay is the amount of time the master will wait before retaking authority back in order to prevent the master from acting before the network connection is ready.	10-300 sec	120
Advertisement Interval	Specify the advertisement interval in milliseconds for the VRRP interface. This determines the interval for the master sending packets to all slave devices to inform them who the master device is.	10-30000 ms	100

VRRP Tracking

✎ **Note**

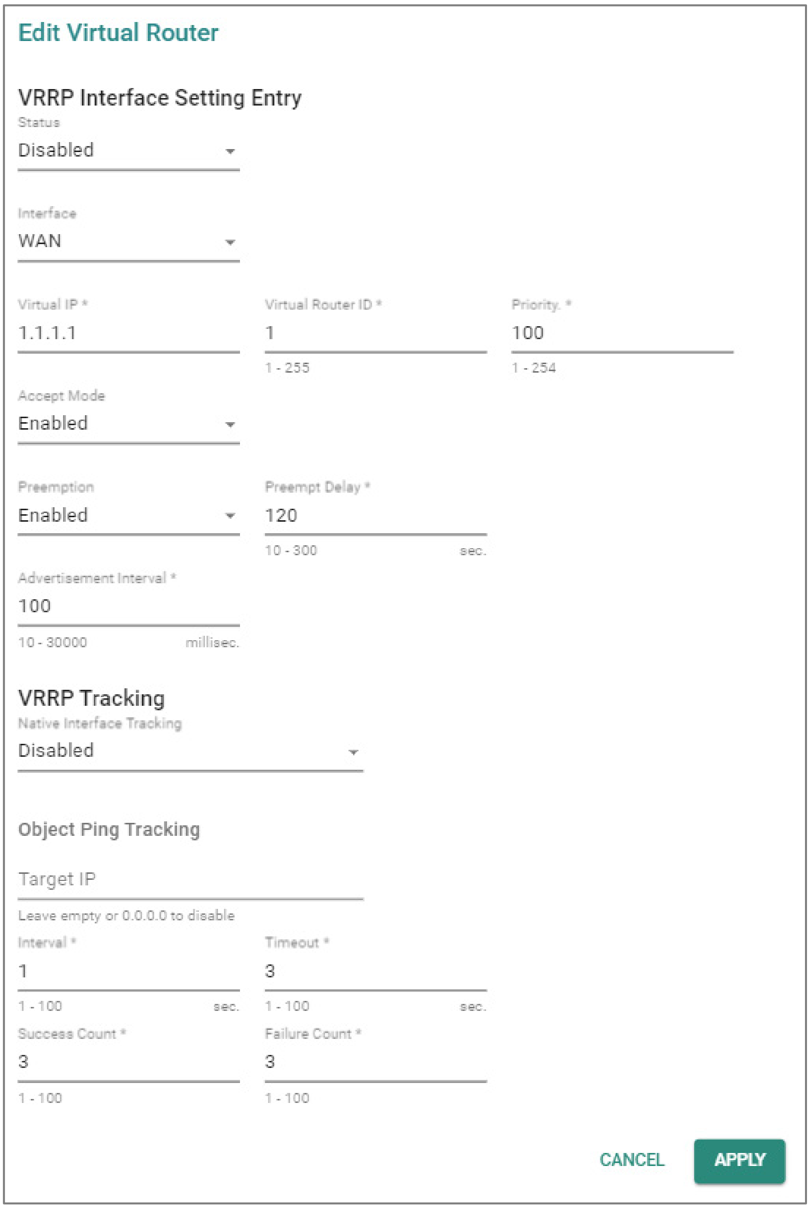
If either Native Interface Tracking or Object Ping Tracking determines a connection failure, the VRRP status will be switched to INIT mode.

UI Setting	Description	Valid Range	Default Value
Native Tracking Interface	Disable or specify which interface to use for Native Interface Tracking for the VRRP interface. When enabled, if all interfaces on the device are disconnected, it will be considered to be a disconnection.	Disabled / Drop-down list of interfaces	Disabled
Target IP	Specify the target IP to ping to verify if the connection to the destination is working. Leaving this field empty or entering 0.0.0.0 will disable object ping tracking for the VRRP interface. ✎ **Note** Moxa devices will decide which interface/source IP to use for pinging the target IP based on the routing table.	Valid IP address	N/A
Interval	Specify the interval in seconds the device will use for pinging the target IP.	1-100 sec	1
Timeout	Specify the timeout duration in seconds the device will wait for a response before timing out.	1-100 sec	3
Success Count	Specify the success count, which indicates how many responses the device must receive to consider the connection as working.	1-100	3
Failure Count	Specify the failure count, which indicates how many times the target IP fails to respond before the device considers the connection as not working.	1-100	3

VRRP - Edit Virtual Router

Menu Path: Redundancy > Layer 3 Redundancy > VRRP - Settings

Clicking the **Edit (✎)** icon for a VRRP interface on the **Redundancy > Layer 3 Redundancy > VRRP - Settings** page will open this dialog box. This dialog lets you edit an existing virtual router. Click **APPLY** to save your changes.



Edit Virtual Router

VRRP Interface Setting Entry

Status: Disabled

Interface: WAN

Virtual IP *: 1.1.1.1

Virtual Router ID *: 1 (1 - 255)

Priority. *: 100 (1 - 254)

Accept Mode: Enabled

Preemption: Enabled

Preempt Delay *: 120 (10 - 300 sec.)

Advertisement Interval *: 100 (10 - 30000 millisec.)

VRRP Tracking

Native Interface Tracking: Disabled

Object Ping Tracking

Target IP (Leave empty or 0.0.0.0 to disable)

Interval *: 1 (1 - 100 sec.)

Timeout *: 3 (1 - 100 sec.)

Success Count *: 3 (1 - 100)

Failure Count *: 3 (1 - 100)

VRRP Interface Setting Entry

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the VRRP interface.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Interface	Specify which network interface to use for the VRRP interface.	Drop-down list of interfaces	
Virtual IP	Specify the virtual router IP address for the VRRP interface. ✎ **Note** Devices in the same VRRP group must be in the same subnet.	Valid IP address	N/A
Virtual Router ID	Specify the virtual router ID to use for the VRRP interface. The virtual router ID is used to assign the virtual router to a VRRP group. ✎ **Note** Devices that operate as master/backup should have the same ID. Each interface supports one virtual router ID.	1-255	1
Priority	Specify the priority of the VRRP interface. Higher numbers indicate higher priority, with 254 being the highest. ✎ **Note** If multiple devices have the same priority, the device with the highest IP address will have priority.	1-254	100
Accept Mode	Enable or disable Accept Mode for the VRRP interface. When enabled, the virtual router designated as the master will allow others to access its own virtual IP address.	Enabled / Disabled	Enabled
Preemption	Enable or disable preemption for the VRRP interface. When enabled, preemption will decide if the master will retake authority or not after being unavailable.	Enabled / Disabled	Enabled
Preempt Delay **(if Preemption is Enabled)**	Specify the preemption delay in seconds to use for the VRRP interface. The preempt delay is the amount of time the master will wait before retaking authority back in order to prevent the master from acting before the network connection is ready.	10-300 sec	120
Advertisement Interval	Specify the advertisement interval in milliseconds for the VRRP interface. This determines the interval for the master sending packets to all slave devices to inform them who the master device is.	10-30000 ms	100

VRRP Tracking

Note

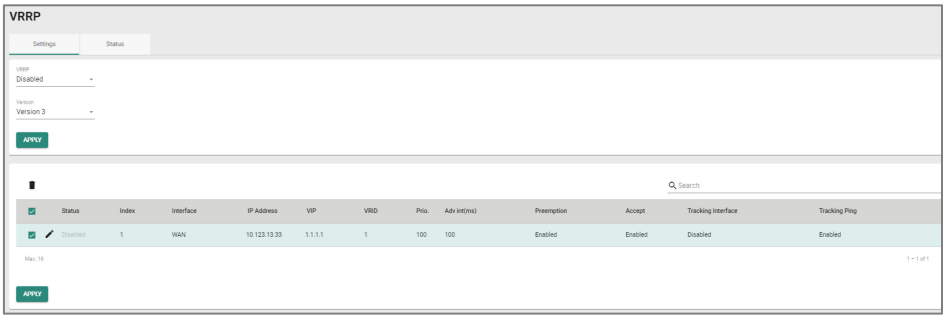
If either Native Interface Tracking or Object Ping Tracking determines a connection failure, the VRRP status will be switched to INIT mode.

UI Setting	Description	Valid Range	Default Value
Native Tracking Interface	Disable or specify which interface to use for Native Interface Tracking for the VRRP interface. When enabled, if all interfaces on the device are disconnected, it will be considered to be a disconnection.	Disabled / Drop-down list of interfaces	Disabled
Target IP	Specify the target IP to ping to verify if the connection to the destination is working. Leaving this field empty or entering 0.0.0.0 will disable object ping tracking for the VRRP interface. **Note** Moxa devices will decide which interface/source IP to use for pinging the target IP based on the routing table.	Valid IP address	N/A
Interval	Specify the interval in seconds the device will use for pinging the target IP.	1-100 sec	1
Timeout	Specify the timeout duration in seconds the device will wait for a response before timing out.	1-100 sec	3
Success Count	Specify the success count, which indicates how many responses the device must receive to consider the connection as working.	1-100	3
Failure Count	Specify the failure count, which indicates how many times the target IP fails to respond before the device considers the connection as not working.	1-100	3

Delete Virtual Router

Menu Path: Redundancy > Layer 3 Redundancy > VRRP - Settings

You can delete VRRP interfaces by using the checkboxes to select the interfaces you want to delete, then clicking the **Delete (🗑)** icon.



VRRP: Disabled

Version: Version 3

☑		Status	Index	Interface	IP Address	VIP	VRID	Prio.	Adv int(ms)	Preemption	Accept	Tracking Interface	Tracking Ping
☑	✎	Disabled	1	WAN	10.123.13.33	1.1.1.1	1	100	100	Enabled	Enabled	Disabled	Enabled

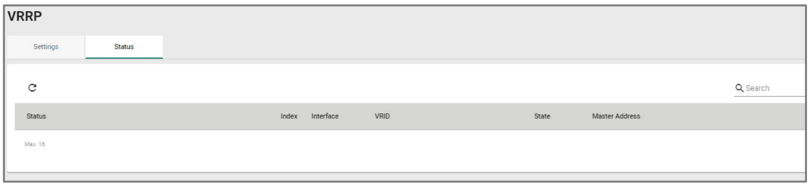
Max. 16

1 – 1 of 1

VRRP - Status

Menu Path: Redundancy > Layer 3 Redundancy > VRRP - Status

This page lets you see the status of your device's VRRP interfaces.



Status	Index	Interface	VRID	State	Master Address

Max. 16

UI Setting	Description
Status	Shows the status of the VRRP interface.
Index	Shows the index number used to identify the VRRP interface.
Interface	Shows which network interface is used for the VRRP interface.
VRID	Shows the virtual router ID for the VRRP interface, which is used to assign the virtual router to a VRRP group.
State	Shows the state of the VRRP interface. **Init State**: This is the initial state when a virtual router starts up. **Master State**: The virtual router is acting as a master, and is responsible for forwarding packets sent to the virtual IP address and acting as the default gateway for the devices in the network. **Backup State**: The virtual router is in the backup state, and waiting to take over the master role if the current master fails.
Master Address	Shows IP address of the current master for the VRRP interface.

Network Service

Menu Path: Network Service

The Network Service settings area lets you configure the main system settings for your device.

This settings area includes these sections:

- DHCP Server
- Dynamic DNS

Network Service - User Privileges

Privileges to Network Service 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
Dynamic DNS	R/W	R/W	R

DHCP Server

Menu Path: Network Service > DHCP Server

This page lets you manage the DHCP server settings of your device.

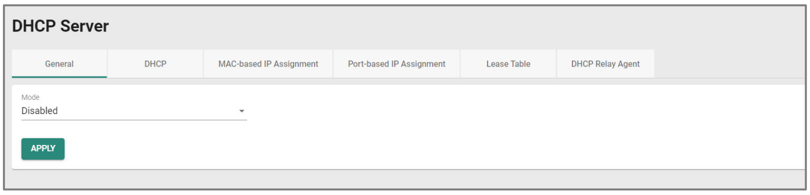
- This page includes these tabs:
- General

- DHCP
- MAC-based IP Assignment
- Port-based IP Assignment
- Lease Table
- DHCP Relay Agent

DHCP Server - General

Menu Path: Network Service > DCHP Server - General

This page lets you enable the DHCP server feature of your device. Click **APPLY** to save your changes.



Mode
Disabled

UI Setting	Description	Valid Range	Default Value
Mode	Select the DHCP Server Mode. Each mode has its own configuration settings.	Disabled / DHCP / MAC-based assignment / Port-based IP assignment	Disabled

DHCP

Menu Path: Network Service > DHCP Server - DHCP

This page lets you set up your device's DHCP server settings to automatically assign an IP address from a user-configured IP address pool to connected Ethernet devices.

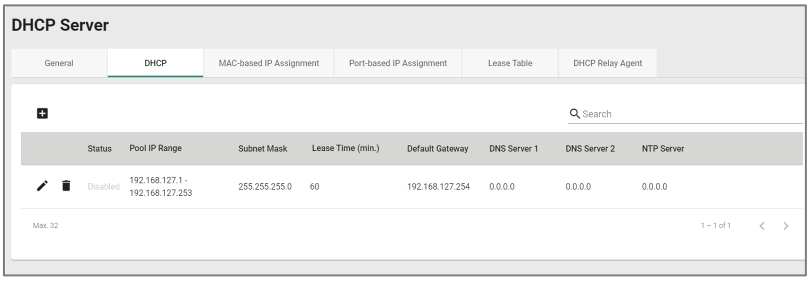
Note

The DHCP Server is only available for LAN interfaces. The DHCP pool’s Starting/Ending IP Address must be in the same LAN subnet.

Limitations

You can create up to 32 DHCP server pools.

DHCP Server Pools



DHCP Server

	Status	Pool IP Range	Subnet Mask	Lease Time (min.)	Default Gateway	DNS Server 1	DNS Server 2	NTP Server
	Disabled	192.168.127.1 - 192.168.127.253	255.255.255.0	60	192.168.127.254	0.0.0.0	0.0.0.0	0.0.0.0

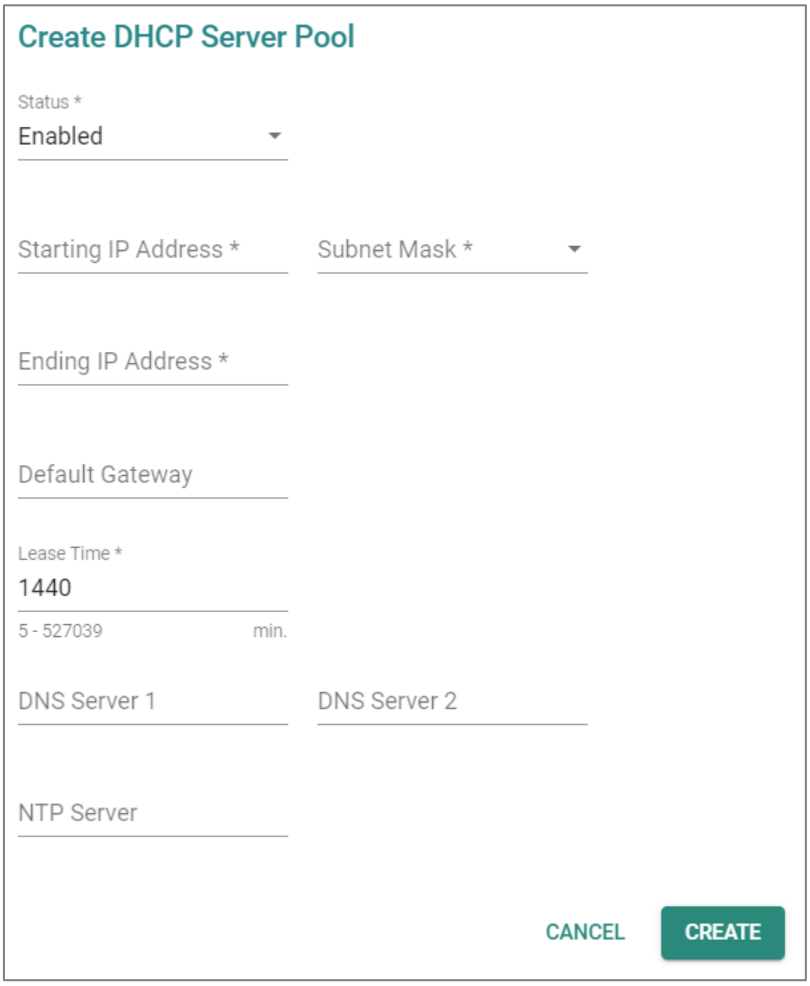
Max. 32

1 – 1 of 1

UI Setting	Description
Status	Shows the status of the DHCP server pool.
Pool IP Range	Shows the IP range of the pool.
Subnet Mask	Shows the subnet mask to use for DHCP clients in the pool.
Lease Time	Shows the lease time to use for IP addresses assigned by the DHCP server for the pool.
DNS Server 1	Shows the IP address to use for the first DNS server for DHCP clients in the pool.
DNS Server 2	Shows the IP address to use for the second DNS server for DHCP clients in the pool.
NTP Server	Shows the IP address to use for the NTP server for DHCP clients in the pool.

DHCP - Create DHCP Server Pool

Menu Path: Network Service > DHCP Server - DHCP Clicking the **Add (** ⊞ **)** icon on the **Network Service > DHCP Server - DHCP** page will open this dialog box. This dialog lets you create a new DHCP server pool. Click **CREATE** to save your changes and add the new account.



Create DHCP Server Pool

Status *
Enabled

Starting IP Address *

Subnet Mask *

Ending IP Address *

Default Gateway

Lease Time *
1440
5 - 527039 min.

DNS Server 1

DNS Server 2

NTP Server

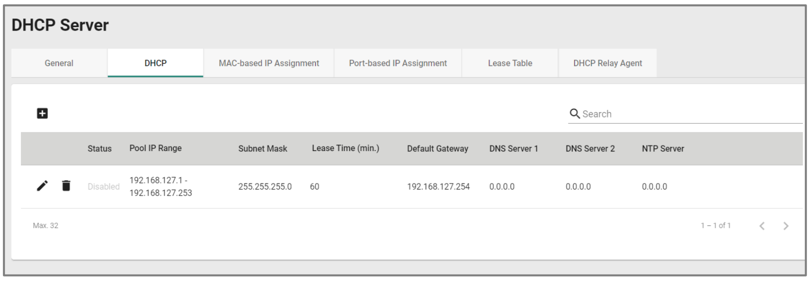
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable DHCP server functionality.	Enabled / Disabled	N/A
Starting IP Address	Specify the starting IP address of the DHCP IP pool.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask for DHCP clients in the pool.	Valid subnet mask	N/A
Ending IP Address	Specify the ending IP address of the DHCP IP pool.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
Default Gateway	Specify the default gateway to use for DHCP clients in the pool.	Valid IP address	N/A
Lease Time	Specify the lease time to use for IP addresses assigned to DHCP clients in the pool.	5 - 527039 minutes	1440
DNS Server 1	Specify the IP address to use for the first DNS server for DHCP clients in the pool.	Valid IP address	N/A
DNS Server 2	Specify the IP address to use for the second DNS server for DHCP clients in the pool.	Valid IP address	N/A
NTP Server	Specify the IP address to use for the NTP server for DHCP clients in the pool.	Valid IP address	N/A

DHCP - Delete DHCP Server Pool

Menu Path: Network Service > DHCP Server - DHCP

You can delete a DHCP server pool by clicking the **Delete (🗑)** icon for the pool.



	Status	Pool IP Range	Subnet Mask	Lease Time (min.)	Default Gateway	DNS Server 1	DNS Server 2	NTP Server
✎ 🗑	Disabled	192.168.127.1 - 192.168.127.253	255.255.255.0	60	192.168.127.254	0.0.0.0	0.0.0.0	0.0.0.0

Max. 32

1 – 1 of 1

DHCP Server - MAC-based IP Assignment

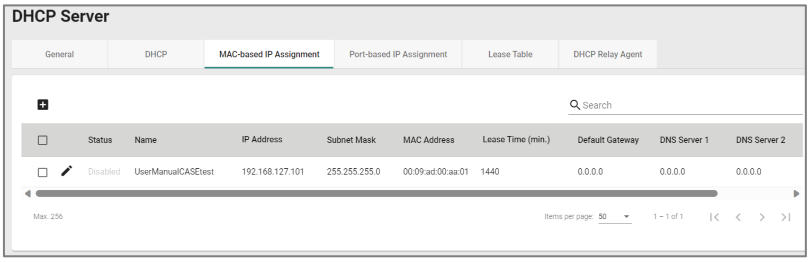
Menu Path: Network Service > DHCP Server - MAC-based IP Assignment

This page lets you manage the DHCP server's MAC-based IP assignments.

MAC-based IP assignment is a method of managing IP address allocation on a DHCP server by associating specific IP addresses with the unique MAC addresses of devices on a network. This approach allows network administrators to ensure that certain devices always receive the same IP address, regardless of their connection order or lease duration. By configuring the DHCP server with a table of MAC addresses and their corresponding IP addresses, administrators can have greater control over IP address allocation and enhance network security and management.

Limitations

You can create up to 256 MAC-based IP assignments.



□		Status	Name	IP Address	Subnet Mask	MAC Address	Lease Time (min.)	Default Gateway	DNS Server 1	DNS Server 2
□	✎	Disabled	UserManualCASEtest	192.168.127.101	255.255.255.0	00:09:ad:00:aa:01	1440	0.0.0.0	0.0.0.0	0.0.0.0

UI Setting	Description
Status	Shows the status of the MAC-based IP assignment.
Name	Shows the hostname for the device.
IP Address	Shows the IP address of the device.
Subnet Mask	Shows the subnet mask of the device.
MAC Address	Shows the MAC address of the device.
Default Gateway	Shows the default gateway of the device.
Lease Time	Shows the lease time for IP addresses assigned by the DHCP server.
DNS Server 1	Shows the IP address for the first DNS server.
DNS Server 2	Shows the IP address for the second DNS server.
NTP Server	Shows the IP address for the NTP server.

MAC-based IP Assignment - Create Entry

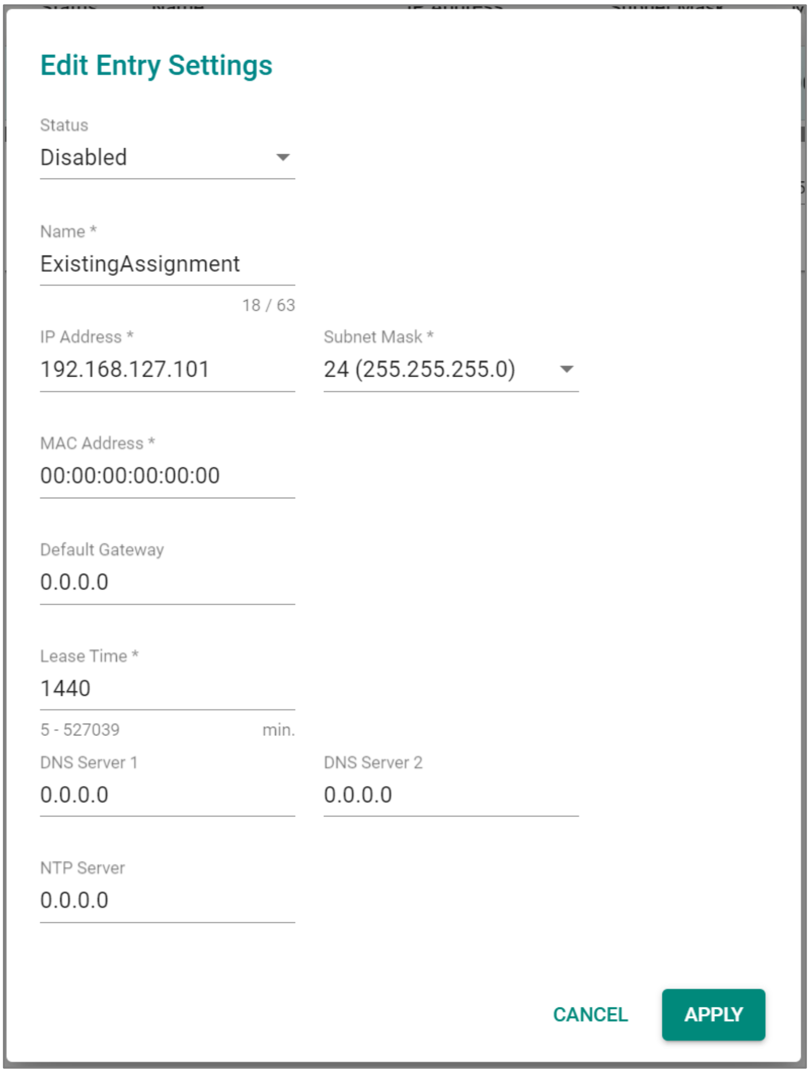
Menu Path: Network Service > DHCP Server - MAC-based IP Assignment

Clicking the **Add (⊞)** icon on the **Network Service > DHCP Server - MAC-based IP Assignment** page will open this dialog box. This dialog lets you add a new MAC-based IP assignment. Click **CREATE** to save your changes and add the new assignment.

MAC-based IP Assignment - Edit Entry

Menu Path: Network Service > DHCP Server - MAC-based IP Assignment

Clicking the **Edit (✎)** icon for an assignment on the **Network Service > DHCP Server - MAC-based IP Assignment** page will open this dialog box. This dialog lets you edit an existing IP assignment. Click **APPLY** to save your changes.



Edit Entry Settings

Status
Disabled

Name *
ExistingAssignment
18 / 63

IP Address *
192.168.127.101

Subnet Mask *
24 (255.255.255.0)

MAC Address *
00:00:00:00:00:00

Default Gateway
0.0.0.0

Lease Time *
1440
5 - 527039 min.

DNS Server 1
0.0.0.0

DNS Server 2
0.0.0.0

NTP Server
0.0.0.0

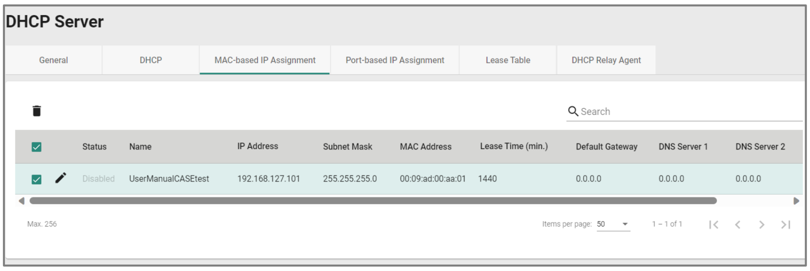
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this MAC-based IP assignment.	Enabled / Disabled	N/A
Name	Enter a hostname for the IP assignment.	Max. 63 characters	N/A
IP Address	Specify the IP address for the IP assignment.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask for the IP assignment.	Valid subnet mask	N/A
MAC Address	Specify the MAC address that this IP assignment will apply to.	Valid MAC address	N/A

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 for for the IP assignment.	5 - 99999 minutes	1440
DNS Server 1	Specify the primary DNS server for the IP assignment.	Valid IP address	N/A
DNS Server 2	Specify the secondary DNS server for the IP assignment.	Valid IP address	N/A
NTP Server	Specify the NTP server for the IP assignment.	Valid IP address	N/A

MAC-based IP Assignment - Delete Entry

Menu Path: Network Service > DHCP Server - MAC-based IP Assignment

You can delete a MAC-based IP assignment by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.



☑		Status	Name	IP Address	Subnet Mask	MAC Address	Lease Time (min.)	Default Gateway	DNS Server 1	DNS Server 2
☑	✎	Disabled	UserManualCASEtest	192.168.127.101	255.255.255.0	00:09:ad:00:aa:01	1440	0.0.0.0	0.0.0.0	0.0.0.0

Max. 256

Items per page: 50

1 – 1 of 1

DHCP Server - Port-based IP Assignment

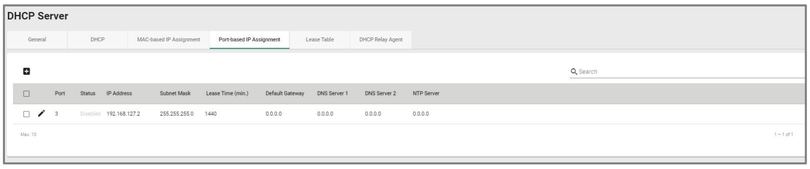
Menu Path: Network Service > DHCP Server - Port-based IP Assignment

This page lets you manage port-based IP assignment for your device's DHCP server.

Port-based IP assignment is a method of managing IP address allocation on a DHCP server by associating specific IP addresses with the physical ports on network equipment, such as switches or routers. This approach provides network administrators with the ability to assign predetermined IP addresses to devices based on the network port they are connected to.

Limitations

You can create up to 10 port-based IP assignments.



□		Port	Status	IP Address	Subnet Mask	Lease Time (min.)	Default Gateway	DNS Server 1	DNS Server 2	NTP Server
□	✎	3	Disabled	192.168.127.2	255.255.255.0	1440	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

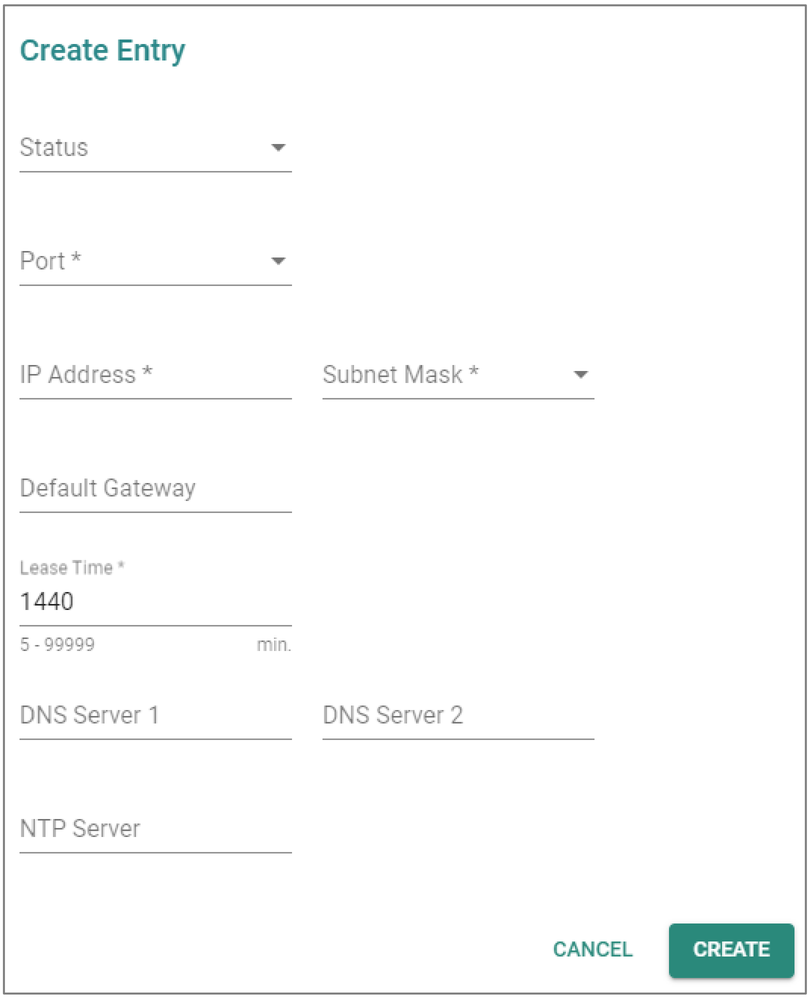
Max. 10

1 – 1 of 1

Create Port-based IP Assignment

Menu Path: Network Service > DHCP Server - Port-based IP Assignment

Clicking the **Add (⊞)** icon on the **Network Service > DHCP Server - Port-based IP Assignment** page will open this dialog box. This dialog lets you create a new port-based IP assignment. Click **CREATE** to save your changes and add the new account.



Create Entry

Status

Port *

IP Address *

Subnet Mask *

Default Gateway

Lease Time *
1440
5 - 99999 min.

DNS Server 1

DNS Server 2

NTP Server

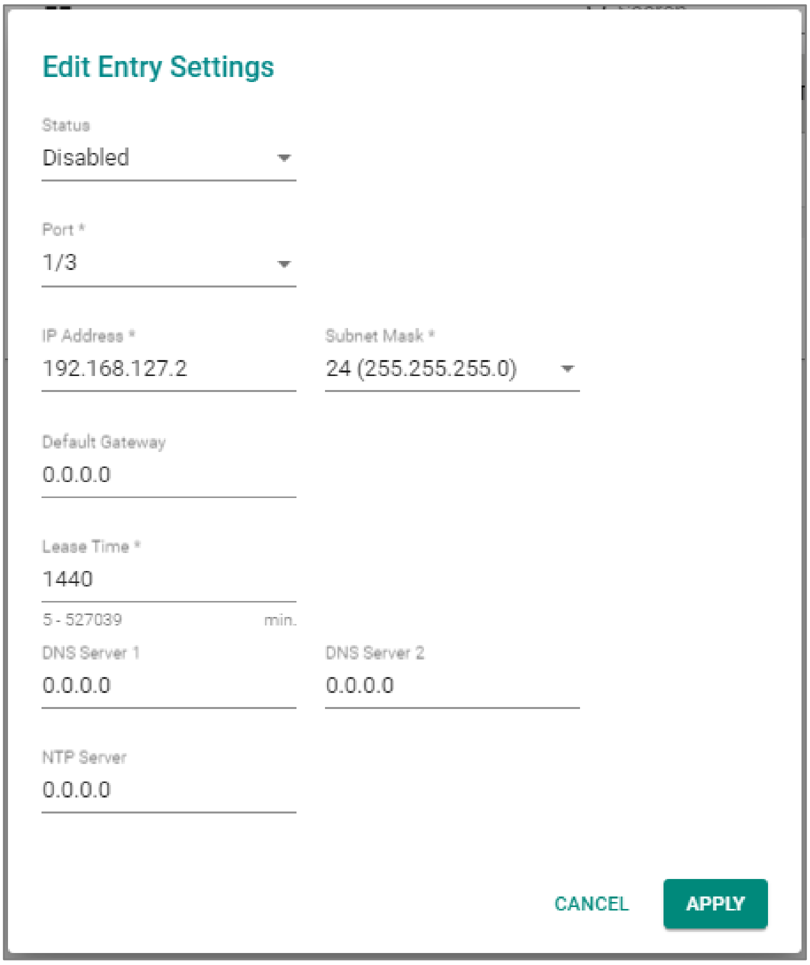
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this port-based IP assignment.	Enabled / Disabled	N/A
Port	Select the physical port on the device to associate the IP with for this entry.	Drop-down list of ports	N/A
IP Address	Specify the IP address of the connected device for this entry.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask of the connected device for this entry.	Valid subnet mask	N/A
Default Gateway	Specify the default gateway of the connected device for this entry.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
Lease Time	Specify the lease time for IP addresses assigned by the DHCP server for this entry.	5 - 99999 minutes	1440
DNS Server 1	Specify the IP address for the first DNS server for DHCP clients for this entry.	Valid IP address	N/A
DNS Server 2	Specify the IP address for the second DNS server for DHCP clients for this entry.	Valid IP address	N/A
NTP Server	Specify the IP address for the NTP server for DHCP clients for this entry.	Valid IP address	N/A

Edit Port-based IP Assignment

Menu Path: Network Service > DHCP Server - Port-based IP Assignment

Clicking the **Edit (✎)** icon for an entry on the **Network Service > DHCP Server - Port-based IP Assignment** page will open this dialog box. This dialog lets you edit an existing port-based IP assignment. Click **APPLY** to save your changes.



Edit Entry Settings

Status
Disabled

Port *
1/3

IP Address *
192.168.127.2

Subnet Mask *
24 (255.255.255.0)

Default Gateway
0.0.0.0

Lease Time *
1440
5 - 527039 min.

DNS Server 1
0.0.0.0

DNS Server 2
0.0.0.0

NTP Server
0.0.0.0

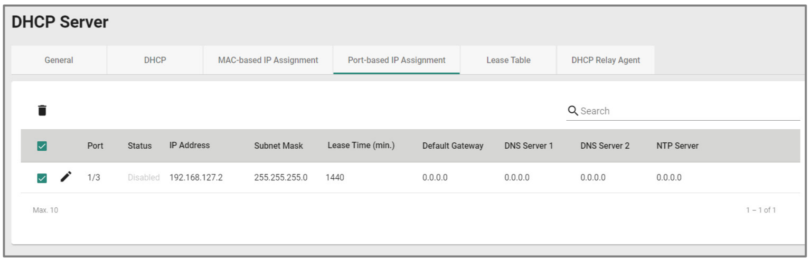
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this port-based IP assignment.	Enabled / Disabled	N/A
Port	Select the physical port on the device to associate the IP with for this entry.	Drop-down list of ports	N/A
IP Address	Specify the IP address of the connected device for this entry.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask of the connected device for this entry.	Valid subnet mask	N/A
Default Gateway	Specify the default gateway of the connected device for this entry.	Valid IP address	N/A
Lease Time	Specify the lease time for IP addresses assigned by the DHCP server for this entry.	5 - 99999 minutes	1440

UI Setting	Description	Valid Range	Default Value
DNS Server 1	Specify the IP address for the first DNS server for DHCP clients for this entry.	Valid IP address	N/A
DNS Server 2	Specify the IP address for the second DNS server for DHCP clients for this entry.	Valid IP address	N/A
NTP Server	Specify the IP address for the NTP server for DHCP clients for this entry.	Valid IP address	N/A

Delete Port-based IP Assignment

Menu Path: Network Service > DHCP Server - Port-based IP Assignment

You can delete a port-based IP assignment by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.



☑		Port	Status	IP Address	Subnet Mask	Lease Time (min.)	Default Gateway	DNS Server 1	DNS Server 2	NTP Server
☑	✎	1/3	Disabled	192.168.127.2	255.255.255.0	1440	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Max. 10

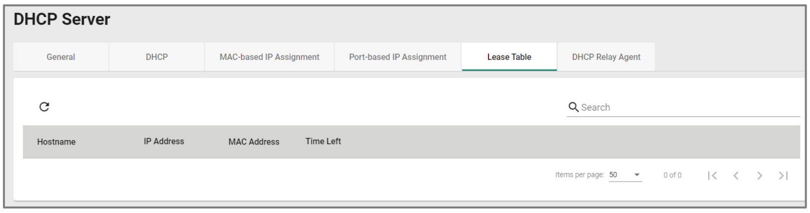
1 – 1 of 1

DHCP Server - Lease Table

Menu Path: Network Service > DHCP Server - Lease Table

This page lets you see an overview of the device's current DHCP clients.

Lease Table



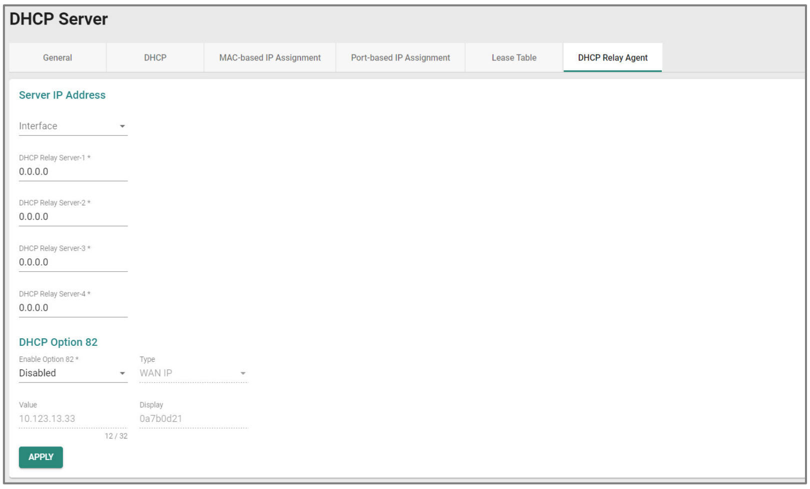
UI Setting	Description
Hostname	Shows the hostname of the DHCP lease.
IP Address	Shows the IP address of the DHCP lease.
MAC Address	Shows the MAC address of the DHCP lease.
Time Left	Shows the time left for the DHCP lease.

DHCP Relay Agent

Menu Path: Network Service > DHCP Server - DHCP Relay Agent

This page allows you to configure the DHCP relay agent, including the settings for remote DHCP server(s) and option-82 related attributes.

DHCP Relay Agent Settings



Server IP Address

Interface

DHCP Relay Server-1 *
0.0.0.0

DHCP Relay Server-2 *
0.0.0.0

DHCP Relay Server-3 *
0.0.0.0

DHCP Relay Server-4 *
0.0.0.0

DHCP Option 82

Enable Option 82 *
Disabled

Type
WAN IP

Value
10.123.13.33
12 / 32

Display
0a7b0d21

Server IP Address

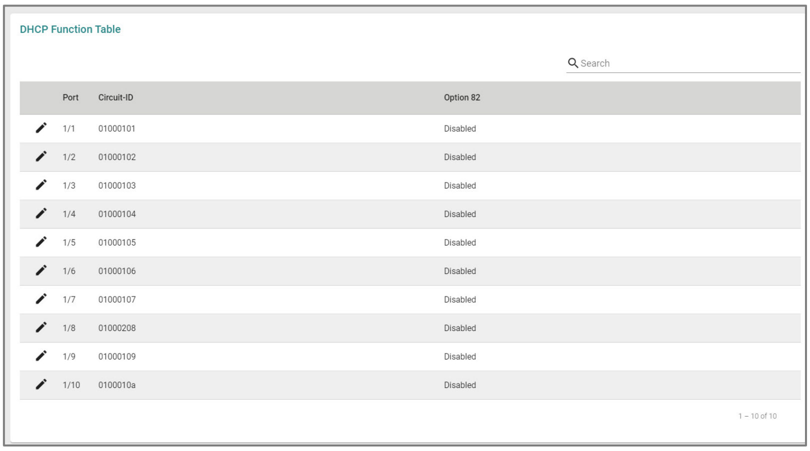
UI Setting	Description	Valid Range	Default Value
Interface	Select a preconfigured network interface.	Drop-down menu of interfaces	None
DHCP Relay Server-1	Specify the IP address of the 1st DHCP server.	Valid IP address	0.0.0.0
DHCP Relay Server-2	Specify the IP address of the 2nd DHCP server.	Valid IP address	0.0.0.0
DHCP Relay Server-3	Specify the IP address of the 3rd DHCP server.	Valid IP address	0.0.0.0
DHCP Relay Server-4	Specify the IP address of the 4th DHCP server.	Valid IP address	0.0.0.0

DHCP Option 82

UI Setting	Description	Valid Range	Default Value
Enable Option 82	Enable or disable DHCP Option 82.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Type	Specify the type of DHCP Option 82 to use. **WAN IP**: Uses the router's IP address as the remote ID sub. **MAC**: Uses the router's MAC addresses as the remote ID sub. **Client-ID**: Uses a combination of the router's MAC address and IP address as the remote ID sub. **Other**: Uses the user-designated ID sub.	WAN IP / MAC / Client-ID / Other	WAN IP
Value	Shows the corresponding value of the selected **Type**. If **Type** is **Other**, specify the value to use.	0 to 32 characters	Depends on the selected **Type**
Display **(View-only)**	Shows the **Value** in hexadecimal.	N/A	N/A

DHCP Function Table



DHCP Function Table

Search

	Port	Circuit-ID	Option 82
✎	1/1	01000101	Disabled
✎	1/2	01000102	Disabled
✎	1/3	01000103	Disabled
✎	1/4	01000104	Disabled
✎	1/5	01000105	Disabled
✎	1/6	01000106	Disabled
✎	1/7	01000107	Disabled
✎	1/8	01000208	Disabled
✎	1/9	01000109	Disabled
✎	1/10	0100010a	Disabled

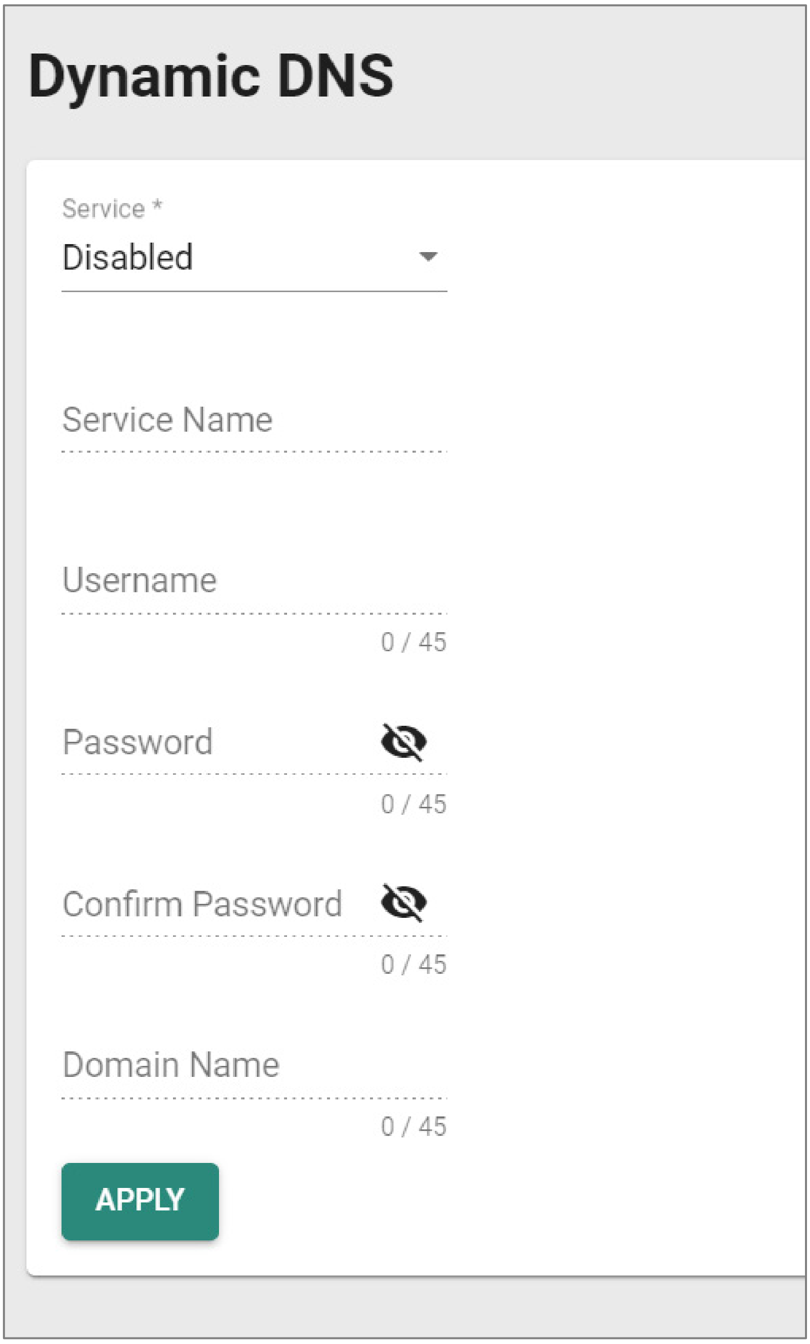
1 – 10 of 10

UI Setting	Description
Port	Shows the number of the port the entry is for.
Circuit-ID	Shows the Circuit-ID of the port.
Option 82	Shows whether Option 82 is enabled or disabled for the port.

Dynamic DNS

Menu Path: Network Service > Dynamic DNS

This page lets you configure your device to use a free dynamic DNS service to enable you to access your device through a domain name rather than an IP. Click **APPLY** to save your changes.



Dynamic DNS

Service *
Disabled

Service Name

Username
0 / 45

Password
0 / 45

Confirm Password
0 / 45

Domain Name
0 / 45

UI Setting	Description	Valid Range	Default Value
Service	Select a dynamic DNS service to use, or disable dynamic DNS..	Disabled / freedns.afraid.org / 3322.org / DynDns.org / NO-IP.com	Disabled

UI Setting	Description	Valid Range	Default Value
Service Name **(View-only)**	Shows the name of the selected dynamic DNS service.	freedns.afraid.org / www.3322.org / members.dyndns.org / dynupdate.no-ip.com	N/A
Username	Specify the username to connect to the dynamic DNS service.	1 to 45 characters	N/A
Password	Specify the password to connect to the dynamic DNS service.	1 to 45 characters	N/A
Confirm Password	Confirm the password to connect to the dynamic DNS service.	1 to 45 characters	N/A
Domain Name	Specify the domain name to use to connect to your device through the dynamic DNS service.	1 to 45 characters	N/A

Routing

Menu Path: Routing

The Routing settings area lets you configure settings related to how your device routes network traffic.

This settings area includes these sections:

- Unicast Route
- Multicast Route
- Broadcast Forwarding

Routing - User Privileges

Privileges to Routing 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
Unicast Routing			
Static Routes	R/W	R/W	R
RIP	R/W	R/W	R
OSPF	R/W	R/W	R
Routing Table	R	R	R
Multicast Route			
Multicast Route Settings	R/W	R/W	R
Static Multicast Route	R/W	R/W	R
Broadcast Forwarding	R/W	R/W	R

Unicast Route

Menu Path: Routing > Unicast Route

This section lets you manage unicast routes for your device.

This section includes these pages:

- Static Routes
- RIP
- OSPF
- Routing Table

Static Routes

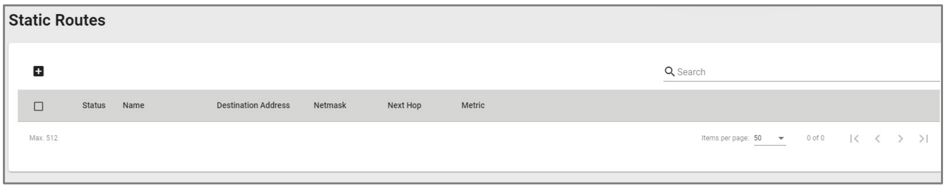
Menu Path: Routing > Unicast Route > Static Routes

This page lets you manage static routes for your device, which allows you to specify the next hop (or router) that the device will forward data to for a specific subnet. Static routes will be added to the routing table and stored on the device.

Limitations

You can create up to 512 static routes.

Static Route List



Static Routes

Search

☐	Status	Name	Destination Address	Netmask	Next Hop	Metric

Max. 512

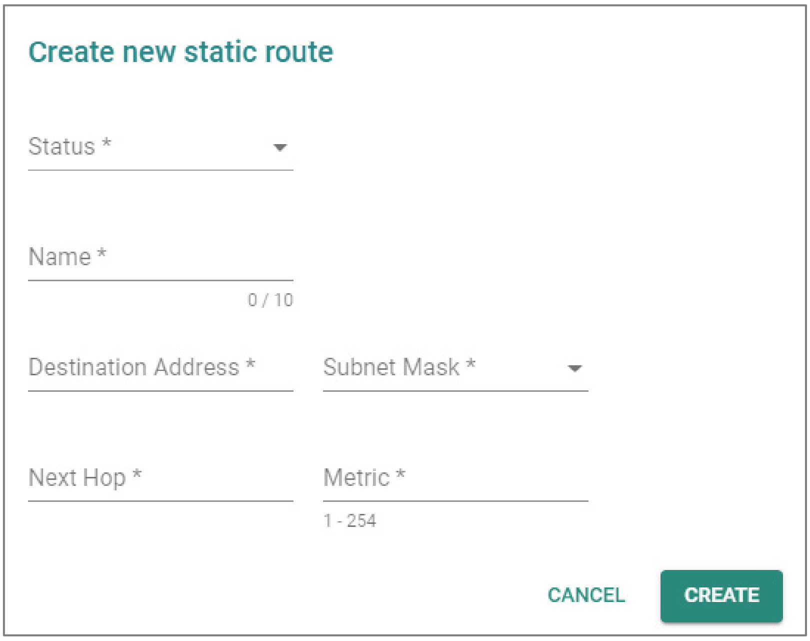
Items per page: 50 ▾ 0 of 0

UI Setting	Description
Status	Shows the status of the static route.
Name	Shows the name of the static route.
Destination Address	Shows the destination IP address for the static route.
Netmask	Shows the subnet mask for the destination IP address.
Next Hop	Shows the next router on the path to the destination IP address.
Metric	Shows the metric value used to determine the priority of the static route. Lower values have higher priority.

Create New Static Route

Menu Path: Routing > Unicast Route > Static Routes

Clicking the **Add (⊞)** icon on the **Routing > Unicast Route > Static Routes** page will open this dialog box. This dialog lets you create a new static route. Click **CREATE** to save your changes and add the new account.



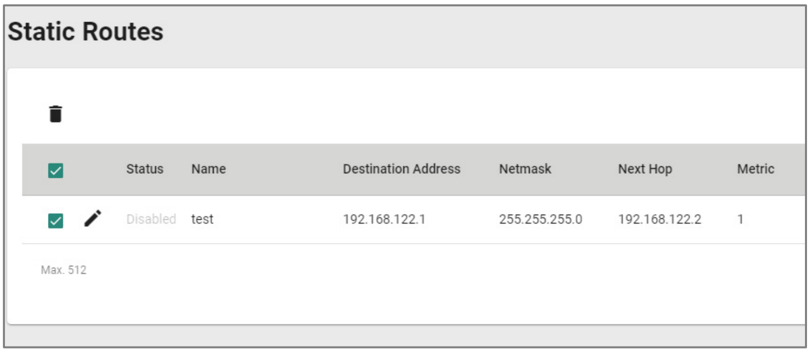
Create new static route

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the static route.	Enabled / Disabled	N/A
Name	Specify a name for the static route.	Max. 10 characters	N/A
Destination Address	Specify the destination IP address for the static route.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask for the destination IP address.	Drop-down list of values	N/A
Next Hop	Specify the next router on the path to the destination IP.	Valid IP address	N/A
Metric	Specify the metric value to determine the priority of the static route. Lower values have higher priority.	1 to 254	N/A

Delete Static Route

Menu Path: Routing > Unicast Route > Static Routes

You can delete entries by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.



Static Routes

☑	Status	Name	Destination Address	Netmask	Next Hop	Metric
☑	Disabled	test	192.168.122.1	255.255.255.0	192.168.122.2	1

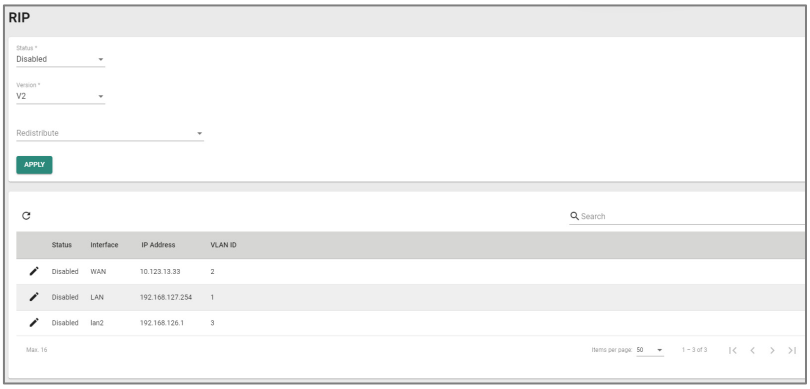
Max. 512

RIP

Menu Path: Routing > Unicast Route > RIP

This page lets you configure RIP (Routing Information Protocol), a distance-vector routing protocol that employs the hop count as a routing metric. RIP prevents routing from looping by implementing a limit on the number of hops allowed in a path from the source to a destination. Click **APPLY** to save your changes.

RIP Settings



RIP

Status *: Disabled

Version *: V2

Redistribute

Status	Interface	IP Address	VLAN ID
Disabled	WAN	10.123.13.33	2
Disabled	LAN	192.168.127.254	1
Disabled	lan2	192.168.126.1	3

Max. 16

Items per page: 50 1 – 3 of 3

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable RIP protocol.	Enabled / Disabled	Disabled

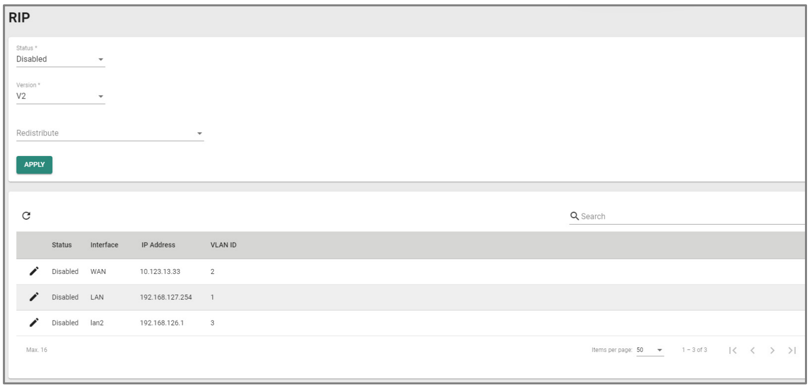
UI Setting	Description	Valid Range	Default Value
Version	Set the RIP protocol version: **V1**: RIP V1 uses classful routing. This means that network addresses are assigned to specific classes, and the subnet mask is determined by the class of the network address. **V2**: RIP V2 uses classless routing. This means that network addresses can be assigned in a more flexible way, and the subnet mask can be specified independently of the network address class.	V1 / V2	V2
Redistribute	Set which rules to enable for RIP redistribution. You can enable multiple redistribution rules. **Connected**: Entries learned from directly connected interfaces will be re-distributed. **Static**: Entries set in a static route will be re-distributed. **OSPF**: Entries learned from the OSPF will be re-distributed. **Note** Redistribute in RIP refers to the process of importing routing information from other routing protocols into the RIP routing table, allowing for interconnectivity between different protocols and complex networks.	Connected / Static / OSPF	N/A

RIP Interface List

This list shows all of your device interfaces and the RIP settings applied to each one.

Note

Interfaces and their settings can be configured in Network Configuration > Network Interfaces. VLAN IDs can be configured in Network Configuration > Layer 2 Switching> VLAN.



RIP

Status *: Disabled

Version *: V2

Redistribute

	Status	Interface	IP Address	VLAN ID
✎	Disabled	WAN	10.123.13.33	2
✎	Disabled	LAN	192.168.127.254	1
✎	Disabled	lan2	192.168.126.1	3

Max. 16

Items per page: 50

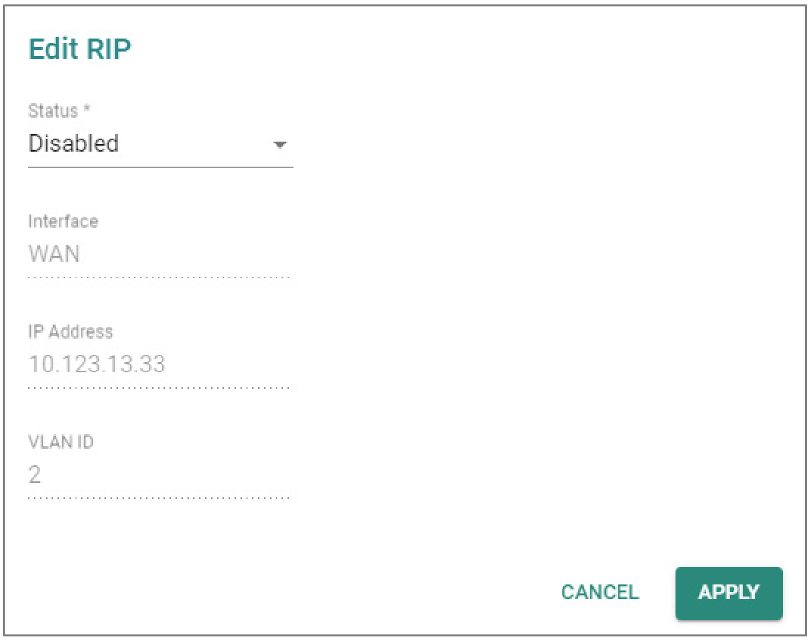
1 – 3 of 3

UI Setting	Description
Status	Shows whether RIP is enabled or disabled for the interface.
Interface (View Only)	Shows the name of the interface.
IP Address (View Only)	Shows the IP address of the interface.
VLAN ID (View Only)	Shows the VLAN ID of the interface.

Edit RIP

Menu Path: Routing > Unicast Route > RIP

Clicking the **Edit (✎)** icon for an interface on the **Routing > Unicast Route > RIP** page will open this dialog box. This dialog lets you edit the RIP settings for the interface. Click **APPLY** to save your changes.



Edit RIP

Status *
Disabled

Interface
WAN

IP Address
10.123.13.33

VLAN ID
2

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable RIP for the interface.	Enabled / Disabled	Disabled
Interface (View Only)	Shows the name of the interface.	Interface name	N/A
IP Address (View Only)	Shows the IP address of the interface.	Interface IP address	N/A
VLAN ID (View Only)	Shows the VLAN ID of the interface.	Interface VLAN ID	N/A

OSPF

Menu Path: Routing > Unicast Route > OSPF

This section lets you configure OSPF (Open Shortest Path First) routing for your device.

This section includes these pages:

- OSPF Settings

- OSPF Status

OSPF Settings

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings

This page lets you configure OSPF settings for your device.

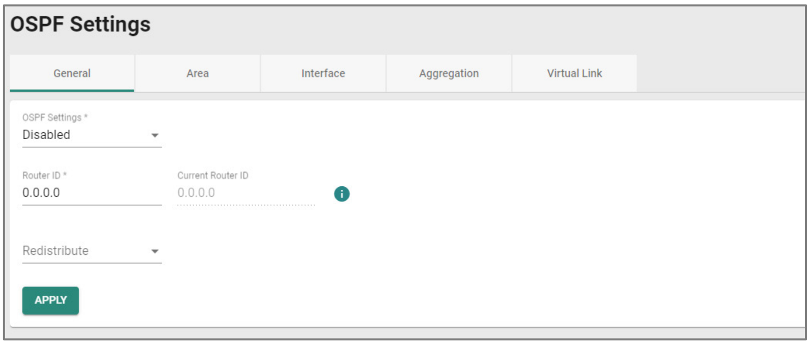
This page includes these tabs:

- General
- Area
- Interface
- Aggregation
- Virtual Link

OSPF Settings - General

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - General

This page lets you adjust the basic settings for OSPF. Click **APPLY** to save your changes.



OSPF Settings

OSPF Settings *: Disabled

Router ID *: 0.0.0.0

Current Router ID: 0.0.0.0

Redistribute

UI Setting	Description	Valid Range	Default Value
OSPF Settings	Enable or disable OSPF for your device.	Enabled / Disabled	Disabled
Router ID	Specify the Router ID of your Moxa router. **Note** The router ID, which must be established for every OSPF instance, should be written in the dot-decimal format of an IP address (e.g., 1.2.3.4) and does not need to be part of any routable subnet on the network, since it is an IP address.	Router ID	0.0.0.0
Current Router ID **(View-only)**	Specify the current Router ID of your Moxa router. **Note** When the Router ID is set to 0.0.0.0, the Current Router ID will automatically use the highest interface IP address.	Current Router ID	0.0.0.0
Redistribute	Specify the OSPF redistribution method: **Connected**: Entries learned from the directly connected interfaces will be redistributed. **Static**: Entries set in a static route will be redistributed. **RIP**: Entries learned from RIP will be redistributed. **Note** Redistributing in OSPF refers to the process of importing routing information from other routing protocols–such as RIP, EIGRP, etc.–into the OSPF routing table.	Connected / Static / RIP	N/A

OSPF Settings - Area

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Area

This page lets you define OSPF areas.

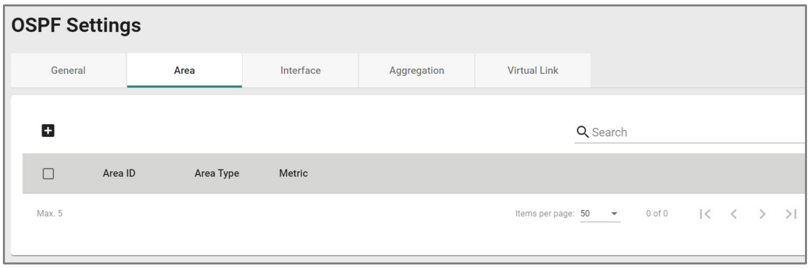
Note

Areas are used to divide a large network into smaller network areas. Each area maintains a separate link state database whose information may be summarized towards the rest of the network by the connecting router. Thus, the topology of an area is unknown outside of the area. This reduces the amount of routing traffic between parts of an autonomous system.

Limitations

You can create up to 5 OSPF areas.

OSPF Area List



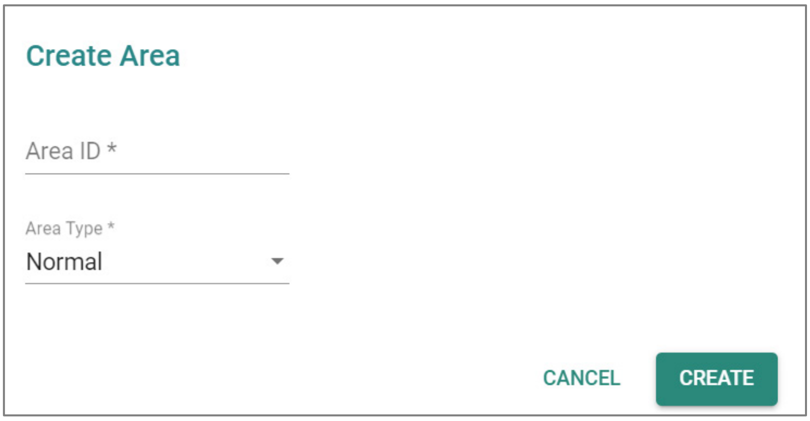
UI Setting	Description
Area ID	Shows the area's ID.
Area Type	Shows the type of OSPF routing used for the area.
Metric **(Only for Mertic is Stub/NSSA)**	Shows the metric value/cost for OSPF in the area.

Create Area

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Area

Clicking the **Add (** ⊞ **)** icon on the **Routing > Unicast Route > OSPF > OSPF Settings**

- Area page will open this dialog box. This dialog lets you create a new OSPF area. Click **CREATE** to save your changes and add the new area.



Create Area

Area ID *

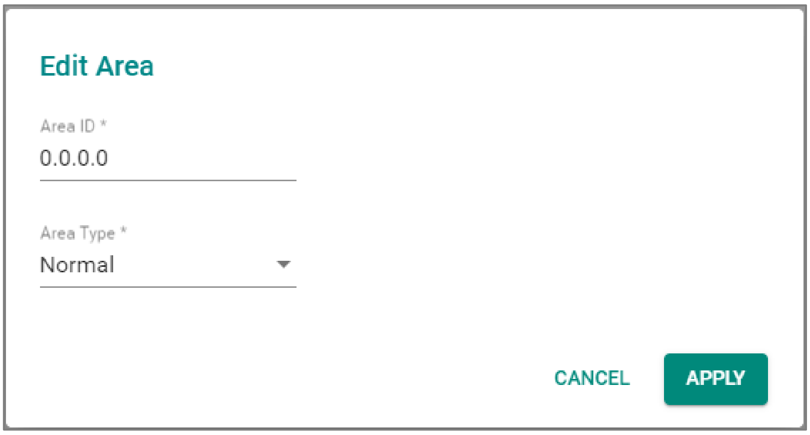
Area Type *
Normal

UI Setting	Description	Valid Range	Default Value
Area ID	Specify an ID for this OSPF area.	N/A	N/A
Area Type	Specify the type of OSPF routing to use for this area: **Normal**: A normal (or standard) area is an OSPF area that allows both intra-area and inter-area routing. **Stub**: A stub area is an OSPF area that does not allow external routes to be imported into the area. **NSSA**: An NSSA (Not-So-Stubby Area) is a special type of OSPF area that allows external routing information to be imported into the area, but does not allow the area to propagate that information to other areas.	Normal / Stub / NSSA	Normal
Metric **(if Metric is Stub or NSSA)**	Specify the metric value/cost to use for this area. **Note** Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.	1 to 65535	1

Edit Area

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Area

Clicking the **Edit (✎)** icon for an OSPF area on the **Insert > Path Here** page will open this dialog box. This dialog lets you modify an existing OSPF area. Click **APPLY** to save your changes.



Edit Area

Area ID *: 0.0.0.0

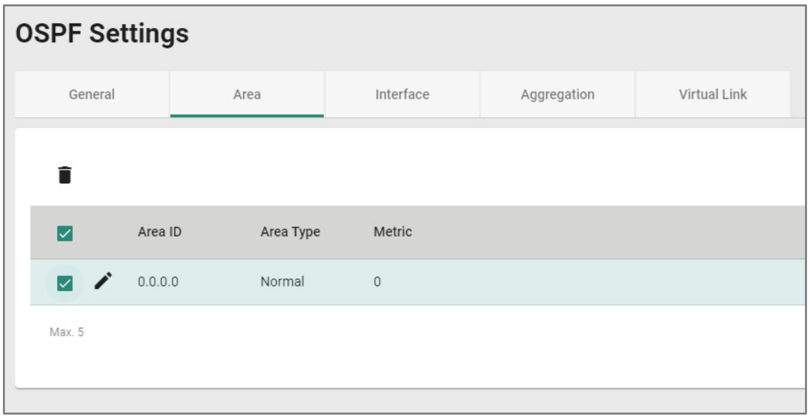
Area Type *: Normal

UI Setting	Description	Valid Range	Default Value
Area ID	Specify an ID for this OSPF area.	N/A	N/A
Area Type	Specify the type of OSPF routing to use for this area: **Normal**: A normal (or standard) area is an OSPF area that allows both intra-area and inter-area routing. **Stub**: A stub area is an OSPF area that does not allow external routes to be imported into the area. **NSSA**: An NSSA (Not-So-Stubby Area) is a special type of OSPF area that allows external routing information to be imported into the area, but does not allow the area to propagate that information to other areas.	Normal / Stub / NSSA	Normal
Metric **(if Metric is Stub or NSSA)**	Specify the metric value/cost to use for this area. ✎ **Note** Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.	1 to 65535	1

Delete Area

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Area

You can delete an OSPF area by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.



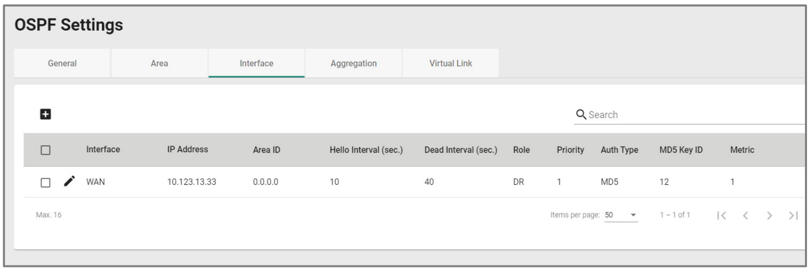
☑		Area ID	Area Type	Metric
☑	✎	0.0.0.0	Normal	0

Max. 5

OSPF Settings - Interface

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Interface

This page lets you configure the OSPF settings for each of your interfaces. To manage your interfaces, refer to Network Configuration > Network Interfaces.



□		Interface	IP Address	Area ID	Hello Interval (sec.)	Dead Interval (sec.)	Role	Priority	Auth Type	MD5 Key ID	Metric
□	✎	WAN	10.123.13.33	0.0.0.0	10	40	DR	1	MD5	12	1

Max. 16

Items per page: 50 1 – 1 of 1

UI Setting	Description
Interface	Shows which interface this entry describes.
IP Address	Shows the IP address of the interface.
Area ID	Shows the OSPF area ID used for the interface.
Hello Interval	Shows the hello message interval for the interface.

UI Setting	Description
Dead Interval	Shows the dead interval for the interface.
Role	Shows the role of the interface.
Priority	Shows the priority of the interface.
Auth Type	Shows the authentication type used to authenticate OSPF neighbors.
MD5 Key ID **(Only if Auth Type is MD5)**	Shows the MD5 key ID used to authenticate OSPF neighbors.
Metric	Shows the metric value/cost to OSPF. **Note** Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.

OSPF Settings - Create Interface

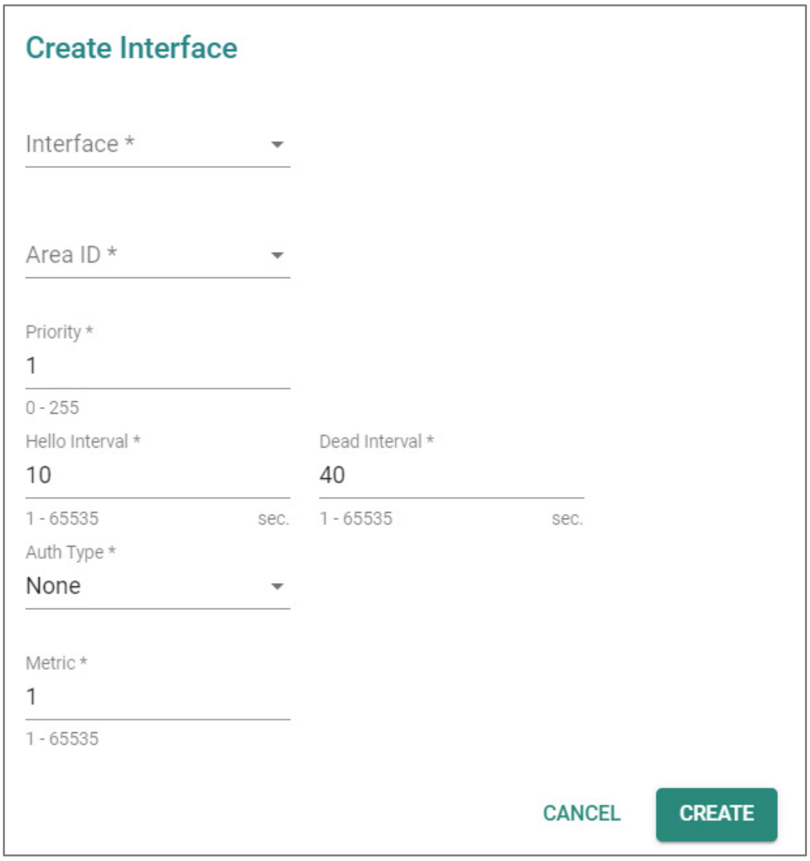
Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Interface

Clicking the **Add (⊞)** icon on the **Insert > Path Here** page will open this dialog box. This dialog lets you select an interface and configure OSPF settings for it.

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

Note

You cannot create new interfaces in this dialog; you can only select existing interfaces. To create a new interface, refer to Network Configuration > Network Interfaces.


Create Interface

Interface *

Area ID *

Priority *
1
0 - 255

Hello Interval *
10
1 - 65535 sec.

Dead Interval *
40
1 - 65535 sec.

Auth Type *
None

Metric *
1
1 - 65535

UI Setting	Description	Valid Range	Default Value
Interface	Specify which interface to assign to an OSPF area.	Dropdown of interfaces	N/A
Area ID	Specify an OSPF area ID to assign to the interface. **Note** To manage OSPF areas, refer to Routing > Unicast Route > OSPF > OSPF Settings - Area.	Dropdown of area IDs	N/A
Priority	Specify the priority of the interface.	0 to 255	1
Hello Interval	Set the hello message interval for the interface. The hello interval is the amount of time between sends of hello packets, which indicate that the device is still alive. The value of all hello intervals must be the same within a network.	1 to 65535 second(s)	10

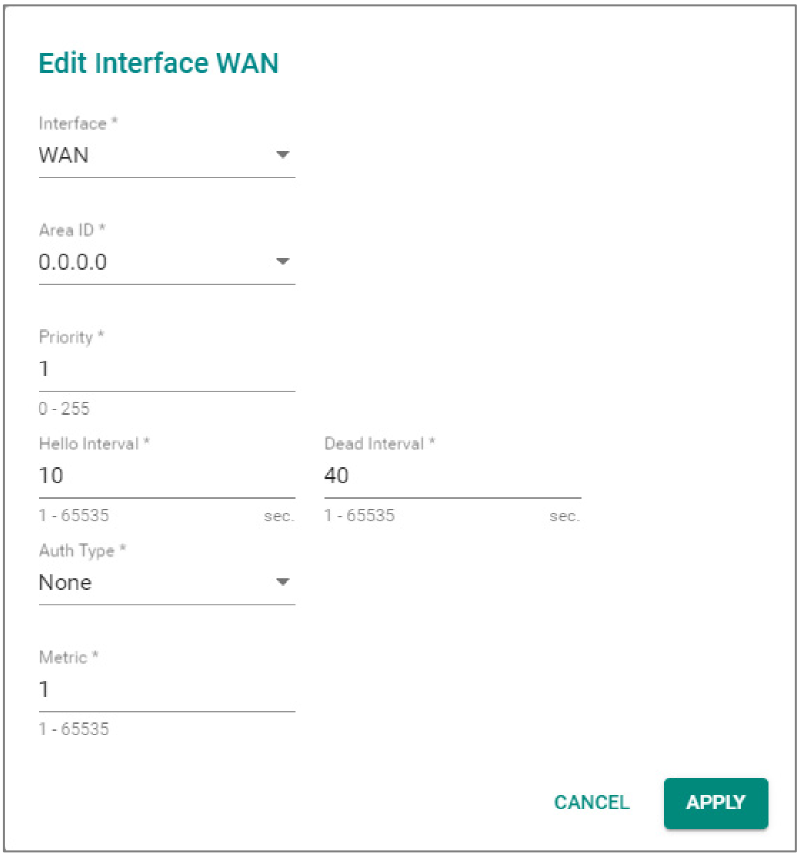
UI Setting	Description	Valid Range	Default Value
Dead Interval	Set the dead interval for the interface. The dead interval is the amount of time a device will wait for a hello packet. If a hello packet is not received in this time, it will consider the other device to be dead or unavailable. By default, the dead interval is set to be four times the value of the hello interval.	1 to 65535 second(s)	40
Auth Type	Specify the authentication type to use when authenticating OSPF neighbors. **None**: No authentication method will be used for neighbor authentication. **Simple**: Neighbors will be authenticated using an auth key. **MD5**: Neighbors will be authenticated more securely by using an auth key and an MD5 key ID.	None / Simple / MD5	N/A
Auth Key (Only if Auth Type is Simple or MD5)	Specify the auth key to use for neighbor authentication. **If the Auth Type is Simple**, the auth key will be a pure-text password. **If the Auth Type is MD5**, the auth key will be an encrypted password.	1 to 8 characters	N/A
MD5 Key ID (Only if Auth Type is MD5)	Specify the MD5 key ID to use for neighbor authentication. ✎ **Note** MD5 authentication method uses MD5 to calculate a hash value from the contents of the OSPF packet and the authentication key. This hash value is transmitted in the packet, along with a key ID.	1 to 255	1
Metric	Specify the metric value/cost for OSPF. ✎ **Note** Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.	1 to 65535	1

OSPF Settings - Edit Interface

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Interface

Clicking the **Edit (✎)** icon for an entry on the **Insert > Path Here** page will open this dialog box. This dialog lets you edit existing OSPF settings for an interface.

Click **APPLY** to save your changes.



Edit Interface WAN

Interface *
WAN

Area ID *
0.0.0.0

Priority *
1
0 - 255

Hello Interval *
10
1 - 65535 sec.

Dead Interval *
40
1 - 65535 sec.

Auth Type *
None

Metric *
1
1 - 65535

UI Setting	Description	Valid Range	Default Value
Interface	Specify which interface to assign to an OSPF area.	Dropdown of interfaces	N/A
Area ID	Specify an OSPF area ID to assign to the interface. **Note** To manage OSPF areas, refer to Routing > Unicast Route > OSPF > OSPF Settings - Area.	Dropdown of area IDs	N/A
Priority	Specify the priority of the interface.	0 to 255	1
Hello Interval	Set the hello message interval for the interface. The hello interval is the amount of time between sends of hello packets, which indicate that the device is still alive. The value of all hello intervals must be the same within a network.	1 to 65535 second(s)	10

UI Setting	Description	Valid Range	Default Value
Dead Interval	Set the dead interval for the interface. The dead interval is the amount of time a device will wait for a hello packet. If a hello packet is not received in this time, it will consider the other device to be dead or unavailable. By default, the dead interval is set to be four times the value of the hello interval.	1 to 65535 second(s)	40
Auth Type	Specify the authentication type to use when authenticating OSPF neighbors. **None**: No authentication method will be used for neighbor authentication. **Simple**: Neighbors will be authenticated using an auth key. **MD5**: Neighbors will be authenticated more securely by using an auth key and an MD5 key ID.	None / Simple / MD5	N/A
Auth Key (Only if Auth Type is Simple or MD5)	Specify the auth key to use for neighbor authentication. **If the Auth Type is Simple**, the auth key will be a pure-text password. **If the Auth Type is MD5**, the auth key will be an encrypted password.	1 to 8 characters	N/A
MD5 Key ID (Only if Auth Type is MD5)	Specify the MD5 key ID to use for neighbor authentication. ✎ **Note** MD5 authentication method uses MD5 to calculate a hash value from the contents of the OSPF packet and the authentication key. This hash value is transmitted in the packet, along with a key ID.	1 to 255	1
Metric	Specify the metric value/cost for OSPF. ✎ **Note** Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.	1 to 65535	1

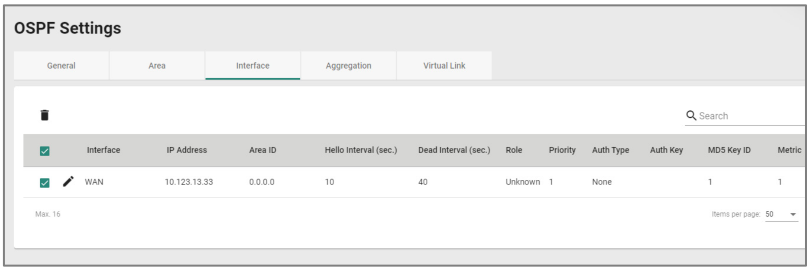
OSPF Settings - Delete Interface

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Interface

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.

Note

Please note that this will delete the OSPF settings for the interface, but it will not delete the interface itself.



☑		Interface	IP Address	Area ID	Hello Interval (sec.)	Dead Interval (sec.)	Role	Priority	Auth Type	Auth Key	MD5 Key ID	Metric
☑	✎	WAN	10.123.13.33	0.0.0.0	10	40	Unknown	1	None		1	1

Max. 16

Items per page: 50

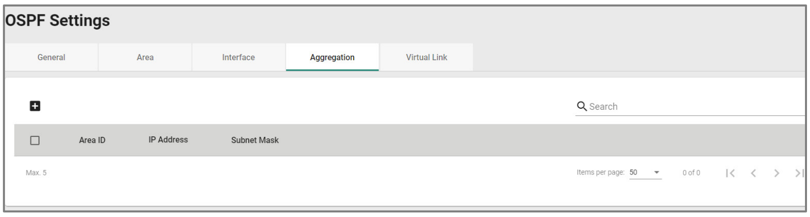
OSPF Settings - Aggregation

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Aggregation

This page lets you aggregate different OSPF areas into a single routing table entry.

Limitations

You can create up to 5 OSPF aggregations.



□	Area ID	IP Address	Subnet Mask

Max. 5

Items per page: 50

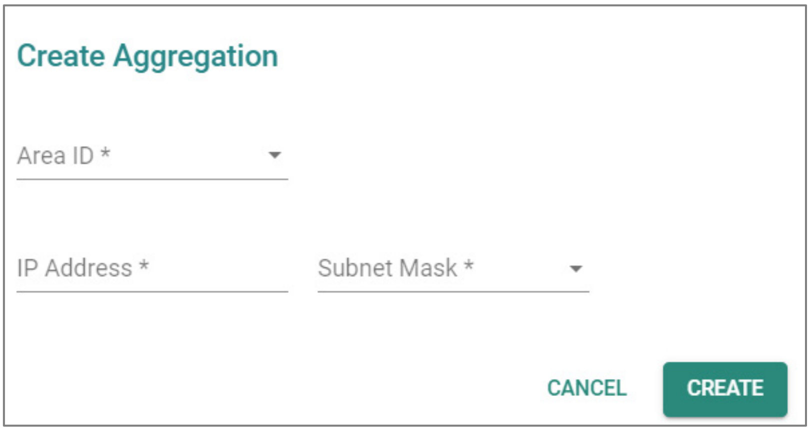
0 of 0

UI Setting	Description
Area ID	Shows the area ID.
IP Address	Shows the IP address of the area.
Subnet Mask	Shows the network subnet mask.

Create an Aggregation

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Aggregation

Clicking the **Add (** ⊞ **)** icon on the **Routing > Unicast Route > OSPF > OSPF Settings - Aggregation** page will open this dialog box. This dialog lets you create an OSPF aggregation. Click **CREATE** to save your changes and add the new aggregation.


Create Aggregation

Area ID *

IP Address *

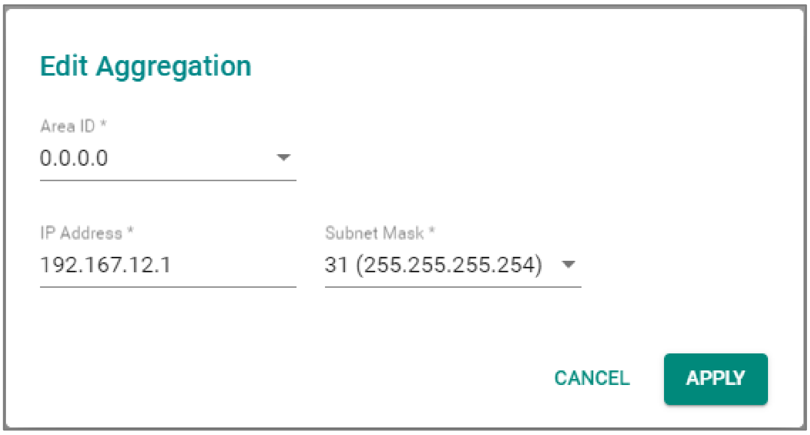
Subnet Mask *

UI Setting	Description	Valid Range	Default Value
Area ID	Select the area ID that you want to use for the aggregation.	Dropdown list of area IDs	N/A
IP Address	Specify the IP address to use for the area.	Valid IP address	N/A
Subnet Mask	Select the network subnet mask to use for the area.	Dropdown list of subnet masks	N/A

Edit an Aggregation

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Aggregation

Clicking the **Edit (** ✎ **)** icon for an entry on the **Routing > Unicast Route > OSPF > OSPF Settings - Aggregation** page will open this dialog box. This dialog lets you modify an existing aggregation. Click **APPLY** to save your changes.



Edit Aggregation

Area ID *
0.0.0.0

IP Address *
192.167.12.1

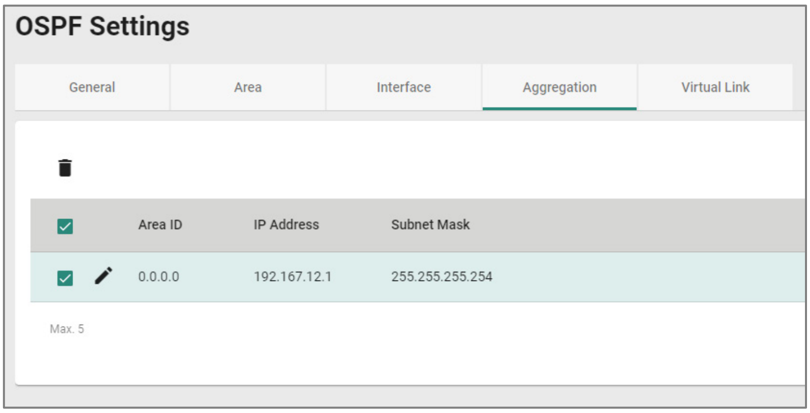
Subnet Mask *
31 (255.255.255.254)

UI Setting	Description	Valid Range	Default Value
Area ID	Select the area ID that you want to use for the aggregation.	Dropdown list of area IDs	N/A
IP Address	Specify the IP address to use for the area.	Valid IP address	N/A
Subnet Mask	Select the network subnet mask to use for the area.	Dropdown list of subnet masks	N/A

Delete an Aggregation

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Aggregation

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.



OSPF Settings

☑		Area ID	IP Address	Subnet Mask
☑	✎	0.0.0.0	192.167.12.1	255.255.255.254

Max. 5

Virtual Link

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Virtual Link

This page lets you configure virtual links, which can be used to connect areas in an OSPF autonomous system when physical connection to the backbone area is not possible.

Limitations

You can create up to 5 OSPF virtual links.

OSPF Status

Menu Path: Routing > Unicast Route > OSPF > OSPF Status

This page lets you view the OSPF routing status of your device.

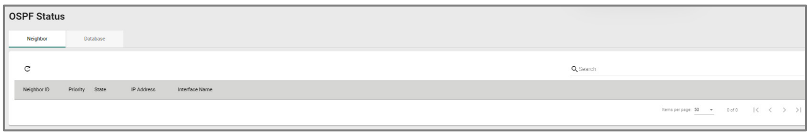
This page includes these tabs:

- Neighbor
- Database

Neighbor

Menu Path: Routing > Unicast Route > OSPF > OSPF Status - Neighbor

This page lets you see the status of OSPF neighbors. OSPF neighbors are devices that share their link-state information with other devices in the network.



OSPF Status

Neighbor ID	Priority	State	IP Address	Interface Name

Items per page: 50

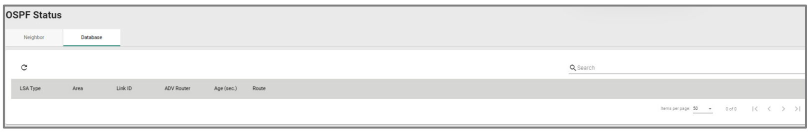
0 of 0

UI Setting	Description
Neighbor ID	Shows the unique identifier for the OSPF neighbor.
Priority	Shows priority value that the neighbor has assigned to itself.
State	Shows the current state of the OSPF neighbor relationship: **Down:** The initial state before any OSPF communication has occurred between two routers. **Init**: The state where the local router has sent an OSPF Hello packet to a neighbor but has not yet received a response. **2-way**: The state where both routers have exchanged Hello packets and can become neighbors, but they have not yet established a bidirectional relationship. **Exstart**: The state where the routers determine which one will be the master and which one will be the slave during the database exchange process. **Exchange**: The state where the routers exchange link-state advertisement (LSA) headers and determine which LSAs need to be sent. **Loading**: The state where the routers exchange LSAs to synchronize their link-state databases. **Full**: The final state where the routers have a complete and accurate view of the network topology and are ready to forward traffic.
IP Address	Shows the IP address of the neighbor router's interface used for OSPF communication.
Interface Name	Shows the name of the local interface used for OSPF communication with the neighbor.

Database

Menu Path: Routing > Unicast Route > OSPF > OSPF Status - Database

This page lets you see the list of link-state advertisements (LSAs) that describe the network topology, which is used to calculate the shortest path to a destination.



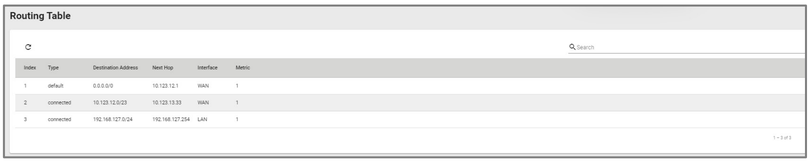
LSA Type	Area	Link ID	ADV Router	Age (sec.)	Route

UI Setting	Description	Valid Range	Default Value
LSA Type	Shows the type of the LSA, which describes the contents of the OSPF LSA packet. **Router LSA**: Describes the links attached to a router and is flooded within the same area as the router. **Network LSA**: Describes the routers attached to a multi-access network. **Summary LSA**: Advertises reachability information between OSPF areas. **AS External LSA**: Advertises routes to networks outside the OSPF domain. **NSSA External LSA**: Similar to the Type 5 LSA, but used in a Not-So-Stubby Area (NSSA) to advertise external routes. **Link-local LSA**: Used to advertise IPv6 link-local addresses and is flooded throughout the same link-local scope.	N/A	N/A
Area	Identifies the area of the network to which the LSA belongs.	N/A	N/A
Link ID	Identifies the endpoint of the link described by the LSA.	N/A	N/A
ADV Router	Identifies the router that the LSA originated from.	N/A	N/A
Route	OSPF uses the information in the LSAs to calculate the shortest path to a destination.	N/A	N/A

Routing Table

Menu Path: Routing > Unicast Route > Routing Table

This page lets you see the current routing table for your device.



Routing Table

Index	Type	Destination Address	Next Hop	Interface	Metric
1	default	0.0.0.0/0	10.123.12.1	WAN	1
2	connected	10.123.12.0/23	10.123.13.33	WAN	1
3	connected	192.168.127.0/24	192.168.127.254	LAN	1

1 – 3 of 3

UI Setting	Description
Index	Shows the unique identifier for the routing table entry.

UI Setting	Description
Type	Shows the source type of the route.
Destination Address	Shows the address of the destination network for the route.
Next Hop	Shows the IP address of the next hop router or gateway that the packet should be forwarded to.
Interface	Shows the outgoing interface that should be used to reach the destination network.
Metric	Shows the metric value/cost of the route to the destination network. **Note** Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.

Multicast Route

Menu Path: Routing > Multicast Route

This section lets you configure multicast routing for your device.

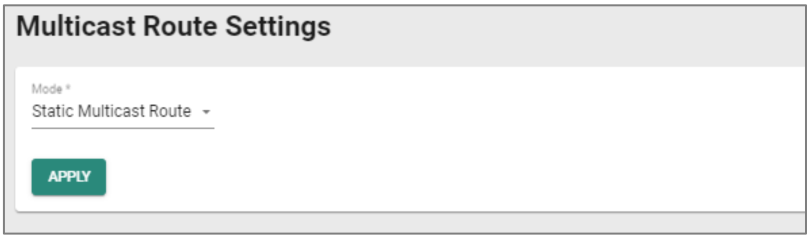
This section includes these pages:

- Multicast Route Settings
- Static Multicast Route
- Multicast Forwarding Table

Multicast Route Settings

Menu Path: Routing > Multicast Route > Multicast Route Settings

This page lets you enable or disable multicast routing. Click **APPLY** to save your changes.



Multicast Route Settings

Mode *
Static Multicast Route

UI Setting	Description	Valid Range	Default Value
Mode	Enable or disable multicast routing.	Disabled / Static Multicast Route	Disabled

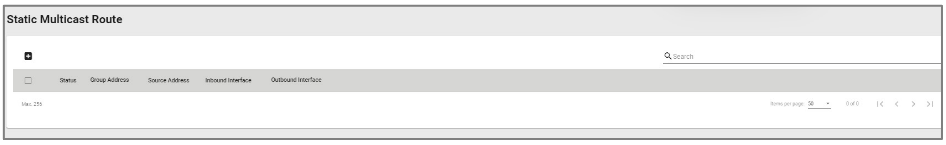
Static Multicast Route

Menu Path: Routing > Multicast Route > Static Multicast Route

This page lets you manage multicast routes for your device.

Limitations

You can create up to 256 static multicast routes.



Static Multicast Route

□	Status	Group Address	Source Address	Inbound Interface	Outbound Interface

Max. 256

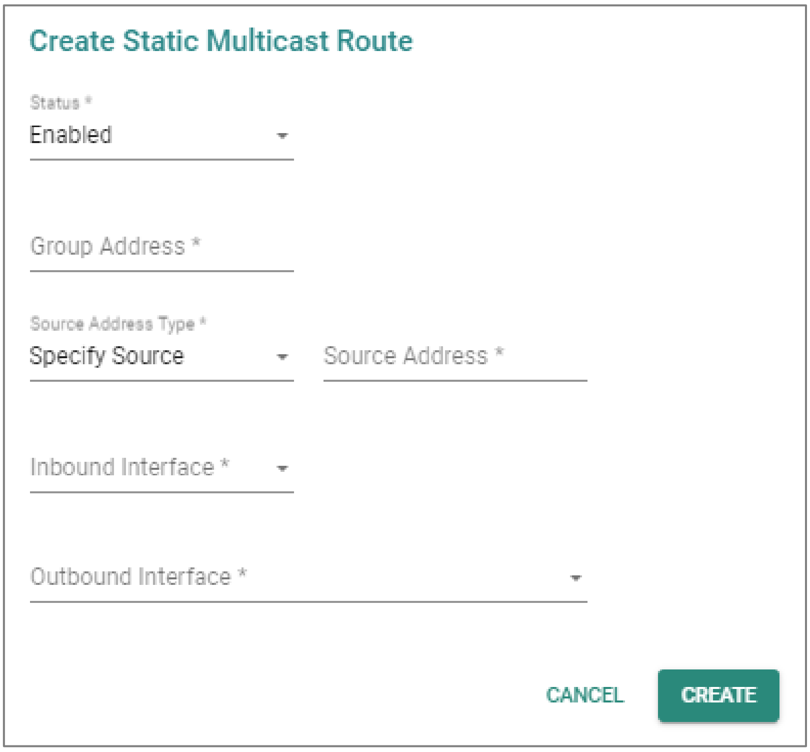
Items per page: 50 0 of 0

UI Setting	Description
Status	Shows whether the static multicast route is enabled or disabled.
Group Address	Shows the group IP address for the route.
Source Address	Shows the source address for the route.
Inboud Interface	Shows the inbound interface for the route.
Outbound Interface	Shows the outbound interfaces for the route.

Create Static Multicast Route

Menu Path: Routing > Multicast Route > Static Multicast Route

Clicking the **Add (⊞)** icon on the **Routing > Multicast Route > Static Multicast Route** page will open this dialog box. This dialog lets you add a new static multicast route. Click **CREATE** to save your changes and add the new account.


Create Static Multicast Route

Status *
Enabled

Group Address *

Source Address Type *
Specify Source

Source Address *

Inbound Interface *

Outbound Interface *

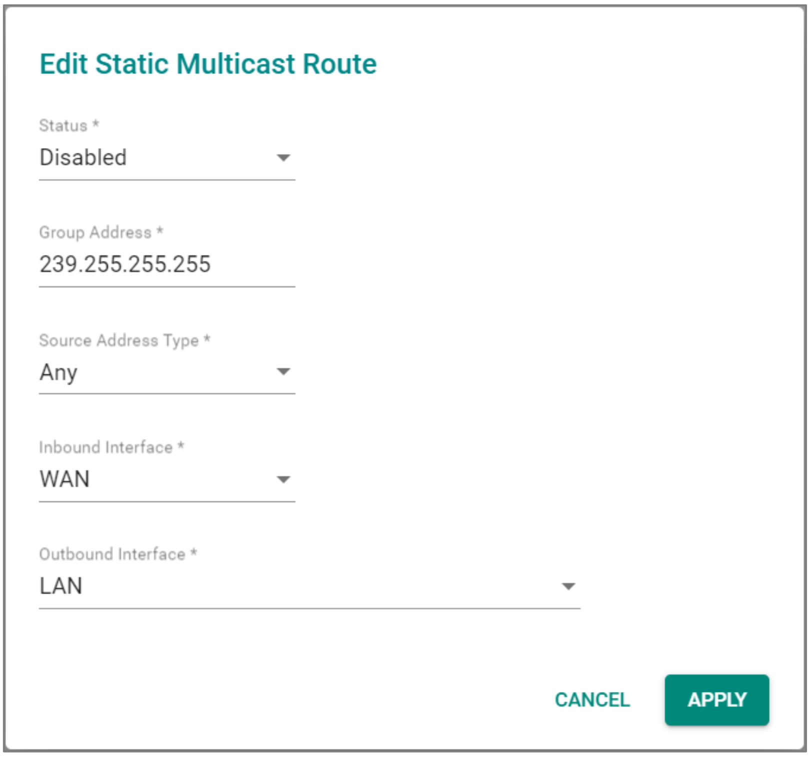
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this route.	Enabled / Disabled	Enabled
Group Address	Specify the group IP address for this route.	N/A	N/A

UI Setting	Description	Valid Range	Default Value
Source Address Type	Specify the type of source address to use for this route. **Any**: Allow any IP to be the source address. **Specify Source**: Use the specified **Source Address**.	Any / Specify Source	Any
Source Address **(Only if Source Address Type is Specify Source)**	Specify the source IP address to use for this route.	N/A	N/A
Inbound Interface	Select which interface broadcast packets will come from.	Drop-down list of interfaces	N/A
Outbound Interface	Select which interfaces the broadcast packets will be routed to.	Drop-down list of interfaces	N/A

Edit Static Multicast Route

Menu Path: Routing > Multicast Route > Static Multicast Route

Clicking the **Edit (✎)** icon for an entry on the **Routing > Multicast Route > Static Multicast Route** page will open this dialog box. This dialog lets you modify an existing static multicast route. Click **APPLY** to save your changes.



Edit Static Multicast Route

Status *
Disabled

Group Address *
239.255.255.255

Source Address Type *
Any

Inbound Interface *
WAN

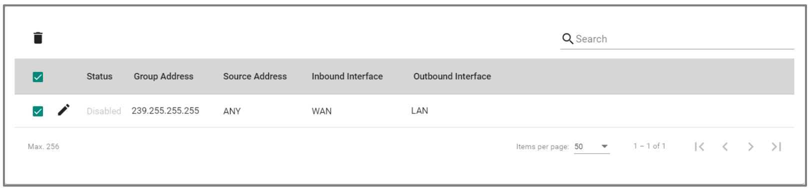
Outbound Interface *
LAN

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this route.	Enabled / Disabled	Enabled
Group Address	Specify the group IP address for this route.	N/A	N/A
Source Address Type	Specify the type of source address to use for this route. **Any**: Allow any IP to be the source address. **Specify Source**: Use the specified **Source Address**.	Any / Specify Source	Any
Source Address **(Only if Source Address Type is Specify Source)**	Specify the source IP address to use for this route.	N/A	N/A
Inbound Interface	Select which interface broadcast packets will come from.	Drop-down list of interfaces	N/A
Outbound Interface	Select which interfaces the broadcast packets will be routed to.	Drop-down list of interfaces	N/A

Delete Static Multicast Route

Menu Path: Routing > Multicast Route > Static Multicast Route

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.



Search

☑		Status	Group Address	Source Address	Inbound Interface	Outbound Interface
☑	✎	Disabled	239.255.255.255	ANY	WAN	LAN

Max. 256

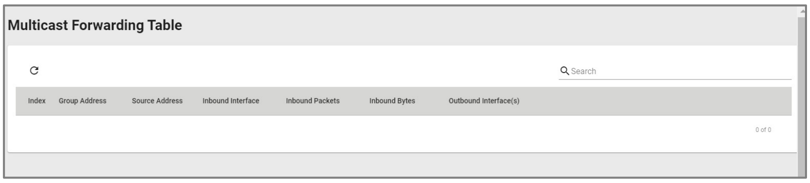
Items per page: 50

1 – 1 of 1

Multicast Forwarding Table

Menu Path: Routing > Multicast Route > Multicast Forwarding Table

This page lets you see the multicast forwarding table for your device.



Multicast Forwarding Table

Search

Index	Group Address	Source Address	Inbound Interface	Inbound Packets	Inbound Bytes	Outbound Interface(s)

0 of 0

UI Setting	Description
Index	Shows the index of the entry.
Group Address	Shows the group IP address of the entry.
Source Address	Shows the source address of the entry.
Inbound Interface	Shows the inbound interface of the entry.
Inbound Packets	Shows the number of inbound packets for the entry.
Inbound Bytes	Shows the size of the inbound payload (in bytes) for the entry.
Outbound Interface(s)	Shows the outbound interfaces of the entry.

Broadcast Forwarding

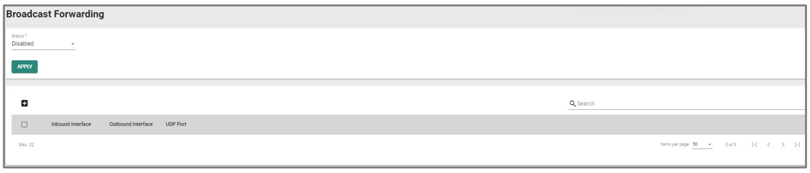
Menu Path: Routing > Broadcast Forwarding

This page lets you set up broadcast forwarding. Broadcast forwarding enables users to specify the interface and UDP ports that broadcast packets will use to pass through the router, allowing devices to be queried on the network, such as Modbus devices.

Limitations

You can create up to 32 broadcast forwarding entries.

Broadcast Forwarding Settings



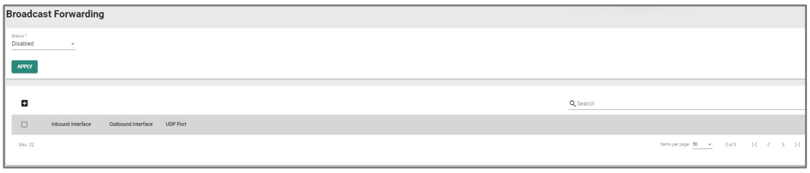
Broadcast Forwarding

Status *: Disabled

☐	Inbound Interface	Outbound Interface	UDP Port

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable broadcast forwarding.	Enabled / Disabled	Disabled

Broadcast Forwarding List



Broadcast Forwarding

Status *: Disabled

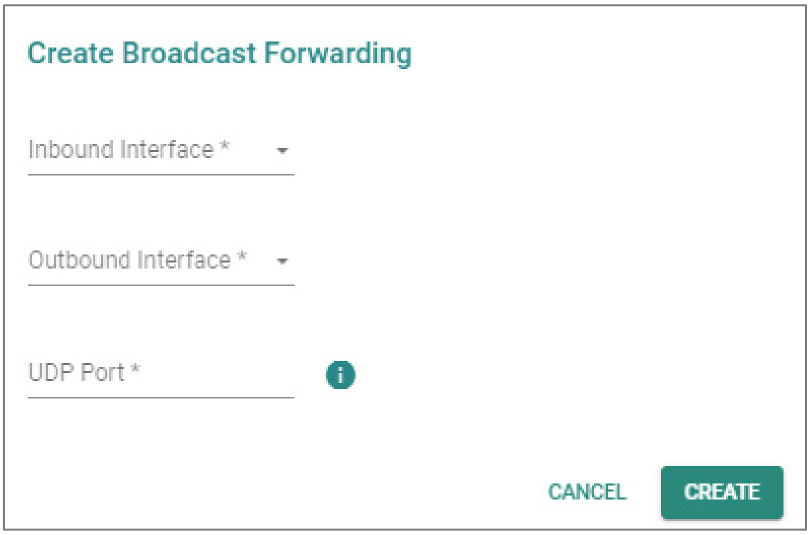
☐	Inbound Interface	Outbound Interface	UDP Port

UI Setting	Description
Inbound Interface	Shows which interface broadcast packets will come from.
Outbound Interface	Shows which interface broadcast packets will pass through.
UDP Port	Shows the UDP ports the device will listen to for broadcast packets.

Create Broadcast Forwarding

Menu Path: Routing > Broadcast Forwarding

Clicking the **Add (⊞)** icon on the **Routing > Broadcast Forwarding** page will open this dialog box. This dialog lets you create a new broadcast forwarding rule.
Click **CREATE** to save your changes and add the new rule.



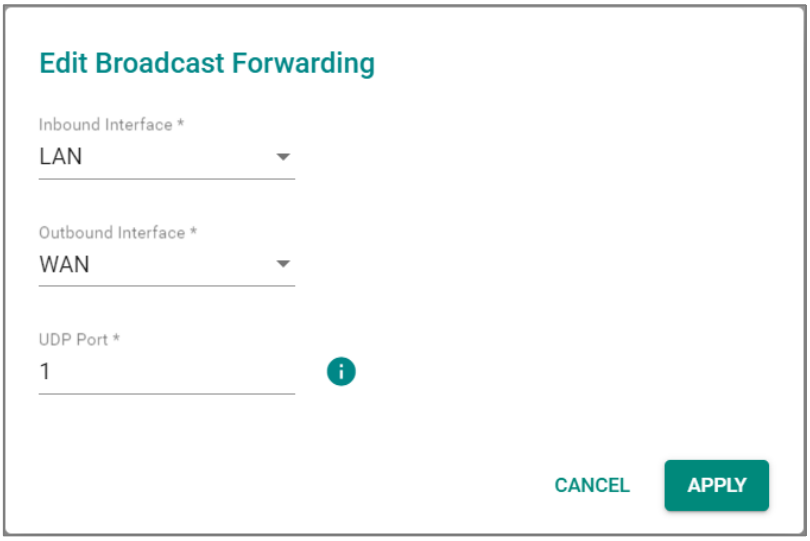
UI Setting	Description	Valid Range	Default Value
Inbound Interface	Select which interface broadcast packets will come from.	Drop-down list of interfaces	N/A
Outbound Interface	Select which interface broadcast packets will pass through.	Drop-down list of interfaces	N/A

UI Setting	Description	Valid Range	Default Value
UDP Port	Specify which UDP ports the device will listen to for broadcast packets. You can enter up to 8 ports, separated by commas.	1 to 65535, up to 8 ports separated by commas	N/A

Edit Broadcast Forwarding

Menu Path: Routing > Broadcast Forwarding

Clicking the **Edit (✎)** icon for an entry on the **Insert > Path Here** page will open this dialog box. This dialog lets you modify an existing broadcast forwarding rule.
Click **APPLY** to save your changes.



Edit Broadcast Forwarding

Inbound Interface *: LAN

Outbound Interface *: WAN

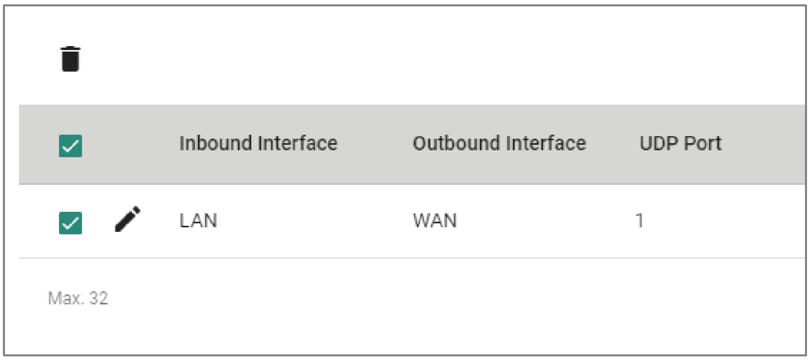
UDP Port *: 1

UI Setting	Description	Valid Range	Default Value
Inbound Interface	Select which interface broadcast packets will come from.	Drop-down list of interfaces	N/A
Outbound Interface	Select which interface broadcast packets will pass through.	Drop-down list of interfaces	N/A
UDP Port	Specify which UDP ports the device will listen to for broadcast packets. You can enter up to 8 ports, separated by commas.	1 to 65535, up to 8 ports separated by commas	N/A

Delete Broadcast Forwarding

Menu Path: Routing > Broadcast Forwarding

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.



☑		Inbound Interface	Outbound Interface	UDP Port
☑	✎	LAN	WAN	1

Max. 32

NAT

Menu Path: NAT

This page allows you to manage your Network Address Translation (NAT) rules.

Limitations

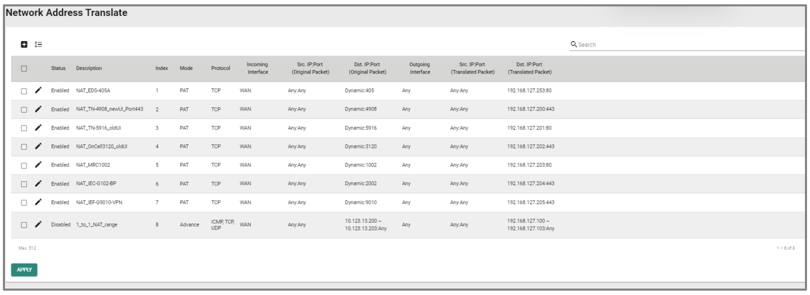
You can create up to 512 NAT rules.

NAT - User Privileges

Privileges to NAT 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
NAT Setting	R/W	R/W	R

NAT Rule List



Network Address Translate

Search

□		Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)
□		Enabled	NAT_EDS-405A	1	PAT	TCP	WAN	Any:Any	Dynamic:405	Any	Any:Any	192.168.127.253:80
□		Enabled	NAT_TN-4908_newUI_Port443	2	PAT	TCP	WAN	Any:Any	Dynamic:4908	Any	Any:Any	192.168.127.200:443
□		Enabled	NAT_TN-5916_oldUI	3	PAT	TCP	WAN	Any:Any	Dynamic:5916	Any	Any:Any	192.168.127.201:80
□		Enabled	NAT_OnCell3120_oldUI	4	PAT	TCP	WAN	Any:Any	Dynamic:3120	Any	Any:Any	192.168.127.202:443
□		Enabled	NAT_MRC1002	5	PAT	TCP	WAN	Any:Any	Dynamic:1002	Any	Any:Any	192.168.127.203:80
□		Enabled	NAT_IEC-G102-BP	6	PAT	TCP	WAN	Any:Any	Dynamic:2002	Any	Any:Any	192.168.127.204:443
□		Enabled	NAT_IEF-G9010-VPN	7	PAT	TCP	WAN	Any:Any	Dynamic:9010	Any	Any:Any	192.168.127.205:443
□		Disabled	1_to_1_NAT_range	8	Advance	ICMP, TCP, UDP	WAN	Any:Any	10.123.13.200 ~ 10.123.13.203:Any	Any	Any:Any	192.168.127.100 ~ 192.168.127.103:Any

Max. 512

1 – 8 of 8

UI Setting	Description
Status	Shows whether the NAT rule is enabled or disabled.
Description	Shows the name of the NAT rule.
Index	Shows the index of the NAT rule.
Mode	Shows the NAT mode used by the rule.
Protocol	Shows the protocols included in the NAT rule.
Incoming Interface	Shows the incoming interface.
Src. IP:Port (Original Packet)	Shows the original source IP address and ports for incoming packets.
Dst. IP:Port (Original Packet)	Shows the original destination IP address and ports for incoming packets.
Outgoing Interface	Shows the outgoing interface.
Src. IP:Port (Translated Packet)	Shows the translated source IP address and ports.
Dst. IP:Port (Translated Packet)	Shows the translated destination IP address and ports.

Create Index

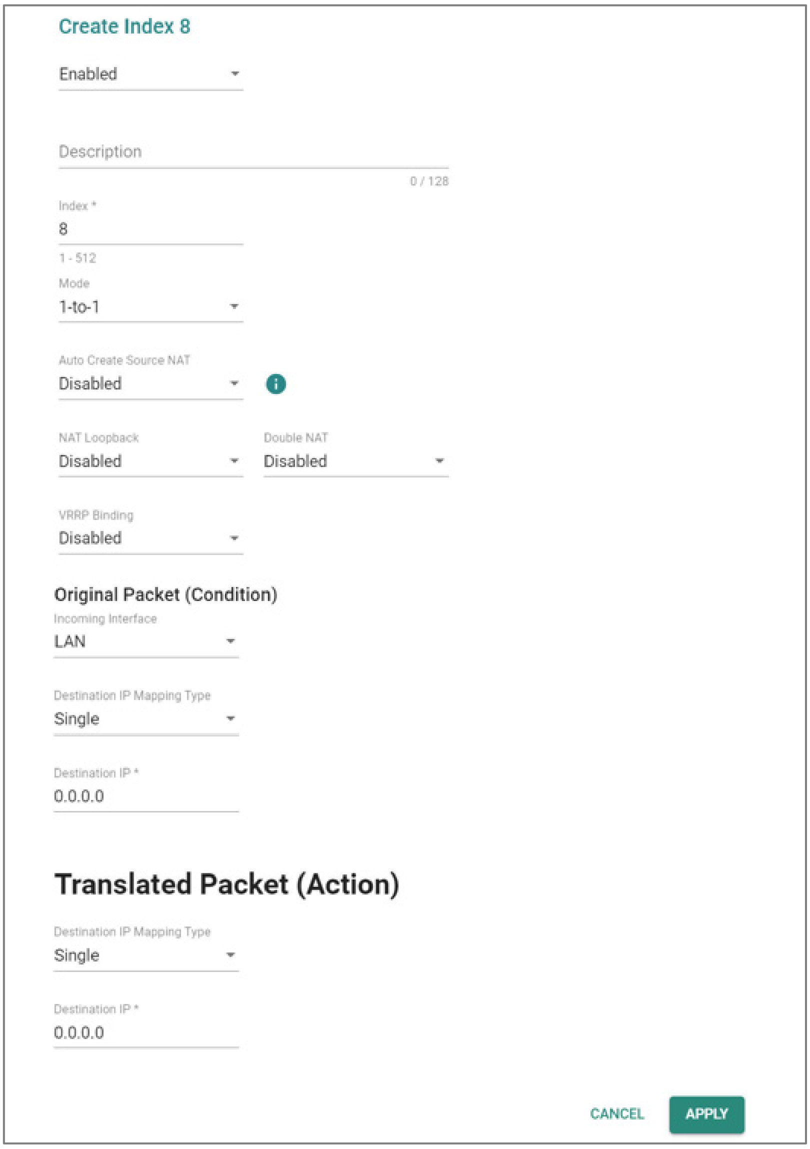
Menu Path: Main > NAT

Clicking the **Add (⊞)** icon on the **Main > NAT** page will open this dialog box. This dialog lets you create a new NAT rule. Click **CREATE** to save your changes and add the new rule.

Available settings will change depending on what **Mode** is selected.

Create Index - 1-to-1 NAT

If **1-to-1** is selected for the **Mode**, these settings will appear. 1-to-1 NAT maps one public IP address to one private IP address.



Create Index 8

Enabled

Description

0 / 128

Index *

8

1 - 512

Mode

1-to-1

Auto Create Source NAT

Disabled

NAT Loopback

Disabled

Double NAT

Disabled

VRRP Binding

Disabled

Original Packet (Condition)

Incoming Interface

LAN

Destination IP Mapping Type

Single

Destination IP *

0.0.0.0

Translated Packet (Action)

Destination IP Mapping Type

Single

Destination IP *

0.0.0.0

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this rule.	Enabled / Disabled	Enabled
Description	Specify a name for this rule.	1 to 128 characters	N/A
Index	Specify the index of this rule.	1 to 512	N/A

UI Setting	Description	Valid Range	Default Value
Mode	Specify which NAT mode to use for this rule**.** **1-to-1**: 1-to-1 NAT maps one public IP address to one private IP address. **N-to-1**: N-to-1 NAT maps multiple private IP addresses to one public IP address. **PAT**: Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers. **Advance**: Allows you to set up an advanced NAT rule.	1-to-1 / N-to-1 / PAT / Advance	1-to-1
Auto Create Source NAT	Enable or disable the Auto Create Source NAT feature. If this is disabled, 1-to-1 NAT will only perform DNAT.	Enabled / Disabled	Disabled
NAT Loopback	Enable or disable NAT Loopback. NAT loopback allows devices on a private network to access a server or service hosted on the same network using the public IP address of the network.	Enabled / Disabled	Disabled
Double NAT	Enable or disable Double NAT. Double NAT enables you to use 1-to-1 rules to facilitate two-way communication.	Enabled / Disabled	Disabled
VRRP Binding	Select which VRRP index this rule should use, or disable VRRP binding. Virtual Router Redundancy Protocol (VRRP) Binding is a feature that allows the 1-to-1 NAT rule to be bound to a VRRP index. VRRP Binding is only supported in 1-to-1 NAT. If a VRRP index is selected, the 1-to-1 NAT rule is only valid when the system is the master. If no VRRP index is selected, the 1-to-1 NAT rule will be valid regardless of whether the system is the master or backup.	Disabled / VRRP Index No.	Disabled

Original Packet (Condition)

UI Setting	Description	Valid Range	Default Value
Incoming Interface	Select the interface to use for this rule.	Drop-down list of interfaces	LAN

UI Setting	Description	Valid Range	Default Value
Destination IP Mapping Type	Specify which destination IP addresses will be handled for incoming packets. **Single**: This rule will apply to a single destination IP for incoming packets. **Range**: This rule will apply to a range of destination IPs for incoming packets. With the 'Range' option, you have the capability to establish several 1-to-1 NAT mappings within a designated IP address range. It's essential to ensure that the 'Range' values in the Original Packet (Condition) align precisely with those in the Translated Packet (Action) for accurate Destination IP Mapping.	Single / Range	Single
Destination IP **(Only if Destination IP Mapping Type is Single)**	Specify the destination IP this rule will apply to.	Valid IP address	0.0.0.0
Destination IP: Start **(Only for Destination IP Mapping Type is Range)**	Specify the start of the destination IP range this rule will apply to.	Valid IP address	0.0.0.0
Destination IP: End **(Only if Destination IP Mapping Type is Range)**	Specify the end of the destination IP range this rule will apply to.	Valid IP address	0.0.0.0

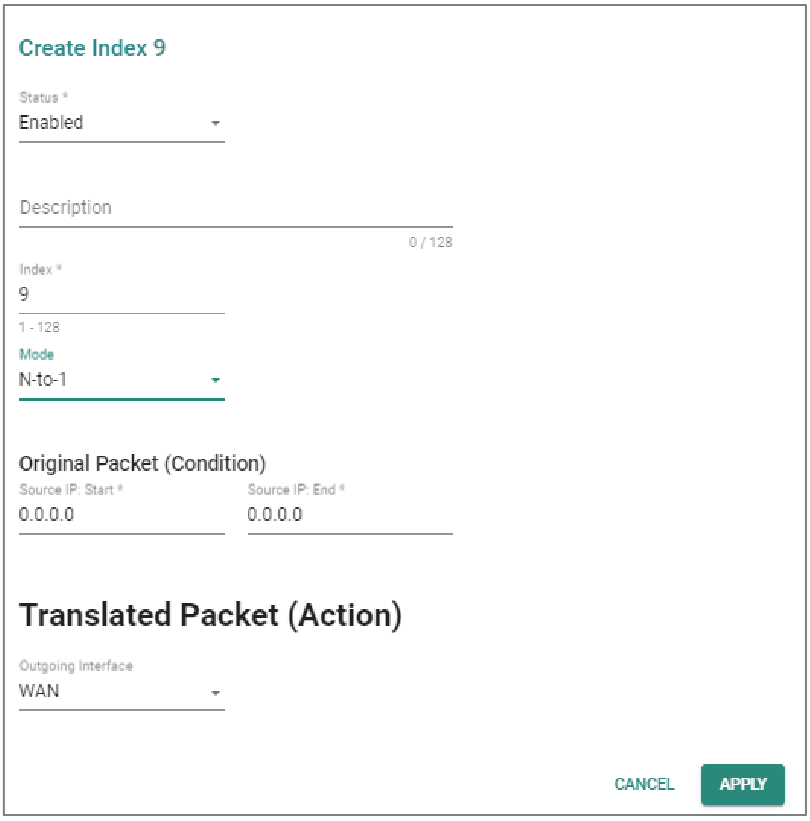
Translated Packet (Action)

UI Setting	Description	Valid Range	Default Value
Destination IP Mapping Type	Specify how to handle the destination IP address translation for the internal network. **Single**: Packets will be translated to a single IP address. **Range**: Packets will be translated to a range of IP addresses. With the 'Range' option, you have the capability to establish several 1-to-1 NAT mappings within a designated IP address range. It's essential to ensure that the 'Range' values in the Original Packet (Condition) align precisely with those in the Translated Packet (Action) for accurate Destination IP Mapping.	Single / Range	Single

UI Setting	Description	Valid Range	Default Value
Destination IP **(Only if Destination IP Mapping Type is Single)**	Specify the destination IP to translate to on the internal network.	Valid IP address	0.0.0.0
Destination IP: Start **(Only for Destination IP Mapping Type is Range)**	Specify the start of the destination IP range to translate to on the internal network.	Valid IP address	0.0.0.0
Destination IP: End **(Only if Destination IP Mapping Type is Range)**	Specify the end of the destination IP range to translate to on the internal network.	Valid IP address	0.0.0.0

Create Index - N-to-1 NAT

If **N-to-1** is selected for the **Mode**, these settings will appear. N-to-1 NAT maps multiple private IP addresses to one public IP address.



Create Index 9

Status * Enabled

Description 0 / 128

Index * 9 1 - 128

Mode N-to-1

Original Packet (Condition)

Source IP: Start * 0.0.0.0

Source IP: End * 0.0.0.0

Translated Packet (Action)

Outgoing Interface WAN

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this rule.	Enabled / Disabled	Enabled
Description	Specify a name for this rule.	1 to 128 characters	N/A
Index	Specify the index of this rule.	1 to 512	N/A
Mode	Specify which NAT mode to use for this rule**.** **1-to-1**: 1-to-1 NAT maps one public IP address to one private IP address. **N-to-1**: N-to-1 NAT maps multiple private IP addresses to one public IP address. **PAT**: Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers. **Advance**: Allows you to set up an advanced NAT rule.	1-to-1 / N-to-1 / PAT / Advance	1-to-1

Original Packet (Condition)

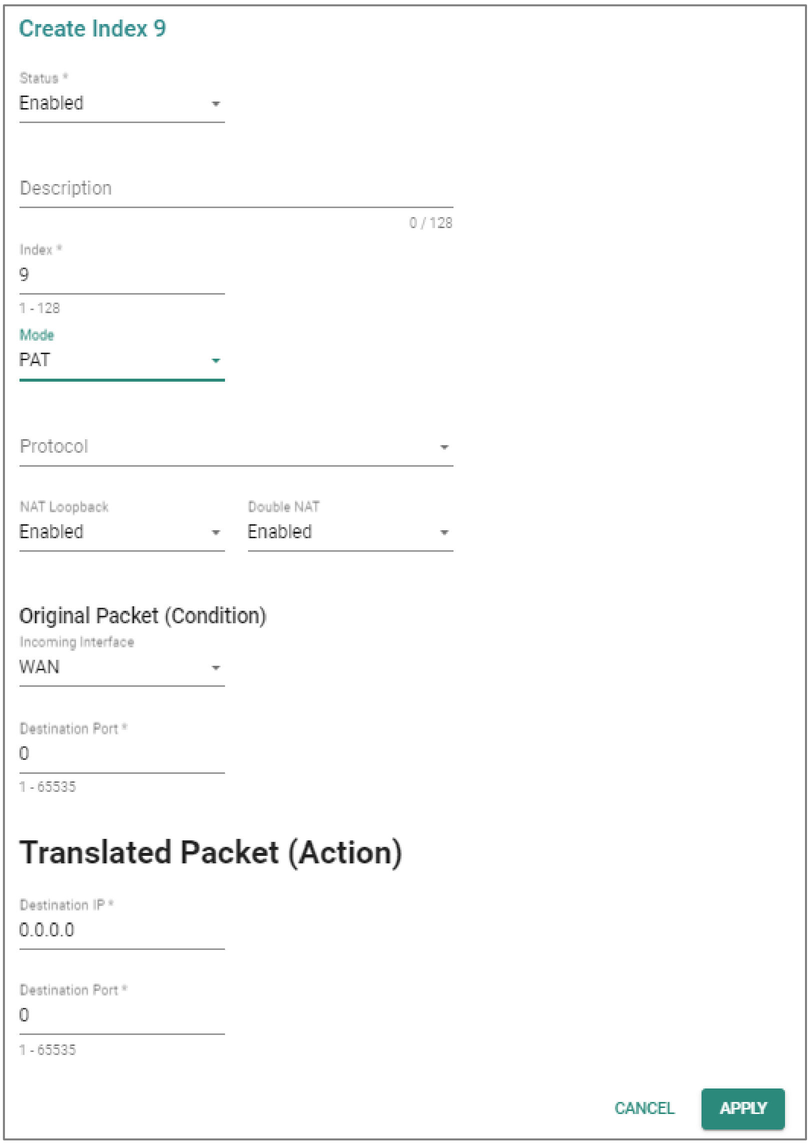
UI Setting	Description	Valid Range	Default Value
Source IP: Start	Specify the starting IP address of the source IP range this rule will apply to.	Valid IP address	0.0.0.0
Source IP: End	Specify the starting IP address of the source IP range this rule will apply to.	Valid IP address	0.0.0.0

Translated Packet (Action)

UI Setting	Description	Valid Range	Default Value
Outgoing Interface	Select the interface for the NAT rule.	Drop-down list of interfaces	Any

Create Index - PAT

If **PAT** is selected for the **Mode**, these settings will appear. Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers.



Create Index 9

Status *
Enabled

Description
0 / 128

Index *
9
1 - 128

Mode
PAT

Protocol

NAT Loopback
Enabled

Double NAT
Enabled

Original Packet (Condition)

Incoming Interface
WAN

Destination Port *
0
1 - 65535

Translated Packet (Action)

Destination IP *
0.0.0.0

Destination Port *
0
1 - 65535

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this rule.	Enabled / Disabled	Enabled
Description	Specify a name for this rule.	1 to 128 characters	N/A
Index	Specify the index of this rule.	1 to 512	N/A

UI Setting	Description	Valid Range	Default Value
Mode	Specify which NAT mode to use for this rule**.** **1-to-1**: 1-to-1 NAT maps one public IP address to one private IP address. **N-to-1**: N-to-1 NAT maps multiple private IP addresses to one public IP address. **PAT**: Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers. **Advance**: Allows you to set up an advanced NAT rule.	1-to-1 / N-to-1 / PAT / Advance	1-to-1
Protocol	Select which protocols this rule will include.	ICMP / TCP / UDP	N/A
NAT Loopback	Enable or disable NAT Loopback. NAT loopback allows devices on a private network to access a server or service hosted on the same network using the public IP address of the network.	Enabled / Disabled	Disabled
Double NAT	Enable or disable Double NAT. Double NAT enables you to use 1-to-1 rules to facilitate two-way communication.	Enabled / Disabled	Disabled

Original Packet (Condition)

UI Setting	Description	Valid Range	Default Value
Incoming Interface	Select the interface to use for this rule.	Drop-down list of interfaces	LAN
Destination Port	Specify the destination port this rule will apply to.	1 to 65535	Any

Translated Packet (Action)

UI Setting	Description	Valid Range	Default Value
Destination IP	Specify the destination IP to translate to on the internal network.	Valid IP address	0.0.0.0
Destination Port	Specify the port number to translate to on the internal network.	1 to 65535	0

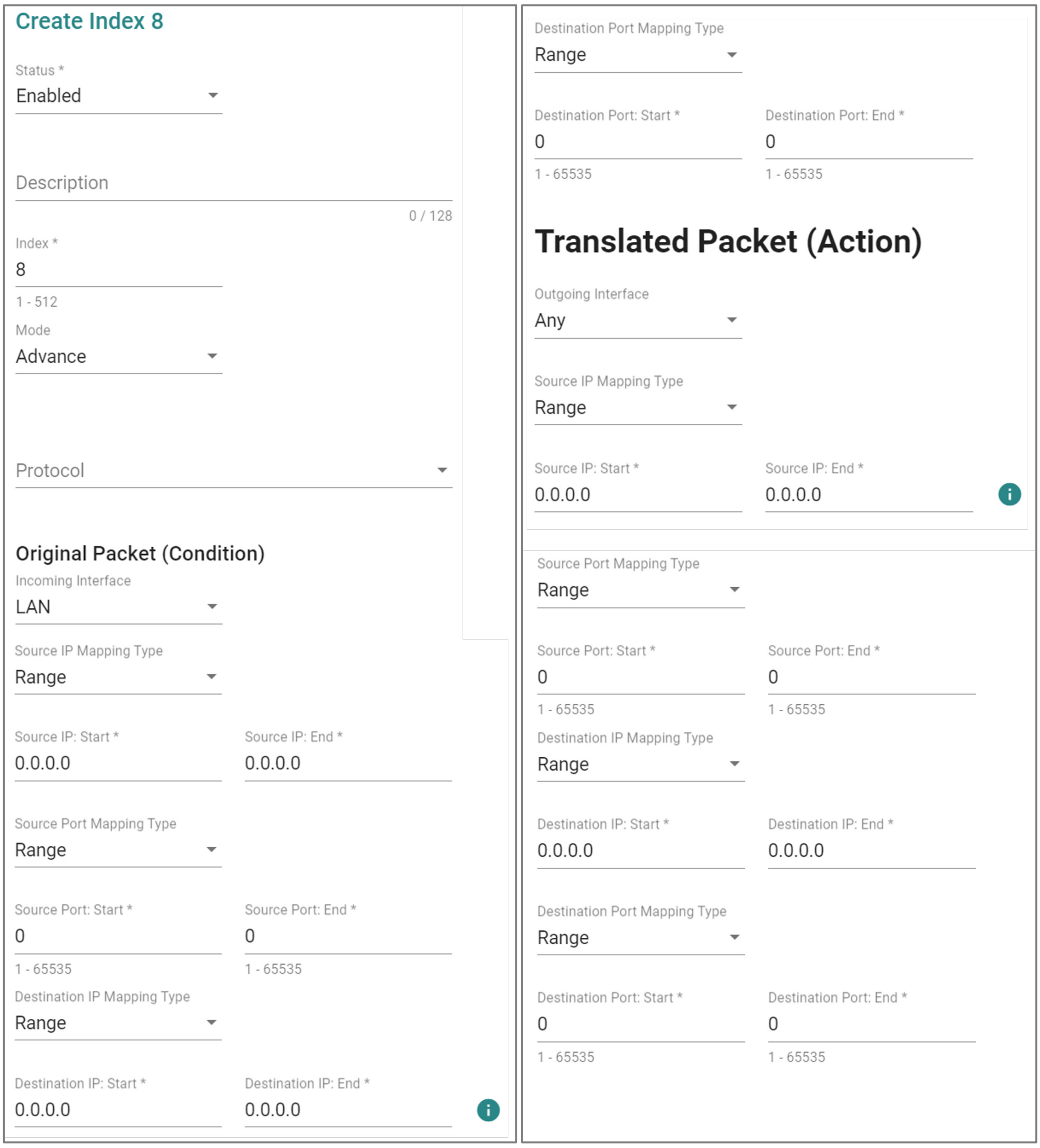
Create Index - Advance

If **Advance** is selected for the **Mode**, these settings will appear. This mode allows you to set up an advanced NAT rule, which can provide you with more flexibility for NAT configuration.

Note

Please keep these in mind before setting up an advanced NAT rule:

- When using a **Range**, please ensure that the corresponding **Range** values are consistent.
- NAT Advance Mode only allows for a single range to be entered and does not support configuring multiple ranges in the same rule.
- Port settings can only be configured when the Protocol includes either TCP or UDP.
- If a **Translated Destination IP** is used, the **Outgoing Interface** cannot be configured.
- If the **Translated Source IP** is set to **Dynamic**, the **Translated Source Port** cannot be set.



Create Index 8

Status *
Enabled

Description
0 / 128

Index *
8
1 - 512

Mode
Advance

Protocol

Original Packet (Condition)

Incoming Interface
LAN

Source IP Mapping Type
Range

Source IP: Start *
0.0.0.0

Source IP: End *
0.0.0.0

Source Port Mapping Type
Range

Source Port: Start *
0
1 - 65535

Source Port: End *
0
1 - 65535

Destination IP Mapping Type
Range

Destination IP: Start *
0.0.0.0

Destination IP: End *
0.0.0.0

Destination Port Mapping Type
Range

Destination Port: Start *
0
1 - 65535

Destination Port: End *
0
1 - 65535

Translated Packet (Action)

Outgoing Interface
Any

Source IP Mapping Type
Range

Source IP: Start *
0.0.0.0

Source IP: End *
0.0.0.0

Source Port Mapping Type
Range

Source Port: Start *
0
1 - 65535

Source Port: End *
0
1 - 65535

Destination IP Mapping Type
Range

Destination IP: Start *
0.0.0.0

Destination IP: End *
0.0.0.0

Destination Port Mapping Type
Range

Destination Port: Start *
0
1 - 65535

Destination Port: End *
0
1 - 65535

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this rule.	Enabled / Disabled	Enabled
Description	Specify a name for this rule.	1 to 128 characters	N/A
Index	Specify the index of this rule.	1 to 512	N/A

UI Setting	Description	Valid Range	Default Value
Mode	Specify which NAT mode to use for this rule**.** **1-to-1**: 1-to-1 NAT maps one public IP address to one private IP address. **N-to-1**: N-to-1 NAT maps multiple private IP addresses to one public IP address. **PAT**: Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers. **Advance**: Allows you to set up an advanced NAT rule.	1-to-1 / N-to-1 / PAT / Advance	1-to-1
Protocol	Select which protocols this rule will include.	ICMP / TCP / UDP	N/A

Original Packet (Condition)

UI Setting	Description	Valid Range	Default Value
Incoming Interface	Select the interface to use for this rule.	Drop-down list of interfaces	LAN
Source IP Mapping Type	Specify which source IP addresses will be handled for incoming packets. **Any**: This rule will apply to all source IPs. **Single**: This rule will apply to a single source IP for incoming packets. **Range**: This rule will apply to a range of source IPs for incoming packets. **Subnet**: This rule will apply to a source IP and subnet mask.	Any / Single / Range / Subnet	Any
Source IP **(Only if Source IP Mapping Type is Single or Subnet)**	Specify the source IP this rule will apply to.	Valid IP address	0.0.0.0
Subnet Mask **(Only if Source IP Mapping Type is Subnet)**	Specify the subnet this rule will apply to.	Valid subnet	24 (255.255.255.0)
Source IP: Start **(Only if Source IP Mapping Type is Range)**	Specify the start of the source IP range this rule will apply to.	Valid IP address	0.0.0.0
Source IP: End **(Only if Source IP Mapping Type is Range)**	Specify the end of the source IP range this rule will apply to.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Source Port Mapping Type	Specify which source ports will be handled for incoming packets. **Any**: This rule will apply to all source ports. **Single**: This rule will apply to a single source port for incoming packets. **Range**: This rule will apply to a range of source ports for incoming packets.	Any / Single / Range	Any
Source Port **(Only if Source Port Mapping Type is Single)**	Specify the source port this rule will apply to.	1 to 65535	N/A
Source Port: Start **(Only if Source Port Mapping Type is Range)**	Specify the start of the source port range this rule will apply to.	1 to 65535	N/A
Source Port: End **(Only if Source Port Mapping Type is Range)**	Specify the end of the source port range this rule will apply to.	1 to 65535	N/A
Destination IP Mapping Type	Specify which destination IP addresses will be handled for incoming packets. **Any**: This rule will apply to all destination IPs. **Single**: This rule will apply to a single destination IP for incoming packets. **Range**: This rule will apply to a range of destination IPs for incoming packets. **Subnet**: This rule will apply to a destination IP and subnet mask.	Any / Single / Range / Subnet	Any
Destination IP **(Only if Destination IP Mapping Type is Single or Subnet)**	Specify the destination IP this rule will apply to. **Note** If your host is directly connected to the device or connected through a L2 switch, and the original destination IP is in the hosts' subnet but different from the incoming interface IP, you may add the original destination IP as a secondary IP for the incoming interface so the device can receive and use NAT for traffic from the host. Refer to Network Configuration > Network Interfaces - Secondary IP for more information.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Subnet Mask **(Only if Destination IP Mapping Type is Subnet)**	Specify the subnet this rule will apply to.	Valid subnet	24 (255.255.255.0)
Destination IP: Start **(Only for Destination IP Mapping Type is Range)**	Specify the start of the destination IP range this rule will apply to.	Valid IP address	0.0.0.0
Destination IP: End **(Only if Destination IP Mapping Type is Range)**	Specify the end of the destination IP range this rule will apply to.	Valid IP address	0.0.0.0
Destination Port Mapping Type	Specify which destination ports will be handled for incoming packets. **Any**: This rule will apply to all destination ports. **Single**: This rule will apply to a single destination port for incoming packets. **Range**: This rule will apply to a range of destination ports for incoming packets.	Any / Single / Range	Any
Destination Port **(Only if Destination Port Mapping Type is Single)**	Specify the destination port this rule will apply to.	1 to 65535	N/A
Destination Port: Start **(Only if Destination Port Mapping Type is Range)**	Specify the start of the destination port range this rule will apply to.	1 to 65535	N/A
Destination IP: End **(Only if Destination Port Mapping Type is Range)**	Specify the end of the destination port range this rule will apply to.	1 to 65535	N/A

Translated Packet (Action)

UI Setting	Description	Valid Range	Default Value
Outgoing Interface	Select the interface for the NAT rule.	Drop-down list of interfaces	Any

UI Setting	Description	Valid Range	Default Value
Source IP Mapping Type	Specify how to handle source IP translation for the internal network. **Any**: This rule will translate to all source IPs. **Single**: This rule will translate to a single source IP. **Range**: This rule will translate to a range of source IPs. **Subnet**: This rule will translate to a source IP and subnet mask. **Dynamic**:	Any / Single / Range / Subnet / Dynamic	Any
Source IP **(Only if Source IP Mapping Type is Single or Subnet)**	Specify the source IP this rule will translate to. **Note** If **Source IP Mapping Type** is **Single**, if the destination host for the desired traffic is directly connected to the device or connected through a L2 switch, and the translated source IP is in the hosts' subnet but different from the outgoing interface IP, you may add the translated source IP as a secondary IP for the outgoing interface so the device can receive and use NAT for traffic going to the destination host. Refer to Network Configuration > Network Interfaces - Secondary IP for more information.	Valid IP address	0.0.0.0
Subnet Mask **(Only if Source IP Mapping Type is Subnet)**	Specify the subnet this rule will translate to.	Valid subnet	24 (255.255.255.0)
Source IP: Start **(Only if Source IP Mapping Type is Range)**	Specify the start of the source IP range this rule will translate to.	Valid IP address	0.0.0.0
Source IP: End **(Only if Source IP Mapping Type is Range)**	Specify the end of the source IP range this rule will translate to.	Valid IP address	0.0.0.0
Source Port Mapping Type	Specify how to handle source port translation for the internal network. **Any**: This rule will translate to all source ports. **Single**: This rule will translate to a single source port. **Range**: This rule will translate to a range of source ports.	Any / Single / Range	Any

UI Setting	Description	Valid Range	Default Value
Source Port **(Only if Source Port Mapping Type is Single)**	Specify the source port this rule will translate to.	1 to 65535	N/A
Source Port: Start **(Only if Source Port Mapping Type is Range)**	Specify the start of the source port range this rule will translate to.	1 to 65535	N/A
Source Port: End **(Only if Source Port Mapping Type is Range)**	Specify the end of the source port range this rule will translate to.	1 to 65535	N/A
Destination IP Mapping Type	Specify how to handle destination IP address translation for the internal network. **Any**: This rule will translate to all destination IPs. **Single**: This rule will translate to a single destination IP. **Range**: This rule will translate to a range of destination IPs. **Subnet**: This rule will translate to a destination IP and subnet mask.	Any / Single / Range / Subnet	Any
Destination IP **(Only if Destination IP Mapping Type is Single or Subnet)**	Specify the destination IP this rule will translate to.	Valid IP address	0.0.0.0
Subnet Mask **(Only if Destination IP Mapping Type is Subnet)**	Specify the subnet this rule will translate to.	Valid subnet	24 (255.255.255.0)
Destination IP: Start **(Only for Destination IP Mapping Type is Range)**	Specify the start of the destination IP range this rule will translate to.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Destination IP: End **(Only if Destination IP Mapping Type is Range)**	Specify the end of the destination IP range this rule will translate to.	Valid IP address	0.0.0.0
Destination Port Mapping Type	Specify how to handle destination port translation for the internal network. **Any**: This rule will apply to all destination ports. **Single**: This rule will apply to a single destination port for incoming packets. **Range**: This rule will apply to a range of destination ports for incoming packets.	Any / Single / Range	Any
Destination Port **(Only if Destination Port Mapping Type is Single)**	Specify the destination port this rule will translate to.	1 to 65535	N/A
Destination Port: Start **(Only if Destination Port Mapping Type is Range)**	Specify the start of the destination port range this rule will translate to.	1 to 65535	N/A
Destination Port: End **(Only if Destination Port Mapping Type is Range)**	Specify the end of the destination port range this rule will translate to.	1 to 65535	N/A

Object Management

Menu Path: Object Management

This page lets you use object-based firewall management to help protect your network on a granular level.

Object Management - User Privileges

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

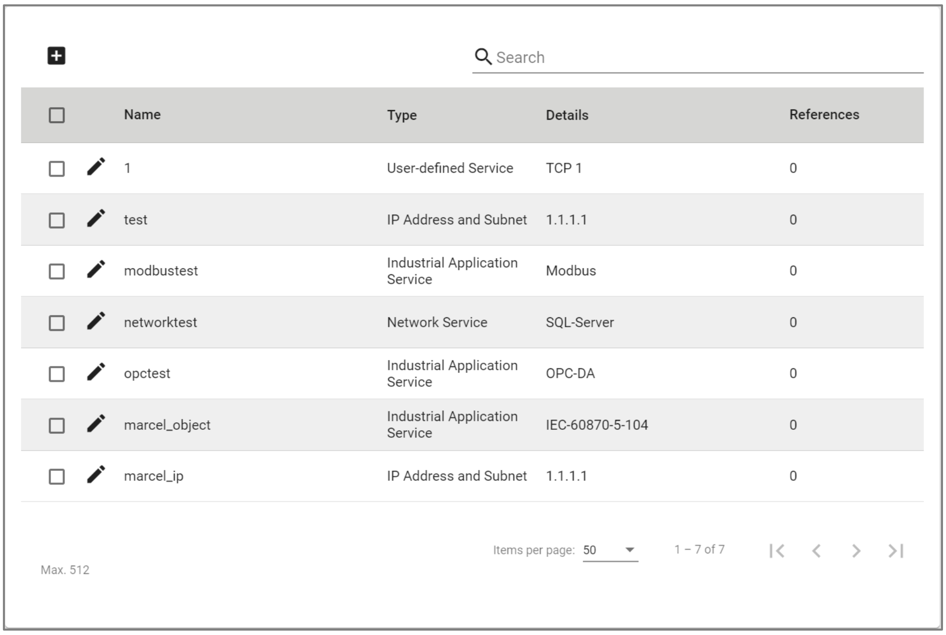
Settings	Admin	Supervisor	User
Object Management	R/W	R/W	R

You can create, modify, and edit the objects you need based on your security requirements. These objects are used when creating Layer 3-7 policies for the device's firewall.

In addition, objects allow for more efficient firewall rule management. A single object can be assigned to multiple rules and changes to the object will apply to all associated rules, removing the need to update individual policies one by one.

Limitations

You can create up to 512 objects.



		Name	Type	Details	References
□	✎	1	User-defined Service	TCP 1	0
□	✎	test	IP Address and Subnet	1.1.1.1	0
□	✎	modbustest	Industrial Application Service	Modbus	0
□	✎	networktest	Network Service	SQL-Server	0
□	✎	opctest	Industrial Application Service	OPC-DA	0
□	✎	marcel_object	Industrial Application Service	IEC-60870-5-104	0
□	✎	marcel_ip	IP Address and Subnet	1.1.1.1	0

Items per page: 50

1 – 7 of 7

Max. 512

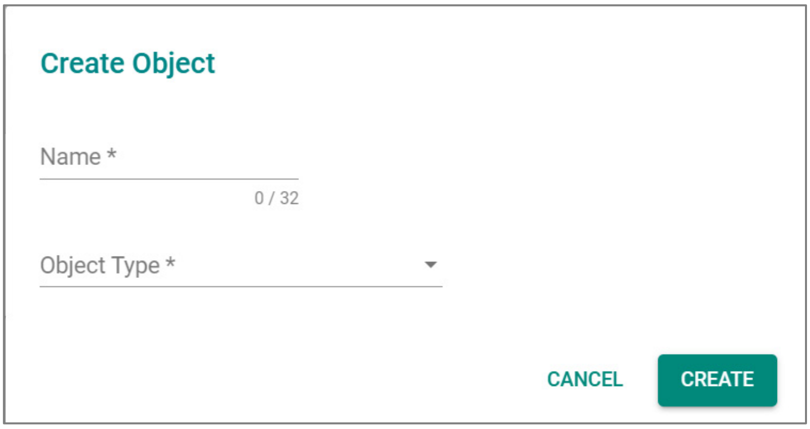
UI Setting	Description
Name	Shows the name of the object.
Type	Shows the type of the object.
Details	Shows the settings for the object. These settings will vary depending on the object's **Type**.
References	Shows the number of times this object is referenced in firewall rules.

Create Object

Menu Path: Main > Object Management

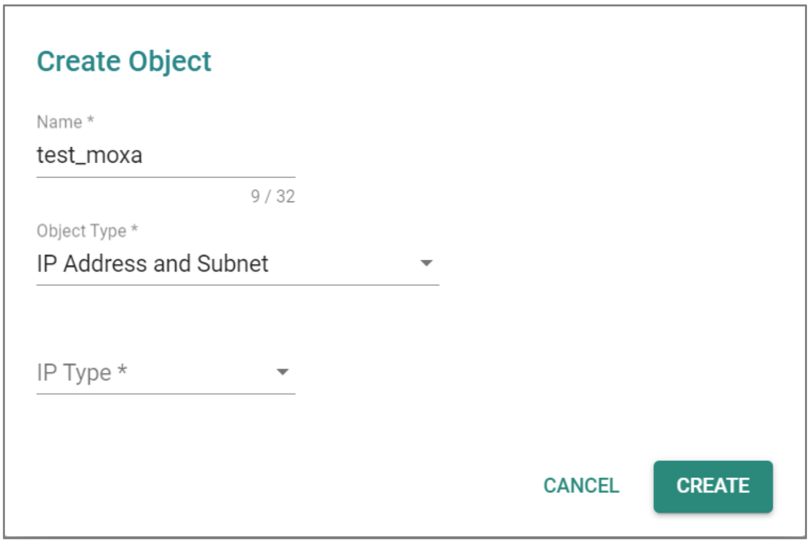
Clicking the **Add (⊞)** icon on the **Main > Object Management** page will open this dialog box. This dialog lets you create a new object. Click **CREATE** to save your changes and add the new object.

The available settings will vary depending on which **Object Type** is selected.



Create Object - IP Address and Subnet

If **IP Address and Subnet** is selected for the **Object Type**, these settings will appear.



Name *
test_moxa
9 / 32

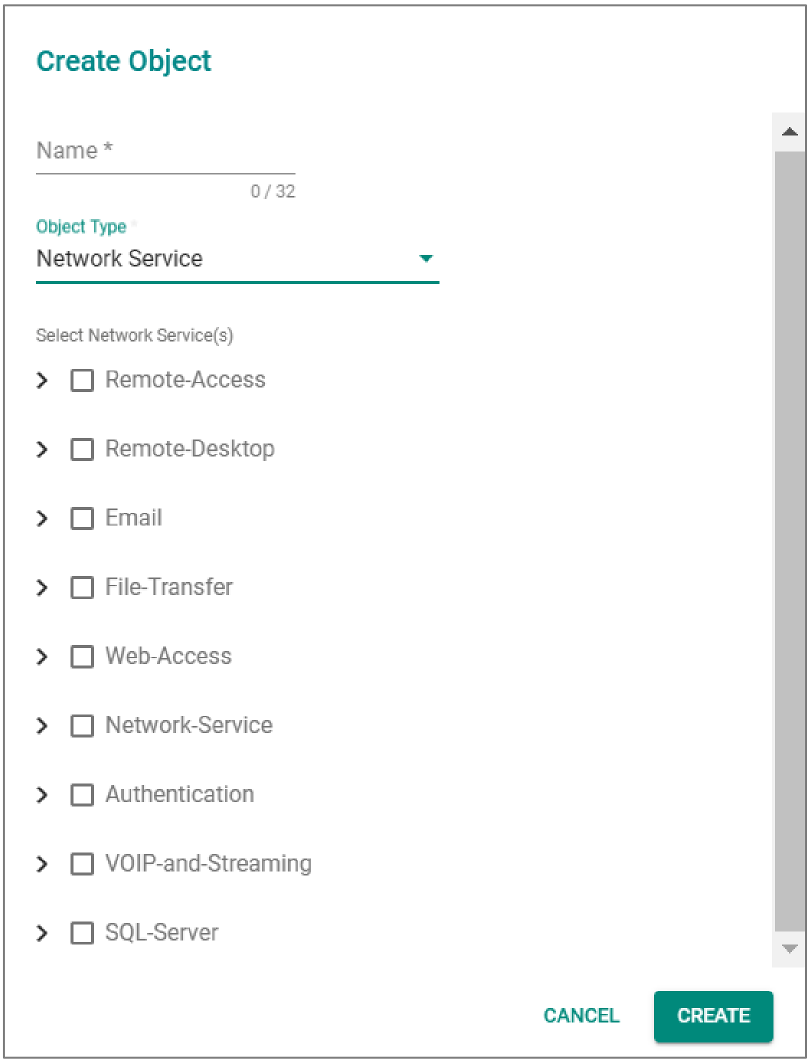
Object Type *
IP Address and Subnet

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
Object Type	Select a type for the object. **IP Address and Subnet**: You can specify an IP address, a range of IP addresses, or a subnet. **Network Service**: You can select from a list of protocol and port combinations used for common network services. **Industrial Application Service**: You can select from a list of protocol and port combinations used for industrial communications and applications. **User-defined Service**: You can specify your own protocol and port combination.	IP Address and Subnet / Network Service / Industrial Application Service / User-defined Service	N/A
IP Type	Select the type of IP address to use for the object.	Single IP / IP Range / Subnet	N/A
IP Address **(If Single is selected for IP Type)**	Specify the IP address to use for the object.	Valid IP Address	N/A
IP Address: Start **(If IP Range is selected for IP Type)**	Specify the start of the IP range to use for the object.	Valid IP Address	N/A
IP Address: End **(If IP Range is selected for IP Type)**	Specify the end of the IP range to use for the object.	Valid IP Address	N/A
Subnet **(If Subnet is selected for IP Type)**	Specify the IP address of the subnet to use for the object.	Valid IP Address	N/A
Subnet Mask **(If Subnet is selected for IP Type)**	Select the subnet mask to use for the object.	Drop-down list of subnet masks	N/A

Create Object - Network Service

If **Network Service** is selected for the **Object Type**, these settings will appear.



Create Object

Name *

0 / 32

Object Type *

Network Service

Select Network Service(s)

- › □ Remote-Access
- › □ Remote-Desktop
- › □ Email
- › □ File-Transfer
- › □ Web-Access
- › □ Network-Service
- › □ Authentication
- › □ VOIP-and-Streaming
- › □ SQL-Server

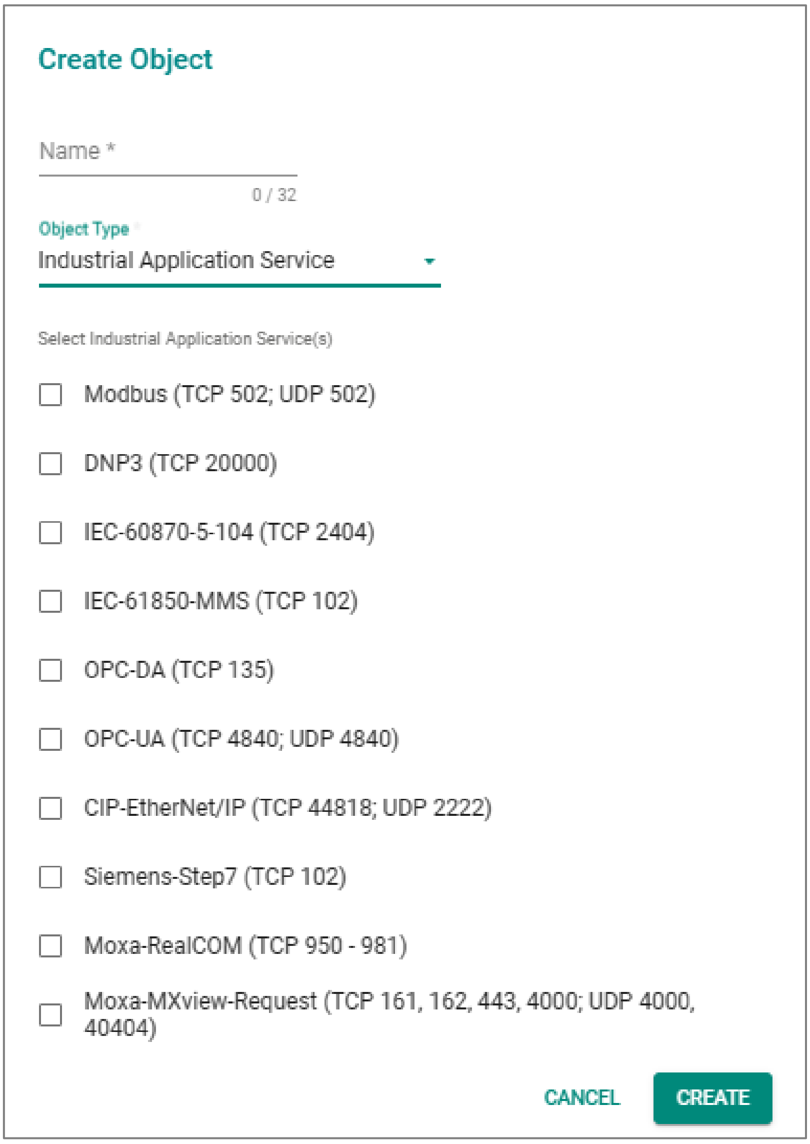
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
Object Type	Select a type for the object. **IP Address and Subnet**: You can specify an IP address, a range of IP addresses, or a subnet. **Network Service**: You can select from a list of protocol and port combinations used for common network services. **Industrial Application Service**: You can select from a list of protocol and port combinations used for industrial communications and applications. **User-defined Service**: You can specify your own protocol and port combination.	IP Address and Subnet / Network Service / Industrial Application Service / User-defined Service	N/A
Select Network Service(s)	Select a category of network services, or individual services to use for the object. You can select multiple options.	Remote-Access / Remote-Desktop / Email / File-Transfer / Web-Access / Network-Service / Authentication / VOIP-and-Streaming / SQL-Server	N/A
Remote-Access	This category includes protocols used for remote access to a device.	WINS (TCP 1512; UDP 1512) TELNET (TCP 23) SSH (TCP 22)	N/A
Remote-Desktop	This category includes protocols used by various remote desktop services.	PC-Anywhere (TCP 5631; UDP 5632) Chrome-Remote-Desktop (UDP 5222) AnyDesk (TCP 6568, 7070; UDP 50001 - 50003) Teamviewer (TCP 5938) RDP (TCP 3389) VNC (TCP 5900) X-WINDOW (TCP 6000 - 6063)	N/A
Email	This category includes protocols used for sending and receiving emails.	IMAP (TCP 143) IMAPS (TCP 993) POP3 (TCP 110) POP3S (TCP 995) SMTP (TCP 25) SMTPS (TCP 465)	N/A

UI Setting	Description	Valid Range	Default Value
File-Transfer	This category includes protocols used for different methods of file transfer.	FTP (TCP 21) FTPS (TCP 990) SFTP (TCP 115; UDP 115) TFTP (UDP 69) NFS (TCP 111, 2049; UDP 111, 2049) SAMBA (TCP 139) AFS3 (TCP 7000 - 7009; UDP 7000 - 7009) SMB (TCP 445)	N/A
Web-Access	This category includes protocols used by web browsers.	HTTP (TCP 80) HTTPS (TCP 443)	N/A
Network-Service	This category includes protocols used by various network services.	BGP (TCP 179) DHCP (UDP 67) DHCP6 (UDP 546) DNS (TCP 53; UDP 53) NTP (TCP 123; UDP 123) ICMP-PING (ICMP Type Any Code Any) OSPF (IP Protocol 89) RIP (TCP 520) SNMP (TCP 161 - 162; UDP 161 - 162) SYSLOG (UDP 514)	N/A
Authentication	This category includes protocols used by authentication services.	LDAP (TCP 389; UDP 389) LDAPS (TCP 636; UDP 636) RADIUS (UDP 1812 - 1813) TACACS+ (TCP 49; UDP 49)	N/A
VOIP-and-Streaming	This category includes protocols used for VOIP calling and streaming video.	SIP (TCP 5060; UDP 5060) RSTP (TCP 554, 7070, 8554; UDP 554)	N/A
SQL-Server	This category includes protocols used for SQL servers.	MS-SQL (TCP 1433 - 1434) MYSQL (TCP 3306)	N/A

Create Object - Industrial Application Service

If **Industrial Application Service** is selected for the **Object Type**, these settings will appear.



Create Object

Name *

0 / 32

Object Type *

Industrial Application Service

Select Industrial Application Service(s)

□ Modbus (TCP 502; UDP 502)

□ DNP3 (TCP 20000)

□ IEC-60870-5-104 (TCP 2404)

□ IEC-61850-MMS (TCP 102)

□ OPC-DA (TCP 135)

□ OPC-UA (TCP 4840; UDP 4840)

□ CIP-EtherNet/IP (TCP 44818; UDP 2222)

□ Siemens-Step7 (TCP 102)

□ Moxa-RealCOM (TCP 950 - 981)

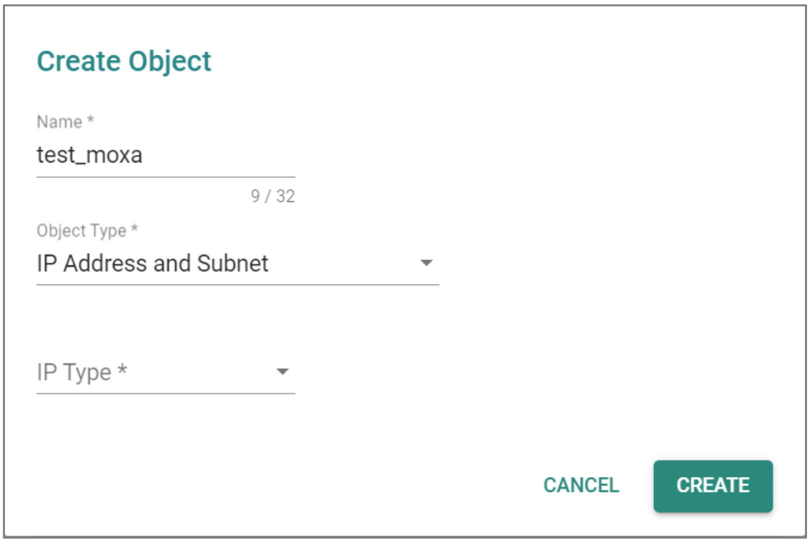
□ Moxa-MXview-Request (TCP 161, 162, 443, 4000; UDP 4000, 40404)

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
Object Type	Select a type for the object. **IP Address and Subnet**: You can specify an IP address, a range of IP addresses, or a subnet. **Network Service**: You can select from a list of protocol and port combinations used for common network services. **Industrial Application Service**: You can select from a list of protocol and port combinations used for industrial communications and applications. **User-defined Service**: You can specify your own protocol and port combination.	IP Address and Subnet / Network Service / Industrial Application Service / User-defined Service	N/A
Select Industrial Application Service(s)	Select a category of network services, or individual services to use for the object. You can select multiple options.	Modbus (TCP 502; UDP 502) DNP3 (TCP 20000) IEC-60870-5-104 (TCP 2404) IEC-61850-MMS (TCP 102) OPC-DA (TCP 135) OPC-UA (TCP 4840; UDP 4840) CIP-EtherNet/IP (TCP 44818; UDP 2222) Siemens-Step7 (TCP 102) Moxa-RealCOM (TCP 950 - 981) Moxa-MXview-Request (TCP 161, 162, 443, 4000; UDP 4000, 40404)	N/A

Create Object - User-defined Service

If **User-defined Service** is selected for the **Object Type**, these settings will appear.



Create Object

Name *

test_moxa

9 / 32

Object Type *

IP Address and Subnet

IP Type *

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A
Object Type	Select a type for the object. **IP Address and Subnet**: You can specify an IP address, a range of IP addresses, or a subnet. **Network Service**: You can select from a list of protocol and port combinations used for common network services. **Industrial Application Service**: You can select from a list of protocol and port combinations used for industrial communications and applications. **User-defined Service**: You can specify your own protocol and port combination.	IP Address and Subnet / Network Service / Industrial Application Service / User-defined Service	N/A
IP Protocol	Select the IP protocols to use for the object.	TCP / UDP / TCP and UDP / ICMP Custom IP Protocol	N/A
Service Port Type **(If TCP, UDP, or TCP and UDP is selected for IP Protocol)**	Select how to define ports for the object. **Any**: All ports will be included. **Single TCP and UDP Port**: Specify a single port to include. **TCP and UDP Port Range**: Specify a range of ports to include.	Any / Single TCP and UDP Port / TCP and UDP Port Range	

UI Setting	Description	Valid Range	Default Value
Port **(If Single TCP and UDP Port is selected for Service Port Type)**	Specify a port to include.	1 to 65535	N/A
Port: Start **(If TCP and UDP Port Range is selected for Service Port Type)**	Specify the start of the port range to use for the object.	1 to 65535	N/A
Port: End **(If TCP and UDP Port Range is selected for Service Port Type)**	Specify the end of the port range to use for the object.	1 to 65535	N/A
ICMP Type (Decimal) **(If ICMP is selected for IP Protocol)**	Specify the ICMP type in decimal form to use for the object. Leave this blank to allow all ICMP types to be included.	Blank, 0 to 255	N/A
ICMP Code (Decimal) **(If ICMP is selected for IP Protocol)**	Specify the ICMP code in decimal form to use for the object. Leave this blank to allow all ICMP codes to be included.	Blank, 0 to 255	N/A
IP Protocol (Decimal) **(If Custom IP Protocol is selected for IP Protocol)**	Specify the IP protocol in decimal form to use for the object.	0 to 255	N/A

Edit Object

Menu Path: Main > Object Management

Clicking the **Edit (✎)** icon for an object on the **Main > Object Management** page will open this dialog box. This dialog lets you edit an existing object. Click **APPLY** to save your changes.

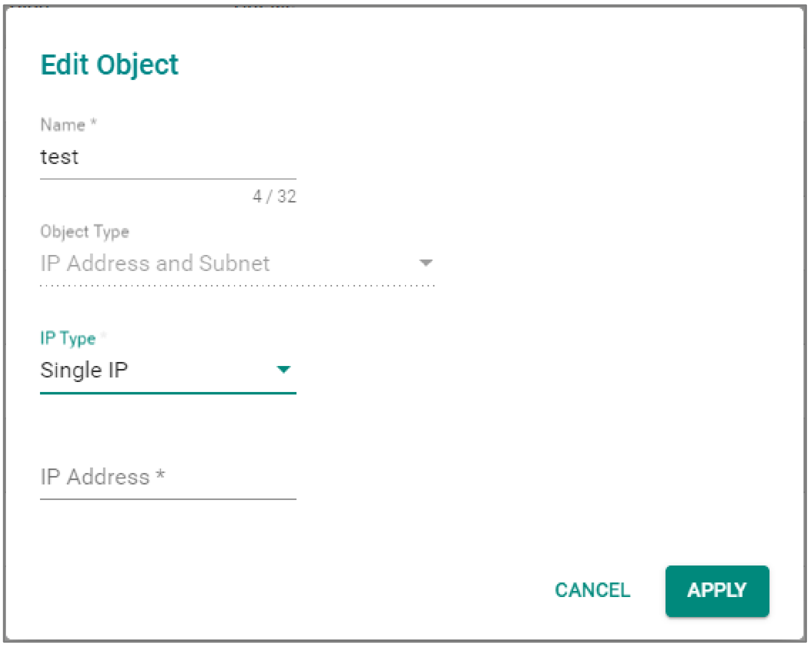
Available settings will vary depending on which **Object Type** the object uses.

Note

When editing an object, you cannot change its **Object Type**.

Edit Object - IP Address and Subnet

If **IP Address and Subnet** is selected for the **Object Type**, these settings will appear.



Edit Object

Name *
test
4 / 32

Object Type
IP Address and Subnet

IP Type
Single IP

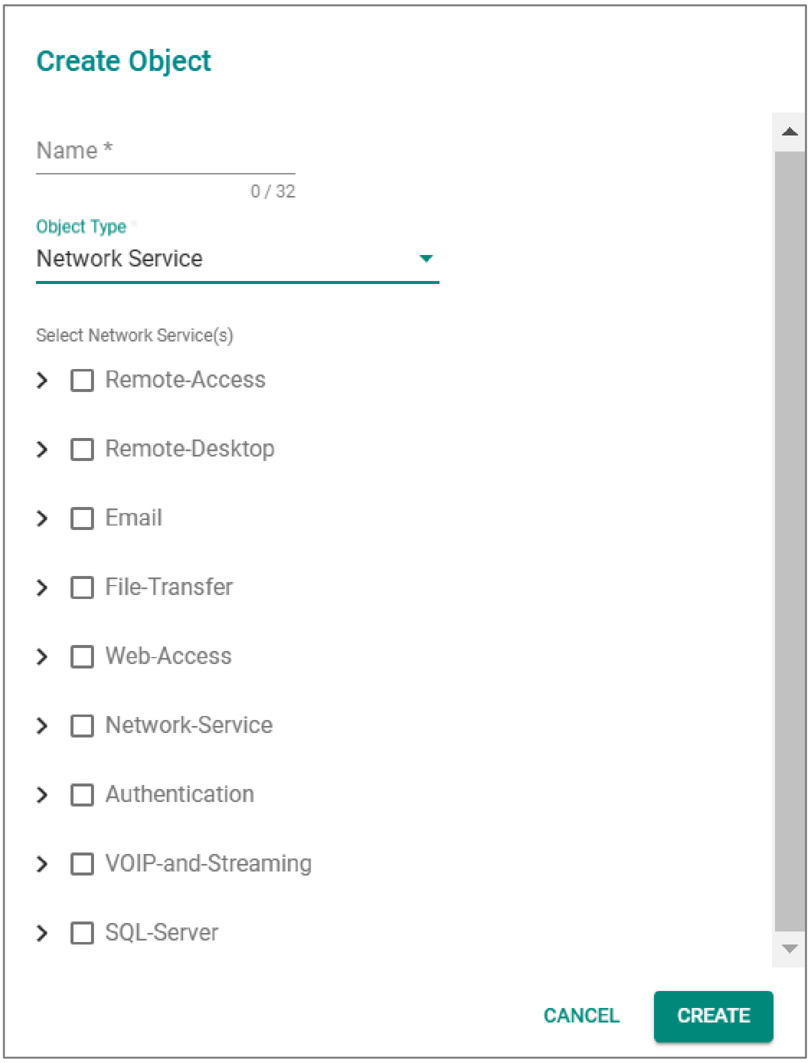
IP Address *

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A
Object Type **(View-only)**	Shows the type for the object. This setting cannot be changed when editing an object.	IP Address and Subnet	IP Address and Subnet
IP Type	Select the type of IP address to use for the object.	Single IP / IP Range / Subnet	N/A
IP Address **(If Single is selected for IP Type)**	Specify the IP address to use for the object.	Valid IP Address	N/A

UI Setting	Description	Valid Range	Default Value
IP Address: Start **(If IP Range is selected for IP Type)**	Specify the start of the IP range to use for the object.	Valid IP Address	N/A
IP Address: End **(If IP Range is selected for IP Type)**	Specify the end of the IP range to use for the object.	Valid IP Address	N/A
Subnet **(If Subnet is selected for IP Type)**	Specify the IP address of the subnet to use for the object.	Valid IP Address	N/A
Subnet Mask **(If Subnet is selected for IP Type)**	Select the subnet mask to use for the object.	Drop-down list of subnet masks	N/A

Edit Object - Network Service

If **Network Service** is selected for the **Object Type**, these settings will appear.



Create Object

Name *

0 / 32

Object Type *

Network Service

Select Network Service(s)

- □ Remote-Access
- □ Remote-Desktop
- □ Email
- □ File-Transfer
- □ Web-Access
- □ Network-Service
- □ Authentication
- □ VOIP-and-Streaming
- □ SQL-Server

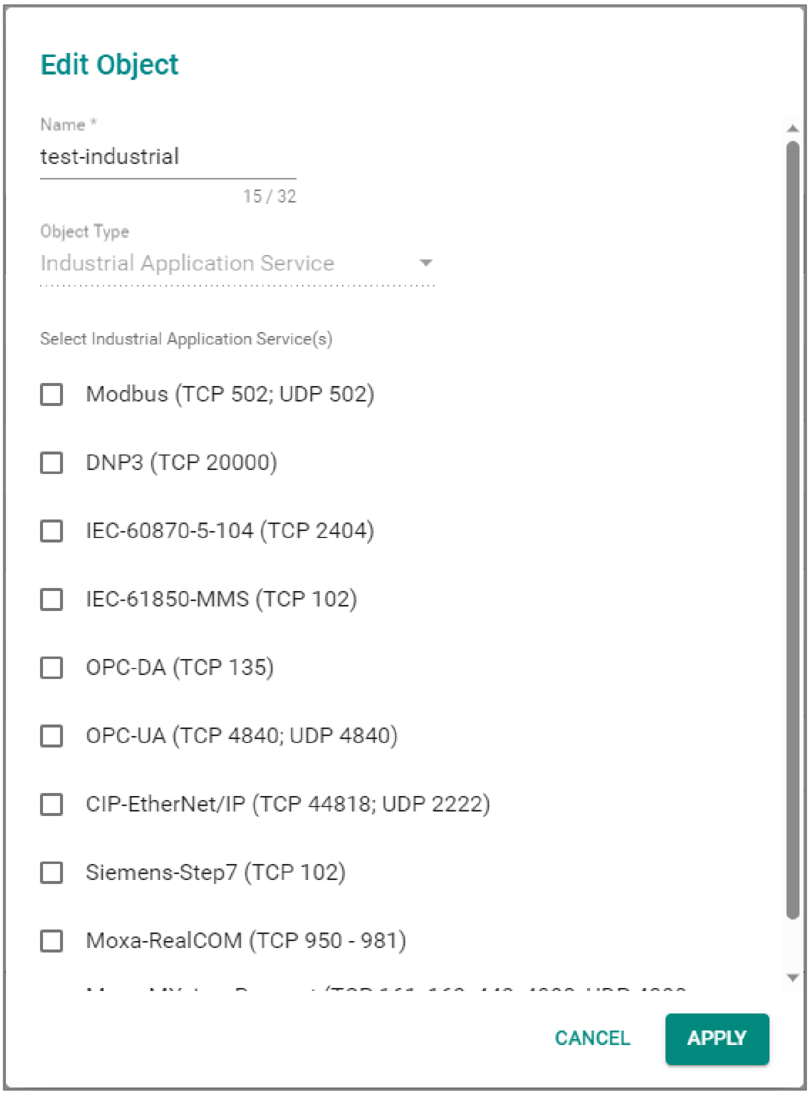
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A
Object Type (View-only)	Shows the type for the object. This setting cannot be changed when editing an object.	Network Service	Network Service
Select Network Service(s)	Select a category of network services, or individual services to use for the object. You can select multiple options.	Remote-Access / Remote-Desktop / Email / File-Transfer / Web-Access / Network-Service / Authentication / VOIP-and-Streaming / SQL-Server	N/A

UI Setting	Description	Valid Range	Default Value
Remote-Access	This category includes protocols used for remote access to a device.	WINS (TCP 1512; UDP 1512) TELNET (TCP 23) SSH (TCP 22)	N/A
Remote-Desktop	This category includes protocols used by various remote desktop services.	PC-Anywhere (TCP 5631; UDP 5632) Chrome-Remote-Desktop (UDP 5222) AnyDesk (TCP 6568, 7070; UDP 50001 - 50003) Teamviewer (TCP 5938) RDP (TCP 3389) VNC (TCP 5900) X-WINDOW (TCP 6000 - 6063)	N/A
Email	This category includes protocols used for sending and receiving emails.	IMAP (TCP 143) IMAPS (TCP 993) POP3 (TCP 110) POP3S (TCP 995) SMTP (TCP 25) SMTPS (TCP 465)	N/A
File-Transfer	This category includes protocols used for different methods of file transfer.	FTP (TCP 21) FTPS (TCP 990) SFTP (TCP 115; UDP 115) TFTP (UDP 69) NFS (TCP 111, 2049; UDP 111, 2049) SAMBA (TCP 139) AFS3 (TCP 7000 - 7009; UDP 7000 - 7009) SMB (TCP 445)	N/A
Web-Access	This category includes protocols used by web browsers.	HTTP (TCP 80) HTTPS (TCP 443)	N/A

UI Setting	Description	Valid Range	Default Value
Network-Service	This category includes protocols used by various network services.	BGP (TCP 179) DHCP (UDP 67) DHCP6 (UDP 546) DNS (TCP 53; UDP 53) NTP (TCP 123; UDP 123) ICMP-PING (ICMP Type Any Code Any) OSPF (IP Protocol 89) RIP (TCP 520) SNMP (TCP 161 - 162; UDP 161 - 162) SYSLOG (UDP 514)	N/A
Authentication	This category includes protocols used by authentication services.	LDAP (TCP 389; UDP 389) LDAPS (TCP 636; UDP 636) RADIUS (UDP 1812 - 1813) TACACS+ (TCP 49; UDP 49)	N/A
VOIP-and-Streaming	This category includes protocols used for VOIP calling and streaming video.	SIP (TCP 5060; UDP 5060) RSTP (TCP 554, 7070, 8554; UDP 554)	N/A
SQL-Server	This category includes protocols used for SQL servers.	MS-SQL (TCP 1433 - 1434) MYSQL (TCP 3306)	N/A

Edit Object - Industrial Application Service

If **Industrial Application Service** is selected for the **Object Type**, these settings will appear.



Edit Object

Name *
test-industrial
15 / 32

Object Type
Industrial Application Service

Select Industrial Application Service(s)

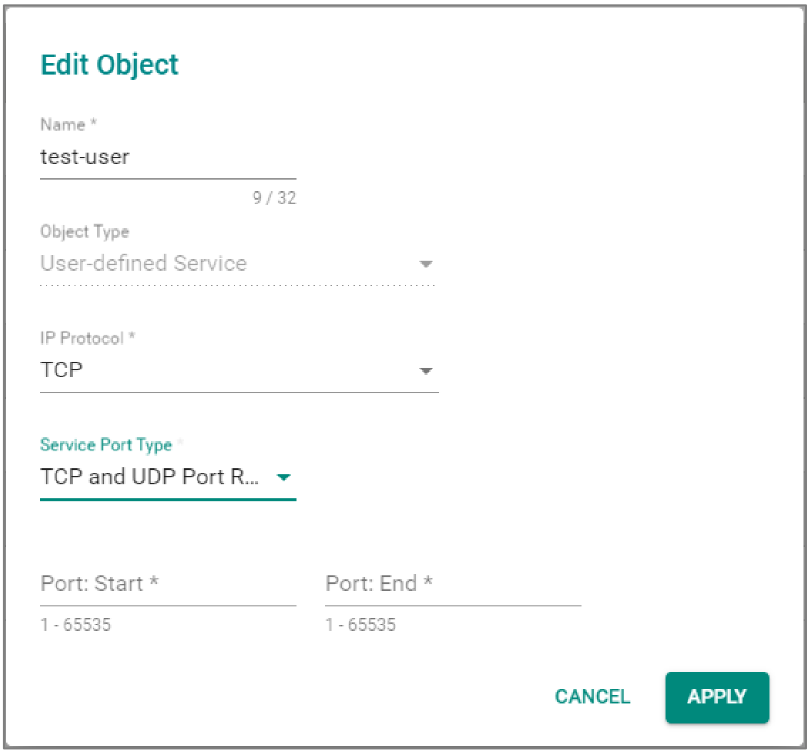
- □ Modbus (TCP 502; UDP 502)
- □ DNP3 (TCP 20000)
- □ IEC-60870-5-104 (TCP 2404)
- □ IEC-61850-MMS (TCP 102)
- □ OPC-DA (TCP 135)
- □ OPC-UA (TCP 4840; UDP 4840)
- □ CIP-EtherNet/IP (TCP 44818; UDP 2222)
- □ Siemens-Step7 (TCP 102)
- □ Moxa-RealCOM (TCP 950 - 981)

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A
Object Type (View-only)	Shows the type for the object. This setting cannot be changed when editing an object.	Industrial Application Service	Industrial Application Service

UI Setting	Description	Valid Range	Default Value
Select Industrial Application Service(s)	Select a category of network services, or individual services to use for the object. You can select multiple options.	Modbus (TCP 502; UDP 502) DNP3 (TCP 20000) IEC-60870-5-104 (TCP 2404) IEC-61850-MMS (TCP 102) OPC-DA (TCP 135) OPC-UA (TCP 4840; UDP 4840) CIP-EtherNet/IP (TCP 44818; UDP 2222) Siemens-Step7 (TCP 102) Moxa-RealCOM (TCP 950 - 981) Moxa-MXview-Request (TCP 161, 162, 443, 4000; UDP 4000, 40404)	N/A

Edit Object - User-defined Service

If **User-defined Service** is selected for the **Object Type**, these settings will appear.



Edit Object

Name *
test-user
9 / 32

Object Type
User-defined Service

IP Protocol *
TCP

Service Port Type *
TCP and UDP Port R...

Port: Start *
1 - 65535

Port: End *
1 - 65535

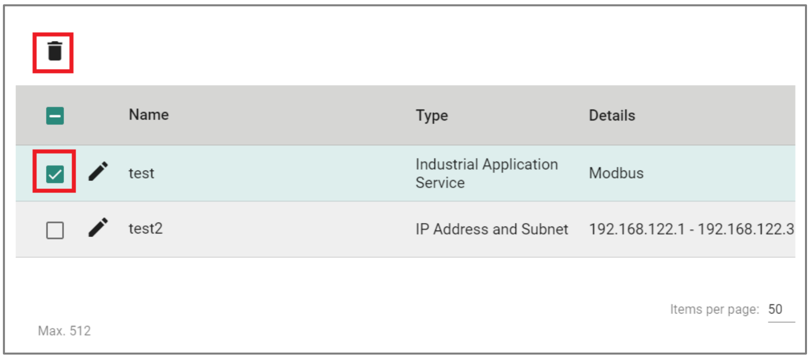
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A
Object Type **(View-only)**	Shows the type for the object. This setting cannot be changed when editing an object.	User-defined Service	User-defined Service
IP Protocol	Select the IP protocols to use for the object.	TCP / UDP / TCP and UDP / ICMP Custom IP Protocol	N/A
Service Port Type **(If TCP, UDP, or TCP and UDP is selected for IP Protocol)**	Select how to define ports for the object. **Any**: All ports will be included. **Single TCP and UDP Port**: Specify a single port to include. **TCP and UDP Port Range**: Specify a range of ports to include.	Any / Single TCP and UDP Port / TCP and UDP Port Range	
Port **(If Single TCP and UDP Port is selected for Service Port Type)**	Specify a port to include.	1 to 65535	N/A

UI Setting	Description	Valid Range	Default Value
Port: Start **(If TCP and UDP Port Range is selected for Service Port Type)**	Specify the start of the port range to use for the object.	1 to 65535	N/A
Port: End **(If TCP and UDP Port Range is selected for Service Port Type)**	Specify the end of the port range to use for the object.	1 to 65535	N/A
ICMP Type (Decimal) **(If ICMP is selected for IP Protocol)**	Specify the ICMP type in decimal form to use for the object. Leave this blank to allow all ICMP types to be included.	Blank, 0 to 255	N/A
ICMP Code (Decimal) **(If ICMP is selected for IP Protocol)**	Specify the ICMP code in decimal form to use for the object. Leave this blank to allow all ICMP codes to be included.	Blank, 0 to 255	N/A
IP Protocol (Decimal) **(If Custom IP Protocol is selected for IP Protocol)**	Specify the IP protocol in decimal form to use for the object.	0 to 255	N/A

Delete Object

Menu Path: Main > Object Management

You can delete an object by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.



		Name	Type	Details
☑	✎	test	Industrial Application Service	Modbus
□	✎	test2	IP Address and Subnet	192.168.122.1 - 192.168.122.3

Items per page: 50

Max. 512

Firewall

Menu Path: Firewall

The Firewall settings area lets you configure settings related to your device's firewall.

This settings area includes these sections:

- Layer 2 Policy
- Layer 3-7 Policy
- Malformed Packets
- Session Control
- DoS Policy
- Advanced Protection

Network Configuration - User Privileges

Privileges to Firewall 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 Policy	R/W	R/W	R
Layer 3 - 7 Policy	R/W	R/W	R
Malformed Packets	R/W	R/W	R
Session Control	R/W	R/W	R
DoS Policy	R/W	R/W	R
Advanced Protection			
Dashboard	R/W	R/W	-
Configuration	R/W	R/W	-
Protocol Filter Policy	R/W	R/W	-

Settings	Admin	Supervisor	User
ADP	R/W	R/W	-
IPS	R/W	R/W	-

Layer 2 Policy

Menu Path: Firewall > Layer 2 Policy

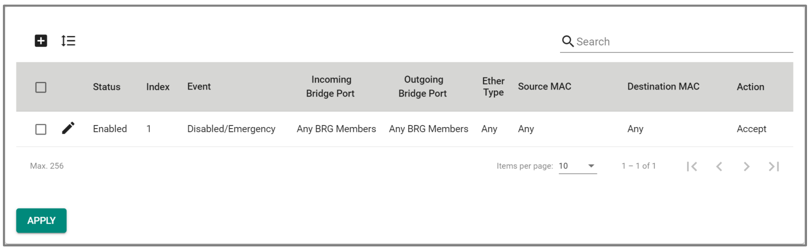
This page lets you configure advanced Layer 2 policies for your device's firewall. Layer 2 firewall policies can filter packets from bridge ports and have a higher priority than Layer 3 policies.

Note

Packets are checked by using the policy with the lowest index number first. If the packet matches the policy, the defined action will be taken and the remaining rules will not be run for the packet. If the packet does not match the policy, the next policy will be used.

Limitations

You can configure up to 256 Layer 2 policies.



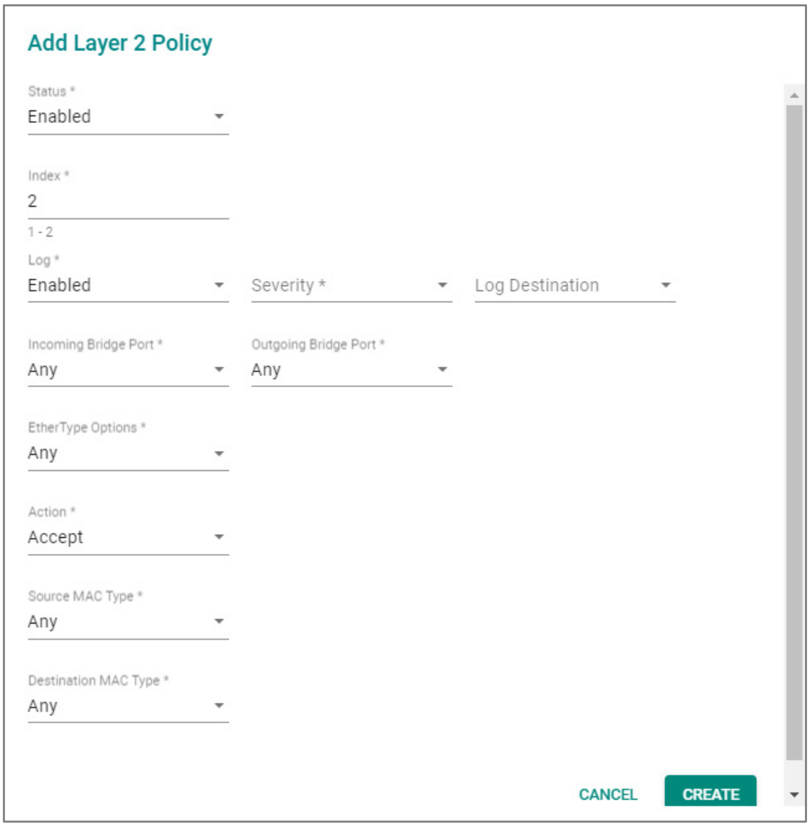
□		Status	Index	Event	Incoming Bridge Port	Outgoing Bridge Port	Ether Type	Source MAC	Destination MAC	Action
□		Enabled	1	Disabled/Emergency	Any BRG Members	Any BRG Members	Any	Any	Any	Accept

UI Setting	Description
Status	Shows whether the policy is enabled or disabled.
Index	Shows the index of the policy. The index determines the order for processing policies.
Event	Shows whether logging is enabled or disabled for the event and the severity assigned to the event.
Incoming Bridge Port	Shows the incoming bridge port for the policy.
Outgoing Bridge Port	Shows the outgoing bridge port for the policy.
Ether Type	Shows the EtherType that the policy applies to.
Source MAC	Shows the source MAC the policy applies to.
Destination MAC	Shows the destination MAC the policy applies to.
Action	Shows the action that will be taken for applicable traffic.

Add Layer 2 Policy

Menu Path: Firewall > Layer 2 Policy

Clicking the **Add (⊞)** icon on the **Firewall > Layer 2 Policy** page will open this dialog box. This dialog lets you create a new policy. Click **CREATE** to save your changes and add the new policy.



Add Layer 2 Policy

Status *
Enabled

Index *
2
1 - 2

Log *
Enabled

Severity *

Log Destination

Incoming Bridge Port *
Any

Outgoing Bridge Port *
Any

EtherType Options *
Any

Action *
Accept

Source MAC Type *
Any

Destination MAC Type *
Any

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Index	Specify the index number for the policy. The index determines the order for processing policies.	1 to 256	Last used index plus 1
Log	Enable or disable firewall event logging for this policy.	Enabled / Disabled	Enabled
Severity	Select the severity level to assign events for this policy. Refer to Appendix > Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A

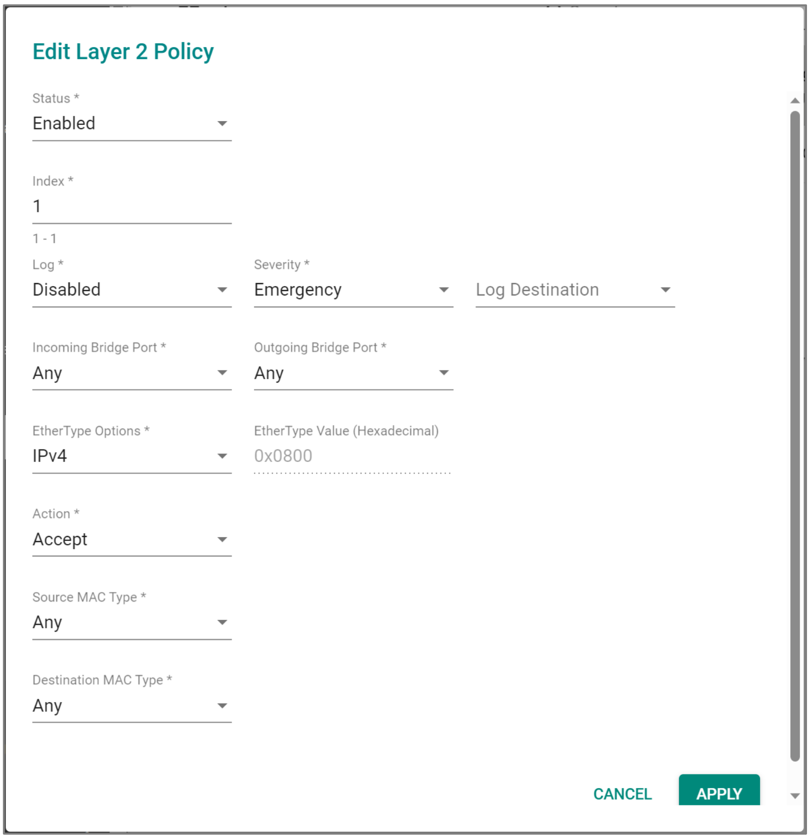
UI Setting	Description	Valid Range	Default Value
Log Destination	Specify where to send firewall event logs. You can select multiple options. **Local Storage**: Firewall event logs will be stored on local storage and will show up in the device's Event Log. Refer to Diagnostics > Event Logs and Notifications > Event Log for more information. **Syslog**: Firewall event logs will be sent to a syslog server. Refer to Diagnostics > Event Logs and Notifications > Syslog for more information.	Local Storage / Syslog	N/A
Incoming Bridge Port	Select the incoming bridge port for this policy.	Any	Any
Outgoing Bridge Port	Select the outgoing bridge port for this policy.	Any	Any
EtherType Options	Select the Layer 2 EtherType protocol that this policy should apply to. You can select a type from the drop-down list, or you can select Manual to specify one manually. Refer to Appendix > EtherTypes for Layer 2 for more information about common EtherTypes.	Any / Manual / IPv4 / X25 / ARP / Frame Relay ARP / G8BPQ AX.25 Ethernet Packet / DEC Assigned proto / DEC DNA Dump/Load / DEC DNA Remote Console / DEC DNA Routing / DEC LAT / DEC Diagnostics / DEC Customer use / DEC Systems Comms Arch / Trans Ether Bridging / Raw Frame Relay / Appletalk AARP / Appletalk / 802.1Q Virtual LAN tagged frame / Novell IPX / NetBEUI / IP version 6 / PPP / MultiProtocol over ATM / PPPoE discovery messages / PPPoE session messages / Frame-based ATM Transport over Ethernet / Loopback	Any
Manual **(if EtherType Options is anything other than Any)**	If **EtherType Options** is set to **Manual**, enter the EtherType value in hexadecimal this policy should apply to. If **EtherType Options** is set to a predefined **EtherType**, its value will be shown here and cannot be changed.	Valid EtherType hex code	N/A, EtherType value for the selected EtherType

UI Setting	Description	Valid Range	Default Value
Action	Select the action the firewall should take for traffic that matches this policy. **Accept**: The firewall will accept packets that match the policy. **Drop**: The firewall will drop packets that match the policy.	Accept / Drop	Accept
Source MAC Type	Select which source MAC addresses to check with this policy. **Any**: The firewall will check packets coming from all source MAC addresses. **Single**: The firewall will only check packets coming from a specified source MAC address.	Any / Single	Any
Destination MAC Type	Select which destination MAC addresses to check with this policy. **Any**: The firewall will check packets going to all destination MAC addresses. **Single**: The firewall will only check packets going to a specific destination MAC address.	Any / Single	Any

Edit Layer 2 Policy

Menu Path: Firewall > Layer 2 Policy

Clicking the **Edit (✎)** icon for a policy on the **Firewall > Layer 2 Policy** page will open this dialog box. This dialog lets you modify an existing policy. Click **APPLY** to save your changes.



Edit Layer 2 Policy

Status * Enabled

Index * 1

1 - 1

Log * Disabled

Severity * Emergency

Log Destination

Incoming Bridge Port * Any

Outgoing Bridge Port * Any

EtherType Options * IPv4

EtherType Value (Hexadecimal) 0x0800

Action * Accept

Source MAC Type * Any

Destination MAC Type * Any

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Index	Specify the index number for the policy. The index determines the order for processing policies.	1 to 256	Last used index plus 1
Log	Enable or disable firewall event logging for this policy.	Enabled / Disabled	Enabled
Severity	Select the severity level to assign events for this policy. Refer to Appendix > Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A

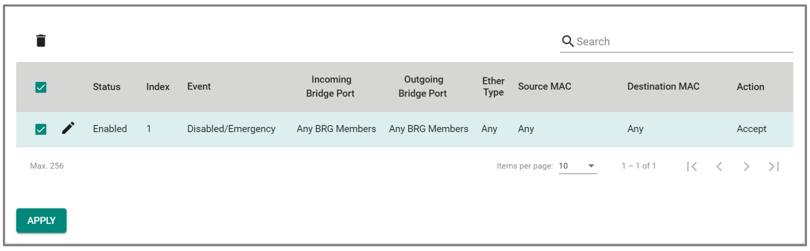
UI Setting	Description	Valid Range	Default Value
Log Destination	Specify where to send firewall event logs. You can select multiple options. **Local Storage**: Firewall event logs will be stored on local storage and will show up in the device's Event Log. Refer to Diagnostics > Event Logs and Notifications > Event Log for more information. **Syslog**: Firewall event logs will be sent to a syslog server. Refer to Diagnostics > Event Logs and Notifications > Syslog for more information.	Local Storage / Syslog	N/A
Incoming Bridge Port	Select the incoming bridge port for this policy.	Any	Any
Outgoing Bridge Port	Select the outgoing bridge port for this policy.	Any	Any
EtherType Options	Select the Layer 2 EtherType protocol that this policy should apply to. You can select a type from the drop-down list, or you can select Manual to specify one manually. Refer to Appendix > EtherTypes for Layer 2 for more information about common EtherTypes.	Any / Manual / IPv4 / X25 / ARP / Frame Relay ARP / G8BPQ AX.25 Ethernet Packet / DEC Assigned proto / DEC DNA Dump/Load / DEC DNA Remote Console / DEC DNA Routing / DEC LAT / DEC Diagnostics / DEC Customer use / DEC Systems Comms Arch / Trans Ether Bridging / Raw Frame Relay / Appletalk AARP / Appletalk / 802.1Q Virtual LAN tagged frame / Novell IPX / NetBEUI / IP version 6 / PPP / MultiProtocol over ATM / PPPoE discovery messages / PPPoE session messages / Frame-based ATM Transport over Ethernet / Loopback	Any
Manual **(if EtherType Options is anything other than Any)**	If **EtherType Options** is set to **Manual**, enter the EtherType value in hexadecimal this policy should apply to. If **EtherType Options** is set to a predefined **EtherType**, its value will be shown here and cannot be changed.	Valid EtherType hex code	N/A, EtherType value for the selected EtherType

UI Setting	Description	Valid Range	Default Value
Action	Select the action the firewall should take for traffic that matches this policy. **Accept**: The firewall will accept packets that match the policy. **Drop**: The firewall will drop packets that match the policy.	Accept / Drop	Accept
Source MAC Type	Select which source MAC addresses to check with this policy. **Any**: The firewall will check packets coming from all source MAC addresses. **Single**: The firewall will only check packets coming from a specified source MAC address.	Any / Single	Any
Destination MAC Type	Select which destination MAC addresses to check with this policy. **Any**: The firewall will check packets going to all destination MAC addresses. **Single**: The firewall will only check packets going to a specific destination MAC address.	Any / Single	Any

Delete Layer 2 Policy

Menu Path: Firewall > Layer 2 Policy

You can delete a policy by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.

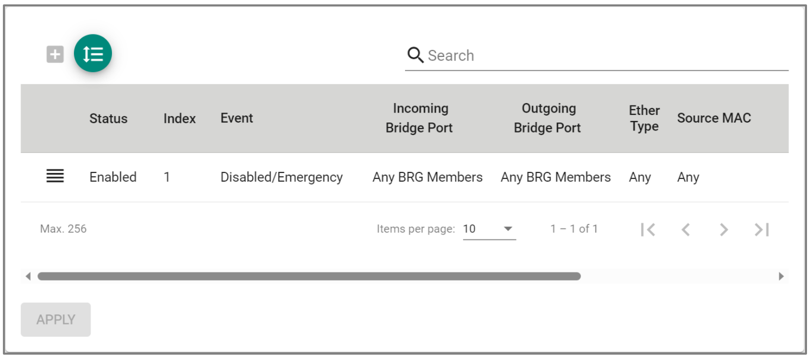


☑		Status	Index	Event	Incoming Bridge Port	Outgoing Bridge Port	Ether Type	Source MAC	Destination MAC	Action
☑	✎	Enabled	1	Disabled/Emergency	Any BRG Members	Any BRG Members	Any	Any	Any	Accept

Reorder Layer 2 Policies

Menu Path: Firewall > Layer 2 Policy

You can reorder policies by clicking the **Reorder Priorities (↕☰)** icon, moving the entries into the order you want, then clicking the **Reorder Priorities (↕☰)** icon again. Reordering policies affects the order used to process the policies.



	Status	Index	Event	Incoming Bridge Port	Outgoing Bridge Port	Ether Type	Source MAC
☰	Enabled	1	Disabled/Emergency	Any BRG Members	Any BRG Members	Any	Any

Layer 3-7 Policy

Menu Path: Firewall > Layer 3-7 Policy

This page lets you configure Layer 3-7 policies to secure and control network traffic. Click **APPLY** to save your changes.

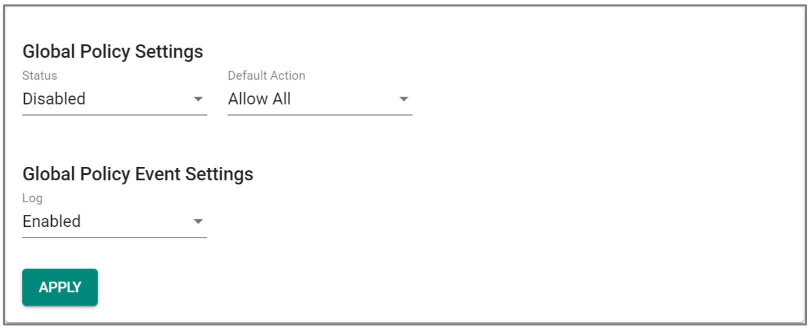
Note

Packets are checked by using the policy with the lowest index number first. If the packet matches the policy, the defined action will be taken and the remaining rules will not be run for the packet. If the packet does not match the policy, the next policy will be used.

Limitations

You can configure up to 1024 Layer 3-7 policies.

Layer 3-7 Policy Settings



Global Policy Settings

Status: Disabled

Default Action: Allow All

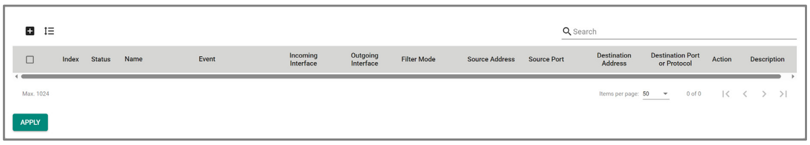
Global Policy Event Settings

Log: Enabled

APPLY

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable global policy enforcement. The global policy allows you to set a **Default Action** for traffic that doesn't match any of the configured firewall rules.	Enabled / Disabled	Disabled
Default Action	Select what the default action should be for traffic that doesn't match any of the configured firewall rules. **Allow All**: Allow all network traffic that does not match any rule. **Deny All**: Block all network traffic that does not match any rule.	Allow All / Deny All	Deny All
Log	Enable or disable global policy event logging. This will allow event logging for actions taken due to the global policy.	Enabled / Disabled	Enabled

Layer 3-7 Policy List



□	Index	Status	Name	Event	Incoming Interface	Outgoing Interface	Filter Mode	Source Address	Source Port	Destination Address	Destination Port or Protocol	Action	Description

Max. 1024

Items per page: 50

0 of 0

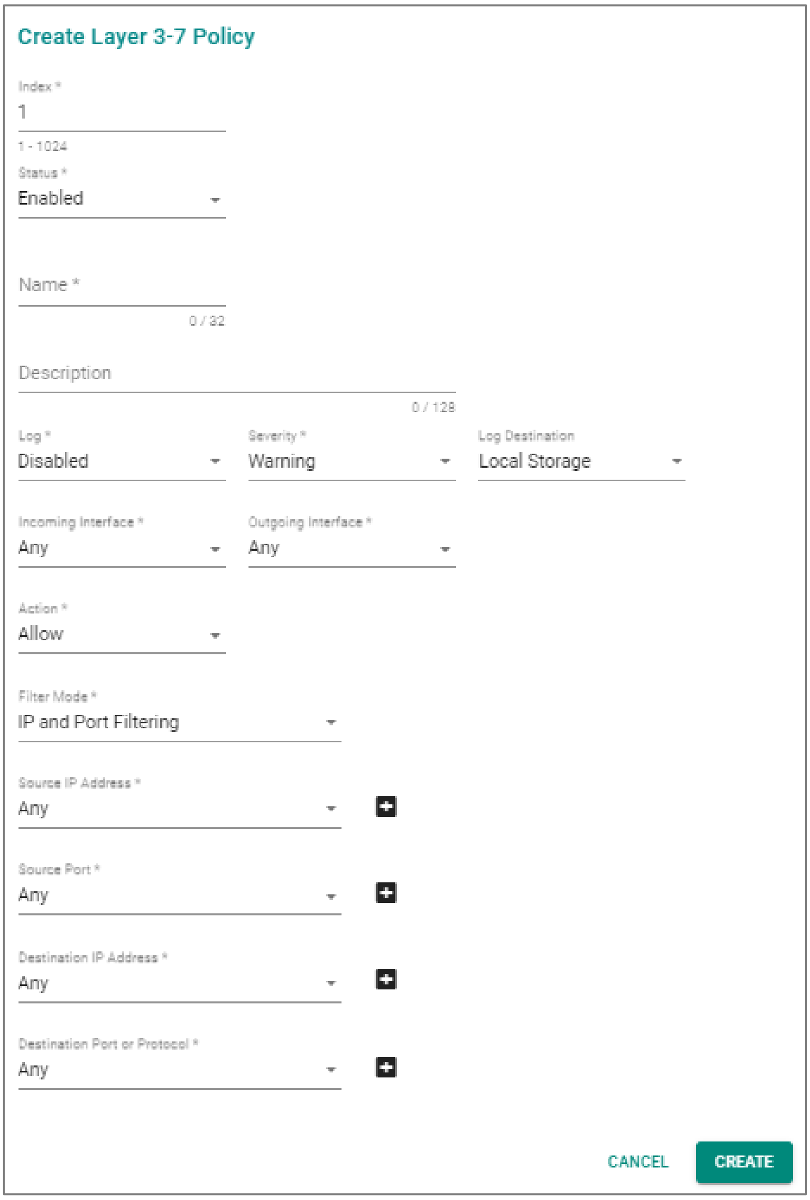
APPLY

UI Setting	Description
Index	Shows the index of the policy. The index determines the order for processing policies.
Status	Shows whether the policy is enabled or disabled.
Name	Shows the name of the policy.
Event	Shows whether logging is enabled or disabled for the event and the severity assigned to the event.
Incoming Interface	Shows the incoming interface for the policy.
Outgoing Interface	Shows the outgoing interface for the policy.
Filter Mode	Shows the filter mode used for the policy.
Source Address	Shows the source IP addresses the policy applies to.
Source Port	Shows the source ports the policy applies to.
Destination Address	Shows the destination IP addresses the policy applies to.
Destination Port or Protocol	Shows the destination ports or protocols the policy applies to.
Action	Shows the action that will be taken for applicable traffic.
Description	Shows the description of the policy.

Create Layer 3-7 Policy

Menu Path: Firewall > Layer 3-7 Policy

Clicking the **Add (⊞)** icon on the **Firewall > Layer 3-7 Policy** page will open this dialog box. This dialog lets you create a new policy. Click **CREATE** to save your changes and add the new policy.



Create Layer 3-7 Policy

Index *
1
1 - 1024

Status *
Enabled

Name *
0 / 32

Description
0 / 128

Log *
Disabled

Severity *
Warning

Log Destination
Local Storage

Incoming Interface *
Any

Outgoing Interface *
Any

Action *
Allow

Filter Mode *
IP and Port Filtering

Source IP Address *
Any

Source Port *
Any

Destination IP Address *
Any

Destination Port or Protocol *
Any

UI Setting	Description	Valid Range	Default Value
Index	Specify the index number for the policy. The index determines the order for processing policies.	1 to 1024	Last used index plus 1
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Name	Specify a name for the policy.	1 to 32 characters	N/A
Description	Specify a description for the policy.	0 to 128 characters	N/A

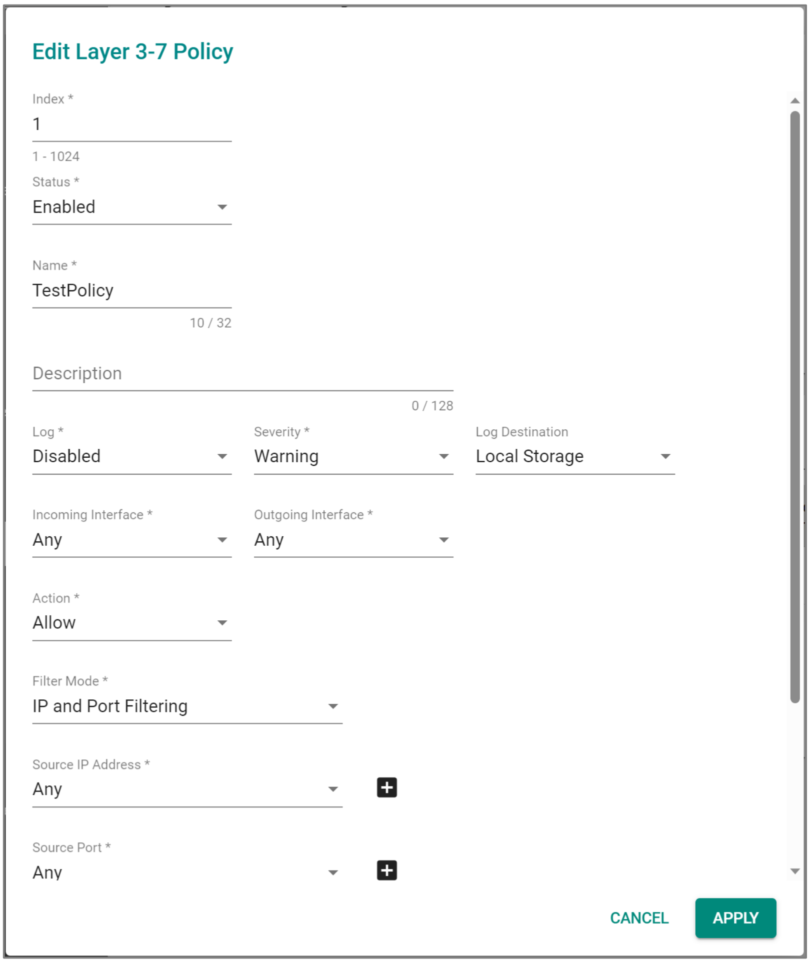
UI Setting	Description	Valid Range	Default Value
Log	Enable or disable firewall event logging for this policy.	Enabled / Disabled	Enabled
Severity	Select the severity level to assign events for this policy. Refer to Appendix > Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A
Log Destination	Specify where to send firewall event logs. You can select multiple options. **Local Storage**: Firewall event logs will be stored on local storage and will show up in the device's Event Log. Refer to Diagnostics > Event Logs and Notifications > Event Log for more information. **Syslog**: Firewall event logs will be sent to a syslog server. Refer to Diagnostics > Event Logs and Notifications > Syslog for more information. **Trap**: Firewall event notifications will be sent to a trap server. Refer to Diagnostics > SNMP Trap/Inform for more information.	Local Storage / Syslog / Trap	N/A
Incoming Interface	Select the incoming interface for this policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Configuration > Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down list of interfaces	Any
Outgoing Interface	Select the outgoing interface for this policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Configuration > Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down list of interfaces	Any
Action	Select the action the firewall should take for traffic that matches this policy. **Accept**: The firewall will accept packets that match the policy. **Drop**: The firewall will drop packets that match the policy.	Accept / Drop	Accept

UI Setting	Description	Valid Range	Default Value
Filter Mode	Select the filter mode to use for packet filtering. **IP and Port Filtering**: The policy will filter based on IP address and port. **IP and Source MAC Binding**: The policy will filter based on IP address and will also check the source MAC address. **Source MAC Filtering**: The policy will filter based on source MAC address.	IP and Port Filtering / IP and Source MAC Binding / Source MAC Filtering	IP and Port Filtering
Source IP Address **(if Filter Mode is IP and Port Filtering or IP and Source MAC Binding)**	Select the source IP addresses this policy will apply to. Select **Any** to check traffic from all source IP addresses, or select a pre-defined object. You can also click the Add (⊞) icon to create a new IP Address and Subnet object. Refer to Create Object for more information.	Any / Drop-down list of IP Address and Subnet objects	Any
Source Port **(if Filter Mode is IP and Port Filtering)**	Select the source ports this policy will apply to. Select **Any** to check traffic from all source ports, or select a pre-defined object. You can also click the Add (⊞) icon to create a new User-defined Service object. Refer to Create Object for more information.	Any / Drop-down list of port-based User-defined Service objects	Any
Source MAC Address **(if Filter Mode is IP and Source MAC Binding or Source MAC Filtering)**	Specify the source MAC address this policy will apply to.	Valid MAC address	N/A
Destination IP Address **(if Filter Mode is IP and Port Filtering)**	Select the destination IP addresses this policy will apply to. Select **Any** to check all traffic going to any destination IP address, or select a pre-defined object. You can also click the Add (⊞) icon to create a new IP Address and Subnet object. Refer to Create Object for more information.	Any / Drop-down list of IP Address and Subnet objects	Any
Destination Port or Protocol **(if Filter Mode is IP and Port Filtering)**	Select the destination ports or protocl this policy will apply to. Select **Any** to check all traffic going to any destination port or protocol, or select a pre-defined service or object. You can also click the Add (⊞) icon to create a new Network Service, Industrial Application Service, or User-defined Service object. Refer to Create Object for more information.	Any / Drop-down list of Network Service, Industrial Application Service, and port-based User-defined Service objects	Any

Edit Layer 3-7 Policy

Menu Path: Firewall > Layer 3-7 Policy

Clicking the **Edit (✎)** icon for a policy on the **Firewall > Layer 3-7 Policy** page will open this dialog box. This dialog lets you modify an existing policy. Click **APPLY** to save your changes.



Edit Layer 3-7 Policy

Index *
1
1 - 1024

Status *
Enabled

Name *
TestPolicy
10 / 32

Description
0 / 128

Log *
Disabled

Severity *
Warning

Log Destination
Local Storage

Incoming Interface *
Any

Outgoing Interface *
Any

Action *
Allow

Filter Mode *
IP and Port Filtering

Source IP Address *
Any

Source Port *
Any

UI Setting	Description	Valid Range	Default Value
Index	Specify the index number for the policy. The index determines the order for processing policies.	1 to 1024	Last used index plus 1

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Name	Specify a name for the policy.	1 to 32 characters	N/A
Description	Specify a description for the policy.	0 to 128 characters	N/A
Log	Enable or disable firewall event logging for this policy.	Enabled / Disabled	Enabled
Severity	Select the severity level to assign events for this policy. Refer to Appendix > Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A
Log Destination	Specify where to send firewall event logs. You can select multiple options. **Local Storage**: Firewall event logs will be stored on local storage and will show up in the device's Event Log. Refer to Diagnostics > Event Logs and Notifications > Event Log for more information. **Syslog**: Firewall event logs will be sent to a syslog server. Refer to Diagnostics > Event Logs and Notifications > Syslog for more information. **Trap**: Firewall event notifications will be sent to a trap server. Refer to Diagnostics > SNMP Trap/Inform for more information.	Local Storage / Syslog / Trap	N/A
Incoming Interface	Select the incoming interface for this policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Configuration > Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down list of interfaces	Any
Outgoing Interface	Select the outgoing interface for this policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Configuration > Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down list of interfaces	Any

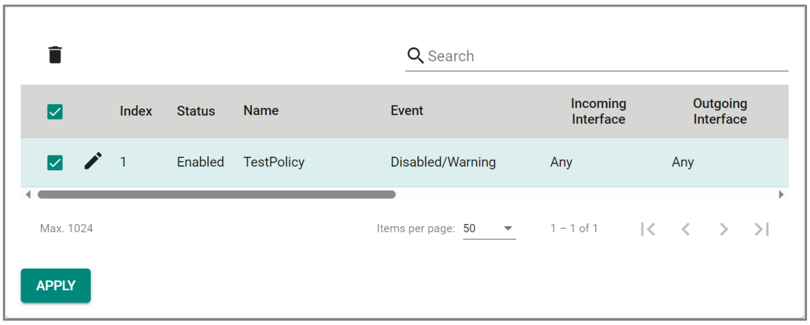
UI Setting	Description	Valid Range	Default Value
Action	Select the action the firewall should take for traffic that matches this policy. **Accept**: The firewall will accept packets that match the policy. **Drop**: The firewall will drop packets that match the policy.	Accept / Drop	Accept
Filter Mode	Select the filter mode to use for packet filtering. **IP and Port Filtering**: The policy will filter based on IP address and port. **IP and Source MAC Binding**: The policy will filter based on IP address and will also check the source MAC address. **Source MAC Filtering**: The policy will filter based on source MAC address.	IP and Port Filtering / IP and Source MAC Binding / Source MAC Filtering	IP and Port Filtering
Source IP Address **(if Filter Mode is IP and Port Filtering or IP and Source MAC Binding)**	Select the source IP addresses this policy will apply to. Select **Any** to check traffic from all source IP addresses, or select a pre-defined object. You can also click the Add (⊞) icon to create a new IP Address and Subnet object. Refer to Create Object for more information.	Any / Drop-down list of IP Address and Subnet objects	Any
Source Port **(if Filter Mode is IP and Port Filtering)**	Select the source ports this policy will apply to. Select **Any** to check traffic from all source ports, or select a pre-defined object. You can also click the Add (⊞) icon to create a new User-defined Service object. Refer to Create Object for more information.	Any / Drop-down list of port-based User-defined Service objects	Any
Source MAC Address **(if Filter Mode is IP and Source MAC Binding or Source MAC Filtering)**	Specify the source MAC address this policy will apply to.	Valid MAC address	N/A
Destination IP Address **(if Filter Mode is IP and Port Filtering)**	Select the destination IP addresses this policy will apply to. Select **Any** to check all traffic going to any destination IP address, or select a pre-defined object. You can also click the Add (⊞) icon to create a new IP Address and Subnet object. Refer to Create Object for more information.	Any / Drop-down list of IP Address and Subnet objects	Any

UI Setting	Description	Valid Range	Default Value
Destination Port or Protocol **(if Filter Mode is IP and Port Filtering)**	Select the destination ports or protocl this policy will apply to. Select **Any** to check all traffic going to any destination port or protocol, or select a pre-defined service or object. You can also click the Add (⊞) icon to create a new Network Service, Industrial Application Service, or User-defined Service object. Refer to [Create Object]() for more information.	Any / Drop-down list of Network Service, Industrial Application Service, and port-based User-defined Service objects	Any

Delete Layer 3-7 Policy

Menu Path: Firewall > Layer 3-7 Policy

You can delete a policy by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.



🗑 Search

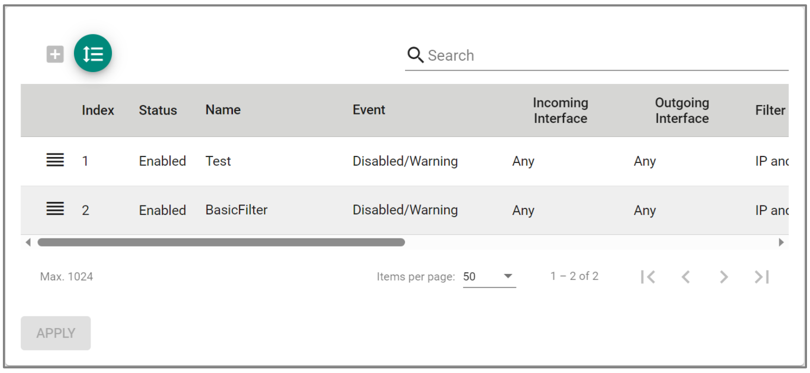
☑		Index	Status	Name	Event	Incoming Interface	Outgoing Interface
☑	✎	1	Enabled	TestPolicy	Disabled/Warning	Any	Any

Max. 1024 Items per page: 50 1 – 1 of 1

Reorder Layer 3-7 Policies

Menu Path: Firewall > Layer 3-7 Policy

You can reorder policies by clicking the **Reorder Priorities (↕☰)** icon, moving the entries into the order you want, then clicking the **Reorder Priorities (↕☰)** icon again. Reordering policies affects the order used to process the policies.

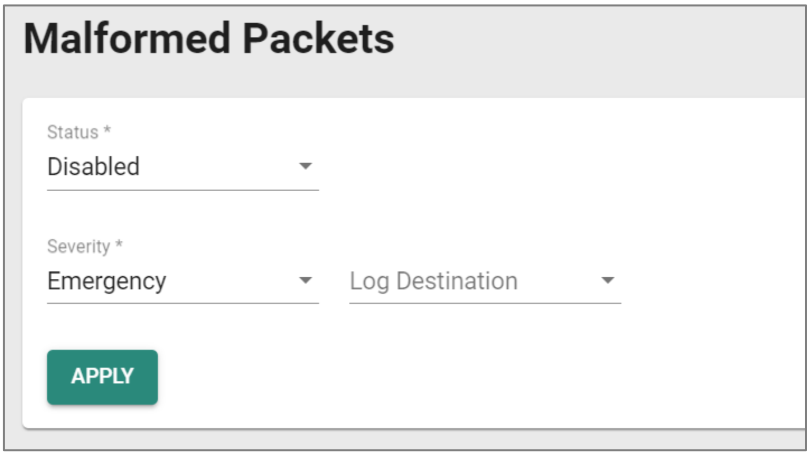


Index	Status	Name	Event	Incoming Interface	Outgoing Interface	Filter
1	Enabled	Test	Disabled/Warning	Any	Any	IP anc
2	Enabled	BasicFilter	Disabled/Warning	Any	Any	IP anc

Malformed Packets

Menu Path: Firewall > Malformed Packets

This page lets you configure the Malformed Packets feature, which enables the device to record event logs with a user-specified severity whenever malformed packets are dropped by the system. Click **APPLY** to save your changes.



Malformed Packets

Status *: Disabled

Severity *: Emergency

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable recording an event when malformed packets are dropped.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Severity	Select the severity level to assign events for this policy. Refer to Appendix > Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency
Log Destination	Specify where to send firewall event logs. You can select multiple options. **Local Storage**: Firewall event logs will be stored on local storage and will show up in the device's Event Log. Refer to Diagnostics > Event Logs and Notifications > Event Log for more information. **Syslog**: Firewall event logs will be sent to a syslog server. Refer to Diagnostics > Event Logs and Notifications > Syslog for more information. **Trap**: Firewall event notifications will be sent to a trap server. Refer to Diagnostics > SNMP Trap/Inform for more information.	Local Storage / Syslog / Trap	N/A

Session Control

Menu Path: Firewall > Session Control

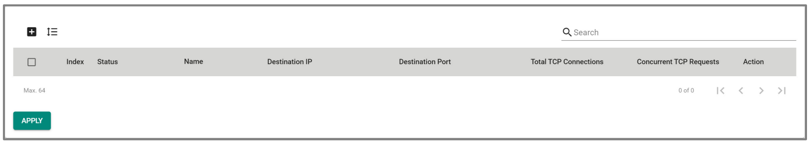
This page lets you configure session control policies to help protect backend hosts or services and avoid system abnormalities. Click **APPLY** to save your changes.

Note

If a TCP connection is successfully established, but no data is sent, the connection will be released after 8 seconds. If the interval between the last data transmission for the connection exceeds 300 seconds, the connection will also be released.

Limitations

You can configure up to 64 session control policies.



□	Index	Status	Name	Destination IP	Destination Port	Total TCP Connections	Concurrent TCP Requests	Action

Max. 64

0 of 0

UI Setting	Description
Index	Shows the index of the policy. The index determines the order for processing policies.
Status	Shows whether the policy is enabled or disabled.
Name	Shows the name of the policy.
Destination IP	Shows the destination IP addresses the policy applies to.
Destination Port	Shows the destination ports the policy applies to.
Total TCP Connections	Shows the total number of TCP connections this policy allows.
Concurrent TCP Connections	Shows the number of concurrent TCP connections this policy allows.
Action	Shows the action that will be taken for applicable traffic.

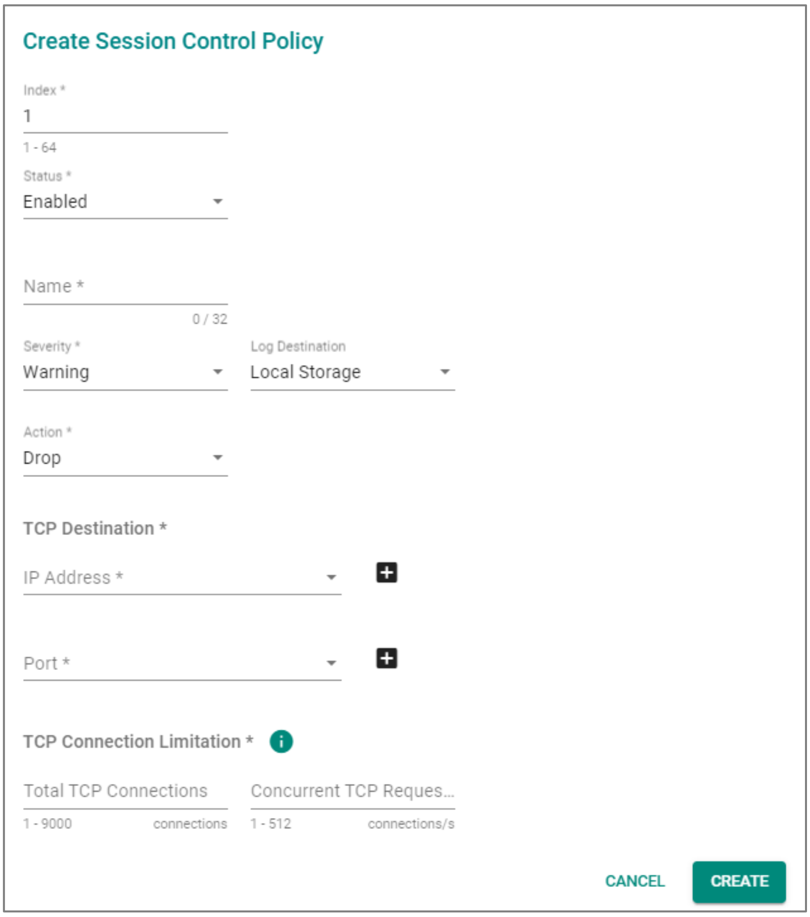
Create Session Control Policy

Menu Path: Firewall > Session Control

Clicking the **Add (** ⊞ **)** icon on the **Firewall > Session Control** page will open this dialog box. This dialog lets you create a new policy. Click **CREATE** to save your changes and add the new policy.

> **Note**
>
> **IP Address** and **Port** cannot both be set to **Any**.

> **Note**
>
> At least one **TCP Connection Limitation** must be defined.



Create Session Control Policy

Index *
1
1 - 64

Status *
Enabled

Name *
0 / 32

Severity *
Warning

Log Destination
Local Storage

Action *
Drop

TCP Destination *

IP Address *

Port *

TCP Connection Limitation *

Total TCP Connections
1 - 9000 connections

Concurrent TCP Reques...
1 - 512 connections/s

UI Setting	Description	Valid Range	Default Value
Index	Specify the index number for the policy. The index determines the order for processing policies.	1 to 64	Last used index plus 1
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Name	Specify a name for the policy.	1 to 32 characters	N/A
Severity	Select the severity level to assign events for this policy. Refer to Appendix > Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A

UI Setting	Description	Valid Range	Default Value
Log Destination	Specify where to send firewall event logs. You can select multiple options. **Syslog**: Firewall event logs will be sent to a syslog server. Refer to Diagnostics > Event Logs and Notifications > Syslog for more information. **Trap**: Firewall event notifications will be sent to a trap server. Refer to Diagnostics > SNMP Trap/Inform for more information. **Local Storage**: Firewall event logs will be stored on local storage and will show up in the device's Event Log. Refer to Diagnostics > Event Logs and Notifications > Event Log for more information.	Syslog / Trap / Local Storage	N/A
Action	Select the action the firewall should take for traffic that matches this policy. **Monitor**: The firewall will monitor packets that match the policy. **Drop**: The firewall will drop packets that match the policy.	Monitor / Drop	Drop
IP Address	Select the IP addresses this policy will apply to. Select **Any** to check traffic from all IP addresses, or select a pre-defined object. You can also click the Add (⊞) icon to create a new IP Address and Subnet object. Refer to Create Object for more information.	Any / Drop-down list of IP Address and Subnet objects	N/A
Port	Select the ports this policy will apply to. Select **Any** to check traffic from all ports, or select a pre-defined object. You can also click the Add (⊞) icon to create a new User-defined Service object. Refer to Create Object for more information.	Any / Drop-down list of port-based User-defined Service objects	N/A
Total TCP Connection	Specify the total allowed number of TCP connections.	1 to 9000	N/A
Concurrent TCP Request	Specify the total allowed number of concurrent TCP requests.	1 to 512	N/A

Edit Session Control Policy

Menu Path: Firewall > Session Control

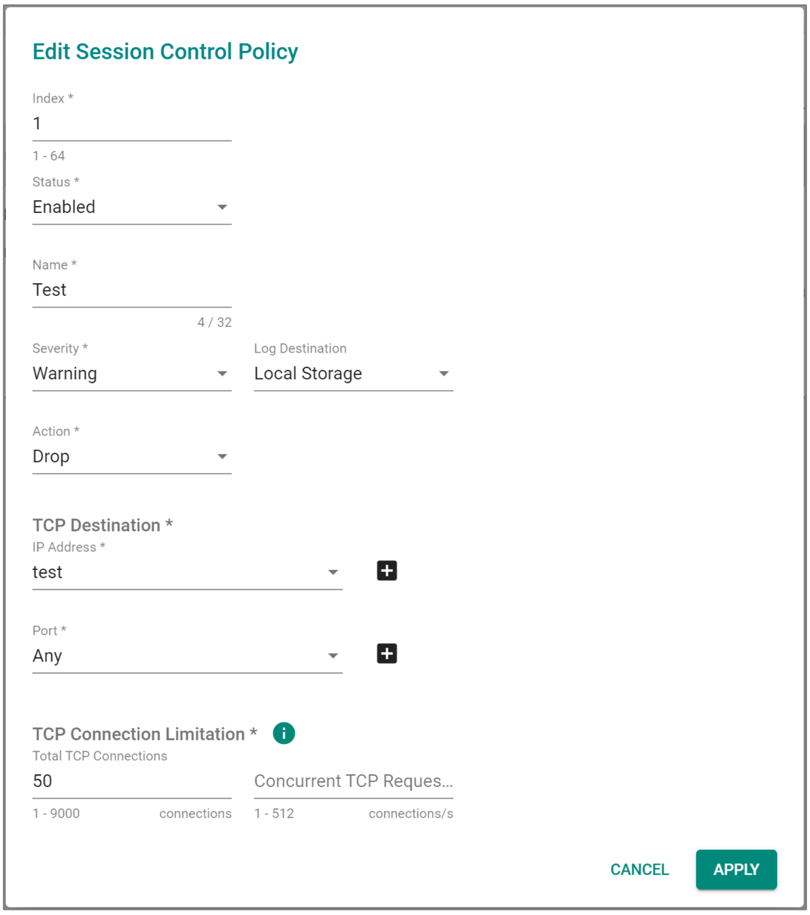
Clicking the **Edit (✎)** icon for a policy on the **Insert > Path Here** page will open this dialog box. This dialog lets you modify an existing policy. Click **APPLY** to save your changes.

Note

IP Address and **Port** cannot both be set to **Any**.

Note

At least one **TCP Connection Limitation** must be defined.



Edit Session Control Policy

Index *
1
1 - 64

Status *
Enabled

Name *
Test
4 / 32

Severity *
Warning

Log Destination
Local Storage

Action *
Drop

TCP Destination *

IP Address *
test

Port *
Any

TCP Connection Limitation *

Total TCP Connections
50
1 - 9000 connections

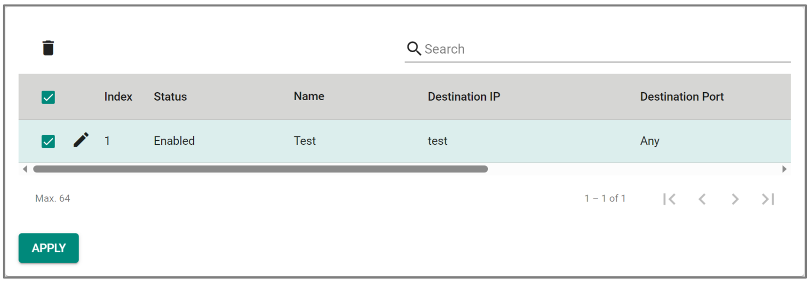
Concurrent TCP Reques...
1 - 512 connections/s

UI Setting	Description	Valid Range	Default Value
Index	Specify the index number for the policy. The index determines the order for processing policies.	1 to 64	Last used index plus 1
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Name	Specify a name for the policy.	1 to 32 characters	N/A
Severity	Select the severity level to assign events for this policy. Refer to Appendix > Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A
Log Destination	Specify where to send firewall event logs. You can select multiple options. **Syslog**: Firewall event logs will be sent to a syslog server. Refer to Diagnostics > Event Logs and Notifications > Syslog for more information. **Trap**: Firewall event notifications will be sent to a trap server. Refer to Diagnostics > SNMP Trap/Inform for more information. **Local Storage**: Firewall event logs will be stored on local storage and will show up in the device's Event Log. Refer to Diagnostics > Event Logs and Notifications > Event Log for more information.	Syslog / Trap / Local Storage	N/A
Action	Select the action the firewall should take for traffic that matches this policy. **Monitor**: The firewall will monitor packets that match the policy. **Drop**: The firewall will drop packets that match the policy.	Monitor / Drop	Drop
IP Address	Select the IP addresses this policy will apply to. Select **Any** to check traffic from all IP addresses, or select a pre-defined object. You can also click the Add (⊞) icon to create a new IP Address and Subnet object. Refer to Create Object for more information.	Any / Drop-down list of IP Address and Subnet objects	N/A
Port	Select the ports this policy will apply to. Select **Any** to check traffic from all ports, or select a pre-defined object. You can also click the Add (⊞) icon to create a new User-defined Service object. Refer to Create Object for more information.	Any / Drop-down list of port-based User-defined Service objects	N/A
Total TCP Connection	Specify the total allowed number of TCP connections.	1 to 9000	N/A
Concurrent TCP Request	Specify the total allowed number of concurrent TCP requests.	1 to 512	N/A

Delete Session Control Policy

Menu Path: Firewall > Session Control

- You can delete a policy by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.

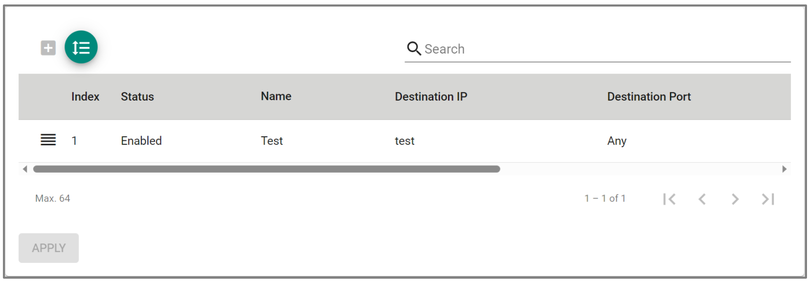


☑		Index	Status	Name	Destination IP	Destination Port
☑	✎	1	Enabled	Test	test	Any

Reorder Session Control Policies

Menu Path: Firewall > Session Control

You can reorder policies by clicking the **Reorder Priorities (↕≡)** icon, moving the entries into the order you want, then clicking the **Reorder Priorities (↕≡)** icon again. Reordering policies affects the order used to process the policies.



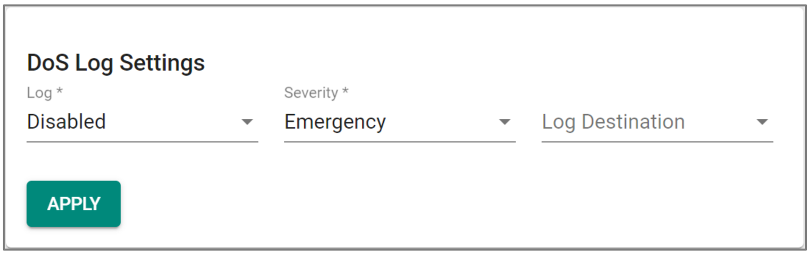
	Index	Status	Name	Destination IP	Destination Port
≡	1	Enabled	Test	test	Any

DoS Policy

Menu Path: Firewall > DoS Policy

This page lets you configure Denial of Service (DoS) protection features. You can configure different DoS functions for detecting abnormal packet formats or traffic flows, allowing your device to drop packets when it detects an abnormal packet format or identifies unusual traffic conditions.

DoS Log Settings



DoS Log Settings

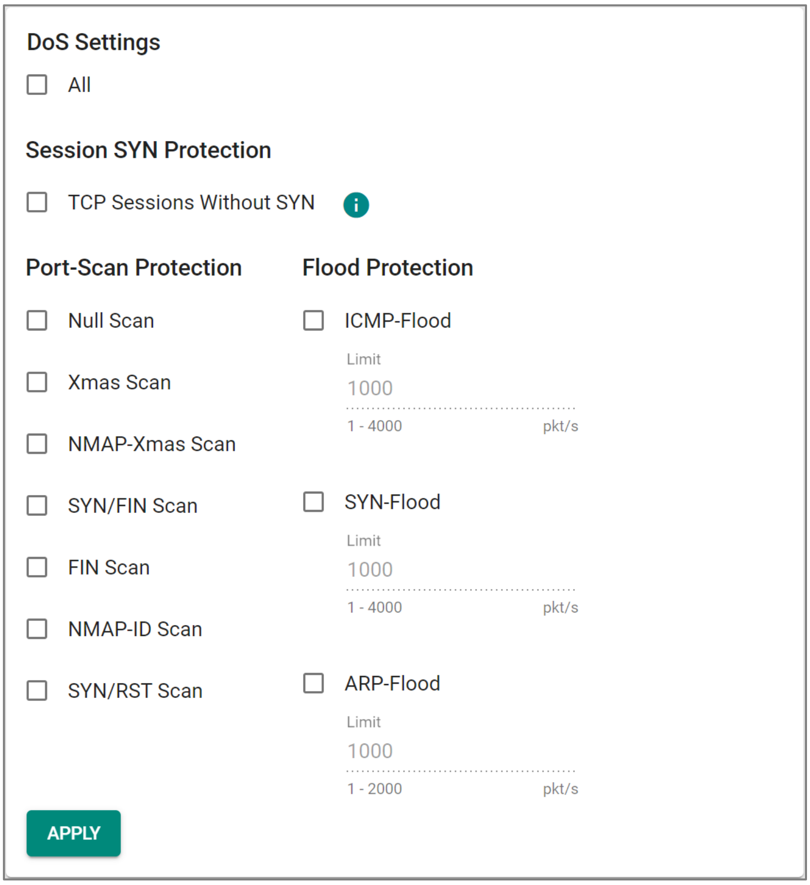
Log *: Disabled

Severity *: Emergency

Log Destination

UI Setting	Description	Valid Range	Default Value
Log	Enable or disable DoS event logs.	Enabled / Disabled	Disabled
Severity	Select the severity level to assign to DoS-related events. Refer to Appendix > Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency
Log Destination	Specify where to send firewall event logs. You can select multiple options. **Syslog**: Firewall event logs will be sent to a syslog server. Refer to Diagnostics > Event Logs and Notifications > Syslog for more information. **Trap**: Firewall event notifications will be sent to a trap server. Refer to Diagnostics > SNMP Trap/Inform for more information. **Local Storage**: Firewall event logs will be stored on local storage and will show up in the device's Event Log. Refer to Diagnostics > Event Logs and Notifications > Event Log for more information.	Local Storage / Syslog / Trap	N/A

DoS Settings


DoS Settings

□ All

Session SYN Protection

□ TCP Sessions Without SYN

Port-Scan Protection

□ Null Scan

□ Xmas Scan

□ NMAP-Xmas Scan

□ SYN/FIN Scan

□ FIN Scan

□ NMAP-ID Scan

□ SYN/RST Scan

Flood Protection

□ ICMP-Flood

Limit 1000 1 - 4000 pkt/s

□ SYN-Flood

Limit 1000 1 - 4000 pkt/s

□ ARP-Flood

Limit 1000 1 - 2000 pkt/s

UI Setting	Description	Valid Range	Default Value
DoS Settings	Toggle all DoS protection methods on or off.	All	N/A
Session SYN Protection	Enable or disable session SYN protection methods. **TCP Sessions Without SYN**: When enabled, this function will verify the SYN state within the TCP flag when establishing TCP sessions. If the SYN tag is missing in the initial packet, the system will drop the packet and block the connection. Running TCP sessions will be re-established to perform the check.	TCP Sessions Without SYN	Checked for all methods

UI Setting	Description	Valid Range	Default Value
Port-Scan Protection	Enable or disable port-scan protection methods.	Null Scan / Xmas Scan / NMAP-Xmas Scan / SYN/FIN Scan / FIN Scan / NMAP-ID Scan / SYN/RST Scan	Checked for all methods
Flood Protection	Enable or disable flood protection methods. When enabling a protection method, specify the limit in packets/second that will trigger the corresponding flood protection. **Note** If **Accept All LAN Port Connections** is enabled in **Trusted Access**, **SYN-Flood** will be disabled. Refer to Security > Device Security > Trusted Access for more information.	ICMP-Flood (1 to 4000) / SYN-Flood (1 to 4000) / ARP-Flood (1 to 2000)	Checked, 1000 for all methods

Advanced Protection

Menu Path: Firewall > Advanced Protection

This section lets you monitor and configure your device's advanced firewall features.

This section includes these pages:

- Dashboard
- Configuration
- Protocol Filter Policy
- ADP
- IPS

Dashboard

Menu Path: Firewall > Advanced Protection > Dashboard

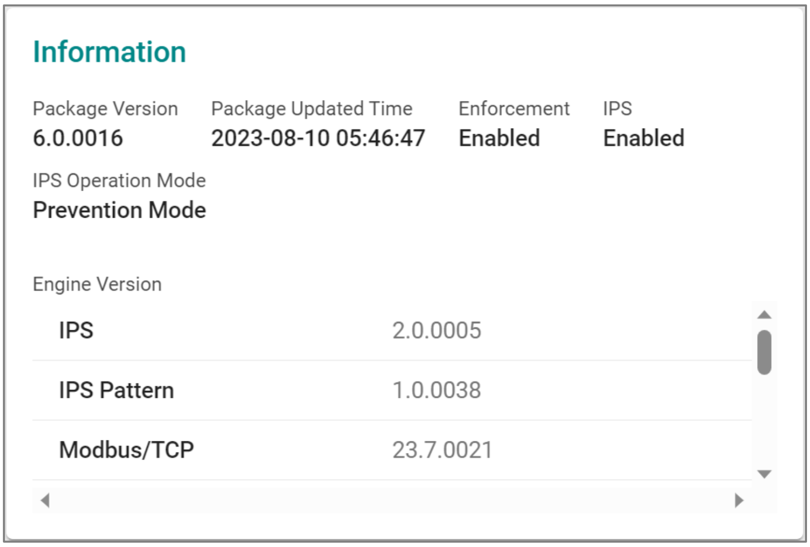
This page lets you see an overview of your firewall's advanced protection activity with real-time event counters.

Note

Please note that available status displays may vary depending on the product and model, and whether an IPS license is installed or not.

Information

This display shows the versions of the installed firewall engines and security packages currently installed on the device, as well as whether various functions are enabled.



Information

Package Version	Package Updated Time	Enforcement	IPS
6.0.0016	2023-08-10 05:46:47	Enabled	Enabled

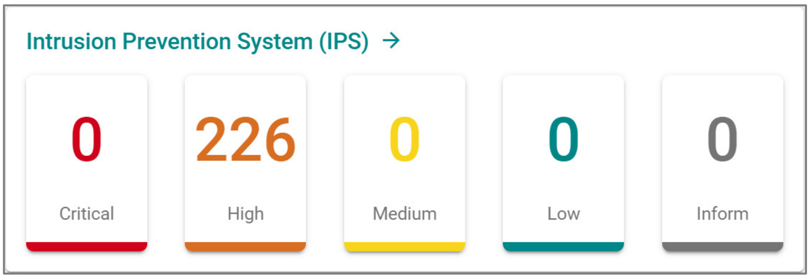
IPS Operation Mode
Prevention Mode

Engine Version

IPS	2.0.0005
IPS Pattern	1.0.0038
Modbus/TCP	23.7.0021

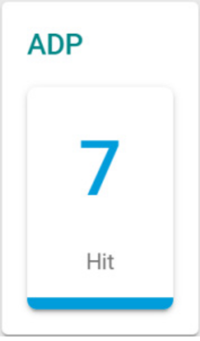
Intrusion Prevention System (IPS)

This display shows the current number of Intrusion Prevention System (IPS) events. Clicking on an item will take you to a filtered view of the IPS event log. Refer to Diagnostics > Event Logs and Notifications > Event Log - Firewall Log for more information.



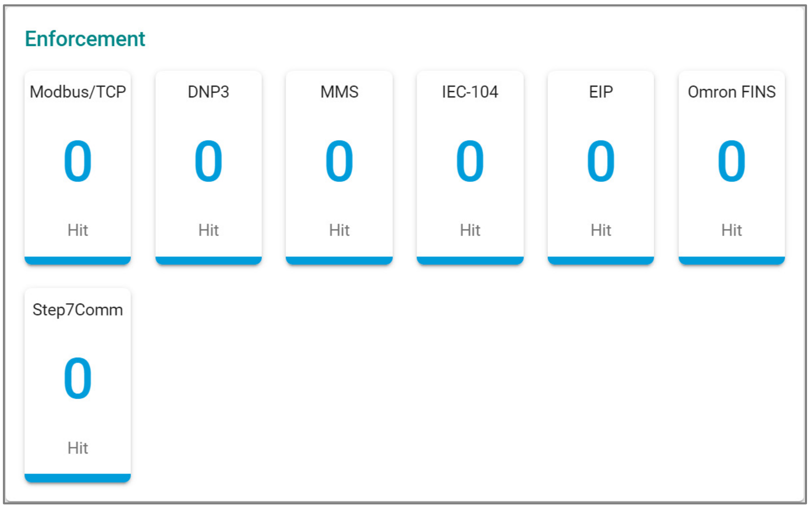
ADP

This display shows the current number of Anomaly Detection and Prevention (ADP) events. Clicking on an item will take you to the ADP event log. Refer to Diagnostics > Event Logs and Notifications > Event Log for more information.



Enforcement

This display shows the current number of industrial protocol events. Clicking on an item will take you to a filtered view of the Protocol Filter Policy event log. Refer to Diagnostics > Event Logs and Notifications > Event Log for more information.



Enforcement

Modbus/TCP	DNP3	MMS	IEC-104	EIP	Omron FINS	Step7Comm
0 Hit	0 Hit	0 Hit	0 Hit	0 Hit	0 Hit	0 Hit

Configuration

Menu Path: Firewall > Advanced Protection > Configuration

This page lets you configure your application firewall's advanced protection settings.

This page includes these tabs:

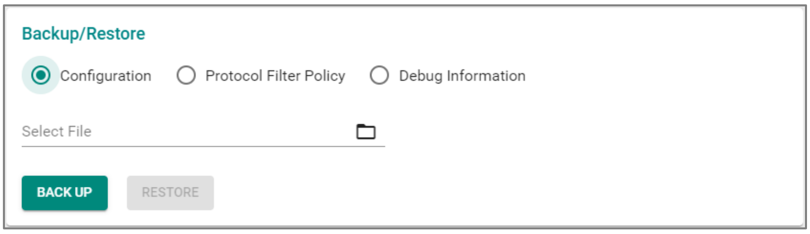
- Global Settings
- Protocol Filter Object
- Protocol Filter Profile

Configuration - Global Settings

Menu Path: Firewall > Advanced Protection > Configuration - Global Settings

This page lets you configure global settings for your application firewall's advanced protection features. You can also back up and restore your advanced protection settings on this page.

Backup/Restore



Backup/Restore

● Configuration ○ Protocol Filter Policy ○ Debug Information

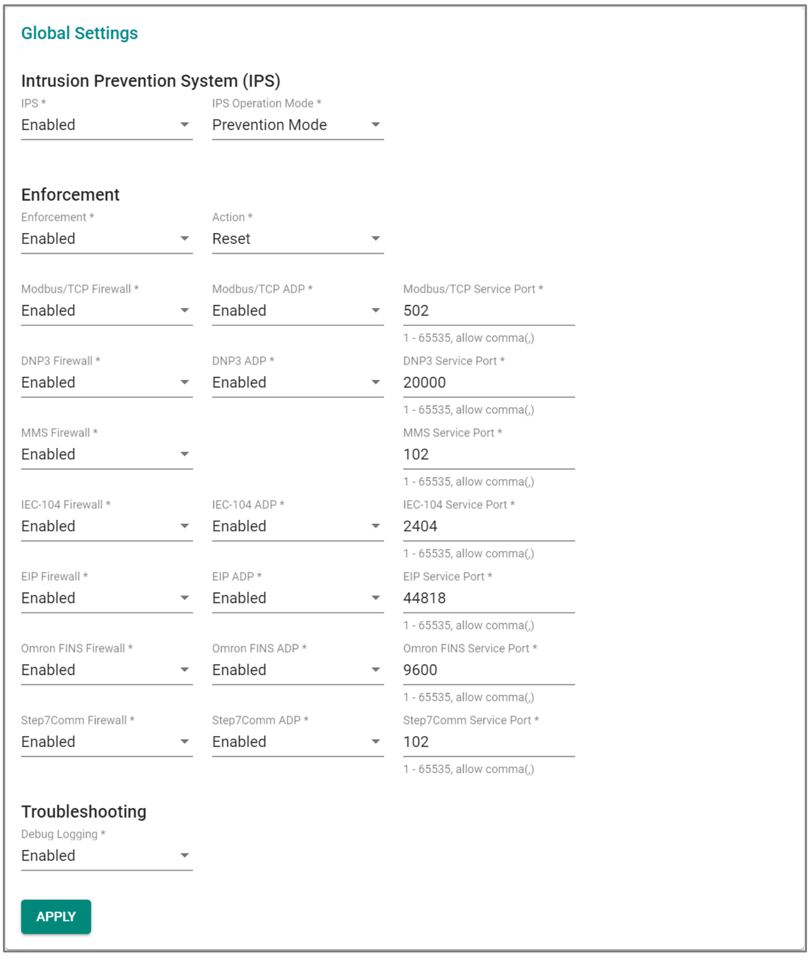
Select File

UI Setting	Description	Valid Range	Default Value
Backup/Restore	Select which settings you want to back up or restore. If you want to back up your settings, click **BACK UP**. **Configuration**: Back up/restore all settings on the **Firewall > Advanced Protection > Configuration** page. **Protocol Filter Policy**: Back up/restore all policies on the **Firewall > Advanced Protection > Protocol Filter Policy** page. **Debug Information**: Back up debug information for your firewall's advanced protection features.	Configuration / Protocol Filter Policy / Debug Information	Configuration
Select File **(if Backup/Restore is Configuration or Protocol Filter Policy)**	If you want to restore settings, click this field and select the settings file from your local computer, then click **RESTORE**.	N/A	N/A

Global Settings

Note

Available settings will vary depending on your product model and whether an active IPS license is installed.



Global Settings

Intrusion Prevention System (IPS)

IPS *: Enabled

IPS Operation Mode *: Prevention Mode

Enforcement

Enforcement *: Enabled

Action *: Reset

Modbus/TCP Firewall *: Enabled

Modbus/TCP ADP *: Enabled

Modbus/TCP Service Port *: 502

1 - 65535, allow comma(,)

DNP3 Firewall *: Enabled

DNP3 ADP *: Enabled

DNP3 Service Port *: 20000

1 - 65535, allow comma(,)

MMS Firewall *: Enabled

MMS Service Port *: 102

1 - 65535, allow comma(,)

IEC-104 Firewall *: Enabled

IEC-104 ADP *: Enabled

IEC-104 Service Port *: 2404

1 - 65535, allow comma(,)

EIP Firewall *: Enabled

EIP ADP *: Enabled

EIP Service Port *: 44818

1 - 65535, allow comma(,)

Omron FINS Firewall *: Enabled

Omron FINS ADP *: Enabled

Omron FINS Service Port *: 9600

1 - 65535, allow comma(,)

Step7Comm Firewall *: Enabled

Step7Comm ADP *: Enabled

Step7Comm Service Port *: 102

1 - 65535, allow comma(,)

Troubleshooting

Debug Logging *: Enabled

Intrusion Prevention System (IPS)

UI Setting	Description	Valid Range	Default Value
IPS	Enable or disable intrusion prevention system (IPS) functionality.	Enabled / Disabled	Enabled
IPS Operation Mode	Select the IPS operation mode.	Prevention Mode / Detection Mode	Prevention Mode

Enforcement

UI Setting	Description	Valid Range	Default Value
Enforcement	Enable or disable protocol filtering.	Enabled / Disabled	Enabled
Action	Select the default action of the protocol filter. **Accept**: The firewall will accept packets that match the policy. **Monitor**: The firewall will monitor packets that match the policy. **Reset**: The firewall will drop packets that match the policy, and the session will be disconnected.	Accept / Monitor / Reset	Reset
Modbus/TCP Firewall	Enable or disable the Modbus/TCP protocol filter engine.	Enabled / Disabled	Enabled
Modbus/TCP ADP	Enable or disable ADP for Modbus/TCP traffic.	Enabled / Disabled	Enabled
Modbus/TCP Service Port	Specify the service port for Modbus/TCP traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	502
DNP3 Firewall	Enable or disable the DNP3 protocol filter engine.	Enabled / Disabled	Enabled
DNP3 ADP	Enable or disable ADP for DNP3 traffic.	Enabled / Disabled	Enabled
DNP3 Service Port	Specify the service port for DNP3 traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	20000
MMS Firewall	Enable or disable the MMS protocol filter engine.	Enabled / Disabled	Enabled
MMS Service Port	Specify the service port for MMS traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	102
IEC-104 Firewall	Enable or disable the IEC-104 protocol filter engine.	Enabled / Disabled	Enabled
IEC-104 ADP	Enable or disable ADP for IEC-104 traffic.	Enabled / Disabled	Enabled
IEC-104 Service Port	Specify the service port for IEC-104 traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	2404
GOOSE Firewall	Enable or disable the GOOSE protocol filter engine.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
EIP Firewall	Enable or disable the EIP protocol filter engine.	Enabled / Disabled	Enabled
EIP ADP	Enable or disable ADP for EIP traffic.	Enabled / Disabled	Enabled
EIP Service Port	Specify the service port for EIP traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	44818
Omron FINS Firewall	Enable or disable the Omron FINS protocol filter engine.	Enabled / Disabled	Enabled
Omron FINS ADP	Enable or disable ADP for Omron FINS traffic.	Enabled / Disabled	Enabled
Omron FINS Service Port	Specify the service port for Omron FINS traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	9600
Step7Comm Firewall	Enable or disable the Step7Comm protocol filter engine.	Enabled / Disabled	Enabled
Step7Comm ADP	Enable or disable ADP for Step7Comm traffic.	Enabled / Disabled	Enabled
Step7Comm Service Port	Specify the service port for Step7Comm traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	102
TRDP Firewall	Enable or disable the TRDP protocol filter engine.	Enabled / Disabled	Enabled
TRDP Service Port	Specify the service port for TRDP traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	17224, 17225

Troubleshooting

UI Setting	Description	Valid Range	Default Value
Debug Logging	Enable or disable debug logging for troubleshooting.	Enables / Disabled	Disabled

Protocol Filter Object

Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Object

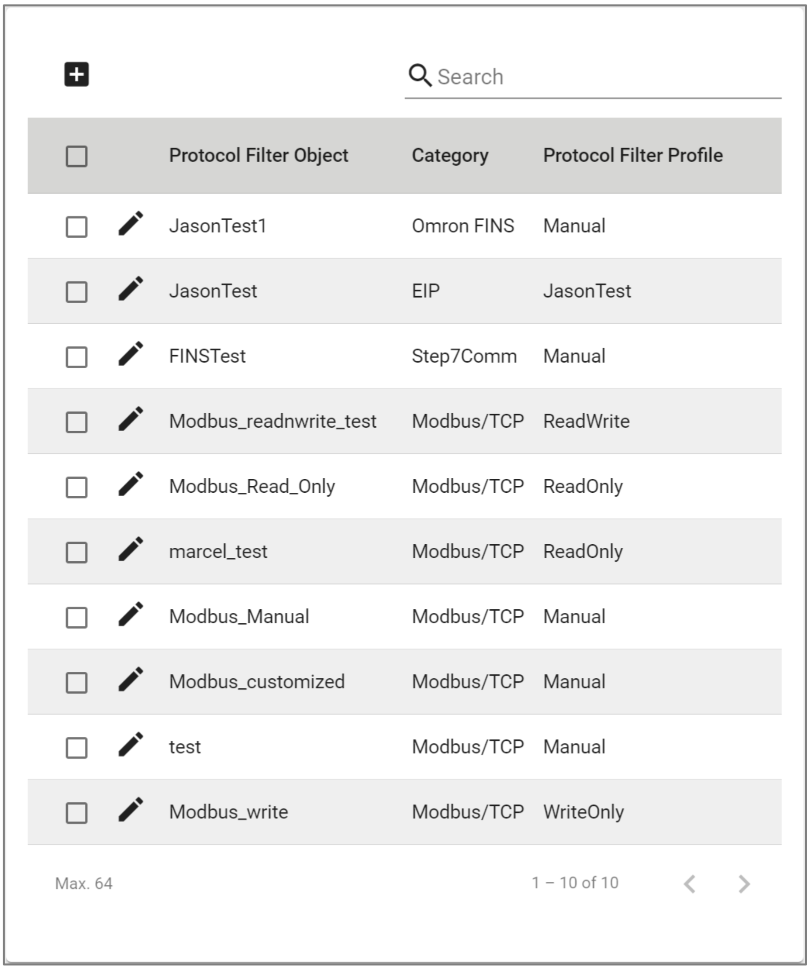
This page lets you create and manage protocol filter objects, which can simplify creation and maintenance of protocol filter policies.

Note

Available protocols may vary across different product models and versions.

Limitations

You can create up to 64 protocol filter objects.



Search

□		Protocol Filter Object	Category	Protocol Filter Profile
□	✎	JasonTest1	Omron FINS	Manual
□	✎	JasonTest	EIP	JasonTest
□	✎	FINSTest	Step7Comm	Manual
□	✎	Modbus_readnwrite_test	Modbus/TCP	ReadWrite
□	✎	Modbus_Read_Only	Modbus/TCP	ReadOnly
□	✎	marcel_test	Modbus/TCP	ReadOnly
□	✎	Modbus_Manual	Modbus/TCP	Manual
□	✎	Modbus_customized	Modbus/TCP	Manual
□	✎	test	Modbus/TCP	Manual
□	✎	Modbus_write	Modbus/TCP	WriteOnly

Max. 64

1 – 10 of 10

UI Setting	Description
Protocol Filter Object	Shows the name of the object
Category	Shows the protocol category of the object.
Protocol Filter Profile	Shows which protocol filter profile the object uses.

Protocol Filter Object - Create Object

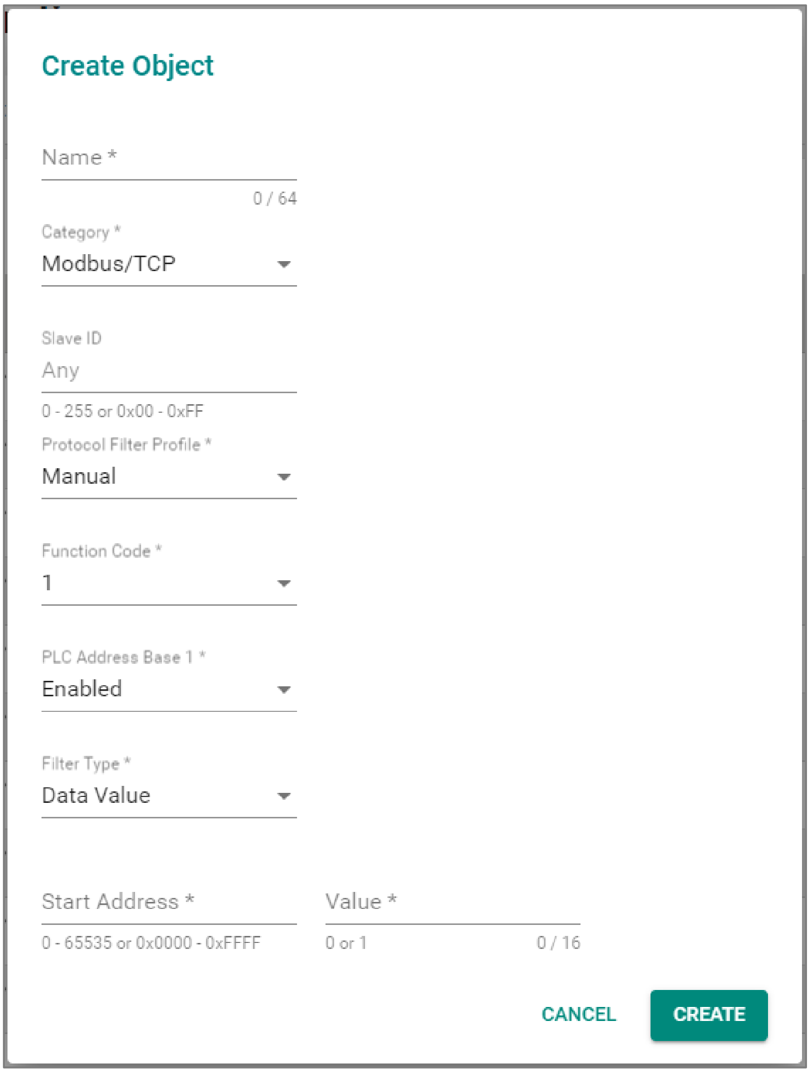
Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Object

Clicking the **Add (**⊞**)** icon on the **Firewall > Advanced Protection > Configuration -**

Protocol Filter Object page will open this dialog box. This dialog lets you create a protocol filter object. Click **CREATE** to save your changes and add the new object.

Create Object - Modbus/TCP

If **Modbus/TCP** is selected for the **Category**, these settings will appear.



Create Object

Name *
0 / 64

Category *
Modbus/TCP

Slave ID
Any
0 - 255 or 0x00 - 0xFF

Protocol Filter Profile *
Manual

Function Code *
1

PLC Address Base 1 *
Enabled

Filter Type *
Data Value

Start Address *
0 - 65535 or 0x0000 - 0xFFFF

Value *
0 or 1
0 / 16

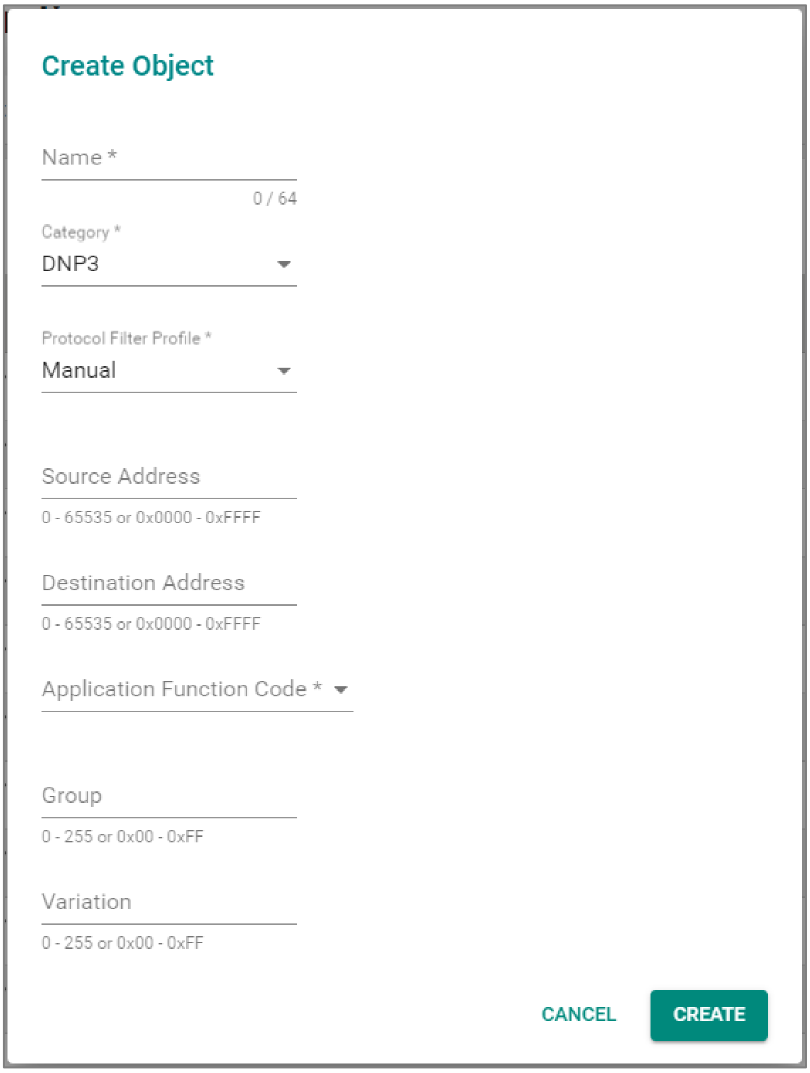
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A

UI Setting	Description	Valid Range	Default Value
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A
Slave ID	Specify the Modbus slave ID. Leave this field blank to represent any ID. The Slave ID is used to identify Modbus devices. This ID can be used to communicate via devices such as bridges and gateways which use a single IP address to support multiple independent end units.	0 to 255 / 0x00 to 0xFF	Any
Protocol Filter Profile	Select preset protocol filter profile or a user-configured protocol filter profile to use for this protocol filter object. **Read Only**: Use a set of commonly used function codes associated with read-only access. **Write Only**: Use a set of commonly used function codes associated with write-only access. **Read/Write**: Use a set of commonly used function codes associated with read/write access. **Manual**: Manually enter the settings for this object. Refer to Firewall > Advanced Protection > Configuration - Protocol Filter Profile for more information on creating protocol filter profiles.	Read Only / Write Only / Read/Write / Drop-down list of related protocol filter profiles / Manual	N/A
Function Code	Shows which function codes will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select which function codes to use for this object. You can select multiple options.	Drop-down list of function codes	Depends on the selected **Protocol Filter Profile**
PLC Address Base 1 **(if only one Function Code is selected)**		Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Filter Type **(if only one Function Code is selected)**		None / Address Range / Data Value	None
Address Range **(if Filter Type is Address Range)**		0 to 65535 / 0x0000 to 0xFFFF	N/A
Start Address **(if Filter Type is Data Value)**		0 to 65535 / 0x0000 to 0xFFFF	N/A
Value **(if Filter Type is Data Value)**		0 to 1	N/A

Create Object - DNP3

If **DNP3** is selected for the **Category**, these settings will appear.



Create Object

Name *

0 / 64

Category *

DNP3

Protocol Filter Profile *

Manual

Source Address

0 - 65535 or 0x0000 - 0xFFFF

Destination Address

0 - 65535 or 0x0000 - 0xFFFF

Application Function Code *

Group

0 - 255 or 0x00 - 0xFF

Variation

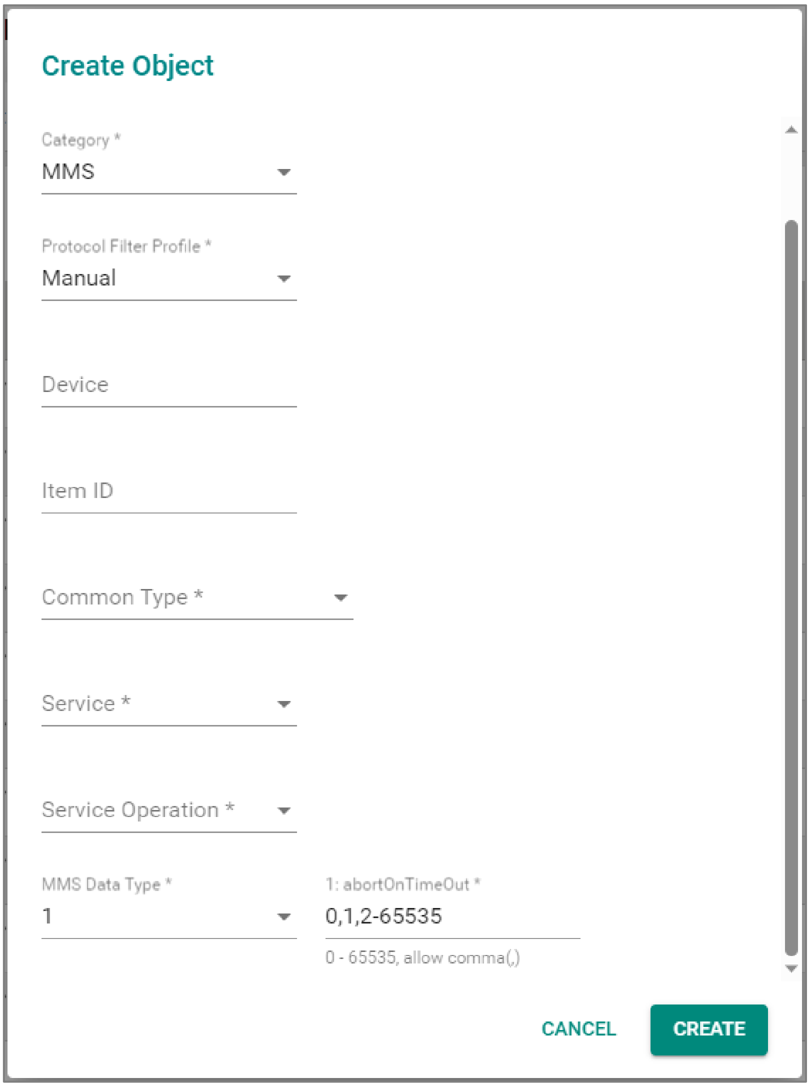
0 - 255 or 0x00 - 0xFF

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A

UI Setting	Description	Valid Range	Default Value
Protocol Filter Profile	Select a user-configured protocol filter profile to use for this protocol filter object. **Manual**: Manually enter the settings for this object. Refer to Firewall > Advanced Protection > Configuration - Protocol Filter Profile for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A
Source Address	Shows the source address to check for in DNP3 packets, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the source address to check for in DNP3 packets.	0 to 65535 / 0x0000 to 0xFFFF	Depends on the selected **Protocol Filter Profile**
Destination Address	Shows the destination address to check for in DNP3 packets, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the destination address to check for in DNP3 packets.	0 to 65535 / 0x0000 to 0xFFFF	Depends on the selected **Protocol Filter Profile**
Application Function Code	Shows which function code will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select which function code to use for this object.	Drop-down list of function codes	Depends on the selected **Protocol Filter Profile**
Group	Shows the group to use to classify types within a message, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the function code to use for this object.	0 to 255 or 0x00 to 0xFF	Depends on the selected **Protocol Filter Profile**
Variation	Shows the variation to use for encoding formats, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the variation to use for this object.	0 to 255 or 0x00 to 0xFF	Depends on the selected **Protocol Filter Profile**

Create Object - MMS

If **MMS** is selected for the **Category**, these settings will appear.



Create Object

Category *: MMS

Protocol Filter Profile *: Manual

Device

Item ID

Common Type *

Service *

Service Operation *

MMS Data Type *: 1

1: abortOnTimeOut *: 0,1,2-65535

0 - 65535, allow comma(,)

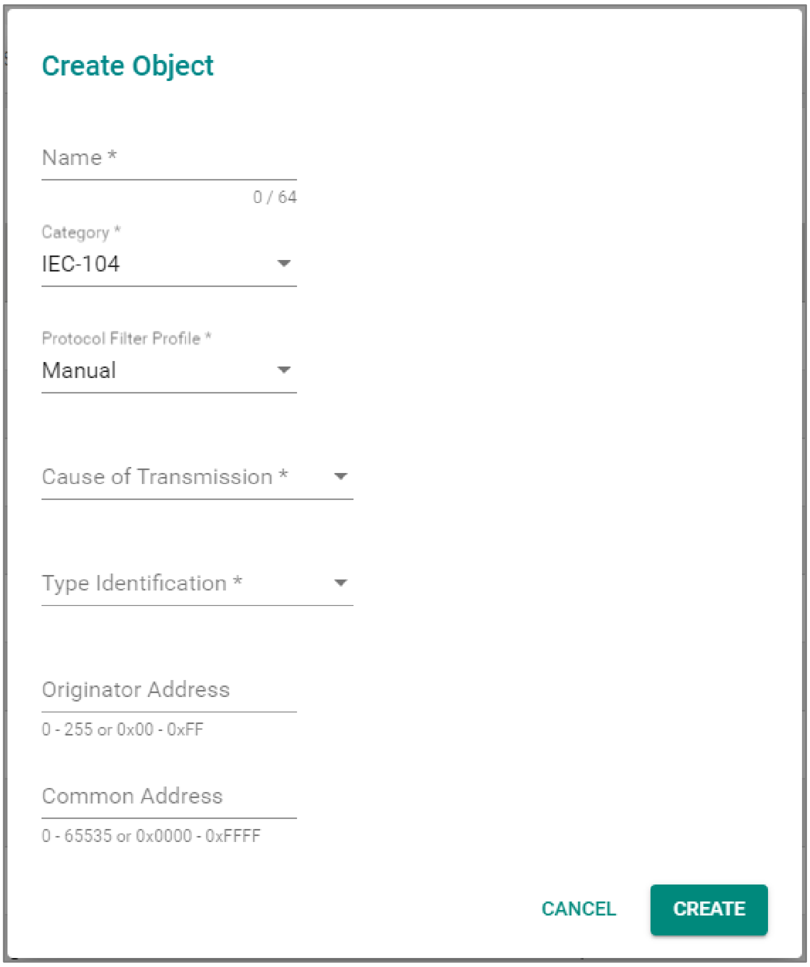
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A

UI Setting	Description	Valid Range	Default Value
Protocol Filter Profile	Select preset protocol filter profile or a user-configured protocol filter profile to use for this protocol filter object. **Manual**: Manually enter the settings for this object. Refer to Firewall > Advanced Protection > Configuration - Protocol Filter Profile for more information on creating protocol filter profiles.	Identify Service / Read Service / Write Service / Report Service / File Operation Service / Journal Service / Drop-down list of related protocol filter profiles / Manual	N/A
Device	Specify a device name for the object.		N/A
Item ID	Specify an item ID for the object.		N/A
Command Type	Shows which MMS command type will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select the command type to use for the object. Refer to MMS Command Type List for an overview of all command types.	Drop-down list of MMS command types	Depends on the selected **Protocol Filter Profile**
Service	Shows which service will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select the service to use for the object.	Any / Confirmed Request / Confirmed Response / Unconfirmed	Depends on the selected **Protocol Filter Profile**
Service Operation	Shows which service operations will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select the service operations to use for the object. You can select multiple options. Refer to MMS Service Operation List for an overview of all service operations.	Drop-down list of service operations	Depends on the selected **Protocol Filter Profile**

UI Setting	Description	Valid Range	Default Value
MMS Data Type	Specify which MMS data types to use for the object. You can select multiple options. For each service operation, specify the values to use. You can specify multiple values by separating them with a comma.	Drop-down list of MMS data types 0 to 65535	N/A

Create Object - IEC-104

If **IEC-104** is selected for the **Category**, these settings will appear.



Create Object

Name *
0 / 64

Category *
IEC-104

Protocol Filter Profile *
Manual

Cause of Transmission *

Type Identification *

Originator Address
0 - 255 or 0x00 - 0xFF

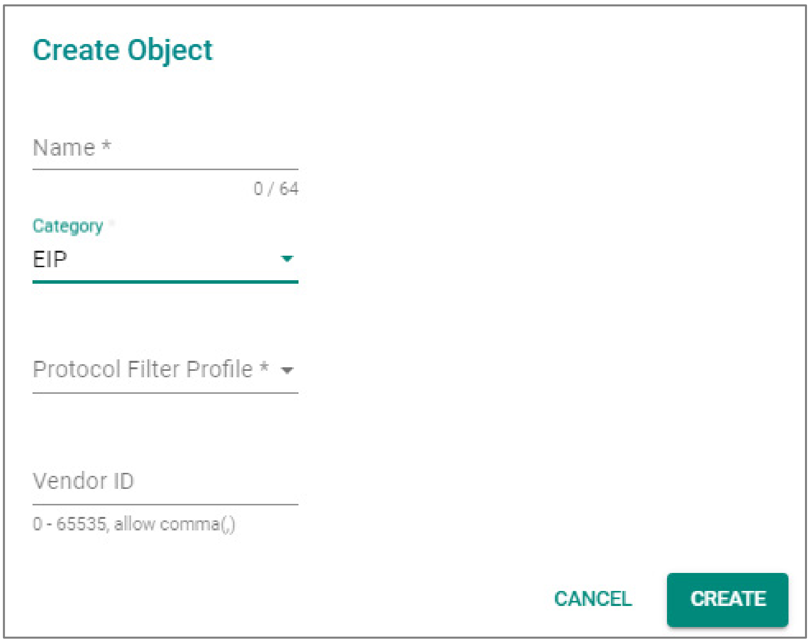
Common Address
0 - 65535 or 0x0000 - 0xFFFF

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A
Protocol Filter Profile	Select a user-configured protocol filter profile to use for this protocol filter object. **Manual**: Manually enter the settings for this object. Refer to Firewall > Advanced Protection > Configuration - Protocol Filter Profile for more information on creating protocol filter profiles.	Identify Service / Read Service / Write Service / Report Service / File Operation Service / Journal Service / Drop-down list of related protocol filter profiles / Manual	N/A
Cause of Transmission	Shows which IEC-104 cause of transmission code will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select the cause to use for the object. Refer to the IEC-104 Cause of Transmission List for an overview of the different codes and corresponding descriptions.	Drop-down list of IEC-104 cause of transmission codes	Depends on the selected **Protocol Filter Profile**
Type Identification	Shows which IEC-104 type identification code will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select the type to use for the object. Refer to the IEC-104 Type Identification List for an overview of the different codes and corresponding descriptions.	Drop-down list of IEC-104 type identification codes	Depends on the selected **Protocol Filter Profile**

UI Setting	Description	Valid Range	Default Value
Originator Address	Shows which originator address will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the address to use for the object.	0 to 255 / 0x00 to 0xFF	Depends on the selected **Protocol Filter Profile**
Common Address	Shows which common address will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the address to use for the object.	0 to 65535 / 0x0000 to 0xFFFF	Depends on the selected **Protocol Filter Profile**

Create Object - EIP

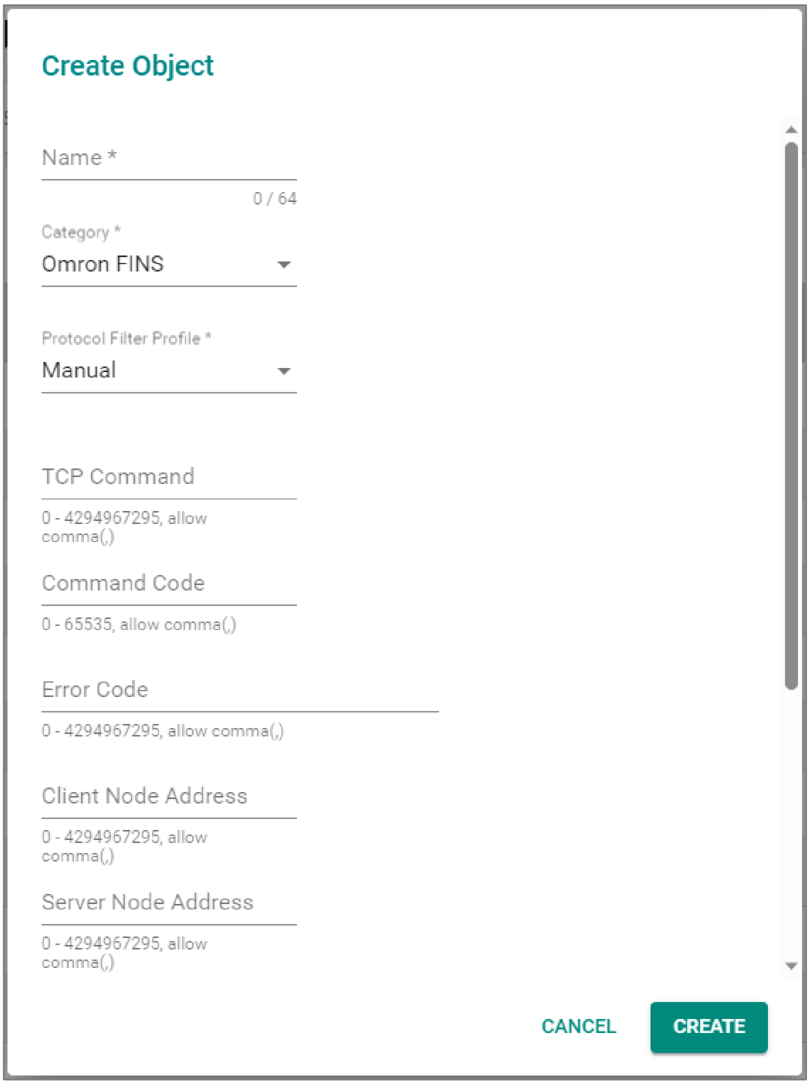
If **EIP** is selected for the **Category**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A
Category	Select a protocol for this object. ✎ **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A
Protocol Filter Profile	Select a user-configured protocol filter profile to use for this protocol filter object. **Manual**: Manually enter the settings for this object. Refer to Firewall > Advanced Protection > Configuration - Protocol Filter Profile for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A
Command Code	Shows the EIP command codes that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the command codes to use for this object. You can specify multiple values by separating them with a comma.	0 - 65535	Depends on the selected **Protocol Filter Profile**
Type ID	Shows the type IDs that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the type IDs to use for this object. You can specify multiple values by separating them with a comma.	0 - 65535	Depends on the selected **Protocol Filter Profile**
Device Type	Shows the device types that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the device types to use for this object. You can specify multiple values by separating them with a comma.	0 - 65535	Depends on the selected **Protocol Filter Profile**
Vendor ID	Specify the vendor IDs to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A

Create Object - Omron FINS

If **Omron FINS** is selected for the **Category**, these settings will appear.



Create Object

Name *

0 / 64

Category *

Omron FINS

Protocol Filter Profile *

Manual

TCP Command

0 - 4294967295, allow comma(,)

Command Code

0 - 65535, allow comma(,)

Error Code

0 - 4294967295, allow comma(,)

Client Node Address

0 - 4294967295, allow comma(,)

Server Node Address

0 - 4294967295, allow comma(,)

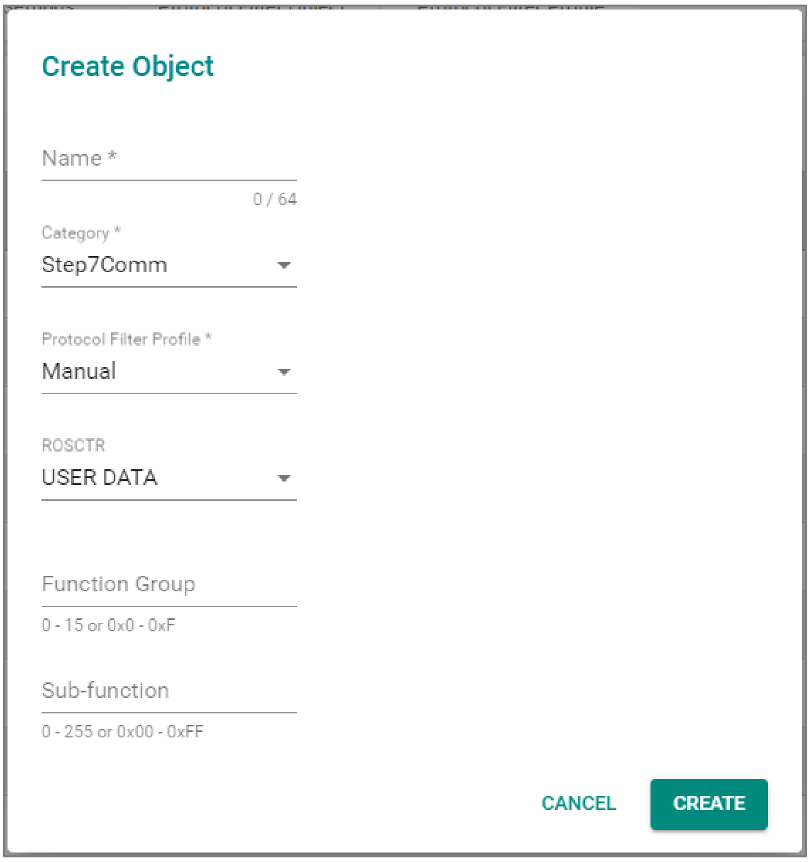
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A

UI Setting	Description	Valid Range	Default Value
Protocol Filter Profile	Select a user-configured protocol filter profile to use for this protocol filter object. **Manual**: Manually enter the settings for this object. Refer to Firewall > Advanced Protection > Configuration - Protocol Filter Profile for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A
TCP Command	Shows the TCP command codes that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the command codes to use for this object. You can specify multiple values by separating them with a comma.	0 to 4294967295	Depends on the selected **Protocol Filter Profile**
Command Code	Shows the command codes that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the command codes to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	Depends on the selected **Protocol Filter Profile**
Error Code	Shows the error codes that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the error codes to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	Depends on the selected **Protocol Filter Profile**
Client Node Address	Specify the client node addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 4294967295	N/A
Server Node Address	Specify the server node addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 4294967295	N/A
File Position	Specify the file positions to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A
File Position Begin Address	Specify the file position begin addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A
Begin Address	Specify the begin addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A

UI Setting	Description	Valid Range	Default Value
Record Begin Address	Specify the record begin addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A

Create Object - Step7Comm

If **Step7Comm** is selected for the **Category**, these settings will appear.



Create Object

Name *

0 / 64

Category *

Step7Comm

Protocol Filter Profile *

Manual

ROSCTR

USER DATA

Function Group

0 - 15 or 0x0 - 0xF

Sub-function

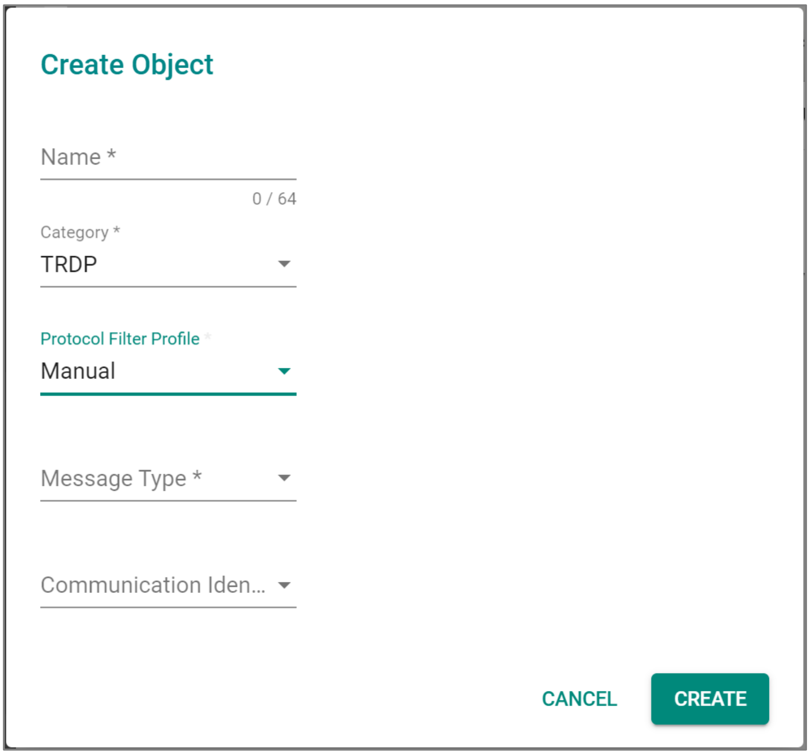
0 - 255 or 0x00 - 0xFF

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A

UI Setting	Description	Valid Range	Default Value
Category	Select a protocol for this object. ✎ **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A
Protocol Filter Profile	Select a user-configured protocol filter profile to use for this protocol filter object. **Manual**: Manually enter the settings for this object. Refer to Firewall > Advanced Protection > Configuration - Protocol Filter Profile for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A
ROSCTR	Shows the ROSCTR control that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the ROSCTR control to use for this object.	ANY / JOB / USER DATA	Depends on the selected **Protocol Filter Profile**
Function **(if ROSCTR is JOB)**	Shows the function code that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the function code to use for this object.	0 to 255 / 0x00 to 0xFF	Depends on the selected **Protocol Filter Profile**
Function Group **(if ROSCTR is USER DATA)**	Shows the function group that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the function group to use for this object.	0 to 15 / 0x0 to 0xF	Depends on the selected **Protocol Filter Profile**
Sub-function **(if ROSCTR is USER DATA)**	Shows the sub-function group that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the sub-function code to use for this object.	0 to 255 / 0x00 to 0xFF	Depends on the selected **Protocol Filter Profile**

Create Object - TRDP

If **TRDP** is selected for the **Category**, these settings will appear.



Create Object

Name *

0 / 64

Category *

TRDP

Protocol Filter Profile *

Manual

Message Type *

Communication Iden...

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A
Protocol Filter Profile	Select a preset protocol filter profile or a user-configured protocol filter profile to use for this protocol filter object. **Manual**: Manually enter the settings for this object. Refer to the TRDP Protocol Filter Profile List for more information on TRDP presets. Refer to Firewall > Advanced Protection > Configuration - Protocol Filter Profile for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A

UI Setting	Description	Valid Range	Default Value
Message Type	Shows which message types will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select which message types to use for this object. You can select multiple options. Refer to the TRDP Message Type List for more information.	Drop-down list of message types	Depends on the selected **Protocol Filter Profile**
Communication Identifier	Shows which communication identifiers will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select which communication identifiers to use for this object. You can select multiple options. The last option in the list lets you add your own communication identifiers. You can specify multiple values by separating them with a comma. Refer to IEC 61375-2-3 Communication Identifiers for more information.	Drop-down list of communication identifiers 1 to 4294967295	Depends on the selected **Protocol Filter Profile**

Protocol Filter Profile

Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Profile

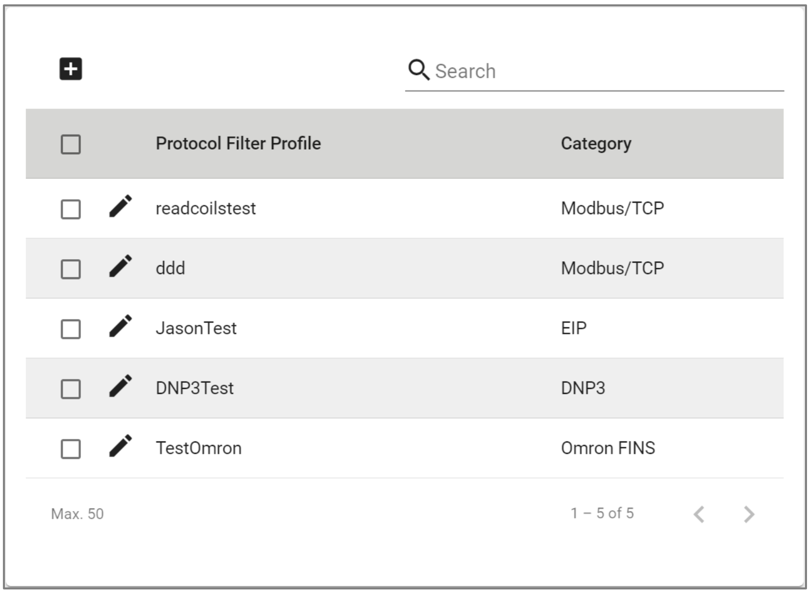
This page lets you create and manage protocol filter profiles to simplify maintaining protocol-related settings. Protocol filter profiles can be used when creating protocol filter objects, and a single profile can be used in multiple protocol filter objects.

Note

Available protocols may vary across different product models and versions.

Limitations

You can create up to 50 protocol filter profiles.



☐		Protocol Filter Profile	Category
☐	✎	readcoilstest	Modbus/TCP
☐	✎	ddd	Modbus/TCP
☐	✎	JasonTest	EIP
☐	✎	DNP3Test	DNP3
☐	✎	TestOmron	Omron FINS

UI Setting	Description
Protocol Filter Profile	Shows the name of the profile.
Category	Shows the protocol category of the profile.

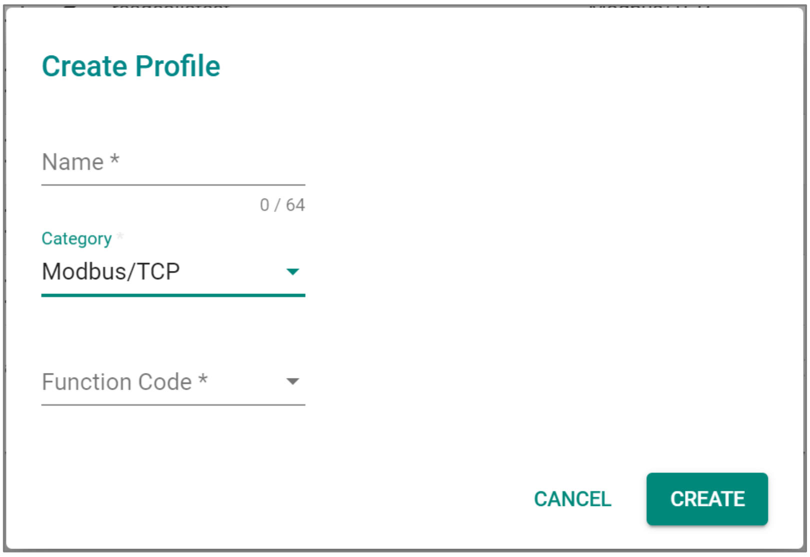
Protocol Filter Profile - Create Profile

Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Profile

Clicking the **Add (**⊞**)** icon on the **Firewall > Advanced Protection > Configuration - Protocol Filter Profile** page will open this dialog box. This dialog lets you create a protocol filter profile. Click **CREATE** to save your changes and add the new profile.

Create Profile - Modbus/TCP

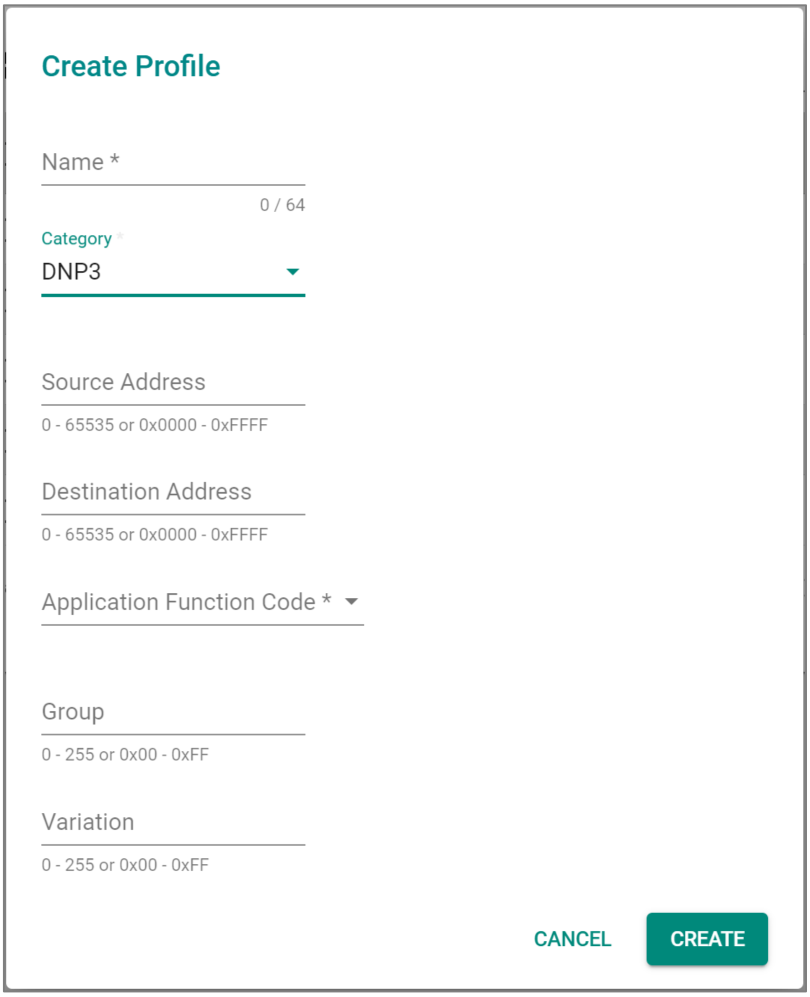
If **Modbus/TCP** is selected for the **Category**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A
Function Code	Select which function codes to use for this profile. You can select multiple options.	Drop-down list of function codes	N/A

Create Profile - DNP3

If **DNP3** is selected for the **Category**, these settings will appear.



Create Profile

Name *

0 / 64

Category *

DNP3

Source Address

0 - 65535 or 0x0000 - 0xFFFF

Destination Address

0 - 65535 or 0x0000 - 0xFFFF

Application Function Code *

Group

0 - 255 or 0x00 - 0xFF

Variation

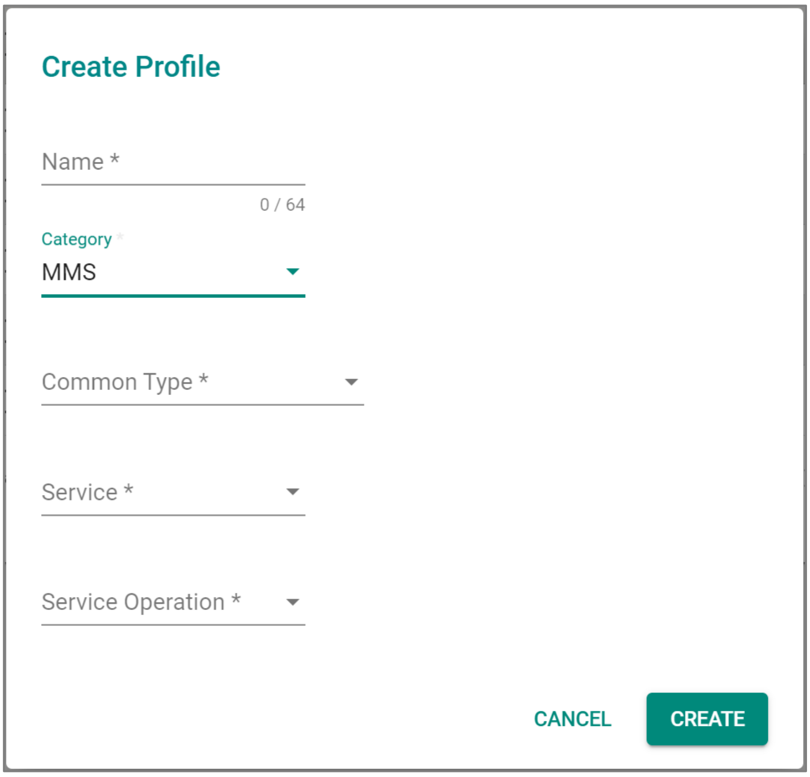
0 - 255 or 0x00 - 0xFF

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A
Category	Select a protocol for this profile. ✎ **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A
Source Address	Specify the source address to check for in DNP3 packets.	0 to 65535 / 0x0000 to 0xFFFF	N/A

UI Setting	Description	Valid Range	Default Value
Destination Address	Specify the destination address to check for in DNP3 packets.	0 to 65535 / 0x0000 to 0xFFFF	N/A
Application Function Code	Select which function code to use for this profile.	Drop-down list of function codes	N/A
Group	Specify the function code to use for this profile.	0 to 255 or 0x00 to 0xFF	N/A
Variation	Specify the variation to use for this profile.	0 to 255 or 0x00 to 0xFF	N/A

Create Profile - MMS

If **MMS** is selected for the **Category**, these settings will appear.


Create Profile

Name *

0 / 64

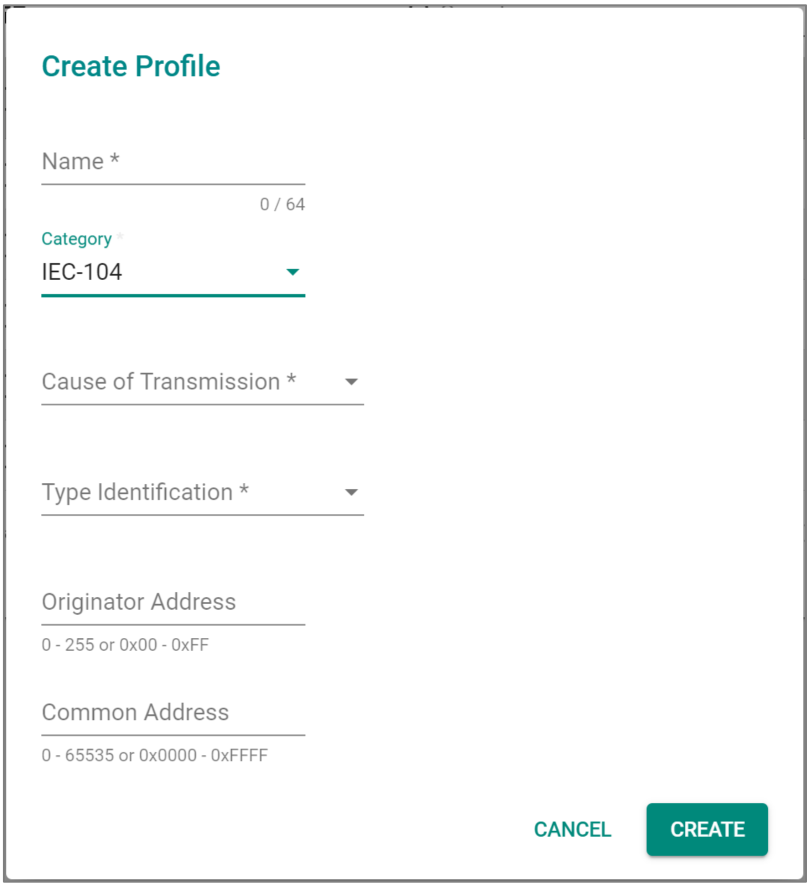
Category *

MMS

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A
Category	Select a protocol for this profile. ✎ **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A
Command Type	Select the command type to use for the profile. Refer to MMS Command Type List for an overview of all command types.	Drop-down list of MMS command types	N/A
Service	Select the service to use for the profile.	Any / Confirmed Request / Confirmed Response / Unconfirmed	N/A
Service Operation	Select the service operations to use for the profile. You can select multiple options. Refer to MMS Service Operation List for an overview of all service operations.	Drop-down list of service operations	N/A

Create Profile - IEC-104

If **IEC-104** is selected for the **Category**, these settings will appear.



Create Profile

Name *

0 / 64

Category *

IEC-104

Cause of Transmission *

Type Identification *

Originator Address

0 - 255 or 0x00 - 0xFF

Common Address

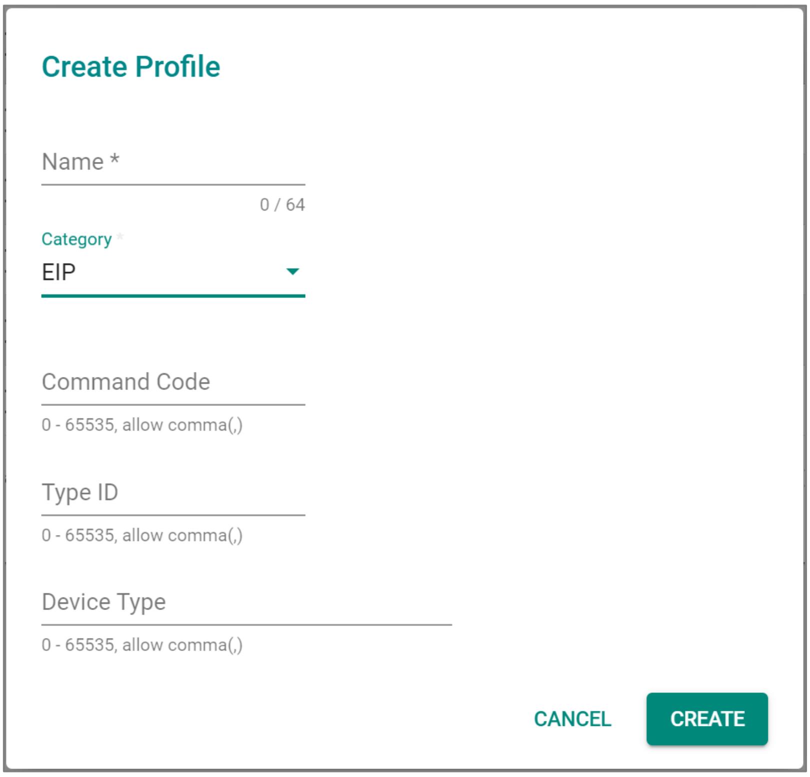
0 - 65535 or 0x0000 - 0xFFFF

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A
Cause of Transmission	Select the IEC-104 cause of transmission code to use for the profile. Refer to the IEC-104 Cause of Transmission List for an overview of the different codes and corresponding descriptions.	D rop-down list of IEC-104 cause of transmission codes	N/A

UI Setting	Description	Valid Range	Default Value
Type Identification	Select the IEC-104 type identification code to use for the profile. Refer to the IEC-104 Type Identification List for an overview of the different codes and corresponding descriptions.	Drop-down list of IEC-104 type identification codes	N/A
Originator Address	Specify the originator address to use for the profile.	0 to 255 / 0x00 to 0xFF	N/A
Common Address	Specify the common address to use for the profile.	0 to 65535 / 0x0000 to 0xFFFF	N/A

Create Profile - EIP

If **EIP** is selected for the **Category**, these settings will appear.



Create Profile

Name *

0 / 64

Category *

EIP

Command Code

0 - 65535, allow comma(,)

Type ID

0 - 65535, allow comma(,)

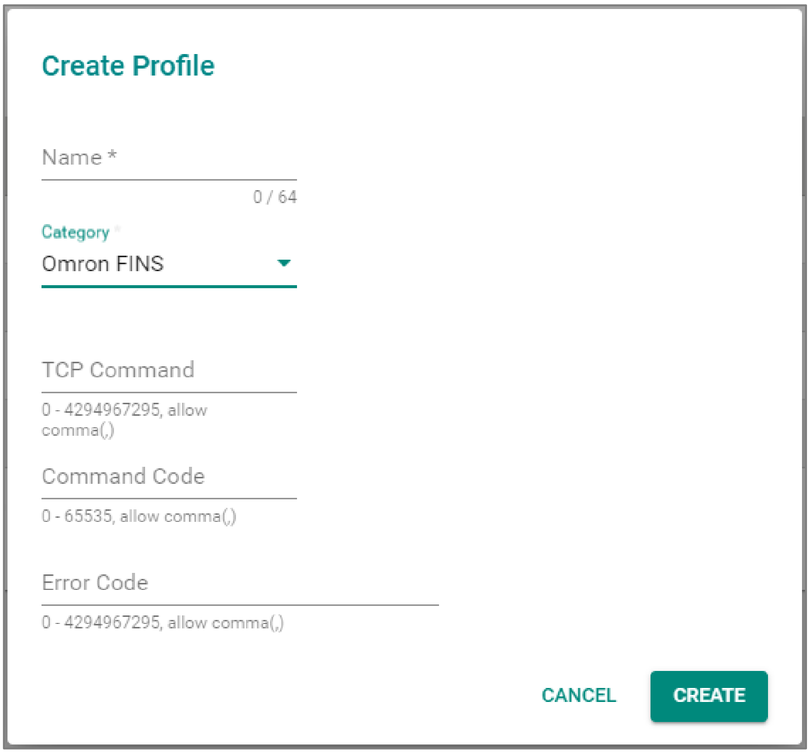
Device Type

0 - 65535, allow comma(,)

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A
Command Code	Specify the command codes to use for this profile. You can specify multiple values by separating them with a comma.	0 - 65535	N/A
Type ID	Specify the type IDs to use for this profile. You can specify multiple values by separating them with a comma.	0 - 65535	N/A
Device Type	Specify the device types to use for this profile. You can specify multiple values by separating them with a comma.	0 - 65535	N/A

Create Profile - Omron FINS

If **Omron FINS** is selected for the **Category**, these settings will appear.



Create Profile

Name *

0 / 64

Category

Omron FINS

TCP Command

0 - 4294967295, allow comma(,)

Command Code

0 - 65535, allow comma(,)

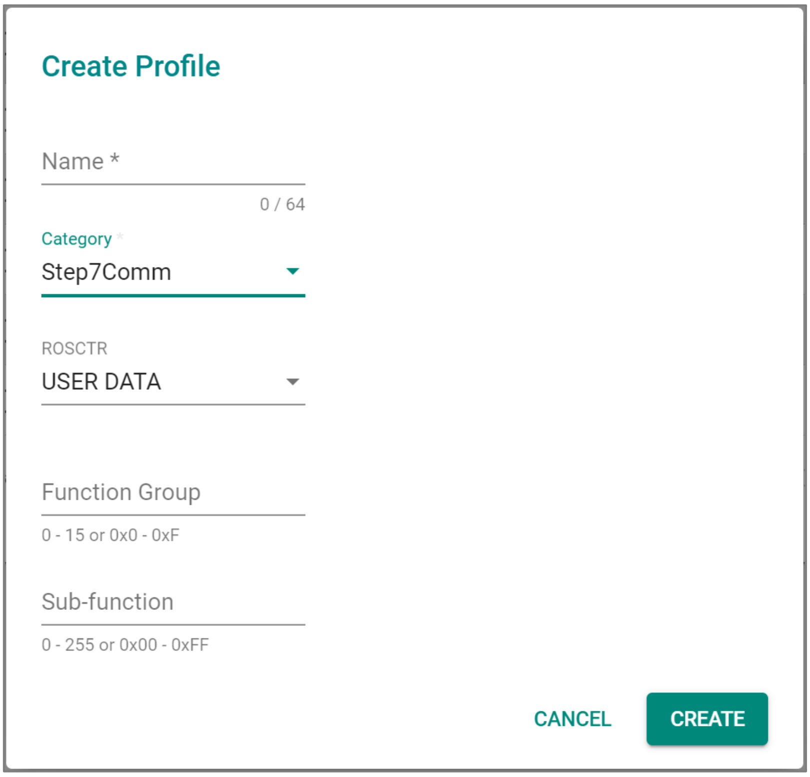
Error Code

0 - 4294967295, allow comma(,)

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A
TCP Command	Specify the TCP command codes to use for this profile. You can specify multiple values by separating them with a comma.	0 to 4294967295	N/A
Command Code	Specify the command codes to use for this profile. You can specify multiple values by separating them with a comma.	0 to 65535	N/A
Error Code	Specify the error codes to use for this profile. You can specify multiple values by separating them with a comma.	0 to 65535	N/A

Create Profile - Step7Comm

If **Step7Comm** is selected for the **Category**, these settings will appear.


Create Profile

Name *
0 / 64

Category *
Step7Comm

ROSCTR
USER DATA

Function Group
0 - 15 or 0x0 - 0xF

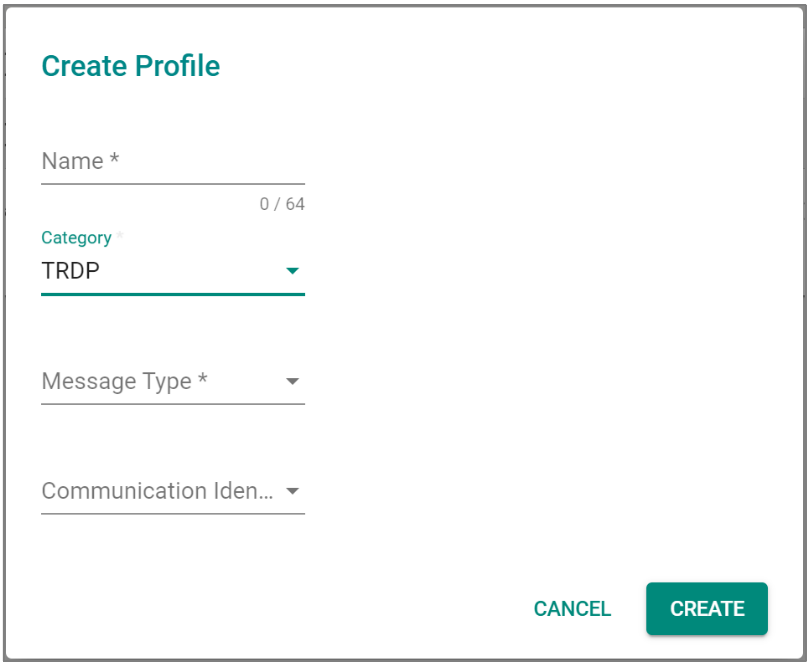
Sub-function
0 - 255 or 0x00 - 0xFF

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A
ROSCTR	Specify the ROSCTR control to use for this profile.	ANY / JOB / USER DATA	N/A

UI Setting	Description	Valid Range	Default Value
Function **(if ROSCTR is JOB)**	Specify the function code to use for this profile.	0 to 255 / 0x00 to 0xFF	N/A
Function Group **(if ROSCTR is USER DATA)**	Specify the function group to use for this profile.	0 to 15 / 0x0 to 0xF	N/A
Sub-function **(if ROSCTR is USER DATA)**	Specify the sub-function code to use for this profile.	0 to 255 / 0x00 to 0xFF	N/A

Create Profile - TRDP

If **TRDP** is selected for the **Category**, these settings will appear.


Create Profile

Name *

0 / 64

Category *

TRDP

Message Type *

Communication Iden...

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A

UI Setting	Description	Valid Range	Default Value
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP	N/A
Message Type	Select which message types to use for this profile. You can select multiple options. Refer to the TRDP Message Type List for more information.	Drop-down list of message types	N/A
Communication Identifier	Select which communication identifiers to use for this profile. You can select multiple options. The last option in the list lets you add your own communication identifier. You can specify multiple values by separating them with a comma. Refer to IEC 61375-2-3 Communication Identifiers for more information.	Drop-down list of communication identifiers 1 to 4294967295	N/A

Protocol Filter Policy

Menu Path: Firewall > Advanced Protection > Protocol Filter Policy

This page lets you manage your application firewall's protocol filtering policies, which allow you to inspect industrial protocol packets. This allows you to control protocol traffic based on the configured protocol filter policies and Anomaly Detection and Protection (ADP) settings.

Refer to ADP for more information.

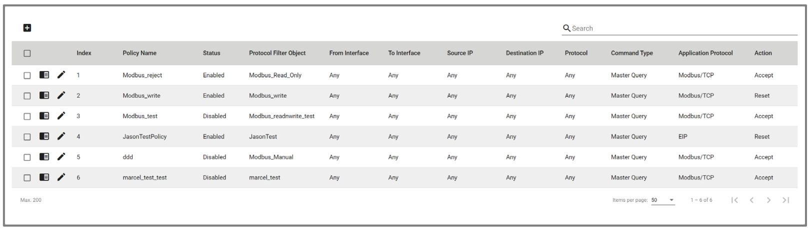
Note

Before creating protocol filter policies, you will need to set up protocol filter objects to define what application protocols your policies will apply to.

Refer to Firewall > Configuration - Protocol Filter Object for more information.

Limitations

You can create up to 200 protocol filter policies.



□		Index	Policy Name	Status	Protocol Filter Object	From Interface	To Interface	Source IP	Destination IP	Protocol	Command Type	Application Protocol	Action
□		1	Modbus_reject	Enabled	Modbus_Read_Only	Any	Any	Any	Any	Any	Master Query	Modbus/TCP	Accept
□		2	Modbus_write	Enabled	Modbus_write	Any	Any	Any	Any	Any	Master Query	Modbus/TCP	Reset
□		3	Modbus_test	Disabled	Modbus_readnwrite_test	Any	Any	Any	Any	Any	Master Query	Modbus/TCP	Accept
□		4	JasonTestPolicy	Enabled	JasonTest	Any	Any	Any	Any	Any	Master Query	EIP	Reset
□		5	ddd	Disabled	Modbus_Manual	Any	Any	Any	Any	Any	Master Query	Modbus/TCP	Accept
□		6	marcel_test_test	Disabled	marcel_test	Any	Any	Any	Any	Any	Master Query	Modbus/TCP	Accept

Max. 200

Items per page: 50

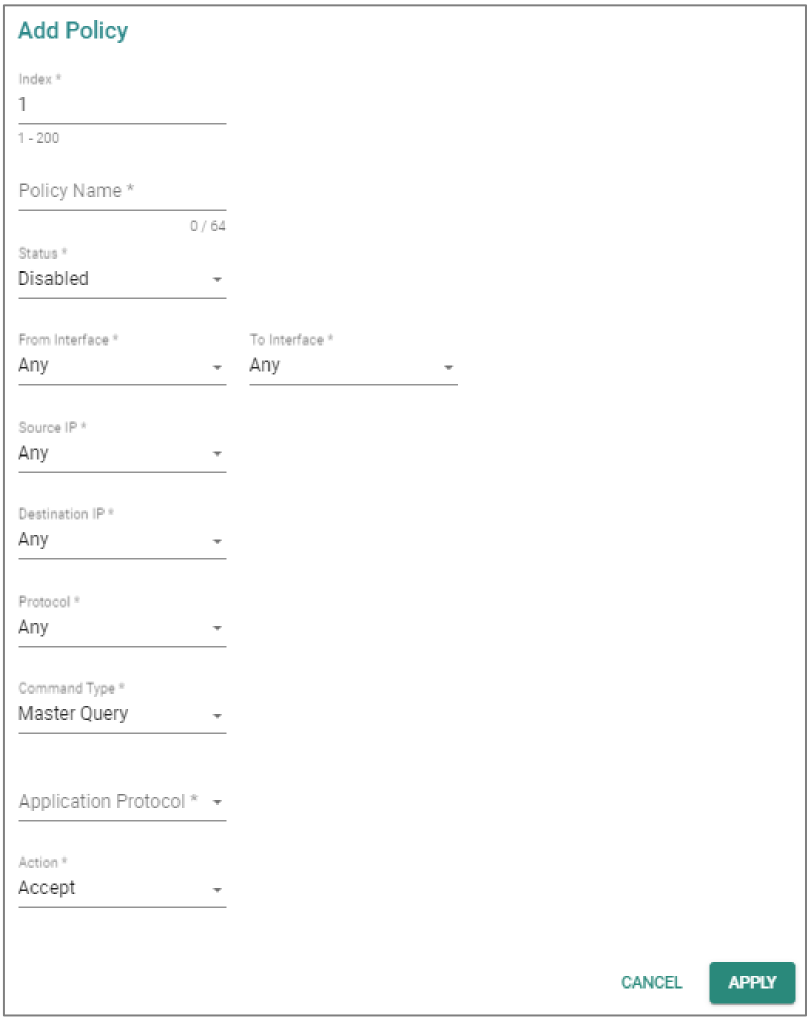
1 – 6 of 6

UI Setting	Description
Index	Shows the index of the policy.
Policy Name	Shows the name of the policy.
Status	Shows whether the policy is enabled or disabled.
Protocol Filter Object	Shows the protocol filter object used for the policy.
From Interface	Shows the From Interface for the policy.
To Interface	Shows the To Interface for the policy.
Source IP	Shows the source IP addresses for the policy.
Destination IP	Shows the destination IP addresses for the policy.
Protocol	Shows the protocols for the policy.
Command Type	Shows the packet transmission direction for this policy.
Application Protocol	Shows the industrial protocol for this policy.
Action	Shows the action the firewall will take for packets that match the policy.

Add Policy

Menu Path: Firewall > Advanced Protection > Protocol Filter Policy

Clicking the **Add (** ⊞ **)** icon on the **Firewall > Advanced Protection > Protocol Filter Policy** page will open this dialog box. This dialog lets you create a new protocol filter policy. Click **APPLY** to save your changes and add the new policy.



Add Policy

Index * 1 (1 - 200)

Policy Name * (0 / 64)

Status * Disabled

From Interface * Any

To Interface * Any

Source IP * Any

Destination IP * Any

Protocol * Any

Command Type * Master Query

Application Protocol *

Action * Accept

UI Setting	Description	Valid Range	Default Value
Index	Specify the index of the policy.	1-200	1
Policy Name	Specify a name for the policy.	1 to 64 characters	N/A
Status	Enable or disable the policy.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
From Interface	Select the From Interface for the policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Configuration > Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down of interfaces	Any
To Interface	Select the To Interface for the policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Configuration > Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down of interfaces	Any
Source IP	Select how the policy will check the packet's source IP address. **Any:** The policy will check all source IP addresses in the packet. **Single**: The policy will only check for the specified source IP address in the packet. **Range**: The policy will check all source IP addresses in the packet within the specified IP range. **Subnet:** The policy will check for source IP addresses in the packet that are within the specified subnet mask.	Any / Single / Range / Subnet	Any
Destination IP	To decide how the policy will check the packet's destination IP address. **Any:** The policy will check all destination IP addresses in the packet. **Single**: The policy will only check for the specified destination IP address in the packet. **Range**: The policy will check all destination IP addresses in the packet within the specified IP range. **Subnet:** The policy will check for destination IP addresses in the packet that are within the specified subnet mask.	Any / Single / Range / Subne	Any
Protocol	Select the protocol for this policy.	Any / TCP / UDP	Any
Command Type	Select the packet transmission direction for this policy.	Master Query / Slave Response	Master Query

UI Setting	Description	Valid Range	Default Value
Application Protocol	Select the protocol filter object to use to define the application protocol for this policy. Refer to Firewall > Advanced Protection > Configuration - Protocol Filter Object for more information.	Custom object	N/A
Action	Select the action to take for packets that match the policy. **Accept**: The firewall will accept packets that match the policy. **Monitor**: The firewall will monitor packets that match the policy. **Reset**: The firewall will drop packets that match the policy, and the session will be disconnected.	Accept / Monitor / Reset	Accept

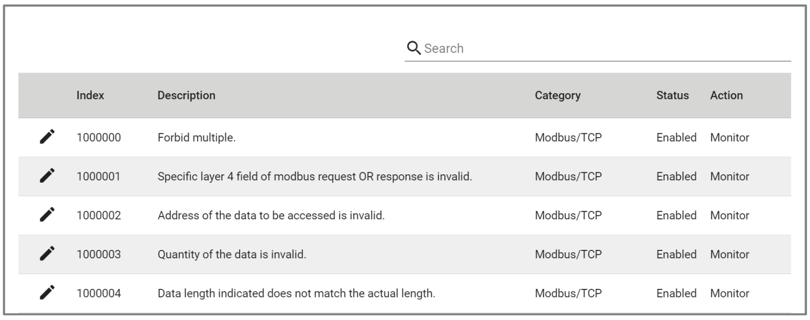
ADP

Menu Path: Firewall > Advanced Protection > ADP

This page lets you configure your device's Anomaly Detection and Protection (ADP) parameters.

Note

Availability of this feature may vary depending on your product model and version.



	Index	Description	Category	Status	Action
✎	1000000	Forbid multiple.	Modbus/TCP	Enabled	Monitor
✎	1000001	Specific layer 4 field of modbus request OR response is invalid.	Modbus/TCP	Enabled	Monitor
✎	1000002	Address of the data to be accessed is invalid.	Modbus/TCP	Enabled	Monitor
✎	1000003	Quantity of the data is invalid.	Modbus/TCP	Enabled	Monitor
✎	1000004	Data length indicated does not match the actual length.	Modbus/TCP	Enabled	Monitor

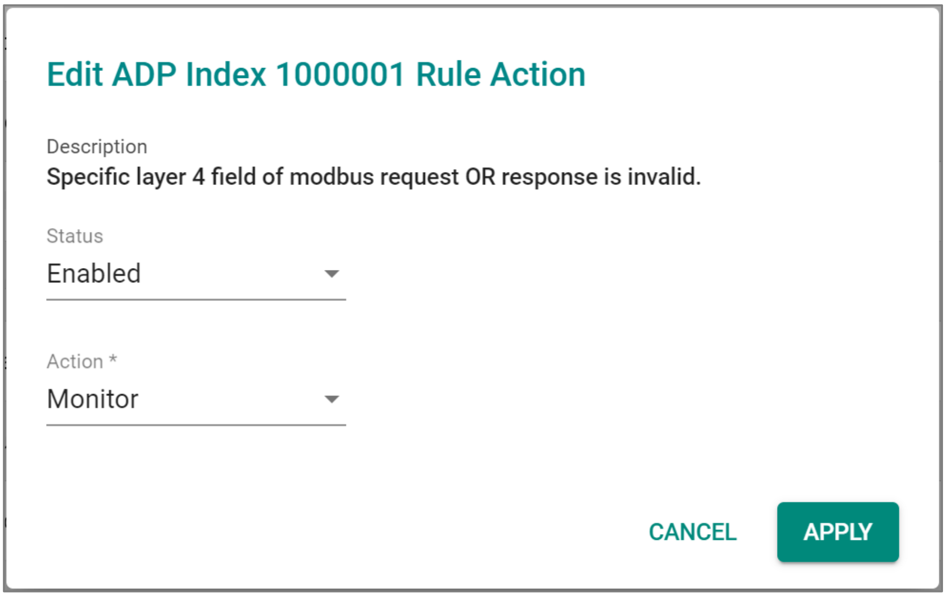
UI Setting	Description
Index	Shows the index of the ADP rule.
Description	Shows a description of the condition that will trigger the ADP rule.

UI Setting	Description
Category	Shows the category of the ADP rule.
Status	Shows whether the ADP rule is enabled or disabled.
Action	Shows the action the application firewall will take when the ADP rule is matched.

Edit ADP Rule Action

Menu Path: Firewall > Advanced Protection > ADP

Clicking the **Edit (✎)** icon for a rule on the **Insert > Path Here** page will open this dialog box. This dialog lets you modify an ADP rule. Click **APPLY** to save your changes.



Edit ADP Index 1000001 Rule Action

Description
Specific layer 4 field of modbus request OR response is invalid.

Status
Enabled

Action *
Monitor

UI Setting	Description	Valid Range	Default Value
Description (View-only)	Shows a description of the condition that will trigger the ADP rule.	N/A	N/A
Status	Enable or disable the ADP rule.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Action	Select the action to take for packets that match the rule. **Accept**: The firewall will accept packets that match the rule. **Monitor**: The firewall will monitor packets that match the rule and an event log will be recorded in Event Log - Firewall Log. **Reset**: The firewall will drop packets that match the rule, and the session will be disconnected.	Accept / Monitor / Reset	Monitor

IPS

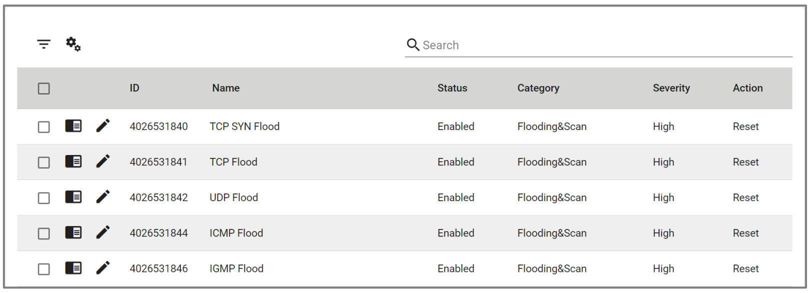
Menu Path: Firewall > Advanced Protection > IPS

This page lets you configure the Intrusion Prevention System (IPS) feature, which helps protect against cyberthreats by performing pattern-based detection and blocking known attacks.

Note

Availability of this feature may vary depending on your product model and version.

A separate IPS license is required to enable IPS functionality on the device.



□			ID	Name	Status	Category	Severity	Action
□			4026531840	TCP SYN Flood	Enabled	Flooding&Scan	High	Reset
□			4026531841	TCP Flood	Enabled	Flooding&Scan	High	Reset
□			4026531842	UDP Flood	Enabled	Flooding&Scan	High	Reset
□			4026531844	ICMP Flood	Enabled	Flooding&Scan	High	Reset
□			4026531846	IGMP Flood	Enabled	Flooding&Scan	High	Reset

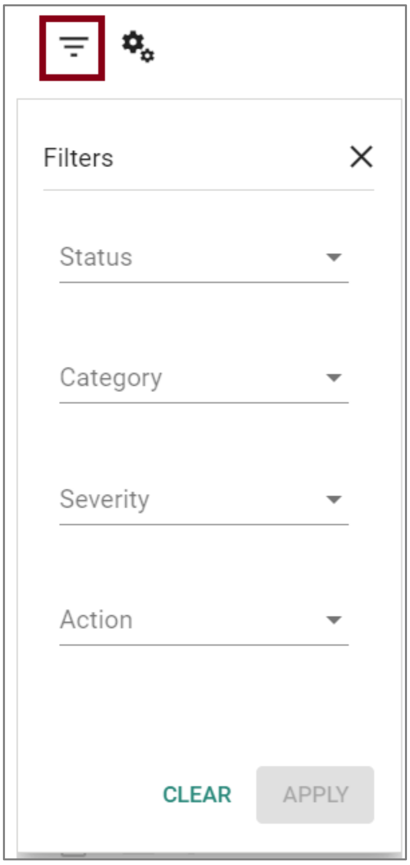
UI Setting	Description
ID	Shows the ID of the rule.
Name	Shows the name of the rule.
Status	Shows whether the rule is enabled or disabled.

UI Setting	Description
Category	Shows the category of the rule.
Severity	Shows the severity assigned to the rule.
Action	Shows the action that will be taken when the rule is triggered.

Filter IPS Rules

Menu Path: Firewall > Advanced Protection > IPS

Clicking the **Filter (** ☰ **)** icon on the **Firewall > Advanced Protection > IPS** page will open this dialog box. This dialog lets you filter the IPS Rule List according to various criteria. Click **APPLY** to apply the filter, or click **CLEAR** to reset all filter criteria.

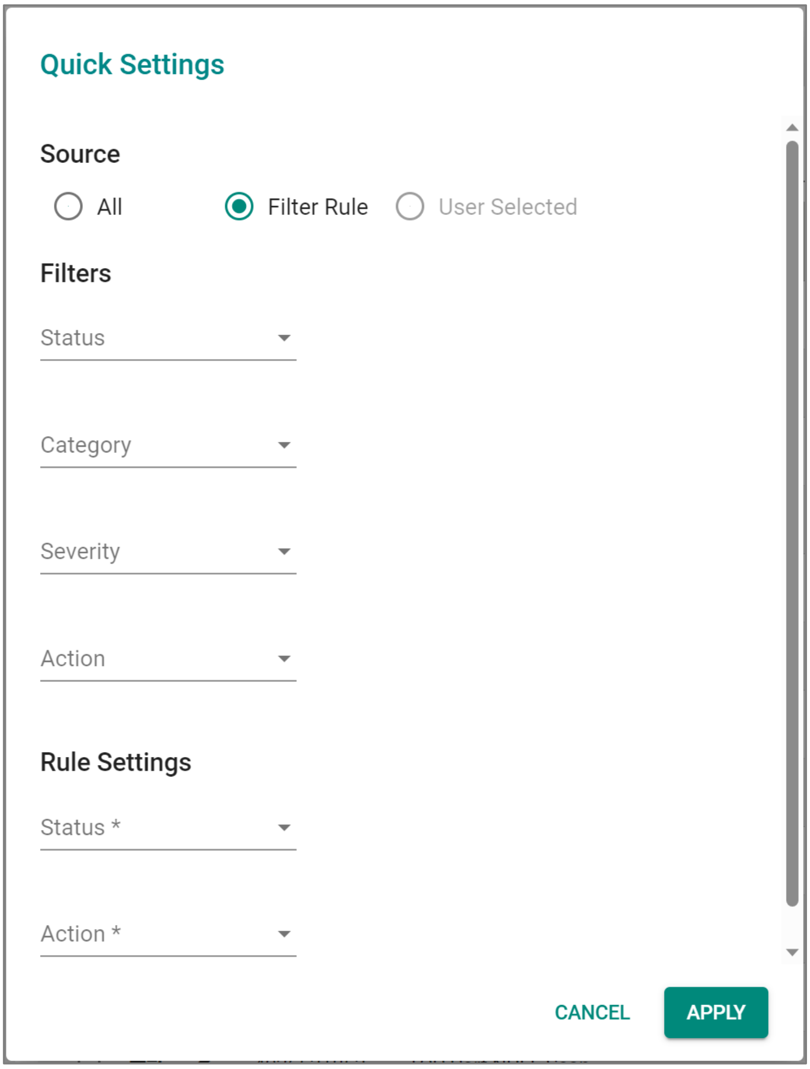


UI Setting	Description	Valid Range	Default Value
Status	Filter for enabled or disabled rules.	Enabled / Disabled	N/A
Category	Filter for a specific rule category.	File vulnerabilities / Buffer Overflow / DoS attacks / Exploits / Malware traffic / Reconnaissance / Web threats / Flooding & Scan / Protocol Attack Protection / IP Spoofing	N/A
Severity	Filter for a specific severity level.	Information / Low / Medium / High / Critical	N/A
Action	Filter for a specific rule action.	Accept / Monitor / Reset	N/A

Quick Settings

Menu Path: Firewall > Advanced Protection > IPS

Clicking the **Settings (⚙)** icon on the **Firewall > Advanced Protection > IPS** page will open this dialog box. This dialog lets you quickly configure many rules at the same time. Click **APPLY** to save your changes.



Quick Settings

Source

○ All ● Filter Rule ○ User Selected

Filters

Status

Category

Severity

Action

Rule Settings

Status *

Action *

Source

UI Setting	Description	Valid Range	Default Value
Source	Select which rules to modify with the **Rule Settings** you specify. **All**: Modify all rules. This option will not be available if you selected rules in the IPS Rule List before opening this dialog. **Filter Rule**: Only modify rules that match the filter criteria you specify. This option will not be available if you selected rules in the IPS Rule List before opening this dialog. **User Selected**: Only modify the rules that you have selected using their checkboxes. This option is only available if you select rules in the IPS Rule List before opening this dialog.	All / Filter Rule / User Selected	All

Filters

(if **Source** is **Filter Rule**)

UI Setting	Description	Valid Range	Default Value
Status	Filter for enabled or disabled rules.	Enabled / Disabled	N/A
Category	Filter for a specific rule category.	File vulnerabilities / Buffer Overflow / DoS attacks / Exploits / Malware traffic / Reconnaissance / Web threats / Flooding & Scan / Protocol Attack Protection / IP Spoofing	N/A
Severity	Filter for a specific severity level.	Information / Low / Medium / High / Critical	N/A
Action	Filter for a specific rule action.	Accept / Monitor / Reset	N/A

Rule Settings

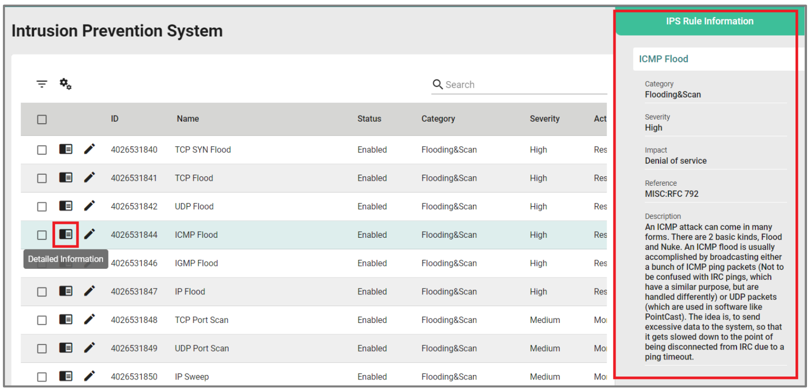
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the IPS rule.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Action	Select the action to take for packets that match the rule. **Accept**: The firewall will accept packets that match the rule. **Monitor**: The firewall will monitor packets that match the rule. **Reset**: The firewall will drop packets that match the rule, and the session will be disconnected.	Accept / Monitor / Reset	Monitor

Detailed Information

Menu Path: Firewall > Advanced Protection > IPS

Clicking the **Detailed Information ( )** icon for a rule on the **Firewall > Advanced Protection > IPS** page will toggle display of a panel with detailed information about the rule.



Intrusion Prevention System

Search

□	ID	Name	Status	Category	Severity	Act
□	4026531840	TCP SYN Flood	Enabled	Flooding&Scan	High	Res
□	4026531841	TCP Flood	Enabled	Flooding&Scan	High	Res
□	4026531842	UDP Flood	Enabled	Flooding&Scan	High	Res
□	4026531844	ICMP Flood	Enabled	Flooding&Scan	High	Res
	4026531846	IGMP Flood	Enabled	Flooding&Scan	High	Res
□	4026531847	IP Flood	Enabled	Flooding&Scan	High	Res
□	4026531848	TCP Port Scan	Enabled	Flooding&Scan	Medium	Mo
□	4026531849	UDP Port Scan	Enabled	Flooding&Scan	Medium	Mo
□	4026531850	IP Sweep	Enabled	Flooding&Scan	Medium	Mo

IPS Rule Information

ICMP Flood

Category
Flooding&Scan

Severity
High

Impact
Denial of service

Reference
MISC:RFC 792

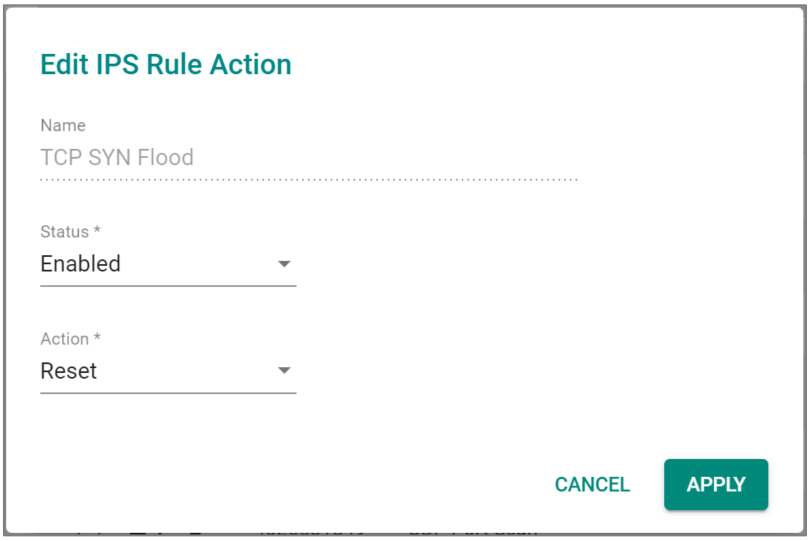
Description
An ICMP attack can come in many forms. There are 2 basic kinds, Flood and Nuke. An ICMP flood is usually accomplished by broadcasting either a bunch of ICMP ping packets (Not to be confused with IRC pings, which have a similar purpose, but are handled differently) or UDP packets (which are used in software like PointCast). The idea is, to send excessive data to the system, so that it gets slowed down to the point of being disconnected from IRC due to a ping timeout.

Edit IPS Rule Action

Menu Path: Firewall > Advanced Protection > IPS

Clicking the **Edit ( )** icon for an ITEM on the **Firewall > Advanced Protection > IPS** page will open this dialog box. This dialog lets you modify an IPS rule.

Click **APPLY** to save your changes.



Edit IPS Rule Action

Name: TCP SYN Flood

Status *: Enabled

Action *: Reset

UI Setting	Description	Valid Range	Default Value
Name (View-only)	Shows the name of the IPS rule.	N/A	N/A
Status	Enable or disable the IPS rule.	Enabled / Disabled	Enabled
Action	Select the action to take for packets that match the rule. **Accept**: The firewall will accept packets that match the rule. **Monitor**: The firewall will monitor packets that match the rule. **Reset**: The firewall will drop packets that match the rule, and the session will be disconnected.	Accept / Monitor / Reset	Monitor

VPN

Menu Path: Main > VPN

The VPN settings area lets you configure settings related to your device's VPN functionality.

This settings area includes these sections:

- IPSec
- L2TP Server

VPN - User Privileges

Privileges to VPN 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
IPsec	R/W	R/W	R
L2TP Server	R/W	R/W	R

IPSec

Menu Path: VPN > IPSec

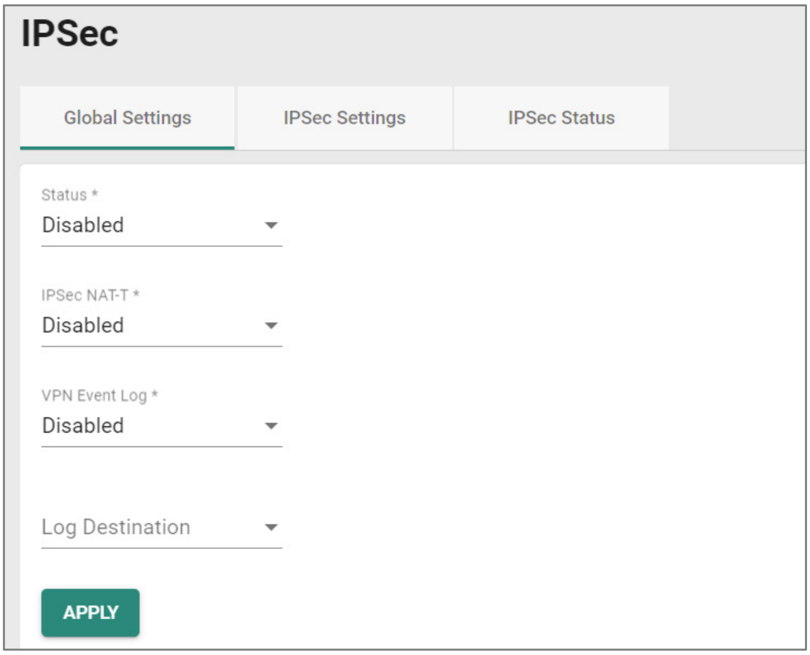
This page lets you set up IPSec VPN tunnels for your device.

This page includes these tabs:

- Global Settings
- IPSec Settings
- IPSec Status

Global Settings

Menu Path: VPN > IPSec - Global Settings This page lets you configure global settings that affect all IPsec tunnels.



IPSec

Status *
Disabled

IPSec NAT-T *
Disabled

VPN Event Log *
Disabled

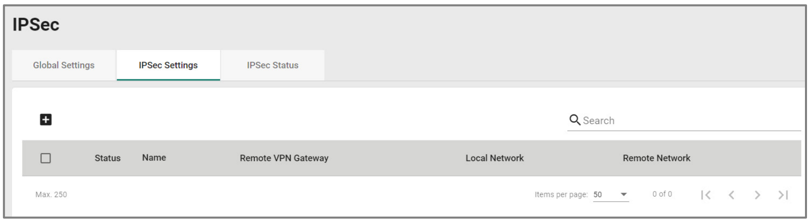
Log Destination

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable all IPSec VPN services.	Enabled / Disabled	Disabled
IPSec NAT-T	Enable or disable IPSec NAT-T (NAT-Traversal). This option should be enabled if there is an external industrial secure router located between VPN tunnels.	Enabled / Disabled	Disabled
VPN Event Log	Enable or disable VPN event logging. Refer to Diagnostics > Event Logs and Notifications > Event Log for more information.	Enabled / Disabled	Disabled
Log Destination	If **VPN Event Log** is enabled, select the VPN event log storage location.	Local Storage / Syslog / Trap	N/A

IPSec Settings

Menu Path: VPN > IPSec - IPSec Settings

This page lets you create and edit IPSec VPN tunnels for your device.



UI Setting	Description
Status	Shows whether the tunnel is enabled or disabled.
Name	Shows the name of the tunnel.
Remote VPN Gateway	Shows the IP address of the remote VPN gateway for the tunnel.
Local Network	Shows the tunnel's local network IP address.
Remote Network	Shows the tunnel's remote network IP address.

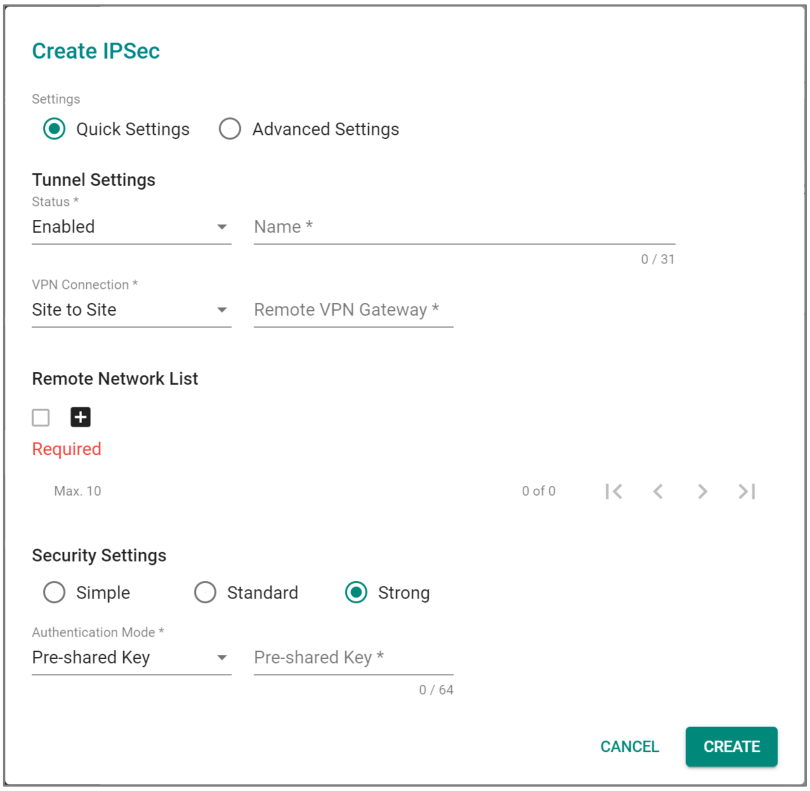
Create IPSec

Menu Path: VPN > IPSec - IPSec Settings

Clicking the **Add (** ⊞ **)** icon on the **VPN > IPSec - IPSec Settings** page will open this dialog box. This dialog lets you create a new IPSec VPN tunnel. Click **CREATE** to save your changes and add the new tunnel.

Create IPSec - Quick Settings

If **Quick Settings** is selected, these settings will appear.



Create IPSec

Settings

● Quick Settings ○ Advanced Settings

Tunnel Settings

Status *: Enabled

Name *: 0 / 31

VPN Connection *: Site to Site

Remote VPN Gateway *

Remote Network List

□ +

Required

Max. 10 0 of 0

Security Settings

○ Simple ○ Standard ● Strong

Authentication Mode *: Pre-shared Key

Pre-shared Key *: 0 / 64

Tunnel Settings

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the tunnel.	Enabled / Disabled	Enabled
Name	Enter a name for this tunnel. **Note** Names must start with a character that is not a number.	Max. 31 characters	N/A
VPN Connection	Select the type of VPN connection to use for this rule. **Site to Site**: The VPN tunnel for the Local and Remote subnets is fixed. **Site to Site(Any)**: The VPN tunnel for the Remote subnet area is dynamic and is fixed for the Local subnet.	Site to Site / Site to Site(Any)	Site to Site

UI Setting	Description	Valid Range	Default Value
Remote VPN Gateway	Specify the IP address of the remote VPN gateway. If **VPN Connection** is set to **Site to Site(Any)**, this does not need to be set.	Valid IP address	N/A

Remote Network List

You can configure multiple remote networks for the tunnel. Click the add icon (⊞) to add a new entry. Select an entry and click the delete icon (🗑) to delete it.

Limitations

You can add up to 10 remote networks for an IPSec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
Remote Network	Specify the IP address and subnet mask of the remote VPN network.	Valid IP address	N/A
Netmask	Select a netmask to use for the remote network.	Drop-down list of netmasks	24 (255.255.255.0)

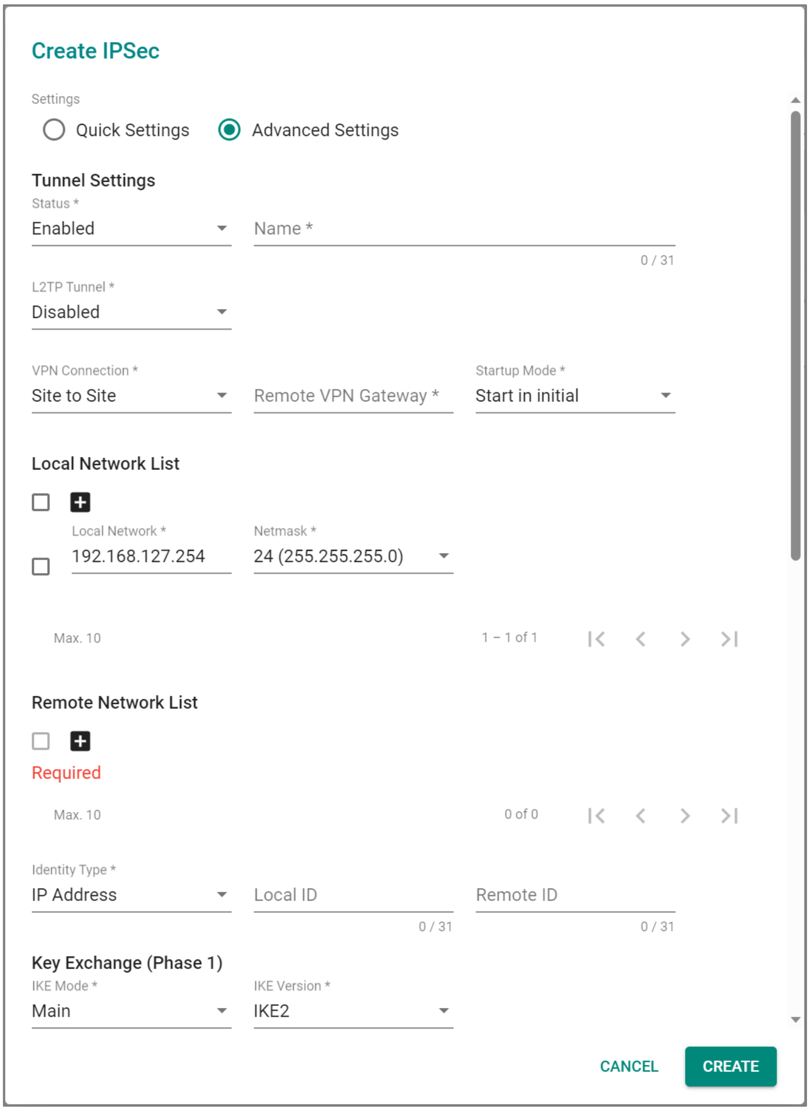
Security Settings

UI Setting	Description	Valid Range	Default Value
Security Strength	Select the security strength for the tunnel. Different settings will change the **Encryption Algorithm** and **Hash Algorithm** used, which can be viewed in **Advanced Settings**. **Simple**: Uses **DES** for the **Encryption Algorithm** and **MD5** for the **Hash Algorithm**. **Standard**: Uses **3DES** for the **Encryption Algorithm** and **SHA-1** for the **Hash Algorithm**. **Strong**: Uses **AES-256** for the **Encryption Algorithm** and **SHA-256** for the **Hash Algorithm**.	Simple / Standard / Strong	Strong

UI Setting	Description	Valid Range	Default Value
Authentication Mode	Select the authentication mode to use for the tunnel. **Note** You must have certificates already imported to select **X.509** or **X.509 With CA**. Refer to Certificate Management for more information. **Pre-Shared Key**: Pre-Shared Key is a user-defined authentication string used by two systems to establish an IPsec VPN connection. **X.509**: The local and remote systems will authenticate the VPN connection using certificates imported in advance by the user on the **Certificate Management > Local Certificate** page. **X.509 With CA**: The local and remote systems will authenticate the VPN connection using both certificates imported in advance by the user on the **Certificate Management > Local Certificate** page and a CA certificate imported on the **Certificate Management > Trusted CA Certificate** page.	Pre-Shared Key / X.509 / X.509 With CA	Pre-Shared Key
Pre-Shared Key	Specify a pre-shared key to use to authenticate the IPSec VPN connection.	0 to 64 characters	N/A

Create IPSec - Advanced Settings

If **Advanced Settings** is selected, these settings will appear.



Create IPSec

Settings

○ Quick Settings ● Advanced Settings

Tunnel Settings

Status * Enabled

Name * 0 / 31

L2TP Tunnel * Disabled

VPN Connection * Site to Site

Remote VPN Gateway *

Startup Mode * Start in initial

Local Network List

Local Network * 192.168.127.254

Netmask * 24 (255.255.255.0)

Max. 10 1 – 1 of 1

Remote Network List

Required

Max. 10 0 of 0

Identity Type * IP Address

Local ID 0 / 31

Remote ID 0 / 31

Key Exchange (Phase 1)

IKE Mode * Main

IKE Version * IKE2

Tunnel Settings

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the tunnel.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Name	Enter a name for this tunnel. ✎ **Note** Names must start with a character that is not a number.	Max. 31 characters	N/A
L2TP Tunnel	Enable or disable L2TP over IPSec.	Enabled / Disabled	Disabled
VPN Connection	Select the type of VPN connection to use for this rule. **Site to Site**: The VPN tunnel for the Local and Remote subnets is fixed. **Site to Site(Any)**: The VPN tunnel for the Remote subnet area is dynamic and is fixed for the Local subnet.	Site to Site / Site to Site(Any)	Site to Site
Remote VPN Gateway	Specify the IP address of the remote VPN gateway. If **VPN Connection** is set to **Site to Site(Any)**, this does not need to be set.	Valid IP address	N/A
Startup Mode	Select a startup mode for the tunnel. **Start in Initial:** The VPN tunnel will actively initiate the connection with the remote VPN gateway. **Wait for Connecting**: The VPN tunnel will wait for the remote VPN gateway to initiate the connection. ✎ **Note** The maximum number of starts for the initial VPN tunnel is 30. The maximum number of waits for connecting to a VPN tunnel is 100. These cannot be changed.	Start in Initial / Wait for Connecting	Start in Initial

Local Network List

You can configure multiple local networks for the tunnel. Click the add icon (⊞) to add a new entry. Select an entry and click the delete icon (🗑) to delete it.

Limitations

You can add up to 10 local networks for an IPSec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
Local Network	Specify the IP address and subnet mask of the local VPN network.	Valid IP address	N/A
Netmask	Select a netmask to use for the local network.	Drop-down list of netmasks	24 (255.255.255.0)

Remote Network List

You can configure multiple remote networks for the tunnel. Click the add icon (⊞) to add a new entry. Select an entry and click the delete icon (🗑) to delete it.

Limitations

You can add up to 10 remote networks for an IPSec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
Remote Network	Specify the IP address and subnet mask of the remote VPN network.	Valid IP address	N/A
Netmask	Select a netmask to use for the remote network.	Drop-down list of netmasks	24 (255.255.255.0)

Identity

UI Setting	Description	Valid Range	Default Value
Identity Type	Select an ID type to use to identify VPN tunnel connections. **IP Address**: Use an IP address. **FQDN**: Use a Fully Qualified Domain Name (FQDN). **Key ID**: Use a user-defined key ID string. **Auto(with Cisco)**: Use this when establishing connections to Cisco systems.	IP Address / FQDN / Key ID / Auto(with Cisco)	IP Address

UI Setting	Description	Valid Range	Default Value
Local ID **(If Identity Type is IP Address, FQDN, or Key ID)**	Specify the local ID for identifying the VPN tunnel connection. The Local ID must be identical to the Remote ID of the connected VPN gateway in order to successfully establish the VPN tunnel connection.	1 to 31 characters	N/A
Remote ID **(If Identity Type is IP Address, FQDN, or Key ID)**	Specify the remote ID for identifying the VPN tunnel connection. The Remote ID must be identical to the Local ID of the connected VPN gateway in order to successfully establish the VPN tunnel connection.	1 to 31 characters	N/A

Key Exchange (Phase 1)

UI Setting	Description	Valid Range	Default Value
IKE Mode	Select the IKE mode to use for authentication. **Main**: Both the remote and local VPN gateway will negotiate which encryption/hash algorithm and DH groups can be used for this VPN tunnel. Both VPN gateways must use the same algorithm to communicate. **Aggressive**: The remote and local VPN gateways will not negotiate the algorithm and will only use the user-defined configuration.	Main / Aggressive	Main
IKE Version	Select which version of IKE to use. **IKE1**: Use IKE Version 1 protocol. **IKE2**: Use IKE Version 2 protocol.	IKE1 / IKE2	IKE2

UI Setting	Description	Valid Range	Default Value
Authentication Mode	Select the authentication mode to use for the tunnel. **Note** You must have certificates already imported to select **X.509** or **X.509 With CA**. Refer to Certificate Management for more information. **Pre-Shared Key**: Pre-Shared Key is a user-defined authentication string used by two systems to establish an IPsec VPN connection. **X.509**: The local and remote systems will authenticate the VPN connection using certificates imported in advance by the user on the **Certificate Management > Local Certificate** page. **X.509 With CA**: The local and remote systems will authenticate the VPN connection using both certificates imported in advance by the user on the **Certificate Management > Local Certificate** page and a CA certificate imported on the **Certificate Management > Trusted CA Certificate** page.	Pre-Shared Key / X.509 / X.509 With CA	Pre-Shared Key
Pre-Shared Key	Specify a pre-shared key to use to authenticate the IPSec VPN connection.	0 to 64 characters	
Encryption Algorithm	Select the encryption algorithm to use for key exchange.	DES / 3DES / AES-128 / AES-192 / AES-256	AES-256
Hash Algorithm	Select the hash algorithm to use for key exchange.	MD5 / SHA-1 / SHA-256	SHA-256
DH Group	Select the Diffie-Hellman group. This is the key exchange group between the remote and VPN gateways.	DH 1(modp768) / DH 2(modp1024) / DH 5(modp1536) / DH 14(modp2048)	DH 14(modp2048)
IKE Lifetime	Specify the lifetime (in minutes) for IKE SA.	30 to 43200	43200

Data Exchange (Phase 2)

UI Setting	Description	Valid Range	Default Value
Encryption Algorithm	Select the encryption algorithm to use for data exchange.	DES / 3DES / AES-128 / AES-192 / AES-256	AES-256

UI Setting	Description	Valid Range	Default Value
Hash Algorithm	Select the hash algorithm to use for data exchange.	MD5 / SHA-1 / SHA-256	SHA-256
Perfect Forward Secrecy	Enable or disable Perfect Forward Secrecy. When enabled, different security keys are used for different IPsec phases in order to enhance security.	Enabled / Disabled	Disabled
DH Group	Select the Diffie-Hellman group. This is the Key Exchange group between the remote and VPN gateways.	DH 1 (modp768), DH 2 (modp1024), DH 5 (modp1536), DH 14 (modp2048)	DH 14 (modp2048)
SA Lifetime	Specify the lifetime (in minutes) for Phase 2 IKE SA.	30 to 43200	43200

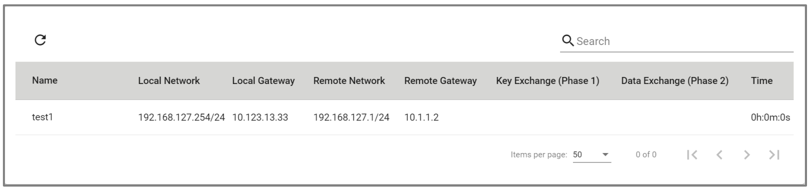
Dead Peer Detection

UI Setting	Description	Valid Range	Default Value
Action	Specify the action the system should take when a dead peer is detected. **Hold**: Maintain the VPN tunnel. **Restart**: Reconnect the VPN tunnel. **Clear**: Clear the VPN tunnel. **Disabled**: Disable Dead Peer Detection.	Hold / Restart / Clear / Disabled	Restart
Retry Interval	Specify the interval (in seconds) at which Dead Peer Detection messages are sent.	0 to 3600	30
Confidence Interval	Specify the interval (in seconds) at which the system will check to see if the connection is alive or not.	0 to 3600	120

IPSec Status

Menu Path: VPN > IPSec - IPSec Status

This page lets you see the status of your IPSec VPN tunnels.



Name	Local Network	Local Gateway	Remote Network	Remote Gateway	Key Exchange (Phase 1)	Data Exchange (Phase 2)	Time
test1	192.168.127.254/24	10.123.13.33	192.168.127.1/24	10.1.1.2			0h:0m:0s

UI Setting	Description
Name	Shows the name of the tunnel.
Local Network	Shows the local network address for the tunnel.
Local Gateway	Shows the local gateway address for the tunnel.
Remote Network	Shows the remote network address for the tunnel.
Remote Gateway	Shows the remote gateway address for the tunnel.
Key Exchange (Phase 1)	Shows the status of key exchange phase.
Data Exchange (Phase 2)	Shows the status of the data exchange phase.
Time	Shows how long the connection has been up.

L2TP Server

Menu Path: VPN > L2TP Server

This page lets you configure the L2TP server function of your device. L2TP is a popular choice for VPN applications with remote roaming users since an L2TP client is built into the Microsoft Windows operating system. Since L2TP does not provide any encryption, it is usually combined with IPsec to provide data encryption.

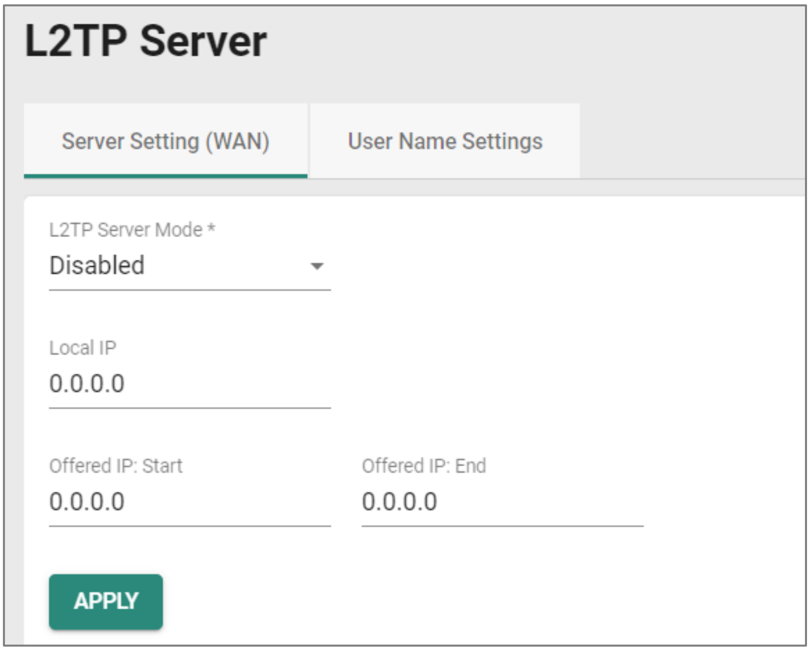
This page includes these tabs:

- Server Setting (WAN)
- User Name Settings

Server Setting (WAN)

Menu Path: VPN > L2TP Server - Server Setting (WAN)

This page lets you enable and configure the L2TP server function of your device.



L2TP Server

L2TP Server Mode *
Disabled

Local IP
0.0.0.0

Offered IP: Start
0.0.0.0

Offered IP: End
0.0.0.0

UI Setting	Description	Valid Range	Default Value
L2TP Server Mode	Enable or disable the L2TP server.	Enabled / Disabled	Disabled
Local IP	Specify the IP address of the local subnet.	Valid IP address	0.0.0.0
Offered IP: Start	Specify the starting IP address of the offered IP range used for L2TP clients.	Valid IP address	0.0.0.0
Offered IP: End	Specify the ending IP address of the offered IP range used for L2TP clients.	Valid IP address	0.0.0.0

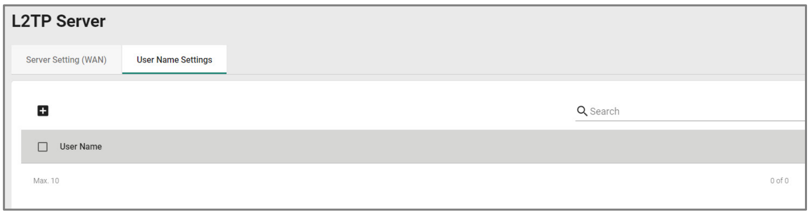
User Name Settings

Menu Path: VPN > L2TP Server - User Name Settings

This page lets you manage users that can connect to your device's L2TP server.

Limitations

You can add up to 10 users for the L2TP Server.

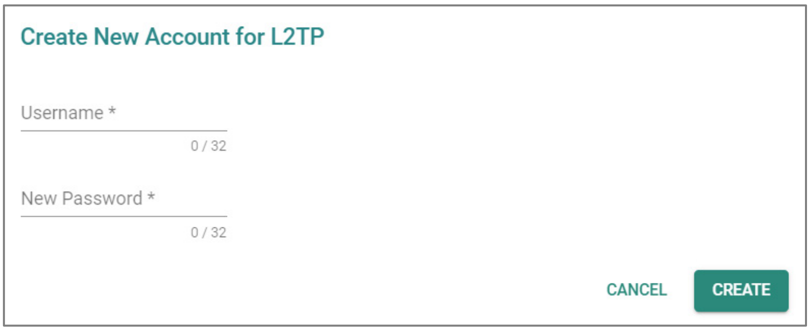


UI Setting	Description
User Name	Shows the name of the user account.

Create New Account for L2TP

Menu Path: VPN > L2TP Server - User Name Settings

Clicking the **Add (⊞)** icon on the **VPN > L2TP Server - User Name Settings** page will open this dialog box. This dialog lets you create a new user account for the device's L2TP server. Click **CREATE** to save your changes and add the new account.



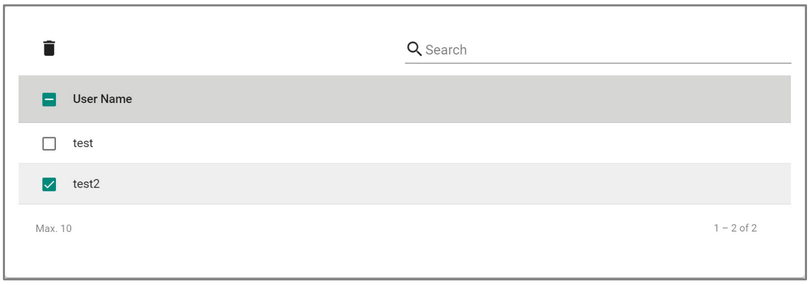
UI Setting	Description	Valid Range	Default Value
Username	Enter a username for the L2TP account.	1 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
New Password	Enter a password for the L2TP account.	1 to 32 characters	N/A

Delete Account for L2TP

Menu Path: VPN > L2TP Server - User Name Settings

You can delete an account by using the checkboxes to select the accounts you want to delete, then clicking the **Delete (🗑)** icon.



🗑 Search

⊟	User Name
□	test
☑	test2

Max. 10 1 – 2 of 2

Certificate Management

Menu Path: Certificate Management

The Certificate Management settings area lets you manage X.509 digital certificates for your device. These certificates are commonly used for IPsec, OpenVPN, and HTTPS authentication. This device can act as a root CA (Certificate Authority) and issue a trusted root certificate. Alternatively, you can import certificates from other CAs.

Certificates are a time-based form of authentication. Before processing certificates, please ensure that your device is synced with the local device. For more information about syncing device time, please refer to System > Time.

This section includes these pages:

- Local Certificate

- Trusted CA Certificate
- Certificate Signing Request

Warning

For security reasons, if the device is deployed without a CA server environment, we strongly recommend using short lifetime certificates (e.g., 24 hours) to ensure system security.

Certificate Management - User Privileges

Privileges to Certificate Management 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
Local Certificate	R/W	-	-
Trusted CA Certificate	R/W	-	-
Certificate Signing Request	R/W	-	-

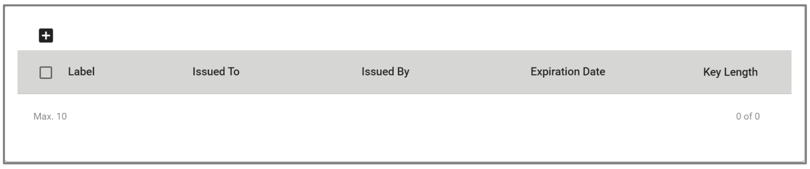
Local Certificate

Menu Path: Certificate Management > Local Certificate

This page lets you import and manage X.509 digital certificates.

Limitations

You can import up to 10 local certificates.

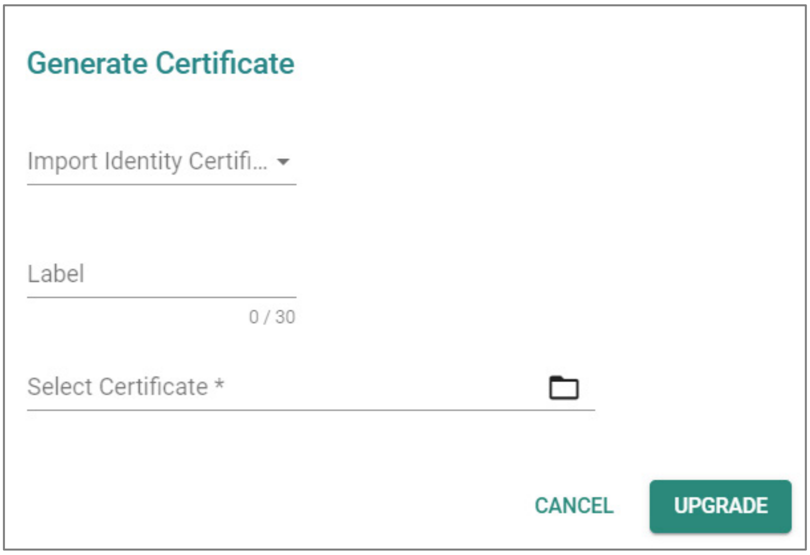


UI Setting	Description
Label	Shows the label identifying the certificate.
Issued To	Shows who the certificate was issued to.
Issued By	Shows who the certificate was issued by.
Expiration Date	Shows the expiration date of the certificate.
Key Length	Shows the key length of the certificate.

Generate Certificate

Menu Path: Certificate Management > Local Certificate

Clicking the **Add (** ⊞ **)** icon on the **Certificate Management > Local Certificate** page will open this dialog box. This dialog lets you import a certificate from your local computer. Click **UPGRADE** to save your changes and add the new certificate.



UI Setting	Description	Valid Range	Default Value
Import Identity Certificate	Select the type of certificate to import. **Certificate**: Used for certificates with a .crt file extension. **Certificate From CSR**: Used for certificates issued by another CA. **Certificate From PKCS#12**: Used for certificates with a .p12 file extension. **Note** Before importing a certificate issued by another CA, you should import its related trusted CA certificate first on the Certificate Management > Trusted CA Certificate page. Otherwise, your device may not recognize the certificate and reject the connection.	Certificate / Certificate From CSR / Certificate From PKCS#12	N/A
Label	Enter a label to help identify the certificate. If this is empty, the file name of the certificate will be used.	1 to 30 characters	N/A
CSR Common Name **(if Import Identity Certificate is Certificate From CSR)**	Select the CSR common name for the certificate. **Note** CSRs must be created in advance on the Certificate Management > Certificate Signing Request - CSR Generate page to select them here.	Drop-down list of CSR names	N/A
Import Password **(if Import Identity Certificate is Certificate From PKCS#12)**	Enter the password for the certificate.	0 to 32 characters	N/A
Select Certificate	Click this field and select the certificate file from your computer.	Select a file from your computer	N/A

Delete Certificate

Menu Path: Certificate Management > Local Certificate

You can delete certificates by using the checkboxes to select the certificates you want to delete, then clicking the **Delete (🗑)** icon.

Note

You cannot delete a certificate if it is currently in use.

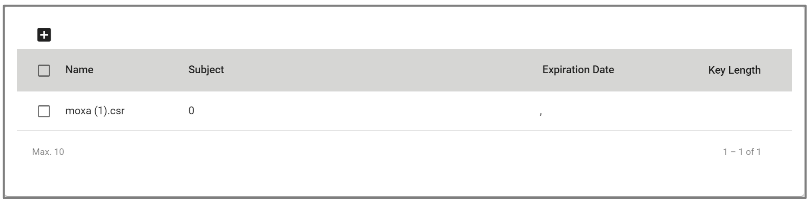
Trusted CA Certificate

Menu Path: Certificate Management > Trusted CA Certificate

This page lets you import and manage trusted CA certificates.

Limitations

You can import up to 10 trusted CA certificates.



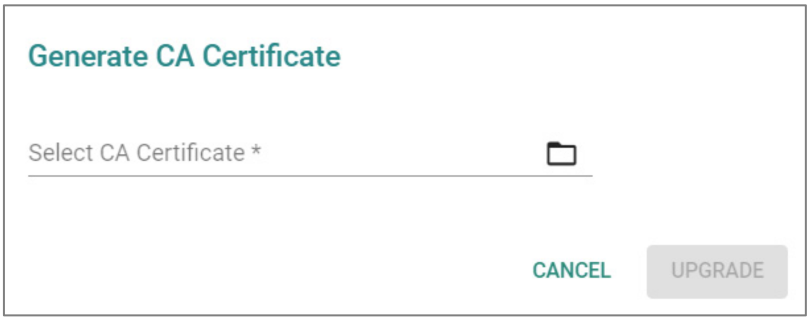
□	Name	Subject	Expiration Date	Key Length
□	moxa (1).csr	0	,	

UI Setting	Description
Name	Shows the name of the certificate file.
Subject	Shows the subject from the certificate.
Expiration Date	Shows the expiration date of the certificate.
Key Length	Shows the key length of the certificate.

Generate CA Certificate

Menu Path: Certificate Management > Trusted CA Certificate

Clicking the **Add (**⊞**)** icon on the **Certificate Management > Trusted CA Certificate** page will open this dialog box. This dialog lets you import a CA certificate from your local computer. Click **UPGRADE** to save your changes and add the new certificate.



Generate CA Certificate

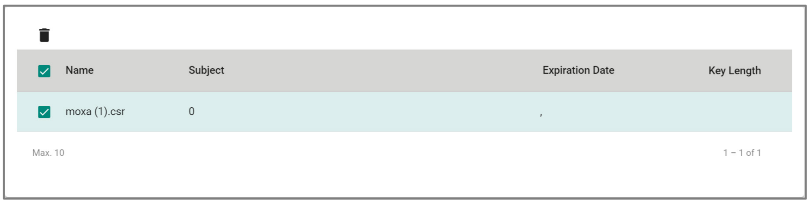
Select CA Certificate *

UI Setting	Description	Valid Range	Default Value
Select Certificate	Click this field and select the certificate file from your computer.	Select a file from your computer	N/A

Delete CA Certificate

Menu Path: Certificate Management > Trusted CA Certificate

You can delete certificates by using the checkboxes to select the certificates you want to delete, then clicking the **Delete (🗑)** icon.



☑	Name	Subject	Expiration Date	Key Length
☑	moxa (1).csr	0	,	

Certificate Signing Request

Menu Path: Certificate Management > Certificate Signing Request

This page lets you generate and manage key pairs and certificate signing requests

(CSRs). Certificate signing requests are needed to apply for and import a digital identity certificate from a CA.

To get a certificate from a CA for connection purposes, you will need to:

1. Generate a key pair
2. Generate a CSR

This page includes these tabs:

- Key Pair Generate
- CSR Generate

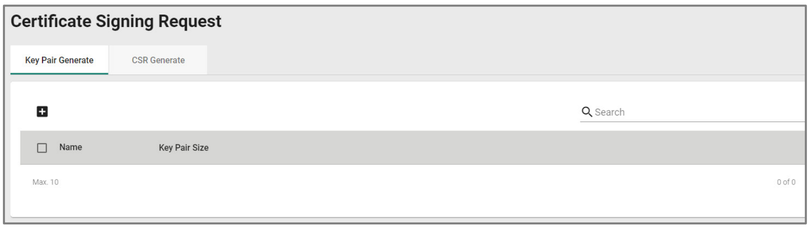
Key Pair Generate

Menu Path: Certificate Management > Certificate Signing Request - Key Pair Generate

This page lets you generate and manage key pairs, which are used to generate CSRs.

Limitations

You can generate up to 10 key pairs.

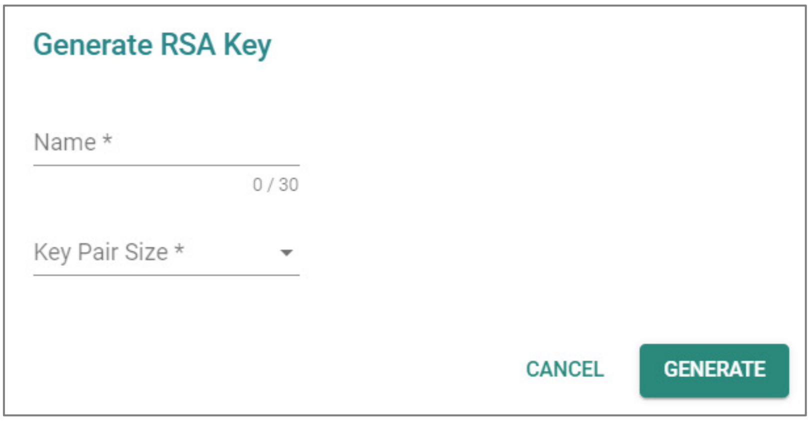


UI Setting	Description
Name	Shows the name of the RSA key.
Key Pair Size	Shows the size used for the key pair.

Generate RSA Key

Menu Path: Certificate Management > Certificate Signing Request - Key Pair Generate

Clicking the **Add (⊞) icon** on the **Certificate Management > Certificate Signing Request - Key Pair Generate** page will open this dialog box. This dialog lets you generate a new key pair to use when generating a CSR. Click **GENERATE** to save your changes and add the new key pair.


Generate RSA Key

Name *

0 / 30

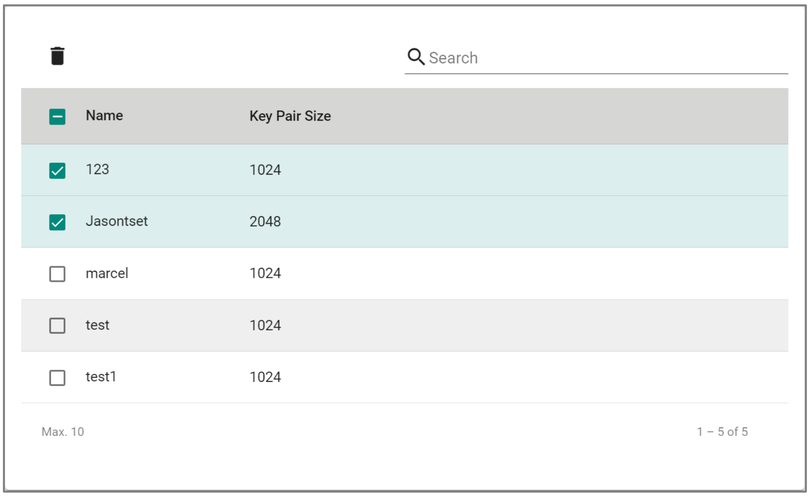
Key Pair Size *

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the RSA key.	1 to 30 characters	N/A
Key Pair Size	Select the key pair size to use.	1024 Bit / 2048 Bit	N/A

Delete RSA Key

Menu Path: Certificate Management > Certificate Signing Request - Key Pair Generate

You can delete key pairs by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.



🗑 Search

☐	Name	Key Pair Size
☑	123	1024
☑	Jasontset	2048
☐	marcel	1024
☐	test	1024
☐	test1	1024

Max. 10 1 – 5 of 5

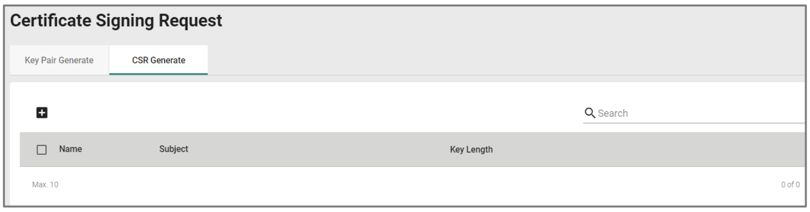
CSR Generate

Menu Path: Certificate Management > Certificate Signing Request - CSR Generate

This page lets you generate and manage CSRs.

Limitations

You can generate up to 10 CSRs.



Certificate Signing Request

☐	Name	Subject	Key Length

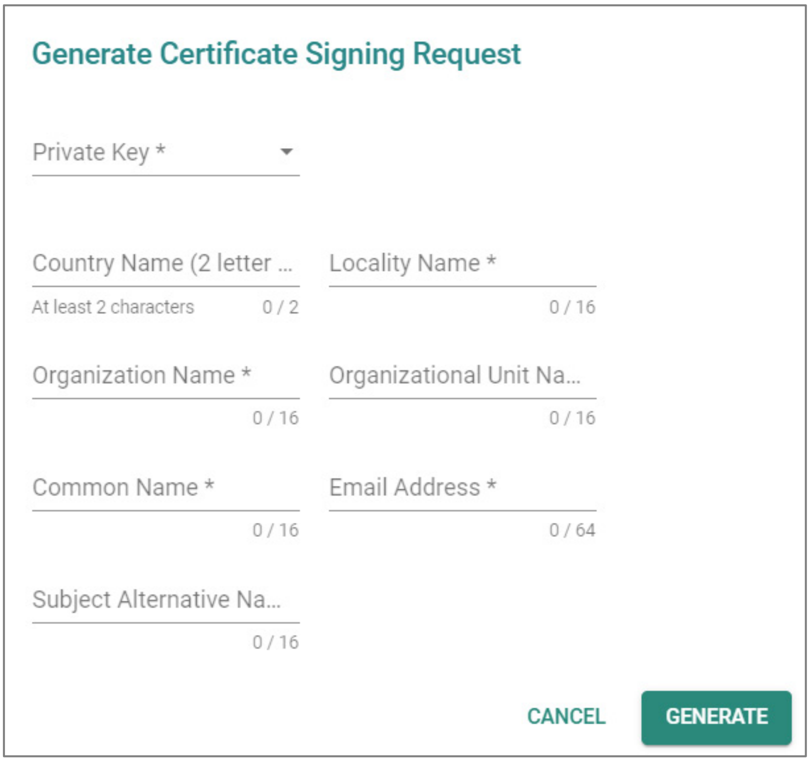
Max. 10 0 of 0

UI Setting	Description
Name	Shows the name of the CSR.
Subject	Shows the subject of the CSR.
Key Length	Shows the key length used by the CSR.

Generate Certificate Signing Request

Menu Path: Certificate Management > Certificate Signing Request - CSR Generate

Clicking the **Add (⊞)** icon on the **Certificate Management > Certificate Signing Request - CSR Generate** page will open this dialog box. This dialog lets you generate a new CSR. Click **CREATE** to save your changes and add the new CSR.



Generate Certificate Signing Request

Private Key *

Country Name (2 letter ...
At least 2 characters 0 / 2

Locality Name *
0 / 16

Organization Name *
0 / 16

Organizational Unit Na...
0 / 16

Common Name *
0 / 16

Email Address *
0 / 64

Subject Alternative Na...
0 / 16

CANCEL GENERATE

UI Setting	Description	Valid Range	Default Value
Private Key	Select the key pair to use. To generate and manage key pairs, refer to Certificate Management > Certificate Signing Request - Key Pair Generate.	Drop-down list of key pairs	N/A
Country Name (2 letter code)	Specify the 2-letter country code for the CSR.	2 characters	N/A
Locality Name	Specify the locality name for the CSR.	1 to 16 characters	N/A
Organization Name	Specify the organization name for the CSR.	1 to 16 characters	N/A
Organization Unit Name	Specify the organization unit name for the CSR.	1 to 16 characters	N/A
Common Name	Specify the common name for the CSR.	1 to 16 characters	N/A
Email Address	Specify the email address for the CSR.	1 to 64 characters	N/A
Subject Alternative Name	Specify the subject alternative name for the CSR.	1 to 16 characters	N/A

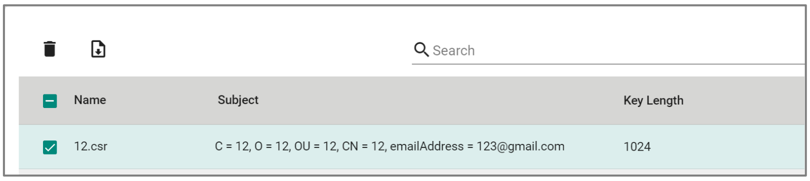
Export Certificate Signing Request

Menu Path: Certificate Management > Certificate Signing Request - CSR Generate

You can export a CSR by using the checkboxes to select the entry you want to export, then clicking the **Export (**⎘**)** icon.

Note

The export icon will only be available when a single entry is selected; it will not be available if multiple entries are selected.

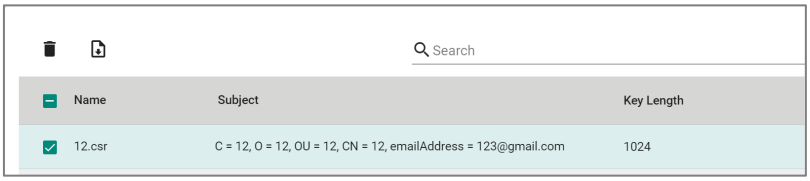


☐	Name	Subject	Key Length
☑	12.csr	C = 12, O = 12, OU = 12, CN = 12, emailAddress = 123@gmail.com	1024

Delete Certificate Signing Request

Menu Path: Certificate Management > Certificate Signing Request - CSR Generate

You can delete CSRs by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.



⊟	Name	Subject	Key Length
☑	12.csr	C = 12, O = 12, OU = 12, CN = 12, emailAddress = 123@gmail.com	1024

Security

Menu Path: Security

The Security settings area lets you configure security settings to help you secure your device and your network.

This settings area includes these sections:

- Device Security
- Network Security
- Authentication
- MXview Alert Notification

Security - User Privileges

Privileges to Security 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/W	R
SSH & SSL	R/W	R/W	-
Network Security			
IEEE 802.1X	R/W	R/W	R
RADIUS	R/W	-	-
MXview Alert Notification	R/W	R/W	R

Device Security

Menu Path: Security > Device Security

This section lets you configure security settings to protect your device.

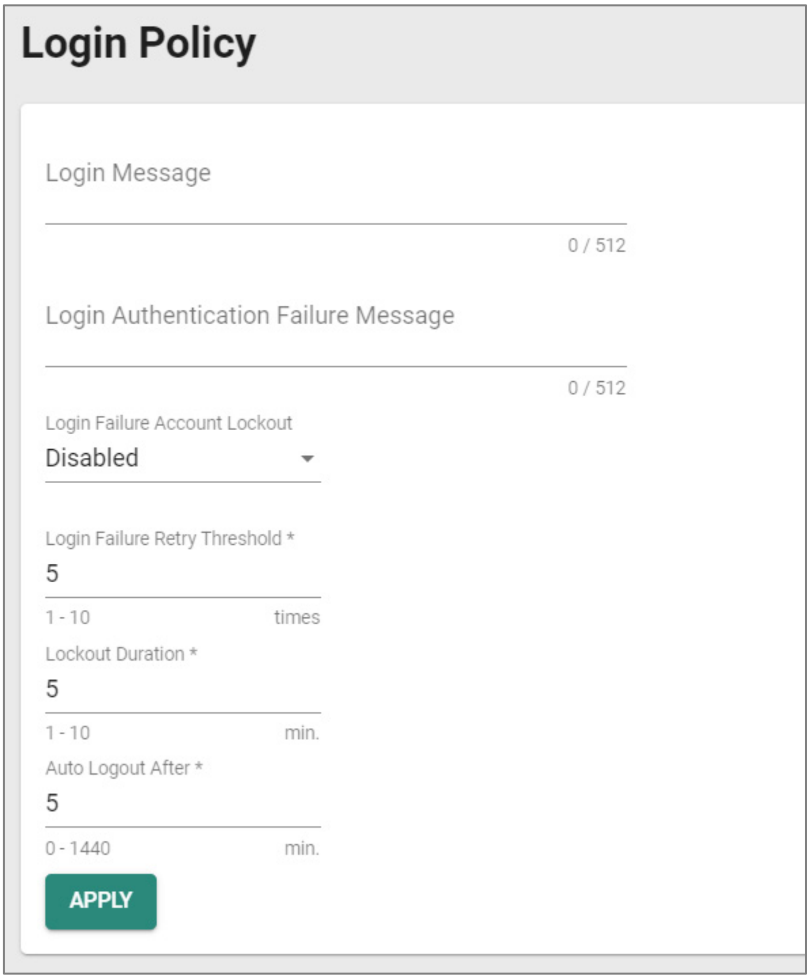
This section includes these pages:

- Login Policy
- Trusted Access
- SSH & SSL

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

Login Message

0 / 512

Login Authentication Failure Message

0 / 512

Login Failure Account Lockout: Disabled

Login Failure Retry Threshold *: 5

1 - 10 times

Lockout Duration *: 5

1 - 10 min.

Auto Logout After *: 5

0 - 1440 min.

UI Setting	Description	Valid Range	Default Value
Login Message	Specify the welcome message to display when users log in to the device.	0 to 512 characters	N/A
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 512 characters	N/A
Login Failure Account Lockout	Enable or disable the lockout function, which will temporarily prevent users from logging in for the **Lockout Duration** after the **Login Failure Retry Threshold** is exceeded. This can be useful for preventing brute force attacks.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Login Failure Retry Threshold	Specify the number of login retry attempts before the user is locked out for the **Lockout Duration**.	1 to 10	5
Lockout Duration	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	Specify the amount of time a user can be idle before they will be automatically logged out from the device.	1 to 1440	5

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.

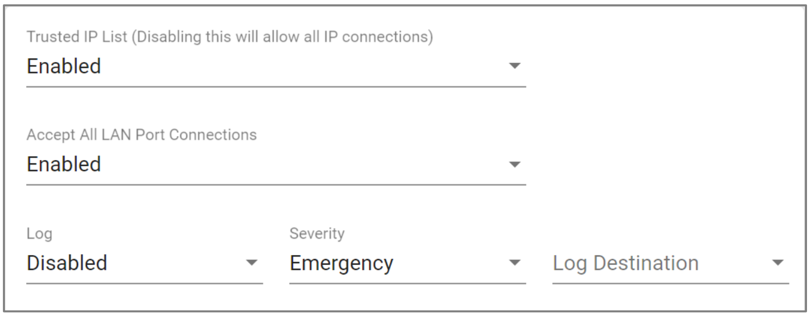
Limitations

You can create up to 10 trusted IP entries.

Trusted Access Settings

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 IP List or connected through a LAN connection..



Trusted IP List (Disabling this will allow all IP connections)
Enabled

Accept All LAN Port Connections
Enabled

Log
Disabled

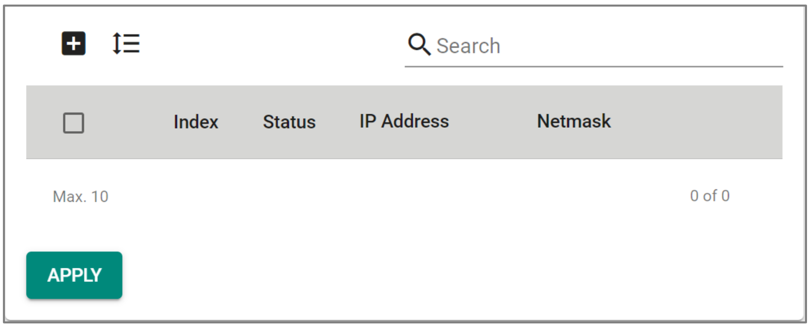
Severity
Emergency

Log Destination

UI Setting	Description	Valid Range	Default Value
Trusted IP List	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.	Enabled / Disabled	Disabled
Accept All LAN Port Connections	Enable or disable accepting all connections from LAN connections. **Enabled:** The device can only be accessed through a LAN connection. **Disabled:** The device can be accessed through any connection.	Enabled / Disabled	Enabled
Log	Enable or disable Trusted Access event logging.	Enabled / Disabled	Disabled
Severity	Select the severity level to assign to Trusted Access events. Refer to Appendix > Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency

UI Setting	Description	Valid Range	Default Value
Log Destination	Specify where to send Trusted Access event logs. You can select multiple options. **Syslog**: Event logs will be sent to a syslog server. Refer to Diagnostics > Event Logs and Notifications > Syslog for more information. **Trap**: Event notifications will be sent to a trap server. Refer to Diagnostics > SNMP Trap/Inform for more information. **Local Storage**: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to for more information.	Syslog / Trap / Local Storage	N/A

Trusted IP List

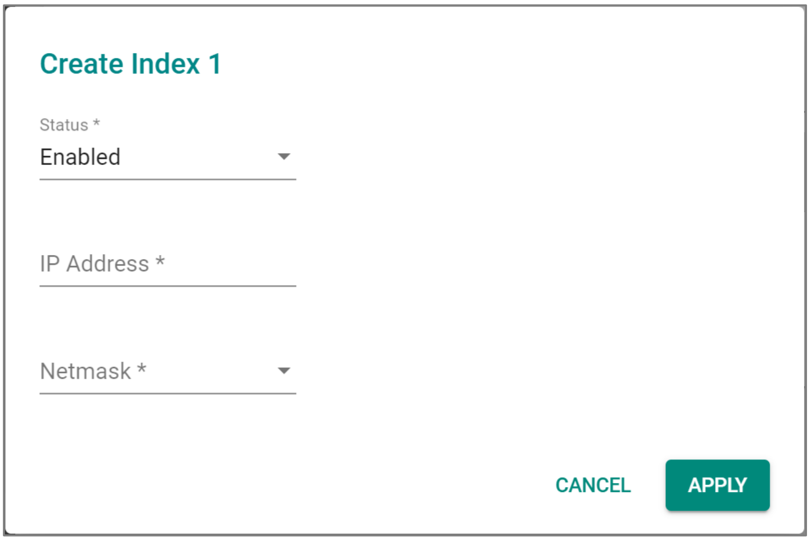


UI Setting	Description
Index	Shows the index of the Trusted IP entry.
Status	Shows whether the Trusted IP entry is enabled or disabled.
IP Address	Shows the IP address of the Trusted IP entry.
Netmask	Shows the netmask of the Trusted IP entry.

Trusted Access - Create Index

Menu Path: Security > Device Security > Trusted Access

Clicking the **Add (⊞)** icon on the **Security > Device Security > Trusted Access** page will open this dialog box. This dialog lets you add a trusted IP entry. Click **CREATE** to save your changes and add the new entry.



Create Index 1

Status *: Enabled

IP Address *

Netmask *

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the Trusted IP entry.	Enabled / Disabled	Enabled
IP Address	Specify the IP address of the trusted host(s).	Valid IP address	N/A
Netmask	Select a netmask for the trusted host(s).	Drop-down list of netmasks	N/A

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

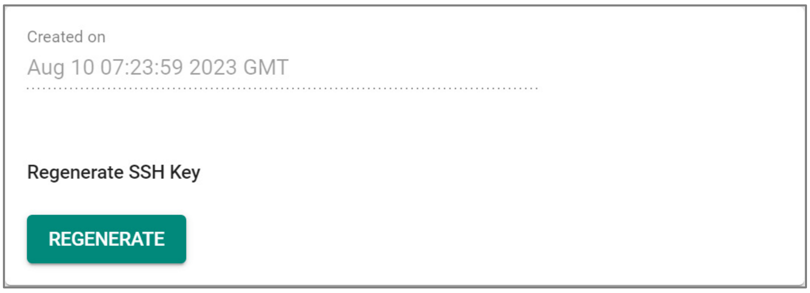
Menu Path: Security > Device Security > SSH & SSL - SSH

This page lets you manage your device's SSH key.

This shows you when the current SSH key was created. Click **REGENERATE** to generate a new SSH key for your device.

Warning

Regenerating the SSH key will restart the device's system services and will make the device temporarily unavailable.



Created on

Aug 10 07:23:59 2023 GMT

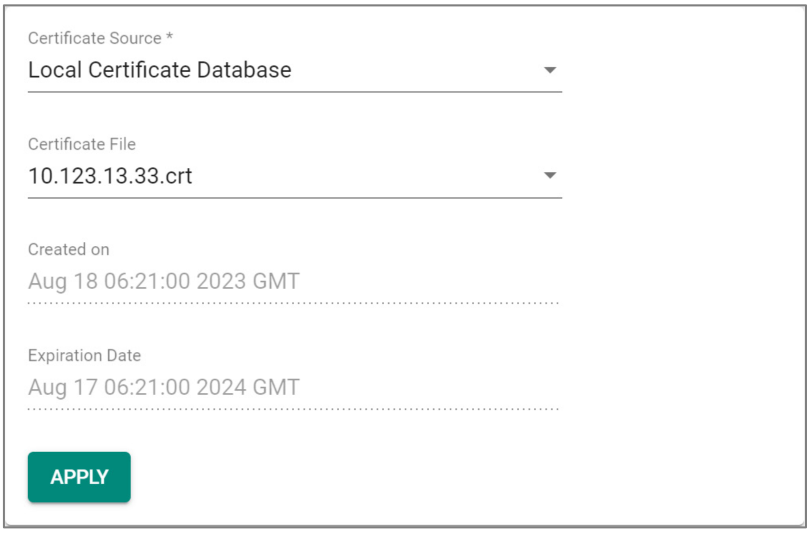
Regenerate SSH Key

SSL

Menu Path: Security > Device Security > SSH & SSL - SSL

This page lets you manage your device's SSL certificate. Click **APPLY** to save your changes.

SSL Settings



Certificate Source *
Local Certificate Database

Certificate File
10.123.13.33.crt

Created on
Aug 18 06:21:00 2023 GMT

Expiration Date
Aug 17 06:21:00 2024 GMT

UI Setting	Description	Valid Range	Default Value
Certificate Source	Select the source for your device's SSL certificate. **Auto Generate**: Your device will generate a certificate automatically. **Local Certificate Database**: Your device will use an imported certificate from the Local Certificate database. You will only be able to select certificates from a CSR or PKCS#12 certificates. Refer to Certificate Management for more information.	Auto Generate / Local Certificate Database	Auto Generate
Certificate File **(if Certificate Source is Local Certificate Database)**	Select the imported certificate file to use.	Drop-down list of applicable imported certificates	N/A
Created on **(View-only)**	Shows when the current certificate was created.	N/A	N/A
Expiration Date **(View-only)**	Shows when the current certificate will expire.	N/A	N/A

Network Security

Menu Path: Security > Network Security

This section lets you manage your device's network security features.

This section includes these pages:

- IEEE 802.1X

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:

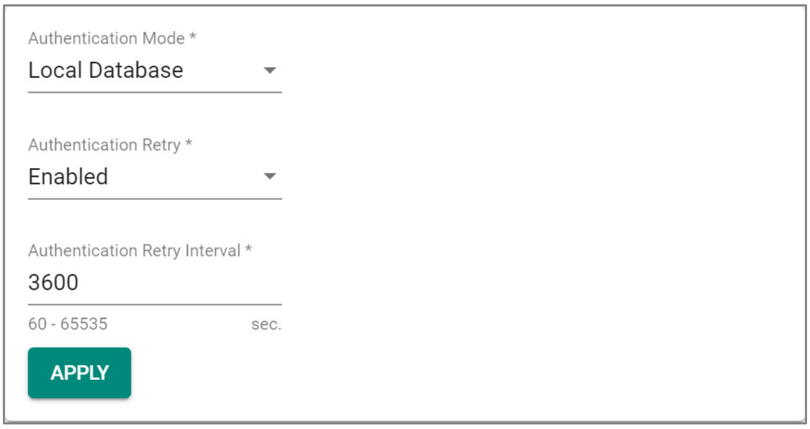
- General
- IEEE 802.1X Status
- RADIUS
- Local Database

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



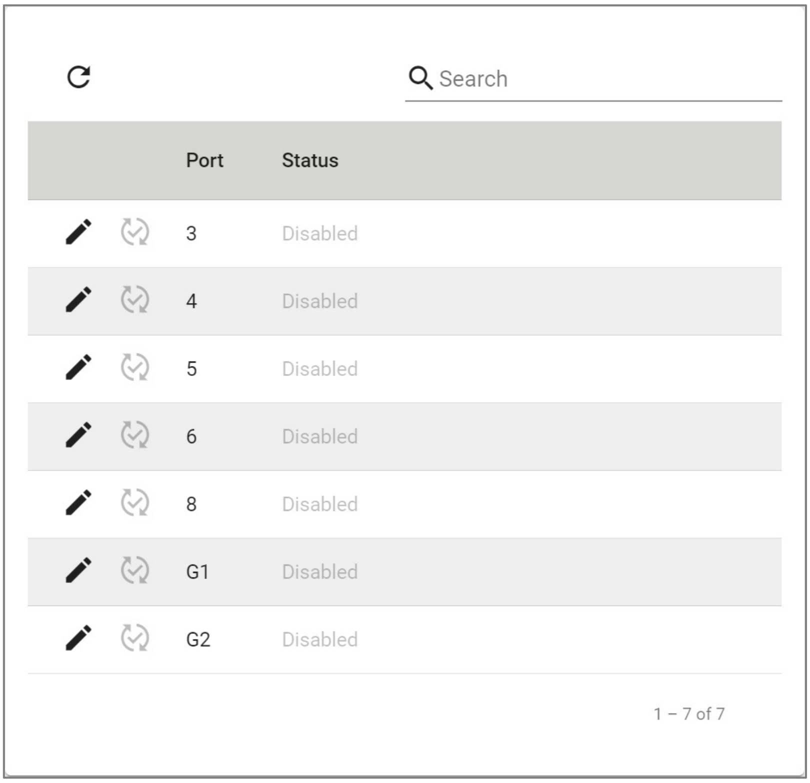
Authentication Mode *
Local Database

Authentication Retry *
Enabled

Authentication Retry Interval *
3600
60 - 65535 sec.

UI Setting	Description	Valid Range	Default Value
Authentication Mode	Select the method of authentication to use. **RADIUS**: Use a RADIUS server for authentication. **Local Database**: Use the local database for authentication. **RADIUS, Local**: Use both a RADIUS server and the local database for authentication.	RADIUS / Local Database / RADIUS, Local	Local Database
Authentication Retry	Enable or disable reauthentication.	Enabled / Disabled	Enabled
Authentication Retry Interval	Specify the authentication retry interval in seconds.	60 to 65535	3600

IEEE 802.1X Port List



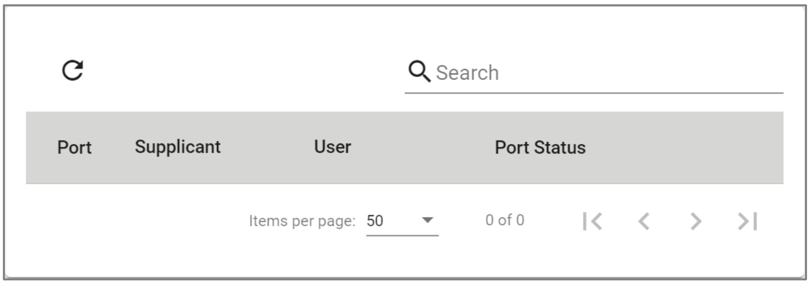
Port	Status
3	Disabled
4	Disabled
5	Disabled
6	Disabled
8	Disabled
G1	Disabled
G2	Disabled

UI Setting	Description
Port	Shows which port the entry is for.
Status	Shows whether IEEE 802.1X port access control is enabled or disabled for the port.

IEEE 802.1X Status

Menu Path: Security > Network Security > IEEE 802.1X - IEEE 802.1X Status

This page lets you see the IEEE 802.1X status of your ports.



UI Setting	Description
Port	Shows which port the entry is for.
Supplicant	Shows the supplicant for the port.
User	Shows the user for the port.
Port Status	Shows the IEEE 802.1X status of the port.

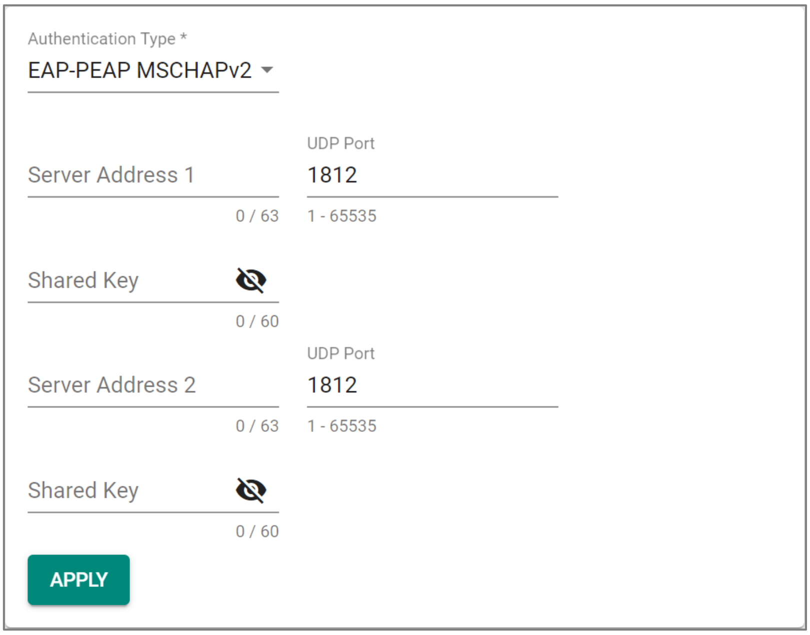
IEEE 802.1X - RADIUS

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.



Authentication Type *

EAP-PEAP MSCHAPv2

Server Address 1 0 / 63

UDP Port 1812 1 - 65535

Shared Key 0 / 60

Server Address 2 0 / 63

UDP Port 1812 1 - 65535

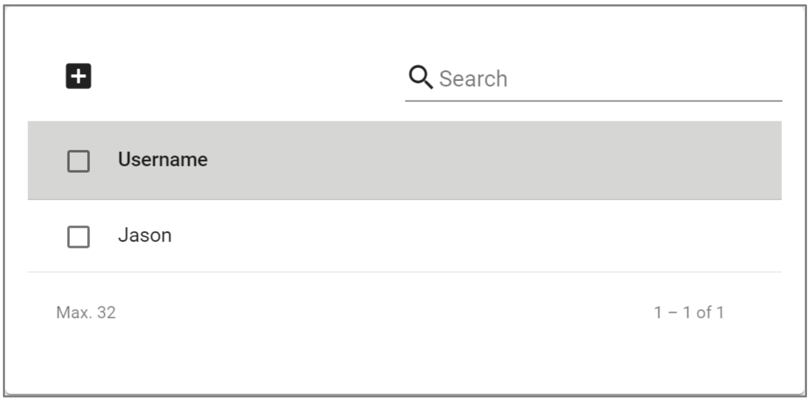
Shared Key 0 / 60

UI Setting	Description	Valid Range	Default Value
Authentication Type	Select the authentication method to use for the RADIUS servers.	PAP / CHAP / EAP-PEAP MSCHAPv2	EAP-PEAP MSCHAPv2
Server Address 1	Specify the IP address or domain name for the primary RADIUS server.	Valid IP address or domain name	N/A
UDP Port	Specify the port number for the primary RADIUS server.	1 to 65535	1812
Shared Key	Specify the shared key for the primary RADIUS server.	0 to 60 characters	N/A
Server Address 2	Specify the IP address or domain name for the secondary RADIUS server.	Valid IP address or domain name	N/A
UDP Port	Specify the port number for the secondary RADIUS server.	1 to 65535	1812
Shared Key	Specify the shared key for the secondary RADIUS server.	0 to 60 characters	N/A

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.



Search

□	Username
□	Jason

Max. 32

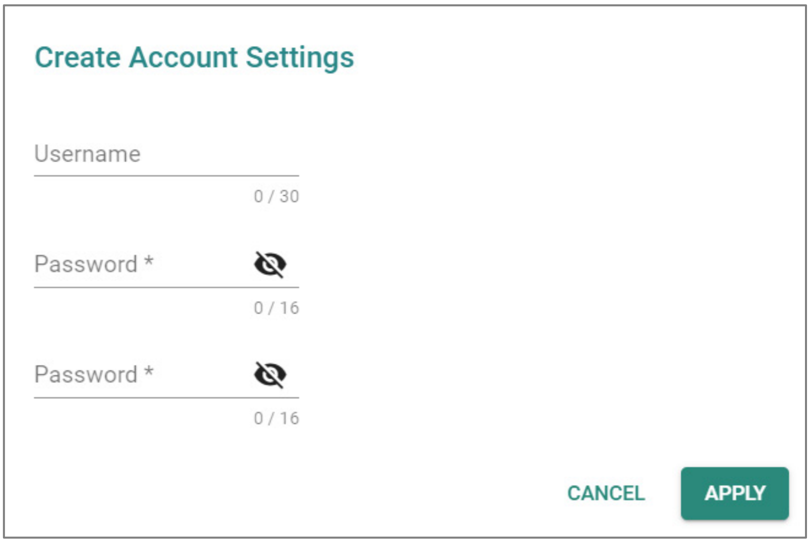
1 – 1 of 1

UI Setting	Description
Username	Shows the username of the account.

Local Database - Create Account Settings

Menu Path: Security > Network Security > IEEE 802.1X > Local Database

Clicking the **Add (**⊞**)** icon 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 **APPLY** to save your changes and add the new account.



Create Account Settings

Username

0 / 30

Password *

0 / 16

Password *

0 / 16

UI Setting	Description	Valid Range	Default Value
Username	Specify the username for this account.	1 to 30 characters	N/A
Password	Specify the password for this user account.	1 to 16 characters	N/A
Password	Re-enter the password for this user account.	1 to 16 characters	N/A

Authentication

Menu Path: Security > Authentication

This section lets you manage login authentication for your device.

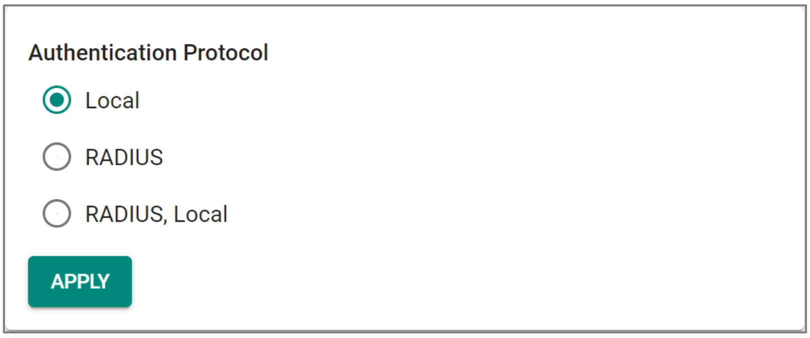
This section includes these pages:

- Login Authentication
- RADIUS

Login Authentication

Menu Path: Security > Authentication > Login Authentication

This page lets you configure your device's login authentication settings. Click **APPLY** to save your changes.



Authentication Protocol

● Local

○ RADIUS

○ RADIUS, Local

UI Setting	Description	Valid Range	Default Value
Authentication Protocol	Select the method of authentication to use. **Local:** Use the local database for authentication. **RADIUS**: Use a RADIUS server for authentication. **RADIUS, Local**: Use both a RADIUS server and the local database for authentication.	Local / RADIUS / RADIUS, Local	Local

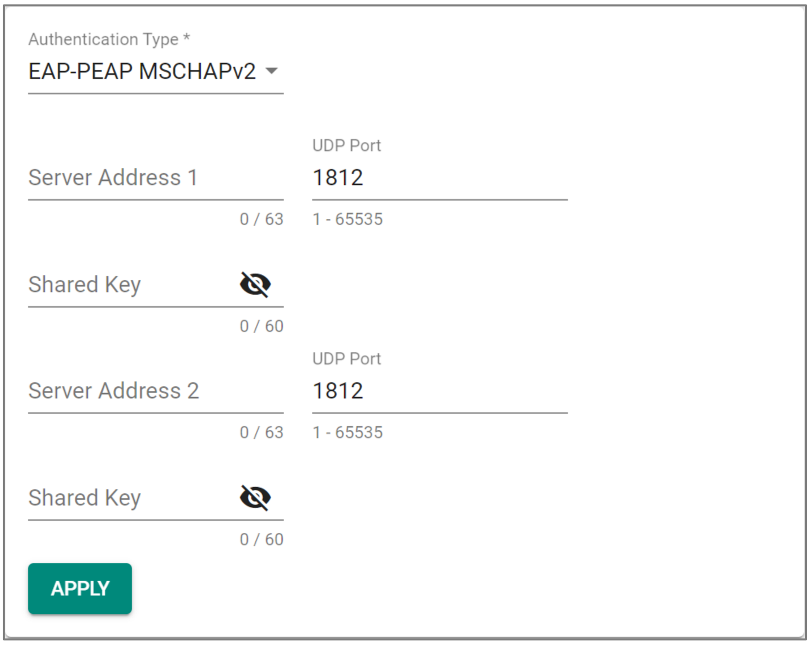
RADIUS

Menu Path: Security > Authentication > RADIUS

This page lets you specify a RADIUS server to use for login 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.



Authentication Type *
EAP-PEAP MSCHAPv2

Server Address 1 0 / 63

UDP Port 1812 1 - 65535

Shared Key 0 / 60

Server Address 2 0 / 63

UDP Port 1812 1 - 65535

Shared Key 0 / 60

UI Setting	Description	Valid Range	Default Value
Authentication Type	Select the authentication method to use for the RADIUS servers.	PAP / CHAP / EAP-PEAP MSCHAPv2	EAP-PEAP MSCHAPv2
Server Address 1	Specify the IP address or domain name for the primary RADIUS server.	Valid IP address or domain name	N/A
UDP Port	Specify the port number for the primary RADIUS server.	1 to 65535	1812
Shared Key	Specify the shared key for the primary RADIUS server.	0 to 60 characters	N/A
Server Address 2	Specify the IP address or domain name for the secondary RADIUS server.	Valid IP address or domain name	N/A
UDP Port	Specify the port number for the secondary RADIUS server.	1 to 65535	1812
Shared Key	Specify the shared key for the secondary RADIUS server.	0 to 60 characters	N/A

MXview Alert Notification

Menu Path: Security > MXview Alert Notification

This page lets you configure device notifications for MXview.

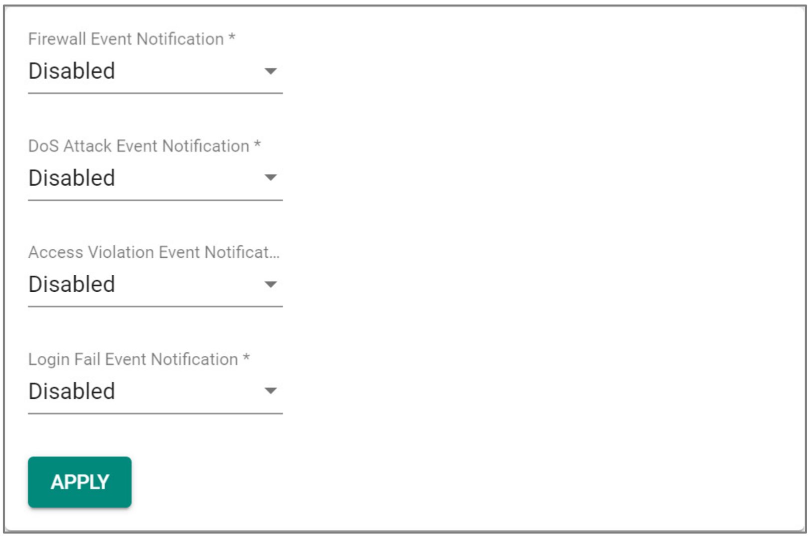
This page includes these tabs:

- Security Notification Setting
- Security Status

Security Notification Setting

Menu Path: Security > MXview Alert Notification - Security Notification Setting

This page lets you configure your MXview security alert notification settings.



Firewall Event Notification *
Disabled

DoS Attack Event Notification *
Disabled

Access Violation Event Notificat...
Disabled

Login Fail Event Notification *
Disabled

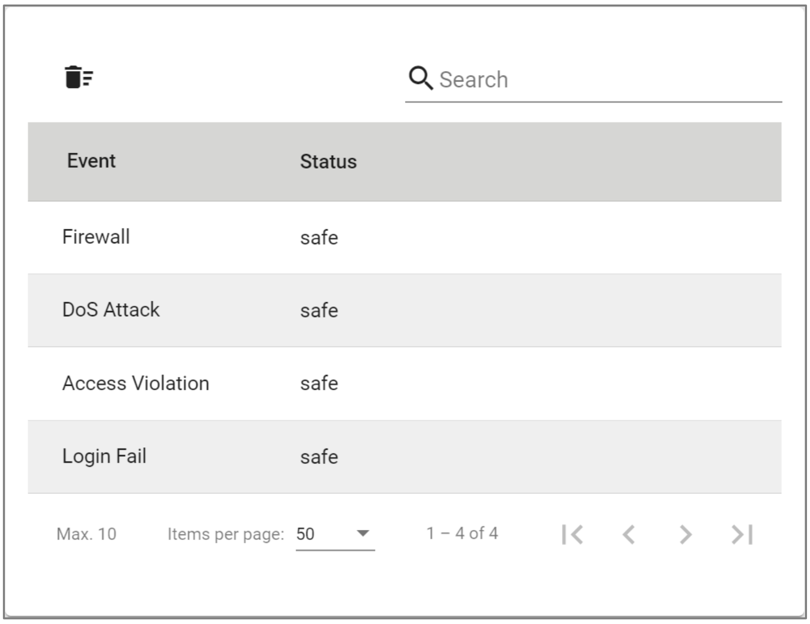
UI Setting	Description	Valid Range	Default Value
Firewall Event Notification	Enable or disable notifications for Firewall events.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
DoS Attack Event Notification	Enable or disable notifications for DoS attack events.	Enabled / Disabled	Disabled
Access Violation Event Notification	Enable or disable notifications for Access Violation events.	Enabled / Disabled	Disabled
Login Fail Event Notification	Enable or disable notifications for Login Fail events.	Enabled / Disabled	Disabled

Security Status

Menu Path: Security > MXview Alert Notification - Security Status

This page lets you see the status of all MXview security event types.



Event	Status
Firewall	safe
DoS Attack	safe
Access Violation	safe
Login Fail	safe

UI Setting	Description
Event	Shows the name of the event type.
Status	Shows the current status of the event type.

Diagnostics

Menu Path: Diagnostics

The Diagnostics settings area lets you keep track of system and network performance, check event logs, and check the status of the port connectors.

This settings area includes these sections:

- System Status
- Network Status
- Event Logs and Notifications
- Tools

Diagnostics - User Privileges

Privileges to Diagnostics 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			
Utilization	R/W	R/W	R
Fiber Check	R/W	R/W	R
Network Status			
Network Statistics	R	R	R
LLDP	R/W	R/W	R
ARP Table	R	R	R
Event Log & Notifications			
Event Log	R/W	R/W	R
Event Notifications	R/W	R/W	R

Settings	Admin	Supervisor	User
Syslog	R/W	R	R
SNMP Trap/Inform	R/W	-	-
Email Settings	R/W	R	R
Tools			
Port Mirror	R/W	R/W	R
Ping	R/W	R/W	R

System Status

Menu Path: Diagnostics > System Status

This section lets you check on various system statuses.

This section includes these pages:

- Utilization
- Fiber Check

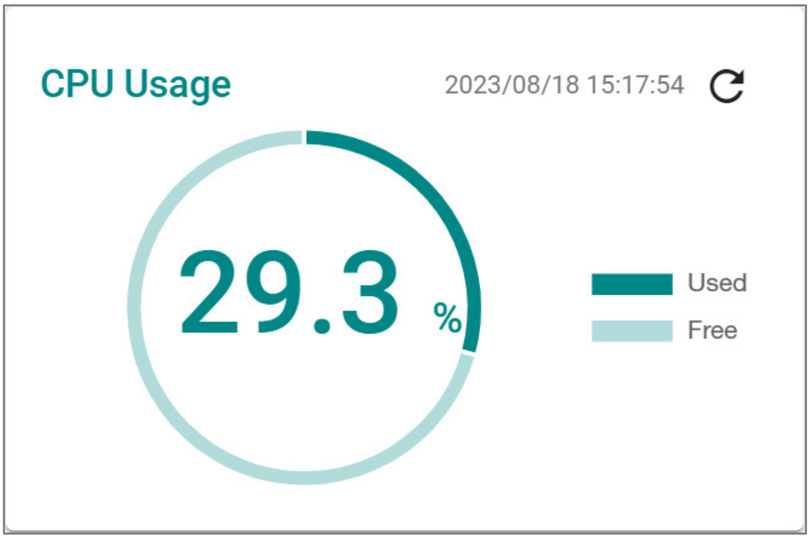
Utilization

Menu Path: Diagnostics > System Status > Utilization

This page lets you monitor current and historical system resource utilization.

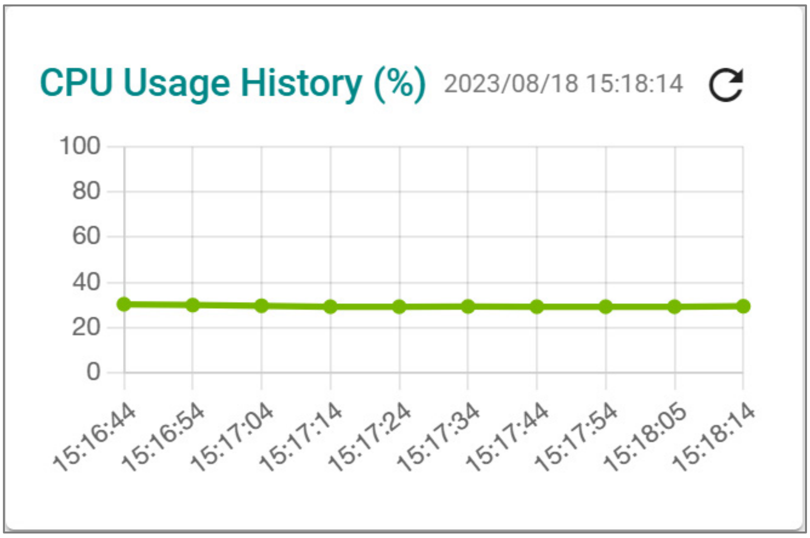
CPU Usage

This shows the current CPU usage of your device.



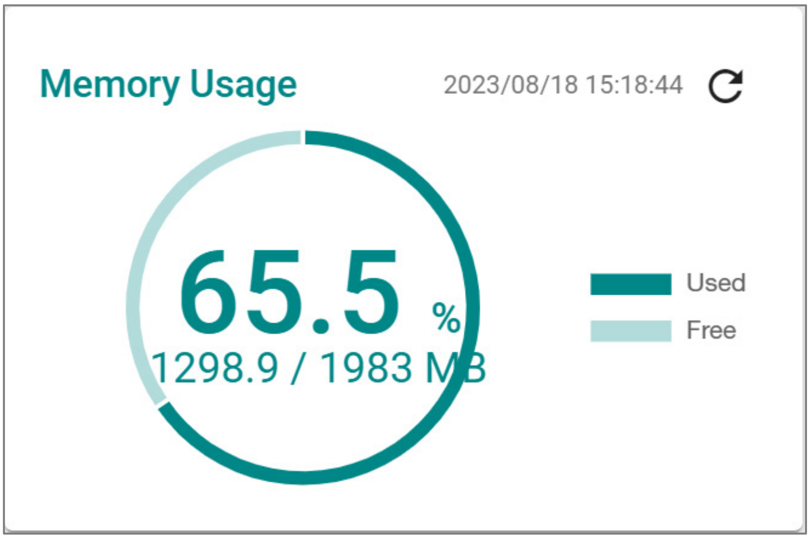
CPU Usage History

This shows the CPU usage of your device over time.



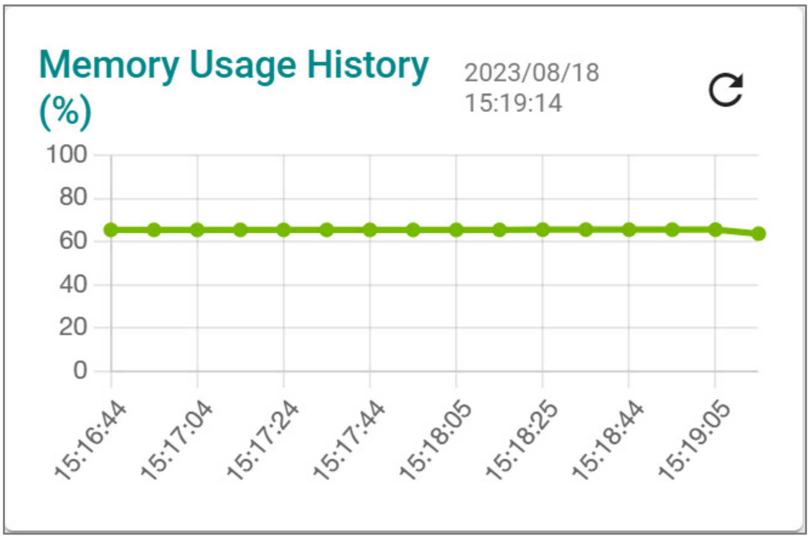
Memory Usage

This shows your device's current memory usage.



Memory Usage History

This shows your device's memory usage over time.



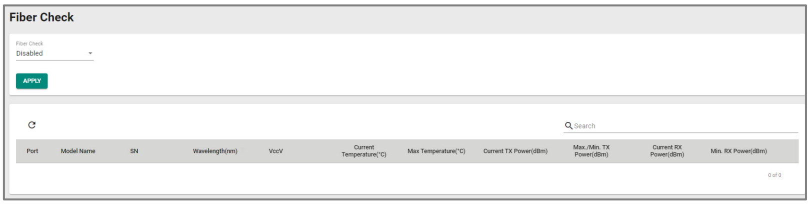
Fiber Check

Menu Path: Diagnostics > System Status > Fiber Check

This page lets you diagnose the link status of the device's fiber connectors, including SFP and fixed type (multi-mode SC/ST and single-mode SC) connectors. It lets you monitor the temperature, TX/RX power, and other parameters on fiber ports to determine if the ports are working properly.

You can enable trap, email warning, and/or relay warning functions to receive an alarm or relay if one of the fiber ports exceeds the threshold for that port. Refer to Diagnostics > Event Logs and Notifications for more information.

Fiber Check Settings



Fiber Check

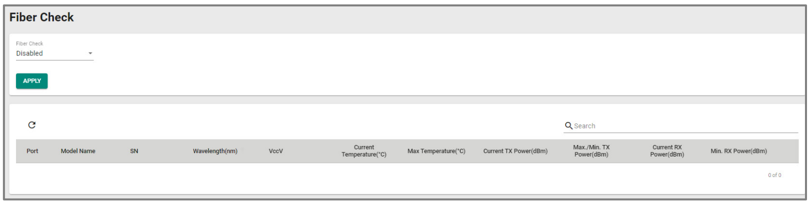
Fiber Check: Disabled

Port	Model Name	SN	Wavelength(nm)	VccV	Current Temperature(°C)	Max Temperature(°C)	Current TX Power(dBm)	Max./Min. TX Power(dBm)	Current RX Power(dBm)	Min. RX Power(dBm)

0 of 0

UI Setting	Description	Valid Range	Default Value
Fiber Check	Enable or disable the fiber check feature.	Enabled / Disabled	Disabled

Fiber Check Status List



Fiber Check

Fiber Check: Disabled

Port	Model Name	SN	Wavelength(nm)	VccV	Current Temperature(°C)	Max Temperature(°C)	Current TX Power(dBm)	Max./Min. TX Power(dBm)	Current RX Power(dBm)	Min. RX Power(dBm)

0 of 0

UI Setting	Description
Port	Shows the port number of the fiber connection.
Model Name	Shows the name of the related SFP module.
SN	Shows the serial number of the related SFP module.

UI Setting	Description
Wavelength (nm)	Shows the wavelength of the fiber connection.
VccV	Shows the voltage supplied to the fiber connection.
Current Temperature (°C)	Shows the current temperature of the fiber connection.
Max. Temperature (°C)	Shows the maximum temperature the fiber connection supports.
Current TX Power(dBm)	Shows the current transmit signal strength for the fiber connection.
Max./Min. TX Power(dBm)	Shows the maximum and minimum transmit signal strength for the fiber connection.
Current RX Power(dBm)	Shows the current receive signal strength for the fiber connection.
Min. RX Power(dBm)	Shows the minimum receive signal strength for the fiber connection.

Network Status

Menu Path: Diagnostics > Network Status

This section lets you check on the status of your device's network connections.

This section includes these pages:

- Network Statistics
- LLDP
- ARP Table

Network Statistics

Menu Path: Diagnostics > Network Status > Network Statistics

This page lets you see the real-time packet and bandwidth status for your device.

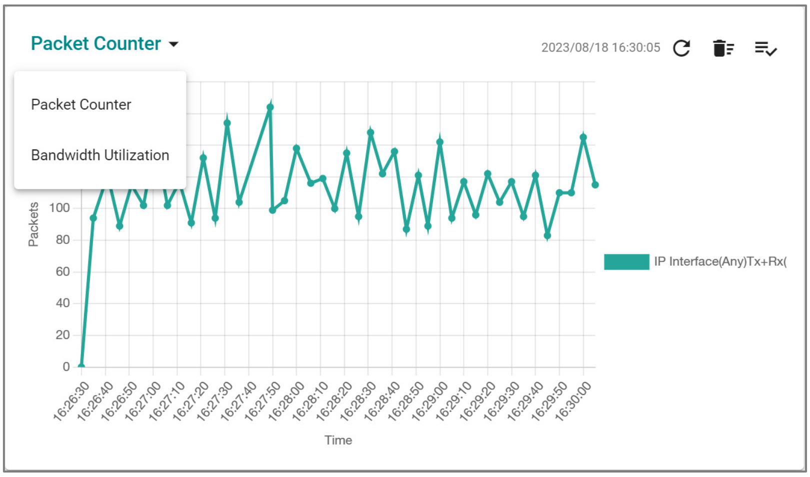
Network Status Display

This display lets you switch between **Packet Counter** and **Bandwidth Utilization** views by clicking on the drop-down menu.

- **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.

Note

The default line shows activity for all IP interfaces for both Tx and Rx activity. You can add additional lines by clicking the **Display Settings** button.

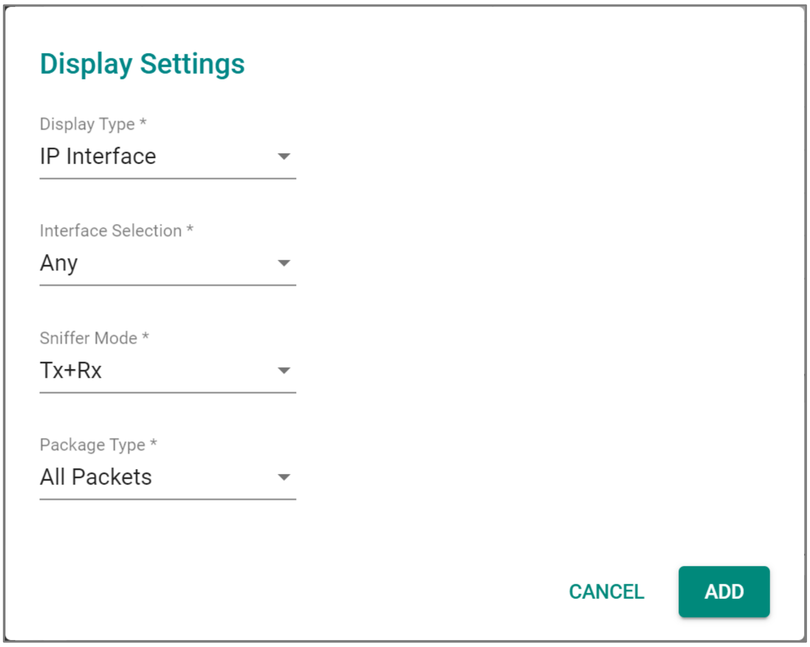


UI Setting	Description
Refresh (↻)	Updates statistics immediately without waiting for the refresh interval.
Reset Statistics Graph (🗑)	Clears the display and resets display settings back to defaults.
Display Settings (≡✓)	Opens **Display Settings**, which allows you to add lines based on user-defined criteria.

Display Settings

Menu Path: Diagnostics > Network Status > Network Statistics

Clicking the **Display Settings (** ≡ **)** icon on the **Diagnostics > Network Status > Network Statistics** page will open this dialog box. This dialog lets you define additional interfaces or ports to monitor. Click **ADD** to save your changes and add the new line.



Display Settings

Display Type *
IP Interface

Interface Selection *
Any

Sniffer Mode *
Tx+Rx

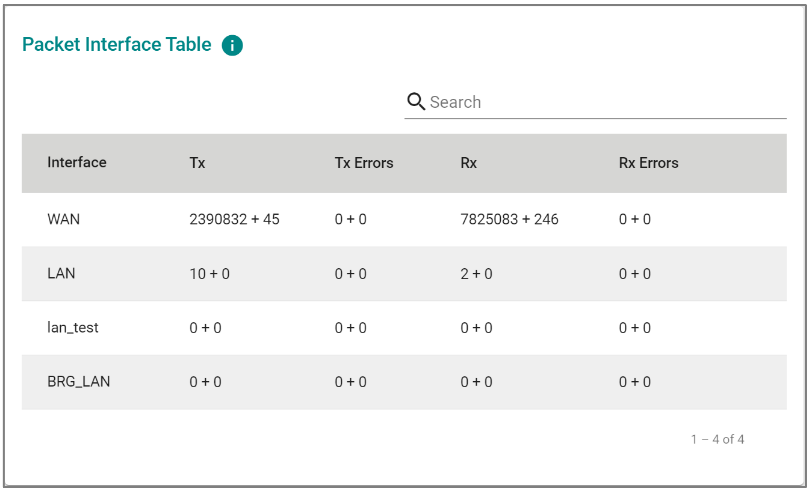
Package Type *
All Packets

UI Setting	Description	Valid Range	Default Value
Display Type	Select whether to monitor an IP interface or a port. **Port**: Monitor traffic for a specific port. **IP Interface**: Monitor traffic for a specific network interface.	Port / IP Interface	IP Interface
Interface Selection **(if Display Type is IP Interface)**	Select which interface to monitor. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Configuration > Network Interfaces for more information about managing your device's interfaces.	Drop-down list of interfaces	Any

UI Setting	Description	Valid Range	Default Value
Port Selection **(if Display Type is Port)**	Select which port to monitor. ✎ **Note** Available ports will vary depending on your product model.	Drop-down list of ports	All ports
Sniffer Mode	Select which type of traffic to monitor. **Tx+Rx**: Monitor both transmit and receive traffic. **Tx**: Only monitor transmit traffic. **Rx**: Only monitor receive traffic.	Tx+Rx / Tx / Rx	Tx+Rx
Package Type	Select which packet type to monitor. **All Packets**: Monitor all packet types. **Unicast**: Only monitor unicast packets. **Broadcast**: Only monitor broadcast packets. **Multicast**: Only monitor multicast packets. **Error Packets**: Only monitor error packets. ✎ **Note** If **Display Type** is **IP Interface**, only **All Packets** and **Error Packets** will be available.	All Packets / Unicast / Broadcast, Multicast / Error Packets	All Packets

Packet Interface Table

This table shows how many packets are being handled by each interface. Values are shown as Total Packets + Packets in the past 5 seconds.



Packet Interface Table

Search

Interface	Tx	Tx Errors	Rx	Rx Errors
WAN	2390832 + 45	0 + 0	7825083 + 246	0 + 0
LAN	10 + 0	0 + 0	2 + 0	0 + 0
lan_test	0 + 0	0 + 0	0 + 0	0 + 0
BRG_LAN	0 + 0	0 + 0	0 + 0	0 + 0

1 – 4 of 4

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 Log
- Event Notifications
- Syslog
- SNMP Trap/Inform
- Email Settings

Event Log

Menu Path: Diagnostics > Event Logs and Notifications > Event Log

This page lets you browse and export your device's various event logs.

This page includes these tabs:

- System Log
- Firewall Log
- VPN Log
- Settings and Backup

Note

The timestamp on event logs will automatically synchronize with the NTP/SNTP server and applies to all new event logs. Refer to System > Time > NTP/SNTP Server for more details.

System Log

Menu Path: Diagnostics > Event Logs and Notifications > Event Log - System Log

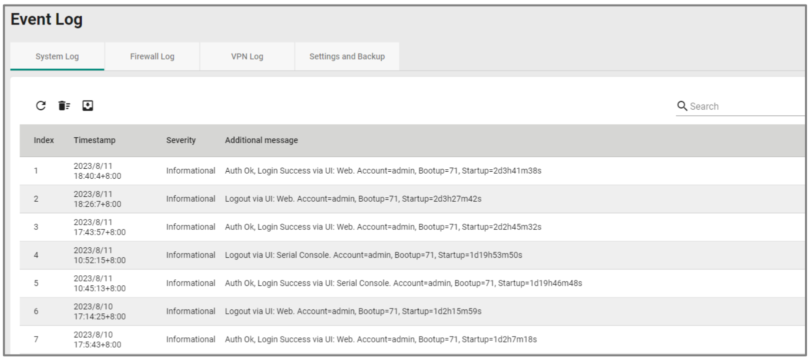
This page lets you view your device's system-related event logs.

Limitations

The system log can record up to 1000 events.

Actions

- Click the **Refresh icon (↻)** to refresh the logs.
- Click the **Clear System Log icon (🗑)** to delete all logs.
- Click the **Export icon (⤓)** to export all logs to a file.



Index	Timestamp	Severity	Additional message
1	2023/8/11 18:40:4+8:00	Informational	Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=2d3h41m38s
2	2023/8/11 18:26:7+8:00	Informational	Logout via UI: Web. Account=admin, Bootup=71, Startup=2d3h27m42s
3	2023/8/11 17:43:57+8:00	Informational	Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=2d2h45m32s
4	2023/8/11 10:52:15+8:00	Informational	Logout via UI: Serial Console. Account=admin, Bootup=71, Startup=1d19h53m50s
5	2023/8/11 10:45:13+8:00	Informational	Auth Ok, Login Success via UI: Serial Console. Account=admin, Bootup=71, Startup=1d19h46m48s
6	2023/8/10 17:14:25+8:00	Informational	Logout via UI: Web. Account=admin, Bootup=71, Startup=1d2h15m59s
7	2023/8/10 17:5:43+8:00	Informational	Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=1d2h7m18s

UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event.
Additional 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**, **Configuration Change**, **User Logout**.

Firewall Log

Menu Path: Diagnostics > Event Logs and Notifications > Event Log - Firewall Log

This page lets you view your device's firewall-related event logs.

Limitations

Each firewall log can record up to 1000 events.

You can switch between different firewall logs by clicking on the drop-down menu.

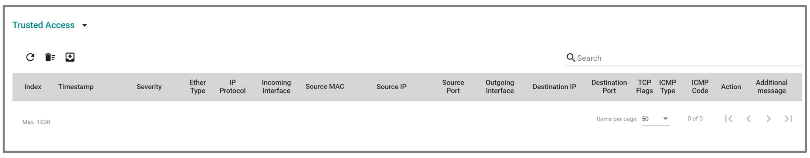
- Trusted Access
- Malformed Packets

- DoS Policy
- Layer 3-7 Policy
- Protocol Filter Policy
- ADP
- IPS
- Session Control
- Layer 2 Policy

Actions

- Click the **Refresh icon (** ⟳ **)** to refresh the logs.
- Click the **Clear System Log icon (** 🗑 **)** to delete all logs.
- Click the **Export icon (** ⤓ **)** to export all logs to a file.

Trusted Access



Trusted Access ▾

Search

Index	Timestamp	Severity	Ether Type	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP Flags	ICMP Type	ICMP Code	Action	Additional message

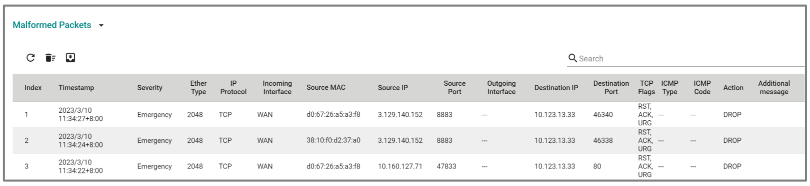
Max. 1000

Items per page: 50 ▾ 0 of 0

UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event.
Ether Type	Shows the EtherType that the event applies to.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.

UI Setting	Description
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
TCP Flags	Shows the TCP flags that apply to this event.
ICMP Type	Shows the ICMP type that applies to this event.
ICMP Code	Shows the ICMP code that applies to this event.
Action	Shows the action taken by the firewall for this event.
Additional message	Shows additional information about the event, based on the type of event.

Malformed Packets

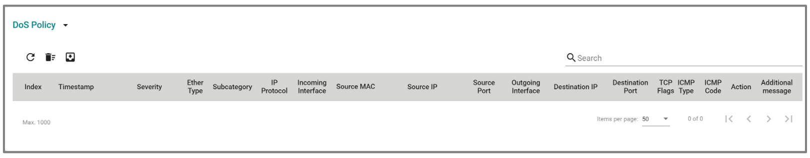


Index	Timestamp	Severity	Ether Type	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP Flags	ICMP Type	ICMP Code	Action	Additional message
1	2023/3/10 11:34:27+8:00	Emergency	2048	TCP	WAN	d0:67:26:a5:a3:f8	3.129.140.152	8883	---	10.123.13.33	46340	RST, ACK, URG	---	---	DROP	
2	2023/3/10 11:34:24+8:00	Emergency	2048	TCP	WAN	38:10:f0:d2:37:a0	3.129.140.152	8883	---	10.123.13.33	46338	RST, ACK, URG	---	---	DROP	
3	2023/3/10 11:34:22+8:00	Emergency	2048	TCP	WAN	d0:67:26:a5:a3:f8	10.160.127.71	47833	---	10.123.13.33	80	RST, ACK, URG	---	---	DROP	

UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event.
Ether Type	Shows the EtherType that the event applies to.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.

UI Setting	Description
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
TCP Flags	Shows the TCP flags related to the event.
ICMP Type	Shows the ICMP type that applies to this event.
ICMP Code	Shows the ICMP code that applies to this event.
Action	Shows the action taken by the firewall for this event.
Additional message	Shows additional information about the event, based on the type of event.

DoS Policy



Index	Timestamp	Severity	Ether Type	Subcategory	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP Flags	ICMP Type	ICMP Code	Action	Additional message

Max. 1000

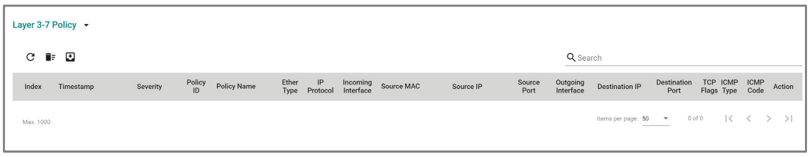
Items per page: 50

0 of 0

UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event.
Ether Type	Shows the EtherType that applies to this event.
Subcategory	Shows the subcategory that applies to this event.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.

UI Setting	Description
TCP Flags	Shows the TCP flags that apply to this event.
ICMP Type	Shows the ICMP type that applies to this event.
ICMP Code	Shows the ICMP code that applies to this event.
Action	Shows the action taken by the firewall for this event.
Additional message	Shows additional information about the event, based on the type of event.

Layer 3-7 Policy



Layer 3-7 Policy

Search

Index	Timestamp	Severity	Policy ID	Policy Name	Ether Type	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP Flags	ICMP Type	ICMP Code	Action

Max. 1000

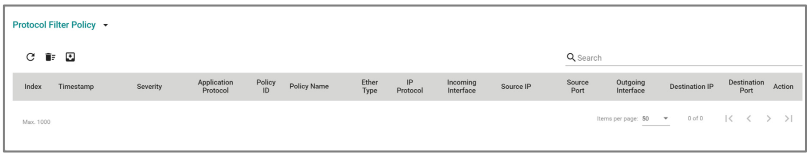
Items per page: 50

0 of 0

UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event.
Policy ID	Shows the ID of the firewall policy that applies to this event.
Policy Name	Shows the name of the firewall policy that applies to this event.
Ether Type	Shows the EtherType that applies to this event.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.

UI Setting	Description
TCP Flags	Shows the TCP flags that apply to this event.
ICMP Type	Shows the ICMP type that applies to this event.
ICMP Code	Shows the ICMP code that applies to this event.
Action	Shows the action taken by the firewall for this event.

Protocol Filter Policy



Protocol Filter Policy

Search

Index	Timestamp	Severity	Application Protocol	Policy ID	Policy Name	Ether Type	IP Protocol	Incoming Interface	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	Action

Max. 1000

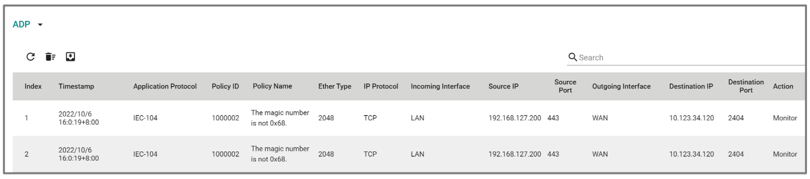
Items per page: 50

0 of 0

UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event.
Application Protocol	Shows which application this event is related to.
Policy ID	Shows the ID of the firewall policy that applies to this event.
Policy Name	Shows the name of the firewall policy that applies to this event.
Ether Type	Shows the EtherTypes for this traffic.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.

UI Setting	Description
TCP Flags	Shows the TCP flags for this traffic.
ICMP Type	Shows the ICMP type that applies to this event.
ICMP Code	Shows the ICMP code that applies to this event.
Action	Shows the action taken by the firewall for this event.

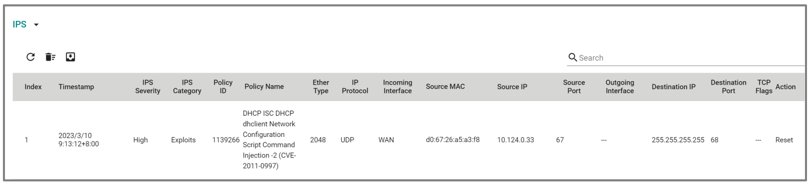
ADP



Index	Timestamp	Application Protocol	Policy ID	Policy Name	Ether Type	IP Protocol	Incoming Interface	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	Action
1	2022/10/6 16:0:19+8:00	IEC-104	1000002	The magic number is not 0x68.	2048	TCP	LAN	192.168.127.200	443	WAN	10.123.34.120	2404	Monitor
2	2022/10/6 16:0:19+8:00	IEC-104	1000002	The magic number is not 0x68.	2048	TCP	LAN	192.168.127.200	443	WAN	10.123.34.120	2404	Monitor

UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Application Protocol	Shows the application protocol that applies to this event.
Policy ID	Shows the ID of the firewall policy that applies to this event.
Policy Name	Shows the name of the firewall policy that applies to this event.
Ether Type	Shows the EtherType that applies to this event.
Subcategory	Shows the subcategory that applies to this event.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
Action	Shows the action taken by the firewall for this event.

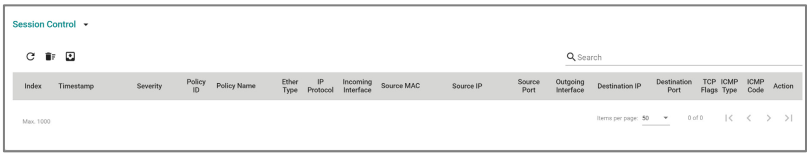
IPS



Index	Timestamp	IPS Severity	IPS Category	Policy ID	Policy Name	Ether Type	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP Flags	Action
1	2023/3/10 9:13:12+8:00	High	Exploits	1139266	DHCP ISC DHCP dhclient Network Configuration Script Command Injection -2 (CVE-2011-0997)	2048	UDP	WAN	d0:67:26:a5:a3:f8	10.124.0.33	67	---	255.255.255.255	68	---	Reset

UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
IPS Severity	Shows the IPS severity of the event.
IPS Category	Shows the IPS category of the event.
Policy ID	Shows the ID of the firewall policy that applies to this event.
Policy Name	Shows the name of the firewall policy that applies to this event.
Ether Type	Shows the EtherType that applies to this event.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
TCP Flags	Shows the TCP flags that apply to this event.
Action	Shows the action taken by the firewall for this event.

Session Control



Index	Timestamp	Severity	Policy ID	Policy Name	Ether Type	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP Flags	ICMP Type	ICMP Code	Action

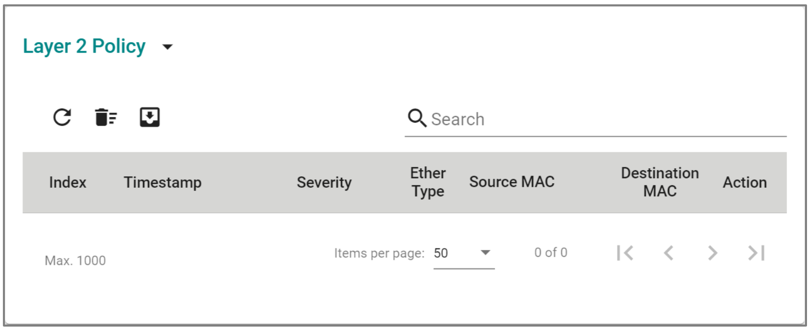
Max. 1000

Items per page: 50

0 of 0

UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event.
Policy ID	Shows the ID of the firewall policy that applies to this event.
Policy Name	Shows the name of the firewall policy that applies to this event.
Ether Type	Shows the EtherType that applies to this event.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
TCP Flags	Shows the TCP flags that apply to this event.
ICMP Type	Shows the ICMP type that applies to this event.
ICMP Code	Shows the ICMP code that applies to this event.
Action	Shows the action taken by the firewall for this event.

Layer 2 Policy



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event.
Ether Type	Shows the EtherType that applies to this event.
Source MAC	Shows the source MAC address for this traffic.
Destination MAC	Shows the destination MAC address for this traffic.
Action	Shows the action taken by the firewall for this event.

VPN Log

Menu Path: Diagnostics > Event Logs and Notifications > Event Log - VPN Log

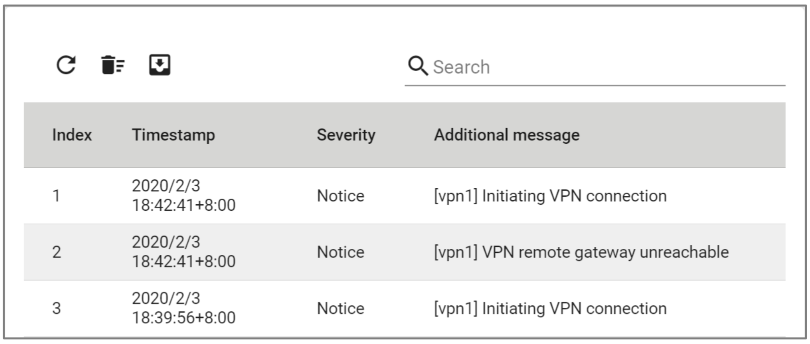
This page lets you view your device's VPN-related event logs.

Limitations

The VPN log can record up to 1000 events.

Actions

- Click the **Refresh icon (** ↻ **)** to refresh the logs.
- Click the **Clear System Log icon (** 🗑 **)** to delete all logs.
- Click the **Export icon (** ⤓ **)** to export all logs to a file.



Index	Timestamp	Severity	Additional message
1	2020/2/3 18:42:41+8:00	Notice	[vpn1] Initiating VPN connection
2	2020/2/3 18:42:41+8:00	Notice	[vpn1] VPN remote gateway unreachable
3	2020/2/3 18:39:56+8:00	Notice	[vpn1] Initiating VPN connection

UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event.
Additional message	Shows additional information about the event, based on the type of event.

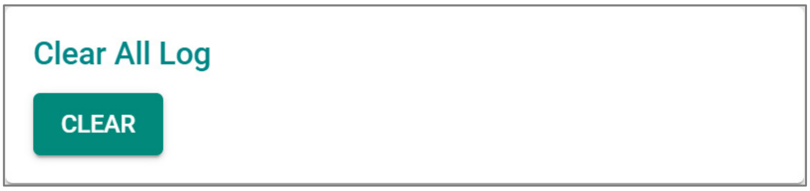
Settings and Backup

Menu Path: Diagnostics > Event Logs and Notifications > Event Log - Settings and Backup

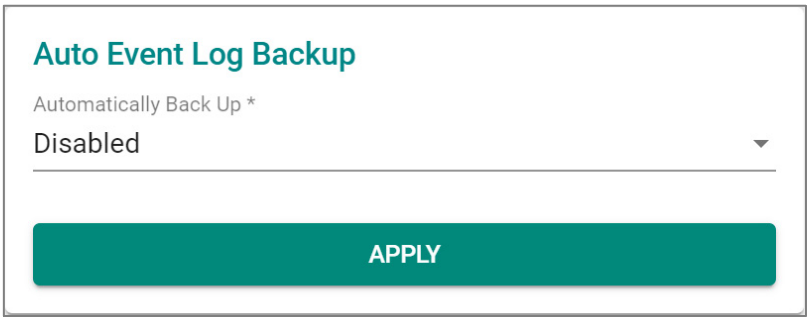
This page lets you clear all the logs or enable automatic event log backups. You can also set up capacity warnings and oversize actions that trigger when log storage has exceeded the specified storage threshold.

Clear All Log

Click the **CLEAR** button to clear all event logs.



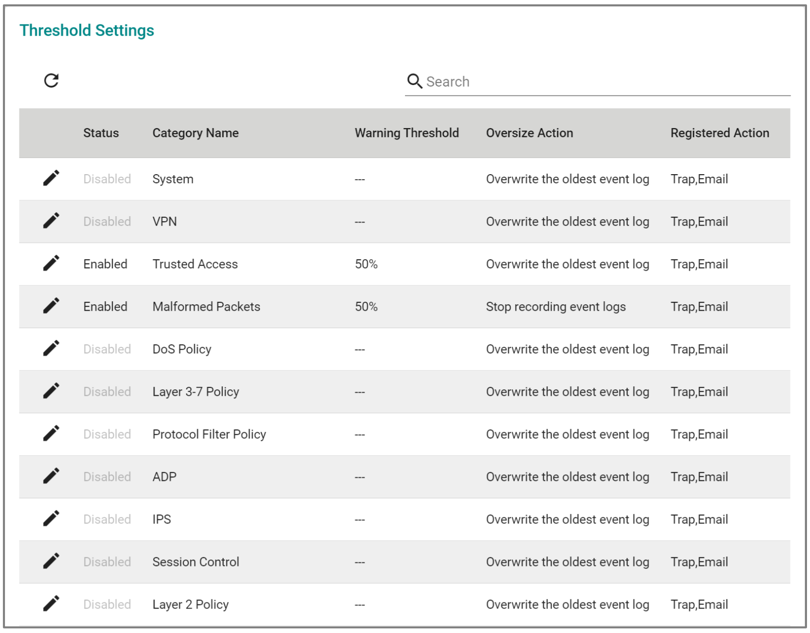
Auto Event Log Backup



Automatically Back Up *
Disabled

UI Setting	Description	Valid Range	Default Value
Automatically Restore	Enable or disable automatic event log backups.	**Enable / Disabled**	Disabled

Threshold Settings



Threshold Settings

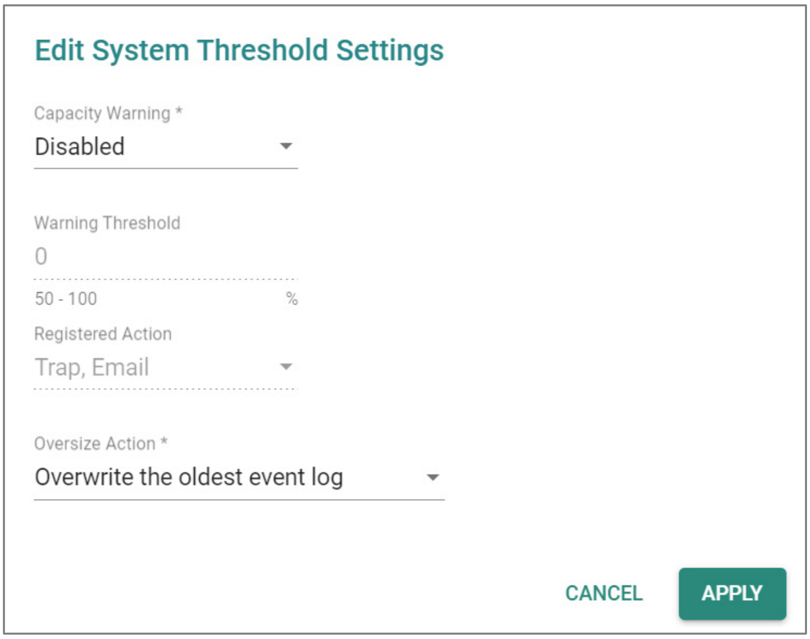
	Status	Category Name	Warning Threshold	Oversize Action	Registered Action
✎	Disabled	System	---	Overwrite the oldest event log	Trap,Email
✎	Disabled	VPN	---	Overwrite the oldest event log	Trap,Email
✎	Enabled	Trusted Access	50%	Overwrite the oldest event log	Trap,Email
✎	Enabled	Malformed Packets	50%	Stop recording event logs	Trap,Email
✎	Disabled	DoS Policy	---	Overwrite the oldest event log	Trap,Email
✎	Disabled	Layer 3-7 Policy	---	Overwrite the oldest event log	Trap,Email
✎	Disabled	Protocol Filter Policy	---	Overwrite the oldest event log	Trap,Email
✎	Disabled	ADP	---	Overwrite the oldest event log	Trap,Email
✎	Disabled	IPS	---	Overwrite the oldest event log	Trap,Email
✎	Disabled	Session Control	---	Overwrite the oldest event log	Trap,Email
✎	Disabled	Layer 2 Policy	---	Overwrite the oldest event log	Trap,Email

UI Setting	Description
Status	Shows whether threshold settings are enabled for the category.
Category Name	Shows which event log the threshold settings apply to.
Warning Threshold	Shows the threshold percentage that must be reached to trigger a warning sent through the **Registered Action** methods.
Oversize Action	Shows what action will be taken when log storage is full for the selected category.
Registered Action	Shows how threshold warnings will be sent.

Edit Threshold Settings

Menu Path: Diagnostics > Event Logs and Notifications > Event Log - Settings and Backup

Clicking the **Edit (✎)** icon for an entry on the **Insert > Path Here** page will open this dialog box. This dialog lets you edit the threshold settings the selected event log category. Click **APPLY** to save your changes.



Edit System Threshold Settings

Capacity Warning *
Disabled

Warning Threshold
0
50 - 100 %

Registered Action
Trap, Email

Oversize Action *
Overwrite the oldest event log

UI Setting	Description	Valid Range	Default Value
Capacity Warning	Enable or disable capacity warnings for the selected event log category.	Enabled / Disabled	Disabled
Warning Threshold	Specify the threshold percentage for the selected event log category. Once event log storage exceeds this percentage, the warning will trigger.	50 to 100 %	50
Registered Action	Select how the warning is sent. You can select multiple options. **Trap**: A trap warning will be sent. **Email**: A warning email will be sent.	Trap / Email	Trap / Email
Oversize Action	Select the oversize action to take when event log storage is full for the selected category. **Overwrite the oldest event log**: The oldest events will be deleted when new events are created. **Stop recording event logs**: No new events will be recorded.	Overwrite the oldest event log / Stop recording event logs	Overwrite the oldest event log

Event Notifications

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications

This page lets you configure notifications for various kinds of events.

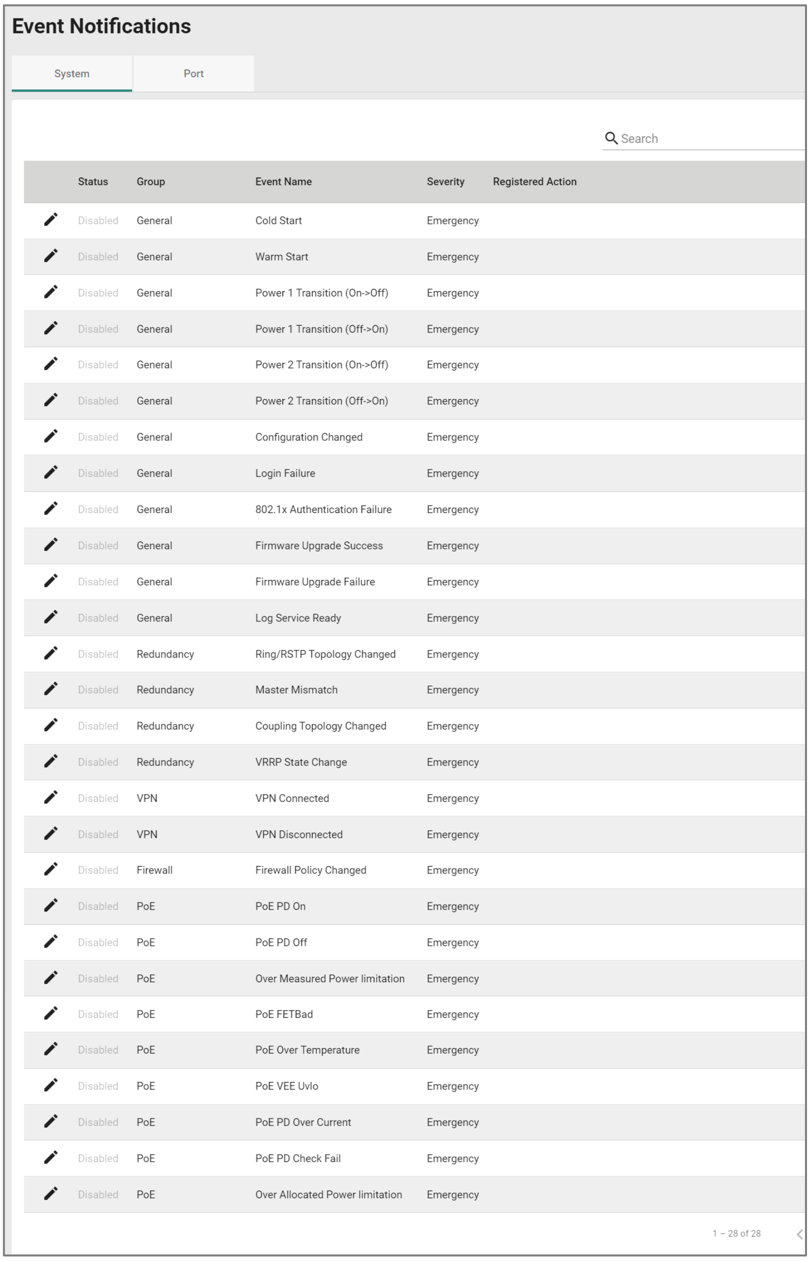
This page includes these tabs:

- System
- Port

Event Notifications - System

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - System

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

	Status	Group	Event Name	Severity	Registered Action
✎	Disabled	General	Cold Start	Emergency	
✎	Disabled	General	Warm Start	Emergency	
✎	Disabled	General	Power 1 Transition (On->Off)	Emergency	
✎	Disabled	General	Power 1 Transition (Off->On)	Emergency	
✎	Disabled	General	Power 2 Transition (On->Off)	Emergency	
✎	Disabled	General	Power 2 Transition (Off->On)	Emergency	
✎	Disabled	General	Configuration Changed	Emergency	
✎	Disabled	General	Login Failure	Emergency	
✎	Disabled	General	802.1x Authentication Failure	Emergency	
✎	Disabled	General	Firmware Upgrade Success	Emergency	
✎	Disabled	General	Firmware Upgrade Failure	Emergency	
✎	Disabled	General	Log Service Ready	Emergency	
✎	Disabled	Redundancy	Ring/RSTP Topology Changed	Emergency	
✎	Disabled	Redundancy	Master Mismatch	Emergency	
✎	Disabled	Redundancy	Coupling Topology Changed	Emergency	
✎	Disabled	Redundancy	VRRP State Change	Emergency	
✎	Disabled	VPN	VPN Connected	Emergency	
✎	Disabled	VPN	VPN Disconnected	Emergency	
✎	Disabled	Firewall	Firewall Policy Changed	Emergency	
✎	Disabled	PoE	PoE PD On	Emergency	
✎	Disabled	PoE	PoE PD Off	Emergency	
✎	Disabled	PoE	Over Measured Power limitation	Emergency	
✎	Disabled	PoE	PoE FETBad	Emergency	
✎	Disabled	PoE	PoE Over Temperature	Emergency	
✎	Disabled	PoE	PoE VEE Uvlo	Emergency	
✎	Disabled	PoE	PoE PD Over Current	Emergency	
✎	Disabled	PoE	PoE PD Check Fail	Emergency	
✎	Disabled	PoE	Over Allocated Power limitation	Emergency	

1 – 28 of 28

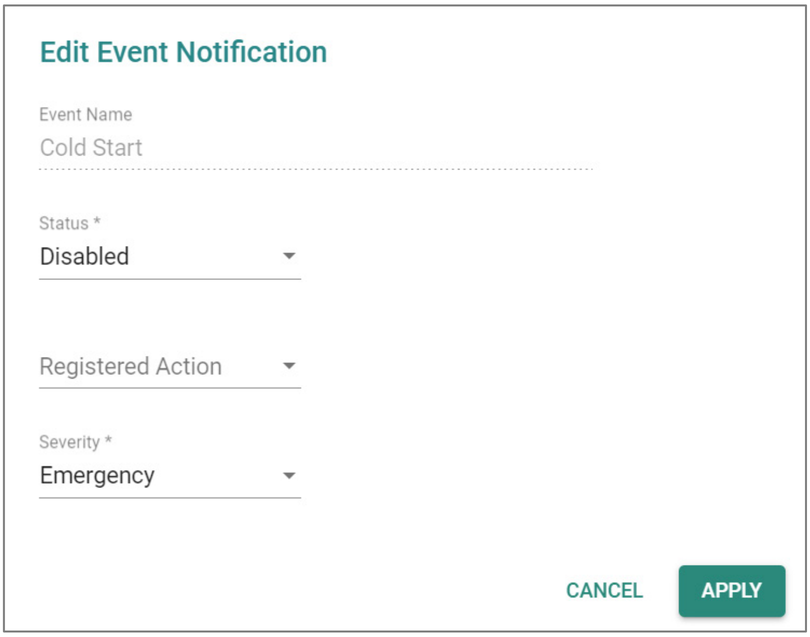
UI Setting	Description
Status	Shows whether event notifications are enabled for this kind of event.
Group	Shows which group this event belongs to.
Event Name	Shows the name of the event. Refer to the System Event List for more details.

UI Setting	Description
Severity	Shows the severity assigned to the event. Refer to Appendix > Severity Level List for more information about severity levels.
Registered Action	Shows which action will be taken for this kind of event. **Trap**: The notification is sent to the Trap server when the event is triggered. **Email**: The notification is sent to the email server defined in the Email Settings section. **Syslog**: The event log is recorded to a Syslog server defined in the Syslog section.

Event Notifications - System - Edit Event Notification

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - System

Clicking the **Edit (✎)** icon for an entry on the **Diagnostics > Event Logs and Notifications > Event Notifications - System** page will open this dialog box. This dialog lets you change the notification settings for the selected event. Click **APPLY** to save your changes.



Edit Event Notification

Event Name: Cold Start

Status *: Disabled

Registered Action

Severity *: Emergency

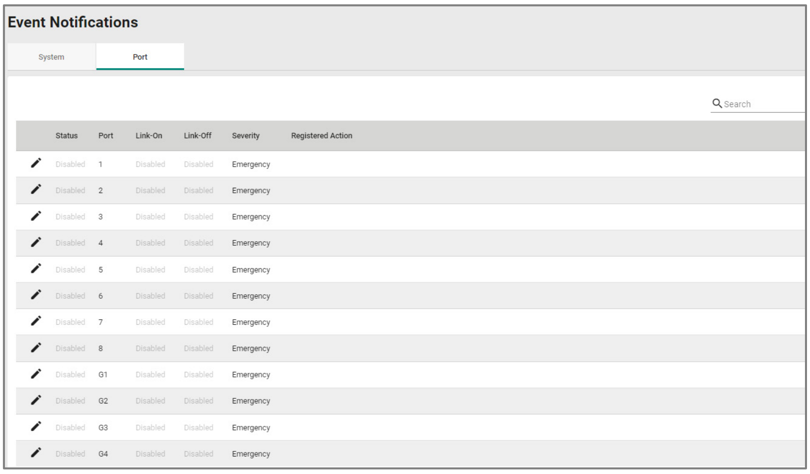
UI Setting	Description	Valid Range	Default Value
Event Name (View-only)	Shows the name of the event. Refer to the System Event List for more information.	(Fixed)	(Fixed)
Status	Enable or disable notifications for this event.	Enabled / Disabled	Disabled
Registered Action	Select which action to take when 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. **Syslog**: The event log is recorded to a Syslog server defined in the Syslog section. **Relay**: An alarm notification will be triggered through the relay output of the device, if your device is equipped with one.	Trap / Email / Syslog / Relay	N/A
Severity	Select the severity to assign for this event. Refer to Appendix > Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency

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.



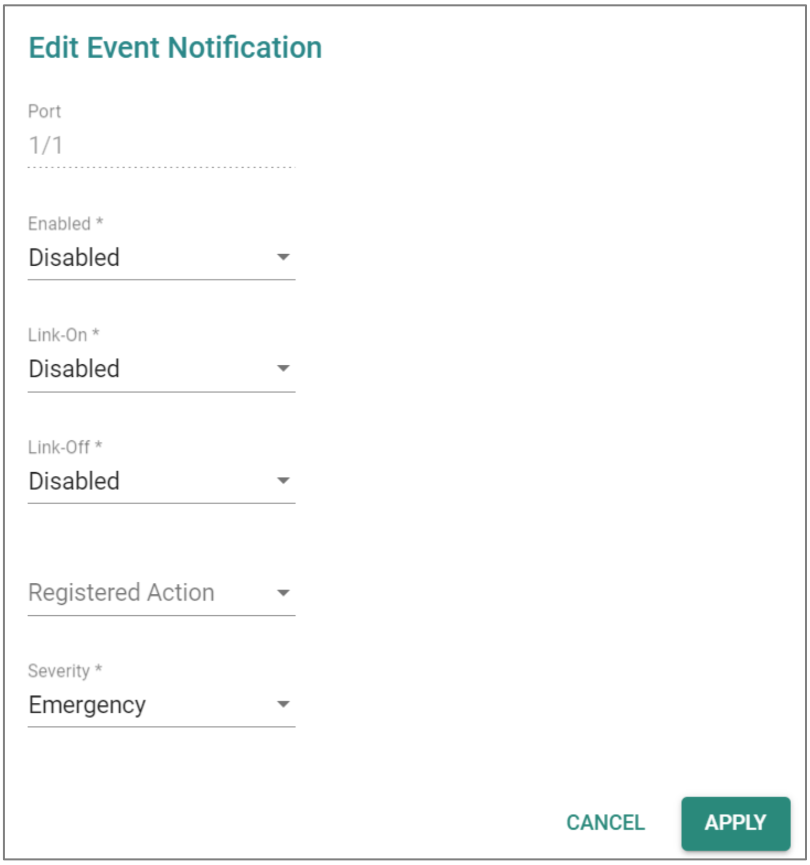
	Status	Port	Link-On	Link-Off	Severity	Registered Action
✎	Disabled	1	Disabled	Disabled	Emergency	
✎	Disabled	2	Disabled	Disabled	Emergency	
✎	Disabled	3	Disabled	Disabled	Emergency	
✎	Disabled	4	Disabled	Disabled	Emergency	
✎	Disabled	5	Disabled	Disabled	Emergency	
✎	Disabled	6	Disabled	Disabled	Emergency	
✎	Disabled	7	Disabled	Disabled	Emergency	
✎	Disabled	8	Disabled	Disabled	Emergency	
✎	Disabled	G1	Disabled	Disabled	Emergency	
✎	Disabled	G2	Disabled	Disabled	Emergency	
✎	Disabled	G3	Disabled	Disabled	Emergency	
✎	Disabled	G4	Disabled	Disabled	Emergency	

UI Setting	Description
Status	Shows whether event notifications are enabled for this kind of event.
Port	Shows which group this event belongs to.
Link-On	Shows whether notifications for Link-On events are enabled or disabled.
Link-Off	Shows whether notifications for Link-Off events are enabled or disabled.
Severity	Shows the severity assigned to the event. Refer to Appendix > Severity Level List for more information about severity levels.
Registered Action	Shows how notifications will be sent for this kind of event.

Event Notifications - Port - Edit Event Notification

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - Port

Clicking the **Edit (✎)** icon for an entry on the **Diagnostics > Event Logs and Notifications > Event Notifications - System** page will open this dialog box. This dialog lets you change the notification settings for the selected port. Click **APPLY** to save your changes.



Edit Event Notification

Port
1/1

Enabled *
Disabled

Link-On *
Disabled

Link-Off *
Disabled

Registered Action

Severity *
Emergency

UI Setting	Description	Valid Range	Default Value
Port (View-only)	Shows which physical port the event notifications are for. **Note** Available ports will vary depending on your product and model.	N/A	N/A
Status	Enable or disable notifications for this port.	Enabled / Disabled	Disabled
Link-On	Enable or disable notifications for Link-On events. If enabled, an event will be triggered when a device connects to the port.	Enabled / Disabled	Disabled
Link-Off	Enable or disable notifications for Link-Off events. If enabled, an event will be triggered when the port is disconnected from a device, such as when a cable is unplugged or the connected device is shut down.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Registered Action	Select which action 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. **Syslog**: The event log is recorded to a Syslog server defined in the Syslog section. **Relay**: An alarm notification will be triggered through the relay output of the device, if your device is equipped with one.	Trap / Email / Syslog / Relay	N/A
Severity	Select the severity to assign for this event. Refer to Appendix > Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency

Syslog

Menu Path: Diagnostics > Event Logs and Notifications > Syslog

This page lets you configure your device to connect to syslog servers to store event logs. When an event occurs, an event notification can be sent as a syslog UDP packet to the 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 by searching the approved certificate pool on the server to identify the imported certificate.

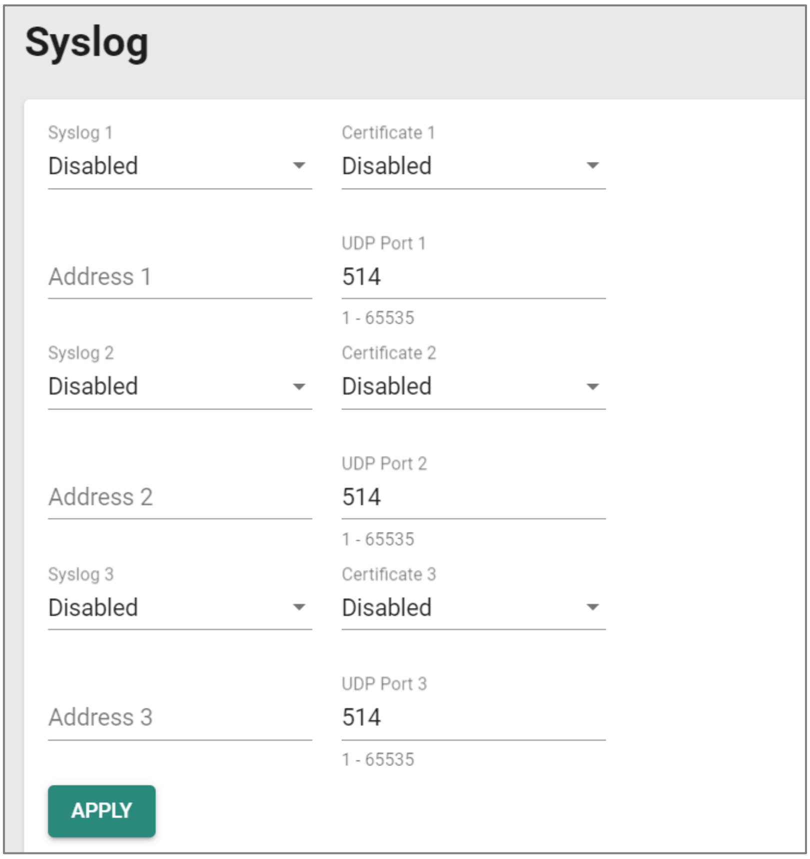
Attention

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.

Limitations

You can connect to up to 3 syslog servers.



Syslog

Syslog 1: Disabled
Certificate 1: Disabled
Address 1
UDP Port 1: 514 (1 - 65535)

Syslog 2: Disabled
Certificate 2: Disabled
Address 2
UDP Port 2: 514 (1 - 65535)

Syslog 3: Disabled
Certificate 3: Disabled
Address 3
UDP Port 3: 514 (1 - 65535)

UI Setting	Description	Valid Range	Default Value
Syslog	Enable or disable the specified syslog server.	Enabled / Disabled	Disabled
Certificate	Select a syslog server certificate to use for the related server, or disable use of certificates.	Drop-down list of certificates / Disabled	Disabled
Address	Enter the IP address of the related syslog server.	Valid IP address	N/A
UDP Port	Specify the UDP port of the related syslog server.	1 to 65535	514

SNMP Trap/Inform

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform

This page lets you configure the SNMP Trap/Inform notification feature.

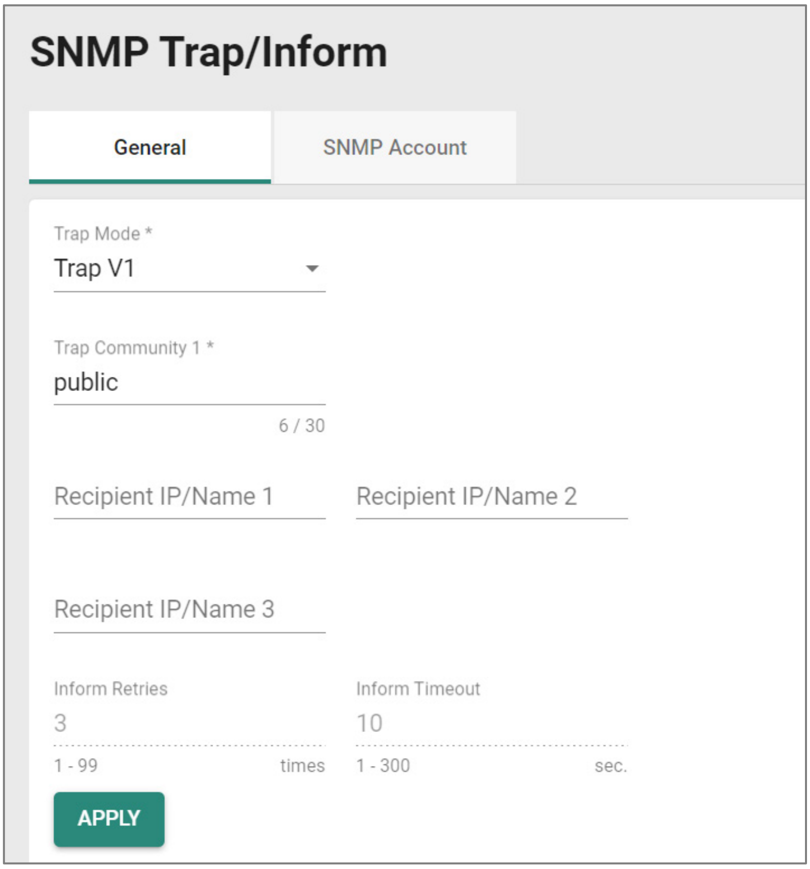
This page includes these tabs:

- General
- SNMP Account

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

Trap Mode *
Trap V1

Trap Community 1 *
public
6 / 30

Recipient IP/Name 1

Recipient IP/Name 2

Recipient IP/Name 3

Inform Retries
3
1 - 99 times

Inform Timeout
10
1 - 300 sec.

UI Setting	Description	Valid Range	Default Value
Trap 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 V2**: Use Trap V2 for SNMP notifications. **Inform V2**: 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	Trap V1
Trap Community 1	Specify the community string that will be used for authentication.	1 to 30 characters	public
Recipient IP/Name 1/2/3	Specify the name of the recipient trap server that will receive notifications.	Recipient IP or name	N/A

UI Setting	Description	Valid Range	Default Value
Inform Retries **(if Trap Mode is Inform V2 or Inform V3)**	Specify the number of times to retry sending an inform notification.	1 to 99	3
Inform Timeout **(if Trap Mode is Inform V2 or Inform V3)**	Specify the amount of time to wait (in seconds) to wait for an acknowledgement before trying to resend an inform notification.	1 to 300	10

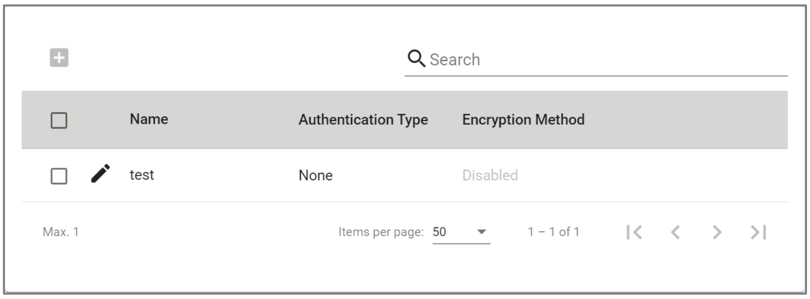
SNMP Account

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Account

This section lets you configure an SNMP trap account for your device.

Limitations

You can configure up to 1 SNMP trap account.



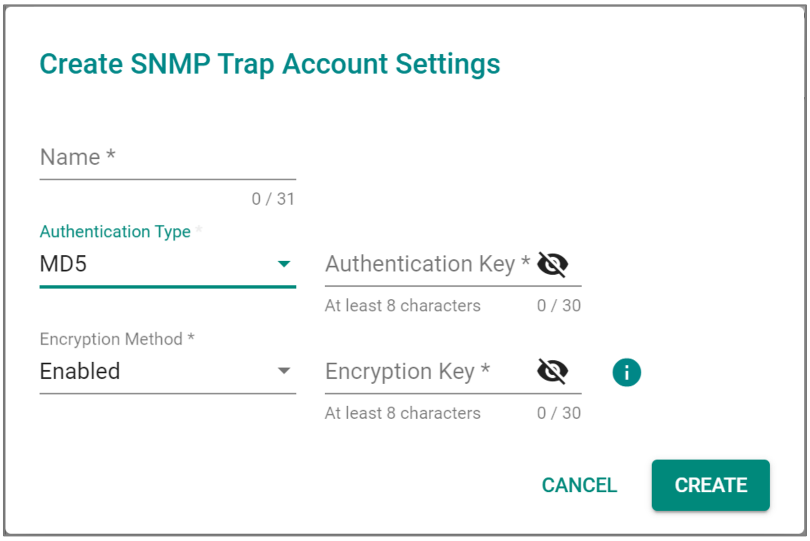
□	Name	Authentication Type	Encryption Method
□	test	None	Disabled

UI Setting	Description
Name	Shows the name of 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.

Create SNMP Trap Account Settings

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Account

Clicking the **Add (** ⊞ **)** icon on the **Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Account** 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.



Create SNMP Trap Account Settings

Name *

0 / 31

Authentication Type

MD5

Authentication Key *

At least 8 characters 0 / 30

Encryption Method *

Enabled

Encryption Key *

At least 8 characters 0 / 30

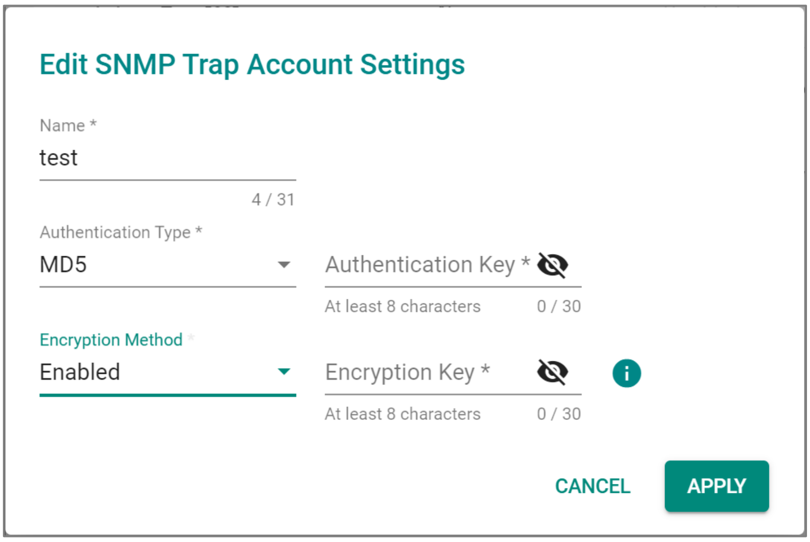
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the account.	1 to 31 characters	N/A
Authentication Type	Select which authentication method to use for the account. **None**: No authentication will be used. **MD5**: Use MD5 authentication. **SHA**: Use SHA authentication.	None / MD5 / SHA	None
Authentication Key **(if Authentication Type is MD5 or SHA)**	Specify an authentication key to use for the account.	8 to 30 characters	N/A

UI Setting	Description	Valid Range	Default Value
Encryption Method	Enable or disable AES encryption for the account.	Enabled / Disabled	Disabled
Encryption Key **(if Encryption Method is Enabled)**	Specify an encryption password for the account.	8 to 30 characters	N/A

Edit SNMP Trap Account Settings

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Account

Clicking the **Edit (✎)** icon for an entry on the **Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Account** page will open this dialog box. This dialog lets you modify an existing SNMP trap account. Click **APPLY** to save your changes.



Edit SNMP Trap Account Settings

Name *: test (4 / 31)

Authentication Type *: MD5

Authentication Key * (At least 8 characters, 0 / 30)

Encryption Method *: Enabled

Encryption Key * (At least 8 characters, 0 / 30)

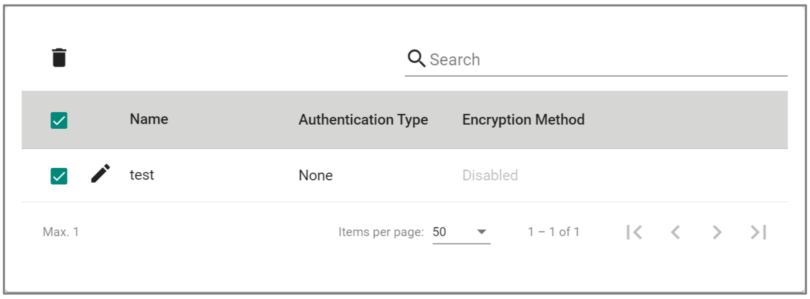
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the account.	1 to 31 characters	N/A

UI Setting	Description	Valid Range	Default Value
Authentication Type	Select which authentication method to use for the account. **None**: No authentication will be used. **MD5**: Use MD5 authentication. **SHA**: Use SHA authentication.	None / MD5 / SHA	None
Authentication Key **(if Authentication Type is MD5 or SHA)**	Specify an authentication key to use for the account.	8 to 30 characters	N/A
Encryption Method	Enable or disable AES encryption for the account.	Enabled / Disabled	Disabled
Encryption Key **(if Encryption Method is Enabled)**	Specify an encryption password for the account.	8 to 30 characters	N/A

Delete SNMP Trap Account

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Account

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



☑	Name	Authentication Type	Encryption Method
☑	test	None	Disabled

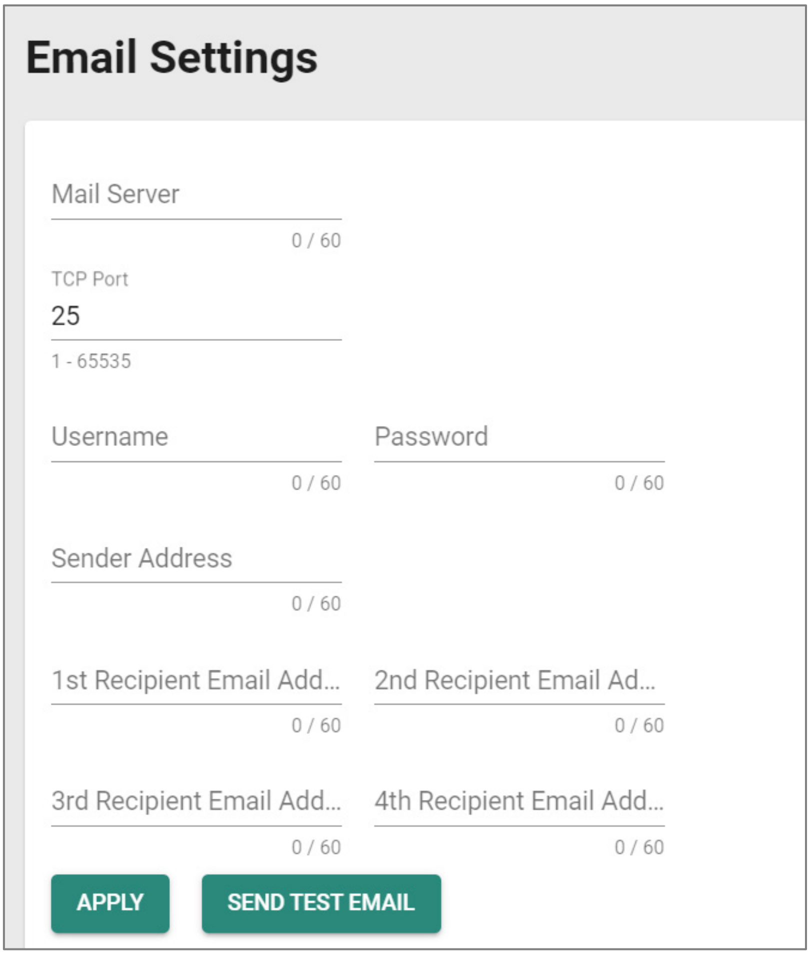
Email Settings

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, or click **SEND TEST MAIL** to send a test email using the current settings and recipients.

Auto warning email messages will be sent through an authentication-protected SMTP server that supports CRAM-MD5, LOGIN, and PAIN methods of SASL (Simple Authentication and Security Layer) authentication.

We strongly recommend not entering your Account Name and Account Password if auto warning e-mail messages can be delivered without using an authentication mechanism.



Email Settings

Mail Server
0 / 60

TCP Port
25
1 - 65535

Username
0 / 60

Password
0 / 60

Sender Address
0 / 60

1st Recipient Email Add...
0 / 60

2nd Recipient Email Ad...
0 / 60

3rd Recipient Email Add...
0 / 60

4th Recipient Email Add...
0 / 60

UI Setting	Description	Valid Range	Default Value
Mail Server	Specify the address of the email server. You can enter a domain name or IP address.	1 to 60 characters	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
Sender Address	Specify the sender email address to use for email notifications.	0 to 60 characters	N/A
Recipient Email Address	Enter an email address to send email notifications to. You can set up to 4 email addresses to receive email notifications.	0 to 60 characters	N/A

Tools

Menu Path: Main > Diagnostics > Tools

This section lets you use various tools to check for network issues.

This section includes these pages:

- Port Mirroring
- Ping

Port Mirroring

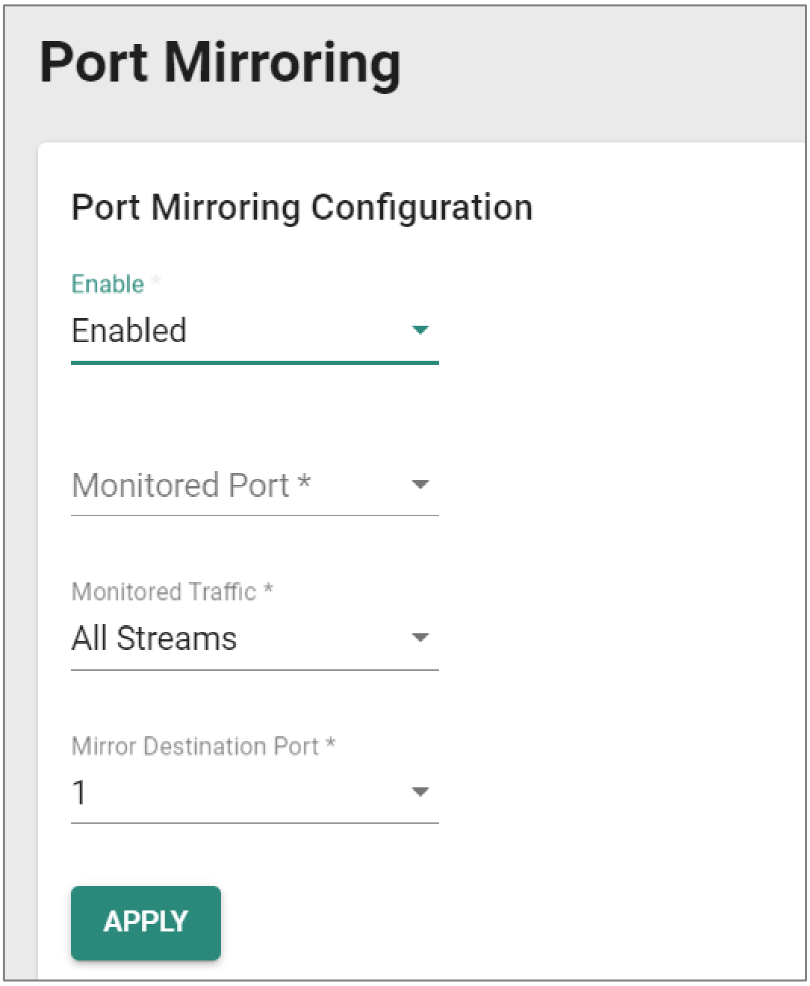
Menu Path: Main > Diagnostics > Tools > Port Mirroring

This page lets you configure the port mirror function, which can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the mirror port) to receive the same data being transmitted from, or both to and from, the port under observation.

Using a mirror port allows the network administrator to sniff the observed port to keep tabs on network activity.

Note

For security reasons, it is recommended to use port mirroring to send traffic to an intrusion detection system (IDS) for analysis.



Port Mirroring

Port Mirroring Configuration

Enable *: Enabled

Monitored Port *

Monitored Traffic *: All Streams

Mirror Destination Port *: 1

UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable the port mirror function.	Enabled / Disabled	Disabled

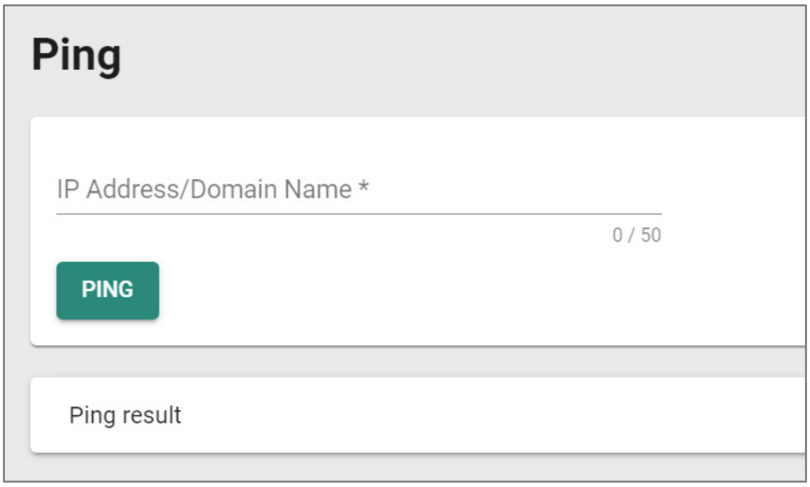
UI Setting	Description	Valid Range	Default Value
Monitored Port	Select the numbers for the ports you want to monitor for network activity. Multiple ports can be selected.	(Selectable ports will vary depending on the device model)	N/A
Monitored Traffic	Select the type of traffic that will be monitored. **Ingress Stream**: Select this option to monitor only those data packets coming into the Moxa industrial secure router's port. **Egress Stream**: Select this option to monitor only those data packets being sent out through the Moxa industrial secure router's port. **All Streams**: Select this option to monitor data packets both coming into and being sent out through the Moxa industrial secure router's port.	Ingress Stream / Egress Stream / All Streams	All Streams
Mirror Destination Port	Select the number of the port that will be used to monitor the activity of the monitored port.	(Selectable ports will vary depending on the device model)	1

Ping

Menu Path: Main > Diagnostics > Tools > Ping

This page lets you use the ping function, which is useful for troubleshooting network problems.

The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from the device itself. In this way, you can use your device to send ping commands out through its ports.



Ping

IP Address/Domain Name *

0 / 50

PING

Ping result

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. The ping result will be displayed below.	Valid IP address or domain name up to 50 characters	N/A

Chapter 4

Other Features

Other Features

This section covers other features of your device that may not have a related user interface.

The features in this section include:

- Firmware Image Recovery

Firmware Image Recovery Overview

Firmware Image Recovery refers to the use of multiple copies of firmware within a device to increase reliability and reduce the risk of system failure due to firmware corruption or errors.

In many electronic devices, firmware is stored in non-volatile memory such as flash memory, and any corruption or errors in the firmware can result in the device malfunctioning or becoming unusable. To mitigate this risk, firmware recovery involves storing multiple copies of the firmware within the device, and using a mechanism to switch to a backup copy of the firmware in case the primary copy becomes corrupted or fails.

Overall, Firmware Image Recovery is a useful technique for increasing the reliability and availability of electronic devices, particularly those used in critical applications where system failure can have serious consequences.

Methodology

This device supports a "Dual-image" firmware mechanism to minimize the possibility of system failure, such as in the following situations:

1. When the user encounters an accident when upgrading the device firmware, such as

a power outage, which may cause firmware corruption.

2. When the memory encounters lifespan issues or damage from external factors, parts of partitions may become corrupted.

This mechanism involves storing two copies of the firmware in separate memory partitions within the device, and using a boot loader to select the active copy at runtime. If a situation occurs, the firmware can still roll back to the previous version to boot the device.

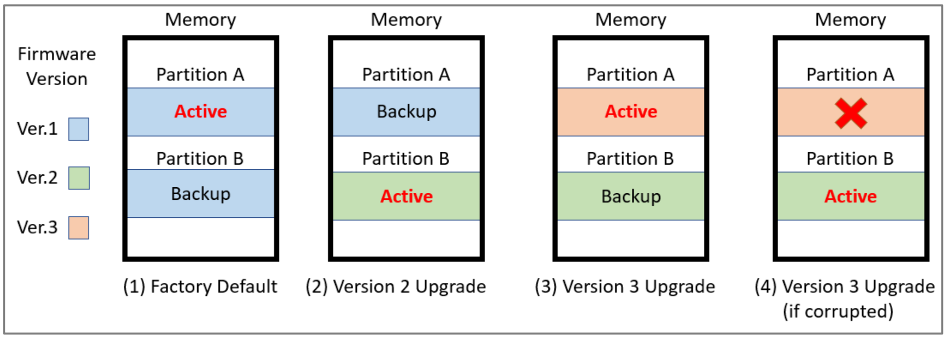
Warning

Firmware Image Recovery will not be able to help if the bootloader sector or the entire memory is corrupted.

How Dual-imaging Works

Here is an overview of how the Dual-image function works.

1. When the product leaves the factory, it will keep two identical copies of the firmware version 1 in separate memory partitions A and B within the device. Partition A will be selected as the active copy by default.
2. When the user upgrades the firmware version 2, Partition B will be overwritten to store the new image as well as be selected as the active copy at the same time. Partition A will keep a previous version 1 as a backup.
3. When the user upgrades the firmware version 3, Partition A will be overwritten to store the new image as well as be selected as the active copy at the same time. Partition B will keep a previous version 2 as a backup.
4. Based on (3), if the user encounters an accident when upgrading the firmware version 3 and Partition A is corrupted, the bootloader will choose backup Partition B as the active one to continue to boot the system and the system will record a “Boot Failed, Fallback to Previous Firmware” event into the system logs.



Note

- Resetting the device to factory default settings only restores user configurations, and will not restore the firmware image in both partitions.

- This mechanism is done automatically by the system and is not user-configurable.

Chapter 5

Security

Security

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.

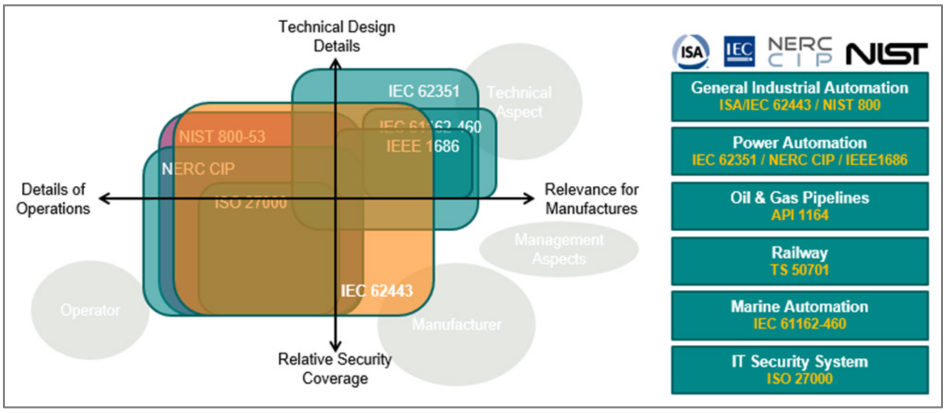
It is crucial to understand that no single protection can guarantee complete security. That's why the Defense-in-Depth approach makes it difficult for attackers to leverage one weakness to attack the product or network as a whole. This approach requires attackers to overcome multiple obstacles undetected, increasing the difficulty level. By leveraging multiple security features and layers of protection in a product, vulnerabilities in any one layer can be mitigated.

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.

Security Standards and Vertical Markets



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.

Breakdown of ISA/IEC 62443

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 life ycle and use-cases
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

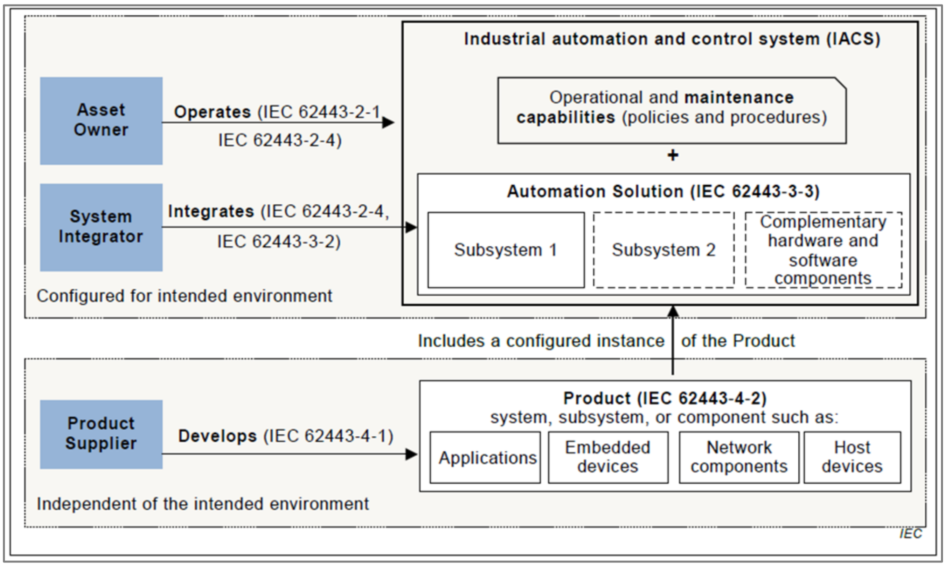
These standards help integrators:

- Determine security zones
- Specify security capability levels for each zone
- Integrate products into an Automation Solution

Key parts of ISA/IEC 62443 Standard

Parts of the ISA/IEC 62443 Standard	Technical Security Requirements
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)

Once the solution is ready, it's installed on-site, becoming a vital part of the IACS.


Industrial automation and control system (IACS)
Asset Owner
Operates (IEC 62443-2-1, IEC 62443-2-4)
Operational and maintenance capabilities (policies and procedures)
+
System Integrator
Integrates (IEC 62443-2-4, IEC 62443-3-2)
Automation Solution (IEC 62443-3-3)
Subsystem 1
Subsystem 2
Complementary hardware and software components
Configured for intended environment
Includes a configured instance
of the Product
Product Supplier
Develops (IEC 62443-4-1)
Product (IEC 62443-4-2)
system, subsystem, or component such as:
Applications
Embedded devices
Network components
Host devices
Independent of the intended environment
IEC

Establishing Foundational Requirements

ISA/IEC 62443-1-1 Foundational Requirements (FR)

FR 1	**Identification and Authentication Control**
FR 2	User Control
FR 3	System Integrity
FR 4	Data Confidentiality
FR 5	Restricted Data Flow
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.

Component Requirements (CR) and specific requirements

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.

FR 1 Example: 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 the system or assets.

Recognizing these distinct needs:

- **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 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 Levels (SLs) and Attack Types

Security Level	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

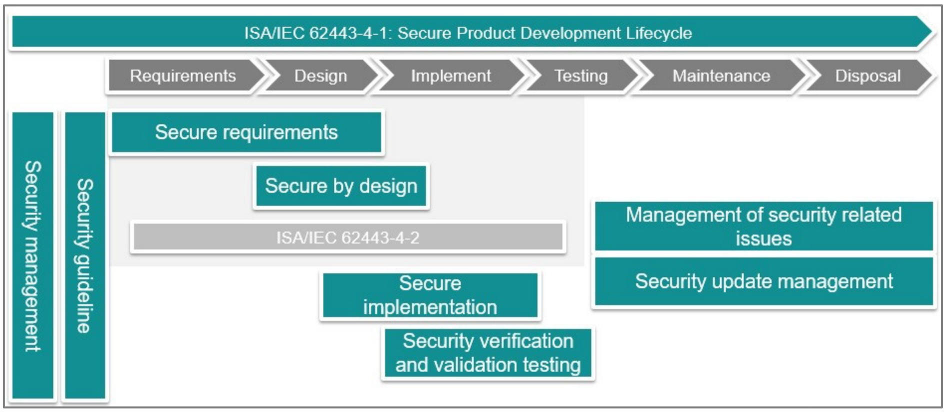
FR, CR and specific requirements

FR 1 - Identification and authentication control	CR 1.1 - Human user identification and authentication
CR 1.2 Software process and device identification and authentication	
CR 1.3 - Account management	
CR 1.4 Identifier management	
CR 1.5 - Authenticator management	
CR 1.6 - Wireless access management	NDR 1.6
CR 1.7 - Strength of password-based authentication	
CR 1.8 - Public key infrastructure certificates	
CR 1.9 - Strength of public key-based authentication	
1.10 - Authenticator feedback	
CR 1.11 - Unsuccessful login attempts	
CR 1.12 - System use notification	
CR 1.13 - Access via untrusted networks	NDR 1.13

Product Lifecycle and Security

Component security plays a role throughout the product lifecycle.

Moxa's Application of ISA/IEC 62443-4-1



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.

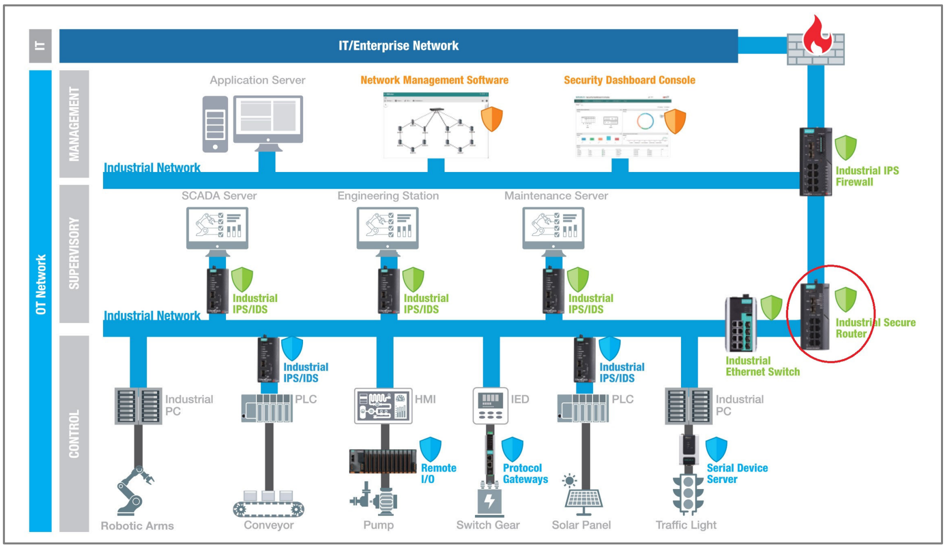
Component Security with IEC 62443-4-2

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.

Product Security Context

Security context describes a product's role in a network and the security features of its environment.

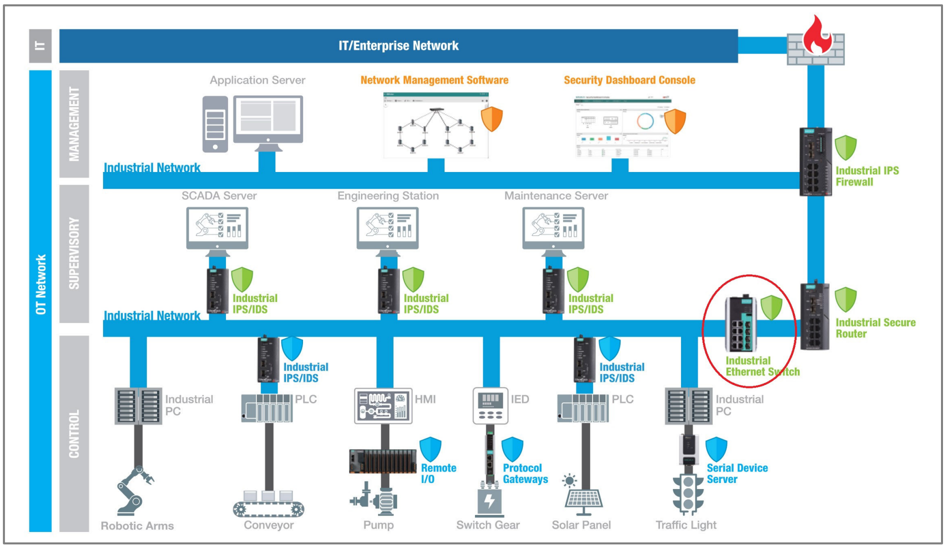
Security Context of an Industrial Secure Router



A secure router is a router with security features. Unlike a firewall—which exclusively filters and controls traffic—a secure router also monitors connections between devices. Secure routers have additional security features such as intrusion detection/prevention systems (IDS/IPS), virtual private network (VPN) support, and advanced encryption capabilities.

Secure router Intrusion Detection Systems (IDS) can be deployed behind the firewall for a defense-in-depth approach, increasing detection of attacks bypassing first-layer firewalls.

Security Context of an Industrial Ethernet Switch



Switches with enhanced security features such as access control lists (ACLs), VLAN support, and support for secure communication protocols, in conjunction with other security measures, can help create a more robust and resilient network.

ACLs and VLANs can help isolate devices on the same physical or logical network segments. This isolation adds further security to minimize or mitigate the effects of an attack.

Security Best Practices

Product Security

This section provides essential information on the installation of your product.

Guidelines for Physical Installation

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 switch/router in an access-controlled area. To further protect your device from potential physical attacks, it is important to implement appropriate physical security measures. This may include CCTV surveillance, security guards, locks, 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.
- Deactivate any ports that are not currently in use. Fewer active ports represent fewer avenues of attack. Refer to Network Interfaces for more information.

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.
- Update passwords regularly
- Never share passwords

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. Use HTTPS instead of HTTP, SSH instead of Telnet, SFTP instead of TFTP, and SNMPv3 instead of SNMPv1/v2c. Refer to Network Interfaces for more information.
- Generate new SSL certificates and SSH keys for devices prior to using HTTPS or SSH applications. Refer to SSH & SSL for more information.

Maintaining Communication Integrity

Ensure that information sent is accurate, complete, and secure.

Maintaining communication integrity reduces risks risk of data corruption or interception, and associated security breaches, data loss, and other negative effects on networks and their users.

- Use encryption.

  Encryption uses mathematical algorithms to convert data into a secret code, making it extremely difficult for people without the correct codes to read or change the data. By using encryption, you can ensure that the data being transmitted is secure and cannot be intercepted by unauthorized users.

- Use digital signatures.

  Digital signatures verify the authenticity and integrity of digital documents or messages. Using a digital signature, you can ensure that the message or document came from the expected sender and has not been altered.

- Implement access control.

  Access control restricts access to only authorized users to the network and its resources. By implementing access control measures, such as firewalls or access control lists, you can prevent unauthorized access and reduce the risk of data breaches.

Communication Integrity Features

Moxa devices provide support for VPNs and secure versions of protocols to help maintain communication integrity.

VPN (Virtual Private Network)

VPN is a secure network connection allowing users to access a private network. VPNs use encryption and authentication to protect the data in transit, which makes it difficult for anyone to intercept or tamper with the data. VPNs also provide access control features to ensure only authorized users can access the network. VPNs are commonly used to securely connect remote workers to a company network securely or to allow secure access to restricted resources over the internet.

Refer to VPN for more information.

HTTPS (Hypertext Transfer Protocol Secure)

HTTPS is a secure version of the regular HTTP protocol for transmitting data over the internet. HTTPS uses TLS (Transport Layer Security) encryption and digital certificates to protect the data in transit from interception, tampering, or eavesdropping.

Refer to Management Interface for more information.

SSH (Secure Shell)

SSH is a secure protocol for remote terminal login and secure file transfers. SSH uses encryption to protect the data in transit, making it difficult for anyone to intercept or tamper with it. SSH also provides authentication and access control features to ensure only authorized users can access the network.

Refer to Management Interface for more information.

SFTP (Secure File Transfer Protocol)

SFTP is a secure version of FTP (File Transfer Protocol) that uses encryption to protect the data in transit. SFTP also provides authentication and access control features to ensure only authorized users can access the network.

Refer to Management Interface for more information.

SNMP v3 (Simple Network Management Protocol version 3)

SNMP v3 is a secure version of the SNMP protocol used for network management and monitoring. SNMP v3 uses encryption and authentication to protect the data in transit, making it difficult for anyone to intercept or tamper with it. SNMP v3 also provides access control features to ensure only authorized users can access the network.

Refer to SNMP for more information.

Device Resource Management and Monitoring

Moxa devices provide a number of features to help customers manage device resources efficiently and monitor security.

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.

Event Logs

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.

Moxa devices offer three kinds of logs:

- System Logs, showing details of all system-related event logs
- Firewall logs, showing details of all patterns from layers 3-7, including
  - Trusted Access
  - Malformed Packets
  - DoS Policy
  - Layer 3 – 7 Policy
  - Protocol Filter Policy
  - Anomaly Detection & Protection (ADP)
  - Intrusion Detection/Prevention System (IDS/IPS)
  - Session Control
- VPN logs, showing all VPN-related events

Related information:

- Event Log
- Event Notifications
- SNMP

Denial of Service (DoS) Protection

In a denial-of-service (DoS) attack, the attacker attempts to overwhelm a target system with a flood of traffic or requests. The deluge of traffic causes the target system to become paralyzed, and also causes disruptions in networks and online services.

Moxa devices can prevent several types of DoS attacks by rejecting requests which ask for a particular network scan, or rejecting too many such requests in a specified period..

Refer to DoS Policy for more information.

Session Control

Session control refers to managing communication sessions between network objects, such as IP addresses or ports. The management process involves establishing, maintaining, and terminating sessions to ensure secure and reliable communication between various objects. Session control allows administrators to allocate device resources more efficiently by limiting the number of active sessions, and improving network security by dropping unused sessions.

Refer to Session Control 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.

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.

Service Name	Default Port	Default Setting	Security Suggestions
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	By default, logs are stored in the device, but limited local storage limits the number of saved logs, resulting in missed logs for critical incidence. Sending logs to an external log server can mitigate limitation, decreasing the chance of missing critical logs.
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
Firewall	Deny All	Without precise firewall rules configuration, "Allow All" has a higher change to allow unwanted packets going into the protected network, so we highly suggest using "Deny All" instead of "Allow All". Refer to Scenario: Airport Integrated Solutions to learn more about Allow Lists.
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.

Security-Related Functions Function	Default Setting	Security Suggestions
802.1X over ports	Disable	Enable 802.1X port authentication to block unauthorized LAN access.
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.

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.

Related information:

- User Interface
- DoS Policy
- Time

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:

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.

Related information:

- User Accounts

Recommended Patching and Backup Practices

Moxa's guidance on ensuring device security through regular firmware upgrades and configuration backups.

Firmware Upgrade

Moxa continuously releases firmware throughout the product lifecycle to improve features and rectify identified issues. Upon discovering a vulnerability, our approach aligns with the Moxa Product Security Incident Response Team (PSIRT) guidelines, ensuring swift and appropriate action.

Maintaining current firmware on your network devices is vital to maintain security. Using outdated firmware can expose the device to potential threats. We strongly advise periodic firmware updates. We consistently release the latest firmware and software on our official website, along with respective release notes. Check for these updates regularly.

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.

Related information:

- Firmware Upgrade
- Configuration Backup and Restore

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 of Moxa products, please submit your findings on the following web page: https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability.

To find the updated Moxa security information, please visit our 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.

Using Security Features

Introduction IPS

IPS (Intrusion Prevention System) is a network security technology used to detect and prevent potential threats in a network.

IPS analyzes the network traffic and identifies potential attacks, including viruses, worms, malware, and unauthorized access. Once an IPS detects a threat, it takes immediate action to block the attack and protect the security of the network and system. IPS uses signature-based and behavior analysis to identify threats and employs various techniques to protect systems, such as blocking IP addresses and protocols. It is an important component of network security architecture designed to enhance the security of networks and systems, prevent unauthorized access, and protect against data breaches.

What is the difference between IDS and IPS?

IDS (Intrusion Detection System) and IPS are network security systems that help protect against security threats and vulnerabilities.

An IDS monitors network traffic and identifies potential security threats and attacks. When it detects a security threat, it saves logs and generates an alert, which is sent to the security team for further analysis and action. An IDS is a passive security system that only monitors network traffic and does not take any action to prevent or stop an attack.

On the other hand, an IPS monitors network traffic like an IDS, but also takes active measures to prevent security threats and attacks. Additionally, an IPS can block, quarantine, or even terminate network traffic or connections deemed suspicious or malicious. IPS systems often use a set of predefined rules or policies to identify and respond to security threats in real-time.

The main difference between IDS and IPS is that IDS only detects and notifies of potential security threats, while IPS takes action to prevent and stop the security threat. IDS is generally considered a more passive security system, whereas IPS is more proactive and can take immediate action to mitigate security risks.

IPS Applications

IPS is typically used to actively prevent and block unauthorized access or malicious activities on your network.

IPS is typically used when you want to actively prevent and block unauthorized access or malicious activities on your network. It's a proactive security solution that acts in real-time to prevent potential security threats from entering or leaving your network.

Here are some common applications of IPS:

- Protecting critical assets: IPS can protect mission-critical assets or systems, such as PLCs, factory automation, ICS (Industrial Control System), from external and internal security threats.
- Resisting zero-day attacks: IPS can help you detect and block unknown or zero-day attacks that have not yet been identified by traditional anti-virus or intrusion detection systems.
- Real-time threat detection: IPS systems can provide real-time threat detection and prevention, reducing the risk of data breaches and other security incidents.
- Virtual patching: Even devices with outdated OS can receive up-to-date protection without regular security updates and patches.

In summary, IPS should be used when you want to actively prevent and block security threats in real-time and protect critical assets or comply with specific regulations or standards.

IPS Limitations

The most notable limitation of IPS is that it relies on updated patterns—updated definitions and countermeasures of known threats—to correctly detect and act on threats. To address this issue, Moxa provides regular updates in the form of a security package.

Example: Updating the Network Security Package via the Web GUI

Download the latest Network Security Package from the Moxa and install via the Web GUI.

Before you begin: Make sure you have purchased an activated an IPS license.

This task uses the Moxa EDR-G9010 series as an example product. Replace this product with your product for each step.

1. From the Moxa support website, navigate to **Resources→Software**

Packages→Network Security Package for EDR-G9010 Series

2. The Moxa support website is located at https://www.moxa.com/en/support.
3. Download the latest version of the Network Security Package to your computer.
4. Open the router's web interface and navigate to **System→System Management→Software Package Management→Network Security Package**.
5. Click **Source**, and then choose **Local**.
6. Click **Select Files**, and then choose a file from your local file system.
7. Click **Upgrade** to start the upgrade process.

The upgrade process will begin, and the result appears at the bottom of the interface.

What to do next:

Confirm that the Network Security Package has been updated by checking the version information from the Package Information Screen. On the web interface, go to **Firewall→Advanced Protection→Information→Package Information**, and check the version listed.

Example: Updating the Network Security Package via MXsecurity

Download the latest Network Security Package from the Moxa website and install with the MXsecurity web console.

Before you begin: Make sure you have purchased an activated an IPS license.

This task uses the Moxa EDR-G9010 series as an example product. Replace this product with your product for each step.

1. From the Moxa support website, navigate to **Resources→Software Packages→Network Security Package for EDR-G9010 Series**
2. The Moxa support website is located at https://www.moxa.com/en/support.
3. Download the latest version of the Network Security Package to your computer.

4. From the MXsecurity web console, go to **Device Deployment→Software Packages→Network Security Packages**.
5. Select the secure routers to update, and then click **Upgrade**.

Results: The upgrade process will begin on the selected routers, with the result displayed within seconds.

What to do next:

Confirm that the Network Security Package has been updated by checking the version information from the Package Information Screen. On the MXsecurity web console, go to **Device Deployment→Software Packages**, and check the version listed.

Example: Configuring IPS Rules via MXsecurity

Enable IPS rules and observe the generated event from the MXsecurity, the centralized cybersecurity visualization platform.

Before you begin: Make sure you have:

- a configured MXsecurity server
- an active IPS license that supports MXsecurity
- at least one Network Security Package uploaded. Refer to Example: Updating the Network Security Package via MXsecurity for upload steps.

1. From the MXsecurity web console, go to **Management→Policy Profile**.
2. Click [Add], and then configure:
   - **Profile Name**
   - **Description** (optional)
3. Select **IPS**, and then choose one of the **Package Versions** from the list.

4. Enable one or more IPS rules, then click **Apply**.

   You can choose **Select All** to enable all protection.

   Result: Your new policy profile is visible in the **Policy Profile** table.

5. To apply the profile, go to **Deployment**→**Policy Profile**.
6. Select the IPS profile, and then click **Apply**.

Results:

If an IPS event is triggered, you can go to **Logging**→**Firewall**→**IPS** to examine the events.

Example: Configuring IPS rules via WebGUI

Enable and configure IPS rules from device web interfaces.

Before you begin: Make sure you have:

- an active IPS license that supports device-based IPS

1. In the device UI, go to **Firewall**→**Advanced Protection**→**IPS**.
2. Identify rules to configure:

   Choose from:

   - Choose rules from the list
   - Filter rules by clicking [Filter]
   - Type search terms in the search box

3. Edit or enable rules by clicking [Edit], then setting **Status** to **Enabled**.

   You can toggle multiple rules by selecting them, and then clicking →**Quick Settings, and then setting Status to Enabled.**

Results: Selected rules will now be enabled.

What to do next: You can check the event log to verify to see actions taken by rules by going to **Diagnostics→Event Logs and Notifications→Event Log→Firewall Log.**

Introduction to Firewalls

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Its primary function is to create a barrier between a private internal network and the public internet, allowing only authorized traffic to pass through and blocking unauthorized access attempts. They use various techniques to filter network traffic, including packet filtering, stateful inspection, and application filtering. Firewalls are an essential component of network security and are used by individuals, small businesses, and large enterprises to protect their networks from various types of cyber threats, such as viruses, malware, hackers, and other malicious attacks.

Stateful vs. Stateless firewalls

Firewalls can be categorized as either stateful or stateless.

Stateless firewalls, also known as packet filtering firewalls, examine individual packets of data and enforce rules based on information in the packet header, such as source and destination IP addresses or port numbers. Stateless firewalls do not keep track of the state of connections and cannot distinguish between packets belonging to different connections.

Stateful firewalls, on the other hand, keep track of the state of connections and use this information to enforce rules. They can distinguish between packets belonging to different connections and apply more complex security policies. Stateful firewalls maintain a state table that tracks information such as source and destination IP addresses, port numbers, and connection status.

Overall, stateful firewalls offer more advanced security features and are generally more effective at protecting networks from threats. However, they also require more resources and may be more complex to configure and manage. Stateless firewalls are simpler and more lightweight, but may not provide as much protection against advanced threats.

Categories of Firewall

- Policy (L2,L3~L7) : A policy in firewall function is a set of rules and criteria that are used to determine how traffic is allowed or denied on a network. Firewall policies define the actions that the firewall should take when specific traffic matches the defined criteria.
- Malformed packet: The Malformed Packets function enables the device to record event logs with a user-specified severity whenever malformed packets are dropped by the system.
- Session control: Session control in a firewall is the process of tracking and controlling the flow of network traffic between two endpoints in a network session. Session control to help users protect backend hosts or services and avoid system abnormalities.
- DoS(Denial of Service) policy: The Industrial Secure Router provides 9 different DoS functions for detecting or defining abnormal packet formats or traffic flows. The Industrial Secure Router will drop packets when it either detects an abnormal packet format or identifies unusual traffic conditions.
- Protocol filter policy: The Industrial Secure Router supports industrial protocol filtering, allowing users to inspect network traffic based on specific protocols to detect anomalies and protect your network.

When to Use Firewalls

Firewalls are a fundamental component of network security and are used to protect networks from unauthorized access and cyber threats. It is a static system that filters traffic based on predefined rules, such as source/destination MAC, IP address or port.

1. Prevent unauthorized access to critical assets : Firewalls are used to prevent

unauthorized access to critical assets, such as a controller of a system, central monitor system.

2. Safeguarding sensitive data: Firewalls are used to safeguard sensitive data such as financial information, healthcare records, and production data.
3. Complying with regulations: Many industries are subject to regulations that require the use of firewalls to protect sensitive data.

In summary, firewalls are used to control traffic based on predefined rules and focus on access control. Firewalls are often used in combination with other network secure technique, like IPS (Intrusion Prevention System) to provide comprehensive protection against cyber threats.

Scenario: Airport Integrated Solutions

A network system provider is configuring a network for an airport.

Airports rely on intricate network systems to enhance efficiency, elevate safety measures, promote environmental sustainability, and reduce operational expenses.

Sub-Systems in an Airport Network:

A airport network system normally contains several sub-systems to facilitate transportation, such as:

- **Air Traffic Management System (ATMS)**: Orchestrates the safe and efficient movement of aircraft.
- **Airport Lighting Control and Monitoring System (ALCMS)**: Manages lighting information for approaches, runways, and taxiways.
- **Apron Docking Guide Systems**: Aids aircraft in safe and precise docking at the airport.
- **Apron Management System**: Supervises the activities on the airport apron area, ensuring smooth operations.

Interoperability and Security

For airports to function seamlessly, these sub-systems must intercommunicate while maintaining security against potential threats. The network should facilitate data sharing for regular flight operations while safeguarding critical systems against intrusions.

Moxa's Solution

Moxa's secure routers bolster this integration through policy-based firewalls. These policies, composed of specific rules, selectively permit or deny traffic among subsystems. For instance, designers can authorize control signals from ATMS to ALCMS, while excluding potentially disruptive traffic from other parts of the airport.

Allowlist Firewall Configuration

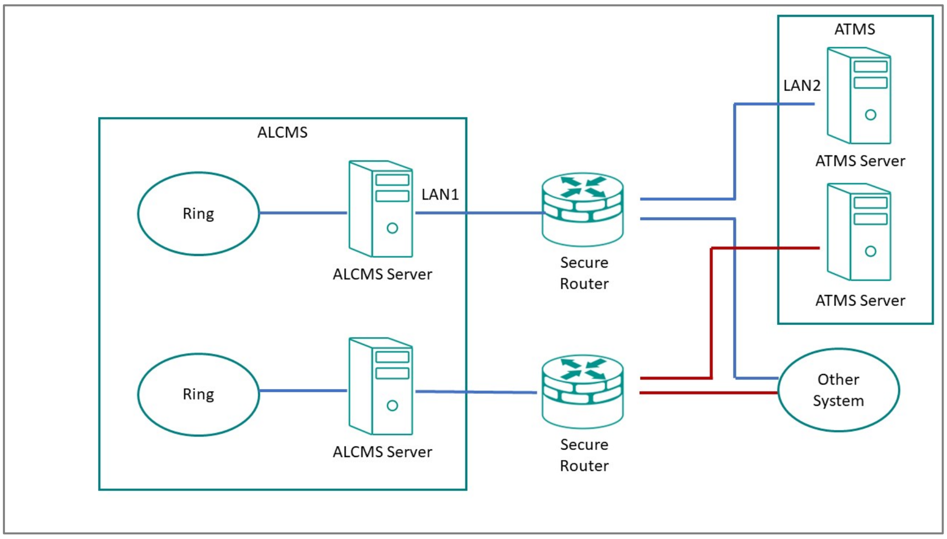
An allowlist is a network configuration that blocks all traffic except those specifically allowed.

Consider a scenario where the network designer employs dual networks for added redundancy. The firewall's rules can be fine-tuned to:

- Allow the ATMS server to communicate with the ALCMS.
- Reject all unrelated traffic and connections.

To achieve this, set up one or more port filters to allow favorable traffic from recognized devices or ports. Then, set up a "deny all" rule to block any unspecified traffic, allowing the systems coexist securely on a shared network.

Integrating subsystems while preserving security and redundancy requires meticulous design and strategic solutions. With the right tools and approaches, airports can achieve high levels of operational efficiency and safety.



Example: Allowing ATMS-ALCMS traffic

Create port filtering rules to allow traffic between the ATMS and ALCMS.

This procedure must be used in tandem with a correctly configured "deny all" policy to correctly implement an allowlist.

Before you begin: Make sure that network interfaces have already been configured with static IP addresses.

Important: This example of an allow list relies on fixed IP addresses. Ensure your network is configured accordingly. If the identified characteristics change, the settings will have to be updated.

1. Go to **Firewall →Layer 3-7 Policy**, and then click ➕[Add].

   Result: The **Layer 3-7 Policy** creation panel appears.
2. Specify all of the following:

Item	Value
Action	**Allow**
Filter Mode	**IP and Port Filtering**
Source IP Address	**LAN2** Refers to the ATMS server
Destination IP Address	**LAN1** Refers to the ALCMS server.

Tutorial Info: In this example, these settings identify the "allowed traffic" by IP address. This requires the IP address to be constant. When configuring in a production environment, make sure the characteristics you choose for your filter clearly distinguish trusted and untrusted network objects, such as IP address, protocol and port, or network interface.

Important: Layer 3-7 Policy rules represent a stateful firewall. This means that once the **Source** initiates traffic with **Destination**, two-way traffic will be allowed through the firewall because the firewall will remember the "state" of the connection. However, if there is a possibility that either **Source** or **Destination** may initiate the connection, it may be best to create separate "mirrored" rules to allow connections in both directions. Refer to Stateful vs. Stateless firewalls for more information.

3. Click **Apply**.

What to do next: Add a policy rule to deny all other traffic to and from the ATMS and ALCMS. See Example: Configuring Blocked Traffic (Air)

Example: Configuring Blocked Traffic (Air)

Once you have specified "allowed" traffic, block all other traffic so that the ATMS and ALCMS systems will be effectively isolated from all other devices.

1. Go to **Firewall** →**Layer 3-7 Policy**, and then click ⊞[Add].

   Result: The **Layer 3-7 Policy** creation panel appears.

2. In the **Action** field, select **Deny**.

3. In the **Filter Mode** field, select **IP and Port Filtering**.
4. Click **Apply**.
5. Make sure that the "deny all" rule is the last rule on the list, otherwise this rule may override the allow rules.
6. To reorder rules, click ↕☰[Reorder Priorities]

Results: Traffic between the ATMS and ALCMS systems will be permitted, but all other traffic to and from these systems will be blocked, effectively isolating these systems from other devices on the network. This helps make sure that even if other systems on the network are compromised, no traffic from these systems will reach the ATMS and ALCMS systems, effectively isolating them from this vector of attack.

What to do next:

Tip: Instead of configuring a "deny all" rule, you can configure a policy from **Global Policy Settings** to deny all traffic. To apply the policy,

1. Go to **Firewall** →**Layer 3-7 Policy**
2. Specify **Status** as **Enabled**.
3. Specify **Default Action** as **Deny All**.
4. Click **Apply**.

Specific rules override generalized policies, effectively making the policy the last rule on the list.

Scenario: Railway Integrated Solutions

Short Description: A network system provider is configuring a network for a railway operator.

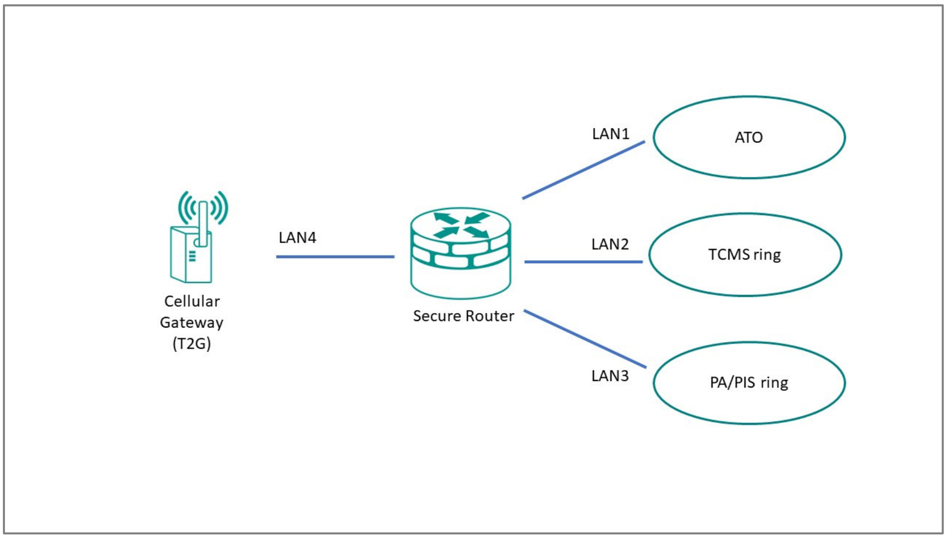
Understanding Railway Network Topology

A typical railway train network comprises multiple sub-systems working in tandem to ensure smooth operations. These sub-systems communicate crucial information, such as train speed, departure/arrival times, door status, climate control, lighting, and station updates to passengers.

Moxa's secure routers offer firewall functionality that allows seamless integration of these systems. By implementing policy-based firewall rules, these routers can permit authorized traffic and block unauthorized exchanges between the different sub-systems.

For instance, the train operating system might consist of various components:

- T2G system (usually a cellular gateway)
- ATO (Automatic Train Operation) system
- TCMS (Train Control and Management System) ring
- PA (Public Announcement system)/PIS (Public Information System) ring
- Control units for each of these systems



As an example scenario: a network designer might want configure the network such that the TCMS is the gatekeeper for all signals to the ATO, and prevent the ATO from talking to any other node on the network. We can achieve this kind of network isolation with an allowlist.

Allowlist Firewall Configuration

An allowlist is a network configuration that blocks all traffic except those specifically allowed.

To apply our example from above, the firewall's rules can be fine-tuned to:

- Allow the TCMS to access the ATO, PA/PIS, and Cellular Gateway.
- Allow the Cellular Gateway to access the TCMS and PA/PIS system.
- Reject all unrelated traffic and connections.

This configuring effectively isolates the ATO from the Cellular Gateway and PA/PIS.

To implement this configuration, set up one or more port filters to allow favorable traffic from recognized devices or ports. Then, set up a "deny all" rule to block any unspecified traffic, allowing the systems coexist securely on a shared network.

Integrating subsystems while preserving security and redundancy requires meticulous design and strategic solutions. With the right tools and approaches, operators can achieve high levels of operational efficiency and safety.

Example: Allowing TCMS traffic

Create port filtering rules to allow the TCMS to act as a gatekeeper for other devices on the network.

This procedure must be used in tandem with a correctly configured "deny all" policy to correctly implement an allowlist.

Before you begin: Make sure that network interfaces have already been configured with static IP addresses.

Important: This example of an allow list relies on fixed IP addresses. Ensure your network is configured accordingly. If the identified characteristics change, the settings will have to be updated.

1. Go to **Firewall** →**Layer 3-7 Policy**, and then click [Add].

   Result: The **Layer 3-7 Policy** creation panel appears.

2. Specify all of the following:

Item	Value
Action	**Allow**
Filter Mode	**IP and Port Filtering**
Source IP Address	**LAN2** **LAN2** should represent the IP address of the TCMS.
Destination IP Address	**LAN1** **LAN1** should represent the IP address of the ATO.

   Tutorial Info: In this example, these settings identify the "allowed traffic" by IP address. This requires the IP address to be constant. When configuring in a production environment, make sure the characteristics you choose for your filter clearly distinguish trusted and untrusted network objects, such as IP address, protocol and port, or network interface.

   Important: Layer 3-7 Policy rules represent a stateful firewall. This means that once the **Source** initiates traffic with **Destination**, two-way traffic will be allowed through the firewall because the firewall will remember the "state" of the connection. However, if there is a possibility that either **Source** or **Destination** may initiate the connection, it may be best to create separate "mirrored" rules to allow connections in both directions. Refer to Stateful vs. Stateless firewalls for more information.

   Tutorial Info: In this case, we will specifically create a bidirectional or "mirrored" rule for TCMS to Cellular Gateway traffic.

3. Create two more **Allow** rules.

Rule Purpose	Source IP	Destination IP
Allow TCMS to PA/PIS Traffic	**LAN2**	**LAN3**
Allow TCMS to Cellular Gateway Traffic	**LAN2**	**LAN4**

4. Click **Apply.**

Results: Rules have been created that will allow the TCMS to access all network nodes, allowing the TCMS to serve as a gatekeeper. Next, create a rule that will the allow the Cellular Gateway to access the TCMS and PA/PIS. Refer to Example: Allowing the T2G to access TCMS and PA/PIS for more information.

Example: Allowing the T2G to access TCMS and PA/PIS

Create port filtering rules to allow traffic from the Cellular Gateway to the TCMS and PA/PIS.

Before you begin: Make sure that network interfaces have already been configured with static IP addresses.

Important: This example of an allow list relies on fixed IP addresses. Ensure your network is configured accordingly. If the identified characteristics change, the settings will have to be updated.

1. Go to **Firewall →Layer 3-7 Policy**, and then click ⊞[Add].

   Result: The **Layer 3-7 Policy** creation panel appears.

2. Specify all of the following:

Item	Value
Action	**Allow**
Filter Mode	**IP and Port Filtering**
Source IP Address	**LAN4** **LAN4** should represent the IP address of the Cellular Gateway.

Item	Value
Destination IP Address	**LAN2** **LAN2** should represent the IP address of the TCMS.

Tutorial Info: In this example, these settings identify the "allowed traffic" by IP address. This requires the IP address to be constant. When configuring in a production environment, make sure the characteristics you choose for your filter clearly distinguish trusted and untrusted network objects, such as IP address, protocol and port, or network interface.

Important: Layer 3-7 Policy rules represent a stateful firewall. This means that once the **Source** initiates traffic with **Destination**, two-way traffic will be allowed through the firewall because the firewall will remember the "state" of the connection. However, if there is a possibility that either **Source** or **Destination** may initiate the connection, it may be best to create separate "mirrored" rules to allow connections in both directions. Refer to Stateful vs. Stateless firewalls for more information.

3. To allow the Cellular Gateway to access the PA/PIS, specify all of the following:

Item	Value
Action	**Allow**
Filter Mode	**IP and Port Filtering**
Source IP Address	**LAN4** **LAN4** should represent the IP address of the Cellular Gateway.
Destination IP Address	**LAN3** **LAN3** should represent the IP address of the PA/PIS.

4. Click **Apply**.

Results: Rules have been created that will allow the Cellular Gateway to access the TCMS and PA/PIS.

What to do next: Add a policy rule to block all other traffic. Refer to Example: Configuring Blocked Traffic (Rail) for more information.

Example: Configuring Blocked Traffic (Rail)

Once you have specified "allowed" traffic, block all other traffic so that the ATO will be effectively isolated from all other devices, relying on the TCMS as a gatekeeper.

1. Go to **Firewall** →**Layer 3-7 Policy**, and then click +[Add].

   Result: The **Layer 3-7 Policy** creation panel appears.
2. In the **Action** field, select **Deny**.
3. In the **Filter Mode** field, select **IP and Port Filtering**.
4. Click **Apply**.
5. Make sure that the "deny all" rule is the last rule on the list, otherwise this rule may override the allow rules.

   To reorder rules, click ↕☰[Reorder Priorities]

Results: The TCMS will be able to access all network devices, and the Cellular Gateway will be able to access the TCMS and PA/PIS, but all other traffic will be blocked, effectively isolating these systems from other devices on the network. This helps make sure that even if other systems on the network are compromised, no traffic from these systems will reach the specified systems, effectively isolating them from this vector of attack.

Tip: Instead of configuring a "deny all" rule, you can configure a policy from **Global Policy Settings** to deny all traffic. To apply the policy,

1. Go to **Firewall** →**Layer 3-7 Policy**
2. Specify **Status** as **Enabled**.
3. Specify **Default Action** as **Deny All**.
4. Click **Apply**.

Specific rules override generalized policies, effectively making the policy the last rule on the list.

Chapter 7

Appendix

Appendix

This section includes additional reference information for your device.

The following information is included:

- EtherTypes for Layer 2
- Fiber Check Threshold Values
- IEC 61375-2-3 Communication Identifiers
- IEC-104 Cause of Transmission List
- IEC-104 Type Identification List
- MIB Groups
- MMS Command Type List
- MMS Service Operation List
- Severity Level List
- Status Codes
- System Event List
- TRDP Message Type List
- TRDP Protocol Filter Profile List
- User Role Privileges

EtherTypes for Layer 2

The following table shows the Layer 2 protocol types commonly used in Ethernet frames.

EtherType Value (Hexadecimal)	Layer 2 Protocol
0x0800	IPv4 (Internet Protocol version 4)
0x0805	X25
0x0806	ARP (Address Resolution Protocol)

EtherType Value (Hexadecimal)	Layer 2 Protocol
0x0808	Frame Relay ARP
0x08FF	G8BPQ AX.25 Ethernet Packet
0x6000	DEC Assigned proto
0x6001	DEC DNA Dump/Load
0x6002	DEC DNA Remote Console
0x6003	DEC DNA Routing
0x6004	DEC LAT
0x6005	DEC Diagnostics
0x6006	DEC Customer use
0x6007	DEC Systems Comms Arch
0x6558	Trans Ether Bridging
0x6559	Raw Frame Relay
0x80F3	Appletalk AARP
0x809B	Appletalk
0x8100	8021Q VLAN tagged frame
0x8137	Novell IPX
0x8191	NetBEUI
0x86DD	IP version 6 (Internet Protocol version 6)
0x880B	PPP
0x884C	MultiProtocol over ATM
0x8863	PPPoE discovery messages
0x8864	PPPoE session messages
0x8884	Frame-based ATM Transport over Ethernet
0x9000	Loopback

Fiber Check Threshold Values

Model Name	Temperature Threshold (°C)	Max./Min. TX Power (dBm)	Min. RX Power (dBm)
FEMST	120	-11.0/-23.0	-31.0
FEMSC	120	-11.0/-23.0	-31.0
FESSC	120	3.0/-8.0	-34.0
SFP-1FEMLC-T	120	-5.0/-21.0	-37.0
SFP-1FESLC-T	120	3.0/-8.0	-37.0
SFP-1FELLC-T	120	3.0/-8.0	-37.0
SFP-1GSXLC-T	110	-1.0/-12.5	-18.0
SFP-1GLSXLC-T	120	2.0/-12.0	-19.0
SFP-1GLXLC-T	120	0.0/-12.5	-20.0
SFP-1GLHLC-T	120	1.0/-11.0	-23.0
SFP-1GLHXLC-T	120	4.0/-7.0	-24.0
SFP-1GZXLC-T	120	8.0/-3.0	-24.0
SFP-1G10ALC-T	120	0.0/-12.0	-21.0
SFP-1G10BLC-T	120	-5.0/-21.0	-34.0
SFP-1G20ALC-T	120	1.0/-11.0	-23.0
SFP-1G20BLC-T	120	-5.0/-21.0	-34.0
SFP-1G40ALC-T	120	5.0/-6.0	-23.0
SFP-1G40BLC-T	120	-5.0/-21.0	-34.0
SFP-1GSXLC	100	-1.0/-12.5	-18.0
SFP-1GLSXLC	100	2.0/-12.0	-19.0
SFP-1GLXLC	100	0.0/-12.5	-20.0
SFP-1GLHLC	100	1.0/-11.0	-23.0
SFP-1GLHXLC	100	4.0/-7.0	-24.0
SFP-1GZXLC	100	8.0/-3.0	-24.0
SFP-1GEZXLC	100	8.0/-3.0	-30.0
SFP-1GEZXLC-120	100	6.0/-5.0	-33.0

Model Name	Temperature Threshold (°C)	Max./Min. TX Power (dBm)	Min. RX Power (dBm)
SFP-1G10ALC	100	0.0/-12.0	-21.0
SFP-1G10BLC	100	-5.0/-21.0	-34.0
SFP-1G20ALC	100	1.0/-11.0	-23.0
SFP-1G20BLC	100	-5.0/-21.0	-34.0
SFP-1G40ALC	100	5.0/-6.0	-23.0
SFP-1G40BLC	100	-5.0/-21.0	-34.0

IEC 61375-2-3 Communication Identifiers

This is a list of IEC 61375-2-3 communication identifier ComIDs and their descriptions.

ComID	Description
0	unspecified PDU
1	ETBCTRL telegram
2	CSTINFO notification message
3	CSTINFOCTRL notification message
10	TRDP Echo
31	TRDP - statistics request command
35	TRDP - global statistics data
36	TRDP - subscription statistics data
37	TRDP - publishing statistics data
38	TRDP - redundancy statistics data
39	TRDP - join statistics data
40	TRDP- UDP listener statistics data
41	TRDP - TCP listener statistics data
80	Conformance test- control telegram
81	Conformance test - status telegram
82	Conformance test - confirmation request telegram

ComID	Description
83	Conformance test - confirmation reply telegram
84	Conformance test - opTrnDir request telegram
85	Conformance test - opTrnDir reply telegram
86	Conformance test - echo request telegram
87	Conformance test - echo reply telegram
88	Conformance test - echo notification telegram
100	TTDB - operational train directory status telegram
101	TTDB - operational train directory notification
102	TTDB - train directory information request
103	TTDB - train directory information reply
104	TTDB - consist information request
105	TTDB - consist information reply
106	TTDB - train network directory information request
107	TTDB - train network directory information reply
108	TTDB - operational train directory information request
109	TTDB - operational train directory information reply
110	TTDB - train information complete request
120	ECSP - control telegram
121	ECSP - status telegram
122	ECSP - Confirmation/Correction request
123	ECSP - Confirmation/Correction reply
130	ETBN - control request
131	ETBN - status reply
132	ETBN - train network directory request
133	ETBN - train network directory reply
140	TCN-DNS - resolving request telegram (query)
141	TCN-DNS - resolving reply telegram

IEC-104 Cause of Transmission List

This is a list of IEC-104 cause of transmission codes and their descriptions.

Cause	Description
0	not used
1	periodic, cyclic
2	background interrogation
3	spontaneous
4	initialized
5	interrogation or interrogated
6	activation
7	confirmation activation
8	deactivation
9	confirmation deactivation
10	termination activation
11	feedback, caused by distant command
12	feedback, caused by local command
13	data transmission
14-19	reserved for further compatible definitions
20	interrogated by general interrogation
21	interrogated by interrogation group 1
22	interrogated by interrogation group 2
23	interrogated by interrogation group 3
24	interrogated by interrogation group 4
25	interrogated by interrogation group 5
26	interrogated by interrogation group 6
27	interrogated by interrogation group 7
28	interrogated by interrogation group 8
29	interrogated by interrogation group 9

Cause	Description
30	interrogated by interrogation group 10
31	interrogated by interrogation group 11
32	interrogated by interrogation group 12
33	interrogated by interrogation group 13
34	interrogated by interrogation group 14
35	interrogated by interrogation group 15
36	interrogated by interrogation group 16
37	interrogated by counter general interrogation
38	interrogated by interrogation counter group 1
39	interrogated by interrogation counter group 2
40	interrogated by interrogation counter group 3
41	interrogated by interrogation counter group 4
44	type-Identification unknown
45	cause unknown
46	ASDU address unknown
47	Information object address unknown

IEC-104 Type Identification List

This is a list of IEC-104 type identification codes and their descriptions.

Process information in monitor direction

Type	Description
1	Single point information
2	Single point information with time tag
3	Double point information
4	Double point information with time tag
5	Step position information

Type	Description
6	Step position information with time tag
7	Bit string of 32 bit
8	Bit string of 32 bit with time tag
9	Measured value, normalized value
10	Measured value, normalized value with time tag
11	Measured value, scaled value
12	Measured value, scaled value with time tag
13	Measured value, short floating-point value
14	Measured value, short floating-point value with time tag
15	Integrated totals
16	Integrated totals with time tag
17	Event of protection equipment with time tag
18	Packed start events of protection equipment with time tag
19	Packed output circuit information of protection equipment with time tag
20	Packed single-point information with status change detection
21	Measured value, normalized value without quality descriptor

Process telegrams with long time tag (7 octets)

Type	Description
30	Single point information with time tag CP56Time2a
31	Double point information with time tag CP56Time2a
32	Step position information with time tag CP56Time2a
33	Bit string of 32 bit with time tag CP56Time2a
34	Measured value, normalized value with time tag CP56Time2a
35	Measured value, scaled value with time tag CP56Time2a
36	Measured value, short floating-point value with time tag CP56Time2a
37	Integrated totals with time tag CP56Time2a

Type	Description
38	Event of protection equipment with time tag CP56Time2a
39	Packed start events of protection equipment with time tag CP56time2a
40	Packed output circuit information of protection equipment with time tag CP56Time2a

Process information in control direction

Type	Description
45	Single command
46	Double command
47	Regulating step command
48	Setpoint command, normalized value
49	Setpoint command, scaled value
50	Setpoint command, short floating-point value
51	Bit string 32 bit

Command telegrams with long time tag (7 octets)

Type	Description
58	Single command with time tag CP56Time2a
59	Double command with time tag CP56Time2a
60	Regulating step command with time tag CP56Time2a
61	Setpoint command, normalized value with time tag CP56Time2a
62	Setpoint command, scaled value with time tag CP56Time2a
63	Setpoint command, short floating-point value with time tag CP56Time2a
64	Bit string 32 bit with time tag CP56Time2a

System information in monitor direction

Type	Description
70	End of initializ

System information in control direction

Type	Description
100	(General-) Interrogation command
101	Counter interrogation command
102	Read command
103	Clock synchronization command
104	(IEC 101) Test command
105	Reset process command
106	(IEC 101) Delay acquisition command
107	Test command with time tag CP56Time2a

Parameter in control direction

Type	Description
110	Parameter of measured value, normalized value
111	Parameter of measured value, scaled value
112	Parameter of measured value, short floating-point value
113	Parameter activation

File transfer

Type	Description
120	File ready
121	Section ready

Type	Description
122	Call directory, select file, call file, call section
123	Last section, last segment
124	Ack file, Ack section
125	Segment
126	Directory
127	QueryLog – Request archive file

MIB Groups

The Industrial Secure Router comes with built-in SNMP (Simple Network Management Protocol) agent software that supports cold start trap, line up/down trap, and RFC 1213 MIB-II.

The standard MIB groups that the Industrial Secure Router series support are:

MIB II.1 – System Group
sysORTable

MIB II.2 – Interfaces Group
ifTable

MIB II.4 – IP Group
ipAddrTable
ipNetToMediaTable
IpGroup
IpBasicStatsGroup
IpStatsGroup

MIB II.5 – ICMP Group
IcmpGroup
IcmpInputStatus

IcmpOutputStats

MIB II.6 – TCP Group

tcpConnTable

TcpGroup

TcpStats

MIB II.7 – UDP Group

udpTable

UdpStats

MIB II.11 – SNMP Group

SnmpBasicGroup

SnmpInputStats

SnmpOutputStats

Public Traps

1. Cold Start
2. Link Up
3. Link Down
4. Authentication Failure

Private Traps

1. Configuration Changed
2. Power On
3. Power Off
4. DI Trap

MMS Command Type List

This is a list of MMS command type codes and command names.

Command Type	Command Name
1	confirmed_RequestPDU
2	confirmed_ResponsePDU
3	confirmed_ErrorPDU
4	unconfirmed_PDU
5	rejectPDU
6	cancel_RequestPDU
7	cancel_ResponsePDU
8	cancel_ErrorPDU
9	initiate_RequestPDU
10	initiate_ResponsePDU
11	initiate_ErrorPDU
12	conclude_RequestPDU
13	conclude_ResponsePDU
14	conclude_ErrorPDU

MMS Service Operation List

This is a list of MMS service operation codes and their names.

Service Operation	Service Operation Name
1	acknowledgeEventNotification
2	alterEventConditionMonitoring
3	alterEventEnrollment
4	createJournal
5	createProgramInvocation
6	defineEventAction
7	defineEventCondition
8	defineEventEnrollment
9	defineNamedType

Service Operation	Service Operation Name
10	defineNamedVariable
11	defineNamedVariableList
12	defineScatteredAccess
13	defineSemaphore
14	deleteDomain
15	deleteEventAction
16	deleteEventCondition
17	deleteEventEnrollment
18	deleteJournal
19	deleteNamedType
20	deleteNamedVariableList
21	deleteProgramInvocation
22	deleteSemaphore
23	deleteVariableAccess
24	downloadSegment
25	eventNotification
26	fileClose
27	fileDelete
28	fileDirectory
29	fileOpen
30	fileRead
31	fileRename
32	getAlarmEnrollmentSummary
33	getAlarmSummary
34	getCapabilityList
35	getDomainAttributes
36	getEventActionAttributes
37	getEventConditionAttributes

Service Operation	Service Operation Name
38	getEventEnrollmentAttributes
39	getNamedTypeAttributes
40	getNamedVariableListAttributes
41	getNameList
42	getProgramInvocationAttributes
43	getScatteredAccessAttributes
44	getVariableAccessAttributes
45	identify
46	informationReport
47	initializeJournal
48	initiateDownloadSequence
49	initiateUploadSequence
50	input
51	kill
52	loadDomainContent
53	obtainFile
54	output
55	read
56	readJournal
57	relinquishControl
58	rename
59	reportActionStatus
60	reportEventActionStatus
61	reportEventConditionStatus
62	reportEventEnrollmentStatus
63	reportJournalStatus
64	reportPoolSemaphoreStatus
65	reportSemaphoreEntryStatus

Service Operation	Service Operation Name
66	reportSemaphoreStatus
67	requestDomainDownLoad
68	requestDomainUpload
69	reset
70	resume
71	start
72	status
73	stop
74	storeDomainContent
75	takeControl
76	terminateDownloadSequence
77	terminateUploadSequence
78	triggerEvent
79	unsolicitedStatus
80	uploadSegment
81	write
82	writeJournal

Severity Level List

This is a list of severity levels and descriptions, which are based on CVSS vulnerability classifications.

Severity	Description
Emergency	System is unusable
Alert	Action must be taken immediately
Critical	Critical conditions
Error	Error conditions
Warning	Warning conditions

Severity	Description
Notice	Normal but significant condition
Infomational	Informational messages
Debug	Debug-level messages

Status Codes

This page shows the different status codes for your device.

Note

Available settings and options will vary depending on the product model.

PoE Status Codes

Classification

Classification	Max Power (watts) by PSE Output
0	15.4
1	4
2	7
3	15.4
4	30

Device Type

Item	Description
Not Present	There are no active connections to the port.
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.

Item	Description
Unknown	An unknown PD is connected to the port.
N/A	The PoE function is disabled.

Configuration Suggestion

Item	Description
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.

System Event List

This is a list of system events and their descriptions.

System Event	Description
Cold Start	Power was cut off and then reconnected.
Warm Start	The Moxa industrial secure router was rebooted, such as when network parameters are changed (IP address, netmask, etc.).
Power 1 Transition (On->Off)	The Moxa industrial secure router’s power 1 is powered down.
Power 1 Transition (Off->On)	The Moxa industrial secure router’s power 1 is powered up.
Power 2 Transition (On->Off)	The Moxa industrial secure router’s power 2 is powered down.

System Event	Description
Power 2 Transition (Off->On)	The Moxa industrial secure router's power 2 is powered up.
Configuration Changed	A configuration setting was changed.
Login Failure	An incorrect password was entered.
802.1X Authentication Failure	An 802.1X authentication failure occurred.
Firmware Upgrade Success	Firmware upgrade was successful.
Firmware Upgrade Failure	An error occurred during the firmware upgrade.
Log Service Ready	Log service is ready.
Ring/RSTP Topology Changed	The Ring/RSTP topology was changed.
Master Mismatch	A Turbo Ring Master mismatch occurred.
Coupling Topology Changed	The Coupling topology was changed.
VRRP State Change	The VRRP state was changed.
VPN Connected	VPN has been connected.
VPN Disconnected	VPN has been disconnected.
Firewall Policy	A firewall policy failure occurred.
PoE PD On	PoE
PoE PD Off	Port#N PD power on.
Over Measured Power limitation	Port#N PD power off.
PoE FETBad	PD Port#N MOSFET is bad.
PoE Over Temperature	The temperature of the environment exceeds the maximum operating temperature of the router.
PoE VEE Uvlo	VEE (PoE input voltage) under Voltage Lockout. The voltage of the power supply has dropped below 44V DC.
PoE PD Over Current	Current of Port#N has exceeded the safety limit.
PoE PD Check Fail	The router does not receive a PD response from Port#N after the defined period for specific time cycles.
Over Allocated Power limitation	The total PD power consumption exceeds the total allocated power.

TRDP Message Type List

Configuration attribute requirements - msgType

This is a list of TRDP msgTypes and their descriptions.

msgType	Description
Pr	PD Request
Pp	PD Reply
Pd	PD Data
Pe	PD Data (Error)
Mn	Notification (Request without reply)
Mr	MD Request with reply
Mp	MD Reply without confirmation
Mq	MD Reply with confirmation
Mc	MD Confirm
Me	MD error

Configuration attribute requirements - msgType Profile

This is a list of TRDP msgType profiles and their descriptions.

Profile	Description
PD-PDU	A collection of "Pr, Pp, Pd, Pe"
MD-PDU	A collection of "Mn, Mr, Mp, Mq, Mc, Me"

TRDP Protocol Filter Profile List

This is a list of the different built-in protocol filter profiles for common applications and their corresponding message types and communication identifiers.

Protocol Filter Profile	Message Type	Communication Identifier (ComID)
PD-PDU	0x5072: PD Request, 0x5070: PD Reply, 0x5064: PD Data, 0x5065: PD Data (Error)	All
MD-PDU	0x4D6E: Notification (Request without reply), 0x4D72: MD Request with reply, 0x4D70: MD Reply without confirmation, -x4D71: MD Reply with confirmation, 0x4D63: MD Confirm, 0x4D65: MD error	All
Communication Framework and ETB Control Service	All	1-29, 50-79, 150-199
TRDP statistics data	All	30-41
Conformance test	All	80-99
TTDB	All	100-119
ECSP	All	120-129
ETBN	All	130-139
TCN-DNS	All	140-149

User Role Privileges

This page shows the privilege levels granted to the different authority levels: Admin, Supervisor, and User. 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.

System

Settings	Admin	Supervisor	User
System Management			
Information Settings	R/W	R/W	R
Firmware Upgrade	R/W	-	-
Software Package Management	R/W	-	-
Configuration Backup and Restore	R/W	-	-
Account Management			
User Account	R/W	-	-
Password Policy	R/W	-	-
License Management	R/W	R	R
Management Interface			
User Interface	R/W	R/W	R
Hardware Interface	R/W	R/W	R
SNMP	R/W	-	-
MXsecurity	R/W	R/W	-
Time			
System Time	R/W	R/W	R
NTP/SNTP Server	R/W	R/W	R
Setting Check	R/W	R/W	R
Power Management	R/W	R/W	R
SMS	R/W	R/W	R
GNSS	R/W	R/W	R

Network Configuration

Settings	Admin	Supervisor	User
Port			
Port Settings	R/W	R/W	R

Settings	Admin	Supervisor	User
Link Aggregation	R/W	R/W	R
Layer 2 Switching			
VLAN	R/W	R/W	R
MAC Address Table	R/W	R/W	R
QoS	R/W	R/W	R
Rate Limit	R/W	R/W	R
Multicast	R/W	R/W	R
Network Interface	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
Layer 3 Redundancy			
VRRP	R/W	R/W	R

Network Service

Settings	Admin	Supervisor	User
DHCP Server	R/W	R/W	R
Dynamic DNS	R/W	R/W	R

Routing

Settings	Admin	Supervisor	User
Unicast Routing			
Static Routes	R/W	R/W	R

Settings	Admin	Supervisor	User
RIP	R/W	R/W	R
OSPF	R/W	R/W	R
Routing Table	R	R	R
Multicast Route			
Multicast Route Settings	R/W	R/W	R
Static Multicast Route	R/W	R/W	R
Broadcast Forwarding	R/W	R/W	R

NAT

Settings	Admin	Supervisor	User
NAT Setting	R/W	R/W	R

Object Management

Settings	Admin	Supervisor	User
Object Management	R/W	R/W	R

Firewall

Settings	Admin	Supervisor	User
Layer 2 Policy	R/W	R/W	R
Layer 3 - 7 Policy	R/W	R/W	R
Malformed Packets	R/W	R/W	R
Session Control	R/W	R/W	R
DoS Policy	R/W	R/W	R
Advanced Protection			
Dashboard	R/W	R/W	-
Configuration	R/W	R/W	-

Settings	Admin	Supervisor	User
Protocol Filter Policy	R/W	R/W	-
ADP	R/W	R/W	-
IPS	R/W	R/W	-

VPN

Settings	Admin	Supervisor	User
IPsec	R/W	R/W	R
L2TP Server	R/W	R/W	R

Certificate Management

Settings	Admin	Supervisor	User
Local Certificate	R/W	-	-
Trusted CA Certificate	R/W	-	-
Certificate Signing Request	R/W	-	-

Security

Settings	Admin	Supervisor	User
Device Security			
Login Policy	R/W	R	R
Trusted Access	R/W	R/W	R
SSH & SSL	R/W	R/W	-
Network Security			
IEEE 802.1X	R/W	R/W	R
RADIUS	R/W	-	-
MXview Alert Notification	R/W	R/W	R

Diagnostics

Settings	Admin	Supervisor	User
System Status			
Utilization	R/W	R/W	R
Fiber Check	R/W	R/W	R
Network Status			
Network Statistics	R	R	R
LLDP	R/W	R/W	R
ARP Table	R	R	R
Event Log & Notifications			
Event Log	R/W	R/W	R
Event Notifications	R/W	R/W	R
Syslog	R/W	R	R
SNMP Trap/Inform	R/W	-	-
Email Settings	R/W	R	R
Tools			
Port Mirror	R/W	R/W	R
Ping	R/W	R/W	R

Moxa Inc.

www.moxa.com/products