MX-ROS V3 - NAT-108 Series

User Manual

Version 1.0

March 2025

Table of Contents

Chapter 1

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.

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.
- **Device Applications**: This section goes through various applications and helps you understand the related technologies, product features, and best practices so you can better configure the device for your own needs.
- **Security Hardening Guide**: 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.

Supported Series and Firmware Versions

Moxa Router Series	Firmware Version
NAT-108 Series	v3.16

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. For more information about which features are supported by each product series, refer to the Supported Features List.

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

Supported Features List

Support for various features varies depending on the product and model. Refer to the table below for an overview of which features are supported by different product series.

> **Note**
>
> Please note that there may still be functional differences between different models within the same product series.

Configuration Section	Function	NAT Series
Device Summary		YES
Setup Wizard		YES
System		YES
	System Management	YES
	Information Settings	YES
	Firmware Upgrade	YES
	Configuration Backup and Restore	YES
	Account Management	YES
	User Accounts	YES
	Password Policy	YES
	Management Interface	YES
	User Interface	YES
	Ping Response	YES
	SNMP	YES
	Time	YES
	System Time	YES
	NTP/SNTP Server	YES

Configuration Section	Function	NAT Series
	Setting Check	YES
Network Configuration		YES
	Ports	YES
	Port Settings	YES
	Layer 2 Switching	YES
	VLAN	YES
	MAC Address Table	YES
	Network Interfaces	YES
Network Service		YES
	DHCP Server	YES
Routing		YES
	Unicast Route	YES
	Static Routes	YES
	Routing Table	YES
NAT		YES
Firewall		YES
	Layer 3 Policy	YES
	Device Lockdown	YES
Certificate Management		YES
	Local Certificate	YES
	Trusted CA Certificate	YES
	Certificate Signing Request	YES
Security		YES

Configuration Section	Function	NAT Series
	Device Security	YES
	Login Policy	YES
	Trusted Access	YES
	SSH & SSL	YES
	Authentication	YES
	Login Authentication	YES
	RADIUS	YES
	TACACS+ Server	YES
	MXview Alert Notification	YES
Diagnostics		YES
	System Status	YES
	Utilization	YES
	Network Status	YES
	Network Statistics	YES
	LLDP	YES
	ARP Table	YES
	Event Log and Notifications	YES
	Event Log	YES
	Event Notifications	YES
	Syslog	YES
	SNMP Trap/Inform	YES
	Email Settings	YES
	Tools	YES

Configuration Section	Function	NAT Series
	Ping	YES

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

Using a Web Browser to Configure the Industrial Secure Router

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

Note

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

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

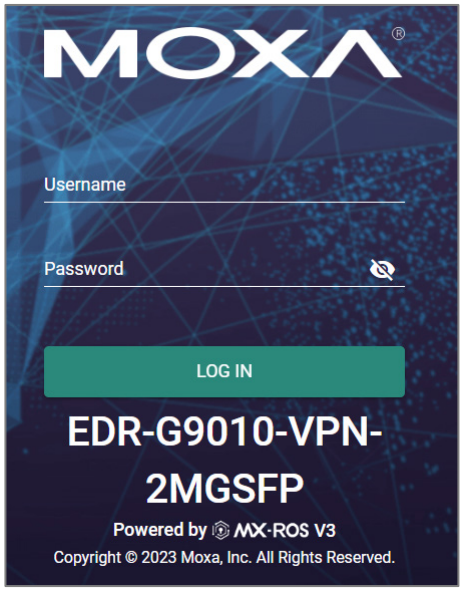
Perform the following steps to access the device's web interface:

1. Make sure your PC host is connected to your device's LAN port, and is on the same subnet as your device.
2. Open a web browser and type the device's LAN IP address (**192.168.127.254** by default) into the address bar and press Enter.

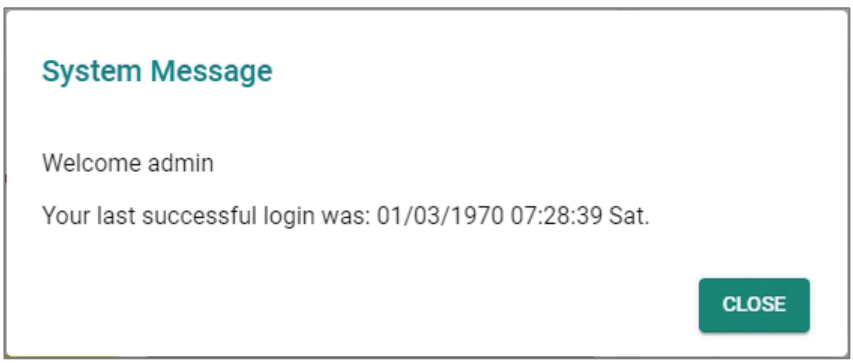
3. The web login page will open. Enter the username (**admin** or **user**) and password (the same as the Console password) and click **LOG IN** to continue.

Note

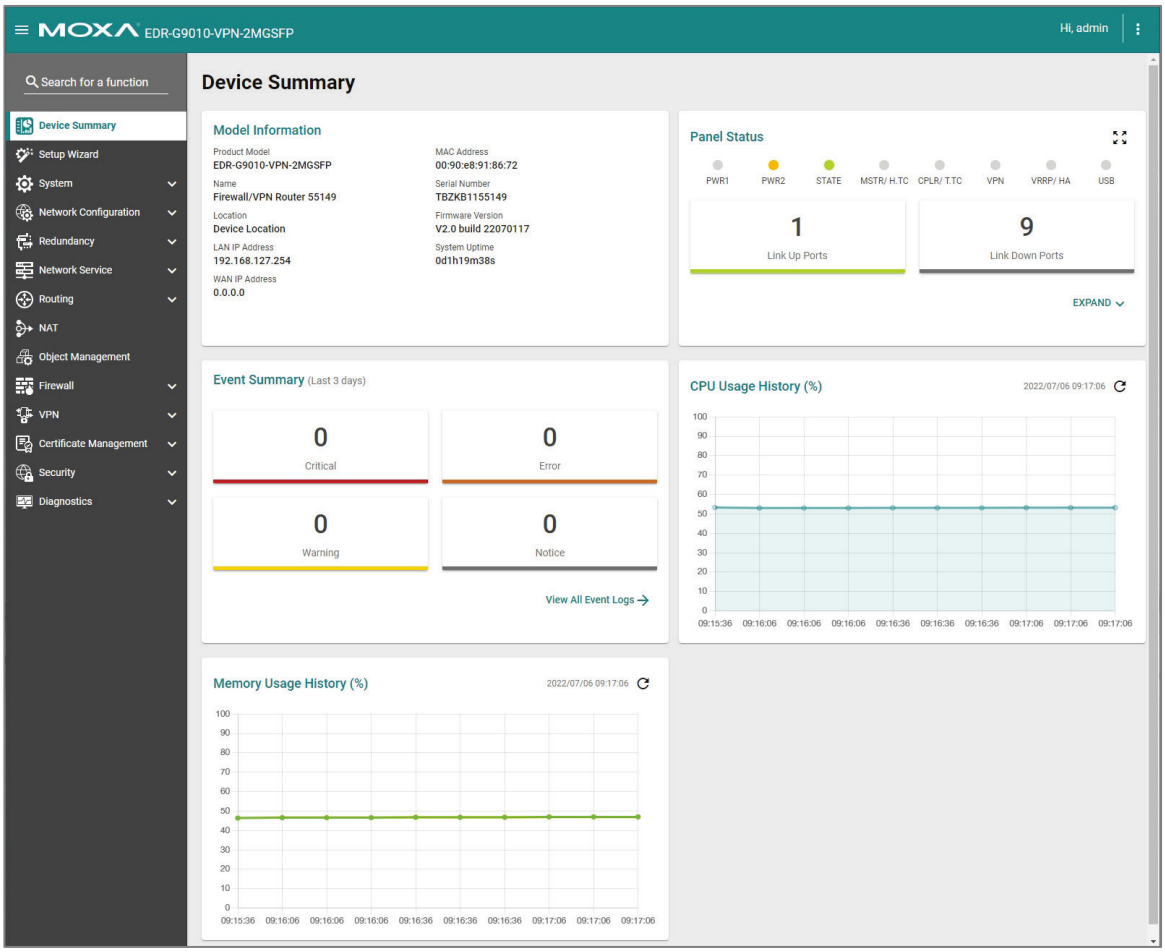
The default username is admin and the default password is moxa. We strongly recommend changing the password as soon as possible to ensure the security of your device.



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



4. 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.


MOXA EDR-G9010-VPN-2MGSFP
Hi, admin
Search for a function
Device Summary
Setup Wizard
System
Network Configuration
Redundancy
Network Service
Routing
NAT
Object Management
Firewall
VPN
Certificate Management
Security
Diagnostics
Device Summary
Model Information
Product Model
EDR-G9010-VPN-2MGSFP
Name
Firewall/VPN Router 55149
Location
Device Location
LAN IP Address
192.168.127.254
WAN IP Address
0.0.0.0
MAC Address
00:90:e8:91:86:72
Serial Number
TBZKB1155149
Firmware Version
V2.0 build 22070117
System Uptime
0d1h19m38s
Panel Status
PWR1
PWR2
STATE
MSTR/ H.TC
CPLR/ T.TC
VPN
VRRP/ HA
USB
1
Link Up Ports
9
Link Down Ports
EXPAND
Event Summary (Last 3 days)
0
Critical
0
Error
0
Warning
0
Notice
View All Event Logs
CPU Usage History (%)
2022/07/06 09:17:06
Memory Usage History (%)
2022/07/06 09:17:06

Chapter 3

UI Reference

UI Reference Overview

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

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

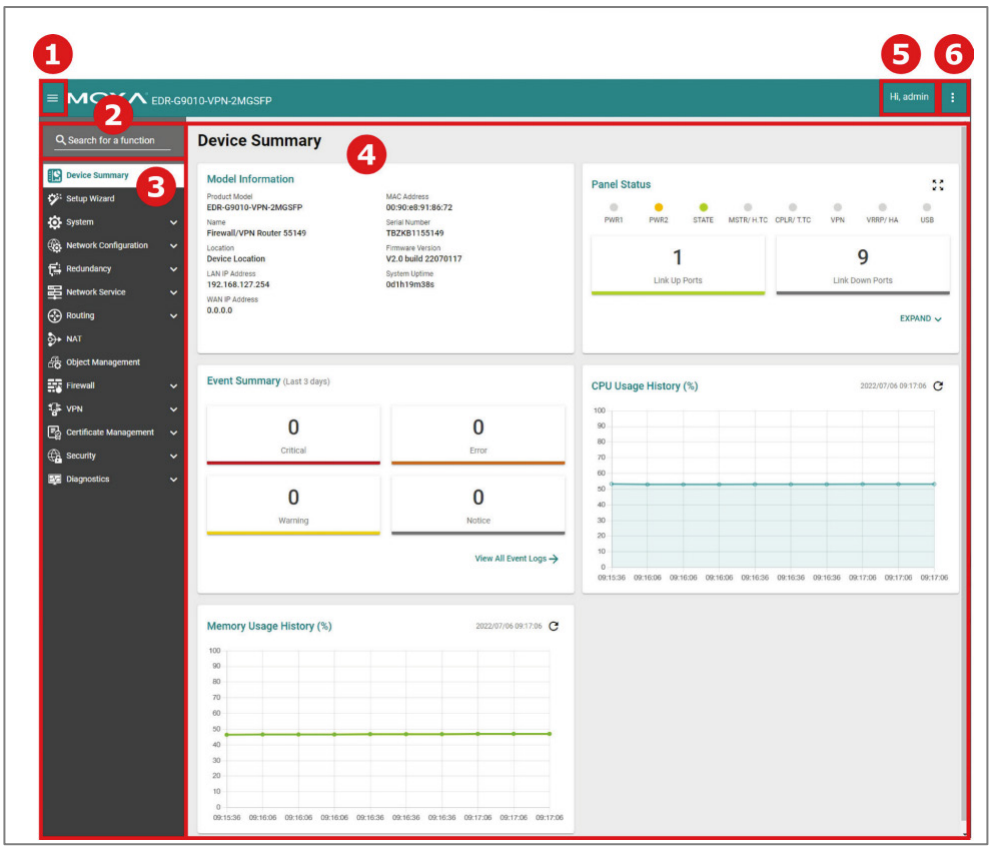
- The MX-ROS User Interface
- Options Menu

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

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

The MX-ROS User Interface

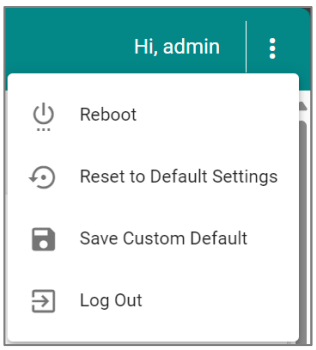
Here is an overview of the MX-ROS user interface.



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 Options menu.

Options Menu

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



Options Menu - User Privileges

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

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

Reboot

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

Reset to Default Settings

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

Save Custom Default

You can save a custom default configuration for your device. This allows you to reset the device to a trusted configuration without uploading a configuration file to restore from. Refer to Reset to Default Settings for more information.

Note

- Ensure that the current startup configuration works as expected and that the user account settings are correct before saving the configuration as a custom default.
- The configuration name can be modified on the Config Backup and Restore page. We recommend including the configuration name for better file differentiation. Please note that each configuration must be unique and not repetitive.
- Each device can only have one set of custom default settings.
- Custom default settings can only save and restore configuration settings. They do not include other uploaded files, such as SSL certificate files, SSH keys, etc.
- Refer to Configuration Types for more information about the different configurations your device uses.

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

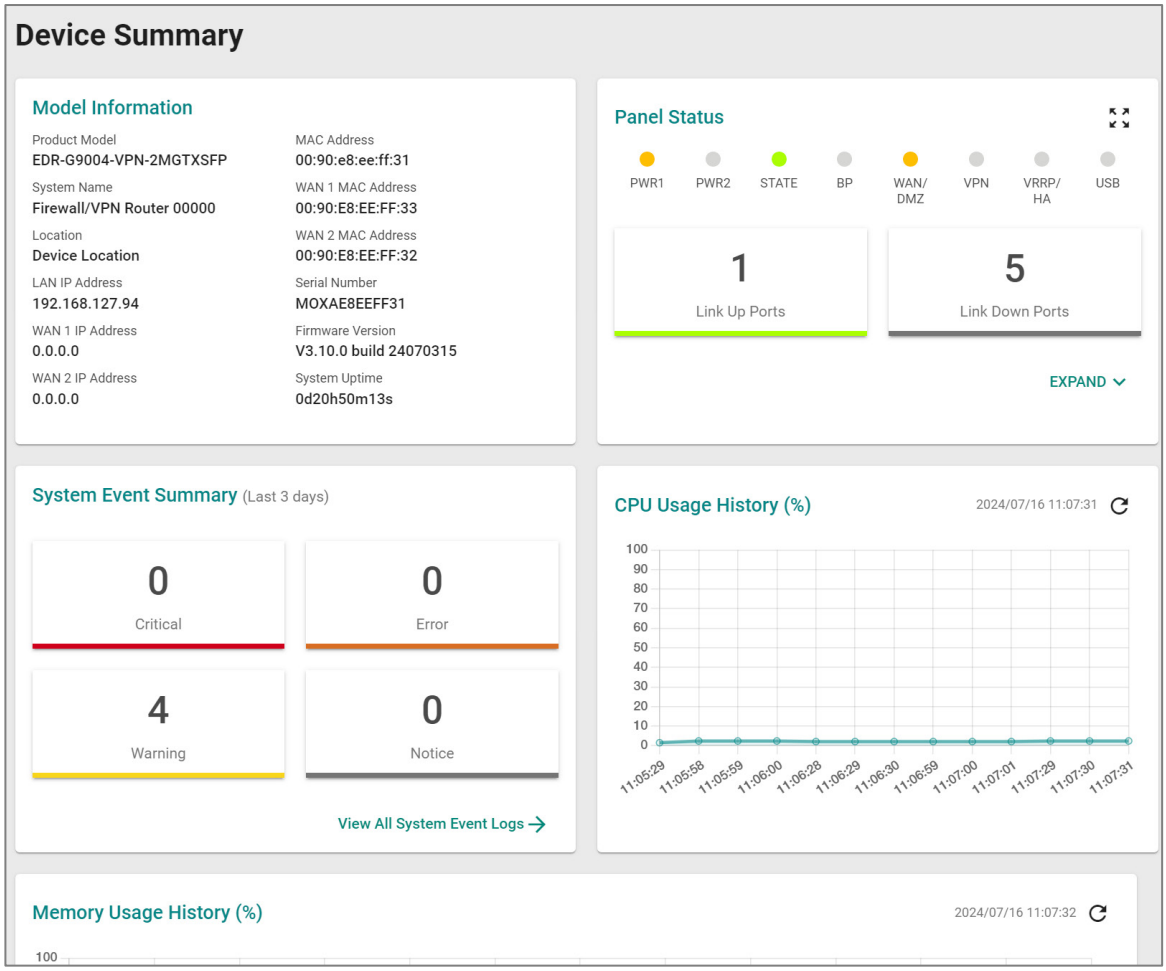
Log Out

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

Device Summary

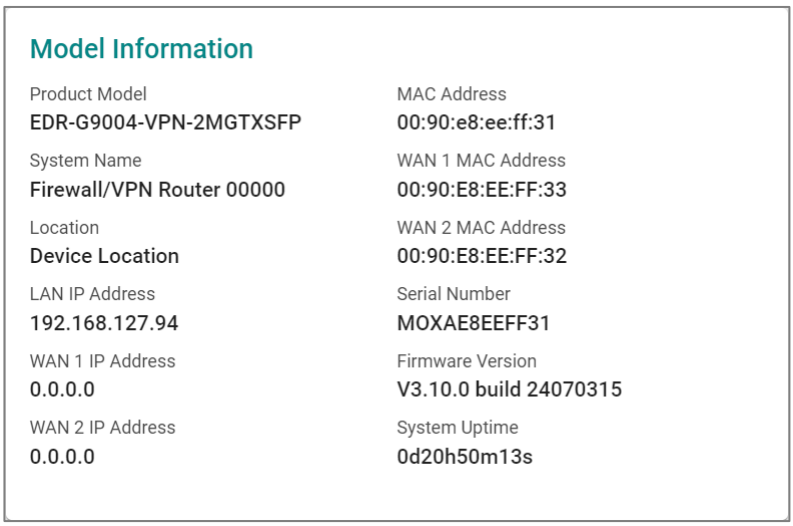
Menu Path: Device Summary

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



Model Information

This display shows basic information about your device.

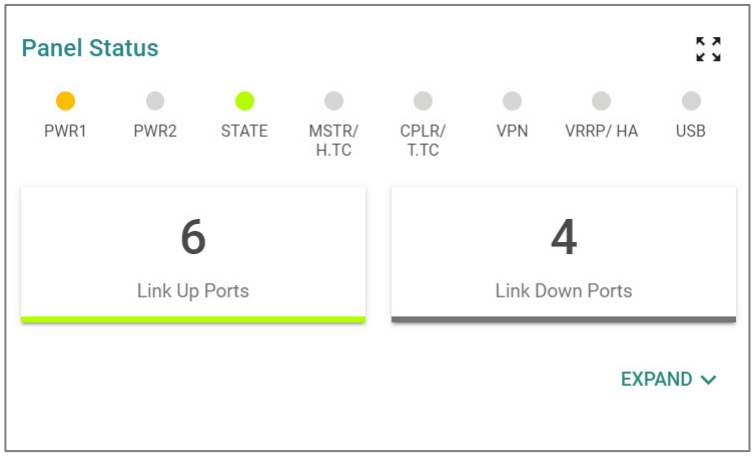


UI Setting	Description
Product Model	Shows the product model of the device.
System Name	Shows the name of the device. Refer to System > System Management > Information Settings for more information.
Location	Shows the location of the device. Refer to System > System Management > Information Settings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

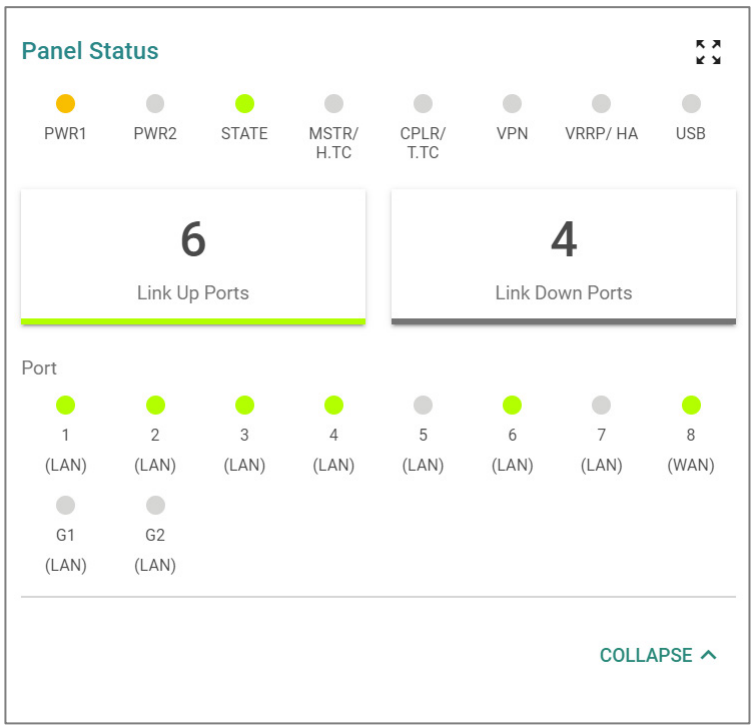
Panel Status

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.



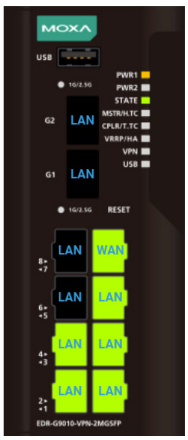
Panel View

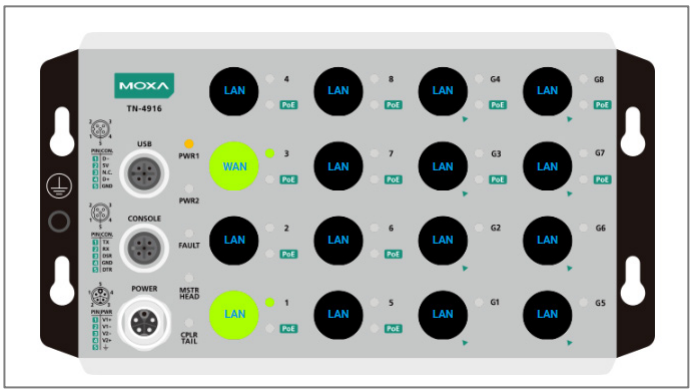
Clicking the **Expand ( )** icon in the **Panel Status** display will show your device's port status on a representative image of the device. This image will vary depending on your device. Click the **Close ( )** icon in the upper-right corner to close the **Panel View**.

Note

Available LEDs may vary across different versions of devices. For more information about status LEDs and their behavior, refer to LED Behavior.

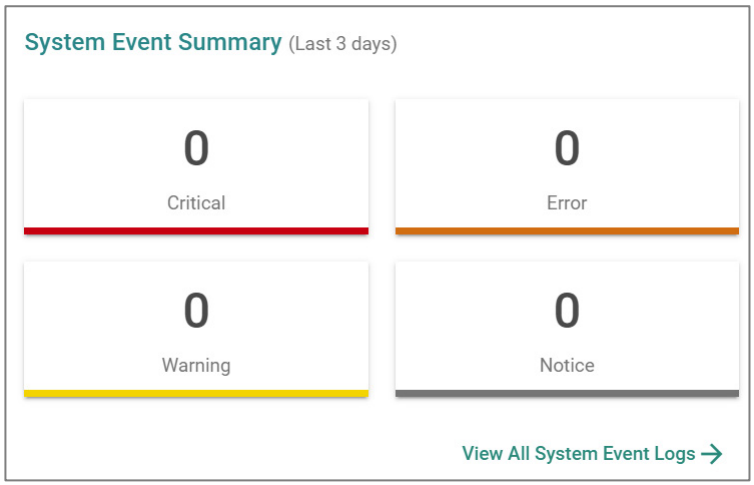
Panel View



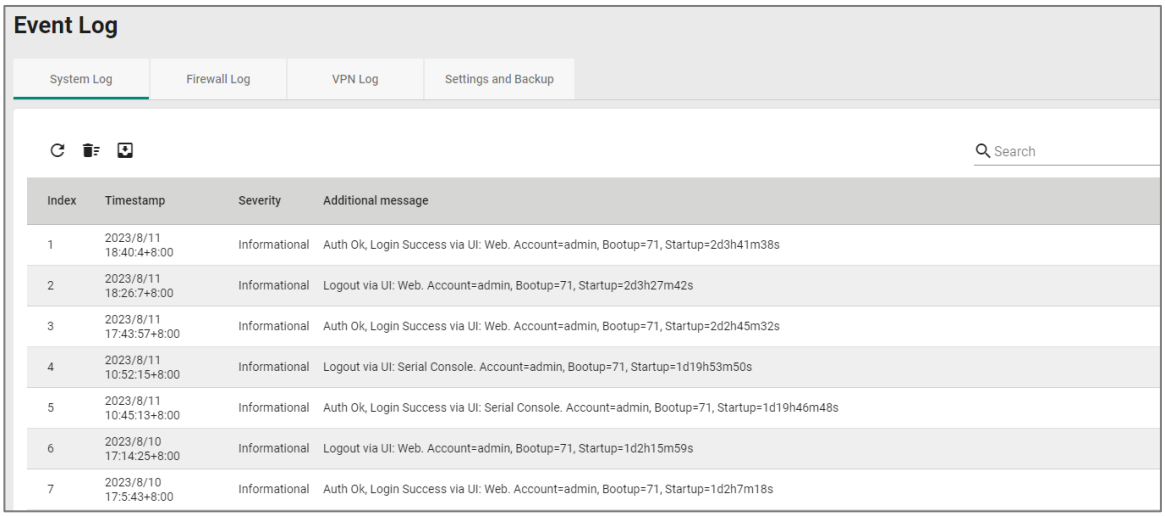


System Event Summary (Last 3 days)

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



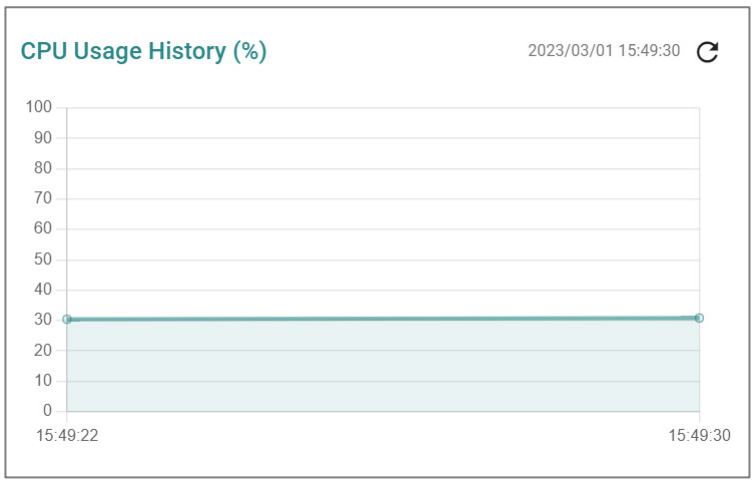
Click **View All System Event Logs** to go to the Event Log page to view event logs in more detail.



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

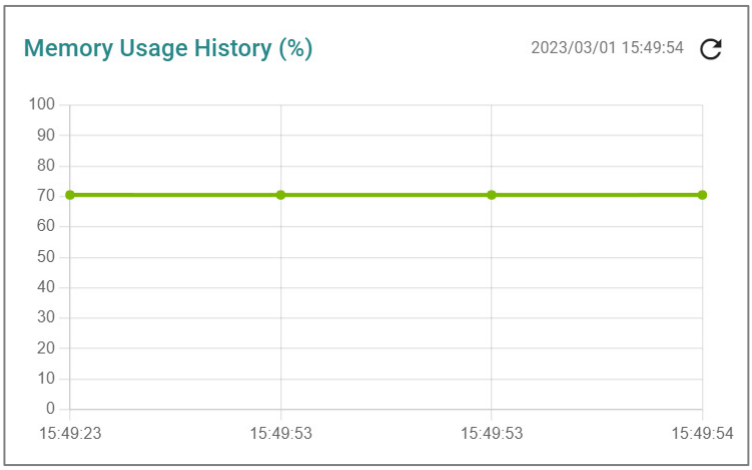
CPU Usage History (%)

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.


Memory Usage History (%)
2023/03/01 15:49:54
100
90
80
70
60
50
40
30
20
10
0
15:49:23
15:49:53
15:49:53
15:49:54

Setup Wizard

Menu Path: Setup Wizard

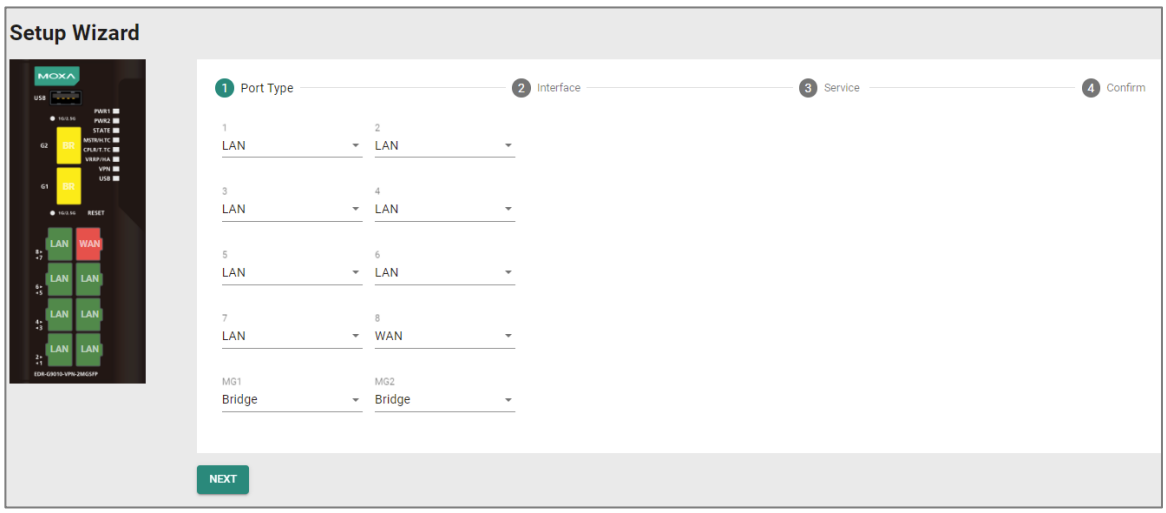
The Setup Wizard helps guide you through basic setup of your device through four steps:

1. Port Type
2. Interface
3. Service
4. 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.



UI Setting	Description	Valid Range	Default Value
MG1 / MG2	Select whether to use this fiber port as a LAN, WAN, or Bridge port.	LAN / WAN / Bridge	LAN

UI Setting	Description	Valid Range	Default Value
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

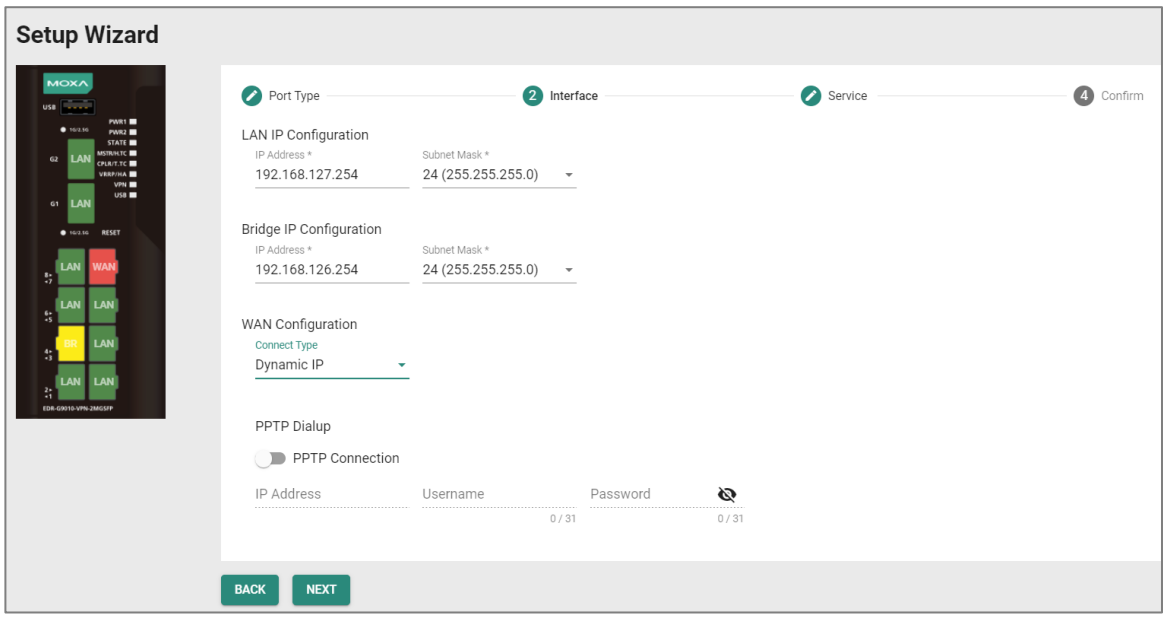
Interface

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

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

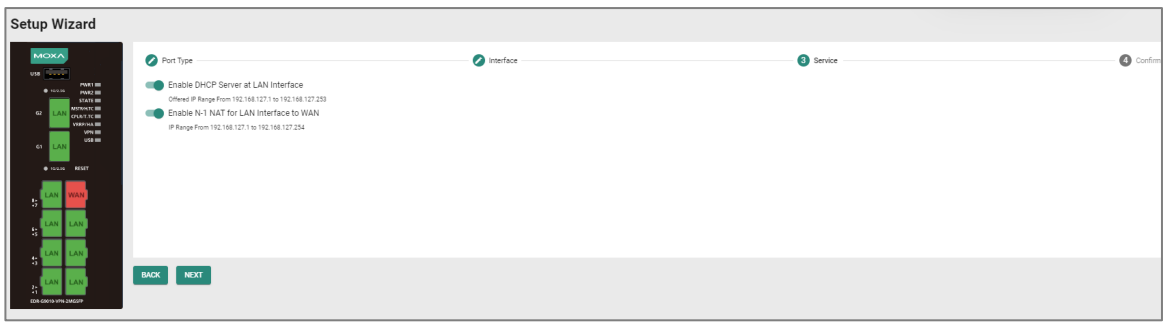
PPPoE Dialup

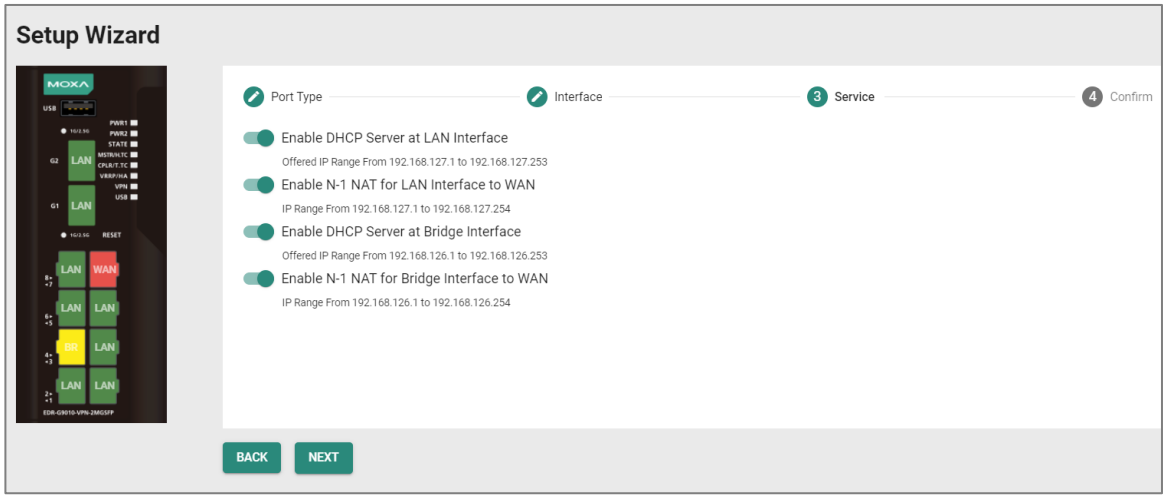
Set the PPPoE Dialup connection details for your device. This section only appears if **PPPoE** is set for **WAN Configuration > Connect Type**.

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.

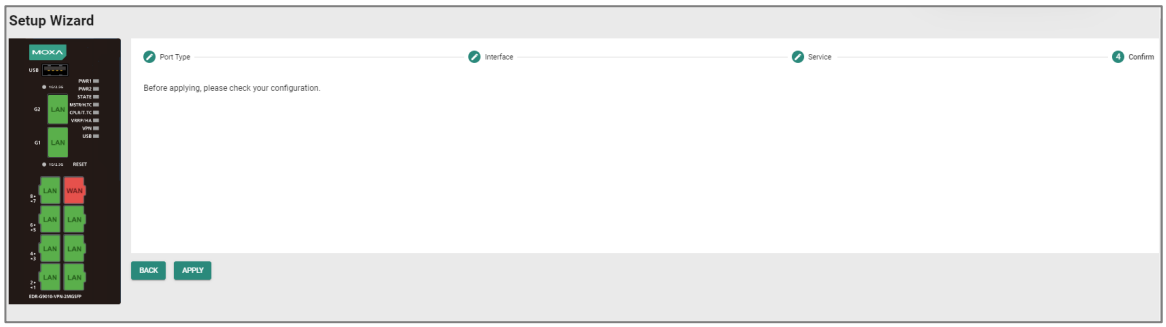




UI Setting	Description	Valid Range	Default Value
Enable DHCP Server at LAN Interface	Enable or disable using a DHCP server for the LAN interface.	Enabled / Disabled	Enabled
Enable N-1 NAT for LAN Interface to WAN	Enable or disable using N-1 NAT for LAN interfaces to WAN.	Enabled / Disabled	Enabled
Enable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

Confirm

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



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
- 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	-	-
Configuration Backup and Restore	R/W	-	-
Account Management			
User Account	R/W	-	-
Password Policy	R/W	-	-
Management Interface			
User Interface	R/W	R/W	R
SNMP	R/W	-	-

Settings	Admin	Supervisor	User
Time			
System Time	R/W	R/W	R
NTP/SNTP Server	R/W	R/W	R
Setting Check	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.

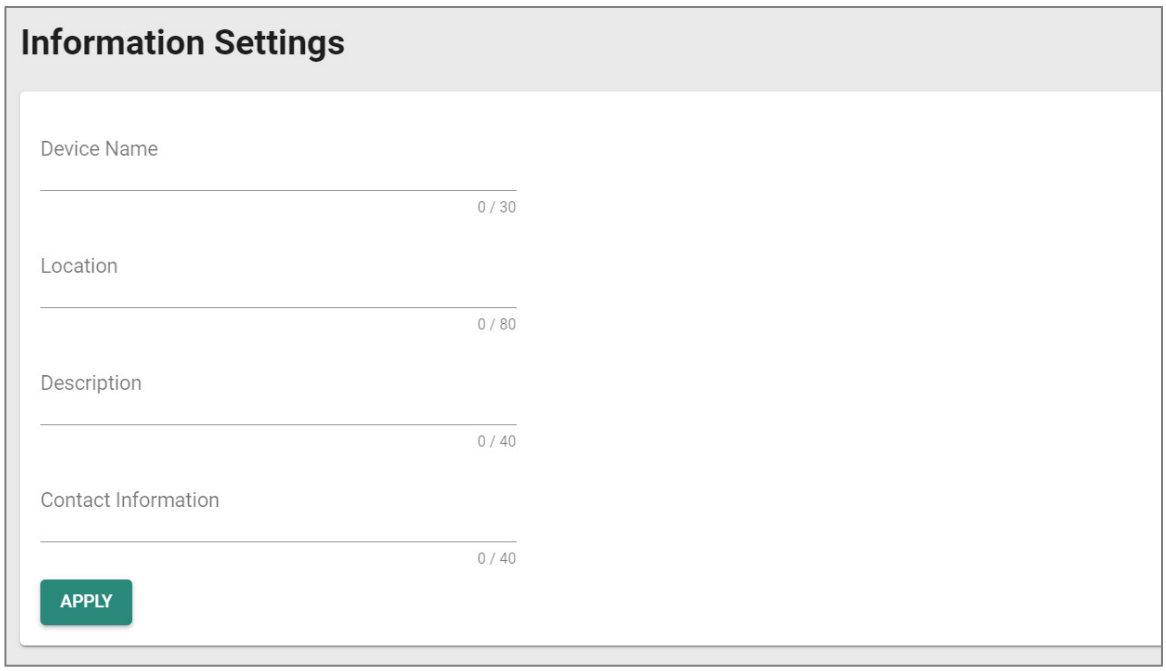
This section includes these pages:

- Information Settings
- Firmware Upgrade
- 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.



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
- Moxa service (refer to the MXview One Series User Manual)

Note

As of v3.12, the device will retain all configuration settings when upgrading to newer firmware.

However, as a precaution, we still recommend backing up your configuration before upgrading firmware. Refer to System > System Management > Configuration Backup and Restore for more information.

Note

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

The device provides specific CLI commands that allow authenticated users to access the CLI interface through SSH at any time and execute commands to obtain the integrity status of the commands and configurations stored on the device. Therefore, it is recommended that system administrators design scripts or programs to connect to the device via SSH regularly.

Users can integrate these CLI commands into system-level scripts for automation or manually verify whether the internal commands and configurations of the device have been modified without authorization.

Warning

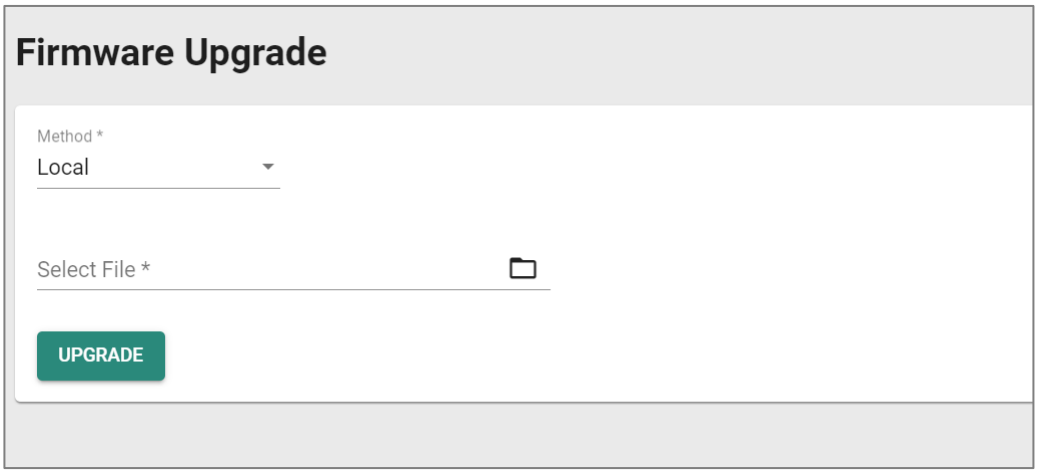
Upgrading the firmware should be only be done by qualified personnel, as it is possible to render the device inoperable if the upgrade is not done properly. If you are not familiar with the process, please request the assistance of qualified personnel. You can also consult with Moxa support and we will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

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

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

Local

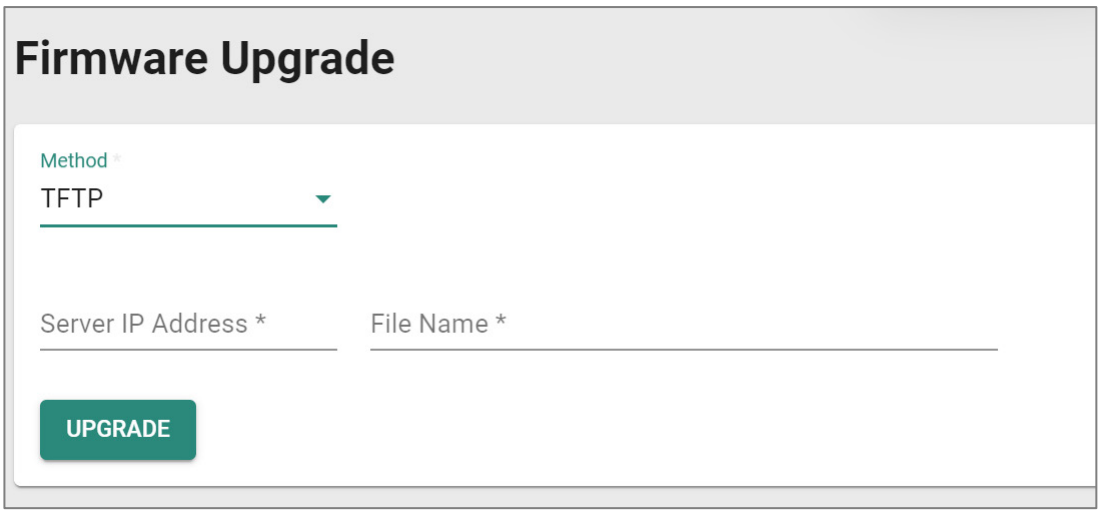
If you select **Local** as your **Method**, these settings will appear. The Local method lets you upload firmware directly from local storage on the host device.



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.

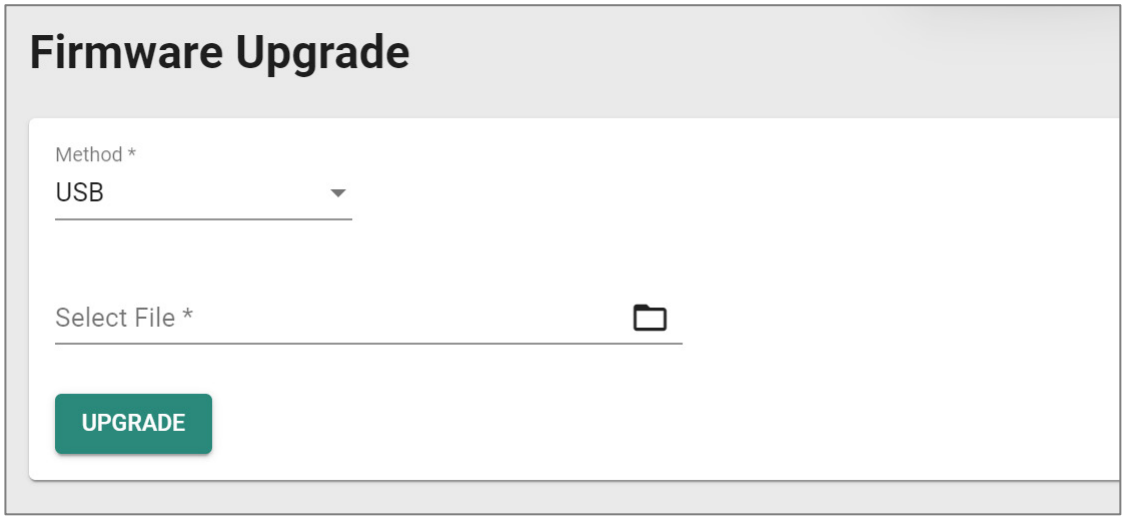


UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the TFTP server.	IP address	N/A
File Name	Specify the filename of the firmware file.	File name	N/A

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.

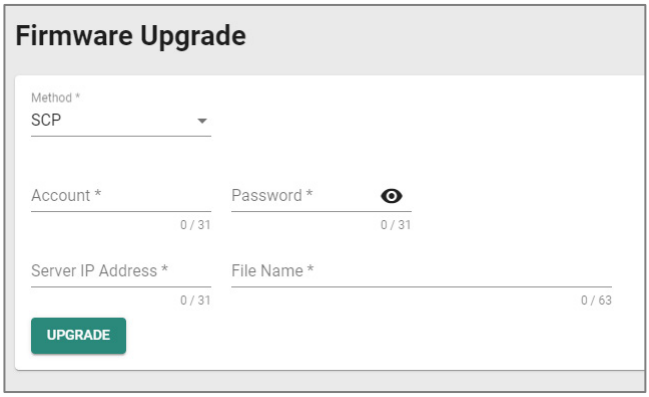
> **Note**
>
> This feature requires USB Function to be enabled in System > Management Interface > Hardware Interface.



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

SCP

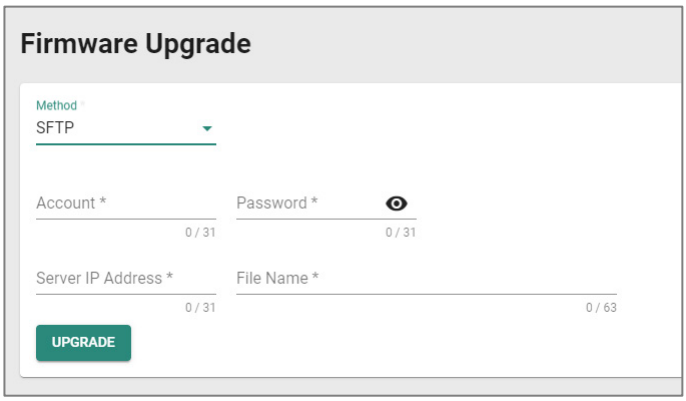
If you select **SCP** as your **Method**, these settings will appear. The SCP (secure copy protocol) method lets you upload and install firmware from a remote system.



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.	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.



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

UI Setting	Description	Valid Range	Default Value
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

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

Note

For the TN-4900 Series, configuration files from firmware version v1.2 are not compatible with firmware v3.0 and higher due to substantial changes made between v1.2 and v3.0. Please create and import a new configuration file when changing from firmware v1.2 to v3.0 or higher. If you encounter any issues, please contact Moxa technical support.

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:

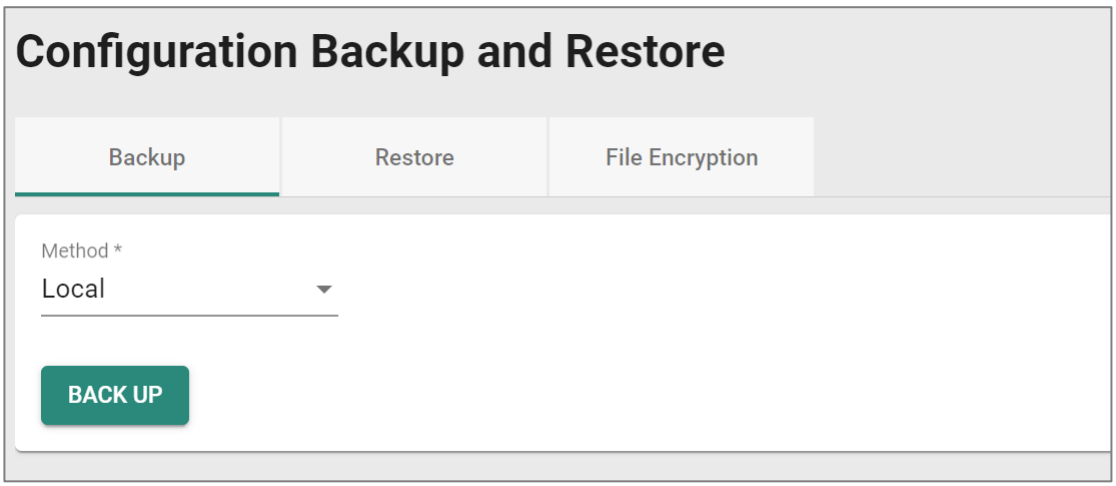
- Local
- TFTP
- USB
- SCP
- SFTP

Note

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

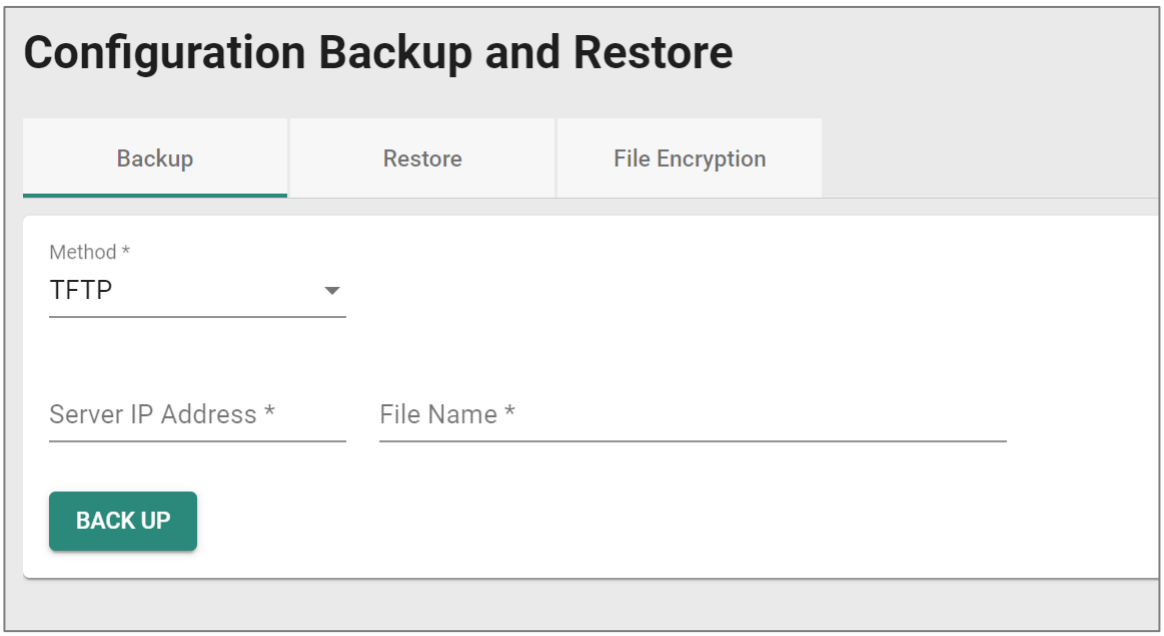
Local

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



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.



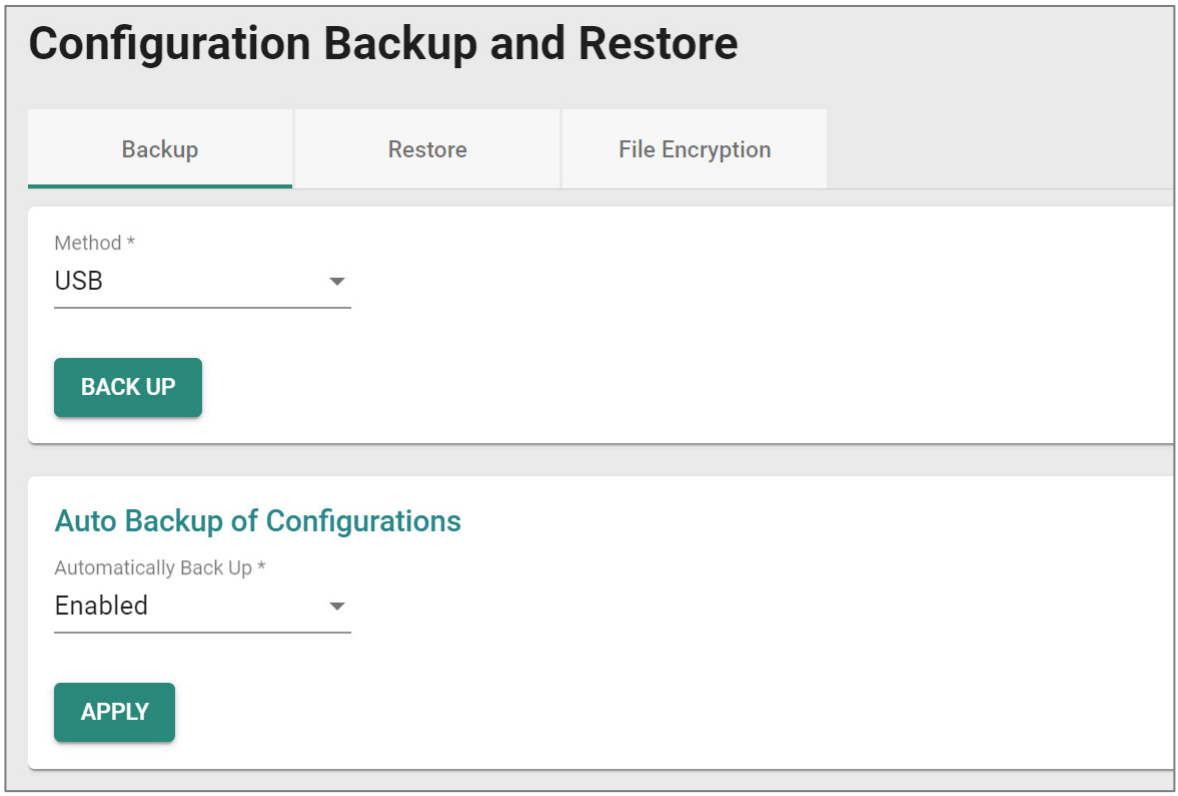
UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the TFTP server.	Valid IP address	N/A
File Name	Specify the file name of the configuration backup file.	1 to 63 characters	N/A

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.

Note

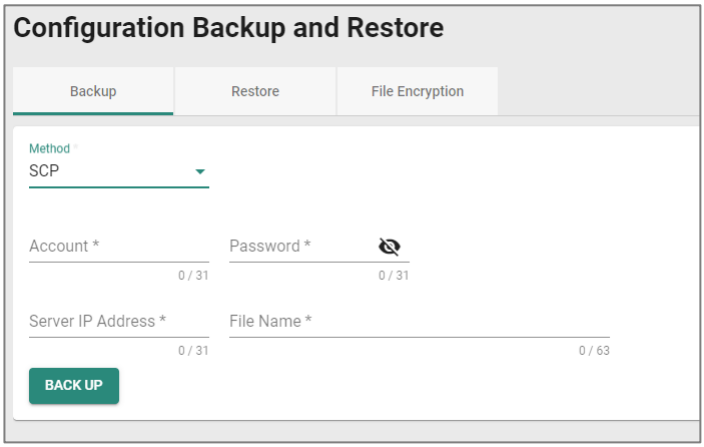
This feature requires USB Function to be enabled in System > Management Interface > Hardware Interface.



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

SCP

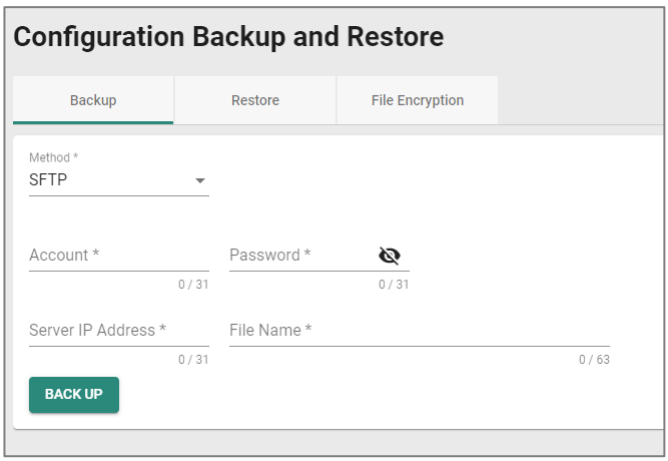
If you select **SCP** as your **Method**, these settings will appear. The SCP (secure copy protocol) method lets you upload the configuration backup file to a remote system.



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.



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

UI Setting	Description	Valid Range	Default Value
File Name	Specify the file name of the configuration backup file.	1 to 63 characters	N/A

Configuration Backup and Restore - Restore

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

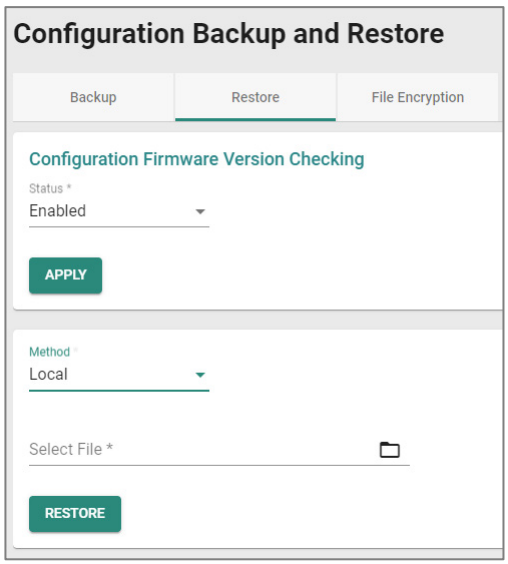
This page lets you restore a previously backed up configuration.

There are multiple methods of restoring the device configuration:

- Local
- TFTP
- USB
- SCP
- SFTP

Local

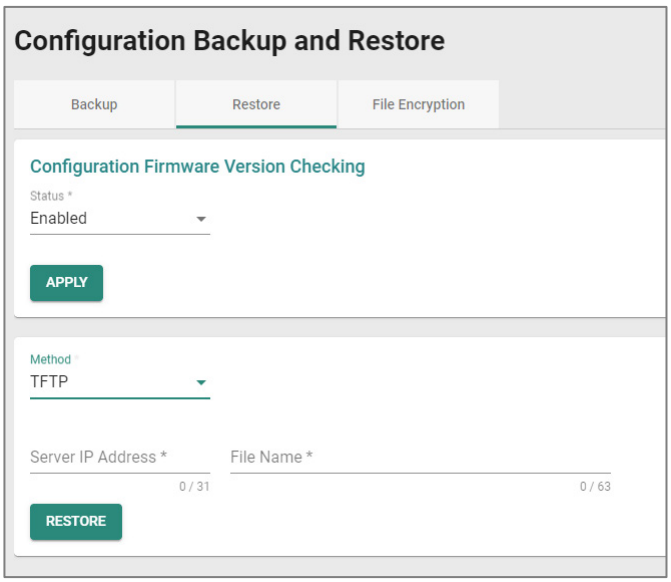
If you select **Local** as your **Method**, these settings will appear. The Local method will restore from a configuration file on the local host.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable configuration file firmware version checking. This checks to make sure the configuration file is for the current firmware version or earlier.	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.

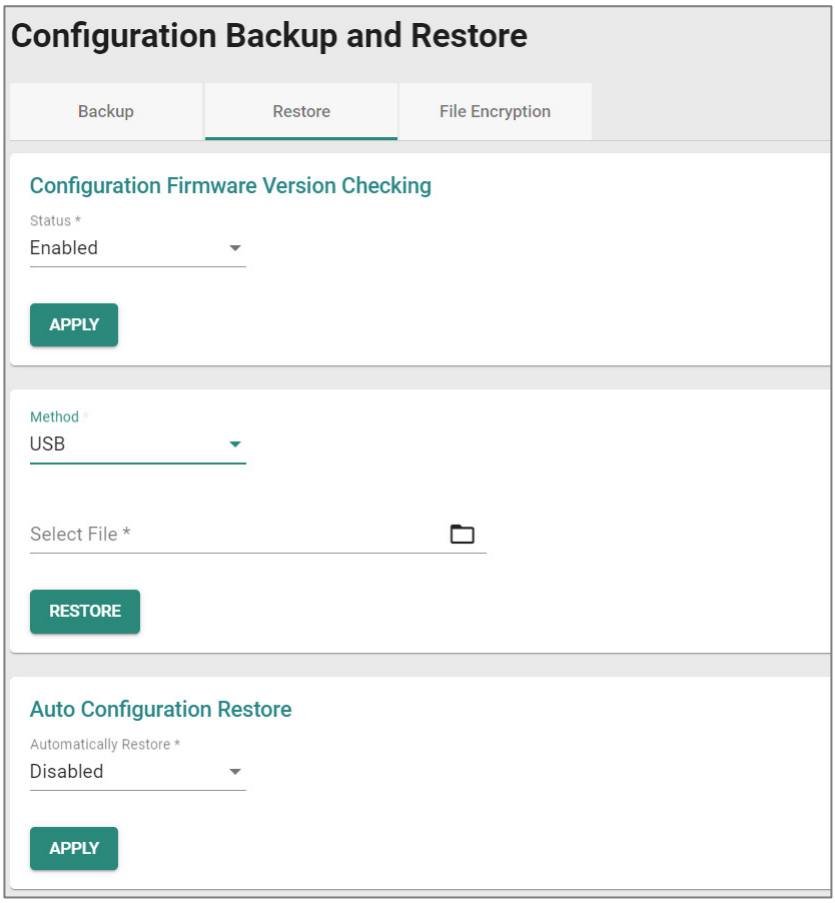


UI Setting	Description	Valid Range	Default Value
Status	Enable or disable configuration file firmware version checking. This checks to make sure the configuration file is for the current firmware version or earlier.	Enabled / Disabled	Disabled
Server IP Address	Specify the IP address of the TFTP server.	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.

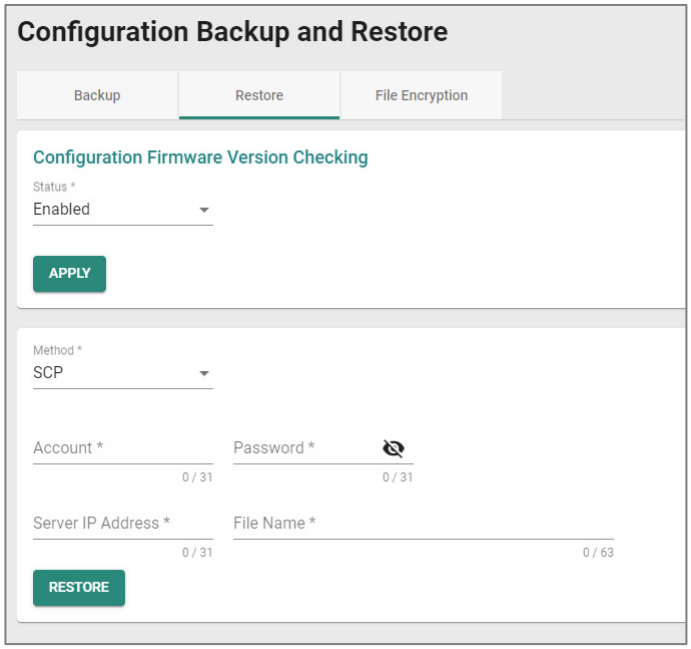
> **Note**
>
> This feature requires USB Function to be enabled in System > Management Interface > Hardware Interface.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable configuration file firmware version checking. This checks to make sure the configuration file is for the current firmware version or earlier. **Note** If the configuration file does not have a version header, it will still be considered to be a valid file to restore from.	Enabled / Disabled	Disabled
Select File	Select the configuration file to restore from.	N/A	N/A
Automatically Restore **(If Method is USB)**	Enable or disable auto restore of the device configuration. If this function is enabled, the device will automatically restore its configuration from an inserted ABC-02 whenever the device is booted. **Note** The auto-restore feature will look for configuration files on an inserted ABC-02 in the following order: 1. An .ini configuration file named with the device's MAC address 2. A sys.ini configuration file	Enabled / Disabled	Disabled

SCP

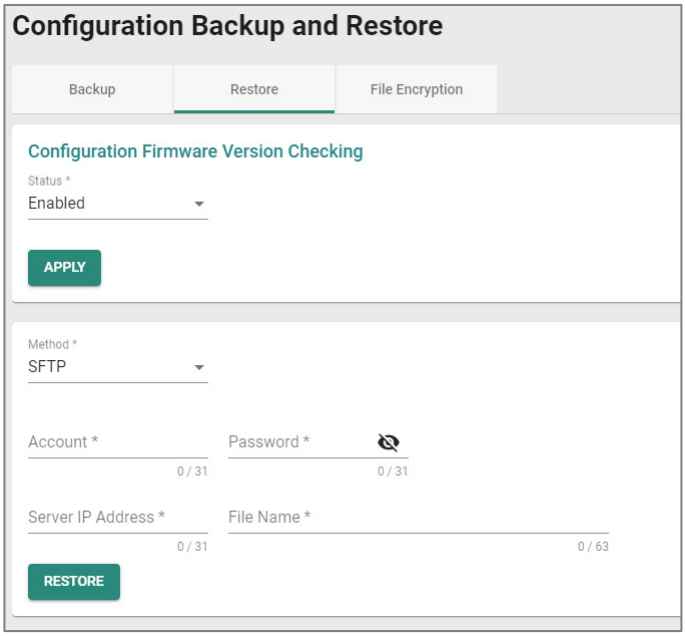
If you select **SCP** as your **Method**, these settings will appear. The SCP (secure copy protocol) method allows you to restore from a configuration file on a remote system.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable configuration file firmware version checking. This checks to make sure the configuration file is for the current firmware version or earlier.	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

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.

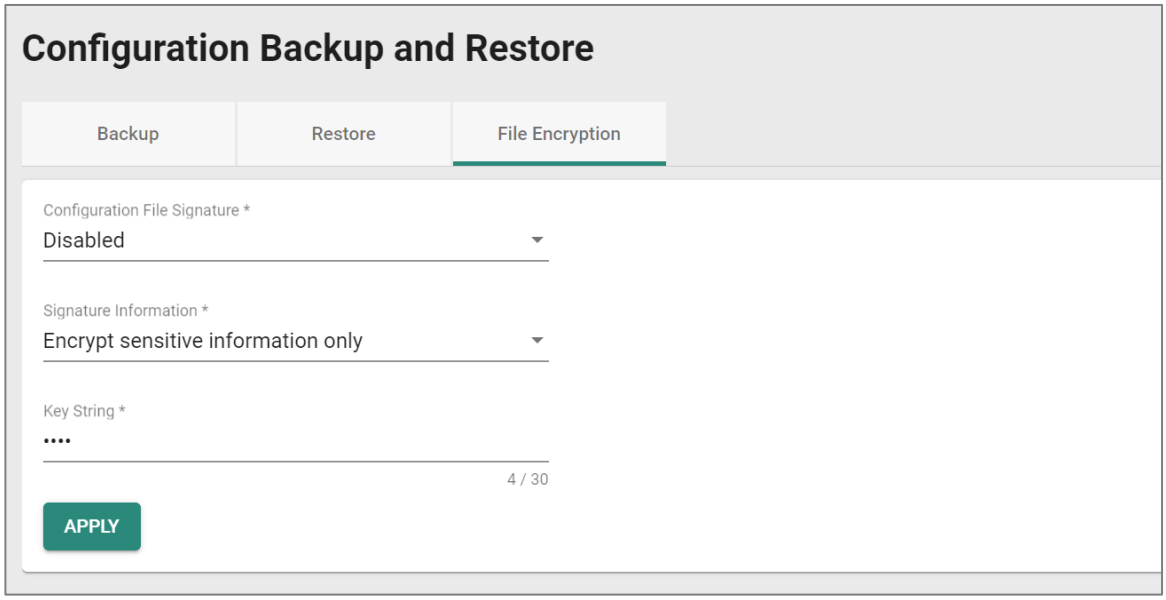


UI Setting	Description	Valid Range	Default Value
Status	Enable or disable configuration file firmware version checking. This checks to make sure the configuration file is for the current firmware version or earlier.	Enabled / Disabled	Disabled
Account	Enter the remote system account name.	1 to 31 characters	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.



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

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

Warning

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:

1. The original firmware version of the user device is V.3.0 or higher.
2. The user downgrades the firmware below to V.3.0 and performs any action on this firmware.
3. 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.

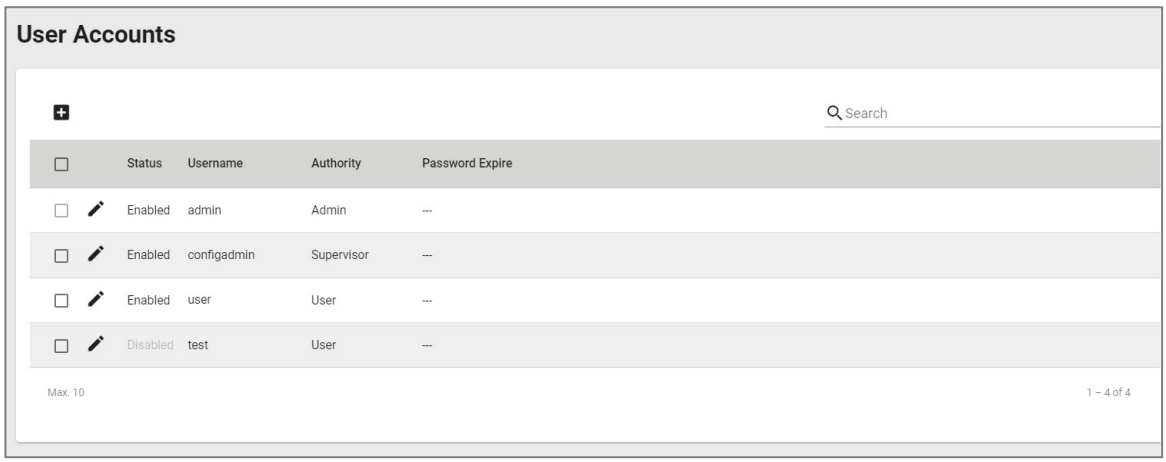
Warning

Starting from firmware v3.17:

- Only the admin account is included in the factory default settings. If you need supervisor or user accounts, you will need to create them manually.
- If you upgrade to firmware v3.17 or later without modifying any of the default user account settings, the system will automatically remove supervisor and user accounts. If any changes have been made to user account settings, such as changing the admin password, then all user accounts will be kept when upgrading the firmware.
- In compliance with the EU Radio Equipment Directive (RED), if the device includes wireless functionality, users must change the password upon first login.

Limitations

You can create up to 10 user accounts.

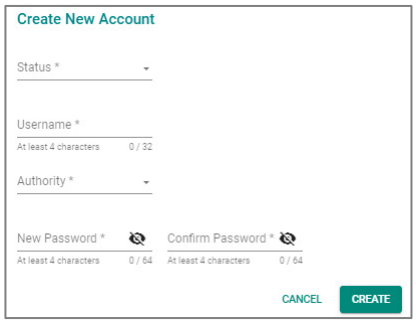


UI Setting	Description
Status	Shows if the account is enabled or disabled.
Username	Shows the username of the account.
Authority	Shows the authority level of the account.
Password Expire	Shows the number of days left before the password expires for the account. A - means the password will not expire. 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: 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.



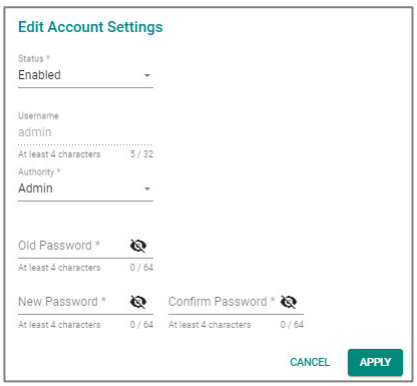
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this user account.	Enabled / Disabled	N/A
Username	Enter a user name for this account.	4 to 32 characters	N/A
Authority	Select an authority role for this account. • **Admin**: The account will have read/write access to all configuration 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
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 64 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 64 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.



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.	4 to 32 characters	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 64 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 64 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 64 characters, additional requirements are based on settings in **System > Account Management > Password Policy**	N/A

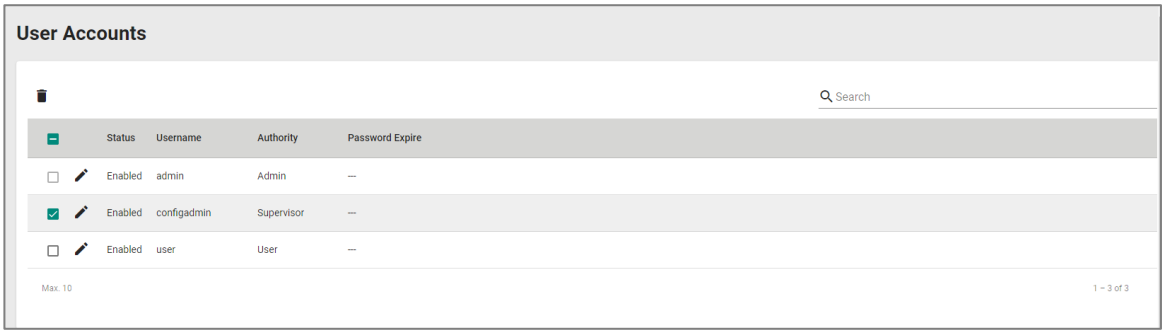
Delete User Account

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.

Note

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



Password Policy

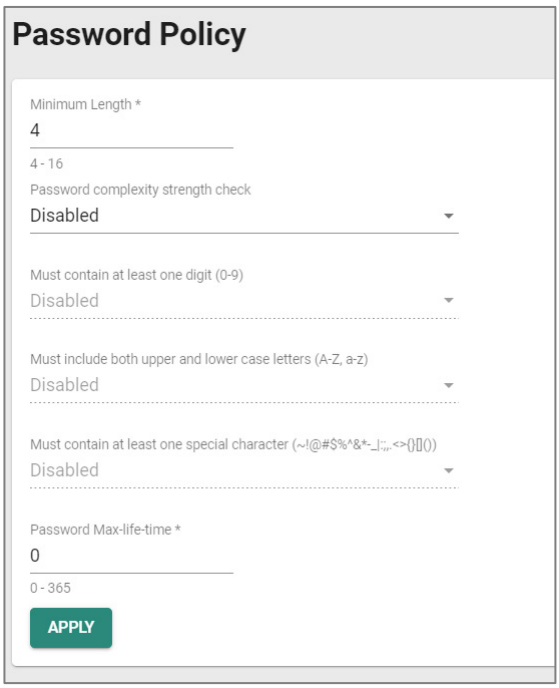
Menu Path: System > Account Management > Password Policy

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.



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
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

UI Setting	Description	Valid Range	Default Value
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

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
- Ping Response
- SNMP

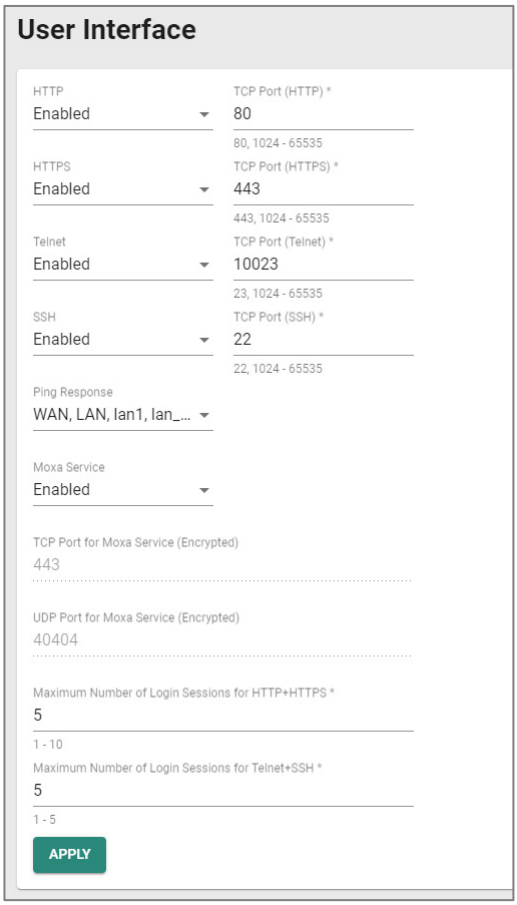
User Interface

Menu Path: System > Management Interface > User Interface

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

Note

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



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

UI Setting	Description	Valid Range	Default Value
HTTPS	Enable or disable HTTPS connections. **Note** The administrator can manually import a self-signed certificate (in .p12 format) for web server (HTTPS) services. However, the administrator should check the root certificate and validity of the signature before importing, according to the organization's security procedures and requirements. After importing a certificate, the administrator should check if the certificate has been revoked and if so, the certificate must be replaced. When 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
Ping Response	Tick the selected interface to be ping. **Note** To ping selected interface, make sure the interface is checked in **Ping Response**.	Drop-down check box	N/A

UI Setting	Description	Valid Range	Default Value
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

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

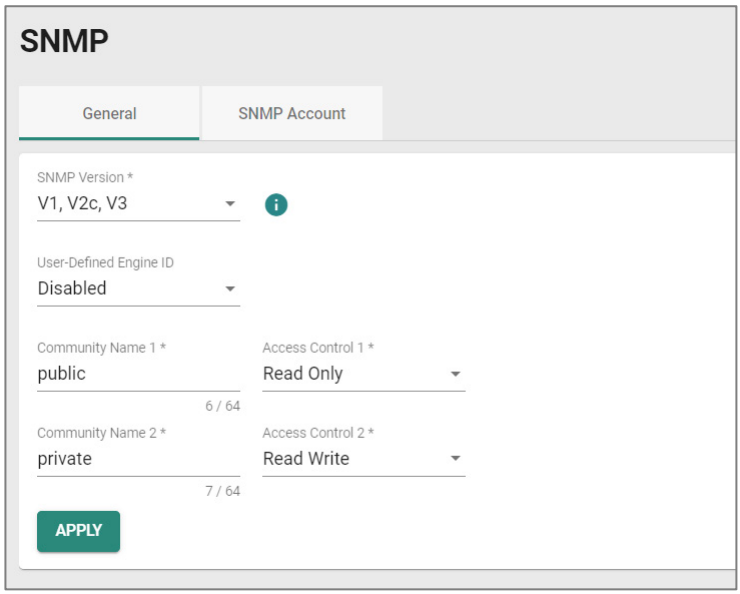
SNMP - General

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.



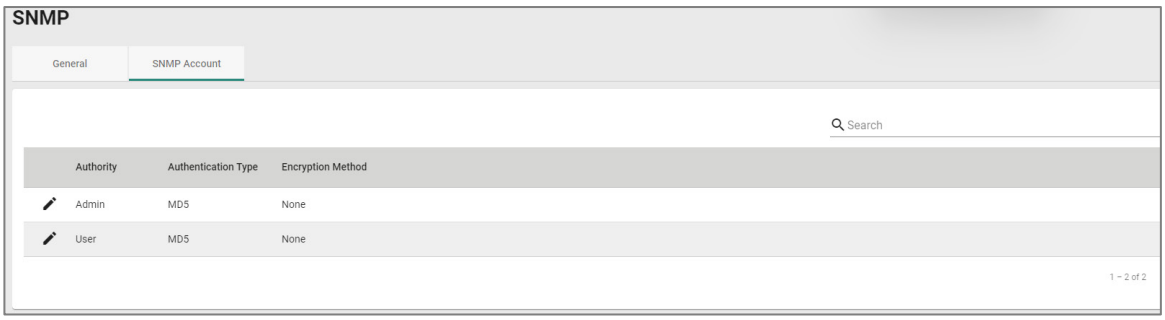
UI Setting	Description	Valid Range	Default Value
SNMP Version	Specify the SNMP protocol version used to manage your device. **Disabled**: Disable SNMP. **V1, V2c, V3**: Enable SNMP V1, V2c, and V3. **V1, V2c**: Enable SNMP V1, V2c only. **V3 only**: Enable SNMP V3 only.	Disabled / V1, V2c, V3 / V1, V2c / V3 only	Disabled
User-Defined Engine ID **(Only for SNMP Verison is V1, V2c, V3 or V3 only)**	Enable or disable use of a user-defined engine ID. If disabled, the system will use the default engine ID.	Disabled / Enabled	Disabled
Engine ID	Specify an engine ID to manage your device. If **User-Defined Engine ID** is disabled, the engine ID will be view-only.	2 to 54 hexadecimal character string. The length of the string must be even.	800021f305

UI Setting	Description	Valid Range	Default Value
Community Name 1	Specify a community string name match to use for authentication.	1 to 64 characters	public
Community Name 2	Specify a community string name match to use for authentication.	1 to 64 characters	private
Access Control 1	Specify the access control type to use when Community String 1 is matched.	Read Write / Read only / No Access	Read Only
Access Control 2	Specify 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.

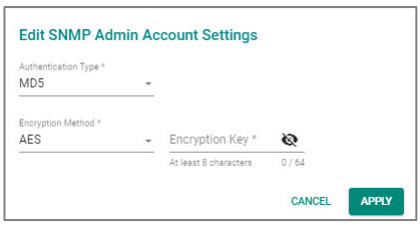


UI Setting	Description
Authority	Shows authority level of the management account. **admin**: Can read/write configuration settings. **user**: Can only read configuration settings.
Authentication Type	Shows the authentication type used for the account.
Encryption Method	Shows the encryption method used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



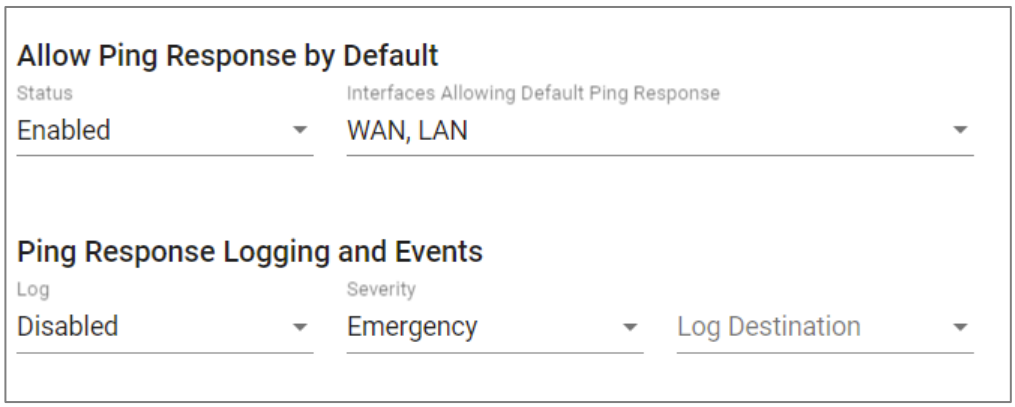
UI Setting	Description	Valid Range	Default Value
Authentication Type	Select which authentication method to use for the account. **None**: No authentication will be used. **MD5**: Use MD5 authentication. **SHA**: Use SHA authentication. **SHA-256**: Use SHA-256 authentication. **SHA-512**: Use SHA-512 authentication.	None / MD5 / SHA / SHA-256 / SHA-512	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 64 characters	N/A

Ping Response

Menu Path: System > Management Interface > Ping Response Policy

This page allows you to configure and manage ping response policies that let you control how your device handles incoming ping requests.

Ping Response Settings



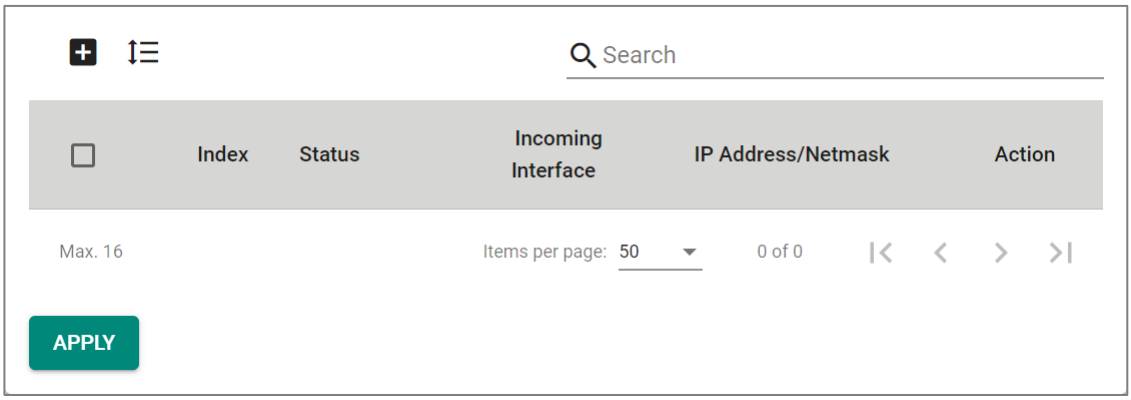
Allow Ping Response by Default

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable allowing ping responses to ping requests through the specified interfaces by default. **Note** If Status is set to Disabled, ping responses will be denied for all ping requests by default. **Note** Ping response policies will override the default behavior.	Enabled / Disabled	Disabled
Interfaces Allowing Default Ping Response	Select the interfaces to allow ping responses for by default.	Drop-down list of interfaces	Existing interfaces

Ping Response Default Rule Event Setting

UI Setting	Description	Valid Range	Default Value
Log	Enable or disable global policy event logging. This will allow event logging for actions taken due to the global policy.	Enabled /Disabled	Disabled
Severity	Select the severity level to assign events for this policy. Refer to Severity Level List for more information.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A
Log Destination	Select the default action log destination.	Syslog / Trap / Local Storage	N/A

Ping Response Policy List



UI Setting	Description
Index	Shows the index of the ping response policy.
Status	Shows whether the policy is enabled.
Incoming Interface	Shows the interface this policy will monitor for ping requests through this policy.
IP Address/Netmask	Shows the IP address and netmask to monitor for ping requests through this policy.
Action	Shows whether the device will allow or deny ping responses for matching ping requests through this policy.

Create Ping Response Policy

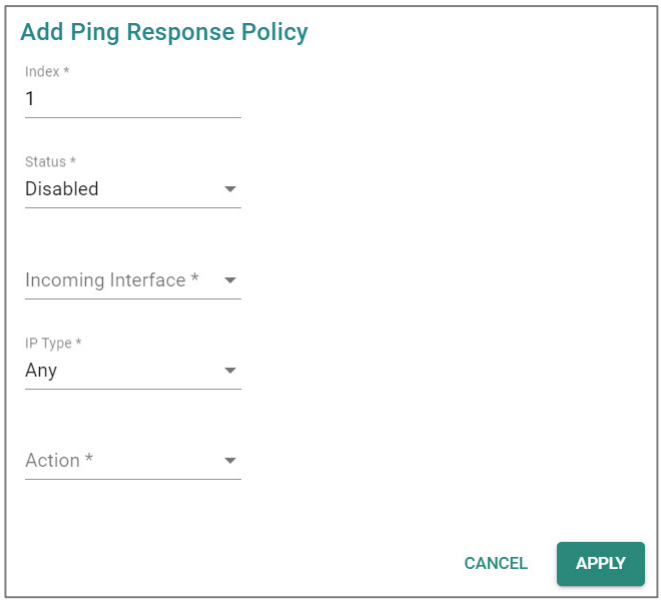
Menu Path: System > Management Interface > Ping Response Policy

Clicking the **Add (+)** icon on the

Unable to render include or excerpt-include. Could not retrieve page.

page will open this dialog box. This dialog lets you create a new ping response policy.

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



UI Setting	Description	Valid Range	Default Value
Index	Specify the index for the ping response policy.	1 to 16	Next available index
Status	Enable or disable the ping response policy.	Enabled /Disabled	Disabled
Incoming Interface	Select the interface this policy will monitor for ping requests.	Drop-down list of interfaces	N/A
IP Type	Select the IP type to monitor for ping requests for this policy.	Any / Single IP / Subnet	Any
IP Address **(If IP Type is Single IP or Subnet)**	Specify the IP address to monitor for ping requests through this policy.	Valid IP Address	N/A

UI Setting	Description	Valid Range	Default Value
Netmask **(If IP Type is Subnet)**	Specify the netmask to monitor for ping requests through this policy.	Drop-down list of netmask	N/A
Action	Select whether the device will allow or deny ping responses for matching ping requests through this policy.	Allow / Deny	N/A

Edit Ping Response Policy

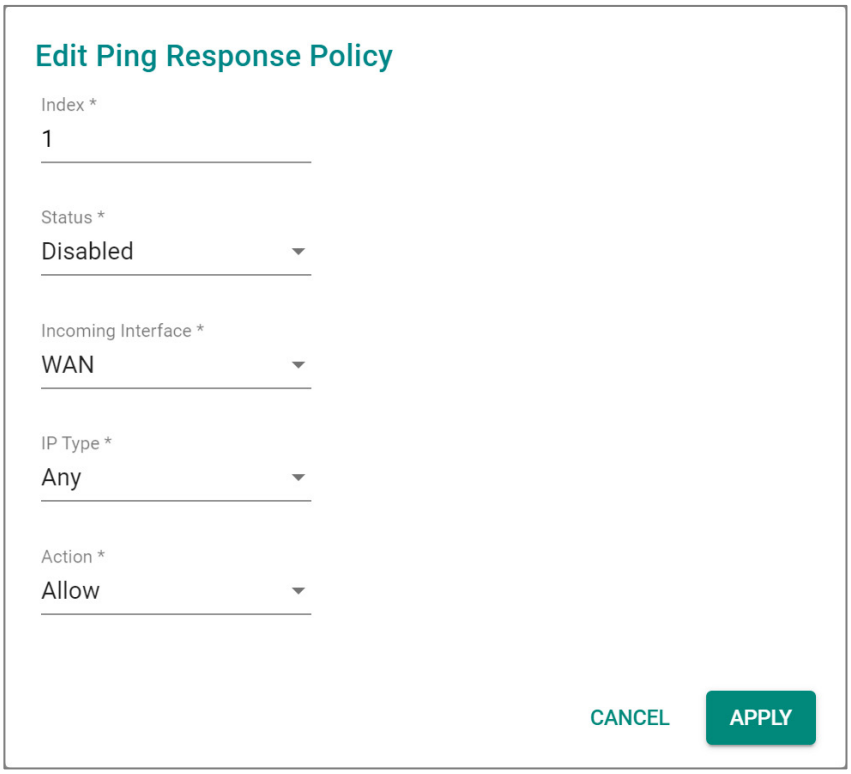
Menu Path: System > Management Interface > Ping Response Policy

Clicking the **Edit ( )** icon for a policy on the

Unable to render include or excerpt-include. Could not retrieve page.

page will open this dialog box. This dialog lets you edit an existing policy.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Index	Specify the index for the ping response policy.	1 to 16	Next available index
Status	Enable or disable the ping response policy.	Enabled /Disabled	Disabled
Incoming Interface	Select the interface this policy will monitor for ping requests.	Drop-down list of interfaces	N/A
IP Type	Select the IP type to monitor for ping requests for this policy.	Any / Single IP / Subnet	Any
IP Address **(If IP Type is Single IP or Subnet)**	Specify the IP address to monitor for ping requests through this policy.	Valid IP Address	N/A
Netmask **(If IP Type is Subnet)**	Specify the netmask to monitor for ping requests through this policy.	Drop-down list of netmask	N/A
Action	Select whether the device will allow or deny ping responses for matching ping requests through this policy.	Allow / Deny	N/A

Delete Ping Response Policy

Menu Path: System > Management Interface > Ping Response Policy

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

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

> **Note**
>
> 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 > Time > System Time - Time

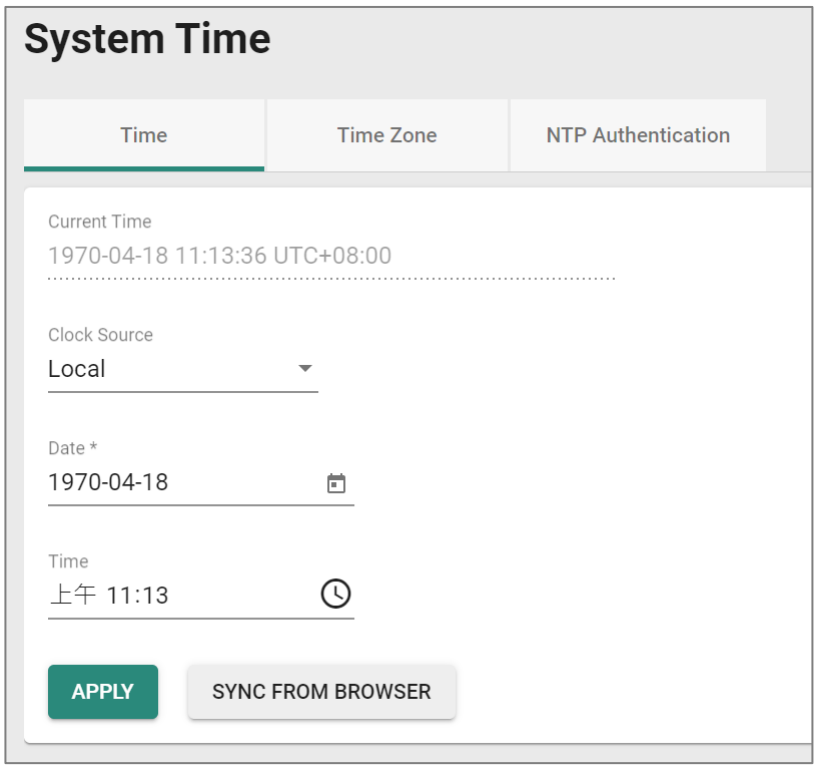
This page lets you set the system time and date.

You can set your system time using these clock sources:

- Local
- SNTP
- NTP

System Time Settings - Local

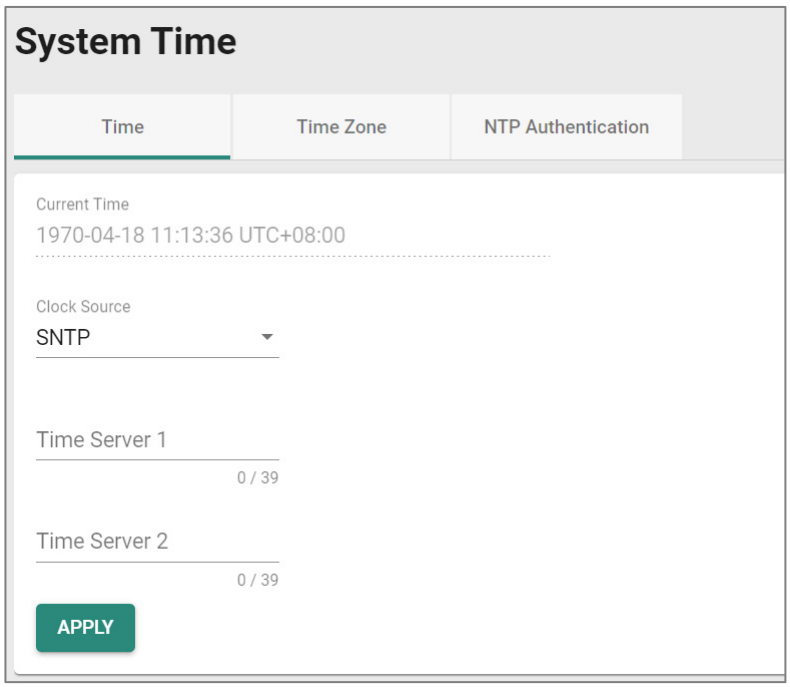
If you select **Local** as your **Clock Source**, these settings will appear. Local lets you set your device's system time manually, or you can copy the time from your local host by clicking **SYNC FROM BROWSER**. Click **APPLY** to save your changes.



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

System Time Settings - SNTP

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.

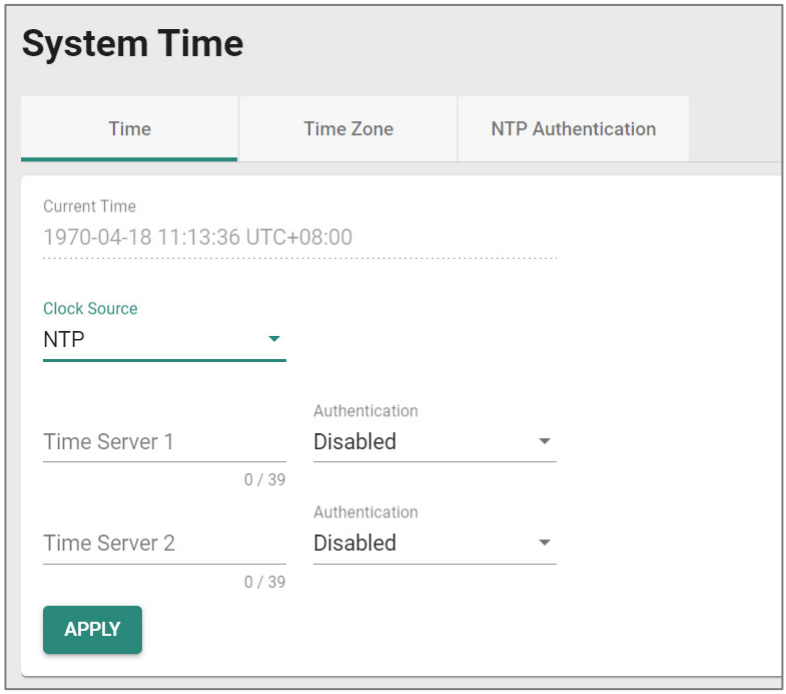


UI Setting	Description	Valid Range	Default Value
Current Time	This shows the device's current system date, time, and time zone.	N/A	N/A
Time Server 1	Set the IP or domain address of the primary time server (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	IP address or domain, 1 to 39 characters	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

System Time Settings - NTP

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.

> **Note**
>
> When synchronizing device time using NTP, we recommend using NTP authentication to reduce cybersecurity risks.



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

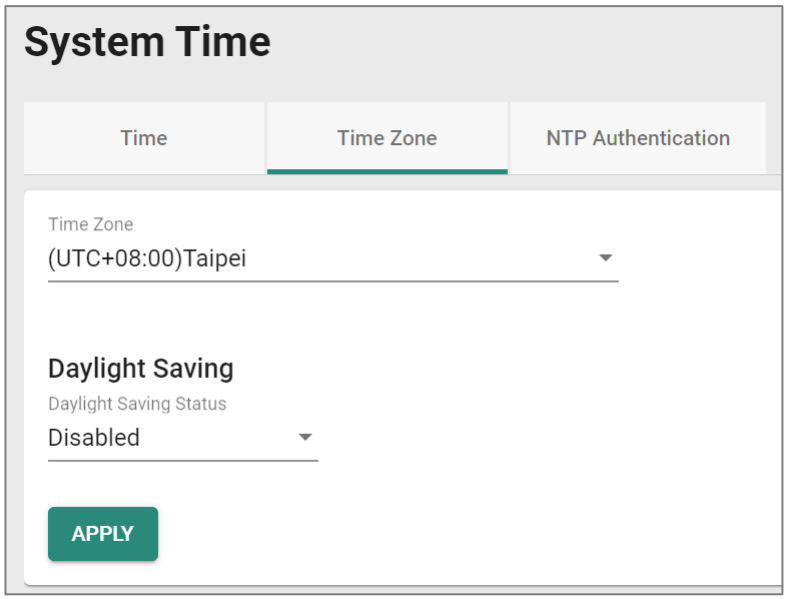
System Time - Time Zone

Menu Path: System > Time > System Time - Time Zone

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

Note

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



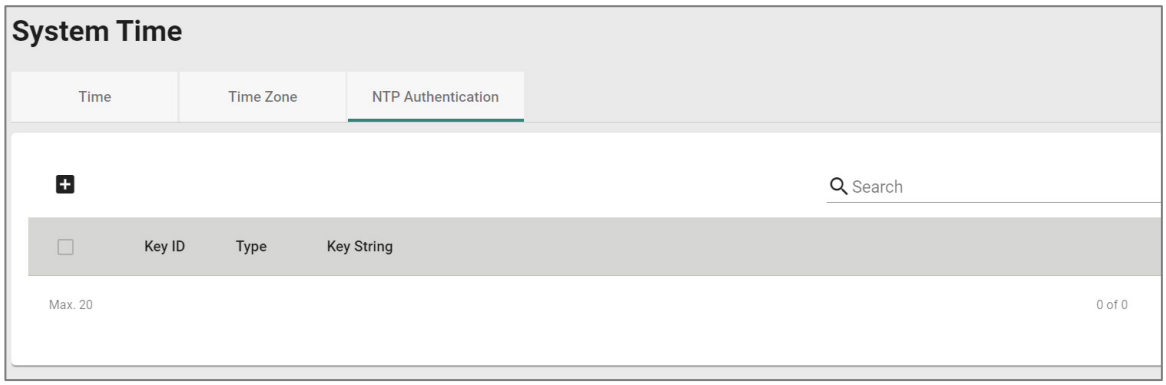
UI Setting	Description	Valid Range	Default Value
Time Zone	Select a time zone from the list of UTC (Coordinated Universal Time) time zones.	N/A	N/A
Daylight Saving Status	Enable or disable Daylight Saving time adjustment.	Enabled / Disabled	Disabled
Offset (if Daylight Saving Status is Enabled)	Set the 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
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 > Time > 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.

> **Note**
> When synchronizing device time using NTP, we recommend using NTP authentication to reduce cybersecurity risks.

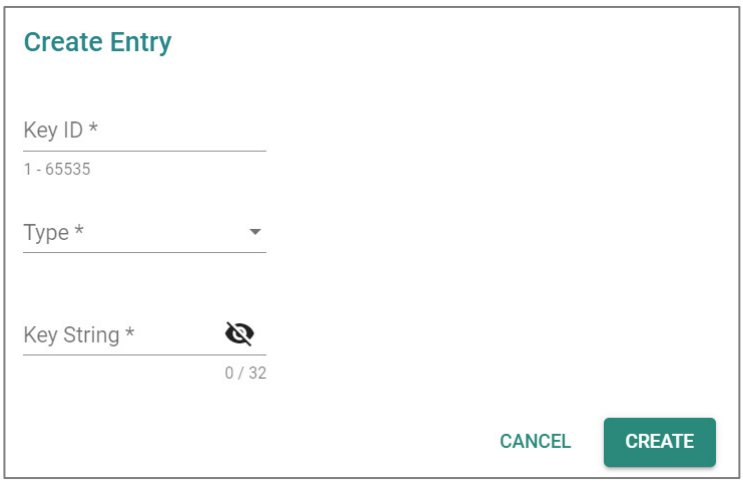


UI Setting	Description
Key ID	Shows the key ID for the authentication key.
Type	Shows the type of NTP authentication the key uses. **MD5**: Uses authentication based on MD5 algorithms. **SHA**: Uses authentication based on SHA-512 algorithms.
Key String	Shows the key string used by the authentication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

Create Entry

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

Clicking the **Add (⊞)** icon on the **System > Time > 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
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

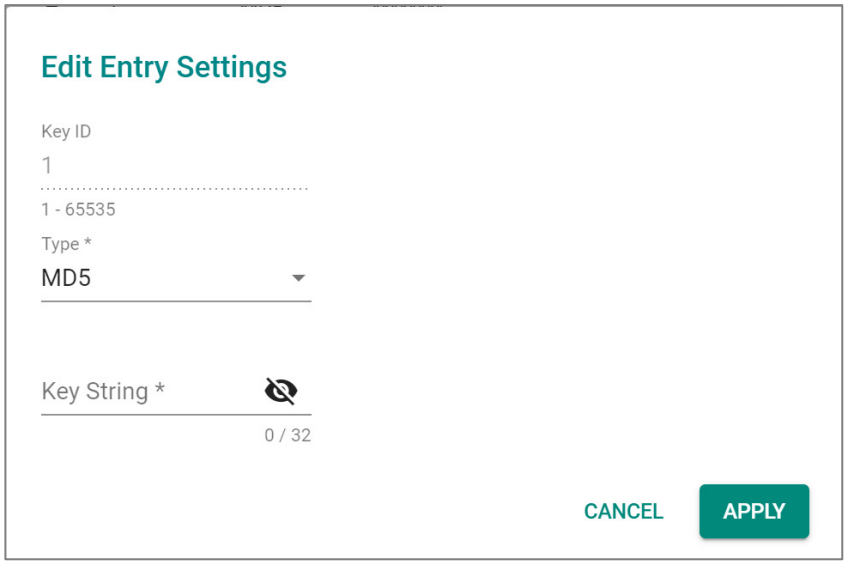
Edit Entry

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

Clicking the **Edit ( )** icon for a key on the **System > Time > 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.

Note

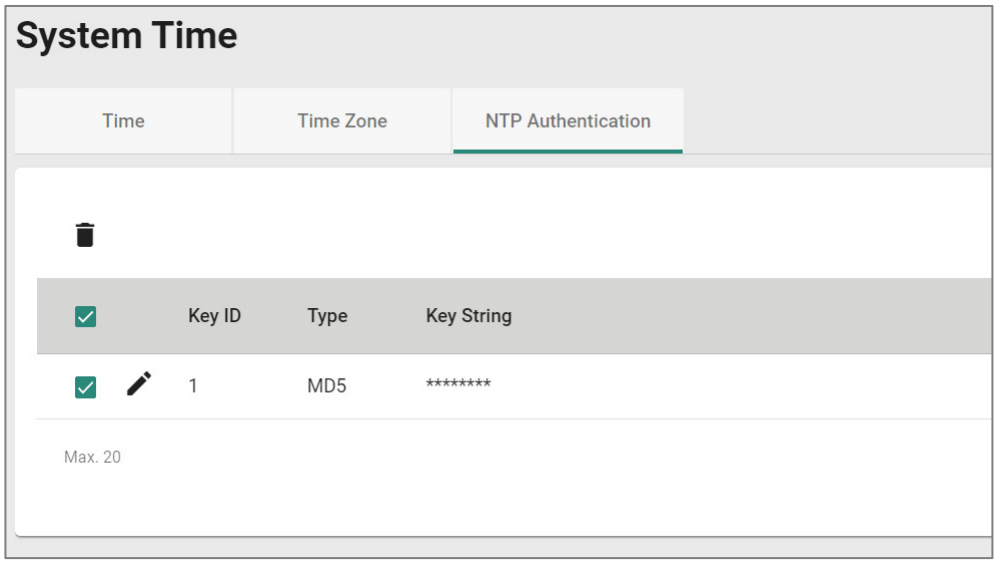
All key parameters can be modified, except for the key ID. To modify the key ID, you must create a new authentication key.



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-512	N/A
Key String	Specify the key string to use for the authentication key.	1 to 32 characters	N/A

Delete Entry

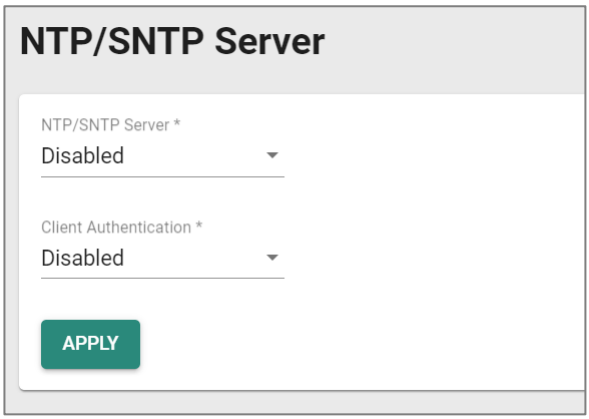
You can delete authentication keys by using the checkboxes to select the keys you want to delete, then clicking the **Delete ( )** icon.



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.



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**

UI Setting	Description	Valid Range	Default Value
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 > System Time - NTP Authentication** for more information. **Disabled**: Disable Client Authentication functionality for clients.	**Enabled / Disabled**	**Disabled**

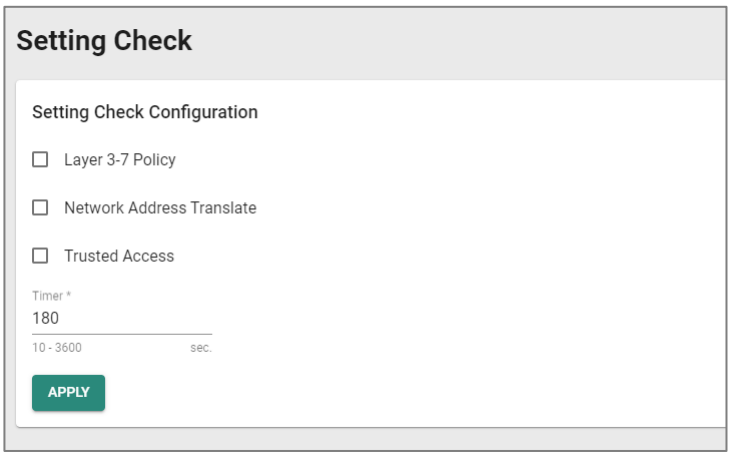
Setting Check

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



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
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
Ports			
Port Settings	R/W	R/W	R
Layer 2 Switching			
VLAN	R/W	R/W	R
MAC Address Table	R/W	R/W	R
Network Interfaces	R/W	R/W	R

Ports

Menu Path: Network Configuration > Ports

This section includes these pages:

- Port Settings

Port Settings

Menu Path: Network Configuration > Ports > Port Settings

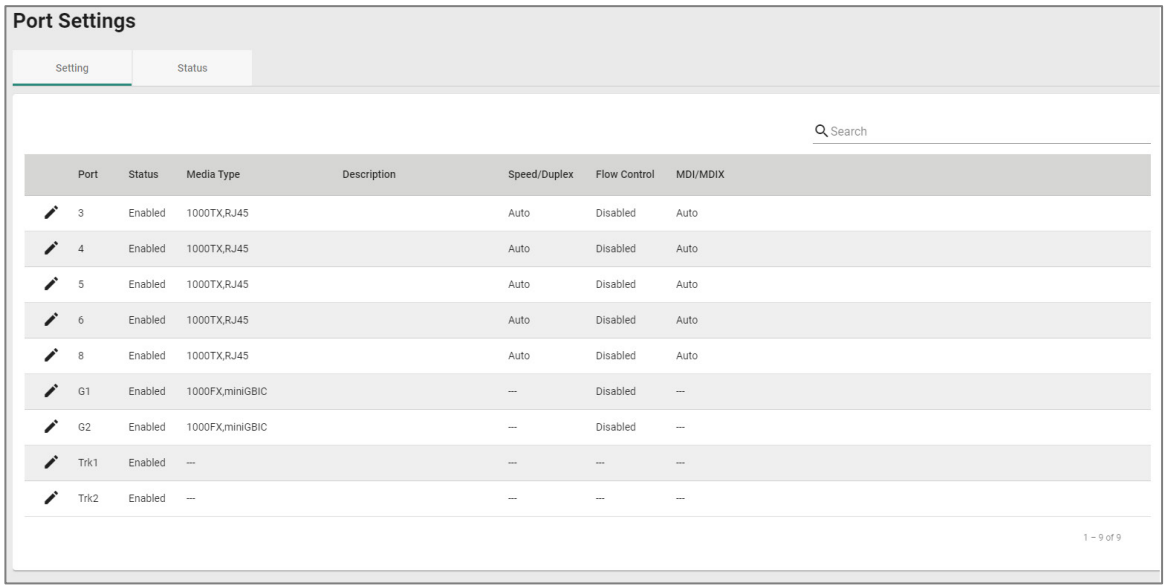
This page includes these tabs:

- Settings
- Status

Port Settings - Settings

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

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



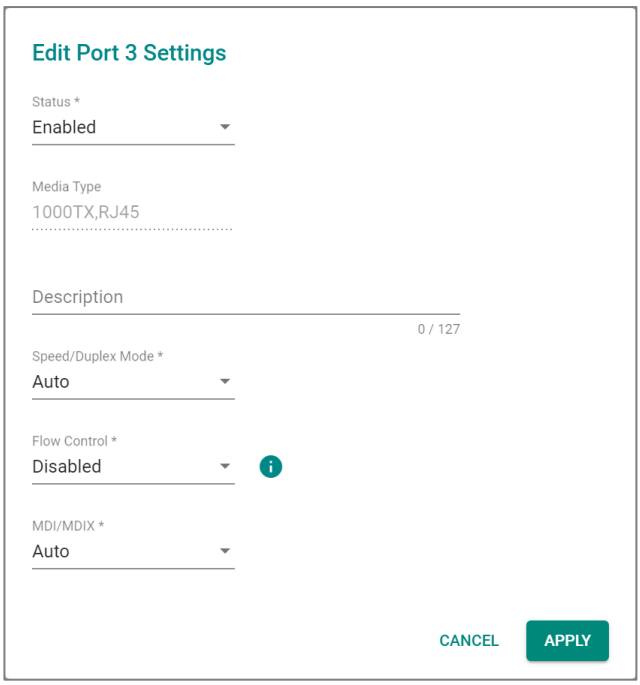
UI Setting	Description
Port	Shows which port this row describes.
Status	Shows the status of the port.
Media Type	Shows the port's media type.
Description	Shows the description for the port.
Speed / Duplex	Shows the speed and duplex mode for the port.
Flow Control	Shows the whether flow control is enabled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

UI Setting	Description
MDI / MDIX	Shows the MDI/MDIX setting for the port.

Edit Port Settings

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



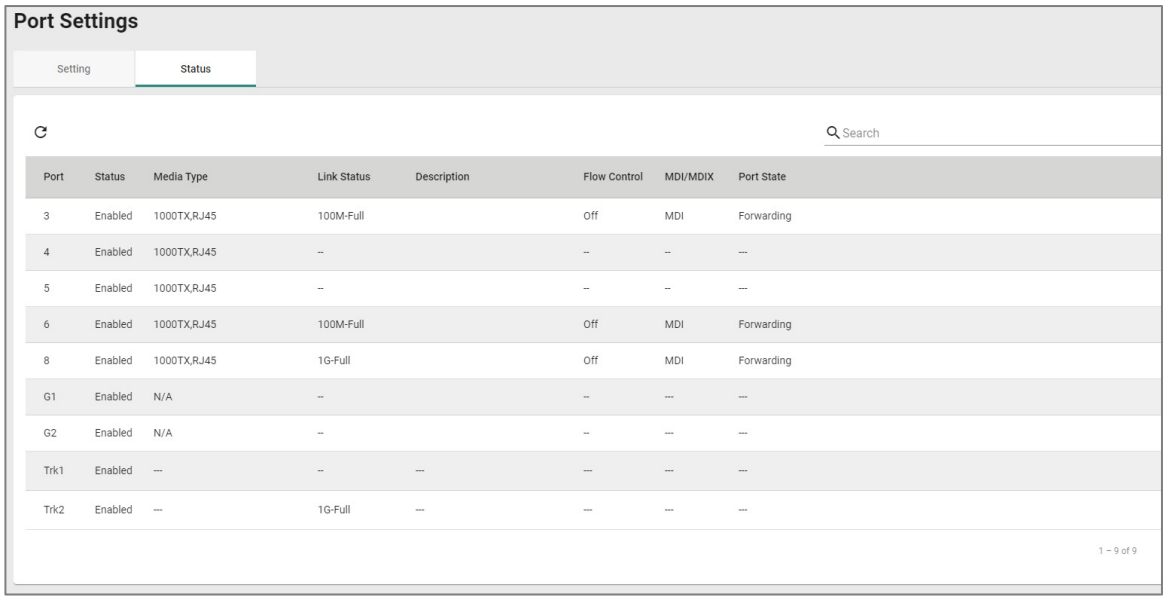
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the port.	Enabled / Disabled	Enabled
Media Type	Displays the port's media type. This setting cannot be changed.	N/A	Port's media type
Description	Enter a description for the port to make it easier to identify.	1 to 127 characters	N/A

UI Setting	Description	Valid Range	Default Value
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
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** Flow Control can be enabled or disabled but is only effective in full-duplex. Back Pressure is enabled by default but works only in half-duplex. When using the SFP ports for WAN1 or WAN2 on the EDR-G9004, Flow Control will be ineffective. **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

Port Settings - Status

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

This tab lets you monitor the status of each port. Click the **Refresh (** ⟳ **)** button to refresh the table.



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.
Link Status	Shows the speed and duplex mode the connection is currently using. If the link is not active, a – will be shown.
Description	Shows the description for the port.
Flow Control	Shows the whether flow control is currently on or off for the port. If the link is not active, a – will be shown.
MDI / MDIX	Shows whether the port is using MDI or MDIX for its connection. If the link is not active, a – will be shown.
Port State	Shows the port state for the port. If the link is not active, a – will be shown.

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

VLAN

Menu Path: Network Configuration > Layer 2 Switching > VLAN

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

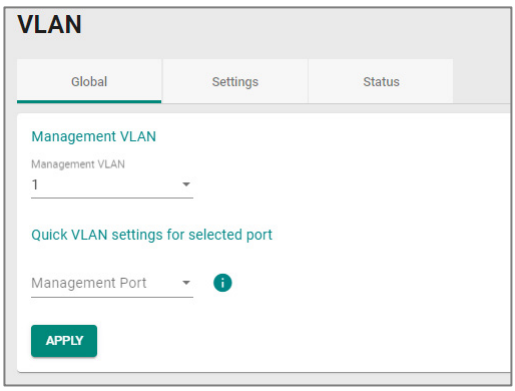
This page includes these tabs:

- 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.



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. **Note** If you do not intend to use the device purely as a Layer 2 switch, it is strongly recommended that you do not use trunk VLANs for most use cases.	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
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

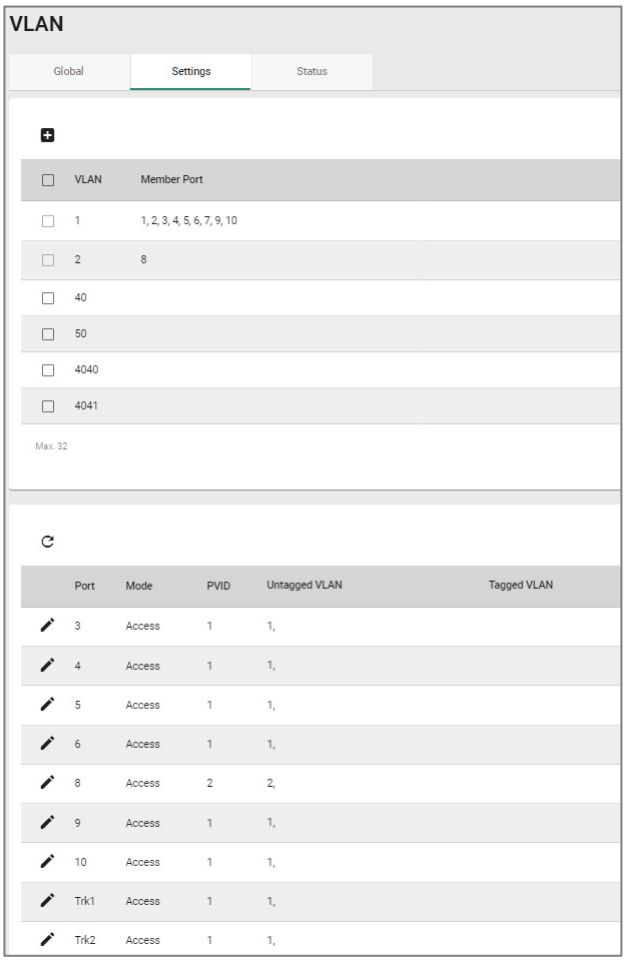
VLAN - Settings

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.

> **Note**
> Please note that port numbers may vary depending on product model.

> **Limitations**
> You can create up to 32 VLANs.



The top table shows a list of VLANs.

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

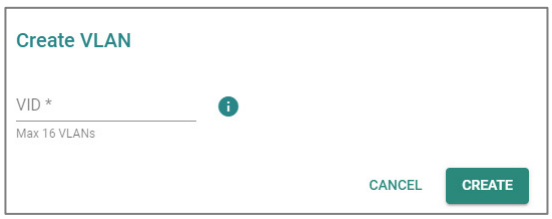
The bottom table shows a list of the device's ports and their VLAN settings.

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.

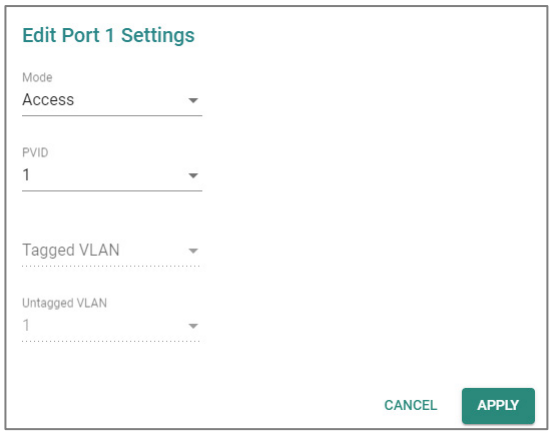


UI Setting	Description	Valid Range	Default Value
VID	Specify the VID to use for the VLAN. You can create multiple VLANs at once by entering single VIDs or VID ranges separated by commas, such as 2, 4-8, 10-13.	1 to 4094. You can enter multiple VIDs and/or VID ranges, separated by commas.	N/A

VLAN - Settings - 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.

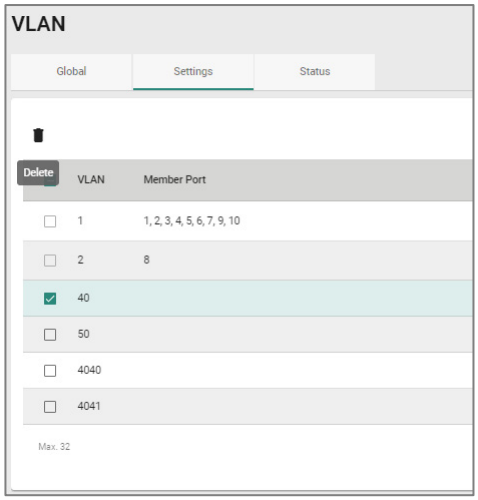


UI Setting	Description	Valid Range	Default Value
Mode	Specify which VLAN mode the port should use: **Access**: Define the port as an Access port. This is used when connecting to single devices without tags. **Trunk**: Define the port as a Trunk port. This is used when connecting to another 802.1Q VLAN-aware 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
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 - Settings - Delete VLAN

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

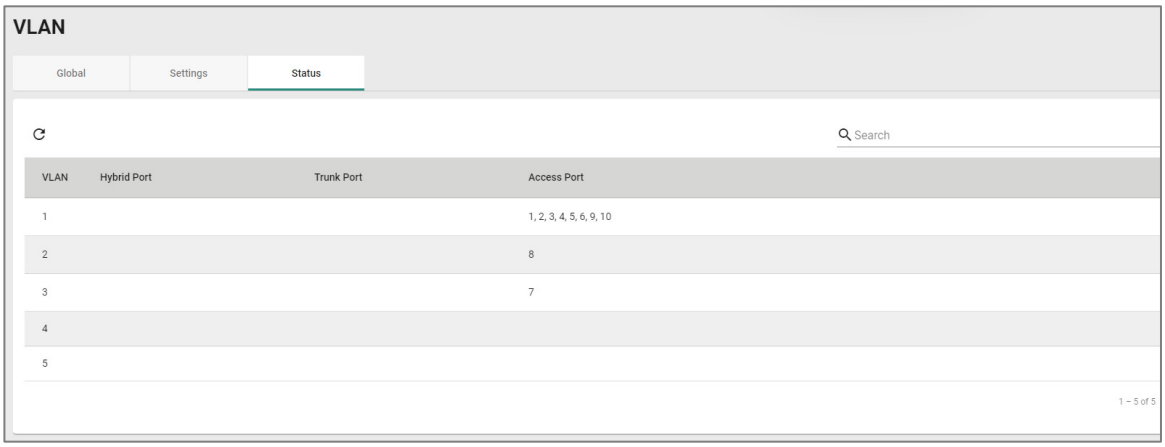
You can delete VLANs by using the checkboxes to select the VLANs you want to delete, then clicking the **Delete ( )** icon.



VLAN - Status

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

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



UI Setting	Description
VLAN	Shows the VID of the VLAN.

UI Setting	Description
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.

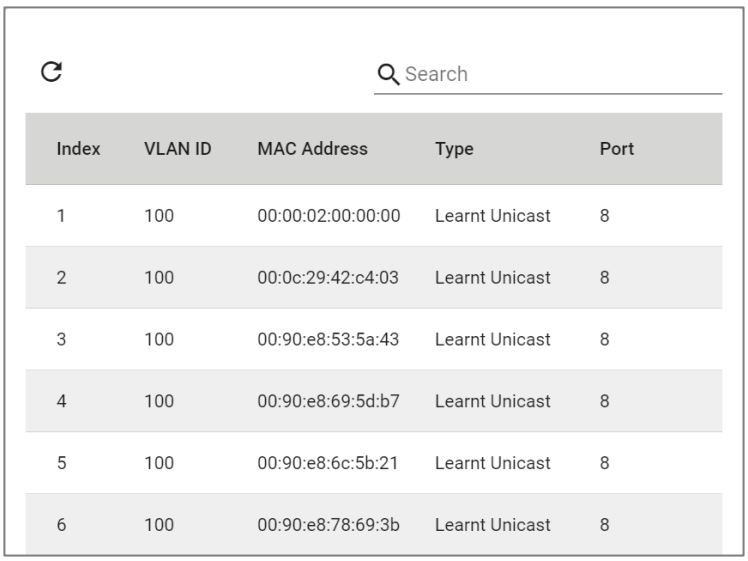
MAC Address Table

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 Settings

MAC Address Table



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.

UI Setting	Description
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.

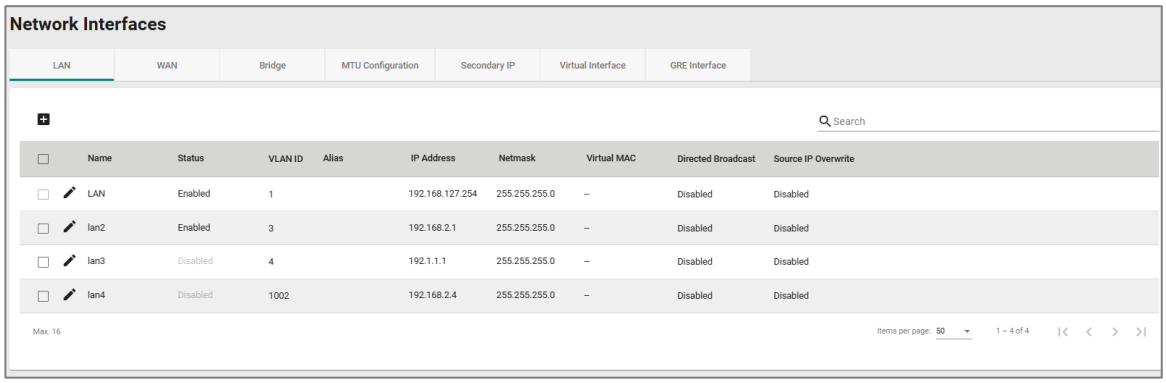
Network Interfaces

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/WAN1
- Secondary IP



LAN

Menu Path: Network Configuration > Network Interfaces - LAN

This tab lets you manage your LAN interfaces.

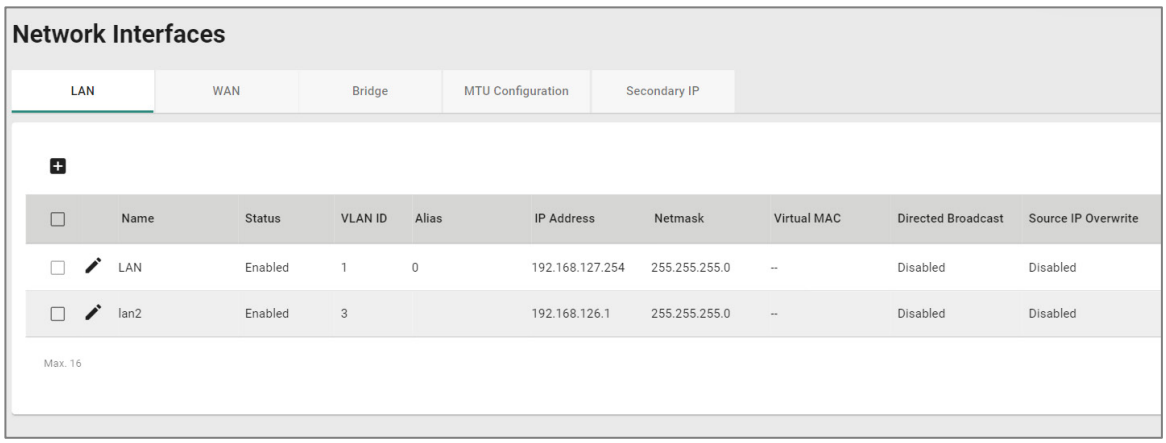
Limitations

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

Note

For the TN-4900 Series, when the Connection Type is set to Dynamic IP for an interface, the interface's information including the IP and the file name/file server (Option 66/67) can be checked through the CLI interface.

Network Interfaces List



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.

UI Setting	Description
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

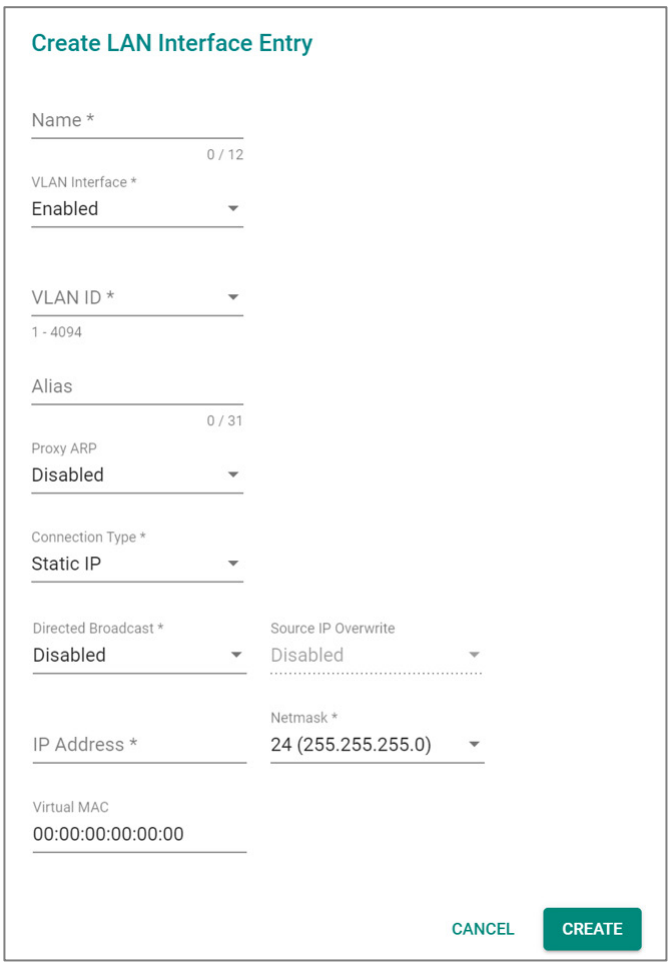
Clicking the **Add (+)** icon on the **Network Configuration > Network Interfaces - LAN** page will open this dialog box. This dialog lets you create new LAN interface entries for your device. Click **CREATE** to save your changes and add the new interface.

Limitations

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

Note

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



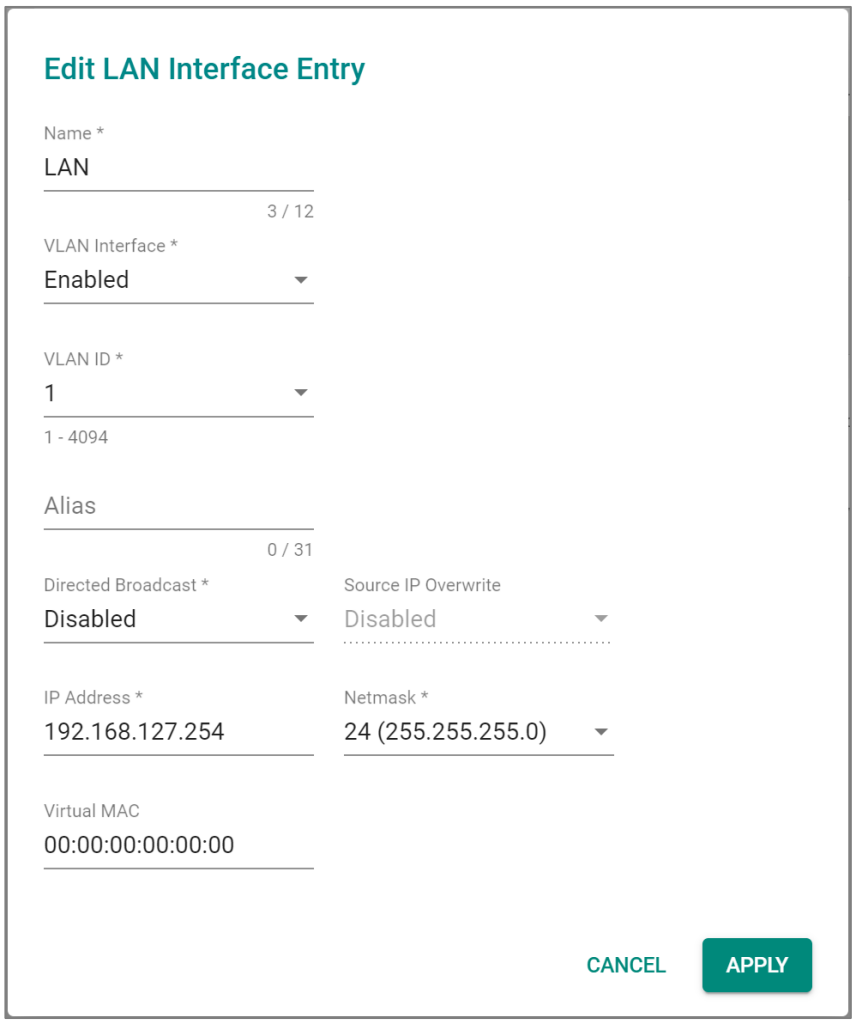
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the interface.	1 to 12 characters	N/A
VLAN Interface	Enable or disable the VLAN interface.	Enabled / Disabled	Enabled
VLAN ID	Specify the VLAN ID.	1 to 4094	N/A
Alias	Specify an alias for the VLAN interface.	1 to 31 characters	N/A
Proxy ARP	Enable or disable proxy ARP for the interface.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Connection Type	Select the connection type for the interface. **Note** The LAN interfaces require static IP addresses; dynamic IPs are not supported.	Static IP / Dynamic IP	Static IP
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
IP Address **(Only when Connection Type set as Static IP)**	Specify the IP address of the interface.	Valid IP address	N/A
Netmask **(Only when Connection Type set as Static IP)**	Specify the subnet mask of the interface.	Valid subnet mask	24 (255.255.255.0)
DHCP Client Option 66/67 **(Only when Connection Type set as Dynamic IP)**	Enable or disable DHCP Client Option 66/67 for the interface, if the device supports it.	Enabled / Disabled	Disabled
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.



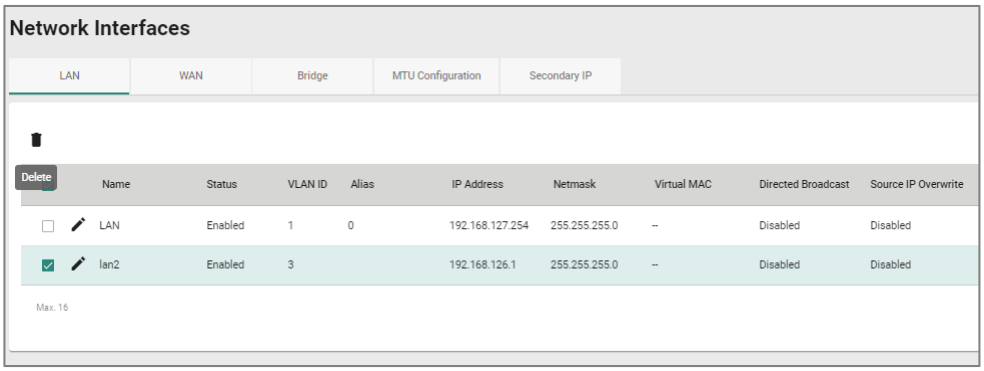
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the interface.	1 to 12 characters	N/A
VLAN Interface	Enable or disable the VLAN interface.	Enabled / Disabled	Enabled
VLAN ID	Specify the VLAN ID.	1 to 4094	N/A
Alias	Specify an alias for the VLAN interface.	1 to 31 characters	N/A
Proxy ARP	Enable or disable proxy ARP for the interface.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Connection Type	Select the connection type for the interface. **Note** The LAN interfaces require static IP addresses; dynamic IPs are not supported.	Static IP / Dynamic IP	Static IP
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
IP Address **(Only when Connection Type set as Static IP)**	Specify the IP address of the interface.	Valid IP address	N/A
Netmask **(Only when Connection Type set as Static IP)**	Specify the subnet mask of the interface.	Valid subnet mask	24 (255.255.255.0)
DHCP Client Option 66/67 **(Only when Connection Type set as Dynamic IP)**	Enable or disable DHCP Client Option 66/67 for the interface, if the device supports it.	Enabled / Disabled	Disabled
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.



WAN/WAN1

Menu Path: Network Configuration > Network Interfaces - WAN/WAN1

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

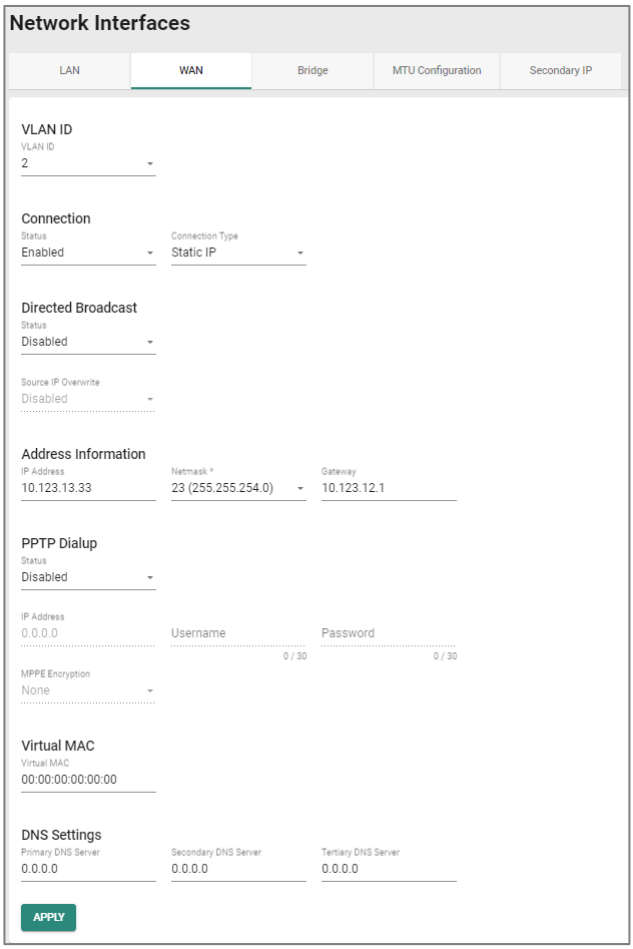
> **Note**
> This tab may appear as WAN or WAN1 depending on your product model.

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.



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

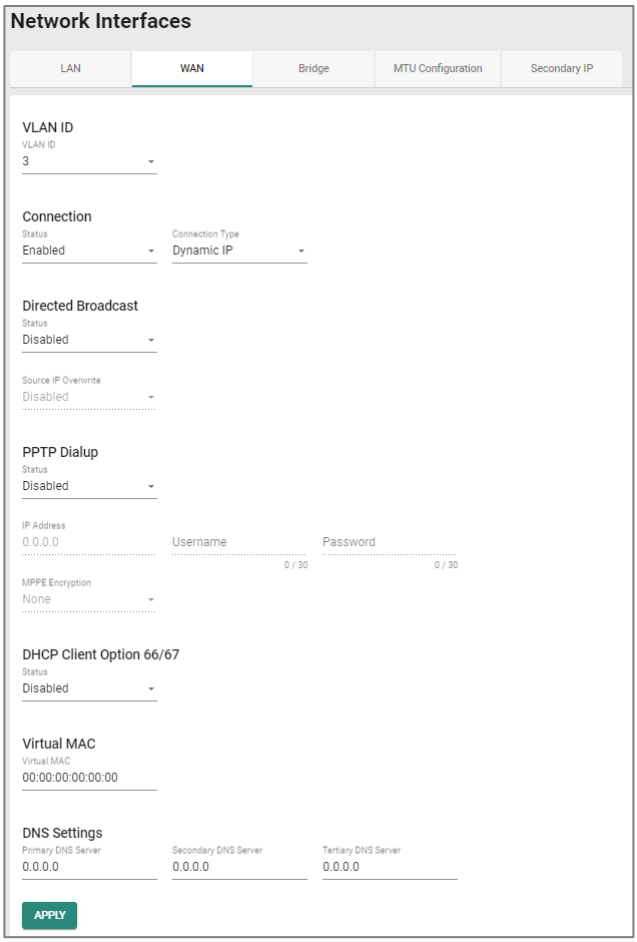
DNS Settings

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.

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



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

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

DHCP Client Option 66/67

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable DHCP client option 66/67.	Enabled/Disabled	Disabled

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

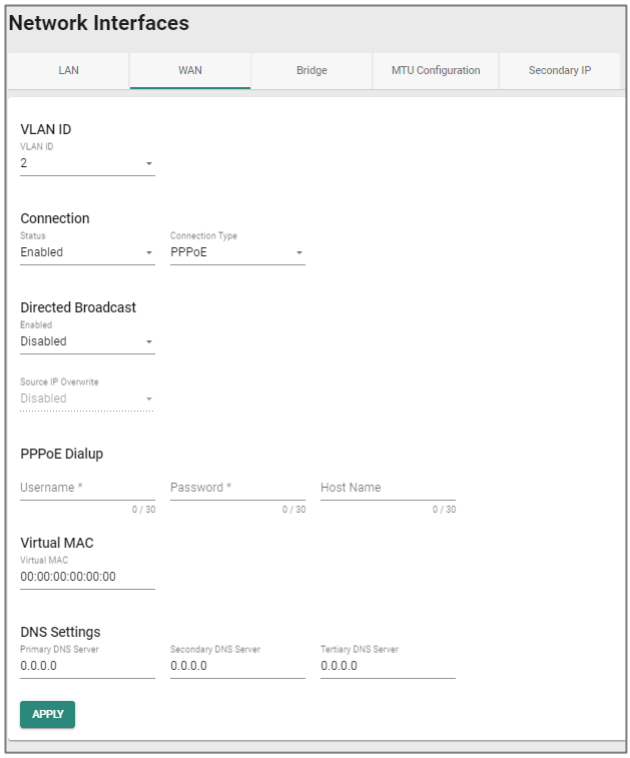
Note

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.



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

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

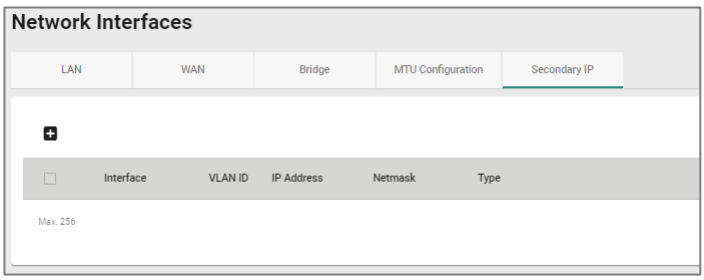
When using PPPoE, you can manually configure DNS servers here. Manually configured DNS servers will have a higher priority than DNS servers coming from the PPPoE server.

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

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.



UI Setting	Description
Interface	Shows which interface the secondary IP is for.
VLAN ID	Shows the VLAN ID used for the interface.

UI Setting	Description
IP Address	Shows the secondary IP address for the interface.
Netmask	Shows the subnet mask of the secondary IP.
Type	Shows the type of the secondary IP.

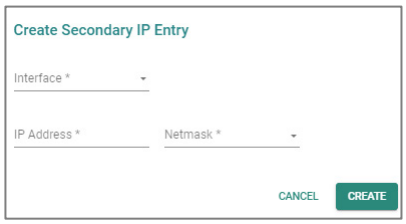
Secondary IP - Create Secondary IP Entry

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.

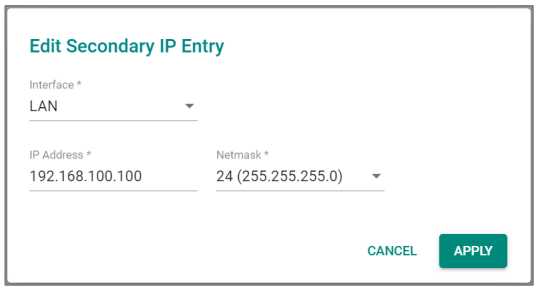


UI Setting	Description	Valid Range	Default Value
Interface	Select which interface the secondary IP is for.	Drop-down list of interfaces	N/A
IP Address	Specify the IP address of the secondary interface.	Valid IP address	N/A
Netmask	Specify the subnet mask of the secondary interface.	Valid netmask	N/A

Secondary IP - Edit Secondary IP Entry

Menu Path: Network Configuration > Network Interfaces - Secondary IP

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

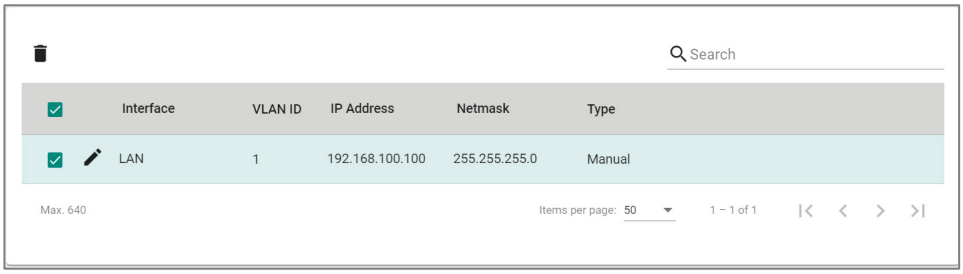


UI Setting	Description	Valid Range	Default Value
Interface	Select which interface the secondary IP is for.	Drop-down list of interfaces	N/A
IP Address	Specify the IP address of the secondary interface.	Valid IP address	N/A
Netmask	Specify the subnet mask of the secondary interface.	Valid netmask	N/A

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.



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
- DNS Server

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

DHCP Server

Menu Path: Network Service > DHCP Server

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

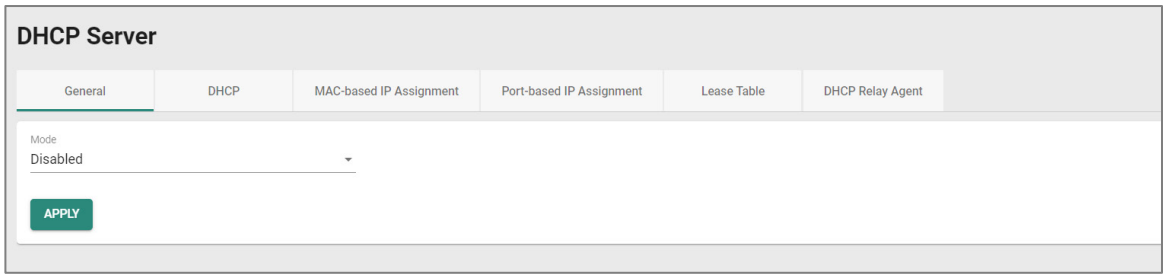
This page includes these tabs:

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

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.



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.

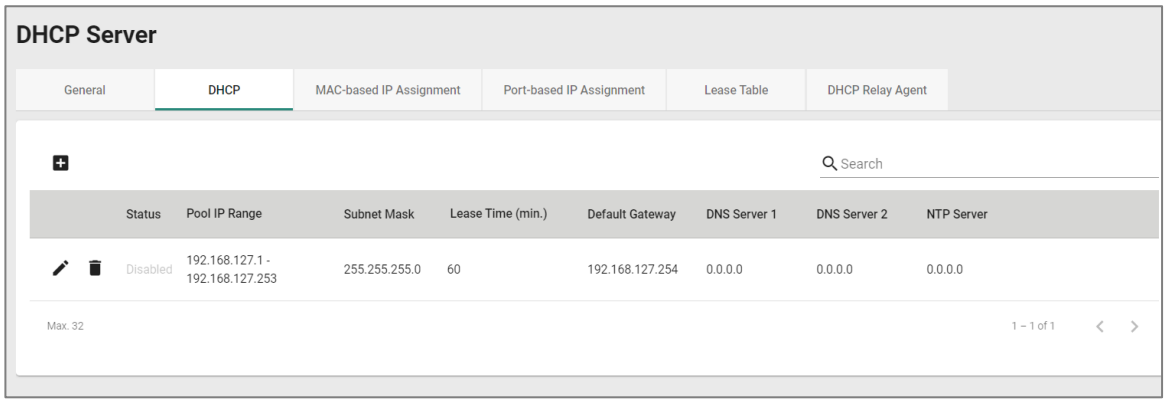
Note

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

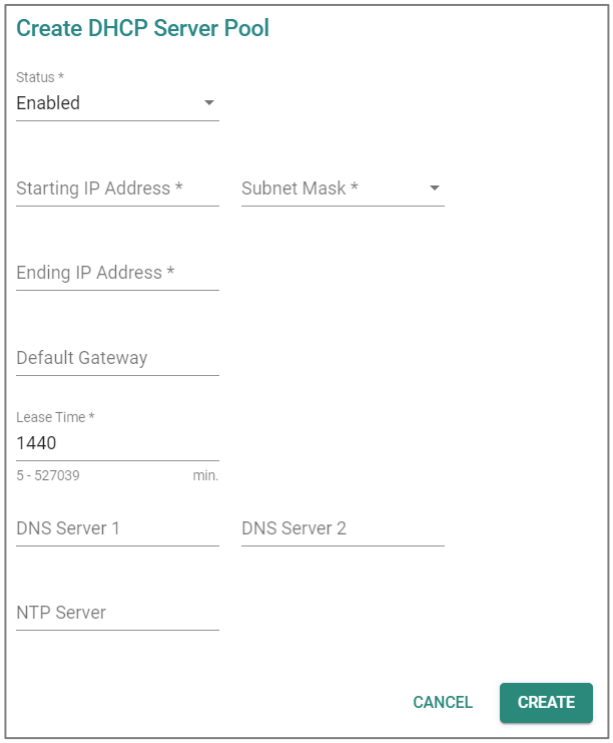


UI Setting	Description
Status	Shows the status of the DHCP server pool.
Pool IP Range	Shows the IP range of the pool.
Subnet Mask	Shows the subnet mask to use for DHCP clients in the pool.
Lease Time	Shows the lease time to use for IP addresses assigned by the DHCP server for the pool.
DNS Server 1	Shows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



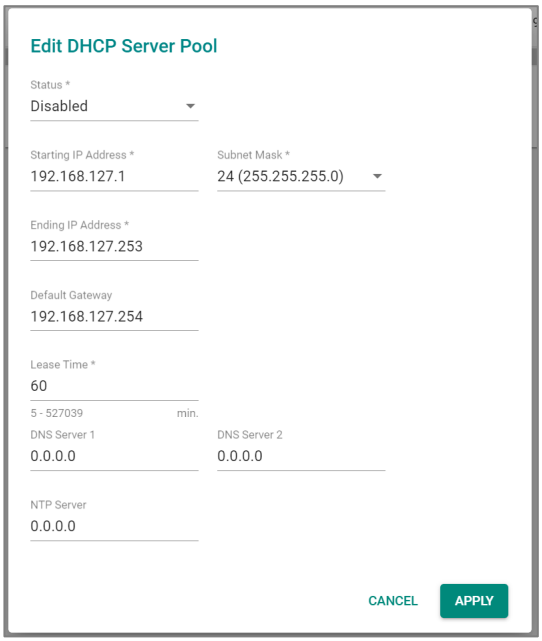
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable DHCP server functionality.	Enabled / Disabled	N/A
Starting IP Address	Specify the starting IP address of the DHCP IP pool.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask for DHCP clients in the pool. **Note** When configuring the DHCP Server, ensure the subnet mask is correctly set and the starting IP address, ending IP addresses, and IP addresses of all devices in the pool fall within this range. Exclude the reserved `.0` (network) and `.255` (broadcast) addresses to avoid conflicts.	Valid subnet mask	N/A
Ending IP Address	Specify the ending IP address of the DHCP IP pool.	Valid IP address	N/A
Default Gateway	Specify the default gateway to use for DHCP clients in the pool.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
Lease Time	Specify the lease time in minutes to use for IP addresses assigned to DHCP clients in the pool.	5 to 527039	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

Edit DHCP Server Pool

Menu Path: Network Service > DHCP Server - DHCP

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

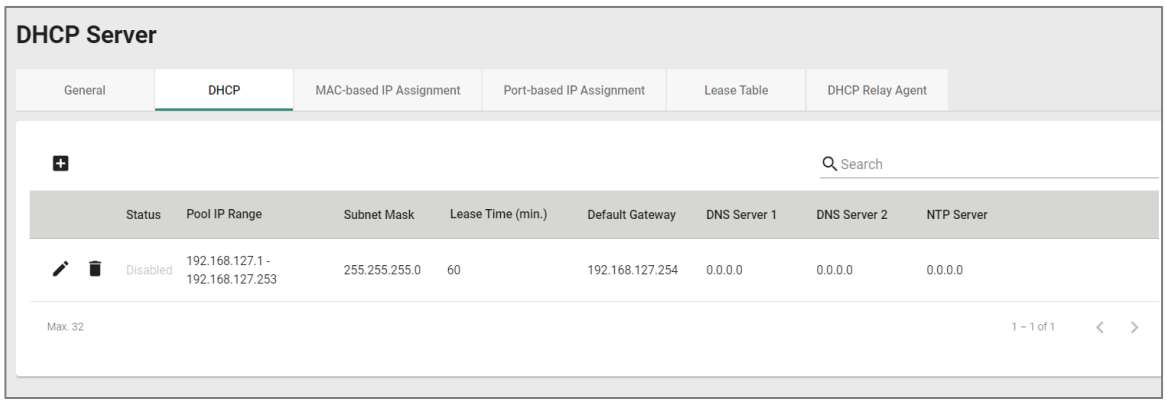


UI Setting	Description	Valid Range	Default Value
Status	Enable or disable DHCP server functionality.	Enabled / Disabled	N/A
Starting IP Address	Specify the starting IP address of the DHCP IP pool.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask for DHCP clients in the pool. **Note** When configuring the DHCP Server, ensure the subnet mask is correctly set and the starting IP address, ending IP addresses, and IP addresses of all devices in the pool fall within this range. Exclude the reserved `.0` (network) and `.255` (broadcast) addresses to avoid conflicts.	Valid subnet mask	N/A
Ending IP Address	Specify the ending IP address of the DHCP IP pool.	Valid IP address	N/A
Default Gateway	Specify the default gateway to use for DHCP clients in the pool.	Valid IP address	N/A
Lease Time	Specify the lease time in minutes to use for IP addresses assigned to DHCP clients in the pool.	5 to 527039	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.



DHCP Server - MAC-based IP Assignment

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

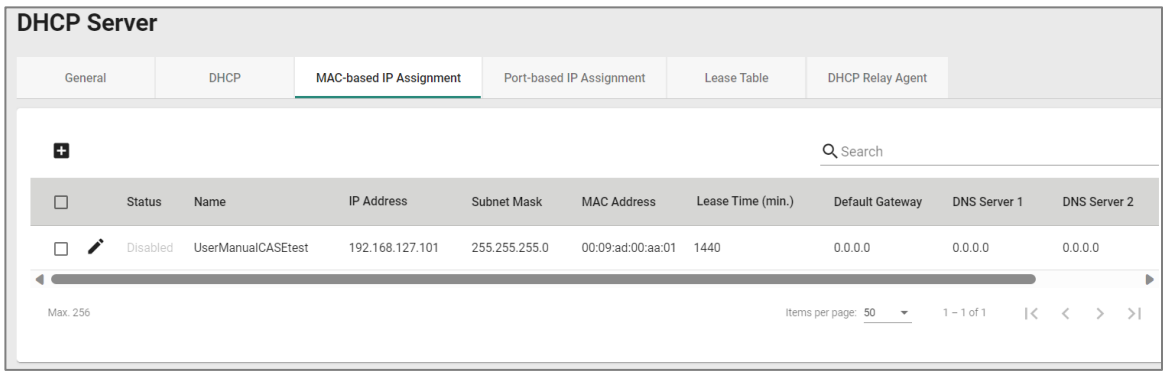
This page lets you manage the DHCP server's MAC-based IP assignments.

Note

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.

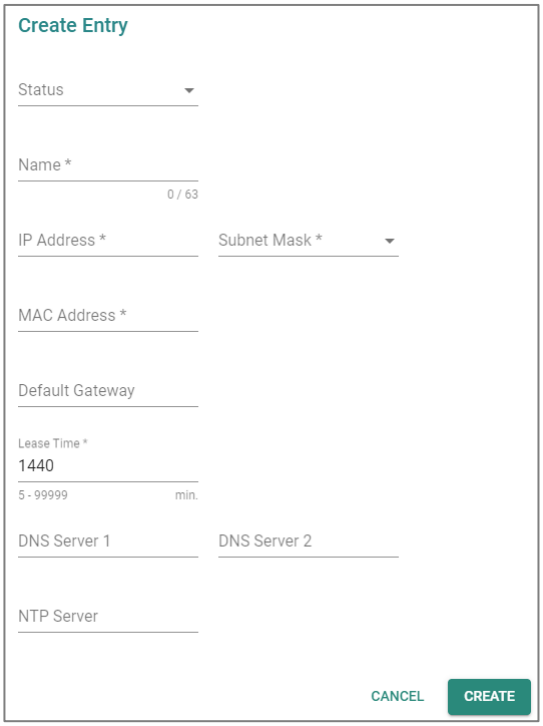


UI Setting	Description
Status	Shows the status of the MAC-based IP assignment.
Name	Shows the hostname for the device.
IP Address	Shows the IP address of the device.
Subnet Mask	Shows the subnet mask of the device.
MAC Address	Shows the MAC address of the device.
Default Gateway	Shows the default gateway 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.



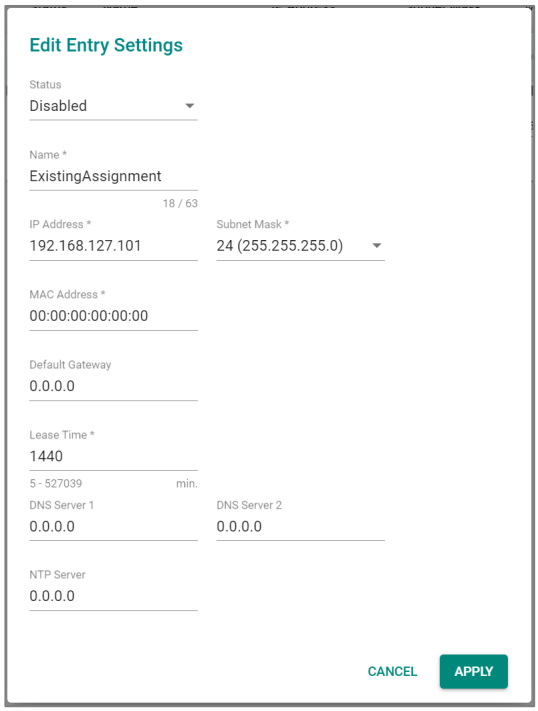
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this MAC-based IP assignment.	Enabled / Disabled	N/A
Name	Enter a hostname for the IP assignment.	Max. 63 characters	N/A
IP Address	Specify the IP address for the IP assignment.	Valid IP address	N/A
Subnet Mask	Specify the subnet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

UI Setting	Description	Valid Range	Default Value
NTP Server	Specify the NTP server for the IP assignment.	Valid IP address	N/A

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.



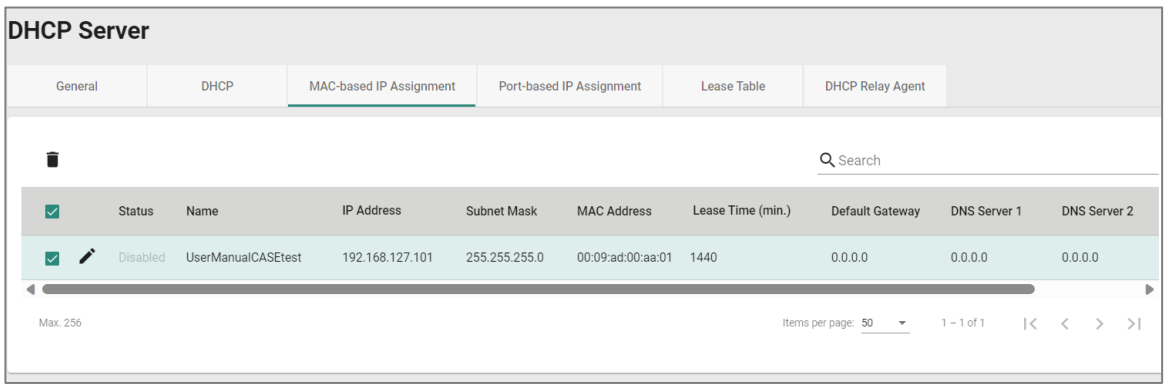
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this MAC-based IP assignment.	Enabled / Disabled	N/A
Name	Enter a hostname for the IP assignment.	Max. 63 characters	N/A
IP Address	Specify the IP address for the IP assignment.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
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
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.

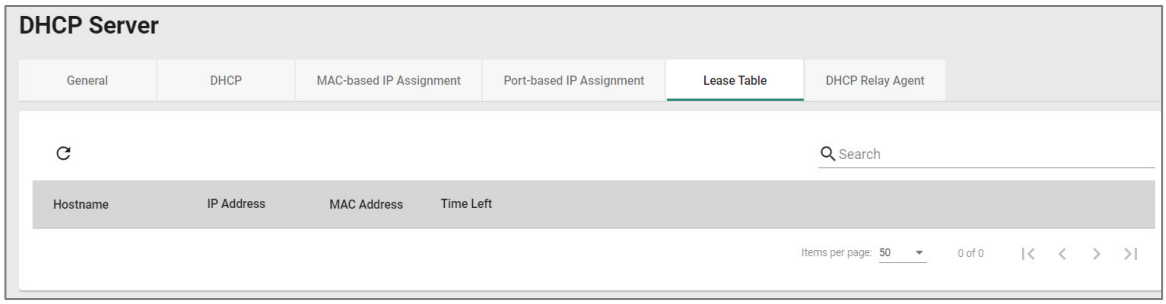


DHCP Server - Lease Table

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.

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

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
Routing Table	R	R	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
- Routing Table

Static Routes

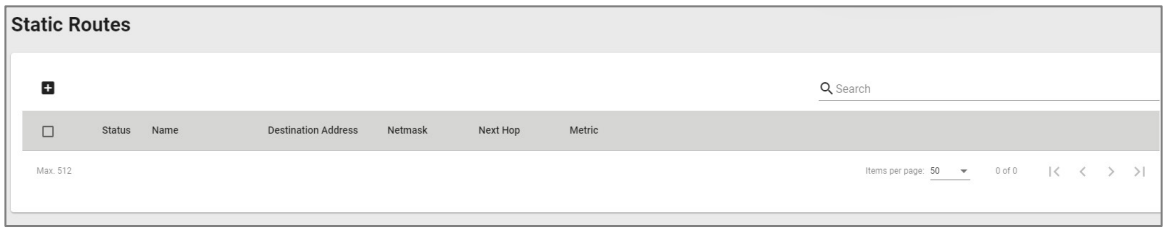
Menu Path: Routing > Unicast Route > Static Routes

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

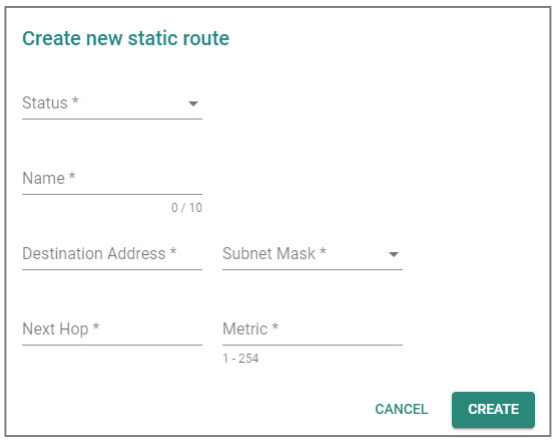


UI Setting	Description
Status	Shows the status of the static route.
Name	Shows the name of the static route.
Destination Address	Shows the destination IP address for the static route.
Netmask	Shows the subnet mask for the destination IP address.
Next Hop	Shows the next router on the path to the destination 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.

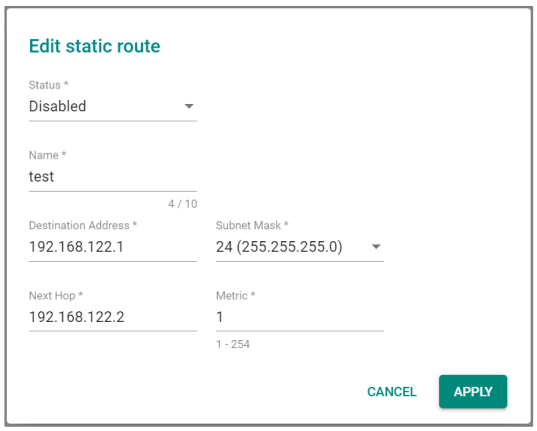


UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the static route.	Enabled / Disabled	N/A
Name	Specify a name for the static route.	Max. 10 characters	N/A
Destination Address	Specify the destination IP address for the static route.	Valid IP address	N/A
Subnet Mask	Specify the 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

Edit a Static Route

Menu Path: Routing > Unicast Route > Static Routes

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

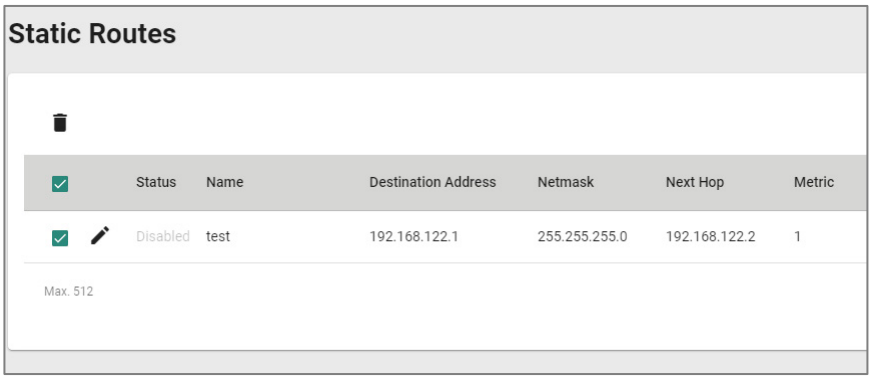


UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the static route.	Enabled / Disabled	N/A
Name	Specify a name for the static route.	Max. 10 characters	N/A
Destination Address	Specify the destination IP address for the static route.	Valid IP address	N/A
Subnet Mask	Specify the 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

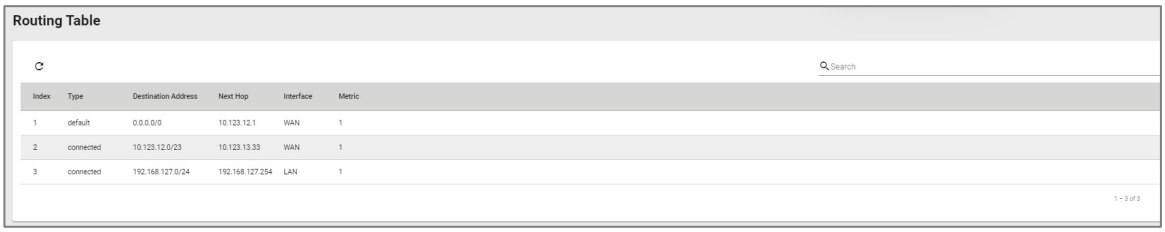
You can delete entries by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.



Routing Table

Menu Path: Routing > Unicast Route > Routing Table

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



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

UI Setting	Description
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.

NAT

Menu Path: NAT

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

> **Note**
> NAT currently supports the following ALG protocols: FTP, TFTP, SNMP.

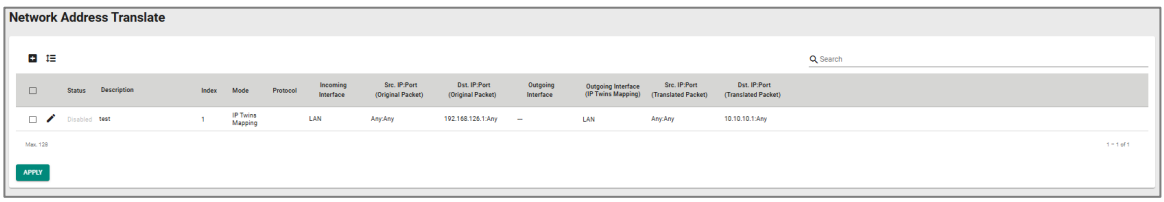
> **Limitations**
> You can create up to 512 NAT rules.

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	R/W	R/W	R

NAT Rule List



UI Setting	Description
Status	Shows whether the NAT rule is enabled or disabled.

UI Setting	Description
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

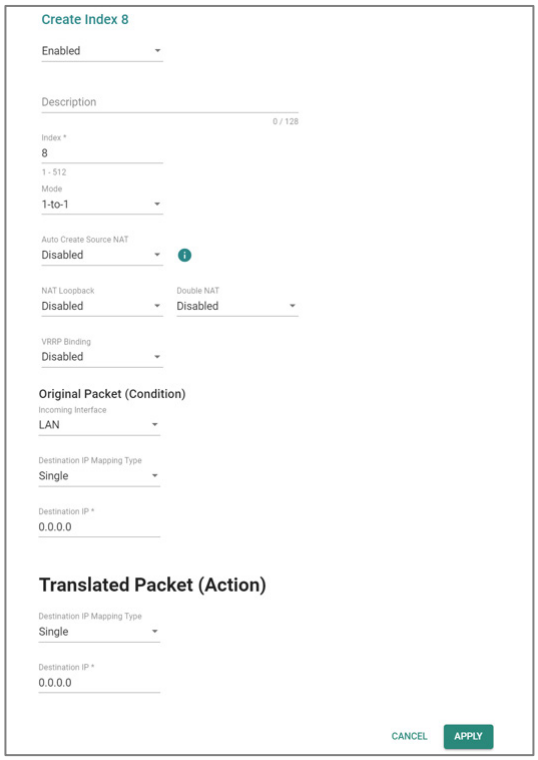
Menu Path: NAT

Clicking the **Add (+)** icon on the **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.



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. **IP Twins Mapping**: Allows you to set up a NAT rule with a duplicated LAN IP.	1-to-1 / N-to-1 / PAT / Advance / IP Twins Mapping	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

UI Setting	Description	Valid Range	Default Value
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
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 can establish several 1-to-1 NAT mappings within a designated IP address range. Make sure that the **Range** values for **Original Packet (Condition)** settings align precisely with the **Range** values in the **Translated Packet (Action)** settings 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

UI Setting	Description	Valid Range	Default Value
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

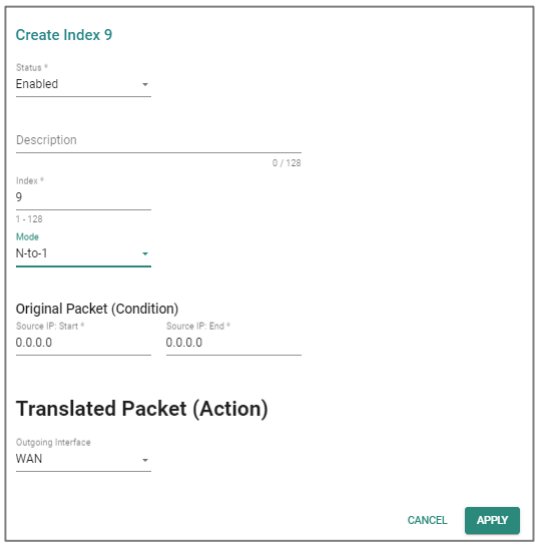
Translated Packet (Action)

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 can establish several 1-to-1 NAT mappings within a designated IP address range. Make sure that the **Range** values for **Original Packet (Condition)** settings align precisely with the **Range** values in the **Translated Packet (Action)** settings for accurate destination IP mapping.	Single / Range	Single
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

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 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.



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. **IP Twins Mapping**: Allows you to set up a NAT rule with a duplicated LAN IP.	1-to-1 / N-to-1 / PAT / Advance / IP Twins Mapping	1-to-1

Original Packet (Condition)

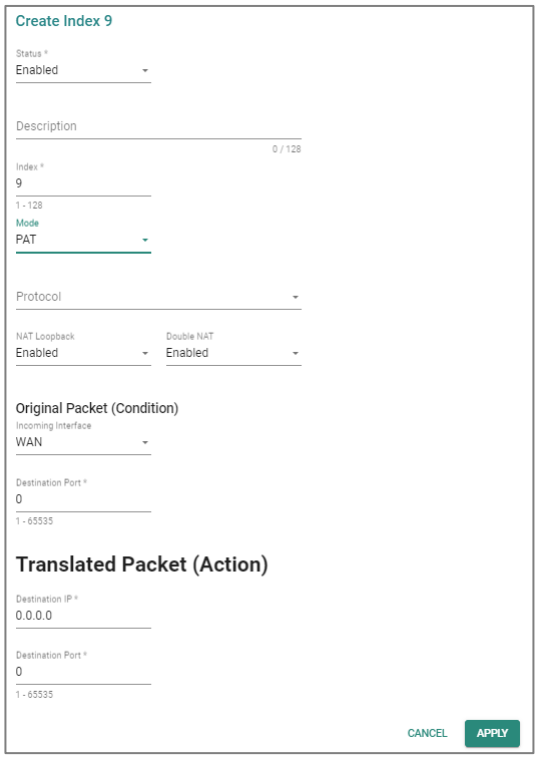
UI Setting	Description	Valid Range	Default Value
Source IP: Start	Specify the starting IP address of the source IP range this rule will apply to.	Valid IP address	0.0.0.0
Source IP: End	Specify the starting IP address of the source IP range this rule will apply to.	Valid IP address	0.0.0.0

Translated Packet (Action)

UI Setting	Description	Valid Range	Default Value
Outgoing Interface	Select the interface for the NAT rule. **Note** The **Outgoing Interface** cannot be set to **Any**, as N-1 NAT requires a specific outgoing interface to be designated.	Drop-down list of interfaces	WAN

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.



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. **IP Twins Mapping**: Allows you to set up a NAT rule with a duplicated LAN IP.	1-to-1 / N-to-1 / PAT / Advance / IP Twins Mapping	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

UI Setting	Description	Valid Range	Default Value
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

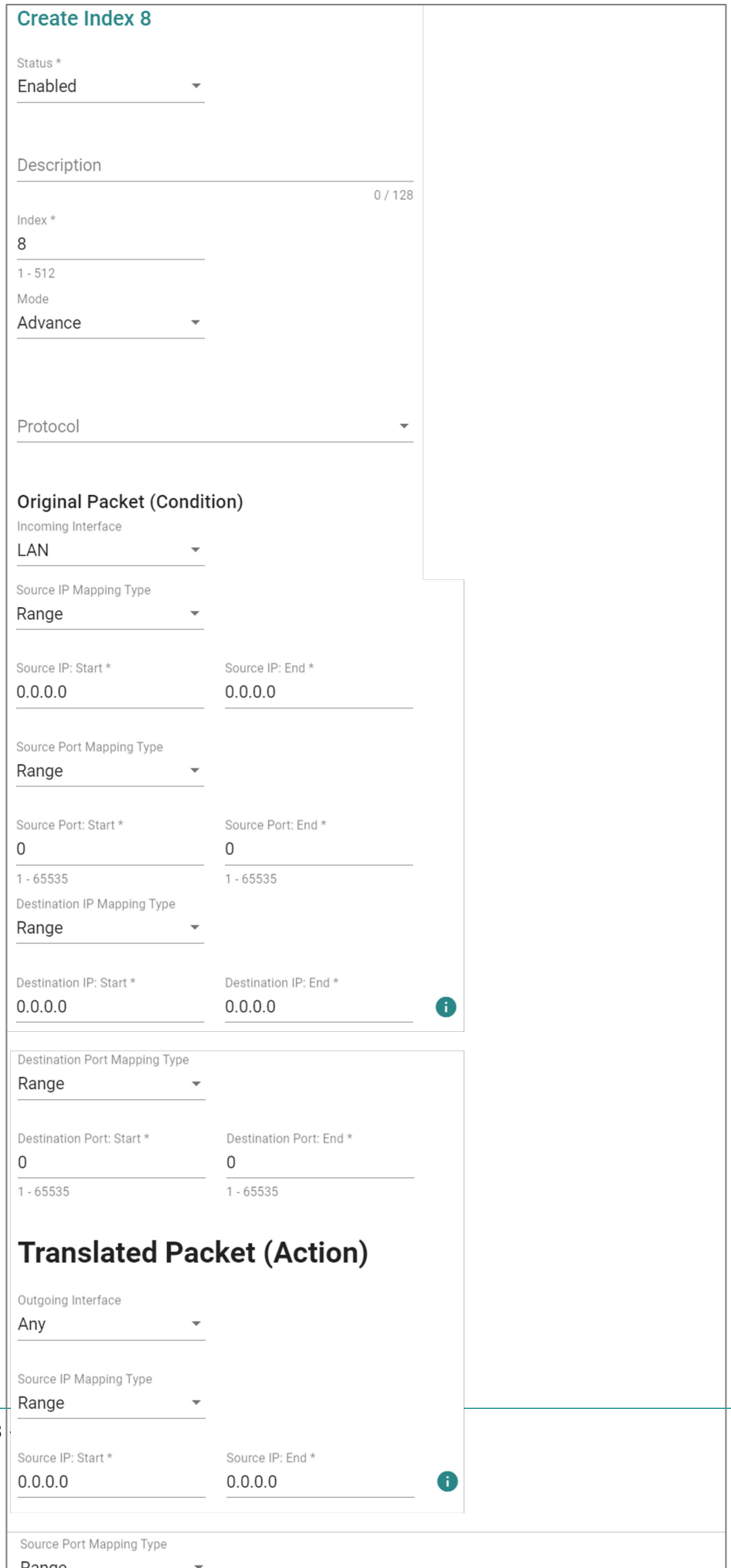
Create Index - Advance

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

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. **IP Twins Mapping**: Allows you to set up a NAT rule with a duplicated LAN IP.	1-to-1 / N-to-1 / PAT / Advance / IP Twins Mapping	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

UI Setting	Description	Valid Range	Default Value
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
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

UI Setting	Description	Valid Range	Default Value
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 > Interface - Secondary IP for more information.	Valid IP address	0.0.0.0
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

UI Setting	Description	Valid Range	Default Value
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
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 > Interface - 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)

UI Setting	Description	Valid Range	Default Value
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
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

UI Setting	Description	Valid Range	Default Value
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
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

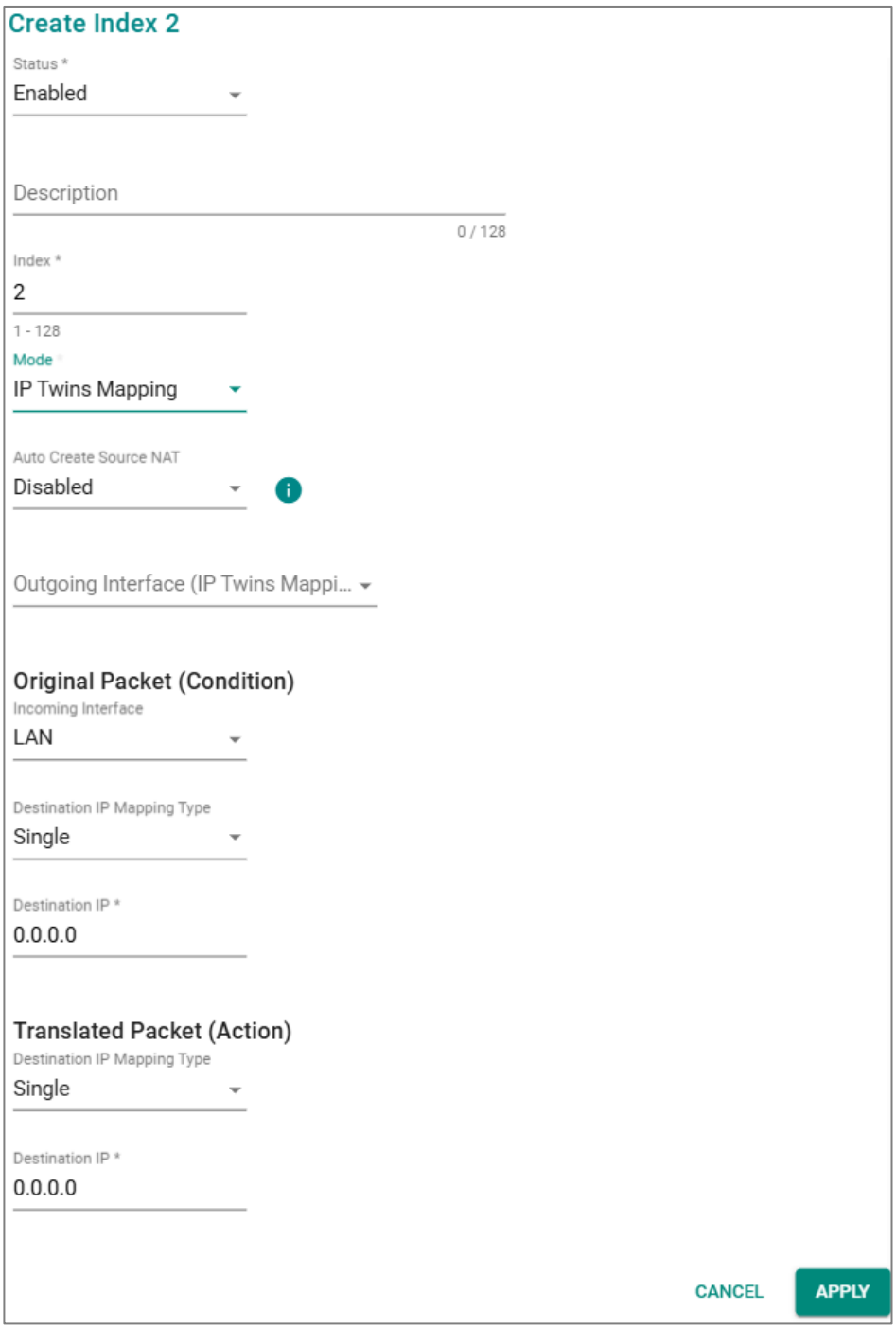
UI Setting	Description	Valid Range	Default Value
Destination Port: End **(Only if Destination Port Mapping Type is Range)**	Specify the end of the destination port range this rule will translate to.	1 to 65535	N/A

Create Index - IP Twins Mapping

If **IP Twins Mapping** is selected for the **Mode**, these settings will appear. This mode allows you to configure NAT with a duplicated LAN IP to provide flexibility for configuring duplicated LAN IP conversion.

Limitations

- Currently, IP Twins Mapping mode is only supported by the NAT-108 Series.
- IP Twins Mapping mode does not support transitioning between duplicate IP devices.
- IP Twins Mapping mode supports a maximum of 3 duplicate-IP interfaces.



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

UI Setting	Description	Valid Range	Default Value
Index	Specify the index of this rule.	1 to 128	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. **IP Twins Mapping**: Allows you to set up a NAT rule with a duplicated LAN IP.	1-to-1 / N-to-1 / PAT / Advance / IP Twins Mapping	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 Destination NAT (DNAT) translation.	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 by using the public IP address of the network.	Enabled / Disabled	Disabled
Double NAT	Enable or disable Double NAT. Double NAT lets 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 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.	Single / Range	Single

UI Setting	Description	Valid Range	Default Value
Destination IP **(Only if Destination IP Mapping Type is Single)**	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 > Interface - Secondary IP for more information.	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)

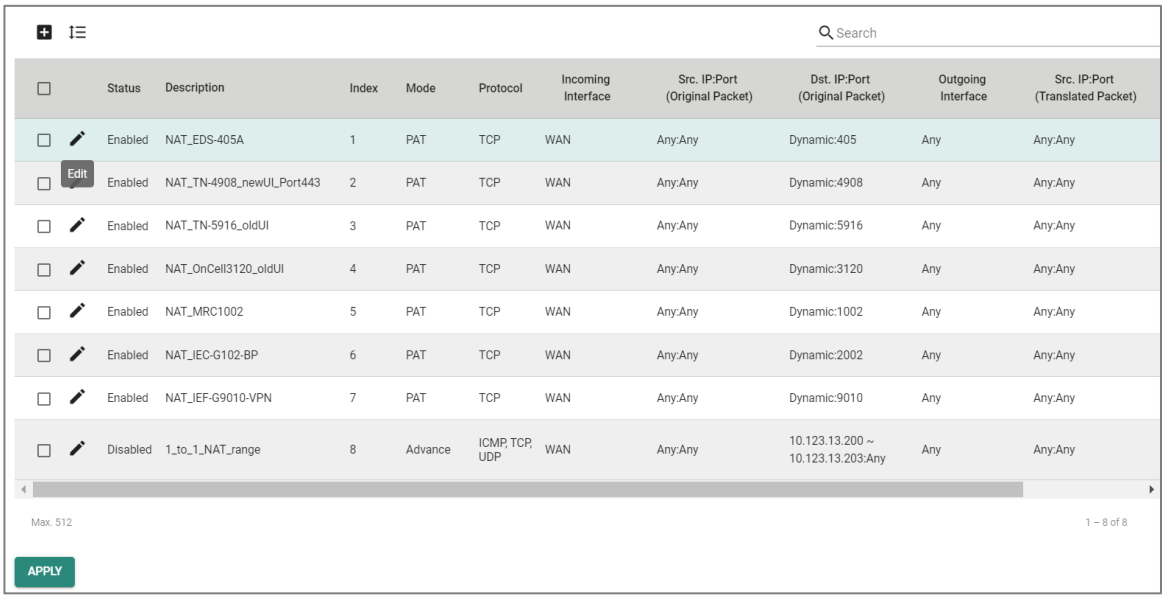
UI Setting	Description	Valid Range	Default Value
Destination IP Mapping Type	Specify how to handle destination IP address translation for the internal network. **Single**: This rule will translate to a single destination IP. **Range**: This rule will translate to a range of destination IPs.	Single / Range	Single
Destination IP **(Only if Destination IP Mapping Type is Single)**	Specify the destination IP this rule will translate 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 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

Edit NAT Rule

Menu Path: Main > NAT

Click on the pencil icon for the NAT rule that you want to edit.

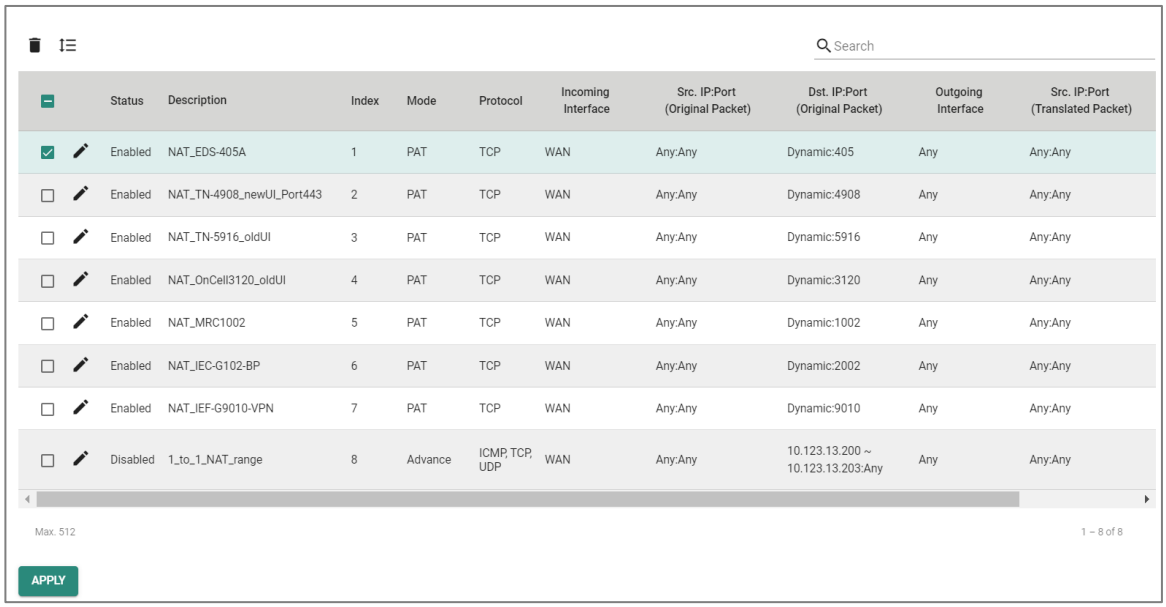


For a complete list of settings, see Create NAT Rule.

Delete NAT Rule

Menu Path: Main > NAT

Select the NAT rules that you want to delete and click the trash can icon to delete.


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)
Enabled NAT_EDS-405A 1 PAT TCP WAN Any:Any Dynamic:405 Any Any:Any
Enabled NAT_TN-4908_newUI_Port443 2 PAT TCP WAN Any:Any Dynamic:4908 Any Any:Any
Enabled NAT_TN-5916_oldUI 3 PAT TCP WAN Any:Any Dynamic:5916 Any Any:Any
Enabled NAT_OnCell3120_oldUI 4 PAT TCP WAN Any:Any Dynamic:3120 Any Any:Any
Enabled NAT_MRC1002 5 PAT TCP WAN Any:Any Dynamic:1002 Any Any:Any
Enabled NAT_IEC-G102-BP 6 PAT TCP WAN Any:Any Dynamic:2002 Any Any:Any
Enabled NAT_IEF-G9010-VPN 7 PAT TCP WAN Any:Any Dynamic:9010 Any Any:Any
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
Max. 512
1 – 8 of 8
APPLY

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 3 Policy
- Device Lockdown

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 3 Policy	R/W	R/W	R
Device Lockdown	R/W	R/W	R

Layer 3 Policy

Menu Path: Firewall > Layer 3 Policy

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

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

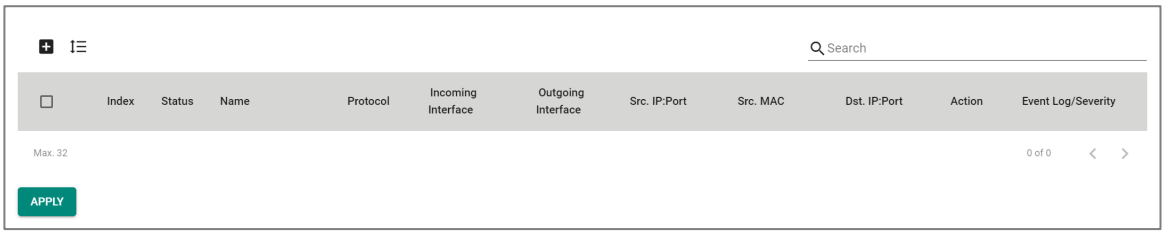
Limitations

You can create up to 32 Layer 3 policies.

Layer 3 Policy Settings

UI Setting	Description	Valid Range	Default Value
Firewall Event Log	Enable or disable logging of Layer 3 firewall events.	Enabled / Disabled	Disabled

Layer 3 Policy List



UI Setting	Description
Index	Shows the index of the policy. Policies with a lower index will be processed before policies with a higher index.
Status	Shows whether the policy is enabled.
Name	Shows the name of the policy.
Protocol	Shows the protocol used by the policy.
Incoming Interface	Shows the incoming interface used by the policy.
Outgoing Interface	Shows the outgoing interface used by the policy.

UI Setting	Description
Src. IP:Port	Shows the source IP address and port used by the policy.
Src. MAC	Shows the source MAC address and port used by the policy.
Dst. IP:Port	Shows the destination IP address and port used by the policy.
Action	Shows the action the firewall should take for traffic that matches this policy.
Event Log/Severity	Shows the event log destination and severity level for events from this policy.

Create Layer 3 Policy

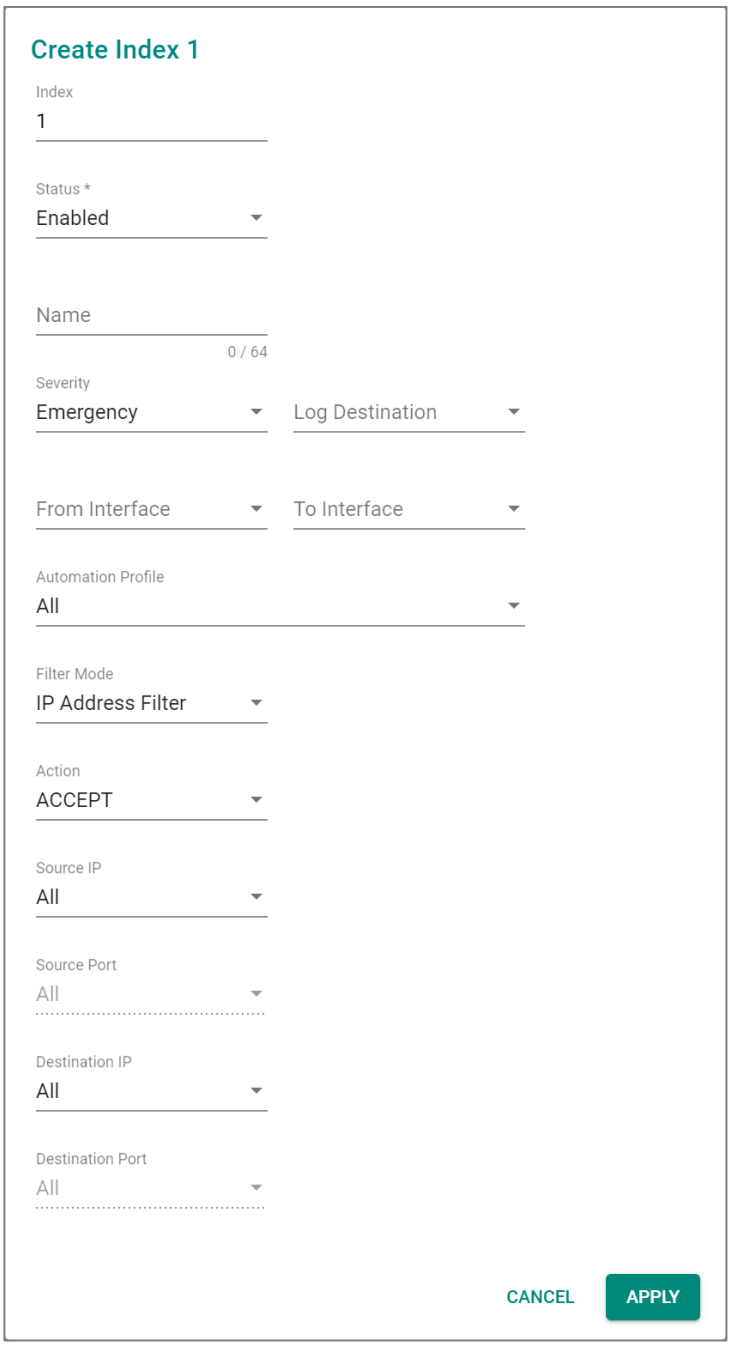
Menu Path: Firewall > Layer 3 Policy

Clicking the **Add (** **)** icon on the

Unable to render include or excerpt-include. Could not retrieve page.

page will open this dialog box. This dialog lets you create a new Layer 3 policy.

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



UI Setting	Description	Valid Range	Default Value
Index	Specify the index number for the policy. Policies with a lower index will be processed before policies with a higher index.	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 64 characters	N/A

UI Setting	Description	Valid Range	Default Value
Severity	Select the severity level to assign events for this policy. Refer to Appendix > Severity 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
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

UI Setting	Description	Valid Range	Default Value
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
Automation Profile	Select a profile to use for this policy. Each profile will automatically set some of the source and destination settings based on the selected protocol.	All / TCP / UDP / ICMP / EtherNet/IP I/O (TCP) / EtherNet/IP I/O (UDP) / EtherNet/IP messaging (TCP) / EtherNet IP messaging (UDP) / FF Annunciation (TCP) / FF Annunciation (UDP) / FF Fieldbus Message Specification (TCP) / FF Fieldbus Message Specification (UDP) / FF System Management (TCP) / FF System Management (UDP) / FF LAN Redundancy Port (TCP) / FF LAN Redundancy Port (UDP) / LonWorks (TCP) / LonWorks (UDP) / LonWorks2 (TCP) / LonWorks2 (UDP) / Modbus TCP/IP (TCP) / Modbus TCP/IP (UDP) / PROFINET RT Unicast (TCP) / PROFINET RT Unicast (UDP) / PROFINET RT Multicast (TCP) / PROFINET RT Multicast (UDP) / PROFINET Context Manager (TCP) / PROFINET Context Manager (UDP) / IEC 60870-5-104 process control over IP (TCP) / IEC 60870-5-104 process control over IP (UDP) / IPsec NAT-Traversal (TCP) / IPsec NAT-Traversal (UDP) / DNP3 (TCP) / DNP3 (UDP) / FTP-data (TCP) / FTP-data (UDP) / FTP-control (TCP) / FTP-control (UDP) / SSH (TCP) / SSH (UDP) / Telnet (TCP) / Telnet (UDP) / HTTP (TCP) / HTTP (UDP) / IPsec (TCP) / IPsec (UDP) / L2TP (TCP) / L2TP (UDP) / PPTP (TCP) / PPTP (UDP) / RADIUS (TCP) / RADIUS (UDP) / RADIUS Accounting (TCP) / RADIUS Accounting (UDP) / EtherCAT (TCP) / EtherCAT (UDP)	All

UI Setting	Description	Valid Range	Default Value
Filter Mode	Select the filter mode to use for packet filtering. **IP Address Filter**: The policy will filter packets based on IP addresses.	IP Address Filter	IP Address Filter
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 IP Address	Select which source IP addresses this policy will apply to. • **All:** The firewall policy will check all source IP addresses in the packet. • **Single:** The firewall policy will check for a single specified source IP address in the packet. • **Range:** The firewall policy will check for any source IP addresses in the packet that are within a specified range.	All / Single / Range	All
Source IP: Start **(If Source IP Address is Single or Range)**	Specify the source IP address or the beginning of the source IP address range this policy will apply to.	Valid IP address	0.0.0.0
Source IP: End **(If Source IP Address is Range)**	Specify the end of the source IP address range this policy will apply to.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Source Port **(If Automation Profile is TCP or UDP)**	Select which source ports this policy will apply to. • **All:** The firewall policy will check all source ports in the packet. • **Single:** The firewall policy will check for a single specified source port in the packet. • **Range:** The firewall policy will check for any source ports in the packet that are within a specified range.	If **Automation Profile** is **TCP** or **UDP**: All / Single / Range For all other **Automation Profile** options: All	All
Source Port: Start **(If Source Port is Single or Range)**	Specify the source port or the start of the source port range this policy will apply to.	1 to 65535	N/A
Source Port: End **(If Source Port is Range)**	Specify the end of the source port range this policy will apply to.	1 to 65535	N/A
Destination IP Address	Select which destination IP addresses this policy will apply to. • **All:** The firewall policy will check all destination IP addresses in the packet. • **Single:** The firewall policy will check for a single specified destination IP address in the packet. • **Range:** The firewall policy will check for any destination IP addresses in the packet that are within a specified range.	All / Single / Range	All
Destination IP: Start **(If Destination IP Address is Single or Range)**	Specify the destination IP address or the beginning of the destination IP address range this policy will apply to.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Destination IP: End **(If Destination IP Address is Range)**	Specify the end of the destination IP address range this policy will apply to.	Valid IP address	0.0.0.0
Destination Port	Select which destination ports this policy will apply to. • **All:** The firewall policy will check all destination ports in the packet. • **Single:** The firewall policy will check for a single specified destination port in the packet. • **Range:** The firewall policy will check for any destination ports in the packet that are within a specified range.	If **Automation Profile** is **All** or **ICMP:** All If **Automation Profile** is **TCP** or **UDP:** All / Single / Range For all other **Automation Profile** options: Single	If **Automation Profile** is **All, TCP, UDP,** or **ICMP:** All For all other **Automation Profile** options: Single
Destination Port: Start **(If Destination Port is Single or Range)**	Specify the destination port or the start of the destination port range this policy will apply to. Most of the **Automation Profile** options will fill in this setting with the default port used for that service. Refer to Ethernet Protocol Default Ports for more information.	1 to 65535	N/A
Destination Port: End **(If Destination Port is Range)**	Specify the end of the destination port range this policy will apply to.	1 to 65535	N/A

Edit Layer 3 Policy

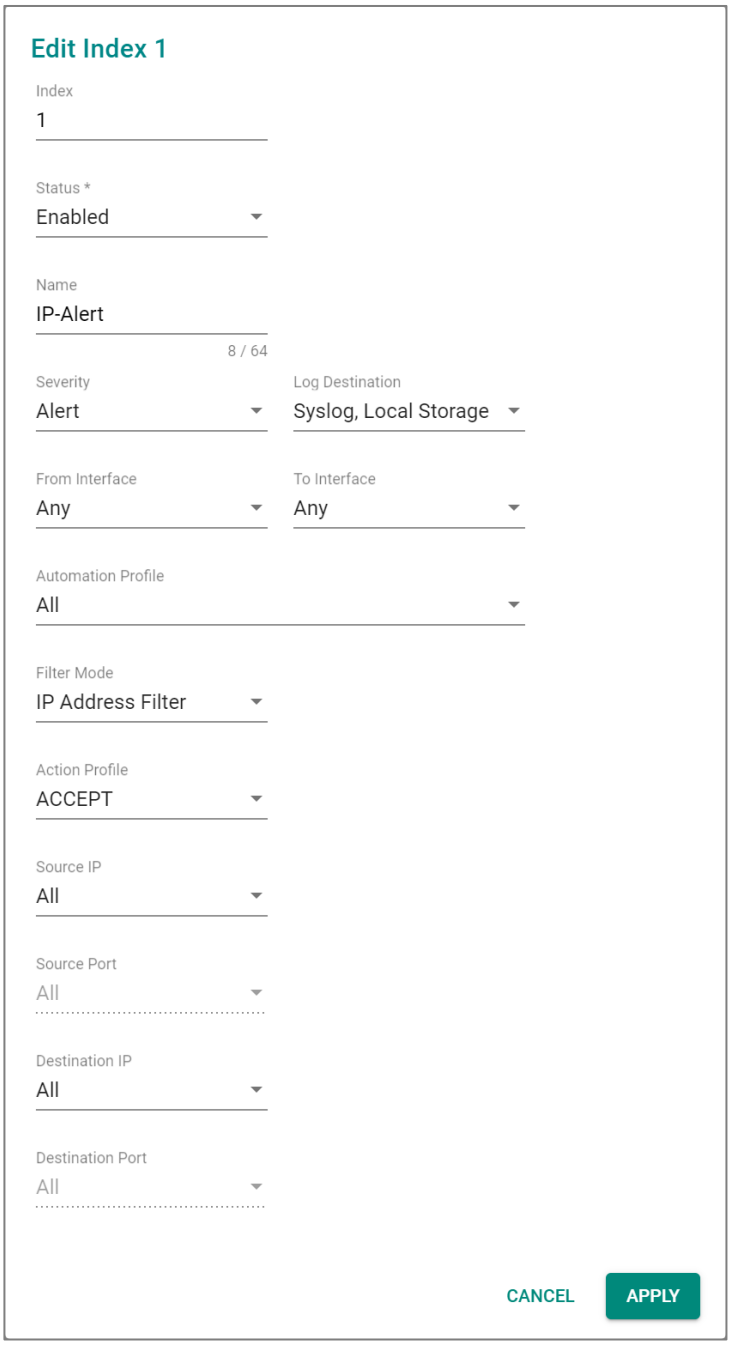
Menu Path: Firewall > Layer 3 Policy

Clicking the **Edit ( )** icon for an entry on the

Unable to render include or excerpt-include. Could not retrieve page.

page will open this dialog box. This dialog lets you edit an existing Layer 3 policy.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Index	Specify the index number for the policy. Policies with a lower index will be processed before policies with a higher index.	1 to 1024	Last used index plus 1
Status	Enable or disable the policy.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the policy.	1 to 64 characters	N/A
Severity	Select the severity level to assign events for this policy. Refer to Appendix > Severity 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
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

UI Setting	Description	Valid Range	Default Value
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
Automation Profile	Select a profile to use for this policy. Each profile will automatically set some of the source and destination settings based on the selected protocol.	All / TCP / UDP / ICMP / EtherNet/IP I/O (TCP) / EtherNet/IP I/O (UDP) / EtherNet/IP messaging (TCP) / EtherNet IP messaging (UDP) / FF Annunciation (TCP) / FF Annunciation (UDP) / FF Fieldbus Message Specification (TCP) / FF Fieldbus Message Specification (UDP) / FF System Management (TCP) / FF System Management (UDP) / FF LAN Redundancy Port (TCP) / FF LAN Redundancy Port (UDP) / LonWorks (TCP) / LonWorks (UDP) / LonWorks2 (TCP) / LonWorks2 (UDP) / Modbus TCP/IP (TCP) / Modbus TCP/IP (UDP) / PROFINET RT Unicast (TCP) / PROFINET RT Unicast (UDP) / PROFINET RT Multicast (TCP) / PROFINET RT Multicast (UDP) / PROFINET Context Manager (TCP) / PROFINET Context Manager (UDP) / IEC 60870-5-104 process control over IP (TCP) / IEC 60870-5-104 process control over IP (UDP) / IPsec NAT-Traversal (TCP) / IPsec NAT-Traversal (UDP) / DNP3 (TCP) / DNP3 (UDP) / FTP-data (TCP) / FTP-data (UDP) / FTP-control (TCP) / FTP-control (UDP) / SSH (TCP) / SSH (UDP) / Telnet (TCP) / Telnet (UDP) / HTTP (TCP) / HTTP (UDP) / IPsec (TCP) / IPsec (UDP) / L2TP (TCP) / L2TP (UDP) / PPTP (TCP) / PPTP (UDP) / RADIUS (TCP) / RADIUS (UDP) / RADIUS Accounting (TCP) / RADIUS Accounting (UDP) / EtherCAT (TCP) / EtherCAT (UDP)	All

UI Setting	Description	Valid Range	Default Value
Filter Mode	Select the filter mode to use for packet filtering. **IP Address Filter**: The policy will filter packets based on IP addresses.	IP Address Filter	IP Address Filter
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 IP Address	Select which source IP addresses this policy will apply to. • **All:** The firewall policy will check all source IP addresses in the packet. • **Single:** The firewall policy will check for a single specified source IP address in the packet. • **Range:** The firewall policy will check for any source IP addresses in the packet that are within a specified range.	All / Single / Range	All
Source IP: Start **(If Source IP Address is Single or Range)**	Specify the source IP address or the beginning of the source IP address range this policy will apply to.	Valid IP address	0.0.0.0
Source IP: End **(If Source IP Address is Range)**	Specify the end of the source IP address range this policy will apply to.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Source Port **(If Automation Profile is TCP or UDP)**	Select which source ports this policy will apply to. • **All:** The firewall policy will check all source ports in the packet. • **Single:** The firewall policy will check for a single specified source port in the packet. • **Range:** The firewall policy will check for any source ports in the packet that are within a specified range.	If **Automation Profile** is **TCP** or **UDP**: All / Single / Range For all other **Automation Profile** options: All	All
Source Port: Start **(If Source Port is Single or Range)**	Specify the source port or the start of the source port range this policy will apply to.	1 to 65535	N/A
Source Port: End **(If Source Port is Range)**	Specify the end of the source port range this policy will apply to.	1 to 65535	N/A
Destination IP Address	Select which destination IP addresses this policy will apply to. • **All:** The firewall policy will check all destination IP addresses in the packet. • **Single:** The firewall policy will check for a single specified destination IP address in the packet. • **Range:** The firewall policy will check for any destination IP addresses in the packet that are within a specified range.	All / Single / Range	All
Destination IP: Start **(If Destination IP Address is Single or Range)**	Specify the destination IP address or the beginning of the destination IP address range this policy will apply to.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Destination IP: End **(If Destination IP Address is Range)**	Specify the end of the destination IP address range this policy will apply to.	Valid IP address	0.0.0.0
Destination Port	Select which destination ports this policy will apply to. • **All:** The firewall policy will check all destination ports in the packet. • **Single:** The firewall policy will check for a single specified destination port in the packet. • **Range:** The firewall policy will check for any destination ports in the packet that are within a specified range.	If **Automation Profile** is **All** or **ICMP:** All If **Automation Profile** is **TCP** or **UDP:** All / Single / Range For all other **Automation Profile** options: Single	If **Automation Profile** is **All, TCP, UDP,** or **ICMP:** All For all other **Automation Profile** options: Single
Destination Port: Start **(If Destination Port is Single or Range)**	Specify the destination port or the start of the destination port range this policy will apply to. Most of the **Automation Profile** options will fill in this setting with the default port used for that service. Refer to Ethernet Protocol Default Ports for more information.	1 to 65535	N/A
Destination Port: End **(If Destination Port is Range)**	Specify the end of the destination port range this policy will apply to.	1 to 65535	N/A

Delete Layer 3 Policy

Menu Path: Firewall > Layer 3 Policy

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

Device Lockdown

Menu Path: Firewall > Device Lockdown

This page lets you configure Device Lockdown to secure and control network traffic.

Device Lockdown offers a straightforward method to automatically configure firewall whitelisting. Users are not required to know the device's IP or MAC address to set up firewall rules. The Learning function enables the device to gather device information from network traffic to establish whitelisting rules. Additionally, users can customize the learning table according to their needs.

> **Note**
> Device Lockdown is specifically designed for and is only available for NAT Series devices.

This page includes these tabs:

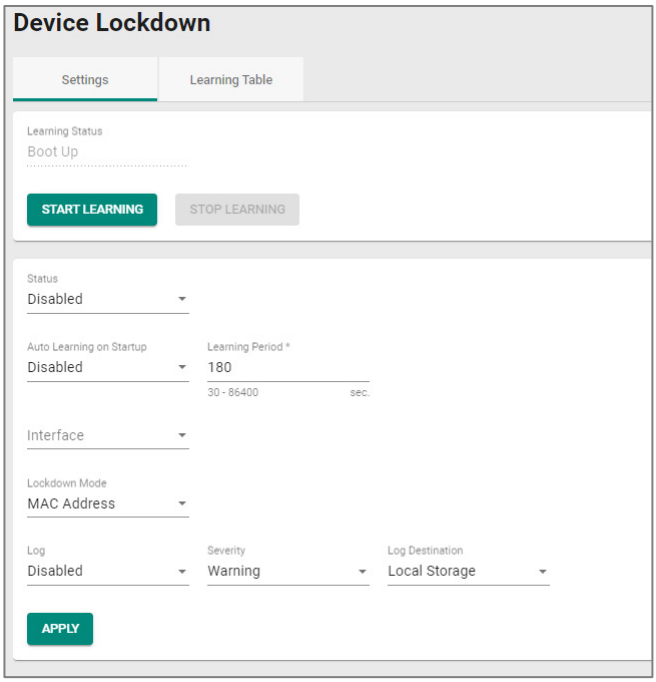
- Settings
- Learning Table

Device Lockdown - Settings

Menu Path: Firewall > Device Lockdown - Settings

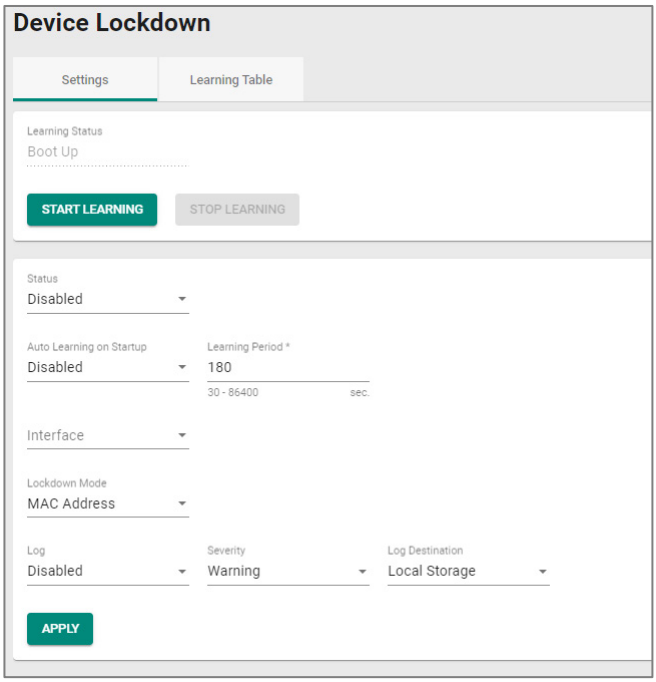
This page lets you manage the Device Lockdown feature.

Learning Status



UI Setting	Description
Learning Status	Shows the learning status for the Device Lockdown feature. **START LEARNING:** Learn whitelist information from ARP tables through network traffic. **Note** When the Learning Status process is in progress, Device Lockdown cannot be enabled until the process is complete. **STOP LEARNING:** Stop the current learning process.

Device Lockdown Settings



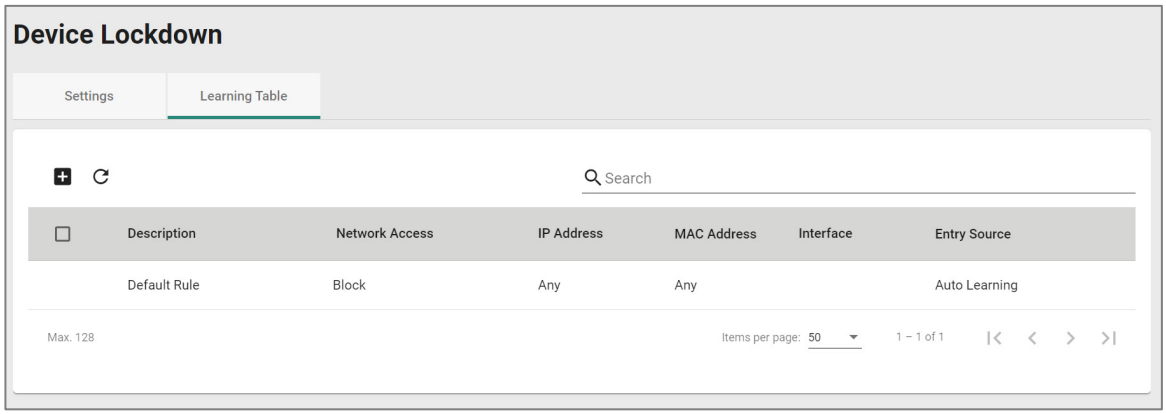
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable device lockdown. **Note** When **Status** is enabled, the Learning Table can't be manually configured. Please disable **Status** to make modifications.	Enabled / Disabled	Disabled
Auto Learning on Startup	Enable or disable auto learning on startup.	Enabled / Disabled	Disabled
Learning Period	Specify the duration auto learning will be enabled for.	30 to 86400 seconds	180
Interface	Select an interface to lock down.	Drop-down list of interfaces	N/A
Lockdown Mode	Select the firewall filtering criteria.	MAC Address / MAC+IP Access	MAC Address
Log	Enable or disable device lockdown event logs.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Severity	Select the severity of device lockdown events.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Warning
Log Destination	Specify whether to store device lockdown event logs locally or send them to a syslog or trap server.	Local Storage / Syslog / Trap	Local Storage

Device Lockdown - Learning Table

Menu Path: Firewall > Device Lockdown - Learning Table

This page lets you view and manage the current learning table used for the Device Lockdown feature.



UI Setting	Description
Description	Shows the description used to identify the learning table rule.
Network Access	Shows the network access rule to apply to the specified IP address or MAC address. **Allow**: Grants access to the specified IP address or MAC address. **Block:** Denies access to the specified IP address or MAC address.
IP Address	Shows the IP address the rule applies to. **Any** means it applies to all IP addresses.
MAC Address	Shows the MAC address the rule applies to. **Any** means it applies to all MAC addresses.
Interface	Shows the interface that the rule applies to.

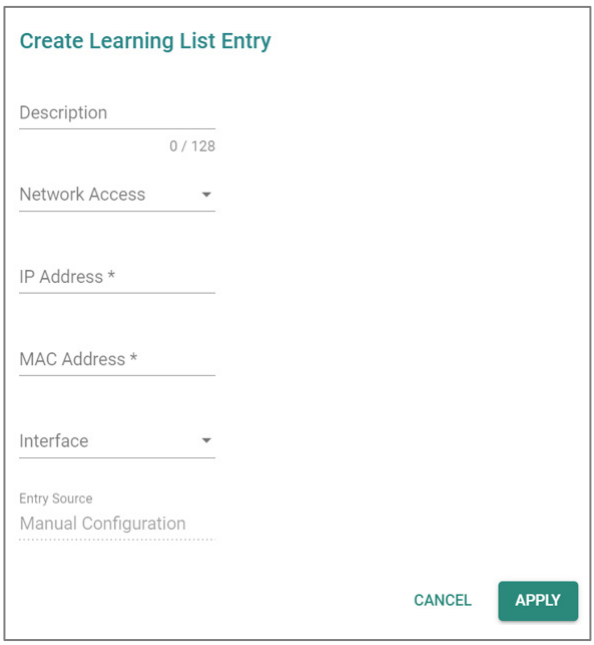
UI Setting	Description
Entry Source	Shows the source of the rule. **Manual Configuration**: The rule was manually created by a user. **Auto Learning**: The rule was created through the learning feature. Refer to Learning Status for more information.

Create Learning List

Menu Path: Firewall > Device Lockdown - Learning Table

Clicking the **Add (⊕)** icon on the **Firewall > Device Lockdown - Learning Table** page will open this dialog box. This dialog lets you manually create a new learning list entry.

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



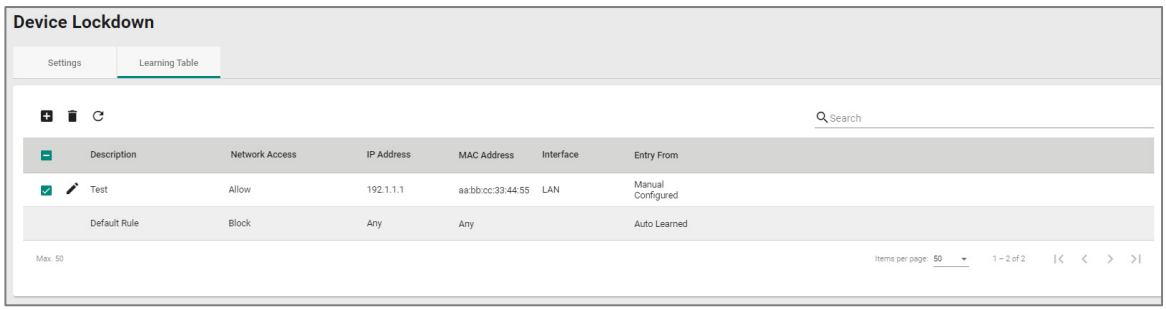
UI Setting	Description	Valid Range	Default Value
Description	Specify a description to help identify the entry.	Up to 128 characters	N/A

UI Setting	Description	Valid Range	Default Value
Network Access	Specify the network access rule to apply for this entry. **Allow**: Grants access to the specified IP address or MAC address. **Block:** Denies access to the specified IP address or MAC address.	Allow / Block	N/A
IP Address	Specify the IP address the rule applies to.	Valid IP address	N/A
MAC Address	Specify the MAC address the rule applies to.	Valid MAC address	N/A
Interface	Specify the interface the rule applies to.	Drop-down menu of interfaces	N/A

Delete Learning List

Menu Path: Firewall > Device Lockdown - Learning Table

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



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.

Note

Because the device's default signature certificates are manufactured without third-party signatures, there is a potential risk of man-in-the-middle attacks that impersonate services, with the client-side being unable to verify.

Therefore, we recommend that upon activating the device, you use the Certificate Management > Local Certificate feature to add or update the certificate to one that belongs to your company and that is issued by a recognized certification authority in order to ensure the security and trustworthiness of your network communications.

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	-	-

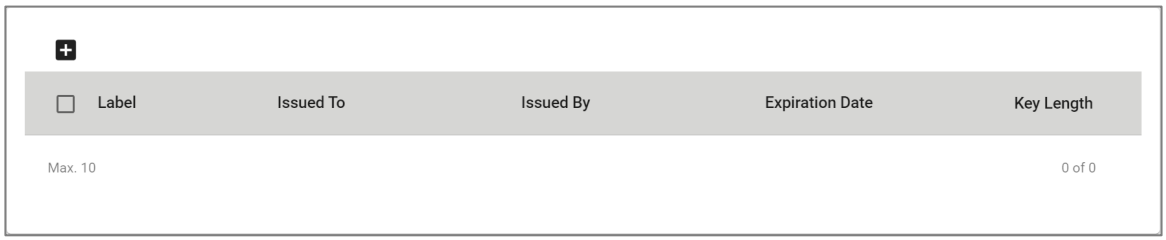
Local Certificate

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.

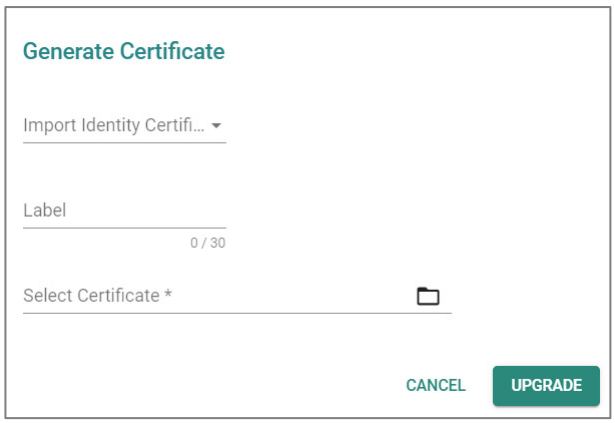


UI Setting	Description
Label	Shows the label identifying the certificate.
Issued To	Shows who the certificate was issued to.
Issued By	Shows who the certificate was issued by.
Expiration Date	Shows the expiration date of the certificate.
Key Length	Shows the key length of the certificate.

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.

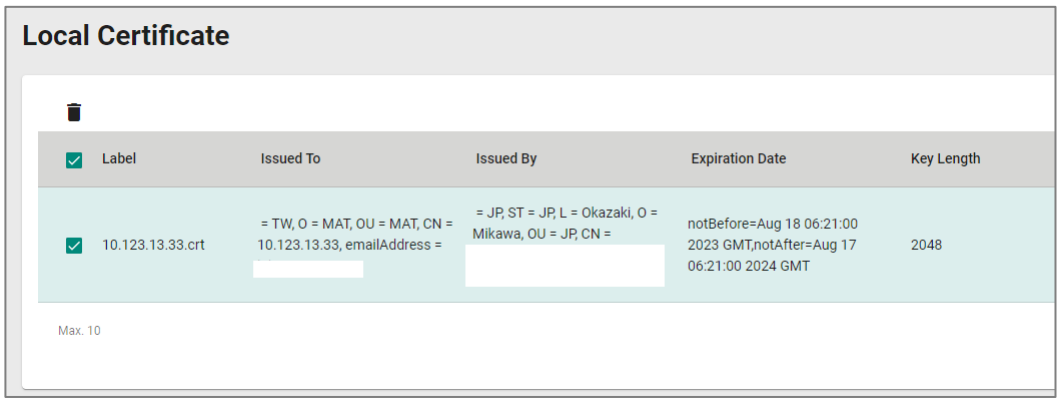


UI Setting	Description	Valid Range	Default Value
Import Identity Certificate	Select the type of certificate to import. **Certificate**: Used for certificates with a .crt file extension. **Certificate From CSR**: Used for certificates issued by another CA. **Certificate From PKCS#12**: Used for certificates 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

UI Setting	Description	Valid Range	Default Value
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. If you would like to delete the item, you can go to SSL setting and change the certificate source to Auto Generate then unlock the certificate you'd like to change.

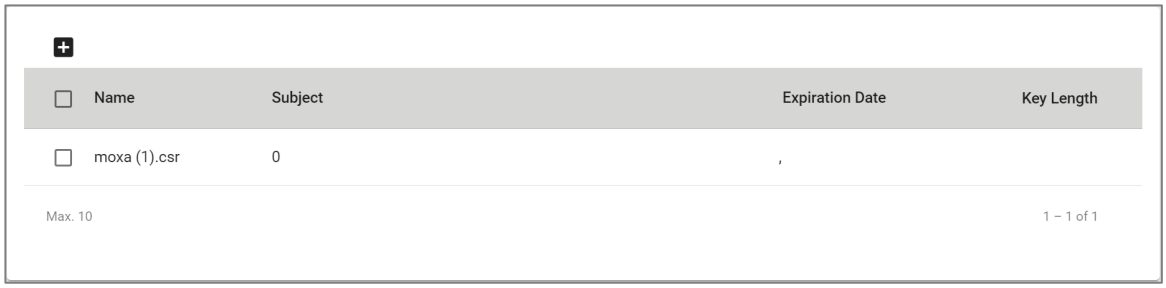
Trusted CA Certificate

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.

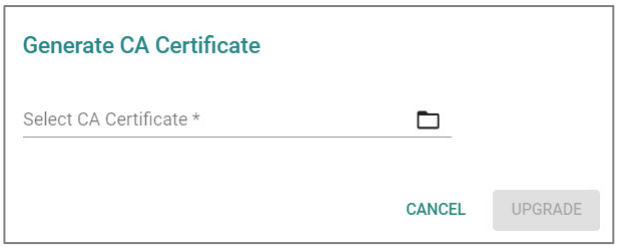


UI Setting	Description
Name	Shows the name of the certificate file.
Subject	Shows the subject from the certificate.
Expiration Date	Shows the expiration date of the certificate.
Key Length	Shows the key length of the certificate.

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.

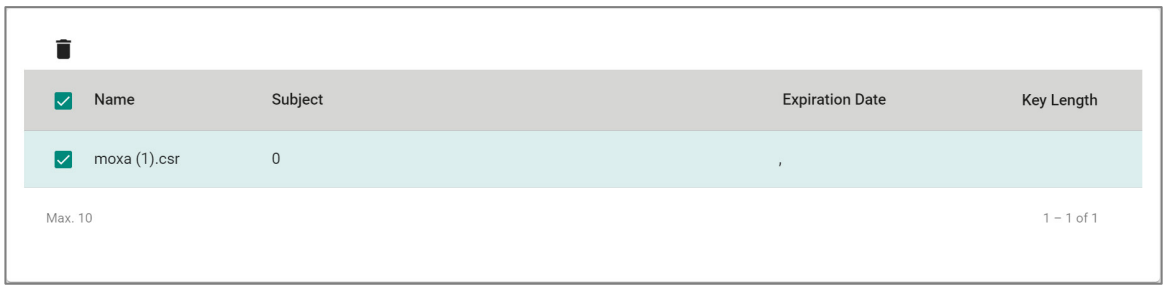


UI Setting	Description	Valid Range	Default Value
Select Certificate	Click this field and select the certificate file from your computer.	Select a file from your computer	N/A

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.



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

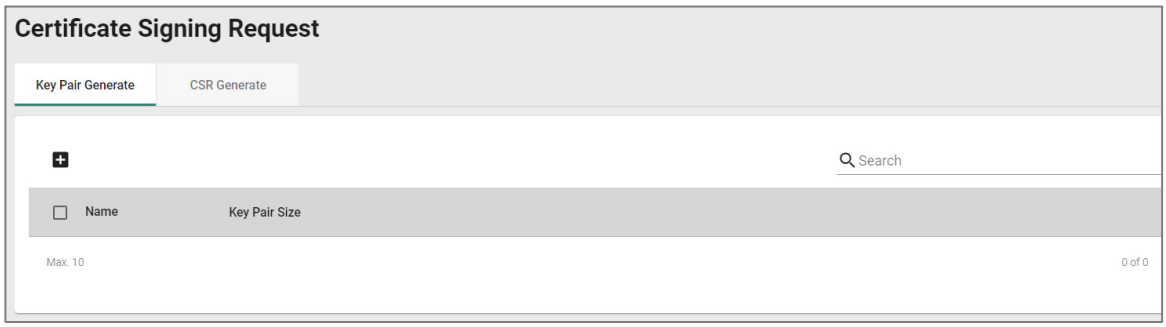
Key Pair Generate

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.



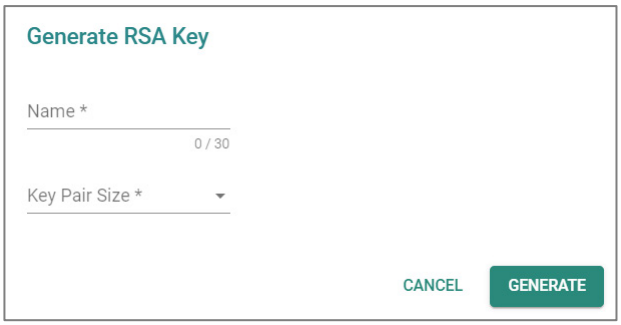
UI Setting	Description
Name	Shows the name of the RSA key.

UI Setting	Description
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.

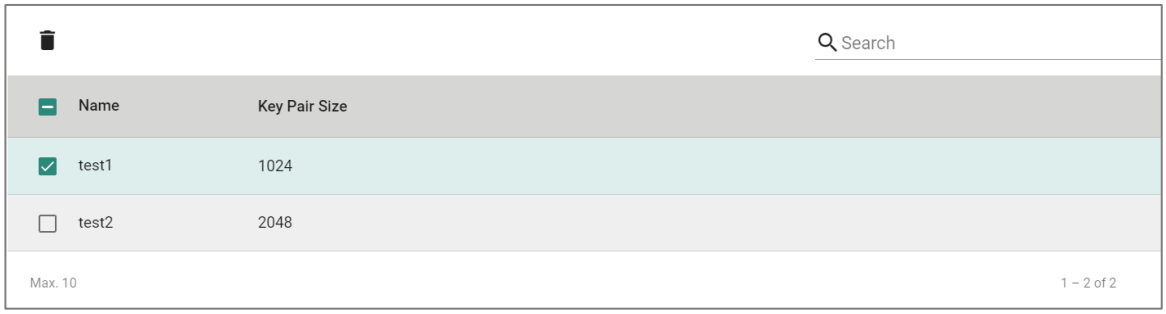


UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the RSA key.	1 to 30 characters	N/A
Key Pair Size	Select the key pair size to use.	1024 Bit / 2048 Bit	N/A

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.



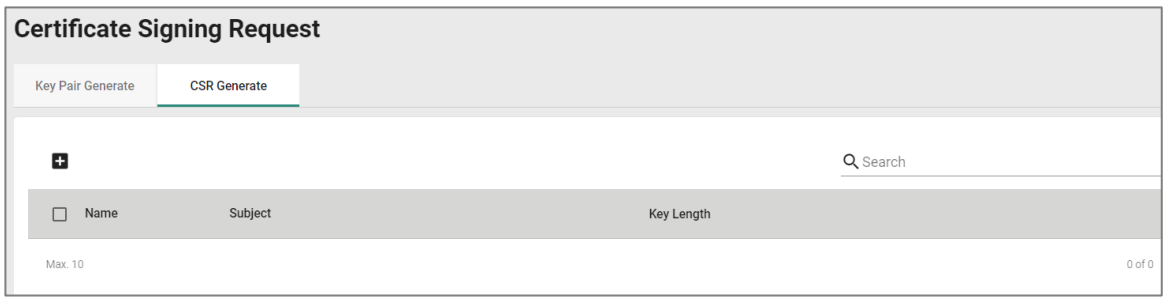
CSR Generate

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.

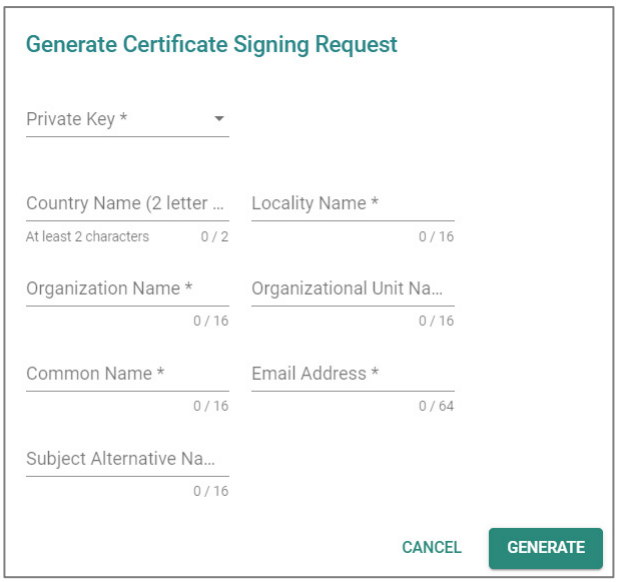


UI Setting	Description
Name	Shows the name of the CSR.
Subject	Shows the subject of the CSR.
Key Length	Shows the key length used by the CSR.

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.



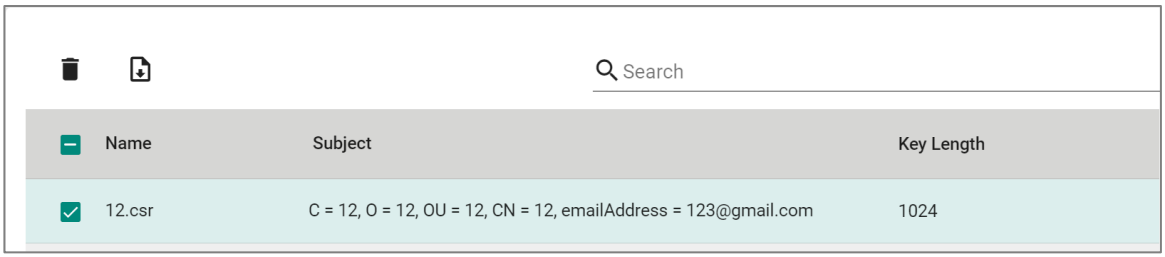
UI Setting	Description	Valid Range	Default Value
Private Key	Select the key pair to use. To generate and manage key pairs, refer to **Certificate Management > Certificate Signing Request - Key Pair Generate**.	Drop-down list of key pairs	N/A
Country Name (2 letter code)	Specify the 2-letter country code 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

UI Setting	Description	Valid Range	Default Value
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

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.



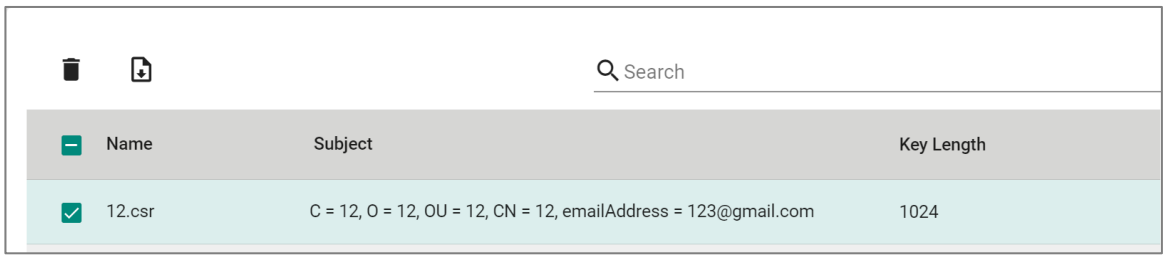
Export Certificate Signing Request

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.


Search
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
- 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	-
Authentication			
Login Authentication	R/W	-	-
RADIUS	R/W	-	-
TACACS+	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.

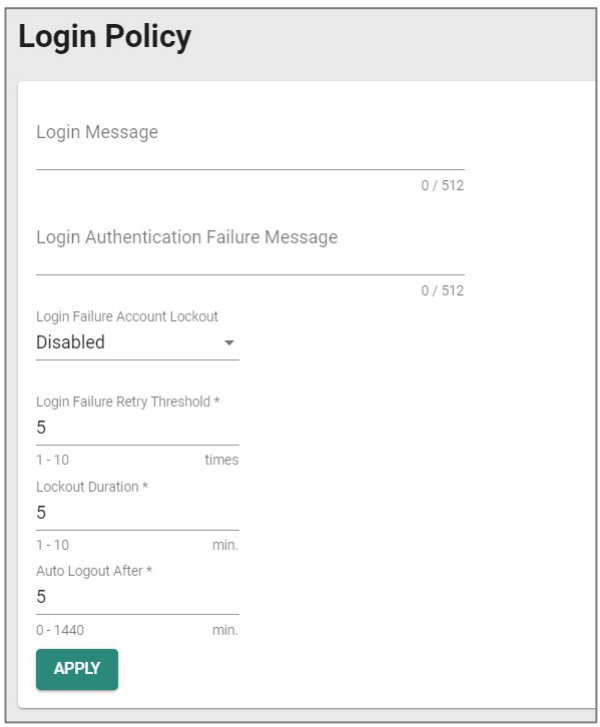
This section includes these pages:

- 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.



UI Setting	Description	Valid Range	Default Value
Login Message	Specify the welcome message to display when users log in to the device. **⚠ Warning** The Login Message should not include login-related information.	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
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.

Note

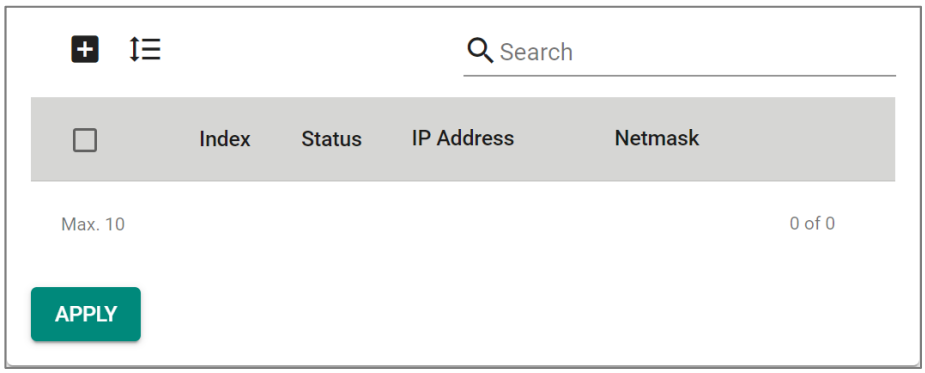
Trusted Access is restricted to the user interface, which includes the Web UI, CLI interface, and Moxa commands from software such as MXconfig and MXview.

Both the DNS Server and NTP Server are only accessible through LAN, VLAN, and Bridge interfaces. In other words, DNS clients and NTP clients cannot access the DNS or NTP service via WAN interfaces on the device.

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	Enabled
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

UI Setting	Description	Valid Range	Default Value
Severity	Select the severity level to assign to Trusted Access events. Refer to the Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency
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 Diagnostics > Event Logs and Notifications > Event Log for more information.	Syslog / Trap / Local Storage	N/A

Trusted IP List



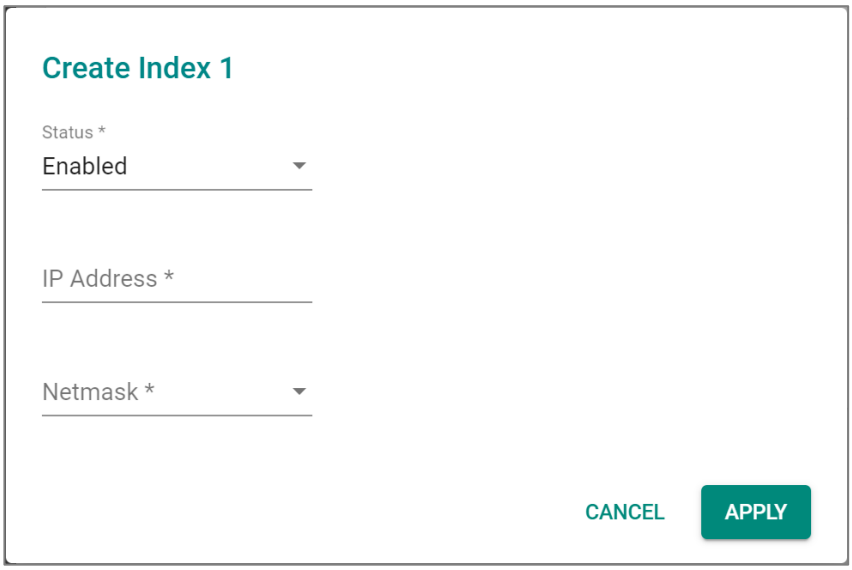
UI Setting	Description
Index	Shows the index of the Trusted IP entry.
Status	Shows whether the Trusted IP entry is enabled or disabled.

UI Setting	Description
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.



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.

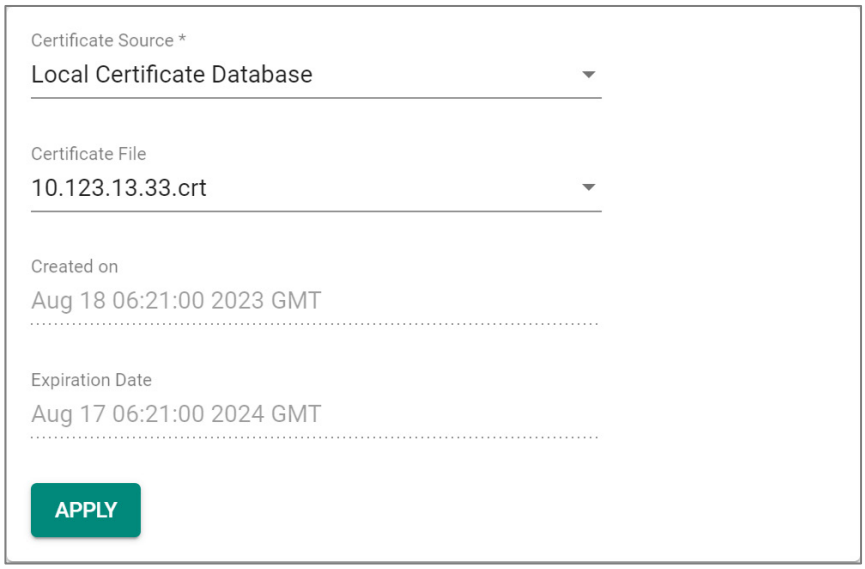
> ⚠ **Warning**
>
> Regenerating the SSH key will restart the device's system services and will make the device temporarily unavailable.

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



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

Authentication

Menu Path: Security > Authentication

This section lets you manage login authentication for your device.

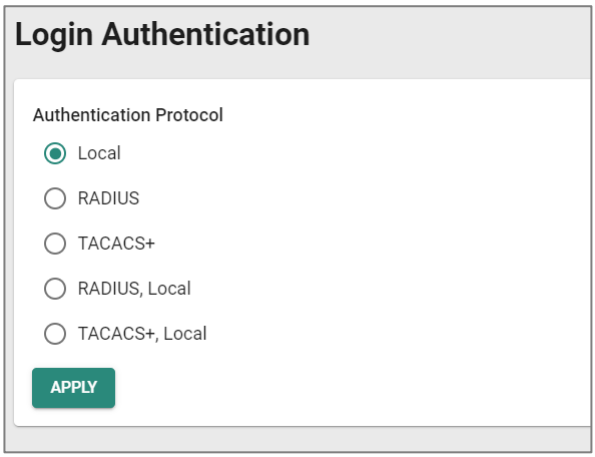
This section includes these pages:

- Login Authentication
- RADIUS
- TACACS+

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.



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. **TACACS+**: Use a TACACS+ Server for authentication. **RADIUS, Local**: Use a RADIUS server for authentication first. If it fails, the device will use the local database for authentication. **TACACS+, Local**: Use a TACACS+ server for authentication first. If it fails, the device wil use the local database for authentication. **⚠ Warning** If you configure the device to use a remote server such as RADIUS or TACACS+ but don't use a local database as a backup, you will unable to log in through network services (HTTP/HTTPS/Telnet/SSH) if the device is unable to connect to the remote server for authentication. In such an event, the only way to access the device would be through the console port.	Local / RADIUS / TACACS+ / RADIUS, Local / TACACS+, Local	Local

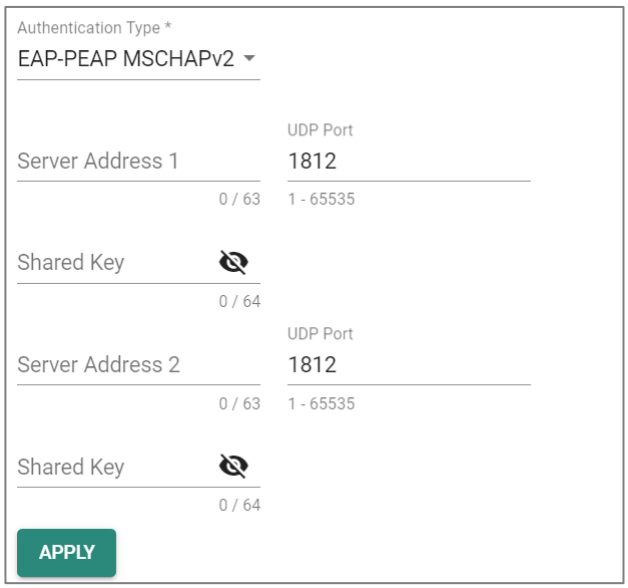
RADIUS

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.

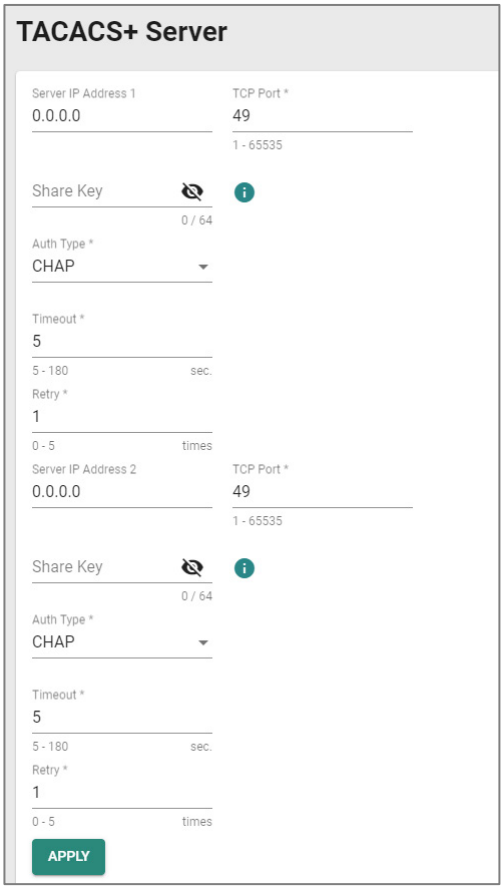


UI Setting	Description	Valid Range	Default Value
Authentication Type	Select the authentication method to use for the RADIUS servers.	PAP / CHAP / EAP-PEAP MSCHAPv2	EAP-PEAP MSCHAPv2
Server Address 1	Specify the IP address or domain name for the primary RADIUS server.	Valid IP address or domain name	N/A
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 64 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 64 characters	N/A

TACACS+

Menu Path: Security > Authentication > TACACS+

This page lets you set up TACACS+ protocol to authenticate remote users.



UI Setting	Description	Valid Range	Default Value
Server IP Address 1	Specify the IPv4 address of the primary TACACS+ server to use. Setting the address to 0.0.0.0 will disable use of a primary TACACS+ server. When authenticating a remote user, the device will try to authenticate them using the primary server specified by **Server IP Address 1**. If the device fails to connect to the primary server, it will try to authenticate by using the secondary server specified by **Server IP Address 2**.	Valid IP address	0.0.0.0
TCP Port	Specify the TCP port to use for authentication requests to the primary TACACS+ server.	1 to 65535	49
Shared Key	Specify the shared encryption key for the primary TACACS+ server.	1 to 64 characters	N/A
Auth Type	Specify which authentication type the primary TACACS+ server uses.	PAP, CHAP, ASCII	CHAP

UI Setting	Description	Valid Range	Default Value
Timeout	Specify the amount of time in seconds a client will wait for a response from the primary TACACS+ server before re-transmitting the request.	5 to 120 (sec)	5
Retry	Specify the number of times the device will try to contact the primary TACACS+ server.	0 to 5	1
Server IP Address2	Specify the IPv4 address of the secondary TACACS+ server to use. Setting the address to 0.0.0.0 will disable use of a secondary TACACS+ server.	Valid IP address	0.0.0.0
TCP Port	Specify the TCP port to use for authentication requests to the secondary TACACS+ server.	1 to 65535	49
Shared Key	Specify the shared encryption key for the secondary TACACS+ server.	1 to 64 characters	N/A
Auth Type	Specify which authentication typethe secondary TACACS+ server uses.	PAP, CHAP, ASCII	CHAP
Time out	Specify the amount of time in seconds a client will wait for a response from the secondary TACACS+ server before re-transmitting the request.	5 to 120 (sec)	5
Retry	Specify the number of times the device will try to contact the secondary TACACS+ server.	0 to 5	1

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

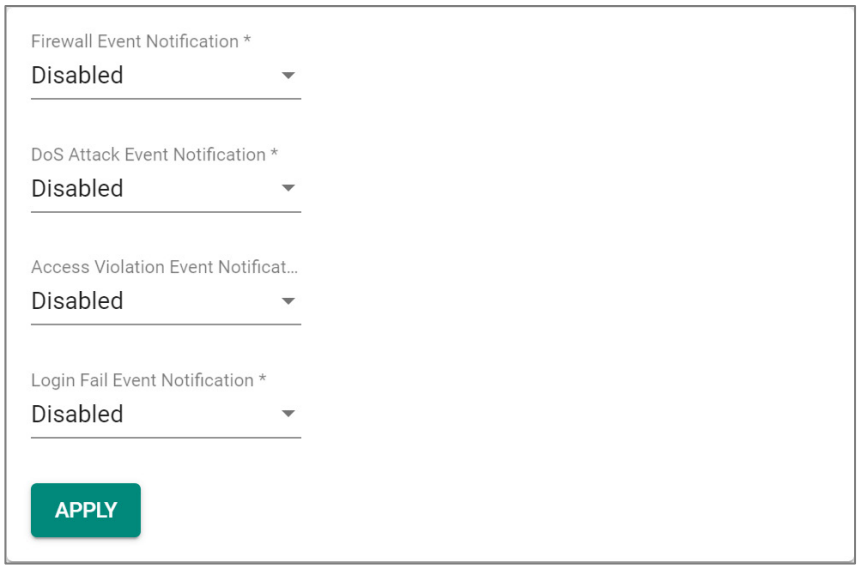
Menu Path: Security > MXview Alert Notification - Security Notification Setting

This page lets you configure your MXview security alert notification settings.

Note

Notifications are handled by the SNMP Trap function, which should be configured in advance. Refer to Diagnostics > Event Logs and Notifications > SNMP Trap/Inform for more information.

In MXview, go to Preferences > Server > SNMP Trap Server and make sure the matching SNMP version is selected.



UI Setting	Description	Valid Range	Default Value
Firewall Event Notification	Enable or disable notifications for Firewall events. **Note** After enabling this, you will need to enable logging and select **Trap** as the log destination for each firewall policy and feature you want notifications for.	Enabled / Disabled	Disabled
DoS Attack Event Notification	Enable or disable notifications for DoS attack events. **Note** After enabling this, you will need to go to Firewall > DoS Policy to enable logging and select **Trap** as the log destination to receive notifications.	Enabled / Disabled	Disabled

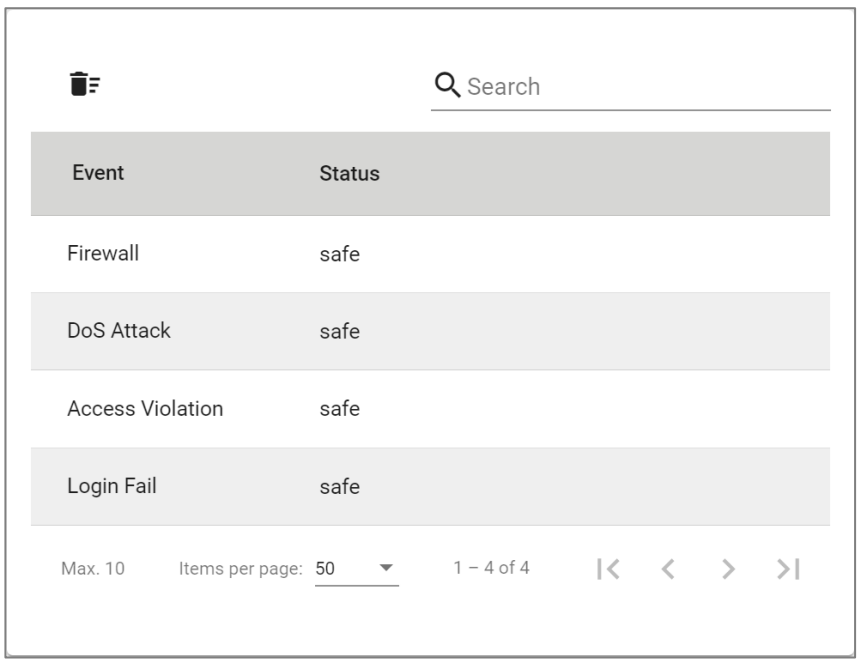
UI Setting	Description	Valid Range	Default Value
Access Violation Event Notification	Enable or disable notifications for Access Violation events. **Note** After enabling this, you will need to go to Security > Device Security > Trusted Access to enable logging and select Trap as the log destination to receive notifications.	Enabled / Disabled	Disabled
Login Fail Event Notification	Enable or disable notifications for Login Fail events. **Note** After enabling this, you will need to go to Diagnostics > Event Logs and Notifications > Event Notifications to enable logging and select Trap as the log destination to receive notifications.	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.

Clicking the **Reset ( )** icon will clear the status of all events to default (**safe**).



UI Setting	Description
Event	Shows the name of the event type. Event types shown will vary depending on the device model. **Note** The status of **Device Lockdown** can not be accessed in MXview One.
Status	Shows the current status of the event type. **safe**: No event of this type has been detected. **attacked**: An event of this type was detected.

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
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

Settings	Admin	Supervisor	User
SNMP Trap/Inform	R/W	-	-
Email Settings	R/W	R	R
Tools			
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

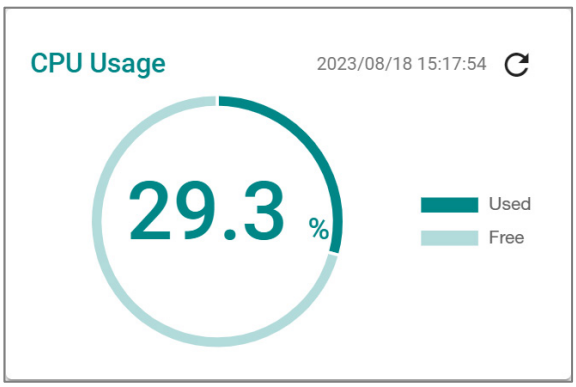
Utilization

Menu Path: Diagnostics > System Status > Utilization

This page lets you monitor current and historical system resource utilization.

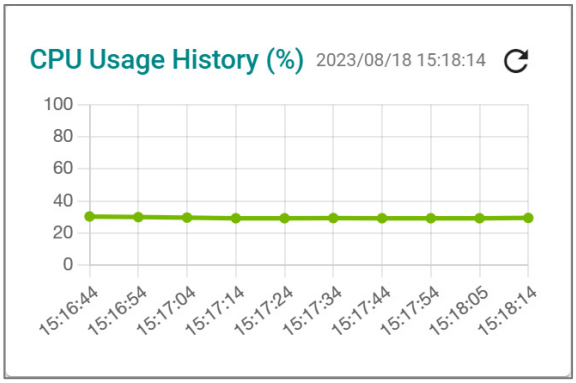
CPU Usage

This shows the current CPU usage of your device.



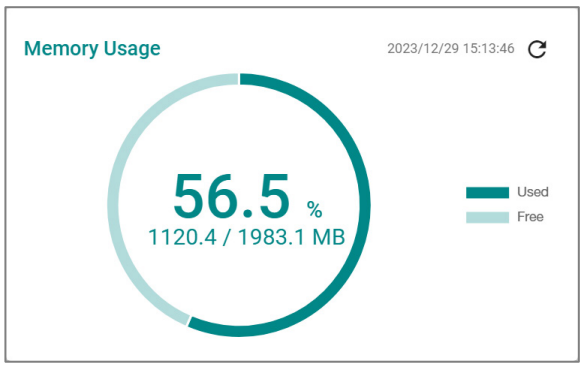
CPU Usage History

This shows the CPU usage of your device over time.



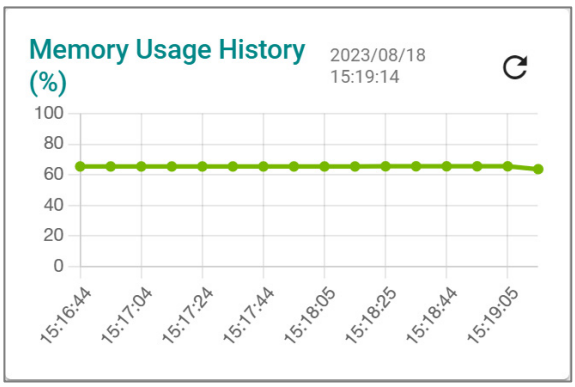
Memory Usage

This shows your device's current memory usage.



Memory Usage History

This shows your device's memory usage over time.



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.

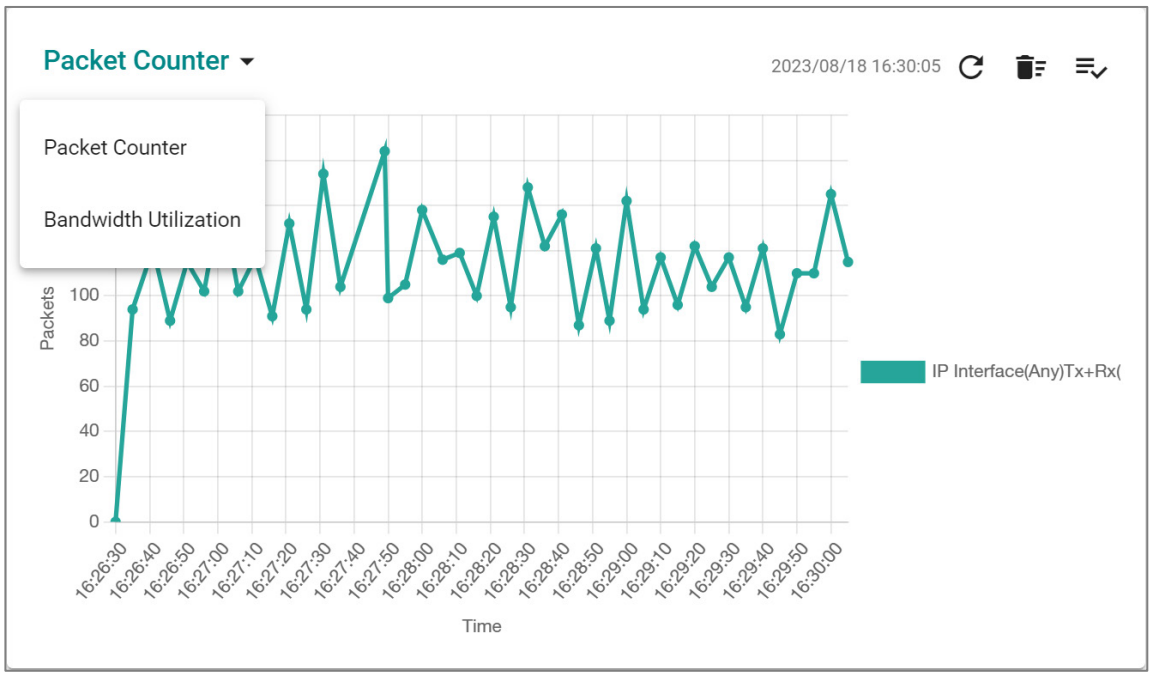
Network Status Display

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.

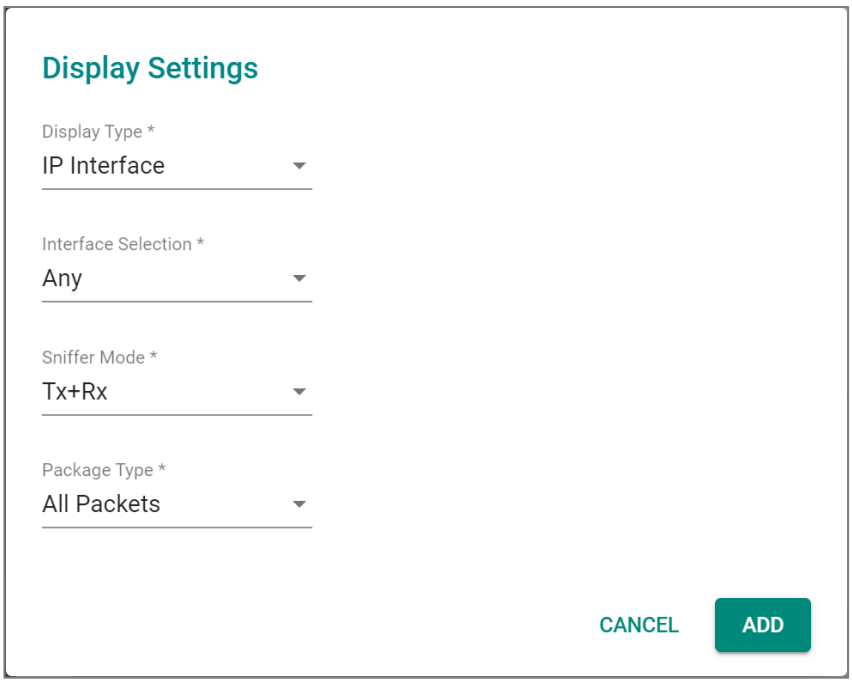


UI Setting	Description
Refresh ( )	Updates statistics immediately without waiting for the refresh interval.
Reset Statistics Graph ( )	Clears the display and resets display settings back to defaults.
Display Settings ( )	Opens **Display Settings**, which allows you to add lines based on user-defined 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.

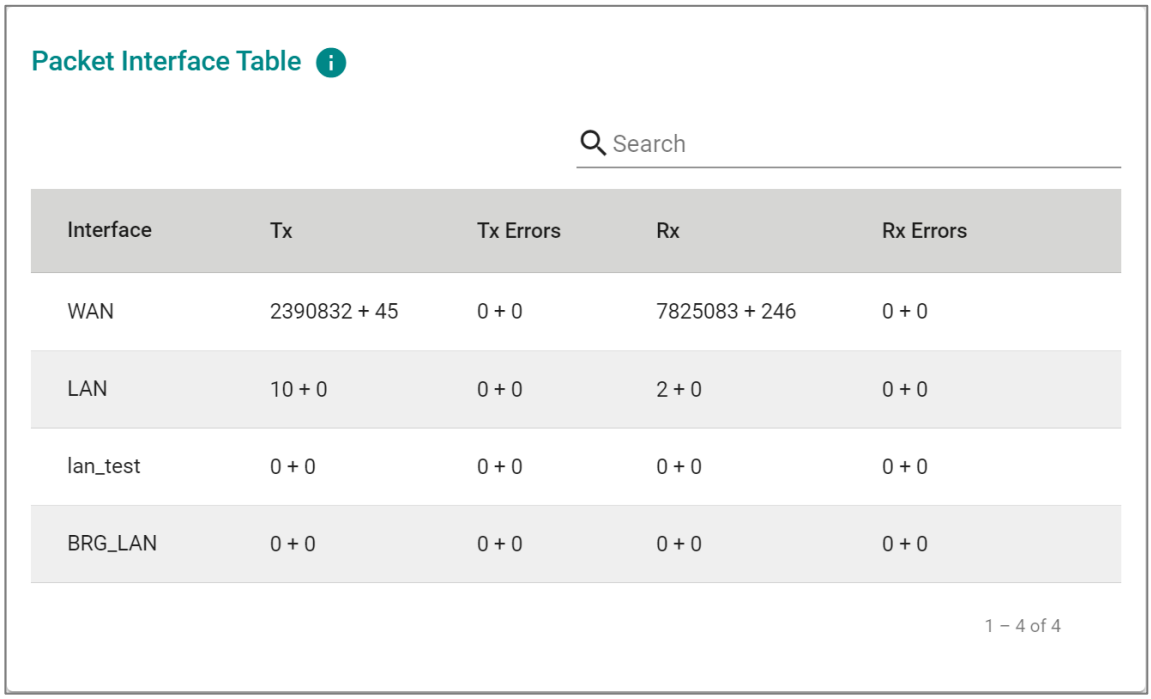


UI Setting	Description	Valid Range	Default Value
Display Type	Select whether to monitor an IP interface or a port. **Port**: Monitor traffic for a specific port. **IP Interface**: Monitor traffic for a specific network interface.	Port / IP Interface	IP Interface
Interface Selection **(if Display Type 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
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

UI Setting	Description	Valid Range	Default Value
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*.

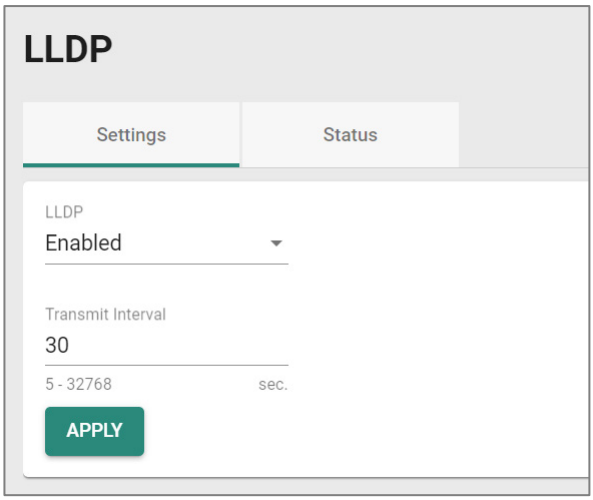


LLDP Settings

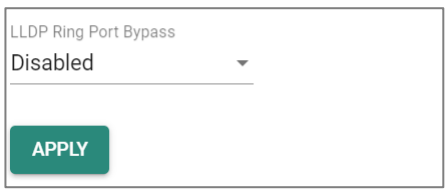
Menu Path: Diagnostics > Network Status > LLDP

This page lets you configure Link Layer Discovery Protocol (LLDP) settings.

LLDP Settings

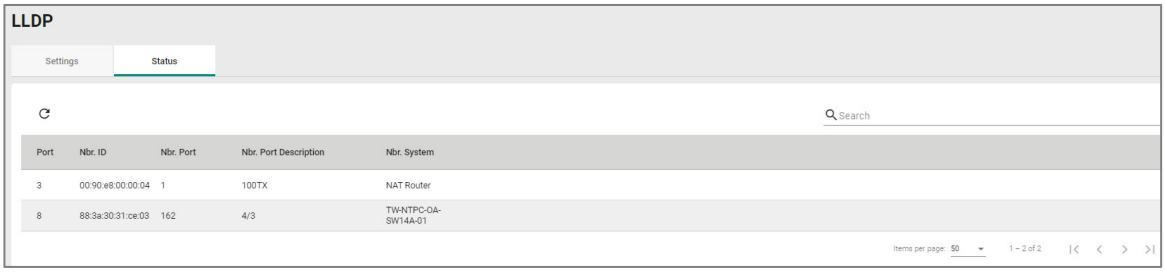


UI Setting	Description	Valid Range	Default Value
LLDP	Enable or disable Link Layer Discovery Protocol (LLDP).	Enabled / Disabled	Enabled
Transmit Interval	Specify the interval in seconds at which LLDP messages are sent.	5 to 32768	30



UI Setting	Description	Valid Range	Default Value
LLDP Ring Port Bypass	Enable or disable LLDP Ring Port Bypass	Enabled / Disabled	Disabled

LLDP Status List



UI Setting	Description
Port	Shows the number of the port that connects to the neighbor device.
Nbr. ID	Shows the unique ID (typically the MAC address) that identifies the neighbor device.
Nbr. Port	Shows the port number of the connected neighbor device's interface that is used to connect to this device.
Nbr. Port Description	Shows the port description of the connected neighbor device's interface that is used to connect to this device.
Nbr. System	Shows the hostname of the neighbor device.

ARP Table

Menu Path: Diagnostics > Network Status > ARP Table

This page lets you see the device’s Address Resolution Protocol (ARP) table.

Limitations

The ARP table can show up to 1024 entries.

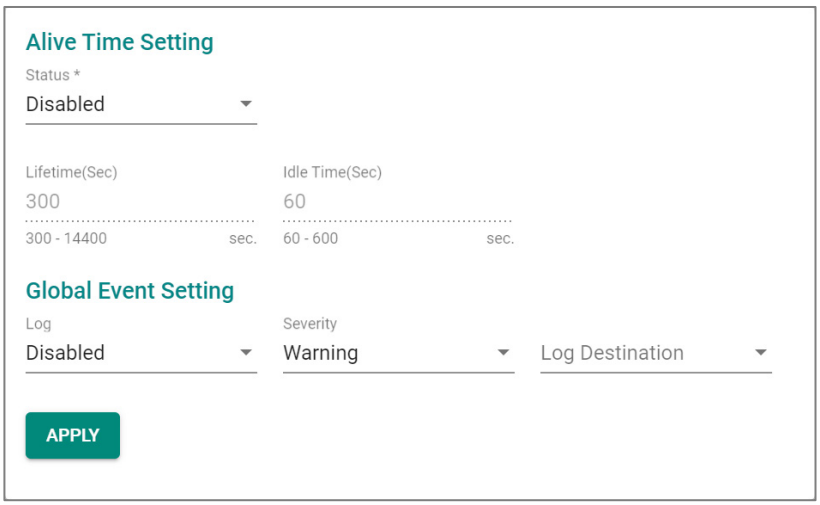
UI Setting	Description
Index	Shows the index of the device entry.
MAC Address	Shows the MAC address of the device.
IP Address	Shows the IP address used for the device.
Interface	Shows the interface the device is connecting through.

Connection Management

Menu Path: Diagnostics > Network Status > Connection Management

This page lets you configure the Connection Management feature of your device. Click **APPLY** to save your changes.

Connection Management Settings



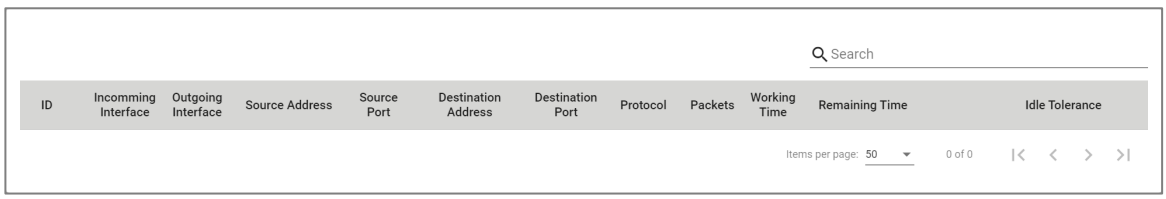
Alive Time Setting

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable connection management through alive time monitoring.	Enabled / Disabled	Disabled
Lifetime(Sec) **(If Status is Enabled)**	Specify the maximum lifetime of a connection in seconds before it will be deleted. Setting this to 0 means that connections will have an infinite lifetime and will not be deleted. **Note** New connections cannot be made if the **Total TCP Connection** limit is reached for an applicable session control policy, or if the device limit of 10000 connections is reached. Refer to Session Control for more information about session control policies.	0, 300 to 144000	300
Idle Time(Sec) **(If Status is Enabled)**	Specify the number of seconds a connection can be idle before deleting the connection. Longer idle times allow connections to stay open without relying on clients to send keep-alive messages.	60 to 600	60

Global Event Setting

UI Setting	Description	Valid Range	Default Value
Log	Enable or disable logging of connection management events.	Enabled / Disabled	Disabled
Severity	Select the severity level to assign events for this policy. Refer to the Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	
Log Destination	Specify where to send logs for this event. 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 Diagnostics > Event Logs and Notifications > Event Log for more information.	Syslog / Trap / Local Storage	None

Connection Table



UI Setting	Description
ID	Shows the ID of the connection the entry is for.
Incoming Interface	Shows the incoming interface for the connection.
Outgoing Interface	Shows the outgoing interface for the connection.
Source Address	Shows the source IP address for the connection.
Source Port	Shows the source port for the connection.
Destination Address	Shows the destination IP address for the connection.

UI Setting	Description
Destination Port	Shows the destination port for the connection.
Protocol	Shows whether the connection uses TCP, UDP, ICMP, or an unknown protocol.
Packets	Shows how many packets have been transferred for the connection.
Working Time	Shows how long the connection has been up.
Remaining Time	Shows how much time is remaining for the connection before it is deleted.
Idle Tolerance	Shows the allowable idle time for the connection.

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 to PDF, JSON, or Excel files.

> **Note**
> Browser extensions such as ad-blockers, uBlock Origin may interfere with file exports. If you encounter this issue, we strongly recommend using a recommended browser and disabling any plug-ins. Refer to Using a Web Browser to Configure the Industrial Secure Router for more information.

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

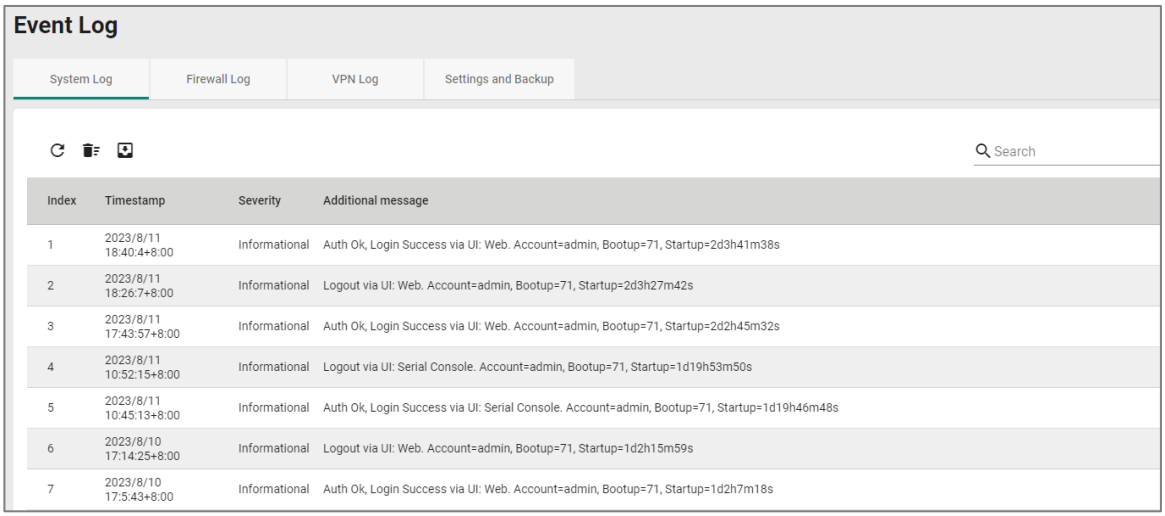
This page lets you view your device's system-related event logs.

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.



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.

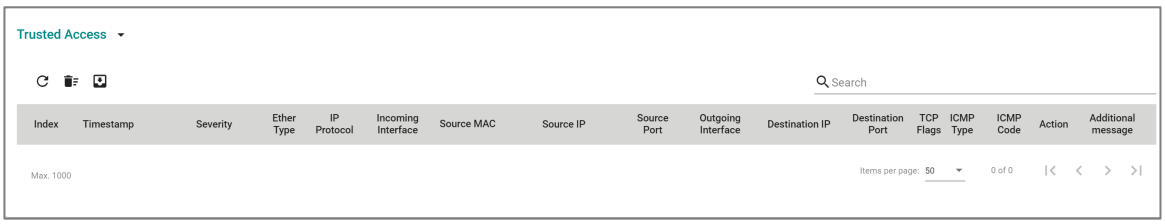
- Trusted Access
- Malformed Packets
- DoS Policy
- Layer 3-7 Policy

- Protocol Filter Policy
- ADP
- IPS
- Session Control
- Layer 2 Policy
- Ping Response
- Device Lockdown

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.

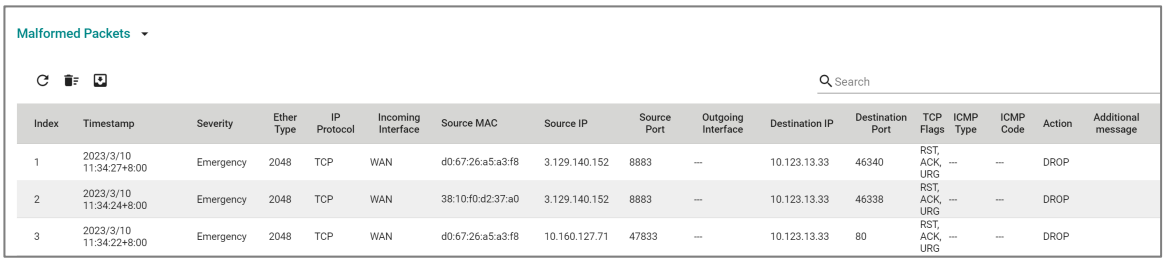
Trusted Access



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: Refer to the Severity Level List for more information.
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.

UI Setting	Description
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.
Additional message	Shows additional information about the event, based on the type of event.

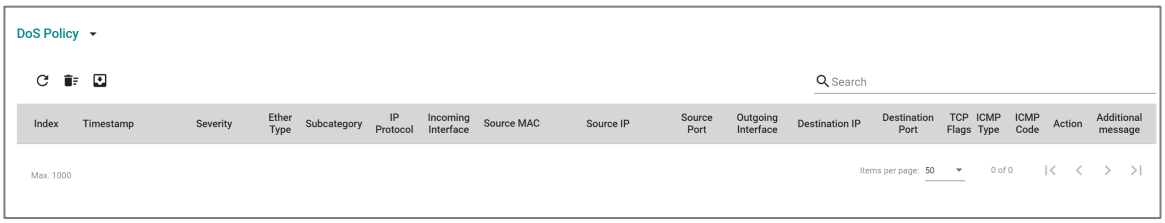
Malformed Packets



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: Refer to the Severity Level List for more information.

UI Setting	Description
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: • Aceept • Drop
Additional message	Shows additional information about the event, based on the type of event.

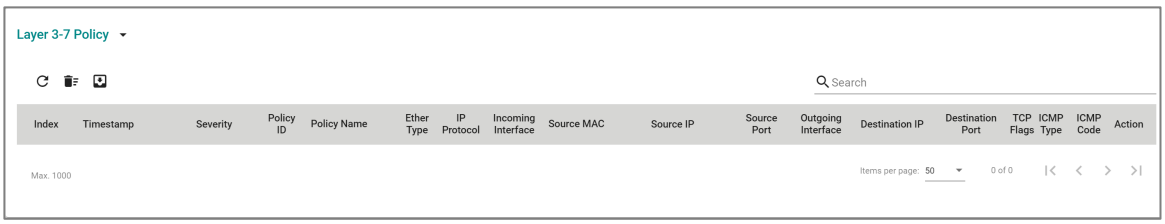
DoS Policy



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: Refer to the Severity Level List for more information.
Ether Type	Shows the EtherType that applies to this event.
Subcategory	Shows the subcategory that applies to this event: • Null Scan • Xmas Scan • NMAP-Xmas Scan • SYN/FIN Scan • FIN Scan • NMAP-ID Scan • SYN/RST Scan • NEW-TCP-Without-SYN Scan • ICMP-Death • SYN-Flood • ARP-Flood • UDP-Flood
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.

UI Setting	Description
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.

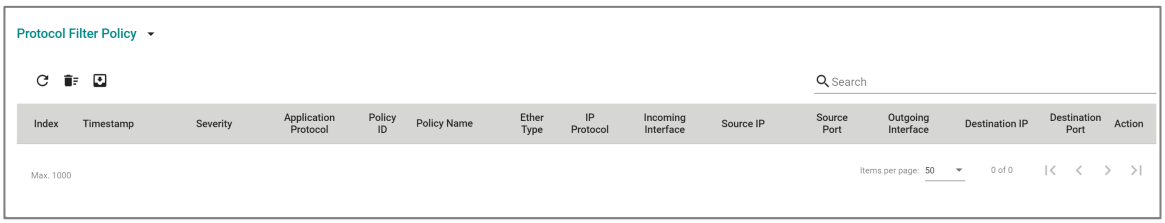
Layer 3-7 Policy



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: Refer to the Severity Level List for more information.
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.

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: • Allow • Deny

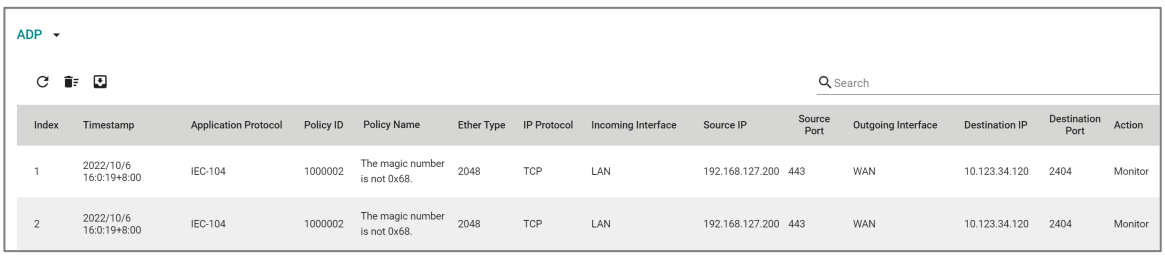
Protocol Filter Policy



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: Refer to the Severity Level List for more information.
Application Protocol	Shows which application this event is related to.
Policy ID	Shows the ID of the firewall policy that applies to this event.

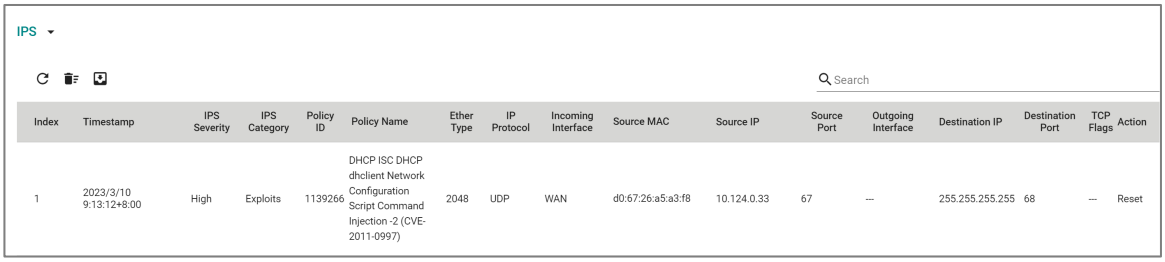
UI Setting	Description
Policy Name	Shows the name of the firewall policy that applies to this event.
Ether Type	Shows the EtherTypes for this traffic.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC 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.
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



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: • **Accept**: The traffic will be allowed to pass through. • **Reset**: The traffic will not be allowed to pass through. • **Monitor**: The traffic will be allowed to pass through, but a log entry will be created for it.

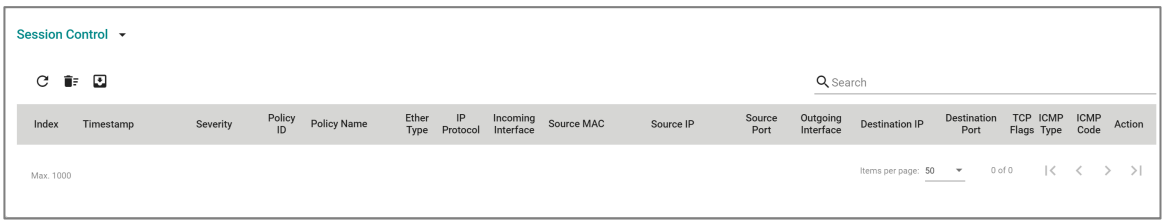
IPS



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: • Information • Low • Medium • High • Critical
IPS Category	Shows the IPS category of the event: • File vulnerabilities • Buffer overflow • DoS attacks • Exploits • Malware traffic • Reconnaissance • Web threats • Flooding & scan • Protocol attack protection • IP spoofing
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.

UI Setting	Description
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.

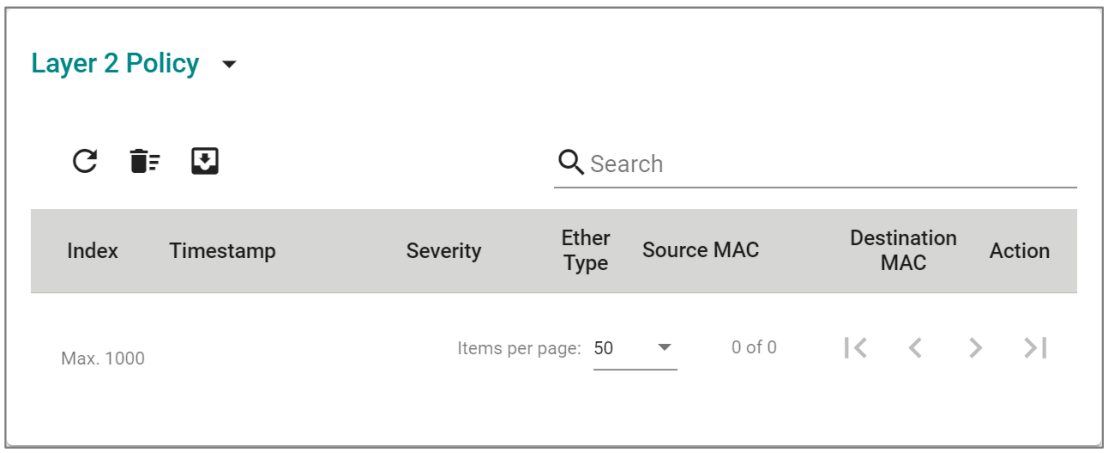
Session Control



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: Refer to the Severity Level List for more information.
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.

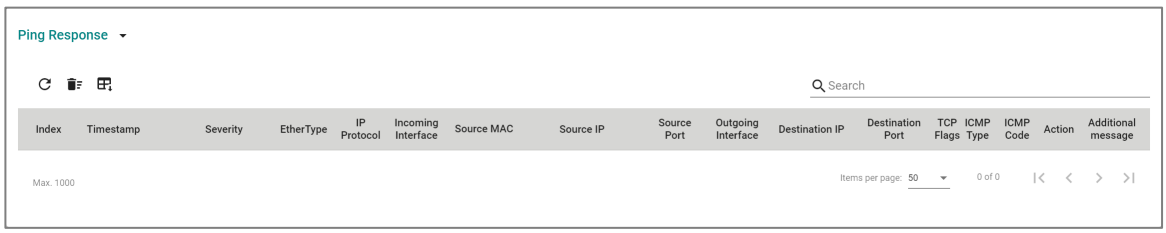
UI Setting	Description
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
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: Refer to the Severity Level List for more information.
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: • Allow • Deny

Ping Response



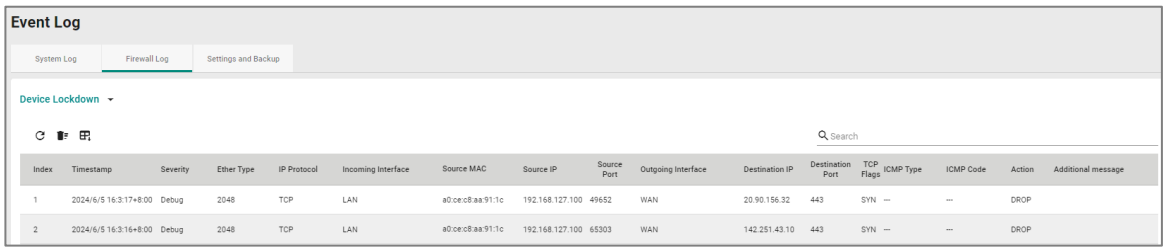
UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
Ether Type	Shows the EtherType that applies to this event.
IP Protocol	Shows the IP protocol for this traffic.

UI Setting	Description
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.
Additional message	Shows additional information about the event, based on the type of event.

Device Lockdown

Note

Device Lockdown is specifically designed for and will only be available on the NAT series.



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: Refer to the Severity Level List for more information.
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.
Additional Message	Shows the additional message for this event.

VPN Log

Menu Path: Diagnostics > Event Logs and Notifications > Event Log - VPN Log

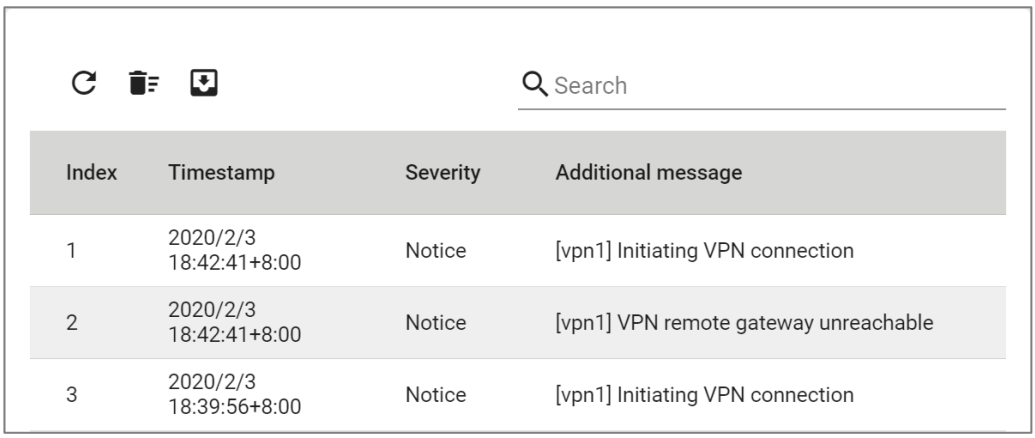
This page lets you view your device's VPN-related event logs.

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.



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.

Network Log

Menu Path: Diagnostics > Event Logs and Notifications > Event Log - Network Log

This page lets you view your device's network-related event logs.

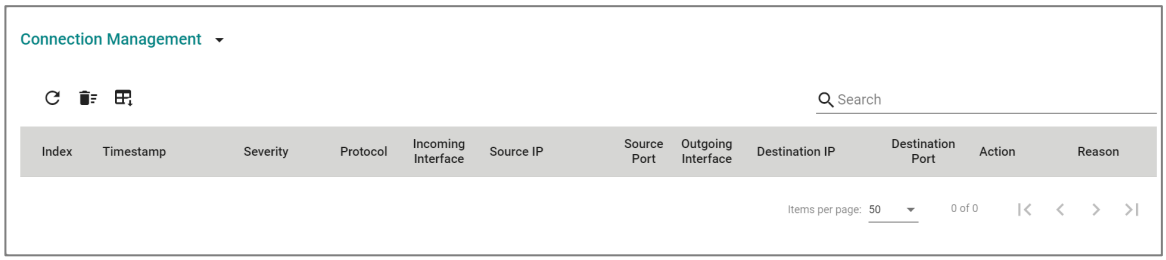
You can switch between different network logs by clicking on the drop-down menu.

- Connection Management
- RX Discard
- Neighbor MAC Change

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.

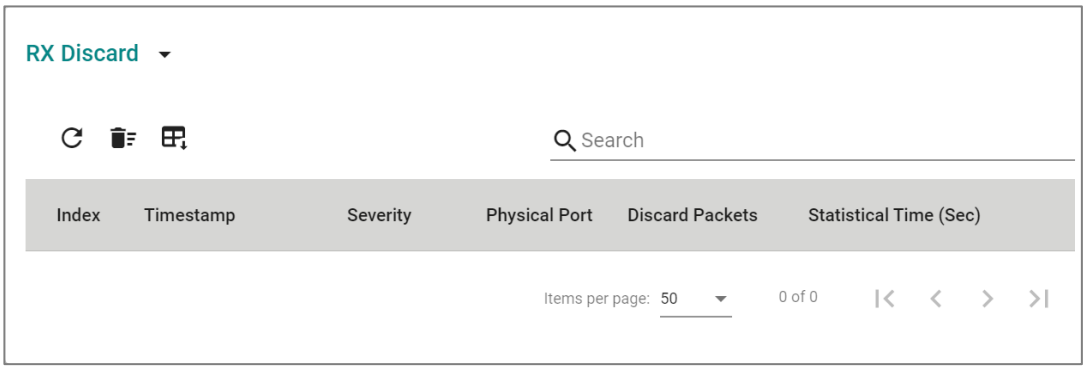
Network Log - Connection Management



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: Refer to the Severity Level List for more information.
Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for the connection.
Source IP	Shows the source IP address for the connection.
Source Port	Shows the source port for the connection.
Outgoing Interface	Shows the outgoing interface for the connection.

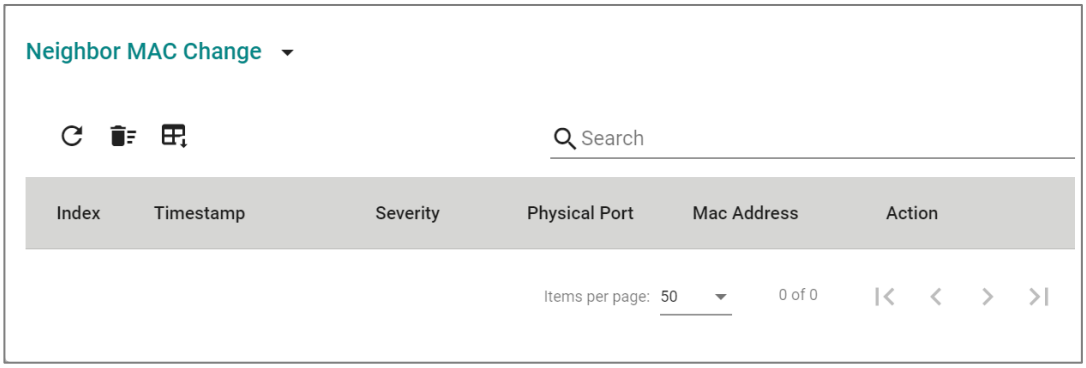
UI Setting	Description
Destination IP	Shows the destination IP address for the connection.
Destination Port	Shows the destination port for the connection.
Action	Shows the action taken by the firewall for this event.
Reason	Shows additional information about the event, based on the type of event.

Network Log - RX Discard



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: Refer to the Severity Level List for more information.
Physical Port	Shows which port has discarded RX packets.
Discard Packets	Shows how many RX packets were discarded. **Note** The Discard Packets count will reset after the device is rebooted.
Statistical Time (Sec)	Shows the interval in seconds between RX discard packet checks.

Network Log - Neighbor MAC Change



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: Refer to the Severity Level List for more information.
Physical Port	Shows the physical port the neghbor device is connected to.
MAC Address	Shows the new MAC address of the neighbor device.
Action	Shows the action taken for this event.

Settings and Backup

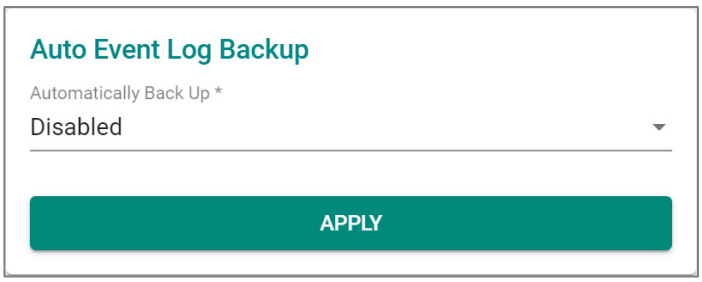
Menu Path: Diagnostics > Event Logs and Notifications > Event Log - Settings and Backup

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

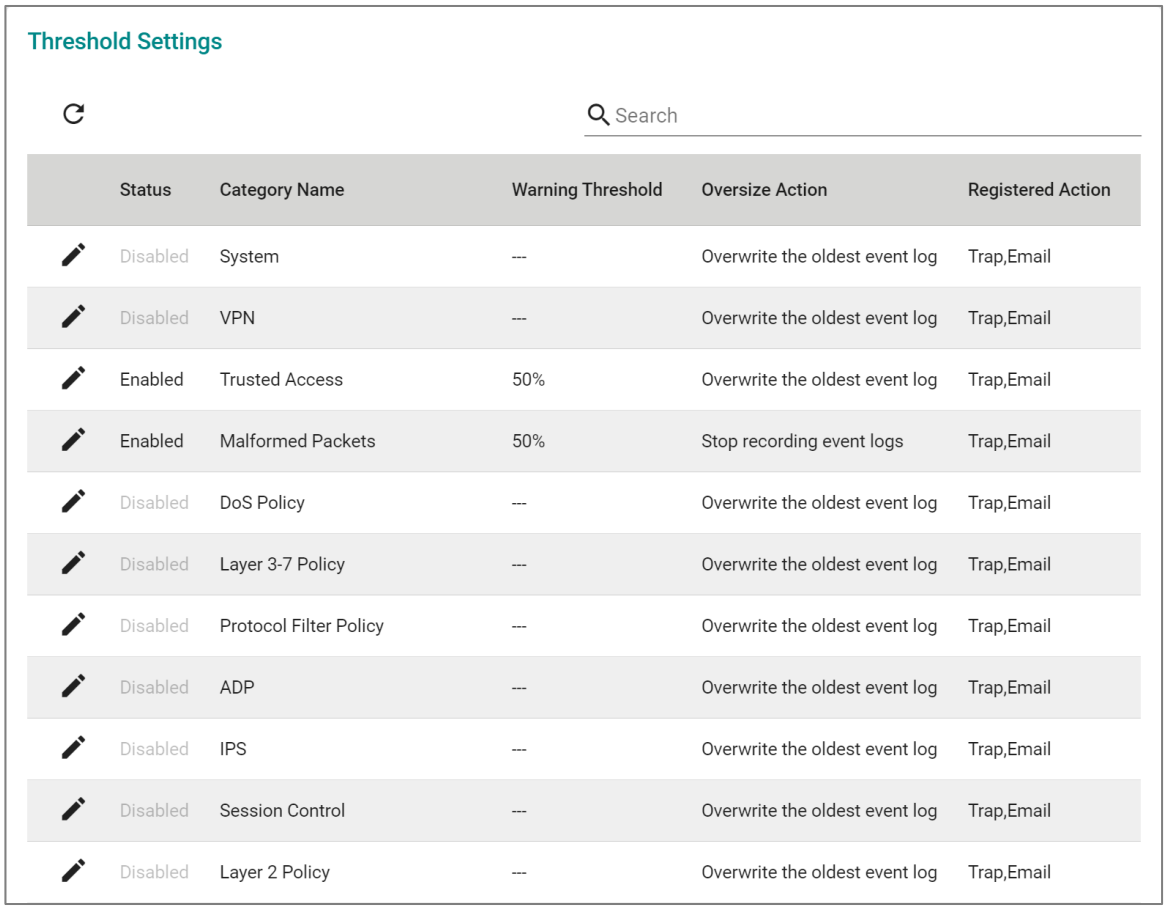
Click the **CLEAR** button to clear all event logs.

Auto Event Log Backup



UI Setting	Description	Valid Range	Default Value
Automatically Restore	Enable or disable automatic event log backups.	**Enabled / Disabled**	Disabled

Threshold Settings

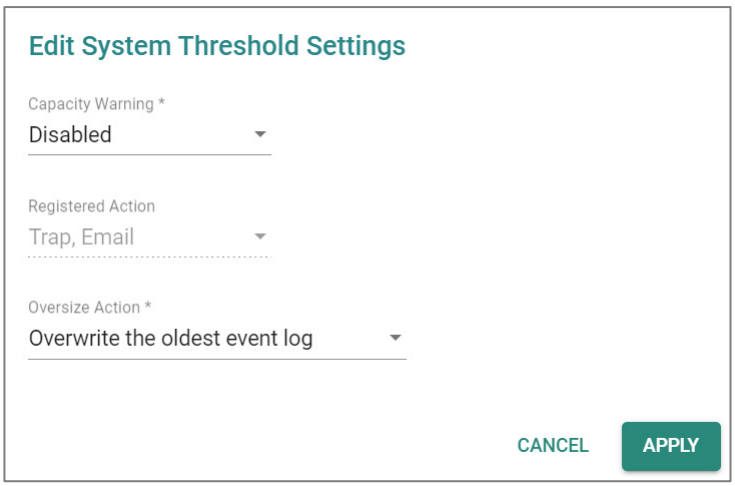


UI Setting	Description
Status	Shows whether threshold settings are enabled for the category.
Category Name	Shows which event log the threshold settings apply to.
Warning Threshold	Shows the threshold percentage that must be reached to trigger a warning sent through the **Registered Action** methods.
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.



UI Setting	Description	Valid Range	Default Value
Capacity Warning	Enable or disable capacity warnings for the selected event log category.	Enabled / Disabled	Disabled
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
- CPU Usage
- Port Usage

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

System | Port

Search

	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	

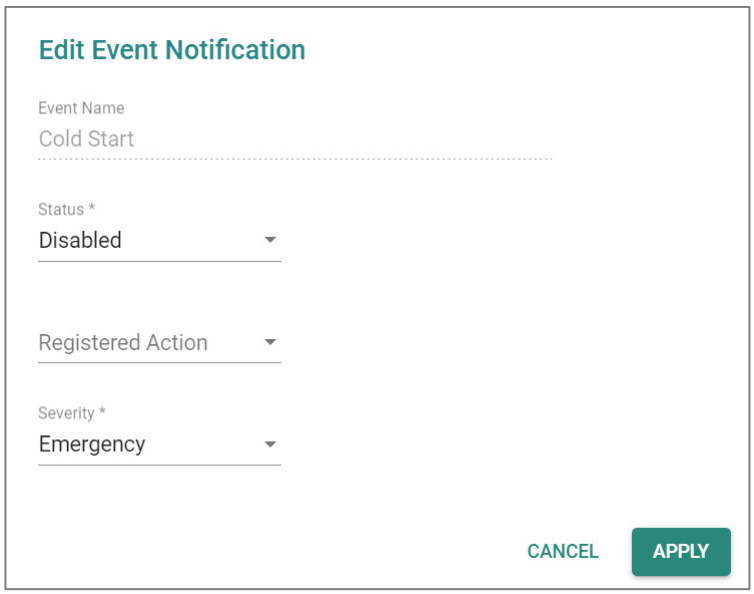
1 – 28 of 28

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.
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
Registered Action	Shows which action will be taken for this kind of event. **Trap**: A notification is sent to the Trap server when the event is triggered. **Email**: A notification is sent to the email server defined in the Email Settings section. **Syslog**: An event log is recorded to the Syslog server defined in the Syslog section. **Relay:** A notification is sent through the relay interface, if the device has one, when the event is triggered. **Note** The types of actions available may vary depending on the event type and the device model.

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.



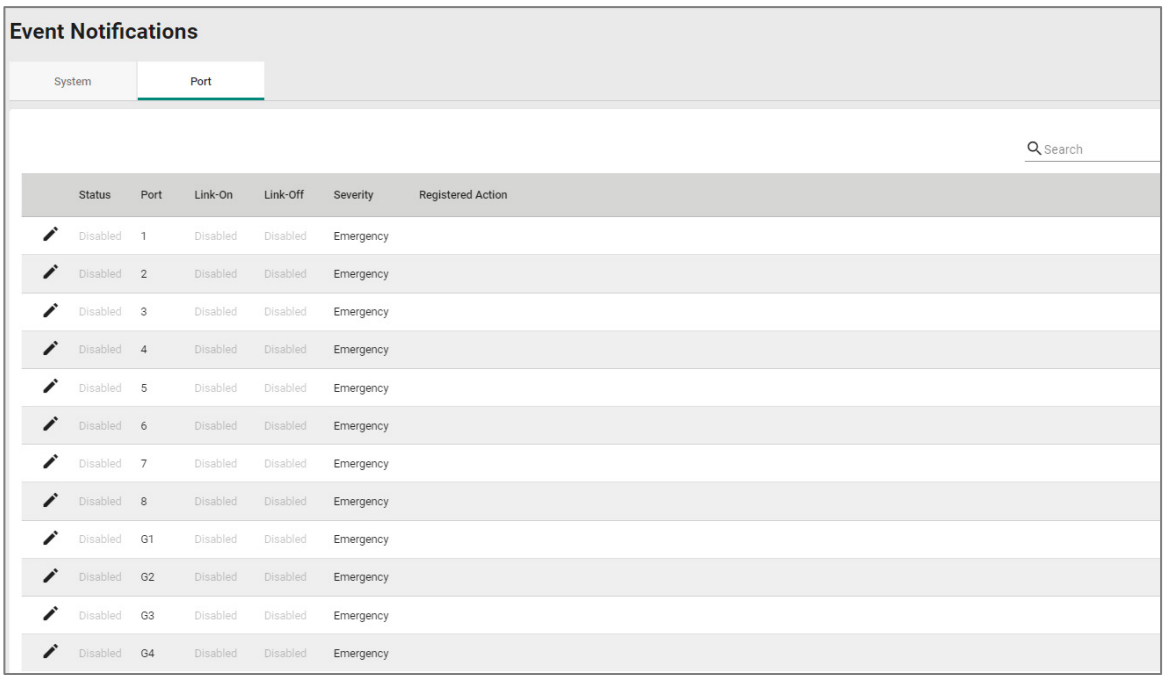
UI Setting	Description	Valid Range	Default Value
Event Name (View-only)	Shows the name of the event. Refer to the System Event List for more information.	(Fixed)	(Fixed)
Status	Enable or disable notifications for this event.	Enabled / Disabled	Disabled
Registered Action	Select which action to take when 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 the Severity Level List for more information about the different 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 port status. Each port can be configured independently with different warning methods and severity classifications.

When a port event is triggered, the FAULT LED/STATE LED on your device will also light up if your device has one.

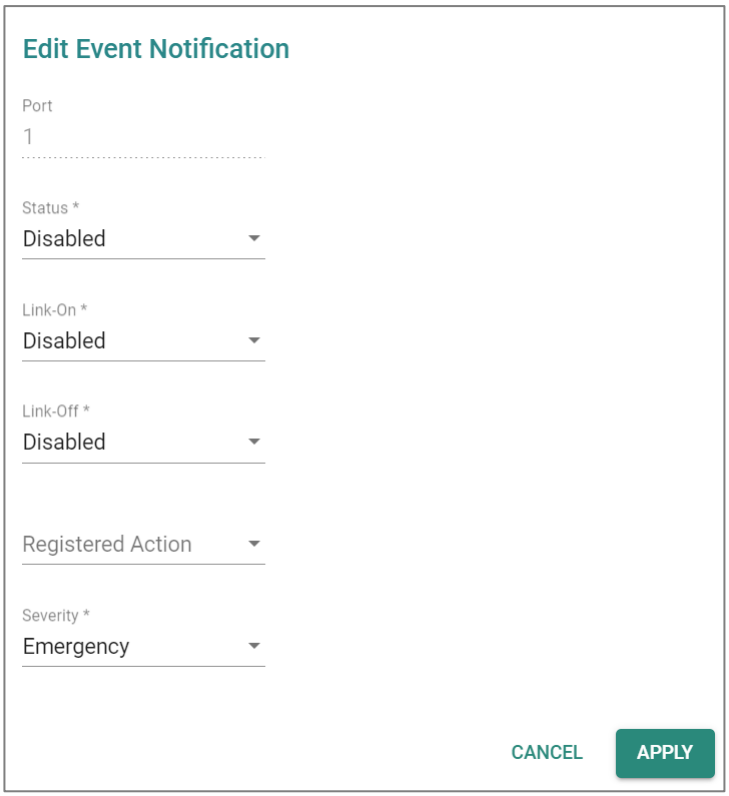


UI Setting	Description
Status	Shows whether event notifications are enabled for this kind of event.
Port	Shows which group this event belongs to.
Link-On	Shows whether notifications for Link-On events are enabled or disabled.
Link-Off	Shows whether notifications for Link-Off events are enabled or disabled.
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
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.



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

UI Setting	Description	Valid Range	Default Value
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
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 the Severity Level List for more information about the different severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency

Event Notifications - CPU Usage

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - CPU Usage

This page lets you configure notification settings based on CPU usage.

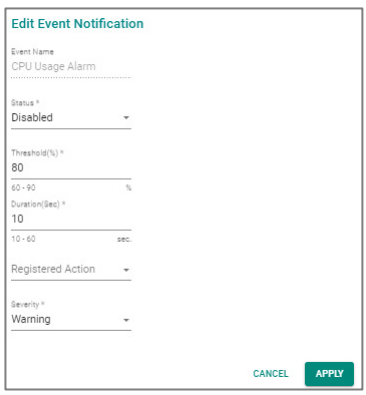
UI Setting	Description
Status	Shows whether event notifications are enabled for this kind of event.

UI Setting	Description
Event Name	Shows which group this event belongs to.
Threshold(%)	Shows the CPU usage threshold percentage that must be exceeded for event notifications.
Duration(Sec)	Shows the amount of time in seconds CPU usage must exceed the threshold to trigger a notification.
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
Registered Action	Shows how notifications will be sent for this kind of event.

Event Notifications - CPU Usage - Edit Event Notification

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - CPU Usage

Clicking the **Edit ( )** icon for an entry on the **Diagnostics > Event Logs and Notifications > Event Notifications - CPU Usage** page will open this dialog box. This dialog lets you change the notification settings for CPU usage. Click **APPLY** to save your changes.



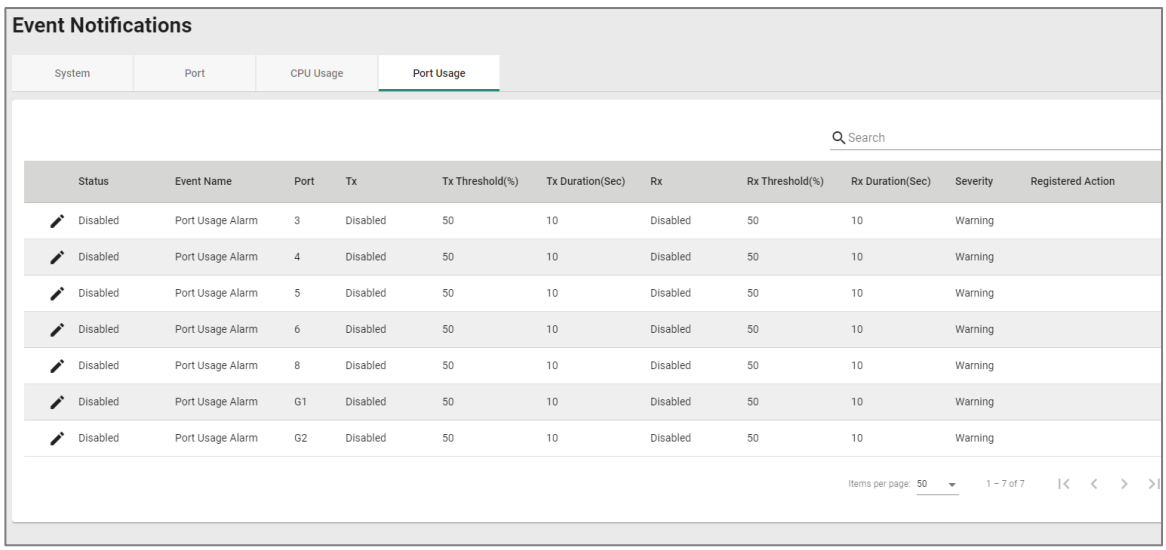
UI Setting	Description	Valid Range	Default Value
Event Name (View-only)	Shows the CPU usage event name.	N/A	N/A

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable event notifications for CPU usage.	Enabled / Disabled	Disabled
Threshold(%)	Shows the CPU usage threshold percentage that must be exceeded for event notifications.	60 to 90	80
Duration(Sec)	Shows the amount of time in seconds CPU usage must exceed the threshold to trigger a notification.	10 to 60	10
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.	Email / Syslog	N/A
Registered Action	Shows how notifications will be sent for this kind of event.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Warning

Event Notifications - Port Usage

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - Port Usage

This page lets you configure notification settings based on port usage. Each port can be configured independently with different warning methods and severity classifications.

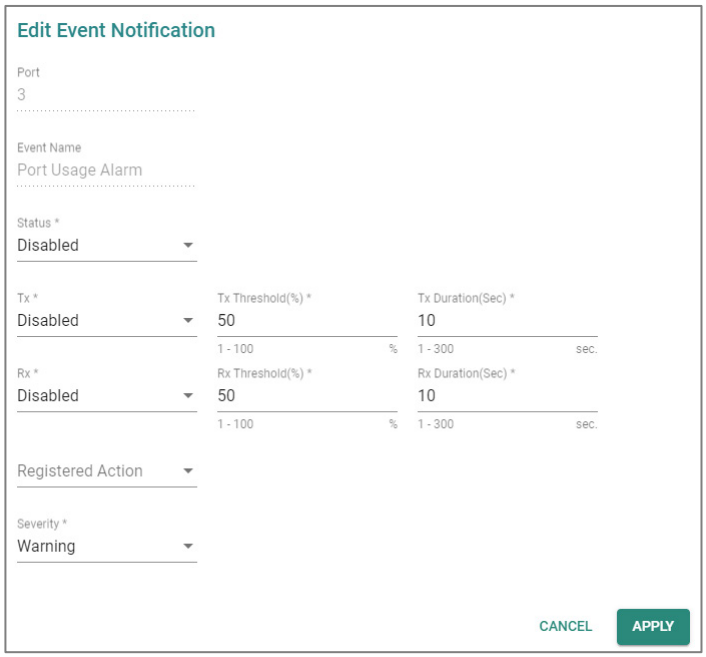


UI Settings	Description
Status	Shows whether event notifications are enabled for this kind of event.
Port	Shows which port this event belongs to. Available ports will vary depending on your product and model.
Tx	Shows whether Tx traffic is being monitored for event notifications.
Tx Threshold(%)	Shows the Tx threshold percentage that must be exceeded for event notifications.
Tx Duration	Shows the amount of time in seconds Tx traffic must exceed the Tx threshold to trigger a notification.
Rx	Shows whether Rx traffic is being monitored for event notifications.
Rx Threshold(%)	Shows the set Rx threshold percentage that must be exceeded for event notifications.
Rx Duration(Sec)	Shows the amount of time in seconds Rx traffic must exceed the Rx threshold to trigger a notification.
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
Registered Action	Shows how notifications will be sent for this kind of event.

Event Notifications - Port Usage - Edit Event Notification

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - Port Usage

Clicking the **Edit ( )** icon for an entry on the **Diagnostics > Event Logs and Notifications > Event Notifications - Port Usage** page will open this dialog box. This dialog lets you change the notification settings for the selected port. Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Port (View-only)	Shows which physical port the event notifications are for. Available ports will vary depending on your product and model.	N/A	N/A
Event Name (View-only)	Shows the event name.	N/A	N/A
Tx	Enable or disable Tx monitoring for event notifications.	Enabled / Disabled	Disabled
Tx Threshold(%)	Specify the Tx threshold percentage that must be exceeded for event notifications.	1 to 100	50
Tx Duration	Specify the amount of time in seconds Tx traffic must exceed the Tx threshold to trigger a notification.	1 to 300	10
Rx	Enable or disable Rx monitoring for event notifications.	Enabled / Disabled	Disabled
Rx Threshold(%)	Specify the Rx threshold percentage that must be exceeded for event notifications.	1 to 100	50

UI Setting	Description	Valid Range	Default Value
Rx Duration(Sec)	Specify the amount of time in seconds Rx traffic must exceed the Rx threshold to trigger a notification.	1 to 300	10
Registered Action	Select which action to take when the event occurs. Multiple actions may be selected. **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.	Email / Syslog	N/A
Severity	Select the severity to assign for this event. Refer to the Severity Level List for more information about the different severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Warning

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.

Note

To centralize data collection and potentially use it for forensic purposes in the future, we recommend that users deploy a syslog server in their environment and enable the syslog functionality on their devices to send logs to the remote server for storage. Additionally, we strongly recommend that these logs be properly stored on a syslog server for at least one year.

It is advised that the syslog server administrator utilize software or design automated processes for syslog management (including protection, collection, etc.).

For syslog management, it is essential to establish SOPs or any automated protection mechanisms to prevent authorized users from inadvertently deleting logs stored on the syslog server.

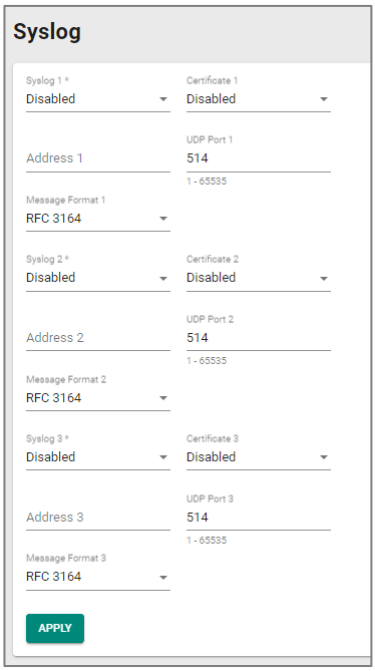
Note

In order to ensure the security of your network, we recommend the following:

- The encryption algorithm of keys should be selected based on internationally recognized and proven security practices and recommendations.
- The lifetime of certificates generated for syslog client services should be short and in accordance with the organization's security procedures and requirements.
- For security reasons, it is recommended to send event logs to a centralized syslog server for continuous network event monitoring.

Limitations

You can connect to up to 3 syslog servers.



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
Message Format	Select the message format of sysylog.	RFC 3164 / RFC 5424	RFC 3164

SNMP Trap/Inform

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform

This page lets you configure the SNMP Trap/Inform notification feature.

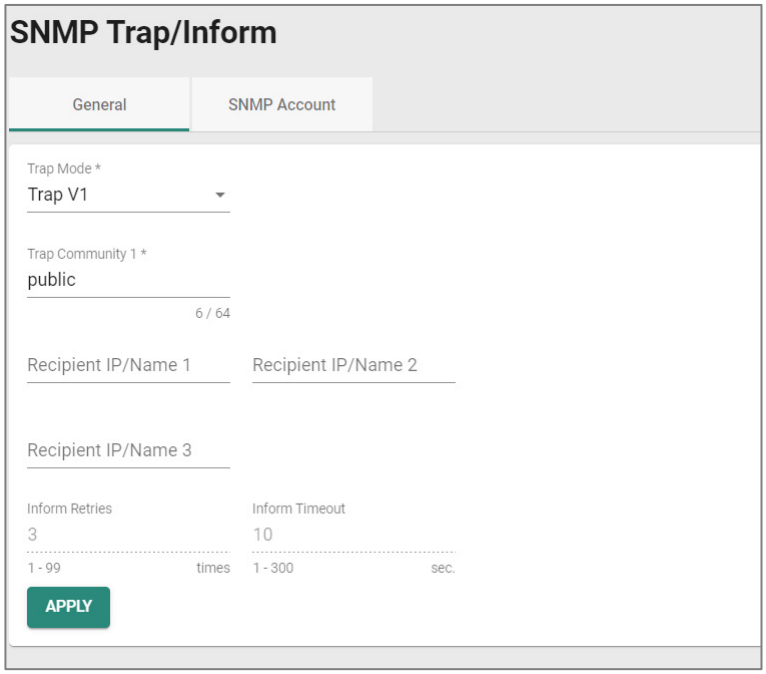
This page includes these tabs:

- 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.



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 64 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
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

UI Setting	Description	Valid Range	Default Value
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

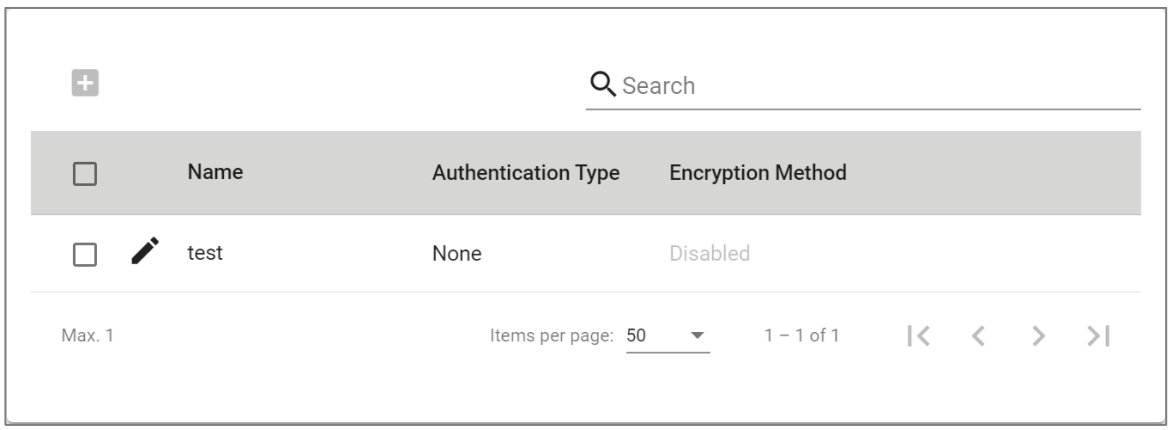
SNMP Account

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.

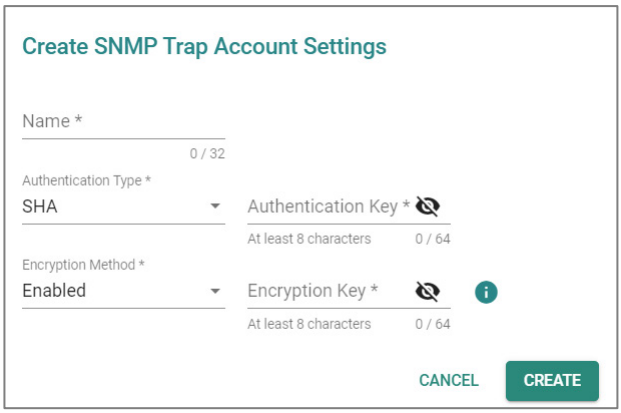


UI Setting	Description
Name	Shows the name of the SNMP trap account.
Authentication Type	Shows which authentication method is used for the account.
Encryption Method	Shows which encryption method is used for the account.

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.

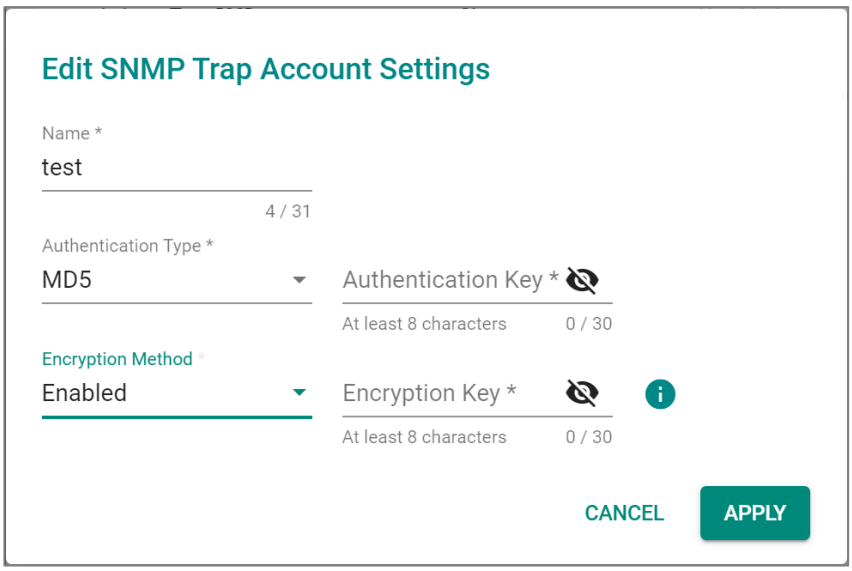


UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the account.	1 to 32 characters	N/A
Authentication Type	Select which authentication method to use for the account. **None**: No authentication will be used. **MD5**: Use MD5 authentication. **SHA**: Use SHA authentication.	None / MD5 / SHA	None
Authentication Key **(if Authentication Type is MD5 or SHA)**	Specify an authentication key to use for the account.	8 to 64 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 64 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.



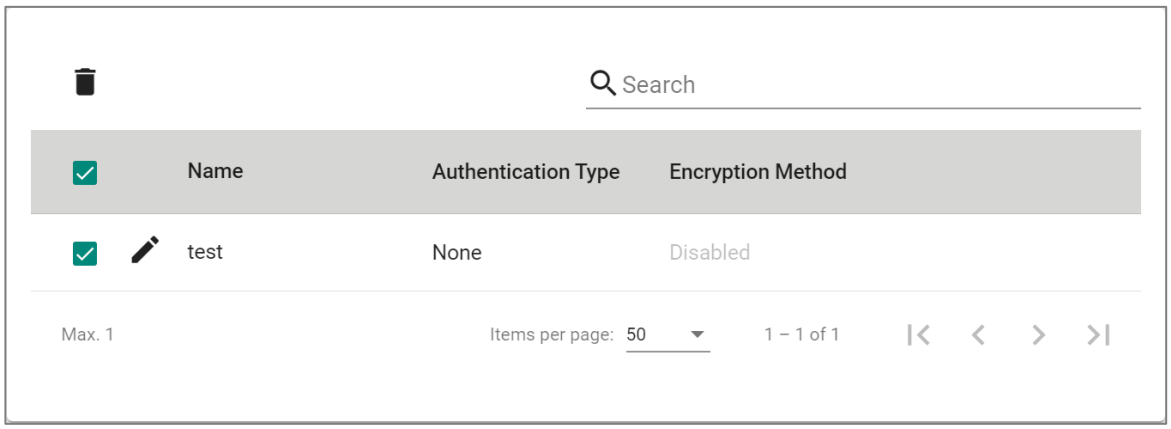
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the account.	1 to 32 characters	N/A
Authentication Type	Select which authentication method to use for the account. **None**: No authentication will be used. **MD5**: Use MD5 authentication. **SHA**: Use SHA authentication.	None / MD5 / SHA	None
Authentication Key **(if Authentication Type is MD5 or SHA)**	Specify an authentication key to use for the account.	8 to 64 characters	N/A
Encryption Method	Enable or disable AES encryption for the account.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Encryption Key **(if Encryption Method is Enabled)**	Specify an encryption password for the account.	8 to 64 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.



Email Settings

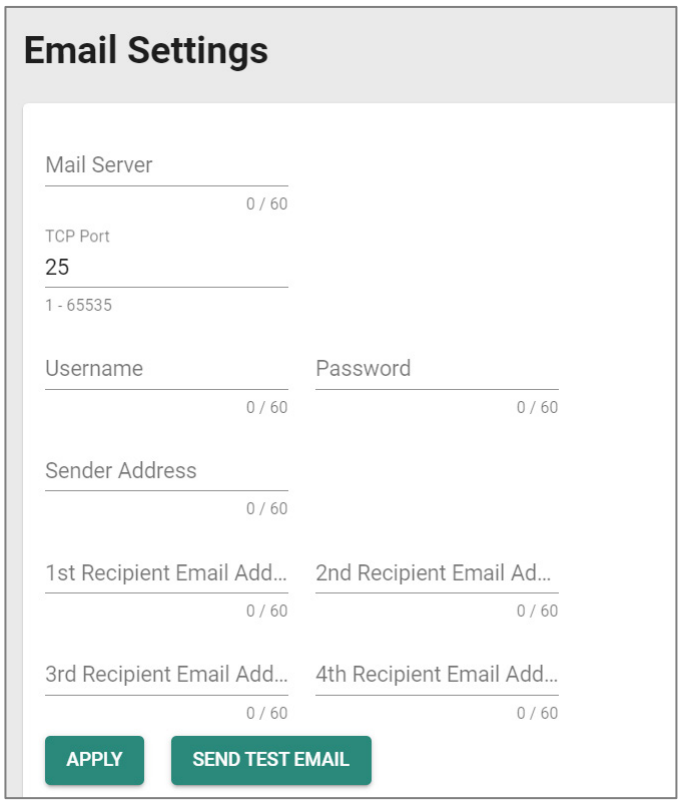
Menu Path: Diagnostics > Event Logs and Notifications > Email Settings

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.

Note

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.



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

UI Setting	Description	Valid Range	Default Value
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: Diagnostics > Tools

This section lets you use various tools to check for network issues.

This section includes these pages:

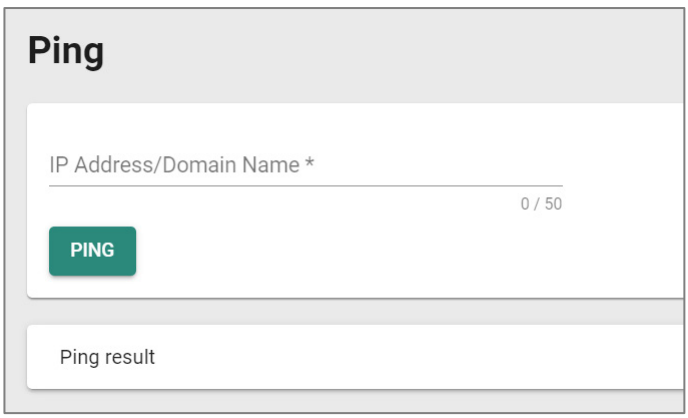
- Ping

Ping

Menu Path: 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.



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

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.

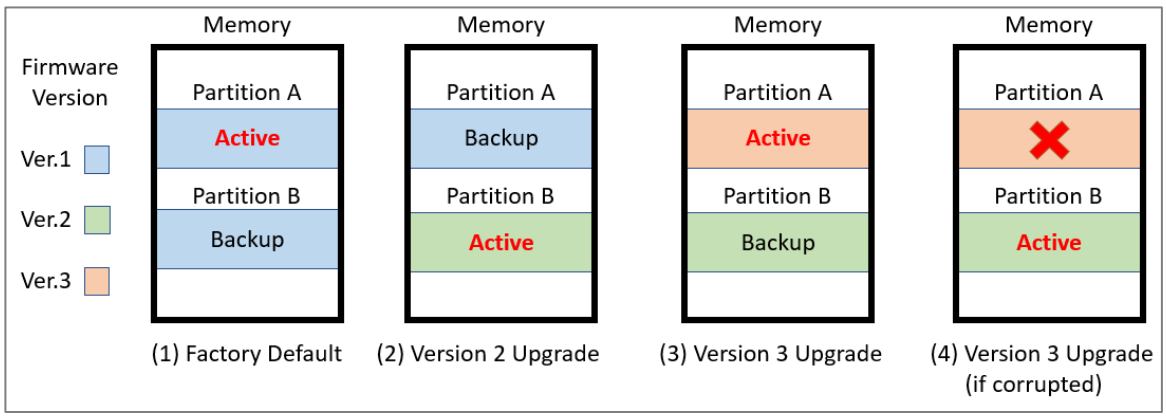
⚠ Warning

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

Device Applications

Device Applications Overview

This section goes over different device applications to help you better understand the applications themselves, and to show you how the device can help you implement those applications.

The following applications are covered:

- Network Segmentation
- Redundancy
- Routing
- OpenVPN Client
- NetFlow
- Loopback Interfaces

Network Segmentation

About Network Segmentation

Network Segmentation creates isolated virtual networks.

Segmenting a network reduces congestion and improves network performance by removing unnecessary traffic in a particular segment. For instance, segregating the passenger Wi-Fi network from the TCMS network in a train communication system ensures that the TCMS devices are not impacted by guest traffic. Such an approach helps to mitigate congestion and enhance the overall efficiency of the network.

There are two types of network segments:

- Layer-2 segments use numbered, virtual LAN segments (VLANs) to create isolated networks.
- Layer-3 segments use unique IP prefixes to create subnets.

Layer-2 Segments

A layer-2 segment is essentially a single broadcast domain. All devices connected to the segment will receive any broadcast traffic sent within it. Layer-2 segmentation uses numbered VLANs to create isolated logical segment, which allows for the separation of traffic between different VLANs.

Layer-3 Segments

In an IP network, a layer-3 segment is referred to as a subnetwork or subnet and includes all nodes that share the same network prefix as defined by their IP addresses and network mask. A router is needed to facilitate communication between layer-3 subnets. Hosts on the same subnet can communicate directly using the layer-2 segment that connects them.

VLANs in Depth

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

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

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

VLAN Standards and Implementation

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

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

Benefits of VLANs

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

VLANs help control traffic

With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether or not they need it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

VLANs simplify device relocation

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

VLANs provide extra security

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

Important

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

Scenario: Layer 2 Segmentation of 3 Factories

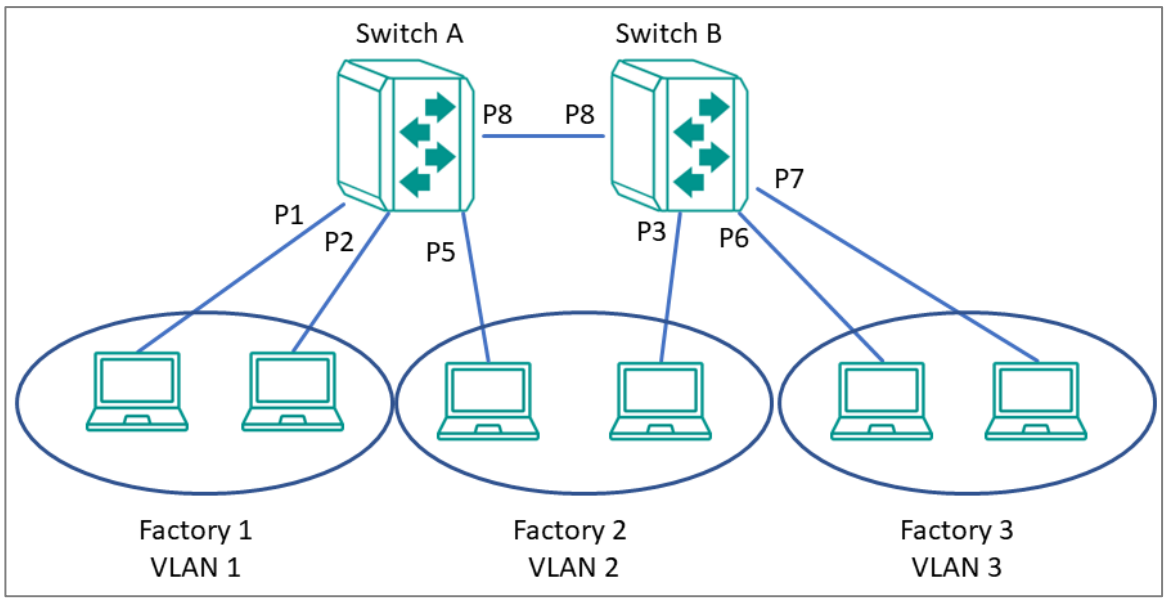
Short Description: A manufacturer uses layer 2 segmentation to manage traffic between three different factories, each with many devices.

Two switches are used to connect the all of the devices together on the same network, but devices from any factory may be connected to either switch. To simplify management and ensure smooth operations, we can configure the switches to make sure that each factory is on its own VLAN.

Each VLAN can be enlarged using simple switches to connect any number of devices in the factory

For our example scenario, we will simplify to two devices connected to each switch. Traffic VLANs are usually assigned to ports, so it's important to note which port we'll be using for each device. The switches are connected each other using port 8, and will allow VLANs to be split between the two switches as necessary, without causing interference or performance drops on the others.
We need a topology that:

- Allows devices on the same VLAN to communicate with each other
- Ensure devices on different VLANs cannot communicate with each other



This diagram outlines how we might create a network meeting these requirements. Each factory is on its own VLAN, and that Factory 2's VLAN is split between two switches. With VLAN segmentation and a Trunk connecting the two switches, Factory 2's VLAN will have comparable performance to VLANs within the same switch. Because of VLAN isolation, administrators can manage and prioritize traffic to ensure that packets do not leave their corresponding VLAN.

Important

Be careful when configuring VLANs on a remote switch. Modifications to the configuration could affect connectivity. For example, if the management VLAN of the switch is VLAN 1 and you are connected to ports that do not belong to VLAN 1, you may be disconnected from the switch during configuration.

Example: Creating VLANs for Layer 2 Segmentation of 3 Factories

Create VLANs in preparation for assigning them to ports.

Before you begin: Make sure you have an environment configured in line with our scenario. This includes:

- 3 routers in a ring topology with backbone connected on ports 7 and 8
- 2 gateways for each router (Service A and Service B), connected at ports 1 and 2, respectively
- Administrator credentials to all three routers

To create VLANs for this example, do the following:

1. Sign in to Switch A using administrator credentials.
2. Go to **Network Configuration→Layer 2 Switching→VLAN**.
3. To add a VLAN ID, click on the **Settings** tab, and then click the **Add ( )** button.
   Result: The **Create VLAN** screen appears.
4. Specify the VLAN to create in the VID, and then click Create. For Factory 1, we will create VLAN 1.
   Result: The VLAN will appear on the VLAN table at the top of the page.
5. Repeat this process to create VLANs 2 and 3 for the factories, and then create VLAN 1000 for the link between switches.

Results: We created VLANs for each factory (VIDs 1, 2, 3) and the VLAN for communication between switches (VID 1000).

What to do next: After you have created all 4 VLANs on Switch A, repeat this process on Switch B. Once Switch B is configured, you can continue on to assigning VLANs to ports.

Example: Assigning VLANs to Ports on Switch A

VLANs must be assigned to ports on Switch A to route traffic correctly.

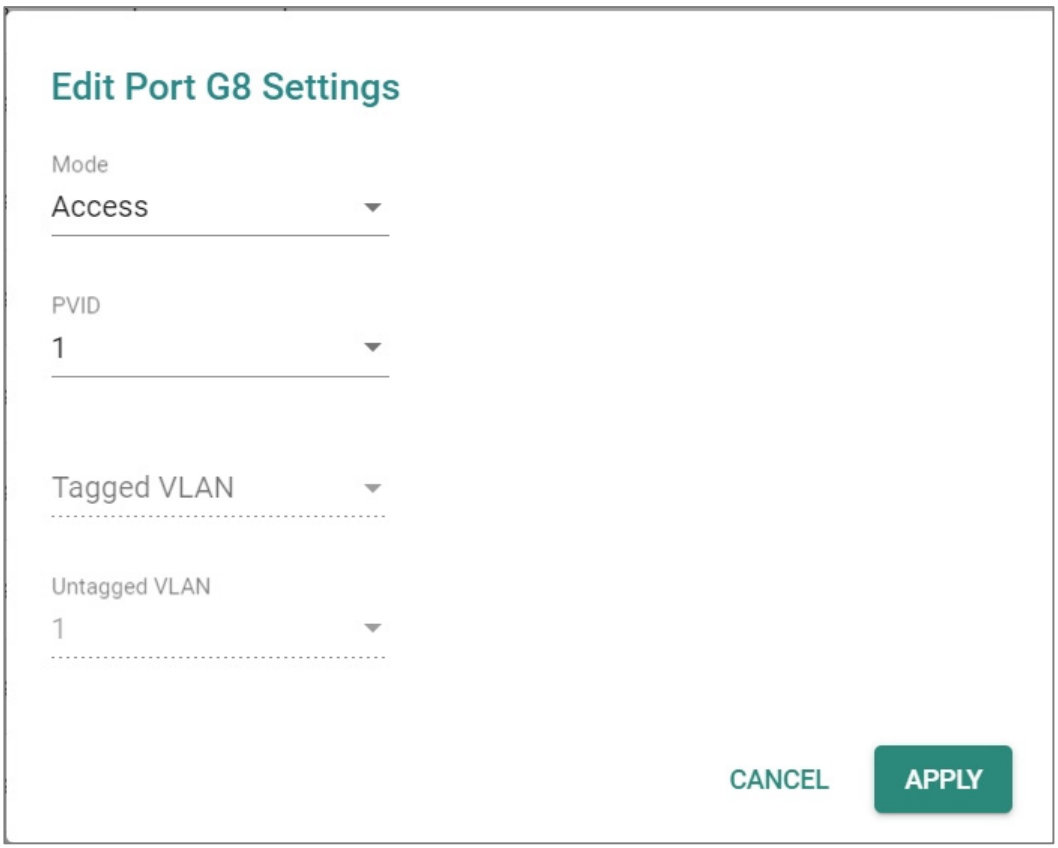
Now that you've created the VLANs, they need to be assigned to ports so that traffic from those ports will be routed over the correct VLAN. A similar procedure must be performed on each switch or router on the network.

1. Sign in to Switch A using administrator credentials.

2. Go to **Network Configuration→Layer 2 Switching→VLAN**.
3. To assign the newly created VLAN ID to a port, find the port on the **Port Table** on the lower part of the page, and the click the corresponding ***[Edit]*** button.

   Since we're assigning factory 1 to ports 1 and 2, start with **Port 1**. If you are repeating this step, you can substitute **Port 1** with information from the table at the end of this procedure.

   Result: The **Edit Port Settings** panel appears.



4. Specify the **Mode** and **PVID** that will be assigned to the port, and then click **Apply**.

   To assign the chosen port to Factory 1, specify **Mode Access** and **PVID** as 1.

Tutorial Info:

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

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

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

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

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

5. To add the remaining ports, repeat this procedure with the following substitutions and settings:

Port	Settings
2	• **PVID**: 1 • **Mode**: **Access Mode**
5	• **PVID**: 2 • **Mode**: **Access Mode**
8	• **PVID**: 1000 • **Mode**: **Trunk Mode** • **Tagged VLAN**: 1, 2, 3

Results: Ports on Switch A have been assigned VIDs and modes, ensuring that untagged traffic on ports 1 and 2 will automatically be tagged as VLAN 1. Traffic on port 5 will be automatically tagged as VLAN 2. Port 8 has been configured as a Trunk that will allow traffic to move between switches while retaining the tags.

What to do next: Assign VLANs to Ports on Switch B.

Important

The Port settings on each switch will be slightly different. Make sure each switch is configured correctly by following the instructions for Switch B.

Example: Assigning VLANs to Ports on Switch B

VLANs must be assigned to ports on Switch B to route traffic correctly.

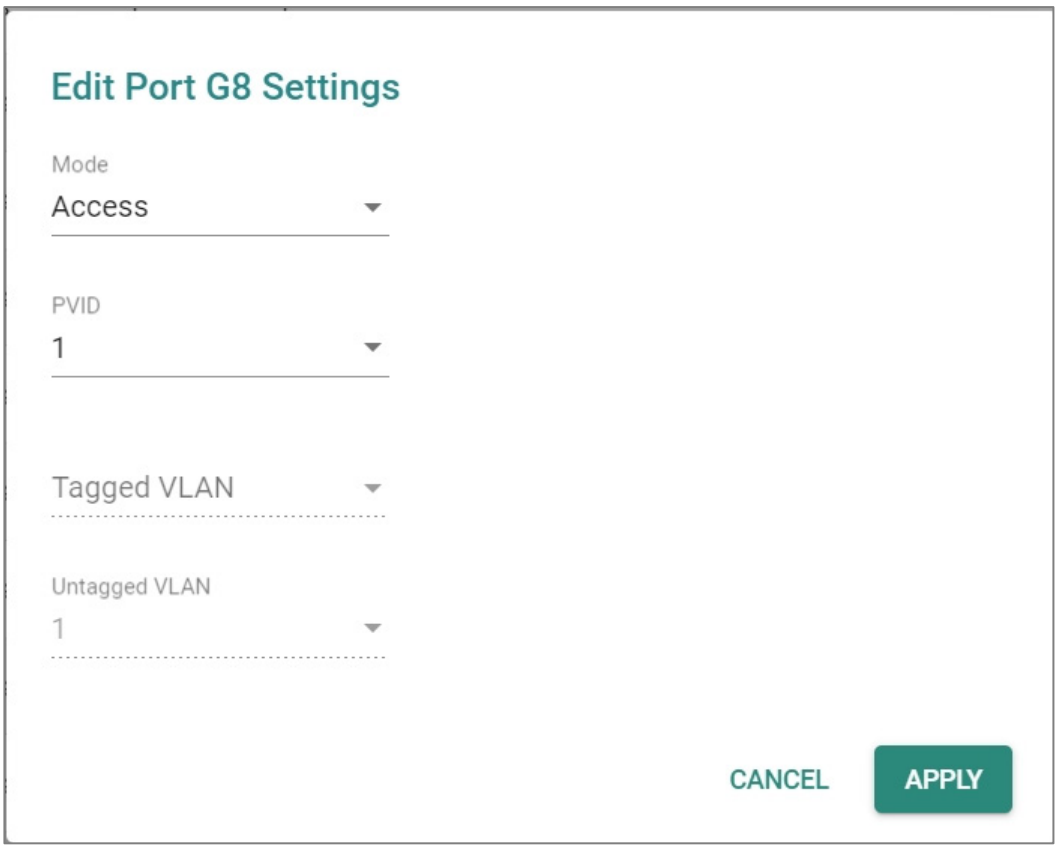
Now that you've created the VLANs, they need to be assigned to ports so that traffic from those ports will be routed over the correct VLAN. A similar procedure must be performed on each switch or router on the network.

1. Sign in to Switch A using administrator credentials.

2. Go to **Network Configuration→Layer 2 Switching→VLAN**.
3. To assign the newly created VLAN ID to a port, find the port on the **Port Table** on the lower part of the page, and the click the corresponding ***[Edit]*** button.

   Since we're assigning factory 2 to port 3, start with **Port 3**. If you are repeating this step, you can substitute **Port 3** with information from the table at the end of this procedure.

   Result: The **Edit Port Settings** panel appears.



4. Specify the **Mode** and **PVID** that will be assigned to the port, and then click **Apply**.

   To assign the chosen port to Factory 3, specify **Mode Access** and **PVID** as 2.

Tutorial Info:

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

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

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

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

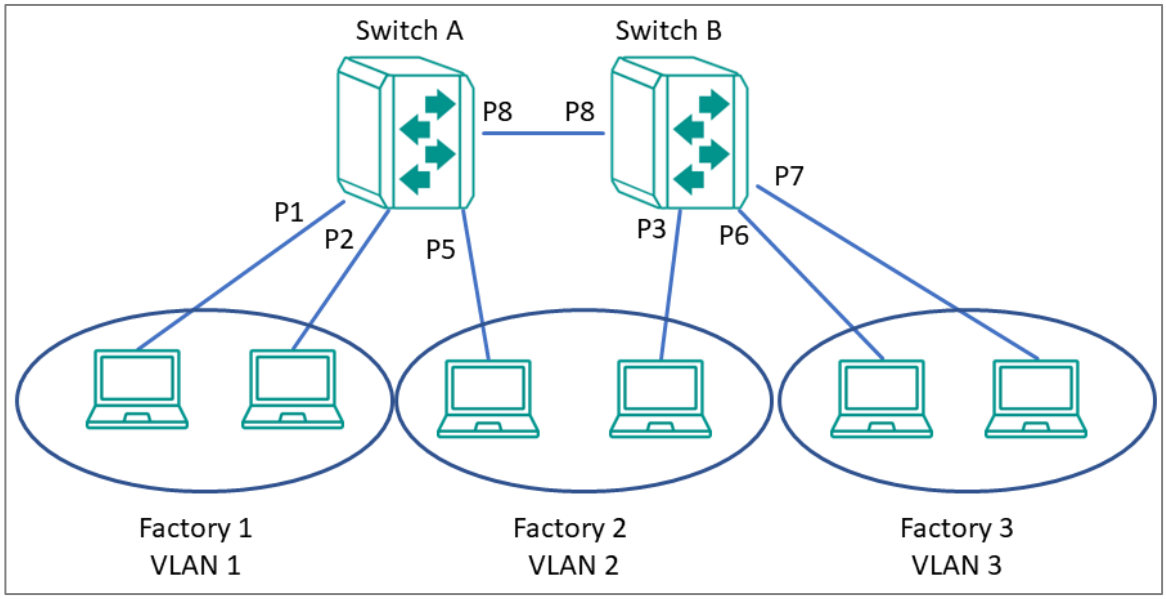
Result: The **Port Table** will show the new port configuration.

5. To add the remaining ports, repeat this procedure with the following substitutions and settings:

Port	Settings
6	• **PVID**: 1 • **Mode**: **Access Mode**
7	• **PVID**: 2 • **Mode**: **Access Mode**
8	• **PVID**: 1000 • **Mode**: **Trunk Mode** • **Tagged VLAN**: 1, 2, 3

Results: Ports on Switch B have been assigned VIDs and modes, ensuring that untagged traffic on ports 6 and 7 will automatically be tagged as VLAN 3. Traffic on port 3 will be automatically tagged as VLAN 2. Port 8 has been configured as a Trunk that will allow traffic to move between switches while retaining the tags.

When combined with the previous settings, we complete the network segmentation. Traffic on VLANs 1-3 will remain isolated, and VLAN 1000 will allow traffic between switches while retaining VLAN tagging.



Scenario: Layer 3 Segmentation of Two Services

Short Description: A manufacturer uses layer 3 segmentation to manage traffic between three different factories, each with many devices.

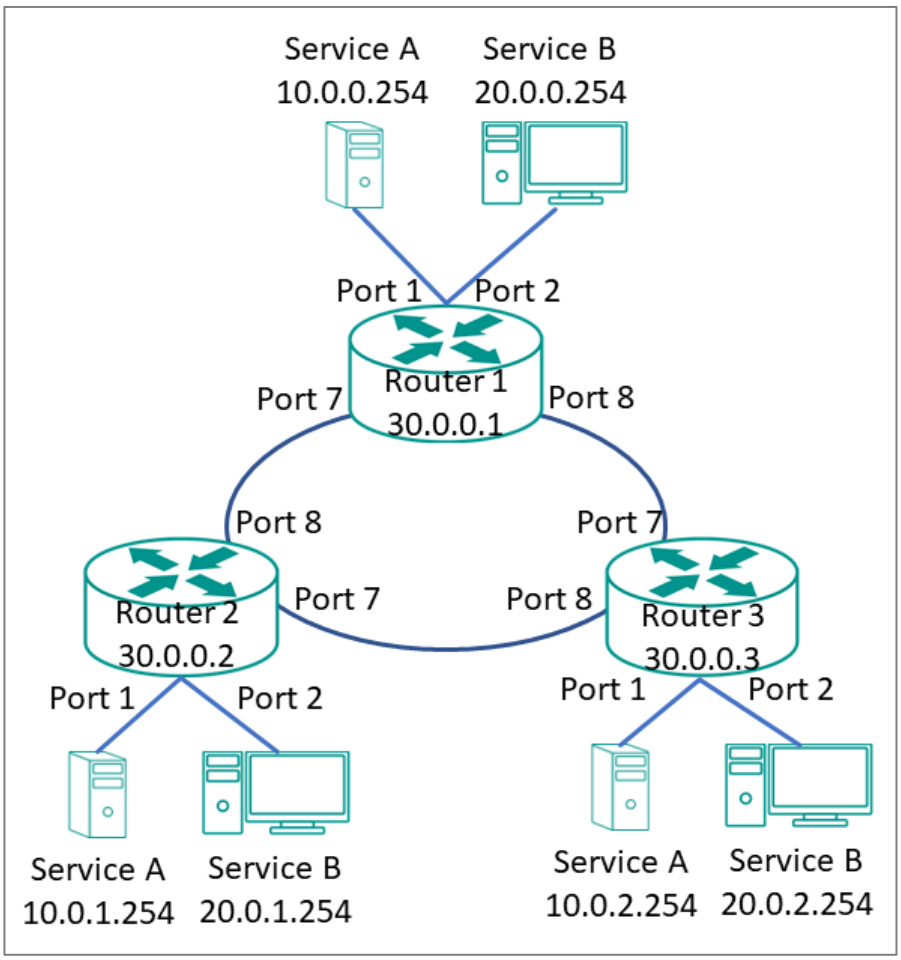
Three routers are used to connect the all of the devices together on the same network, but devices from any factory may be connected to either switch. Each factory has devices running Service A and Service B. Devices need to connect to the corresponding service in other factories, while being isolated from the different services in their own factories.

Each VLAN can be enlarged using simple switches to connect any number of devices in the factory.

For our example scenario, we will simplify to two devices (one for each service) connected to each router. These devices will serve as gateways for additional devices connected to their corresponding service. We can assign separate subnets to each port (an interface), so it's important to note which port we'll be using for each device.

We need a topology that:

- Allows devices on the same subnet to communicate with each other
- Ensure devices on different subnet cannot communicate with each other



This diagram outlines how we might create a network meeting these requirements. Each service is on its own subnet. Routers are connected in a ring topology, also on its own subnet. Because of subnet isolation, administrators can manage and prioritize traffic to ensure that packets do not leave their corresponding subnet.

To deploy this topology we need to do the following:

- Configure VLANs for each interface and bind them to ports
- Configure IP ranges for each interface and assign them to ports

In our example, we are segmenting by Service, rather than by area.

Example: Creating VLANs for Layer 3 Segmentation

Create VLANs in preparation for assigning them to ports.

Before you begin: Make sure you have an environment configured in line with our scenario. This includes:

- 3 routers in a ring topology with backbone connected on ports 7 and 8
- 2 gateways for each router (Service A and Service B), connected at ports 1 and 2, respectively
- Administrator credentials to all three routers

To create VLANs for this example, do the following:

1. Sign in to Switch A using administrator credentials.
2. Go to **Network Configuration→Layer 2 Switching→VLAN**.
3. To add a VLAN ID, click on the **Settings** tab, and then click the ***[Add]*** button.

   Result: The **Create VLAN** screen appears.
4. Specify the VLAN to create in the **VID**, and then click **Create**. For Service A, we will create VLAN `10`.
   Result: The VLAN will appear on the VLAN table at the top of the page.
5. Repeat this process to create VLAN `20` for Service B, and then create VLAN `1000` for the link between switches.

Results: We created VLANs for each Service (VIDs 10 and 20) and the VLAN for backbone between different sites (VID `1000`).

What to do next: After you have created all 3 VLANs on Router 1, repeat this process on Routers 2 and 3. The configuration options will be the same. Once VLANs have been configured on all routers, you can move on to assigning VLANs to ports.

Example: Assigning VLANs to Ports for Layer 3 Segmentation

VLANs must be assigned to ports on each router to route traffic correctly.

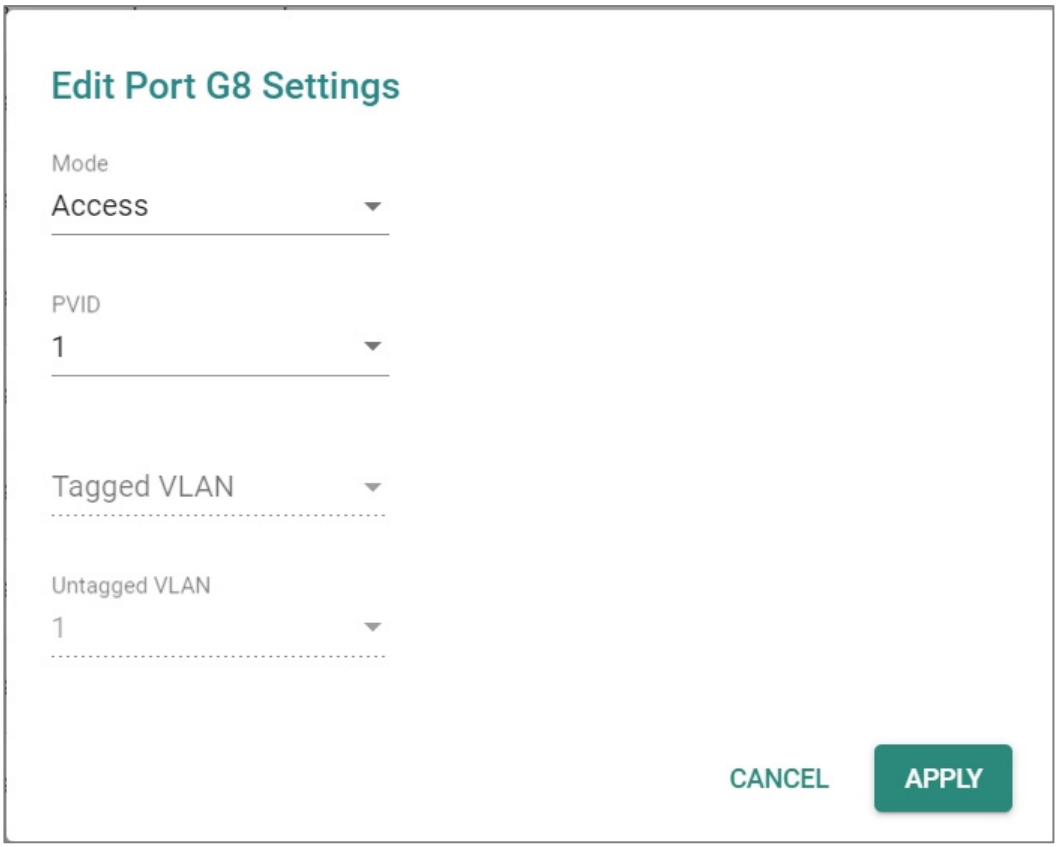
Now that you've created the VLANs, they need to be assigned to ports so that traffic from those ports will be routed over the correct VLAN. A similar procedure must be performed on each switch or router on the network.

1. Sign in to Router 1 using administrator credentials.
2. Go to **Network Configuration→Layer 2 Switching→VLAN**.

3. To assign the newly created VLAN ID to a port, find the port on the **Port Table** on the lower part of the page, and the click the corresponding ***[Edit]*** button.

   Since we're assigning Service A to port 1, start with **Port 1**. If you are repeating this step, you can substitute **Port 1** with information from the table at the end of this procedure.

   Result: The **Edit Port Settings** panel appears.



4. Specify the **Mode** and **PVID** that will be assigned to the port, and then click **Apply**.

   To assign the chosen port to Service A, specify **Mode Access** and **PVID** as `10`.

Tutorial Info:

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

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

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

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

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

5. To add the remaining ports, repeat this procedure with the following substitutions and settings:

Port	Settings
2	• **PVID**: 10 • **Mode**: **Access Mode**
5	• **PVID**: 20 • **Mode**: **Access Mode**
7	• **PVID**: 1000 • **Mode**: **Trunk Mode** • **Tagged VLAN**: 10, 20
8	• **PVID**: 1000 • **Mode**: **Trunk Mode** • **Tagged VLAN**: 10, 20

Results: Ports on Router 1 have been assigned VIDs and modes, ensuring that untagged traffic on Port 1 will automatically be tagged as VLAN 10. Traffic on port 2 will be automatically tagged as VLAN 20. Port 8 has been configured as a Trunk that will allow traffic to move between switches while retaining the tags.

Example: Assigning IPs to Router Interfaces

IP subnets must be assigned to interfaces to ensure traffic from corresponding VLANs is segmented correctly.

To assign IPs to router interfaces:

1. Sign in to Router 1 using administrator credentials.

2. Go to **Network Configuration→Network Interfaces→LAN**, and then press  ***[Add]***.
   Result: The **Create LAN Interface Entry** screen appears.
3. To add the interface for Service A, specify all of the following, and then click **Create**:

Field	Setting
Name	`Service A`
VLAN ID	`10`
IP Address	`10.0.1.254`
Netmask	**8 (255.0.0.0)**

Result: The LAN interface will appear on the Network Interface list.

4. To add the interface for Service B, specify all of the following, and then click **Create**:

Field	Setting
Name	`Service B`
VLAN ID	`20`
IP Address	`20.0.1.254`
Netmask	**8 (255.0.0.0)**

Result: The LAN interface will appear on the Network Interface list.

5. To add the interface for the backbone connection, specify all of the following, and then click **Create**:

Field	Setting
Name	`Backbone`
VLAN ID	`1000`

Field	Setting
IP Address	30.0.0.1
Netmask	**8 (255.0.0.0)**

Result: The LAN interface will appear on the Network Interface list.

Results: Interfaces have been configured on Router 1 to allow effective network segmentation. Now you need to configure the additional networks.

What to do next: Repeat this task with the following adjustments:

Router	Item	Value
Router 2	Service A	10.0.2.254
	Service B	20.0.2.254
	Backbone	30.0.0.2
Router 3	Service A	10.0.3.254
	Service B	20.0.3.254
	Backbone	30.0.0.3

Once all routers have been configured with the correct IP interfaces, you can configure a routing solution. Once that's done, your network will be ready to use.

Example: Configuring Static Routing for Layer 3 Segmentation

For complex environments, routing must be configured.

This example uses simple static routing to route traffic across the network. A production network may chose a dynamic routing option instead.

To configure dynamic routing for the Layer 3 example:

1. Sign in to Switch A using administrator credentials.
2. Go to **Routing→Unicast Route→Static Routes**, and then click the **Add (** **)** icon.

Result: The **Create new static route** panel appears.

3. Specify all of the following:

Item	Value
Name	Serivce A Router 2
Status	**Enable**
Destination Address	**10.0.1.254** Refers to Production Service A on Router 2.
Subnet Mask	**8 (255.0.0.0)** Refers to the subnet mask of the destination address.
Next Hop	`30.0.0.2` Refers to the Router 2 Interface as the next hop on the network.
Metric	1

4. Click **Create**.

Result: The new static routing entry should appear in the routing table.

5. Repeat this process for Service B. Specify all of the following:

Item	Value
Name	**Service B Router 2**
Status	**Enable**
Destination Address	**20.0.1.254** Refers to Production Service A on Router 2.
Subnet Mask	**8 (255.0.0.0)** Refers to the subnet mask of the destination address.
Next Hop	`30.0.0.2` Refers to the Router 2 Interface as the next hop on the network.
Metric	**1**

6. Once this step is complete, repeat the process on Routers 2 and 3. The information for each router should appear as follows:

Item	Service A Router 1	Service B Router 1	Service A Router 2	Service B Router 2	Service A Router 3	Service B Router 3
Appears On	Routers 2/3	Routers 2/3	Routers 1/3	Routers 1/3	Routers 1/2	Routers 1/2
Name	Service A Router 1	Service B Router 1	Service A Router 2	Service B Router 2	Service A Router 3	Service B Router 3
Status	**Enable**	**Enable**	**Enable**	**Enable**	**Enable**	**Enable**
Destination Address	10.0.0.254	20.0.0.254	10.0.0.254	20.0.1.254	10.0.0.254	20.0.2.254
Subnet Mask	**8 (255.0.0.0)**	**8 (255.0.0.0)**	**8 (255.0.0.0)**	**8 (255.0.0.0)**	**8 (255.0.0.0)**	**8 (255.0.0.0)**
Next Hop	30.0.0.1	30.0.0.1	30.0.0.2	30.0.0.2	30.0.0.3	30.0.0.3
Metric	1	1	1	1	1	1

Results: Once the routing configuration is completed, the Example Layer 3 Segmented Network will be ready to use. This will ensure that packets for each service will be isolated from the other, while still be efficiently guided around the network.

Routing

About Routing

IP routing is the process of forwarding Internet Protocol (IP) traffic between different networks using one or more intermediate devices.

When one device wants to send a packet to another on a different network, it forwards the packet to its default gateway—usually a router. The router examines the destination IP address and determines the next "hop" along the path to the destination. This process continues with subsequent routers until the packet reaches its destination. Each router along the path checks its own routing table to determine the best path for the packet. Routing tables contain information about network topology and a list of networks and associated routes. Each route correlates information by destination IP or IP range, and includes information such as the next-hop router and the cost of sending packets along that route.

Static routing and **dynamic routing** are two methods of populating the routing table with information about how to reach different networks.

Static routing is manually-configured. Network administrators configure the routing table on each router. This method is simple to configure and allows packets to take predictable paths as long as network topology does not change.

Dynamic routing protocols automatically update the routing table on each router. This method is more flexible and scalable, making it suitable for larger and more complex networks.

In addition to how routes are configured, packets can be routed between a single sender and single recipient (**unicast**), or from one sender to multiple devices at a time (**multicast**).

Unicast delivery is used to send packets from one sender to one recipient, as is typically the case with most network traffic. When a device sends a packet with an unicast destination address, the router looks up the destination address in its routing table and forwards the packet to the next hop on the path to the destination.

Multicast delivery, on the other hand, is used to send packets from one sender to many recipients. With multicast, a single packet is sent out to a group of devices on the

network that have expressed interest in receiving packets for that group. This is useful for applications such as video streaming, where the same content needs to be sent to multiple devices simultaneously. Dynamic multicast routing protocols, such as Protocol Independent Multicast (**PIM**), are used to ensure that multicast packets are delivered only to devices that have expressed interest in receiving them.

Routing and Packet Delivery

	Unicast	Multicast
Static	Manual Configuration	Manual Configuration
Dynamic	• **RIP** • **OSPF**	**PIM**

Note

The TN-4908 series currently only supports static multicast routes in multicast stream routing.

About Static Routing

A static route is a manually configured network path used to deliver network traffic to a specific destination network or host. Unlike dynamic routes established by routing protocols, static routes are created and managed by a network administrator. They are typically used in small networks or situations where there is a limited number of destinations that need to be reached.

Among these static routes, a special type known as the default route, or 'gateway of last resort', plays a critical role. This default route, often designated as 0.0.0.0/0, represents a catch-all path. When a device doesn't have a specific route for a packet's destination IP address, it will utilize the default route, sending the data along this path. This ensures that all data, regardless of its destination, has a route to follow.

While both default and static routes are manually configured, they serve different purposes. Static routes are used for specific, predefined network paths, while the default route is a catch-all, used when no other path is available for a specific data packet. This allows for increased control over network traffic while ensuring that data can reach otherwise unspecified networks, typically including the public Internet.

Static routes, including default routes, offer several advantages, including:

- More control over network traffic, allowing administrators to direct traffic along specific paths.
- Less overhead and resource usage, as static routes don't require routers to exchange routing information.
- Faster convergence, since there are no routing updates to process.

However, static routes also have some disadvantages:

- May be time-consuming and prone to human error, as administrators must manually configure and update routes.
- Unable to adapt to network changes automatically, requiring manual intervention to update routing tables when network topology changes.
- May not scale well in large networks with numerous destinations and frequent changes.

In summary, static routing is a method for unicast communication in which network paths are manually configured by network administrators. While they offer more control over network traffic and can improve performance in some cases, static routes can be time-consuming to manage and may not be well-suited for large, dynamic networks.

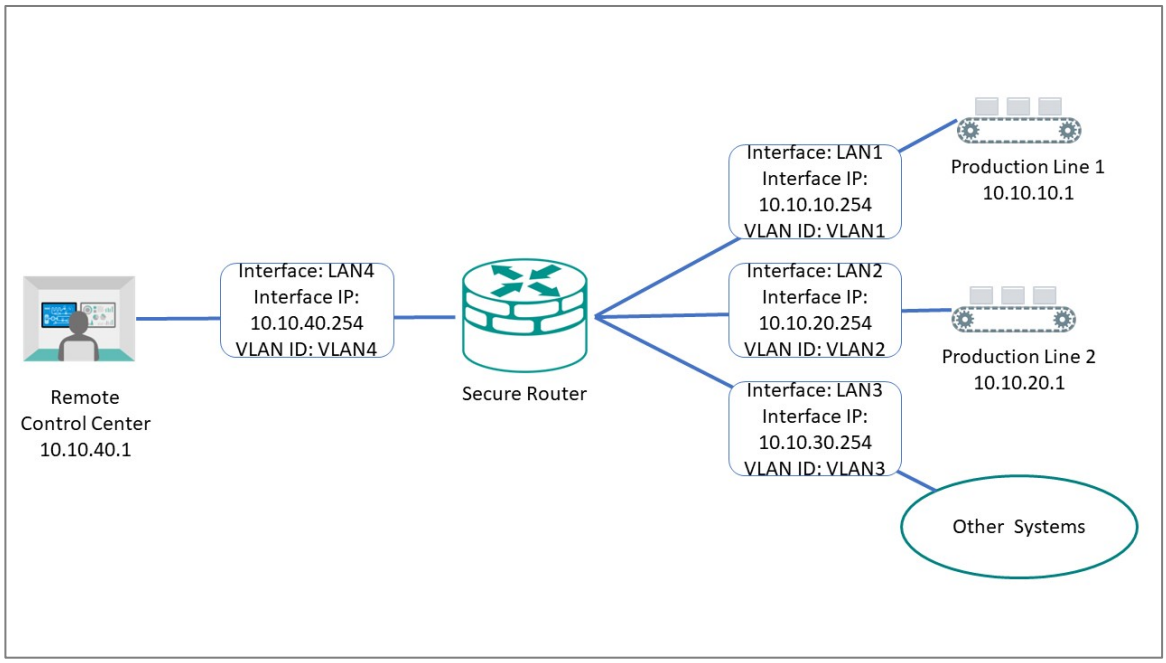
Example: Adding a Static Unicast Route for Factory Automation

A factory operator wants to create static routes between two production lines to coordinate handoffs in a multistage manufacturing process. Static routes allow packets to traverse different subnets, and will ensure efficient routing of packets between the two production lines, as well as to the central control center. This also improves performance by reducing network congestion, ensuring that packets will not be retransmitted to other devices or other subnets.

Before you begin: Make sure you have correctly configured:

- Each device with an IP address.
- VLANs for each subnet. Refer to VLAN for more information.

- VLAN assignment to an Interface. Refer to Network Interfaces for more information.



To create a static route to Production Line 1, do the following:

1. Go to **Routing→Unicast Route→Static Routes**, and then click ***[Add]***.

   Result: The **Create new static route** panel appears.

2. Specify all of the following:

Item	Value
Name	Specify a name for the route. Names must not exceed 10 characters. Names are for user reference only and do not affect functionality.
Status	**Enable**
Destination Address	`10.10.10.1` Refers to Production Line 1.
Subnet Mask	**24(255.255.255.0)** Refers to the subnet mask of the destination address.
Next Hop	`10.10.10.254` Refers to the Secure Router LAN1 Interface as the next hop on the network.

Item	Value
Metric	1 Indicates the preference or priority of a particular route, with lower values having higher priority. When multiple static routes are available (or both static and dynamic routing protocols are available), the router uses the **Metric** value to determine the best route to use. For static routes, a value of 1 is recommended.

Note

The Destination Address and Subnet Mask identify which traffic forwards to the next hop. For multi-hop entries, the Subnet Mask will correspond to the Destination Address and not the Next Hop.

3. Click **Create**.

Result: The new static routing entry should appear in the routing table.

Results:

Packets meeting the destination criteria will be routed to the appropriate interface and applicable subnet, and will not be propagated further.

What to do next: Repeat this procedure to add Production Line 2 (`10.10.20.1`), the Remote Control Center (`10.10.40.1`), and Other Systems (`10.10.30.1`) to the Static Routing Table.

About NAT

Network Address Translation (NAT) is a networking technique that allows multiple devices on a private network to share a single public IP address for accessing external networks, such as the internet.NAT is widely used to conserve IPv4 addresses, improve security, and provide flexibility in network design.

NAT in Depth

NAT has two main mechanisms:

1. **IP Address Translation:**
    - NAT operates on a router or gateway, translating private IP addresses (e.g., 192.168.x.x, 10.x.x.x) to a single public IP address for outbound traffic.
    - Inbound traffic addressed to the public IP is translated back to the corresponding private IP.
2. **Mapping Mechanism**:
    - NAT maintains a **translation table** that maps private IP addresses and ports to public IP addresses and ports.
    - When an internal device initiates a connection, NAT creates an entry in this table to track the session.

Types of NAT

1. **NAT 1-1**:
    - A one-to-one mapping between private and public IP addresses.
    - Commonly used for devices that require a consistent public IP, such as web servers.
2. **NAT N-1**:
    - Maps private IP addresses to a pool of public IP addresses on a first-come, first-served basis.

- Useful when there are fewer public IPs than private devices.

3. **Port Forwarding**:
    - Maps multiple private IP addresses to a single public IP by using different port numbers.
    - This is the most common NAT implementation in residential and small-business networks.

NAT Advantages

1. **Conservation of IPv4 Addresses**:
    - Reduces the need for unique public IPs for each device in a private network.
2. **Improved Security**:
    - Hides internal network structure, making it harder for attackers to directly access private devices.
3. **Simplified IP Management**:
    - Allows the use of private IPs internally, avoiding conflicts with public IP address space.
4. **Flexibility in Addressing**:
    - Facilitates network merging or renumbering without requiring changes to the internal IP schema.

Scenario: NAT for Renewable Power Generators

A renewable energy company specializes in manufacturing tidal power generators. Each generator comes pre-installed with a set of monitoring and control devices (e.g., sensors, PLCs, and communication modules) that have identical configurations, including static IP addresses, to simplify the manufacturing process. For instance, every generator's internal devices use the same private IP scheme (e.g., 192.168.100.x).

When these generators are deployed at a tidal power farm, they are connected to a shared local network. However:

This system has the following risks:

1. IP Address Conflicts:
    - The identical IP configurations of the internal devices create conflicts when multiple generators are connected to the same network.
2. High Manual Configuration Effort:
    - Manually reconfiguring each generator's devices to assign unique IPs would be time-consuming and prone to error, especially when dealing with dozens or hundreds of generators.
3. Centralized Monitoring:
    - The company’s energy management system relies on an Endpoint Detection and Response (EDR) platform to monitor and manage the networked devices. The EDR must differentiate devices across generators without altering their default configurations.

In this scenario, NAT 1-to-1 mapping can be deployed at each generator.

This approach allows the company to map the internal, identical IP ranges of each generator to unique IP ranges or subnets on the shared local network, without altering the original configurations.

See the following sections for guidelines for configuring this scenario.

Example: Configuring 1-to-1 NAT for Device Management

You can add manual network address translation to accommodate fixed IPs on devices.

Make sure that IP interfaces have been assigned.

1. Sign in to the device with administrator credentials.
2. Go to **NAT**, and then click ***[Add]***.

   The Create Index screen appears.
3. Configuring the First Device on Generator 1.
4. To add the inbound NAT rule for the first generator, specify all of the following, and then click **Apply**:

Option	Value
Mode	**1-to-1**
Original Packet (Condition) - Incoming Interface	**WAN**
Original Packet (Condition) - Destination IP	`10.10.0.1`
Translated Packet (Action) - Destination IP	`192.168.100.1`

The Index appears on the table.

5. Click ***[Add]***.
6. To add the outbound NAT rule for the first generator, specify all of the following, and then click **Apply**:

Option	Value
Mode	**1-to-1**
Original Packet (Condition) - Incoming Interface	**LAN**
Original Packet (Condition) - Destination IP	`192.168.100.1`
Translated Packet (Action) - Destination IP	`10.10.0.1`

The Index appears on the table.

The network device will translate between 10.10.0.1 on WAN and 192.168.100.1 without the needing to adjust the settings of the sender or the recipient, or even having them be aware that they have cross a network boundary.

To configure additional devices in this scenario, repeat the above procedure with the following differences:

Options	Generator 1				Generator 2					
	Device 2		Device 3		Device 1		Device 2		Device 3	
	Inbound Rule	Outbound Rule	Inbound Rule	Outbound Rule	Inbound Rule	Outbound Rule	Inbound Rule	Outbound Rule	Inbound Rule	Outbound Rule
Original Packet (Condition) - Incoming Interface	WAN	LAN	WAN	LAN	WAN	LAN	WAN	LAN	WAN	LAN
Original Packet (Condition) - Destination IP	10.10.0.2	192.168.100.2	10.10.0.3	192.168.100.3	10.10.0.4	192.168.100.1	10.10.0.5	192.168.100.2	10.10.0.6	192.168.100.3
Translated Packet (Action) - Destination IP	192.168.100.2	10.10.0.2	192.168.100.3	10.10.0.3	192.168.100.1	10.10.0.4	192.168.100.2	10.10.0.5	192.168.100.3	10.10.0.6

Scenario: Isolated Product Network with Limited Internet Access (NAT N-to-1)

Note

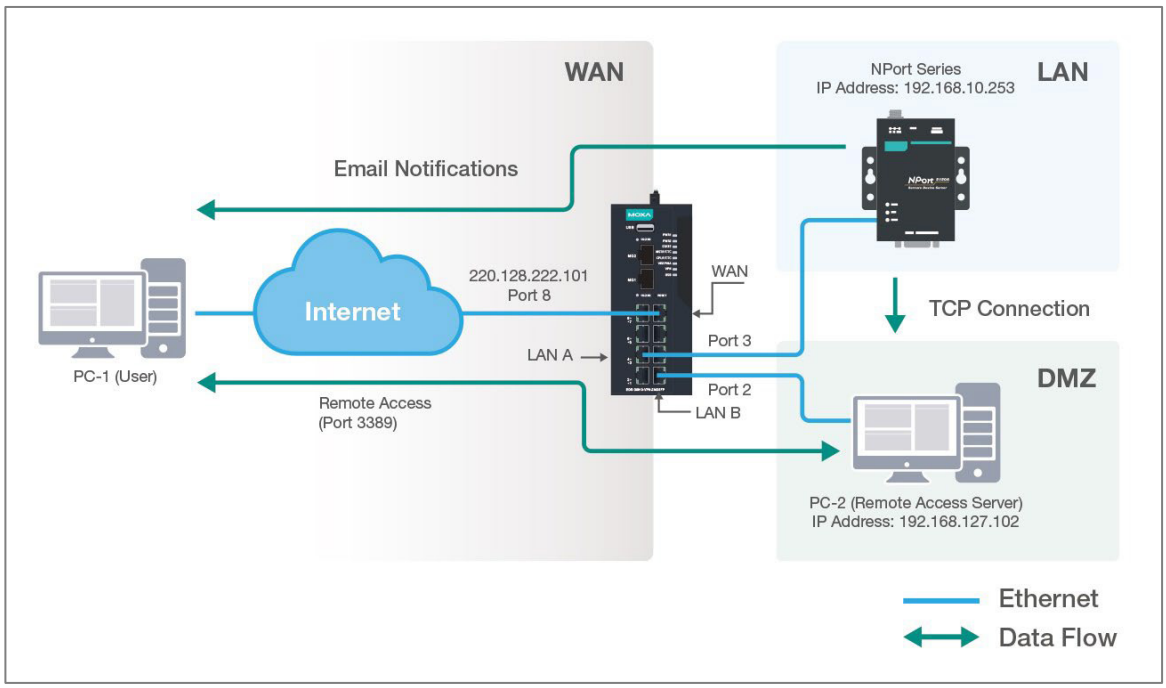
Warning: This is not a security tutorial. While Moxa firewalls can block incoming connections from the internet, internet-connected computers with outbound-only internet access are still vulnerable to high-level compromises that could allow lateral movement within a network. For example, a desktop could become infected with malware through a fishing email, which then sends an outgoing connection request to a command-and-control server, allowing unauthorized remote access.

The security of this example is contingent on the security and access control of all internet-connected computers in the example. The example provided is should be viewed as a tutorial on NAT and DMZ concepts, which can be used in tandem with comprehensive security measures for network protection. NAT and DMZ are tools in a security toolkit, and are not a replacement for or guarantee of comprehensive network security. Secure your devices. Develop, implement, and maintain a comprehensive, multi-layered security strategy.

A DMZ (demilitarized zone) is a region located between an organization's internal trusted network and the external untrusted network. The primary purpose of a DMZ is to provide an additional layer of security while allowing certain network services and resources to be visible to the external world.

A factory has the following networking needs:

- An production network (LAN). This network will contain production equipment that must be protected, but PCs must be able to access the Internet.
- A DMZ network with a single computer serving as a remote access server for connections from the internet, which has network access to the production equipment. Security is contingent on the security of the remote access server.
- A WAN network (Internet Connection).



The this architecture can be created using a series of N-to-1 NAT/PAT rules and Firewall rules on a MOXA router.

The following steps will outline how to configure this scenario. For details on each step, see subsequent sections. Your actual setup will vary depending on local conditions.

1. Configure network interfaces **WAN** (**WAN1** for dual-WAN devices), **LAN**, and **DMZ**.
2. Configure firewall rules to enforce traffic flows.
    a. Create an allowlist paradigm by configuring **Global Policy Default Action** to **Deny All**
    b. Add Layer 3 firewall rules for directional access between each interface:
        - WAN-to-DMZ
        - DMZ-to-WAN
        - LAN-to-DMZ
        - LAN-to-WAN
3. Configure NAT rules to route data between interfaces. This is done after creating firewall rules to ensure no unfiltered traffic gets through.
4. Create the following rules

a. **N-to-1** based on an IP range for directional **WAN** (**WAN1** for dual-WAN devices) access for **LAN**.

b. **PAT** to allow port-specific, directional access from **WAN** and **DMZ** to accommodate the remote desktop protocol.

No port other than 3389 will be forwarded to minimize the potential attack surface.

c. **N-to-1** based on an IP range for directional **WAN** (**WAN1** for dual-WAN devices) access for **DMZ**.

See subsequent sections for detailed configuration instructions.

Example: Configuring Interfaces for DMZ

Interfaces must be defined so they can be referenced for Firewall and NAT rules.

1. Sign in to the device with administrator credentials.
2. To add interface **LAN**, go to **Network Configuration** > **Network Interfaces** > **LAN**, and then press **Add**.
3. Specify all of the following, and then click **Create**:

Field	Setting
Name	LAN
VLAN ID	10
Connection Type	**Static IP**
IP Address	192.168.10.0
Netmask	**24 (255.255.255.0)**

The LAN interface will appear on the Network Interface list.

4. To add interface **WAN**, go to **Network Configuration** > **Network Interfaces** > **WAN1** (**WAN1** for dual-WAN devices), and then press **Add**.
5. Specify all of the following, and then click **Apply**:

Field	Setting
Connection Type	**Static IP**
IP Address	220.128.222.101
Netmask	**8 (255.0.0.0)**

6. To add interface **DMZ**, go to **Network Configuration** > **Network Interfaces** > **WAN2/DMZ**, and then select **DMZ**.
7. Specify all of the following, and then click **Apply**:

Field	Setting
IP Address	192.168.127.102
Netmask	**24 (255.255.255.0)**

The interfaces will be available within the other rule-making screens.

Example: Creating Firewall Rules for DMZ

Firewall rules allow us to configure an allowlist paradigm, blocking any unexpected traffic.

Make sure that network interfaces have already been assigned and configured.

Important: This example of an allow list relies on interfaces, which may in turn rely on static IP addresses. Ensure your network is configured accordingly. If the identified characteristics change, the settings will have to be updated to avoid unpredictable or potentially insecure behavior.

1. Sign in to the device with administrator credentials.
2. Go to **Firewall** > **Layer 3-7 Policy**.
3. To configure the allowlist paradigm, under **Global Policy Settings**, set **Status** to **Enabled**, and make sure **Default Action** is set to **Deny All**, and then click **Apply**.
4. To add the WAN-to-DMZ rule, click **Add** and configure the following:

Option	Value
Name	WAN-DMZ
Action	**Allow**
Incoming Interface	**WAN** (**WAN1** for dual-WAN devices)
Outgoing Interface	**DMZ**
Filter Mode	**IP and Port Filtering**

Click **Create** to add the entry to the table.

5. To add the DMZ-to-WAN rule, click **Add** and configure the following:

Option	Value
Name	DMZ-WAN
Action	**Allow**
Incoming Interface	**DMZ**
Outgoing Interface	**WAN** (**WAN1** for dual-WAN devices)
Filter Mode	**IP and Port Filtering**

Click **Create** to add the entry to the table.

6. To add the LAN-to-DMZ rule, click **Add** and configure the following:

Option	Value
Name	DMZ-WAN
Action	**Allow**
Incoming Interface	**LAN**
Outgoing Interface	**DMZ**
Filter Mode	**IP and Port Filtering**

Click **Create** to add the entry to the table.

7. To add the LAN-to-WAN rule, click **Add** and configure the following:

Option	Value
Name	DMZ-WAN
Action	**Allow**
Incoming Interface	**LAN**
Outgoing Interface	**WAN** (**WAN1** for dual-WAN devices)
Filter Mode	**IP and Port Filtering**

Click **Create** to add the entry to the table.

8. Click **Apply** to apply newly created firewall rules.

All traffic not conforming to the above rules will be blocked by the firewall.

Add NAT rule to ensure traffic is routed correctly between different interface.

Example: Configuring NAT Rules for DMZ

NAT rules allow the device to translate packets between different interfaces and IP subnets.

1. Sign in to the device with administrator credentials.
2. Go to **NAT**, click **Add**, and then configure the following to add a NAT rule to allow **LAN** access to **WAN** (**WAN1** for dual-WAN devices):

Option	Value
Description	LAN-WAN
Mode	**N-to-1**
Source IP Start	192.168.127.1
Source IP END	192.168.127.254
Outgoing Interface	**WAN** (**WAN1** for dual-WAN devices)

Click **Apply** to add the rule to the table.

3. To add a NAT rule to allow **DMZ** access to **WAN** (**WAN1** for dual-WAN devices), click **Add**, and then configure the following:

Option	Value
Description	DMZ-WAN
Mode	**N-to-1**
Source IP Start	192.168.10.1
Source IP END	192.168.255.254
Outgoing Interface	**WAN** (**WAN1** for dual-WAN devices)

Click **Apply** to add the rule to the table.

4. To add a NAT rule to allow **WAN** (**WAN1** for dual-WAN devices) traffic to the remote access server on **DMZ**, click **Add**, and then configure the following:

Option	Value
Description	Remote-Access-Server
Mode	**PAT**
Original Packet (Condition) - Incoming Interface	**WAN** (**WAN1** for dual-WAN devices)
Original Packet (Condition) - Destination Port	3389
Translated Packet (Action) - Destination IP	192.168.127.102
Translated Packet (Action) - Destination Port	3389

Click **Apply** to add the rule to the table.

5. Click **Apply** under the table to save your changes.

Chapter 6

Security Hardening Guide

Security Hardening Guide Overview

This chapter provides an overview of security strategy, standards, and recommended best practices to improve the security landscape.

The threat landscape is constantly evolving, and no security guide can ever provide 100% protection. This chapter is constantly being expanded, and is not exhaustive.

Security Best Practices

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.

Product Security

This section provides essential information on the installation of your product.

Physical Installation Guidelines

Physical protection of devices is vital to network security.

With physical access to devices, prospective attackers can physically bypass security mechanisms, alter network conditions, or plant additional malicious devices in networks. Follow these tips to help reduce the risk of tampering with networking devices by unauthorized personnel.

- Install switch/router in an access-controlled area. To further protect your device from potential physical attacks, it is important to important to conduct a risk analysis and implement appropriate physical security measures. Consider physical security like installation within a locked cabinet,surveillance, security guards, and access control systems, among other measures. The specific measures you choose should be based on your environment and the level of risk you face.

- Install a Layer 2 switch within the security perimeter. This perimeter can be established by setting up a firewall at the border, as the switch is not designed to be directly connected to the Internet. Note that the switch should not be classified as zone or boundary equipment. Avoid connecting the device directly to the Internet, as this can leave your network vulnerable to security breaches.
- Follow the Quick Installation Guide included in the package of your device. It contains step-by-step instructions that are easy to follow and will help you set up the device quickly and efficiently.
- Examine and monitor anti-tamper labels applied to the device enclosures. These labels provide a quick and easy way for administrators to determine if the device has been tampered with.
- 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.
  - Setting password expiration.
  - Updating passwords regularly.
  - Never sharing passwords.

Note

Based on trends in cybersecurity regulations, we recommend users increase the complexity of their passwords to the highest level to further strengthen password security.

Refer to Password Policy for more information about password policies.

Protecting Vulnerable Network Ports

Understand security risks and mitigate them by configuring network ports correctly.

- Changing port numbers for active services, 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.
- Configure automatic session locking or idle timeouts so that idle sessions cannot be hijacked.
- Generate new SSL certificates and SSH keys for devices prior to using HTTPS or SSH applications. Refer to SSH & SSL for more information.

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.

> **Note**
> SNMP managers should be used in accordance with their own security hardening guides and recommended security procedures.

Refer to SNMP for more information.

Device Access Control Best Practices

Device access control is an essential aspect of network security that helps protect against unauthorized access to network resources.

Unauthorized access can occur through various means, including physical access to network devices, hacking, or social engineering. Without proper access control measures

in place, networks are vulnerable to security breaches, data theft, and other malicious activities.

Device access control is particularly important for organizations that handle sensitive data, such as financial institutions, healthcare providers, and government agencies. By implementing device access control, these organizations can limit access to sensitive information and prevent security breaches. Below are some ways to ensure device access control:

- Adopt the Principle of Least Privilege. This principle involves granting users, applications, or systems the minimum level of access or permissions they need to perform their specific tasks and nothing more. Requests for additional access, such as HTTPS, SSH, or Moxa services for administration, should be carefully evaluated before being approved
- Use strong passwords. Passwords should be complex and unique for each device. Passwords should also be changed regularly to maintain security.
  Refer to Password Policy for further information.
- Implement allowlists. Allowlists are authorized devices or users allowed to access a particular network resource. Allowlists can be managed at the device, network, or application levels. Network administrators can use allowlists to ensure that only authorized devices or users can access sensitive resources. The key feature of an allowlist is that anything not on the allowlist is automatically blocked, ensuring only authorized devices, uses, or services can operate freely in a network environment.
  Refer to Trusted Access for further information.
- Implement an L3 firewall. An L3 firewall, also known as a Layer 3 firewall, is a network security device operating at the OSI model's network layer. L3 firewalls can monitor and filter traffic based on IP addresses, ports, protocols, and other network-level attributes. Using L3 firewalls, network administrators can prevent unauthorized access to the network and block potential security threats.

Note

You can block intranet hosts from all external access with isolation, such as with a DMZ, and only allow connections from specifically authorized IP addresses.

Note

To enhance device security and ensure compliance with IEC 61162-460, consider the following practices:

1. Restrict Access:
    - Only allow connections from specific, verified, and secure hosts within a controlled network.
    - Maintain an authorized list of these approved source IPs, ensuring it is documented and regularly reviewed.
2. Block Uncontrolled Networks:
    - Do not permit direct access from hosts in uncontrolled or unverified networks.
3. Example Configuration:
    - Configure trusted access to accept traffic exclusively from source IPs within the 460-network.
    - Any IP address not on this allowlist, including those from non-control networks, will be blocked.

By adhering to these guidelines, you help maintain network security and comply with IEC 61162-460 requirements.

Refer to Firewall for further information.

Configuring Allowlists in Compliance with IEC 61162-460

To enhance device security and ensure compliance with IEC 61162-460, implement the following practices:

- Restrict Access
    - Only allow connections from specific, verified, and secure hosts within a controlled network.
    - Maintain an authorized list of these approved source IPs, ensuring it is documented and regularly reviewed.
- Block Uncontrolled Networks
    - Do not permit direct access from hosts in uncontrolled or unverified networks.

By adhering to these guidelines, you help maintain network security and comply with IEC 61162-460 requirements.

Example Configuration

- Configure trusted access to accept traffic exclusively from source IPs within the 460-network.
- Any IP address not on this allowlist, including those from non-control networks, will be blocked.

About Device Integrity and Authenticity

Integrity and authenticity are vital elements of trust within a network.

Device integrity refers to the state of a device being complete, unaltered, and free from any unauthorized changes or modifications.

Authenticity refers to the assurance that the device is genuine and comes from a trusted source.

Both integrity and authenticity are critical aspects of device security. Methods to sustain these aspects include:

- Configuration Backup & Encryption
- Secure Boot

Configuration Backup and Encryption

Configuration backup and encryption protects a device's sensitive data and configuration by created an encrypted copy storing it securely. In the event of unauthorized device changes, correct configuration information can be quickly and securely restored.

The process involves creating a backup of the device's configuration and then encrypting it using a strong encryption algorithm. The encrypted backup is then stored securely to prevent unauthorized access. This process is particularly important for devices that store sensitive information, such as network equipment, servers, and other critical infrastructure. Encrypting the configuration backup ensures that the data remains protected even if the backup location is compromised.

Secure Boot

Secure Boot is a security mechanism designed to ensure that devices boot using only software that is verified as trusted. The primary function of Secure Boot is to prevent

unauthorized software from running during the boot process. It achieves this by verifying the integrity and authenticity of the bootloader and firmware.

A bootloader refers to the initial software that runs when a device is powered on. Its primary role is to load the device's operating system. Firmware is software embedded within the device that manages and controls the device's hardware functions.

Moxa hardware makes use of cryptographic modules embedded in devices to support verification processes. The device's ROM (read-only memory) contains approved bootloaders and associated digital certificates, which are used to verify the integrity of the firmware.

When the device boots, the first thing to run is the bootloader. Secure boot checks the digital signature against the certificate stored in ROM. If the signatures match, the boot process continues. If they do not match, or there is evidence of tampering, the boot process halts to prevent potential security breaches.

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

Refer to Event Log for more information about Event Logs.

Refer to Event Notifications for more information about Event Notifications.

Refer to SNMP for more information about SNMP configuration.

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.
SNMP	UDP 161 UDP 162 TCP 10161 TCP 10162	Disabled	For V1 & V2c, change default community string names, i.e. public & private, to other unique names. For V3, enable SNMP admin account authentication.
Syslog	UDP 514	Disabled	Enabling Syslog is recommended to avoid missing critical logs due to limited local storage. This sends logs to an external syslog server, where they can be securely stored and retained. The syslog server is responsible for keeping these logs for a minimum period required by local regulations, ensuring critical incidents are properly documented and accessible when needed.
RADIUS	UDP 1812	Disabled	Enabling RADIUS authentication can help administrators manage password changes more efficiently.
Moxa Services	TCP 443 UDP 40404	Enabled	These 2 ports are only used by the Moxa management software. Disable it if you don’t use Moxa management software.

Security-Related Functions

Function	Default Setting	Security Suggestions
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.
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.

Incident Category	Detailed Description	Mitigation Suggestions
Information Disclosure	Data flowing across TFTP may be sniffed by an attacker.	Use SFTP instead of FTP.
Denial of Service	SNMP Server crashes, halts, stops or runs slowly by excessive quires.	Enable rate limit to stop excessive SNMP requests.
Denial of Service	RADIUS Server crashes, halts, stops or runs slowly by excessive quires.	Enable rate limit to stop excessive RADIUS requests.
Repudiation	Devices fail to synchronize a system time with a trusted NTP/SNTP server.	Enable NTP authentication to verify a connection with the trusted NTP/SNTP server.

Note

Create an incident response plan and follow it carefully. Ensure your procedures allow for user reporting and admin response to those reports. Many threats manifest themselves as irregular device behavior – such as device inability to provide basic services like routing or firewall functions, which in turn lead to interruptions or unauthorized access. Create a plan that allows admins to prepare, reboot, and monitor devices with abnormal behavior.

Recommended Operational Roles and Duties

Adhering to the principle of least privilege reduces risks by ensuring users operate at the minimum privilege required to complete their tasks.

Instead of individual allocation, privilege levels should be tied to specific job functions. For optimized device security, we recommend three distinct privilege levels, each tailored for different management needs:

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.

Refer to:

- 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.

Note

Firmware updates may cause downtime. Assess the impacts of downtime and prepare appropriately before initiating updates.

Note

Device performance may be degraded during the update process. Normal function should be restored once the update is complete and the device restarts.

Configuration Backup

For network operators and system administrators, it is essential to regularly back up device configurations. This precaution allows for quick recovery in unforeseen scenarios, such as cyber attacks.

Note

Prioritize use of secure transfer protocols – such as SFTP – for file transfers to protect the configuration maintenance process.

Refer to:

- 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 for Moxa products, please submit your findings on the following web page: https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability.

For the most up-to-date Moxa security information, please visit our security advisory page: https://www.moxa.com/en/support/product-support/security-advisory

Recommendations for Decommissioning

Recommendations for Decommissioning

To avoid any sensitive information such as account passwords or network configurations from disclosure, always delete all imported certificates and reset devices to factory default before you decommission your devices.

Note

Things to keep in mind when decommissioning or re-purposing devices:

- Device data can be cleared using the Factory Reset options. When reseting devices, make sure to confirm the operation and allow it sufficient time to complete.
- Delete all logs, and verify deletion.
- After all reset processes are complete, verify that all sensitive data has been cleared.

Using Security Features

Ensuring the security features of your network device operate effectively is vital for maintaining a secure and reliable system. During field validation, include these features—such as firewalls, encryption, and intrusion prevention—in your testing plan to confirm they function properly in real-world conditions.

This chapter outlines the available security features, how to configure them, and best practices to ensure consistent protection for your network.

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. Policies can be used to enact other kinds of filing, such as:
    - Physical Port Filtering: If unique VLANs are assigned to each port, and L3-7 policies are applied to each VLAN, this has the effect of applying policies to the physical port.
    - High-precision traffic control and QoS: Layer 3-7 policy can be configured to filter out unnecessary traffic, reducing bandwidth waste.
- 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.

- 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.
- Safeguarding sensitive data: Firewalls are used to safeguard sensitive data such as financial information, healthcare records, and production data.
- 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

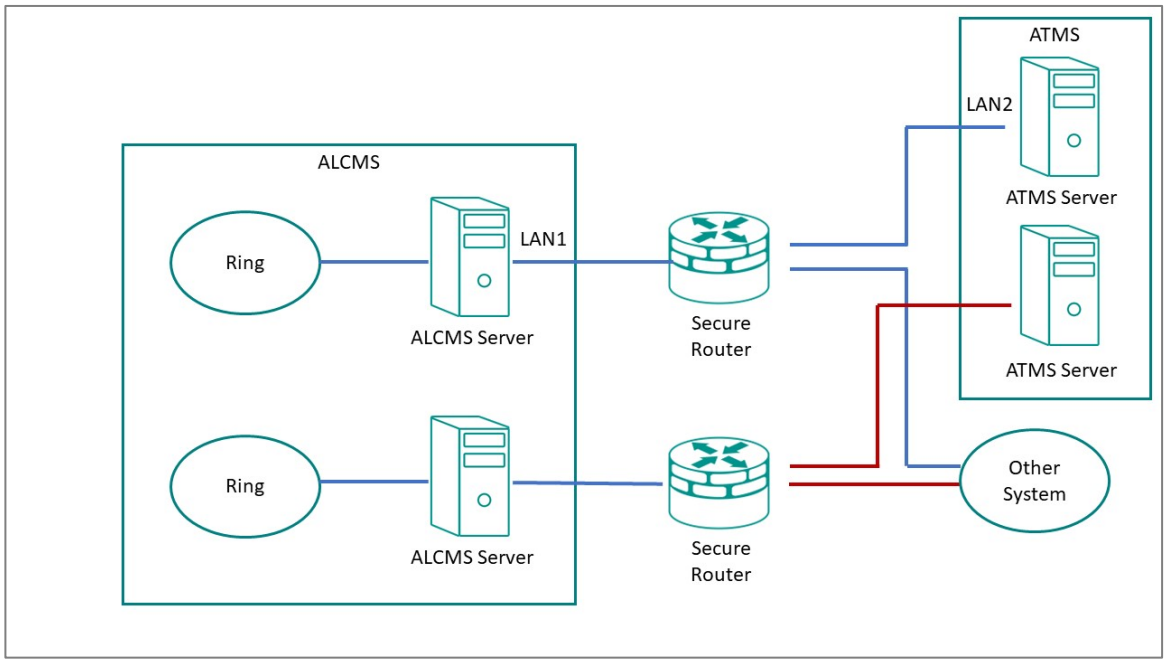
An allowlist is a network configuration that blocks all traffic except those specifically allowed.

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.

> **Note**
> 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**

Item	Value
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.

Note

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.

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.

Security Standards and Concepts

AAA

About AAA - Authentication, Authorization, and Accounting

Authentication, **A**uthorization, and **A**ccounting (AAA) is a user-based access control paradigm.

AAA coexists with other security practices. While product security and network security focus on device or process security, AAA focuses on users.

AAA comprises a set of functions for an administrator to determine which users can access a network device, which services are available to authorized users, and collect information about user activities for audits or charging purposes if required. When implemented well, AAA can provide an extra layer of security across different aspects.

Authentication

Authentication provides a method of identifying a user before access to the network device is granted, typically by having the user enter a valid username and password and/or provide a physical token or digital certificate. Additional policies such as a password complexity check or login failure lockout can also increase access security.

Authorization

After authentication is successful, a user can be authorized to use specific resources on the device or perform specific operations. For instance, a normal user with limited permissions may only view the device's system settings, whereas an administrator would have full control to view or edit all system settings.

Accounting

Accounting keeps track of user activities on the device. It monitors the resources a user consumes during network access. This can include the amount of data sent and received through an Ethernet port or the number of user login failures.

About Authentication Types

Handle authentication with the local device exclusively, or with a remote server using local accounts only as a fallback.

It is important to choose the right authentication method, or combination of authentication methods for your network environment and use case. Moxa devices offer the following authentication options.

Local Authentication

Local authentication uses the accounts and settings stored on the local network device to identify users (authentication), determine which services they can use (authorization), and track basic user activities such as amount of data transferred or number of login failures (accounting).

Remote Authentication

Remote authentication uses accounts configured on a RADIUS server - allowing AAA to be configured from a single, centralized location. However, it is important to note that local authentication is retained as a fallback mechanism to ensure the device can be configured if the RADIUS server becomes inaccessible. Additionally, Moxa products support backup RADIUS servers if the primary becomes inaccessible. Due consideration should be given to the configuration and maintenance of backup servers for redundancy.

Local vs. Remote Authentication Feature Comparison

Features	Local	Remote
Configuration location	Local device	Remote RADIUS server, local as fallback
Number of accounts	Few	Many

Features	Local	Remote
Password security requirements	Limited	Many
Allowed services*	Specified locally	Determined by server
Authority types	Admin, User, Supervisor	Admin, User
User feedback on failed login	Custom prompt	Server-defined
Setup effort	Low	High

*Allowed services are usually dependent on Authority types.

Example: Creating a Local User

Local accounts are authenticated and managed by the local device, and function even when remote RADIUS servers are unavailable.

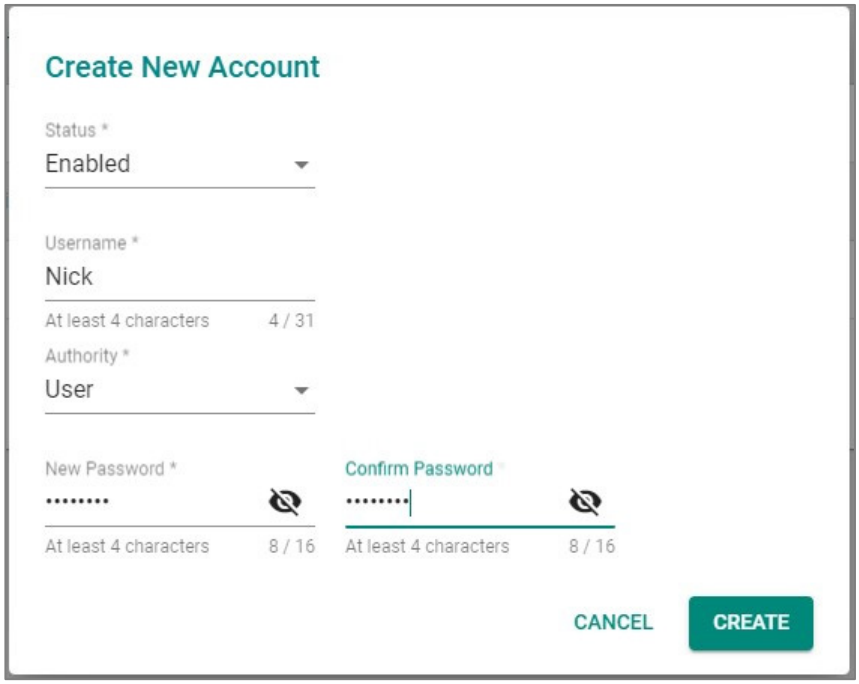
Before you begin: Make sure you have an account with **Admin** authority.

In this example, create a local user with simple **User** level authority to fill the Authentication of the AAA tripod. Once the user has been created, add additional access controls.

1. Using an account with **Admin** authority, log in to the network device.
2. Go to **System→Account Management→User Accounts**, and then click the plus icon.

   Result: The **Create New Account** panel appears.
3. Set **Status** to **Enabled**.
4. In the **Username** field, type `Nick`.
5. Set **Authority** as **User**.
6. In the **New Password** field, type `1qaz!@#$`, and then type again to confirm.
7. Click **Create**.

Results: By creating the user **Nick**, Authorization and Accounting details can now be configured.



What to do next: Now that a user account has been created, add account controls. Account controls allow setting a warning for incorrect passwords, account lockouts, and automatic logout. For details, see Example: Configuring Account Controls for Local Users.

Example: Configuring Account Controls for Local Users

Login Failure Account Lockout and Auto Logout increase the security of local accounts.

Enabling additional account controls can increase resistance to brute-force attacks as well as enable troubleshooting. This example demonstrates how to set account lockouts after failed login attempts and manage idle users.

1. Using an account with **Admin** authority, log in to the network device.
2. Go to **Security→Device Security→Login Policy**.

   Result: The **Login Policy** panel appears.
3. In the **Login Authentication Failure Message** field, type `Warning! The account will be temporarily locked if there are too many consecutive login failures.`
4. Set **Login Failure Account Lockout** to **Enabled**.
5. In the **Login Failure Retry Threshold** field, type `3`.

This is the number of failed attempts before the user account will be temporarily blocked.

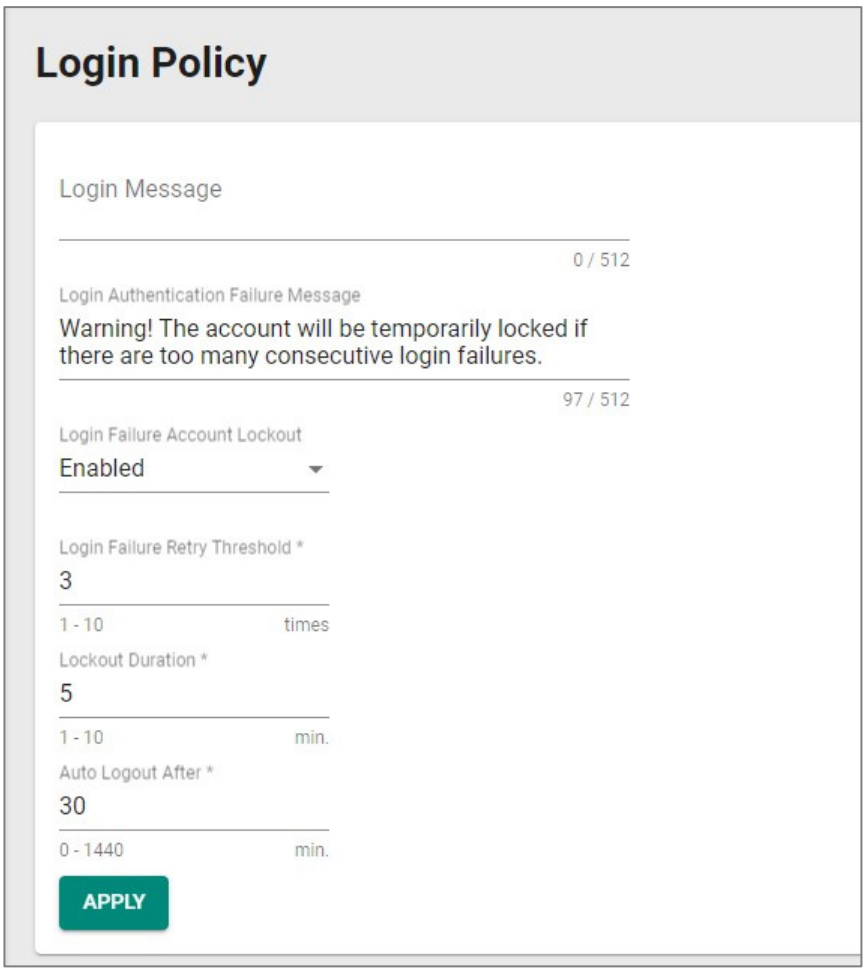
Temporary bans can help prevent password guessing and brute force attacks by preventing attackers from rapidly guessing many passwords.

6. In the **Lockout Duration** field, type `5`.

This specifies the number of minutes the account will be locked.

7. In the **Auto Lockout After** field, type `30`.

This is the amount of time in minutes before inactive accounts automatically log out.



Results: This configuration:

- Displays a warning message on failed login attempts, enabling troubleshooting
- Blocks accounts for five minutes after three unsuccessful login attempts, limiting the effectiveness of credential guessing

- Automatically logs out inactive user accounts after thirty minutes, reducing risks of unauthorized access through idle consoles

What to do next: Optionally, configure allowed access protocols. For details, see User Interface.

Example: Configuring a Remote RADIUS Server

In this example, the RADIUS server handles all Authentication, Authorization, and Accounting.

Before you begin:

- Make sure you have a working RADIUS server and corresponding configuration information. In our example, we use a server that has the following settings:
  - **PAP** authentication protocol
  - An address of `192.168.127.1`
  - UDP port 1812
  - A preconfigured shared key

Remote Authentication Dial-In User Service (RADIUS) servers may make it easier to manage large numbers of users from a central location.

1. Using an account with **Admin** authority, log in to the network device.
2. Go to **Security→Authentication→Login Authentication**, and then set **Authentication Protocol** to **RADIUS, Local**.

   Tutorial Info: This setting will use the remote RADIUS server as the primary authentication source, and use local authentication as a fallback if the RADIUS server is unavailable.

> **Note**
>
> Enabling RADIUS authentication will not remove local accounts. Make sure local accounts have a strong, unique password. Local accounts are still required both for RADIUS server configuration as well as for local fallback if the RADIUS server is not reachable. For details, see Example: Creating a Local User.

3. Go to **Security→Authentication→RADIUS**.

   Result: The **RADIUS Server** will appear.

4. Configure all of the following:

Field	Setting
Authentication Type	**PAP**
Server Address 1	192.168.127.1
UDP Port	1812
Shared Key	Enter your Shared Key here.

Tutorial Info: These configuration options are provided as an example only, and will need to match your network environment.

5. Click **Apply**.

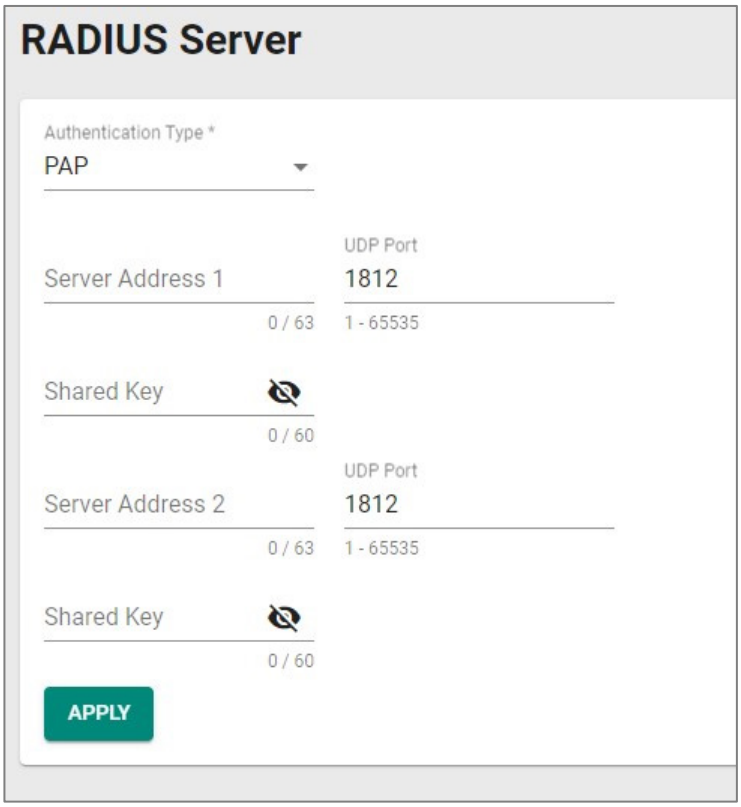
Results:

By configuring remote authentication, the network device will redirect user login requests to the RADIUS server. When logging in with remote user `Peter`, the RADIUS server will process the authentication request and determine whether to grant access to the device. If `Peter` does not match RADIUS or Local information, access will be denied.

In situations where the RADIUS server is not reachable or unavailable, users such as `Nick` (created in Example: Creating a Local User or other existing local users can still access the network device using their local passwords.

Note

If RADIUS is enabled, but unreachable, network-based logins (HTTP/HTTPS/Telnet/SSH) will not be possible, and users will be limited to logins through the console port only.

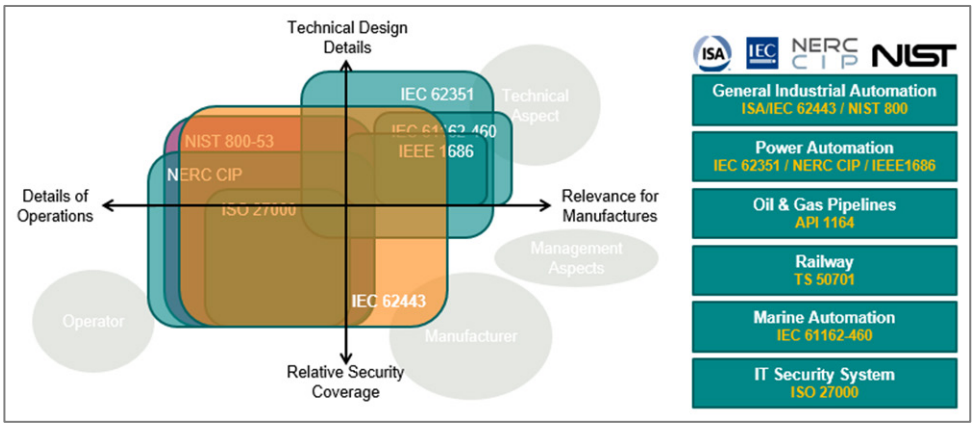


ISA/IEC 62443 Standards and Architecture

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 cycle and use-cases

Parts of ISA/IEC 62443	Scope	Sections
ISA/IEC 62443-2	Process and Program requirements	Part 2-1: Establishing an industrial automation and control system security program Part 2-2: Implementation guidance for an IACS security management system Part 2-3: Patch management in the IACS environment Part 2-4: Security program requirements for IACS service providers
ISA/IEC 62443-3	Systems	Part 3-1: Security technologies for industrial automation and control systems Part 3-2: Security risk assessment and system design Part 3-3: System security requirements and security levels
ISA/IEC 62443-4	Components	Part 4-1: Secure product development lifecycle requirements Part 4-2: Technical security requirements for IACS components

Product suppliers adhere to the ISA/IEC 62443 standard to provide components for Industrial Automation and Control System (IACS) solutions. These components can be:

- Individual items
- Combined products forming a system or subsystem

Additionally, system integrators use the following sections of the ISA/IEC 62443 standard:

- IEC 62443-2-1
- IEC 62443-2-4
- IEC 62443-3-2
- IEC 62443-3-3

These standards help integrators:

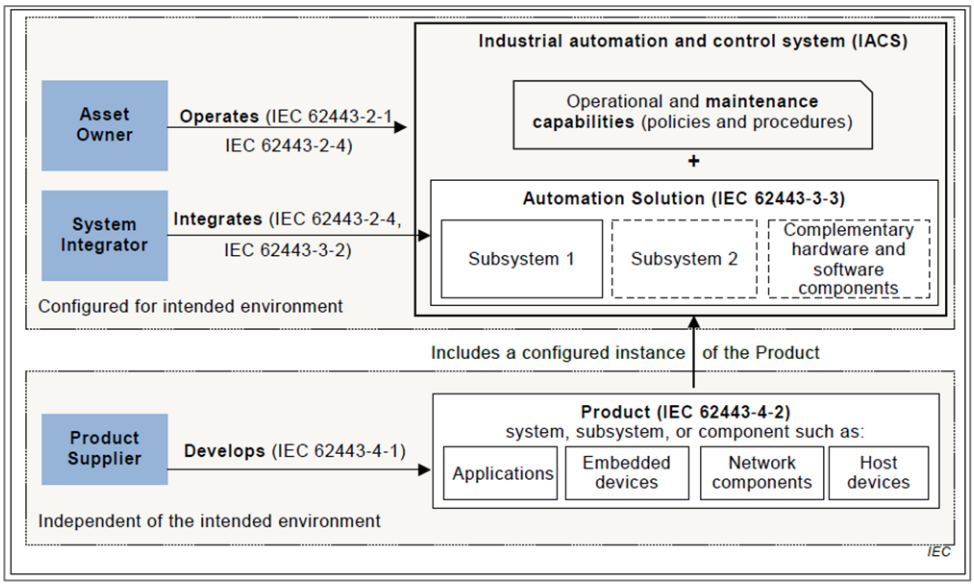
- Determine security zones
- Specify security capability levels for each zone
- Integrate products into an Automation Solution

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.

Summary of IEC 62443 Stakeholders



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 1	Identification and Authentication Control
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 of SRs:

- Software Applications
- Embedded Devices
- Host Devices
- Network Devices

While a majority of Part 4-2's criteria are generic and apply uniformly across categories, there are exceptions. Unique, component-specific stipulations are clearly signposted, with exhaustive details available in dedicated clauses. For details, consult the original standards.

Requirement Enhancements

CRs may contain one or more requirement enhancements (RE). REs are additional requirements attached to CRs that add additional conditions to accommodate higher security levels.

FR 1 Applications: 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 the need to verify different kinds of users, FR 1 uses the following CRs:

- **CR 1.1** focuses on human users.
- **CR 1.2** addresses software processes and devices.

Identification vs. Authentication: Consider a person's ID card. While the card identifies its owner, can someone else misuse it? Certainly. Here, the distinction between 'identifying' (matching a person to an ID card) and 'authenticating' (confirming the card holder's authenticity) becomes crucial. Each process has distinct methods and requirements.

Understanding CR and RE in Determining Security Levels: CR represents foundational requirements, whereas RE 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

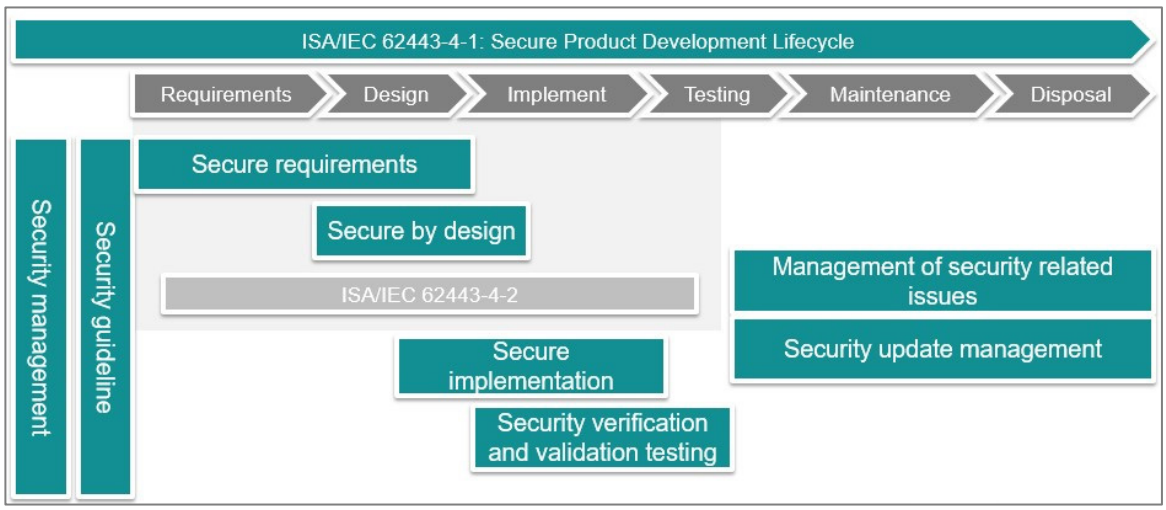
Security Level	Example Threat Actor	Violation Type	Means	Resource Level	Motivation
SL-1	• Ordinary user	Coincidental	N/A	N/A	N/A
SL-2	• Entry-level hacker	Intentional	Simple	Low	Low
SL-3	• Terrorist Organization • Organized crime	Intentional	Sophisticated	Moderate	Moderate
SL-4	• Nation state	Intentional	Sophisticated	Extended	High

For more information about CRs, SLs, and REs, refer to the ISA/IEC 62443 standard.

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.

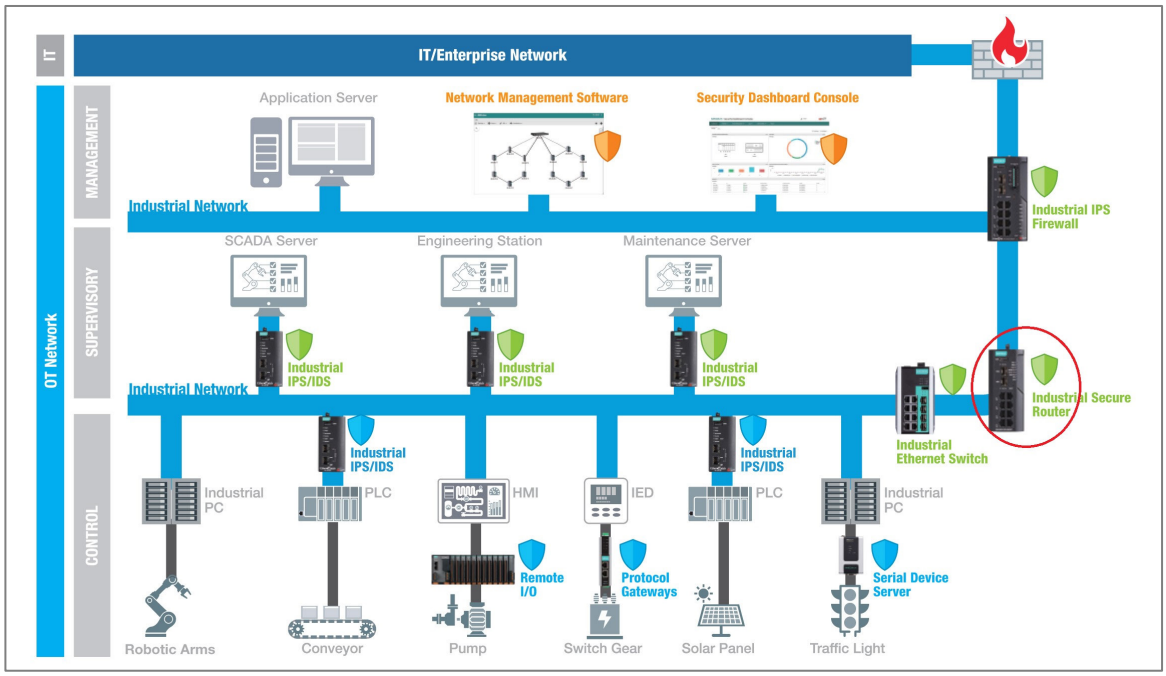
Component Security with IEC 62443-4-2

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.

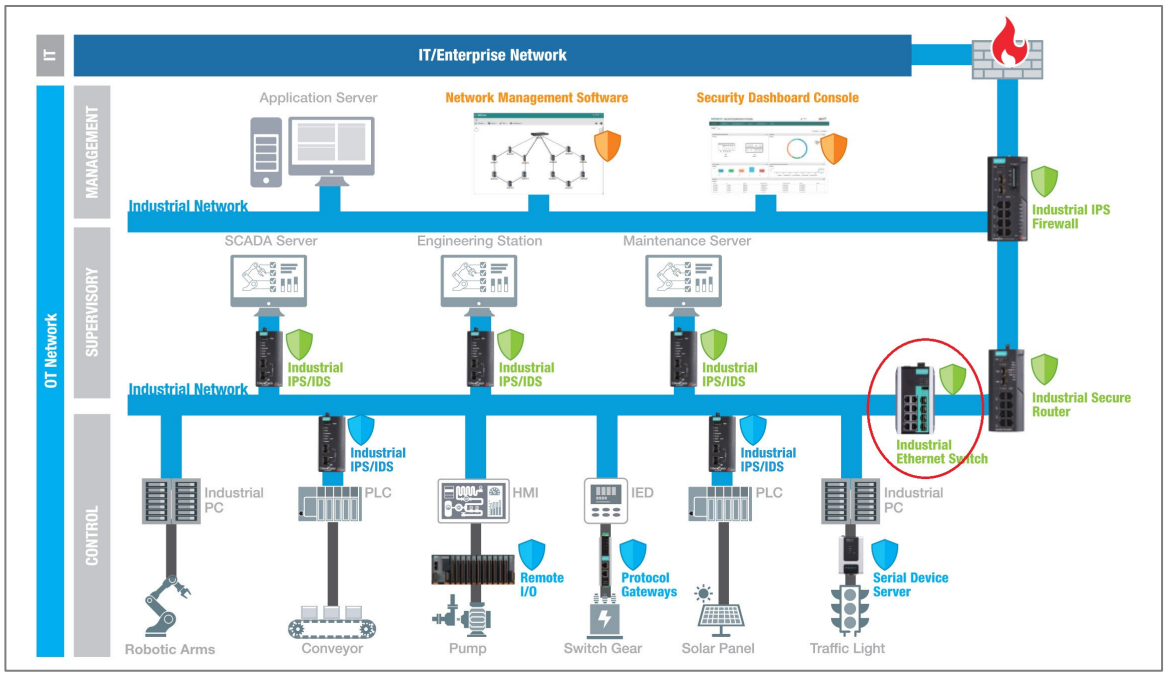
Security Context of an Industrial Secure Router



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.

Chapter 7

Appendix

Destination Ports for Layer 3 – 7 Protocol

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

Industrial Application Service
Modbus
DNP3
IEC-60870-5-104
IEC-61850-MMS
OPC-DA
OPC-UA
CIP-EtherNet/IP
Siemens-Step7
Moxa-RealCOM

Industrial Application Service
moxa-MXview-Request

Glossary

1-to-1 NAT

1-to-1 NAT maps one public IP address to one private IP address.

Dead Interval

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.

Double NAT

Double NAT enables you to use 1-to-1 rules to facilitate two-way communication.

N-to-1 NAT

N-to-1 NAT maps multiple private IP addresses to one public IP address.

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.

Network Address Translation (NAT)

NAT (Network Address Translation) is method of changing an IP address during Ethernet packet transmission, which can also enhance network security. If you wan to hide an

internal IP address (LAN) from the external network (WAN), NAT can translate the internal IP address to a specific IP address, or an internal IP address range to one external IP address.

Port Address Translation (PAT)

Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers.

IEC 61162-460 Supplementary Declaration

Preface

IEC 61162-460 is an international standard developed by the International Electrotechnical Commission (IEC) that specifies requirements for digital interfaces used in maritime navigation and radiocommunication equipment. It serves as an extension to IEC 61162-450, focusing on enhancing safety and security within Ethernet-based shipboard networks.

The standard outlines requirements and test methods for equipment intended for use in IEC 61162-460 compliant networks. It also provides guidelines for the network's architecture and its interconnections with other networks, including provisions for redundant network configurations to ensure reliability.

By implementing IEC 61162-460, maritime systems can achieve higher safety and security standards, addressing potential external threats and improving overall network integrity. This is particularly important in modern maritime operations, where robust and secure communication networks are essential for safe navigation and effective radiocommunication.

Explanation

The configuration recommendations required for equipment to comply with IEC-61162-460 can largely refer directly to the Security Hardening Guide section. This section serves only as supplementary explanation and declaration.

Supplementary Declaration

When users configure this device, they need to additionally consider the following requirements to determine if they are necessary for the specific site. If they are, the following recommendations can be referenced:

1. It is recommended that the bandwidth allocated to each port on a 460-switch be greater than or equal to the total traffic handled by the switch.
2. When considering the configuration of trusted access, it is recommended that users restrict access to the device to specific IPs originating from the 460-network. Source IPs outside the allowlist (e.g., IPs from uncontrolled networks) will be blocked.
3. When configuring or adjusting Layer 3-7 policies, users can only access the device and configure Layer 3-7 policies through the trusted access allowlist, which specifies source IPs from the 460-network.
4. Arbitrarily replacing or modifying equipment within the 460 network may lead to cybersecurity concerns. It is recommended to first consult with the system integrator or manufacturer to assess potential risks.
5. If filtering based on each physical port is required, it is recommended to configure a VLAN interface with only one port member. Subsequently, apply the relevant rules to this interface through the Layer 3-7 policy.
6. The communication between devices or software defined within the 460-network must be managed through the EDR-G9010/EDR-8010 or by using alternative devices equipped with 460-switch and 460-forwarder functionalities to achieve control.

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
83	Conformance test - confirmation reply telegram
84	Conformance test - opTrnDir request telegram
85	Conformance test - opTrnDir reply telegram

ComID	Description
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)

ComID	Description
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

Cause	Description
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
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
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

Type	Description
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
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

Type	Description
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

LED Behavior

This page describes the LED behaviors for different product series.

> **Note**
> Please note that some LEDs are only on models with related features.

NAT-108 Series LED Behavior

LED	Color	State	Description
PWR	Amber	On	Power is being supplied to the power input.
		Off	Power is NOT being supplied to the power.
STATE	Green	On	The system passed the self-diagnosis test on boot-up and is ready to run.
		Blinking	Device reset is in progress, blinking once per second.
		Off	The system failed the self-diagnosis test on boot-up.
LEARN	Amber	Blinking	The device lockdown learning is in progress.
		Off	Learning finished.
LOCKDOWN	Green	On	The device lockdown allowlist is enabled.
		Off	The device lockdown allowlist is disabled.

MIB Groups

Your device comes with integrated SNMP (Simple Network Management Protocol) agent software, compliant with RFC-123 standard MIB and properties MIB. The following is a list of all the folders and related MIB files.

For comprehensive MIB information, you can use MIB browser tools. These tools provide a detailed view of the MIB tree, allowing for easier management and monitoring of network devices. Additionally, the complete MIB files can be downloaded from the product page on the Moxa website. Visit the Moxa product pages to access the latest MIB files and other related resources.

MIB Tree Structure

The MIB tree structure is designed for all Moxa router series. However, some MIB files may not be supported due to the varying support levels of each product series. Refer to the Supported Features List for detailed information about supported features.

```
--insrouter(1.3.6.1.4.1.8691.6.100)
  |
  +--swTraps(0)
  |  |
  |  +-- r-n Enumeration   varconfigChangeTrap(1)
  |  +-- r-n Enumeration   varpower1Trap(2)
  |  +-- r-n Enumeration   varpower2Trap(3)
  |  +-- r-n Enumeration   vardi1Trap(4)
  |  +-- r-n Enumeration   vardi2Trap(5)
  |  +-- r-n Enumeration   varredundancyTopologyChangedTrap(10)
  |  +-- r-n Enumeration   varturboRingCouplingPortChangedTrap(11)
  |  +-- r-n Enumeration   varturboRingMasterChangedTrap(12)
  |  +-- r-n DisplayString varVRRPStateChangeTrap(13)
  |  +-- r-n Integer32     varFiberWarningTrap(28)
  |  +-- r-n DisplayString varVPNConnectedTrap(40)
  |  +-- r-n DisplayString varVPNDisconnectedTrap(41)
  |  +-- r-n DisplayString varFirewallPolicyTrap(50)
  |  +-- r-n DisplayString varSecurityNotificationTrap(51)
  |  +-- r-n Enumeration   varLoggingCapacityTrap(52)
  |  +-- r-n DisplayString varDot1xAuthFailTrap(53)
  |  +-- r-n Enumeration   varFirmwareUpgradeTrap(54)
  |  +-- r-n DisplayString varFirewallConfigChangeTrap(55)
  |  +-- r-n DisplayString varCellularIpChange(56)
  |  +-- r-n DisplayString varCellularModuleFail(57)
  |  +-- r-n DisplayString varCellularSimDetectFail(58)
  |  +-- r-n DisplayString varCellularPinCodeFail(59)
  |  +-- r-n DisplayString varCellularSimSwitch(60)
  |  +-- r-n DisplayString varCellularModuleHighTemperature(61)
  |  +-- r-n DisplayString varCellularGuaranlinkCellularReconnect(62)
  |  +-- r-n DisplayString varCellularGuaranlinkTriggerIspReregister(63)
  |  +-- r-n DisplayString varCellularGuaranlinkTriggerCellularModuleReset(64)
  |  +-- r-n DisplayString varCellularGuaranlinkTriggerSystemReboot(65)
  |  +-- r-n DisplayString varCellularPmPowerSavingStart(66)
  |  +-- r-n DisplayString varCellularPmPowerSavingEnd(67)
  |  +-- r-n DisplayString varCellularPmSchedulingRuleExpired(68)
  |  +-- r-n DisplayString varCellularSmsWrongPassword(69)
  |  +-- r-n DisplayString varCellularSmsWrongCommand(70)
  |  +-- r-n DisplayString varCellularSmsWrongFormat(71)
  |  +-- r-n DisplayString varCellularSmsCommandDisabled(72)
  |  +-- r-n DisplayString varCellularSmsTrustedNumberAuthenticationFail(73)
  |  +-- r-n DisplayString varWanInterfaceChange(74)
  |  +-- r-n DisplayString varWanInterfacePingFail(75)
  |  +-- r-n DisplayString varSerialOpModeStateChange(76)
  |  +-- r-n DisplayString varSerialDSRStateChange(77)
  |  +-- r-n DisplayString varSerialDCDStateChange(78)
  |  +-- r-n DisplayString varLfpOn(79)
  |  +-- r-n DisplayString varLfpOff(80)
  |  +-- r-n DisplayString varDeviceLockdownStateChangeTrap(81)
  |
  +--swMgmt(1)
  |  |
  |  +--basicSetting(2)
  |  |  |
  |  |  +--systemSetting(1)
  |  |  |  |
  |  |  |  +-- rwn DisplayString sysRouterName(1)
  |  |  |  |
  |  |  +--accessibleIP(2)
  |  |     |
  |  |     +-- r-n Enumeration enableAccessibleIP(1)
  |  |     +-- r-n Enumeration enableAccessibleLan(2)
  |  |     |
  |  |     +--accessibleIpTable(3)
  |  |        |
  |  |        +--accessibleIpEntry(1) [accessibleIpAddress]
  |  |           |
  |  |           +-- r-n IpAddress   accessibleIpAddress(1)
  |  |           +-- r-n IpAddress   accessibleIpNetMask(2)
  |  |           +-- r-n Enumeration accessibleIpState(3)
  |  |
```

```
|  +--network(3)
|  |  |
|  |  +--networkSetting(1)
|  |     |
|  |     +--wanSetting(1)
|  |     |  |
|  |     |  +-- r-n Enumeration   wanConnMode(1)
|  |     |  +-- r-n Enumeration   wanConnType(2)
|  |     |  +-- r-n IpAddress     wanStaticIpAddr(3)
|  |     |  +-- r-n IpAddress     wanStaticIpMask(4)
|  |     |  +-- r-n IpAddress     wanStaticDefaultGateway(5)
|  |     |  +-- r-n DisplayString wanAdslName(6)
|  |     |  +-- r-n DisplayString wanAdslHost(7)
|  |     |  +-- r-n Enumeration   wanPptpEnable(9)
|  |     |  +-- r-n IpAddress     wanPptpAddr(10)
|  |     |  +-- r-n DisplayString wanPptpUsrName(11)
|  |     |  +-- r-n IpAddress     wanDnsServer1(13)
|  |     |  +-- r-n IpAddress     wanDnsServer2(14)
|  |     |  +-- r-n IpAddress     wanDnsServer3(15)
|  |     |  +-- r-n IpAddress     ipAddr(16)
|  |     |  +-- r-n IpAddress     ipMask(17)
|  |     |  +-- r-n IpAddress     defaultGateway(18)
|  |     |  +-- r-n Enumeration   directedBroadcast(19)
|  |     |  +-- r-n Enumeration   sourceIPOverwrite(20)
|  |     |
|  |     +--wan2Setting(2)
|  |     |  |
|  |     |  +-- r-n Enumeration   wan2ConnMode(1)
|  |     |  +-- r-n Enumeration   wan2ConnType(2)
|  |     |  +-- r-n Enumeration   wan2DmzState(3)
|  |     |  +-- r-n IpAddress     wan2StaticIpAddr(4)
|  |     |  +-- r-n IpAddress     wan2StaticIpMask(5)
|  |     |  +-- r-n IpAddress     wan2StaticDefaultGateway(6)
|  |     |  +-- r-n DisplayString wan2AdslName(7)
|  |     |  +-- r-n DisplayString wan2AdslHost(8)
|  |     |  +-- r-n Enumeration   wan2PptpEnable(10)
|  |     |  +-- r-n IpAddress     wan2PptpAddr(11)
|  |     |  +-- r-n DisplayString wan2PptpUsrName(12)
|  |     |  +-- r-n IpAddress     wan2DnsServer1(14)
|  |     |  +-- r-n IpAddress     wan2DnsServer2(15)
|  |     |  +-- r-n IpAddress     wan2DnsServer3(16)
|  |     |  +-- r-n IpAddress     wan2IpAddr(17)
|  |     |  +-- r-n IpAddress     wan2IpMask(18)
|  |     |  +-- r-n IpAddress     wan2DefaultGateway(19)
|  |     |  +-- r-n Enumeration   wan2DirectedBroadcast(20)
|  |     |  +-- r-n Enumeration   wan2SourceIPOverwrite(21)
|  |     |
|  |     +--lanSetting(3)
|  |     |  |
|  |     |  +--lanTable(1)
|  |     |     |
|  |     |     +--lanEntry(1) [lanVlanId]
|  |     |        |
|  |     |        +-- r-n Integer32     lanVlanId(1)
|  |     |        +-- r-n Enumeration   lanEnable(2)
|  |     |        +-- r-n DisplayString lanName(3)
|  |     |        +-- r-n IpAddress     lanIpAddr(4)
|  |     |        +-- r-n IpAddress     lanIpMask(5)
|  |     |        +-- r-n Enumeration   lanDirectedBroadcast(6)
|  |     |        +-- r-n Enumeration   lanSourceIPOverwrite(7)
|  |     |
|  |     +--dhcpServer(4)
|  |     |  |
|  |     |  +--dhcpSrvTable(1)
|  |     |  |  |
|  |     |  |  +--dhcpSrvEntry(1) [dhcpSvrEnable]
|  |     |  |     |
|  |     |  |     +-- r-n Enumeration dhcpSvrEnable(1)
|  |     |  |     +-- r-n Integer32   dhcpSvrLeaseTime(2)
|  |     |  |     +-- r-n IpAddress   dhcpSvrDns1(3)
```

```
|  |     |  |     +-- r-n IpAddress   dhcpSvrDns2(4)
|  |     |  |     +-- r-n IpAddress   dhcpIpRangeStart(5)
|  |     |  |     +-- r-n IpAddress   dhcpIpRangeEnd(6)
|  |     |  |     +-- r-n IpAddress   dhcpNTP(7)
|  |     |  |     +-- r-n IpAddress   dhcpDefaultGateway(8)
|  |     |  |     +-- r-n IpAddress   dhcpNetmask(9)
|  |     |  |
|  |     |  +--dhcpStaticTable(8)
|  |     |  |  |
|  |     |  |  +--dhcpStaticEntry(1) [dhcpStaticEnable]
|  |     |  |     |
|  |     |  |     +-- r-n Enumeration   dhcpStaticEnable(1)
|  |     |  |     +-- r-n DisplayString dhcpStaticName(2)
|  |     |  |     +-- r-n IpAddress     dhcpStaticIp(3)
|  |     |  |     +-- r-n MacAddress    dhcpStaticMac(4)
|  |     |  |     +-- r-n Integer32     dhcpStaticLeasetime(5)
|  |     |  |     +-- r-n IpAddress     dhcpStaticDns1(6)
|  |     |  |     +-- r-n IpAddress     dhcpStaticDns2(7)
|  |     |  |     +-- r-n IpAddress     dhcpStaticNtp(8)
|  |     |  |     +-- r-n IpAddress     dhcpStaticDefaultGateway(9)
|  |     |  |     +-- r-n IpAddress     dhcpStaticNetmask(10)
|  |     |  |
|  |     |  +--dhcpSvrPipTable(9)
|  |     |     |
|  |     |     +--dhcpSvrPipEntry(1) [dhcpPipEnable]
|  |     |        |
|  |     |        +-- r-n Enumeration dhcpPipEnable(1)
|  |     |        +-- r-n Integer32   dhcpPipPortNumber(2)
|  |     |        +-- r-n IpAddress   dhcpPipIp(3)
|  |     |        +-- r-n IpAddress   dhcpPipNetmask(4)
|  |     |        +-- r-n Integer32   dhcpPipLeasetime(5)
|  |     |        +-- r-n IpAddress   dhcpPipDns1(6)
|  |     |        +-- r-n IpAddress   dhcpPipDns2(7)
|  |     |        +-- r-n IpAddress   dhcpPipNtp(8)
|  |     |        +-- r-n IpAddress   dhcpPipGateway(9)
|  |     |
|  |     +--dhcpList(5)
|  |     |  |
|  |     |  +--dhcpListTable(1)
|  |     |     |
|  |     |     +--dhcpListEntry(1) [dhcpListName]
|  |     |        |
|  |     |        +-- r-n DisplayString dhcpListName(1)
|  |     |        +-- r-n DisplayString dhcpListMac(2)
|  |     |        +-- r-n IpAddress     dhcpListAddr(3)
|  |     |
|  |     +--dhcpServerMode(8)
|  |     |  |
|  |     |  +-- r-n Enumeration dhcpServerModeStatus(1)
|  |     |
|  |     +--brigdeSetting(9)
|  |     |  |
|  |     |  +-- r-n Enumeration   bridgeEnable(1)
|  |     |  +-- r-n DisplayString bridgeName(2)
|  |     |  +-- r-n IpAddress     birdgeIpAddr(3)
|  |     |  +-- r-n IpAddress     bridgeIpMask(4)
|  |     |
|  |     +--cellularSetting(10)
|  |        |
|  |        +-- rwn Enumeration cellularEnable(1)
|  |        +-- rwn Enumeration cellularConnectionEnable(2)
|  |        |
|  |        +--cellularSimTable(3)
|  |        |  |
|  |        |  +--cellularSimEntry(1) [cellularSimIndex]
|  |        |     |
|  |        |     +-- r-n Integer32   cellularSimIndex(1)
|  |        |     +-- rwn Enumeration cellularSimEnable(2)
|  |        |     +-- rwn Enumeration cellularSimPriority(3)
|  |        |
```

```
|  |        +--guaranlinkSetting(4)
|  |        |  |
|  |        |  +-- rwn Enumeration glinkEnable(1)
|  |        |  +-- rwn Enumeration glinkCheckTiming(2)
|  |        |
|  |        +--remoteSmsSetting(5)
|  |        |  |
|  |        |  +-- rwn Enumeration remoteSmsEnable(1)
|  |        |
|  |        +--gnssSetting(6)
|  |           |
|  |           +-- rwn Enumeration   gnssEnable(1)
|  |           +-- rwn Enumeration   gnssServerEnable(2)
|  |           +-- rwn Enumeration   gnssClientEnable(3)
|  |           +-- r-n DisplayString gnssSatelliteStatus(4)
|  |           +-- r-n DisplayString gnssLongitudeStatus(5)
|  |           +-- r-n DisplayString gnssLatitudeStatus(6)
|  |
|  +--routeSetting(5)
|  |  |
|  |  +--showRoutingTable(3)
|  |     |
|  |     +--rTable(1)
|  |        |
|  |        +--rEntry(1) [rIndex]
|  |           |
|  |           +-- rwn DisplayString rType(1)
|  |           +-- rwn DisplayString rDestination(2)
|  |           +-- rwn IpAddress     rNextHop(3)
|  |           +-- rwn DisplayString rIfsName(4)
|  |           +-- rwn Integer32     rMetric(5)
|  |           +-- --- Integer32     rIndex(6)
|  |
|  +--natSetting(6)
|  |  |
|  |  +--natTable(1)
|  |     |
|  |     +--natEntry(1) [natIndex]
|  |        |
|  |        +-- r-n Integer32     natIndex(1)
|  |        +-- r-n Enumeration   natEnable(2)
|  |        +-- r-n DisplayString natDesc(3)
|  |        +-- r-n Enumeration   natMode(4)
|  |        +-- r-n Enumeration   natProtocolTcp(10)
|  |        +-- r-n Enumeration   natProtocolUdp(11)
|  |        +-- r-n Enumeration   natProtocolIcmp(12)
|  |        +-- r-n Enumeration   natNatLoopback(50)
|  |        +-- r-n Enumeration   natDoubleNat(51)
|  |        +-- r-n Integer32     natVrrpBinding(52)
|  |        +-- r-n DisplayString natOriIface(100)
|  |        +-- r-n IpAddress     natOriSrcIp1(110)
|  |        +-- r-n IpAddress     natOriSrcIp2(111)
|  |        +-- r-n IpAddress     natOriSrcMask(112)
|  |        +-- r-n Integer32     natOriSrcPort1(114)
|  |        +-- r-n Integer32     natOriSrcPort2(115)
|  |        +-- r-n IpAddress     natOriDstIp1(130)
|  |        +-- r-n IpAddress     natOriDstIp2(131)
|  |        +-- r-n IpAddress     natOriDstMask(132)
|  |        +-- r-n Integer32     natOriDstPort1(134)
|  |        +-- r-n Integer32     natOriDstPort2(135)
|  |        +-- r-n DisplayString natTransIface(150)
|  |        +-- r-n IpAddress     natTransSrcIp1(160)
|  |        +-- r-n IpAddress     natTransSrcIp2(161)
|  |        +-- r-n IpAddress     natTransSrcMask(162)
|  |        +-- r-n Enumeration   natTransSrcDyn(163)
|  |        +-- r-n Integer32     natTransSrcPort1(164)
|  |        +-- r-n Integer32     natTransSrcPort2(165)
|  |        +-- r-n IpAddress     natTransDstIp1(180)
|  |        +-- r-n IpAddress     natTransDstIp2(181)
|  |        +-- r-n IpAddress     natTransDstMask(182)
```

```
|  |        +-- r-n Integer32     natTransDstPort1(184)
|  |        +-- r-n Integer32     natTransDstPort2(185)
|  |
|  +--filterSetting(7)
|  |  |
|  |  +--firewallPolicy(1)
|  |  |  |
|  |  |  +-- r-n Enumeration firewallGlobalLogEnable(20)
|  |  |  +-- r-n Enumeration firewallGlobalMalEnable(21)
|  |  |  +-- r-n Enumeration firewallGlobalMalLevel(22)
|  |  |  +-- r-n Enumeration firewallGlobalMalFlash(23)
|  |  |  +-- r-n Enumeration firewallGlobalMalSyslog(24)
|  |  |  +-- r-n Enumeration firewallGlobalMalTrap(25)
|  |  |
|  |  +--dosSetting(2)
|  |     |
|  |     +-- r-n Enumeration dosNullScanEnable(1)
|  |     +-- r-n Enumeration dosXmasScanEnable(2)
|  |     +-- r-n Enumeration dosNmapXmasScanEnable(3)
|  |     +-- r-n Enumeration dosSynFinScanEnable(4)
|  |     +-- r-n Enumeration dosFinScanEnable(5)
|  |     +-- r-n Enumeration dosNmapIdScanEnable(6)
|  |     +-- r-n Enumeration dosSynRstScanEnable(7)
|  |     +-- r-n Enumeration dosIcmpDeathScanEnable(8)
|  |     +-- r-n Integer32   dosIcmpLimit(9)
|  |     +-- r-n Enumeration dosSynFloodScanEnable(10)
|  |     +-- r-n Integer32   dosSynLimit(11)
|  |     +-- r-n Enumeration dosArpFloodScanEnable(12)
|  |     +-- r-n Integer32   dosArpLimit(13)
|  |     +-- r-n Enumeration dosNewTCPWithoutSYNScan(14)
|  |     +-- r-n Enumeration dosUdpFloodScanEnable(15)
|  |     +-- r-n Integer32   dosUdpLimit(16)
|  |
|  +--vpnSetting(8)
|  |  |
|  |  +--vpnIpsec(1)
|  |  |  |
|  |  |  +--ipsecGlobal(1)
|  |  |  |  |
|  |  |  |  +-- r-n Enumeration ipsecGlobalState(1)
|  |  |  |  +-- r-n Enumeration ipsecGlobalNatt(2)
|  |  |  |  +-- r-n Enumeration ipsecGlobalEventLog(3)
|  |  |  |  +-- r-n Enumeration ipsecGlobalEventLogFlash(4)
|  |  |  |  +-- r-n Enumeration ipsecGlobalEventLogSyslog(5)
|  |  |  |  +-- r-n Enumeration ipsecGlobalEventLogSNMPTrap(6)
|  |  |  |
|  |  |  +--ipsecSetting(2)
|  |  |  |  |
|  |  |  |  +--ipsecSettingTable(1)
|  |  |  |     |
|  |  |  |     +--ipsecSettingEntry(1) [ipsecSettingEnable]
|  |  |  |        |
|  |  |  |        +-- r-n Enumeration   ipsecSettingEnable(1)
|  |  |  |        +-- r-n IpAddress     ipsecSettingRemoteEndIp(2)
|  |  |  |        +-- r-n Enumeration   ipsecSettingL2tp(4)
|  |  |  |        +-- r-n Enumeration   ipsecSettingPfs(5)
|  |  |  |        +-- r-n DisplayString ipsecSettingName(6)
|  |  |  |        +-- r-n Enumeration   ipsecSettingSecurityLevel(7)
|  |  |  |        +-- r-n Enumeration   ipsecConnIfs(8)
|  |  |  |        +-- r-n Enumeration   ipsecStartup(9)
|  |  |  |        +-- r-n IpAddress     ipsecLocalNetwork(10)
|  |  |  |        +-- r-n IpAddress     ipsecLocalMask(11)
|  |  |  |        +-- r-n DisplayString ipsecLocalId(13)
|  |  |  |        +-- r-n IpAddress     ipsecRemoteNetwork(14)
|  |  |  |        +-- r-n IpAddress     ipsecRemoteMask(15)
|  |  |  |        +-- r-n DisplayString ipsecRemoteId(17)
|  |  |  |        +-- r-n Enumeration   ipsecAuthMode(18)
|  |  |  |        +-- r-n DisplayString ipsecPsk(19)
|  |  |  |        +-- r-n DisplayString ipsecLocalSelectPem(20)
|  |  |  |        +-- r-n DisplayString ipsecRemoteSelectPem(21)
```

```
|  |  |  |        +-- r-n Enumeration   ipsecExchange(22)
|  |  |  |        +-- r-n Enumeration   ipsecP1Encrypt(23)
|  |  |  |        +-- r-n Enumeration   ipsecP1Ah(24)
|  |  |  |        +-- r-n Enumeration   ipsecP1Dh(25)
|  |  |  |        +-- r-n Integer32     ipsecIKELifetime(27)
|  |  |  |        +-- r-n Integer32     ipsecSaLifetime(30)
|  |  |  |        +-- r-n Enumeration   ipsecP2Encrypt(31)
|  |  |  |        +-- r-n Enumeration   ipsecP2Ah(32)
|  |  |  |        +-- r-n Enumeration   ipsecDpdAction(33)
|  |  |  |        +-- r-n Integer32     ipsecDpdDelay(34)
|  |  |  |        +-- r-n Integer32     ipsecDpdTimeout(35)
|  |  |  |        +-- r-n Enumeration   ipsecIdentityType(36)
|  |  |  |        +-- r-n Enumeration   ipsecPfsDHGroup(37)
|  |  |  |        +-- r-n DisplayString ipsecLocalSubnet(38)
|  |  |  |        +-- r-n DisplayString ipsecRemoteSubnet(39)
|  |  |  |
|  |  |  +--ipsecStatus(3)
|  |  |     |
|  |  |     +--ipsecStatusTable(1)
|  |  |        |
|  |  |        +--ipsecStatusEntry(1) [ipsecStatusIndex]
|  |  |           |
|  |  |           +-- r-n DisplayString ipsecStatusName(1)
|  |  |           +-- r-n DisplayString ipsecStatusLocSubnet(2)
|  |  |           +-- r-n IpAddress     ipsecStatusLocGateway(3)
|  |  |           +-- r-n IpAddress     ipsecStatusRemGateway(4)
|  |  |           +-- r-n DisplayString ipsecStatusRemSubnet(5)
|  |  |           +-- r-n DisplayString ipsecStatusPhase1(6)
|  |  |           +-- r-n DisplayString ipsecStatusPhase2(7)
|  |  |           +-- r-n Enumeration   ipsecl2tp(8)
|  |  |           +-- --- Integer32     ipsecStatusIndex(9)
|  |  |
|  |  +--vpnL2tp(2)
|  |     |
|  |     +-- r-n Enumeration l2tpModeWan1(1)
|  |     +-- r-n IpAddress   l2tpLocalIpWan1(2)
|  |     +-- r-n IpAddress   l2tpOfferIpStartWan1(3)
|  |     +-- r-n IpAddress   l2tpOfferIpEndWan1(4)
|  |     |
|  |     +--l2tpTable(9)
|  |        |
|  |        +--l2tpEntry(1) [l2tpLoginUserName]
|  |           |
|  |           +-- r-n DisplayString l2tpLoginUserName(1)
|  |
|  +--snmpSetting(9)
|  |  |
|  |  +--snmpSetup(1)
|  |     |
|  |     +-- r-n Enumeration   snmpVersion(1)
|  |     +-- rwn Enumeration   snmpAuthType(3)
|  |     +-- rwn Integer32     snmpAccessControl1(7)
|  |     +-- rwn Integer32     snmpAccessControl2(9)
|  |     +-- rwn DisplayString trap1ServerAddr(10)
|  |     +-- rwn DisplayString trap2ServerAddr(11)
|  |     +-- rwn DisplayString trap3ServerAddr(12)
|  |     +-- rwn Enumeration   snmpInformEnable(13)
|  |     +-- rwn DisplayString snmpReadCommunity1(14)
|  |     +-- rwn DisplayString snmpReadCommunity2(15)
|  |     +-- rwn DisplayString snmpTrapCommunity(16)
|  |     +-- rwn Enumeration   snmpTrapMode(17)
|  |     +-- r-n Enumeration   snmpAdminSecurityLevel(22)
|  |     +-- r-n Enumeration   snmpUserSecurityLevel(23)
|  |
|  +--diagnosisSetting(12)
|  |  |
|  |  +--lldpSetting(2)
|  |     |
|  |     +-- rwn Enumeration lldpEnable(1)
|  |     +-- rwn Integer32   lldpInterval(2)
```

```
|  |     +-- rwn Enumeration lldpRingPortBypass(3)
|  |
|  +--monitor(13)
|  |  |
|  |  +-- r-n Enumeration power1InputStatus(7)
|  |  +-- r-n Enumeration power2InputStatus(8)
|  |  |
|  |  +--monitorFiberCheckTable(11)
|  |     |
|  |     +--monitorFiberCheckEntry(1) [portIndex]
|  |        |
|  |        +-- r-n DisplayString fiberPort(1)
|  |        +-- r-n DisplayString fiberModelName(2)
|  |        +-- r-n DisplayString fiberWaveLength(3)
|  |        +-- r-n DisplayString fiberVoltage(4)
|  |        +-- r-n DisplayString fiberTemperature(5)
|  |        +-- r-n DisplayString fiberTempWarn(6)
|  |        +-- r-n DisplayString fiberTxPower(7)
|  |        +-- r-n DisplayString fiberTxPowerWarn(8)
|  |        +-- r-n DisplayString fiberRxPower(9)
|  |        +-- r-n DisplayString fiberRxPowerWarn(10)
|  |        +-- r-n DisplayString fiberSN(13)
|  |
|  +--systemLog(14)
|  |  |
|  |  +--syslog(2)
|  |     |
|  |     +-- r-n Enumeration   syslogServer1Enable(1)
|  |     +-- r-n DisplayString syslogServer1(2)
|  |     +-- r-n Integer32     syslogServer1Port(3)
|  |     +-- r-n Enumeration   syslogServer2Enable(4)
|  |     +-- r-n DisplayString syslogServer2(5)
|  |     +-- r-n Integer32     syslogServer2Port(6)
|  |     +-- r-n Enumeration   syslogServer3Enable(7)
|  |     +-- r-n DisplayString syslogServer3(8)
|  |     +-- r-n Integer32     syslogServer3Port(9)
|  |     +-- r-n DisplayString syslogServer1Cert(10)
|  |     +-- r-n DisplayString syslogServer2Cert(11)
|  |     +-- r-n DisplayString syslogServer3Cert(12)
|  |     +-- r-n Enumeration   syslogServer1MsgFormat(13)
|  |     +-- r-n Enumeration   syslogServer2MsgFormat(14)
|  |     +-- r-n Enumeration   syslogServer3MsgFormat(15)
|  |
|  +--networkMode(15)
|  |  |
|  |  +-- r-n Enumeration networkModeSelection(1)
|  |
|  +--routingRedundancy(16)
|  |  |
|  |  +--vrrp(1)
|  |     |
|  |     +--vrrpInterfaceTable(1)
|  |     |  |
|  |     |  +--vrrpInterfaceEntry(1) [vrrpIfIndex]
|  |     |     |
|  |     |     +-- rwn DisplayString vrrpIfName(1)
|  |     |     +-- r-n IpAddress     vrrpIfAddr(2)
|  |     |     +-- rwn Enumeration   vrrpIfEnable(3)
|  |     |     +-- rwn IpAddress     vrrpIfVirtualIp(4)
|  |     |     +-- rwn Integer32     vrrpIfRouterId(5)
|  |     |     +-- rwn Integer32     vrrpIfPriority(6)
|  |     |     +-- rwn Enumeration   vrrpIfPreemption(7)
|  |     |     +-- r-n Enumeration   vrrpIfStatus(8)
|  |     |     +-- rwn DisplayString vrrpIfTrack(9)
|  |     |     +-- rwn IpAddress     vrrpPingTrackIP(10)
|  |     |     +-- rwn Integer32     vrrpPingTrackInt(11)
|  |     |     +-- rwn Integer32     vrrpPingTimeout(12)
|  |     |     +-- rwn Integer32     vrrpPingTrackSuccess(13)
|  |     |     +-- rwn Integer32     vrrpPingTrackFailure(14)
|  |     |     +-- rwn Integer32     vrrpAdvInt(15)
```

```
|  |     |     +-- rwn Integer32     vrrpPreemptDelay(16)
|  |     |     +-- --- Integer32     vrrpIfIndex(17)
|  |     |
|  |     +-- rwn Enumeration vrrpEnable(2)
|  |
|  +--portSetting(17)
|  |  |
|  |  +--portTable(1)
|  |     |
|  |     +--portEntry(1) [portIndex]
|  |        |
|  |        +-- r-n DisplayString portDesc(1)
|  |        +-- rwn Enumeration   portEnable(2)
|  |        +-- r-n Enumeration   portSpeed(3)
|  |        +-- r-n Enumeration   portMDI(4)
|  |        +-- r-n Enumeration   portFDXFlowCtrl(5)
|  |        +-- rwn DisplayString portName(6)
|  |        +-- r-n Enumeration   portType(7)
|  |        +-- r-n Integer32     portIndex(8)
|  |
|  +--portTrunking(19)
|  |  |
|  |  +--trunkSettingTable(1)
|  |  |  |
|  |  |  +--trunkSettingEntry(1) [trunkSettingIndex]
|  |  |     |
|  |  |     +-- r-n Integer32   trunkSettingIndex(1)
|  |  |     +-- r-n Enumeration trunkType(2)
|  |  |     +-- r-n PortList    trunkMemberPorts(3)
|  |  |
|  |  +--trunkTable(2)
|  |     |
|  |     +--trunkEntry(1) [trunkIndex,trunkPort]
|  |        |
|  |        +-- r-n Integer32   trunkIndex(1)
|  |        +-- r-n Integer32   trunkPort(2)
|  |        +-- r-n Enumeration trunkStatus(3)
|  |
|  +--commRedundancy(20)
|  |  |
|  |  +--spanningTree(3)
|  |  |  |
|  |  |  +-- r-n Enumeration spanningTreeRoot(1)
|  |  |  +-- r-n Enumeration spanningTreeBridgePriority(2)
|  |  |  +-- r-n Integer32   spanningTreeHelloTime(3)
|  |  |  +-- r-n Integer32   spanningTreeMaxAge(4)
|  |  |  +-- r-n Integer32   spanningTreeForwardingDelay(5)
|  |  |  |
|  |  |  +--spanningTreeTable(6)
|  |  |     |
|  |  |     +--spanningTreeEntry(1) [enableSpanningTree]
|  |  |        |
|  |  |        +-- r-n Enumeration enableSpanningTree(2)
|  |  |        +-- r-n Enumeration spanningTreePortPriority(3)
|  |  |        +-- r-n Integer32   spanningTreePortCost(4)
|  |  |        +-- r-n Enumeration spanningTreePortStatus(5)
|  |  |        +-- r-n Enumeration spanningTreePortEdge(6)
|  |  |
|  |  +-- r-n Enumeration activeProtocolOfRedundancy(4)
|  |  |
|  |  +--turboRingV2(5)
|  |  |  |
|  |  |  +--turboRingV2Ring1(1)
|  |  |  |  |
|  |  |  |  +-- r-n Integer32   ringIndexRing1(1)
|  |  |  |  +-- r-n Enumeration ringEnableRing1(2)
|  |  |  |  +-- r-n Enumeration masterSetupRing1(3)
|  |  |  |  +-- r-n Enumeration masterStatusRing1(4)
|  |  |  |  +-- r-n MacAddress  designatedMasterRing1(5)
|  |  |  |  +-- r-n Integer32   rdnt1stPortRing1(6)
```

```
|  |  |  |  +-- r-n Enumeration rdnt1stPortStatusRing1(7)
|  |  |  |  +-- r-n Integer32   rdnt2ndPortRing1(8)
|  |  |  |  +-- r-n Enumeration rdnt2ndPortStatusRing1(9)
|  |  |  |  +-- r-n Enumeration brokenStatusRing1(10)
|  |  |  |
|  |  |  +--turboRingV2Ring2(2)
|  |  |  |  |
|  |  |  |  +-- r-n Integer32   ringIndexRing2(1)
|  |  |  |  +-- r-n Enumeration ringEnableRing2(2)
|  |  |  |  +-- r-n Enumeration masterSetupRing2(3)
|  |  |  |  +-- r-n Enumeration masterStatusRing2(4)
|  |  |  |  +-- r-n MacAddress  designatedMasterRing2(5)
|  |  |  |  +-- r-n Integer32   rdnt1stPortRing2(6)
|  |  |  |  +-- r-n Enumeration rdnt1stPortStatusRing2(7)
|  |  |  |  +-- r-n Integer32   rdnt2ndPortRing2(8)
|  |  |  |  +-- r-n Enumeration rdnt2ndPortStatusRing2(9)
|  |  |  |  +-- r-n Enumeration brokenStatusRing2(10)
|  |  |  |
|  |  |  +--turboRingV2Coupling(3)
|  |  |     |
|  |  |     +-- r-n Enumeration couplingEnable(1)
|  |  |     +-- r-n Enumeration couplingMode(2)
|  |  |     +-- r-n Integer32   coupling1stPort(3)
|  |  |     +-- r-n Enumeration coupling1stPortStatus(4)
|  |  |     +-- r-n Integer32   coupling2ndPort(5)
|  |  |     +-- r-n Enumeration coupling2ndPortStatus(6)
|  |  |
|  |  +--turboChain(6)
|  |     |
|  |     +-- rwn Enumeration turboChainRole(1)
|  |     +-- rwn Integer32   turboChainPort1(2)
|  |     +-- rwn Integer32   turboChainPort2(3)
|  |     +-- r-n Enumeration turboChainPort1Status(4)
|  |     +-- r-n Enumeration turboChainPort2Status(5)
|  |
|  +--vlan(21)
|  |  |
|  |  +--vlanPortSettingTable(1)
|  |  |  |
|  |  |  +--vlanPortSettingEntry(1) [portIndex]
|  |  |     |
|  |  |     +-- r-n Enumeration   portVlanType(1)
|  |  |     +-- r-n Integer32     portDefaultVid(2)
|  |  |     +-- r-n DisplayString portFixedVid(3)
|  |  |     +-- r-n DisplayString portFixedVidUntag(5)
|  |  |
|  |  +--vlanTable(2)
|  |  |  |
|  |  |  +--vlanEntry(1) [vlanId]
|  |  |     |
|  |  |     +-- r-n Integer32 vlanId(1)
|  |  |     +-- r-n PortList  joinedAccessPorts(2)
|  |  |     +-- r-n PortList  joinedTrunkPorts(3)
|  |  |     +-- r-n PortList  joinedHybirdPorts(4)
|  |  |
|  |  +-- r-n Integer32   managementVlanId(3)
|  |  +-- r-n Enumeration vlanType(4)
|  |
|  +--swMgmtGroup(22)
|  |  |
|  |  +-- r-n Integer32     numberOfPorts(1)
|  |  +-- r-n DisplayString switchModel(2)
|  |  +-- r-n DisplayString firmwareVersion(4)
|  |
|  +--globalStatus(23)
|  |  |
|  |  +-- r-n Enumeration firewallGlobalStatus(1)
|  |  +-- r-n Enumeration natGlobalStatus(2)
|  |  +-- r-n Enumeration vpnGlobalStatus(3)
|  |  +-- r-n Enumeration securityNotificationFirewallStatus(4)
```

```
|  |  +-- r-n Enumeration securityNotificationDoSAttackStatus(5)
|  |  +-- r-n Enumeration securityNotificationAccessViolationStatus(6)
|  |  +-- r-n Enumeration securityNotificationLoginFailStatus(7)
|  |  +-- r-n Enumeration defaultPasswordChange(8)
|  |  +-- r-n Enumeration securityNotificationDeviceLockdownStatus(9)
|  |  +-- r-n Enumeration securityNotificationLayer3FilterStatus(10)
|  |
|  +--interfaceStatus(24)
|  |  |
|  |  +--interfaceStatusTable(1)
|  |  |  |
|  |  |  +--interfaceStatusEntry(1) [interfaceOverallStatus]
|  |  |     |
|  |  |     +-- r-n DisplayString interfaceOverallStatus(1)
|  |  |     +-- r-n Enumeration   interfaceOverallType(2)
|  |  |
|  |  +--cellularStatus(2)
|  |     |
|  |     +-- r-n DisplayString cellularMode(1)
|  |     +-- r-n DisplayString cellularCarrier(2)
|  |     +-- r-n DisplayString cellularRSSI(3)
|  |     +-- r-n DisplayString cellularIP(4)
|  |     +-- r-n DisplayString cellularIMEI(5)
|  |     +-- r-n DisplayString cellularIMSI(6)
|  |     +-- r-n Enumeration   cellularConnectionStatus(7)
|  |     +-- r-n DisplayString cellularSim1Status(8)
|  |     +-- r-n DisplayString cellularSim2Status(9)
|  |     +-- r-n DisplayString cellularRSRP(10)
|  |     +-- r-n DisplayString cellularRSRQ(11)
|  |     +-- r-n DisplayString cellularSINR(12)
|  |
|  +--securityNotification(25)
|  |  |
|  |  +-- r-n Enumeration eventFirewall(1)
|  |  +-- r-n Enumeration eventDoSAttack(2)
|  |  +-- r-n Enumeration eventAccessViolation(3)
|  |  +-- r-n Enumeration eventLoginFail(4)
|  |  +-- r-n Enumeration eventDeviceLockdown(5)
|  |  +-- r-n Enumeration eventLayer3Filter(6)
|  |
|  +--mtuAdjustment(28)
|  |  |
|  |  +--mtuAdjustmentTable(1)
|  |     |
|  |     +--mtuAdjustmentEntry(1) [mtuAdjustmentIndex]
|  |        |
|  |        +-- r-n DisplayString mtuAdjustmentIfName(1)
|  |        +-- rwn Integer32     mtuAdjustmentMTUsize(2)
|  |        +-- rwn Enumeration   mtuAdjustmentPRPtraffic(3)
|  |        +-- --- Integer32     mtuAdjustmentIndex(4)
|  |
|  +--poeSetting(40)
|  |  |
|  |  +--poePortTable(3)
|  |  |  |
|  |  |  +--poePortEntry(1) [poePortIndex]
|  |  |     |
|  |  |     +-- r-n Integer32     poePortIndex(1)
|  |  |     +-- rwn Enumeration   poePortEnable(2)
|  |  |     +-- rwn Integer32     powerLimit(4)
|  |  |     +-- rwn Enumeration   pdfailure(5)
|  |  |     +-- rwn DisplayString pdipaddr(6)
|  |  |     +-- rwn Integer32     pdPollingInterval(7)
|  |  |     +-- rwn Enumeration   poePortLegacyPdDetect(9)
|  |  |     +-- rwn Integer32     pdNoResponseTimeout(10)
|  |  |     +-- rwn Enumeration   pdNoResponseAction(11)
|  |  |     +-- rwn Enumeration   poePowerOutputMode(12)
|  |  |
|  |  +--poeStatusTable(6)
|  |  |  |
```

```
|  |  |  +--poeStatusEntry(1) [poePortIndex]
|  |  |     |
|  |  |     +-- r-n Enumeration poePortStatus(1)
|  |  |     +-- r-n Enumeration poePortConsumption(2)
|  |  |     +-- r-n Enumeration poePortVoltage(3)
|  |  |     +-- r-n Enumeration poePortCurrent(4)
|  |  |     +-- r-n Enumeration poePortPowerOutput(5)
|  |  |     +-- r-n Enumeration poePortClass(6)
|  |  |     +-- r-n Enumeration poePortPdFailCheck(7)
|  |  |     +-- r-n Enumeration poePortPdStatusDescription(8)
|  |  |
|  |  +--poeSystemSetting(9)
|  |     |
|  |     +-- rwn Enumeration poeSysPowerEnable(1)
|  |     +-- rwn Integer32   poeSysPowerThreshold(2)
|  |     +-- rwn Enumeration poeSysThresholdCutOff(3)
|  |     +-- r-n Integer32   poeSysAllocatedPower(4)
|  |     +-- r-n Integer32   poeSysMeasuredPower(5)
|  |     +-- rwn Integer32   poeSysPowerBudget(7)
|  |
|  +--eventlog(46)
|  |  |
|  |  +--eventlogSystem(1)
|  |  |  |
|  |  |  +--eventlogSystemTable(1)
|  |  |  |  |
|  |  |  |  +--eventlogSystemEntry(1) [eventlogSystemIndex]
|  |  |  |     |
|  |  |  |     +-- r-n Integer32     eventlogSystemIndex(1)
|  |  |  |     +-- r-n DisplayString eventlogSystemTimestamp(2)
|  |  |  |     +-- r-n Integer32     eventlogSystemSeverity(3)
|  |  |  |     +-- r-n DisplayString eventlogSystemEvent(4)
|  |  |  |
|  |  |  +-- rwn Enumeration eventlogSystemClear(2)
|  |  |
|  |  +--eventlogVPN(2)
|  |  |  |
|  |  |  +--eventlogVPNTable(1)
|  |  |  |  |
|  |  |  |  +--eventlogVPNEntry(1) [eventlogVPNIndex]
|  |  |  |     |
|  |  |  |     +-- r-n Integer32     eventlogVPNIndex(1)
|  |  |  |     +-- r-n DisplayString eventlogVPNTimestamp(2)
|  |  |  |     +-- r-n Integer32     eventlogVPNSeverity(3)
|  |  |  |     +-- r-n DisplayString eventlogVPNEvent(4)
|  |  |  |
|  |  |  +-- rwn Enumeration eventlogVPNClear(2)
|  |  |
|  |  +--eventlogTruseAccess(3)
|  |  |  |
|  |  |  +--eventlogTruseAccessTable(1)
|  |  |  |  |
|  |  |  |  +--eventlogTruseAccessEntry(1) [eventlogTruseAccessIndex]
|  |  |  |     |
|  |  |  |     +-- r-n Integer32     eventlogTruseAccessIndex(1)
|  |  |  |     +-- r-n DisplayString eventlogTruseAccessTimestamp(2)
|  |  |  |     +-- r-n Integer32     eventlogTruseAccessSeverity(3)
|  |  |  |     +-- r-n DisplayString eventlogTruseAccessEvent(4)
|  |  |  |
|  |  |  +-- rwn Enumeration eventlogTruseAccessClear(2)
|  |  |
|  |  +--eventlogMalformed(4)
|  |  |  |
|  |  |  +--eventlogMalformedTable(1)
|  |  |  |  |
|  |  |  |  +--eventlogMalformedEntry(1) [eventlogMalformedIndex]
|  |  |  |     |
|  |  |  |     +-- r-n Integer32     eventlogMalformedIndex(1)
|  |  |  |     +-- r-n DisplayString eventlogMalformedTimestamp(2)
|  |  |  |     +-- r-n Integer32     eventlogMalformedSeverity(3)
```

```
      |  |  |  |     +-- r-n DisplayString eventlogMalformedEvent(4)
      |  |  |  |
      |  |  |  +-- rwn Enumeration eventlogMalformedClear(2)
      |  |  |
      |  |  +--eventlogDOS(5)
      |  |  |  |
      |  |  |  +--eventlogDOSTable(1)
      |  |  |  |  |
      |  |  |  |  +--eventlogDOSEntry(1) [eventlogDOSIndex]
      |  |  |  |     |
      |  |  |  |     +-- r-n Integer32     eventlogDOSIndex(1)
      |  |  |  |     +-- r-n DisplayString eventlogDOSTimestamp(2)
      |  |  |  |     +-- r-n Integer32     eventlogDOSSeverity(3)
      |  |  |  |     +-- r-n DisplayString eventlogDOSEvent(4)
      |  |  |  |
      |  |  |  +-- rwn Enumeration eventlogDOSClear(2)
      |  |  |
      |  |  +--eventlogDevLockdown(6)
      |  |  |  |
      |  |  |  +--eventlogDevLockdownTable(1)
      |  |  |  |  |
      |  |  |  |  +--eventlogDevLockdownEntry(1) [eventlogDevLockdownIndex]
      |  |  |  |     |
      |  |  |  |     +-- r-n Integer32     eventlogDevLockdownIndex(1)
      |  |  |  |     +-- r-n DisplayString eventlogDevLockdownTimestamp(2)
      |  |  |  |     +-- r-n Integer32     eventlogDevLockdownSeverity(3)
      |  |  |  |     +-- r-n DisplayString eventlogDevLockdownEvent(4)
      |  |  |  |
      |  |  |  +-- rwn Enumeration eventlogDevLockdownClear(2)
      |  |  |
      |  |  +--eventlogL3Policy(7)
      |  |  |  |
      |  |  |  +--eventlogL3PolicyTable(1)
      |  |  |  |  |
      |  |  |  |  +--eventlogL3PolicyEntry(1) [eventlogL3PolicyIndex]
      |  |  |  |     |
      |  |  |  |     +-- r-n Integer32     eventlogL3PolicyIndex(1)
      |  |  |  |     +-- r-n DisplayString eventlogL3PolicyTimestamp(2)
      |  |  |  |     +-- r-n Integer32     eventlogL3PolicySeverity(3)
      |  |  |  |     +-- r-n DisplayString eventlogL3PolicyEvent(4)
      |  |  |  |
      |  |  |  +-- rwn Enumeration eventlogL3PolicyClear(2)
      |  |  |
      |  |  +--eventlogProtocolFilterPolicy(8)
      |  |  |  |
      |  |  |  +--eventlogProtocolFilterPolicyTable(1)
      |  |  |  |  |
      |  |  |  |  +--eventlogProtocolFilterPolicyEntry(1)
   [eventlogProtocolFilterPolicyIndex]
      |  |  |  |     |
      |  |  |  |     +-- r-n Integer32     eventlogProtocolFilterPolicyIndex(1)
      |  |  |  |     +-- r-n DisplayString eventlogProtocolFilterPolicyTimestamp(2)
      |  |  |  |     +-- r-n Integer32     eventlogProtocolFilterPolicySeverity(3)
      |  |  |  |     +-- r-n DisplayString eventlogProtocolFilterPolicyEvent(4)
      |  |  |  |
      |  |  |  +-- rwn Enumeration eventlogProtocolFilterPolicyClear(2)
      |  |  |
      |  |  +--eventlogADP(9)
      |  |  |  |
      |  |  |  +--eventlogADPTable(1)
      |  |  |  |  |
      |  |  |  |  +--eventlogADPEntry(1) [eventlogADPIndex]
      |  |  |  |     |
      |  |  |  |     +-- r-n Integer32     eventlogADPIndex(1)
      |  |  |  |     +-- r-n DisplayString eventlogADPTimestamp(2)
      |  |  |  |     +-- r-n Integer32     eventlogADPSeverity(3)
      |  |  |  |     +-- r-n DisplayString eventlogADPEvent(4)
      |  |  |  |
      |  |  |  +-- rwn Enumeration eventlogADPClear(2)
      |  |  |
```

```
|   |  +--eventlogIPS(10)
|   |  |  |
|   |  |  +--eventlogIPSTable(1)
|   |  |  |  |
|   |  |  |  +--eventlogIPSEntry(1) [eventlogIPSIndex]
|   |  |  |     |
|   |  |  |     +-- r-n Integer32     eventlogIPSIndex(1)
|   |  |  |     +-- r-n DisplayString eventlogIPSTimestamp(2)
|   |  |  |     +-- r-n Integer32     eventlogIPSSeverity(3)
|   |  |  |     +-- r-n DisplayString eventlogIPSEvent(4)
|   |  |  |  |
|   |  |  |  +-- rwn Enumeration eventlogIPSClear(2)
|   |  |  |
|   |  |  +--eventlogSessionControl(11)
|   |  |  |  |
|   |  |  |  +--eventlogSessionControlTable(1)
|   |  |  |  |  |
|   |  |  |  |  +--eventlogSessionControlEntry(1) [eventlogSessionControlIndex]
|   |  |  |  |     |
|   |  |  |  |     +-- r-n Integer32     eventlogSessionControlIndex(1)
|   |  |  |  |     +-- r-n DisplayString eventlogSessionControlTimestamp(2)
|   |  |  |  |     +-- r-n Integer32     eventlogSessionControlSeverity(3)
|   |  |  |  |     +-- r-n DisplayString eventlogSessionControlEvent(4)
|   |  |  |  |  |
|   |  |  |  |  +-- rwn Enumeration eventlogSessionControlClear(2)
|   |  |  |  |
|   |  |  +--eventlogL2Filter(12)
|   |  |  |  |
|   |  |  |  +--eventlogL2FilterTable(1)
|   |  |  |  |  |
|   |  |  |  |  +--eventlogL2FilterEntry(1) [eventlogL2FilterIndex]
|   |  |  |  |     |
|   |  |  |  |     +-- r-n Integer32     eventlogL2FilterIndex(1)
|   |  |  |  |     +-- r-n DisplayString eventlogL2FilterTimestamp(2)
|   |  |  |  |     +-- r-n Integer32     eventlogL2FilterSeverity(3)
|   |  |  |  |     +-- r-n DisplayString eventlogL2FilterEvent(4)
|   |  |  |  |  |
|   |  |  |  |  +-- rwn Enumeration eventlogL2FilterClear(2)
|   |  |  |  |
|   |  |  +--eventlogPingResponse(15)
|   |  |     |
|   |  |     +--eventlogPingResponseTable(1)
|   |  |     |  |
|   |  |     |  +--eventlogPingResponseEntry(1) [eventlogPingResponseIndex]
|   |  |     |     |
|   |  |     |     +-- r-n Integer32     eventlogPingResponseIndex(1)
|   |  |     |     +-- r-n DisplayString eventlogPingResponseTimestamp(2)
|   |  |     |     +-- r-n Integer32     eventlogPingResponseSeverity(3)
|   |  |     |     +-- r-n DisplayString eventlogPingResponseEvent(4)
|   |  |     |
|   |  |     +-- rwn Enumeration eventlogPingResponseClear(2)
|   |  |
|   |  +-- r-n Integer32     cpuLoading5s(53)
|   |  +-- r-n Integer32     cpuLoading30s(54)
|   |  +-- r-n Integer32     cpuLoading300s(55)
|   |  +-- r-n Integer32     totalMemory(56)
|   |  +-- r-n Integer32     freeMemory(57)
|   |  +-- r-n Integer32     usedMemory(58)
|   |  +-- r-n Integer32     memoryUsage(59)
|   |  |
|   |  +--managementInterface(63)
|   |  |  |
|   |  |  +-- rwn Enumeration   httpEnable(1)
|   |  |  +-- rwn Integer32     httpPort(2)
|   |  |  +-- rwn Enumeration   sslEnable(3)
|   |  |  +-- rwn Integer32     sslPort(4)
|   |  |  +-- rwn Enumeration   telnetEnable(5)
|   |  |  +-- rwn Integer32     telnetPort(6)
|   |  |  +-- rwn Enumeration   sshEnable(7)
|   |  |  +-- rwn Integer32     sshPort(8)
```

```
|  |  +-- rwn Integer32     mgmtInterfaceAutoLogout(9)
|  |  +-- r-n DisplayString moxaUtilityServicePort(13)
|  |  +-- rwn Integer32     httpMaxLoginUsers(14)
|  |  +-- rwn Integer32     telnetMaxLoginUsers(15)
|  |  +-- rwn Enumeration   moxaUtilityServiceEnable(16)
|  |
|  +--pingResponse(64)
|  |  |
|  |  +--pingResponsePolicyTable(1)
|  |  |  |
|  |  |  +--pingResponsePolicyEntry(1) [pingResponsePolicyIndex]
|  |  |     |
|  |  |     +-- r-n Integer32     pingResponsePolicyIndex(1)
|  |  |     +-- r-n Enumeration   pingResponsePolicyExist(2)
|  |  |     +-- r-n Enumeration   pingResponsePolicyEnable(3)
|  |  |     +-- r-n DisplayString pingResponsePolicyIf(4)
|  |  |     +-- r-n Enumeration   pingResponsePolicyIpType(5)
|  |  |     +-- r-n IpAddress     pingResponsePolicyIp(6)
|  |  |     +-- r-n IpAddress     pingResponsePolicyMask(7)
|  |  |     +-- r-n Enumeration   pingResponsePolicyAction(8)
|  |  |
|  |  +-- rwn Enumeration pingResponseIfEnable(2)
|  |  |
|  |  +--pingResponseIfTable(3)
|  |  |  |
|  |  |  +--pingResponseIfEntry(1) [pingResponseIf]
|  |  |     |
|  |  |     +-- rwn DisplayString pingResponseIf(1)
|  |  |
|  |  +-- rwn Enumeration pingResponslLogEnable(4)
|  |  +-- rwn Enumeration pingResponslLogLevel(5)
|  |  +-- rwn Enumeration pingResponslLogFlash(6)
|  |  +-- rwn Enumeration pingResponslLogSyslog(7)
|  |  +-- rwn Enumeration pingResponslLogTrap(8)
|  |
|  +--passwordPolicy(70)
|  |  |
|  |  +-- rwn Integer32   pwdMinLength(1)
|  |  +-- rwn Enumeration pwdComplexityCheckEnable(2)
|  |  +-- rwn Enumeration pwdComplexityCheckDigitEnable(3)
|  |  +-- rwn Enumeration pwdComplexityCheckAlphabetEnable(4)
|  |  +-- rwn Enumeration pwdComplexityCheckSpecialCharEnable(5)
|  |
|  +--loginLockout(71)
|  |  |
|  |  +-- rwn Enumeration loginFailureLockoutEnable(1)
|  |  +-- rwn Integer32   loginFailureLockoutRetrys(2)
|  |  +-- rwn Integer32   loginFailureLockoutTime(3)
|  |
|  +--systemNotifyMessage(72)
|  |  |
|  |  +-- r-n DisplayString httpLoginMessage(1)
|  |  +-- r-n DisplayString httpLoginFailureMessage(2)
|  |
|  +-- r-n DisplayString serialNumber(78)
|  +-- r-n Enumeration   configEncryptEnable(79)
|  |
|  +--security(80)
|  |  |
|  |  +--portAccessControl(2)
|  |     |
|  |     +--dot1x(2)
|  |        |
|  |        +-- rwn Enumeration dataBaseOption(1)
|  |        +-- rwn Enumeration dot1xReauthEnable(5)
|  |        +-- rwn Integer32   dot1xReauthPeriod(6)
|  |        |
|  |        +--dot1xSettingTable(7)
|  |        |  |
|  |        |  +--dot1xSettingEntry(1) [portIndex]
```

```
|  |        |     |
|  |        |     +-- rwn Enumeration enableDot1X(1)
|  |        |
|  |        +--dot1xReauthTable(8)
|  |        |  |
|  |        |  +--dot1xReauthEntry(1) [dot1xReauthPortIndex]
|  |        |     |
|  |        |     +-- r-n Integer32   dot1xReauthPortIndex(1)
|  |        |     +-- rwn Enumeration dot1xReauth(2)
|  |        |
|  |        +--dot1xRadius(9)
|  |           |
|  |           +-- rwn DisplayString dot1x1stRadiusServer(2)
|  |           +-- rwn Integer32     dot1x1stRadiusPort(3)
|  |           +-- rwn DisplayString dot1x1stRadiusSharedKey(4)
|  |           +-- rwn DisplayString dot1x2ndRadiusServer(5)
|  |           +-- rwn Integer32     dot1x2ndRadiusPort(6)
|  |           +-- rwn DisplayString dot1x2ndRadiusSharedKey(7)
|  |
|  +--powerMgmtSetting(81)
|  |  |
|  |  +-- rwn Enumeration powerMgmtEnable(1)
|  |
|  +--serialSetting(82)
|  |  |
|  |  +-- rwn Enumeration serialPort(1)
|  |  +-- rwn Enumeration serialPortIfType(2)
|  |  +-- rwn Enumeration serialPortOpMode(3)
|  |  +-- rwn Enumeration serialDataLog(4)
|  |  +-- rwn Enumeration serialPortBuffer(5)
|  |
|  +--linkFaultPassthrough(83)
|  |  |
|  |  +-- rwn Enumeration lfpState(1)
|  |  +-- rwn Integer32   lfpPort1(2)
|  |  +-- rwn Integer32   lfpPort2(3)
|  |
|  +--softLockdownModeStatus(84)
|     |
|     +-- r-n Enumeration softLockdownModeStatusStatus(1)
|     +-- r-n Enumeration softLockdownModeStatusTr2(2)
|     +-- r-n Enumeration softLockdownModeStatusDhcpSvr(3)
|     +-- r-n Enumeration softLockdownModeStatusDhcpRelayAgent(4)
|     +-- r-n Enumeration softLockdownModeStatusSnmpSvr(5)
|
+--mibNotificationsPrefix(3)
   |
   +--configChangeTrap(1) [varconfigChangeTrap]
   |
   +--power1Trap(2) [varpower1Trap]
   |
   +--power2Trap(3) [varpower2Trap]
   |
   +--di1Trap(4) [vardi1Trap]
   |
   +--di2Trap(5) [vardi2Trap]
   |
   +--redundancyTopologyChangedTrap(10) [varredundancyTopologyChangedTrap]
   |
   +--turboRingCouplingPortChangedTrap(11) [varturboRingCouplingPortChangedTrap]
   |
   +--turboRingMasterChangedTrap(12) [varturboRingMasterChangedTrap]
   |
   +--vpnConnectedTrap(40) [varVPNConnectedTrap]
   |
   +--vpnDisconnectedTrap(41) [varVPNDisconnectedTrap]
   |
   +--firewallPolicyTrap(50) [varFirewallPolicyTrap]
   |
   +--securityNotificationTrap(51) [varSecurityNotificationTrap]
```

```
        |
        +--loggingCapacityTrap(52) [varLoggingCapacityTrap]
```

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
10	defineNamedVariable
11	defineNamedVariableList
12	defineScatteredAccess
13	defineSemaphore
14	deleteDomain
15	deleteEventAction
16	deleteEventCondition
17	deleteEventEnrollment
18	deleteJournal
19	deleteNamedType
20	deleteNamedVariableList

Service Operation	Service Operation Name
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
38	getEventEnrollmentAttributes
39	getNamedTypeAttributes
40	getNamedVariableListAttributes
41	getNameList
42	getProgramInvocationAttributes
43	getScatteredAccessAttributes

Service Operation	Service Operation Name
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
66	reportSemaphoreStatus

Service Operation	Service Operation Name
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

Sample Local Consist Info File

The following example provides a copy-and-paste compatible Local Consist Info File for use with ETBN examples. This example assumes a single consist. Further modifications may be required for multi-consist examples.

Refer to Structure and Syntax of Local Consist Info Files for more information about XML configuration files.

```
<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE consistinfo SYSTEM
"consistinfo.dtd"><consistinfo>    <cstId>consist1</cstId>
                <cstOwner>Moxa</cstOwner>          <cstType>Regional
train</cstType>  <vehicleinfo tractVeh="false">
                <cstVehNo>1</cstVehNo>
                <vehId>vehicle1</vehId>
                <vehOrient>same</vehOrient>
                <vehType>Passenger vehicle</vehType>
                <functioninfo>
                <cnId>1</cnId>
                <fctId>112</fctId>
                <fctName>devECSC</fctName>
                </functioninfo>                    <functioninfo>
                                <cnId>1</cnId>
                <fctId>11</fctId>
                <fctName>devCam1</fctName>
                </functioninfo>                    <functioninfo>
                                <cnId>1</cnId>
                <fctId>20</fctId>
                <fctName>grpDoor</fctName>
                </functioninfo>                    <functioninfo>
                                <cnId>1</cnId>
                <fctId>30</fctId>
                <fctName>grpDoor1</fctName>
                </functioninfo>  </vehicleinfo></consistinfo>
```

This page explains security practices for installing, operating, maintaining, and decommissioning the device. We strongly recommend that our customers follow these guidelines to enhance network and equipment security.

Installation

Physical Installation

1. The device MUST be installed in an access-controlled area, where only the necessary personnel have physical access to the device.
2. The device MUST be installed at the security perimeter or the boundary between different zones to provide network segmentation.
3. Please follow the instructions in the Quick Installation Guide, which is included in the package, to ensure you install the device correctly in your environment.
4. The device has anti-tamper labels on the enclosures. This allows an administrator to tell whether the device has been tampered with.
5. The ports that are not in use should be deactivated. Please refer to the Ports section for detailed instructions.

Acoount Management

Follow these best practices when setting up an account:
1. Each account should be assigned the correct privileges: Only allow the minimum number of people to have admin privilege so they can perform device configuration or modifications, while other users should only have read access privilege. The device supports both local account authentication and a remote centralized mechanism, including RADIUS.
2. Change the default password, and strengthen the account password complexity by:
   a. Enabling the “Password Policy” function.
   b. Increasing the minimum password length to at least eight characters.
   c. Defining a password policy to ensure that it contains at least an uppercase and lowercase letter, a digit, and a special character.
   d. Setting user passwords to expire after a certain period of time.
3. Enforce regulations that ensure that only a trusted host can access the device. Please refer to the Trusted Access section for detailed instructions.

Vulnerable Network Ports

1. For network security concerns, we strongly recommend that you change the port numbers, such as TCP port numbers for HTTP, HTTPS, Telnet, and SSH, for the protocols that are in use. Ports that are not in use but are still reachable pose an unacceptable security risk and should be disabled. Refer to the Management Interface section for detailed instructions.
2. In order to avoid eavesdroppers from snooping confidential information, users should adopt encryptionbased communication protocols, such as HTTPS instead of HTTP, SSH instead of Telnet, SFTP instead of TFTP, SNMPv3 instead of SNMPv1/v2c, etc. In addition, the maximum n umber of sessions should be kept to an absolute minimum. Please refer to the Management Interface section for detailed instructions.

3. Users should generate the SSL certificate for the device before commissioning HTTPS or SSH applications. Please refer to the SSH & SSL section for detailed instructions.

Operation

In order to ensure that communications are properly protected, use a strong cryptographic algorithm for key exchange or encryption protocols for HTTPS/SSH applications. The device follows the NIST SP800- 52 and SP800-131 standards and supports TLS v1.2 and v1.3 with the following cipher suites:

TLS V1.2

Cypher Suite Name	Key Exchange	Authentication	Encryption	Hash Function
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE	RSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE	ECDSA	AES128	SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE	RSA	AES128	SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE	RSA	AES256	SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Ephemeral DH	RSA	AES128	SHA256

Cypher Suite Name	Key Exchange	Authentication	Encryption	Hash Function
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Ephemeral DH	RSA	AES256	SHA384
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Ephemeral DH	RSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE_RSA_WITH_AES256_SHA384	ECDHE	RSA	AES256	SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE	RSA	AES128	SHA256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE	ECDSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE	RSA	AES256	SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE	ECDSA	AES256	SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE	ECDSA	AES128	SHA256

TLS V1.3

Cypher Suite Name	Key Exchange	Authentication	Encryption	Hash Function
TLS_AES_256_GCM_SHA384	Any	N/A	AES256 GCM	SHA384
TLS_CHACHA20_POLY1305_SHA256	Any	N/A	CHACHA20-POLY1305	SHA256
TLS_AES_128_GCM_SHA256	Any	N/A	AES128 GCM	SHA256

2. Below is a list of the recommended secure browsers that support TLS v1.2 or above:

Browser	Version
Microsoft Edge	All
Microsoft Internet Explorer	v11 or above
Mozilla Firefox	v27 or above

Browser	Version
Google Chrome	v38 or above
Apple Safari	v7 or above

Reference: https://support.globalsign.com/ssl/general-ssl/tls-protocol-compatibility#Browsers

The device supports event logs and syslog for SIEM integration:
a. Event log: Due to limited storage capacity, the event log can only accommodate a maximum of 1,000 entries per category. Administrators can set a warning for a pre-defined threshold. We that users regularly back up system event logs. Please refer to the Event Log section for
detailed instructions.
b. Syslog: the device supports syslog, and advanced secure TLS-based syslog for centralized SIEM integration. Please refer to the Syslog section for detailed instructions.

4. The device can provide information for control system inventory:
a. SNMPv1, v2c, v3: We recommend administrators use SNMPv3 with authentication and encryption to manage the network. Please refer to the SNMP for detailed instructions.
b. Telnet/SSH: We recommend that administrators use SSH with authentication and encryption to retrieve device properties.
c. HTTP/HTTPS: We recommend that administrators use HTTPS with a certificate that has been granted by a Certificate Authority to configure the device.

5. Denial of Service protection: To avoid disruption of the normal operation of the router, administrators should configure the QoS and DoS policy functions. The device supports ingress rate limiting and egress shaper. Administrators can decide how to deal with excess data flow and configure the device accordingly. This process will regulate the resulted data rate per port. Please refer to the QoS section for detailed instructions. Furthermore, the device provides 9 different DoS functions for detecting or defining abnormal packet formats or traffic flows. Please refer to the DoS (Denial of Service) Policy section for detailed instructions.

6. Time synchronization with authentication: Time synchronization is crucial for process control. To prevent malicious attacks whereby the settings are changed without permission, authentication must be in place between the NTP server and client. The

device supports NTP with a pre-shared key. Please refer to the Time section for detailed instructions.

7. Periodically regenerate the SSH and SSL certificates: Even though the device supports RSA 2048-bit and SHA-256 to ensure sufficient complexity, we strongly recommend that users frequently renew their SSH key and SSL certificate in case the key is compromised. Please refer to the SSH & SSL section fordetailed instructions.

8. Below is the list for the protocol port numbers used for all external interfaces:

Protocol	Service Type	Port Number
TCP	SSH	22
TCP	Telnet	23
TCP	HTTP	80
TCP	HTTPS	443
UDP	DHCP	67
UDP	NTP	123
UDP	SNMP	161
UDP	Moxa Service	40404

Maintenance

1. Perform firmware upgrades frequently to enhance features, deploy security patches, or fix bugs.
2. Frequently back up the system configurations: In order to properly protect the system configuration files from being tampered with, the device supports password encryption and signature authentication for backup files.
3. Examine event logs frequently to detect any anomalies.
4. 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.

Decommission

To avoid any sensitive information such as your account password or certificate from being disclosed, always reset the system settings to factory default before decommissioning the device.

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
Notice	Normal but significant condition
Infomational	Informational messages
Debug	Debug-level messages

System Event List

This is a list of system events and their descriptions.

Group	System Event	Description
General	Cold Start	Power was cut off and then reconnected.
General	Warm Start	The device was rebooted, such as when network parameters are changed (IP address, netmask, etc.).
General	Power 1 Transition (On->Off)	The device's power 1 is powered down.
General	Power 1 Transition (Off->On)	The device's power 1 is powered up.
General	Power 2 Transition (On->Off)	The device's power 2 is powered down.
General	Power 2 Transition (Off->On)	The device's power 2 is powered up.
General	Digital Input Transition (On->Off)	The device's input is turning off.
General	Digital Input Transition (Off->On)	The device's input is turning on.
General	Configuration Changed	A configuration setting was changed.
General	Login Failure	An incorrect password was entered.
General	802.1X Authentication Failure	An 802.1X authentication failure occurred.
General	Firmware Upgrade Success	Firmware upgrade was successful.
General	Firmware Upgrade Failure	An error occurred during the firmware upgrade.
General	Log Service Ready	Log service is ready.
Redundancy	Ring/RSTP Topology Changed	The Ring/RSTP topology was changed.
Redundancy	Master Mismatch	A Turbo Ring Master mismatch occurred.
Redundancy	Coupling Topology Changed	The Coupling topology was changed.

Group	System Event	Description
Redundancy	VRRP State Change	The VRRP state was changed.
VPN	VPN Connected	VPN has been connected.
VPN	VPN Disconnected	VPN has been disconnected.
PoE	PoE PD On	Port#N PD power on.
PoE	PoE PD Off	Port#N PD power off.
PoE	Over Measured Power limitation	Over the total measured power limit.
PoE	PoE FETBad	PD Port#N MOSFET is bad.
PoE	PoE Over Temperature	The temperature of the environment exceeds the maximum operating temperature of the device.
PoE	PoE VEE Uvlo	VEE (PoE input voltage) under Voltage Lockout. The voltage of the power supply has dropped below 44V DC.
PoE	PoE PD Over Current	Current of Port#N has exceeded the safety limit.
PoE	PoE PD Check Fail	PD Port#N check failed.
PoE	Over Allocated Power limitation	The total PD power consumption exceeds the total allocated power.
Cellular	IP Change	The cellular IP address of the device has changed.
Cellular	Cellular Module Failure	The cellular module has encountered a failure and is not functioning.
Cellular	Detect SIM Failure	The system has detected a failure in the inserted SIM.
Cellular	PIN Code Failure	The device failed to validate the PIN code for the SIM card.
Cellular	SIM Switch	The active SIM has been switched to another SIM card.
Cellular	GuaranLink Cellular Reconnected	GuaranLink has successfully reconnected the cellular network.
Cellular	Guaranlink Triggered ISP Reregister	GuaranLink triggered re-registration with the Internet Service Provider.

Group	System Event	Description
Cellular	Guaranlink Triggered Cellular Module Reset	The cellular module was reset by GuaranLink due to an error condition.
Cellular	Guaranlink Triggered System Reboot	GuaranLink triggered a system reboot due to error recovery.
Power Management	Power Saving Start	The device enters the power saving mode.
Power Management	Power Saving End	The device leaves the power saving mode.
Power Management	Scheduling Rule Expired	The power saving rule has passed the set end time.
SMS	Wrong Password	The password of the remote control SMS received by the device is wrong.
SMS	Wrong Command	The command of the remote control SMS received by the device is wrong.
SMS	Wrong Format	The format of the remote control SMS received by the device is wrong.
SMS	Command Disabled	The remote control SMS received by the device is not enabled.
SMS	Trusted Number Authentication Failure	The remote control SMS received by the device is not from the Trusted Number List.
WAN Redundancy	WAN Interface Changed	The active WAN interface change to a different WAN interface.
WAN Redundancy	WAN Interface Ping Failure	The active WAN interface fails to ping the specified server.
Serial	Serial OP Mode State Changed	The serial operational mode has changed.
Serial	Serial DSR State Changed	The Data Set Ready (DSR) state of the serial port has changed.
Serial	Serial DCD State Changed	The Data Carrier Detect (DCD) state of the serial port has changed.
DHCP	DHCP Error Log	An error occurred in the DHCP process, and it has been logged.
General	Device Lockdown State Change	The device lockdown learning status has changed.

Group	System Event	Description
General	Fiber Check Warning	The system detected that monitored values exceeded their safety thresholds.
General	Layer 3 - 7 Policy Changed	A user configured firewall rule in Layer 3-7 Policy has been added, modified, or deleted.
IGMP Snooping	IGMP Snooping Error Log	An error occurred in IGMP snooping and has been logged.
NTP/SNTP Error Log	NTP/SNTP Error Log	An error occurred in NTP/SNTP synchronization and has been logged.
Redundancy	Ring/Chain/RSTP Topology Changed	The topology of the ring, chain, or RSTP network has changed.

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.

Options Menu

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

System

Settings	Admin	Supervisor	User
System Management			
Information Settings	R/W	R/W	R
Firmware Upgrade	R/W	-	-

Settings	Admin	Supervisor	User
Configuration Backup and Restore	R/W	-	-
Account Management			
User Account	R/W	-	-
Password Policy	R/W	-	-
Management Interface			
User Interface	R/W	R/W	R
SNMP	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

Network Configuration

Settings	Admin	Supervisor	User
Ports			
Port Settings	R/W	R/W	R
Layer 2 Switching			
VLAN	R/W	R/W	R
MAC Address Table	R/W	R/W	R
Network Interfaces	R/W	R/W	R

Network Service

Settings	Admin	Supervisor	User
DHCP Server	R/W	R/W	R

Routing

Settings	Admin	Supervisor	User
Unicast Routing			
Static Routes	R/W	R/W	R
Routing Table	R	R	R

NAT

Settings	Admin	Supervisor	User
NAT	R/W	R/W	R

Firewall

Settings	Admin	Supervisor	User
Layer 3 Policy	R/W	R/W	R
Device Lockdown	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	-
Authentication			
Login Authentication	R/W	-	-
RADIUS	R/W	-	-
TACACS+	R/W	-	-
MXview Alert Notification	R/W	R/W	R

Diagnostics

Settings	Admin	Supervisor	User
System Status			
Utilization	R/W	R/W	R

Settings	Admin	Supervisor	User
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			
Ping	R/W	R/W	R

www.moxa.com/products