

# MX-ROS V3 User Manual

**Version 1.8**  
November 2024



# Table of Contents

- Overview ..... 11**
  - Introduction .....11
  - What's in This Document .....11
  - Who This Document Is For .....11
  - Supported Series and Firmware Versions .....12
  - Supported Features List.....12
  - Document Conventions.....19
- Quick Start ..... 21**
  - Using a Web Browser to Configure the Industrial Secure Router .....21
- UI Reference ..... 25**
  - The MX-ROS User Interface.....25
  - Options Menu .....26
    - Change Language* .....27
    - Reboot* .....27
    - Reset to Default Settings*.....27
    - Save Custom Default* .....28
    - Log Out*.....29
  - Device Summary .....29
    - Model Information* .....29
    - Panel Status* .....30
    - System Event Summary (Last 3 days)* .....33
    - CPU Usage History (%)* .....34
    - Memory Usage History (%)*.....34
  - Setup Wizard .....35
    - Port Type* .....35
    - Interface* .....36
    - Service*.....39
    - Confirm*.....40
  - System.....40
    - System - User Privileges*.....41
    - System Management* .....42
    - Account Management*.....59
    - License Management*.....67

<i>Management Interface</i> .....	74
<i>Time</i> .....	91
<i>Power Management</i> .....	101
<i>SMS</i> .....	113
<i>GNSS</i> .....	119
<i>Status</i> .....	123
<i>Setting Check</i> .....	123
Cellular .....	125
<i>Cellular - User Privileges</i> .....	125
<i>Cellular - General</i> .....	125
<i>SIM Settings</i> .....	126
<i>GuaranLink</i> .....	127
<i>Cellular - Status</i> .....	132
Serial .....	135
<i>Serial - User Privileges</i> .....	136
<i>Serial - Port Settings</i> .....	136
<i>Operation Mode</i> .....	138
<i>Data Packing</i> .....	147
<i>Serial - Status</i> .....	149
<i>Serial Data Logs</i> .....	152
Network Configuration.....	152
<i>Network Configuration - User Privileges</i> .....	152
<i>Ports</i> .....	153
<i>Layer 2 Switching</i> .....	173
<i>Network Interfaces</i> .....	201
Redundancy .....	235
<i>Redundancy - User Privileges</i> .....	235
<i>Layer 2 Redundancy</i> .....	236
<i>Layer 3 Redundancy</i> .....	248
<i>VRRP</i> .....	248
<i>WAN Redundancy</i> .....	258
Network Service .....	262
<i>Network Service - User Privileges</i> .....	262
<i>DHCP Server</i> .....	263
<i>Dynamic DNS</i> .....	279
<i>DNS Server</i> .....	280

Routing .....	286
<i>Routing - User Privileges</i> .....	286
<i>Unicast Route</i> .....	287
<i>Multicast Route</i> .....	309
<i>Broadcast Forwarding</i> .....	314
NAT .....	317
<i>NAT - User Privileges</i> .....	317
<i>NAT Rule List</i> .....	318
Object Management.....	335
<i>Object Management - User Privileges</i> .....	335
<i>Create Object</i> .....	336
<i>Edit Object</i> .....	345
<i>Delete Object</i> .....	353
Firewall .....	353
<i>Network Configuration - User Privileges</i> .....	354
<i>Layer 2 Policy</i> .....	354
<i>Layer 3-7 Policy</i> .....	362
<i>Malformed Packets</i> .....	372
<i>Session Control</i> .....	373
<i>DoS Policy</i> .....	379
<i>Soft Lockdown Mode</i> .....	382
<i>Advanced Protection</i> .....	385
VPN .....	440
<i>VPN - User Privileges</i> .....	440
<i>IPSec</i> .....	440
<i>L2TP Server</i> .....	464
<i>OpenVPN Client</i> .....	466
Certificate Management.....	470
<i>Certificate Management - User Privileges</i> .....	470
<i>Local Certificate</i> .....	471
<i>Trusted CA Certificate</i> .....	474
<i>Certificate Signing Request</i> .....	475
Security .....	480
<i>Security - User Privileges</i> .....	481
<i>Device Security</i> .....	481
<i>Network Security</i> .....	488



<i>Authentication</i> .....	494
<i>MXview Alert Notification</i> .....	499
Diagnostics .....	501
<i>Diagnostics - User Privileges</i> .....	502
<i>System Status</i> .....	503
<i>Network Status</i> .....	506
<i>Event Logs and Notifications</i> .....	512
<i>Tools</i> .....	552
Industrial Application .....	562
<i>IEC 61375 Setting</i> .....	562
<b>Other Features .....</b>	<b>593</b>
Firmware Image Recovery Overview .....	593
<i>Methodology</i> .....	593
<i>How Dual-imaging Works</i> .....	594
Soft Lockdown.....	595
<i>Soft Lockdown Criteria</i> .....	595
<i>Entering Soft Lockdown Mode</i> .....	596
<i>When in Soft Lockdown Mode</i> .....	596
<i>Leaving Soft Lockdown Mode</i> .....	597
<b>Device Applications .....</b>	<b>599</b>
Network Segmentation .....	599
<i>About Network Segmentation</i> .....	599
<i>VLANs in Depth</i> .....	600
<i>Scenario: Layer 2 Segmentation of 3 Factories</i> .....	601
<i>Scenario: Layer 3 Segmentation of Two Services</i> .....	607
About Redundancy .....	613
<i>What kinds of redundancy protocols are there?</i> .....	614
<i>About Layer 2 Redundancy Protocols</i> .....	614
<i>About Turbo Ring v2</i> .....	617
<i>About RSTP</i> .....	626
<i>About Turbo Chain</i> .....	631
<i>About VRRP</i> .....	635
Routing .....	641
<i>About Routing</i> .....	641
<i>About Static Routing</i> .....	643
<i>About Multicast Routing</i> .....	644

<i>About Selecting a Routing Protocol</i> .....	644
<i>Example: Adding a Static Unicast Route for Factory Automation</i> .....	645
<i>Example: Adding Static Multicast Route for Passenger Speed Display</i> .....	647
About OpenVPN Client.....	649
<i>Scenario: Using a Site-to-Site OpenVPN Tunnel</i> .....	649
About NetFlow .....	652
<i>NetFlow In Depth</i> .....	653
<i>Scenario: Using NetFlow to Collect LAN Interface Data</i> .....	653
About Loopback Interfaces.....	657
<i>Scenario: Connecting Two Subnets</i> .....	657
<b>Railway Applications .....</b>	<b>664</b>
Overview of IEC 61375 for Rail Applications .....	664
<i>Ease of Coupling/Decoupling</i> .....	664
<i>Simplify On-board Device Communication</i> .....	664
<i>Failover Supports Redundancy</i> .....	665
Getting to Know IEC 61375.....	665
<i>About Communication Profiles (IEC 61375-2-3)</i> .....	666
<i>About Ethernet Train Backbones (IEC 61375-2-5)</i> .....	669
<i>About Ethernet Consist Networks (IEC 61375-3-4)</i> .....	669
Scenario: 2 Consists, Each with 2 Redundant ETBNs/ECSPs .....	670
<i>About Traffic Flows in ETBNs</i> .....	671
<i>Example: Configuring 2 Consists with 2 Redundant ETBN Routers Each</i> .....	674
<i>Checking End-Device IPs</i> .....	689
<i>Getting ECSP Data with a Network Analyzer</i> .....	690
<i>Getting ECSP Data with the Web GUI</i> .....	691
Scenario: 2 Consists, with 1 ETBN/ECSP Each .....	692
<i>Example: Configuring 2 Consists with 1 ETBN/ECSP Each</i> .....	693
Example: Configuring Local Consist Info for ETBNs/ECSPs .....	701
<b>Security Hardening Guide .....</b>	<b>704</b>
Security Best Practices .....	704
<i>Product Security</i> .....	704
<i>Physical Installation Guidelines</i> .....	704
<i>Account Management Guidelines</i> .....	705
<i>Protecting Vulnerable Network Ports</i> .....	705
<i>Maintaining Communication Integrity</i> .....	706
<i>Communication Integrity Features</i> .....	706

<i>Device Access Control Best Practices</i> .....	707
<i>About Device Integrity and Authenticity</i> .....	708
<i>Device Resource Management and Monitoring</i> .....	709
<i>Recommended Settings for Services and Features</i> .....	711
<i>Common Threats and Countermeasures</i> .....	713
<i>Recommended Operational Roles and Duties</i> .....	714
<i>Recommended Patching and Backup Practices</i> .....	715
<i>Recommendations for Vulnerability Management</i> .....	716
<i>Recommendations for Decommissioning</i> .....	716
Using Security Features .....	716
<i>Introduction to IPS</i> .....	716
<i>Introduction to Firewalls</i> .....	721
<i>Scenario: Airport Integrated Solutions</i> .....	732
<i>Scenario: Railway Integrated Solutions</i> .....	736
Security Standards and Concepts .....	742
<i>Introduction to Defense in Depth</i> .....	742
AAA .....	742
<i>ISA/IEC 62443 Standards and Architecture</i> .....	748
<i>Product Security Context</i> .....	755
<b>Appendix .....</b>	<b>758</b>
Destination Ports for Layer 3 – 7 Protocol .....	758
EtherTypes for Layer 2 .....	759
Fiber Check Threshold Values.....	761
IEC 61375-2-3 Communication Identifiers .....	762
IEC-104 Cause of Transmission List.....	764
IEC-104 Type Identification List .....	766
<i>Process information in monitor direction</i> .....	767
<i>Process telegrams with long time tag (7 octets)</i> .....	768
<i>Process information in control direction</i> .....	768
<i>Command telegrams with long time tag (7 octets)</i> .....	769
<i>System information in monitor direction</i> .....	769
<i>System information in control direction</i> .....	769
<i>Parameter in control direction</i> .....	770
<i>File transfer</i> .....	770
LED Behavior .....	770
<i>EDF-G1002 Series LED Behavior</i> .....	771

<i>EDR-8010 Series LED Behavior</i> .....	772
<i>EDR-G9004 Series LED Behavior</i> .....	773
<i>EDR-G9010 Series LED Behavior</i> .....	774
MIB Groups.....	776
<i>MIB Tree Structure</i> .....	776
MMS Command Type List.....	804
MMS Service Operation List.....	805
Severity Level List .....	809
Status Codes.....	809
<i>PoE Status Codes</i> .....	809
Structure and Syntax of Local Consist Info Files .....	811
<i>consistinfo</i> .....	811
<i>vehicleinfo</i> .....	812
<i>functioninfo</i> .....	813
Supported Features List.....	813
System Event List .....	819
System Log Events .....	821
TRDP Message Type List .....	824
<i>Configuration attribute requirements - msgType</i> .....	824
<i>Configuration attribute requirements - msgType Profile</i> .....	825
TRDP Protocol Filter Profile List.....	825
User Role Privileges .....	826
<i>System</i> .....	826
<i>Cellular</i> .....	827
<i>Serial</i> .....	827
<i>Network Configuration</i> .....	828
<i>Redundancy</i> .....	828
<i>Network Service</i> .....	829
<i>Routing</i> .....	829
<i>NAT</i> .....	829
<i>Object Management</i> .....	830
<i>Firewall</i> .....	830
<i>VPN</i> .....	830
<i>Certificate Management</i> .....	831
<i>Security</i> .....	831
<i>Diagnostics</i> .....	831





# Chapter 1

---

## Overview

# Overview

## Introduction

Welcome to the Moxa RouterOS (MX-ROS) manual. This comprehensive guide is designed to help you understand and navigate the UI features, technical concepts, and tasks you may encounter while using your MX-ROS device. The goal is to simplify your experience and make the setup process easier.

## 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
<b>EDR-8000 Series</b>	v3.13
<b>EDR-G9000 Series</b>	v3.13
<b>EDF-G1000 Series</b>	v3.13
<b>OnCell G4000 Series</b>	v3.13
<b>TN-4900 Series</b>	v3.13

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	EDR Series	EDF Series	OnCell Series	TN Series
<b>Device Summary</b>		YES	YES	YES	YES
<b>Setup Wizard</b>		YES	-	-	YES
<b>System</b>		YES	YES	YES	YES
	System Management	YES	YES	YES	YES
	Information Settings	YES	YES	YES	YES
	Firmware Upgrade	YES	YES	YES	YES
	Software Package Management	YES	YES	YES	YES
	Configuration Backup and Restore	YES	YES	YES	YES
	Account Management	YES	YES	YES	YES
	User Accounts	YES	YES	YES	YES
	Password Policy	YES	YES	YES	YES
	License Management	YES	YES	YES	YES
	Management Interface	YES	YES	YES	YES
	Out of Band Management	-	YES	-	-
	User Interface	YES	YES	YES	YES
	Hardware Interface	YES	YES	YES	YES
	SNMP	YES	YES	YES	YES
	Moxa Remote Connect	-	-	YES	YES
	MXsecurity	YES	YES	YES	YES
	Time	YES	YES	YES	YES
	System Time	YES	YES	YES	YES

Configuration Section	Function	EDR Series	EDF Series	OnCell Series	TN Series
	NTP/SNTP Server	YES	-	YES	-
	Power Management	-	-	YES	-
	SMS	-	-	YES	-
	GNSS	-	-	YES	-
	Setting Check	YES	YES	YES	YES
<b>Cellular</b>		-	-	YES	-
<b>Serial</b>		-	-	YES	-
<b>Network Configuration</b>		YES	YES	YES	YES
	Ports	YES	YES	YES	YES
	Port Settings	YES	YES	YES	YES
	Link Aggregation	YES	-	-	YES
	PoE	-	-	-	YES
	Link Fault Passthrough	YES	YES	-	-
	LAN Bypass Gen3	YES	YES	-	-
	Layer 2 Switching	YES	-	YES	YES
	VLAN	YES	-	YES	YES
	MAC Address Table	YES	-	YES	YES
	QoS	YES	-	-	YES
	Rate Limit	YES	-	-	YES
	Multicast	YES	-	YES	YES
	IGMP Snooping	YES	-	-	YES
	Static Multicast Table	YES	-	YES	YES



Configuration Section	Function	EDR Series	EDF Series	OnCell Series	TN Series
	Network Interfaces	YES	YES	YES	YES
<b>Redundancy</b>		YES	-	-	YES
	Layer 2 Redundancy	YES	-	-	-
	Spanning Tree	YES	-	-	YES
	Turbo Ring V2	YES	-	-	YES
	Turbo Chain	YES	-	-	-
	Layer 3 Redundancy	YES	-	YES	YES
	VRRP	YES	-	YES	YES
	WAN Redundancy	YES	-	YES	YES
<b>Network Service</b>		YES	-	YES	YES
	DHCP Server	YES	-	YES	YES
	Dynamic DNS	YES	-	YES	YES
	DNS Server	-	-	-	YES
<b>Routing</b>		YES	-	YES	YES
	Unicast Route	YES	-	YES	YES
	Static Routes	YES	-	YES	YES
	RIP	YES	-	-	YES
	OSPF	YES	-	-	YES
	Routing Table	YES	-	YES	YES
	Multicast Route	YES	-	YES	YES
	Multicast Route Settings	YES	-	YES	YES
	Static Multicast Route	YES	-	YES	YES

Configuration Section	Function	EDR Series	EDF Series	OnCell Series	TN Series
	Multicast Forwarding Table	YES	-	YES	YES
	Broadcast Forwarding	YES	-	YES	YES
<b>NAT</b>		YES	-	YES	YES
<b>Object Management</b>		YES	YES	YES	YES
<b>Firewall</b>		YES	YES	YES	YES
	Layer 2 Policy	YES	YES	YES	YES
	Layer 3-7 Policy	YES	YES	YES	YES
	Malformed Packets	YES	YES	YES	YES
	Session Control	YES	YES	YES	YES
	DoS Policy	YES	YES	YES	YES
	Soft Lockdown Mode	-	-	-	YES
	Advanced Protection	YES	YES	YES	YES
	Dashboard	YES	YES	YES	YES
	Configuration	YES	YES	YES	YES
	Protocol Filter Policy	YES	YES	YES	YES
	ADP	YES	YES	YES	YES
	IPS	YES	YES	-	YES
<b>VPN</b>		YES	-	YES	YES
	IPSec	YES	-	YES	YES
	L2TP Server	YES	-	-	YES
	OpenVPN Client	YES	-	-	-
<b>Certificate Management</b>		YES	YES	YES	YES

Configuration Section	Function	EDR Series	EDF Series	OnCell Series	TN Series
	Local Certificate	YES	YES	YES	YES
	Trusted CA Certificate	YES	YES	YES	YES
	Certificate Signing Request	YES	YES	YES	YES
<b>Security</b>		YES	YES	YES	YES
	Device Security	YES	YES	YES	YES
	Login Policy	YES	YES	YES	YES
	Trusted Access	YES	YES	YES	YES
	SSH & SSL	YES	YES	YES	YES
	Network Security	YES	YES	-	YES
	IEEE 802.1X	YES	-	-	YES
	Authentication	YES	YES	YES	YES
	Login Authentication	YES	YES	YES	YES
	RADIUS	YES	YES	YES	YES
	TACACS+ Server	YES	YES	YES	YES
	MXview Alert Notification	YES	YES	YES	YES
<b>Diagnostics</b>		YES	YES	YES	YES
	System Status	YES	YES	YES	YES
	Utilization	YES	YES	YES	YES
	Fiber Check	YES	-	-	-
	Network Status	YES	YES	YES	YES
	Network Statistics	YES	YES	YES	YES
	LLDP	YES	YES	YES	YES

Configuration Section	Function	EDR Series	EDF Series	OnCell Series	TN Series
	ARP Table	YES	YES	YES	YES
	Event Log and Notifications	YES	YES	YES	YES
	Event Log	YES	YES	YES	YES
	Event Notifications	YES	YES	YES	YES
	Syslog	YES	YES	YES	YES
	SNMP Trap/Inform	YES	YES	YES	YES
	Email Settings	YES	YES	YES	-
	SMS Settings	-	YES	YES	-
	Tools	YES	YES	YES	YES
	Port Mirroring	YES	-	-	YES
	Ping	YES	YES	YES	YES
	Diagnostic Support	-	-	YES	YES
	Netflow	YES	YES	-	-
<b>Industrial Application</b>		-	-	-	YES
	IEC 61375	-	-	-	YES
	Ethernet Train Backbone	-	-	-	YES
	TTDP Settings	-	-	-	YES
	Local ETBN Status	-	-	-	YES
	ETB Status	-	-	-	YES
	TCN Multicast Table	-	-	-	YES
	Communication Profile	-	-	-	YES
	ECSP Settings	-	-	-	YES

Configuration Section	Function	EDR Series	EDF Series	OnCell Series	TN Series
	SDTv2 Settings	-	-	-	YES
	ECSP Status	-	-	-	YES
	SDTv2 Status	-	-	-	YES
	Operational Status	-	-	-	YES
	Consist Info	-	-	-	YES
	Train Directory	-	-	-	YES
	Operational Train Directory	-	-	-	YES
	TCN-URI Table	-	-	-	YES

## Document Conventions

This document uses the following formatting conventions:

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



## Chapter 2

---

# Quick Start

# Quick Start

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

## Using a Web Browser to Configure the Industrial Secure Router

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

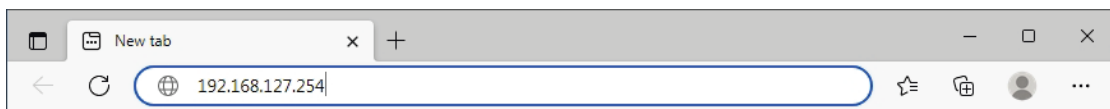
### Note

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:

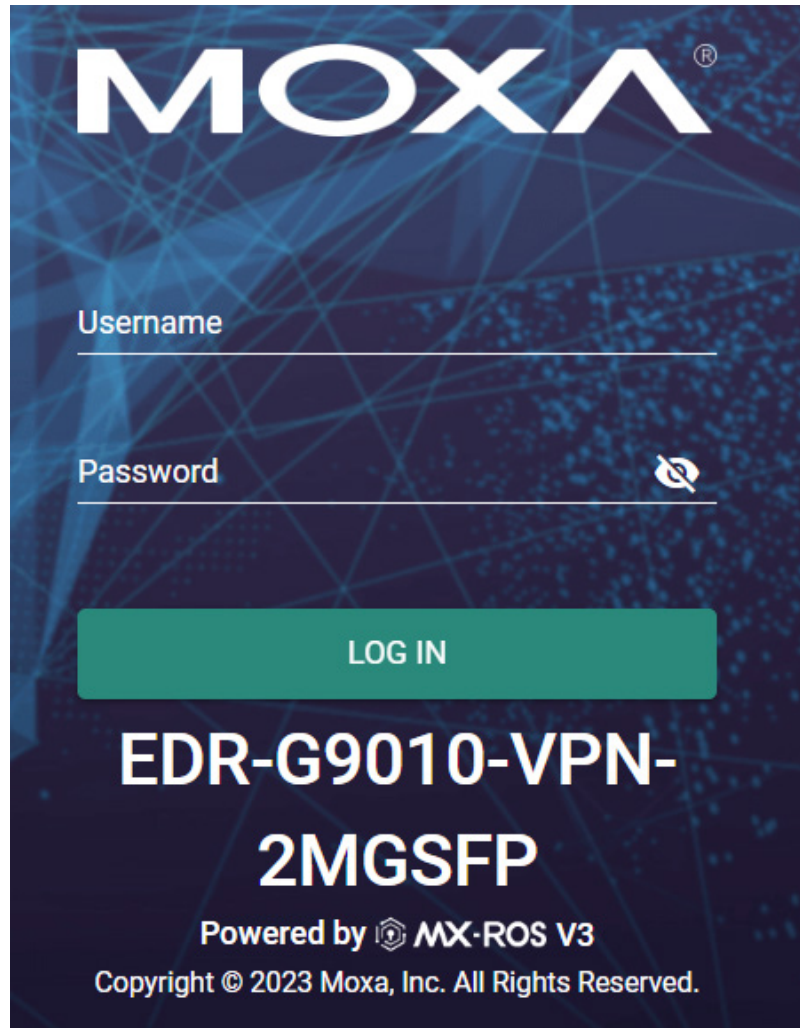
1. Make sure your PC host is connected to your device's LAN port, and is on the same subnet as your device.
2. Open a web browser and type the device's LAN IP address (**192.168.127.254** by default) into the address bar and press Enter.



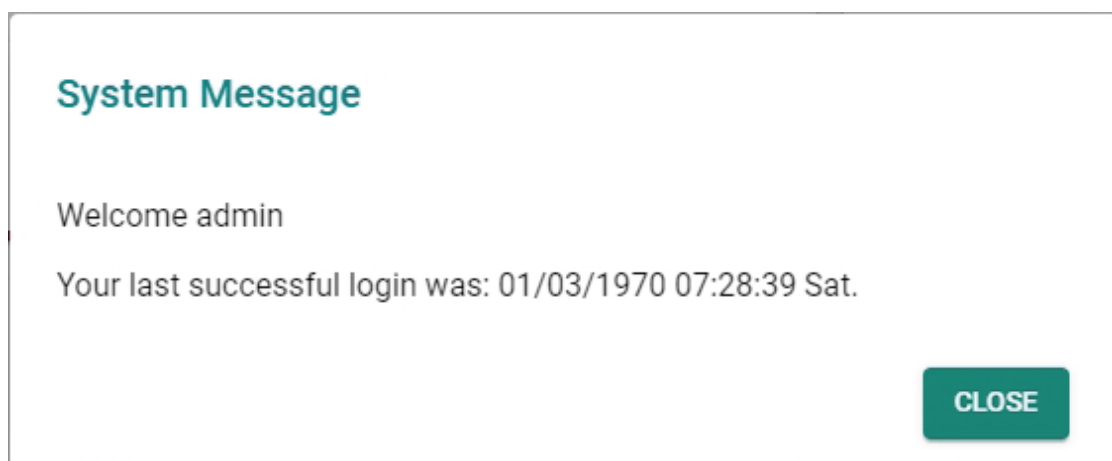
3. The web login page will open. Enter the username (**admin** or **user**) and password (the same as the Console password) and click **LOG IN** to continue.

### Note

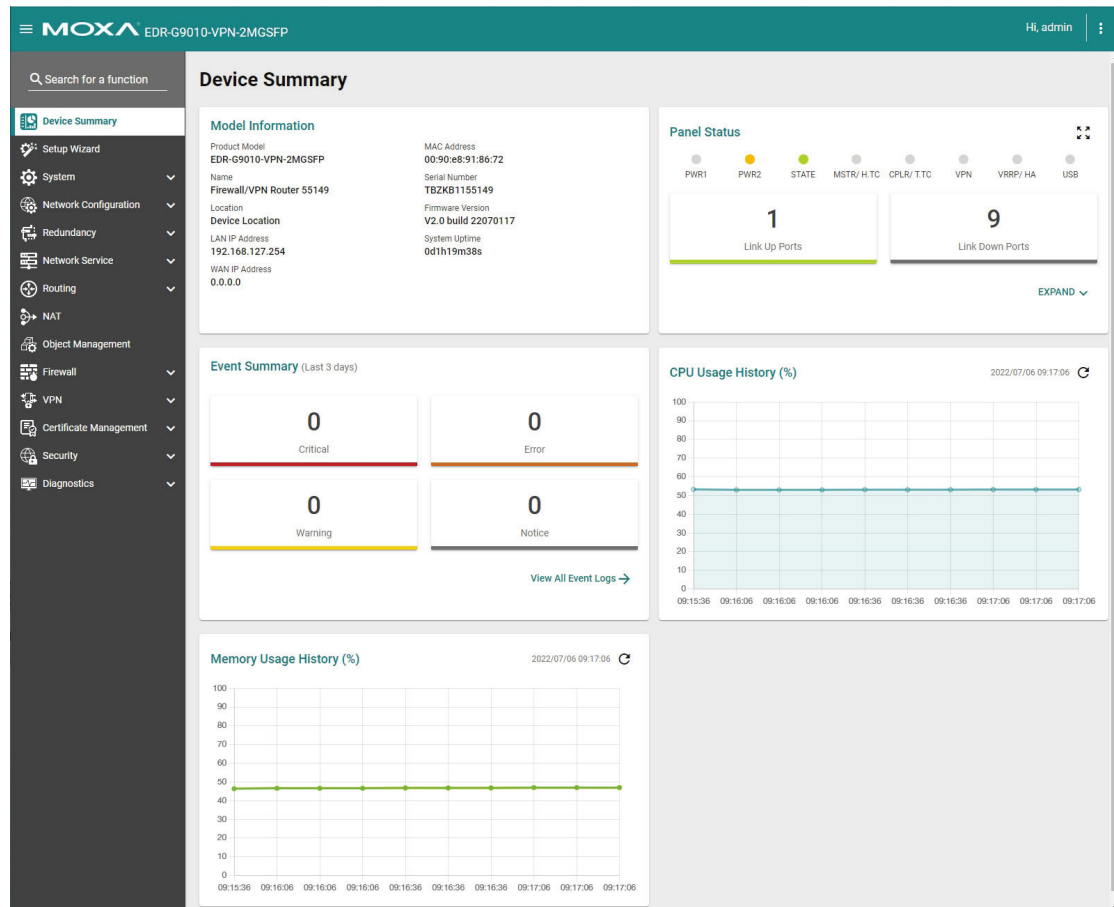
The default username is admin and the default password is moxa. We strongly recommend changing the password as soon as possible to ensure the security of your device.



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.



## Chapter 3

---

# UI Reference



# UI Reference

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

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

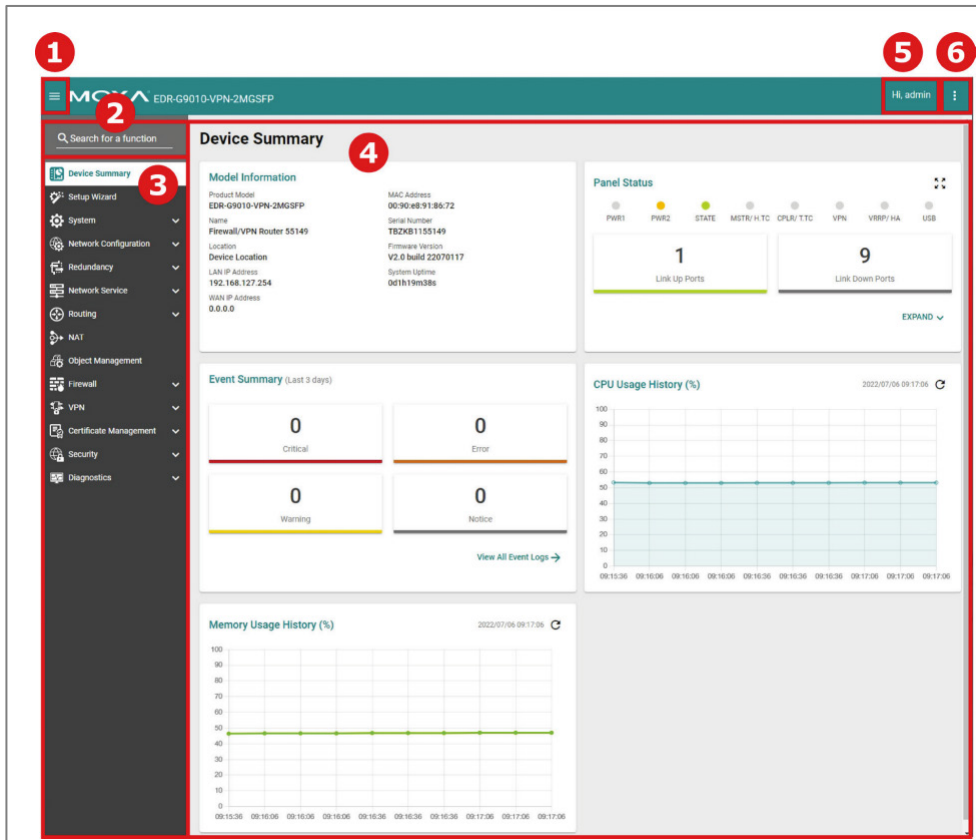
- The MX-ROS User Interface



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

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


## The MX-ROS User Interface

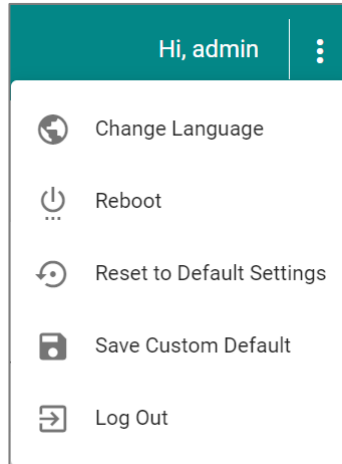
Here is an overview of the MX-ROS user interface.




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.



## Change Language

To change the language of the interface, click the **Options** (  ) icon in the upper-right corner of the page, and select **Change Language**.

## Reboot

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

## Reset to Default Settings

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

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

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

### Note

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

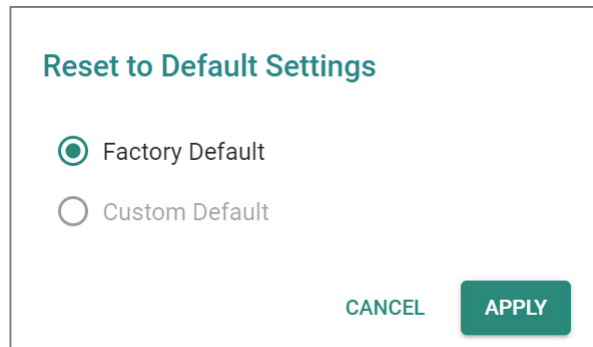
### Note

**Custom Default** is only available for the TN-4900 Series.

### ⚠ Warning

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

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



The image shows a dialog box titled "Reset to Default Settings". It contains two radio button options: "Factory Default" (which is selected) and "Custom Default". At the bottom right of the dialog, there are two buttons: "CANCEL" and "APPLY".

## 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


**Save Custom Default** is only available for the TN-4900 Series.

### ✎ 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**.

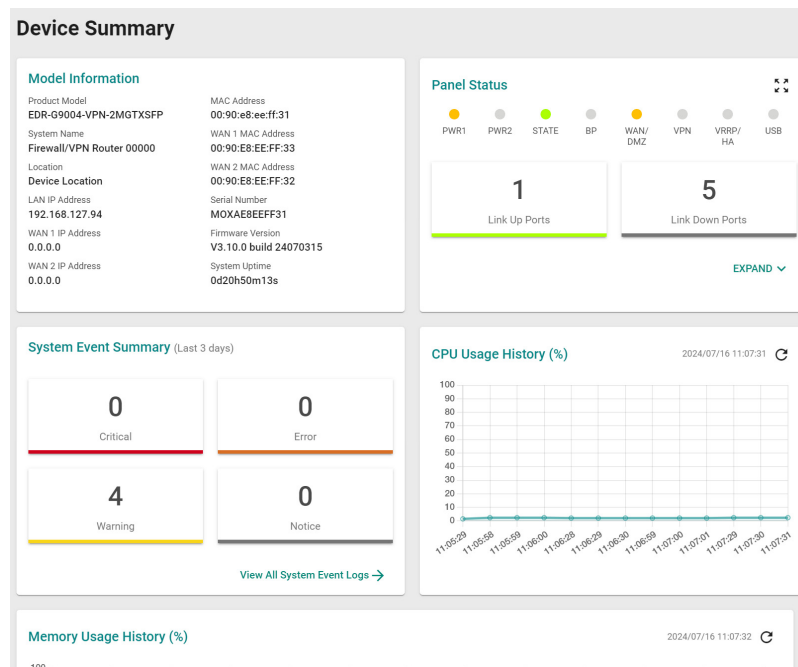
## Log Out

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.

### Model Information

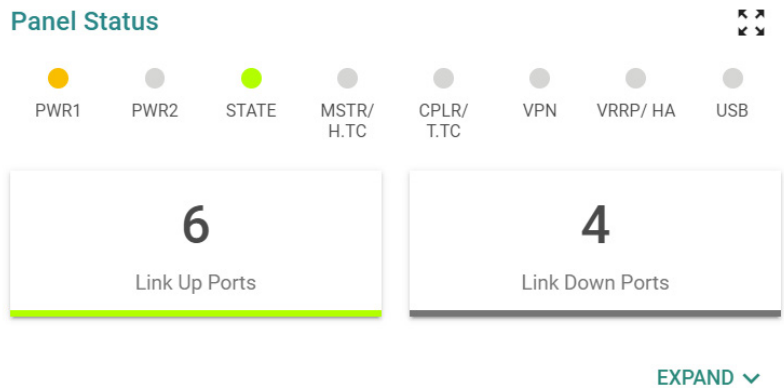
Product Model	MAC Address
<b>EDR-G9004-VPN-2MGTXSFP</b>	<b>00:90:e8:ee:ff:31</b>
System Name	WAN 1 MAC Address
<b>Firewall/VPN Router 00000</b>	<b>00:90:E8:EE:FF:33</b>
Location	WAN 2 MAC Address
<b>Device Location</b>	<b>00:90:E8:EE:FF:32</b>
LAN IP Address	Serial Number
<b>192.168.127.94</b>	<b>MOXAE8EEFF31</b>
WAN 1 IP Address	Firmware Version
<b>0.0.0.0</b>	<b>V3.10.0 build 24070315</b>
WAN 2 IP Address	System Uptime
<b>0.0.0.0</b>	<b>0d20h50m13s</b>

UI Setting	Description
<b>Product Model</b>	Shows the product model of the device.
<b>System Name</b>	Shows the name of the device. Refer to System > System Management > Information Settings for more information.
<b>Location</b>	Shows the location of the device. Refer to System > System Management > Information Settings for more information.
<b>LAN IP Address</b>	Shows the LAN IP address of the device. This can be configured in the Setup Wizard.
<b>WAN IP Address</b>	Shows the WAN IP address of your device. This can be configured in the Setup Wizard.
<b>MAC Address</b>	Shows the MAC address of your device.
<b>Serial Number</b>	Shows the serial number of your device.
<b>Firmware Version</b>	Shows the firmware version of your device.
<b>System Uptime</b>	Shows the amount of time your device has been continuously running for.

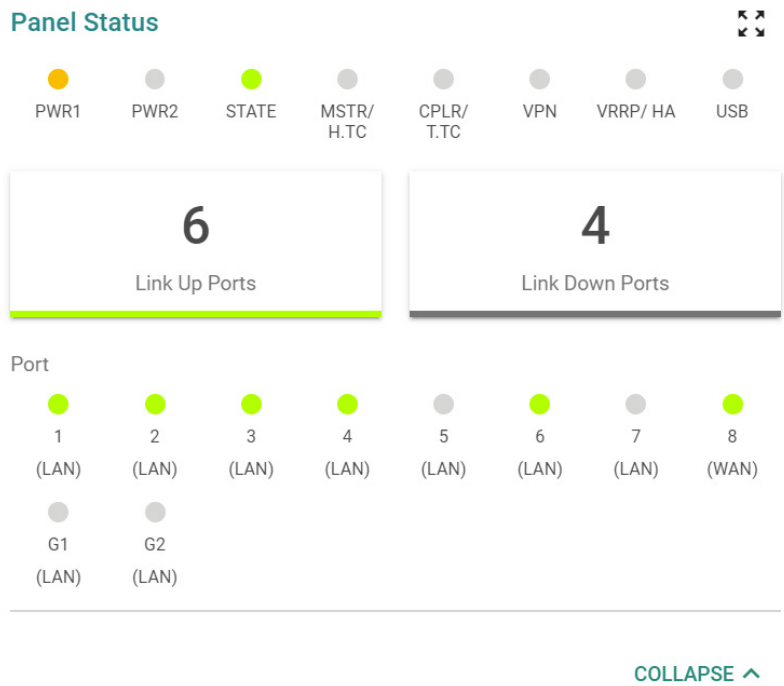
### Panel Status

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

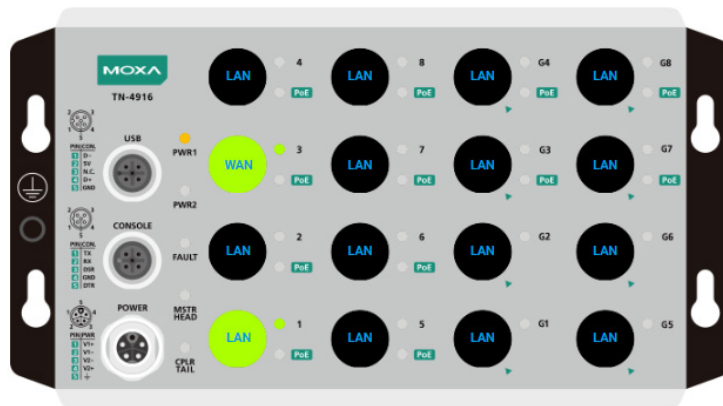
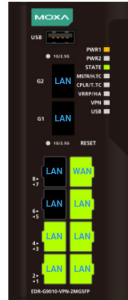
Clicking the **Expand** (⌵) icon in the **Panel Status** display will show your device's port status on a representative image of the device. This image will vary depending on your device. Click the **Close** (✕) icon in the upper-right corner to close the **Panel View**.

**Note**

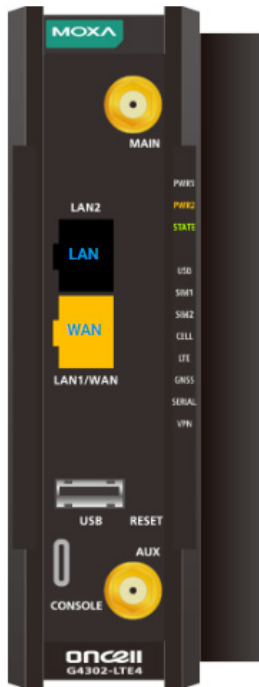
Available LEDs may vary across different versions of devices. For more information about status LEDs and their behavior, refer to LED Behavior.

Panel View

×



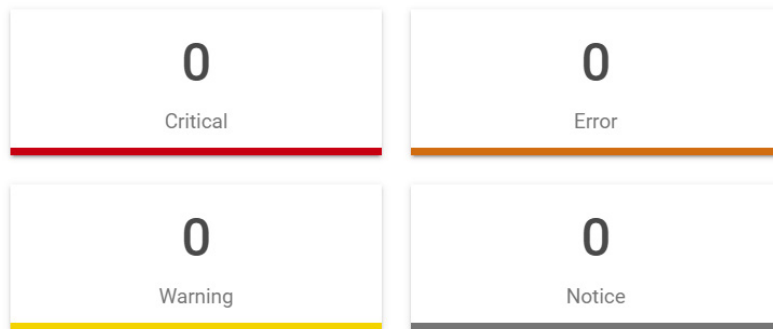




## System Event Summary (Last 3 days)

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

### System Event Summary (Last 3 days)



[View All System Event Logs →](#)

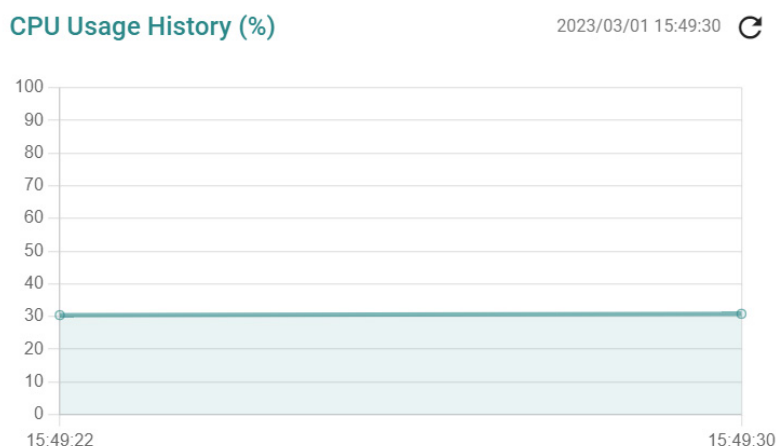
Click **View All System Event Logs** to go to the Event Log page to view event logs in more detail.

Event Log																																			
System Log	Firewall Log	VPN Log	Settings and Backup																																
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>🔄 📄 🗑️</span> <span>🔍 Search</span> </div> <table border="1"> <thead> <tr> <th>Index</th> <th>Timestamp</th> <th>Severity</th> <th>Additional message</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>2023/8/11 18:40:48.00</td> <td>Informational</td> <td>Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=2d3h41m38s</td> </tr> <tr> <td>2</td> <td>2023/8/11 18:26:7.8.00</td> <td>Informational</td> <td>Logout via UI: Web. Account=admin, Bootup=71, Startup=2d3h27m42s</td> </tr> <tr> <td>3</td> <td>2023/8/11 17:43:57+8.00</td> <td>Informational</td> <td>Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=2d2h45m32s</td> </tr> <tr> <td>4</td> <td>2023/8/11 10:52:15+8.00</td> <td>Informational</td> <td>Logout via UI: Serial Console. Account=admin, Bootup=71, Startup=1d19h53m50s</td> </tr> <tr> <td>5</td> <td>2023/8/11 10:45:13+8.00</td> <td>Informational</td> <td>Auth Ok, Login Success via UI: Serial Console. Account=admin, Bootup=71, Startup=1d19h46m48s</td> </tr> <tr> <td>6</td> <td>2023/8/10 17:14:25+8.00</td> <td>Informational</td> <td>Logout via UI: Web. Account=admin, Bootup=71, Startup=1d2h15m59s</td> </tr> <tr> <td>7</td> <td>2023/8/10 17:5:43+8.00</td> <td>Informational</td> <td>Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=1d2h7m18s</td> </tr> </tbody> </table>				Index	Timestamp	Severity	Additional message	1	2023/8/11 18:40:48.00	Informational	Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=2d3h41m38s	2	2023/8/11 18:26:7.8.00	Informational	Logout via UI: Web. Account=admin, Bootup=71, Startup=2d3h27m42s	3	2023/8/11 17:43:57+8.00	Informational	Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=2d2h45m32s	4	2023/8/11 10:52:15+8.00	Informational	Logout via UI: Serial Console. Account=admin, Bootup=71, Startup=1d19h53m50s	5	2023/8/11 10:45:13+8.00	Informational	Auth Ok, Login Success via UI: Serial Console. Account=admin, Bootup=71, Startup=1d19h46m48s	6	2023/8/10 17:14:25+8.00	Informational	Logout via UI: Web. Account=admin, Bootup=71, Startup=1d2h15m59s	7	2023/8/10 17:5:43+8.00	Informational	Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=1d2h7m18s
Index	Timestamp	Severity	Additional message																																
1	2023/8/11 18:40:48.00	Informational	Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=2d3h41m38s																																
2	2023/8/11 18:26:7.8.00	Informational	Logout via UI: Web. Account=admin, Bootup=71, Startup=2d3h27m42s																																
3	2023/8/11 17:43:57+8.00	Informational	Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=2d2h45m32s																																
4	2023/8/11 10:52:15+8.00	Informational	Logout via UI: Serial Console. Account=admin, Bootup=71, Startup=1d19h53m50s																																
5	2023/8/11 10:45:13+8.00	Informational	Auth Ok, Login Success via UI: Serial Console. Account=admin, Bootup=71, Startup=1d19h46m48s																																
6	2023/8/10 17:14:25+8.00	Informational	Logout via UI: Web. Account=admin, Bootup=71, Startup=1d2h15m59s																																
7	2023/8/10 17:5:43+8.00	Informational	Auth Ok, Login Success via UI: Web. Account=admin, Bootup=71, Startup=1d2h7m18s																																

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

## CPU Usage History (%)

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

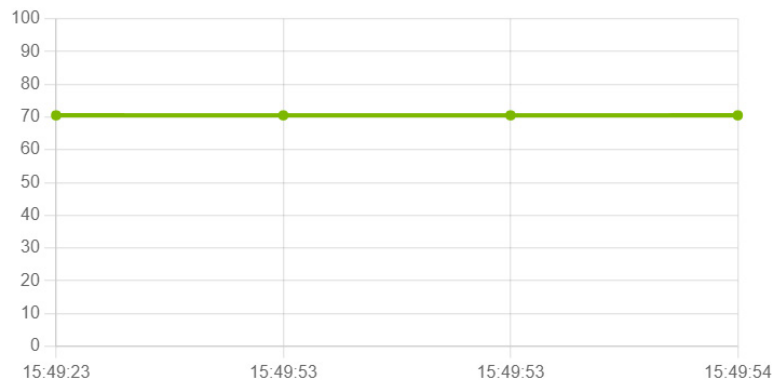


## Memory Usage History (%)

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

## Memory Usage History (%)

2023/03/01 15:49:54 



## Setup Wizard

### Menu Path: Setup Wizard

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

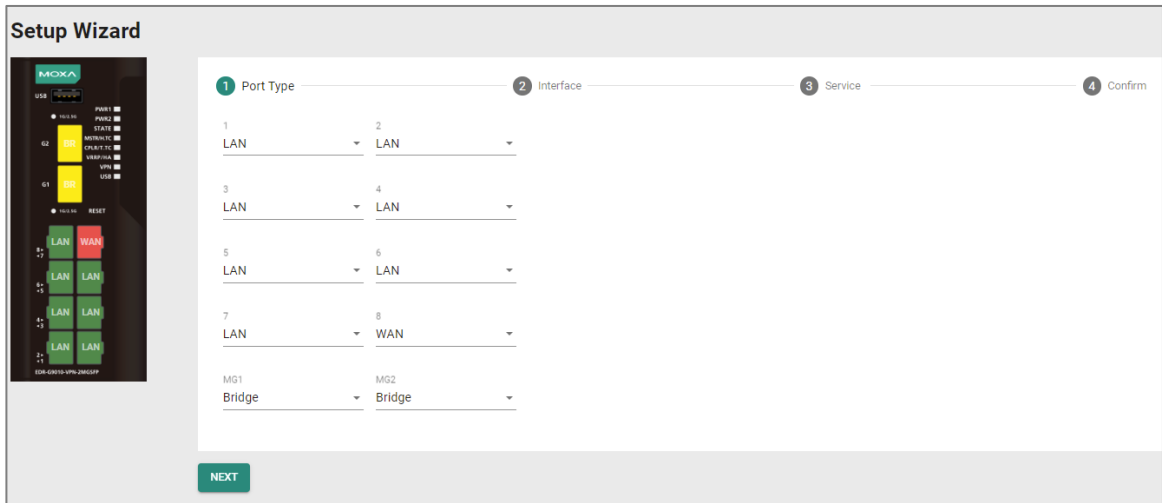
- Port Type
- Interface
- Service
- Confirm

#### Note

Available settings will vary depending on your product model.

## Port Type

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



UI Setting	Description	Valid Range	Default Value
<b>MG1 / MG2</b>	Select whether to use this fiber port as a LAN, WAN, or Bridge port.	LAN / WAN / Bridge	LAN
<b>1 / 2 / 3 / 4 / 5 / 6 / 7 / 8</b>	Select whether to use this Ethernet port as a LAN, WAN, or Bridge port.	LAN / WAN / Bridge	LAN

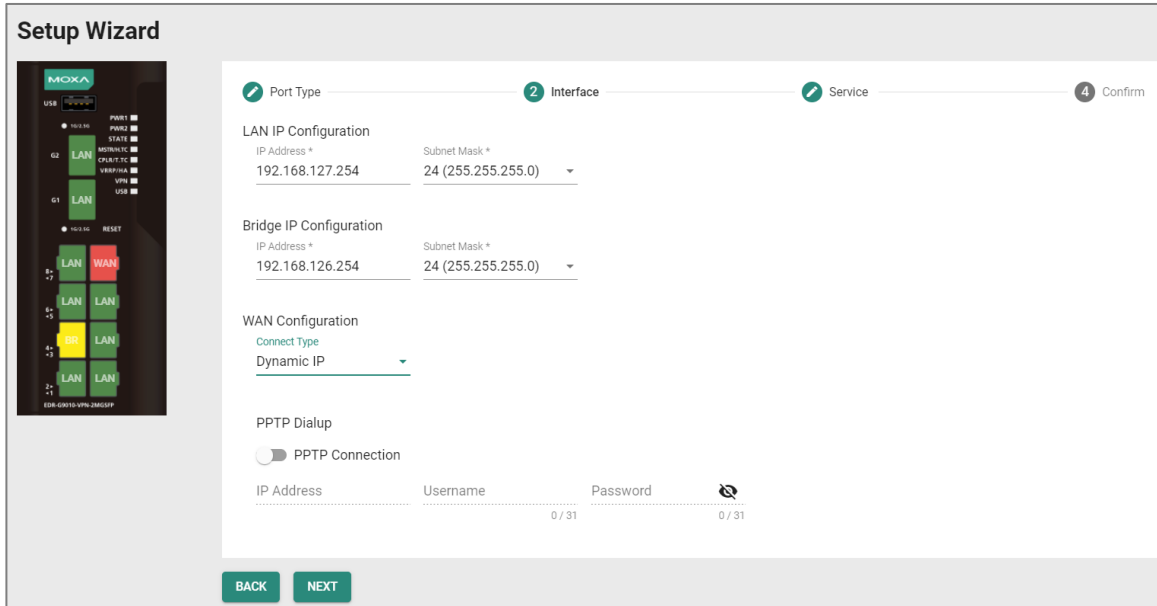
## Interface

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
<b>IP Address</b>	Specify the IP address for your LAN port.	Valid IP address	192.168.127.245
	<p><b>Note</b></p> <p>The IP Address should be inputted as unicast IP address.</p>		
<b>Subnet Mask</b>	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
------------	-------------	-------------	---------------

<b>Connect Type</b>	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
------------	-------------	-------------	---------------

<b>IP Address</b>	Specify the IP address for your WAN port.	Valid IP address	N/A
<b>Gateway</b>	Specify the gateway for your WAN port.	Valid IP address	N/A
<b>Subnet Mask</b>	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
------------	-------------	-------------	---------------

<b>PPTP Connection</b>	Enable or disable using a PPTP connection.	Enabled / Disabled	Disabled
<b>IP Address</b>	Specify the IP address of your PPTP connection.	Valid IP address	N/A
<b>Username</b>	Specify the username for your PPTP connection.	1 to 31 characters	N/A
<b>Password</b>	Specify the password for your PPTP connection.	1 to 31 characters	N/A

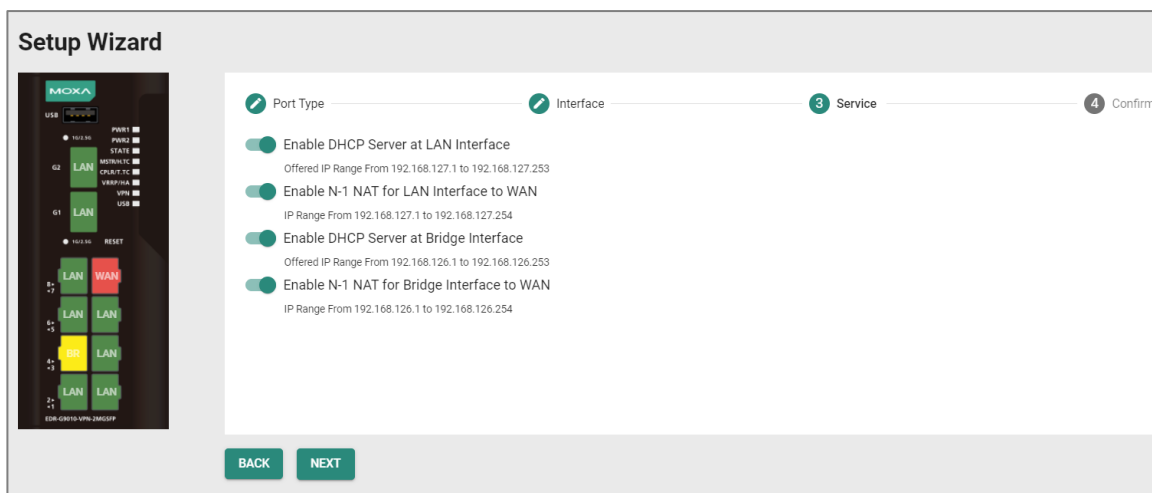
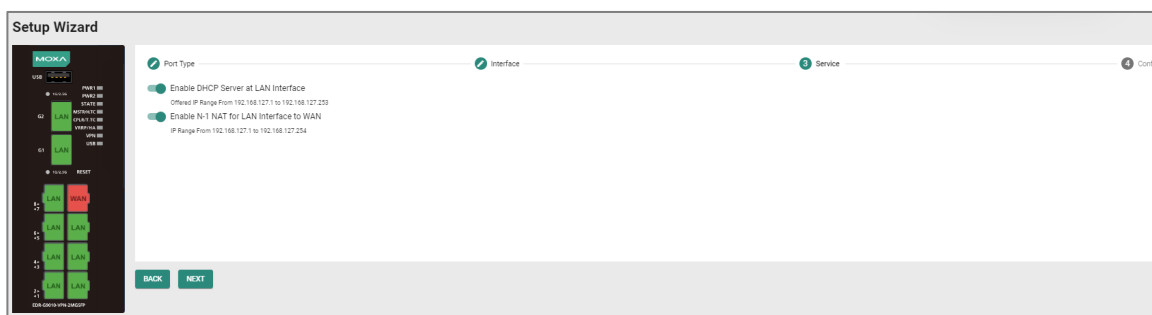
## PPPoE Dialup

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
<b>Username</b>	Specify the username for your PPPoE connection.	1 to 31 characters	N/A
<b>Password</b>	Specify the password for your PPTP connection.	1 to 31 characters	N/A
<b>Host Name</b>	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
<b>Enable DHCP Server at LAN Interface</b>	Enable or disable using a DHCP server for the LAN interface.	Enable / Disable	Enable
<b>Enable N-1 NAT for LAN Interface to WAN</b>	Enable or disable using N-1 NAT for LAN interfaces to WAN.	Enable / Disable	Enable





## 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
<b>System Management</b>			
<b>Information Settings</b>	R/W	R/W	R
<b>Firmware Upgrade</b>	R/W	-	-
<b>Software Package Management</b>	R/W	-	-
<b>Configuration Backup and Restore</b>	R/W	-	-
<b>Account Management</b>			
<b>User Account</b>	R/W	-	-
<b>Password Policy</b>	R/W	-	-
<b>License Management</b>	R/W	R	R
<b>Management Interface</b>			
<b>Out of Band Management</b>	R/W	R/W	R
<b>User Interface</b>	R/W	R/W	R
<b>Hardware Interface</b>	R/W	R/W	R
<b>SNMP</b>	R/W	-	-
<b>Moxa Remote Connect</b>	R/W	-	-
<b>MXsecurity</b>	R/W	R/W	-
<b>Time</b>			
<b>System Time</b>	R/W	R/W	R
<b>NTP/SNTP Server</b>	R/W	R/W	R

Settings	Admin	Supervisor	User
<b>Power Management</b>	R/W	R/W	R
<b>SMS</b>	R/W	R/W	R
<b>GNSS</b>	R/W	R/W	R
<b>Setting Check</b>	R/W	R/W	R

## System Management

### Menu Path: System > System Management

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

This section includes these pages:

- Information Settings
- Firmware Upgrade
- Software Package Management
- Configuration Backup and Restore

## Information Settings

### Menu Path: System > System Management > Information Settings

This page lets you add additional information about the device to make it easier to identify on the network.

### Information Settings

Device Name 0 / 30

Location 0 / 80

Description 0 / 40

Contact Information 0 / 40

UI Setting	Description	Valid Range	Default Value
<b>Device Name</b>	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)
<b>Location</b>	Enter a location for the device.	1 to 80 characters	Device Location
<b>Description</b>	Enter a description for the device.	1 to 40 characters	N/A
<b>Contact Information</b>	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

#### **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.

### ⚠ Warning

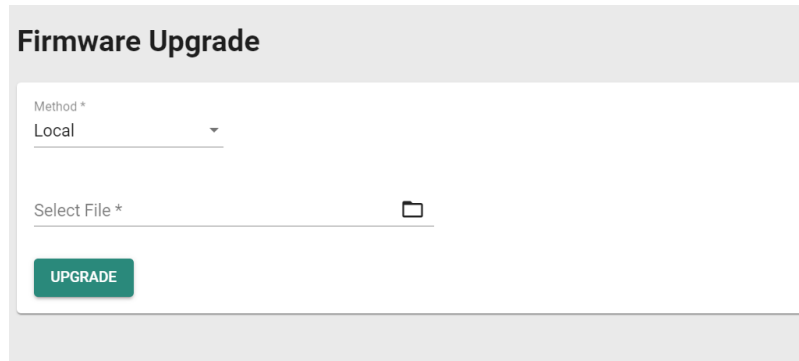
Upgrading the firmware should be only be done by qualified personnel, as it is possible to render the device inoperable if the upgrade is not done properly. If you are not familiar with the process, please request the assistance of qualified personnel. You can also consult with Moxa support and we will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



The screenshot shows a web interface titled "Firmware Upgrade". It features a dropdown menu for "Method \*" with "Local" selected. Below this is a "Select File \*" field with a folder icon, and a green "UPGRADE" button.

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

## TFTP

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

## Firmware Upgrade

The screenshot shows the 'Firmware Upgrade' form with the 'Method' dropdown menu set to 'TFTP'. Below the dropdown are two input fields: 'Server IP Address \*' and 'File Name \*'. A green 'UPGRADE' button is located at the bottom left of the form.

UI Setting	Description	Valid Range	Default Value
<b>Server IP Address</b>	Specify the IP address of the TFTP server.	IP address	N/A
<b>File Name</b>	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.

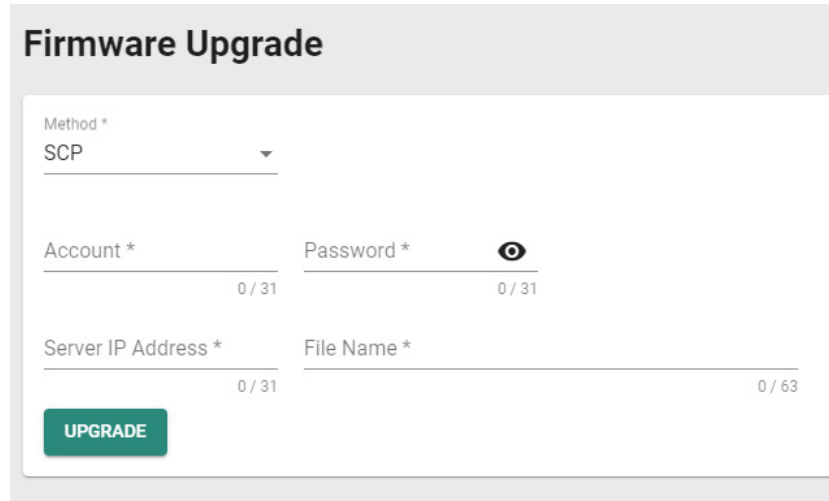
## Firmware Upgrade

The screenshot shows the 'Firmware Upgrade' form with the 'Method' dropdown menu set to 'USB'. Below the dropdown is a 'Select File \*' input field with a folder icon to its right. A green 'UPGRADE' button is located at the bottom left of the form.

UI Setting	Description	Valid Range	Default Value
<b>Select File</b>	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.



The screenshot shows a web interface titled "Firmware Upgrade". It contains a dropdown menu for "Method \*" with "SCP" selected. Below are four input fields: "Account \*" (0/31), "Password \*" (0/31) with a toggle icon, "Server IP Address \*" (0/31), and "File Name \*" (0/63). A green "UPGRADE" button is at the bottom left.

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

## SFTP

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

## Firmware Upgrade

Method  
SFTP

---

Account \* 0 / 31

Password \* 0 / 31

---

Server IP Address \* 0 / 31

File Name \* 0 / 63

**UPGRADE**

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

## Software Package Management

### Menu Path: System > System Management > Software Package Management

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

[www.moxa.com](http://www.moxa.com).

#### Note

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

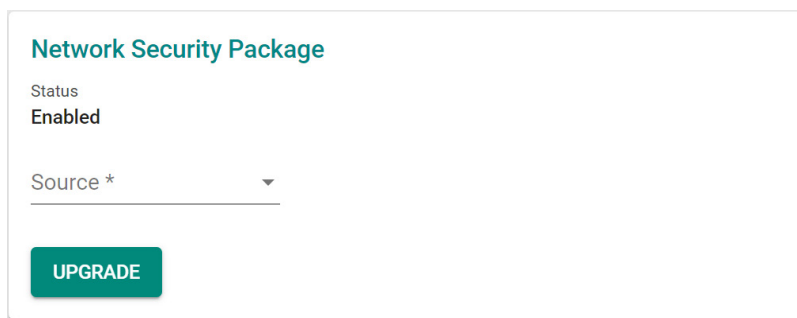
- Network Security Package:** Helps you protect your device and network with IPS (Intrusion Prevention System) patterns and a DPI (Deep Packet Inspection) engine.

**Note**

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

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

## Network Security Package



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



## MXsecurity Agent Package

**MXsecurity Agent Package**

Status  
Enabled

Source \* ▼

---

**UPGRADE**

UI Setting	Description	Valid Range	Default Value
<b>Source</b>	<p>Select a source to use to upgrade the software package.</p> <p><b>Local:</b> Use a file stored on the local host.</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p><b>Note</b></p> <p>The <b>Local</b> option is not commonly used in standard environments. However, if you experience issues with your device and MXsecurity, please reach out to Moxa Technical Support. They can utilize the <b>Local</b> option as a troubleshooting interface.</p> </div> <p><b>Firmware:</b> Use the package included with the current firmware.</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p><b>Note</b></p> <p>Starting from v3.10, the MXsecurity Agent Package will be automatically upgraded when the firmware is upgraded. When upgraded, a "Successfully installed MXSecurity agent package" notification will appear when logging in, and a notification can be found in the <b>Event Log &gt; System Log</b>.</p> </div>	Local / Firmware	N/A
<b>Select File (if Source is Local)</b>	This is a troubleshooting interface in case you encounter issues with your device and MXsecurity.	N/A	N/A
<b>Package Version (if Source is Firmware)</b>	This shows the included package version of the current firmware.	N/A	Current Package Version


## Configuration Backup and Restore

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

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

This page includes these tabs:

- Backup
- Restore
- File Encryption

 **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.

**Configuration Backup and Restore**

Backup | Restore | File Encryption

Method \*  
Local

BACK UP

## TFTP

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

**Configuration Backup and Restore**

Backup | Restore | File Encryption

Method \*  
TFTP

Server IP Address \*    File Name \*

BACK UP

UI Setting	Description	Valid Range	Default Value
<b>Server IP Address</b>	Specify the IP address of the TFTP server.	Valid IP address	N/A
<b>File Name</b>	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.

### Configuration Backup and Restore

Backup | Restore | File Encryption

Method \*  
USB

BACK UP

---

#### Auto Backup of Configurations

Automatically Back Up \*  
Enabled

APPLY

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

### SCP

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

### Configuration Backup and Restore

Backup | Restore | File Encryption

Method \*  
SCP

Account \* 0 / 31 Password \* 0 / 31

Server IP Address \* 0 / 31 File Name \* 0 / 63

BACK UP

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

The screenshot shows the 'Configuration Backup and Restore' interface. It has three tabs: 'Backup', 'Restore', and 'File Encryption'. The 'Backup' tab is active. Below the tabs, there is a 'Method \*' dropdown menu set to 'SFTP'. Below that are four input fields: 'Account \*' (0 / 31), 'Password \*' (0 / 31) with a password icon, 'Server IP Address \*' (0 / 31), and 'File Name \*' (0 / 63). A green 'BACK UP' button is located at the bottom left of the form area.

UI Setting	Description	Valid Range	Default Value
<b>Account</b>	Enter the SFTP server account name.	1 to 31 characters	N/A
<b>Password</b>	Enter the SFTP server account password.	1 to 31 characters	N/A
<b>Server IP Address</b>	Specify the IP address of the SFTP server.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
<b>File Name</b>	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.

The screenshot shows the 'Configuration Backup and Restore' interface with the 'Restore' tab active. It includes a 'Configuration Firmware Version Checking' section with a dropdown menu set to 'Enabled' and an 'APPLY' button. Below this is a 'Method' dropdown menu set to 'Local' and a 'Select File \*' field with a folder icon and a 'RESTORE' button.

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	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
<b>Select File</b>	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.

The screenshot shows the 'Configuration Backup and Restore' interface. It has three tabs: 'Backup', 'Restore', and 'File Encryption'. The 'Restore' tab is active. Under 'Configuration Firmware Version Checking', there is a 'Status \*' dropdown menu set to 'Enabled' and an 'APPLY' button. Below that, the 'Method' dropdown menu is set to 'TFTP'. There are two input fields: 'Server IP Address \*' with a character count of '0 / 31' and 'File Name \*' with a character count of '0 / 63'. A 'RESTORE' button is located at the bottom of the form.

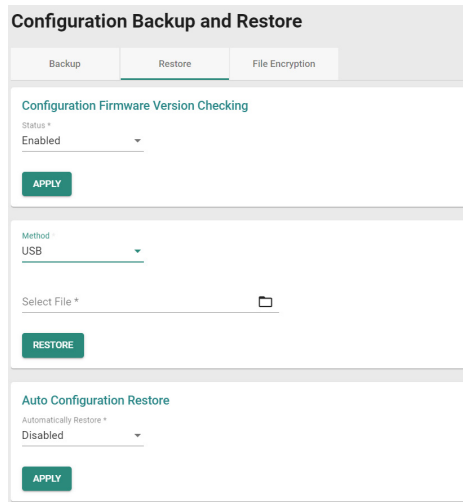
UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable configuration file firmware version checking. This checks to make sure the configuration file is for the current firmware version or earlier.	Enabled / Disabled	Disabled
<b>Server IP Address</b>	Specify the IP address of the TFTP server.	Valid IP address	N/A
<b>File Name</b>	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
<b>Status</b>	Enable or disable configuration file firmware version checking. This checks to make sure the configuration file is for the current firmware version or earlier.  <b>Note</b> 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
<b>Select File</b>	Select the configuration file to restore from.	N/A	N/A
<b>Automatically Restore (If Method is USB)</b>	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.  <b>Note</b> The auto-restore feature will look for configuration files on an inserted ABC-02 in the following order: <ol style="list-style-type: none"><li>1. An .ini configuration file named with the device's MAC address</li><li>2. A sys.ini configuration file</li></ol>	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.

The screenshot shows a web interface titled "Configuration Backup and Restore" with three tabs: "Backup", "Restore", and "File Encryption". The "Restore" tab is active. Under "Configuration Firmware Version Checking", the "Status" dropdown is set to "Enabled" and there is an "APPLY" button. Below this, the "Method" dropdown is set to "SCP". There are four input fields: "Account \*" (0/31), "Password \*" (0/31) with a toggle icon, "Server IP Address \*" (0/31), and "File Name \*" (0/63). A "RESTORE" button is located at the bottom of the form.

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

## SFTP

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

### Configuration Backup and Restore

Backup
Restore
File Encryption

**Configuration Firmware Version Checking**

Status \*  
Enabled ▼

APPLY

Method \*  
SFTP ▼

Account \* 0 / 31      Password \* 0 / 31

Server IP Address \* 0 / 31      File Name \* 0 / 63

RESTORE

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

## Configuration Backup and Restore - File Encryption

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

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

### Configuration Backup and Restore

Backup
Restore
File Encryption

Configuration File Signature \*  
Disabled ▾

Signature Information \*  
Encrypt sensitive information only ▾

Key String \*  
.... 4 / 30

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Configuration File Signature</b>	Enables or disables the use of a digital signature for checking the integrity of a configuration file.	Enabled / Disabled	Disabled
<b>Signature Information</b>	Select the type of data to encrypt.  <b>Encrypt sensitive information only:</b> Only encrypt password-related sensitive information in the exported configuration file.  <b>Encrypt all information:</b> Encrypt all information in the exported configuration file.	Encrypt sensitive information only / Encrypt all information	Encrypt sensitive information only
<b>Key String</b>	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:

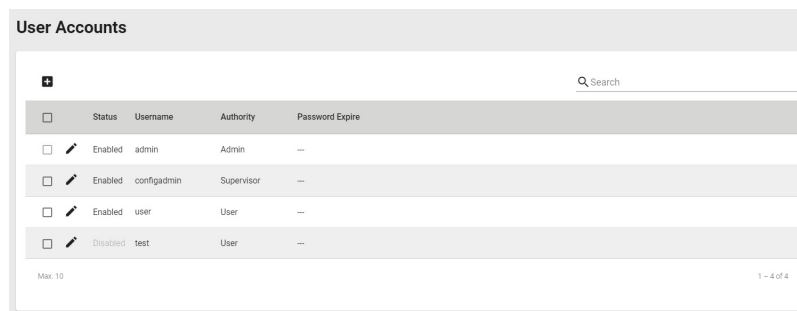
1. The original firmware version of the user device is V.3.0 or higher.
2. The user downgrades the firmware below to V.3.0 and performs any action on this firmware.
3. The firmware version is subsequently upgraded back to V.3.0 or higher.

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.

### **Limitations**

You can create up to 10 user accounts.



<input type="checkbox"/>	Status	Username	Authority	Password Expire
<input type="checkbox"/>	Enabled	admin	Admin	—
<input type="checkbox"/>	Enabled	configadmin	Supervisor	—
<input type="checkbox"/>	Enabled	user	User	—
<input type="checkbox"/>	Disabled	test	User	—

### **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.

UI Setting	Description
------------	-------------

<b>Password Expire</b>	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 <b>Password Max-life-time</b> setting on the <b>Password Policy</b> 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
------------	-------------	-------------	---------------

<b>Status</b>	Enable or disable this user account.	Enabled / Disabled	N/A
<b>Username</b>	Enter a user name for this account.	4 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
<b>Authority</b>	<p>Select an authority role for this account.</p> <ul style="list-style-type: none"> <li><b>Admin:</b> The account will have read/write access to all configuration parameters.</li> <li><b>Supervisor:</b> The account will have read/write access to all configuration parameters except create, delete, and modify accounts.</li> <li><b>User:</b> The account can only view configurations and cannot make any modifications.</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Refer to User Role Privileges for a list of what read/write access privileges are granted for the different authority levels.</p> </div>	Admin / Supervisor / User	N/A
<b>New Password</b>	<p>Enter a password for this account.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>The new password must follow any requirements set on the <b>System &gt; Account Management &gt; Password Policy</b> page.</p> </div>	4 to 64 characters, additional requirements are based on settings in <b>System &gt; Account Management &gt; Password Policy</b>	N/A
<b>Confirm Password</b>	<p>Enter the password again to confirm.</p>	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.

### Edit Account Settings

Status \*  
Enabled

Username  
admin  
At least 4 characters 5 / 32

Authority \*  
Admin

Old Password \*  
At least 4 characters 0 / 64

New Password \*  
At least 4 characters 0 / 64

Confirm Password \*  
At least 4 characters 0 / 64

CANCEL


APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable this user account.	Enabled / Disabled	N/A
<b>Username</b>	Shows the username for this account. The username cannot be changed.	4 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
<b>Authority</b>	<p>Select an authority role for this account.</p> <ul style="list-style-type: none"> <li><b>Admin:</b> The account will have read/write access to all configuration parameters.</li> <li><b>Supervisor:</b> The account will have read/write access to all configuration parameters except create, delete, and modify accounts.</li> <li><b>User:</b> The account can only view configurations and cannot make any modifications.</li> </ul> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Refer to User Role Privileges for a list of what read/write access privileges are granted for the different authority levels.</p> </div>	Admin / Supervisor / User	N/A
<b>Old Password</b>	<p>Enter the old password for this account.</p>	4 to 64 characters	N/A
<b>New Password</b>	<p>Enter the new password for this account.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>The new password must follow any requirements set on the <b>System &gt; Account Management &gt; Password Policy</b> page.</p> </div>	4 to 64 characters, additional requirements are based on settings in <b>System &gt; Account Management &gt; Password Policy</b>	N/A
<b>Confirm Password</b>	<p>Enter the password again to confirm.</p>	4 to 64 characters, additional requirements are based on settings in <b>System &gt; Account Management &gt; Password Policy</b>	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.

Status	Username	Authority	Password Expire
<input type="checkbox"/> Enabled	admin	Admin	--
<input checked="" type="checkbox"/> Enabled	configadmin	Supervisor	--
<input type="checkbox"/> Enabled	user	User	--

## Password Policy

**Menu Path: System > Account Management > Password Policy**

This page allows you to set password complexity rules for user accounts to improve security. Click **APPLY** to save your changes.

**Note**

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

- Set the Minimum Length for passwords to 16.
- Enable the Password complexity strength check and enable all the requirement options.
- Set a Password Max-life-time to ensure that users change their password regularly.

## Password Policy

Minimum Length \*

4

4 - 16

Password complexity strength check

Disabled

Must contain at least one digit (0-9)

Disabled

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

Disabled

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

Disabled

Password Max-life-time \*

0

0 - 365

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Minimum Length</b>	Set the minimum required password length.	4 to 16 characters	4
<b>Password complexity strength check</b>	Enable or disable the password complexity strength check.	Enabled / Disabled	Disabled
<b>Must contain at least one digit (0-9)</b> (if Password complexity strength check is Enabled)	Enable or disable requiring the password to contain at least one digit.	Enabled / Disabled	Disabled
<b>Must include both upper and lower case letters (A-Z, a-z)</b> (if Password complexity strength check is Enabled)	Enable or disable requiring the password to include both uppercase and lowercase letters.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
<b>Must contain at least one special character</b> (~!@#\$%^&*~  ;,:.<>{}[]()) <b>(if Password complexity strength check is Enabled)</b>	Enable or disable requiring the password to contain at least one special character.	Enabled / Disabled	Disabled
<b>Password Max-life-time</b>	Specify how long in days passwords will be valid for. When the password expires, the system will require the user to change their password. If this is set to 0, passwords will not expire.	0 to 365	0

## License Management

### Menu Path: System > License Management

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

This page includes these sections:



- Overview
- License History

### Overview

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

**License Management**

**Overview**

	<b>Name</b> IPS-DEVICE <small>Valid Durations (days)</small> 11246	<b>Start Date</b> 2022-04-01 12:20:00 <b>End Date</b> 2053-12-08 02:06:40	<b>Status</b> Valid <a href="#">Get New License Here</a> 
---	---	--	--

**ADD NEW LICENSE**

**License History**

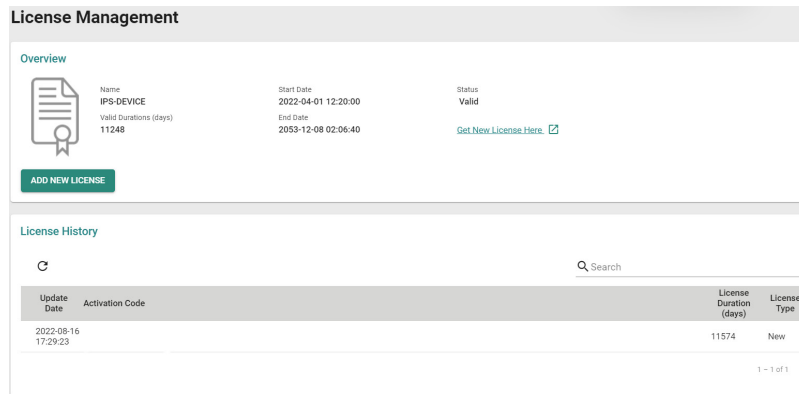
🔄 Search

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

1 - 1 of 1

## License History

This area lets you see details about previously installed licenses.



The screenshot shows the 'License Management' interface. It has an 'Overview' section with a document icon and a 'Name' field containing 'IPS-DEVICE'. Below the name is the 'Valid Durations (days)' field with the value '11248'. To the right, the 'Start Date' is '2022-04-01 12:20:00' and the 'End Date' is '2053-12-08 02:06:40'. The 'Status' is 'Valid'. There is a link 'Get New License Here' with an external icon. Below the overview is an 'ADD NEW LICENSE' button. The 'License History' section has a search bar and a table with the following data:

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

At the bottom right of the history section, it says '1 - 1 of 1'.

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

## Adding a New License

### Goal

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

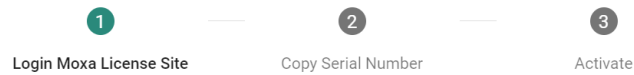
### Prerequisites

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

### Procedure

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

## Add New License



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

CLOSE **NEXT**

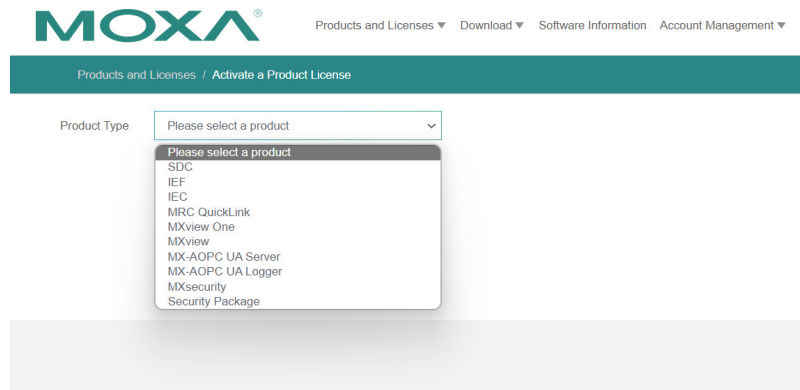
2. Click on the **Moxa License Site** link to open a new browser window for the Moxa Software Licensing site and log in.



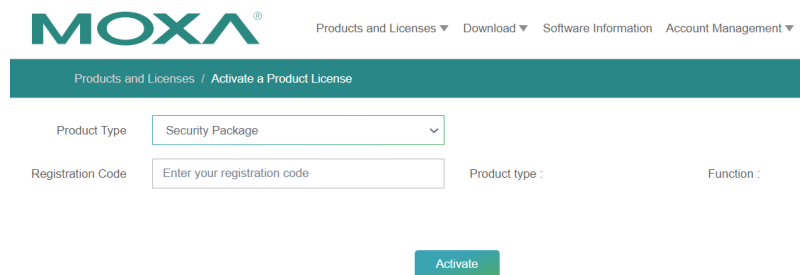
3. Click on the **Products and Licenses** category at the top of the page to expand it, and then select **Activate a Product License**.

Product type	Activate an add-on or renewal License	About to expire (Quantity)
SDC Activation Code	0	0
IEF Activation Code	0	0
IEC Activation Code	0	0
MRC QuickLink Activation Code	0	0
MXview One Activation Code	0	0
MXview Activation Code	0	N/A
MX-ADPC UA Server Activation Code	0	N/A
MX-ADPC UA Logger Activation Code	0	N/A
MXsecurity Activation Code	0	0
Security Package Activation Code	1	0

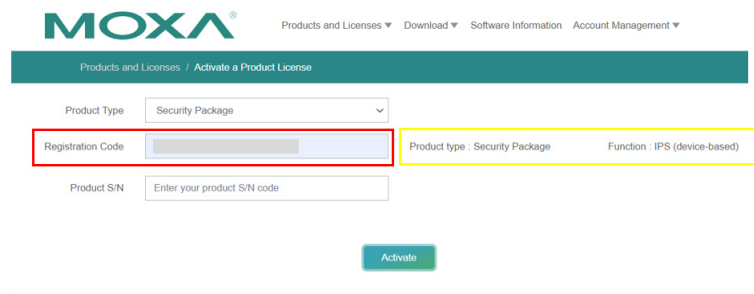
4. Choose the product type for which you want to add a license. In this example, we will be adding a **Security Package**.



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

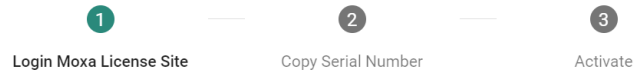


6. Once you click **Activate**, the **Product S/N** (Serial Number) will be displayed, and additional information will appear on the right side of the page.



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

## Add New License

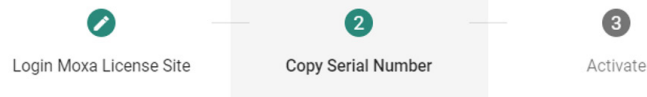


1. Login [Moxa License Site](#) .
2. Choose "Activate a Product License" and product type "Security Package" on the site.
3. Key in the Registration Code and Serial Number on Moxa License Site. Serial Number would be get at the next step.

CLOSE **NEXT**

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

## Add New License



Copy the Serial Number to [Moxa License Site](#) .

Serial Number:

CLOSE **NEXT**

The screenshot shows the Moxa website interface for activating a license. The page title is 'MOXA®' with navigation links for 'Products and Licenses', 'Download', 'Software Information', and 'Account Management'. The breadcrumb trail is 'Products and Licenses / Activate a Product License'. The form includes a 'Product Type' dropdown menu set to 'Security Package', a 'Registration Code' field, and a 'Product S/N' field which is highlighted with a red box. Below the form is an 'Activate' button. The page also displays 'Product type : Security Package' and 'Function : IPS (device-based)'.

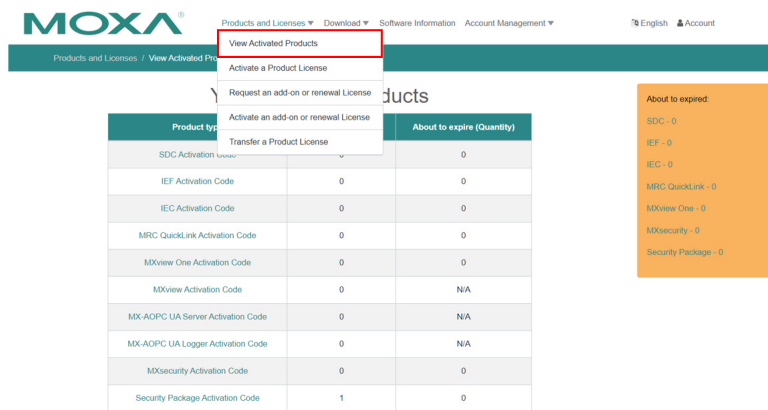
9. A message notification page will appear to confirm that your registration code was successfully activated.

## Message notification

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

I know

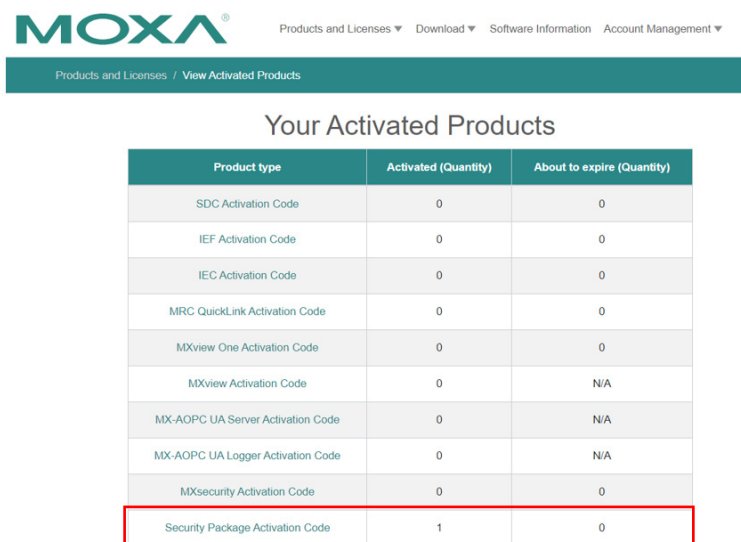
10. In the Software Licensing window, click on **Products and Licenses** to expand it, then select **View Activated Products**.



The screenshot shows the MOXA Software Licensing interface. The 'Products and Licenses' menu is expanded, and 'View Activated Products' is highlighted with a red box. Below the menu, a table displays the activated products and their quantities.

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

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

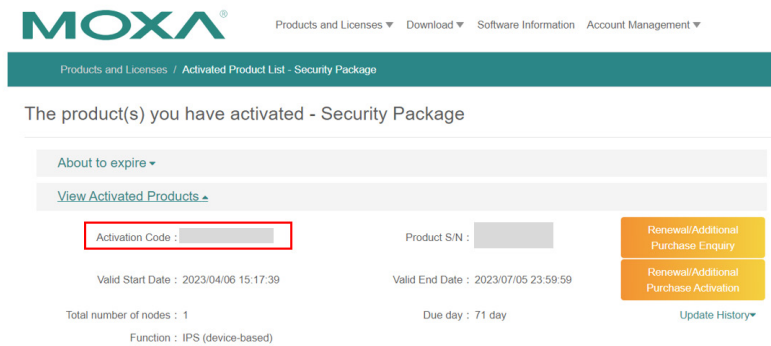


The screenshot shows the MOXA Software Licensing interface with the 'Your Activated Products' table. The 'Security Package Activation Code' row is highlighted with a red box.

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



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



MOXA® Products and Licenses ▾ Download ▾ Software Information Account Management ▾

Products and Licenses / Activated Product List - Security Package

The product(s) you have activated - Security Package

About to expire ▾

[View Activated Products ▾](#)

Activation Code :

Product S/N :

Valid Start Date : 2023/04/06 15:17:39 Valid End Date : 2023/07/05 23:59:59

Total number of nodes : 1 Due day : 71 day

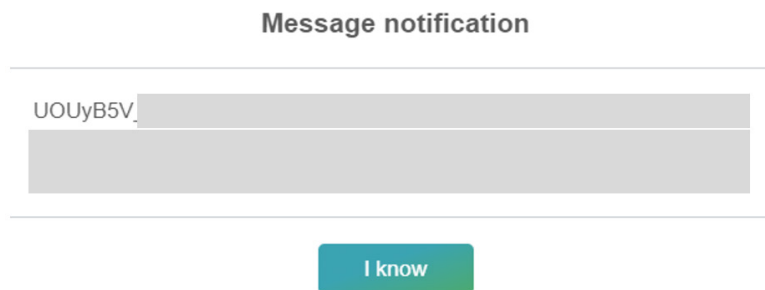
Function : IPS (device-based)

[Renewal/Additional Purchase Enquiry](#)

[Renewal/Additional Purchase Activation](#)

[Update History](#)

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

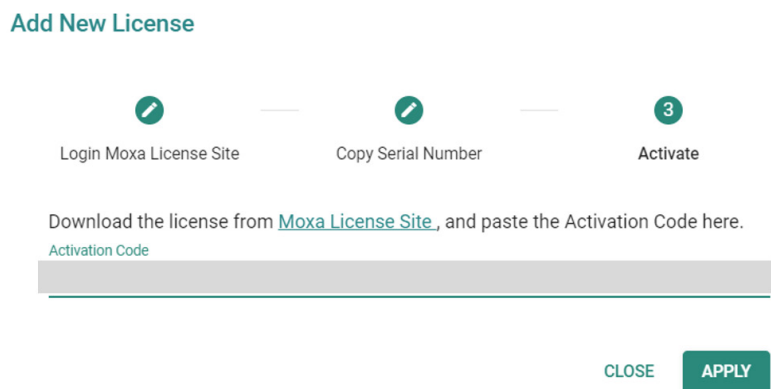


Message notification

UOUyB5V

[I know](#)

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



Add New License

Login Moxa License Site  Copy Serial Number  3 Activate

Download the license from [Moxa License Site](#), and paste the Activation Code here.

Activation Code


[CLOSE](#) [APPLY](#)

## End Result

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


**License Management**

**Overview**


 Name: IPS-DEVICE  
 Valid Durations (days): 71  
 Start Date: 2023-04-06 03:17:39  
 End Date: 2023-07-05 11:59:59  
 Status: Valid  
[Get New License Here](#)

**ADD NEW LICENSE**

**License History**


Q Search

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

## Management Interface

### Menu Path: System > Management Interface

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

This section includes these pages:

- Out of Band Management
- User Interface
- Hardware Interface
- SNMP
- Moxa Remote Connect
- MXsecurity

## Out of Band Management

### Menu Path: System > Management Interface > Out of Band Management

This page lets you enable and monitor your device's out of band management port, which segregates traffic from the LAN port to provide a fully isolated and more secure Ethernet connection. This port uses an independent IP address so users can securely connect and configure devices without interfering with operational traffic.

**Note**

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

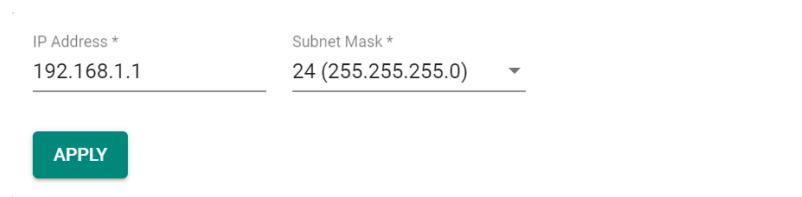
This page includes these tabs:

- Settings
- Status

## Out of Band Management - Settings

**Menu Path:** System > Management Interface > Out of Band Management - Settings

This page lets you configure the settings of your device's out of band management port.



IP Address \* 192.168.1.1 Subnet Mask \* 24 (255.255.255.0) ▾

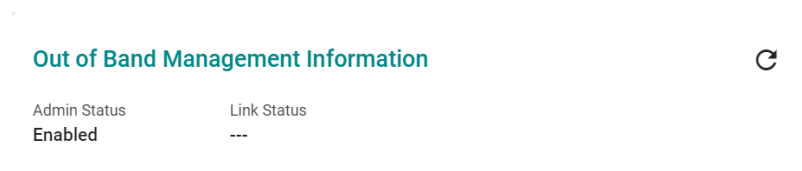
APPLY


UI Setting	Description	Valid Range	Default Value
<b>IP Address</b>	Specify the IP address to use for the out of band management port.	Valid IP address	192.168.1.1
<b>Subnet Mask</b>	Specify the subnet mask to use for the out of band management port.	Valid subnet mask	24 (255.255.255.0)

## Out of Band Management - Status

**Menu Path:** System > Management Interface > Out of Band Management - Settings

This page lets you view the status of your device's out of band management port.



Out of Band Management Information 

Admin Status Enabled Link Status ---

UI Setting	Description
<b>Admin Status</b>	Shows whether the out of band management port is enabled or disabled. Refer to <b>System &gt; Management Interface &gt; Hardware Interface</b> for more information.


UI Setting	Description
------------	-------------

<b>Link Status</b>	Shows the link status of the out of band management port.
--------------------	---

## 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.



## User Interface

HTTP	TCP Port (HTTP) *
Enabled <input type="checkbox"/>	80
	80, 1024 - 65535
HTTPS	TCP Port (HTTPS) *
Enabled <input type="checkbox"/>	443
	443, 1024 - 65535
Telnet	TCP Port (Telnet) *
Enabled <input type="checkbox"/>	10023
	23, 1024 - 65535
SSH	TCP Port (SSH) *
Enabled <input type="checkbox"/>	22
	22, 1024 - 65535
Ping Response	
WAN, LAN, lan1, lan_...	
Moxa Service	
Enabled <input type="checkbox"/>	
TCP Port for Moxa Service (Encrypted)	
443	
UDP Port for Moxa Service (Encrypted)	
40404	
Maximum Number of Login Sessions for HTTP+HTTPS *	
5	
1 - 10	
Maximum Number of Login Sessions for Telnet+SSH *	
5	
1 - 5	

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>HTTP</b>	Enable or disable HTTP connections.	Enabled / Disabled	Enabled


UI Setting	Description	Valid Range	Default Value
<b>TCP Port (HTTP)</b>	Set the TCP port number for HTTP.	80, 1024 to 65535	80
<b>HTTPS</b>	Enable or disable HTTPS connections. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>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.</p> </div> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>The encryption algorithm of keys should be selected based on internationally recognized and proven security practices and recommendations.</p> <p>The lifetime of certificates generated for web server (HTTPS) services should be short and in accordance with the organization's security procedures and requirements.</p> </div>	Enabled / Disabled	Enabled
<b>TCP Port (HTTPS)</b>	Set the TCP port number for HTTPS.	443, 1024 to 65535	443
<b>Telnet</b>	Enable or disable HTTPS connections.	Enabled / Disabled	Enabled
<b>TCP Port (Telnet)</b>	Set the TCP port number for Telnet.	23, 1024 to 65535	23
<b>SSH</b>	Enable or disable HTTPS connections.	Enabled / Disabled	Enabled
<b>TCP Port (SSH)</b>	Set the TCP port number for SSH.	22, 1024 to 65535	22

UI Setting	Description	Valid Range	Default Value
<b>Ping Response</b>	<p>Tick the selected interface to be ping.</p> <p> <b>Note</b> To ping selected interface, make sure the interface is checked in <b>Ping Response</b>.</p>	Drop-down check box	N/A
<b>MOXA Service</b>	<p>Enable or disable the MOXA Service.</p> <p> <b>Note</b> Moxa Service is only used for Moxa network management software. Moxa Service is only available for user accounts with admin privileges.</p>	Enabled / Disabled	Enabled
<b>TCP Port for Moxa Service (Encrypted)</b>	The TCP port number for Moxa Service. This setting cannot be changed.	443	443
<b>UDP Port for Moxa Service (Encrypted)</b>	The UDP port number for Moxa Service. This setting cannot be changed.	40404	40404
<b>Maximum Number of Login Sessions for HTTP+HTTPS</b>	Set the maximum combined number of users that can be logged in to the Moxa Router using HTTP and HTTPS.	1 to 10	5
<b>Maximum Number of Login Sessions for Telnet+SSH</b>	Set the maximum combined number of users that can be logged in to the Moxa Router using Telnet and SSH.	1 to 5	5

## Hardware Interface (all products except TN Series)

**Menu Path:** [System](#) > [Management Interface](#) > [Hardware Interface](#)

This section lets you configure the additional hardware interfaces for your device.

 **Note**

Available settings will vary depending on your product model.

USB Function \*
Out of Band Interface \*

Disabled ▾
Enabled ▾

APPLY

UI Setting	Description	Valid Range	Default Value
<b>USB Function</b>	Enable or disable the USB interface on the device.	Enabled / Disabled	Enabled
<b>Out of Band Interface</b>	Enable or disable the out of band port on the device.	Enabled / Disabled	Enabled

## Hardware Interface (TN Series only)

**Menu Path:** [System](#) > [Management Interface](#) > [Hardware Interface](#)

This page lets you configure the additional hardware interfaces for your device.

This page includes these tabs:

- USB
- Fault LED

### USB

**Menu Path:** [System](#) > [Management Interface](#) > [Hardware Interface - USB](#)

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

USB Function \*  
Disabled ▾

APPLY

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



## Fault LED

**Menu Path: System > Management Interface > Hardware Interface - Fault LED**

This page lets you select the behavior of the Fault LED.

LED Mode

Moxa Default / System Fault Alarm

Advanced / Configuration Change Alarm

**APPLY**

Fault LED Mode Option Description

	Moxa Default	Advanced
Off	Device is operating normally	Device is operating normally
On	System Fault	System Fault
Rapid blinking for 6 sec	N/A	Configuration Importing and Saving

UI Setting	Description	Valid Range	Default Value
<b>LED Mode</b>	Select the behavior mode to use for the Fault LED. <b>Moxa Default / System Fault Alarm:</b> The Fault LED will be off when the device is operating normally, and on when there is a system fault. <b>Advanced / Configuration Change Alarm:</b> The Fault LED will be off when the device is operating normally, and on when there is a system fault. When the device configuration is being imported and saved, the Fault LED will blink rapidly for 6 seconds.	Moxa Default / Advanced	Moxa Default

## SNMP

**Menu Path: System > Management Interface > SNMP**

This section lets you configure SNMP settings for your device.

There are two tabs in this section:

- General
- SNMP Account

## SNMP - General

**Menu Path: System > Management Interface > SNMP - General**

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

### **Limitations**

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

**SNMP**

General | SNMP Account

SNMP Version \*  
V1, V2c, V3

User-Defined Engine ID  
Disabled

Community Name 1 \*  
public  
6 / 64

Access Control 1 \*  
Read Only

Community Name 2 \*  
private  
7 / 64

Access Control 2 \*  
Read Write

APPLY

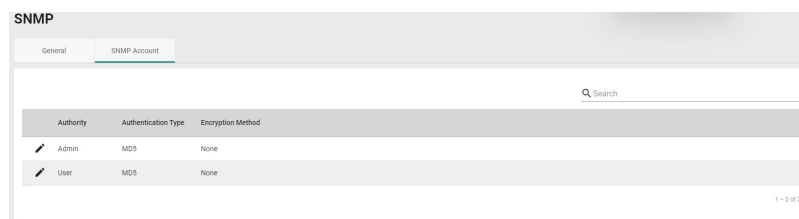
UI Setting	Description	Valid Range	Default Value
<b>SNMP Version</b>	Specify the SNMP protocol version used to manage your device. <b>Disabled:</b> Disable SNMP. <b>V1, V2c, V3:</b> Enable SNMP V1, V2c, and V3. <b>V1, V2c:</b> Enable SNMP V1, V2c only. <b>V3 only:</b> Enable SNMP V3 only.	Disabled / V1, V2c, V3 / V1, V2c / V3 only	Disabled
<b>User-Defined Engine ID</b> <b>(Only for SNMP Version is V1, V2c, V3 or V3 only)</b>	Enable or disable use of a user-defined engine ID. If disabled, the system will use the default engine ID.	Disabled / Enabled	Disabled

UI Setting	Description	Valid Range	Default Value
<b>Engine ID</b>	Specify an engine ID to manage your device. If <b>User-Defined Engine ID</b> is disabled, the engine ID will be view-only.	2 to 54 hexadecimal character string. The length of the string must be even.	800021f305
<b>Community Name 1</b>	Specify a community string name match to use for authentication.	1 to 64 characters	public
<b>Community Name 2</b>	Specify a community string name match to use for authentication.	1 to 64 characters	private
<b>Access Control 1</b>	Specify the access control type to use when Community String 1 is matched.	Read Write / Read only / No Access	Read Only
<b>Access Control 2</b>	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
<b>Authority</b>	Shows authority level of the management account. <b>admin:</b> Can read/write configuration settings. <b>user:</b> Can only read configuration settings.
<b>Authentication Type</b>	Shows the authentication type used for the account.
<b>Encryption Method</b>	Shows the encryption method used for the account.

## Edit SNMP Account Settings


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

Clicking the **Edit** (✎) icon for an account on the **System > Management Interface > SNMP - SNMP Account** page will open this dialog box. This dialog lets you modify the selected account. Click **APPLY** to save your changes.

### Edit SNMP Admin Account Settings

Authentication Type \*  
MD5

Encryption Method \*  
AES

Encryption Key \*   
At least 8 characters 0 / 64


CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Authentication Type</b>	Select which authentication method to use for the account. <b>None:</b> No authentication will be used. <b>MD5:</b> Use MD5 authentication. <b>SHA:</b> Use SHA authentication.	None / MD5 / SHA	None
<b>Encryption Method</b>	Select which encryption method to use for the account.	None / DES / AES	None
<b>Encryption Key</b> (if Encryption Method is DES or AES)	Specify an encryption password for the account.	8 to 64 characters	N/A

## Moxa Remote Connect

**Menu Path:** System > Management Interface > Moxa Remote Connect

This section lets you establish a connection to the MRC Quick Link cloud platform to monitor and remotely access your device. Visit the [Moxa Remote Connect Suite](#) page for more information.

 **Note**

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

There are two tabs in this section:

- Settings
- Status

## Moxa Remote Connect - Settings

**Menu Path:** [System](#) > [Management Interface](#) > [Moxa Remote Connect - Settings](#)

This page lets you enable or disable MRC service and configure its connection parameters.

### MRC

Click **APPLY** to activate the device in MRC Quick Link.

Click **RESET KEY** to unbind the device from MRC Quick Link.

 **Note**

When the gateway exhibits any of the following behaviors, it will appear as offline in MRC Quick Link:

- Clicking RESET KEY in the MRC settings page of the gateway web console
- Clicking Reset to Defaults in the gateway web console
- Physically pressing the reset button on the hardware

To reactivate the gateway, you will need to perform the deactivate function and download a new activation key in MRC Quick Link and then enter it into the gateway, or create a new gateway in MRC Quick Link and enter a new key into the gateway.

**MRC**

MRC Service \*  
 Disabled ▾


Activation Type \*  
 Enter Activation Key ▾    Activation Key \_\_\_\_\_

**Bridge IP Configuration** ⓘ

IP Address \*                      Subnet Mask \*  
 192.168.126.254                  24 (255.255.255.0) ▾

Bridge Member \*                  ⓘ

**APPLY**    RESET KEY

UI Setting	Description	Valid Range	Default Value
<b>MRC Service</b>	Enable or disable the MRC service for establishing remote access connections.	Enabled / Disabled	Disabled
<b>Activation Type</b>	Select the Activation Type. <b>Enter Activation Key:</b> Manually enter an activation key for authentication. <b>Import from USB drive:</b> Insert a USB drive that has an activation key on it for authentication.	Enter Activation Key / Import from USB	Enter Activation Key
	<p> <b>Note</b></p> <p>To use this, USB functionality must be enabled in <b>System &gt; Management Interface &gt; Hardware Interface</b>.</p>		

### Bridge IP Configuration

UI Setting	Description	Valid Range	Default Value
<b>IP Address</b>	Specify an IP address for the bridge.	Valid IP address	192.168.126.254
<b>Subnet Mask</b>	Specify a subnet mask for the bridge.	Valid subnet mask	24(255.255.255.0)

UI Setting	Description	Valid Range	Default Value
<b>Bridge Member</b>	<p>Select which ports will be members of the bridge.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> <p><b>Note</b></p> <p>Only devices connected to the Bridge port can be remotely accessed via MRC service. Please ensure that the device's IP and the Bridge IP are set within the same subnet.</p> </div> <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b></p> <p>Bridge members are limited to LAN ports only. If any port is used as a WAN port, please do not add that port as a bridge member to avoid affecting the WAN network settings.</p> </div>	Drop-down list of ports	N/A

## Tunnel Control Settings

### Tunnel Control Settings

Tunnel Control ▼

---

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Tunnel Control</b>	<p>Select the Tunnel Control Type.</p> <p><b>Persistent Connection:</b> Always establish a tunnel for remote access.</p> <p><b>Controlled by Key file from USB drive:</b> Establish a tunnel for remote access only when a USB containing the key is inserted into the device.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p><b>Note</b></p> <p>This feature requires <b>USB Function</b> to be enabled in <b>System &gt; Management Interface &gt; Hardware Interface</b>.</p> </div> <p><b>Controlled by DI:</b> Establish a tunnel for remote access only when the Digital Input is detected as On.</p>	Persistent Connection / Controlled by USB Key / Controlled by DI	Permanent Connection

## Moxa Remote Connect - Status

**Menu Path:** System > Management Interface > Moxa Remote Connect - Status

This page lets you view the status and details of your Moxa Remote Connect connection.

### MRC Status

This shows the current status of your MRC connection.



UI Setting	Description
<b>Internet</b>	<p>Shows the status of your device's Internet connection.</p> <p><b>Green:</b> The device is connected to the Internet.</p> <p><b>Red:</b> The device failed to connect to the Internet.</p> <p><b>Gray:</b> The device has not been activated yet.</p>



UI Setting	Description
<b>MRC Cloud</b>	Shows the status of your device's MRC Cloud connection. <b>Green:</b> Connected to MRC Cloud successfully. <b>Red:</b> Failed to connect to MRC Cloud. <b>Gray:</b> Have not tried to connect to MRC Cloud yet.
<b>Key Verification</b>	Shows the status of your device's key verification. <b>Green:</b> Successfully verified the activation key. <b>Red:</b> Failed to verify the activation key. <b>Gray:</b> Have not tried to verify the activation key yet.
<b>Online</b>	Shows the status of your device in MRC Quick Link. <b>Green:</b> Device online. <b>Red:</b> Device offline. <b>Gray:</b> Device not authenticated yet.
<b>Connected</b>	Shows the status of your device's remote connection. <b>Green:</b> Remote connection established successfully. <b>Red:</b> Failed to establish remote connection. <b>Gray:</b> Remote connection not yet established yet.

## MRC Information


### MRC Information

Gateway Name  
 gw\_status\_4302\_test

UI Setting	Description
<b>Gateway Name</b>	Shows the name of this device in MRC Quick Link.

## Local Device List

### Local Device List

Local Device Name	Status	Device Type	IP Address	Virtual IP	Connectivity Check
 device_903	<span style="color: green;">●</span> Online	IP Ethernet Device	192.168.126.3	10.11.64.2	Ping Check (10 sec.)

UI Setting	Description
<b>Local Device Name</b>	Shows the name of the local device connected to this device.
<b>Status</b>	Shows the connection status of the local device.
<b>Device Type</b>	Shows the type of the local device. (IP Ethernet Device / Layer 2 Ethernet Device / Serial Device)
<b>IP Address</b>	Shows the IP address of the local device.
<b>Virtual IP</b>	Shows the virtual IP address of the local device that is assigned by the MRC Quick Link server.
<b>Connectivity Check</b>	Shows how the local device's alive status will be checked for connectivity.

## MXsecurity

### Menu Path: [System](#) > [Management Interface](#) > [MXsecurity](#)

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

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

#### **Note**

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

## MXsecurity

### Connection Status

Status	Connecting	Package Version	1.0.0017
Service Address	3.129.140.152	Profile Synchronization	---

---

### New Connection

Service Address

0 / 64

HTTPS Port

1 - 65535

Communication Port

1 - 65535

**CONNECT**

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

## Time

### Menu Path: System > Time

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

This section includes these pages:

- System Time
- NTP/SNTP Server

## System Time

### Menu Path: System > Time > System Time

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

This page includes these tabs:

- Time
- Time Zone
- NTP Authentication

#### 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 > System Time - Time

This page lets you set the system time and date.

You can set your system time using these clock sources:

- Local
- SNTP Time
- NTP Time

### Local Time

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

## System Time

Time
Time Zone
NTP Authentication

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

---

Clock Source  
Local ▼

Date \*  
1970-04-18 📅

Time  
上午 11:13 🕒

APPLY
SYNC FROM BROWSER

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

### SNTP Time

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

## System Time

Time
Time Zone
NTP Authentication

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

---

Clock Source  
SNTP

Time Server 1  
0 / 39

Time Server 2  
0 / 39

**APPLY**

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

### NTP Time

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

## System Time

Time
Time Zone
NTP Authentication

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

---

Clock Source  
NTP

Time Server 1  
0 / 39

Time Server 2  
0 / 39

Authentication  
Disabled

Authentication  
Disabled

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Current Time</b>	This shows the device's current system date, time, and time zone.	N/A	N/A
<b>Time Server 1</b>	Set the IP or domain address of the primary time server (e.g., 192.168.1.1, <a href="http://time.stdtime.gov.tw">time.stdtime.gov.tw</a> , or <a href="http://time.nist.gov">time.nist.gov</a> ).	IP address or domain, 1 to 39 characters	N/A
<b>Time Server 2</b>	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
<b>Authentication</b>	Specify whether to disable or use a key ID for NTP server authentication. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 5px;">To use authentication, set up the Key ID value in the <b>NTP Authentication</b> tab first. After setting it up, it will become available in the <b>Authentication</b> drop-down.</div>	Disabled / Key IDs created in the <b>NTP Authentication</b> tab	Disabled

## System Time - Time Zone

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

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

**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.

**System Time**

Time    Time Zone    NTP Authentication

Time Zone  
(UTC+08:00)Taipei

Daylight Saving  
Daylight Saving Status  
Disabled

APPLY

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

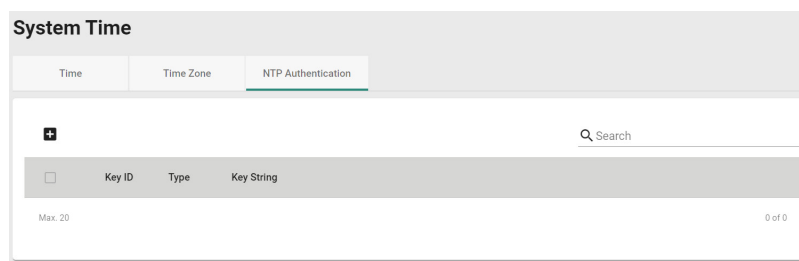


UI Setting	Description	Valid Range	Default Value
<b>Hour (if Daylight Saving Status is Enabled)</b>	Set the hour Daylight Saving time begins/ends.	User-specified hour	00
<b>Minutes (if Daylight Saving Status is Enabled)</b>	Set the minute Daylight Saving time begins/ends.	User-specified minute(s)	00

## System Time - NTP Authentication

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


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

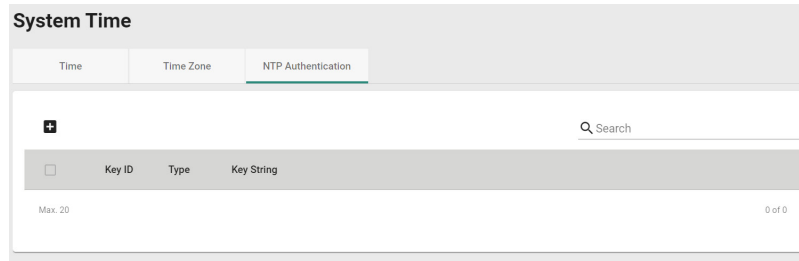


UI Setting	Description
<b>Key ID</b>	Shows the key ID for the authentication key.
<b>Type</b>	Shows the type of NTP authentication the key uses. <b>MD5:</b> Uses authentication based on MD5 algorithms. <b>SHA:</b> Uses authentication based on SHA-512 algorithms.
<b>Key String</b>	Shows the key string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

### Create Entry

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


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



### Create Entry

Key ID \*  
 1 - 65535

Type \*  
 ▼

Key String \*   
 0 / 32

CANCEL

CREATE

UI Setting	Description	Valid Range	Default Value
<b>Key ID</b>	Specify the key ID to use for the authentication key.	1 to 65535 characters	N/A
<b>Type</b>	Specify the type of NTP authentication the key should use.  <b>MD5:</b> Sets authentication based on MD5 algorithms. <b>SHA:</b> Sets authentication based on SHA-512 algorithms.	MD5 / SHA-512	N/A
<b>Key String</b>	Specify the key string to use for the authentication key.	1 to 32 characters	N/A

### Edit Entry

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

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


**Note**

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

### Edit Entry Settings

Key ID  
1  
1 - 65535

Type \*  
MD5

Key String \*   
0 / 32

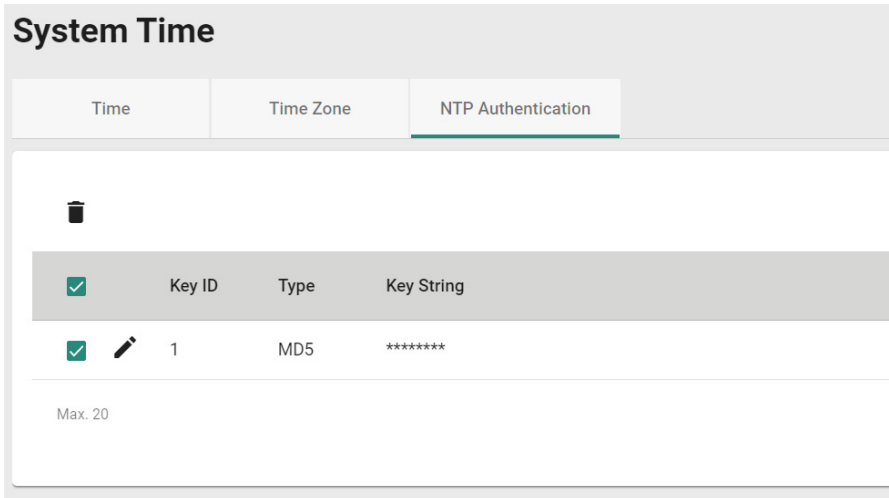
CANCEL

APPLY

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

### Delete Entry

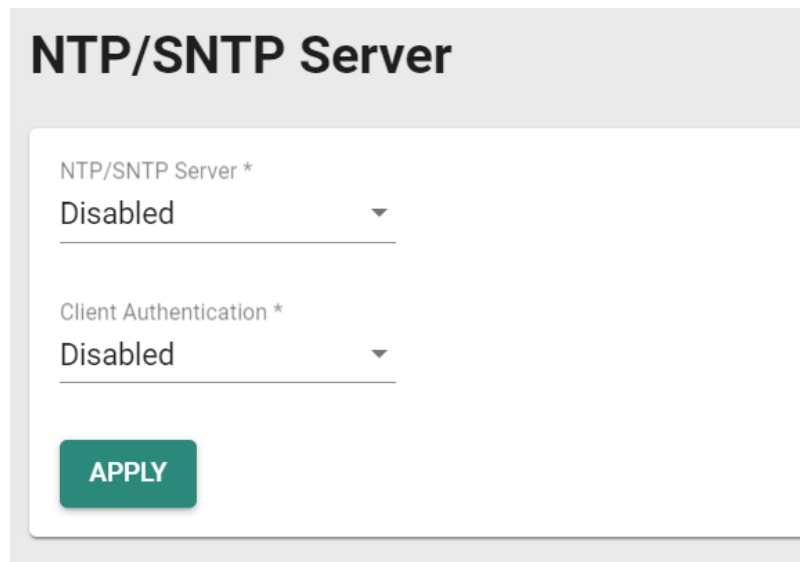
You can delete authentication keys by using the checkboxes to select the keys you want to delete, then clicking the **Delete (🗑)** icon.



## 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
<b>NTP/SNTP Server</b>	<p>Enable or disable NTP/SNTP server functionality for clients:</p> <p><b>Enabled:</b> Enable NTP/SNTP server functionality for clients.</p> <p><b>Disabled:</b> Disabled NTP/SNTP server functionality for clients.</p>	<b>Enabled / Disabled</b>	<b>Disabled</b>
<b>Client Authentication</b>	<p>Enable or disable client authentication of NTP/SNTP server:</p> <p><b>Enabled:</b> Enable Client Authentication functionality for clients.</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p><b>Note</b></p> <p>Before enabling Client Authentication, you will need to create NTP authentication keys first.</p> <p>Refer to <b>System &gt; System Time - NTP Authentication</b> for more information.</p> </div> <p><b>Disabled:</b> Disable Client Authentication functionality for clients.</p>	<b>Enabled / Disabled</b>	<b>Disabled</b>

## Power Management

### Menu Path: System > Power Management

This page lets you configure the power management features of your device.

#### **Note**

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

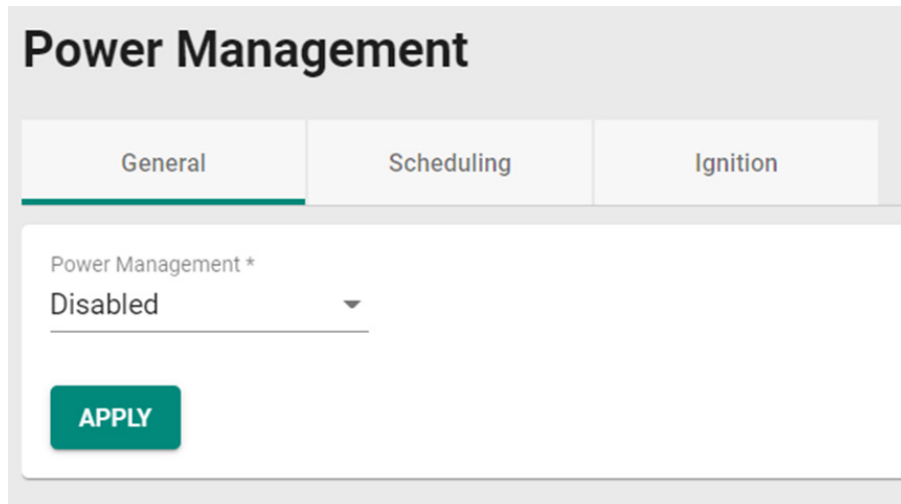
This page includes these tabs:

- General
- Scheduling
- Ignition

## Power Management - General

### Menu Path: System > Power Management - General

This page lets you enable power management for your device. If enabled, you can control how and when the device enters a power-saving state. If disabled, the device will never enter power-saving mode.



UI Setting	Description	Valid Range	Default Value
<b>Power Management</b>	<p>Select a power management setting for your device.</p> <p><b>Disabled:</b> Disables power management.</p> <p><b>Scheduling:</b> Enables power-saving mode based on a schedule you define. Refer to Scheduling for more details.</p> <p><b>Ignition:</b> Enables power-saving mode based on signals sent to the digital input, allowing the device to enter power-saving mode when a vehicle ignition is off.</p>	Disabled / Scheduling / Ignition	Disabled

## Power Management - Scheduling

### Menu Path: System > Power Management - Scheduling

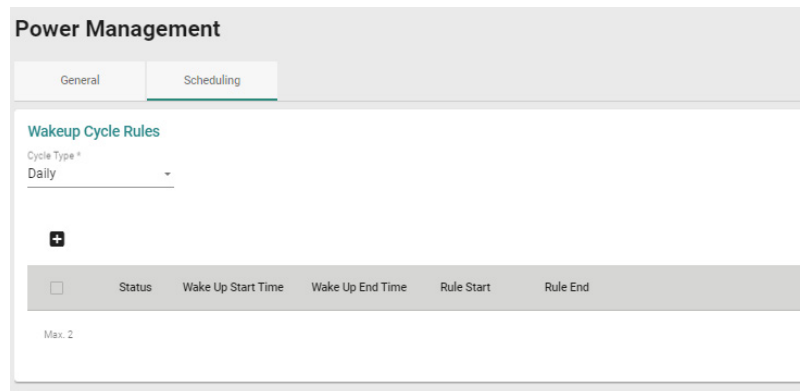
This page lets you create both one-time and repeating schedules to determine when the device should enter and leave power-saving mode.

## 🔔 Limitations

You can create up to 2 cycle rules, and up to 12 one-time rules.

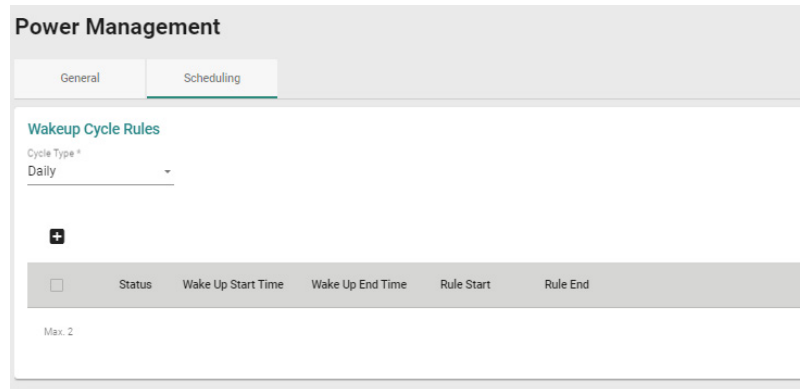
- Both cycle rules must use the same Cycle Type. If the Cycle Type is changed, all existing cycle rules will be deleted.
- If the Cycle Type is set to Weekly or Monthly, the start and end times must be within the same day. If you need the start and end times to be on different days, create a One Time Rule.

## Wakeup Cycle Rules



UI Setting	Description	Valid Range	Default Value
<b>Cycle Type</b>	<p>Select a wakeup cycle to use for power-saving mode scheduling.</p> <p><b>Hourly:</b> The device will enter and leave power-saving mode according to specific times every hour.</p> <p><b>Daily:</b> The device will enter and leave power-saving mode according to specific times every day.</p> <p><b>Weekly:</b> The device will enter and leave power-saving mode according to specific times on specific days of the week. Multiple days of the week may be selected.</p> <p><b>Monthly:</b> The device will enter and leave power-saving mode according to specific times on specific days of the month. Multiple days of the month may be selected.</p>	Hourly / Daily / Weekly / Monthly	Daily

## Wakeup Cycle Rule List



UI Setting	Description
<b>Status</b>	Shows the status of the wakeup cycle rule.
<b>Wake Up Start Time</b>	Shows when the device will leave power-saving mode. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 5px;">The units shown will vary depending on the wakeup cycle type used.</div>
<b>Wake Up End Time</b>	Shows when the device will enter power-saving mode. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 5px;">The units shown will vary depending on the wakeup cycle type used.</div>
<b>Rule Start</b>	Shows when the wakeup cycle rule will start taking effect.
<b>Rule End</b>	Shows when the wakeup cycle rule will no longer take effect.

## Add Cycle Rule

### Menu Path: System > Power Management - Scheduling

Clicking the **Add (+)** icon in the **Wakeup Cycle Rule List** on the **System > Power Management - Scheduling** page will open this dialog box. This dialog lets you create a new wakeup cycle rule. The options shown will vary depending on what **Cycle Type** is selected.

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



## Add Cycle Rule - Hourly

If the **Cycle Type** is set to **Hourly**, these options will appear.


### Add Cycle Rule


Status \*  
Enabled

Wake Up Start Time \*  
HH:00

Wake Up End Time \*  
HH:15

Rule Schedule

Start Date \* 

End Date \* 

CANCEL

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the cycle rule.	Enabled / Disabled	Enabled
<b>Wakeup Start Time</b>	Specify the minute when the device will leave power-saving mode each hour.	00 to 59	00
<b>Wakeup End Time</b>	Specify the minute when the device will enter power-saving mode each hour.	00 to 59	15
<b>Start Date</b>	Specify when this cycle rule will take effect.	Date	N/A
<b>End Date</b>	Specify when this cycle rule will end.	Date	N/A

## Add Cycle Rule - Daily

If the **Cycle Type** is set to **Daily**, these options will appear.

## Add Cycle Rule

Status \*  
Enabled ▾

Wake Up Start Time  
上午 12:00 ⌚

Wake Up End Time  
上午 12:15 ⌚

### Rule Schedule

Start Date \* 📅

End Date \* 📅

CANCEL

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the cycle rule.	Enabled / Disabled	Enabled
<b>Wakeup Start Time</b>	Specify the hour and minute when the device will leave power-saving mode every day. You can also click the clock icon to select the time from a drop-down list.	Time	12:00 AM
<b>Wakeup End Time</b>	Specify the hour and minute when the device will enter power-saving mode every day. You can also click the clock icon to select the time from a drop-down list.	Time	12:15 AM
<b>Start Date</b>	Specify when this cycle rule will take effect.	Date	N/A
<b>End Date</b>	Specify when this cycle rule will end.	Date	N/A

## Add Cycle Rule - Weekly

If the **Cycle Type** is set to **Weekly**, these options will appear.

## Edit Cycle Rule

Status *	Day(s) of the Week *
Enabled ▾	Mon, Tue, Wed, Thu, F... ▾
Wake Up Start Time	Wake Up End Time
上午 12:00 ⌚	上午 12:15 ⌚

## Rule Schedule

Start Date *
2023-11-21 📅
End Date *
2023-11-28 📅

CANCEL

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the cycle rule.	Enabled / Disabled	Enabled
<b>Day(s) of the Week</b>	Select which days of the week this rule will apply to. You can select multiple days.	Days of the week	N/A
<b>Wakeup Start Time</b>	Specify the hour and minute when the device will leave power-saving mode on the specified <b>Day(s) of the Week</b> . You can also click the clock icon to select the time from a drop-down list.	Time	12:00 AM
<b>Wakeup End Time</b>	Specify the hour and minute when the device will enter power-saving mode on the specified <b>Day(s) of the Week</b> . You can also click the clock icon to select the time from a drop-down list.	Time	12:15 AM
<b>Start Date</b>	Specify when this cycle rule will take effect.	Date	N/A
<b>End Date</b>	Specify when this cycle rule will end.	Date	N/A

## Add Cycle Rule - Monthly

If the **Cycle Type** is set to **Monthly**, these options will appear.

## Edit Cycle Rule

Status *	Enabled	Day(s) of the Month	1,31
		1 - 31, allow comma(,)	day
Wake Up Start Time	上午 12:00	Wake Up End Time	上午 12:15

## Rule Schedule

Start Date *	2023-11-28
End Date *	2023-11-28


CANCEL

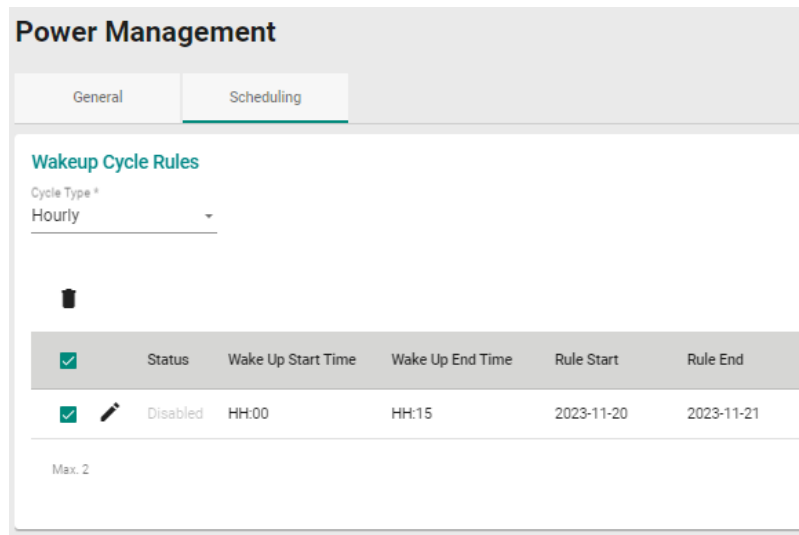
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the cycle rule.	Enabled / Disabled	Enabled
<b>Day(s) of the Month</b>	Select which days of the month this rule will apply to. You can select multiple days by entering a comma in between each day (e.g., 1,2,16). If a month does not have a specified day in it, the rule will be ignored for that day.	1 to 31, multiple days should be separated by a comma	N/A
<b>Wakeup Start Time</b>	Specify the hour and minute when the device will leave power-saving mode on the specified <b>Day(s) of the Month</b> . You can also click the clock icon to select the time from a drop-down list.	Time	12:00 AM
<b>Wakeup End Time</b>	Specify the hour and minute when the device will enter power-saving mode on the specified <b>Day(s) of the Month</b> . You can also click the clock icon to select the time from a drop-down list.	Time	12:15 AM
<b>Start Date</b>	Specify when this cycle rule will take effect.	Date	N/A
<b>End Date</b>	Specify when this cycle rule will end.	Date	N/A

## Delete Cycle Rule

**Menu Path: System > Power Management - Scheduling**

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



## One Time Rule List



UI Setting	Description
<b>Status</b>	Shows the status of the one-time rule.
<b>Type</b>	Shows the type of the one-time rule. <b>Power Saving:</b> The device will enter power-saving mode during the specified period. <b>Wake Up:</b> The device will leave power-saving mode during the specified period.
<b>Rule Start</b>	Shows the rule start date.
<b>Rule End</b>	Shows the rule end date.

## Add One-time Rule

**Menu Path:** [System](#) > [Power Management - Scheduling](#)

Clicking the **Add (+)** icon in the **One Time Rule** list on the **System > Power Management - Scheduling** page will open this dialog box. This dialog lets you create a new one-time rule.



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

### Add One-time Rule



Status \*  
Enabled ▾

Type \*  
Power Saving ▾

**Start**

Start Date \*  Start Time  --:--

**End**


End Date \*  End Time  --:--

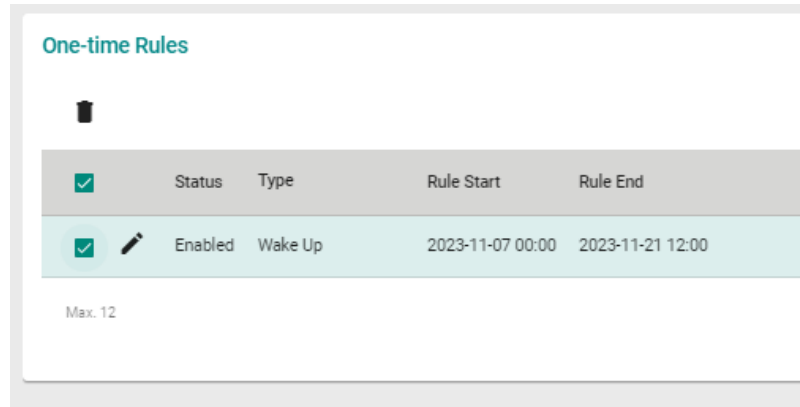
[CANCEL](#) [APPLY](#)

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the one-time rule.	Enabled / Disabled	Enabled
<b>Type</b>	Select the type for the one-time rule. <b>Power Saving:</b> The device will enter power-saving mode during the specified period. <b>Wake Up:</b> The device will leave power-saving mode during the specified period. This requires an active cycle rule.	Power Saving / Wake up	Power Saving
<b>Start Date</b>	Specify the date this one-time rule will take effect.	Date	N/A
<b>Start Time</b>	Specify the time this one-time rule will take effect.	Time	N/A
<b>End Date</b>	Specify the date this one-time rule will end.	Date	N/A
<b>End Time</b>	Specify the time this one-time rule will end.	Time	N/A

## Delete One-time Rule

### Menu Path: System > Power Management - Scheduling

You can delete a one-time rule by using the checkboxes to select the one-time rules you want to delete, then clicking the **Delete** (  ) icon.



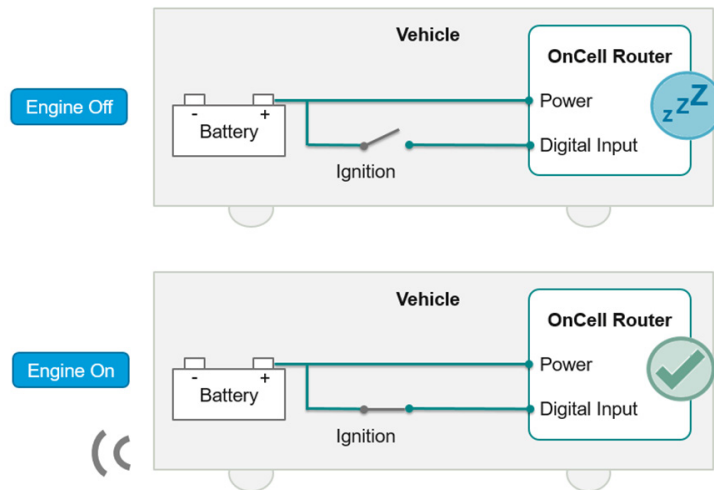
## Power Management - Ignition

### Menu Path: System > Power Management - Ignition

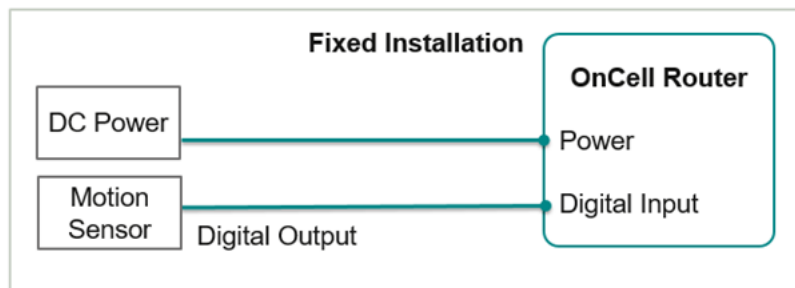
#### Note

The Ignition feature is only applicable to OnCell G4302 hardware rev 1.1 and higher.

This page lets you enable the Ignition feature, which lets you use the digital input to determine when the device should enter and leave power-saving mode. This allows the device to enter and leave power saving modes when a vehicle starts or turns off. The device detects the ignition status through the digital input, and the device will enter power saving mode when the vehicle ignition is off to save battery power.



This feature can also use on fixed installations with an I/O to monitor an external device such as a motion sensor. You can configure the I/O line to wake the device or put the device in power saving mode.



General	Scheduling	Ignition
Wakeup DI Status *		
Low		
DI Sensing Time		
5		
5 - 3600 sec.		
Power Saving Delay Time		
15		
0 - 15 min.		
APPLY		



UI Setting	Description	Valid Range	Default Value
<b>Wakeup DI Status</b>	Select the DI status when waking up the device. <b>High:</b> The device will leave power saving mode when it detects the DI high and enters power saving mode when it detects DI is low. <b>Low:</b> The device will leave power saving mode when it detects the DI is low and enters power saving mode when it detects DI is high.	High / Low	High
<b>DI Sensing Time</b>	Enter the number of seconds the DI status must remain changed for before the device determines there is a change in DI status. This is useful for avoiding erratic behavior when the DI signal is unstable.	5-3600	5
<b>Power Saving Delay Time</b>	Enter the number of minutes to delay entering enter power saving mode after the vehicle's ignition shuts off. This is useful if you want to maintain a network connection while the vehicle's engine is off for a short period of time.	0-15	15

## SMS

### Menu Path: System > SMS

This page allows you to configure your device's SMS settings.

When a cellular connection is not available or if there is limited service, SMS provides an emergency recovery mechanism and a way for performing out-of-band management. The remote SMS control feature helps you get the current cellular status of the device, re-establish the cellular connection, and restart the system by sending specific SMS messages to the device. To ensure the security of out-of-band communication, the SMS function supports password protection and trusted number authentication. With wireless out-of-band management, engineers can control and troubleshoot remote devices, avoiding costly onsite visits by service technicians and minimizing service downtime.

#### Note

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

#### Note

When sending remote control SMS messages, wait 30 seconds between each message to ensure optimal system stability.

This settings area includes these sections:

- General

- Remote Control List
- Send SMS

## SMS - General

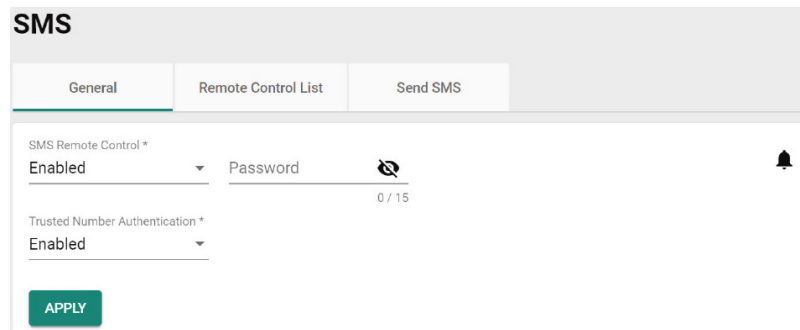
### Menu Path: System > SMS - General


This page lets you configure basic SMS settings and the trusted number list.

#### Limitations

You can add up to 4 trusted numbers.


## SMS Settings



UI Setting	Description	Valid Range	Default Value
<b>SMS Remote Control</b>	Enable or disable SMS remote control. If enabled, the device can be controlled remotely through specific SMS messages. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>The cellular module must be enabled for this feature. Refer to Cellular for more information.</p> </div>	Enabled / Disabled	Enabled
<b>Password</b>	Specify the required password in SMS remote control message format: @password@command	0 to 15 characters	N/A
<b>Trusted Number Authentication</b>	Enable or disable trusted number authentication. If enabled, the device will only accept SMS messages from numbers added to the Trusted Numbers List. If disabled, the device can be controlled by messages sent from any number. Refer to Add Trusted Number Entry.	Enabled / Disabled	Enabled

## Trusted Number List

Trusted Number List




<input type="checkbox"/>	Name	Country Code	Number

Max: 4 0 of 0

UI Setting	Description
<b>Name</b>	Shows the name used to identify the trusted number.
<b>Country Code</b>	Shows the country code for the trusted number.
<b>Number</b>	Shows the trusted number.

### Add Trusted Number Entry

Clicking the **Add** () icon on the **SMS > General > Trusted Number List** will open this dialog box. This dialog lets you create a new trusted number list. Click **CREATE** to save your changes and add the new trusted number.

#### Add Trusted Number Entry

Name \*

0 / 15

+ Country Code \*  Number \*

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name to help identify the number. This is for reference only.	1 to 15 characters	N/A
<b>Country Code</b>	Specify the country code of the number.	Valid country code	N/A

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Number</b>	Enter the phone number.	Valid phone number	Enabled
---------------	-------------------------	--------------------	---------

### Edit Trusted Number Entry

Clicking the **Edit** (✎) icon for an account on the **SMS > General > Trusted Number List** will open this dialog box. This dialog lets you edit an existing trusted number list. Click **APPLY** to save your changes.

Trusted Number List

🔍 Search

<input type="checkbox"/>	Name	Country Code	Number
<input type="checkbox"/>	✎ Moxa 1	886	0911111111
<input type="checkbox"/>	✎ Moxa 2	886	0912222222
<input type="checkbox"/>	✎ Moxa 3	886	0913333333
<input type="checkbox"/>	✎ Moxa 4	886	0914444444

Max. 4

### Edit Trusted Number Entry

Name \*

Moxa 1

6 / 15

Country Code \*      Number \*

+ 886                      0911111111

CANCEL

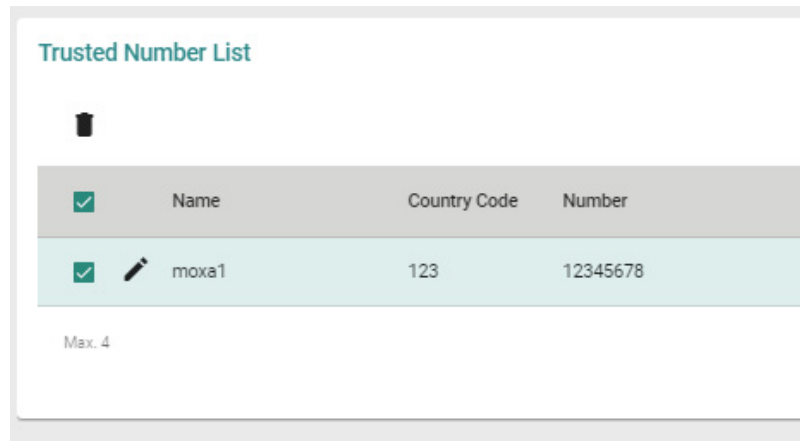
APPLY

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Name</b>	Specify a name to help identify the number. This is for reference only.	1 to 15 characters	N/A
<b>Country Code</b>	Specify the country code of the number.	Country code	N/A
<b>Number</b>	Enter the phone number.	Phone number	Enabled

## Delete Trusted Number Entry

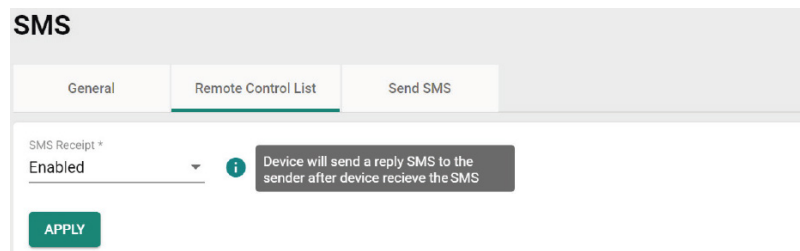
You can delete trusted numbers by using the checkboxes to select the ones you want to delete, then clicking the **Delete (🗑)** icon.



## Remote Control List

This page lets you manage the remote control commands your device will respond to.


## Remote Control List Settings

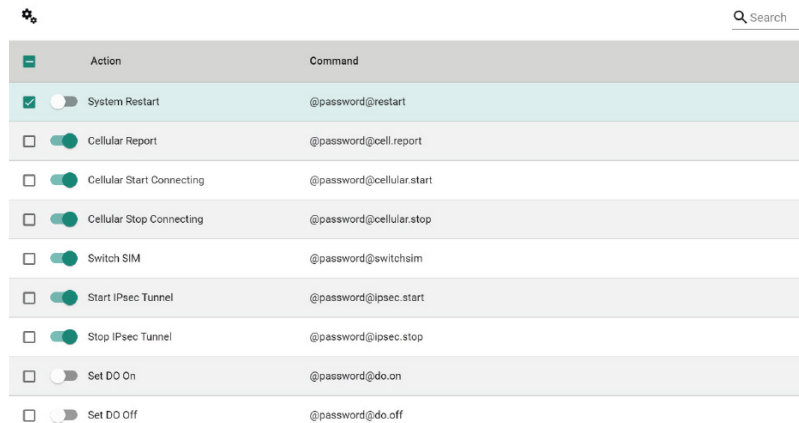


UI Setting	Description	Valid Range	Default Value
<b>SMS Receipt</b>	Enable or disable SMS receipts. If enabled, the device will send a confirmation SMS when receiving a command SMS.	Enabled / Disabled	Enabled

## Remote Control Command List

Use the toggle buttons to enable or disable the corresponding SMS command. Alternatively, check the boxes of the commands you want to manage and use the Quick

Setting (  ) icon to enable or disable the selected commands in bulk. Refer to the table below for an overview of each command.

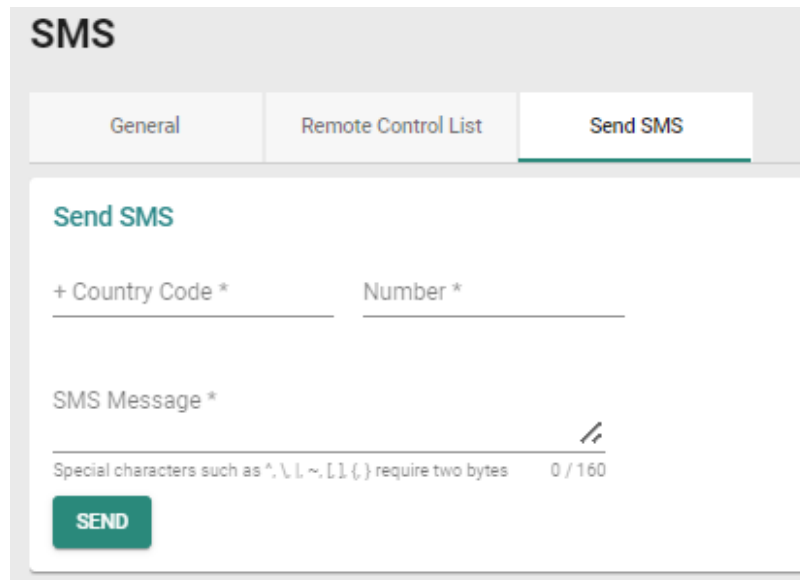


Action	Command
<input checked="" type="checkbox"/> <input type="checkbox"/> System Restart	@password@restart
<input type="checkbox"/> <input type="checkbox"/> Cellular Report	@password@cell.report
<input type="checkbox"/> <input type="checkbox"/> Cellular Start Connecting	@password@cellular.start
<input type="checkbox"/> <input type="checkbox"/> Cellular Stop Connecting	@password@cellular.stop
<input type="checkbox"/> <input type="checkbox"/> Switch SIM	@password@switchsim
<input type="checkbox"/> <input type="checkbox"/> Start IPsec Tunnel	@password@ipsec.start
<input type="checkbox"/> <input type="checkbox"/> Stop IPsec Tunnel	@password@ipsec.stop
<input type="checkbox"/> <input type="checkbox"/> Set DO On	@password@do.on
<input type="checkbox"/> <input type="checkbox"/> Set DO Off	@password@do.off

Action	Command	Description
<b>System Restart</b>	@password@restart	The device will reboot.
<b>Cellular Report</b>	@password@cell.report	The device will reply with an SMS message containing the current cellular status of the device.
<b>Cellular Start Connecting</b>	@password@cellular.start	The device will enable the cellular data connection.
<b>Cellular Stop Connecting</b>	@password@cellular.stop	The device will disable the cellular data connection.
<b>Switch SIM</b>	@password@switchsim	The device will restart the cellular module and use the SIM card installed in the other SIM slot.
<b>Start IPsec Tunnel</b>	@password@ipsec.start	The device will establish an IPsec tunnel.
<b>Stop IPsec Tunnel</b>	@password@ipsec.stop	The device will disconnect the IPsec tunnel.
<b>Set DO On</b>	@password@do.on	The device will set the status of the relay output to On.
<b>Set DO Off</b>	@password@do.off	The device will set the status of the relay output to Off.

## Send SMS

This page lets you send a custom SMS message from the device to a specified recipient, which can be useful for testing the device's SMS connection. Click **SEND** to send the SMS message.



UI Setting	Description	Valid Range	Default Value
<b>Country Code</b>	Specify the country code for the recipient's number.	Valid country code	N/A
<b>Number</b>	Specify the recipient's phone number.	Valid phone number	N/A
<b>Message</b>	Specify the text of the message to send.	0 to 160 characters	N/A

## GNSS

### Menu Path: System > GNSS

These pages let you configure the GNSS settings of your device.

#### Note

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

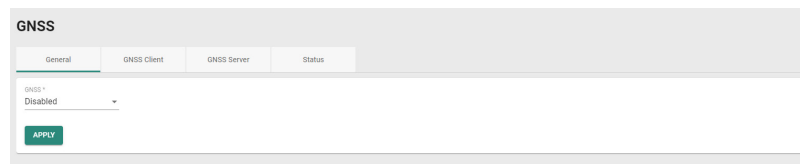
This page includes these tabs:

- General
- GNSS Client
- GNSS Server
- Status

## GNSS - General

**Menu Path: System > GNSS - General**

This page lets you enable or disable GNSS functionality.



UI Setting	Description	Valid Range	Default Value
<b>GNSS</b>	Enable or disable GNSS functionality. If enabled, the device will use satellite positioning to show its real-time physical location on a map.	Enabled / Disabled	Enabled

**Note**  
The cellular module must be enabled for this feature. Refer to Cellular for more information.

## GNSS Client

**Menu Path: System > GNSS - GNSS Client**

This page lets you configure GNSS Client settings to allow the device to send GNSS data to a user-configured server.



## GNSS

General
GNSS Client
GNSS Server
Status

GNSS Client \*  
 Disabled i

Report Protocol \*  
 TCP

Host Address  
 IP Address/Domain Name

Host Port  
 8919

Report Period  
 30

10 - 86400 sec.

Report Format \*  
 NMEA

Report ID  
 \_\_\_\_\_

0 / 15

APPLY

UI Setting	Description	Valid Range	Default Value
<b>GNSS Client</b>	Enable or disable GNSS Client functionality. If enabled, the device will send GNSS data to the configured server at a specified interval.	Enabled / Disabled	Disabled
<b>Report Protocol</b>	Select the report protocol to use.  <b>TCP:</b> Send reports over TCP. This requires a receipt from the server to confirm the data was delivered.  <b>UDP:</b> Send reports over UDP. This does not require a receipt from the server.	TCP / UDP	TCP
<b>Host Address</b>	Specify the IP address or host name of the server that will receive the GNSS data.	IP address / host name	N/A
<b>Host Port</b>	Specify the TCP or UDP port number of the server that will receive the GNSS data.	1 to 65535	8919
<b>Report Period</b>	Specify the interval (in seconds) at which GNSS data reports are generated.	10 to 86400	30
<b>Report Format</b>	Select the report format to use.  <b>NMEA:</b> Send GNSS data in standard NMEA format.  <b>General:</b> Send GNSS data in latitude-longitude format.	NMEA / General	NMEA
<b>Report ID</b>	Enter the ID to use in the GNSS data report header. The Report ID and device MAC address will be included in both report formats.	1 to 15 characters	N/A

MX-ROS V3 User Manual

121

## GNSS Server

### Menu Path: System > GNSS - GNSS Server

This page lets you configure the the device to act as a GNSS Server to allow clients to request GNSS data reports.

The screenshot shows the 'GNSS Server' configuration page. It features a header with the title 'GNSS' and four tabs: 'General', 'GNSS Client', 'GNSS Server' (which is active), and 'Status'. Below the tabs, there are several configuration fields:
 

- 'GNSS Server \*': A dropdown menu set to 'Disabled' with an information icon.
- 'Server Port': A text input field containing '8919', with a range indicator '1 - 65535' below it.
- 'Report Period': A text input field containing '30', with a range indicator '10 - 86400' and the unit 'sec.' below it.
- 'Report Format \*': A dropdown menu set to 'NMEA'.
- 'Report ID': A text input field containing '0/15'.

 An 'APPLY' button is located at the bottom left of the configuration area.

UI Setting	Description	Valid Range	Default Value
<b>GNSS Server</b>	Enable or disable GNSS Server functionality. If enabled, clients will be able to request GNSS data reports from this server.	Enabled / Disabled	Disabled
<b>Server Port</b>	Specify the UDP port number for clients to access the server.	1 to 65535	8919
<b>Report Period</b>	Specify the interval in seconds at which GNSS data reports are generated.	10 to 86400	30
<b>Report Format</b>	Select the report format. <b>NMEA:</b> Send GNSS data in standard NMEA format. <b>General:</b> Send GNSS data in latitude-longitude format.	NMEA / General	NMEA
<b>Report ID</b>	Enter the ID to use in the GNSS data report header. The Report ID and device MAC address will be included in both report formats.	1 to 15 characters	N/A

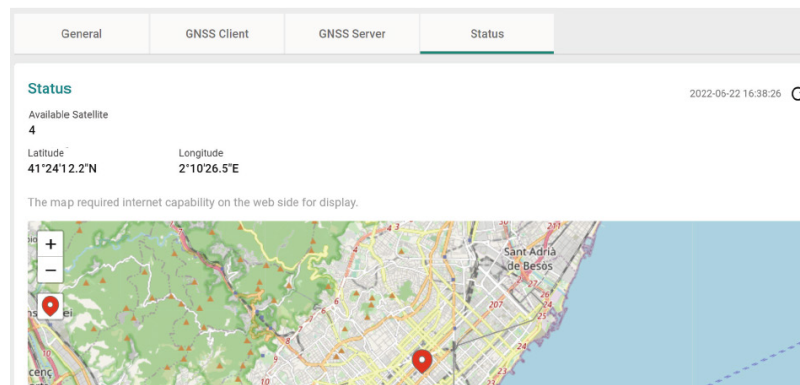
## Status




### Menu Path: System > GNSS - Status

The Status screen shows the current geolocational information of the device, as well the device's current physical location on an interactive map.

#### Note

The device's physical location and coordinates will only appear if GNSS is enabled.



UI Setting	Description
<b>Available Satellite</b>	Shows number of satellites the device is receiving information from.
<b>Latitude</b>	Shows the north–south position of the device.
<b>Longitude</b>	Shows the east–west position of the device.
	Click to refresh the coordinate data.
	Click to zoom in or zoom out on the map.
	Click to center the map on the device's location.

## Setting Check

### Menu Path: System > Setting Check

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

Setting Check is available for the following configuration settings:

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

### Setting Check

**Setting Check Configuration**

Layer 3-7 Policy

Network Address Translate

Trusted Access

Timer \*

180

10 - 3600 sec.

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Layer 3-7 Policy</b>	Enable or disable Setting Check for Layer 3 - 7 policy changes.	Enabled / Disabled	Disabled
<b>Network Address Translate</b>	Enable or disable Setting Check for NAT policy changes.	Enabled / Disabled	Disabled
<b>Trusted Access</b>	Enable or disable Setting Check for Trusted IP address changes.	Enabled / Disabled	Disabled
<b>Timer</b>	Set the time (in seconds) the user has to confirm the changes.	10 to 3600	180

**Note**

If the user does not confirm the changes within the specified time period, the system will automatically undo the changes.

# Cellular

## Menu Path: Cellular

This page lets you configure mobile network connection settings.

This page includes these tabs:

- General
- SIM Settings
- GuaranLink
- Status

### Note

These features are only available on devices with cellular capabilities.

## Cellular - User Privileges

Privileges to Cellular 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
Cellular	R/W	R/W	R

## Cellular - General

### Menu Path: Cellular - General

This page lets you configure basic cellular settings for your device. Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
<b>Cellular Module</b>	Enable or disable the cellular module for establishing cellular connections, sending SMS messages, and using GNSS services.	Enabled / Disabled	Enabled
<b>Cellular Operation Mode</b>	The device will function as an IP router for IP data communication.	Router	Router
<b>Cellular Data Connection</b>	Enable or disable cellular data connections. If enabled, cellular connections may incur data usage costs based on your cellular service and ISP.	Enabled / Disabled	Enabled
<b>MTU</b>	Specify the Maximum Transmission Unit (MTU) value for router mode. The recommended MTU size may vary depending on the cellular carrier. Make sure the end device is set to the same MTU value for optimal performance.	576 to 1500	1428



## SIM Settings

### Menu Path: Cellular - SIM Settings


This section lets you enable or disable SIM cards and manage the SIM card settings including the priority, cellular bands, and authentication method.

### Reordering SIM Card Priority

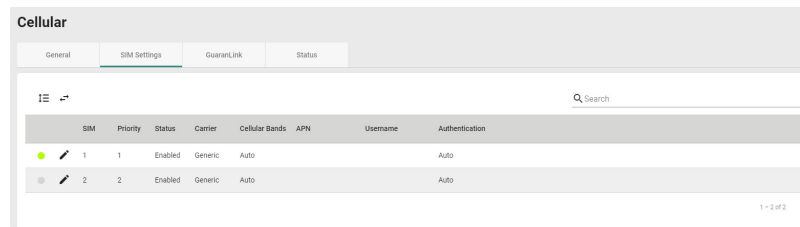
The device will always connect to the Internet using the SIM card designated with priority 1. The secondary SIM card will act as a redundant backup. To change the priority of the



SIM cards, click the **Reorder Priorities** (  ) icon then click and drag the SIM card to the desired priority. Click the **Finish Reorder** (  ) icon to confirm the change.

## Changing the Active SIM Card

The green dot icon indicates the SIM card is active and connected to the Internet. By default, the SIM card designated with priority 1 will be used to connect to the Internet while the SIM with priority 2 acts as a backup. If necessary, you can manually change the active SIM card. Click the **Change SIM** (  ) icon to swap the active SIM card.

## SIM Card List



SIM	Priority	Status	Carrier	Cellular Bands	APN	Username	Authentication
 1	1	Enabled	Generic	Auto			Auto
 2	2	Enabled	Generic	Auto			Auto

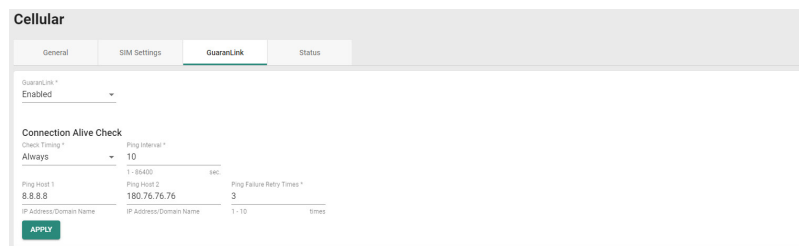
UI Setting	Description
<b>SIM</b>	Shows which SIM slot the entry is for.
<b>Priority</b>	Shows the priority of the SIM card.
<b>Status</b>	Shows the configured status of the SIM card.
<b>Carrier</b>	Shows the carrier for the SIM card.
<b>Cellular Bands</b>	Shows the cellular bands the SIM card will use.
<b>APN</b>	Shows the access point network (APN) information.
<b>Username</b>	Shows the username for PAP authentication.
<b>Authentication</b>	Shows the authentication method.

## GuaranLink

**Menu Path: Cellular - GuaranLink**

This page lets you set up Moxa's GuaranLink feature, which enables reliable connectivity with 3 different connection checks and 4 levels of recovery actions. A number of factors can contribute to connection failures in cellular communications, including loss of cellular signal, interference, connection errors caused by the base station, or termination by the operator for unknown reasons. GuaranLink is designed to address various needs, including minimizing cellular costs by optimizing the number of cellular packets sent to check connection status and optimizing the time it takes to swap to a backup SIM.

## GuaranLink Settings



UI Setting	Description	Valid Range	Default Value
<b>GuaranLink</b>	<p>Enable or disable GuaranLink. If enabled, the device will monitor cellular connections. If a connection failure is detected, the device will attempt to automatically recover the connection.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>Enabling this function will send additional alive check cellular messages, which may incur additional cellular costs.</p> </div>	Enabled / Disabled	Enabled
<b>Check Time</b>	<p>Specify the check time.</p> <p><b>Always:</b> The device will constantly send out alive check packets to check for cellular connection issues.</p> <p><b>Idle Transmission:</b> The device will only send alive check packets when the device has not received any data transmissions during the specified Ping Interval period.</p> <p><b>Poor Signal:</b> The device will only send alive check packets when the device identifies poor signal quality.</p>	Always / Idle Transmission / Poor Signal	Always
<b>Ping Interval (Only when Check Time is Always)</b>	Specify the interval (in seconds) at which the device will send out an alive check packet.	1 to 86400 seconds	10



UI Setting	Description	Valid Range	Default Value
<b>Ping Interval</b> (Only when Check Time is Idle Transmission)	Specify the interval (in minutes) the device will wait for data transmissions. If no data transmissions take place during the interval, the device will perform a connection alive check.	1 to 600 minutes	5
<b>Signal Checking Interval</b> (Only when Check Time is Poor Signal)	Specify the interval (in minutes) the device will check the host for poor signal quality. If the device detects poor signal quality from the host, the device will perform a connection alive check.	1 to 600 minutes	5
<b>Ping Host 1/2</b>	Enter the IP address or domain name of the remote host to ping. If both ping host 1 and 2 are configured, the device will perform connection alive checks for both hosts simultaneously. The device will only consider the connection to have failed if the device receives no response from both hosts.	IP address/domain name	N/A
<b>Ping Failure Retry Times</b>	Specify the number of times the device will perform the connection alive check. If the check fails the specified number of retry times, the device will determine that the cellular connection has failed and will initiate the GuaranLink recovery process.	1 to 10	3

## GuaranLink Recovery Settings

### GuaranLink Recovery Settings

Recovery Step	Recovery Action	Attempts ↑
1	Cellular Reconnect	1
2	ISP Reregister	1
3	Cellular Module Reset	3
4	System Reboot	0

UI Setting	Description
<b>Recovery Step</b>	Shows the sequence of the recovery step.

UI Setting	Description
<b>Recovery Action</b>	Shows the recovery action.
<b>Attempts</b>	Shows the number of times the action will be attempted.

## Edit Recovery Action Settings

### Menu Path: Cellular - GuaranLink

Clicking the **Edit** (✎) icon for an action on the **Cellular - GuaranLink** page will open this dialog box. This dialog lets you specify the number of times to attempt each recovery action before moving to the next recovery action. Click **APPLY** to save your changes.

### Edit Recovery Action Settings

#### Step 1 Cellular Reconnect

Attempts \*

1

#### Step 2 ISP Reregister

Attempts \*

1

#### Step 3 Cellular Module Reset

Attempts \*

3

#### Step 4 System Reboot

Attempts \*

0

CANCEL

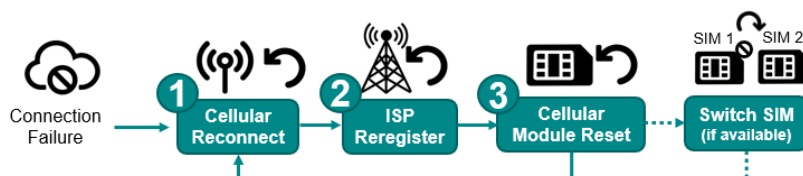
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Step 1 Cellular Reconnect Attempts</b>	<p>Specify the number of times the device will try to disconnect and re-establish the cellular connection.</p> <p>If the connection is not restored after the specified number of attempts, the device will move on to the next recovery step.</p> <p>If set to 0, the device will skip this step and move on to the next recovery step.</p>	0 to 5	1
<b>Step 2 Re-register Attempts</b>	<p>Specify the number of times the device will try to re-register with the ISP to obtain a new IP address from the base station to re-establish the cellular connection.</p> <p>If the connection is not restored after the specified number of attempts, the device will move on to the next recovery step.</p> <p>If set to 0, the device will skip this step and move on to the next recovery step.</p>	0 to 5	1
<b>Step 3 Cellular Module Reset Attempts</b>	<p>Specify the number of times the device will try to reset the cellular module to re-establish the cellular connection.</p> <p>If the connection is not restored after the specified number of attempts, the device will move on to the next recovery step.</p> <p>If set to 0, the device will skip this step and move on to the next recovery step.</p>	0 to 10	3
<b>Step 4 System Reboot Attempts</b>	<p>Specify whether the device will reboot in order to re-establish the cellular connection.</p> <p>If the connection is not restored after rebooting, the device will restart the recovery process from step 1.</p>	0 to 1	0



If set to 0, the device will not perform a system reboot and will restart the recovery process from step 1.

If two SIM cards are inserted the device, the device will attempt to use another SIM card to restart the recovery process from step 1.



## Cellular - Status

### Menu Path: Cellular - Status

This section lets you see the current status of the cellular connection as well as information about the cellular carrier and SIM card, cellular module, and signal strength.

## Cellular Status

This section shows you the cellular connection status of your device.

UI Setting	Description
<b>SIM</b>	Shows the status of the SIM card. <b>Green:</b> The SIM card is active. <b>Red:</b> The SIM card is inactive. <b>Gray:</b> No SIM card inserted.
<b>Signal</b>	Shows the status of the device's cellular signal. <b>Green:</b> Good cellular signal. <b>Amber:</b> Fair cellular signal. <b>Red:</b> Poor cellular signal. <b>Gray:</b> No cellular signal.

UI Setting	Description
<b>Register</b>	Shows the status of the device's cellular registration. <b>Green:</b> The device successfully registered with the base station. <b>Red:</b> The device failed to register with the base station. <b>Gray:</b> The registration phase has not been reached yet.
<b>Connection</b>	Shows the status of the device's network connection. <b>Green:</b> The device obtained an IP address from the base station. <b>Red:</b> The device failed to obtain an IP address from the base station. <b>Gray:</b> The connection phase has not been reached yet.
<b>Internet</b>	Shows the status of the device's Internet connection. <b>Green:</b> The device is connected to the Internet. <b>Red:</b> The device failed to connect to the Internet. <b>Gray:</b> Alive checks are not being performed.

**Note**

GuaranLink must be enabled to perform connection alive checks. Refer to Cellular - GuaranLink for more information.

## Cellular Module Information

### Cellular Module Information

Cellular Module

Enabled

IMEI

XXXXXXXXXXXX

Cellular Module Firmware

SWI9X07Y\_02.37.06.05

UI Setting	Description
<b>Cellular Module</b>	Shows the current status of the cellular module.
<b>Cellular Module Software</b>	Shows the firmware version of the cellular module.
<b>IMEI</b>	Shows the International Mobile Equipment Identity (IMEI) number of the cellular module.

## Carrier and SIM

### Carrier and SIM

Cellular SIM	SIM 1 Status
<b>SIM 1</b>	<b>SIM Absent</b>
Cellular Carrier	SIM 1 Phone Number
---	---
Cellular Mode	SIM 1 ICCID
---	---
Cellular Bands	SIM 2 Status
---	<b>SIM Absent</b>
Cellular IP Address	SIM 2 Phone Number
---	---
IMSI	SIM 2 ICCID
---	---

UI Setting	Description
<b>Cellular SIM</b>	Shows the SIM card used for establishing the cellular connection.
<b>Cellular Carrier</b>	Shows the cellular service provider being used.
<b>Cellular Mode</b>	Shows the cellular connection technology being used, such as LTE or HSPA.
<b>Cellular Band</b>	Shows the cellular band frequency being used.
<b>Cellular IP Address</b>	Shows the cellular IP address assigned by the cellular carrier.
<b>IMSI</b>	Shows the International Mobile Subscriber Identity number.
<b>SIM 1 Status</b>	Shows the status of the SIM card installed in SIM slot 1.
<b>SIM 1 Phone Number</b>	Shows the phone number of the SIM card in SIM slot 1.
<b>SIM 1 ICCID</b>	Shows the Integrated Circuit Card ID of the SIM card in SIM slot 1.
<b>SIM 2 Status</b>	Shows the status of the SIM card installed in SIM slot 2.
<b>SIM 2 Phone Number</b>	Shows the phone number of the SIM card in SIM slot 2.
<b>SIM 2 ICCID</b>	Shows the Integrated Circuit Card ID of the SIM card in SIM slot 2.

## Signal Status

### Signal Status

Signal Strength

---

Received Signal Strength Indicator (RSSI)

---

Reference Signal Received Power(RSRP)

---

Reference Signal Received Quality (RSRQ)

---

Signal-to-interference-plus-noise Ratio (SINR)

---

UI Setting	Description
<b>Signal Strength</b>	Shows the current overall signal strength of the device.
<b>RSRP (Reference Signal Received Power)</b>	Shows the current RSRP. <b>Good:</b> Higher than -80 dBm <b>Average:</b> -80 to -90 dBm <b>Poor:</b> -90 to -100 dBm <b>Inadequate:</b> Less than -100 dBm
<b>RSSI (Received Signal Strength Indicator)</b>	Shows the current RSSI. <b>Good:</b> Higher than -73 dBm <b>Average:</b> -73 to -89 dBm <b>Poor:</b> -89 to -113 dBm <b>Inadequate:</b> Less than -113 dBm
<b>RSRQ (Reference Signal Received Quality)</b>	Shows the current RSRQ. <b>Good:</b> Higher than -10 dB <b>Average:</b> -10 to -15 dB <b>Poor:</b> -15 to -20 dB <b>Inadequate:</b> Less than -20 dB
<b>SINR (Signal to Interference and Noise Ratio)</b>	Shows the current SINR. <b>Good:</b> Higher than 20 dB <b>Average:</b> 13 to 20 dB <b>Poor:</b> 0 to 13 dB <b>Inadequate:</b> Less than 0 dB

## Serial

### Menu Path: Serial

This page lets you configure your device's serial settings.

**Note**

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

This page includes these tabs:

- Port Settings
- Operation Mode
- Data Packing
- Status
- Serial Data Logs

## Serial - User Privileges

Privileges to Serial 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
Serial	R/W	R/W	R

## Serial - Port Settings

### Menu Path: Serial - Port Settings

This page lets you enable or disable the serial port and configure the serial communication parameters. When enabled, the device allows for traditional serial (RS-232/422/485) devices to transmit data over the cellular network.

**Note**

The serial port settings on the device should match the parameters configured for the connected serial device. Refer to your serial device's user manual to determine the appropriate serial communication parameters.



Serial Port \*  
 Disabled ▼

---

Interface Type \*  
 RS-232 ▼

---

Baudrate \*  
 115200 ▼

---

Data Bits \*      Stop Bits \*  
 8                      1 ▼

---

Parity \*  
 None ▼

---

Flow Control \*  
 RTS, CTS ▼

UI Setting	Description	Valid Range	Default Value
<b>Serial Port</b>	Enable or disable the serial port.	Enabled / Disabled	Disabled
<b>Interface Type</b>	Select the serial interface type to use for the serial device.	RS-232 / RS-422 / 2-wire-RS-485/ 2-wire-RS-485	RS-232
<b>Baud Rate</b>	Specify the data transmission rate to and from the serial device.	300 to 921600	115200
<b>Data Bits</b>	Specify the size for data characters.	5 to 8	8
<b>Stop Bits</b>	Specify the size for stop characters.	1 to 2	1
<b>Parity</b>	Select the parity mode. Even and odd parity provide rudimentary error-checking. Space and mark parity are rarely used.	None / Even / Odd / Space / Mark	None
<b>Flow Control</b>	Select the flow control method. This determines how the system will suspend and resume data transmissions to prevent data loss. RTS/CTS (hardware) flow control is recommended.	None / RTS/CTS / DTR/DSR / Xon/Xoff	RTS/CTS

# Port Buffering and Logs Settings



Serial Port Buffering (10 MB) \*

Disabled ▼

Serial Data Logs (64 KB) \*

Disabled ▼

## Port Buffering and Logs Settings

UI Setting	Description	Valid Range	Default Value
<b>Serial Port Buffering</b>	<p>Enable or disable serial port buffering. When enabled, if the WAN connection goes down, the router will keep the serial data and retransmit the buffered data when the WAN connection is back. If disabled, serial data will be lost if the WAN connection goes down.</p> <div><p> <b>Note</b></p><ul style="list-style-type: none"><li>• Port buffering can be used in Real COM, RFC2217, TCP Server, and TCP Client modes.</li><li>• For other modes, the port buffering settings will have no effect.</li><li>• The maximum buffer size is 10 MB.</li><li>• Buffer data exceeding 10 MB will overwrite previous data.</li></ul></div>	Enabled / Disabled	Disabled
<b>Serial Data Logs</b>	<p>Enable or disable serial data logs. If enabled, the router will store the serial data logs in the system RAM.</p> <div><p> <b>Note</b></p><p>The system RAM can save up to 64 kb of serial data logs. Serial log data will be cleared when the router is powered off.</p></div>	Enabled / Disabled	Disabled

## Operation Mode

### Menu Path: Serial - Operation Mode

This page lets you set up and configure a serial operation mode. Refer to Serial Operation Modes for more information about the different modes.

## Operation Mode - Real COM

If you select **Real COM** as your **Operation Mode**, these settings will appear.

Operation Mode \*  
Real COM

**Connection Settings**  
TCP Alive Check Interval  
7  
1 - 99 min.  
Max. Connections  
1  
1 - 2 connection

**Connection Down Settings**  
Set RTS Signal \* High Set DTR Signal \* High

APPLY

## Connection Settings

UI Setting	Description	Valid Range	Default Value
<b>TCP Alive Check Interval</b>	Specify the interval (in minutes) at which to check if the TCP connection is still alive. If there is no response from the other end of the connection after the specified time, the TCP connection will be terminated. A setting of 0 means the system will keep the TCP connection open and will not send any "keep alive" packets. Disabling this option can help free up device resources.	1 to 99	7
<b>Max. Connections</b>	Specify the maximum number of simultaneous connections that the port will accept. Up to 2 hosts can simultaneously collect data from the same serial device.	1 to 2	1

## Connection Down Settings

UI Setting	Description	Valid Range	Default Value
<b>Set RTS Signal</b>	Select the RTS signal method to use. <b>High:</b> The cellular or Ethernet connection status will not affect RTS signals. <b>Low:</b> If the cellular or Ethernet connection is lost, RTS signals will change to low.	High / Low	High

UI Setting	Description	Valid Range	Default Value
<b>Set DTR Signal</b>	<p>Select the DTR signal method to use.</p> <p><b>High:</b> The cellular or Ethernet connection status will not affect DTR signals.</p> <p><b>Low:</b> If the cellular or Ethernet connection is lost, DTR signals will change to low.</p>	High / Low	High

## Operation Mode - TCP Server

If you select **TCP Server** as your **Operation Mode**, these settings will appear.

The screenshot shows a configuration page for 'TCP Server'. At the top, 'Operation Mode' is set to 'TCP Server'. Below this, there are several sections of settings:

- Connection Settings:**
  - TCP Alive Check Interval: 7 (range 1-99 min)
  - Max. Connections: 1 (range 1-2 connection)
  - TCP Data Port: 4001 (range 1-65535)
  - TCP Command Port: 966 (range 1-65535)
  - Serial Port Inactivity Time: 0 (range 0-65535 ms)
- Connection Down Settings:**
  - Set RTS Signal: High
  - Set DTR Signal: High

An 'APPLY' button is located at the bottom of the settings area.

## Connection Settings

UI Setting	Description	Valid Range	Default Value
<b>TCP Alive Check Interval</b>	<p>Specify the interval (in minutes) at which to check if the TCP connection is still alive. If there is no response from the other end of the connection after the specified time, the TCP connection will be terminated. A setting of 0 means the system will keep the TCP connection open and will not send any "keep alive" packets.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>Disabling this option can help free up device resources.</p> </div>	1 to 99	7
<b>Max. Connections</b>	<p>Specify the maximum number of simultaneous connections that the port will accept. Up to 2 hosts can simultaneously collect data from the same serial device.</p>	1 to 2	1

UI Setting	Description	Valid Range	Default Value
<b>TCP Data Port</b>	Specify the TCP port number for the serial port used to listen to connections and for other devices to contact. To avoid conflicts with well-known TCP ports, the default port is 4001.	1 to 65535	4001
<b>TCP Command Port</b>	Specify the TCP port number for MOXA IP-Serial Library commands.	1 to 65535	9006
	<p><b>Note</b></p> <p>It is not necessary to reference this port number in your application when using the Moxa IP-Serial Library since the library automatically obtains the number from the device server. Only change this setting if there is a port number conflict with another application or device.</p>		
<b>Serial Port Inactivity Time</b>	Specify the time limit in milliseconds to keep the connection open if there is no data going to or from the serial device. If there is no activity for the specified time period, the connection will be terminated. A setting of 0 means the system will always keep the TCP connection open regardless of data activity.	1 to 65535	0
	<p>For many applications, this option should be set to 0, as the serial device may be idle for long periods of time.</p> <p><b>Warning</b></p> <p>Serial Port Inactivity Time setting should be greater than the Force Transmit Interval in Data Packing settings. Otherwise, the connection may be closed before the data in the buffer can be transmitted.</p> <p>To prevent the unintended loss of data due to the session being disconnected, it is highly recommended that this value is set large enough so that the intended data transfer is completed.</p>		

## Connection Down Settings

UI Setting	Description	Valid Range	Default Value
<b>Set RTS Signal</b>	Select the RTS signal method to use. <b>High:</b> The cellular or Ethernet connection status will not affect RTS signals. <b>Low:</b> If the cellular or Ethernet connection is lost, RTS signals will change to low.	High / Low	High

UI Setting	Description	Valid Range	Default Value
<b>Set DTR Signal</b>	<p>Select the DTR signal method to use.</p> <p><b>High:</b> The cellular or Ethernet connection status will not affect DTR signals.</p> <p><b>Low:</b> If the cellular or Ethernet connection is lost, DTR signals will change to low.</p>	High / Low	High

## Operation Mode - TCP Client

If you select **TCP Client** as your **Operation Mode**, these settings will appear.

Operation Mode \*  
 TCP Client ▼

**Connection Settings**

TCP Alive Check Interval  
 7  
 1 - 99 min.



Serial Port Inactivity Time  
 0  
 0 - 65535 ms

Connection Control \*  
 Startup/None ▼

**APPLY**

## Connection Settings

UI Setting	Description	Valid Range	Default Value
<b>TCP Alive Check Interval</b>	<p>Specify the interval (in minutes) at which to check if the TCP connection is still alive. If there is no response from the other end of the connection after the specified time, the TCP connection will be terminated. A setting of 0 means the system will keep the TCP connection open and will not send any "keep alive" packets.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Disabling this option can help free up device resources.</p> </div>	1 to 99	7

UI Setting	Description	Valid Range	Default Value
<b>Serial Port Inactivity Time</b>	<p>Specify the time limit in milliseconds to keep the connection open if there is no data going to or from the serial device. If there is no activity for the specified time period, the connection will be terminated. A setting of 0 means the system will always keep the TCP connection open regardless of data activity.</p> <p>For many applications, this option should be set to 0, as the serial device may be idle for long periods of time.</p> <div data-bbox="379 622 890 831" style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b></p> <p>The serial port inactivity time is only applied when the <b>Connection Control</b> option is set to <b>Any Character/Inactivity Time</b>.</p> </div> <div data-bbox="379 891 890 1288" style="background-color: #fff9c4; padding: 5px;"> <p> <b>Warning</b></p> <p><b>Serial Port Inactivity Time</b> setting should be greater than the <b>Force Transmit Interval</b> in <b>Data Packing</b> settings. Otherwise, the connection may be closed before the data in the buffer can be transmitted.</p> <p>To prevent the unintended loss of data due to the session being disconnected, it is highly recommended that this value is set large enough so that the intended data transfer is completed.</p> </div>	1 to 65535	0

UI Setting	Description	Valid Range	Default Value
<b>Connection Control</b>	<p>Select a connection control method.</p> <p><b>Startup/None:</b> A TCP connection will be established on startup and will remain active indefinitely.</p> <p><b>Any Character/None:</b> A TCP connection will be established when any character is received from the serial interface and will remain active indefinitely.</p> <p><b>Any Character/Inactivity Time:</b> A TCP connection will be established when any character is received from the serial interface and will be disconnected after the specified Serial Port Inactivity Time.</p> <p><b>DSR On/DSR Off:</b> A TCP connection will be established when a DSR "On" signal is received and will be disconnected when a DSR "Off" signal is received.</p> <p><b>DSR On/None:</b> A TCP connection will be established when a DSR "On" signal is received and will remain active indefinitely.</p> <p><b>DCD On/DCD Off:</b> A TCP connection will be established when a DCD "On" signal is received and will be disconnected when a DCD "Off" signal is received.</p> <p><b>DCD On/None:</b> A TCP connection will be established when a DCD "On" signal is received and will remain active indefinitely.</p>	Startup/None / Any Character/None / Any Character/Inactivity Time / DSR On/DSR Off / DSR On/None / DCD On/DCD Off / DCD On/None	Startup/None

## Add a Destination Entry (TCP Client)

### Menu Path: Serial - Operation Mode (TCP Client)

Clicking the **Add (+)** icon on the **Serial - Operation Mode (TCP Client)** page will open this dialog box. This dialog lets you add a destination entry. Click **CREATE** to save your changes and add the new entry.



## Add Destination

IP Address \*

Destination Data Port \* 

1 - 65535

Local Data Port \* 

1 - 65535


CANCEL

CREATE


UI Setting	Description	Valid Range	Default Value
<b>IP Address</b>	Specify the IP address of the remote host.	Valid IP address	N/A
<b>Destination Data Port</b>	Specify the TCP port number of the remote host.	1 to 65535	N/A
<b>Local Data Port</b>	Specify a designated local port or leave this field blank to let the system assign a port.	1 to 65535	N/A


## Delete a Destination Entry (TCP Client)

### Menu Path: Serial - Operation Mode (TCP Server)

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

Destination Settings

 Q Search

<input checked="" type="checkbox"/>	IP Address	Destination Data Port	Local Data Port
<input checked="" type="checkbox"/> 	19.122.111.111	4001	60

Max. 4

## Operation Mode - UDP

If you select **UDP** as your **Operation Mode**, these settings will appear.

Operation Mode \*  
UDP

### Connection Settings

UDP Data Port  
4001  
1 - 65535

APPLY

## Connection Settings

UI Setting	Description	Valid Range	Default Value
<b>UDP Data Port</b>	Enter the UDP port number for contacting the serial device.	1 to 65535	4001

## Add a Destination Entry (UDP)

### Menu Path: Serial - Operation Mode (UDP)

Clicking the **Add (+)** icon on the **Serial - Operation Mode (UDP)** page will open this dialog box. This dialog lets you add a destination entry. Click **CREATE** to save your changes and add the new entry.

#### Note

The maximum IP address range size is 64 addresses. However, when using multicast, you may enter IP addresses in the form xxx.xxx.xxx.255 in the Start IP Address field.

For example, enter 192.168.127.255 to allow the system to broadcast UDP packets to all hosts with IP addresses between 192.168.127.1 and 192.168.127.254.

## Add Destination

Start IP Address \*

End IP Address \*

Destination Data Port \* 

1 - 65535


CANCEL

CREATE


UI Setting	Description	Valid Range	Default Value
<b>Starting IP Address</b>	Enter the starting IP address of the remote host IP range.	IP Address	N/A
<b>End IP Address</b>	Enter the ending IP address of the remote host IP range.	IP Address	N/A
<b>Destination Data Port</b>	Enter the UDP port number of the remote host.	1 to 65535	N/A


## Delete a Destination Entry (UDP)

### Menu Path: Serial - Operation Mode (UDP)

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

#### Destination Settings

 🔍 Search

<input checked="" type="checkbox"/>	IP Address	Destination Data Port	Local Data Port
<input checked="" type="checkbox"/> 	19.122.111.111	4001	60

Max. 4

## Data Packing

### Menu Path: Serial - Data Packing

This page lets you configure the conditions and delimiter settings for serial port data buffering and transmission.

Packet Length  
  
 0 - 1024 bytes

Force Transmit Interval  
  
 0 - 65535 ms

**Delimiter Settings**

Delimiter 1 Enable \*  
 ▼

Delimiter 1 \*  
  
 Hex digit

Delimiter 2 Enable \*  
 ▼

Delimiter 2 \*  
  
 Hex digit

Delimiter Process \*  
 ▼

UI Setting	Description	Valid Range	Default Value
<b>Packet Length</b>	<p>Specify the Packet Length in bytes for the serial port buffer. The packet length refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending.</p> <p>At the default packet length of 0, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full.</p> <p>If a packet length of 1 to 1024 bytes is specified, data in the buffer will be sent as soon as it reaches the specified length.</p>	0 to 1024	0
<b>Force Transmit Interval</b>	<p>Specify the interval in milliseconds to force transmission of serial port data if no activity is recorded.</p> <p>This setting controls data packing by the amount of time that elapses between bits of data. As serial data is received, it accumulates in the device port's buffer. If serial data is not received for the specified amount of time, the data that is currently in the buffer is packed for network transmission.</p> <p>A setting of 0 means that data in the buffer will not be automatically packed when additional data is not received from the device.</p>	0 to 65535	0

## Delimiter Settings

UI Setting	Description	Valid Range	Default Value
<b>Delimiter 1/2 Enable</b>	<p>Enable or disable delimiter 1 or 2.</p> <p><b>Enabled:</b> The serial port will queue data in the buffer and send it to the cellular or Ethernet port when a specific hex character is received. When both Delimiter 1 and 2 are enabled and specified, both of them will be used to control when data should be sent.</p> <p><b>Disabled:</b> The serial port will not check for specific characters for data transmission.</p> <div style="background-color: #fff9c4; padding: 5px; margin-top: 10px;"> <p><b>⚠ Warning</b></p> <p>When <b>Delimiter</b> is enabled, the <b>Packet Length</b> must be set to 0.</p> </div>	Disabled / Enabled	Disabled
<b>Delimiter 1/2</b>	<p>Specify the character that acts as the delimiter to control when data should be sent.</p> <div style="background-color: #fff9c4; padding: 5px; margin-top: 10px;"> <p><b>⚠ Warning</b></p> <p>When the device port buffer is full, the data will be packed for network transmission regardless of the <b>Delimiter 1, Delimiter 2, and Force Transmit Interval</b> settings.</p> </div>	0x00 to 0xFF	0x00
<b>Delimiter Process</b>	<p>Select the delimiter process.</p> <p><b>Delimiter:</b> Data in the buffer will be transmitted when the delimiter is received.</p> <p><b>Delimiter +1:</b> Data in the buffer will be transmitted after 1 additional byte is received following the delimiter.</p> <p><b>Delimiter +2:</b> Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter.</p> <p><b>Strip Delimiter:</b> Data in the buffer is stripped of the delimiter before being transmitted.</p>	Delimiter / Delimiter +1 / Delimiter +2 / Strip Delimiter	Delimiter

## Serial - Status

### Menu Path: Serial - Status

This page lets you see detailed statistics and information about the serial port data and connections.

# Serial State

### Serial State

- DSR
- DTR
- RTS
- CTS
- DCD

UI Setting	Description
<b>Serial State</b>	Shows the status of the serial signal. <b>Green:</b> The signal pins are connected. <b>Grey:</b> The signal pins are disconnected.

# Serial Counter

## Serial Counter

TX Count	TX Total Count	RX Count	RX Total Count
0	0	0	0

UI Setting	Description
<b>TX Count</b>	Shows the number of packets transmitted.
<b>TX Total Count</b>	Shows the total total number of packets transmitted since the device was powered on.
<b>RX Count</b>	Shows the number of packets received.

UI Setting	Description
------------	-------------

**RX Total Count** Shows the total total number of packets received since the device was powered on.

## Error Counter

### Error Counter

Frame Error Count	Parity Error Count	Overrun Count	Break Count
0	0	0	0

UI Setting	Description
------------	-------------

**Frame Error Count** Shows the number of frame errors since the device was powered on.

**Parity Error Count** Shows the number of parity errors since the device was powered on.

**Overrun Count** Shows the number of overrun errors since the device was powered on.

**Break Count** Shows the number of break errors since the device was powered on.

## Serial - Connection List

### Connection List

🔍 Search

Operation Mode	IP Address
----------------	------------

UI Setting	Description
------------	-------------

**Operation Mode** Shows the operation mode for the connection.

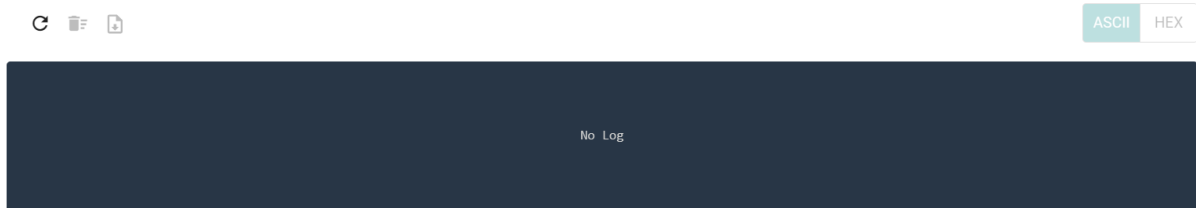
**IP Address** Shows the IP address of the connection.

## Serial Data Logs

### Menu Path: Serial - Serial Data Logs

This page lets you see the device's serial data logs in ASCII or HEX format.

- Click the **Refresh icon** (↻) icon to refresh the serial data logs.
- Click the **Clear Data Log icon** (🗑️) icon to delete all serial data logs.
- Click the **Export icon** (📄) icon to export all serial data logs to a file.
- Click **ASCII** or **HEX** to change the format of the logs.



## 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



Settings	Admin	Supervisor	User
<b>Port Settings</b>	R/W	R/W	R
<b>Link Aggregation</b>	R/W	R/W	R
<b>PoE</b>	R/W	R/W	R
<b>Link Fault Passthrough</b>	R/W	R/W	R
<b>LAN Bypass Gen3</b>	R/W	R/W	R
<b>Layer 2 Switching</b>			
<b>VLAN</b>	R/W	R/W	R
<b>MAC Address Table</b>	R/W	R/W	R
<b>QoS</b>	R/W	R/W	R
<b>Rate Limit</b>	R/W	R/W	R
<b>Multicast</b>	R/W	R/W	R
<b>Network Interfaces</b>	R/W	R/W	R

## Ports

### Menu Path: [Network Configuration](#) > [Ports](#)

This section includes these pages:

- [Port Settings](#)
- [Link Aggregation](#)
- [PoE](#)
- [Link Fault Passthrough](#)
- [LAN Bypass Gen3](#)

## 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.

The screenshot shows the 'Port Settings' interface with two tabs: 'Setting' and 'Status'. The 'Setting' tab is active. Below the tabs is a search bar and a table with the following columns: Port, Status, Media Type, Description, Speed/Duplex, Flow Control, and MDI/MDIX. The table contains 9 rows of data for ports 3 through 12.

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

1 - 9 of 9

### UI Setting

### Description

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

## Edit Port Settings

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

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

### Edit Port 3 Settings

Status \*  
Enabled ▾

Media Type  
1000TX,RJ45

Description  
0 / 127

Speed/Duplex Mode \*  
Auto ▾

Flow Control \*  
Disabled ▾ ⓘ

MDI/MDIX \*  
Auto ▾

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or Disable the port.	Enabled / Disabled	Enabled
<b>Media Type</b>	Displays the port's media type. This setting cannot be changed.	N/A	Port's media type
<b>Description</b>	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
<b>Speed / Duplex</b>	<p>Select the speed and duplex mode for the port.</p> <p><b>Auto:</b> Allows the port to use IEEE 802.3u protocol to negotiate the best port speed and duplex mode to use for the connected device.</p> <p><b>100M-Full:</b> This will force the port to connect using 100 Mbps at full-duplex.</p> <p><b>100M-Half:</b> This will force the port to connect using 100 Mbps at half-duplex.</p> <p><b>10M-Full:</b> This will force the port to connect using 10 Mbps at full-duplex.</p> <p><b>10M-Half:</b> This will force the port to connect using 10 Mbps at half-duplex.</p>	Auto / 100M-Full / 100M-Half / 10M-Full / 10M-Half	Auto
<b>Flow Control</b>	<p>Enable or disable flow control for this port when the port's <b>Speed/Duplex</b> setting is set to <b>Auto</b>. Flow control helps manage the data transfer rate between the device and the connected Ethernet devices.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>If <b>Speed/Duplex</b> is set to something other than <b>Auto</b>, <b>Flow Control</b> will be disabled.</p> </div>	Enabled / Disabled	Disabled
<b>MDI / MDIX</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>Auto:</b> Allow the port to auto-detect whether to use MDI or MDIX for connected devices.</li> <li>• <b>MDI:</b> Force the port to use MDI (also known as "straight-through").</li> <li>• <b>MDIX:</b> Force the port to use MDIX (also known as "crossover").</li> </ul> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Only choose MDI or MDIX if your connected Ethernet device has trouble auto-negotiating the correct port type.</p> </div>	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.

**Port Settings**

Setting **Status**

C Search

Port	Status	Media Type	Link Status	Description	Flow Control	MDI/MDIX	Port State
3	Enabled	1000TX,RJ45	100M-Full		Off	MDI	Forwarding
4	Enabled	1000TX,RJ45	-		-	-	-
5	Enabled	1000TX,RJ45	-		-	-	-
6	Enabled	1000TX,RJ45	100M-Full		Off	MDI	Forwarding
8	Enabled	1000TX,RJ45	1G-Full		Off	MDI	Forwarding
G1	Enabled	N/A	-		-	-	-
G2	Enabled	N/A	-		-	-	-
Tk1	Enabled	-	-		-	-	-
Tk2	Enabled	-	1G-Full		-	-	-

1 - 9 of 9

## UI Setting

## Description

<b>Port</b>	Shows which port this row describes.
<b>Status</b>	Shows the status of the port.
<b>Media Type</b>	Shows the port's media type.
<b>Link Status</b>	Shows the speed and duplex mode the connection is currently using. If the link is not active, a - will be shown.
<b>Description</b>	Shows the description for the port.
<b>Flow Control</b>	Shows the whether flow control is currently on or off for the port. If the link is not active, a - will be shown.
<b>MDI / MDIX</b>	Shows whether the port is using MDI or MDIX for its connection. If the link is not active, a - will be shown.
<b>Port State</b>	Shows the port state for the port. If the link is not active, a - will be shown.

## Link Aggregation

### Menu Path: Network Configuration > Ports > Link Aggregation

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

**Note**

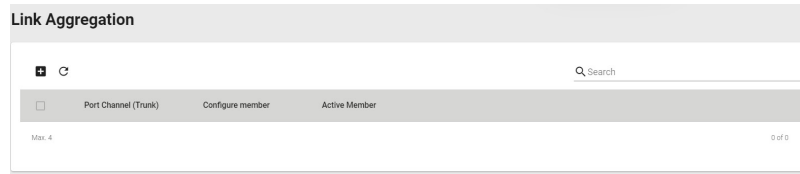
Ports in the same link aggregation must have the same speed.

**Note**

If a port is being used for Turbo Ring or Turbo Chain, it will not appear in the Link Aggregation list.

**Note**

For TN-4916 models with only 4 Gigabit ports, ports 1 to 8 cannot be aggregated with ports 9-12 due to design limitations.



## Create Link Aggregation

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

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

### Create Link Aggregation

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

Config Member Port \* 

CANCEL

CREATE

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Config Member Port</b>	Select the ports you want to include in the link aggregation group.	Port drop-down menu	N/A
---------------------------	---	---------------------	-----

## Edit Link Aggregation

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

Clicking the **Edit** (✎) icon for a link aggregation on the **Network Configuration > Ports > Link Aggregation** page will open this dialog box. This dialog lets you edit an existing link aggregation with member ports.

#### Edit Port Channel 1 Settings

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

Config Member Port \*  
 

CANCEL

APPLY

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Config Member Port</b>	Select the ports you want to include in the link aggregation group.	Port drop-down menu	N/A
---------------------------	---	---------------------	-----

## Delete Link Aggregation

### Menu Path: Network Configuration > Ports > Link Aggregation

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

Link Aggregation

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

Max: 4 1 - 2 of 2

## PoE

### Menu Path: Network Configuration > Ports > PoE

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

#### Note

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

This page includes these tabs:

- General
- PD Failure Check
- Scheduling
- Status

MOXA TN-4908-4GPoE-4GTX Hi, admin

Search for a function

**PoE**

General | PD Failure Check | Scheduling | Status

Power Output\*   
 Enabled

Power Management Mode\*   
 Consumed Power

Auto Power Cutting\*   
 Enabled

System Power Budget\*   
 50   
 30-50   
 Watt

APPLY

Port	PoE Supported	Power Output	Output Mode	Power Allocation	Legacy PD Detection	Prior
1	No	--	--	--	--	--
2	No	--	--	--	--	--
3	Yes	Enabled	Auto	0	Disabled	Low
4	Yes	Enabled	Auto	0	Disabled	Low

## PoE - General

### Menu Path: Network Configuration > Ports > PoE - General



This page lets you enable or disable various PoE related features. Click **APPLY** to save your changes.

The screenshot shows the PoE configuration interface with the following settings:

- Power Output \***: Enabled
- Power Management Mode \***: Consumed Power (with an information icon)
- Auto Power Cutting \***: Enabled (with an information icon)
- System Power Budget \***: 50 (with an information icon)

The System Power Budget is shown with a range of 30 - 50 Watt. An **APPLY** button is located at the bottom left of the configuration area.

UI Setting	Description	Valid Range	Default Value
<b>Power Output</b>	Enable or disable PoE.	Enabled / Disabled	Enabled
<b>Power Management Mode</b>	Specify whether the power budget for all ports should be calculated. <ul style="list-style-type: none"> <li><b>Allocated Power:</b> This calculates the power budget based on the Power Allocation settings of all ports. For more information on per-port power allocation, refer to Network Configuration &gt; Ports &gt; PoE - General - Edit Port Settings.</li> <li><b>Consumed Power:</b> This calculates the power budget based on actual power consumed by all ports.</li> </ul>	Allocated Power / Consumed Power	Consumed Power
<b>Auto Power Cutting</b>	Enable or disable auto power cutting, which allows PoE to be disabled for ports when total power consumption exceeds the system power budget threshold. Ports with lower priority will be disabled before ports with higher priority.	Enabled / Disabled	Disabled
<b>System Power Budget</b>	Specify the "total measured power" limit to use for all PoE ports combined.	<i>(Depends on your device model)</i>	<i>(Depends on your device model)</i> TN-4916 PoE models: 95 W TN-4908 PoE models: 50 W

## PoE - General - Edit Port Settings

### Menu Path: Network Configuration > Ports > PoE - General

Clicking the **Edit** (↗) icon for a port on the **Network Configuration > Ports > PoE - General** page will open this dialog box. This dialog lets you configure the PoE settings for each port. Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
<b>Power Output</b>	Enable or disable PoE for all PoE ports.	Enable / Disable	Enable
<b>Output Mode</b>	Specify whether to set the PoE output mode to Auto or Force. <b>Auto:</b> Power output will be determined by using 802.3at auto-detection. <b>High Power:</b> Power mode allocates 36 watts of power to the PD if it requires more than 30 watts of power <b>Force:</b> Power output will be determined by the Power Allocation setting for the port. This may be necessary for PDs that do not follow 802.3af/at standards.	Auto / High Power / Force	Auto

UI Setting	Description	Valid Range	Default Value
<b>Legacy PD Detection</b>	Enable or disable Legacy PD Detection. When the capacitance of a PD is higher than 2.7 $\mu$ F and less than 10 $\mu$ F, Legacy PD Detection will trigger the system to output power to the PD. It will take a few seconds for PoE power to be output through the port (if triggered) after enabling Legacy PD Detection.	Enable / Disable	Disable
<b>Power Allocation</b>	Specify the power in watts to allocate to a connected PD when the <b>Output Mode</b> is set to <b>Force</b> .  This setting is not used and cannot be adjusted if the <b>Output Mode</b> is set to <b>Auto or High Power</b> . It will be fixed as <b>0</b> in <b>Auto mode</b> , and as <b>36</b> in <b>High Power</b> model	0 to 36 W	0
<b>Priority</b>	Specify the priority of the port to use with the <b>Auto Power Cutting</b> feature. If Auto Power Cutting is enabled, PoE will be disabled for ports with lower priority when total power consumption exceeds the system power budget threshold. Ports with lower priority will be disabled before ports with higher priority.  Refer to Network Configuration > Ports > PoE - General for more information.	Critical / High / Low	Low
<b>Copy Config to Ports</b>	Specify which ports you want to copy this configuration to.	Select port(s) from the drop-down list	None

## PoE PD Failure Check

### Menu Path: Network Configuration > Ports > PoE - PD Failure Check

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

PoE

General PD Failure Check Scheduling Status

Search

Port	PoE Supported	Enable	Device IP	Check Frequency (sec.)	No Response Times	Action
1	No	--	--	--	--	--
2	No	--	--	--	--	--
3	Yes	Disabled		10	3	No Action
4	Yes	Disabled		10	3	No Action
5	No	--	--	--	--	--
6	No	--	--	--	--	--
7	Yes	Disabled		10	3	No Action
8	Yes	Disabled		10	3	No Action

1 - 8 of 8

UI Setting	Description
<b>Port</b>	Shows which port this row describes.
<b>PoE Supported</b>	Shows whether the port supports PoE.
<b>Enable</b>	Shows whether PD failure checking is enabled or disabled for the port.
<b>Device IP</b>	Shows what IP will be monitored for PD failure checking for the port.
<b>Check Frequency (sec.)</b>	Shows how often PD failure checks will be performed for the port.
<b>No Response Times</b>	Shows how many IP checking cycles will be tried before determining a PD is not responding.
<b>Action</b>	Shows what action will be taken if a PD failure is detected for the port.

## PoE - PD Failure Check - Edit Port Settings

### Menu Path: Network Configuration > Ports > PoE - PD Failure Check

Clicking the **Edit** (✎) icon for a port on the **Network Configuration > Ports > PoE - PD Failure Check** page will open this dialog box. This dialog lets you configure the PD failure check settings for each port. Click **APPLY** to save your changes.

## Edit Port 3 Settings


Enable \*  
Disabled ▼

Device IP  
\_\_\_\_\_

Check Frequency \*  
10  
5 - 300 sec.

No Response Times \*  
3  
1 - 10 times

Action \*  
No Action ▼

Copy Configurations to Ports ▼ 

CANCEL

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Enable</b>	Enable or disable the PD failure check function.	Enabled / Disabled	Disabled
<b>Device IP</b>	Specify the PD's IP address.	IP address	0.0.0.0
<b>Check Frequency</b>	Specify how often PD failure checks will run.	5 to 300 seconds	10
<b>No Response Times</b>	Specify the maximum number of IP checking cycles to try before determining a PD is not responding.	1 to 10	3
<b>Action</b>	Decide what action to take when a PD failure is detected.	No Action / Restart PD / Shutdown PD	No Action
<b>Copy Config to Ports</b>	Specify which ports you want to copy this configuration to.	Select port(s) from the drop-down list	None

## PoE - Scheduling

Menu Path: Network Configuration > Ports > PoE - Scheduling

This tab lets you set schedules for each PoE port. Switch to Advanced Mode, click the Scheduling tab, and then click the + icon to create the scheduling settings.

### Limitations

You can create up to 20 scheduling rules.

UI Setting	Description
<b>Rule Name</b>	Shows the name for the scheduling rule.
<b>Status</b>	Shows whether the rule is enabled or disabled.
<b>Start Date</b>	Shows what date the rule will start on.
<b>Schedule Time</b>	Shows the time when the rule will be active.
<b>End Time</b>	Select the end time for the rule.
<b>Apply the rule to port</b>	Shows which ports will use this rule.

### PoE - Scheduling - Create Rule

**Menu Path:** [Network Configuration > Ports > PoE - Scheduling](#)

Clicking the **Add (+)** icon on the **Network Configuration > Ports > PoE - Scheduling** page will open this dialog box. This dialog lets you create a PoE scheduling rule. Click **CREATE** to save your changes and add the new rule.

### Create Rule

Rule Name \* 0 / 63

Rule \*  
Enabled ▼

Start Date \* 📅

Start Time \* 🕒      End Time \* 🕒

Repeat Execution \* ▼

Apply the rule to the ... ▼

CANCEL
CREATE

UI Setting	Description	Valid Range	Default Value
<b>Rule Name</b>	Specify a name for the scheduling rule.	1 to 63 characters	None
<b>Enable</b>	Enable or disable the scheduling rule.	Enable / Disable	Enabled
<b>Start Date</b>	Specify a start date for the rule.	mm/dd/yyyy	None
<b>Start Time</b>	Specify a start time for the rule.	AM/PM hh/mm	None
<b>End Time</b>	Specify an end time for the rule.	AM/PM hh/mm	None
<b>Repeat Execution</b>	Specify whether to repeat execution of the rule on a daily or weekly basis.	None / Daily / Weekly	None
<b>Apply the rule to port</b>	Specify which ports should use this rule.	Select port(s) from the drop-down list	None

## PoE - Scheduling - Edit Rule

**Menu Path:** Network Configuration > Ports > PoE - Scheduling

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

Click **APPLY** to save your changes.

### Edit Rule

Rule Name \*  
poerule1  
8 / 63

Rule \*  
Disabled

Start Date \*  
2024-05-13

Start Time \*      End Time \*  
下午 06:00      下午 09:00

Repeat Execution \*  
Daily

Apply the rule to the port \*  
1

CANCEL    APPLY

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




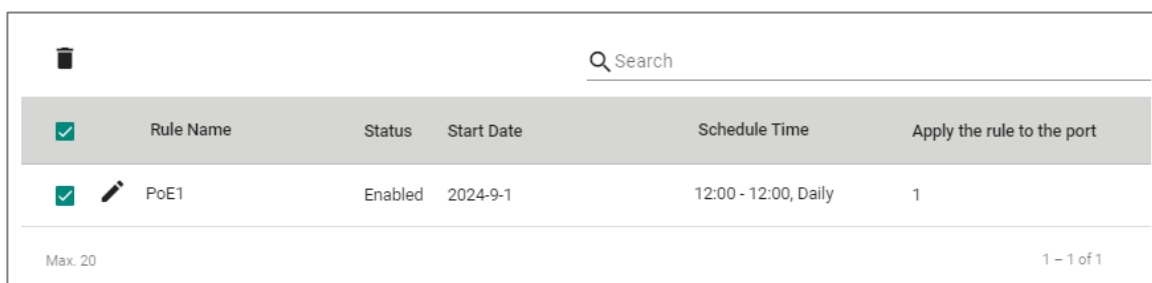
UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Apply the rule to port</b>	Specify which ports should use this rule.	Select port(s) from the drop-down list	None
-------------------------------	---	--	------

## PoE - Scheduling - Delete Rule

### Menu Path: Port > PoE – Scheduling

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



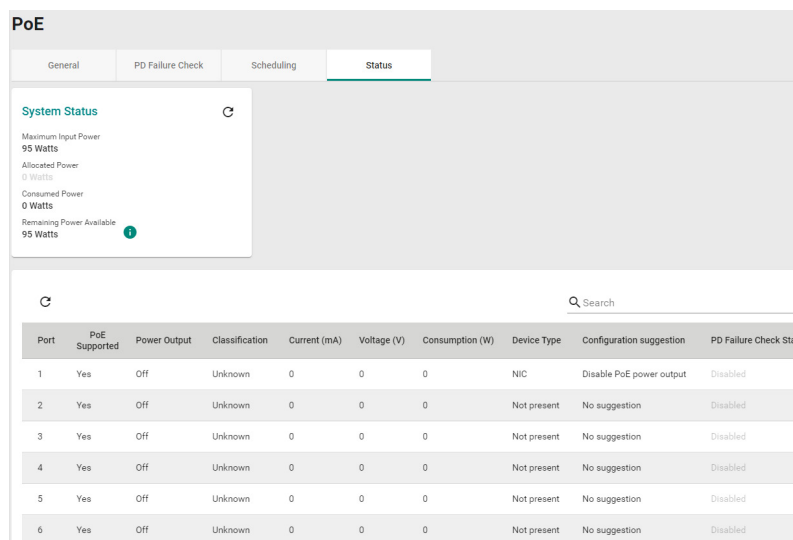
<input checked="" type="checkbox"/>	Rule Name	Status	Start Date	Schedule Time	Apply the rule to the port
<input checked="" type="checkbox"/>	PoE1	Enabled	2024-9-1	12:00 - 12:00, Daily	1

Max. 20 1 - 1 of 1

## PoE - Status

### Menu Path: Network Configuration > Ports > PoE - Status

This tab lets you view the current PoE status of your ports.



Port	PoE Supported	Power Output	Classification	Current (mA)	Voltage (V)	Consumption (W)	Device Type	Configuration suggestion	PD Failure Check Status
1	Yes	Off	Unknown	0	0	0	NIC	Disable PoE power output	Disabled
2	Yes	Off	Unknown	0	0	0	Not present	No suggestion	Disabled
3	Yes	Off	Unknown	0	0	0	Not present	No suggestion	Disabled
4	Yes	Off	Unknown	0	0	0	Not present	No suggestion	Disabled
5	Yes	Off	Unknown	0	0	0	Not present	No suggestion	Disabled
6	Yes	Off	Unknown	0	0	0	Not present	No suggestion	Disabled

Name	Description
------	-------------

<b>Port</b>	Shows the number of the PoE port.
-------------	-----------------------------------

Name	Description
<b>PoE Supported</b>	Shows whether the port supports PoE.
<b>Power Output</b>	Shows whether PoE power output is on or off for the port.
<b>Classification</b>	Shows the PoE power classification of the port. Each PoE power classification has a different maximum power (in watts) by PSE output as follows: <b>0:</b> 15.4 watts <b>1:</b> 4 watts <b>2:</b> 7 watts <b>3:</b> 15.4 watts <b>4:</b> 30 watts
<b>Current (mA)</b>	Shows the amount of current (in mA) being supplied to the port.
<b>Voltage (V)</b>	Shows the voltage (in V) being used for the port.
<b>Consumption (W)</b>	Shows the power consumption (in W) of the device connected to the port.
<b>Device Type</b>	Shows the device type of the device currently connected to the port. <b>Not Present:</b> There are no active connections to the port. <b>802.3at:</b> An IEEE 802.3at PD is connected to the port. <b>802.3af:</b> An IEEE 802.3af PD is connected to the port. <b>NIC:</b> A NIC is connected to the port. <b>Unknown:</b> An unknown PD is connected to the port. <b>N/A:</b> The PoE function is disabled.
<b>Configuration Suggestion</b>	Shows configuration suggestions based on detected conditions. <b>Disable PoE power output:</b> A NIC or unknown PD was detected; you may want to disable PoE power output for the port. <b>Select Force Mode:</b> A higher/lower resistance or higher capacitance was detected; you may want to select <b>Force Mode</b> for the port. <b>Select high power output:</b> An unknown classification was detected; you may want to select <b>High Power</b> output. <b>Raise the external power supply voltage to greater than 46 VDC:</b> When the external supply voltage is detected at less than 46 V, the system suggests raising the voltage. <b>Enable PoE function for detection:</b> The system suggests enabling the PoE function. <b>Select IEEE 802.3at auto mode:</b> When detecting an IEEE 802.3at PD, the system suggests selecting 802.3at Auto mode. <b>Select IEEE 802.3af auto mode:</b> When detecting an IEEE 802.3af PD, the system suggests selecting 802.3af Auto mode.

Name	Description
<b>PD Failure Check</b>	Shows the results of the last PD failure check, if checking is enabled. Refer to Network Configuration > Ports > PoE - PD Failure Check for more information. <ul style="list-style-type: none"> <li>• <b>Disable:</b> PD failure checking is not enabled for the port.</li> <li>• <b>Alive:</b> The port is alive, and passed the last PD failure check.</li> <li>• <b>Not Alive:</b> The port is not alive, and failed the last PD failure check.</li> </ul>

## Link Fault Passthrough

**Menu Path:** Network Configuration > Ports > Link Fault Passthrough

This page lets you enable and configure the Link Fault Passthrough function.

### Note

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

### Note

When Link Fault Passthrough is enabled, both ports need to be linked up. Otherwise, traffic between LAN ports or access from LAN ports to the device's web console might be shut down.

### Note

Available ports may vary depending on the model, and port selection may be fixed for some models.

Status \*  
Enabled ▼

Port 1  
1 ▼

Port 2  
2 ▼

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the Link Fault Passthrough function. When enabled, when any of the port links are down, the other port will be shut down.	Enabled / Disabled	Disabled
<b>Port 1</b>	Specify which port to use as Port 1 in the Link Fault Passthrough pair.	Dropdown list of ports	1
<b>Port 2</b>	Specify which port to use as Port 2 in the Link Fault Passthrough pair.	Dropdown list of ports	2

## LAN Bypass Gen3

**Menu Path:** [Network Configuration](#) > [Ports](#) > [LAN Bypass Gen3](#)

This page lets you enable and configure different LAN bypass modes for your device.

### System Failure Bypass Configuration

**System Failure Bypass Configuration**

Mode  
Disabled ▼

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Mode</b>	<p>Specify which system failure bypass mode to use. When triggered, system failure bypass allows traffic to continue to flow between LAN ports during system failure events, minimizing disruption and maintaining operational integrity.</p> <p><b>Disabled:</b> Disable system failure bypass. Traffic will not pass between LAN ports during device failure.</p> <p><b>Shutdown:</b> Enable system failure bypass only when there is a hardware failure, such as a power outage.</p> <p><b>Shutdown and Halted:</b> Enable bypass function for both hardware failures and software issues, such as the CPU becoming unresponsive.</p>	Disabled / Shutdown / Shutdown and Halted	Shutdown and Halted

## System Runtime Bypass Configuration

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable/ Disable the system runtime bypass feature. When system runtime bypass is enabled, this will temporarily allow traffic to flow through LAN ports unimpeded, ensuring continuous network operation.	Disabled / Enabled	Disabled
<b>Auto Recovery Time</b>	<p>Specify the number of minutes after which the device will automatically disable system runtime bypass after it is enabled, and will then recover to normal LAN port behavior.</p> <p>If this is set to 0, the device will not exit system runtime bypass after it is enabled.</p>	0 to 43200	5

## Layer 2 Switching

### Menu Path: Network Configuration > Layer 2 Switching

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

This section includes these pages:

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

## VLAN

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

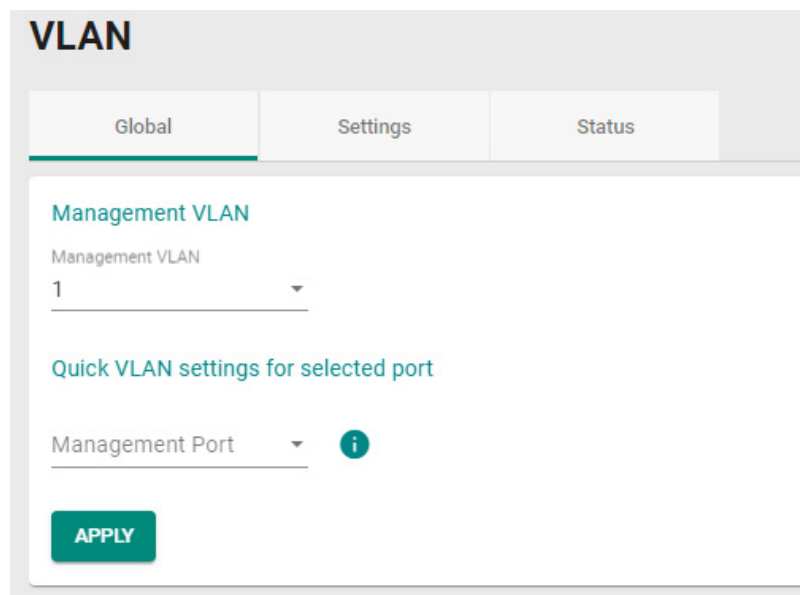
This page includes these tabs:

- Global
- Settings
- Status

## VLAN Settings - Global

**Menu Path:** [Network Configuration](#) > [Layer 2 Switching](#) > [VLAN - Global](#)

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



The screenshot shows the 'VLAN' configuration page with the 'Global' tab selected. The 'Management VLAN' is set to '1'. Below it, there is a section for 'Quick VLAN settings for selected port' with a 'Management Port' dropdown menu and an information icon. An 'APPLY' button is located at the bottom left of the configuration area.

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

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

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

### VLAN

Global Settings Status

**+**

<input type="checkbox"/>	VLAN	Member Port
<input type="checkbox"/>	1	1, 2, 3, 4, 5, 6, 7, 9, 10
<input type="checkbox"/>	2	8
<input type="checkbox"/>	40	
<input type="checkbox"/>	50	
<input type="checkbox"/>	4040	
<input type="checkbox"/>	4041	

Max. 32

**↻**

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

The top table shows a list of VLANs.



UI Setting	Description
------------	-------------

<b>VLAN</b>	Shows the VID for the VLAN.
<b>Member Port</b>	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
------------	-------------

<b>Port</b>	Shows which port this row describes.
<b>Mode</b>	Shows the VLAN mode for the port.
<b>PVID</b>	Shows the PVID for the port.
<b>Untagged VLAN</b>	Shows the Untagged VLAN.
<b>Tagged VLAN</b>	Shows the Tagged VLAN.

## VLAN - Settings - Create VLAN

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

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

### Create VLAN

VID \* i

Max 16 VLANs

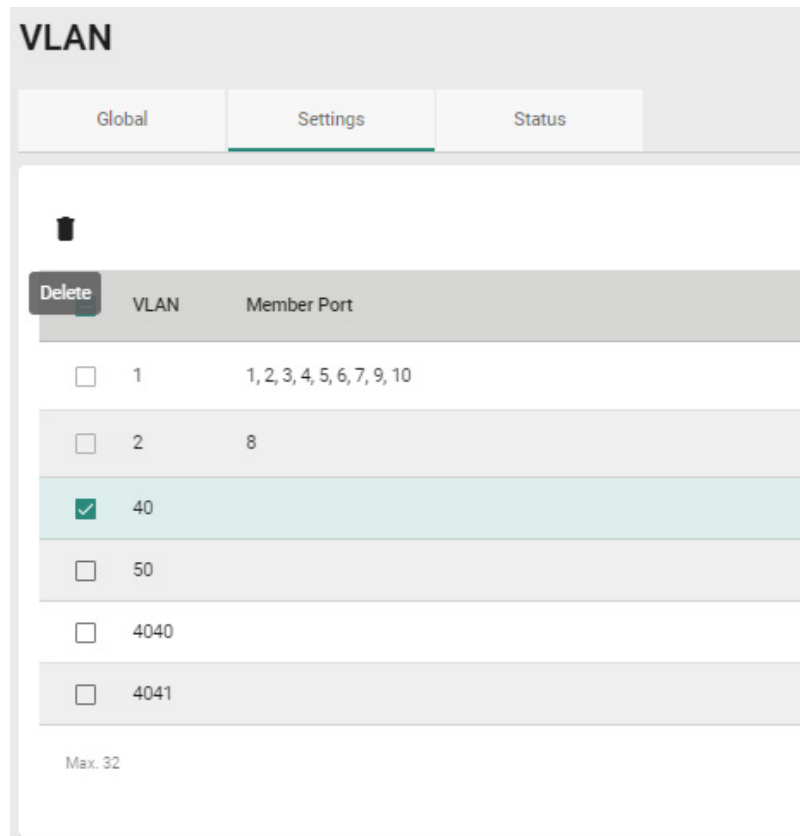
CANCEL **CREATE**

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

## VLAN - Settings - Delete VLAN

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

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



## VLAN - Settings - Edit Port Settings

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

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

## Edit Port 1 Settings

Mode  
Access ▼

---

PVID  
1 ▼

---

Tagged VLAN  
..... ▼

---

Untagged VLAN  
1 ▼

---

CANCEL

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Mode</b>	Specify which VLAN mode the port should use: <b>Access:</b> Define the port as an Access port. This is used when connecting to single devices without tags. <b>Trunk:</b> Define the port as a Trunk port. This is used when connecting to another 802.1Q VLAN-aware router. <b>Hybrid:</b> 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
<b>PVID</b>	Set the default VLAN ID to use for traffic from untagged devices that connect to the port.	1 to 4094	1
<b>Tagged VLAN</b> (when editing settings for the Management Port)	If the <b>Mode</b> is set to <b>Trunk</b> or <b>Hybrid</b> , you can specify what VLAN IDs tagged devices that connect to the port will use. Use commas to separate different VLANs.	All Member VLANs / 1 to 4094	N/A
<b>Untagged VLAN</b> (when editing settings for the Management Port)	If the <b>Mode</b> is set to <b>Access</b> , 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 VLANs / 1 to 4094	N/A

## VLAN - Status

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

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

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

UI Setting	Description
<b>VLAN</b>	Shows the VID of the VLAN.
<b>Hybrid Port</b>	Shows ports acting as a Hybrid Port for the VLAN.
<b>Trunk Port</b>	Shows ports acting as a Trunk Port for the VLAN.
<b>Access Port</b>	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

Aging Time

300

5 - 300 sec.

APPLY



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

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Aging Time</b>	Specify the aging time for MAC address entries in seconds. The aging time determines how long entries will be kept in the MAC address table in the device's memory before expiring.	5 to 300	300
-------------------	---	----------	-----

The MAC address table shows the following information:

UI Setting	Description
------------	-------------

<b>Index</b>	Shows the index number of the MAC address.
<b>VLAN ID</b>	Shows which VLAN ID is being used for the MAC address.
<b>MAC Address</b>	Shows the MAC address.

UI Setting	Description
<b>Type</b>	Shows what kind of MAC address entry this is: <b>Learnt Unicast:</b> Used for all learnt unicast MAC addresses. <b>Learnt Multicast:</b> Used for all learnt multicast MAC addresses. <b>Static Unicast:</b> Used for all static unicast MAC addresses. <b>Static Multicast:</b> Used for all static multicast MAC addresses.
<b>Port</b>	Shows which port on the device the MAC address is connected to.

## QoS

### Menu Path: [Network Configuration](#) > [Layer 2 Switching](#) > [QoS](#)

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

This page includes these tabs:

- CoS Mapping
- DSCP Mapping
- Port Classification









### CoS Mapping

#### Menu Path: [Network Configuration](#) > [Layer 2 Switching](#) > [QoS - CoS Mapping](#)

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

**QoS**

CoS Mapping    DSCP Mapping    Port Classification

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

UI Setting	Description
<b>CoS</b>	Shows the CoS level. Higher numbers indicate higher priority.
<b>Level</b>	Shows the priority queue. Higher numbers indicate higher priority.

**CoS Mapping - Edit a CoS Mapping**

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

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

**Edit CoS 0 Settings**

Priority Queue \*

0 ▼

CANCEL    APPLY

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

## DSCP Mapping

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

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

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

UI Setting	Description
<b>DSCP</b>	Shows the DSCP level. Higher numbers indicate higher priority.
<b>Level</b>	Shows the priority queue. Higher numbers indicate higher priority.



## DSCP Mapping - Edit a DSCP Mapping

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

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

### Edit DSCP 0x0 (1) Settings

Priority Queue \*  
0

CANCEL

APPLY

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

## Port Classification

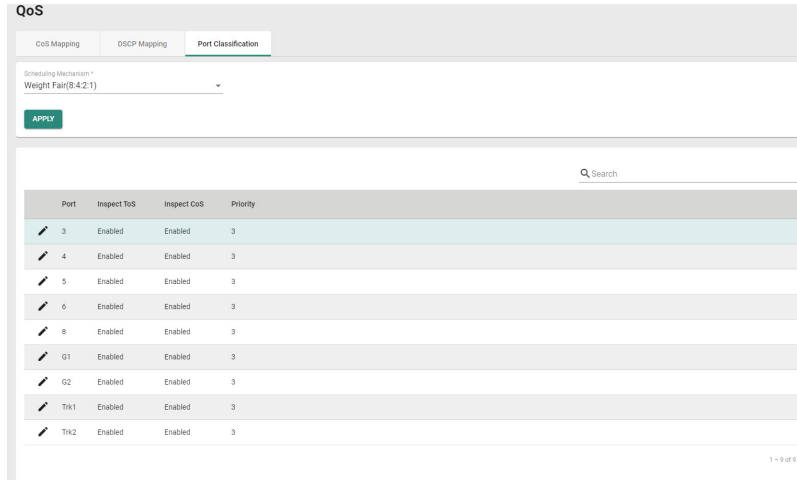
**Menu Path:** Network Configuration > Layer 2 Switching > QoS - Port Classification

This tab lets you set up QoS queueing mechanisms.

### ✎ Note

For TN-4900 Series 16-port models, port priority must be handled in 2 separate groups as follows, due to design limitations:

- Ports 1 to 8
- Ports G1 to G8  
or  
Ports 9 to 12 and G1 to G4  
(depends on your model)



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

The port classification table shows the following information:

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

## Port Classification - Edit Port Setting

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

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

**Edit Port 3 Settings**

Inspect ToS \*  
Enabled

Inspect CoS \*  
Enabled

Priority \*  
3

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Inspect ToS</b>	Enable or disable inspection of Type of Service (ToS) bits in the IPv4 frame to determine the priority of each frame.	Enabled or Disabled	Enabled
<b>Inspect CoS</b>	Enable or disable inspection of 802.1p CoS tags in the MAC frame to determine the priority of each frame.	Enabled or Disabled	Enabled
<b>Priority</b>	Specify the priority of the port. Higher numbers indicate higher priority.	0 to 7	3

## Rate Limit

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

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

**Note**

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

**Rate Limit**

Ingress Policy \*  
Limit Broadcast

Ingress Action \*  
Drop Packet

APPLY

Search

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

1 - 7 of 7

## Rate Limit Settings

Ingress Policy \*  
Limit Broadcast

Ingress Action \*  
Drop Packet

APPLY

## Rate Limit

Ingress Policy \*  
Limit Broadcast

---

Ingress Action \*  
Port Disable

Port Disable Period \*  
0

1 - 65535

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Ingress Policy</b>	<p>Select which kind of traffic ingress rate limiting will be applied to.</p> <p><b>Limit All:</b> Rate limit will be applied to all traffic.</p> <p><b>Limit Broadcast, Multicast and Flooded Unicast:</b> Rate limit will be applied to broadcast, multicast, and flooded unicast traffic only.</p> <p><b>Limit Broadcast, Multicast:</b> Rate limit will be applied to broadcast and multicast traffic only.</p> <p><b>Limit Broadcast:</b> Rate limit will be applied to broadcast traffic only.</p>	Limit All / Limit Broadcast, Multicast and Flooded Unicast / Limit Broadcast / Limit Broadcast	Limit Broadcast
<b>Ingress Action</b>	<p>Select the ingress action.</p> <p><b>Drop Packet:</b> The rate limit will discard incoming packets that do not comply with the ingress policy.</p> <p><b>Port Disable:</b> The rate limit will disable the port that do not comply with the ingress policy.</p>	Drop Packet / Port Disable	Drop Pakcet
<b>Port Disabled Period</b> <b>(Only if Ingress Action is set as Port Disable)</b>	<p>Select the port disable period during which the port will be disabled. Once this period is over, the port will be re-enabled. However, if the port does not comply with the ingress policy again, it will be disabled then.</p>	1-65535	0

## Rate Limit Port List

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

UI Setting	Description
<b>Port</b>	Shows which port this row describes.
<b>Ingress</b>	Shows the ingress bandwidth rate limit method and bandwidth.
<b>Egress</b>	Shows the egress bandwidth rate limit method and bandwidth.

## Rate Limit - Edit Port Settings

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

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

### Edit Port 1/1 Settings

Ingress \*

Not Limited

---

Egress \*

Not Limited

---

CANCEL **APPLY**

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

## Multicast

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

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

This section includes these pages:

- IGMP Snooping
- Static Multicast Table

## IGMP Snooping

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

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

This page includes these tabs:

- VLAN Settings
- Group Table
- Forwarding Table

### IGMP Snooping

VLAN Settings    Group Table    Forwarding Table

Query Interval \*  
125  
20 - 600 sec.  
**APPLY**

↻

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

## VLAN Settings

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

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

### IGMP Snooping

VLAN Settings    Group Table    Forwarding Table

Query Interval \*  
125  
20 - 600 sec.  
**APPLY**

↻

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



## IGMP VLAN Settings

### IGMP Snooping

VLAN Settings
Group Table
Forwarding Table

Query Interval \*  
  
20 - 600 sec.

APPLY

---

↻

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

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

## IGMP VLAN List

### IGMP Snooping

VLAN Settings    Group Table    Forwarding Table

Query Interval \*  
125  
20 - 600 sec.  
**APPLY**

↻

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

### UI Setting

### Description

#### VLAN ID

Shows which VLAN ID this row describes.

#### IGMP Snooping

Shows whether IGMP snooping is enabled or disabled for the VLAN.

#### Querier

Shows which version of IGMP snooping the VLAN will use.

#### Static Router Port

Shows the static router port the VLAN will use to connect to the multicast router for IGMP snooping.

## VLAN Settings - Edit VLAN Settings

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

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

## Edit VLAN 1 Settings

IGMP Snooping \*  
 Disabled ▾

Querier \*  
 V1/V2 ▾

Static Router Port ▾

CANCEL

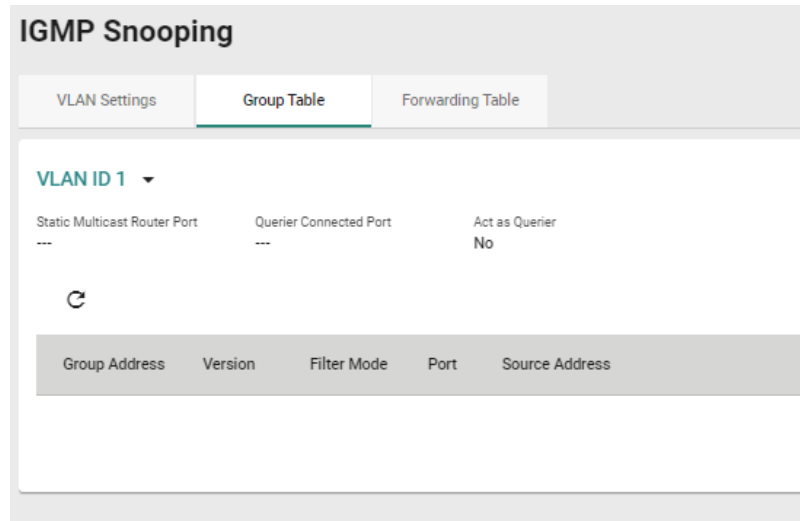
APPLY

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

## Group Table

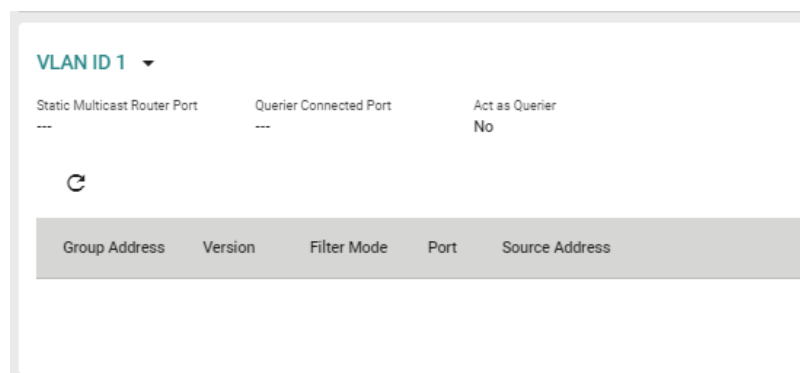
**Menu Path: Network Configuration > Layer 2 Switching > Multicast > IGMP Snooping - Group Table**

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



## VLAN Group Table List

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



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

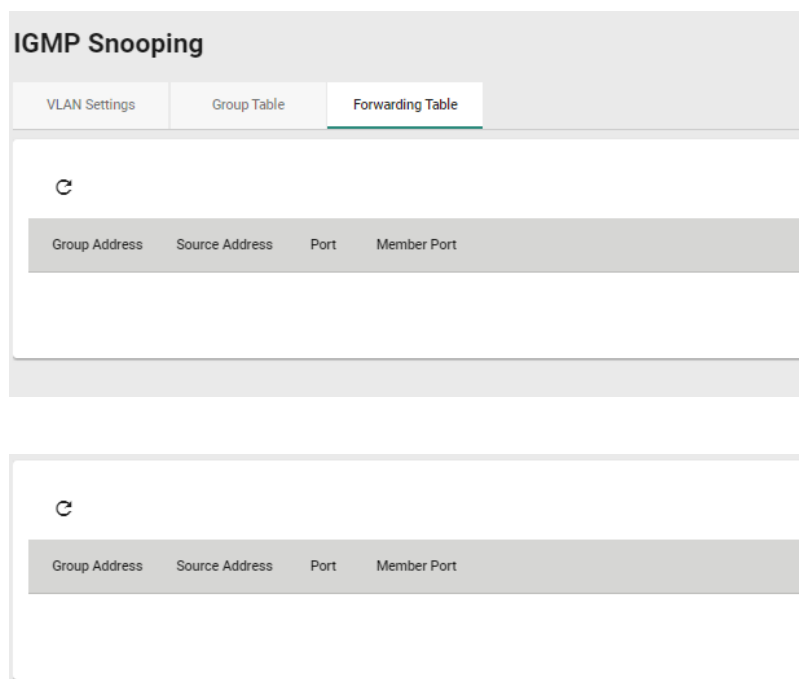
UI Setting	Description
------------	-------------

**Source Address** When IGMP v3 is enabled, this shows the multicast source address for the group address.

## Forwarding Table

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

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



UI Setting	Description
------------	-------------

**Group Address** Shows the multicast group IP address.

**Source Address** Shows the IP address the multicast group will receive multicast streams from.

**Port** Shows the port receiving the multicast stream.

**Member Port** Shows the port the multicast stream is forwarded to.

# Static Multicast Table

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

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

### Note

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

### Note

Moxa's Router Series devices manage MAC address learning for VLANs using IVL (Independent VLAN Learning), which uses separate MAC address tables for each VLAN so that MAC address learning for different VLANs do not interfere with each other. This allows the same MAC address to be used in multiple VLANs without causing forwarding issues.

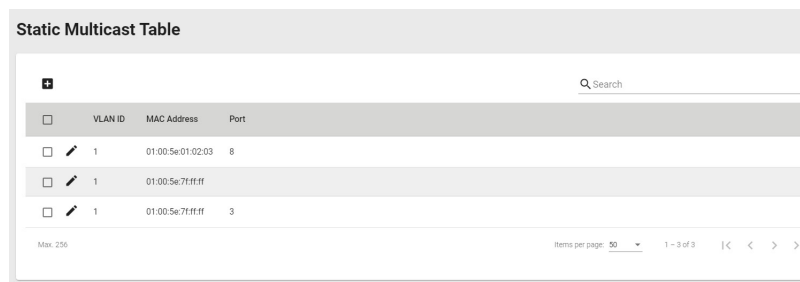
This may lead to a larger MAC address table size, as each VLAN maintains its own individual address table, and the number of MAC address entries will increase based on the number of VLAN member ports used.

### Limitations

You can create up to 256 static multicast entries, though some models may support up to 1000 static multicast entries.

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

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



<input type="checkbox"/>	VLAN ID	MAC Address	Port
<input type="checkbox"/>	1	01:00:5e:01:02:03	8
<input type="checkbox"/>	1	01:00:5e:71:ff:ff	
<input type="checkbox"/>	1	01:00:5e:71:ff:ff	3

UI Setting	Description
<b>VLAN ID</b>	Shows the VLAN ID used for the static multicast entry.
<b>MAC Address</b>	Shows the MAC address used for the static multicast entry.

UI Setting	Description
------------	-------------

**Port** Shows which ports are included for the static multicast entry.

### Static Multicast Table - Create Static Multicast

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

Clicking the **Add (+)** icon on the **Network Configuration > Layer 2 Switching > Multicast > Static Multicast Table** page will open this dialog box. This dialog lets you add a static multicast entry. Click **CREATE** to save your changes and add the new static multicast entry.

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

#### Create Static Multicast

VLAN ID \*    MAC Address \*    ⓘ

Port \*

CANCEL    CREATE


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

## Static Multicast Table - Edit Static Multicast

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

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

### Edit Static Multicast

VLAN ID *	MAC Address *
1	01:00:5e:01:02:03 
Port *	
8	

CANCEL **APPLY**

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

## Static Multicast Table - Delete Static Multicast

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

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



**Static Multicast Table**

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

Max: 255      Items per page: 50      1 - 3 of 3

## Network Interfaces

### Menu Path: Network Configuration > Network Interfaces

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

This page includes these tabs:

- LAN
- WAN/WAN1
- WAN2/DMZ
- Bridge
- MTU Configuration
- Secondary IP
- Virtual Interface

**Network Interfaces**

LAN    WAN    Bridge    MTU Configuration    Secondary IP    Virtual Interface

Name	Status	VLAN ID	Alias	IP Address	Netmask	Virtual MAC	Directed Broadcast	Source IP Override
LAN	Enabled	1		192.168.127.254	255.255.255.0	-	Disabled	Disabled
lan1	Enabled	40		192.168.126.254	255.255.255.0	-	Disabled	Disabled
lan_test	Enabled	50		192.168.125.29	255.255.255.0	-	Disabled	Disabled
lan_test2	Disabled	4040		192.168.9.2	255.255.255.0	-	Disabled	Disabled

Max: 15      Items per page: 50      1 - 4 of 4

## 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

Network Interfaces									
LAN	WAN	Bridge	MTU Configuration	Secondary IP					
<input type="checkbox"/>	Name	Status	VLAN ID	Alias	IP Address	Netmask	Virtual MAC	Directed Broadcast	Source IP Overwrite
<input type="checkbox"/>	 LAN	Enabled	1	0	192.168.127.254	255.255.255.0	--	Disabled	Disabled
<input type="checkbox"/>	 lan2	Enabled	3		192.168.126.1	255.255.255.0	--	Disabled	Disabled
Max. 16									

### UI Setting

### Description

<b>Name</b>	Shows the name of the interface.
<b>Status</b>	Shows the status of the interface.
<b>VLAN ID</b>	Shows the VLAN ID used for the interface.
<b>Alias</b>	Shows the alias for the interface.
<b>IP Address</b>	Shows the IP address of the interface.
<b>Netmask</b>	Shows the subnet mask of the interface.
<b>Virtual MAC</b>	Shows the virtual MAC address of the interface.
<b>Directed Broadcast</b>	Shows whether directed broadcast is enabled for the interface.
<b>Source IP Overwrite</b>	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.

## Create LAN Interface Entry

Name \*  
0 / 12

VLAN Interface \*  
Enabled

VLAN ID \*  
1 - 4094

Alias  
0 / 31

Proxy ARP  
Disabled

Connection Type \*  
Static IP

Directed Broadcast \*  
Disabled

Source IP Overwrite  
Disabled

IP Address \*  
24 (255.255.255.0)


Netmask \*  
24 (255.255.255.0)

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

CANCEL


CREATE

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

UI Setting	Description	Valid Range	Default Value
<b>Proxy ARP</b>	Enable or disable proxy ARP for the interface.	Enabled / Disabled	Disabled
<b>Connection Type</b>	Select the connection type for the interface.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> <b>Note</b> The LAN interfaces require static IP addresses; dynamic IPs are not supported.</p> </div>	Static IP / Dynamic IP	Static IP
<b>Directed Broadcast</b>	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
<b>Source IP Overwrite</b>	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled
<b>IP Address</b> (Only when Connection Type set as Static IP)	Specify the IP address of the interface.	Valid IP address	N/A
<b>Netmask</b> (Only when Connection Type set as Static IP)	Specify the subnet mask of the interface.	Valid subnet mask	24 (255.255.255.0)
<b>DHCP Client Option 66/67</b> (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
<b>Virtual MAC</b>	Specify the virtual MAC address of the interface.	Valid MAC address	00:00:00:00:00:00

## LAN - Edit LAN Interface Entry

### Menu Path: [Network Configuration](#) > [Network Interfaces - LAN](#)

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

### Edit LAN Interface Entry

Name \*  
 3 / 12

VLAN Interface \*

VLAN ID \*  
 1 - 4094

Alias  
 0 / 31

Directed Broadcast \*  Source IP Overwrite

IP Address \*  Netmask \*

Virtual MAC

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

UI Setting	Description	Valid Range	Default Value
<b>Connection Type</b>	Select the connection type for the interface.  <b>Note</b> The LAN interfaces require static IP addresses; dynamic IPs are not supported.	Static IP / Dynamic IP	Static IP
<b>Directed Broadcast</b>	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
<b>Source IP Overwrite</b>	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled
<b>IP Address</b> (Only when Connection Type set as Static IP)	Specify the IP address of the interface.	Valid IP address	N/A
<b>Netmask</b> (Only when Connection Type set as Static IP)	Specify the subnet mask of the interface.	Valid subnet mask	24 (255.255.255.0)
<b>DHCP Client Option 66/67</b> (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
<b>Virtual MAC</b>	Specify the virtual MAC address of the interface.	Valid MAC address	00:00:00:00:00:00

## Delete LAN Interface Entry

### Menu Path: Network Configuration > Network Interfaces - LAN

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

Network Interfaces																																				
LAN		WAN		Bridge		MTU Configuration		Secondary IP																												
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>Delete</span> <table border="1"> <thead> <tr> <th>Name</th> <th>Status</th> <th>VLAN ID</th> <th>Alias</th> <th>IP Address</th> <th>Netmask</th> <th>Virtual MAC</th> <th>Directed Broadcast</th> <th>Source IP Overwrite</th> </tr> </thead> <tbody> <tr> <td>LAN</td> <td>Enabled</td> <td>1</td> <td>0</td> <td>192.168.127.254</td> <td>255.255.255.0</td> <td>-</td> <td>Disabled</td> <td>Disabled</td> </tr> <tr style="background-color: #e0f2f1;"> <td>lan2</td> <td>Enabled</td> <td>3</td> <td></td> <td>192.168.126.1</td> <td>255.255.255.0</td> <td>-</td> <td>Disabled</td> <td>Disabled</td> </tr> </tbody> </table> </div>										Name	Status	VLAN ID	Alias	IP Address	Netmask	Virtual MAC	Directed Broadcast	Source IP Overwrite	LAN	Enabled	1	0	192.168.127.254	255.255.255.0	-	Disabled	Disabled	lan2	Enabled	3		192.168.126.1	255.255.255.0	-	Disabled	Disabled
Name	Status	VLAN ID	Alias	IP Address	Netmask	Virtual MAC	Directed Broadcast	Source IP Overwrite																												
LAN	Enabled	1	0	192.168.127.254	255.255.255.0	-	Disabled	Disabled																												
lan2	Enabled	3		192.168.126.1	255.255.255.0	-	Disabled	Disabled																												
Max. 16																																				

## WAN/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.



### Network Interfaces

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

**VLAN ID**  
 VLAN ID  
 2

**Connection**  
 Status: Enabled  
 Connection Type: Static IP

**Directed Broadcast**  
 Status: Disabled

Source IP Overwrite: Disabled

**Address Information**  
 IP Address: 10.123.13.33  
 Netmask \*: 23 (255.255.254.0)  
 Gateway: 10.123.12.1

**PPTP Dialup**  
 Status: Disabled

IP Address: 0.0.0.0  
 Username: \_\_\_\_\_ Password: \_\_\_\_\_  
0 / 30 0 / 30

MPPE Encryption: None

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

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

**APPLY**

## VLAN ID

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

## Connection

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

## Address Information

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

## PPTP Dialup

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable PPTP connection for the interface.	Enabled / Disabled	Disabled
<b>IP Address</b>	Specify the PPTP service IP address.	Valid IP address	0.0.0.0
<b>User Name</b>	Enter the username to use for dialing in to the PPTP service.	1 to 30 characters	N/A
<b>Password</b>	Enter the password to use for dialing in to the PPTP service.	1 to 30 characters	N/A

UI Setting	Description	Valid Range	Default Value
<b>MPPE Encryption</b>	Enable or disable MPPE encryption.	None / Encrypt	None

## Virtual MAC

UI Setting	Description	Valid Range	Default Value
<b>Virtual MAC</b>	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
<b>Primary DNS Server</b>	Specify the primary DNS IP address.	IP Address	0.0.0.0
<b>Secondary DNS Server</b>	Specify the secondary DNS IP address.	IP Address	0.0.0.0
<b>Tertiary DNS Server</b>	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.

### Network Interfaces

LAN
WAN
Bridge
MTU Configuration
Secondary IP

**VLAN ID**  
 VLAN ID  
 3

**Connection**  
 Status: Enabled  
 Connection Type: Dynamic IP

**Directed Broadcast**  
 Status: Disabled

Source IP Overwrite: Disabled

**PPTP Dialup**  
 Status: Disabled

IP Address: 0.0.0.0    Username:    Password:   

MPPE Encryption: None

**DHCP Client Option 66/67**  
 Status: Disabled

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

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

**APPLY**

## VLAN ID

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

## Connection

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

## PPTP Dialup

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

## DHCP Client Option 66/67

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

## Virtual MAC

UI Setting	Description	Valid Range	Default Value
<b>Virtual MAC</b>	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
<b>Primary DNS Server</b>	Specify the primary DNS IP address.	IP Address	0.0.0.0
<b>Secondary DNS Server</b>	Specify the secondary DNS IP address.	IP Address	0.0.0.0
<b>Tertiary DNS Server</b>	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

## PPPoE

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

### Network Interfaces

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

**VLAN ID**  
 VLAN ID  
 2

**Connection**  
 Status: Enabled  
 Connection Type: PPPoE

**Directed Broadcast**  
 Enabled / Disabled

Source IP Overwrite: Disabled

**PPPoE Dialup**  
 Username \* (0/30) Password \* (0/30) Host Name (0/30)

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

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

**APPLY**

## VLAN ID

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

## Connection

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

## PPPoE Dialup

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

## Virtual MAC

UI Setting	Description	Valid Range	Default Value
<b>Virtual MAC</b>	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
<b>Primary DNS Server</b>	Specify the primary DNS IP address.	IP Address	0.0.0.0
<b>Secondary DNS Server</b>	Specify the secondary DNS IP address.	IP Address	0.0.0.0
<b>Tertiary DNS Server</b>	Specify the tertiary DNS IP address.	IP Address	0.0.0.0



## WAN2/DMZ

### Menu Path: Network Configuration > Network Interfaces - WAN2/DMZ

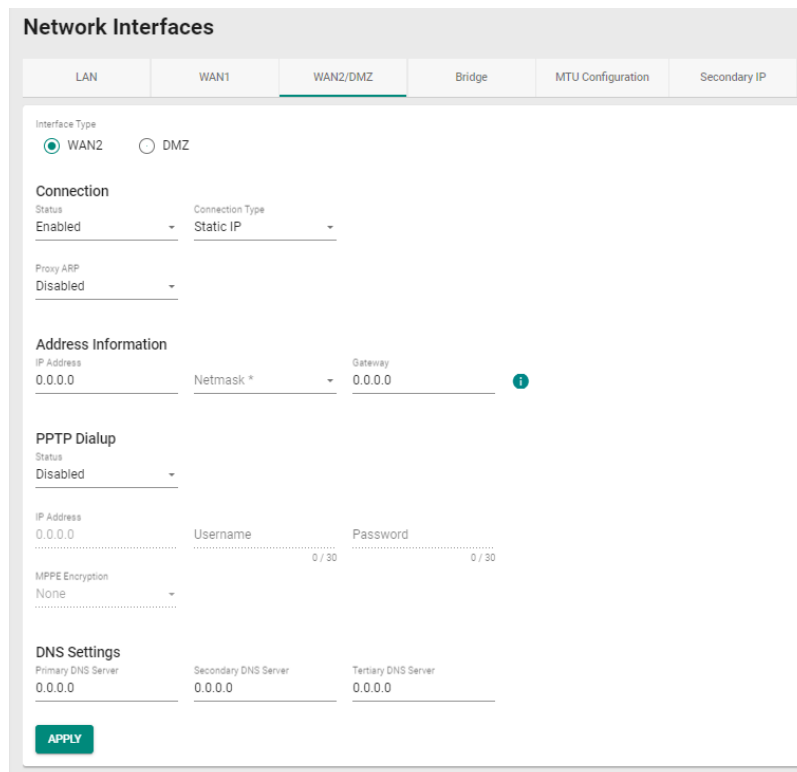
This page lets you configure the settings for the WAN2 or DMZ interfaces of your device. WAN interfaces are VLAN-based; when WAN is enabled for a VLAN ID, all ports associated with that VLAN ID will act as a single WAN interface.

#### Note

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

## Static IP

If you select **WAN2** as the **Interface Type** and **Static IP** for the **Connection Type**, these settings will appear.



The screenshot shows the 'Network Interfaces' configuration page. The 'WAN2/DMZ' tab is selected. Under 'Interface Type', 'WAN2' is selected. Under 'Connection', 'Status' is 'Enabled' and 'Connection Type' is 'Static IP'. Under 'Address Information', 'IP Address' is '0.0.0.0', 'Netmask \*' is a dropdown, and 'Gateway' is '0.0.0.0'. Under 'PPTP Dialup', 'Status' is 'Disabled'. Under 'MPPE Encryption', it is 'None'. Under 'DNS Settings', 'Primary DNS Server', 'Secondary DNS Server', and 'Tertiary DNS Server' are all '0.0.0.0'. An 'APPLY' button is at the bottom.

## Connection

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

## Address Information

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

## PPTP Dialup

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

## Virtual MAC

UI Setting	Description	Valid Range	Default Value
<b>Virtual MAC</b>	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
<b>Primary DNS Server</b>	Specify the primary DNS IP address.	IP Address	0.0.0.0
<b>Secondary DNS Server</b>	Specify the secondary DNS IP address.	IP Address	0.0.0.0
<b>Tertiary DNS Server</b>	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

## Dynamic IP

If you select **WAN2** as the **Interface Type** and **Dynamic IP** for the **Connection Type**, these settings will appear.

### Network Interfaces

LAN
WAN1
WAN2/DMZ
Bridge
MTU Configuration
Secondary IP

Interface Type  
 WAN2     DMZ

Connection  
 Status: Enabled    Connection Type: Dynamic IP

Proxy ARP  
 Disabled

PPTP Dialup  
 Status: Disabled

IP Address: 0.0.0.0    Username: \_\_\_\_\_    Password: \_\_\_\_\_  
0 / 30                                  0 / 30

MPPE Encryption  
 None

DHCP Client Option 66/67  
 Status: Disabled

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

APPLY

## Connection

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

## PPTP Dialup

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

## DHCP Client Option 66/67

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

## DNS Settings

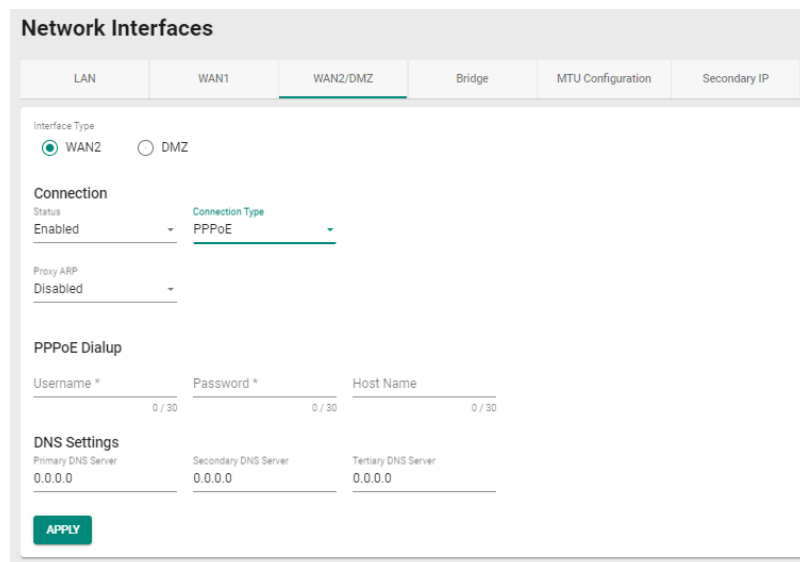
### Note

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
<b>Primary DNS Server</b>	Specify the primary DNS IP address.	IP Address	0.0.0.0
<b>Secondary DNS Server</b>	Specify the secondary DNS IP address.	IP Address	0.0.0.0
<b>Tertiary DNS Server</b>	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

## PPPoE

If you select **WAN2** as the **Interface Type** and **PPPoE** for the **Connection Type**, these settings will appear.



The screenshot shows the 'Network Interfaces' configuration page. The 'WAN2/DMZ' tab is selected. Under 'Interface Type', 'WAN2' is selected. Under 'Connection', 'Status' is 'Enabled' and 'Connection Type' is 'PPPoE'. Under 'Proxy ARP', it is 'Disabled'. The 'PPPoE Dialup' section has three input fields: 'Username \*' (0/30), 'Password \*' (0/30), and 'Host Name' (0/30). The 'DNS Settings' section has three input fields: 'Primary DNS Server' (0.0.0.0), 'Secondary DNS Server' (0.0.0.0), and 'Tertiary DNS Server' (0.0.0.0). An 'APPLY' button is at the bottom.

## Connection

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

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Proxy ARP</b>	Enable or disable the Proxy ARP.	Enabled / Disabled	Disabled
------------------	----------------------------------	--------------------	----------

## PPPoE Dialup

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>User Name</b>	Specify the username used to connect to the PPPoE service.	1 to 30 characters	N/A
------------------	--	--------------------	-----

<b>Password</b>	Specify the password used to connect to the PPPoE service.	1 to 30 characters	N/A
-----------------	--	--------------------	-----

<b>Host Name</b>	Specify the hostname of the PPPoE server.	1 to 30 characters	N/A
------------------	---	--------------------	-----

## 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
------------	-------------	-------------	---------------

<b>Primary DNS Server</b>	Specify the primary DNS IP address.	IP Address	0.0.0.0
---------------------------	-------------------------------------	------------	---------

<b>Secondary DNS Server</b>	Specify the secondary DNS IP address.	IP Address	0.0.0.0
-----------------------------	---------------------------------------	------------	---------

<b>Tertiary DNS Server</b>	Specify the tertiary DNS IP address.	IP Address	0.0.0.0
----------------------------	--------------------------------------	------------	---------

## DMZ

If you select **DMZ** as the **Interface Type**, these settings will appear.

**Network Interfaces**

LAN | WAN1 | **WAN2/DMZ** | Bridge | MTU Configuration | Secondary IP

Interface Type  
 WAN2  DMZ

Address Information  
 IP Address: 0.0.0.0 | Netmask \*

**APPLY** **DMZ Setup Wizard**

## Address Information

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

## DMZ Setup Wizard

### Menu Path: Network Configuration > Network Interfaces - WAN2/DMZ

Clicking the **DMZ Setup Wizard** button on the **Network Configuration > Network Interfaces - WAN2/DMZ** page will start a wizard to help you configure security policies for the DMZ.

### Step 1: Select Mode

Select between basic or advanced configuration mode.

**DMZ Setup Wizard**

1 Select Mode | 2 Enable DoS & IPS Setting | 3 Create Firewall Policy

**Configuration Mode**

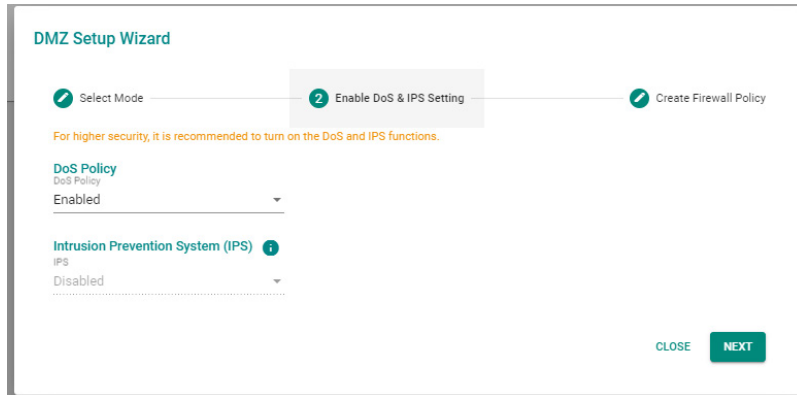
**Basic**  
 This mode will guide users in establishing the default firewall settings to achieve network traffic management for DMZ applications.

**Advanced**  
 In addition to establishing default firewall settings, this mode provides users with advanced options (destination address, service, protocol, port) to create whitelist settings, enabling network traffic management for DMZ applications.

**CLOSE** **NEXT**

### Step 2: Enable DoS & IPS Setting

Select whether to enable DoS protection and IPS functionality.

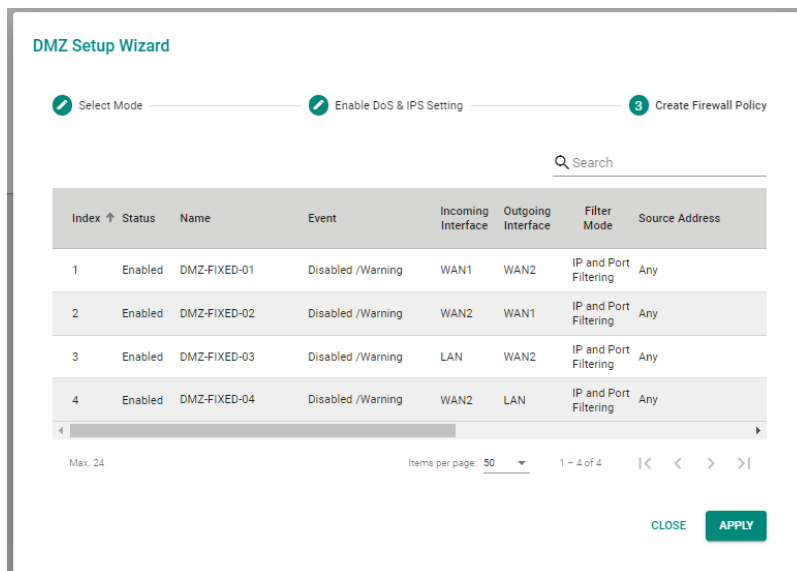


### Step 3: Create Firewall Policy

#### Basic Mode

In basic mode, four policies are preconfigured for you so you don't need to set them manually.

- WAN1 to DMZ (Allow)
- DMZ to WAN1 (Allow)
- LAN to DMZ (Allow)
- DMZ to LAN (Deny)

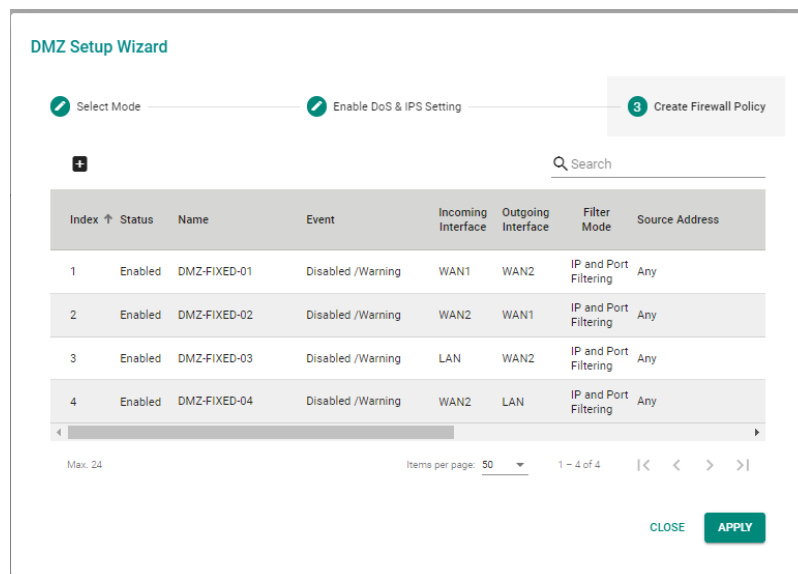




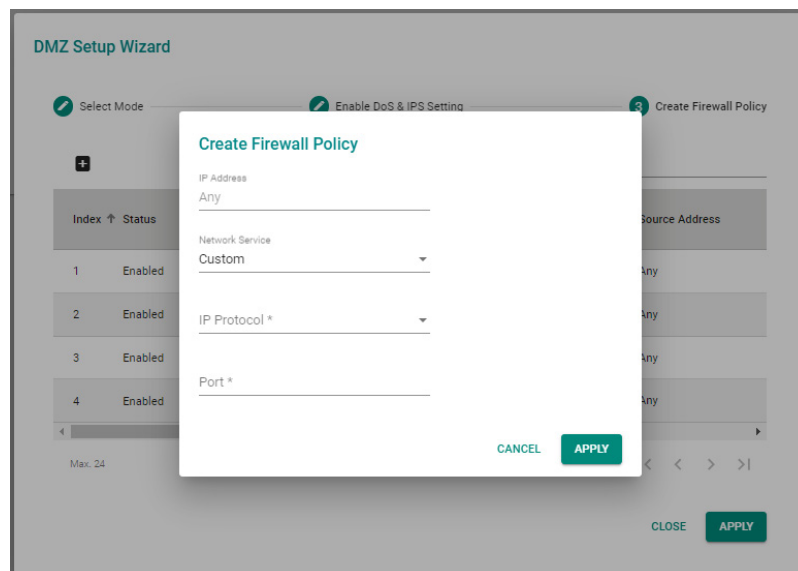
## Advanced Mode

In advanced mode, you will need to set up the correct destination address, service, protocol, and port whitelist policies according to each policy's requirements.

- WAN1 to DMZ (Deny)
- DMZ to WAN1 (Allow)
- LAN to DMZ (Deny)
- DMZ to LAN (Deny)

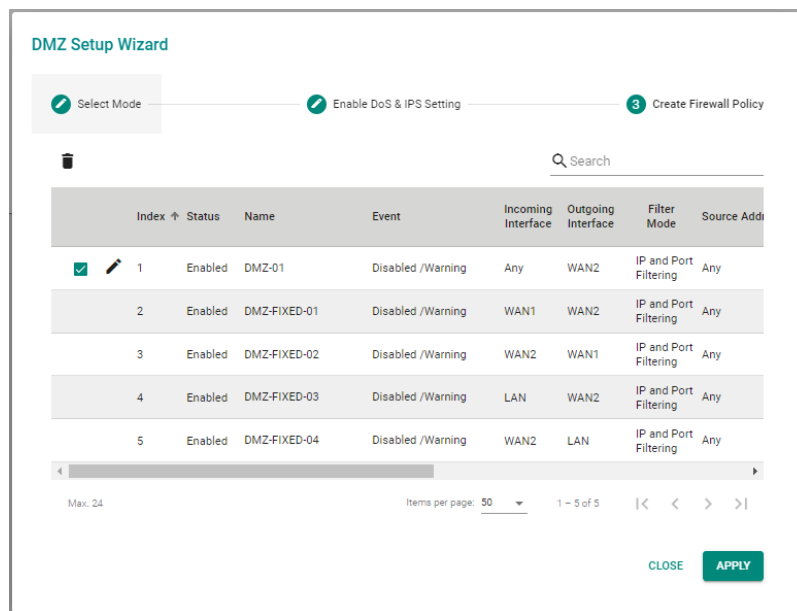


You can also click the **Add (+)** button to add additional firewall policies.



UI Setting	Description	Valid Range	Default Value
<b>IP Address</b>	Specify the IP address.	Valid IP address	Any
<b>Network Service</b>	Specify the network service.	Custom / TELNET / SSH / SMTP / FTP / HTTP / HTTPS / DNS	Custom
<b>IP Protocol</b>	Specify the IP protocol.	TCP / UDP / TCP and UDP	N/A
<b>Port</b>	Specify the port number.	Valid port number	N/A

To delete a firewall policy, select the checkbox next to it and click the **Delete** (🗑️) button.



After confirming your changes, click the **APPLY** button to save your changes and finish the setup wizard.

## Bridge

### Menu Path: Network Configuration > Network Interfaces - Bridge

This page lets you configure a bridge for your device.

You can set up these kinds of bridges:

- Port-based
- Zone-based

## Port-Based

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

### Bridge IP Configuration

Bridge Type

Port-Based  Zone-Based

Name \*

BRG\_LAN

7 / 12

Status \*

Enabled i

IP Address \*

192.168.120.254

Subnet Mask \*

24 (255.255.255.0)

Bridge Member

APPLY

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

## Zone-Based

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

## 🔔 Limitations

You can create up to 4 different bridge zones.

### Bridge IP Configuration

Bridge Type

Port-Based  Zone-Based

Name \*  
ZONE\_BRG  
8 / 12

Status \*  
Disabled ⓘ

IP Address \* 0.0.0.0 Subnet Mask \* 0 (0.0.0.0) ▼

**Zone 1**

Name Bridge Member ▼  
0 / 12

**Zone 2**

Name Bridge Member ▼  
0 / 12

**Zone 3**

Name Bridge Member ▼  
0 / 12

**Zone 4**

Name Bridge Member ▼  
0 / 12

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Bridge Type</b>	Select which bridge type you want to use.	Port-Based / Zone-Based	N/A

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the bridge.	1 to 12 characters	ZONE_BRG
<b>Status</b>	Enable or disable the bridge.	Enabled / Disabled	Disabled
<b>IP Address</b>	Specify an IP address for the bridge.	Valid IP address	0.0.0.0
<b>Subnet Mask</b>	Specify a subnet mask for the bridge.	Valid subnet mask	0 (0.0.0.0)

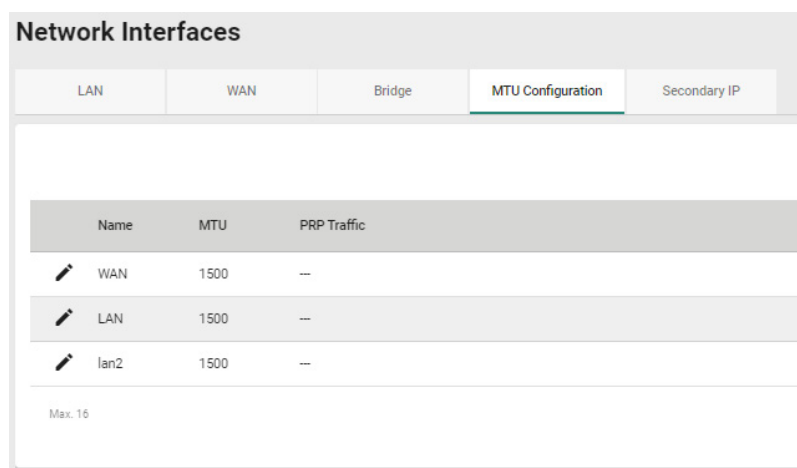
Each zone has the following settings:

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

## MTU Configuration

**Menu Path: Network Configuration > Network Interfaces - MTU**

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



UI Setting	Description
<b>Name</b>	Shows the name of the interface.
<b>MTU</b>	Shows the MTU size used for the interface.

UI Setting	Description
------------	-------------

<b>PRP Traffic</b>	Shows the PRP traffic status for the interface.
--------------------	---

## MTU Configuration - Edit MTU Entry

### Menu Path: Network Configuration > Network Interfaces - MTU Configuration

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

### Edit MTU Entry

Name  
WAN  
.....

MTU \*  
1500  
-----  
68 - 1578

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Name</b>	Shows the name of of this interface. This setting cannot be changed here.	N/A	Name of interface
-------------	---	-----	-------------------

<b>MTU</b>	Specify the MTU size to use for the interface.	68 to 1578	1500
------------	--	------------	------

**Note**  
Jumbo Frames are not currently supported.

## Secondary IP

### Menu Path: Network Configuration > Network Interfaces - Secondary IP

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

## Secondary IP - Create Secondary IP Entry

**Menu Path:** Network Configuration > Network Interfaces - Secondary IP

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

### **Limitations**

You can create up to 640 secondary IPs.

### Create Secondary IP Entry

Interface \*

IP Address \*

Netmask \*

CANCEL

CREATE

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

### Edit Secondary IP Entry

Interface \*  
LAN ▼

IP Address \*  
192.168.100.100

Netmask \*  
24 (255.255.255.0) ▼

CANCEL
APPLY

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



<input checked="" type="checkbox"/>	Interface	VLAN ID	IP Address	Netmask	Type
<input checked="" type="checkbox"/>	LAN	1	192.168.100.100	255.255.255.0	Manual

Max. 640      Items per page: 50      1 - 1 of 1      |< < > >|

## Virtual Interface

**Menu Path: Network Configuration > Network Interfaces - Virtual Interface**

This page lets you create virtual interfaces for your device.

## Loopback Interface List

**Network Interfaces**

LAN    WAN    Bridge    MTU Configuration    Secondary IP    Virtual Interface

Loopback Interface

<input checked="" type="checkbox"/>	Name	Status	ID	IP Address	Netmask
<input checked="" type="checkbox"/>	test	Disabled	1	192.168.1.1	255.255.255.254

Max. 10      Items per page: 50      1 - 1 of 1      |< < > >|

UI Setting	Description
<b>Name</b>	Shows the name of the loopback interface.
<b>Status</b>	Shows whether the loopback interface is enabled or disabled.
<b>ID</b>	Specify the ID of the loopback interface.
<b>IP Address</b>	Specify the IP address of the loopback interface.
<b>Netmask</b>	Specify the subnet mask of the loopback interface.

## Create Loopback Interface Entry

**Menu Path: Network Configuration > Network Interfaces - Virtual Interface - Loopback Interface**

Clicking the **Add (+)** icon on the **Network Configuration > Network Interfaces - Virtual Interface - Loopback Interface** page will open this dialog box. This dialog lets you create a loopback interface.

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

### Create Loopback Interface Entry

Name \*  
 0 / 12

Status \*

ID \* i  
 1 - 64

IP Address \*      Netmask \*  
     

CANCEL      CREATE

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify the name of the loopback interface.	1 to 12 characters	N/A
<b>Status</b>	Enable or disable the loopback interface.	Enabled / Disabled	N/A
<b>ID</b>	Specify the ID for the loopback interface.	1 to 64	N/A
<b>IP Address</b>	Specify the IP address of the secondary interface.	Valid IP address	N/A
<b>Netmask</b>	Specify the subnet mask of the secondary interface.	Valid subnet mask	N/A

## Delete Loopback Interface

**Menu Path: Network Configuration > Network Interfaces - Virtual Interface - Loopback Interface**

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

Network Interfaces						
LAN	WAN	Bridge	MTU Configuration	Secondary IP	Virtual Interface	
Loopback Interface						
						Search
<input checked="" type="checkbox"/>	Name	Status	ID	IP Address	Netmask	
<input checked="" type="checkbox"/>	test	Disabled	1	192.168.1.1	255.255.255.254	
<small>Max. 10</small>			<small>Items per page: 50 1 - 1 of 1  &lt; &gt; &gt; </small>			

## Redundancy

### Menu Path: Redundancy

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

This settings area includes these sections:

- Layer 2 Redundancy
- Layer 3 Redundancy
- WAN Redundancy

### Redundancy - User Privileges

Privileges to Redundancy 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
<b>Layer 2 Redundancy</b>			
Spanning Tree	R/W	R/W	R
Turbo Ring V2	R/W	R/W	R
Turbo Chain	R/W	R/W	R
<b>Layer 3 Redundancy</b>			
VRRP	R/W	R/W	R
WAN Redundancy	R/W	R/W	R

## Layer 2 Redundancy

### Menu Path: [Redundancy](#) > [Layer 2 Redundancy](#)

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

This section includes these pages:

- [Spanning Tree](#)
- [Turbo Ring V2](#)
- [Turbo Chain](#)

## Spanning Tree

### Menu Path: [Redundancy](#) > [Layer 2 Redundancy](#) > [Spanning Tree](#)

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

This page includes these tabs:

- [General](#)
- [Status](#)

#### **Note**

Spanning Tree can only run on the Management VLAN.

## Spanning Tree - General

### Menu Path: [Redundancy](#) > [Layer 2 Redundancy](#) > [Spanning Tree - General](#)

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

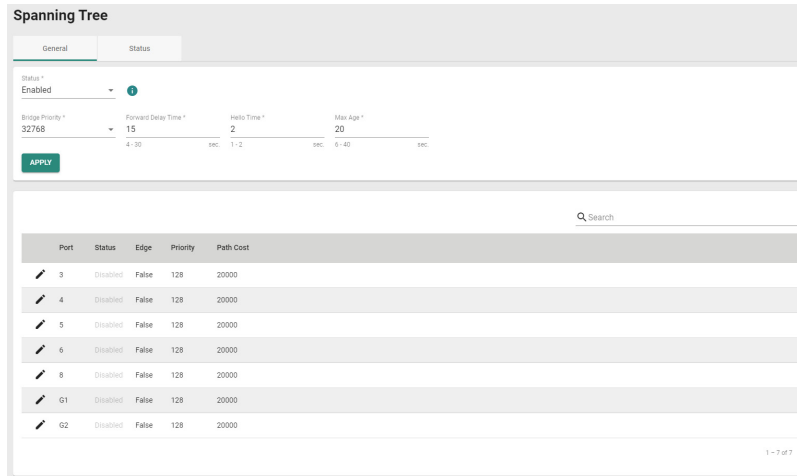
## Spanning Tree Settings

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

## Spanning Tree List

### Note

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



## UI Setting

## Description

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

## Spanning Tree - Edit Port Settings

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

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

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

**Note**

The default value may vary depending on the maximum speed supported by the port.

## Spanning Tree - Status

**Menu Path:** [Redundancy](#) > [Layer 2 Redundancy](#) > [Spanning Tree - Status](#)

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

## Root Information

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

### UI Setting Description

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

## Spanning Tree Port List

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

### UI Setting Description

**Port** Shows the port number.

**Enable** Shows whether Spanning Tree Protocol is enabled for the port.



## UI Setting

## Description

### Edge

Shows whether the port is an edge port or not.

**Force Edge:** The port is fixed as an edge port and will always be in the forwarding state.

**True:** The port is currently designated as an edge port.

**False:** The port is not an edge port.

### Priority

Shows the priority of the port. Lower numbers indicate higher priority.

### Path Cost

Shows the path cost for the port. Higher path costs indicate that this port is less suitable as a node for the spanning tree topology.

If set to 0, the path cost will be automatically calculated based on different port speeds.

### Port State

Shows the current spanning tree status of the port.

**Forwarding:** Indicates the port is allowing transmissions normally.

**Blocking:** Indicates the port is blocking transmissions.

## Turbo Ring V2

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

This page includes these tabs:

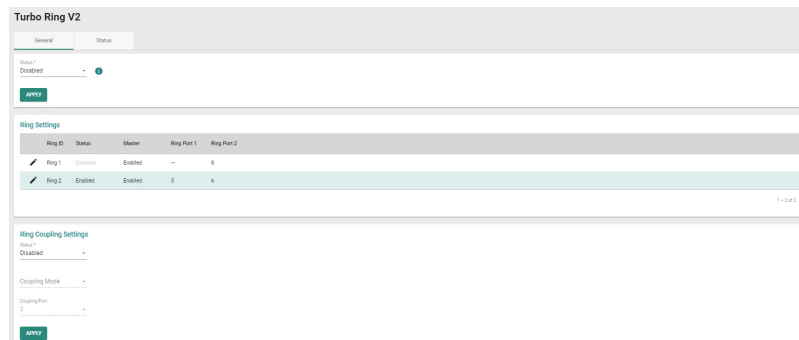
- General
- Status

## Turbo Ring V2 - General

**Menu Path:** [Redundancy](#) > [Layer 2 Redundancy](#) > [Turbo Ring V2 - General](#)

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

## Turbo Ring Settings



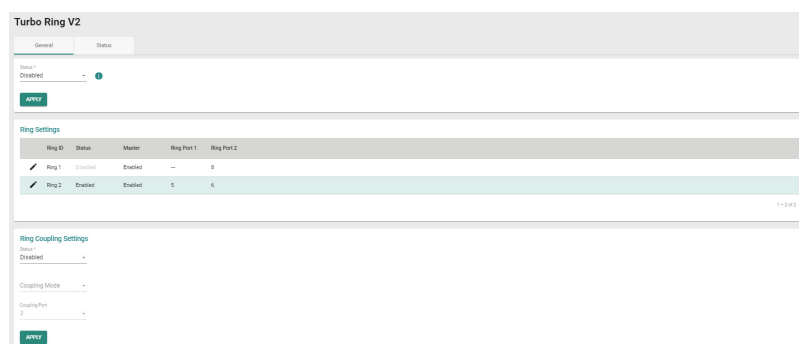
UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Status</b>	Enable or disable Turbo Ring V2 for the device.	Enabled / Disabled	Disabled
---------------	---	--------------------	----------

## Ring Settings

### Note

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



UI Setting	Description
------------	-------------

<b>Ring ID</b>	Shows the ring ID.
<b>Status</b>	Shows the status of the ring.
<b>Master</b>	Shows whether this device is designated as the master for the ring.
<b>Ring Port 1</b>	Shows which port will act as ring port 1. If this device is designated as the master for the ring, this will be the primary ring connection.
<b>Ring Port 2</b>	Shows which port will act as ring port 2. If this device is designated as the master for the ring, this will be the backup ring connection, and will be blocked normally.

## Turbo Ring V2 - Ring Settings

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

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

### Ring 1 Settings

Status \*  
Enabled ▾

Master \*  
Enabled ▾

Ring Port 1 \*  
3 ▾

Ring Port 2 \*  
8 ▾

CANCEL

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable Turbo Ring V2 for the device.	Enabled / Disabled	Disabled
<b>Master</b>	Enable or disable whether this device will be designated as the master for the ring.	Enabled / Disabled	Disabled
<b>Ring Port 1</b>	Specify which port will act as ring port 1. If this device is designated as the master for the ring, this will be the primary ring connection.	Select a port from the drop-down menu	7
<b>Ring Port 2</b>	Specify which port will act as ring port 2. If this device is designated as the master for the ring, this will be the backup ring connection, and will be blocked normally.	Select a port from the drop-down menu	8

## Ring Coupling Settings

### Ring Coupling Settings

Status \*

Enabled ▼

Coupling Mode \*

Dual Homing ▼

Primary Port \*

3 ▼

Backup Port \*

4 ▼

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable ring coupling for the device.	Enabled / Disabled	Disabled
<b>Coupling Mode</b> (if Status is Enabled)	Specify the coupling mode for the device. <b>Dual Homing:</b> This device will handle both the primary path and backup path for ring coupling. <b>Backup Path:</b> This device only handles the backup path for ring coupling; the primary path will be handled by another device. <b>Primary Path:</b> This device only handles the primary path for ring coupling; the backup path will be handled by another device.	Dual Homing / Backup Path / Primary Path	N/A
<b>Primary Port</b> (if Coupling Mode is Dual Homing)	Specify the port that connects to the primary path for ring coupling.	Select a port from the drop-down menu	3
<b>Backup Port</b> (if Coupling Mode is Dual Homing)	Specify the port that connects to the backup path for ring coupling.	Select a port from the drop-down menu	N/A
<b>Coupling Port</b> (if Coupling Mode is Primary Path or Backup Path)	Specify the port that connects to primary path or backup path for ring coupling.	Select a port from the drop-down menu	3

## Turbo Ring V2 - Status

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

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

### Ring Status

**Turbo Ring V2**

General | **Status**

**Ring Status**

Refresh Search

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

0 of 0

**Ring Coupling Status**

Refresh Search

Coupling Mode	Primary Port	Backup Port
---------------	--------------	-------------

0 of 0

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

## Ring Coupling Status

**Turbo Ring V2**

General | **Status**

**Ring Status**

🔄 Search

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

0 of 0

**Ring Coupling Status**

🔄 Search

Coupling Mode	Primary Port	Backup Port
---------------	--------------	-------------

0 of 0

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

## Turbo Chain

**Menu Path: Redundancy > Layer 2 Redundancy > Turbo Chain**

This page lets you configure Turbo Chain settings for redundancy.

This page includes these tabs:

- Settings
- Status

### Turbo Chain - Settings

**Menu Path: Redundancy > Layer 2 Redundancy > Turbo Chain - Settings**

This section lets you enable and configure Turbo Chain for your device.

Status \*  
Disabled ▼

---

Chain Role \*  
Member ▼

---

Member Port 1 \*  
G1 ▼

---

Member Port 2 \*  
G2 ▼

---

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Turbo Chain</b>	Enable or disable Turbo Chain.	Enabled / Disabled	Disabled
<b>Chain Role</b>	Select the chain role of the device.	Head / Member / Tail	Member
<b>Member Port 1</b>	Select which port will be Member Port 1.	Drop-down menu of ports	1/9
<b>Member Port 2</b>	Select which port will be Member Port 2.	Drop-down menu of ports	1/10

## Turbo Chain - Status

**Menu Path: Redundancy > Layer 2 Redundancy > Turbo Chain - Status**

This page lets you view the current status of Turbo Chain for your device.

**Chain Information** ↻

Status	Chain Role
<b>Disabled</b>	<b>Member</b>
Member 1 Port Status	Member 2 Port Status
<b>Disabled</b>	<b>Disabled</b>

UI Setting	Description
<b>Turbo Chain</b>	Shows the status of Turbo Chain.
<b>Chain Role</b>	Shows the chain role for your device.
<b>Member Port 1 Status</b>	Shows the status of Member Port 1.

UI Setting	Description
Member Port 2 Status	Shows the status of Member Port 2.

## Layer 3 Redundancy

### Menu Path: Redundancy > Layer 3 Redundancy

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

This section includes these pages:

- VRRP

## VRRP

### Menu Path: Redundancy > Layer 3 Redundancy > VRRP

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

This page includes these tabs:

- Settings
- Status

## VRRP - Settings

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

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

#### Note

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

#### Limitations

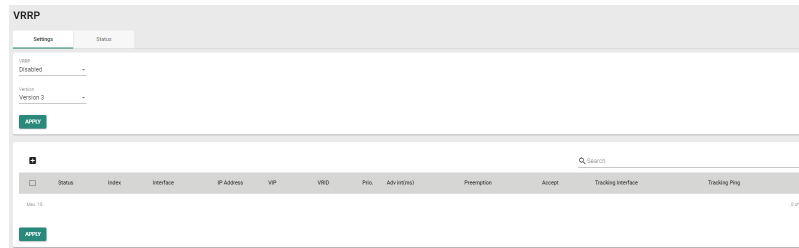
You can create up to 16 virtual routers.



## VRRP Settings

UI Setting	Description	Valid Range	Default Value
<b>VRRP</b>	Enable or disable VRRP for the device.	Enabled / Disabled	Disabled
<b>Version</b>	Select the VRRP version to use.	Version 2 / Version 3	Version 3
<b>Event</b>	Select the event for VRRP.	No Event / Link Status / DI Status	No Event
<b>On - VRRP Priority (If Event is Link Status or DI Status)</b>	Specify the VRRP Priority when the event is On.  <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p><b>Note</b></p> <p>If this is 0, the device will use the priority assigned to each VRRP interface.</p> </div>	0 to 254	0
<b>Off - VRRP Priority (If Event is Link Status or DI Status)</b>	Specify the VRRP Priority when the event is Off.  <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p><b>Note</b></p> <p>If this is 0, the device will use the priority assigned to each VRRP interface.</p> </div>	0 to 254	0
<b>Monitored Port (If Event is Link Status)</b>	Select the port to monitor.	Drop-down list of ports	1

## VRRP List



UI Setting	Description
<b>Status</b>	Shows the status of the VRRP interface.
<b>Index</b>	Shows the index number used to identify the VRRP interface.
<b>Interface</b>	Shows which network interface is used for the VRRP interface.
<b>IP Address</b>	Shows the IP address of the VRRP interface.
<b>VIP</b>	Shows the virtual router IP address for the VRRP interface.
<b>VRID</b>	Shows the virtual router ID for the VRRP interface, which is used to assign the virtual router to a VRRP group.
<b>Prio.</b>	Shows the priority of the VRRP interface. Higher numbers indicate higher priority, with 254 being the highest.
<b>Adv int(ms)</b>	Shows the advertisement interval for the VRRP interface in milliseconds.
<b>Preemption</b>	Shows the preemption status of the VRRP interface.
<b>Accept</b>	Shows whether Accept Mode is enabled for the VRRP interface. When enabled, the virtual router designated as the master will allow others to access its own virtual IP address.
<b>Tracking Interface</b>	Shows whether Native Interface Tracking is enabled for the VRRP interface.
<b>Tracking Ping</b>	Shows the tracking ping status of the VRRP interface.

## VRRP - Create Virtual Router

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

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

## 🔒 Limitations

You can create up to 16 virtual routers.

### Create Virtual Router

#### VRRP Interface Setting

Status

Disabled

Interface

WAN

Virtual IP \*

Virtual Router ID \*

Priority \*

1

100

1 - 255

1 - 254

Accept Mode

Enabled

Preemption

Enabled

Preempt Delay \*

120

0 - 300

sec.

Advertisement Interval \*

100

10 - 30000

millisec.

#### VRRP Tracking

Native Interface Tracking

Disabled

#### Object Ping Tracking

Target IP

Leave empty or set to 0.0.0.0 to disable

Interval \*

Timeout \*

1

3

1 - 100

sec.

1 - 100

sec.

Success Count \*

Failure Count \*

3

3




1 - 100

1 - 100

CANCEL

CREATE


## VRRP Interface Setting Entry

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the VRRP interface.	Enabled / Disabled	Disabled
<b>Interface</b>	Specify which network interface to use for the VRRP interface.	Drop-down list of interfaces	
<b>Virtual IP</b>	Specify the virtual router IP address for the VRRP interface.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b> Devices in the same VRRP group must be in the same subnet.</p> </div>	Valid IP address	N/A
<b>Virtual Router ID</b>	Specify the virtual router ID to use for the VRRP interface. The virtual router ID is used to assign the virtual router to a VRRP group.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b> Devices that operate as master/backup should have the same ID. Each interface supports one virtual router ID.</p> </div>	1-255	1
<b>Priority</b>	Specify the priority of the VRRP interface. Higher numbers indicate higher priority, with 254 being the highest.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b> If multiple devices have the same priority, the device with the highest IP address will have priority.</p> </div>	1-254	100
<b>Accept Mode</b>	Enable or disable Accept Mode for the VRRP interface. When enabled, the virtual router designated as the master will allow others to access its own virtual IP address.	Enabled / Disabled	Enabled
<b>Preemption</b>	Enable or disable preemption for the VRRP interface. When enabled, preemption will decide if the master will retake authority or not after being unavailable.	Enabled / Disabled	Enabled
<b>Preempt Delay (if Preemption is Enabled)</b>	Specify the preemption delay in seconds to use for the VRRP interface. The preempt delay is the amount of time the master will wait before retaking authority back in order to prevent the master from acting before the network connection is ready.	0-300 sec	120
<b>Advertisement Interval</b>	Specify the advertisement interval in milliseconds for the VRRP interface. This determines the interval for the master sending packets to all slave devices to inform them who the master device is.	10-30000 ms	100

## VRRP Tracking


### Note

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

UI Setting	Description	Valid Range	Default Value
<b>Native Tracking Interface</b>	Disable or specify which interface to use for Native Interface Tracking for the VRRP interface. When enabled, if all interfaces on the device are disconnected, it will be considered to be a disconnection.	Disabled / Drop-down list of interfaces	Disabled
<b>Target IP</b>	Specify the target IP to ping to verify if the connection to the destination is working. Leaving this field empty or entering 0.0.0.0 will disable object ping tracking for the VRRP interface.  <div data-bbox="389 819 1046 1003"><h3> Note</h3><p>Moxa devices will decide which interface/source IP to use for pinging the target IP based on the routing table.</p></div>	Valid IP address	N/A
<b>Interval</b>	Specify the interval in seconds the device will use for pinging the target IP.	1-100 sec	1
<b>Timeout</b>	Specify the timeout duration in seconds the device will wait for a response before timing out.	1-100 sec	3
<b>Success Count</b>	Specify the success count, which indicates how many responses the device must receive to consider the connection as working.	1-100	3
<b>Failure Count</b>	Specify the failure count, which indicates how many times the target IP fails to respond before the device considers the connection as not working.	1-100	3

## VRRP - Edit Virtual Router

### Menu Path: [Redundancy](#) > [Layer 3 Redundancy](#) > [VRRP - Settings](#)

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

## Edit Virtual Router

### VRRP Interface Setting

Status

Disabled

Interface

WAN

Virtual IP \*

1.1.1.1

Virtual Router ID \*

1

Priority \*

100

1 - 255

1 - 254

Accept Mode

Enabled

Preemption

Enabled

Preempt Delay \*

120

0 - 300 sec.

Advertisement Interval \*

100

10 - 30000 millisec.

### VRRP Tracking

Native Interface Tracking

Disabled

### Object Ping Tracking

Target IP

Leave empty or set to 0.0.0.0 to disable

Interval \*

1

1 - 100 sec.

Timeout \*

3

1 - 100 sec.

Success Count \*

3

1 - 100

Failure Count \*

3




1 - 100

CANCEL

APPLY

## VRRP Interface Setting Entry


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

UI Setting	Description	Valid Range	Default Value
<b>Virtual IP</b>	<p>Specify the virtual router IP address for the VRRP interface.</p> <p> <b>Note</b></p> <p>Devices in the same VRRP group must be in the same subnet.</p>	Valid IP address	N/A
<b>Virtual Router ID</b>	<p>Specify the virtual router ID to use for the VRRP interface. The virtual router ID is used to assign the virtual router to a VRRP group.</p> <p> <b>Note</b></p> <p>Devices that operate as master/backup should have the same ID. Each interface supports one virtual router ID.</p>	1-255	1
<b>Priority</b>	<p>Specify the priority of the VRRP interface. Higher numbers indicate higher priority, with 254 being the highest.</p> <p> <b>Note</b></p> <p>If multiple devices have the same priority, the device with the highest IP address will have priority.</p>	1-254	100
<b>Accept Mode</b>	<p>Enable or disable Accept Mode for the VRRP interface. When enabled, the virtual router designated as the master will allow others to access its own virtual IP address.</p>	Enabled / Disabled	Enabled
<b>Preemption</b>	<p>Enable or disable preemption for the VRRP interface. When enabled, preemption will decide if the master will retake authority or not after being unavailable.</p>	Enabled / Disabled	Enabled
<b>Preempt Delay (if Preemption is Enabled)</b>	<p>Specify the preemption delay in seconds to use for the VRRP interface. The preempt delay is the amount of time the master will wait before retaking authority back in order to prevent the master from acting before the network connection is ready.</p>	0-300 sec	120
<b>Advertisement Interval</b>	<p>Specify the advertisement interval in milliseconds for the VRRP interface. This determines the interval for the master sending packets to all slave devices to inform them who the master device is.</p>	10-30000 ms	100

## VRRP Tracking


### Note

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

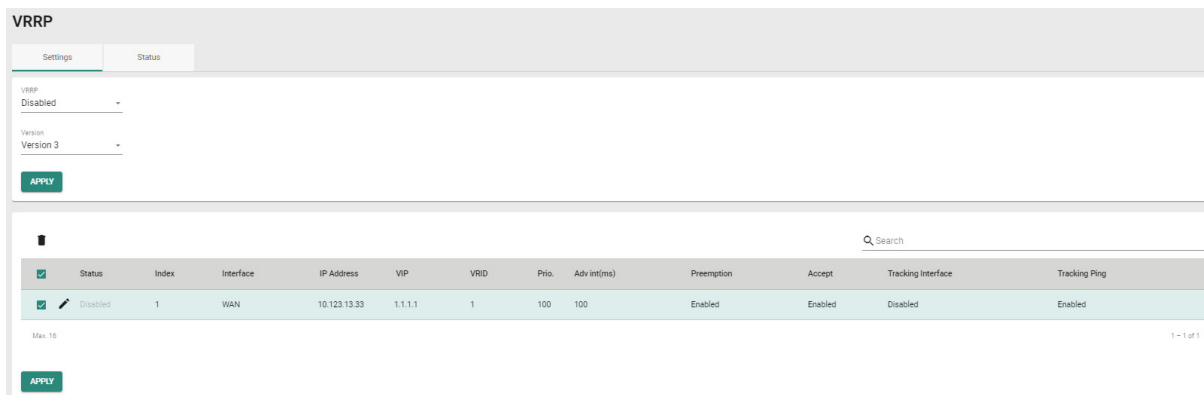
UI Setting	Description	Valid Range	Default Value
<b>Native Tracking Interface</b>	Disable or specify which interface to use for Native Interface Tracking for the VRRP interface. When enabled, if all interfaces on the device are disconnected, it will be considered to be a disconnection.	Disabled / Drop-down list of interfaces	Disabled
<b>Target IP</b>	Specify the target IP to ping to verify if the connection to the destination is working. Leaving this field empty or entering 0.0.0.0 will disable object ping tracking for the VRRP interface.  <div data-bbox="389 819 1046 1003"><h3> Note</h3><p>Moxa devices will decide which interface/source IP to use for pinging the target IP based on the routing table.</p></div>	Valid IP address	N/A
<b>Interval</b>	Specify the interval in seconds the device will use for pinging the target IP.	1-100 sec	1
<b>Timeout</b>	Specify the timeout duration in seconds the device will wait for a response before timing out.	1-100 sec	3
<b>Success Count</b>	Specify the success count, which indicates how many responses the device must receive to consider the connection as working.	1-100	3
<b>Failure Count</b>	Specify the failure count, which indicates how many times the target IP fails to respond before the device considers the connection as not working.	1-100	3

## Delete Virtual Router

### Menu Path: [Redundancy](#) > [Layer 3 Redundancy](#) > [VRRP - Settings](#)

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

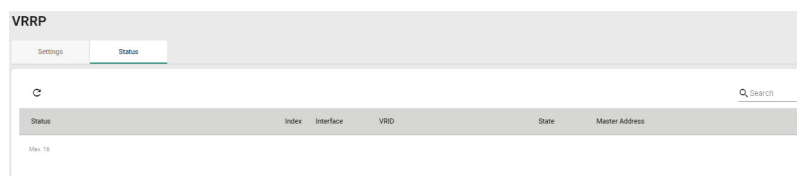




## VRRP - Status

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

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



UI Setting	Description
------------	-------------

<b>Status</b>	Shows the status of the VRRP interface.
---------------	---

<b>Index</b>	Shows the index number used to identify the VRRP interface.
--------------	---

<b>Interface</b>	Shows which network interface is used for the VRRP interface.
------------------	---

<b>VRID</b>	Shows the virtual router ID for the VRRP interface, which is used to assign the virtual router to a VRRP group.
-------------	---

<b>State</b>	Shows the state of the VRRP interface.
--------------	--

**Init State:** This is the initial state when a virtual router starts up.

**Master State:** The virtual router is acting as a master, and is responsible for forwarding packets sent to the virtual IP address and acting as the default gateway for the devices in the network.

**Backup State:** The virtual router is in the backup state, and waiting to take over the master role if the current master fails.

<b>Master Address</b>	Shows IP address of the current master for the VRRP interface.
-----------------------	--

## WAN Redundancy

### Menu Path: Redundancy > WAN Redundancy

This section lets you configure the WAN Redundancy features of your device.

This page includes these tabs:

- Settings
- Status

#### Note

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

## WAN Redundancy - Settings

### Menu Path: Redundancy > Layer 3 Redundancy > WAN Redundancy - Settings

This page lets you configure the WAN Redundancy settings for your device.

### WAN Redundancy

Settings Status

WAN Redundancy Mode \*  
Disabled

WAN Switching Mode \*  
Failback

Ping Check  
Disabled

Ping Interval \*  
5  
1 - 3600 sec.



Ping Success Retry Times \*  
3  
1 - 10 times

Ping Failure Retry Times \*  
3  
1 - 10 times

Ping Timeout \*  
5  
1 - 10 sec.

**APPLY**

#### WAN Backup Priority

Priority	Interface	WAN Redundancy	Host IP Address
 1	Ethernet WAN 1	Enabled	0.0.0.0
 2	Ethernet WAN 2	Disabled	0.0.0.0

WAN Redundancy Mode \*  
Disabled

WAN Switching Mode \*  
Failback

Ping Check  
Disabled

Ping Interval \* 5  
1 - 3600 sec.

Ping Success Retry Times \* 3  
1 - 10 times

Ping Failure Retry Times \* 3  
1 - 10 times

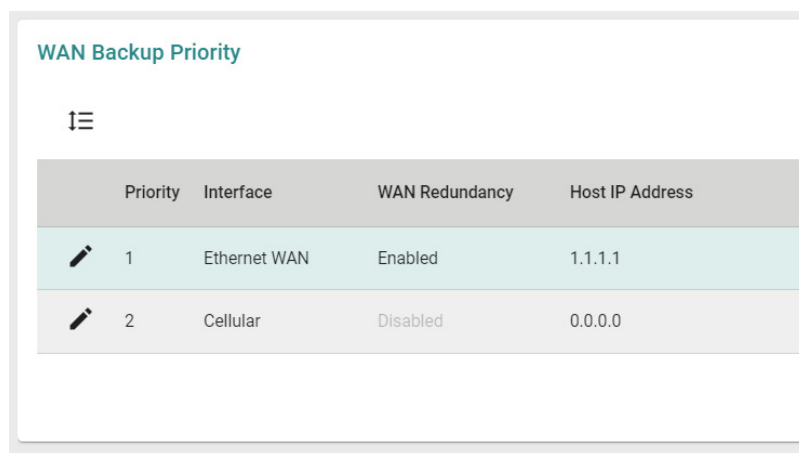
Ping Timeout \* 5  
1 - 10 sec.

APPLY

UI Setting	Description	Valid Range	Default Value
<b>WAN Redundancy Mode</b>	<p>Select the WAN Redundancy Mode.</p> <p><b>Disabled:</b> Disable redundancy. If the connection on the WAN interface becomes unavailable, the connection will be lost.</p> <p><b>Backup:</b> If the connection on the active WAN interface becomes unavailable, the system will automatically switch to the other WAN interface to recover the connection.</p>	Disabled / Backup	Disabled
<b>WAN Switching Mode</b>	<p>Select the WAN Switching Mode.</p> <p><b>Failover:</b> The system will only switch to the backup WAN interface when the current WAN interface becomes unavailable.</p> <p><b>Failback:</b> The system will switch to the backup WAN interface when the current WAN interface becomes unavailable. When the original higher priority WAN interface recovers, the system will switch back.</p>	Failover / Failback	Failback
<b>Ping Check</b>	Enable or disable ping checks to determine whether a connection is still alive.	Enabled/Disabled	Disabled
<b>Ping Interval</b>	Specify the interval in seconds at which the device will perform a connection alive check.	1 to 3600	5
<b>Ping Failure Retry Times</b>	Specify the number of times the device will ping the configured host IP through the active WAN interface. If the ping check consecutively fails for the specified number of retries, the device will consider the WAN interface unavailable and will switch to the backup WAN interface. The host IP is configured per WAN interface.	1 to 10	3
<b>Ping Success Retry Times</b>	Specify the number of times the device will ping the configured host IP through the higher priority WAN interface in Failback mode. If the ping check consecutively succeeds for the specified number of retries, the device will consider the WAN interface recovered and will switch back to that WAN interface. The host IP is configured per WAN interface.	1 to 10	3

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Ping Timeout</b>	Specify the timeout duration in seconds the device will wait for a response before timing out.	1 to 10	5
---------------------	--	---------	---



UI Setting	Description
------------	-------------

<b>Priority</b>	Shows the WAN Backup Priority.
<b>Interface</b>	Shows the interface of WAN Backup Priority.
<b>WAN Redundancy</b>	Shows the status of WAN Redundancy.
<b>Host IP Address</b>	Shows the Host IP Address.

## WAN Redundancy - Edit WAN Backup Priority

**Menu Path:** [Redundancy](#) > [WAN Redundancy](#) > [Settings](#)

Clicking the **Edit** (✎) icon for an entry on the **Redundancy > WAN Redundancy > Settings** page will open this dialog box. This dialog lets you edit the WAN Redundancy settings for an interface. Click **APPLY** to save your changes.

## Edit Cellular Interface Settings

WAN Redundancy \*

Disabled i

Host IP Address

0.0.0.0

CANCEL

APPLY

UI Setting	Description	Valid Range	Default Value
<b>WAN Redundancy</b>	Enable or disable using WAN Redundancy for the interface.	Enabled / Disabled	Disabled
<b>Host IP Address</b>	Specify the IP address for performing the connection alive check.	Valid IP address	0.0.0.0

## WAN Redundancy - Status

**Menu Path:** [Redundancy](#) > [Layer 3 Redundancy](#) > [WAN Redundancy - Status](#)

This page lets you see the status of your device's WAN Redundancy.

### WAN Redundancy

Settings | **Status**

Priority	Interface	WAN Redundancy
● 1	Ethernet WAN	Enabled
● 2	Cellular (Disabled)	Disabled

UI Setting	Description
<b>Light</b>	Green: the WAN interface is in use. Gray: the WAN interface is not in use.
<b>Priority</b>	Shows the priority of WAN Redundancy.
<b>Interface</b>	Shows the interface for WAN Redundancy.
<b>WAN Redundancy</b>	Shows the status of WAN Redundancy.

## 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
<b>DHCP Server</b>	R/W	R/W	R
<b>Dynamic DNS</b>	R/W	R/W	R
<b>DNS Server</b>	R/W	R/W	R

## DHCP Server

### Menu Path: Network Service > DHCP Server

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

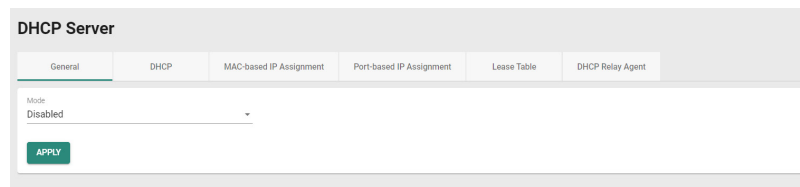
This page includes these tabs:

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

## DHCP Server - General

### Menu Path: Network Service > DHCP 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
<b>Mode</b>	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.

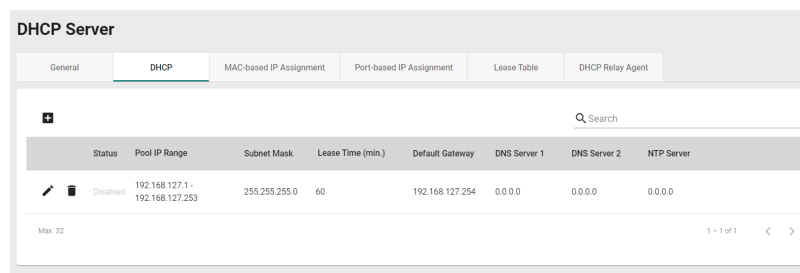
### **Note**



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



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

### UI Setting

### Description

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

## DHCP - Create DHCP Server Pool

**Menu Path:** [Network Service](#) > [DHCP Server - DHCP](#)



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

### Create DHCP Server Pool

Status \*  
 Enabled ▾

Starting IP Address \*      Subnet Mask \* ▾

Ending IP Address \*

Default Gateway

Lease Time \*  
 1440  
 5 - 527039 min.

DNS Server 1      DNS Server 2

NTP Server

CANCEL

CREATE

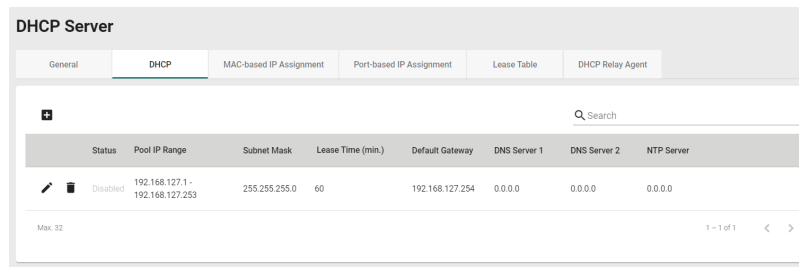
UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable DHCP server functionality.	Enabled / Disabled	N/A
<b>Starting IP Address</b>	Specify the starting IP address of the DHCP IP pool.	Valid IP address	N/A
<b>Subnet Mask</b>	Specify the subnet mask for DHCP clients in the pool.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

UI Setting	Description	Valid Range	Default Value
<b>Default Gateway</b>	Specify the default gateway to use for DHCP clients in the pool.	Valid IP address	N/A
<b>Lease Time</b>	Specify the lease time to use for IP addresses assigned to DHCP clients in the pool.	5 - 527039 minutes	1440
<b>DNS Server 1</b>	Specify the IP address to use for the first DNS server for DHCP clients in the pool.	Valid IP address	N/A
<b>DNS Server 2</b>	Specify the IP address to use for the second DNS server for DHCP clients in the pool.	Valid IP address	N/A
<b>NTP Server</b>	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							
General	DHCP	MAC-based IP Assignment	Port-based IP Assignment	Lease Table	DHCP Relay Agent		
Status	Pool IP Range	Subnet Mask	Lease Time (min.)	Default Gateway	DNS Server 1	DNS Server 2	NTP Server
Disabled	192.168.127.1 - 192.168.127.253	255.255.255.0	60	192.168.127.254	0.0.0.0	0.0.0.0	0.0.0.0

## 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.

DHCP Server									
General	DHCP	MAC-based IP Assignment	Port-based IP Assignment	Lease Table	DHCP Relay Agent				
Status	Name	IP Address	Subnet Mask	MAC Address	Lease Time (min.)	Default Gateway	DNS Server 1	DNS Server 2	
<input type="checkbox"/>	Disabled	UserManualCASEtest	192.168.127.101	255.255.255.0	00:09:ad:00:aa:01	1440	0.0.0.0	0.0.0.0	0.0.0.0

### UI Setting

### Description

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

## Create Entry

Status

Name \*  0 / 63

IP Address \*  Subnet Mask \*

MAC Address \*

Default Gateway

Lease Time \*  1440  
5 - 99999 min.

DNS Server 1  DNS Server 2

NTP Server

CANCEL

CREATE

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

UI Setting	Description	Valid Range	Default Value
<b>Default Gateway</b>	Specify the default gateway for the IP assignment.	Valid IP address	N/A
<b>Lease Time</b>	Specify the lease time for for the IP assignment.	5 - 99999 minutes	1440
<b>DNS Server 1</b>	Specify the primary DNS server for the IP assignment.	Valid IP address	N/A
<b>DNS Server 2</b>	Specify the secondary DNS server for the IP assignment.	Valid IP address	N/A
<b>NTP Server</b>	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.

### Edit Entry Settings

Status  
 Disabled ▼

Name \*  
 ExistingAssignment  
 18 / 63

IP Address \*      Subnet Mask \*  
 192.168.127.101      24 (255.255.255.0) ▼

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

Default Gateway  
 0.0.0.0

Lease Time \*  
 1440  
 5 - 527039 min.

DNS Server 1      DNS Server 2  
 0.0.0.0      0.0.0.0

NTP Server  
 0.0.0.0


CANCEL      APPLY

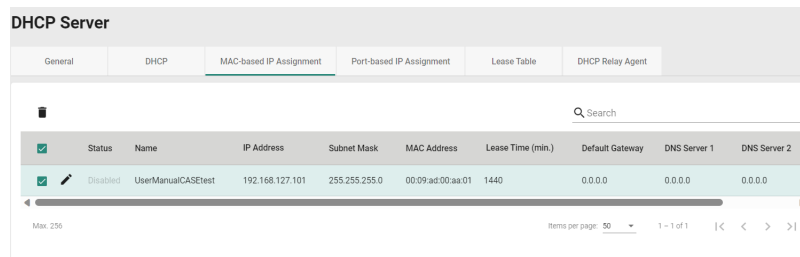
UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable this MAC-based IP assignment.	Enabled / Disabled	N/A
<b>Name</b>	Enter a hostname for the IP assignment.	Max. 63 characters	N/A
<b>IP Address</b>	Specify the IP address for the IP assignment.	Valid IP address	N/A
<b>Subnet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

UI Setting	Description	Valid Range	Default Value
<b>MAC Address</b>	Specify the MAC address that this IP assignment will apply to.	Valid MAC address	N/A
<b>Default Gateway</b>	Specify the default gateway for the IP assignment.	Valid IP address	N/A
<b>Lease Time</b>	Specify the lease time for for the IP assignment.	5 - 99999 minutes	1440
<b>DNS Server 1</b>	Specify the primary DNS server for the IP assignment.	Valid IP address	N/A
<b>DNS Server 2</b>	Specify the secondary DNS server for the IP assignment.	Valid IP address	N/A
<b>NTP Server</b>	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											
General		DHCP		MAC-based IP Assignment		Port-based IP Assignment		Lease Table		DHCP Relay Agent	
<input checked="" type="checkbox"/>	Status	Name	IP Address	Subnet Mask	MAC Address	Lease Time (min.)	Default Gateway	DNS Server 1	DNS Server 2		
<input checked="" type="checkbox"/>	Disabled	UserManualCASEtest	192.168.127.101	255.255.255.0	00:09:ad:00:aa:01	1440	0.0.0.0	0.0.0.0	0.0.0.0		

## DHCP Server - Port-based IP Assignment

**Menu Path:** [Network Service](#) > [DHCP Server - Port-based IP Assignment](#)

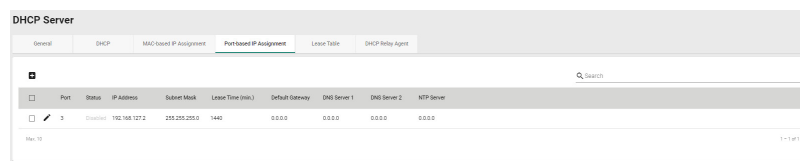
This page lets you manage port-based IP assignment for your device's DHCP server.

### **Note**

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

### **Limitations**


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



DHCP Server											
General		DHCP		MAC-based IP Assignment		Port-based IP Assignment		Lease Table		DHCP Relay Agent	
Port	Status	IP Address	Subnet Mask	Lease Time (min)	Default Gateway	DNS Server 1	DNS Server 2	NTP Server			
1	Enabled	192.168.121.2	255.255.255.0	1440	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0			

## Create Port-based IP Assignment

**Menu Path:** [Network Service > DHCP Server - Port-based IP Assignment](#)

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



## Create Entry

Status

Port \*

IP Address \*  Subnet Mask \*

Default Gateway

Lease Time \*  
1440  
5 - 99999 min.

DNS Server 1  DNS Server 2

NTP Server

CANCEL

CREATE

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

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

## Edit Port-based IP Assignment

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

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

### Edit Entry Settings

Status  
Disabled ▾

Port \*  
1/3 ▾

IP Address \*  
192.168.127.2

Subnet Mask \*  
24 (255.255.255.0) ▾

Default Gateway  
0.0.0.0

Lease Time \*  
1440  
5 - 527039 min.

DNS Server 1  
0.0.0.0

DNS Server 2  
0.0.0.0


NTP Server  
0.0.0.0

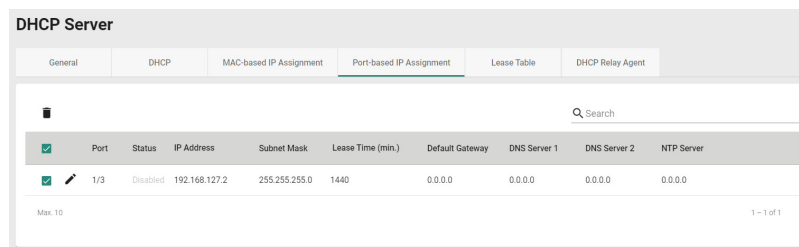
CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable this port-based IP assignment.	Enabled / Disabled	N/A
<b>Port</b>	Select the physical port on the device to associate the IP with for this entry.	Drop-down list of ports	N/A
<b>IP Address</b>	Specify the IP address of the connected device for this entry.	Valid IP address	N/A
<b>Subnet Mask</b>	Specify the subnet mask of the connected device for this entry.	Valid subnet mask	N/A
<b>Default Gateway</b>	Specify the default gateway of the connected device for this entry.	Valid IP address	N/A
<b>Lease Time</b>	Specify the lease time for IP addresses assigned by the DHCP server for this entry.	5 - 99999 minutes	1440
<b>DNS Server 1</b>	Specify the IP address for the first DNS server for DHCP clients for this entry.	Valid IP address	N/A
<b>DNS Server 2</b>	Specify the IP address for the second DNS server for DHCP clients for this entry.	Valid IP address	N/A
<b>NTP Server</b>	Specify the IP address for the NTP server for DHCP clients for this entry.	Valid IP address	N/A

## Delete Port-based IP Assignment

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

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

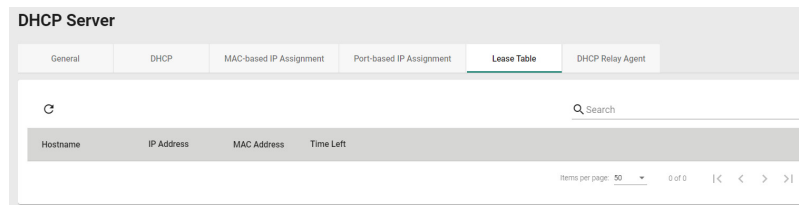


## DHCP Server - Lease Table

**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
<b>Hostname</b>	Shows the hostname of the DHCP lease.
<b>IP Address</b>	Shows the IP address of the DHCP lease.
<b>MAC Address</b>	Shows the MAC address of the DHCP lease.
<b>Time Left</b>	Shows the time left for the DHCP lease.

## DHCP Relay Agent

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

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

## DHCP Relay Agent Settings

**DHCP Server**

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

---

**Server IP Address**

Interface ▼

DHCP Relay Server-1 \*  
0.0.0.0

DHCP Relay Server-2 \*  
0.0.0.0

DHCP Relay Server-3 \*  
0.0.0.0

DHCP Relay Server-4 \*  
0.0.0.0

**DHCP Option 82**

Enable Option 82 \*   Type \*   Interface \*

Enabled   Interface   LAN

Value: 192.168.127.254   Display: c0a87ffe

15 / 32

**APPLY**

### Server IP Address

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

### DHCP Option 82

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

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

## DHCP Function Table

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

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

## Dynamic DNS

**Menu Path:** Network Service > Dynamic DNS


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


### Dynamic DNS

Service \*  
Disabled ▾

Service Name  
.....

Username  
.....  
0 / 45

Password   
.....  
0 / 45

Confirm Password   
.....  
0 / 45

Domain Name  
.....  
0 / 45

**APPLY**

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

## DNS Server

### Menu Path: Network Service > DNS Server

This page lets you configure the DNS server settings.

This page includes these tabs:

- Global
- Settings
- Status

#### Note

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

## DNS Server - Global

### Menu Path: Network Service > DNS Server - Global

This page lets you configure the DNS server related settings. Click **APPLY** to save your changes.



## DNS Server Settings

### DNS Server

Global
Settings
Status

DNS Server \*

Disabled ▼

---

DNS Reverse Lookup \*

Disabled ▼

---

APPLY

UI Setting	Description	Valid Range	Default Value
<b>DNS Server</b>	Enable or disable the DNS server for your device.	Enabled / Disabled	Disabled
<b>DNS Reverse Lookup</b>	Enable or disable DNS reverse lookup for your device. DNS reverse lookup allows the router to identify the hostname (device name) associated with a known IP address on the network.	Enabled / Disabled	Disabled

### DNS Server - Settings

**Menu Path:** [Network Service](#) > [DNS Server - Settings](#)

This page lets you configure the DNS server zone settings.

#### **ⓘ Limitations**

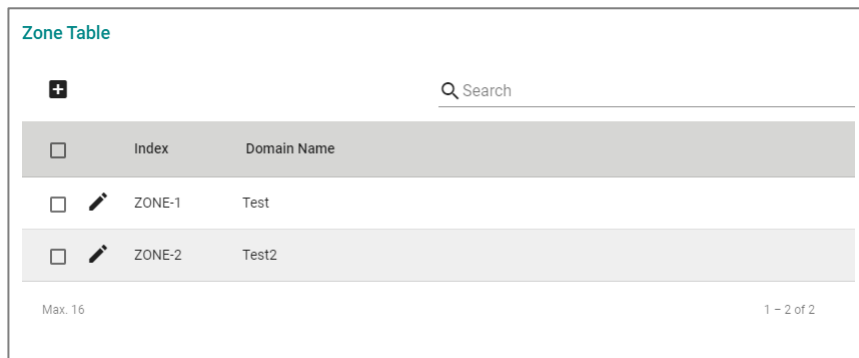
Up to 16 DNS zones can be created.

### 🔒 Limitations

Up to 256 resource records can be created for each zone.

## Zone Table

Zones provide a structured way to manage and organize DNS records for a domain. They allow administrators to group related records together and apply consistent configurations across the domain.



The screenshot shows a web interface titled "Zone Table". It features a search bar with a magnifying glass icon and the text "Search". Below the search bar is a table with the following structure:

<input type="checkbox"/>	Index	Domain Name
<input type="checkbox"/>	ZONE-1	Test
<input type="checkbox"/>	ZONE-2	Test2

At the bottom left of the table area, it says "Max. 16". At the bottom right, it says "1 - 2 of 2".

### UI Setting

### Description

#### Index

Shows the number of the zone the entry is for.

#### Domain Name

Shows the domain name of the zone.

## Create a Zone

### Menu Path: [Network Service > DNS Server - Settings](#)

Clicking the **Add (🔑)** icon on the **Network Service > DNS Server - Settings** page will open this dialog box. This dialog lets you create a zone for the DNS server.

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

### Create a Zone

Index \*  
ZONE-1 ▼

Domain Name \*  
Test  
4 / 63

CANCEL
CREATE

UI Setting	Description	Valid Range	Default Value
<b>Index</b>	Select a zone to create.	Drop-down list of zones	N/A
<b>Domain Name</b>	Specify a domain name for the zone.	Up to 63 characters	N/A

## DNS Table

Select a zone from the drop-down list to see its DNS table.

DNS Table for ZONE-1 ▼

+
Search

	Hostname	IP Address
<input type="checkbox"/>	Test	19.126.255.5

1 - 1 of 1

UI Setting	Description
<b>Hostname</b>	Shows the hostname of the resource record.
<b>IP Address</b>	Shows the IP address of the resource record.

## Create a Resource Record

**Menu Path:** [Network Service](#) > [DNS Server - Settings](#)

Clicking the **Add (+)** icon in a DNS table on the **Network Service > DNS Server - Settings** page will open this dialog box. This dialog lets you create resource records for the displayed zone.

Click **CREATE** to save your changes and add the resource record for the displayed zone.

**Note**

Resource records cannot be created for a zone until the corresponding zone has been created.

UI Setting	Description	Valid Range	Default Value
<b>Hostname</b>	Specify the host name for the resource record.	1 to 63 characters	N/A
<b>IP Address</b>	Specify the IP address for the resource record.	Valid IP address	N/A

## DNS Server - Status

**Menu Path:** [Network Service > DNS Server - Status](#)

This page lets you see the DNS server's overall status.

## DNS Server Summary

UI Setting	Description
------------	-------------

- DNS Server** Shows whether the DNS server is enabled for the device.
- DNS Reverse Lookup** Shows whether DNS reverse lookup is enabled for the device

### Status - Zone Table

Index	Domain Name
ZONE-1	Test
ZONE-2	Test2

1 - 2 of 2

UI Setting	Description
------------	-------------

- Index** Shows the index of the zone the entry is for.
- Domain Name** Shows the domain name of the zone.

### Status - DNS Table

FQDN ↓	IP Address
Test.Test	19.126.255.5

1 - 1 of 1

UI Setting	Description
------------	-------------

- FQDN** Shows the full qualified domain name (FQDN) of the resource record, which is in the format "Hostname.Domain Name".  
For example, if the hostname is "door1" and the domain name for the zone is "train1", the FQDN will be "door1.train1".

UI Setting	Description
------------	-------------

<b>IP Address</b>	Shows the IP address of the resource record.
-------------------	--

## Routing

### Menu Path: Routing

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

This settings area includes these sections:

- Unicast Route
- Multicast Route
- Broadcast Forwarding

### Routing - User Privileges

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

Settings	Admin	Supervisor	User
<b>Unicast Routing</b>			
<b>Static Routes</b>	R/W	R/W	R
<b>RIP</b>	R/W	R/W	R
<b>OSPF</b>	R/W	R/W	R
<b>Routing Table</b>	R	R	R
<b>Multicast Route</b>			
<b>Multicast Route Settings</b>	R/W	R/W	R
<b>Static Multicast Route</b>	R/W	R/W	R

Settings	Admin	Supervisor	User
<b>Multicast Forwarding Table</b>	R	R	R
<b>Broadcast Forwarding</b>	R/W	R/W	R

## Unicast Route

### Menu Path: [Routing](#) > [Unicast Route](#)

This section lets you manage unicast routes for your device.

This section includes these pages:

- [Static Routes](#)
- [RIP](#)
- [OSPF](#)
- [Routing Table](#)

## Static Routes

### Menu Path: [Routing](#) > [Unicast Route](#) > [Static Routes](#)

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

#### Limitations

You can create up to 512 static routes.


## Static Route List

Static Routes						
<input type="checkbox"/>	Status	Name	Destination Address	Netmask	Next Hop	Metric
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>Max. 512</span> <span>Items per page: <b>50</b> 0 of 0  &lt; &lt; &gt; &gt; </span> </div>						

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

## Create New Static Route

### Menu Path: [Routing](#) > [Unicast Route](#) > [Static Routes](#)

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

#### Create new static route

Status \*

Name \*  0 / 10

Destination Address \*  Subnet Mask \*

Next Hop \*  Metric \*  1 - 254

CANCEL

CREATE



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

The screenshot shows the 'Static Routes' configuration page. At the top left, there is a trash can icon for deleting routes. Below it is a table with the following columns: Status, Name, Destination Address, Netmask, Next Hop, and Metric. One entry is visible with the following details:

Status	Name	Destination Address	Netmask	Next Hop	Metric
<input checked="" type="checkbox"/> Disabled	test	192.168.122.1	255.255.255.0	192.168.122.2	1

Below the table, there is a note: 'Max. 512'.

## RIP

### Menu Path: [Routing](#) > [Unicast Route](#) > [RIP](#)

This page lets you configure RIP (Routing Information Protocol), a distance-vector routing protocol that employs the hop count as a routing metric. RIP prevents routing

from looping by implementing a limit on the number of hops allowed in a path from the source to a destination. Click **APPLY** to save your changes.

## RIP Settings

**RIP**

Status: Disabled

Version: V2

Redistribute:

**APPLY**

---

**C** Search

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

Max 16 Items per page: 50 1 - 3 of 3

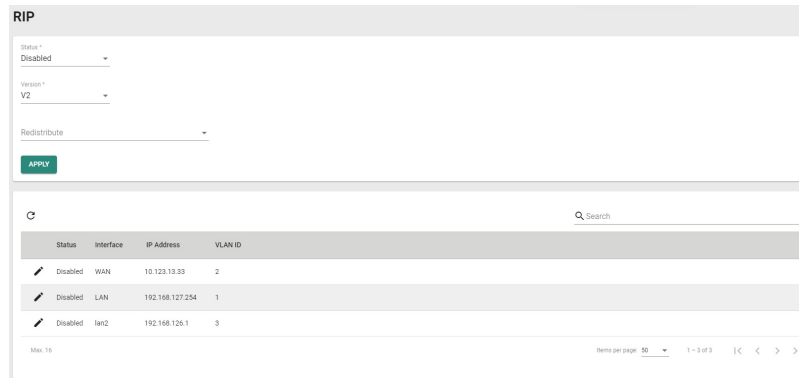
UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable RIP protocol.	Enabled / Disabled	Disabled
<b>Version</b>	Set the RIP protocol version: <b>V1:</b> RIP V1 uses classful routing. This means that network addresses are assigned to specific classes, and the subnet mask is determined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

## RIP Interface List

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

### **Note**

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



### UI Setting

### Description

#### **Status**

Shows whether RIP is enabled or disabled for the interface.

#### **Interface (View Only)**

Shows the name of the interface.

#### **IP Address (View Only)**


Shows the IP address of the interface.

#### **VLAN ID (View Only)**

Shows the VLAN ID of the interface.

### **Edit RIP**

#### **Menu Path: Routing > Unicast Route > RIP**

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

## Edit RIP

Status \*  
Disabled ▾

Interface  
WAN

IP Address  
10.123.13.33

VLAN ID  
2

CANCEL

APPLY

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

## OSPF

### Menu Path: [Routing](#) > [Unicast Route](#) > [OSPF](#)

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

This section includes these pages:

- [OSPF Settings](#)
- [OSPF Status](#)

## OSPF Settings

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

This page lets you configure OSPF settings for your device.

This page includes these tabs:

- General
- Area
- Interface
- Aggregation
- Virtual Link

### OSPF Settings - General

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

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

OSPF Settings

General Area Interface Aggregation Virtual Link

OSPF Settings \*  
Disabled

Router ID \*  
0.0.0.0

Current Router ID  
0.0.0.0



Redistribute

APPLY

UI Setting	Description	Valid Range	Default Value
<b>OSPF Settings</b>	Enable or disable OSPF for your device.	Enabled / Disabled	Disabled
<b>Router ID</b>	Specify the Router ID of your Moxa router.	Router ID	0.0.0.0

**Note**

The router ID, which must be established for every OSPF instance, should be written in the dot-decimal format of an IP address (e.g., 1.2.3.4) and does not need to be part of any routable subnet on the network, since it is an IP address.

UI Setting	Description	Valid Range	Default Value
<b>Current Router ID</b> (View-only)	Specify the current Router ID of your Moxa router.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b></p> <p>When the Router ID is set to 0.0.0.0, the Current Router ID will automatically use the highest interface IP address.</p> </div>	Current Router ID	0.0.0.0
<b>Redistribute</b>	Specify the OSPF redistribution method:  <b>Connected:</b> Entries learned from the directly connected interfaces will be redistributed.  <b>Static:</b> Entries set in a static route will be redistributed.  <b>RIP:</b> Entries learned from RIP will be redistributed.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b></p> <p><i>Redistributing</i> in OSPF refers to the process of importing routing information from other routing protocols—such as RIP, EIGRP, etc.—into the OSPF routing table.</p> </div>	Connected / Static / RIP	N/A

## OSPF Settings - Area

**Menu Path:** [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings - Area](#)

This page lets you define OSPF areas.

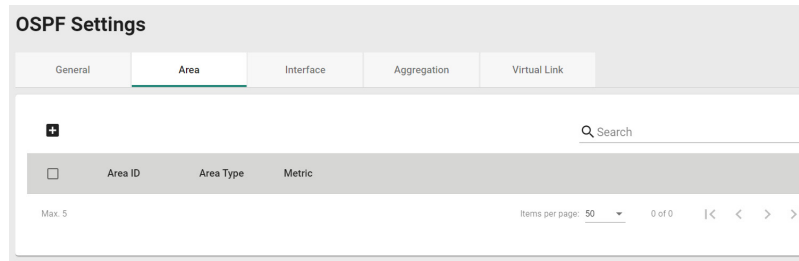
### Note

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

### Limitations

You can create up to 5 OSPF areas.

## OSPF Area List



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

## Create Area

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

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

### Create Area

Area ID \*

---

Area Type \*

Normal ▼

CANCEL

CREATE

UI Setting	Description	Valid Range	Default Value
<b>Area ID</b>	Specify an ID for this OSPF area.	N/A	N/A

UI Setting	Description	Valid Range	Default Value
<b>Area Type</b>	<p>Specify the type of OSPF routing to use for this area:</p> <p><b>Normal:</b> A normal (or standard) area is an OSPF area that allows both intra-area and inter-area routing.</p> <p><b>Stub:</b> A stub area is an OSPF area that does not allow external routes to be imported into the area.</p> <p><b>NSSA:</b> An NSSA (Not-So-Stubby Area) is a special type of OSPF area that allows external routing information to be imported into the area, but does not allow the area to propagate that information to other areas.</p>	Normal / Stub / NSSA	Normal
<b>Metric (if Metric is Stub or NSSA)</b>	<p>Specify the metric value/cost to use for this area.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>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.</p> </div>	1 to 65535	1

## Edit Area

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

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

### Edit Area

Area ID \*  
0.0.0.0

---

Area Type \*  
Normal ▼

---

CANCEL
APPLY

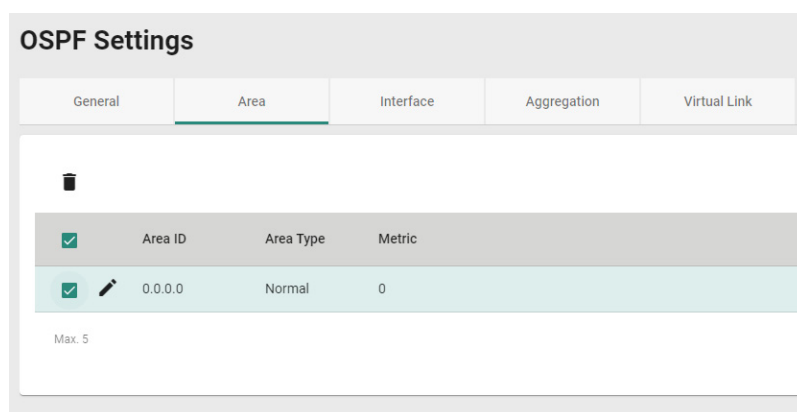


UI Setting	Description	Valid Range	Default Value
<b>Area ID</b>	Specify an ID for this OSPF area.	N/A	N/A
<b>Area Type</b>	Specify the type of OSPF routing to use for this area: <b>Normal:</b> A normal (or standard) area is an OSPF area that allows both intra-area and inter-area routing. <b>Stub:</b> A stub area is an OSPF area that does not allow external routes to be imported into the area. <b>NSSA:</b> An NSSA (Not-So-Stubby Area) is a special type of OSPF area that allows external routing information to be imported into the area, but does not allow the area to propagate that information to other areas.	Normal / Stub / NSSA	Normal
<b>Metric (if Metric is Stub or NSSA)</b>	Specify the metric value/cost to use for this area.	1 to 65535	1
<p><b>Note</b></p> <p>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.</p>			

## Delete Area

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

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



## OSPF Settings - Interface

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

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

OSPF Settings										
General		Area		Interface		Aggregation		Virtual Link		
Interface	IP Address	Area ID	Hello Interval (sec.)	Dead Interval (sec.)	Role	Priority	Auth Type	MD5 Key ID	Metric	
<input type="checkbox"/> WAN	10.123.13.33	0.0.0.0	10	40	DR	1	MD5	12	1	

UI Setting	Description
<b>Interface</b>	Shows which interface this entry describes.
<b>IP Address</b>	Shows the IP address of the interface.
<b>Area ID</b>	Shows the OSPF area ID used for the interface.
<b>Hello Interval</b>	Shows the hello message interval for the interface.
<b>Dead Interval</b>	Shows the dead interval for the interface.
<b>Role</b>	Shows the role of the interface.
<b>Priority</b>	Shows the priority of the interface.
<b>Auth Type</b>	Shows the authentication type used to authenticate OSPF neighbors.
<b>MD5 Key ID</b> <b>(Only if Auth Type is MD5)</b>	Shows the MD5 key ID used to authenticate OSPF neighbors.
<b>Metric</b>	Shows the metric value/cost to OSPF.

**Note**  
Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.

## OSPF Settings - Create Interface

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

Clicking the **Add (+)** icon on the **Insert > Path Here** page will open this dialog box. This dialog lets you select an interface and configure OSPF settings for it. Click **CREATE** to save your changes and add the new entry.

**Note**

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

### Create Interface

Interface \*

Area ID \*

Priority \*  
1  
0 - 255

Hello Interval \*  Dead Interval \*   
10 40  
1 - 65535 sec. 1 - 65535 sec.

Auth Type \*  
None

Metric \*  
1  
1 - 65535



CANCEL

CREATE

UI Setting	Description	Valid Range	Default Value
<b>Interface</b>	Specify which interface to assign to an OSPF area.	Dropdown of interfaces	N/A
<b>Area ID</b>	Specify an OSPF area ID to assign to the interface.	Dropdown of area IDs	N/A

**Note**

To manage OSPF areas, refer to Routing > Unicast Route > OSPF > OSPF Settings - Area.

UI Setting	Description	Valid Range	Default Value
<b>Priority</b>	Specify the priority of the interface.	0 to 255	1
<b>Hello Interval</b>	Set the hello message interval for the interface. The hello interval is the amount of time between sends of hello packets, which indicate that the device is still alive. The value of all hello intervals must be the same within a network.	1 to 65535 second(s)	10
<b>Dead Interval</b>	Set the dead interval for the interface. The dead interval is the amount of time a device will wait for a hello packet. If a hello packet is not received in this time, it will consider the other device to be dead or unavailable. By default, the dead interval is set to be four times the value of the hello interval.	1 to 65535 second(s)	40
<b>Auth Type</b>	Specify the authentication type to use when authenticating OSPF neighbors.  <b>None:</b> No authentication method will be used for neighbor authentication.  <b>Simple:</b> Neighbors will be authenticated using an auth key.  <b>MD5:</b> Neighbors will be authenticated more securely by using an auth key and an MD5 key ID.	None / Simple / MD5	N/A
<b>Auth Key (Only if Auth Type is Simple or MD5)</b>	Specify the auth key to use for neighbor authentication.  <b>If the Auth Type is Simple,</b> the auth key will be a pure-text password.  <b>If the Auth Type is MD5,</b> the auth key will be an encrypted password.	1 to 8 characters	N/A
<b>MD5 Key ID (Only if Auth Type is MD5)</b>	Specify the MD5 key ID to use for neighbor authentication.   <b>Note</b>  MD5 authentication method uses MD5 to calculate a hash value from the contents of the OSPF packet and the authentication key. This hash value is transmitted in the packet, along with a key ID.	1 to 255	1
<b>Metric</b>	Specify the metric value/cost for OSPF.   <b>Note</b>  Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.	1 to 65535	1

## OSPF Settings - Edit Interface

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

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

**Edit Interface WAN**

Interface \*  
WAN

Area ID \*  
0.0.0.0

Priority \*  
1  
0 - 255

Hello Interval \*  
10  
1 - 65535 sec.



Dead Interval \*  
40  
1 - 65535 sec.

Auth Type \*  
None

Metric \*  
1  
1 - 65535


CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Interface</b>	Specify which interface to assign to an OSPF area.	Dropdown of interfaces	N/A
<b>Area ID</b>	Specify an OSPF area ID to assign to the interface.	Dropdown of area IDs	N/A
<p><b>Note</b></p> <p>To manage OSPF areas, refer to Routing &gt; Unicast Route &gt; OSPF &gt; OSPF Settings - Area.</p>			

UI Setting	Description	Valid Range	Default Value
<b>Priority</b>	Specify the priority of the interface.	0 to 255	1
<b>Hello Interval</b>	Set the hello message interval for the interface. The hello interval is the amount of time between sends of hello packets, which indicate that the device is still alive. The value of all hello intervals must be the same within a network.	1 to 65535 second(s)	10
<b>Dead Interval</b>	Set the dead interval for the interface. The dead interval is the amount of time a device will wait for a hello packet. If a hello packet is not received in this time, it will consider the other device to be dead or unavailable. By default, the dead interval is set to be four times the value of the hello interval.	1 to 65535 second(s)	40
<b>Auth Type</b>	Specify the authentication type to use when authenticating OSPF neighbors.  <b>None:</b> No authentication method will be used for neighbor authentication.  <b>Simple:</b> Neighbors will be authenticated using an auth key.  <b>MD5:</b> Neighbors will be authenticated more securely by using an auth key and an MD5 key ID.	None / Simple / MD5	N/A
<b>Auth Key (Only if Auth Type is Simple or MD5)</b>	Specify the auth key to use for neighbor authentication.  <b>If the Auth Type is Simple,</b> the auth key will be a pure-text password.  <b>If the Auth Type is MD5,</b> the auth key will be an encrypted password.	1 to 8 characters	N/A
<b>MD5 Key ID (Only if Auth Type is MD5)</b>	Specify the MD5 key ID to use for neighbor authentication.   <b>Note</b>  MD5 authentication method uses MD5 to calculate a hash value from the contents of the OSPF packet and the authentication key. This hash value is transmitted in the packet, along with a key ID.	1 to 255	1
<b>Metric</b>	Specify the metric value/cost for OSPF.   <b>Note</b>  Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.	1 to 65535	1

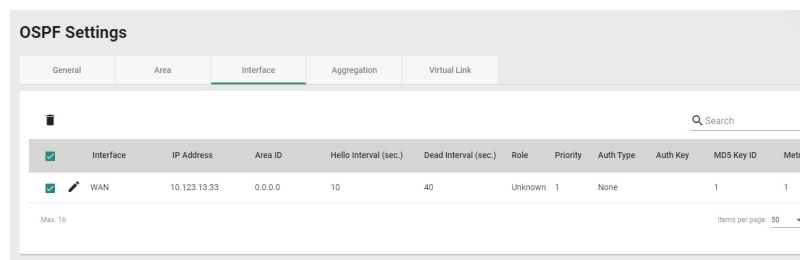
## OSPF Settings - Delete Interface

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

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

#### **Note**

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



The screenshot shows the 'OSPF Settings' page with the 'Interface' tab selected. A table lists OSPF settings for the 'WAN' interface. The table has columns for Interface, IP Address, Area ID, Hello Interval (sec.), Dead Interval (sec.), Role, Priority, Auth Type, Auth Key, MD5 Key ID, and Metric. The 'WAN' entry is selected with a checkbox.

Interface	IP Address	Area ID	Hello Interval (sec.)	Dead Interval (sec.)	Role	Priority	Auth Type	Auth Key	MD5 Key ID	Metric
<input checked="" type="checkbox"/> WAN	10.123.13.33	0.0.0.0	10	40	Unknown	1	None		1	1

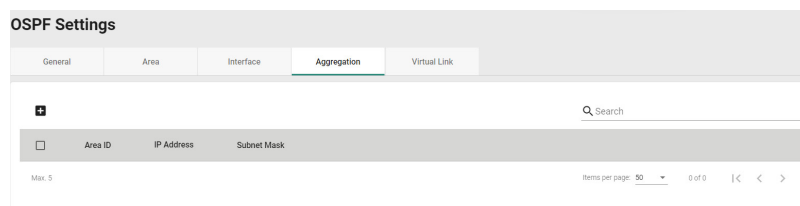
## OSPF Settings - Aggregation

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

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

#### **Limitations**

You can create up to 5 OSPF aggregations.



The screenshot shows the 'OSPF Settings' page with the 'Aggregation' tab selected. The table is currently empty, with columns for Area ID, IP Address, and Subnet Mask. A search bar and pagination controls are visible.

Area ID	IP Address	Subnet Mask
---------	------------	-------------

#### UI Setting

#### Description

##### **Area ID**

Shows the area ID.

UI Setting	Description
<b>IP Address</b>	Shows the IP address of the area.
<b>Subnet Mask</b>	Shows the network subnet mask.

## Create an Aggregation

**Menu Path:** [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings - Aggregation](#)

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

### Create Aggregation

Area ID \*

IP Address \*  Subnet Mask \*

[CANCEL](#) [CREATE](#)

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

## Edit an Aggregation

**Menu Path:** [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings - Aggregation](#)



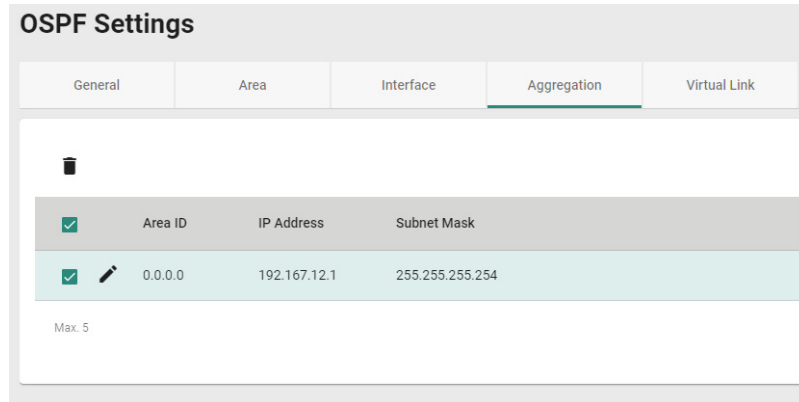
Clicking the **Edit** (✎) icon for an entry on the **Routing > Unicast Route > OSPF > OSPF Settings - Aggregation** page will open this dialog box. This dialog lets you modify an existing aggregation. Click **APPLY** to save your changes.

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

### Delete an Aggregation

**Menu Path:** [Routing > Unicast Route > OSPF > OSPF Settings - Aggregation](#)

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



## Virtual Link

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

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

### **Limitations**

You can create up to 5 OSPF virtual links.

## OSPF Status

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

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

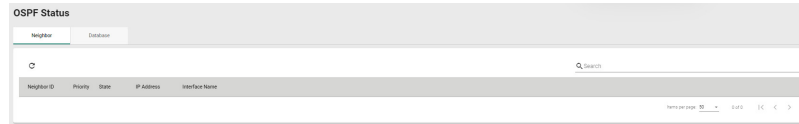
This page includes these tabs:

- Neighbor
- Database

### Neighbor

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

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



UI Setting	Description
------------	-------------

<b>Neighbor ID</b>	Shows the unique identifier for the OSPF neighbor.
--------------------	--

<b>Priority</b>	Shows priority value that the neighbor has assigned to itself.
-----------------	--

<b>State</b>	Shows the current state of the OSPF neighbor relationship: <ul style="list-style-type: none"> <li>• <b>Down:</b> The initial state before any OSPF communication has occurred between two routers.</li> <li>• <b>Init:</b> The state where the local router has sent an OSPF Hello packet to a neighbor but has not yet received a response.</li> <li>• <b>2-way:</b> The state where both routers have exchanged Hello packets and can become neighbors, but they have not yet established a bidirectional relationship.</li> <li>• <b>Exstart:</b> The state where the routers determine which one will be the master and which one will be the slave during the database exchange process.</li> <li>• <b>Exchange:</b> The state where the routers exchange link-state advertisement (LSA) headers and determine which LSAs need to be sent.</li> <li>• <b>Loading:</b> The state where the routers exchange LSAs to synchronize their link-state databases.</li> <li>• <b>Full:</b> The final state where the routers have a complete and accurate view of the network topology and are ready to forward traffic.</li> </ul>
--------------	--

<b>IP Address</b>	Shows the IP address of the neighbor router's interface used for OSPF communication.
-------------------	--

<b>Interface Name</b>	Shows the name of the local interface used for OSPF communication with the neighbor.
-----------------------	--

## Database

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

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



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

## Routing Table

### Menu Path: [Routing](#) > [Unicast Route](#) > [Routing Table](#)

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

Index	Type	Destination Address	Next Hop	Interface	Metric
1	default	0.0.0.0	10.120.12.1	9000	1
2	connected	10.120.12.0/23	10.120.12.20	9000	1
3	connected	192.168.127.0/24	192.168.127.254	LAN	1

UI Setting	Description
<b>Index</b>	Shows the unique identifier for the routing table entry.

UI Setting	Description
<b>Type</b>	Shows the source type of the route.
<b>Destination Address</b>	Shows the address of the destination network for the route.
<b>Next Hop</b>	Shows the IP address of the next hop router or gateway that the packet should be forwarded to.
<b>Interface</b>	Shows the outgoing interface that should be used to reach the destination network.
<b>Metric</b>	Shows the metric value/cost of the route to the destination network.

 **Note**

Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.

## Multicast Route

### Menu Path: [Routing](#) > [Multicast Route](#)

This section lets you configure multicast routing for your device.

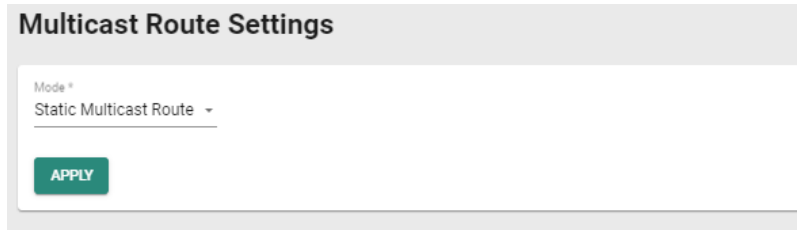
This section includes these pages:

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

## Multicast Route Settings

### Menu Path: [Routing](#) > [Multicast Route](#) > [Multicast Route Settings](#)

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



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

## Static Multicast Route

### Menu Path: [Routing](#) > [Multicast Route](#) > [Static Multicast Route](#)

This page lets you manage multicast routes for your device.

#### Limitations

You can create up to 256 static multicast routes.



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

## Create Static Multicast Route

**Menu Path:** Routing > Multicast Route > Static Multicast Route

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

**Create Static Multicast Route**

Status \*  
Enabled ▾

Group Address \*

Source Address Type \*  
Specify Source ▾ Source Address \*

Inbound Interface \* ▾

Outbound Interface \* ▾

CANCEL CREATE

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable this route.	Enabled / Disabled	Enabled
<b>Group Address</b>	Specify the group IP address for this route.	N/A	N/A
<b>Source Address Type</b>	Specify the type of source address to use for this route. <b>Any:</b> Allow any IP to be the source address. <b>Specify Source:</b> Use the specified <b>Source Address</b> .	Any / Specify Source	Any
<b>Source Address</b> <b>(Only if Source Address Type is Specify Source)</b>	Specify the source IP address to use for this route.	N/A	N/A

UI Setting	Description	Valid Range	Default Value
<b>Inbound Interface</b>	Select which interface broadcast packets will come from.	Drop-down list of interfaces	N/A
<b>Outbound Interface</b>	Select which interfaces the broadcast packets will be routed to.	Drop-down list of interfaces	N/A

## Edit Static Multicast Route

**Menu Path: Routing > Multicast Route > Static Multicast Route**

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

### Edit Static Multicast Route

Status \*

Group Address \*

Source Address Type \*

Inbound Interface \*

Outbound Interface \*

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable this route.	Enabled / Disabled	Enabled



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

## Delete Static Multicast Route

### Menu Path: Routing > Multicast Route > Static Multicast Route

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

<input checked="" type="checkbox"/>	Status	Group Address	Source Address	Inbound Interface	Outbound Interface
<input checked="" type="checkbox"/>	Disabled	239.255.255.255	ANY	WAN	LAN

Max: 255 | Items per page: 50 | 1 - 1 of 1

## Multicast Forwarding Table

### Menu Path: Routing > Multicast Route > Multicast Forwarding Table

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

Index	Group Address	Source Address	Inbound Interface	Inbound Packets	Inbound Bytes	Outbound Interface(s)
0 of 0						

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

## Broadcast Forwarding

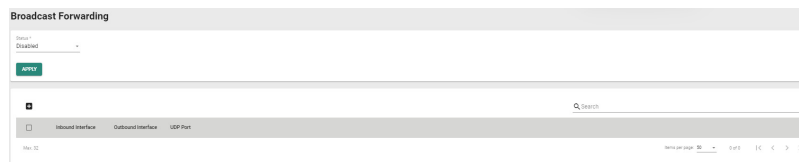
### Menu Path: [Routing](#) > [Broadcast Forwarding](#)

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

#### Limitations

You can create up to 32 broadcast forwarding entries.

## Broadcast Forwarding Settings



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


## Broadcast Forwarding List



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

## Create Broadcast Forwarding

### Menu Path: [Routing](#) > [Broadcast Forwarding](#)

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

### Create Broadcast Forwarding

CANCEL
CREATE

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

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

## Edit Broadcast Forwarding

### Menu Path: Routing > Broadcast Forwarding

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

### Edit Broadcast Forwarding

Inbound Interface \*

LAN ▼

---

Outbound Interface \*

WAN ▼

---

UDP Port \*

1 i

---


CANCEL APPLY


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


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

## Delete Broadcast Forwarding

### Menu Path: Routing > Broadcast Forwarding

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



<input checked="" type="checkbox"/>	Inbound Interface	Outbound Interface	UDP Port
<input checked="" type="checkbox"/> 	LAN	WAN	1

Max. 32

## 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

Network Address Translate

Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)
<input type="checkbox"/>	Enabled NAT_001-454	1	NAT	TCP	WAN	Any Any	Dynamic:45	Any	Any Any	192.168.127.225:80
<input checked="" type="checkbox"/>	Enabled NAT_7h40L_een4L_P0rN403	2	NAT	TCP	WAN	Any Any	Dynamic:408	Any	Any Any	192.168.127.225:443
<input checked="" type="checkbox"/>	Enabled NAT_7h40L_een4L_P0rN403	3	NAT	TCP	WAN	Any Any	Dynamic:316	Any	Any Any	192.168.127.225:80
<input checked="" type="checkbox"/>	Enabled NAT_0nD48112L_4663	4	NAT	TCP	WAN	Any Any	Dynamic:3120	Any	Any Any	192.168.127.225:443
<input checked="" type="checkbox"/>	Enabled NAT_0nD48112L_4663	5	NAT	TCP	WAN	Any Any	Dynamic:1002	Any	Any Any	192.168.127.225:80
<input checked="" type="checkbox"/>	Enabled NAT_0nD48112L_4663	6	NAT	TCP	WAN	Any Any	Dynamic:2002	Any	Any Any	192.168.127.225:443
<input checked="" type="checkbox"/>	Enabled NAT_0nD48112L_4663	7	NAT	TCP	WAN	Any Any	Dynamic:7010	Any	Any Any	192.168.127.225:443
<input checked="" type="checkbox"/>	Disabled 1_n_NAT_4663	8	Advanced	OSPF-TCP	WAN	Any Any	10.10.1.1:200-10.123.12.225:Any	Any	Any Any	192.168.127.100-192.168.127.102:Any

1-8 of 8

Apply

**UI Setting****Description****Status**

Shows whether the NAT rule is enabled or disabled.

**Description**

Shows the name of the NAT rule.

**Index**

Shows the index of the NAT rule.

**Mode**

Shows the NAT mode used by the rule.

**Protocol**

Shows the protocols included in the NAT rule.

**Incoming Interface**

Shows the incoming interface.

**Src. IP:Port (Original Packet)**

Shows the original source IP address and ports for incoming packets.

**Dst. IP:Port (Original Packet)**

Shows the original destination IP address and ports for incoming packets.

**Outgoing Interface**

Shows the outgoing interface.

**Src. IP:Port (Translated Packet)**

Shows the translated source IP address and ports.

**Dst. IP:Port (Translated Packet)**

Shows the translated destination IP address and ports.

## Create Index

### Menu Path: 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.

The screenshot shows a dialog box titled "Create Index 8" with the following settings:

- Enabled:** Enabled
- Description:** (Empty text field, 0 / 128 characters)
- Index \*:** 8 (Range: 1 - 512)
- Mode:** 1-to-1
- Auto Create Source NAT:** Disabled (with an information icon)
- NAT Loopback:** Disabled
- Double NAT:** Disabled
- VRRP Binding:** Disabled
- Original Packet (Condition):**
  - Incoming Interface:** LAN
  - Destination IP Mapping Type:** Single
  - Destination IP \*:** 0.0.0.0
- Translated Packet (Action):**
  - Destination IP Mapping Type:** Single
  - Destination IP \*:** 0.0.0.0

Buttons: CANCEL, APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable this rule.	Enabled / Disabled	Enabled
<b>Description</b>	Specify a name for this rule.	1 to 128 characters	N/A
<b>Index</b>	Specify the index of this rule.	1 to 512	N/A
<b>Mode</b>	Specify which NAT mode to use for this rule. <b>1-to-1:</b> 1-to-1 NAT maps one public IP address to one private IP address. <b>N-to-1:</b> N-to-1 NAT maps multiple private IP addresses to one public IP address. <b>PAT:</b> Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers. <b>Advance:</b> Allows you to set up an advanced NAT rule.	1-to-1 / N-to-1 / PAT / Advance	1-to-1
<b>Auto Create Source NAT</b>	Enable or disable the Auto Create Source NAT feature. If this is disabled, 1-to-1 NAT will only perform DNAT.	Enabled / Disabled	Disabled
<b>NAT Loopback</b>	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
<b>Double NAT</b>	Enable or disable Double NAT. Double NAT enables you to use 1-to-1 rules to facilitate two-way communication.	Enabled / Disabled	Disabled
<b>VRRP Binding</b>	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
<b>Incoming Interface</b>	Select the interface to use for this rule.	Drop-down list of interfaces	LAN



UI Setting	Description	Valid Range	Default Value
<b>Destination IP Mapping Type</b>	<p>Specify which destination IP addresses will be handled for incoming packets.</p> <p><b>Single:</b> This rule will apply to a single destination IP for incoming packets.</p> <p><b>Range:</b> This rule will apply to a range of destination IPs for incoming packets.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>With the 'Range' option, you have the capability to establish several 1-to-1 NAT mappings within a designated IP address range. It's essential to ensure that the 'Range' values in the Original Packet (Condition) align precisely with those in the Translated Packet (Action) for accurate Destination IP Mapping.</p> </div>	Single / Range	Single
<b>Destination IP (Only if Destination IP Mapping Type is Single)</b>	Specify the destination IP this rule will apply to.	Valid IP address	0.0.0.0
<b>Destination IP: Start (Only for Destination IP Mapping Type is Range)</b>	Specify the start of the destination IP range this rule will apply to.	Valid IP address	0.0.0.0
<b>Destination IP: End (Only if Destination IP Mapping Type is Range)</b>	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
<b>Destination IP Mapping Type</b>	<p>Specify how to handle the destination IP address translation for the internal network.</p> <p><b>Single:</b> Packets will be translated to a single IP address.</p> <p><b>Range:</b> Packets will be translated to a range of IP addresses.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>With the 'Range' option, you have the capability to establish several 1-to-1 NAT mappings within a designated IP address range. It's essential to ensure that the 'Range' values in the Original Packet (Condition) align precisely with those in the Translated Packet (Action) for accurate Destination IP Mapping.</p> </div>	Single / Range	Single
<b>Destination IP (Only if Destination IP Mapping Type is Single)</b>	Specify the destination IP to translate to on the internal network.	Valid IP address	0.0.0.0
<b>Destination IP: Start (Only for Destination IP Mapping Type is Range)</b>	Specify the start of the destination IP range to translate to on the internal network.	Valid IP address	0.0.0.0
<b>Destination IP: End (Only if Destination IP Mapping Type is Range)</b>	Specify the end of the destination IP range to translate to on the internal network.	Valid IP address	0.0.0.0

## Create Index - N-to-1 NAT

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

### Create Index 9

Status \*  
Enabled ▾

---

Description  
\_\_\_\_\_ 0 / 128

Index \*  
9  
1 - 128

Mode  
N-to-1 ▾

---

**Original Packet (Condition)**

Source IP: Start \*      Source IP: End \*  
0.0.0.0                      0.0.0.0

---

**Translated Packet (Action)**

Outgoing Interface  
WAN ▾


CANCEL    APPLY

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

## Original Packet (Condition)

UI Setting	Description	Valid Range	Default Value
<b>Source IP: Start</b>	Specify the starting IP address of the source IP range this rule will apply to.	Valid IP address	0.0.0.0
<b>Source IP: End</b>	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
<b>Outgoing Interface</b>	Select the interface for the NAT rule.   <b>Note</b> The <b>Outgoing Interface</b> 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.

### Create Index 9

Status \*  
Enabled ▾

Description  
\_\_\_\_\_ 0 / 128

Index \*  
9  
1 - 128

Mode  
PAT ▾

Protocol  
\_\_\_\_\_ ▾

NAT Loopback  
Enabled ▾

Double NAT  
Enabled ▾

**Original Packet (Condition)**

Incoming Interface  
WAN ▾

Destination Port \*  
0  
1 - 65535

**Translated Packet (Action)**

Destination IP \*  
0.0.0.0  
\_\_\_\_\_

Destination Port \*  
0  
1 - 65535

CANCEL APPLY

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

UI Setting	Description	Valid Range	Default Value
<b>Mode</b>	Specify which NAT mode to use for this rule. <b>1-to-1:</b> 1-to-1 NAT maps one public IP address to one private IP address. <b>N-to-1:</b> N-to-1 NAT maps multiple private IP addresses to one public IP address. <b>PAT:</b> Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers. <b>Advance:</b> Allows you to set up an advanced NAT rule.	1-to-1 / N-to-1 / PAT / Advance	1-to-1
<b>Protocol</b>	Select which protocols this rule will include.	ICMP / TCP / UDP	N/A
<b>NAT Loopback</b>	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
<b>Double NAT</b>	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
<b>Incoming Interface</b>	Select the interface to use for this rule.	Drop-down list of interfaces	LAN
<b>Destination Port</b>	Specify the destination port this rule will apply to.	1 to 65535	Any

### Translated Packet (Action)

UI Setting	Description	Valid Range	Default Value
<b>Destination IP</b>	Specify the destination IP to translate to on the internal network.	Valid IP address	0.0.0.0
<b>Destination Port</b>	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 \* Source IP: End \*  
0.0.0.0 0.0.0.0

Source Port Mapping Type  
Range

Source Port: Start \* Source Port: End \*  
0 0

1 - 65535 1 - 65535

Destination IP Mapping Type  
Range

Destination IP: Start \* Destination IP: End \*  
0.0.0.0 0.0.0.0

Destination Port Mapping Type  
Range

Destination Port: Start \* Destination Port: End \*  
0 0

1 - 65535 1 - 65535

#### Translated Packet (Action)

Outgoing Interface  
Any

Source IP Mapping Type  
Range

Source IP: Start \* Source IP: End \*  
0.0.0.0 0.0.0.0

Source Port Mapping Type  
Range

Source Port: Start \* Source Port: End \*  
0 0

1 - 65535 1 - 65535

Destination IP Mapping Type  
Range

Destination IP: Start \* Destination IP: End \*  
0.0.0.0 0.0.0.0

Destination Port Mapping Type  
Range

Destination Port: Start \* Destination Port: End \*  
0 0

1 - 65535 1 - 65535

CANCEL APPLY



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

### Original Packet (Condition)

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

UI Setting	Description	Valid Range	Default Value
<b>Subnet Mask</b> (Only if Source IP Mapping Type is Subnet)	Specify the subnet this rule will apply to.	Valid subnet	24 (255.255.255.0)
<b>Source IP: Start</b> (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
<b>Source IP: End</b> (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
<b>Source Port Mapping Type</b>	Specify which source ports will be handled for incoming packets. <b>Any:</b> This rule will apply to all source ports. <b>Single:</b> This rule will apply to a single source port for incoming packets. <b>Range:</b> This rule will apply to a range of source ports for incoming packets.	Any / Single / Range	Any
<b>Source Port</b> (Only if Source Port Mapping Type is Single)	Specify the source port this rule will apply to.	1 to 65535	N/A
<b>Source Port: Start</b> (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
<b>Source Port: End</b> (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
<b>Destination IP Mapping Type</b>	Specify which destination IP addresses will be handled for incoming packets. <b>Any:</b> This rule will apply to all destination IPs. <b>Single:</b> This rule will apply to a single destination IP for incoming packets. <b>Range:</b> This rule will apply to a range of destination IPs for incoming packets. <b>Subnet:</b> This rule will apply to a destination IP and subnet mask.	Any / Single / Range / Subnet	Any

UI Setting	Description	Valid Range	Default Value
<b>Destination IP</b> <b>(Only if Destination IP Mapping Type is Single or Subnet)</b>	Specify the destination IP this rule will apply to.  <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p><b>Note</b></p> <p>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.</p> <p>Refer to Network Configuration &gt; Interface - Secondary IP for more information.</p> </div>	Valid IP address	0.0.0.0
<b>Subnet Mask</b> <b>(Only if Destination IP Mapping Type is Subnet)</b>	Specify the subnet this rule will apply to.	Valid subnet	24 (255.255.255.0)
<b>Destination IP: Start</b> <b>(Only for Destination IP Mapping Type is Range)</b>	Specify the start of the destination IP range this rule will apply to.	Valid IP address	0.0.0.0
<b>Destination IP: End</b> <b>(Only if Destination IP Mapping Type is Range)</b>	Specify the end of the destination IP range this rule will apply to.	Valid IP address	0.0.0.0
<b>Destination Port Mapping Type</b>	Specify which destination ports will be handled for incoming packets.  <b>Any:</b> This rule will apply to all destination ports.  <b>Single:</b> This rule will apply to a single destination port for incoming packets.  <b>Range:</b> This rule will apply to a range of destination ports for incoming packets.	Any / Single / Range	Any
<b>Destination Port</b> <b>(Only if Destination Port Mapping Type is Single)</b>	Specify the destination port this rule will apply to.	1 to 65535	N/A
<b>Destination Port: Start</b> <b>(Only if Destination Port Mapping Type is Range)</b>	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
<b>Destination IP: End</b> <b>(Only if Destination Port Mapping Type is Range)</b>	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
<b>Outgoing Interface</b>	Select the interface for the NAT rule.	Drop-down list of interfaces	Any
<b>Source IP Mapping Type</b>	Specify how to handle source IP translation for the internal network. <b>Any:</b> This rule will translate to all source IPs. <b>Single:</b> This rule will translate to a single source IP. <b>Range:</b> This rule will translate to a range of source IPs. <b>Subnet:</b> This rule will translate to a source IP and subnet mask. <b>Dynamic:</b>	Any / Single / Range / Subnet / Dynamic	Any
<b>Source IP</b> <b>(Only if Source IP Mapping Type is Single or Subnet)</b>	Specify the source IP this rule will translate to.  <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p><b>Note</b></p> <p>If <b>Source IP Mapping Type</b> is <b>Single</b>, 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.</p> <p>Refer to Network Configuration &gt; Interface - Secondary IP for more information.</p> </div>	Valid IP address	0.0.0.0
<b>Subnet Mask</b> <b>(Only if Source IP Mapping Type is Subnet)</b>	Specify the subnet this rule will translate to.	Valid subnet	24 (255.255.255.0)

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

UI Setting	Description	Valid Range	Default Value
<b>Destination IP</b> (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
<b>Subnet Mask</b> (Only if Destination IP Mapping Type is Subnet)	Specify the subnet this rule will translate to.	Valid subnet	24 (255.255.255.0)
<b>Destination IP: Start</b> (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
<b>Destination IP: End</b> (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
<b>Destination Port Mapping Type</b>	Specify how to handle destination port translation for the internal network. <b>Any:</b> This rule will apply to all destination ports. <b>Single:</b> This rule will apply to a single destination port for incoming packets. <b>Range:</b> This rule will apply to a range of destination ports for incoming packets.	Any / Single / Range	Any
<b>Destination Port</b> (Only if Destination Port Mapping Type is Single)	Specify the destination port this rule will translate to.	1 to 65535	N/A
<b>Destination Port: Start</b> (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
<b>Destination Port: End</b>  (Only if Destination Port Mapping Type is Range)	Specify the end of the destination port range this rule will translate to.	1 to 65535	N/A

## Object Management

### Menu Path: Object Management

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

### Object Management - User Privileges

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

Settings	Admin	Supervisor	User
<b>Object Management</b>	R/W	R/W	R

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

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

#### Limitations

You can create up to 512 objects.

<input type="checkbox"/>	Name	Type	Details	References
<input type="checkbox"/>	MOXA_Test	IP Address and Subnet	10.0.0.1 - 10.0.0.10	0
<input type="checkbox"/>	MOXA_Test2	Industrial Application Service	DNP3	0
<input type="checkbox"/>	MOXA_Test3	Industrial Application Service	Modbus	0

Max: 512      Items per page: 50      1 - 3 of 3      |< < > >|

UI Setting	Description
------------	-------------

- |                   |   |
|-------------------|---|
| <b>Name</b>       | Shows the name of the object.   |
| <b>Type</b>       | Shows the type of the object.   |
| <b>Details</b>    | Shows the settings for the object. These settings will vary depending on the object's <b>Type</b> . |
| <b>References</b> | Shows the number of times this object is referenced in firewall rules.                              |

## Create Object

### Menu Path: Object Management

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

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

### Create Object

Name \*

0 / 32

Object Type \*

CANCEL    CREATE

## Create Object - IP Address and Subnet

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



## Create Object

Name \*  
test\_moxa  
9 / 32

Object Type \*  
IP Address and Subnet

IP Type \*

CANCEL

CREATE

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the object.	1 to 32 characters	N/A
<b>Object Type</b>	<p>Select a type for the object.</p> <p><b>IP Address and Subnet:</b> You can specify an IP address, a range of IP addresses, or a subnet.</p> <p><b>Network Service:</b> You can select from a list of protocol and port combinations used for common network services.</p> <p><b>Industrial Application Service:</b> You can select from a list of protocol and port combinations used for industrial communications and applications.</p> <p><b>User-defined Service:</b> You can specify your own protocol and port combination.</p>	IP Address and Subnet / Network Service / Industrial Application Service / User-defined Service	N/A
<b>IP Type</b>	Select the type of IP address to use for the object.	Single IP / IP Range / Subnet	N/A
<b>IP Address (If Single is selected for IP Type)</b>	Specify the IP address to use for the object.	Valid IP Address	N/A
<b>IP Address: Start (If IP Range is selected for IP Type)</b>	Specify the start of the IP range to use for the object.	Valid IP Address	N/A

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

## Create Object - Network Service

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

## Create Object

Name \*

0 / 32

Object Type

Network Service

Select Network Service(s)

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

CANCEL

CREATE

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

UI Setting	Description	Valid Range	Default Value
<b>Object Type</b>	<p>Select a type for the object.</p> <p><b>IP Address and Subnet:</b> You can specify an IP address, a range of IP addresses, or a subnet.</p> <p><b>Network Service:</b> You can select from a list of protocol and port combinations used for common network services.</p> <p><b>Industrial Application Service:</b> You can select from a list of protocol and port combinations used for industrial communications and applications.</p> <p><b>User-defined Service:</b> You can specify your own protocol and port combination.</p>	IP Address and Subnet / Network Service / Industrial Application Service / User-defined Service	N/A
<b>Select Network Service(s)</b>	Select a category of network services, or individual services to use for the object. You can select multiple options.	Remote-Access / Remote-Desktop / Email / File-Transfer / Web-Access / Network-Service / Authentication / VOIP-and-Streaming / SQL-Server	N/A
<b>Remote-Access</b>	This category includes protocols used for remote access to a device.	WINS (TCP 1512; UDP 1512) TELNET (TCP 23) SSH (TCP 22)	N/A
<b>Remote-Desktop</b>	This category includes protocols used by various remote desktop services.	PC-Anywhere (TCP 5631; UDP 5632) Chrome-Remote-Desktop (UDP 5222) AnyDesk (TCP 6568, 7070; UDP 50001 - 50003) Teamviewer (TCP 5938) RDP (TCP 3389) VNC (TCP 5900) X-WINDOW (TCP 6000 - 6063)	N/A
<b>Email</b>	This category includes protocols used for sending and receiving emails.	IMAP (TCP 143) IMAPS (TCP 993) POP3 (TCP 110) POP3S (TCP 995) SMTP (TCP 25) SMTPS (TCP 465)	N/A
<b>File-Transfer</b>	This category includes protocols used for different methods of file transfer.	FTP (TCP 21) FTPS (TCP 990) SFTP (TCP 115; UDP 115) TFTP (UDP 69) NFS (TCP 111, 2049; UDP 111, 2049) SAMBA (TCP 139) AFS3 (TCP 7000 - 7009; UDP 7000 - 7009) SMB (TCP 445)	N/A

UI Setting	Description	Valid Range	Default Value
<b>Web-Access</b>	This category includes protocols used by web browsers.	HTTP (TCP 80) HTTPS (TCP 443)	N/A
<b>Network-Service</b>	This category includes protocols used by various network services.	BGP (TCP 179) DHCP (UDP 67) DHCP6 (UDP 546) DNS (TCP 53; UDP 53) NTP (TCP 123; UDP 123) ICMP-PING (ICMP Type Any Code Any) OSPF (IP Protocol 89) RIP (TCP 520) SNMP (TCP 161 - 162; UDP 161 - 162) SYSLOG (UDP 514)	N/A
<b>Authentication</b>	This category includes protocols used by authentication services.	LDAP (TCP 389; UDP 389) LDAPS (TCP 636; UDP 636) RADIUS (UDP 1812 - 1813) TACACS+ (TCP 49; UDP 49)	N/A
<b>VOIP-and-Streaming</b>	This category includes protocols used for VOIP calling and streaming video.	SIP (TCP 5060; UDP 5060) RSTP (TCP 554, 7070, 8554; UDP 554)	N/A
<b>SQL-Server</b>	This category includes protocols used for SQL servers.	MS-SQL (TCP 1433 - 1434) MYSQL (TCP 3306)	N/A

## Create Object - Industrial Application Service

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

## Create Object

Name \*

0 / 32

Object Type

Industrial Application Service

Select Industrial Application Service(s)

- Modbus (TCP 502; UDP 502)
- DNP3 (TCP 20000)
- IEC-60870-5-104 (TCP 2404)
- IEC-61850-MMS (TCP 102)
- OPC-DA (TCP 135)
- OPC-UA (TCP 4840; UDP 4840)
- CIP-EtherNet/IP (TCP 44818; UDP 2222)
- Siemens-Step7 (TCP 102)
- Moxa-RealCOM (TCP 950 - 981)
- Moxa-MXview-Request (TCP 161, 162, 443, 4000; UDP 4000, 40404)

CANCEL

CREATE

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

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

## Create Object - User-defined Service

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

## Create Object

Name \*  
test\_moxa  
9 / 32

Object Type \*  
IP Address and Subnet

IP Type \*

CANCEL

CREATE

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



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

## Edit Object

### Menu Path: Object Management

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

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

**Note**

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

## Edit Object - IP Address and Subnet

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

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

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

## Edit Object - Network Service

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

## Create Object

Name \*

0 / 32

Object Type

Network Service

Select Network Service(s)

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

CANCEL

CREATE

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the object.	1 to 32 characters	N/A
<b>Object Type (View-only)</b>	Shows the type for the object. This setting cannot be changed when editing an object.	Network Service	Network Service
<b>Select Network Service(s)</b>	Select a category of network services, or individual services to use for the object. You can select multiple options.	Remote-Access / Remote-Desktop / Email / File-Transfer / Web-Access / Network-Service / Authentication / VOIP-and-Streaming / SQL-Server	N/A
<b>Remote-Access</b>	This category includes protocols used for remote access to a device.	WINS (TCP 1512; UDP 1512) TELNET (TCP 23) SSH (TCP 22)	N/A

UI Setting	Description	Valid Range	Default Value
<b>Remote-Desktop</b>	This category includes protocols used by various remote desktop services.	PC-Anywhere (TCP 5631; UDP 5632) Chrome-Remote-Desktop (UDP 5222) AnyDesk (TCP 6568, 7070; UDP 50001 - 50003) Teamviewer (TCP 5938) RDP (TCP 3389) VNC (TCP 5900) X-WINDOW (TCP 6000 - 6063)	N/A
<b>Email</b>	This category includes protocols used for sending and receiving emails.	IMAP (TCP 143) IMAPS (TCP 993) POP3 (TCP 110) POP3S (TCP 995) SMTP (TCP 25) SMTPS (TCP 465)	N/A
<b>File-Transfer</b>	This category includes protocols used for different methods of file transfer.	FTP (TCP 21) FTPS (TCP 990) SFTP (TCP 115; UDP 115) TFTP (UDP 69) NFS (TCP 111, 2049; UDP 111, 2049) SAMBA (TCP 139) AFS3 (TCP 7000 - 7009; UDP 7000 - 7009) SMB (TCP 445)	N/A
<b>Web-Access</b>	This category includes protocols used by web browsers.	HTTP (TCP 80) HTTPS (TCP 443)	N/A
<b>Network-Service</b>	This category includes protocols used by various network services.	BGP (TCP 179) DHCP (UDP 67) DHCP6 (UDP 546) DNS (TCP 53; UDP 53) NTP (TCP 123; UDP 123) ICMP-PING (ICMP Type Any Code Any) OSPF (IP Protocol 89) RIP (TCP 520) SNMP (TCP 161 - 162; UDP 161 - 162) SYSLOG (UDP 514)	N/A
<b>Authentication</b>	This category includes protocols used by authentication services.	LDAP (TCP 389; UDP 389) LDAPS (TCP 636; UDP 636) RADIUS (UDP 1812 - 1813) TACACS+ (TCP 49; UDP 49)	N/A
<b>VOIP-and-Streaming</b>	This category includes protocols used for VOIP calling and streaming video.	SIP (TCP 5060; UDP 5060) RSTP (TCP 554, 7070, 8554; UDP 554)	N/A
<b>SQL-Server</b>	This category includes protocols used for SQL servers.	MS-SQL (TCP 1433 - 1434) MYSQL (TCP 3306)	N/A

## Edit Object - Industrial Application Service

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

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

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

## Edit Object - User-defined Service

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

### Edit Object

Name \*  
test-user  
9 / 32

Object Type  
User-defined Service ▼

IP Protocol \*  
TCP ▼

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

Port: Start \*      Port: End \*  
1 - 65535      1 - 65535

CANCEL
APPLY


UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the object.	1 to 32 characters	N/A
<b>Object Type (View-only)</b>	Shows the type for the object. This setting cannot be changed when editing an object.	User-defined Service	User-defined Service
<b>IP Protocol</b>	Select the IP protocols to use for the object.	TCP / UDP / TCP and UDP / ICMP Custom IP Protocol	N/A
<b>Service Port Type (If TCP, UDP, or TCP and UDP is selected for IP Protocol)</b>	Select how to define ports for the object. <b>Any:</b> All ports will be included. <b>Single TCP and UDP Port:</b> Specify a single port to include. <b>TCP and UDP Port Range:</b> Specify a range of ports to include.	Any / Single TCP and UDP Port / TCP and UDP Port Range	
<b>Port (If Single TCP and UDP Port is selected for Service Port Type)</b>	Specify a port to include.	1 to 65535	N/A
<b>Port: Start (If TCP and UDP Port Range is selected for Service Port Type)</b>	Specify the start of the port range to use for the object.	1 to 65535	N/A
<b>Port: End (If TCP and UDP Port Range is selected for Service Port Type)</b>	Specify the end of the port range to use for the object.	1 to 65535	N/A
<b>ICMP Type (Decimal) (If ICMP is selected for IP Protocol)</b>	Specify the ICMP type in decimal form to use for the object. Leave this blank to allow all ICMP types to be included.	Blank, 0 to 255	N/A
<b>ICMP Code (Decimal) (If ICMP is selected for IP Protocol)</b>	Specify the ICMP code in decimal form to use for the object. Leave this blank to allow all ICMP codes to be included.	Blank, 0 to 255	N/A

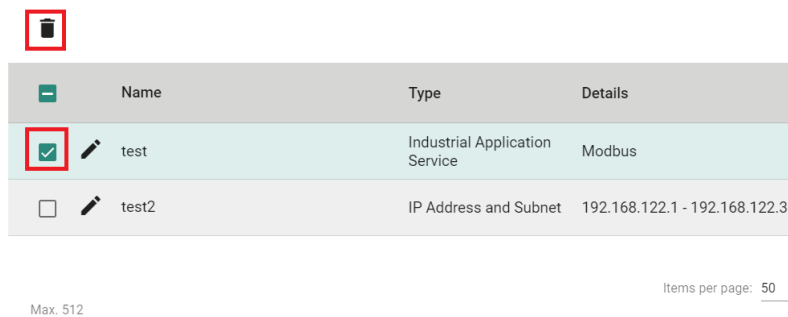



UI Setting	Description	Valid Range	Default Value
<b>IP Protocol (Decimal)</b> <b>(If Custom IP Protocol is selected for IP Protocol)</b>	Specify the IP protocol in decimal form to use for the object.	0 to 255	N/A

## Delete Object

### Menu Path: Object Management

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



	Name	Type	Details
<input checked="" type="checkbox"/>	test	Industrial Application Service	Modbus
<input type="checkbox"/>	test2	IP Address and Subnet	192.168.122.1 - 192.168.122.3

Max. 512 Items per page: 50

## Firewall

### Menu Path: Firewall

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

This settings area includes these sections:

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

## Network Configuration - User Privileges

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

Settings	Admin	Supervisor	User
<b>Layer 2 Policy</b>	R/W	R/W	R
<b>Layer 3 - 7 Policy</b>	R/W	R/W	R
<b>Malformed Packets</b>	R/W	R/W	R
<b>Session Control</b>	R/W	R/W	R
<b>DoS Policy</b>	R/W	R/W	R
<b>Advanced Protection</b>			
<b>Dashboard</b>	R/W	R/W	-
<b>Configuration</b>	R/W	R/W	-
<b>Protocol Filter Policy</b>	R/W	R/W	-
<b>ADP</b>	R/W	R/W	-
<b>IPS</b>	R/W	R/W	-

### Layer 2 Policy

#### Menu Path: Firewall > Layer 2 Policy

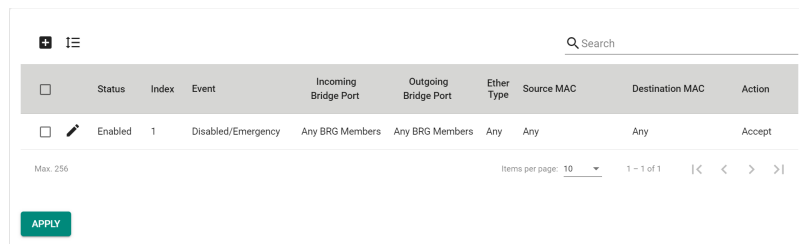
This page lets you configure advanced Layer 2 policies for your device's firewall. Layer 2 firewall policies can filter packets from bridge ports and have a higher priority than Layer 3 policies.

### **Note**

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

### **Limitations**

You can configure up to 256 Layer 2 policies.



The screenshot shows a table with the following columns: Status, Index, Event, Incoming Bridge Port, Outgoing Bridge Port, Ether Type, Source MAC, Destination MAC, and Action. The first row of data shows: Status: Enabled, Index: 1, Event: Disabled/Emergency, Incoming Bridge Port: Any BRG Members, Outgoing Bridge Port: Any BRG Members, Ether Type: Any, Source MAC: Any, Destination MAC: Any, Action: Accept. Below the table, there is a search bar, a dropdown for 'Items per page' set to 10, and a page indicator '1 - 1 of 1'. An 'APPLY' button is located at the bottom left of the table area.

### **UI Setting**

### **Description**

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

## **Add Layer 2 Policy**

**Menu Path:** Firewall > Layer 2 Policy

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

**Add Layer 2 Policy**

Status \*  
Enabled

Index \*  
2

Log \*  
Enabled

Severity \*  
Severity \*

Log Destination  
Log Destination

Incoming Bridge Port \*  
Any

Outgoing Bridge Port \*  
Any

EtherType Options \*  
Any

Action \*  
Accept

Source MAC Type \*  
Any

Destination MAC Type \*  
Any

CANCEL CREATE

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the policy.	Enabled / Disabled	Enabled
<b>Index</b>	Specify the index number for the policy. The index determines the order for processing policies.	1 to 256	Last used index plus 1
<b>Log</b>	Enable or disable firewall event logging for this policy.	Enabled / Disabled	Enabled
<b>Severity</b>	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	N/A

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

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

## Edit Layer 2 Policy

### Menu Path: Firewall > Layer 2 Policy

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

### Edit Layer 2 Policy

Status \*  
Enabled

Index \*  
1

1 - 1

Log \*  
Disabled

Severity \*  
Emergency

Log Destination

Incoming Bridge Port \*  
Any

Outgoing Bridge Port \*  
Any

EtherType Options \*  
IPv4

EtherType Value (Hexadecimal)  
0x0800

Action \*  
Accept

Source MAC Type \*  
Any

Destination MAC Type \*  
Any

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the policy.	Enabled / Disabled	Enabled
<b>Index</b>	Specify the index number for the policy. The index determines the order for processing policies.	1 to 256	Last used index plus 1
<b>Log</b>	Enable or disable firewall event logging for this policy.	Enabled / Disabled	Enabled
<b>Severity</b>	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	N/A

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

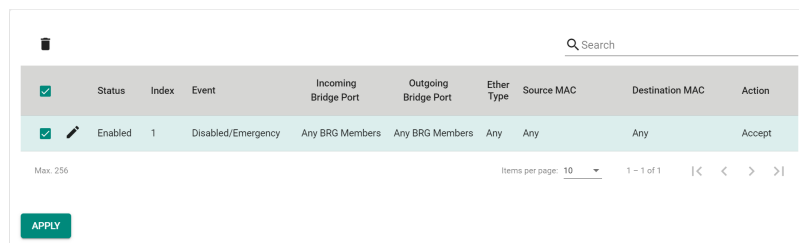


UI Setting	Description	Valid Range	Default Value
<b>Action</b>	Select the action the firewall should take for traffic that matches this policy.  <b>Accept:</b> The firewall will accept packets that match the policy.  <b>Drop:</b> The firewall will drop packets that match the policy.	Accept / Drop	Accept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

## Delete Layer 2 Policy

### Menu Path: Firewall > Layer 2 Policy

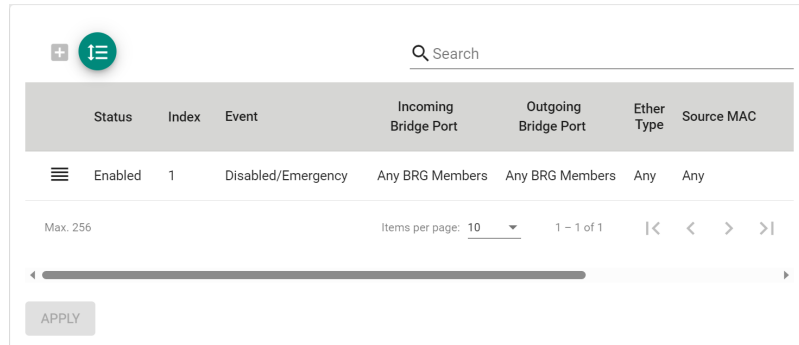
You can delete a policy by using the checkboxes to select the entries you want to delete, then clicking the **Delete** (🗑️) icon.



## Reorder Layer 2 Policies

### Menu Path: Firewall > Layer 2 Policy

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



The screenshot shows a web interface for configuring policies. At the top, there is a search bar with a magnifying glass icon and the text 'Search'. Below the search bar is a table with the following columns: Status, Index, Event, Incoming Bridge Port, Outgoing Bridge Port, Ether Type, and Source MAC. The table contains one row with the following values: Enabled, 1, Disabled/Emergency, Any BRG Members, Any BRG Members, Any, and Any. Below the table, there is a pagination bar showing 'Max. 256', 'Items per page: 10', and '1 - 1 of 1'. There are also navigation arrows and a scroll bar. At the bottom left of the interface, there is an 'APPLY' button.

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

## Layer 3-7 Policy

### Menu Path: Firewall > Layer 3-7 Policy

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

#### Note

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

#### Limitations

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

## Layer 3-7 Policy Settings

**Global Policy Settings**

Status: Disabled Default Action: Allow All

---

**Global Policy Event Settings**

Log: Enabled

**APPLY**

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

## Layer 3-7 Policy List

Search

Index	Status	Name	Event	Incoming Interface	Outgoing Interface	Filter Mode	Source Address	Source Port	Destination Address	Destination Port or Protocol	Action	Description
Max: 1024												
											Items per page: 50	0 of 0


**APPLY**

UI Setting	Description
<b>Index</b>	Shows the index of the policy. The index determines the order for processing policies.
<b>Status</b>	Shows whether the policy is enabled or disabled.
<b>Name</b>	Shows the name of the policy.
<b>Event</b>	Shows whether logging is enabled or disabled for the event and the severity assigned to the event.

UI Setting	Description
<b>Incoming Interface</b>	Shows the incoming interface for the policy.
<b>Outgoing Interface</b>	Shows the outgoing interface for the policy.
<b>Filter Mode</b>	Shows the filter mode used for the policy.
<b>Source Address</b>	Shows the source IP addresses the policy applies to.
<b>Source Port</b>	Shows the source ports the policy applies to.
<b>Destination Address</b>	Shows the destination IP addresses the policy applies to.
<b>Destination Port or Protocol</b>	Shows the destination ports or protocols the policy applies to.
<b>Action</b>	Shows the action that will be taken for applicable traffic.
<b>Description</b>	Shows the description of the policy.

## Create Layer 3-7 Policy

### Menu Path: Firewall > Layer 3-7 Policy

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

## Create Layer 3-7 Policy

Index \*  
1

1 - 1024

Status \*  
Enabled

Name \*  
0 / 32

Description  
0 / 128

Log \*  
Disabled

Severity \*  
Warning

Log Destination  
Local Storage

Incoming Interface \*  
Any

Outgoing Interface \*  
Any

Action \*  
Allow

Filter Mode \*  
IP and Port Filtering

Source IP Address \*  
Any

Source Port \*  
Any

Destination IP Address \*  
Any

Destination Port or Protocol \*  
Any

CANCEL

CREATE

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

UI Setting	Description	Valid Range	Default Value
<b>Log</b>	Enable or disable firewall event logging for this policy.	Enabled / Disabled	Enabled
<b>Severity</b>	Select the severity level to assign events for this policy. Refer to <b>Appendix &gt; Severity</b> for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A
<b>Log Destination</b>	Specify where to send firewall event logs. You can select multiple options.  <b>Local Storage:</b> Firewall event logs will be stored on local storage and will show up in the device's Event Log. Refer to <b>Diagnostics &gt; Event Logs and Notifications &gt; Event Log</b> for more information.  <b>Syslog:</b> Firewall event logs will be sent to a syslog server. Refer to <b>Diagnostics &gt; Event Logs and Notifications &gt; Syslog</b> for more information.  <b>Trap:</b> Firewall event notifications will be sent to a trap server. Refer to <b>Diagnostics &gt; SNMP Trap/Inform</b> for more information.	Local Storage / Syslog / Trap	N/A
<b>Incoming Interface</b>	Select the incoming interface for this policy.  <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p><b>Note</b></p> <p>Available interfaces will vary depending on your product model and configuration. Refer to <b>Network Configuration &gt; Network Interfaces</b> for more information about managing your device's interfaces.</p> </div>	Any / Drop-down list of interfaces	Any
<b>Outgoing Interface</b>	Select the outgoing interface for this policy.  <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p><b>Note</b></p> <p>Available interfaces will vary depending on your product model and configuration. Refer to <b>Network Configuration &gt; Network Interfaces</b> for more information about managing your device's interfaces.</p> </div>	Any / Drop-down list of interfaces	Any
<b>Action</b>	Select the action the firewall should take for traffic that matches this policy.  <b>Accept:</b> The firewall will accept packets that match the policy.  <b>Drop:</b> The firewall will drop packets that match the policy.	Accept / Drop	Accept

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

## Edit Layer 3-7 Policy

### Menu Path: Firewall > Layer 3-7 Policy

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

**Edit Layer 3-7 Policy**

Index \*  
1  
1 - 1024

Status \*  
Enabled

Name \*  
TestPolicy  
10 / 32

Description  
0 / 128

Log \*  
Disabled

Severity \*  
Warning

Log Destination  
Local Storage

Incoming Interface \*  
Any

Outgoing Interface \*  
Any

Action \*  
Allow

Filter Mode \*  
IP and Port Filtering

Source IP Address \*  
Any

Source Port \*  
Any

CANCEL APPLY

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



UI Setting	Description	Valid Range	Default Value
<b>Description</b>	Specify a description for the policy.	0 to 128 characters	N/A
<b>Log</b>	Enable or disable firewall event logging for this policy.	Enabled / Disabled	Enabled
<b>Severity</b>	Select the severity level to assign events for this policy. Refer to <b>Appendix &gt; Severity</b> for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A
<b>Log Destination</b>	Specify where to send firewall event logs. You can select multiple options.  <b>Local Storage:</b> Firewall event logs will be stored on local storage and will show up in the device's Event Log. Refer to <b>Diagnostics &gt; Event Logs and Notifications &gt; Event Log</b> for more information.  <b>Syslog:</b> Firewall event logs will be sent to a syslog server. Refer to <b>Diagnostics &gt; Event Logs and Notifications &gt; Syslog</b> for more information.  <b>Trap:</b> Firewall event notifications will be sent to a trap server. Refer to <b>Diagnostics &gt; SNMP Trap/Inform</b> for more information.	Local Storage / Syslog / Trap	N/A
<b>Incoming Interface</b>	Select the incoming interface for this policy.  <b>Note</b> Available interfaces will vary depending on your product model and configuration. Refer to <b>Network Configuration &gt; Network Interfaces</b> for more information about managing your device's interfaces.	Any / Drop-down list of interfaces	Any
<b>Outgoing Interface</b>	Select the outgoing interface for this policy.  <b>Note</b> Available interfaces will vary depending on your product model and configuration. Refer to <b>Network Configuration &gt; Network Interfaces</b> for more information about managing your device's interfaces.	Any / Drop-down list of interfaces	Any

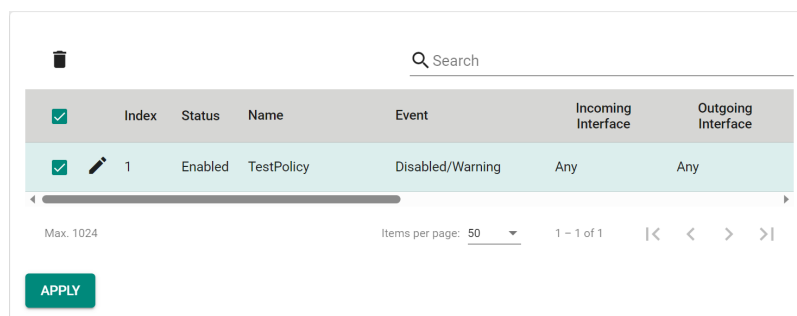
UI Setting	Description	Valid Range	Default Value
<b>Action</b>	<p>Select the action the firewall should take for traffic that matches this policy.</p> <p><b>Accept:</b> The firewall will accept packets that match the policy.</p> <p><b>Drop:</b> The firewall will drop packets that match the policy.</p>	Accept / Drop	Accept
<b>Filter Mode</b>	<p>Select the filter mode to use for packet filtering.</p> <p><b>IP and Port Filtering:</b> The policy will filter based on IP address and port.</p> <p><b>IP and Source MAC Binding:</b> The policy will filter based on IP address and will also check the source MAC address.</p> <p><b>Source MAC Filtering:</b> The policy will filter based on source MAC address.</p>	IP and Port Filtering / IP and Source MAC Binding / Source MAC Filtering	IP and Port Filtering
<b>Source IP Address</b> (if Filter Mode is IP and Port Filtering or IP and Source MAC Binding)	<p>Select the source IP addresses this policy will apply to. Select <b>Any</b> to check traffic from all source IP addresses, or select a pre-defined object. You can also click the Add (+) icon to create a new IP Address and Subnet object.</p> <p>Refer to <b>Create Object</b> for more information.</p>	Any / Drop-down list of IP Address and Subnet objects	Any
<b>Source Port</b> (if Filter Mode is IP and Port Filtering)	<p>Select the source ports this policy will apply to. Select <b>Any</b> to check traffic from all source ports, or select a pre-defined object. You can also click the Add (+) icon to create a new User-defined Service object.</p> <p>Refer to <b>Create Object</b> for more information.</p>	Any / Drop-down list of port-based User-defined Service objects	Any
<b>Source MAC Address</b> (if Filter Mode is IP and Source MAC Binding or Source MAC Filtering)	<p>Specify the source MAC address this policy will apply to.</p>	Valid MAC address	N/A
<b>Destination IP Address</b> (if Filter Mode is IP and Port Filtering)	<p>Select the destination IP addresses this policy will apply to. Select <b>Any</b> to check all traffic going to any destination IP address, or select a pre-defined object. You can also click the Add (+) icon to create a new IP Address and Subnet object.</p> <p>Refer to <b>Create Object</b> for more information.</p>	Any / Drop-down list of IP Address and Subnet objects	Any

UI Setting	Description	Valid Range	Default Value
<b>Destination Port or Protocol</b> <b>(if Filter Mode is IP and Port Filtering)</b>	Select the destination ports or protocol this policy will apply to. Select <b>Any</b> to check all traffic going to any destination port or protocol, or select a pre-defined service or object. You can also click the Add (+) icon to create a new Network Service, Industrial Application Service, or User-defined Service object.  Refer to <b>Create Object</b> for more information.	Any / Drop-down list of Network Service, Industrial Application Service, and port-based User-defined Service objects	Any

## Delete Layer 3-7 Policy

### Menu Path: Firewall > Layer 3-7 Policy

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



## Reorder Layer 3-7 Policies

### Menu Path: Firewall > Layer 3-7 Policy

You can reorder policies by clicking the **Reorder Priorities** (⌵) icon, moving the entries into the order you want, then clicking the **Reorder Priorities** (⌶) icon again.

Reordering policies affects the order used to process the policies.

Index	Status	Name	Event	Incoming Interface	Outgoing Interface	Filter
1	Enabled	Test	Disabled/Warning	Any	Any	IP and
2	Enabled	BasicFilter	Disabled/Warning	Any	Any	IP and

## Malformed Packets

### Menu Path: Firewall > Malformed Packets

This page lets you configure the Malformed Packets feature, which enables the device to record event logs with a user-specified severity whenever malformed packets are dropped by the system. Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable recording an event when malformed packets are dropped.	Enabled / Disabled	Disabled
<b>Severity</b>	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	Emergency

UI Setting	Description	Valid Range	Default Value
<b>Log Destination</b>	<p>Specify where to send firewall event logs. You can select multiple options.</p> <p><b>Local Storage:</b> Firewall event logs will be stored on local storage and will show up in the device's Event Log. Refer to <a href="#">Diagnostics &gt; Event Logs and Notifications &gt; Event Log</a> for more information.</p> <p><b>Syslog:</b> Firewall event logs will be sent to a syslog server. Refer to <a href="#">Diagnostics &gt; Event Logs and Notifications &gt; Syslog</a> for more information.</p> <p><b>Trap:</b> Firewall event notifications will be sent to a trap server. Refer to <a href="#">Diagnostics &gt; SNMP Trap/Inform</a> for more information.</p>	Local Storage / Syslog / Trap	N/A

## Session Control

### Menu Path: Firewall > Session Control

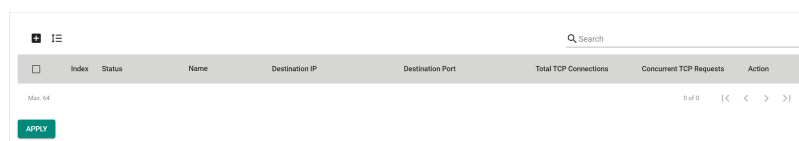
This page lets you configure session control policies to help protect backend hosts or services and avoid system abnormalities. Click **APPLY** to save your changes.

#### Note

If a TCP connection is successfully established, but no data is sent, the connection will be released after 8 seconds. If the interval between the last data transmission for the connection exceeds 300 seconds, the connection will also be released.

#### Limitations

You can configure up to 64 session control policies.



UI Setting	Description
<b>Index</b>	Shows the index of the policy. The index determines the order for processing policies.
<b>Status</b>	Shows whether the policy is enabled or disabled.

UI Setting	Description
<b>Name</b>	Shows the name of the policy.
<b>Destination IP</b>	Shows the destination IP addresses the policy applies to.
<b>Destination Port</b>	Shows the destination ports the policy applies to.
<b>Total TCP Connections</b>	Shows the total number of TCP connections this policy allows.
<b>Concurrent TCP Connections</b>	Shows the number of concurrent TCP connections this policy allows.
<b>Action</b>	Shows the action that will be taken for applicable traffic.

## Create Session Control Policy

### Menu Path: Firewall > Session Control

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

#### Note

IP Address and Port cannot both be set to Any.

#### Note

At least one TCP Connection Limitation must be defined.

### Create Session Control Policy

Index \*  
 1  
1 - 64

Status \*  
 Enabled

Name \*  
0 / 32

Severity \*  
 Warning

Log Destination  
 Local Storage

Action \*  
 Drop

TCP Destination \*

IP Address \* +

Port \* +

TCP Connection Limitation \* i



Total TCP Connections  
 1 - 9000 connections

Concurrent TCP Reques...  
 1 - 512 connections/s

CANCEL


CREATE

UI Setting	Description	Valid Range	Default Value
<b>Index</b>	Specify the index number for the policy. The index determines the order for processing policies.	1 to 64	Last used index plus 1
<b>Status</b>	Enable or disable the policy.	Enabled / Disabled	Enabled
<b>Name</b>	Specify a name for the policy.	1 to 32 characters	N/A
<b>Severity</b>	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	N/A

UI Setting	Description	Valid Range	Default Value
<b>Log Destination</b>	<p>Specify where to send firewall event logs. You can select multiple options.</p> <p><b>Syslog:</b> Firewall event logs will be sent to a syslog server. Refer to Diagnostics &gt; Event Logs and Notifications &gt; Syslog for more information.</p> <p><b>Trap:</b> Firewall event notifications will be sent to a trap server. Refer to Diagnostics &gt; SNMP Trap/Inform for more information.</p> <p><b>Local Storage:</b> Firewall event logs will be stored on local storage and will show up in the device's Event Log. Refer to Diagnostics &gt; Event Logs and Notifications &gt; Event Log for more information.</p>	Syslog / Trap / Local Storage	N/A
<b>Action</b>	<p>Select the action the firewall should take for traffic that matches this policy.</p> <p><b>Monitor:</b> The firewall will monitor packets that match the policy.</p> <p><b>Drop:</b> The firewall will drop packets that match the policy.</p>	Monitor / Drop	Drop
<b>IP Address</b>	<p>Select the IP addresses this policy will apply to. Select <b>Any</b> to check traffic from all IP addresses, or select a pre-defined object. You can also click the Add (  ) icon to create a new IP Address and Subnet object.</p> <p>Refer to Create Object for more information.</p>	Any / Drop-down list of IP Address and Subnet objects	N/A
<b>Port</b>	<p>Select the ports this policy will apply to. Select <b>Any</b> to check traffic from all ports, or select a pre-defined object. You can also click the Add (  ) icon to create a new User-defined Service object.</p> <p>Refer to Create Object for more information.</p>	Any / Drop-down list of port-based User-defined Service objects	N/A
<b>Total TCP Connection</b>	Specify the total allowed number of TCP connections.	1 to 9000	N/A
<b>Concurrent TCP Request</b>	Specify the total allowed number of concurrent TCP requests.	1 to 512	N/A

## Edit Session Control Policy

### Menu Path: Firewall > Session Control

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



**Note**

IP Address and Port cannot both be set to Any.

**Note**

At least one TCP Connection Limitation must be defined.

**Edit Session Control Policy**

Index \*  
1  
1 - 64

Status \*  
Enabled

Name \*  
Test  
4 / 32

Severity \*  
Warning

Log Destination  
Local Storage

Action \*  
Drop

TCP Destination \*  
IP Address \*  
test



Port \*  
Any

TCP Connection Limitation \*  
Total TCP Connections  
50  
1 - 9000 connections

Concurrent TCP Reques...  
1 - 512 connections/s

CANCEL APPLY

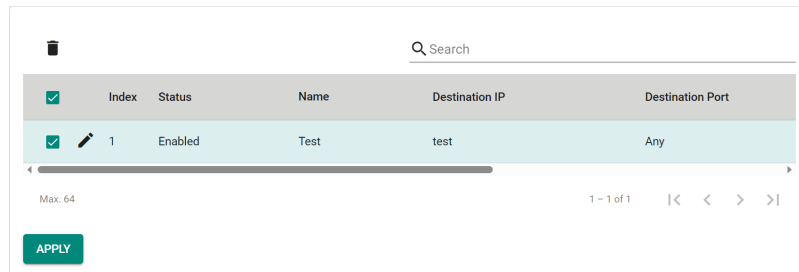
UI Setting	Description	Valid Range	Default Value
<b>Index</b>	Specify the index number for the policy. The index determines the order for processing policies.	1 to 64	Last used index plus 1

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the policy.	Enabled / Disabled	Enabled
<b>Name</b>	Specify a name for the policy.	1 to 32 characters	N/A
<b>Severity</b>	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	N/A
<b>Log Destination</b>	Specify where to send firewall event logs. You can select multiple options. <b>Syslog:</b> Firewall event logs will be sent to a syslog server. Refer to Diagnostics > Event Logs and Notifications > Syslog for more information. <b>Trap:</b> Firewall event notifications will be sent to a trap server. Refer to Diagnostics > SNMP Trap/Inform for more information. <b>Local Storage:</b> Firewall event logs will be stored on local storage and will show up in the device's Event Log. Refer to Diagnostics > Event Logs and Notifications > Event Log for more information.	Syslog / Trap / Local Storage	N/A
<b>Action</b>	Select the action the firewall should take for traffic that matches this policy. <b>Monitor:</b> The firewall will monitor packets that match the policy. <b>Drop:</b> The firewall will drop packets that match the policy.	Monitor / Drop	Drop
<b>IP Address</b>	Select the IP addresses this policy will apply to. Select <b>Any</b> to check traffic from all IP addresses, or select a pre-defined object. You can also click the Add (  ) icon to create a new IP Address and Subnet object. Refer to Create Object for more information.	Any / Drop-down list of IP Address and Subnet objects	N/A
<b>Port</b>	Select the ports this policy will apply to. Select <b>Any</b> to check traffic from all ports, or select a pre-defined object. You can also click the Add (  ) icon to create a new User-defined Service object. Refer to Create Object for more information.	Any / Drop-down list of port-based User-defined Service objects	N/A
<b>Total TCP Connection</b>	Specify the total allowed number of TCP connections.	1 to 9000	N/A
<b>Concurrent TCP Request</b>	Specify the total allowed number of concurrent TCP requests.	1 to 512	N/A

## Delete Session Control Policy

### Menu Path: Firewall > Session Control

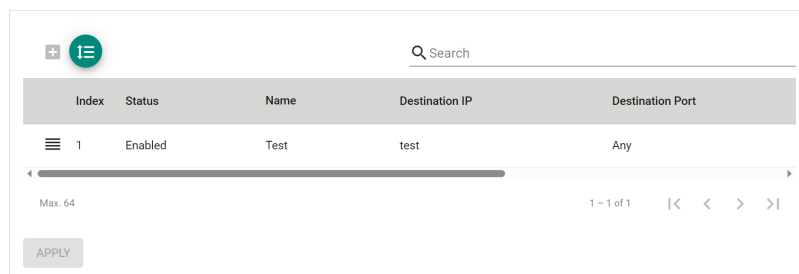
You can delete a policy by using the checkboxes to select the entries you want to delete, then clicking the **Delete** (🗑️) icon.



## Reorder Session Control Policies

### Menu Path: Firewall > Session Control

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



## DoS Policy

### Menu Path: Firewall > DoS Policy

This page lets you configure Denial of Service (DoS) protection features. You can configure different DoS functions for detecting abnormal packet formats or traffic flows, allowing your device to drop packets when it detects an abnormal packet format or identifies unusual traffic conditions.

## DoS Log Settings

**DoS Log Settings**

Log \* Severity \*

Disabled Emergency Log Destination

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Log</b>	Enable or disable DoS event logs.	Enabled / Disabled	Disabled
<b>Severity</b>	Select the severity level to assign to DoS-related events. Refer to the Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency
<b>Log Destination</b>	Specify where to send firewall event logs. You can select multiple options.  <b>Syslog:</b> Firewall event logs will be sent to a syslog server. Refer to Diagnostics > Event Logs and Notifications > Syslog for more information.  <b>Trap:</b> Firewall event notifications will be sent to a trap server. Refer to Diagnostics > SNMP Trap/Inform for more information.  <b>Local Storage:</b> Firewall event logs will be stored on local storage and will show up in the device's Event Log. Refer to Diagnostics > Event Logs and Notifications > Event Log for more information.	Local Storage / Syslog / Trap	N/A

## DoS Settings

### DoS Settings

All

### Session SYN Protection

TCP Sessions Without SYN i

### Port Scan Protection

Null Scan

Xmas Scan

NMAP-Xmas Scan

SYN/FIN Scan

FIN Scan

NMAP-ID Scan

SYN/RST Scan

### Flood Protection

ICMP-Flood

Limit

1000

1 - 4000 pkt/s

SYN-Flood

Limit

1000

1 - 4000 pkt/s

ARP-Flood

Limit

1000

1 - 2000 pkt/s

UDP-Flood

Limit

2000

1 - 8000 pkt/s

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>DoS Settings</b>	Toggle all DoS protection methods on or off.	All	N/A

UI Setting	Description	Valid Range	Default Value
<b>Session SYN Protection</b>	<p>Enable or disable session SYN protection methods.</p> <p><b>TCP Sessions Without SYN:</b> When enabled, this function will verify the SYN state within the TCP flag when establishing TCP sessions.</p> <p>If the SYN tag is missing in the initial packet, the system will drop the packet and block the connection. Running TCP sessions will be re-established to perform the check.</p> <div style="background-color: #fff9c4; padding: 10px; margin-top: 10px;"> <p><b>⚠ Warning</b></p> <p>When NAT is enabled for asymmetric network architectures, it is strongly advised to keep <b>TCP Sessions Without SYN</b> disabled to avoid unexpected disconnections.</p> </div>	TCP Sessions Without SYN	Checked for all methods
<b>Port Scan Protection</b>	<p>Enable or disable port-scan protection methods.</p>	Null Scan / Xmas Scan / NMAP-Xmas Scan / SYN/FIN Scan / FIN Scan / NMAP-ID Scan / SYN/RST Scan	Enabled for all methods
<b>Flood Protection</b>	<p>Enable or disable flood protection methods. When enabling a protection method, specify the limit in packets/second that will trigger the corresponding flood protection.</p> <div style="background-color: #e0e0e0; padding: 10px; margin-top: 10px;"> <p><b>✍ Note</b></p> <p>If <b>Accept All LAN Port Connections</b> is enabled in <b>Trusted Access</b>, <b>Flood Protection</b> will be disabled.</p> <p>Refer to <b>Security &gt; Device Security &gt; Trusted Access</b> for more information.</p> </div> <div style="background-color: #e0e0e0; padding: 10px; margin-top: 10px;"> <p><b>✍ Note</b></p> <p>For Flood Protection, each interface has an independent limit which does not affect the limits of other interfaces.</p> </div>	ICMP-Flood (1 to 4000) / SYN-Flood (1 to 4000) / ARP-Flood (1 to 2000) / UDP-Flood (1 to 8000)	<p>Enabled with Limit set to 1000 for ICMP-Flood, SYN-Flood, ARP-Flood</p> <p>Disabled with Limit set to 0 for UDP-Flood</p>

## Soft Lockdown Mode

**Menu Path: Firewall > Soft Lockdown Mode**

This page lets you configure Soft Lockdown Mode for your device. For more information on how this feature works, refer to [Soft Lockdown](#).

**Note**

Soft Lockdown Mode is a feature designed for railway applications and is only supported by the TN-4900 Series.

**Note**

In addition to the criteria defined in these settings, the device will enter Soft Lockdown Mode if any enabled critical service is no longer alive, and all enabled critical services must be alive to leave Soft Lockdown Mode.

The critical services that apply to Soft Lockdown Mode are as follows:

- DHCP Server (refer to Network Service > DHCP Server)
- DHCP Relay Agent (refer to Network Service > DHCP Server - DHCP Relay Agent)
- SNMP Server (refer to SNMP)
- Turbo Ring V2 (refer to Redundancy > Layer 2 Redundancy > Turbo Ring V2)

**Note**

If Soft Lockdown Mode and DHCP Server are both enabled, make sure at least one LAN interface's IP is within the DHCP server pool and at least one physical port is assigned to this LAN interface.

## Soft Lockdown Mode

### Soft Lockdown Status

Status  
**Not in Soft Lockdown Mode**

---

Enable \*  
Disabled ▼

Interface \* ▼

CPU utilization threshold \*  
70  
1 - 90 %

Free memory space threshold \*  
20  
1 - 50 %

Status monitoring interval \*  
1  
1 - 5 sec.

Failure cycles to enter lockdown mode \*  
5  
3 - 10

Normal cycles to leave lockdown mode \*  
5  
3 - 10

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Enable</b>	Enable/Disable use of the Soft Lockdown Mode feature.	Enabled/Disabled	Disable
<b>Interface</b>	Specify which interface Soft Lockdown Mode will apply to. When in Soft Lockdown Mode, all traffic on this interface (both ingress and egress) will be blocked.	Drop-down list of interfaces	N/A



UI Setting	Description	Valid Range	Default Value
<b>CPU utilization threshold</b>	Specify the maximum CPU utilization % allowed. If the CPU utilization % goes over this threshold, a failure will be triggered for the current cycle.	1 to 90%	70
<b>Free memory space threshold</b>	Specify the minimum free memory % allowed. If the free memory % goes below this threshold, a failure will be triggered for the current cycle.	1 to 50%	20
<b>Status monitoring interval</b>	Specify a cycle time in seconds to monitor CPU and memory usage for failure detection.	1 to 5 seconds	1
<b>Failure cycles to enter lockdown mode</b>	Specify the number of consecutive cycles with failures allowed before entering soft lockdown mode.	3 to 10	5
<b>Normal cycles to leave lockdown mode</b>	Specify the required number of normal consecutive cycles without failures to leave soft lockdown mode.	3 to 10	5

## Advanced Protection

### Menu Path: Firewall > Advanced Protection

This section lets you monitor and configure your device's advanced firewall features.

This section includes these pages:

- Dashboard
- Configuration
- Protocol Filter Policy
- ADP
- IPS

## Dashboard

### Menu Path: Firewall > Advanced Protection > Dashboard

This page lets you see an overview of your firewall's advanced protection activity with real-time event counters.

**Note**

Please note that available status displays may vary depending on the product and model, and whether an IPS license is installed or not.

## Information

This display shows the versions of the installed firewall engines and security packages currently installed on the device, as well as whether various functions are enabled.

The screenshot shows a user interface titled "Information" with the following data:

Package Version	Package Updated Time	Enforcement	IPS
6.0.0016	2023-08-10 05:46:47	Enabled	Enabled

Below this, it shows "IPS Operation Mode" set to "Prevention Mode".

Then, under "Engine Version", there is a scrollable list:

Engine Name	Version
IPS	2.0.0005
IPS Pattern	1.0.0038
Modbus/TCP	23.7.0021

UI Setting	Description
<b>Package Version</b>	Shows the version of the current Network Security Package installed on the device.
<b>Package Updated Time</b>	Shows when the current Network Security Package was installed.
<b>Enforcement</b>	Shows whether Protocol Filtering is enabled.
<b>IPS</b>	Shows whether IPS is enabled.
<b>IPS Operation Mode</b>	Shows which operation mode IPS is using.

UI Setting	Description
------------	-------------

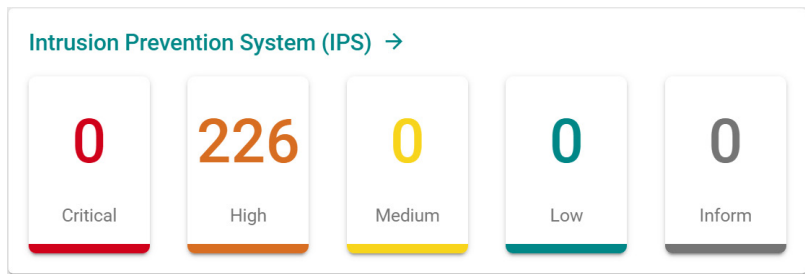
**Engine Version** Shows the versions of the different engines being used.

**Note**

Starting from v9.0 of the Network Security Package, when the IPS license expires, existing IPS patterns can still be used for IPS protection. However, the IPS patterns will not be updated and will remain at their current versions when you update the Network Security Package.

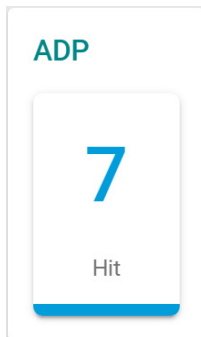
### Intrusion Prevention System (IPS)

This display shows the current number of Intrusion Prevention System (IPS) events. Clicking on an item will take you to a filtered view of the IPS event log. Refer to **Diagnostics > Event Logs and Notifications > Event Log - Firewall Log** for more information.



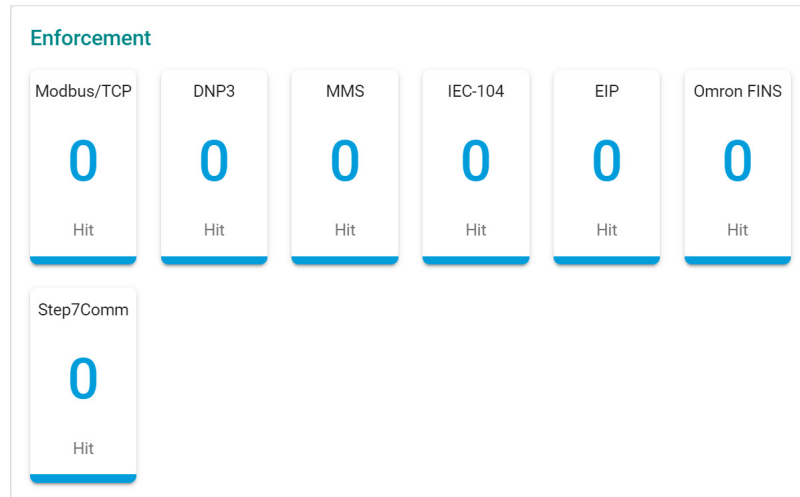
### ADP

This display shows the current number of Anomaly Detection and Prevention (ADP) events. Clicking on an item will take you to the ADP event log. Refer to **Diagnostics > Event Logs and Notifications > Event Log - Firewall Log** for more information.



## Enforcement

This display shows the current number of industrial protocol events. Clicking on an item will take you to a filtered view of the Protocol Filter Policy event log. Refer to **Diagnostics > Event Logs and Notifications > Event Log - Firewall Log** for more information.



## Configuration

**Menu Path: Firewall > Advanced Protection > Configuration**

This page lets you configure your application firewall's advanced protection settings.

This page includes these tabs:

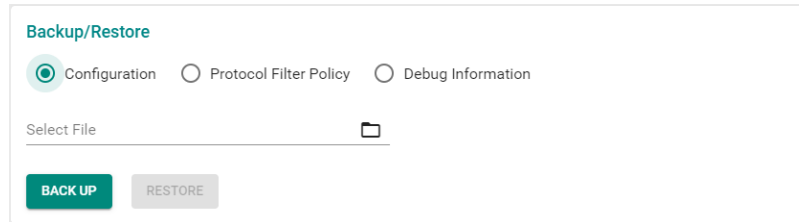
- Global Settings
- Protocol Filter Object
- Protocol Filter Profile

### Configuration - Global Settings

**Menu Path: Firewall > Advanced Protection > Configuration - Global Settings**

This page lets you configure global settings for your application firewall's advanced protection features. You can also back up and restore your advanced protection settings on this page.

## Backup/Restore



UI Setting	Description	Valid Range	Default Value
<b>Backup/Restore</b>	<p>Select which settings you want to back up or restore. If you want to back up your settings, click <b>BACK UP</b>.</p> <p><b>Configuration:</b> Back up/restore all settings on the <b>Firewall &gt; Advanced Protection &gt; Configuration</b> page.</p> <p><b>Protocol Filter Policy:</b> Back up/restore all policies on the <b>Firewall &gt; Advanced Protection &gt; Protocol Filter Policy</b> page.</p> <p><b>Debug Information:</b> Back up debug information for your firewall's advanced protection features.</p>	Configuration / Protocol Filter Policy / Debug Information	Configuration
<b>Select File</b> <b>(if Backup/Restore is Configuration or Protocol Filter Policy)</b>	<p>If you want to restore settings, click this field and select the settings file from your local computer, then click <b>RESTORE</b>.</p>	N/A	N/A

## Global Settings

### Note

Available settings will vary depending on your product model and whether an active IPS license is installed.

**Global Settings**

**Intrusion Prevention System (IPS)**

IPS \* IPS Operation Mode \*  
 Enabled Prevention Mode

**Enforcement**

Enforcement \* Action \*  
 Enabled Reset

Modbus/TCP Firewall \* Modbus/TCP ADP \* Modbus/TCP Service Port \*  
 Enabled Enabled 502  
1 - 65535, allow comma(,)

DNP3 Firewall \* DNP3 ADP \* DNP3 Service Port \*  
 Enabled Enabled 20000  
1 - 65535, allow comma(,)

MMS Firewall \* MMS Service Port \*  
 Enabled 102  
1 - 65535, allow comma(,)

IEC-104 Firewall \* IEC-104 ADP \* IEC-104 Service Port \*  
 Enabled Enabled 2404  
1 - 65535, allow comma(,)

EIP Firewall \* EIP ADP \* EIP Service Port \*  
 Enabled Enabled 44818  
1 - 65535, allow comma(,)

Omron FINS Firewall \* Omron FINS ADP \* Omron FINS Service Port \*  
 Enabled Enabled 9600  
1 - 65535, allow comma(,)

Step7Comm Firewall \* Step7Comm ADP \* Step7Comm Service Port \*  
 Enabled Enabled 102  
1 - 65535, allow comma(,)

**Troubleshooting**

Debug Logging \*  
 Enabled

**APPLY**

## Intrusion Prevention System (IPS)

UI Setting	Description	Valid Range	Default Value
<b>IPS</b>	Enable or disable intrusion prevention system (IPS) functionality.	Enabled / Disabled	Enabled
<b>IPS Operation Mode</b>	Select the IPS operation mode.	Prevention Mode / Detection Mode	Prevention Mode

## Enforcement

UI Setting	Description	Valid Range	Default Value
<b>Enforcement</b>	Enable or disable protocol filtering.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
<b>Action</b>	<p>Select the default action of the protocol filter when enforcement is enabled.</p> <p>The Event Log (Firewall Log) will display Policy ID '99999' when this default action is activated.</p> <p><b>Accept:</b> The firewall will accept packets when no defined Protocol Filter Policy matches. With this setting, no logs are recorded.</p> <p><b>Monitor:</b> The firewall will accept packets when no defined Protocol Filter Policy matches. With this setting, each packet of an identified application protocol will have a corresponding Event Log entry.</p> <p><b>Reset:</b> The firewall will drop packets when no defined Protocol Filter Policy matches. With this setting, only the first packet of an identified application protocol will be recorded in Event Log.</p>	Accept / Monitor / Reset	Reset
<b>Modbus/TCP Firewall</b>	Enable or disable the Modbus/TCP protocol filter engine.	Enabled / Disabled	Enabled
<b>Modbus/TCP ADP</b>	Enable or disable ADP for Modbus/TCP traffic.	Enabled / Disabled	Enabled
<b>Modbus/TCP Service Port</b>	Specify the service port for Modbus/TCP traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	502
<b>DNP3 Firewall</b>	Enable or disable the DNP3 protocol filter engine.	Enabled / Disabled	Enabled
<b>DNP3 ADP</b>	Enable or disable ADP for DNP3 traffic.	Enabled / Disabled	Enabled
<b>DNP3 Service Port</b>	Specify the service port for DNP3 traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	20000
<b>MMS Firewall</b>	Enable or disable the MMS protocol filter engine.	Enabled / Disabled	Enabled
<b>MMS Service Port</b>	Specify the service port for MMS traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	102
<b>IEC-104 Firewall</b>	Enable or disable the IEC-104 protocol filter engine.	Enabled / Disabled	Enabled
<b>IEC-104 ADP</b>	Enable or disable ADP for IEC-104 traffic.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
<b>IEC-104 Service Port</b>	Specify the service port for IEC-104 traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	2404
<b>GOOSE Firewall</b>	Enable or disable the GOOSE protocol filter engine.	Enabled / Disabled	Enabled
<b>EIP Firewall</b>	Enable or disable the EIP protocol filter engine.	Enabled / Disabled	Enabled
<b>EIP ADP</b>	Enable or disable ADP for EIP traffic.	Enabled / Disabled	Enabled
<b>EIP Service Port</b>	Specify the service port for EIP traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	44818
<b>Omron FINS Firewall</b>	Enable or disable the Omron FINS protocol filter engine.	Enabled / Disabled	Enabled
<b>Omron FINS ADP</b>	Enable or disable ADP for Omron FINS traffic.	Enabled / Disabled	Enabled
<b>Omron FINS Service Port</b>	Specify the service port for Omron FINS traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	9600
<b>Step7Comm Firewall</b>	Enable or disable the Step7Comm protocol filter engine.	Enabled / Disabled	Enabled
<b>Step7Comm ADP</b>	Enable or disable ADP for Step7Comm traffic.	Enabled / Disabled	Enabled
<b>Step7Comm Service Port</b>	Specify the service port for Step7Comm traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	102
<b>TRDP Firewall</b>	Enable or disable the TRDP protocol filter engine.	Enabled / Disabled	Enabled
<b>TRDP Service Port</b>	Specify the service port for TRDP traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	17224, 17225

## Troubleshooting

UI Setting	Description	Valid Range	Default Value
<b>Debug Logging</b>	Enable or disable debug logging for troubleshooting.	Enables / Disabled	Disabled



## Protocol Filter Object

### Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Object











This page lets you create and manage protocol filter objects, which can simplify creation and maintenance of protocol filter policies.

#### Note

Available protocols may vary across different product models and versions.

#### Limitations

You can create up to 64 protocol filter objects.

<input type="checkbox"/>	Protocol Filter Object	Category	Protocol Filter Profile
<input type="checkbox"/>	 Modbus_readwrite_test	Modbus/TCP	ReadWrite
<input type="checkbox"/>	 Modbus_Read_Only	Modbus/TCP	ReadOnly
<input type="checkbox"/>	 MOXA_test	Modbus/TCP	ReadOnly
<input type="checkbox"/>	 Modbus_Manual	Modbus/TCP	Manual
<input type="checkbox"/>	 Modbus_customized	Modbus/TCP	Manual
<input type="checkbox"/>	 test	Modbus/TCP	Manual
<input type="checkbox"/>	 Modbus_write	Modbus/TCP	WriteOnly
<input type="checkbox"/>	 EIP_Test	EIP	JasonTest
<input type="checkbox"/>	 Omron_Test	Omron FINS	Manual
<input type="checkbox"/>	 FINSTest	Step7Comm	Manual

Max. 64 1 - 10 of 10 < >

#### UI Setting

#### Description

##### Protocol Filter Object

Shows the name of the object

##### Category

Shows the protocol category of the object.

UI Setting	Description
------------	-------------

<b>Protocol Filter Profile</b>	Shows which protocol filter profile the object uses.
--------------------------------	--

### Protocol Filter Object - Create Object

#### Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Object


Clicking the **Add (+)** icon on the **Firewall > Advanced Protection > Configuration - Protocol Filter Object** page will open this dialog box. This dialog lets you create a protocol filter object. Click **CREATE** to save your changes and add the new object.

#### Create Object - Modbus/TCP

If **Modbus/TCP** is selected for the **Category**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Name</b>	Specify a name for the object.	1 to 64 characters	N/A
-------------	--------------------------------	--------------------	-----

UI Setting	Description	Valid Range	Default Value
<b>Category</b>	<p>Select a protocol for this object.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Slave ID</b>	<p>Specify the Modbus slave ID. Leave this field blank to represent any ID.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>The Slave ID is used to identify Modbus devices. This ID can be used to communicate via devices such as bridges and gateways which use a single IP address to support multiple independent end units.</p> </div>	0 to 255 / 0x00 to 0xFF	Any
<b>Protocol Filter Profile</b>	<p>Select preset protocol filter profile or a user-configured protocol filter profile to use for this protocol filter object.</p> <p><b>Read Only:</b> Use a set of commonly used function codes associated with read-only access.</p> <p><b>Write Only:</b> Use a set of commonly used function codes associated with write-only access.</p> <p><b>Read/Write:</b> Use a set of commonly used function codes associated with read/write access.</p> <p><b>Manual:</b> Manually enter the settings for this object.</p> <p>Refer to <b>Firewall &gt; Advanced Protection &gt; Configuration - Protocol Filter Profile</b> for more information on creating protocol filter profiles.</p>	Read Only / Write Only / Read/Write / Drop-down list of related protocol filter profiles / Manual	N/A
<b>Function Code</b>	<p>Shows which function codes will be used for the object, based on the selected <b>Protocol Filter Profile</b>.</p> <p>If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b>, select which function codes to use for this object. You can select multiple options.</p>	Drop-down list of function codes	Depends on the selected <b>Protocol Filter Profile</b>

UI Setting	Description	Valid Range	Default Value
<b>PLC Address Base 1</b> (if only one Function Code is selected)	Select whether the PLC's starting address should start from 0x00 or 0x01. This should be set based on your PLCs to ensure DPI filters the correct addresses and values. <b>Enabled:</b> The PLC's starting address starts at 0x01. <b>Disabled:</b> The PLC's starting address starts at 0x00.	Enabled / Disabled	Disabled
<b>Filter Type</b> (if only one Function Code is selected)	Select the filter type to use. <b>None:</b> Filter traffic by specified function codes. <b>Address Range:</b> Filter traffic by specified PLC register addresses. <b>Data Value:</b> Filter the traffic by specified data values in the registers.	None / Address Range / Data Value	None
<b>Address Range</b> (if Filter Type is Address Range)	Define the address range to use for the filter. You can enter the address range in decimal or hexadecimal format.	0 to 65535 / 0x0000 to 0xFFFF	N/A
<b>Start Address</b> (if Filter Type is Data Value)	Specify the starting address for the PLC register address. You can enter the address in decimal or hexadecimal format.	0 to 65535 / 0x0000 to 0xFFFF	N/A
<b>Value</b> (if Filter Type is Data Value)	Specify a data value to filter for. You can enter up to 16 bits (2 bytes) of binary data for the data value.	0 to 1111111111111111 (binary data)	N/A

### Create Object - DNP3

If **DNP3** is selected for the **Category**, these settings will appear.

**Create Object**

Name \*  0 / 64

Category \*  
DNP3 ▼

Protocol Filter Profile \*  
Manual ▼

Source Address  
0 - 65535 or 0x0000 - 0xFFFF

Destination Address  
0 - 65535 or 0x0000 - 0xFFFF

Application Function Code \* ▼

Group  
0 - 255 or 0x00 - 0xFF

Variation  
0 - 255 or 0x00 - 0xFF

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the object.	1 to 64 characters	N/A
<b>Category</b>	Select a protocol for this object. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Protocol Filter Profile</b>	Select a user-configured protocol filter profile to use for this protocol filter object. <p><b>Manual:</b> Manually enter the settings for this object.</p> <p>Refer to <b>Firewall &gt; Advanced Protection &gt; Configuration - Protocol Filter Profile</b> for more information on creating protocol filter profiles.</p>	Drop-down list of related protocol filter profiles / Manual	N/A
<b>Source Address</b>	Shows the source address to check for in DNP3 packets, based on the selected <b>Protocol Filter Profile</b> . <p>If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b>, specify the source address to check for in DNP3 packets.</p>	0 to 65535 / 0x0000 to 0xFFFF	Depends on the selected <b>Protocol Filter Profile</b>

UI Setting	Description	Valid Range	Default Value
<b>Destination Address</b>	Shows the destination address to check for in DNP3 packets, based on the selected <b>Protocol Filter Profile</b> .  If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , specify the destination address to check for in DNP3 packets.	0 to 65535 / 0x0000 to 0xFFFF	Depends on the selected <b>Protocol Filter Profile</b>
<b>Application Function Code</b>	Shows which function code will be used for the object, based on the selected <b>Protocol Filter Profile</b> .  If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , select which function code to use for this object.	Drop-down list of function codes	Depends on the selected <b>Protocol Filter Profile</b>
<b>Group</b>	Shows the group to use to classify types within a message, based on the selected <b>Protocol Filter Profile</b> .  If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , specify the function code to use for this object.	0 to 255 or 0x00 to 0xFF	Depends on the selected <b>Protocol Filter Profile</b>
<b>Variation</b>	Shows the variation to use for encoding formats, based on the selected <b>Protocol Filter Profile</b> .  If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , specify the variation to use for this object.	0 to 255 or 0x00 to 0xFF	Depends on the selected <b>Protocol Filter Profile</b>

## Create Object - MMS

If **MMS** is selected for the **Category**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the object.	1 to 64 characters	N/A
<b>Category</b>	Select a protocol for this object. <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Protocol Filter Profile</b>	Select preset protocol filter profile or a user-configured protocol filter profile to use for this protocol filter object. <p><b>Manual:</b> Manually enter the settings for this object.</p> <p>Refer to <b>Firewall &gt; Advanced Protection &gt; Configuration - Protocol Filter Profile</b> for more information on creating protocol filter profiles.</p>	Identify Service / Read Service / Write Service / Report Service / File Operation Service / Journal Service / Drop-down list of related protocol filter profiles / Manual	N/A
<b>Device</b>	Specify a device name for the object.		N/A
<b>Item ID</b>	Specify an item ID for the object.		N/A

UI Setting	Description	Valid Range	Default Value
<b>Command Type</b>	<p>Shows which MMS command type will be used for the object, based on the selected <b>Protocol Filter Profile</b>.</p> <p>If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b>, select the command type to use for the object.</p> <p>Refer to <b>MMS Command Types</b> for an overview of all command types.</p>	Drop-down list of MMS command types	Depends on the selected <b>Protocol Filter Profile</b>
<b>Service</b>	<p>Shows which service will be used for the object, based on the selected <b>Protocol Filter Profile</b>.</p> <p>If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b>, select the service to use for the object.</p>	Any / Confirmed Request / Confirmed Response / Unconfirmed	Depends on the selected <b>Protocol Filter Profile</b>
<b>Service Operation</b>	<p>Shows which service operations will be used for the object, based on the selected <b>Protocol Filter Profile</b>.</p> <p>If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b>, select the service operations to use for the object. You can select multiple options.</p> <p>Refer to <b>MMS Service Operation List</b> for an overview of all service operations.</p>	Drop-down list of service operations	Depends on the selected <b>Protocol Filter Profile</b>
<b>MMS Data Type</b>	<p>Specify which MMS data types to use for the object. You can select multiple options.</p> <p>For each service operation, specify the values to use. You can specify multiple values by separating them with a comma.</p>	Drop-down list of MMS data types 0 to 65535	N/A

## Create Object - IEC-104

If **IEC-104** is selected for the **Category**, these settings will appear.



**Create Object**

Name \*  0 / 64

Category \*  
IEC-104 ▾

Protocol Filter Profile \*  
Manual ▾

Cause of Transmission \* ▾

Type Identification \* ▾

Originator Address  
 0 - 255 or 0x00 - 0xFF

Common Address  
 0 - 65535 or 0x0000 - 0xFFFF

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the object.	1 to 64 characters	N/A
<b>Category</b>	Select a protocol for this object. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Protocol Filter Profile</b>	Select a user-configured protocol filter profile to use for this protocol filter object.  <b>Manual:</b> Manually enter the settings for this object.  Refer to <b>Firewall &gt; Advanced Protection &gt; Configuration - Protocol Filter Profile</b> for more information on creating protocol filter profiles.	Identify Service / Read Service / Write Service / Report Service / File Operation Service / Journal Service / Drop-down list of related protocol filter profiles / Manual	N/A

UI Setting	Description	Valid Range	Default Value
<b>Cause of Transmission</b>	<p>Shows which IEC-104 cause of transmission code will be used for the object, based on the selected <b>Protocol Filter Profile</b>.</p> <p>If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b>, select the cause to use for the object.</p> <p>Refer to the <a href="#">IEC-104 Cause of Transmission List</a> for an overview of the different codes and corresponding descriptions.</p>	Drop-down list of IEC-104 cause of transmission codes	Depends on the selected <b>Protocol Filter Profile</b>
<b>Type Identification</b>	<p>Shows which IEC-104 type identification code will be used for the object, based on the selected <b>Protocol Filter Profile</b>.</p> <p>If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b>, select the type to use for the object.</p> <p>Refer to the IEC-104 Type Identification List for an overview of the different codes and corresponding descriptions.</p>	Drop-down list of IEC-104 type identification codes	Depends on the selected <b>Protocol Filter Profile</b>
<b>Originator Address</b>	<p>Shows which originator address will be used for the object, based on the selected <b>Protocol Filter Profile</b>.</p> <p>If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b>, specify the address to use for the object.</p>	0 to 255 / 0x00 to 0xFF	Depends on the selected <b>Protocol Filter Profile</b>
<b>Common Address</b>	<p>Shows which common address will be used for the object, based on the selected <b>Protocol Filter Profile</b>.</p> <p>If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b>, specify the address to use for the object.</p>	0 to 65535 / 0x0000 to 0xFFFF	Depends on the selected <b>Protocol Filter Profile</b>

## Create Object - EIP

If **EIP** is selected for the **Category**, these settings will appear.

### Create Object

Name \* 0 / 64

---

Category \*  
EIP ▼

---

Protocol Filter Profile \*  
Manual ▼

---

Command Code  
0 - 65535, allow comma(,)

---

Type ID  
0 - 65535, allow comma(,)

---

Device Type  
0 - 65535, allow comma(,)

---

Vendor ID  
0 - 65535, allow comma(,)

---

CANCEL
CREATE

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the object.	1 to 64 characters	N/A
<b>Category</b>	Select a protocol for this object. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p> <b>Note</b> Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Protocol Filter Profile</b>	Select a user-configured protocol filter profile to use for this protocol filter object. <b>Manual:</b> Manually enter the settings for this object.  Refer to <b>Firewall &gt; Advanced Protection &gt; Configuration - Protocol Filter Profile</b> for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A

UI Setting	Description	Valid Range	Default Value
<b>Command Code</b>	Shows the EIP command codes that will be used for the object, based on the selected <b>Protocol Filter Profile</b> .  If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , specify the command codes to use for this object. You can specify multiple values by separating them with a comma.	0 - 65535	Depends on the selected <b>Protocol Filter Profile</b>
<b>Type ID</b>	Shows the type IDs that will be used for the object, based on the selected <b>Protocol Filter Profile</b> .  If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , specify the type IDs to use for this object. You can specify multiple values by separating them with a comma.	0 - 65535	Depends on the selected <b>Protocol Filter Profile</b>
<b>Device Type</b>	Shows the device types that will be used for the object, based on the selected <b>Protocol Filter Profile</b> .  If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , specify the device types to use for this object. You can specify multiple values by separating them with a comma.	0 - 65535	Depends on the selected <b>Protocol Filter Profile</b>
<b>Vendor ID</b>	Specify the vendor IDs to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A

### Create Object - Omron FINS

If **Omron FINS** is selected for the **Category**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the object.	1 to 64 characters	N/A
<b>Category</b>	Select a protocol for this object. <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Protocol Filter Profile</b>	Select a user-configured protocol filter profile to use for this protocol filter object. <b>Manual:</b> Manually enter the settings for this object. Refer to <b>Firewall &gt; Advanced Protection &gt; Configuration - Protocol Filter Profile</b> for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A
<b>TCP Command</b>	Shows the TCP command codes that will be used for the object, based on the selected <b>Protocol Filter Profile</b> . If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , specify the command codes to use for this object. You can specify multiple values by separating them with a comma.	0 to 4294967295	Depends on the selected <b>Protocol Filter Profile</b>

UI Setting	Description	Valid Range	Default Value
<b>Command Code</b>	Shows the command codes that will be used for the object, based on the selected <b>Protocol Filter Profile</b> .  If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , specify the command codes to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	Depends on the selected <b>Protocol Filter Profile</b>
<b>Error Code</b>	Shows the error codes that will be used for the object, based on the selected <b>Protocol Filter Profile</b> .  If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , specify the error codes to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	Depends on the selected <b>Protocol Filter Profile</b>
<b>Client Node Address</b>	Specify the client node addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 4294967295	N/A
<b>Server Node Address</b>	Specify the server node addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 4294967295	N/A
<b>File Position</b>	Specify the file positions to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A
<b>File Position Begin Address</b>	Specify the file position begin addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A
<b>Begin Address</b>	Specify the begin addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A
<b>Record Begin Address</b>	Specify the record begin addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A

### Create Object - Step7Comm

If **Step7Comm** is selected for the **Category**, these settings will appear.

**Create Object**

Name \*  0 / 64

Category \*  
Step7Comm ▼

Protocol Filter Profile \*  
Manual ▼

ROSCTR  
USER DATA ▼

Function Group  
0 - 15 or 0x0 - 0xF

Sub-function  
0 - 255 or 0x00 - 0xFF

CANCEL CREATE

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the object.	1 to 64 characters	N/A
<b>Category</b>	Select a protocol for this object. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Protocol Filter Profile</b>	Select a user-configured protocol filter profile to use for this protocol filter object. <p><b>Manual:</b> Manually enter the settings for this object.</p> <p>Refer to <b>Firewall &gt; Advanced Protection &gt; Configuration - Protocol Filter Profile</b> for more information on creating protocol filter profiles.</p>	Drop-down list of related protocol filter profiles / Manual	N/A
<b>ROSCTR</b>	Shows the ROSCTR control that will be used for the object, based on the selected <b>Protocol Filter Profile</b> . <p>If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b>, specify the ROSCTR control to use for this object.</p>	ANY / JOB / USER DATA	Depends on the selected <b>Protocol Filter Profile</b>

UI Setting	Description	Valid Range	Default Value
<b>Function</b> (if ROSCTR is JOB)	Shows the function code that will be used for the object, based on the selected <b>Protocol Filter Profile</b> . If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , specify the function code to use for this object.	0 to 255 / 0x00 to 0xFF	Depends on the selected <b>Protocol Filter Profile</b>
<b>Function Group</b> (if ROSCTR is USER DATA)	Shows the function group that will be used for the object, based on the selected <b>Protocol Filter Profile</b> . If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , specify the function group to use for this object.	0 to 15 / 0x0 to 0xF	Depends on the selected <b>Protocol Filter Profile</b>
<b>Sub-function</b> (if ROSCTR is USER DATA)	Shows the sub-function group that will be used for the object, based on the selected <b>Protocol Filter Profile</b> . If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , specify the sub-function code to use for this object.	0 to 255 / 0x00 to 0xFF	Depends on the selected <b>Protocol Filter Profile</b>

## Create Object - TRDP

If **TRDP** is selected for the **Category**, these settings will appear.

### Create Object

Name \* 0 / 64

Category \*  
TRDP ▼


Protocol Filter Profile  
Manual ▼

Message Type \* ▼

Communication Iden... ▼

CANCEL
CREATE



UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the object.	1 to 64 characters	N/A
<b>Category</b>	Select a protocol for this object.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Protocol Filter Profile</b>	Select a preset protocol filter profile or a user-configured protocol filter profile to use for this protocol filter object.  <b>Manual:</b> Manually enter the settings for this object.  Refer to <b>TRDP Protocol Filter Profiles</b> for more information on TRDP presets.  Refer to <b>Firewall &gt; Advanced Protection &gt; Configuration - Protocol Filter Profile</b> for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A
<b>Message Type</b>	Shows which message types will be used for the object, based on the selected <b>Protocol Filter Profile</b> .  If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , select which message types to use for this object. You can select multiple options.  Refer to <b>TRDP Message Types</b> for more information.	Drop-down list of message types	Depends on the selected <b>Protocol Filter Profile</b>
<b>Communication Identifier</b>	Shows which communication identifiers will be used for the object, based on the selected <b>Protocol Filter Profile</b> .  If <b>Manual</b> is selected for the <b>Protocol Filter Profile</b> , select which communication identifiers to use for this object. You can select multiple options. The last option in the list lets you add your own communication identifiers. You can specify multiple values by separating them with a comma.  Refer to <b>IEC 61375-2-3 Communication Identifiers</b> for more information.	Drop-down list of communication identifiers  1 to 4294967295	Depends on the selected <b>Protocol Filter Profile</b>

## Create Object - OPC UA

If **OPC UA** is selected for the **Category**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the object.	1 to 64 characters	N/A
<b>Category</b>	Select a protocol for this object. <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Protocol Filter Profile</b>	Select a preset protocol filter profile or a user-configured protocol filter profile to use for this protocol filter object. <p><b>Manual:</b> Manually enter the settings for this object.</p> <p>Refer to <b>Firewall &gt; Advanced Protection &gt; Configuration - Protocol Filter Profile</b> for more information on creating protocol filter profiles.</p>	Drop-down list of related protocol filter profiles / Manual	N/A

### Create Object - MELSEC


If **MELSEC** is selected for the **Category**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the object. Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	1 to 64 characters	N/A
<b>Category</b>	Select a protocol for this object.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Protocol Filter Profile</b>	Select a preset protocol filter profile or a user-configured protocol filter profile to use for this protocol filter object.  <b>Manual:</b> Manually enter the settings for this object.  Refer to <b>Firewall &gt; Advanced Protection &gt; Configuration - Protocol Filter Profile</b> for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A

### Create Object - Step7Plus

If **Step7Plus** is selected for the **Category**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the object. Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	1 to 64 characters	N/A

UI Setting	Description	Valid Range	Default Value
<b>Category</b>	Select a protocol for this object.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> <b>Note</b> Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Protocol Filter Profile</b>	Select a preset protocol filter profile or a user-configured protocol filter profile to use for this protocol filter object.  <b>Manual:</b> Manually enter the settings for this object.  Refer to <b>Firewall &gt; Advanced Protection &gt; Configuration - Protocol Filter Profile</b> for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A

## Protocol Filter Profile

### Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Profile







This page lets you create and manage protocol filter profiles to simplify maintaining protocol-related settings. Protocol filter profiles can be used when creating protocol filter objects, and a single profile can be used in multiple protocol filter objects.

#### Note

Available protocols may vary across different product models and versions.

#### Limitations

You can create up to 50 protocol filter profiles.

		Q Search
<input type="checkbox"/>	Protocol Filter Profile	Category
<input type="checkbox"/>	 readcoilstest	Modbus/TCP
<input type="checkbox"/>	 ddd	Modbus/TCP
<input type="checkbox"/>	 EIPTest	EIP
<input type="checkbox"/>	 DNP3Test	DNP3
<input type="checkbox"/>	 TestOmron	Omron FINS
<input type="checkbox"/>	 TestMMS	MMS

Max. 50 1 - 6 of 6 < >

UI Setting	Description
<b>Protocol Filter Profile</b>	Shows the name of the profile.
<b>Category</b>	Shows the protocol category of the profile.

### Protocol Filter Profile - Create Profile

#### Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Profile

Clicking the **Add (+)** icon on the **Firewall > Advanced Protection > Configuration - Protocol Filter Profile** page will open this dialog box. This dialog lets you create a protocol filter profile. Click **CREATE** to save your changes and add the new profile.

#### Create Profile - Modbus/TCP

If **Modbus/TCP** is selected for the **Category**, these settings will appear.

### Create Profile

Name \*  0 / 64

Category \*  
Modbus/TCP ▼

Function Code \* ▼

CANCEL
CREATE

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the profile.	1 to 64 characters	N/A
<b>Category</b>	Select a protocol for this profile. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b> Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Function Code</b>	Select which function codes to use for this profile. You can select multiple options.	Drop-down list of function codes	N/A

### Create Profile - DNP3

If **DNP3** is selected for the **Category**, these settings will appear.

### Create Profile

Name \*  
 0 / 64

Category \*  
 DNP3 ▼

Source Address  
  
 0 - 65535 or 0x0000 - 0xFFFF

Destination Address  
  
 0 - 65535 or 0x0000 - 0xFFFF

Application Function Code \* ▼

Group  
  
 0 - 255 or 0x00 - 0xFF

Variation  
  
 0 - 255 or 0x00 - 0xFF

CANCEL CREATE

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the profile.	1 to 64 characters	N/A
<b>Category</b>	Select a protocol for this profile.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
	<div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b></p> <p>Available settings will vary depending on your product model.</p> </div>		
<b>Source Address</b>	Specify the source address to check for in DNP3 packets.	0 to 65535 / 0x0000 to 0xFFFF	N/A

UI Setting	Description	Valid Range	Default Value
<b>Destination Address</b>	Specify the destination address to check for in DNP3 packets.	0 to 65535 / 0x0000 to 0xFFFF	N/A
<b>Application Function Code</b>	Select which function code to use for this profile.	Drop-down list of function codes	N/A
<b>Group</b>	Specify the function code to use for this profile.	0 to 255 or 0x00 to 0xFF	N/A
<b>Variation</b>	Specify the variation to use for this profile.	0 to 255 or 0x00 to 0xFF	N/A

### Create Profile - MMS

If **MMS** is selected for the **Category**, these settings will appear.

#### Create Profile

Name \*  0 / 64

Category \*  
MMS ▼

Common Type \* ▼


Service \* ▼

Service Operation \* ▼

CANCEL CREATE

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the profile.	1 to 64 characters	N/A



UI Setting	Description	Valid Range	Default Value
<b>Category</b>	Select a protocol for this profile.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> <b>Note</b> Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Command Type</b>	Select the command type to use for the profile.  Refer to <b>MMS Command Types</b> for an overview of all command types.	Drop-down list of MMS command types	N/A
<b>Service</b>	Select the service to use for the profile.	Any / Confirmed Request / Confirmed Response / Unconfirmed	N/A
<b>Service Operation</b>	Select the service operations to use for the profile. You can select multiple options.  Refer to <b>MMS Service Operation List</b> for an overview of all service operations.	Drop-down list of service operations	N/A

### Create Profile - IEC-104

If **IEC-104** is selected for the **Category**, these settings will appear.

### Create Profile

Name \*  0 / 64

Category \*  
IEC-104 ▼

Cause of Transmission \* ▼

Type Identification \* ▼

Originator Address  
0 - 255 or 0x00 - 0xFF

Common Address  
0 - 65535 or 0x0000 - 0xFFFF

CANCEL CREATE

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the profile.	1 to 64 characters	N/A
<b>Category</b>	Select a protocol for this profile. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Cause of Transmission</b>	Select the IEC-104 cause of transmission code to use for the profile. <p>Refer to the <a href="#">IEC-104 Cause of Transmission List</a> for an overview of the different codes and corresponding descriptions.</p>	Drop-down list of IEC-104 cause of transmission codes	N/A

UI Setting	Description	Valid Range	Default Value
<b>Type Identification</b>	Select the IEC-104 type identification code to use for the profile.  Refer to the IEC-104 Type Identification List for an overview of the different codes and corresponding descriptions.	Drop-down list of IEC-104 type identification codes	N/A
<b>Originator Address</b>	Specify the originator address to use for the profile.	0 to 255 / 0x00 to 0xFF	N/A
<b>Common Address</b>	Specify the common address to use for the profile.	0 to 65535 / 0x0000 to 0xFFFF	N/A

### Create Profile - EIP

If **EIP** is selected for the **Category**, these settings will appear.

#### Create Profile

Name \*

0 / 64

Category \*

Command Code

0 - 65535, allow comma(,)

Type ID

0 - 65535, allow comma(,)

Device Type

0 - 65535, allow comma(,)

CANCEL CREATE

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the profile.	1 to 64 characters	N/A

UI Setting	Description	Valid Range	Default Value
<b>Category</b>	Select a protocol for this profile.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Command Code</b>	Specify the command codes to use for this profile. You can specify multiple values by separating them with a comma.	0 - 65535	N/A
<b>Type ID</b>	Specify the type IDs to use for this profile. You can specify multiple values by separating them with a comma.	0 - 65535	N/A
<b>Device Type</b>	Specify the device types to use for this profile. You can specify multiple values by separating them with a comma.	0 - 65535	N/A

### Create Profile - Omron FINS

If **Omron FINS** is selected for the **Category**, these settings will appear.

**Create Profile**

Name \*  0 / 64

Category   
 Omron FINS ▼


TCP Command    
 0 - 4294967295, allow comma(,)

Command Code    
 0 - 65535, allow comma(,)

Error Code    
 0 - 4294967295, allow comma(,)

CANCEL CREATE

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the profile.	1 to 64 characters	N/A

UI Setting	Description	Valid Range	Default Value
<b>Category</b>	Select a protocol for this profile.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> <b>Note</b> Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>TCP Command</b>	Specify the TCP command codes to use for this profile. You can specify multiple values by separating them with a comma.	0 to 4294967295	N/A
<b>Command Code</b>	Specify the command codes to use for this profile. You can specify multiple values by separating them with a comma.	0 to 65535	N/A
<b>Error Code</b>	Specify the error codes to use for this profile. You can specify multiple values by separating them with a comma.	0 to 65535	N/A

### Create Profile - Step7Comm

If **Step7Comm** is selected for the **Category**, these settings will appear.

### Create Profile

Name \*  
  
0 / 64

Category \*  
Step7Comm ▼

ROSCTR  
USER DATA ▼

Function Group  
  
0 - 15 or 0x0 - 0xF

Sub-function  
  
0 - 255 or 0x00 - 0xFF

CANCEL
CREATE

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the profile.	1 to 64 characters	N/A
<b>Category</b>	Select a protocol for this profile. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>ROSCTR</b>	Specify the ROSCTR control to use for this profile.	ANY / JOB / USER DATA	N/A
<b>Function (if ROSCTR is JOB)</b>	Specify the function code to use for this profile.	0 to 255 / 0x00 to 0xFF	N/A

UI Setting	Description	Valid Range	Default Value
<b>Function Group</b> (if ROSCTR is USER DATA)	Specify the function group to use for this profile.	0 to 15 / 0x0 to 0xF	N/A
<b>Sub-function</b> (if ROSCTR is USER DATA)	Specify the sub-function code to use for this profile.	0 to 255 / 0x00 to 0xFF	N/A

### Create Profile - TRDP

If **TRDP** is selected for the **Category**, these settings will appear.

#### Create Profile

Name \*

0 / 64

Category \* ▼


TRDP

Message Type \* ▼

Communication Iden... ▼

CANCEL CREATE

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the profile.	1 to 64 characters	N/A

UI Setting	Description	Valid Range	Default Value
<b>Category</b>	<p>Select a protocol for this profile.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Message Type</b>	<p>Select which message types to use for this profile. You can select multiple options.</p> <p>Refer to <b>TRDP Message Types</b> for more information.</p>	Drop-down list of message types	N/A
<b>Communication Identifier</b>	<p>Select which communication identifiers to use for this profile. You can select multiple options. The last option in the list lets you add your own communication identifier. You can specify multiple values by separating them with a comma.</p> <p>Refer to <b>IEC 61375-2-3 Communication Identifiers</b> for more information.</p>	Drop-down list of communication identifiers  1 to 4294967295	N/A

### Create Profile - OPC UA

If **OPC UA** is selected for the **Category**, these settings will appear.



## Edit Profile

Name \*

OPC-UA

6 / 32

Category \*

OPC UA

Service ID

0 - 4294967295 or 0x00000000  
- 0xFFFFFFFF

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the profile.	1 to 32 characters	N/A
<b>Category</b>	Select a protocol for this profile.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<p><b>Note</b></p> <p>Available settings will vary depending on your product model.</p>			
<b>Service ID</b>	Specify an OPC UA Service ID for this profile.	0-4294967295 or 0x00000000 - 0xFFFFFFFF	N/A

### Create Profile - MELSEC

If **MELSEC** is selected for the **Category**, these settings will appear.

## Edit Profile

Name \*  
 MELSEC\_Test  
 11 / 32

Category \*  
 MELSEC ▼

Command  
 0 - 65535 or 0x0000 - 0xFFFF

SUB-Command  
 0 - 65535 or 0x0000 - 0xFFFF

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the profile.	1 to 32 characters	N/A
<b>Category</b>	Select a protocol for this profile.  <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b>              Available settings will vary depending on your product model.</p> </div>	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
<b>Command</b>	Specify a command for this profile.	0 - 65535 or 0x0000 - 0xFFFF	N/A
<b>SUB-Command</b>	Specify a sub-command for this profile.	0 - 65535 or 0x0000 - 0xFFFF	N/A

## Create Profile - Step7Plus

If **Step7Plus** is selected for the **Category**, these settings will appear.

### Edit Profile

Name \*

Step7Plus

9 / 32

Category \*

Step7Plus ▼

Function

0 - 65535 or 0x0000 - 0xFFFF

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the profile.	1 to 32 characters	N/A
<b>Category</b>	Select a protocol for this profile.	Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / TRDP / OPC UA / MELSEC / Step7Plus	N/A
	<p> <b>Note</b></p> <p>Available settings will vary depending on your product model.</p>		
<b>Function</b>	Specify a Step7Plus function code for this profile.	0 - 65535 or 0x0000 - 0xFFFF	N/A

## Protocol Filter Policy

**Menu Path:** Firewall > Advanced Protection > Protocol Filter Policy

This page lets you manage your application firewall's protocol filtering policies, which allow you to inspect industrial protocol packets. This allows you to control protocol traffic based on the configured protocol filter policies and Anomaly Detection and Protection (ADP) settings.

Refer to **ADP** for more information.

**Note**

Before creating protocol filter policies, you will need to set up protocol filter objects to define what application protocols your policies will apply to.

Refer to Firewall > Configuration - Protocol Filter Object for more information.

**Limitations**

You can create up to 200 protocol filter policies.


Index	Policy Name	Status	Protocol Filter Object	From Interface	To Interface	Source IP	Destination IP	Protocol	Command Type	Application Protocol	Action
1	Modbus_reject	Enabled	Modbus_Read_Only	Any	Any	Any	Any	Any	Master Query	Modbus/TCP	Accept
2	Modbus_write	Enabled	Modbus_write	Any	Any	Any	Any	Any	Master Query	Modbus/TCP	Reset
3	Modbus_test	Disabled	Modbus_readwrite_test	Any	Any	Any	Any	Any	Master Query	Modbus/TCP	Accept
4	EIPTestPolicy	Enabled	EIP_Test	Any	Any	Any	Any	Any	Master Query	EIP	Reset
5	ddd	Disabled	Modbus_Manual	Any	Any	Any	Any	Any	Master Query	Modbus/TCP	Accept
6	MOXA_test_test	Disabled	MOXA_test	Any	Any	Any	Any	Any	Master Query	Modbus/TCP	Accept

UI Setting	Description
<b>Index</b>	Shows the index of the policy.
<b>Policy Name</b>	Shows the name of the policy.
<b>Status</b>	Shows whether the policy is enabled or disabled.
<b>Protocol Filter Object</b>	Shows the protocol filter object used for the policy.
<b>From Interface</b>	Shows the From Interface for the policy.
<b>To Interface</b>	Shows the To Interface for the policy.
<b>Source IP</b>	Shows the source IP addresses for the policy.

UI Setting	Description
<b>Destination IP</b>	Shows the destination IP addresses for the policy.
<b>Protocol</b>	Shows the protocols for the policy.
<b>Command Type</b>	Shows the packet transmission direction for this policy.
<b>Application Protocol</b>	Shows the industrial protocol for this policy.
<b>Action</b>	Shows the action the firewall will take for packets that match the policy.

## Add Policy

### Menu Path: Firewall > Advanced Protection > Protocol Filter Policy

Clicking the **Add** (  ) icon on the **Firewall > Advanced Protection > Protocol Filter Policy** page will open this dialog box. This dialog lets you create a new protocol filter policy. Click **APPLY** to save your changes and add the new policy.

## Add Policy

Index \*  
**1**  
 1 - 200

Policy Name \*  
 \_\_\_\_\_  
 0 / 64

Status \*  
 Disabled ▾

From Interface \*  
 Any ▾

To Interface \*  
 Any ▾

Source IP \*  
 Any ▾

Destination IP \*  
 Any ▾

Protocol \*  
 Any ▾


Command Type \*  
 Master Query ▾


Application Protocol \* ▾

Action \*  
 Accept ▾

CANCEL

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Index</b>	Specify the index of the policy.	1-200	1
<b>Policy Name</b>	Specify a name for the policy.	1 to 64 characters	N/A
<b>Status</b>	Enable or disable the policy.	Enabled / Disabled	Disabled
<b>From Interface</b>	Select the From Interface for the policy.	Any / Drop-down of interfaces	Any
<p> <b>Note</b></p> <p>Available interfaces will vary depending on your product model and configuration. Refer to <b>Network Configuration &gt; Network Interfaces</b> for more information about managing your device's interfaces.</p>			

UI Setting	Description	Valid Range	Default Value
<b>To Interface</b>	Select the To Interface for the policy.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Available interfaces will vary depending on your product model and configuration. Refer to <b>Network Configuration &gt; Network Interfaces</b> for more information about managing your device's interfaces.</p> </div>	Any / Drop-down of interfaces	Any
<b>Source IP</b>	Select how the policy will check the packet's source IP address.  <b>Any:</b> The policy will check all source IP addresses in the packet.  <b>Single:</b> The policy will only check for the specified source IP address in the packet.  <b>Range:</b> The policy will check all source IP addresses in the packet within the specified IP range.  <b>Subnet:</b> The policy will check for source IP addresses in the packet that are within the specified subnet mask.	Any / Single / Range / Subnet	Any
<b>Destination IP</b>	To decide how the policy will check the packet's destination IP address.  <b>Any:</b> The policy will check all destination IP addresses in the packet.  <b>Single:</b> The policy will only check for the specified destination IP address in the packet.  <b>Range:</b> The policy will check all destination IP addresses in the packet within the specified IP range.  <b>Subnet:</b> The policy will check for destination IP addresses in the packet that are within the specified subnet mask.	Any / Single / Range / Subnet	Any
<b>Protocol</b>	Select the protocol for this policy.	Any / TCP / UDP	Any
<b>Command Type</b>	Select the packet transmission direction for this policy.	Master Query / Slave Response	Master Query
<b>Application Protocol</b>	Select the protocol filter object to use to define the application protocol for this policy.  Refer to <b>Firewall &gt; Advanced Protection &gt; Configuration - Protocol Filter Object</b> for more information.	Custom object	N/A

UI Setting	Description	Valid Range	Default Value
<b>Action</b>	<p>Select the action to take for packets that match the policy.</p> <p><b>Accept:</b> The firewall will accept packets that match the policy.</p> <p><b>Monitor:</b> The firewall will monitor packets that match the policy. With this setting, each packet of an identified application protocol will have a corresponding Event Log entry.</p> <p><b>Reset:</b> The firewall will drop packets that match the policy, and the session will be disconnected. With this setting, only the first packet of an identified application protocol will be recorded in Event Log.</p>	Accept / Monitor / Reset	Accept






## ADP

### Menu Path: Firewall > Advanced Protection > ADP

This page lets you configure your device's Anomaly Detection and Protection (ADP) parameters.

#### Note

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

Q Search					
Index	Description	Category	Status	Action	
 1000000	Forbid multiple.	Modbus/TCP	Enabled	Monitor	
 1000001	Specific layer 4 field of modbus request OR response is invalid.	Modbus/TCP	Enabled	Monitor	
 1000002	Address of the data to be accessed is invalid.	Modbus/TCP	Enabled	Monitor	
 1000003	Quantity of the data is invalid.	Modbus/TCP	Enabled	Monitor	
 1000004	Data length indicated does not match the actual length.	Modbus/TCP	Enabled	Monitor	

UI Setting	Description
<b>Index</b>	Shows the index of the ADP rule.
<b>Description</b>	Shows a description of the condition that will trigger the ADP rule.
<b>Category</b>	Shows the category of the ADP rule.



UI Setting	Description
<b>Status</b>	Shows whether the ADP rule is enabled or disabled.
<b>Action</b>	Shows the action the application firewall will take when the ADP rule is matched.

## Edit ADP Rule Action

**Menu Path:** Firewall > Advanced Protection > ADP

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

### Edit ADP Index 1000001 Rule Action

Description  
Specific layer 4 field of modbus request OR response is invalid.

Status  
Enabled ▼

Action \*  
Monitor ▼

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Description (View-only)</b>	Shows a description of the condition that will trigger the ADP rule.	N/A	N/A
<b>Status</b>	Enable or disable the ADP rule.	Enabled / Disabled	Enabled
<b>Action</b>	Select the action to take for packets that match the rule. <b>Accept:</b> The firewall will accept packets that match the rule. <b>Monitor:</b> The firewall will monitor packets that match the rule and an event log will be recorded in Event Log - Firewall Log. <b>Reset:</b> The firewall will drop packets that match the rule, and the session will be disconnected.	Accept / Monitor / Reset	Monitor

## IPS

### Menu Path: Firewall > Advanced Protection > IPS

This page lets you configure the Intrusion Prevention System (IPS) feature, which helps protect against cyberthreats by performing pattern-based detection and blocking known attacks.

#### Note

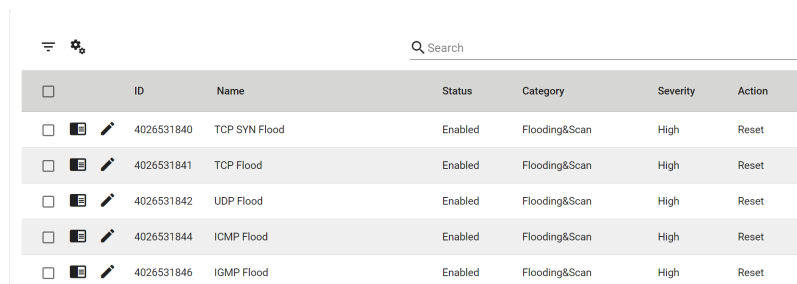
Availability of this feature may vary depending on your product model and version.

#### Note

A separate IPS license is required to enable IPS functionality on the device.

#### Note

Starting from v9.0 of the Network Security Package, when the IPS license expires, existing IPS patterns can still be used for IPS protection. However, the IPS patterns will not be updated and will remain at their current versions when you update the Network Security Package.



The screenshot shows a web interface for configuring IPS rules. At the top, there is a search bar and a settings icon. Below is a table with columns for ID, Name, Status, Category, Severity, and Action. The table contains five rows of rules, all with a status of 'Enabled' and a severity of 'High'.

ID	Name	Status	Category	Severity	Action
4026531840	TCP SYN Flood	Enabled	Flooding&Scan	High	Reset
4026531841	TCP Flood	Enabled	Flooding&Scan	High	Reset
4026531842	UDP Flood	Enabled	Flooding&Scan	High	Reset
4026531844	ICMP Flood	Enabled	Flooding&Scan	High	Reset
4026531846	IGMP Flood	Enabled	Flooding&Scan	High	Reset

#### UI Setting

#### Description

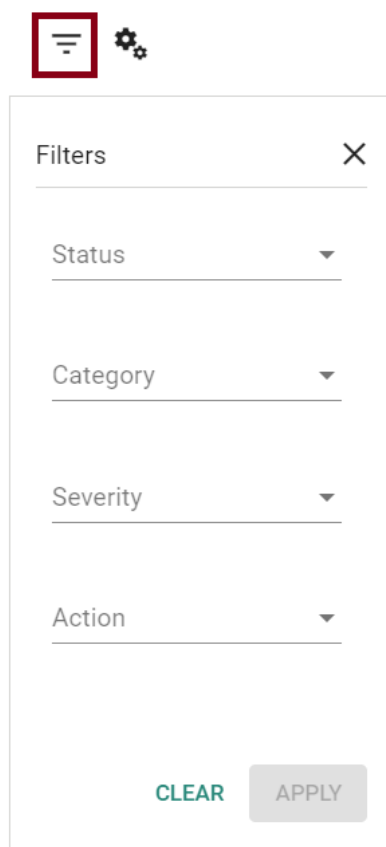
- ID** Shows the ID of the rule.
- Name** Shows the name of the rule.
- Status** Shows whether the rule is enabled or disabled.

UI Setting	Description
<b>Category</b>	Shows the category of the rule.
<b>Severity</b>	Shows the severity assigned to the rule.
<b>Action</b>	Shows the action that will be taken when the rule is triggered.

## Filter IPS Rules

### Menu Path: Firewall > Advanced Protection > IPS

Clicking the **Filter** (☰) icon on the **Firewall > Advanced Protection > IPS** page will open this dialog box. This dialog lets you filter the IPS Rule List according to various criteria. Click **APPLY** to apply the filter, or click **CLEAR** to reset all filter criteria.



UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Filter for enabled or disabled rules.	Enabled / Disabled	N/A
<b>Category</b>	Filter for a specific rule category.	File vulnerabilities / Buffer Overflow / DoS attacks / Exploits / Malware traffic / Reconnaissance / Web threats / Flooding & Scan / Protocol Attack Protection / IP Spoofing	N/A
<b>Severity</b>	Filter for a specific severity level.	Information / Low / Medium / High / Critical	N/A
<b>Action</b>	Filter for a specific rule action.	Accept / Monitor / Reset	N/A

## Quick Settings

### Menu Path: Firewall > Advanced Protection > IPS

Clicking the **Settings** (⚙️) icon on the **Firewall > Advanced Protection > IPS** page will open this dialog box. This dialog lets you quickly configure many rules at the same time. Click **APPLY** to save your changes.

### Quick Settings

**Source**

All
  Filter Rule
  User Selected

**Filters**

Status ▼

---

Category ▼

---

Severity ▼

---

Action ▼

---

**Rule Settings**

Status \* ▼

---

Action \* ▼

---

CANCEL
APPLY

## Source

UI Setting	Description	Valid Range	Default Value
<b>Source</b>	<p>Select which rules to modify with the <b>Rule Settings</b> you specify.</p> <p><b>All:</b> Modify all rules. This option will not be available if you selected rules in the IPS Rule List before opening this dialog.</p> <p><b>Filter Rule:</b> Only modify rules that match the filter criteria you specify. This option will not be available if you selected rules in the IPS Rule List before opening this dialog.</p> <p><b>User Selected:</b> Only modify the rules that you have selected using their checkboxes. This option is only available if you select rules in the IPS Rule List before opening this dialog.</p>	All / Filter Rule / User Selected	All

## Filters

(if **Source** is **Filter Rule**)


UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Filter for enabled or disabled rules.	Enabled / Disabled	N/A
<b>Category</b>	Filter for a specific rule category.	File vulnerabilities / Buffer Overflow / DoS attacks / Exploits / Malware traffic / Reconnaissance / Web threats / Flooding & Scan / Protocol Attack Protection / IP Spoofing	N/A
<b>Severity</b>	Filter for a specific severity level.	Information / Low / Medium / High / Critical	N/A
<b>Action</b>	Filter for a specific rule action.	Accept / Monitor / Reset	N/A

## Rule Settings

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the IPS rule.	Enabled / Disabled	Enabled
<b>Action</b>	Select the action to take for packets that match the rule. <b>Accept:</b> The firewall will accept packets that match the rule. <b>Monitor:</b> The firewall will monitor packets that match the rule. <b>Reset:</b> The firewall will drop packets that match the rule, and the session will be disconnected.	Accept / Monitor / Reset	Monitor

## Detailed Information

**Menu Path:** Firewall > Advanced Protection > IPS

Clicking the **Detailed Information** (  ) icon for a rule on the **Firewall > Advanced Protection > IPS** page will toggle display of a panel with detailed information about the rule.

## Edit IPS Rule Action

### Menu Path: Firewall > Advanced Protection > IPS

Clicking the **Edit (✎)** icon for a rule on the **Firewall > Advanced Protection > IPS** page will open this dialog box. This dialog lets you modify an IPS rule. Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
<b>Name</b> (View-only)	Shows the name of the IPS rule.	N/A	N/A
<b>Status</b>	Enable or disable the IPS rule.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
<b>Action</b>	Select the action to take for packets that match the rule. <b>Accept:</b> The firewall will accept packets that match the rule. <b>Monitor:</b> The firewall will monitor packets that match the rule. <b>Reset:</b> The firewall will drop packets that match the rule, and the session will be disconnected.	Accept / Monitor / Reset	Monitor

## VPN

### Menu Path: VPN

The VPN settings area lets you configure settings related to your device's VPN functionality.

This settings area includes these sections:

- IPsec
- L2TP Server
- OpenVPN Client

### VPN - User Privileges

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

Settings	Admin	Supervisor	User
<b>IPsec</b>	R/W	R/W	R
<b>L2TP Server</b>	R/W	R/W	R
<b>OpenVPN Client</b>	R/W	R/W	-

## IPSec

### Menu Path: VPN > IPSec

This page lets you set up IPSec VPN tunnels for your device.



This page includes these tabs:

- Global Settings
- IPsec Settings
- IPsec Status

## Global Settings

**Menu Path: VPN > IPsec - Global Settings**

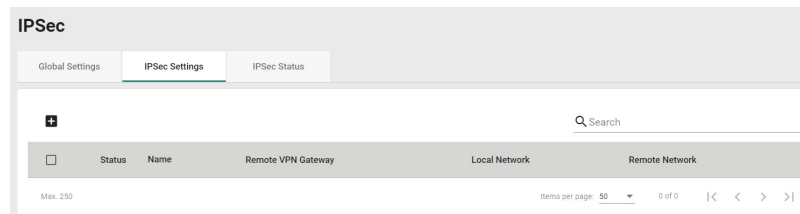
This page lets you configure global settings that affect all IPsec tunnels.

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable all IPsec VPN services.	Enabled / Disabled	Disabled
<b>IPsec NAT-T</b>	Enable or disable IPsec NAT-T (NAT-Traversal). This option should be enabled if there is an external industrial secure router located between VPN tunnels.	Enabled / Disabled	Disabled
<b>VPN Event Log</b>	Enable or disable VPN event logging. Refer to Diagnostics > Event Logs and Notifications > Event Log for more information.	Enabled / Disabled	Disabled
<b>Log Destination</b>	If <b>VPN Event Log</b> is enabled, select the VPN event log storage location.	Local Storage / Syslog / Trap	N/A

## IPSec Settings

### Menu Path: VPN > IPSec - IPSec Settings

This page lets you create and edit IPSec VPN tunnels for your device.



UI Setting	Description
<b>Status</b>	Shows whether the tunnel is enabled or disabled.
<b>Name</b>	Shows the name of the tunnel.
<b>Remote VPN Gateway</b>	Shows the IP address of the remote VPN gateway for the tunnel.
<b>Local Network</b>	Shows the tunnel's local network IP address.
<b>Remote Network</b>	Shows the tunnel's remote network IP address.

## Create IPSec

### Menu Path: VPN > IPSec - IPSec Settings

Clicking the **Add (+)** icon on the **VPN > IPSec - IPSec Settings** page will open this dialog box. This dialog lets you create a new IPSec VPN tunnel. Click **CREATE** to save your changes and add the new tunnel.

### Create IPSec - Quick Settings

If **Quick Settings** is selected, these settings will appear.

## Create IPSec

Settings

Quick Settings  Advanced Settings

### Tunnel Settings

Status \*

Enabled  0 / 31

VPN Connection \*

Site to Site

### Remote Network List

Required

Max. 10

0 of 0

|< < > >|

### Security Settings

Simple  Standard  Strong  Extra

Authentication Mode \*

Pre-shared Key  0 / 64



CANCEL

CREATE

## Tunnel Settings

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the tunnel.	Enabled / Disabled	Enabled
<b>Name</b>	Enter a name for this tunnel.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px;"> <p><b>Note</b> Names must start with a character that is not a number.</p> </div>	Max. 31 characters	N/A
<b>VPN Connection</b>	Select the type of VPN connection to use for this rule. <b>Site to Site:</b> The VPN tunnel for the Local and Remote subnets is fixed. <b>Site to Site(Any):</b> The VPN tunnel for the Remote subnet area is dynamic and is fixed for the Local subnet.	Site to Site / Site to Site(Any)	Site to Site
<b>Remote VPN Gateway</b>	Specify the IP address of the remote VPN gateway. If <b>VPN Connection</b> is set to <b>Site to Site(Any)</b> , this does not need to be set.	Valid IP address	N/A

## Remote Network List

You can configure multiple remote networks for the tunnel. Click the add icon (  ) to add a new entry. Select an entry and click the delete icon (  ) to delete it.

### Limitations

You can add up to 10 remote networks for an IPSec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
<b>Remote Network</b>	Specify the IP address and subnet mask of the remote VPN network.	Valid IP address	N/A
<b>Netmask</b>	Select a netmask to use for the remote network.	Drop-down list of netmasks	24 (255.255.255.0)

## Security Settings

UI Setting	Description	Valid Range	Default Value
<b>Security Strength</b>	Select the security strength for the tunnel. Different settings will change the <b>Encryption Algorithm</b> and <b>Hash Algorithm</b> used, which can be viewed in <b>Advanced Settings</b> .	Simple / Standard / Strong / Extra	Strong

 **Note**

When creating an IPsec connection, it is highly recommended to use similar levels of algorithms between IPsec devices.

The different security levels use the following settings:

### Key Exchange 1

Type	Simple	Standard	Strong	Extra
Encryption Algorithm	DES	3DES	AES-256	AES-256-GCM
Hash Algorithm	MD5	SHA-1	SHA-256	N/A
PRF	N/A	N/A	N/A	PRFSHA512
DH Group	DH1	DH2	DH14	DH31

### Key Exchange 2

Type	Simple	Standard	Strong	Extra
Encryption Algorithm	DES	3DES	AES-256	AES-256-GCM
Hash	MD5	SHA-1	SHA-256	N/A
PRF	N/A	N/A	N/A	prfsha512

UI Setting	Description	Valid Range	Default Value
<b>Authentication Mode</b>	<p>Select the authentication mode to use for the tunnel.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin: 5px 0;"> <p><b>Note</b></p> <p>You must have certificates already imported to select <b>X.509</b> or <b>X.509 With CA</b>. Refer to Certificate Management for more information.</p> </div> <p><b>Pre-Shared Key:</b> Pre-Shared Key is a user-defined authentication string used by two systems to establish an IPsec VPN connection.</p> <p><b>X.509:</b> The local and remote systems will authenticate the VPN connection using certificates imported in advance by the user on the <b>Certificate Management &gt; Local Certificate</b> page.</p> <p><b>X.509 With CA:</b> The local and remote systems will authenticate the VPN connection using both certificates imported in advance by the user on the <b>Certificate Management &gt; Local Certificate</b> page and a CA certificate imported on the <b>Certificate Management &gt; Trusted CA Certificate</b> page.</p>	Pre-Shared Key / X.509 / X.509 With CA	Pre-Shared Key
<b>Pre-Shared Key</b>	Specify a pre-shared key to use to authenticate the IPsec VPN connection.	0 to 64 characters	N/A

### Create IPsec - Advanced Settings

If **Advanced Settings** is selected, these settings will appear.

### Create IPsec

Settings

Quick Settings
  Advanced Settings

#### Tunnel Settings

Status \*

Enabled Name \* 0 / 31

L2TP Tunnel \*

Disabled

VPN Connection \*

Site to Site Remote VPN Gateway \* Startup Mode \* Start in initial

#### Local Network List

+

Local Network \* Netmask \* 24 (255.255.255.0)

192.168.127.254 24 (255.255.255.0)

Max. 10 1 - 1 of 1 |< < > >|

#### Remote Network List

+

Required

Max. 10 0 of 0 |< < > >|

Identity Type \*

IP Address Local ID 0 / 31 Remote ID 0 / 31

#### Key Exchange (Phase 1)

IKE Mode \* IKE Version \* IKE2

Main



CANCEL
CREATE

## Tunnel Settings

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the tunnel.	Enabled / Disabled	Enabled
<b>Name</b>	Enter a name for this tunnel.	Max. 31 characters	N/A
	<p><span style="font-size: 0.8em;">✎</span> <b>Note</b></p> <p>Names must start with a character that is not a number.</p>		
<b>L2TP Tunnel</b>	Enable or disable L2TP over IPsec.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
<b>VPN Connection</b>	Select the type of VPN connection to use for this rule. <b>Site to Site:</b> The VPN tunnel for the Local and Remote subnets is fixed. <b>Site to Site(Any):</b> The VPN tunnel for the Remote subnet area is dynamic and is fixed for the Local subnet.	Site to Site / Site to Site(Any)	Site to Site
<b>Remote VPN Gateway</b>	Specify the IP address of the remote VPN gateway. If <b>VPN Connection</b> is set to <b>Site to Site(Any)</b> , this does not need to be set.	Valid IP address	N/A
<b>Startup Mode</b>	Select a startup mode for the tunnel. <b>Start in Initial:</b> The VPN tunnel will actively initiate the connection with the remote VPN gateway. <b>Wait for Connecting:</b> The VPN tunnel will wait for the remote VPN gateway to initiate the connection.	Start in Initial / Wait for Connecting	Start in Initial

## Local Network List



You can configure multiple local networks for the tunnel. Click the add icon (  ) to add a new entry. Select an entry and click the delete icon (  ) to delete it.

### Limitations

You can add up to 10 local networks for an IPsec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
<b>Local Network</b>	Specify the IP address and subnet mask of the local VPN network.	Valid IP address	N/A
<b>Netmask</b>	Select a netmask to use for the local network.	Drop-down list of netmasks	24 (255.255.255.0)

## Remote Network List

You can configure multiple remote networks for the tunnel. Click the add icon (  ) to add a new entry. Select an entry and click the delete icon (  ) to delete it.



## 🔔 Limitations


You can add up to 10 remote networks for an IPSec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
<b>Remote Network</b>	Specify the IP address and subnet mask of the remote VPN network.	Valid IP address	N/A
<b>Netmask</b>	Select a netmask to use for the remote network.	Drop-down list of netmasks	24 (255.255.255.0)

## Identity

UI Setting	Description	Valid Range	Default Value
<b>Identity Type</b>	Select an ID type to use to identify VPN tunnel connections. <b>IP Address:</b> Use an IP address. <b>FQDN:</b> Use a Fully Qualified Domain Name (FQDN). <b>Key ID:</b> Use a user-defined key ID string. <b>Auto(with Cisco):</b> Use this when establishing connections to Cisco systems.	IP Address / FQDN / Key ID / Auto(with Cisco)	IP Address
<b>Local ID</b> <b>(If Identity Type is IP Address, FQDN, or Key ID)</b>	Specify the local ID for identifying the VPN tunnel connection. The Local ID must be identical to the Remote ID of the connected VPN gateway in order to successfully establish the VPN tunnel connection.	1 to 31 characters	N/A
<b>Remote ID</b> <b>(If Identity Type is IP Address, FQDN, or Key ID)</b>	Specify the remote ID for identifying the VPN tunnel connection. The Remote ID must be identical to the Local ID of the connected VPN gateway in order to successfully establish the VPN tunnel connection.	1 to 31 characters	N/A

## Key Exchange (Phase 1)

UI Setting	Description	Valid Range	Default Value
<b>IKE Mode</b>	<p>Select the IKE mode to use for authentication.</p> <p><b>Main:</b> Both the remote and local VPN gateway will negotiate which encryption/hash algorithm and DH groups can be used for this VPN tunnel. Both VPN gateways must use the same algorithm to communicate.</p> <p><b>Aggressive:</b> The remote and local VPN gateways will not negotiate the algorithm and will only use the user-defined configuration.</p>	Main / Aggressive	Main
<b>IKE Version</b>	<p>Select which version of IKE to use.</p> <p><b>IKE1:</b> Use IKE Version 1 protocol.</p> <p><b>IKE2:</b> Use IKE Version 2 protocol.</p>	IKE1 / IKE2	IKE2
<b>Authentication Mode</b>	<p>Select the authentication mode to use for the tunnel.</p> <div data-bbox="434 1032 825 1294" style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p> <b>Note</b></p> <p>You must have certificates already imported to select <b>X.509</b> or <b>X.509 With CA</b>. Refer to Certificate Management for more information.</p> </div> <p><b>Pre-Shared Key:</b> Pre-Shared Key is a user-defined authentication string used by two systems to establish an IPsec VPN connection.</p> <p><b>X.509:</b> The local and remote systems will authenticate the VPN connection using certificates imported in advance by the user on the <b>Certificate Management &gt; Local Certificate</b> page.</p> <p><b>X.509 With CA:</b> The local and remote systems will authenticate the VPN connection using both certificates imported in advance by the user on the <b>Certificate Management &gt; Local Certificate</b> page and a CA certificate imported on the <b>Certificate Management &gt; Trusted CA Certificate</b> page.</p>	Pre-Shared Key / X.509 / X.509 With CA	Pre-Shared Key

UI Setting	Description	Valid Range	Default Value
<b>Pre-Shared Key</b>	Specify a pre-shared key to use to authenticate the IPsec VPN connection.	0 to 64 characters	
<b>Encryption Algorithm</b>	Select the encryption algorithm to use for key exchange.	DES / 3DES / AES-128 / AES-192 / AES-256 / AES-256-GCM	AES-256
<b>Hash Algorithm (If Encryption Algorithm is not AES-256-GCM)</b>	Select the hash algorithm to use for key exchange.	MD5 / SHA-1 / SHA-256 / SHA-512	SHA-256
<b>PRF (If Encryption Algorithm is AES-256-GCM)</b>	Select the PRF algorithm for AES-256-GCM.	PRFSHA256 / PRFSHA384 / PRFSHA512	PRFSHA256
<b>DH Group</b>	Select the Diffie-Hellman group. This is the key exchange group between the remote and VPN gateways.	DH 1(modp768) / DH 2(modp1024) / DH 5(modp1536) / DH 14(modp2048) / DH15(modp3072) / DH16(modp4096) / DH17(modp6144) / DH18(modp8192) / DH22(modp1024s160) / DH23(modp2048s224) / DH24(modp2048s256) / DH31(curve25519)	DH 14(modp2048)
<b>IKE Lifetime</b>	Specify the lifetime (in minutes) for IKE SA.	30 to 43200	43200

## Data Exchange (Phase 2)

UI Setting	Description	Valid Range	Default Value
<b>Encryption Algorithm</b>	Select the encryption algorithm to use for data exchange.	DES / 3DES / AES-128 / AES-192 / AES-256 / AES-256-GCM	AES-256
<b>Hash Algorithm (If Encryption Algorithm is not AES-256-GCM)</b>	Select the hash algorithm to use for data exchange.	MD5 / SHA-1 / SHA-256 / SHA-512	SHA-256

UI Setting	Description	Valid Range	Default Value
<b>PRF</b> <b>(If Encryption Algorithm is AES-256-GCM)</b>	Select the PRF algorithm for AES-256-GCM.	PRFSHA256 / PRFSHA384 / PRFSHA512	PRFSHA256
<b>Perfect Forward Secrecy</b>	Enable or disable Perfect Forward Secrecy. When enabled, different security keys are used for different IPsec phases in order to enhance security.	Enabled / Disabled	Disabled
<b>DH Group</b> <b>(If Perfect Forward Secrecy is Enabled)</b>	Select the Diffie-Hellman group. This is the Key Exchange group between the remote and VPN gateways.	DH 1(modp768) / DH 2(modp1024) / DH 5(modp1536) / DH 14(modp2048) /DH15 (modp3072) / DH16 (modp4096) / DH17 (modp6144) / DH18 (modp8192) / DH22 (modp1024s160) / DH23 (modp2048s224) / DH24 (modp2048s256) / DH31 (curve25519)	DH 14 (modp2048)
<b>SA Lifetime</b>	Specify the lifetime (in minutes) for Phase 2 IKE SA.	30 to 43200	43200

## Dead Peer Detection

UI Setting	Description	Valid Range	Default Value
<b>Action</b>	Specify the action the system should take when a dead peer is detected. <b>Hold:</b> Maintain the VPN tunnel. <b>Restart:</b> Reconnect the VPN tunnel. <b>Clear:</b> Clear the VPN tunnel. <b>Disabled:</b> Disable Dead Peer Detection.	Hold / Restart / Clear / Disabled	Restart
<b>Retry Interval</b>	Specify the interval (in seconds) at which Dead Peer Detection messages are sent.	0 to 3600	30
<b>Confidence Interval</b>	Specify the interval (in seconds) at which the system will check to see if the connection is alive or not.	0 to 3600	120

## Edit IPsec

**Menu Path:** VPN > IPsec - IPsec Settings

Clicking the **Edit** (✎) icon for an entry on the **VPN > IPSec - IPSec Settings** page will open this dialog box. This dialog lets you edit an existing IPSec VPN tunnel. Click **APPLY** to save your changes.

### Edit IPSec - Quick Settings

If **Quick Settings** is selected, these settings will appear.

**Edit IPSec**

Settings

Quick Settings  Advanced Settings

**Tunnel Settings**

Status \* Enabled 5 / 31

Name \* test1

VPN Connection \* Site to Site

Remote VPN Gateway \* 10.1.1.2

**Remote Network List**

+

Remote Network \* 192.168.127.1

Netmask \* 24 (255.255.255.0)

Max. 10 1 - 1 of 1 |< < > >|

**Security Settings**

Simple  Standard  Strong

Authentication Mode \* Pre-shared Key \*

Pre-shared Key ..... 8 / 64



**CANCEL** **APPLY**

### Tunnel Settings

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the tunnel.	Enabled / Disabled	Enabled
<b>Name</b>	Enter a name for this tunnel.	Max. 31 characters	N/A
<p><b>Note</b></p> <p>Names must start with a character that is not a number.</p>			

UI Setting	Description	Valid Range	Default Value
<b>VPN Connection</b>	Select the type of VPN connection to use for this rule. <b>Site to Site:</b> The VPN tunnel for the Local and Remote subnets is fixed. <b>Site to Site(Any):</b> The VPN tunnel for the Remote subnet area is dynamic and is fixed for the Local subnet.	Site to Site / Site to Site(Any)	Site to Site
<b>Remote VPN Gateway</b>	Specify the IP address of the remote VPN gateway. If <b>VPN Connection</b> is set to <b>Site to Site(Any)</b> , this does not need to be set.	Valid IP address	N/A

### Remote Network List

You can configure multiple remote networks for the tunnel. Click the add icon (  ) to add a new entry. Select an entry and click the delete icon (  ) to delete it.

#### Limitations

You can add up to 10 remote networks for an IPSec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
<b>Remote Network</b>	Specify the IP address and subnet mask of the remote VPN network.	Valid IP address	N/A
<b>Netmask</b>	Select a netmask to use for the remote network.	Drop-down list of netmasks	24 (255.255.255.0)

## Security Settings

UI Setting	Description	Valid Range	Default Value
<b>Security Strength</b>	Select the security strength for the tunnel. Different settings will change the <b>Encryption Algorithm</b> and <b>Hash Algorithm</b> used, which can be viewed in <b>Advanced Settings</b> .	Simple / Standard / Strong / Extra	Strong

**Note**

When creating an IPsec connection, it is highly recommended to use similar levels of algorithms between IPsec devices.

The different security levels use the following settings:

### Key Exchange 1

Type	Simple	Standard	Strong	Extra
Encryption Algorithm	DES	3DES	AES-256	AES-256-GCM
Hash Algorithm	MD5	SHA-1	SHA-256	N/A
PRF	N/A	N/A	N/A	PRFSHA512
DH Group	DH1	DH2	DH14	DH31

### Key Exchange 2

Type	Simple	Standard	Strong	Extra
Encryption Algorithm	DES	3DES	AES-256	AES-256-GCM
Hash	MD5	SHA-1	SHA-256	N/A
PRF	N/A	N/A	N/A	prfsha512

UI Setting	Description	Valid Range	Default Value
<b>Authentication Mode</b>	<p>Select the authentication mode to use for the tunnel.</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p><b>Note</b></p> <p>You must have certificates already imported to select <b>X.509</b> or <b>X.509 With CA</b>. Refer to Certificate Management for more information.</p> </div> <p><b>Pre-Shared Key:</b> Pre-Shared Key is a user-defined authentication string used by two systems to establish an IPsec VPN connection.</p> <p><b>X.509:</b> The local and remote systems will authenticate the VPN connection using certificates imported in advance by the user on the <b>Certificate Management &gt; Local Certificate</b> page.</p> <p><b>X.509 With CA:</b> The local and remote systems will authenticate the VPN connection using both certificates imported in advance by the user on the <b>Certificate Management &gt; Local Certificate</b> page and a CA certificate imported on the <b>Certificate Management &gt; Trusted CA Certificate</b> page.</p>	Pre-Shared Key / X.509 / X.509 With CA	Pre-Shared Key
<b>Pre-Shared Key</b>	Specify a pre-shared key to use to authenticate the IPsec VPN connection.	0 to 64 characters	N/A

## Edit IPsec - Advanced Settings

If **Advanced Settings** is selected, these settings will appear.



### Edit IPsec

Settings

Quick Settings
  Advanced Settings

#### Tunnel Settings

Status \* Name \*

Enabled test1

5 / 31

L2TP Tunnel \*

Disabled

VPN Connection \* Remote VPN Gateway \* Startup Mode \*

Site to Site 10.1.1.2 Start in initial

#### Local Network List

+

Local Network \* Netmask \*

192.168.127.254 24 (255.255.255.0)

Max. 10 1 - 1 of 1 |< < > >|

#### Remote Network List

+

Remote Network \* Netmask \*

192.168.127.1 24 (255.255.255.0)

Max. 10 1 - 1 of 1 |< < > >|



CANCEL
APPLY

## Tunnel Settings

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the tunnel.	Enabled / Disabled	Enabled
<b>Name</b>	Enter a name for this tunnel.	Max. 31 characters	N/A
	<p><span style="font-size: 0.8em;">✎</span> <b>Note</b></p> <p>Names must start with a character that is not a number.</p>		
<b>L2TP Tunnel</b>	Enable or disable L2TP over IPsec.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
<b>VPN Connection</b>	Select the type of VPN connection to use for this rule. <b>Site to Site:</b> The VPN tunnel for the Local and Remote subnets is fixed. <b>Site to Site(Any):</b> The VPN tunnel for the Remote subnet area is dynamic and is fixed for the Local subnet.	Site to Site / Site to Site(Any)	Site to Site
<b>Remote VPN Gateway</b>	Specify the IP address of the remote VPN gateway. If <b>VPN Connection</b> is set to <b>Site to Site(Any)</b> , this does not need to be set.	Valid IP address	N/A
<b>Startup Mode</b>	Select a startup mode for the tunnel. <b>Start in Initial:</b> The VPN tunnel will actively initiate the connection with the remote VPN gateway. <b>Wait for Connecting:</b> The VPN tunnel will wait for the remote VPN gateway to initiate the connection.	Start in Initial / Wait for Connecting	Start in Initial

## Local Network List



You can configure multiple local networks for the tunnel. Click the add icon (  ) to add a new entry. Select an entry and click the delete icon (  ) to delete it.

### Limitations

You can add up to 10 local networks for an IPsec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
<b>Local Network</b>	Specify the IP address and subnet mask of the local VPN network.	Valid IP address	N/A
<b>Netmask</b>	Select a netmask to use for the local network.	Drop-down list of netmasks	24 (255.255.255.0)

## Remote Network List

You can configure multiple remote networks for the tunnel. Click the add icon (  ) to add a new entry. Select an entry and click the delete icon (  ) to delete it.

## 🔔 Limitations


You can add up to 10 remote networks for an IPSec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
<b>Remote Network</b>	Specify the IP address and subnet mask of the remote VPN network.	Valid IP address	N/A
<b>Netmask</b>	Select a netmask to use for the remote network.	Drop-down list of netmasks	24 (255.255.255.0)

## Identity

UI Setting	Description	Valid Range	Default Value
<b>Identity Type</b>	Select an ID type to use to identify VPN tunnel connections. <b>IP Address:</b> Use an IP address. <b>FQDN:</b> Use a Fully Qualified Domain Name (FQDN). <b>Key ID:</b> Use a user-defined key ID string. <b>Auto(with Cisco):</b> Use this when establishing connections to Cisco systems.	IP Address / FQDN / Key ID / Auto(with Cisco)	IP Address
<b>Local ID</b> <b>(If Identity Type is IP Address, FQDN, or Key ID)</b>	Specify the local ID for identifying the VPN tunnel connection. The Local ID must be identical to the Remote ID of the connected VPN gateway in order to successfully establish the VPN tunnel connection.	1 to 31 characters	N/A
<b>Remote ID</b> <b>(If Identity Type is IP Address, FQDN, or Key ID)</b>	Specify the remote ID for identifying the VPN tunnel connection. The Remote ID must be identical to the Local ID of the connected VPN gateway in order to successfully establish the VPN tunnel connection.	1 to 31 characters	N/A

## Key Exchange (Phase 1)

UI Setting	Description	Valid Range	Default Value
<b>IKE Mode</b>	<p>Select the IKE mode to use for authentication.</p> <p><b>Main:</b> Both the remote and local VPN gateway will negotiate which encryption/hash algorithm and DH groups can be used for this VPN tunnel. Both VPN gateways must use the same algorithm to communicate.</p> <p><b>Aggressive:</b> The remote and local VPN gateways will not negotiate the algorithm and will only use the user-defined configuration.</p>	Main / Aggressive	Main
<b>IKE Version</b>	<p>Select which version of IKE to use.</p> <p><b>IKE1:</b> Use IKE Version 1 protocol.</p> <p><b>IKE2:</b> Use IKE Version 2 protocol.</p>	IKE1 / IKE2	IKE2
<b>Authentication Mode</b>	<p>Select the authentication mode to use for the tunnel.</p> <div data-bbox="434 1032 825 1294" style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p> <b>Note</b></p> <p>You must have certificates already imported to select <b>X.509</b> or <b>X.509 With CA</b>. Refer to Certificate Management for more information.</p> </div> <p><b>Pre-Shared Key:</b> Pre-Shared Key is a user-defined authentication string used by two systems to establish an IPsec VPN connection.</p> <p><b>X.509:</b> The local and remote systems will authenticate the VPN connection using certificates imported in advance by the user on the <b>Certificate Management &gt; Local Certificate</b> page.</p> <p><b>X.509 With CA:</b> The local and remote systems will authenticate the VPN connection using both certificates imported in advance by the user on the <b>Certificate Management &gt; Local Certificate</b> page and a CA certificate imported on the <b>Certificate Management &gt; Trusted CA Certificate</b> page.</p>	Pre-Shared Key / X.509 / X.509 With CA	Pre-Shared Key

UI Setting	Description	Valid Range	Default Value
<b>Pre-Shared Key</b>	Specify a pre-shared key to use to authenticate the IPsec VPN connection.	0 to 64 characters	
<b>Encryption Algorithm</b>	Select the encryption algorithm to use for key exchange.	DES / 3DES / AES-128 / AES-192 / AES-256 / AES-256-GCM	AES-256
<b>Hash Algorithm (If Encryption Algorithm is not AES-256-GCM)</b>	Select the hash algorithm to use for key exchange.	MD5 / SHA-1 / SHA-256 / SHA-512	SHA-256
<b>PRF (If Encryption Algorithm is AES-256-GCM)</b>	Select the PRF algorithm for AES-256-GCM.	PRFSHA256 / PRFSHA384 / PRFSHA512	PRFSHA256
<b>DH Group</b>	Select the Diffie-Hellman group. This is the key exchange group between the remote and VPN gateways.	DH 1(modp768) / DH 2(modp1024) / DH 5(modp1536) / DH 14(modp2048) / DH15(modp3072) / DH16(modp4096) / DH17(modp6144) / DH18(modp8192) / DH22(modp1024s160) / DH23(modp2048s224) / DH24(modp2048s256) / DH31(curve25519)	DH 14(modp2048)
<b>IKE Lifetime</b>	Specify the lifetime (in minutes) for IKE SA.	30 to 43200	43200

## Data Exchange (Phase 2)

UI Setting	Description	Valid Range	Default Value
<b>Encryption Algorithm</b>	Select the encryption algorithm to use for data exchange.	DES / 3DES / AES-128 / AES-192 / AES-256 / AES-256-GCM	AES-256
<b>Hash Algorithm (If Encryption Algorithm is not AES-256-GCM)</b>	Select the hash algorithm to use for data exchange.	MD5 / SHA-1 / SHA-256 / SHA-512	SHA-256


UI Setting	Description	Valid Range	Default Value
<b>PRF</b> <b>(If Encryption Algorithm is AES-256-GCM)</b>	Select the PRF algorithm for AES-256-GCM.	PRFSHA256 / PRFSHA384 / PRFSHA512	PRFSHA256
<b>Perfect Forward Security</b>	Enable or disable Perfect Forward Secrecy. When enabled, different security keys are used for different IPsec phases in order to enhance security.	Enabled / Disabled	Disabled
<b>DH Group</b> <b>(If Perfect Forward Security is Enabled)</b>	Select the Diffie-Hellman group. This is the Key Exchange group between the remote and VPN gateways.	DH 1(modp768) / DH 2(modp1024) / DH 5(modp1536) / DH 14(modp2048) /DH15 (modp3072) / DH16 (modp4096) / DH17 (modp6144) / DH18 (modp8192) / DH22 (modp1024s160) / DH23 (modp2048s224) / DH24 (modp2048s256) / DH31 (curve25519)	DH 14 (modp2048)
<b>SA Lifetime</b>	Specify the lifetime (in minutes) for Phase 2 IKE SA.	30 to 43200	43200

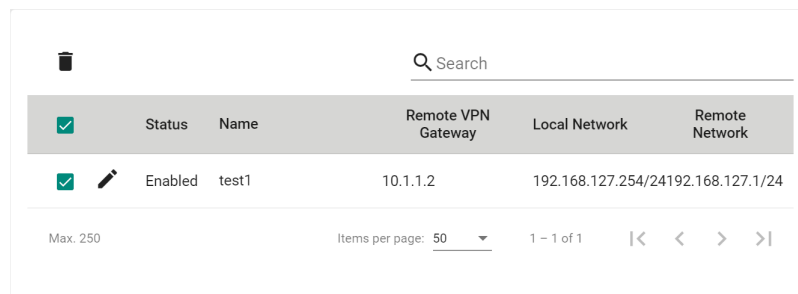
## Dead Peer Detection

UI Setting	Description	Valid Range	Default Value
<b>Action</b>	Specify the action the system should take when a dead peer is detected. <b>Hold:</b> Maintain the VPN tunnel. <b>Restart:</b> Reconnect the VPN tunnel. <b>Clear:</b> Clear the VPN tunnel. <b>Disabled:</b> Disable Dead Peer Detection.	Hold / Restart / Clear / Disabled	Restart
<b>Retry Interval</b>	Specify the interval (in seconds) at which Dead Peer Detection messages are sent.	0 to 3600	30
<b>Confidence Interval</b>	Specify the interval (in seconds) at which the system will check to see if the connection is alive or not.	0 to 3600	120

## Delete IPsec

**Menu Path:** VPN > IPsec - IPsec Settings

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

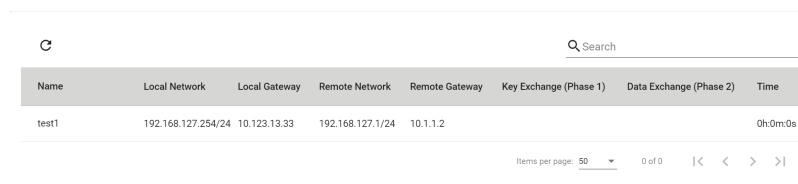


<input checked="" type="checkbox"/>	Status	Name	Remote VPN Gateway	Local Network	Remote Network
<input checked="" type="checkbox"/>	Enabled	test1	10.1.1.2	192.168.127.254/24	192.168.127.1/24

## IPSec Status

**Menu Path: VPN > IPSec - IPSec Status**

This page lets you see the status of your IPSec VPN tunnels.



Name	Local Network	Local Gateway	Remote Network	Remote Gateway	Key Exchange (Phase 1)	Data Exchange (Phase 2)	Time
test1	192.168.127.254/24	10.123.13.33	192.168.127.1/24	10.1.1.2			0h:0m:0s

UI Setting	Description
<b>Name</b>	Shows the name of the tunnel.
<b>Local Network</b>	Shows the local network address for the tunnel.
<b>Local Gateway</b>	Shows the local gateway address for the tunnel.
<b>Remote Network</b>	Shows the remote network address for the tunnel.
<b>Remote Gateway</b>	Shows the remote gateway address for the tunnel.
<b>Key Exchange (Phase 1)</b>	Shows the status of key exchange phase.
<b>Data Exchange (Phase 2)</b>	Shows the status of the data exchange phase.
<b>Time</b>	Shows how long the connection has been up.

## L2TP Server

### Menu Path: VPN > L2TP Server

This page lets you configure the L2TP server function of your device. L2TP is a popular choice for VPN applications with remote roaming users since an L2TP client is built into the Microsoft Windows operating system. Since L2TP does not provide any encryption, it is usually combined with IPsec to provide data encryption.

This page includes these tabs:

- Server Setting (WAN)
- User Name Settings

### Server Setting (WAN)

#### Menu Path: VPN > L2TP Server - Server Setting (WAN)

This page lets you enable and configure the L2TP server function of your device.

The screenshot shows the 'L2TP Server' configuration interface. It features two tabs: 'Server Setting (WAN)' and 'User Name Settings'. The 'Server Setting (WAN)' tab is selected. The configuration fields are as follows:

- L2TP Server Mode \***: A dropdown menu currently set to 'Disabled'.
- Local IP**: A text input field containing '0.0.0.0'.
- Offered IP: Start**: A text input field containing '0.0.0.0'.
- Offered IP: End**: A text input field containing '0.0.0.0'.

An 'APPLY' button is located at the bottom of the configuration area.

UI Setting	Description	Valid Range	Default Value
<b>L2TP Server Mode</b>	Enable or disable the L2TP server.	Enabled / Disabled	Disabled
<b>Local IP</b>	Specify the IP address of the local subnet.	Valid IP address	0.0.0.0



UI Setting	Description	Valid Range	Default Value
<b>Offered IP: Start</b>	Specify the starting IP address of the offered IP range used for L2TP clients.	Valid IP address	0.0.0.0
<b>Offered IP: End</b>	Specify the ending IP address of the offered IP range used for L2TP clients.	Valid IP address	0.0.0.0

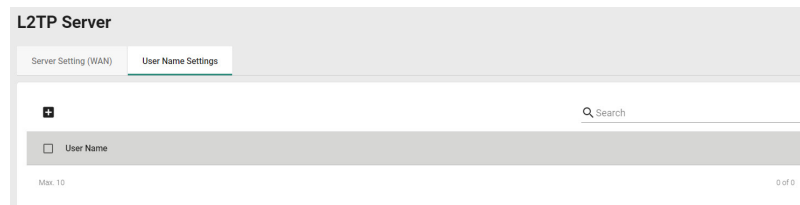
## User Name Settings

### Menu Path: VPN > L2TP Server - User Name Settings

This page lets you manage users that can connect to your device's L2TP server.

#### Limitations


You can add up to 10 users for the L2TP Server.



UI Setting	Description
<b>User Name</b>	Shows the name of the user account.

## Create New Account for L2TP

### Menu Path: VPN > L2TP Server - User Name Settings

Clicking the **Add** () icon on the **VPN > L2TP Server - User Name Settings** page will open this dialog box. This dialog lets you create a new user account for the device's L2TP server. Click **CREATE** to save your changes and add the new account.

### Create New Account for L2TP

Username \*  
0 / 32

New Password \*  
0 / 32

CANCEL

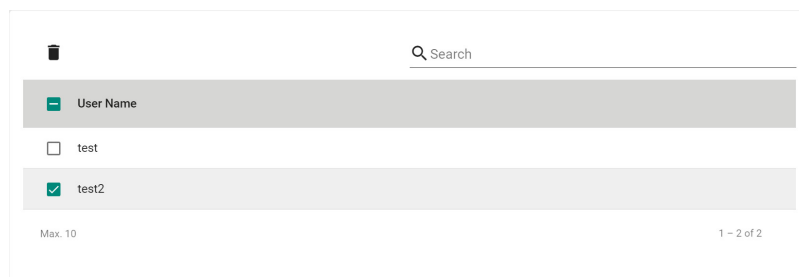
CREATE

UI Setting	Description	Valid Range	Default Value
<b>Username</b>	Enter a username for the L2TP account.	1 to 32 characters	N/A
<b>New Password</b>	Enter a password for the L2TP account.	1 to 32 characters	N/A

## Delete Account for L2TP

### Menu Path: VPN > L2TP Server - User Name Settings

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



## OpenVPN Client

### Menu Path: VPN > OpenVPN Client

This page lets you manage the OpenVPN Client feature of your device.

#### Note

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

 **Note**

For models with WAN redundancy, such as the EDR-G9004, running the OpenVPN client under WAN redundancy mode currently only supports failover, not failback. This means the device will not automatically switch back to the primary connection once it is restored.

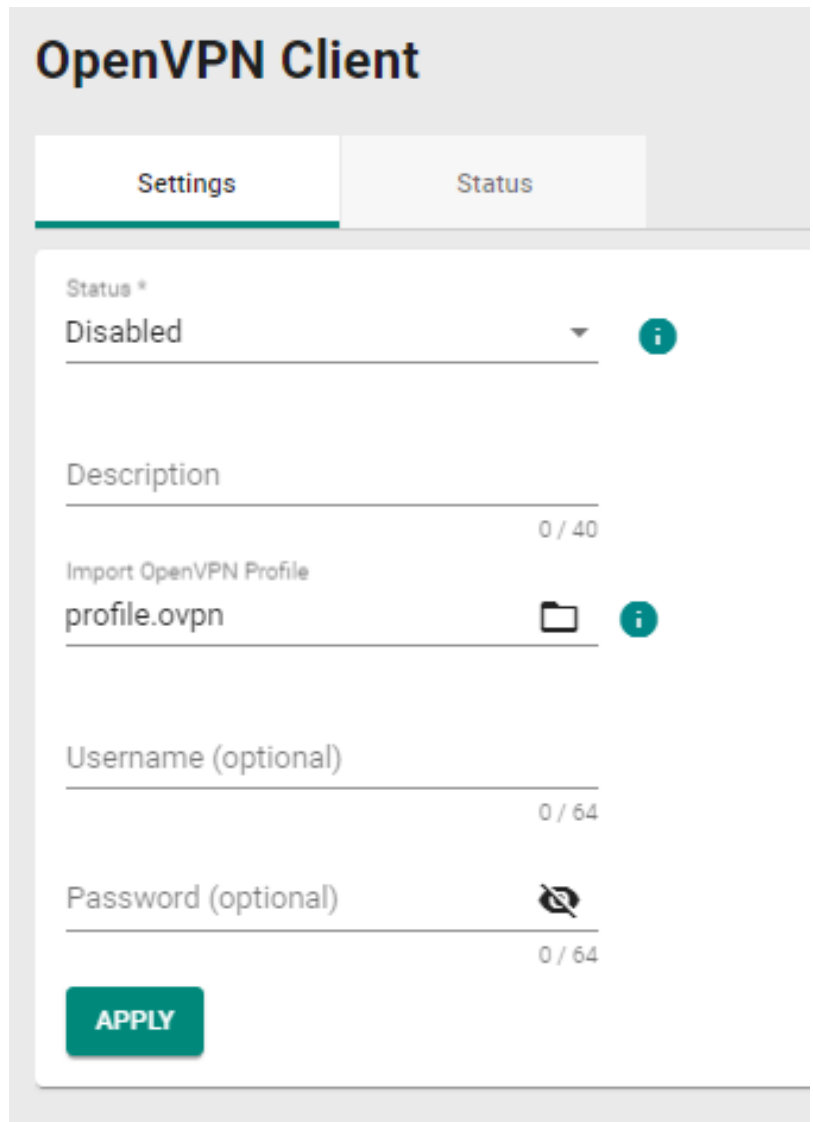
This page includes these tabs:

- Settings
- Status

## **OpenVPN Client - Settings**

**Menu Path:** [VPN](#) > [OpenVPN Client - Settings](#)

This page lets you manage your OpenVPN Client settings.



UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or Disable OpenVPN Client. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 5px;">             IPsec and OpenVPN cannot be enabled simultaneously.           </div>	Enabled / Disabled	Disabled
<b>Description</b>	Specify the description for the OpenVPN Client connection.	0 to 40 characters	N/A

UI Setting	Description	Valid Range	Default Value
<b>Import OpenVPN Profile</b>	Import the .ovpn file for OpenVPN Client setup.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px;"> <p><b>Note</b> Importing OpenVPN profiles is not supported in the CLI interface.</p> </div>	.ovpn files	N/A
<b>Username (optional)</b>	Specify the username.	0 to 64 characters	N/A
<b>Password (optional)</b>	Specify the password.	0 to 64 characters	N/A

## OpenVPN Client - Status

### Menu Path: VPN > OpenVPN Client - Status

This page lets you view the status of your OpenVPN Client connection.

Status	Description	OpenVPN Server	OpenVPN Client IP Address	Duration	Data Received / Sent	Last Connection
Disconnected	test			0h:0m:0s	0 Byte / 0 Byte	

UI Setting	Description
<b>Status</b>	Shows the status of the connection.
<b>Description</b>	Shows the description of the connection.
<b>OpenVPN Server</b>	Shows the OpenVPN Server IP Address.
<b>OpenVPN Client IP Address</b>	Shows the OpenVPN Client IP Address.
<b>Duration</b>	Shows the duration of OpenVPN connection.
<b>Data Received / Sent</b>	Shows the number of bytes received/sent through the OpenVPN tunnel.
<b>Last Connection</b>	Shows when the device was last connected to the OpenVPN server.

# 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	-	-

Settings	Admin	Supervisor	User
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.

Label	Issued To	Issued By	Expiration Date	Key Length
Max. 10 <span style="float: right;">0 of 0</span>				

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

### Generate Certificate

Import Identity Certifi... ▾

Label  
0 / 30

Select Certificate \* 

CANCEL

UPGRADE

UI Setting	Description	Valid Range	Default Value
<b>Import Identity Certificate</b>	<p>Select the type of certificate to import.</p> <p><b>Certificate:</b> Used for certificates with a .crt file extension.</p> <p><b>Certificate From CSR:</b> Used for certificates issued by another CA.</p> <p><b>Certificate From PKCS#12:</b> Used for certificates with a .p12 file extension.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Before importing a certificate issued by another CA, you should import its related trusted CA certificate first on the <b>Certificate Management &gt; Trusted CA Certificate</b> page. Otherwise, your device may not recognize the certificate and reject the connection.</p> </div>	Certificate / Certificate From CSR / Certificate From PKCS#12	N/A
<b>Label</b>	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
<b>CSR Common Name</b> (if Import Identity Certificate is Certificate From CSR)	Select the CSR common name for the certificate.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px;"> <p><b>Note</b></p> <p>CSRs must be created in advance on the <b>Certificate Management &gt; Certificate Signing Request - CSR Generate</b> page to select them here.</p> </div>	Drop-down list of CSR names	N/A
<b>Import Password</b> (if Import Identity Certificate is Certificate From PKCS#12)	Enter the password for the certificate.	0 to 32 characters	N/A
<b>Select Certificate</b>	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**

**Local Certificate**

<input checked="" type="checkbox"/>	Label	Issued To	Issued By	Expiration Date	Key Length
<input checked="" type="checkbox"/>	10.123.13.33.crt	= TW, O = MAT, OU = MAT, CN = 10.123.13.33, emailAddress =	= JP, ST = JP, L = Okazaki, O = Mikawa, OU = JP, CN =	notBefore=Aug 18 06:21:00 2023 GMT,notAfter=Aug 17 06:21:00 2024 GMT	2048

Max. 10

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.



<input type="checkbox"/>	Name	Subject	Expiration Date	Key Length
<input type="checkbox"/>	moxa (1).csr	0	.	

Max: 10 1 - 1 of 1


#### UI Setting

#### Description

<b>Name</b>	Shows the name of the certificate file.
<b>Subject</b>	Shows the subject from the certificate.
<b>Expiration Date</b>	Shows the expiration date of the certificate.
<b>Key Length</b>	Shows the key length of the certificate.

## Generate CA Certificate

### Menu Path: Certificate Management > Trusted CA Certificate

Clicking the **Add** () icon on the **Certificate Management > Trusted CA Certificate** page will open this dialog box. This dialog lets you import a CA certificate from your local computer. Click **UPGRADE** to save your changes and add the new certificate.

## Generate CA Certificate

Select CA Certificate \*




CANCEL

UPGRADE

UI Setting	Description	Valid Range	Default Value
<b>Select Certificate</b>	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.



<input checked="" type="checkbox"/>	Name	Subject	Expiration Date	Key Length
<input checked="" type="checkbox"/>	moxa (1).csr	0	,	.

Max. 10 1 - 1 of 1

## 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
<b>Name</b>	Shows the name of the RSA key.
<b>Key Pair Size</b>	Shows the size used for the key pair.

## Generate RSA Key

**Menu Path: Certificate Management > Certificate Signing Request - Key Pair Generate**

Clicking the **Add (+)** icon on the **Certificate Management > Certificate Signing Request - Key Pair Generate** page will open this dialog box. This dialog lets you generate a new key pair to use when generating a CSR. Click **GENERATE** to save your changes and add the new key pair.

## Generate RSA Key

Name \*  
0 / 30

Key Pair Size \*  
▼


CANCEL


GENERATE

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Specify a name for the RSA key.	1 to 30 characters	N/A
<b>Key Pair Size</b>	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.



<input type="checkbox"/>	Name	Key Pair Size
<input checked="" type="checkbox"/>	test1	1024
<input type="checkbox"/>	test2	2048

Max. 10 1 - 2 of 2

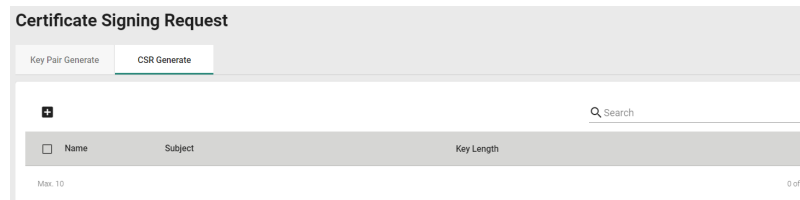
## CSR Generate

**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.

## Generate Certificate Signing Request

Private Key \*

Country Name (2 letter ...  At least 2 characters 0 / 2

Locality Name \*  0 / 16

Organization Name \*  0 / 16

Organizational Unit Na...  0 / 16

Common Name \*  0 / 16

Email Address \*  0 / 64

Subject Alternative Na...  0 / 16

CANCEL

GENERATE

UI Setting	Description	Valid Range	Default Value
<b>Private Key</b>	Select the key pair to use. To generate and manage key pairs, refer to <b>Certificate Management &gt; Certificate Signing Request - Key Pair Generate</b> .	Drop-down list of key pairs	N/A
<b>Country Name (2 letter code)</b>	Specify the 2-letter country code for the CSR.	2 characters	N/A
<b>Locality Name</b>	Specify the locality name for the CSR.	1 to 16 characters	N/A
<b>Organization Name</b>	Specify the organization name for the CSR.	1 to 16 characters	N/A
<b>Organization Unit Name</b>	Specify the organization unit name for the CSR.	1 to 16 characters	N/A
<b>Common Name</b>	Specify the common name for the CSR.	1 to 16 characters	N/A
<b>Email Address</b>	Specify the email address for the CSR.	1 to 64 characters	N/A
<b>Subject Alternative Name</b>	Specify the subject alternative name for the CSR.	1 to 16 characters	N/A

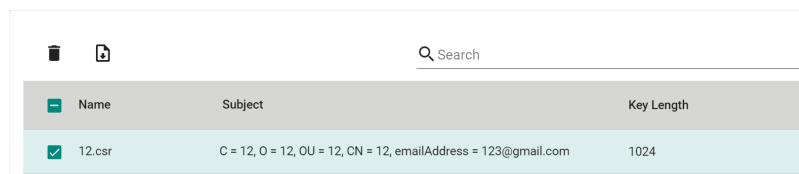
## Export Certificate Signing Request

**Menu Path: Certificate Management > Certificate Signing Request - CSR Generate**

You can export a CSR by using the checkboxes to select the entry you want to export, then clicking the **Export** (📄) icon.

### **Note**

The export icon will only be available when a single entry is selected; it will not be available if multiple entries are selected.

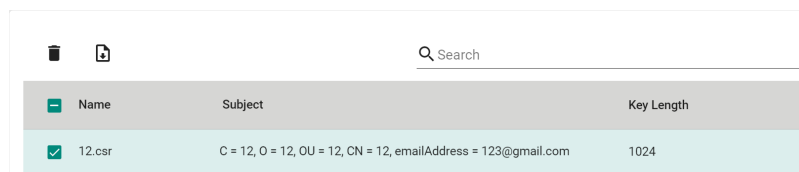


<input type="checkbox"/>	Name	Subject	Key Length
<input checked="" type="checkbox"/>	12.csr	C = 12, O = 12, OU = 12, CN = 12, emailAddress = 123@gmail.com	1024

## Delete Certificate Signing Request

**Menu Path: Certificate Management > Certificate Signing Request - CSR Generate**

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



<input type="checkbox"/>	Name	Subject	Key Length
<input checked="" type="checkbox"/>	12.csr	C = 12, O = 12, OU = 12, CN = 12, emailAddress = 123@gmail.com	1024

## Security

**Menu Path: Security**

The Security settings area lets you configure security settings to help you secure your device and your network.

This settings area includes these sections:

- Device Security
- Network Security
- Authentication



- MXview Alert Notification

## Security - User Privileges

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

Settings	Admin	Supervisor	User
<b>Device Security</b>			
<b>Login Policy</b>	R/W	R	R
<b>Trusted Access</b>	R/W	R/W	R
<b>SSH &amp; SSL</b>	R/W	R/W	-
<b>Network Security</b>			
<b>IEEE 802.1X</b>	R/W	R/W	R
<b>Authentication</b>			
<b>Login Authentication</b>	R/W	-	-
<b>RADIUS</b>	R/W	-	-
<b>TACACS+</b>	R/W	-	-
<b>MXview Alert Notification</b>	R/W	R/W	R

## Device Security

### Menu Path: Security > Device Security

This section lets you configure security settings to protect your device.

This section includes these pages:

- Login Policy
- Trusted Access
- SSH & SSL

## Login Policy

**Menu Path:** Security > Device Security > Login Policy

This page lets you configure the login policies for your device. Click **APPLY** to save your changes.

### Login Policy

Login Message  
0 / 512

Login Authentication Failure Message  
0 / 512

Login Failure Account Lockout  
Disabled

Login Failure Retry Threshold \*  
5  
1 - 10 times

Lockout Duration \*  
5  
1 - 10 min.

Auto Logout After \*  
5  
0 - 1440 min.

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Login Message</b>	Specify the welcome message to display when users log in to the device.	0 to 512 characters	N/A
<b>Login Authentication Failure Message</b>	Specify the message to display if the user fails to log in. <div style="background-color: #fff9c4; padding: 5px;"><p><b>⚠ Warning</b></p><p>The Login Authentication Failure Message should not include information about passwords or other sensitive information.</p></div>	0 to 512 characters	N/A

UI Setting	Description	Valid Range	Default Value
<b>Login Failure Account Lockout</b>	Enable or disable the lockout function, which will temporarily prevent users from logging in for the <b>Lockout Duration</b> after the <b>Login Failure Retry Threshold</b> is exceeded. This can be useful for preventing brute force attacks.	Enabled / Disabled	Disabled
<b>Login Failure Retry Threshold</b>	Specify the number of login retry attempts before the user is locked out for the <b>Lockout Duration</b> .	1 to 10	5
<b>Lockout Duration</b>	Specify the lockout duration (in minutes) during which a locked-out user will be unable to log in.	1 to 10	5
<b>Auto Logout After</b>	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.

Trusted IP List (Disabling this will allow all IP connections)

Disabled

Accept All LAN Port Connections

Enabled

Log

Disabled

Severity

Emergency

Log Destination

UI Setting	Description	Valid Range	Default Value
<b>Trusted IP List</b>	Enable or disable the Trusted IP List. <b>Enabled:</b> Only IP addresses in the Trusted IP List can access the device. <b>Disabled:</b> Any IP address can access the device.	Enabled / Disabled	Disabled
<b>Accept All LAN Port Connections</b>	Enable or disable accepting all connections from LAN connections. <b>Enabled:</b> The device can only be accessed through a LAN connection. <b>Disabled:</b> The device can be accessed through any connection.	Enabled / Disabled	Enabled
<b>Log</b>	Enable or disable Trusted Access event logging.	Enabled / Disabled	Disabled
<b>Severity</b>	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

UI Setting	Description	Valid Range	Default Value
<b>Log Destination</b>	<p>Specify where to send Trusted Access event logs. You can select multiple options.</p> <p><b>Syslog:</b> Event logs will be sent to a syslog server.</p> <p>Refer to Diagnostics &gt; Event Logs and Notifications &gt; Syslog for more information.</p> <p><b>Trap:</b> Event notifications will be sent to a trap server.</p> <p>Refer to Diagnostics &gt; SNMP Trap/Inform for more information.</p> <p><b>Local Storage:</b> Event logs will be stored on local storage and will show up in the device's Event Log.</p> <p>Refer to Diagnostics &gt; Event Logs and Notifications &gt; Event Log for more information.</p>	Syslog / Trap / Local Storage	N/A

## Trusted IP List

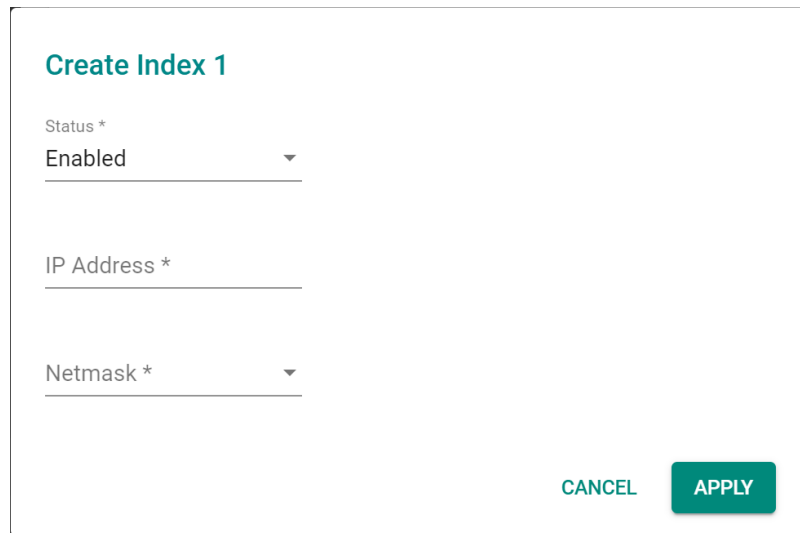
The screenshot displays a configuration window for the 'Trusted IP List'. At the top left, there are icons for adding (+) and sorting (≡). A search bar with a magnifying glass icon and the text 'Search' is located at the top right. Below these is a table with a header row containing a checkbox, 'Index', 'Status', 'IP Address', and 'Netmask'. The table body is empty. Below the table, it indicates 'Max. 10' entries and '0 of 0' are currently listed. An 'APPLY' button is positioned at the bottom left of the configuration area.

UI Setting	Description
<b>Index</b>	Shows the index of the Trusted IP entry.
<b>Status</b>	Shows whether the Trusted IP entry is enabled or disabled.
<b>IP Address</b>	Shows the IP address of the Trusted IP entry.
<b>Netmask</b>	Shows the netmask of the Trusted IP entry.

## Trusted Access - Create Index

### Menu Path: Security > Device Security > Trusted Access

Clicking the **Add (+)** icon on the **Security > Device Security > Trusted Access** page will open this dialog box. This dialog lets you add a trusted IP entry. Click **CREATE** to save your changes and add the new entry.



**Create Index 1**

Status \*  
Enabled

IP Address \*

Netmask \*

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the Trusted IP entry.	Enabled / Disabled	Enabled
<b>IP Address</b>	Specify the IP address of the trusted host(s).	Valid IP address	N/A
<b>Netmask</b>	Select a netmask for the trusted host(s).	Drop-down list of netmasks	N/A

## SSH & SSL

### Menu Path: Security > Device Security > SSH & SSL

This page lets you manage your SSH key and SSL certificate.

This page includes these tabs:

- SSH
- SSL

## SSH

### Menu Path: Security > Device Security > SSH & SSL - SSH

This page lets you manage your device's SSH key.

This shows you when the current SSH key was created. Click **REGENERATE** to generate a new SSH key for your device.

#### ▲ Warning

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

Created on  
Aug 10 07:23:59 2023 GMT  
.....

Regenerate SSH Key

**REGENERATE**

## SSL

### Menu Path: Security > Device Security > SSH & SSL - SSL

This page lets you manage your device's SSL certificate. Click **APPLY** to save your changes.

#### SSL Settings

Certificate Source \*  
Local Certificate Database ▾

Certificate File  
10.123.13.33.crt ▾

Created on  
Aug 18 06:21:00 2023 GMT  
.....

Expiration Date  
Aug 17 06:21:00 2024 GMT  
.....

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Certificate Source</b>	<p>Select the source for your device's SSL certificate.</p> <p><b>Auto Generate:</b> Your device will generate a certificate automatically.</p> <p><b>Local Certificate Database:</b> 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.</p> <p>Refer to Certificate Management for more information.</p>	Auto Generate / Local Certificate Database	Auto Generate
<b>Certificate File (if Certificate Source is Local Certificate Database)</b>	Select the imported certificate file to use.	Drop-down list of applicable imported certificates	N/A
<b>Created on (View-only)</b>	Shows when the current certificate was created.	N/A	N/A
<b>Expiration Date (View-only)</b>	Shows when the current certificate will expire.	N/A	N/A

## Network Security

### Menu Path: Security > Network Security

This section lets you manage your device's network security features.

This section includes these pages:

- IEEE 802.1X

### IEEE 802.1X

#### Menu Path: Security > Network Security > IEEE 802.1X

This page lets you manage your device's IEEE 802.1X authentication feature.

This page includes these tabs:

- General
- IEEE 802.1X Status
- RADIUS



- Local Database

## IEEE 802.1X - General

**Menu Path:** Security > Network Security > IEEE 802.1X - General

This page lets you configure your device's IEEE 802.1X settings.

### IEEE 802.1X Settings

Authentication Mode \*  
Local Database ▼

---

Authentication Retry \*  
Enabled ▼

---

Authentication Retry Interval \*  
3600

60 - 65535 sec.

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Authentication Mode</b>	Select the method of authentication to use. <b>RADIUS:</b> Use a RADIUS server for authentication. <b>Local Database:</b> Use the local database for authentication. <b>RADIUS, Local:</b> Use both a RADIUS server and the local database for authentication.	RADIUS / Local Database / RADIUS, Local	Local Database
<b>Authentication Retry</b>	Enable or disable reauthentication.	Enabled / Disabled	Enabled
<b>Authentication Retry Interval</b>	Specify the authentication retry interval in seconds.	60 to 65535	3600

## IEEE 802.1X Port List

Port	Status
3	Disabled
4	Disabled
5	Disabled
6	Disabled
8	Disabled
G1	Disabled
G2	Disabled

UI Setting	Description
------------	-------------

<b>Port</b>	Shows which port the entry is for.
-------------	------------------------------------

<b>Status</b>	Shows whether IEEE 802.1X port access control is enabled or disabled for the port.
---------------	--

## IEEE 802.1X Status

**Menu Path:** [Security](#) > [Network Security](#) > [IEEE 802.1X - IEEE 802.1X Status](#)

This page lets you see the IEEE 802.1X status of your ports.

Port	Supplicant	User	Port Status
------	------------	------	-------------

UI Setting	Description
<b>Port</b>	Shows which port the entry is for.
<b>Supplicant</b>	Shows the MAC address of the device requesting access.
<b>User</b>	Shows the user's name.
<b>Port Status</b>	Shows the status of the 802.1X port. <b>INITIALIZE:</b> The device is rebooting, the supplicant is sending an EAPoL start packet, or the port link is down. <b>CONNECTING:</b> Communication is being established with a supplicant. <b>DISCONNECTED:</b> This state is entered from the CONNECTING state, the AUTHENTICATED state, and the ABORTING state if an explicit logoff request is received from the supplicant, and from the CONNECTING state if the number of allowed reauthentication attempts has been exceeded. <b>AUTHENTICATING:</b> The supplicant is being authenticated. <b>AUTHENTICATED:</b> The supplicant was successfully authenticated. <b>ABORTING:</b> The authentication procedure is being prematurely aborted due to receipt of a reauthentication request, an EAPoL-Start frame, an EAPoL-Logoff frame, or an authTimeout. <b>HELD:</b> Authentication of the supplicant was unsuccessful.

## IEEE 802.1X - RADIUS

**Menu Path:** [Security](#) > [Network Security](#) > [IEEE 802.1X - RADIUS](#)

This page lets you specify a RADIUS server to use for IEEE 802.1X authentication. Click **APPLY** to save your changes.

### **Note**

The system will use the primary RADIUS server by default. If the primary RADIUS server is unavailable, it will use the secondary RADIUS server.

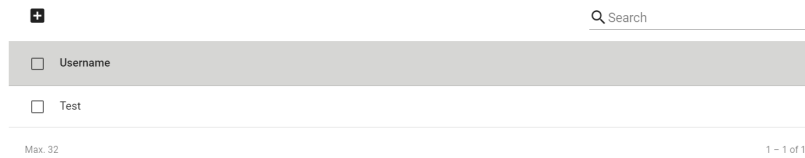
Server Address 1	Port
<input type="text" value=""/>	<input type="text" value="1812"/>
0 / 64	1 - 65535
Shared Key	<input type="password" value=""/>
0 / 30	
Server Address 2	Port
<input type="text" value=""/>	<input type="text" value="1812"/>
0 / 64	1 - 65535
Shared Key	<input type="password" value=""/>
0 / 30	
<input type="button" value="APPLY"/>	

UI Setting	Description	Valid Range	Default Value
<b>Server Address 1</b>	Specify the IP address or domain name for the primary RADIUS server.	Valid IP address or domain name	N/A
<b>UDP Port</b>	Specify the port number for the primary RADIUS server.	1 to 65535	1812
<b>Shared Key</b>	Specify the shared key for the primary RADIUS server.	0 to 60 characters	N/A
<b>Server Address 2</b>	Specify the IP address or domain name for the secondary RADIUS server.	Valid IP address or domain name	N/A
<b>UDP Port</b>	Specify the port number for the secondary RADIUS server.	1 to 65535	1812
<b>Shared Key</b>	Specify the shared key for the secondary RADIUS server.	0 to 60 characters	N/A

## Local Database

### Menu Path: [Security](#) > [Network Security](#) > [IEEE 802.1X - Local Database](#)

This page lets you create local database user accounts to use with IEEE 802.1X authentication.



UI Setting	Description
------------	-------------

<b>Username</b>	Shows the username of the account.
-----------------	------------------------------------

### Local Database - Create Account Settings

#### Menu Path: Security > Network Security > IEEE 802.1X - Local Database

Clicking the **Add** (  ) icon on the **Security > Network Security > IEEE 802.1X - Local Database** page will open this dialog box. This dialog lets you create a new user account for IEEE 802.1X authentication. Click **APPLY** to save your changes and add the new account.

#### Create Account Settings

Username  0 / 32

Password \*   0 / 64

Confirm Password \*   0 / 64

CANCEL

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Username</b>	Specify the username for this account.	1 to 32 characters	N/A
<b>Password</b>	Specify the password for this user account.	1 to 64 characters	N/A
<b>Password</b>	Re-enter the password for this user account.	1 to 64 characters	N/A

## Authentication

### Menu Path: Security > Authentication

This section lets you manage login authentication for your device.

This section includes these pages:

- Login Authentication
- RADIUS
- 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.

### Login Authentication

Authentication Protocol

Local

RADIUS

TACACS+

RADIUS, Local

TACACS+, Local

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Authentication Protocol</b>	<p>Select the method of authentication to use.</p> <p><b>Local:</b> Use the local database for authentication.</p> <p><b>RADIUS:</b> Use a RADIUS server for authentication.</p> <p><b>TACACS+:</b> Use a TACACS+ Server for authentication.</p> <p><b>RADIUS, Local:</b> Use a RADIUS server for authentication first. If it fails, the device will use the local database for authentication.</p> <p><b>TACACS+, Local:</b> Use a TACACS+ server for authentication first. If it fails, the device will use the local database for authentication.</p>	Local / RADIUS / TACACS+ / RADIUS, Local / TACACS+, Local	Local
<p><b>Warning</b></p> <p>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 be 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.</p>			

## RADIUS

### Menu Path: Security > Authentication > RADIUS

This page lets you specify a RADIUS server to use for login authentication. Click **APPLY** to save your changes.

#### Note

The system will use the primary RADIUS server by default. If the primary RADIUS server is unavailable, it will use the secondary RADIUS server.

Authentication Type \*

EAP-PEAP MSCHAPv2 ▾

Server Address 1 UDP Port  
1812  
0 / 63 1 - 65535

Shared Key   
0 / 64

Server Address 2 UDP Port  
1812  
0 / 63 1 - 65535

Shared Key   
0 / 64

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Authentication Type</b>	Select the authentication method to use for the RADIUS servers.	PAP / CHAP / EAP-PEAP MSCHAPv2	EAP-PEAP MSCHAPv2
<b>Server Address 1</b>	Specify the IP address or domain name for the primary RADIUS server.	Valid IP address or domain name	N/A
<b>UDP Port</b>	Specify the port number for the primary RADIUS server.	1 to 65535	1812
<b>Shared Key</b>	Specify the shared key for the primary RADIUS server.	0 to 64 characters	N/A
<b>Server Address 2</b>	Specify the IP address or domain name for the secondary RADIUS server.	Valid IP address or domain name	N/A
<b>UDP Port</b>	Specify the port number for the secondary RADIUS server.	1 to 65535	1812
<b>Shared Key</b>	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.

## TACACS+ Server

Server IP Address 1	TCP Port *
0.0.0.0	49
	1 - 65535
Share Key	 
0 / 64	
Auth Type *	
CHAP	▼
Timeout *	
5	
5 - 180	sec.
Retry *	
1	
0 - 5	times
Server IP Address 2	TCP Port *
0.0.0.0	49
	1 - 65535
Share Key	 
0 / 64	
Auth Type *	
CHAP	▼
Timeout *	
5	
5 - 180	sec.
Retry *	
1	
0 - 5	times

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Server IP Address 1</b>	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 <b>Server IP Address 1</b> . If the device fails to connect to the primary server, it will try to authenticate by using the secondary server specified by <b>Server IP Address 2</b> .	Valid IP address	0.0.0.0
<b>TCP Port</b>	Specify the TCP port to use for authentication requests to the primary TACACS+ server.	1 to 65535	49
<b>Shared Key</b>	Specify the shared encryption key for the primary TACACS+ server.	1 to 64 characters	N/A
<b>Auth Type</b>	Specify which authentication type the primary TACACS+ server uses.	PAP, CHAP, ASCII	CHAP
<b>Timeout</b>	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
<b>Retry</b>	Specify the number of times the device will try to contact the primary TACACS+ server.	0 to 5	1
<b>Server IP Address2</b>	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
<b>TCP Port</b>	Specify the TCP port to use for authentication requests to the secondary TACACS+ server.	1 to 65535	49
<b>Shared Key</b>	Specify the shared encryption key for the secondary TACACS+ server.	1 to 64 characters	N/A
<b>Auth Type</b>	Specify which authentication type the secondary TACACS+ server uses.	PAP, CHAP, ASCII	CHAP
<b>Time out</b>	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
<b>Retry</b>	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

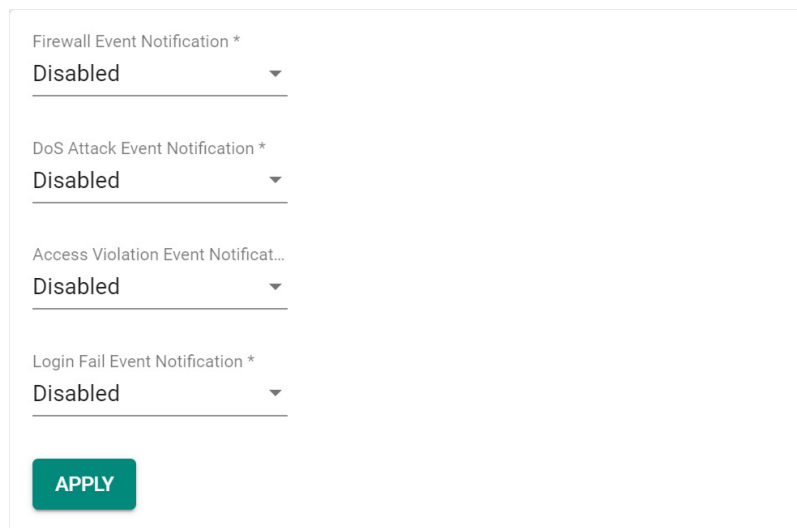
### Menu Path: Security > MXview Alert Notification - Security Notification Setting

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.



Firewall Event Notification \*

Disabled

DoS Attack Event Notification \*

Disabled





Access Violation Event Notificat...

Disabled

Login Fail Event Notification \*

Disabled


APPLY

UI Setting	Description	Valid Range	Default Value
<b>Firewall Event Notification</b>	<p>Enable or disable notifications for Firewall events.</p> <p> <b>Note</b></p> <p>After enabling this, you will need to enable logging and select <b>Trap</b> as the log destination for each firewall policy and feature you want notifications for.</p>	Enabled / Disabled	Disabled
<b>DoS Attack Event Notification</b>	<p>Enable or disable notifications for DoS attack events.</p> <p> <b>Note</b></p> <p>After enabling this, you will need to go to Firewall &gt; DoS Policy to enable logging and select <b>Trap</b> as the log destination to receive notifications.</p>	Enabled / Disabled	Disabled
<b>Access Violation Event Notification</b>	<p>Enable or disable notifications for Access Violation events.</p> <p> <b>Note</b></p> <p>After enabling this, you will need to go to Security &gt; Device Security &gt; Trusted Access to enable logging and select <b>Trap</b> as the log destination to receive notifications.</p>	Enabled / Disabled	Disabled
<b>Login Fail Event Notification</b>	<p>Enable or disable notifications for Login Fail events.</p> <p> <b>Note</b></p> <p>After enabling this, you will need to go to Diagnostics &gt; Event Logs and Notifications &gt; Event Notifications to enable logging and select <b>Trap</b> as the log destination to receive notifications.</p>	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**).

Event	Status
Firewall	safe
DoS Attack	safe
Access Violation	safe
Login Fail	safe

Max. 10    Items per page: 50    1 - 4 of 4    << < > >>

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
<b>System Status</b>			
Utilization	R/W	R/W	R
Fiber Check	R/W	R/W	R
<b>Network Status</b>			
Network Statistics	R	R	R
LLDP	R/W	R/W	R
ARP Table	R	R	R
<b>Event Log &amp; Notifications</b>			
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
SMS Settings	R/W	R/W	R
<b>Tools</b>			
Port Mirroring	R/W	R/W	R
Ping	R/W	R/W	R
Diagnostic Support	R/W	R/W	R
NetFlow	R/W	R/W	R

## System Status

**Menu Path:** [Diagnostics > System Status](#)

This section lets you check on various system statuses.

This section includes these pages:

- Utilization
- Fiber Check

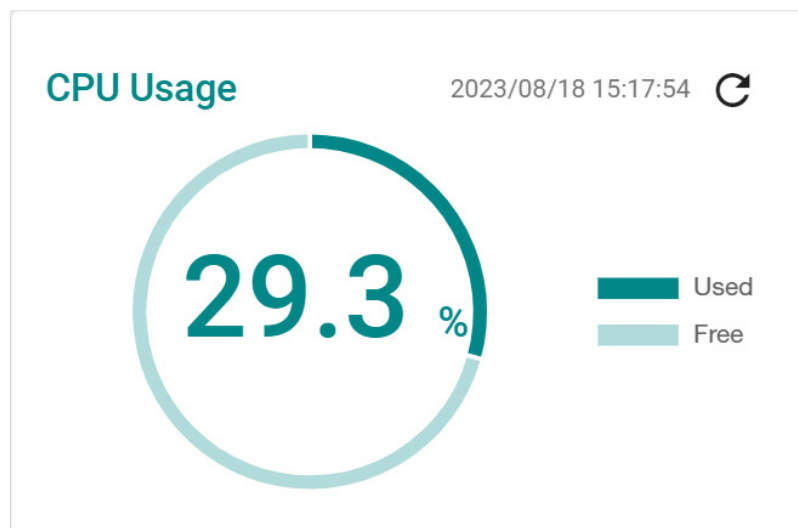
## Utilization

**Menu Path:** [Diagnostics > System Status > Utilization](#)

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

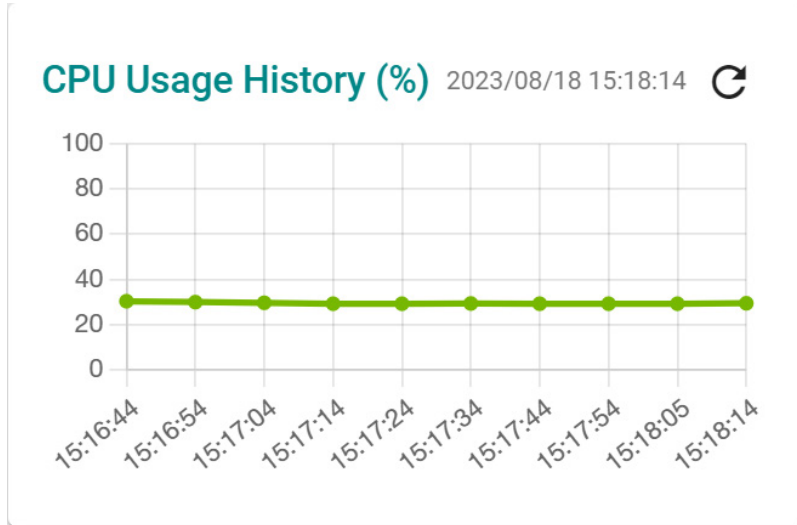
## CPU Usage

This shows the current CPU usage of your device.



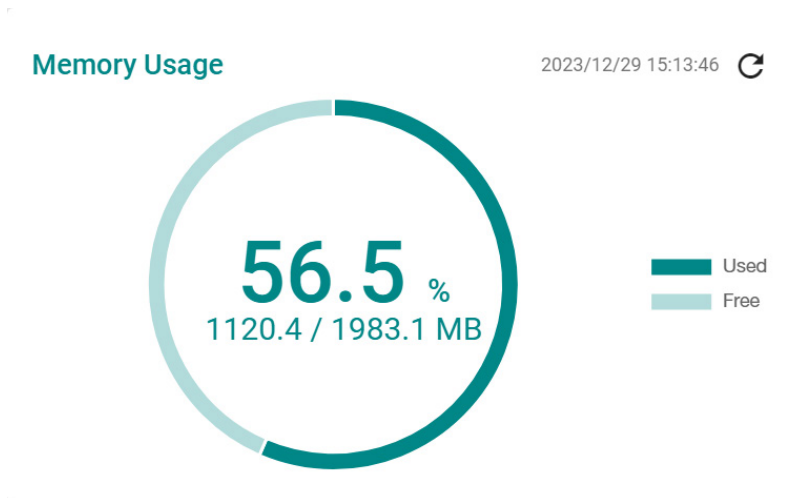
## CPU Usage History

This shows the CPU usage of your device over time.



## Memory Usage

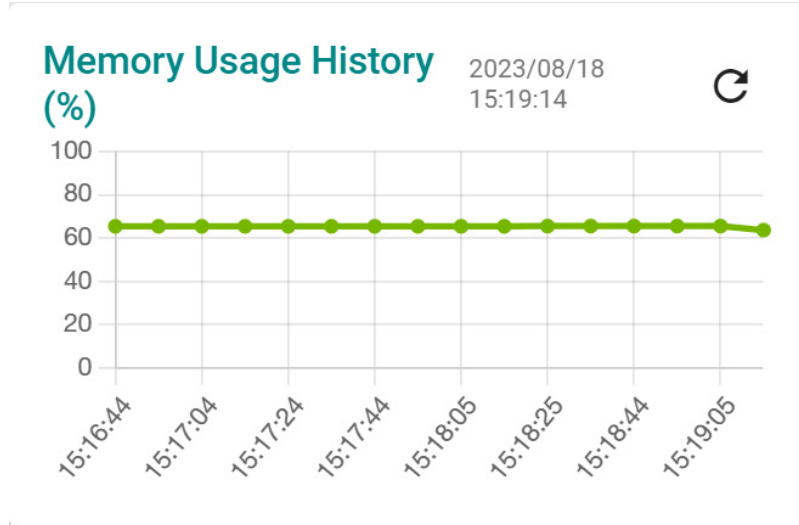
This shows your device's current memory usage.



## Memory Usage History

This shows your device's memory usage over time.





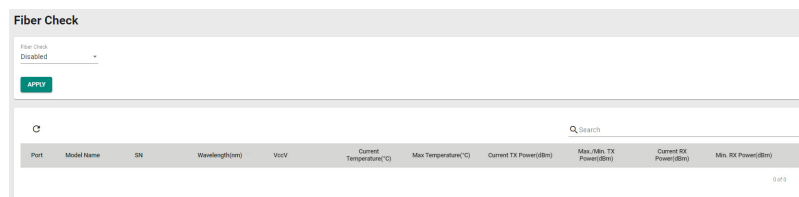
## Fiber Check

**Menu Path: Diagnostics > System Status > Fiber Check**

This page lets you diagnose the link status of the device's fiber connectors, including SFP and fixed type (multi-mode SC/ST and single-mode SC) connectors. It lets you monitor the temperature, TX/RX power, and other parameters on fiber ports to determine if the ports are working properly.

You can enable trap, email warning, and/or relay warning functions to receive an alarm or relay if one of the fiber ports exceeds the threshold for that port. Refer to **Diagnostics > Event Logs and Notifications** for more information.

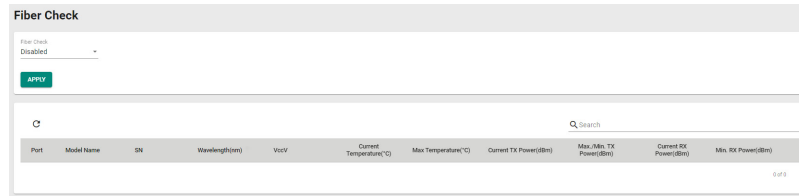
## Fiber Check Settings



UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Fiber Check</b>	Enable or disable the fiber check feature.	Enabled / Disabled	Disabled
--------------------	--	--------------------	----------

## Fiber Check Status List



UI Setting	Description
<b>Port</b>	Shows the port number of the fiber connection.
<b>Model Name</b>	Shows the name of the related SFP module.
<b>SN</b>	Shows the serial number of the related SFP module.
<b>Wavelength (nm)</b>	Shows the wavelength of the fiber connection.
<b>VccV</b>	Shows the voltage supplied to the fiber connection.
<b>Current Temperature (°C)</b>	Shows the current temperature of the fiber connection.
<b>Max. Temperature (°C)</b>	Shows the maximum temperature the fiber connection supports.
<b>Current TX Power(dBm)</b>	Shows the current transmit signal strength for the fiber connection.
<b>Max./Min. TX Power(dBm)</b>	Shows the maximum and minimum transmit signal strength for the fiber connection.
<b>Current RX Power(dBm)</b>	Shows the current receive signal strength for the fiber connection.
<b>Min. RX Power(dBm)</b>	Shows the minimum receive signal strength for the fiber connection.

## Network Status

### Menu Path: [Diagnostics > Network Status](#)

This section lets you check on the status of your device's network connections.

This section includes these pages:

- Network Statistics
- LLDP

- ARP Table

## Network Statistics

**Menu Path: Diagnostics > Network Status > Network Statistics**

This page lets you see the real-time packet and bandwidth status for your device.

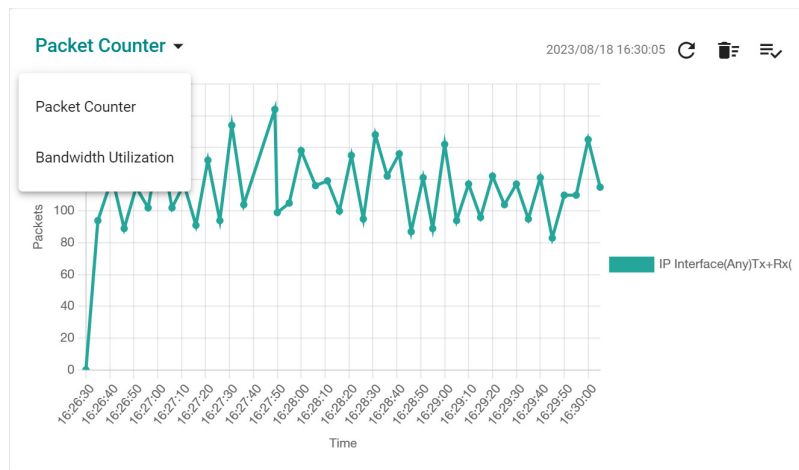
### Network Status Display



This display lets you switch between **Packet Counter** and **Bandwidth Utilization** views by clicking on the drop-down menu.

- **Packet Counter:** This view shows how many packets are being handled over time. This view updates every 5 seconds.
- **Bandwidth Utilization:** This view shows bandwidth utilization over time. This view updates every 3 seconds.

#### Note

The default line shows activity for all IP interfaces for both Tx and Rx activity. You can add additional lines by clicking the Display Settings button.



UI Setting	Description
<b>Refresh</b> (  )	Updates statistics immediately without waiting for the refresh interval.
<b>Reset Statistics Graph</b> (  )	Clears the display and resets display settings back to defaults.

UI Setting	Description
------------	-------------

<b>Display Settings</b> (☰✓)	Opens <b>Display Settings</b> , which allows you to add lines based on user-defined criteria.
------------------------------	---

## Display Settings

**Menu Path: Diagnostics > Network Status > Network Statistics**

Clicking the **Display Settings** (☰✓) icon on the **Diagnostics > Network Status > Network Statistics** page will open this dialog box. This dialog lets you define additional interfaces or ports to monitor. Click **ADD** to save your changes and add the new line.

**Display Settings**

Display Type \*  
IP Interface

Interface Selection \*  
Any

Sniffer Mode \*  
Tx+Rx

Package Type \*  
All Packets

CANCEL ADD

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

UI Setting	Description	Valid Range	Default Value
<b>Interface Selection</b> (if Display Type is IP Interface)	Select which interface to monitor.  <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b></p> <p>Available interfaces will vary depending on your product model and configuration. Refer to <b>Network Configuration &gt; Network Interfaces</b> for more information about managing your device's interfaces.</p> </div>	Drop-down list of interfaces	Any
<b>Port Selection</b> (if Display Type is Port)	Select which port to monitor.  <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b></p> <p>Available ports will vary depending on your product model.</p> </div>	Drop-down list of ports	All ports
<b>Sniffer Mode</b>	Select which type of traffic to monitor. <b>Tx+Rx:</b> Monitor both transmit and receive traffic. <b>Tx:</b> Only monitor transmit traffic. <b>Rx:</b> Only monitor receive traffic.	Tx+Rx / Tx / Rx	Tx+Rx
<b>Package Type</b>	Select which packet type to monitor. <b>All Packets:</b> Monitor all packet types. <b>Unicast:</b> Only monitor unicast packets. <b>Broadcast:</b> Only monitor broadcast packets. <b>Multicast:</b> Only monitor multicast packets. <b>Error Packets:</b> Only monitor error packets.  <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b></p> <p>If <b>Display Type</b> is <b>IP Interface</b>, only <b>All Packets</b> and <b>Error Packets</b> will be available.</p> </div>	All Packets / Unicast / Broadcast, Multicast / Error Packets	All Packets

## Packet Interface Table

This table shows how many packets are being handled by each interface. Values are shown as *Total Packets + Packets in the past 5 seconds*.

Packet Interface Table ⓘ

Search

Interface	Tx	Tx Errors	Rx	Rx Errors
WAN	2390832 + 45	0 + 0	7825083 + 246	0 + 0
LAN	10 + 0	0 + 0	2 + 0	0 + 0
lan_test	0 + 0	0 + 0	0 + 0	0 + 0
BRG_LAN	0 + 0	0 + 0	0 + 0	0 + 0

1 - 4 of 4

## LLDP Settings

**Menu Path: Diagnostics > Network Status > LLDP**

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

## LLDP Settings

### LLDP

Settings
Status

LLDP

Enabled ▼

---

Transmit Interval

30

---

5 - 32768 sec.

APPLY

UI Setting	Description	Valid Range	Default Value
<b>LLDP</b>	Enable or disable Link Layer Discovery Protocol (LLDP).	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Transmit Interval</b>	Specify the interval in seconds at which LLDP messages are sent.	5 to 32768	30
--------------------------	--	------------	----

LLDP Ring Port Bypass  
 Disabled

APPLY

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>LLDP Ring Port Bypass</b>	Enable or disable LLDP Ring Port Bypass	Enabled / Disabled	Disabled
------------------------------	---	--------------------	----------

## LLDP Status List

Port	Nbr. ID	Nbr. Port	Nbr. Port Description	Nbr. System
3	0090a8000004	1	100TX	100T Router
8	883a3031ca03	152	4/3	TRAFIC-SIG-SW1(AA-C)

UI Setting	Description
------------	-------------

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

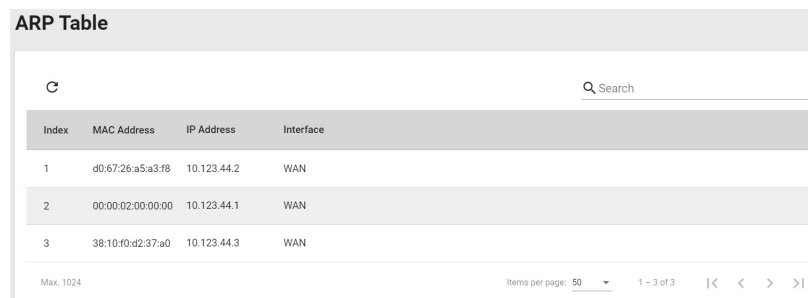
## ARP Table

### 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.



The screenshot shows the ARP Table interface. At the top, there is a title "ARP Table" and a search bar with a magnifying glass icon and the text "Search". Below the search bar is a table with the following columns: Index, MAC Address, IP Address, and Interface. The table contains three entries:

Index	MAC Address	IP Address	Interface
1	d0:67:26:a5:a3:f8	10.123.44.2	WAN
2	00:00:02:00:00:00	10.123.44.1	WAN
3	38:10:f0:d2:37:a0	10.123.44.3	WAN

At the bottom of the table, there is a pagination control showing "Max. 1024" and "Items per page: 50" with a dropdown arrow. To the right, it shows "1 - 3 of 3" and navigation arrows: "<<" (disabled), "<" (disabled), ">" (disabled), and ">>" (disabled).

#### UI Setting

#### Description

<b>Index</b>	Shows the index of the device entry.
<b>MAC Address</b>	Shows the MAC address of the device.
<b>IP Address</b>	Shows the IP address used for the device.
<b>Interface</b>	Shows the interface the device is connecting through.

## 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
- SMS 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](#)

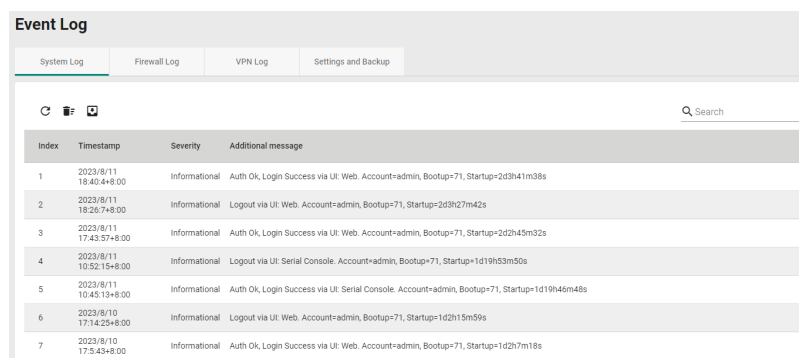
This page lets you view your device's system-related event logs.

## 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.



The screenshot shows the 'Event Log' interface with tabs for System Log, Firewall Log, VPN Log, and Settings and Backup. The System Log tab is active. At the top, there are icons for refresh, clear, and export, along with a search bar. Below is a table with the following data:

Index	Timestamp	Severity	Additional message
1	2023/8/11 18:40:4+8:00	Informational	Auth Ok, Login Success via Ui: Web. Account=admin, Bootup=71, Startup=2d3h41m38s
2	2023/8/11 18:28:7+8:00	Informational	Logout via Ui: Web. Account=admin, Bootup=71, Startup=2d3h27m42s
3	2023/8/11 17:43:57+8:00	Informational	Auth Ok, Login Success via Ui: Web. Account=admin, Bootup=71, Startup=2d2h45m32s
4	2023/8/11 10:52:15+8:00	Informational	Logout via Ui: Serial Console. Account=admin, Bootup=71, Startup=1d19h53m50s
5	2023/8/11 10:45:13+8:00	Informational	Auth Ok, Login Success via Ui: Serial Console. Account=admin, Bootup=71, Startup=1d19h46m48s
6	2023/8/10 17:14:25+8:00	Informational	Logout via Ui: Web. Account=admin, Bootup=71, Startup=1d2h15m59s
7	2023/8/10 17:5:43+8:00	Informational	Auth Ok, Login Success via Ui: Web. Account=admin, Bootup=71, Startup=1d2h7m18s

## UI Setting

## Description

### Index

Shows the index of the event.

### Timestamp

Shows the time of the event, including the date, time, and UTC time zone adjustment.

### Severity

Shows the severity categorization of the event.

### Additional message

Shows additional information about the event, based on the type of event. The username of the account will also be recorded for the following events: **Login Success**, **Login Fail**, **Configuration Change**, **User Logout**.

## Firewall Log

**Menu Path: Diagnostics > Event Logs and Notifications > Event Log - Firewall Log**

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

## 🔔 Limitations

Each firewall log can record up to 1000 events.

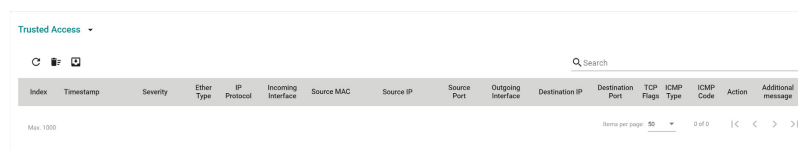
You can switch between different firewall logs by clicking on the drop-down menu.

- Trusted Access
- Malformed Packets
- DoS Policy
- Layer 3-7 Policy
- Protocol Filter Policy
- ADP
- IPS
- Session Control
- Layer 2 Policy

## Actions

- Click the **Refresh icon** (🔄) to refresh the logs.
- Click the **Clear System Log icon** (🗑️) to delete all logs.
- Click the **Export icon** (📄) to export all logs to a file.

## Trusted Access



Index	Timestamp	Severity	Ether Type	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP Flags	ICMP Type	ICMP Code	Action	Additional message
-------	-----------	----------	------------	-------------	--------------------	------------	-----------	-------------	--------------------	----------------	------------------	-----------	-----------	-----------	--------	--------------------

### 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.

UI Setting	Description
<b>Severity</b>	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
<b>Ether Type</b>	Shows the EtherType that applies to this event.
<b>IP Protocol</b>	Shows the IP protocol for this traffic.
<b>Incoming Interface</b>	Shows the incoming interface for this traffic.
<b>Source MAC</b>	Shows the source MAC address for this traffic.
<b>Source IP</b>	Shows the source IP address for this traffic.
<b>Source Port</b>	Shows the source port for this traffic.
<b>Outgoing Interface</b>	Shows the destination interface for this traffic.
<b>Destination IP</b>	Shows the destination IP address for this traffic.
<b>Destination Port</b>	Shows the destination port for this traffic.
<b>TCP Flags</b>	Shows the TCP flags that apply to this event.
<b>ICMP Type</b>	Shows the ICMP type that applies to this event.
<b>ICMP Code</b>	Shows the ICMP code that applies to this event.
<b>Action</b>	Shows the action taken by the firewall for this event.
<b>Additional message</b>	Shows additional information about the event, based on the type of event.

## Malformed Packets

Malformed Packets

Index	Timestamp	Severity	Ether Type	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP Flags	ICMP Type	ICMP Code	Action	Additional message
1	2023/9/10 11:34:27+8:00	Emergency	2048	TCP	WAN	d0:67:26:a5:a3:f8	3.129.140.152	8883	---	10.123.13.33	46340	RST, ACK, URG	---	---	DROP	
2	2023/9/10 11:34:24+8:00	Emergency	2048	TCP	WAN	38:10c0:d2:37:a0	3.129.140.152	8883	---	10.123.13.33	46338	RST, ACK, URG	---	---	DROP	
3	2023/9/10 11:34:22+8:00	Emergency	2048	TCP	WAN	d0:67:26:a5:a3:f8	10.160.127.71	47893	---	10.123.13.33	80	RST, ACK, URG	---	---	DROP	

UI Setting	Description
<b>Index</b>	Shows the index of the event.
<b>Timestamp</b>	Shows the time of the event, including the date, time, and UTC time zone adjustment.
<b>Severity</b>	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
<b>Ether Type</b>	Shows the EtherType that applies to this event.
<b>IP Protocol</b>	Shows the IP protocol for this traffic.
<b>Incoming Interface</b>	Shows the incoming interface for this traffic.
<b>Source MAC</b>	Shows the source MAC address for this traffic.
<b>Source IP</b>	Shows the source IP address for this traffic.
<b>Source Port</b>	Shows the source port for this traffic.
<b>Outgoing Interface</b>	Shows the destination interface for this traffic.
<b>Destination IP</b>	Shows the destination IP address for this traffic.
<b>Destination Port</b>	Shows the destination port for this traffic.
<b>TCP Flags</b>	Shows the TCP flags that apply to this event.
<b>ICMP Type</b>	Shows the ICMP type that applies to this event.
<b>ICMP Code</b>	Shows the ICMP code that applies to this event.
<b>Action</b>	Shows the action taken by the firewall for this event: <ul style="list-style-type: none"> <li>• Accept</li> <li>• Drop</li> </ul>
<b>Additional message</b>	Shows additional information about the event, based on the type of event.

## DoS Policy

UI Setting	Description
<b>Index</b>	Shows the index of the event.
<b>Timestamp</b>	Shows the time of the event, including the date, time, and UTC time zone adjustment.
<b>Severity</b>	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
<b>Ether Type</b>	Shows the EtherType that applies to this event.
<b>Subcategory</b>	Shows the subcategory that applies to this event: <ul style="list-style-type: none"> <li>• Null Scan</li> <li>• Xmas Scan</li> <li>• NMAP-Xmas Scan</li> <li>• SYN/FIN Scan</li> <li>• FIN Scan</li> <li>• NMAP-ID Scan</li> <li>• SYN/RST Scan</li> <li>• NEW-TCP-Without-SYN Scan</li> <li>• ICMP-Death</li> <li>• SYN-Flood</li> <li>• ARP-Flood</li> <li>• UDP-Flood</li> </ul>
<b>IP Protocol</b>	Shows the IP protocol for this traffic.
<b>Incoming Interface</b>	Shows the incoming interface for this traffic.
<b>Source MAC</b>	Shows the source MAC address for this traffic.
<b>Source IP</b>	Shows the source IP address for this traffic.
<b>Source Port</b>	Shows the source port for this traffic.

UI Setting	Description
<b>Outgoing Interface</b>	Shows the destination interface for this traffic.
<b>Destination IP</b>	Shows the destination IP address for this traffic.
<b>Destination Port</b>	Shows the destination port for this traffic.
<b>TCP Flags</b>	Shows the TCP flags that apply to this event.
<b>ICMP Type</b>	Shows the ICMP type that applies to this event.
<b>ICMP Code</b>	Shows the ICMP code that applies to this event.
<b>Action</b>	Shows the action taken by the firewall for this event.
<b>Additional message</b>	Shows additional information about the event, based on the type of event.

## Layer 3-7 Policy

Index	Timestamp	Severity	Policy ID	Policy Name	Ether Type	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP Flags	ICMP Type	ICMP Code	Action
Max: 1000																	

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

UI Setting	Description
<b>Incoming Interface</b>	Shows the incoming interface for this traffic.
<b>Source MAC</b>	Shows the source MAC address for this traffic.
<b>Source IP</b>	Shows the source IP address for this traffic.
<b>Source Port</b>	Shows the source port for this traffic.
<b>Outgoing Interface</b>	Shows the destination interface for this traffic.
<b>Destination IP</b>	Shows the destination IP address for this traffic.
<b>Destination Port</b>	Shows the destination port for this traffic.
<b>TCP Flags</b>	Shows the TCP flags that apply to this event.
<b>ICMP Type</b>	Shows the ICMP type that applies to this event.
<b>ICMP Code</b>	Shows the ICMP code that applies to this event.
<b>Action</b>	Shows the action taken by the firewall for this event: <ul style="list-style-type: none"> <li>• Allow</li> <li>• Deny</li> </ul>

## Protocol Filter Policy

Index	Timestamp	Severity	Application Protocol	Policy ID	Policy Name	Ether Type	IP Protocol	Incoming Interface	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	Action
Max: 1000														

UI Setting	Description
<b>Index</b>	Shows the index of the event.
<b>Timestamp</b>	Shows the time of the event, including the date, time, and UTC time zone adjustment.
<b>Severity</b>	Shows the severity categorization of the event: Refer to the Severity Level List for more information.



UI Setting	Description
<b>Application Protocol</b>	Shows which application this event is related to.
<b>Policy ID</b>	Shows the ID of the firewall policy that applies to this event.
<b>Policy Name</b>	Shows the name of the firewall policy that applies to this event.
<b>Ether Type</b>	Shows the EtherTypes for this traffic.
<b>IP Protocol</b>	Shows the IP protocol for this traffic.
<b>Incoming Interface</b>	Shows the incoming interface for this traffic.
<b>Source MAC</b>	Shows the source MAC address for this traffic.
<b>Source IP</b>	Shows the source IP address for this traffic.
<b>Source Port</b>	Shows the source port for this traffic.
<b>Outgoing Interface</b>	Shows the destination interface for this traffic.
<b>Destination IP</b>	Shows the destination IP address for this traffic.
<b>Destination Port</b>	Shows the destination port for this traffic.
<b>TCP Flags</b>	Shows the TCP flags for this traffic.
<b>ICMP Type</b>	Shows the ICMP type that applies to this event.
<b>ICMP Code</b>	Shows the ICMP code that applies to this event.
<b>Action</b>	Shows the action taken by the firewall for this event.

## ADP

Index	Timestamp	Application Protocol	Policy ID	Policy Name	Ether Type	IP Protocol	Incoming Interface	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	Action
1	2022/10/6 16:01:19+08:00	IEC-104	1000002	The magic number is not 0x68.	2048	TCP	LAN	192.168.127.200	443	WAN	10.123.34.120	2404	Monitor
2	2022/10/6 16:01:19+08:00	IEC-104	1000002	The magic number is not 0x68.	2048	TCP	LAN	192.168.127.200	443	WAN	10.123.34.120	2404	Monitor

UI Setting	Description
<b>Index</b>	Shows the index of the event.
<b>Timestamp</b>	Shows the time of the event, including the date, time, and UTC time zone adjustment.
<b>Application Protocol</b>	Shows the application protocol that applies to this event.
<b>Policy ID</b>	Shows the ID of the firewall policy that applies to this event.
<b>Policy Name</b>	Shows the name of the firewall policy that applies to this event.
<b>Ether Type</b>	Shows the EtherType that applies to this event.
<b>Subcategory</b>	Shows the subcategory that applies to this event.
<b>IP Protocol</b>	Shows the IP protocol for this traffic.
<b>Incoming Interface</b>	Shows the incoming interface for this traffic.
<b>Source IP</b>	Shows the source IP address for this traffic.
<b>Source Port</b>	Shows the source port for this traffic.
<b>Outgoing Interface</b>	Shows the destination interface for this traffic.
<b>Destination IP</b>	Shows the destination IP address for this traffic.
<b>Destination Port</b>	Shows the destination port for this traffic.
<b>Action</b>	Shows the action taken by the firewall for this event: <ul style="list-style-type: none"> <li>• <b>Accept:</b> The traffic will be allowed to pass through.</li> <li>• <b>Reset:</b> The traffic will not be allowed to pass through.</li> <li>• <b>Monitor:</b> The traffic will be allowed to pass through, but a log entry will be created for it.</li> </ul>

## IPS

Index	Timestamp	IPS Severity	IPS Category	Policy ID	Policy Name	Ether Type	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP Flags	Action
1	2023/8/10 9:12:48.00	High	Exploits	1139266	DHCP-ISC DHCP Client Network Configuration Script Command Injection-2 (CVE-2011-0997)	2048	UDP	WAN	08:07:26:a5:a3:18	10.124.0.33	67	-	255.255.255.255	68	-	Reset

UI Setting	Description
<b>Index</b>	Shows the index of the event.
<b>Timestamp</b>	Shows the time of the event, including the date, time, and UTC time zone adjustment.
<b>IPS Severity</b>	Shows the IPS severity of the event: <ul style="list-style-type: none"> <li>• Information</li> <li>• Low</li> <li>• Medium</li> <li>• High</li> <li>• Critical</li> </ul>
<b>IPS Category</b>	Shows the IPS category of the event: <ul style="list-style-type: none"> <li>• File vulnerabilities</li> <li>• Buffer overflow</li> <li>• DoS attacks</li> <li>• Exploits</li> <li>• Malware traffic</li> <li>• Reconnaissance</li> <li>• Web threats</li> <li>• Flooding &amp; scan</li> <li>• Protocol attack protection</li> <li>• IP spoofing</li> </ul>
<b>Policy ID</b>	Shows the ID of the firewall policy that applies to this event.
<b>Policy Name</b>	Shows the name of the firewall policy that applies to this event.
<b>Ether Type</b>	Shows the EtherType that applies to this event.
<b>IP Protocol</b>	Shows the IP protocol for this traffic.
<b>Incoming Interface</b>	Shows the incoming interface for this traffic.
<b>Source MAC</b>	Shows the source MAC address for this traffic.
<b>Source IP</b>	Shows the source IP address for this traffic.
<b>Source Port</b>	Shows the source port for this traffic.
<b>Outgoing Interface</b>	Shows the destination interface for this traffic.

UI Setting	Description
<b>Destination IP</b>	Shows the destination IP address for this traffic.
<b>Destination Port</b>	Shows the destination port for this traffic.
<b>TCP Flags</b>	Shows the TCP flags that apply to this event.
<b>Action</b>	Shows the action taken by the firewall for this event.

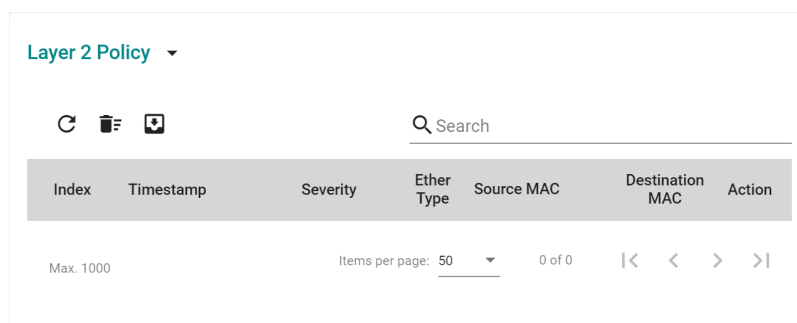
## Session Control

The screenshot shows a table titled "Session Control" with a search bar and a table header. The header includes the following columns: Index, Timestamp, Severity, Policy ID, Policy Name, Ether Type, IP Protocol, Incoming Interface, Source MAC, Source IP, Source Port, Outgoing Interface, Destination IP, Destination Port, TCP Flags, ICMP Type, and Action. Below the header, there is a "Max: 1000" label and a "Items per page: 50" dropdown menu, along with navigation arrows.

UI Setting	Description
<b>Index</b>	Shows the index of the event.
<b>Timestamp</b>	Shows the time of the event, including the date, time, and UTC time zone adjustment.
<b>Severity</b>	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
<b>Policy ID</b>	Shows the ID of the firewall policy that applies to this event.
<b>Policy Name</b>	Shows the name of the firewall policy that applies to this event.
<b>Ether Type</b>	Shows the EtherType that applies to this event.
<b>IP Protocol</b>	Shows the IP protocol for this traffic.
<b>Incoming Interface</b>	Shows the incoming interface for this traffic.
<b>Source MAC</b>	Shows the source MAC address for this traffic.
<b>Source IP</b>	Shows the source IP address for this traffic.
<b>Source Port</b>	Shows the source port for this traffic.

UI Setting	Description
<b>Outgoing Interface</b>	Shows the destination interface for this traffic.
<b>Destination IP</b>	Shows the destination IP address for this traffic.
<b>Destination Port</b>	Shows the destination port for this traffic.
<b>TCP Flags</b>	Shows the TCP flags that apply to this event.
<b>ICMP Type</b>	Shows the ICMP type that applies to this event.
<b>ICMP Code</b>	Shows the ICMP code that applies to this event.
<b>Action</b>	Shows the action taken by the firewall for this event.

## Layer 2 Policy



UI Setting	Description
<b>Index</b>	Shows the index of the event.
<b>Timestamp</b>	Shows the time of the event, including the date, time, and UTC time zone adjustment.
<b>Severity</b>	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
<b>Ether Type</b>	Shows the EtherType that applies to this event.
<b>Source MAC</b>	Shows the source MAC address for this traffic.
<b>Destination MAC</b>	Shows the destination MAC address for this traffic.

UI Setting	Description
------------	-------------

- |               |  |
|---------------|--|
| <b>Action</b> | Shows the action taken by the firewall for this event: <ul style="list-style-type: none"> <li>• Allow</li> <li>• Deny</li> </ul> |
|---------------|--|

## VPN Log

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

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

### ⚠ Limitations

The VPN log can record up to 1000 events.

### Actions

- Click the **Refresh icon** (🔄) to refresh the logs.
- Click the **Clear System Log icon** (🗑️) to delete all logs.
- Click the **Export icon** (📄) to export all logs to a file.

Index	Timestamp	Severity	Additional message
1	2020/2/3 18:42:41+8:00	Notice	[vpn1] Initiating VPN connection
2	2020/2/3 18:42:41+8:00	Notice	[vpn1] VPN remote gateway unreachable
3	2020/2/3 18:39:56+8:00	Notice	[vpn1] Initiating VPN connection

UI Setting	Description
------------	-------------

- |                  |  |
|------------------|--|
| <b>Index</b>     | Shows the index of the event.  |
| <b>Timestamp</b> | Shows the time of the event, including the date, time, and UTC time zone adjustment. |
| <b>Severity</b>  | Shows the severity categorization of the event.                                      |

UI Setting	Description
------------	-------------

**Additional message** Shows additional information about the event, based on the type of event.

## Settings and Backup

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

This page lets you clear all the logs or enable automatic event log backups. You can also set up capacity warnings and oversize actions that trigger when log storage has exceeded the specified storage threshold.

#### Clear All Log

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

Clear All Log

**CLEAR**

#### Auto Event Log Backup

Auto Event Log Backup

Automatically Back Up \*

Disabled ▼

---

**APPLY**

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Automatically Restore</b>	Enable or disable automatic event log backups.	<b>Enable / Disabled</b>	Disabled
------------------------------	--	--------------------------	----------

## Threshold Settings

Threshold Settings					
		Q Search			
	Status	Category Name	Warning Threshold	Oversize Action	Registered Action
	Disabled	System	--	Overwrite the oldest event log	Trap,Email
	Disabled	VPN	--	Overwrite the oldest event log	Trap,Email
	Enabled	Trusted Access	50%	Overwrite the oldest event log	Trap,Email
	Enabled	Malformed Packets	50%	Stop recording event logs	Trap,Email
	Disabled	DoS Policy	--	Overwrite the oldest event log	Trap,Email
	Disabled	Layer 3-7 Policy	--	Overwrite the oldest event log	Trap,Email
	Disabled	Protocol Filter Policy	--	Overwrite the oldest event log	Trap,Email
	Disabled	ADP	--	Overwrite the oldest event log	Trap,Email
	Disabled	IPS	--	Overwrite the oldest event log	Trap,Email
	Disabled	Session Control	--	Overwrite the oldest event log	Trap,Email
	Disabled	Layer 2 Policy	--	Overwrite the oldest event log	Trap,Email

### UI Setting

### Description

#### Status

Shows whether threshold settings are enabled for the category.

#### Category Name

Shows which event log the threshold settings apply to.

#### Warning Threshold

Shows the threshold percentage that must be reached to trigger a warning sent through the **Registered Action** methods.

#### Oversize Action

Shows what action will be taken when log storage is full for the selected category.

#### Registered Action

Shows how threshold warnings will be sent.

## Edit Threshold Settings

### Menu Path: [Diagnostics](#) > [Event Logs and Notifications](#) > [Event Log - Settings and Backup](#)

Clicking the **Edit** ( ) icon for an entry on the **Insert > Path Here** page will open this dialog box. This dialog lets you edit the threshold settings the selected event log category. Click **APPLY** to save your changes.



## Edit System Threshold Settings

Capacity Warning \*  
Disabled ▼

Registered Action  
Trap, Email ▼

Oversize Action \*  
Overwrite the oldest event log ▼

CANCEL

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Capacity Warning</b>	Enable or disable capacity warnings for the selected event log category.	Enabled / Disabled	Disabled
<b>Registered Action</b>	Select how the warning is sent. You can select multiple options. <b>Trap:</b> A trap warning will be sent. <b>Email:</b> A warning email will be sent.	Trap / Email	Trap / Email
<b>Oversize Action</b>	Select the oversize action to take when event log storage is full for the selected category. <b>Overwrite the oldest event log:</b> The oldest events will be deleted when new events are created. <b>Stop recording event logs:</b> 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			
<input type="text" value="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		

UI Setting	Description
<b>Status</b>	Shows whether event notifications are enabled for this kind of event.
<b>Group</b>	Shows which group this event belongs to.
<b>Event Name</b>	Shows the name of the event. Refer to the System Event List for more details.
<b>Severity</b>	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
<b>Registered Action</b>	<p>Shows which action will be taken for this kind of event.</p> <p><b>Trap:</b> A notification is sent to the Trap server when the event is triggered.</p> <p><b>Email:</b> A notification is sent to the email server defined in the Email Settings section.</p> <p><b>Syslog:</b> An event log is recorded to the Syslog server defined in the Syslog section.</p> <p><b>Relay:</b> A notification is sent through the relay interface, if the device has one, when the event is triggered.</p>
	<p> <b>Note</b></p> <p>The types of actions available may vary depending on the event type and the device model.</p>

## Event Notifications - System - Edit Event Notification

**Menu Path:** [Diagnostics](#) > [Event Logs and Notifications](#) > [Event Notifications - System](#)

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

### Edit Event Notification

Event Name  
Cold Start

---

Status \*  
Disabled ▼

Registered Action ▼

Severity \*  
Emergency ▼

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Event Name (View-only)</b>	Shows the name of the event. Refer to the System Event List for more information.	(Fixed)	(Fixed)
<b>Status</b>	Enable or disable notifications for this event.	Enabled / Disabled	Disabled
<b>Registered Action</b>	<p>Select which action to take when the event occurs. Multiple actions may be selected.</p> <p><b>Trap:</b> A notification will be sent to the Trap server.</p> <p><b>Email:</b> A notification email will be sent to the email server defined in the Email Settings section.</p> <p><b>Syslog:</b> The event log is recorded to a Syslog server defined in the Syslog section.</p> <p><b>Relay:</b> An alarm notification will be triggered through the relay output of the device, if your device is equipped with one.</p>	Trap / Email / Syslog / Relay	N/A
<b>Severity</b>	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 on your device will also light up if your device has one.

Event Notifications					
System	Port				
					Search
Status	Port	Link-On	Link-Off	Severity	Registered Action
	Disabled	1	Disabled	Disabled	Emergency
	Disabled	2	Disabled	Disabled	Emergency
	Disabled	3	Disabled	Disabled	Emergency
	Disabled	4	Disabled	Disabled	Emergency
	Disabled	5	Disabled	Disabled	Emergency
	Disabled	6	Disabled	Disabled	Emergency
	Disabled	7	Disabled	Disabled	Emergency
	Disabled	8	Disabled	Disabled	Emergency
	Disabled	G1	Disabled	Disabled	Emergency
	Disabled	G2	Disabled	Disabled	Emergency
	Disabled	G3	Disabled	Disabled	Emergency
	Disabled	G4	Disabled	Disabled	Emergency

### UI Setting

### Description

<b>Status</b>	Shows whether event notifications are enabled for this kind of event.
<b>Port</b>	Shows which group this event belongs to.
<b>Link-On</b>	Shows whether notifications for Link-On events are enabled or disabled.
<b>Link-Off</b>	Shows whether notifications for Link-Off events are enabled or disabled.
<b>Severity</b>	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
<b>Registered Action</b>	Shows how notifications will be sent for this kind of event.

## Event Notifications - Port - Edit Event Notification

**Menu Path:** [Diagnostics > Event Logs and Notifications > Event Notifications - Port](#)

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

### Edit Event Notification

Port  
1

Status \*  
Disabled

Link-On \*  
Disabled

Link-Off \*  
Disabled

Registered Action

Severity \*  
Emergency

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Port</b> (View-only)	Shows which physical port the event notifications are for.  <b>Note</b> Available ports will vary depending on your product and model.	N/A	N/A

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable notifications for this port.	Enabled / Disabled	Disabled
<b>Link-On</b>	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
<b>Link-Off</b>	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
<b>Registered Action</b>	Select which action to take when the event occurs. Multiple actions may be selected.  <b>Trap:</b> A notification will be sent to the Trap server.  <b>Email:</b> A notification email will be sent to the email server defined in the Email Settings section.  <b>Syslog:</b> The event log is recorded to a Syslog server defined in the Syslog section.  <b>Relay:</b> 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
<b>Severity</b>	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.

Status	Event Name	Threshold(%)	Duration(Sec)	Severity	Registered Action
Disabled	CPU Usage Alarm	80	10	Warning	



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

The screenshot shows a dialog box titled "Edit Event Notification" with the following fields and values:

- Event Name: CPU Usage Alarm
- Status\*: Disabled
- Threshold(%)\*: 80
- Duration(Sec)\*: 10
- Registered Action: (empty)
- Severity\*: Warning

At the bottom right of the dialog, there are two buttons: "CANCEL" and "APPLY".

UI Setting	Description	Valid Range	Default Value
<b>Event Name (View-only)</b>	Shows the CPU usage event name.	N/A	N/A
<b>Status</b>	Enable or disable event notifications for CPU usage.	Enabled / Disabled	Disabled
<b>Threshold(%)</b>	Shows the CPU usage threshold percentage that must be exceeded for event notifications.	60 to 90	80
<b>Duration(Sec)</b>	Shows the amount of time in seconds CPU usage must exceed the threshold to trigger a notification.	10 to 60	10
<b>Severity</b>	Shows the severity assigned to the event. Refer to the Severity Level List for more details.	Email / Syslog	N/A
<b>Registered Action</b>	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.

Event Notifications										
System	Port	CPU Usage	Port Usage							
										Q Search
Status	Event Name	Port	Tx	Tx Threshold(%)	Tx Duration(Sec)	Rx	Rx Threshold(%)	Rx Duration(Sec)	Severity	Registered Action
Disabled	Port Usage Alarm	3	Disabled	50	10	Disabled	50	10	Warning	
Disabled	Port Usage Alarm	4	Disabled	50	10	Disabled	50	10	Warning	
Disabled	Port Usage Alarm	5	Disabled	50	10	Disabled	50	10	Warning	
Disabled	Port Usage Alarm	6	Disabled	50	10	Disabled	50	10	Warning	
Disabled	Port Usage Alarm	8	Disabled	50	10	Disabled	50	10	Warning	
Disabled	Port Usage Alarm	G1	Disabled	50	10	Disabled	50	10	Warning	
Disabled	Port Usage Alarm	G2	Disabled	50	10	Disabled	50	10	Warning	
										Items per page: 50 1 - 7 of 7  < < > >

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

**Edit Event Notification**

Port  
3

Event Name  
Port Usage Alarm

Status \*  
Disabled

Tx \*  
Disabled

Tx Threshold(%) \*  
50

Tx Duration(Sec) \*  
10

Rx \*  
Disabled

Rx Threshold(%) \*  
50

Rx Duration(Sec) \*  
10

Registered Action

Severity \*  
Warning

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Port</b> (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
<b>Event Name</b> (View-only)	Shows the event name.	N/A	N/A
<b>Tx</b>	Enable or disable Tx monitoring for event notifications.	Enabled / Disabled	Disabled
<b>Tx Threshold(%)</b>	Specify the Tx threshold percentage that must be exceeded for event notifications.	1 to 100	50

UI Setting	Description	Valid Range	Default Value
<b>Tx Duration</b>	Specify the amount of time in seconds Tx traffic must exceed the Tx threshold to trigger a notification.	1 to 300	10
<b>Rx</b>	Enable or disable Rx monitoring for event notifications.	Enabled / Disabled	Disabled
<b>Rx Threshold(%)</b>	Specify the Rx threshold percentage that must be exceeded for event notifications.	1 to 100	50
<b>Rx Duration(Sec)</b>	Specify the amount of time in seconds Rx traffic must exceed the Rx threshold to trigger a notification.	1 to 300	10
<b>Registered Action</b>	Select which action to take when the event occurs. Multiple actions may be selected.  <b>Email:</b> A notification email will be sent to the email server defined in the Email Settings section.  <b>Syslog:</b> The event log is recorded to a Syslog server defined in the Syslog section.	Email / Syslog	N/A
<b>Severity</b>	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**

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

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

**Limitations**

You can connect to up to 3 syslog servers.

### Syslog

Syslog 1	Certificate 1
Disabled	Disabled
Address 1	UDP Port 1
	514
	1 - 65535
Syslog 2	Certificate 2
Disabled	Disabled
Address 2	UDP Port 2
	514
	1 - 65535
Syslog 3	Certificate 3
Disabled	Disabled
Address 3	UDP Port 3
	514
	1 - 65535

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Syslog</b>	Enable or disable the specified syslog server.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
<b>Certificate</b>	Select a syslog server certificate to use for the related server, or disable use of certificates.	Drop-down list of certificates / Disabled	Disabled
<b>Address</b>	Enter the IP address of the related syslog server.	Valid IP address	N/A
<b>UDP Port</b>	Specify the UDP port of the related syslog server.	1 to 65535	514

## SNMP Trap/Inform

**Menu Path:** [Diagnostics](#) > [Event Logs and Notifications](#) > [SNMP Trap/Inform](#)

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

This page includes these tabs:

- General
- SNMP Account

### SNMP Trap/Inform - General

**Menu Path:** [Diagnostics](#) > [Event Logs and Notifications](#) > [SNMP Trap/Inform - General](#)

This page lets you configure the SNMP Trap/Inform settings of your device. Click **APPLY** to save your changes.

## SNMP Trap/Inform

General

SNMP Account

Trap Mode \*  
Trap V1 ▼

Trap Community 1 \*  
public 6 / 64

Recipient IP/Name 1 Recipient IP/Name 2

Recipient IP/Name 3

Inform Retries Inform Timeout  
3 10

1 - 99 times 1 - 300 sec.

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Trap Mode</b>	<p>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.</p> <p><b>Trap V1:</b> Use Trap V1 for SNMP notifications.</p> <p><b>Trap V2:</b> Use Trap V2 for SNMP notifications.</p> <p><b>Inform V2:</b> Use Inform V2 for SNMP notifications.</p> <p><b>Trap V3:</b> Use Trap V3 for SNMP notifications.</p> <p><b>Inform V3:</b> Use Inform V3 for SNMP notifications.</p>	Trap V1 / Trap V2 / Inform V2 / Trap V3 / Inform V3	Trap V1
<b>Trap Community 1</b>	Specify the community string that will be used for authentication.	1 to 64 characters	public
<b>Recipient IP/Name 1/2/3</b>	Specify the name of the recipient trap server that will receive notifications.	Recipient IP or name	N/A
<b>Inform Retries (if Trap Mode is Inform V2 or Inform V3)</b>	Specify the number of times to retry sending an inform notification.	1 to 99	3



UI Setting	Description	Valid Range	Default Value
<b>Inform Timeout</b> (if Trap Mode is Inform V2 or Inform V3)	Specify the amount of time to wait (in seconds) to wait for an acknowledgement before trying to resend an inform notification.	1 to 300	10

## SNMP Account

**Menu Path:** [Diagnostics](#) > [Event Logs and Notifications](#) > [SNMP Trap/Inform - SNMP Account](#)

This section lets you configure an SNMP trap account for your device.

### Limitations

You can configure up to 1 SNMP trap account.

	Name	Authentication Type	Encryption Method
<input type="checkbox"/>	test	None	Disabled

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


## Create SNMP Trap Account Settings



**Menu Path:** [Diagnostics](#) > [Event Logs and Notifications](#) > [SNMP Trap/Inform - SNMP Account](#)

Clicking the **Add (+)** icon on the **Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Account** page will open this dialog box. This dialog lets you add an SNMP trap account for your device. Click **CREATE** to save your changes and add the new account.

### Create SNMP Trap Account Settings

Name \*  
 0 / 32

Authentication Type \*  
 SHA  Authentication Key \*    
At least 8 characters 0 / 64

Encryption Method \*  
 Enabled  Encryption Key \*     
At least 8 characters 0 / 64

[CANCEL](#) [CREATE](#)

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

**Edit SNMP Trap Account Settings**

Name \*  
test  
4 / 31

Authentication Type \*  
MD5

Authentication Key \*  
At least 8 characters 0 / 30

Encryption Method \*  
Enabled

Encryption Key \*  
At least 8 characters 0 / 30

CANCEL APPLY

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

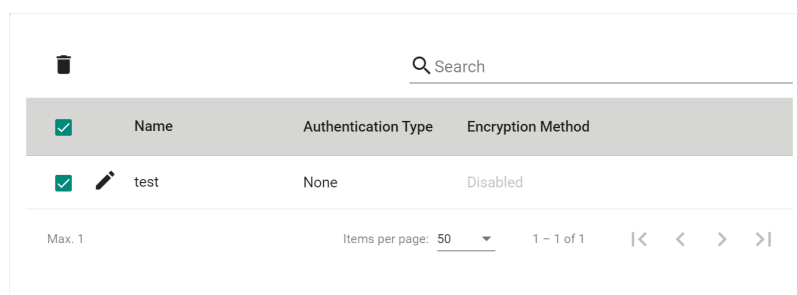
UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Encryption Key (if Encryption Method is Enabled)</b>	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 PLAIN methods of SASL (Simple Authentication and Security Layer) authentication.

We strongly recommend not entering your Account Name and Account Password if auto warning e-mail messages can be delivered without using an authentication mechanism.

## Email Settings

Mail Server  0 / 60

TCP Port  1 - 65535

Username  0 / 60 Password  0 / 60

Sender Address  0 / 60

1st Recipient Email Add...  0 / 60 2nd Recipient Email Ad...  0 / 60


3rd Recipient Email Add...  0 / 60 4th Recipient Email Add...  0 / 60

UI Setting	Description	Valid Range	Default Value
<b>Mail Server</b>	Specify the address of the email server. You can enter a domain name or IP address.	1 to 60 characters	N/A
<b>TCP Port</b>	Specify the TCP port of the email server.	1 to 65535	25
<b>Username</b>	Specify the username used to log in to the email server.	0 to 60 characters	N/A
<b>Password</b>	Specify the password used to log in to the email server.	0 to 60 characters	N/A
<b>Sender Address</b>	Specify the sender email address to use for email notifications.	0 to 60 characters	N/A
<b>Recipient Email Address</b>	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

## SMS Settings


**Menu Path: Diagnostics > Event Logs and Notifications > SMS Settings**


This page lets you configure your device's SMS notification settings. You can specify which phone number to send SMS notifications to.

 **Note**

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

### SMS Settings




<input type="checkbox"/>	Name	Country Code	Number
<input type="checkbox"/>	 Test	886	12345678

Max. 4

UI Setting	Description
<b>Name</b>	Shows the SMS recipient's name.
<b>Country Code</b>	Shows the SMS recipient number's country code.
<b>Number</b>	Shows the SMS recipient's phone number.

## Add SMS Number

**Menu Path: Diagnostics > Event Logs and Notifications > SMS Settings**

Clicking the **Add** () icon on the **Diagnostics > Event Logs and Notifications > SMS Settings** page will open this dialog box. This dialog lets you add an SMS recipient

for your device notification. Click **CREATE** to save your changes and add the new SMS recipient.

### Add SMS Number

Name \*  0 / 15

+ Country Code \*  Number \*

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Name</b>	Enter the SMS recipient's name.	1 to 15 characters	N/A
<b>Country Code</b>	Enter the SMS recipient number's country code.	Country code	N/A
<b>Number</b>	Enter the SMS recipient's phone number.	Phone number	N/A

### Delete SMS Number

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

#### SMS Settings

<input checked="" type="checkbox"/>	Name	Country Code	Number
<input checked="" type="checkbox"/>	Test	886	12345678

Max. 4

## Tools

### Menu Path: [Diagnostics > Tools](#)

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

This section includes these pages:

- [Port Mirroring](#)
- [Ping](#)
- [Diagnostic Support](#)
- [NetFlow](#)

## Port Mirroring

### Menu Path: [Diagnostics > Tools > Port Mirroring](#)

This page lets you configure the port mirror function, which can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the mirror port) to receive the same data being transmitted from, or both to and from, the port under observation.

Using a mirror port allows the network administrator to sniff the observed port to keep tabs on network activity.

#### **Note**

For security reasons, it is recommended to use port mirroring to send traffic to an intrusion detection system (IDS) for analysis.



# Port Mirroring

## Port Mirroring Configuration

Enable\*

Enabled ▼

Monitored Port \*

Monitored Traffic \*

All Streams ▼

Mirror Destination Port \*

1 ▼

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Enable</b>	Enable or disable the port mirror function.	Enabled / Disabled	Disabled
<b>Monitored Port</b>	Select the numbers for the ports you want to monitor for network activity. Multiple ports can be selected.	(Selectable ports will vary depending on the device model)	N/A
<b>Monitored Traffic</b>	Select the type of traffic that will be monitored. <b>Ingress Stream:</b> Select this option to monitor only those data packets coming into the Moxa industrial secure router's port. <b>Egress Stream:</b> Select this option to monitor only those data packets being sent out through the Moxa industrial secure router's port. <b>All Streams:</b> Select this option to monitor data packets both coming into and being sent out through the Moxa industrial secure router's port.	Ingress Stream / Egress Stream / All Streams	All Streams

UI Setting	Description	Valid Range	Default Value
<b>Mirror Destination Port</b>	Select the number of the port that will be used to monitor the activity of the monitored port.	(Selectable ports will vary depending on the device model)	1

## Ping

### Menu Path: [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
<b>IP Address/Domain Name</b>	Specify the IP address or domain name you want to ping, then click the <b>PING</b> button. The ping result will be displayed below.	Valid IP address or domain name up to 50 characters	N/A

## Diagnostic Support

### Menu Path: [Diagnostics > Tools > Diagnostic Support](#)

This page lets you generate files and import files for troubleshooting.

This page includes these tabs:

- System Profile
- Module Firmware

**Note**

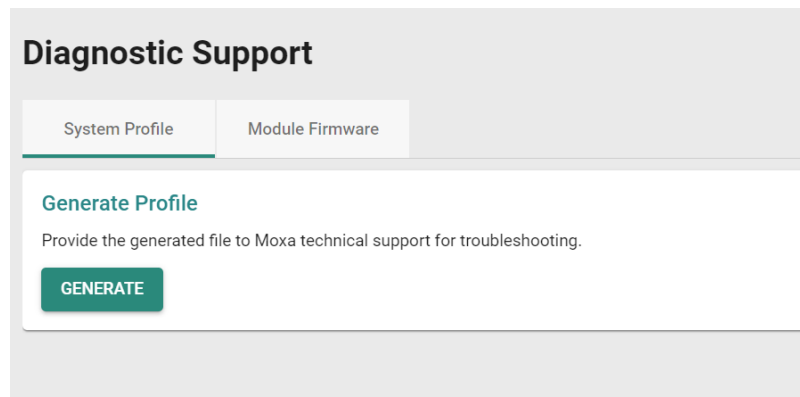
Please note that settings and available options may vary depending on the product model.

## System Profile

### Menu Path: [Diagnostics](#) > [Tools](#) > [Diagnostic Support - System Profile](#)

This page lets you generate a system profile file, which includes device information such as system logs, system status, and configurations. This file can be used to assist troubleshooting.

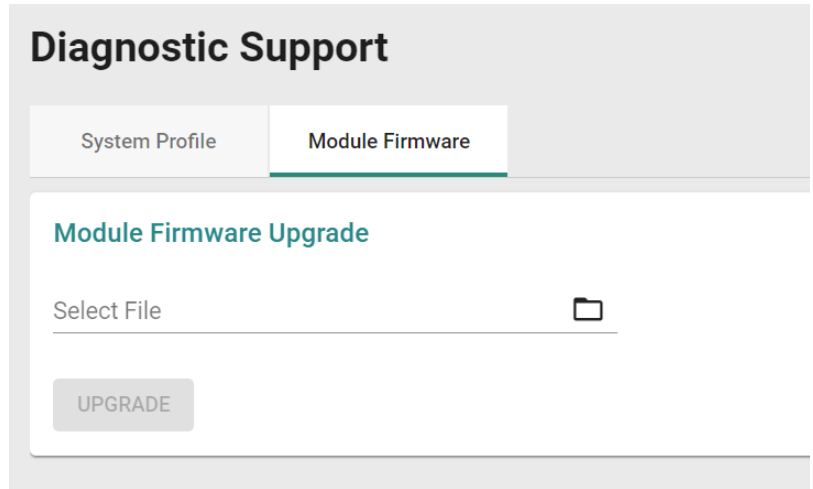
Click the **GENERATE** button to generate and save a system profile file to your local host.



## Module Firmware

### Menu Path: [Diagnostics](#) > [Tools](#) > [Diagnostic Support - Module Firmware](#)

This page lets you upgrade the firmware of the cellular module using a firmware file provided by Moxa Technical Support.



UI Setting	Description	Valid Range	Default Value
<b>Select File</b>	Select the firmware upgrade file from your local host, then click <b>UPGRADE</b> to upgrade the module's firmware.	N/A	N/A

## NetFlow

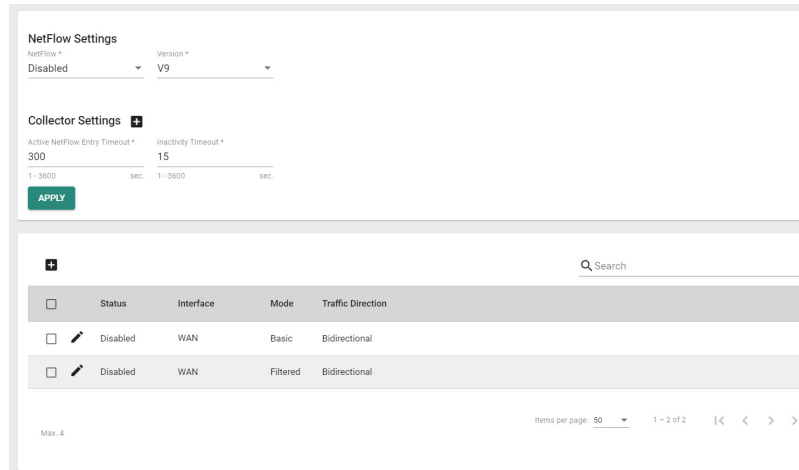
### Menu Path: Diagnostics > Tools > NetFlow

This page lets you create and edit NetFlows for your device.

#### 🔑 Limitations

You can create up to 1 entry per interface.

## NetFlow Settings



## NetFlow Settings

UI Setting	Description	Valid Range	Default Value
<b>NetFlow</b>	Enable or disable NetFlow.	Enabled / Disabled	Disabled
<b>Version</b>	Specify which version of NetFlow to use.	V5 / V9 / IPFIX	V9

## Collector Settings

UI Setting	Description	Valid Range	Default Value
<b>Collector 1 IP/ Host Name</b>	Specify the collector 1 IP or host name.	Valid IP address or host name	N/A
<b>Collector 1 Port</b>	Specify the collector 1 port number.	1 to 65535	9996
<b>Collector 2 IP/ Host Name</b>	Specify the collector 2 IP or host name.	Valid IP address or host name	N/A
<b>Collector 2 Port</b>	Specify the collector 2 port number.	1 to 65535	9996
<b>Active NetFlow Entry Timeout</b>	Specify the active NetFlow entry timeout in seconds. This is the maximum duration a flow can remain "active" in the router's flow cache.	1 to 3600 seconds	300

UI Setting	Description	Valid Range	Default Value
<b>Inactivity Timeout</b>	Specify the inactivity timeout in seconds. This is the maximum duration a flow can remain "inactive" without new packet matches.	1 to 3600 seconds	15

## Create NetFlow Entry

### Menu Path: **Diagnostics > Tools > NetFlow**

Clicking the **Add (+)** icon on the **Diagnostics > Tools > NetFlow** page will open this dialog box. This dialog lets you create a new NetFlow entry. Click **CREATE** to save your changes and add the new NetFlow entry.

#### Create NetFlow Entry

Status \*  
 Disabled

Interface \*  
 WAN

Traffic Direction \*  
 Bidirectional

Mode \*  
 Basic

Sampling Rate \*  
 0  
 0 - 65535

CANCEL CREATE

## Create NetFlow Entry

Status \*  
Disabled

Interface \*  
WAN

Traffic Direction \*  
Bidirectional

Mode \*  
Filtered

### Source IP Filter

Source IP \*  
Subnet Mask \*  
24 (255.255.255.0)

Source Port \*  
0 - 65535

### Destination IP Filter

Destination IP \*  
Subnet Mask \*  
24 (255.255.255.0)

Destination Port \*  
0 - 65535


### Protocol Filter

Protocol \*  
All

CANCEL

CREATE

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

UI Setting	Description	Valid Range	Default Value
<b>Interface</b>	Specify the interface for the NetFlow entry.	Drop-down list of interfaces	WAN
<b>Traffic Direction</b>	Select the traffic direction for the NetFlow entry.	Bidirectional / Ingress / Egress	Bidirectional
<b>Mode</b>	Select the mode for the NetFlow entry. <b>Basic:</b> This mode enables you to configure a NetFlow entry for your device. <b>Filtered:</b> This mode allows you to filter traffic by IP address or specific protocol.	Basic / Filtered	Basic
<b>Sampling Rate (Only when Mode is set as Basic)</b>	Specify the sampling rate of the NetFlow entry. 0 means the sampling rate will be set to 1.  <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>A lower number indicates more frequent sampling, with 1 representing sampling every packet, thus providing full visibility and accuracy. However, more intensive sampling may adversely affect performance.</p> </div>	0 to 65535	N/A
<b>Source IP (Only when Mode is set as Filtered)</b>	Specify the source IP.	Valid IP address	N/A
<b>Subnet Mask (Only when Mode is set as Filtered)</b>	Specify the subnet mask for the source IP.	Valid subnet mask	N/A
<b>Source Port (Only when Mode is set as Filtered)</b>	Specify the port for the source IP. Setting this to 0 means all ports will be allowed.	Valid port	N/A
<b>Destination IP (Only when Mode is set as Filtered)</b>	Specify the destination IP.	Valid IP address	N/A
<b>Subnet Mask (Only when Mode is set as Filtered)</b>	Specify the subnet mask for the destination IP.	Valid subnet mask	N/A



UI Setting	Description	Valid Range	Default Value
<b>Destination Port</b> <b>(Only when Mode is set as Filtered)</b>	Specify the port for the destination IP. Setting this to 0 means all ports will be allowed.	Valid port	N/A
<b>Protocol</b> <b>(Only when Mode is set as Filtered)</b>	Select the protocol to filter.	All / TCP / UDP	N/A

## Delete NetFlow

### Menu Path: [Diagnostics](#) > [Tools](#) > [NetFlow](#)

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

The screenshot shows a table with a search bar at the top right. The table has a header row with columns: Status, Interface, Mode, and Traffic Direction. Below the header, there is one row with the following values: Disabled, WAN, Basic, Bidirectional. At the bottom of the table, there are pagination controls: 'Items per page: 50', '1 - 1 of 1', and navigation arrows. The text 'Max. 4' is visible in the bottom left corner of the table area.

Status	Interface	Mode	Traffic Direction
<input checked="" type="checkbox"/> Disabled	WAN	Basic	Bidirectional

# Chapter 4

---

## Other Features

### Industrial Application

#### Menu Path: Industrial Application

This menu settings area lets you configure settings related to specific industrial applications.

This settings area includes these sections:

- IEC 61375

#### **Note**

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

### IEC 61375 Setting

#### Menu Path: Industrial Application > IEC 61375

This section lets you configure IEC 61375 settings related to Ethernet Train Backbone Nodes (ETBN).

The IEC 61375 section includes these pages:

- Ethernet Train Backbone
- Communication Profile
- Operational Status

### **⚠ Warning**

Do not connect ETBNs through ETB ports before the ETBN has been configured.

If Turbo Ring V2 and ETBN are enabled at the same time, Turbo Ring V2 must be configured before ETBN for Turbo Ring V2 to work normally.

## **Ethernet Train Backbone**

**Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone**

This page lets you configure Ethernet Train Backbone settings for your device.

This page includes these tabs:

- [TTDP Settings](#)
- [Local ETBN Status](#)
- [ETB Status](#)
- [TCN Multicast Table](#)

## **TTDP Settings**

**Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone - TTDP Settings**

This page lets you set up Train Topology Discovery Protocol (TTDP) for your router. Click **APPLY** to save your changes.

### **⚠ Warning**

Enabling TTDP will overwrite settings for Port Trunk, VLAN, Interface, QoS, VRRP, and Turbo Ring V2.

## Note

We recommend setting ETB ports to MDI mode, and using crossover cables for the interconnection of ETBNs.

### Ethernet Train Backbone

TTDP Settings	Local ETBN Status	ETB Status	TCN Multicast Table
TTDP Enable Disabled	ETB Backbone ID 0 (TCMS)		

UI Setting	Description	Valid Range	Default Value
<b>TTDP Enable</b>	Enable or Disable TTDP.	Enable / Disable	Disable
<b>ETB Backbone ID</b>	Specify an ETB backbone ID to use.	0 (TCMS) / 1 (Multimedia) / 2 (Not specialized) / 3 (Not specialized)	0 (TCMS)

## Local Consist

### Local Consist

Consist UUID  
0 X ⓘ

8bit-4bit-4bit-4bit-12bit

ETBN(s) in Consist  
1 ECN(s) in Consist

User can manually assign or generate random Consist UUID

UI Setting	Description	Valid Range	Default Value
<b>Consist UUID</b>	Shows the UUID of the local consist.  Consists with the same UUID will be considered to be the same consist. Therefore, the consist UUIDs for different consists should be unique.  You can manually assign a consist UUID, or you can generate a random one by clicking on the <b>X</b> button to erase the existing UUID, then clicking the <b>Refresh</b> (🔄) icon to generate a random UUID.	Valid 8bit-4bit-4bit-4bit-12bit UUID	0
<b>ETBN(s) in Consist</b>	Specify the number of ETBNs in this consist.	1 to 32	1

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>ECN(s) in Consist</b>	Specify the number of ECNs in this consist.	1 to 32	N/A
--------------------------	---	---------	-----

## Local ETBN

**Local ETBN** i

Local ETBN Static ID	Direction 1	ETB Port Speed
1	Trunk 1	Auto
<hr/>		
ETB Port VLAN ID	Direction 2	Port MDI/MDIX
1000	Trunk 2	Auto
<hr/>		
1-4094, 492 is reserved		

UI Setting	Description	Valid Range	Default Value
------------	-------------	-------------	---------------

<b>Local ETB Static ID</b>	Specify the static ID of this ETBN within the consist.	Drop-down list of ETBN Static IDs (depends on the <b>ETBN(s) in Consist</b> setting in <a href="#">Industrial Application &gt; IEC 61375 &gt; Ethernet Train Backbone - TTDP Setting</a> )	1
<b>Direction 1</b>	Specify the consist direction for Direction 1.  The default setting is ports 1 and 2 will point towards direction 1, and ports 5 and 6 will point towards direction 2.	Trunk 1 / Trunk 2	Trunk 1
<b>ETB Port Speed</b>	Specify the ETB port speed to use. When set to <b>Auto</b> , the port will use its default speed. For example, a 1G port set to <b>Auto</b> will use 1G for its port speed.	Auto / 1G / 100M	Auto
<b>ETB Port VLAN ID</b>	Specify the VLAN ID for the ETB ports.  We recommend using the same VLAN ID for all ETBNs on each train.	1-4094, 492 is reserved	1000



## Add ECN

### Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone - TTDP Settings

Clicking the **Add (+)** icon on the **Industrial Application > IEC 61375 > Ethernet Train Backbone - TTDP Settings** page will open this dialog box. This dialog lets you create a new ECN entry. Click **CREATE** to save your changes and add the new entry.

UI Setting	Description	Valid Range	Default Value
<b>ECN to ETBN</b>	Specify which ETBN in the consist will be connected by the ECN.	Drop-down list of ETBN Static IDs (depends on the <b>ETBN(s) in Consist</b> setting in <a href="#">Industrial Application &gt; IEC 61375 &gt; Ethernet Train Backbone - TTDP Setting</a> )	N/A
<b>ECN port VLAN ID</b>	Specify the VLAN ID of the ECN port. Specifying a VLAN ID is required if the selected ECN is connected to this ETBN.	Valid VLAN ID	N/A
<b>ECN interface IP address</b>	Set the interface IP address for the ECN.	Valid IP address	N/A



UI Setting	Description	Valid Range	Default Value
<b>ECN Ports</b>	Specify which ports the selected ECN will connect to. Specifying ports is required if the selected ECN is connected to this ETBN.  Available ports will vary depending on the product model. The port used by the ETBN cannot be selected.	Drop-down list of ports	N/A

## Edit ECN

### Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone - TTDP Settings

Clicking the **Edit** (✎) icon for an entry on the **Industrial Application > IEC 61375 > Ethernet Train Backbone - TTDP Settings** page will open this dialog box. This dialog lets you edit an existing ECN entry. Click **APPLY** to save your changes.

### Edit ECN 1

ECN to ETBN  
ETB 2

---

ECN Port VLAN ID  
1

---

Default 1000 + static ID  
ECN interface IP address  
1.1.1.1 i

---

ECN Ports  
port 2,3 i

---

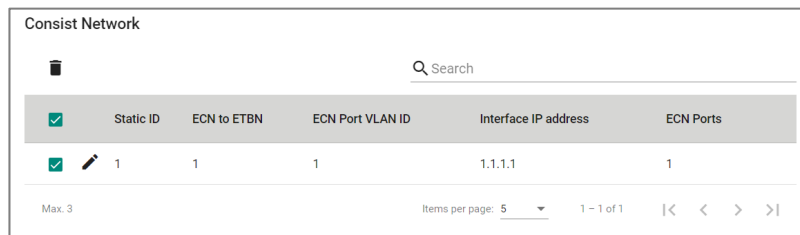
CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>ECN to ETBN</b>	Specify which ETBN in the consist will be connected by the ECN.	Drop-down list of ETBN Static IDs (depends on the <b>ETBN(s) in Consist</b> setting in <a href="#">Industrial Application &gt; IEC 61375 &gt; Ethernet Train Backbone - TTDP Setting</a> )	N/A
<b>ECN port VLAN ID</b>	Specify the VLAN ID of the ECN port. Specifying a VLAN ID is required if the selected ECN is connected to this ETBN.	Valid VLAN ID	N/A
<b>ECN interface IP address</b>	Set the interface IP address for the ECN.	Valid IP address	N/A
<b>ECN Ports</b>	Specify which ports the selected ECN will connect to. Specifying ports is required if the selected ECN is connected to this ETBN.  Available ports will vary depending on the product model. The port used by the ETBN cannot be selected.	Drop-down list of ports	N/A

## Delete ECN

### Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone - TTDP Settings

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



## Local ETBN Status

**Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone - Local ETBN Status**

This page lets you see the status of your local ETBN.

### Local ETBN Status

Ethernet Train Backbone			
TTDP Settings	Local ETBN Status	ETB Status	TCN Multicast Table
Local ETBN Status			2023/09/20 17:41:13
ETBN State	etbnInhibition	InaugInhibition	
Inaugurated	Not Inhibited	Not Inhibited	
remoteInhibition	Lengthen	Shorten	
Undefined	False	False	

UI Setting	Description
<b>ETBN State</b>	Shows the inauguration status of the ETBN state machine.
<b>etbnInhibition</b>	Shows information about any inhibition requests from this node.
<b>inaugInhibition</b>	Shows flags that are the result of the <b>etbnInhibition</b> field of topology frames received from all other ETBNs and the CN local value.  During power-up, <b>inaugInhibition</b> is meaningless until the ETBN reaches the <b>INAUGURATED</b> state at least once. The value at startup is set to <b>False</b> to allow for the first inauguration.
<b>remoteInhibition</b>	This shows whether the remote composition is allowed to inaugurate (only set by end nodes) when lengthening takes place.  The initial value should be set as <b>UNDEFINED</b> , which means it shall not be taken into account.
<b>Lengthen</b>	Shows the lengthen status due to a lengthening by an inaugurated composition (can be set by any node), such as the appearance of a new consist.  Set to <b>TRUE</b> if a node detects a new node with a consist UUID different from those contained in the Train Network Directory.

UI Setting	Description
------------	-------------

**Shorten** Shows the shorten status due to a shortening, which is the loss of at least one consist at the end of a train (can be set by any node).  
 Set to **TRUE** if a node detects at least one consist is lost at the end of the train according to the Train Network Directory.  
 It resets to **FALSE** ("stable") by default if the consist appears again or the Train Network Directory is updated.

### ETBN Line Status

ETBN Line Status				
Search				
Line	Line Status (DIR 1)	Line Status (DIR 2)	Hello Frame (DIR 1)	Hello Frame (DIR 2)
A	Off	On	-	Valid
B	Off	On	-	Valid

Items per page: 5 1 - 2 of 2 |< < > >|

UI Setting	Description
------------	-------------

**Line** Shows which ETBN line (A or B) the entry is for.

**Line Status (DIR 1)** Shows the link status of the line for Direction 1 of the ETBN line.

**Line Status (DIR 2)** Shows the link status of the line for Direction 2 of the ETBN line.

**Hello Frame (DIR 1)** Shows whether the neighbor Ethernet port in Direction 1 for the ETBN is up, and will send Hello Frames.

**Hello Frame (DIR 2)** Shows whether the neighbor Ethernet port in Direction 2 for the ETBN is up, and will send Hello Frames.

## Local ETBN Redundant Role

Local ETBN Redundant Role				
<div style="text-align: right; margin-bottom: 5px;"> <input type="text" value="Search"/> </div> <table border="1"> <thead> <tr> <th>CN ID</th> <th>Local ETBN Redundant Role</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Not Redundant</td> </tr> </tbody> </table> <div style="text-align: right; margin-top: 5px;">             Items per page: 5    1 - 1 of 1    &lt;&lt; &lt; &gt; &gt;&gt;         </div>	CN ID	Local ETBN Redundant Role	1	Not Redundant
CN ID	Local ETBN Redundant Role			
1	Not Redundant			

UI Setting	Description
<b>CN ID</b>	Shows the ID of the consist node, which is statically defined.
<b>Local ETBN Redundant Role</b>	Shows which CN is connected to the Local ETBN and whether the CN has ETBN redundancy.

## ETB Status

### Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone - ETB Status

This page lets you see the status of your ETB.

### ETB Status

Ethernet Train Backbone									
TTDP Settings	Local ETBN Status	ETB Status	TCN Multicast Table						
<div style="display: flex; justify-content: space-between;"> <div> <b>ETB Status</b> </div> <div> <span>2023/09/20 17:49:10</span> </div> </div> <table border="1"> <thead> <tr> <th>remoteInhibition</th> <th>Lengthen</th> <th>Shorten</th> </tr> </thead> <tbody> <tr> <td>Undefined</td> <td>False</td> <td>False</td> </tr> </tbody> </table>				remoteInhibition	Lengthen	Shorten	Undefined	False	False
remoteInhibition	Lengthen	Shorten							
Undefined	False	False							

UI Setting	Description
<b>remoteInhibition</b>	<p>This shows whether the remote composition is allowed to inaugurate (only set by end nodes) when lengthening takes place.</p> <p>The initial value should be set as <b>UNDEFINED</b>, which means it shall not be taken into account.</p>

UI Setting	Description
<b>Lengthen</b>	Shows the lengthen status due to a lengthening by an inaugurated composition (can be set by any node), such as the appearance of a new consist.  Set to <b>TRUE</b> if a node detects a new node with a consist UUID different from those contained in the Train Network Directory.
<b>Shorten</b>	Shows the shorten status due to a shortening, which is the loss of at least one consist at the end of a train (can be set by any node).  Set to <b>TRUE</b> if a node detects at least one consist is lost at the end of the train according to the Train Network Directory.  It resets to <b>FALSE</b> ("stable") by default if the consist appears again or the Train Network Directory is updated.

## Connectivity Table

Connectivity Table

ConnTableValid: True    ConnTableCrc32: 8411CB11

Search

Index	Orientation	Mac Address
1	Direct	00:90:E8:03:04:05
2	Direct	00:90:E8:49:08:A1
3	Inverse	00:90:E8:49:16:F8
4	Inverse	00:90:E8:49:08:F2

Items per page: 5    1 - 4 of 4

UI Setting	Description
<b>ConnTableValid</b>	Shows whether the Physical Topology is shared by all ETBNs (same connectivity table CRC is used for all ETBNs).
<b>ConnTableCrc32</b>	Shows the CRC32 value of the internal Connectivity Table.
<b>Index</b>	Shows the Index number of a node. The number of entries will vary between models and depending on how many ports have been set up.
<b>Orientation</b>	Shows information about the orientation of the node with respect to the ETB reference direction.
<b>MAC address</b>	Shows the MAC address of the node.

## Train Network Directory

**Train Network Directory**

EtbTopoCntValid  
True

EtbTopoCnt      Memorized EtbTopoCnt  
BEDE0458      BEDE0458

🔍 Search

Index	CstUUID	CN ID	Subnet ID (Train Subnet)	ETBN ID	CstOrientation
1	00000000-0000-0000-0000-000000000002	1	10.128.64.0/18	1	Direct
2	00000000-0000-0000-0000-000000000003	1	10.128.128.0/18	2	Direct
3	00000000-0000-0000-0000-000000000004	1	10.128.192.0/18	3	Inverse
4	00000000-0000-0000-0000-000000000004	1	10.128.192.0/18	4	Inverse

Items per page: 5      1 - 4 of 4      < >

UI Setting	Description
<b>EtbTopoCntValid</b>	Shows whether the Logical Topology is shared by all ETBNs (same Train Network Directory CRC is used for all ETBNs).
<b>etbTopoCnt</b>	Shows the CRC32 checksum of the internal Train Network Directory.
<b>Memorized etbTopoCnt</b>	While the ETB node is in state INAUGURATED, etbTopoCnt field in TTDP TOPOLOGY frame is fixed to the memorized CRC of the Train Network Directory. The Mermorized etbTopoCnt and etbTopoCnt may be different when "inaugInhibition" is inhibited
<b>Index</b>	Shows the Index number of a CN.
<b>CstUUID</b>	Shows the Consist Universal Unique ID (refer to IETF RFC 4122) of the CN.
<b>CN Id</b>	Shows the ID of the CN, which is statically defined.
<b>Subnet Id</b>	Shows the subnet ID of the CN on the ETB.
<b>Train Subnet</b>	Shows the Train Subnet IP of the CN.
<b>ETBN Id</b>	Shows the ID of the ETBN on the ETB.
<b>CstOrientation</b>	Shows the orientation of the consist in relation to the direction of the train.

## TCN Multicast Table

**Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone - TCN Multicast Table**

This page lets you see the status of your TCN multicast entries.

The screenshot shows a web interface titled "Ethernet Train Backbone". It has four tabs: "TTDP Settings", "Local ETBN Status", "ETB Status", and "TCN Multicast Table" (which is selected). Below the tabs, there is a refresh icon and a timestamp "2023/09/20 17:51:38" on the left, and a search bar on the right. The main content is a table with the following data:

Index	TCN Group Address	Inbound Interface	Outbound Interface(s)
1	239.192.0.0	ETB	ECN1
2	239.192.0.0	ECN1	ETB
3	239.192.0.1	ETB	ECN1
4	239.192.0.1	ECN1	ETB
5	239.192.0.2	ECN1	ETB

At the bottom of the table, there is a pagination control showing "Items per page: 5" and "1 - 5 of 15" with navigation arrows.

UI Setting	Description
<b>Index</b>	Shows the index of the TCN entry.
<b>TCN Group Address</b>	Shows the group address for the TCN.
<b>Inbound Interface</b>	Shows the ETBN inbound interface of the TCN.
<b>Outbound Interface(s)</b>	Shows the ETBN outbound interface of the TCN.



## Communication Profile

**Menu Path: Industrial Application > IEC 61375 > Communication Profile**

This section lets you set up communication profiles for your device.

This section includes these pages:

- ECSP Settings
- SDTV2 Settings
- ECSP Status
- SDTV2 Status

### ECSP Settings

**Menu Path: Industrial Application > IEC 61375 > Communication Profile > ECSP Settings**

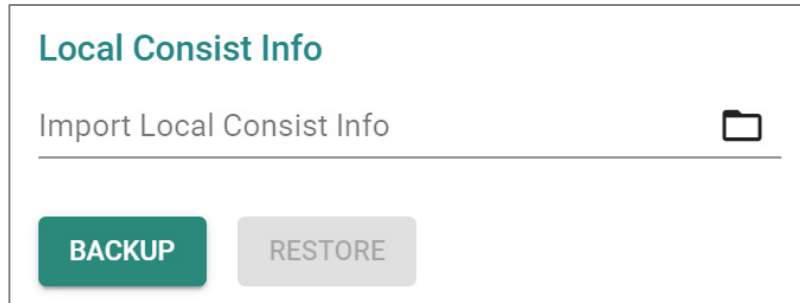
This page lets you back up or restore the local consist info file and the TRDP configuration file.

#### Local Consist Info

Click **BACKUP** to back up the current local consist info file to your local host. To restore, select a local consist info file from your local host, then click **RESTORE**.

#### **Note**

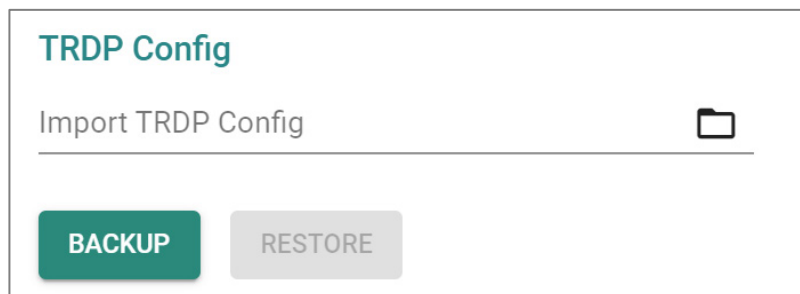
You cannot back up the local consist info file if one hasn't been previously loaded onto your router.



UI Setting	Description	Valid Range	Default Value
<b>Import Local Consist Info</b>	Select a local consist info file to restore from by clicking on the <b>Folder (📁) icon</b> , selecting the file to restore from, then clicking <b>RESTORE</b> . Refer to <a href="#">Structure and Syntax of Local Consist Info Files</a> for more information.	Local file	N/A

### TRDP Config

Click **BACKUP** to back up the current TRDP configuration to your local host. To restore, select a TRDP configuration file from your local host, then click **RESTORE**.



UI Setting	Description	Valid Range	Default Value
<b>Import TRDP Config</b>	Select a local TRDP configuration file to restore from by clicking on the <b>Folder (📁) icon</b> , selecting the file to restore from, then clicking <b>RESTORE</b> .	Local file	N/A

## SDTv2 Settings

### Menu Path: Industrial Application > IEC 61375 > Communication Profile - SDTV2 Settings

This page lets you enable or disable Safe Data Transmission protocol (SDTv2) telegrams.

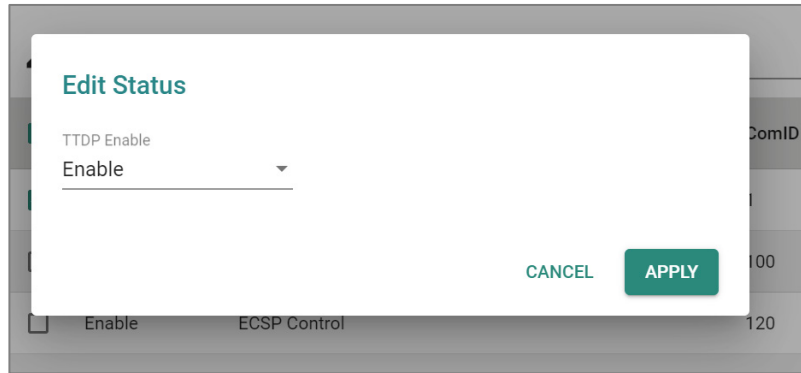
Status	Telegram	ComID
<input type="checkbox"/> Enable	ETBCTRL	1
<input type="checkbox"/> Enable	TTDB Status	100
<input type="checkbox"/> Enable	ECSP Control	120
<input type="checkbox"/> Enable	ECSP Status	121

UI Setting	Description
<b>Status</b>	Shows whether the telegram is enabled.
<b>Telegram</b>	Shows the name of the telegram.
<b>ComID</b>	Shows the ComID of the telegram.

### Edit Status

### Menu Path: Industrial Application > IEC 61375 > Communication Profile - SDTV2 Settings

Clicking the **Edit (✎)** icon after selecting entries on the **Industrial Application > IEC 61375 > Communication Profile - SDTV2 Settings** page will open this dialog box. This dialog lets you enable or disable the selected entries. Click **APPLY** to save your changes.



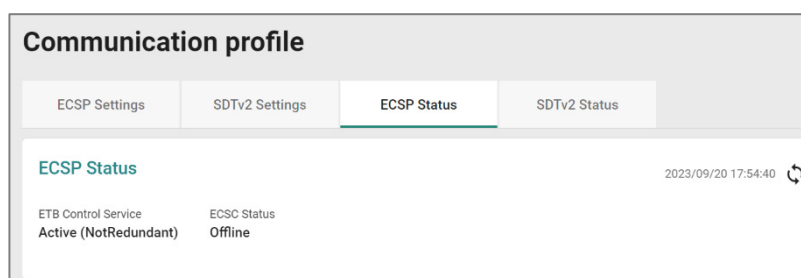
UI Setting	Description	Valid Range	Default Value
<b>TTDP Enable</b>	Enable or disable the selected telegrams.	Enable / Disable	Enable

## ECSP Status

### Menu Path: Industrial Application > IEC 61375 > Communication Profile - ECSP Status

This page lets you see the current status of the ECSP and the state machines.

## ECSP Status



UI Setting	Description
<b>ETB Control Service</b>	<p>Shows whether the ETB Control Service Provider (ECSP) is providing ETB Control Service or not, which may be impacted by the VRRP role.</p> <p><b>Active:</b> Local ECSP (ETBN) is VRRP master, and has found an ECSC Local ECSP (ETBN) has no redundancy</p> <p><b>Not Active:</b> Local ECSP (ETBN) is the VRRP backup</p>
<b>ECSC Status</b>	<p>Shows whether an ETB Control Service Client (ECSC) is communicating with the ECSP.</p> <p><b>Online:</b> The ECSP received a ECSP Control Telegram from an ECSC and is currently connected.</p> <p><b>Offline:</b> An ECSC previously connected to the ECSP, but is not currently connected.</p> <p><b>NotExist:</b> The ECSP has not connected to an ECSC yet.</p>

## State Machine List

The State Machine List includes the 5 state machines that have been defined in IEC 61375-2-3.

State Machine	State
Leading	WaitForLeadReq
Confirmation/Correction	CompUnknown
ETB Control	EtbCtrlSetUp
Train Directory	TrnDirSetup
Operational Train Directory	Shared

UI Settings	Description
<b>State Machines</b>	Shows the name of the state machine.

UI Settings	Description
<b>State</b>	Shows the current state of the state machine.
	<b>Leading</b> Init / WaitForLeadReq / WaitForAccept / WaitForLead / WaitForLed / IsLeading / IsLed
	<b>Confirmation / Correction</b> Init / CompClear / CompUnknown / CompSet / CompStored / CompReset
	<b>ETB Control</b> Init / WaitForEtbCtrl / EtbCtrlSetUp
	<b>Train Directory</b> Init / WaitForEtbInaug / WaitForCstInfo / TrnDirSetup
	<b>Operational Train Directory</b> Init / Invalid / Valid / Shared

## SDTv2 Status

### Menu Path: Industrial Application > IEC 61375 > Communication Profile - SDTv2 Status

This page lets you see the SDSRC and SDSINK information for SDTv2 telegrams.

#### ECSP SDSRC

This table shows the Safe Data Source (SDSRC) used for sending vital data packets (VDPs) in SDTv2 telegrams to a Safe Data Sink (SDSINK).

ECSP SDSRC		
Telegram	ComID	Source Identifier (SID)
ETBCTRL	1	0x9d9e7b4f
TTDB Status	100	0xb163bea5
ECSP Status	121	0x43206c09

UI Setting	Description
<b>Telegram</b>	Shows the name of the telegram.
<b>ComID</b>	Shows the ComID for the telegram.

UI Setting	Description
------------	-------------

**Source Identifier (SID)** Shows the SID for the telegram, which is an unsigned32 value computed as an SC-32 signature of the data structure.

## ECSP SDSINK

This table shows the Safe Data Sink (SDSINK) used to receive vital data packets (VDPs) in SDTv2 telegrams from a Safe Data Source (SDSRC).

Telegram	ComID	State	Expected Source Identifier (SID)
---	---	---	---

UI Setting	Description
------------	-------------

**Telegram** Shows the name of the telegram.

**ComID** Shows the ComID for the telegram.

**State** Shows the state of the telegram.

**RegularCommunication:** In this state, transmitted VDPs cannot be considered to be safe.

**State SafeCommunication:** In this state, transmitted VDPs can be considered to be safe.

**Expected Source Identifier (SID)** Shows the SID of the expected SDSRC to receive VDPs from. This information is retrieved from the Train Topology Database (TTDB).

## Operational Status

**Menu Path: Industrial Application > IEC 61375 > Operational Status**

This page lets you know the Status of your IEC 61375 related operational settings.

This page includes these tabs:

- Consist Info
- Train Directory
- Operational Train Directory
- TCN-URI Table

### Consist Info

**Menu Path: Industrial Application > IEC 61375 > Operational Status - Consist Info**

This page lets you see information about the current consist.

### Consist Info

**Operational Status**

Consist Info    Train Directory    Operational Train Directory    TCN-URI Table

**Consist Info** 2023/09/20 18:01:34 ↻

Consist Class	Consist Type
consist	test
Consist ID	Consist Owner
consist2	TCMS
Consist UUID	
00000000-0000-0000-0000-000000000002	

UI Setting	Description
<b>Consist Class</b>	Shows the CSTINFO class of the consist.
<b>Consist Type</b>	Shows the type of the consist.



UI Setting	Description
<b>Consist ID</b>	Shows the ID of the consist.
<b>Consist Owner</b>	Shows the owner of the consist.
<b>Consist UUID</b>	Shows the UUID of the consist.

## ETB List

The screenshot shows a web interface titled "ETB List". At the top right, there is a search bar with a magnifying glass icon and the text "Search". Below the search bar is a table with two columns: "ETB ID" and "Consist Network Count". The table has one data row with the values "0" and "1". At the bottom of the table, there are pagination controls: "Items per page: 5" (with a dropdown arrow), "1 - 1 of 1", and navigation arrows (|< < > >|).

UI Setting	Description
<b>ETB ID</b>	Shows the ID of the ETB. <b>0:</b> ETB0 (operational network) <b>1:</b> ETB1 (multimedia network) <b>2:</b> ETB2 (other network) <b>3:</b> ETB3 (other network)
<b>Consist Network Count</b>	Shows how many CNs are in the consists connected to the ETB.

## Vehicle List

Vehicle List				
Search				
Vehicle ID	Vehicle Type	Vehicle Orientation	Consist Vehicle Number	Traction
veh2	intercity_train	same	1	true

Items per page: 5 1 - 1 of 1 |< < > >|

UI Setting	Description
<b>Vehicle ID</b>	Shows the ID of the vehicle.
<b>Vehicle type</b>	Shows the type of the vehicle.
<b>Vehicle Orientation</b>	Shows the orientation of the vehicle. <b>same:</b> Indicates that vehicle has the same direction with respect to the consist direction. <b>inverse:</b> Indicates that the vehicle is in the opposite direction with respect to the consist direction.
<b>Consist Vehicle Number</b>	Shows the index of the vehicle within the consist.
<b>Traction</b>	Shows whether the vehicle has traction.

## Function List

Function List					
Search					
Name	Function ID	Group	Consist Vehicle Number	ETB ID	Consist Network ID
devCam1	11	false	1	0	1
devECSC	201	false	1	0	1
grpDoor	20	true	1	0	0

Items per page: 5 1 - 3 of 3 |< < > >|

UI Setting	Description
<b>Name</b>	Shows the name of the device/functional group.
<b>Function ID</b>	Shows the ID of the device/functional group.
<b>Group</b>	Shows whether this is a functional group.
<b>Consist Vehicle Number</b>	Shows the index of the vehicle Sequence number of the vehicle within the consist the device/functional group belongs to.
<b>ETB ID</b>	Shows the ID of the ETB the device/functional group is on. <b>0:</b> ETB0 (operational network) <b>1:</b> ETB1 (multimedia network) <b>2:</b> ETB2 (other network) <b>3:</b> ETB3 (other network)
<b>Consist Network ID</b>	Shows the ID of the consist network the device/functional group is in.

## Train Directory

**Menu Path: Industrial Application > IEC 61375 > Operational Status - Train Directory**

This page shows information about the train and the consists in it.

### Train Directory

**Operational Status**

Consist Info
**Train Directory**
Operational Train Directory
TCN-URI Table

**Train Directory**

ETB ID  
ETB0 (operational network)

Train Topography Counter  
0x1BD3CBE9

2023/09/20 18:03:11

UI Setting	Description
<b>ETB ID</b>	Shows the ID of the ETB. <b>0:</b> ETB0 (operational network) <b>1:</b> ETB1 (multimedia network) <b>2:</b> ETB2 (other network) <b>3:</b> ETB3 (other network)
<b>Train Topography Counter</b>	Shows a counter used to check whether all the ECSPs in the train have the same train direction during ECSP negotiation.

## Consist List

Consist UUID	Consist Orientation	Consist Number	Consist Topography Counter
00000000-0000-0000-0000-000000000002	same	1	0x82088A3A
00000000-0000-0000-0000-000000000003	same	2	0x5841F1BA
00000000-0000-0000-0000-000000000004	inverse	3	0x424A9E0F

Items per page: 5    1 - 3 of 3    < > >>

UI Setting	Description
<b>Consist UUID</b>	Shows the UUID of the consist.
<b>Consist Orientation</b>	Shows the orientation of the consist. <b>same:</b> Indicates that consist has the same direction with respect to the train direction. <b>inverse:</b> Indicates that the consist is in the opposite direction with respect to the train direction.
<b>Consist Number</b>	Shows the index of the consist within the train.
<b>Consist Topology Counter</b>	Shows the consist topography counter provided with the CSTINFO.

## Operational Train Directory

**Menu Path: Industrial Application > IEC 61375 > Operational Status - Operational Train Directory**

This page shows information about the operational train, consists, and vehicles.

## Operational Train Directory

### Operational Status

Consist Info
Train Directory
Operational Train Directory
TCN-URI Table

**Operational Train Directory**

ETB ID  
ETB0 (operational network)

Operational Train Orientation: **same**

Operational Train Topography Counter: **0xA61014B3**

2023/09/20 18:08:55

UI Setting	Description
<b>ETB ID</b>	<p>Shows the ID of the ETB.</p> <p><b>0</b>: ETB0 (operational network)</p> <p><b>1</b>: ETB1 (multimedia network)</p> <p><b>2</b>: ETB2 (other network)</p> <p><b>3</b>: ETB3 (other network)</p>
<b>Operational Train Orientation</b>	<p>Shows the orientation of the vehicle.</p> <p><b>same</b>: Indicates that operational train has the same direction with respect to the train direction.</p> <p><b>inverse</b>: Indicates that the operational train is in the opposite direction with respect to the train direction.</p> <p><b>unknown</b>: The direction of the operational train is unknown.</p>
<b>Operational Train Topography Counter</b>	<p>Shows the computed operational train topography counter, which is automatically configured.</p>

## Operational Consist List

### Operational Consist List

Consist UUID	Operational Consist Number	Consist Number	Operational Consist Orientation
00000000-0000-0000-0000-0000000000000021		1	same
00000000-0000-0000-0000-0000000000000032		2	same
00000000-0000-0000-0000-0000000000000043		3	inverse

Items per page: 5    1 - 3 of 3    < < > >

UI Setting	Description
<b>Consist UUID</b>	Shows the UUID of the operational consist.
<b>Operational Consist Number</b>	Shows the index of the operational consist, which is automatically configured.
<b>Consist Number</b>	Shows the index of the consist that the operational consist is in.
<b>Operational Consist Orientation</b>	Shows the orientation of the operational consist. <b>same:</b> Indicates that the operational consist has the same direction with respect to the train direction. <b>inverse:</b> Indicates that the operational consist is in the opposite direction with respect to the train direction. <b>unknown:</b> The direction of the operational consist is unknown.

## Operational Vehicle List

Operational Vehicle List

Q Search

Vehicle ID	Vehicle Orientation	Lead	Lead Direction	Operational Vehicle Number	Train Vehicle Number	Operational Consist Number
veh2	same	false	Not relevant	1	1	1
veh3	same	false	Not relevant	2	2	2
veh4	inverse	false	Not relevant	3	3	3

Items per page: 5 1 - 3 of 3 < >

UI Setting	Description
<b>Vehicle ID</b>	Shows the ID of the operational vehicle.
<b>Vehicle Orientation</b>	Shows the orientation of the operational vehicle. <b>same:</b> Indicates that the operational vehicle has the same direction with respect to the operational train direction. <b>inverse:</b> Indicates that the operational vehicle is in the opposite direction with respect to the operational train direction. <b>unknown:</b> The direction of the operational vehicle is unknown.
<b>Lead</b>	Shows whether the operational vehicle is leading.
<b>Lead Direction</b>	Shows the direction used for the operational vehicle.
<b>Operational Vehicle Number</b>	Shows the index of the operational vehicle in the operational train.

UI Setting	Description
------------	-------------

- Train Vehicle Number** Shows the index of the vehicle that the operational vehicle belongs to.
- Operational Consist Number** Shows the index of the operational consist the operational vehicle belongs to.

## TCN-URI Table

### Menu Path: Industrial Application > IEC 61375 > Operational Status - TCN-URI Table

This page lets you see the mappings between Train Communication Network Uniform Resource Identifiers (TCN-URIs) and IP addresses.

Index	TCN-URI	Train Network IP	Local IP
1	grpAll.aVeh.aCst.ITrn	239.193.0.0	
2	grpAll.aVeh.ICst.ITrn	239.194.0.0	
3	devCam1.opVeh01.anyCst.ITrn	10.128.64.11	10.1.0.11
4	devECSC.opVeh01.anyCst.ITrn	10.128.64.201	10.1.0.201
5	grpDoor.aVeh.aCst.ITrn	239.193.0.20	

UI Setting	Description
------------	-------------

- Index** Shows the index number of the TCN-URI.
- TCN-URI** Shows the Train Communication Network Uniform Resource Identifier (TCN-URI) of a component on the train.
- Train Network IP** Shows the train network IP used for the TCN-URI.
- Local IP** Shows the local IP used for the TCN-URI.

## Chapter 4

---

# Other Features



# Other Features

This section covers other features of your device that may not have a related user interface.

The features in this section include:

- Firmware Image Recovery
- Soft Lockdown

## 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.

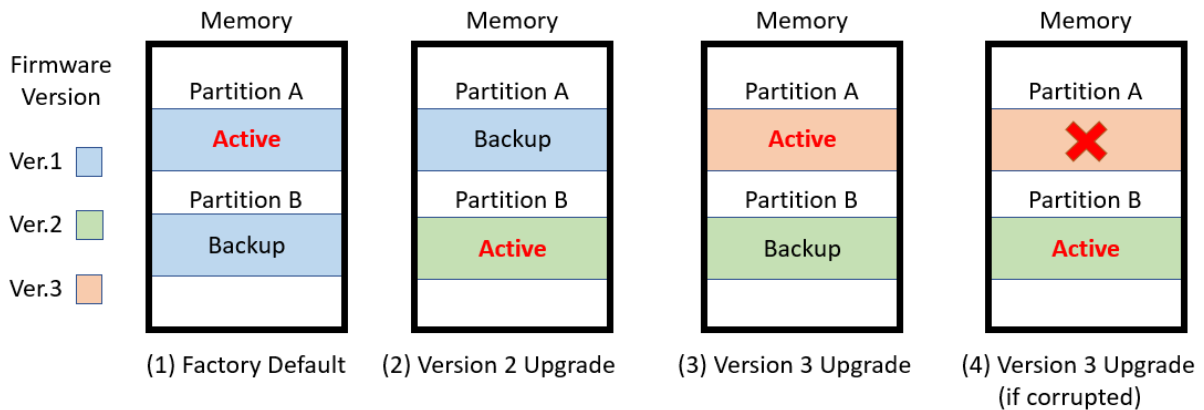
### ▲ Warning

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.

## Soft Lockdown

 **Note**

Soft Lockdown Mode is a feature designed for railway applications and is only supported by the TN-4900 Series.

Moxa routers can act as firewalls to help provide protection from external attacks that try to gain access and control over the network. On the other hand, while protecting the network, it is also important to prevent potential malfunctions that may occur and avoid unexpected network operation failures.

To handle this, Soft Lockdown Mode is a monitoring and protection mechanism that monitors important indicators and enters Soft Lockdown Mode once user-defined failure criteria are reached to ensure that device operation remains stable. For details about Soft Lockdown Mode settings, refer to Firewall > Soft Lockdown Mode.

### Soft Lockdown Criteria

The criteria for entering and leaving Soft Lockdown Mode are defined by the following:

- **Performance Thresholds:** If the CPU utilization % exceeds a user-defined threshold, or the amount of free memory % goes below a user-defined threshold, a failure will be detected for the current cycle.
- **Monitoring Interval:** This defines how long a single monitoring cycle will be.
- **Number of Cycles to Enter Soft Lockdown Mode:** This defines how many consecutive cycles with failures are required to enter Soft Lockdown Mode.
- **Number of Cycles to Leave Soft Lockdown Mode:** This defines how many consecutive cycles without failures are required to leave Soft Lockdown Mode.
- **Critical Services:** If any of the following critical services are enabled, the device continually check to see whether the services are alive. The device will enter Soft

Lockdown Mode if any enabled critical service is no longer alive, and all enabled critical services must be alive to leave Soft Lockdown Mode.

The critical services that apply to Soft Lockdown Mode are as follows:

- DHCP Server (refer to Network Service > DHCP Server)
- DHCP Relay Agent (refer to Network Service > DHCP Server - DHCP Relay Agent)
- SNMP Server (refer to SNMP)
- Turbo Ring V2 (refer to Redundancy > Layer 2 Redundancy > Turbo Ring V2)

#### ▲ Warning

When the device is operating normally, its CPU and memory usage can vary due to various factors. Apart from potential attacks, the number of devices connected to the router and application settings can also lead to increased demands on CPU and memory.

It is important to carefully assess the usage and configuration of this feature to avoid triggering Soft Lockdown Mode due to normal usage to avoid impacting regular operations.

## Entering Soft Lockdown Mode

The device will enter Soft Lockdown Mode when any of the following occur:

- The number of consecutive cycles with failures reaches the defined **Number of Cycles to Enter Soft Lockdown Mode**
- Any of the enabled **Critical Services** are no longer alive

## When in Soft Lockdown Mode

In Soft Lockdown Mode, the device will do the following:

- Block all traffic (both ingress and egress) on the interface specified for Soft Lockdown Mode
- Log the event and the reason for the event in the system log

#### ▲ Warning

When Soft Lockdown Mode is enabled, the port settings and VLAN settings should not be modified in order to prevent a mismatch for the Soft Lockdown Mode interface settings.

## Leaving Soft Lockdown Mode

The device will leave Soft Lockdown Mode under any of the following conditions:

- The number of normal consecutive cycles without failures reaches the defined **Number of Cycles to Leave Soft Lockdown Mode** AND all enabled **Critical Services** are alive.
- The device is restarted. After restarting, the device will enter normal operation and will only enter Soft Lockdown Mode if the criteria are fulfilled.

When leaving Soft Lockdown Mode, the device will do the following:

- Resume all traffic (both ingress and egress) on the interfaces where firewall rules are applied
- Log the event in the system log

## Chapter 5

---

# Device Applications

# Device Applications

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
- 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.

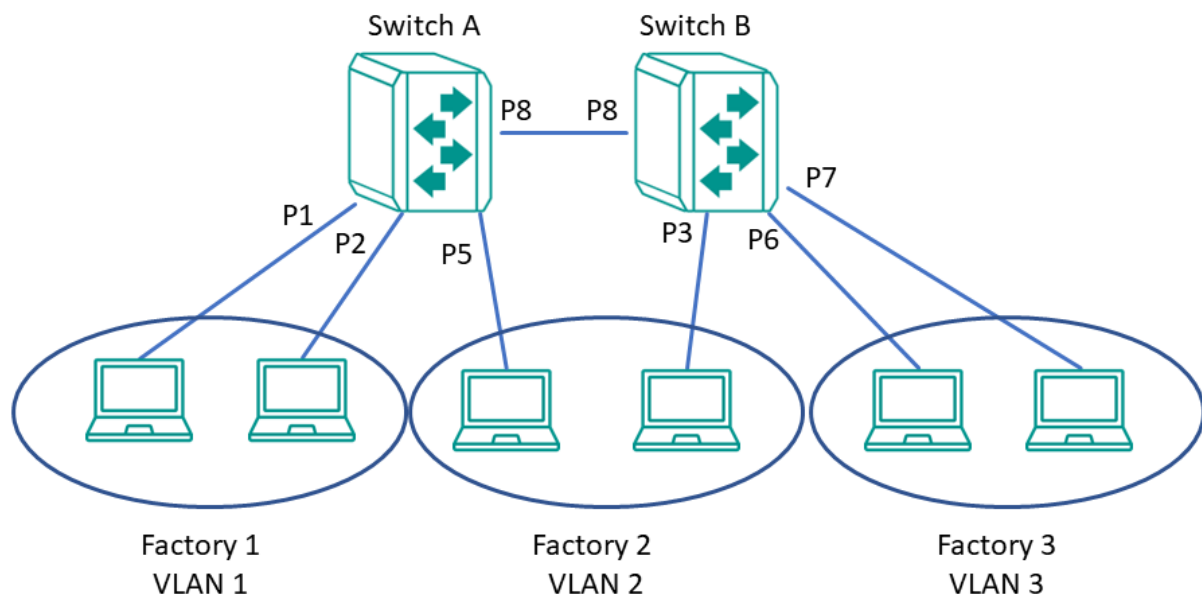
Two switches are used to connect all of the devices together on the same network, but devices from any factory may be connected to either switch. To simplify management and ensure smooth operations, we can configure the switches to make sure that each factory is on its own VLAN.

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

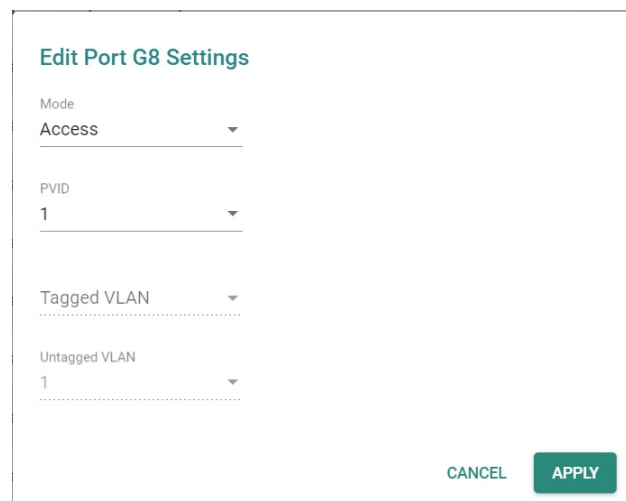
VLANs must be assigned to ports on Switch A to route traffic correctly.

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 then 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.



**Edit Port G8 Settings**

Mode  
Access

PVID  
1

Tagged VLAN

Untagged VLAN  
1

CANCEL APPLY

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	<ul style="list-style-type: none"><li>• <b>PVID:</b> 1</li><li>• <b>Mode:</b> Access Mode</li></ul>
5	<ul style="list-style-type: none"><li>• <b>PVID:</b> 2</li><li>• <b>Mode:</b> Access Mode</li></ul>
8	<ul style="list-style-type: none"><li>• <b>PVID:</b> 1000</li><li>• <b>Mode:</b> Trunk Mode</li><li>• <b>Tagged VLAN:</b> 1, 2, 3</li></ul>

**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.

**Edit Port G8 Settings**

Mode  
Access

PVID  
1

Tagged VLAN

Untagged VLAN  
1

CANCEL APPLY

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:

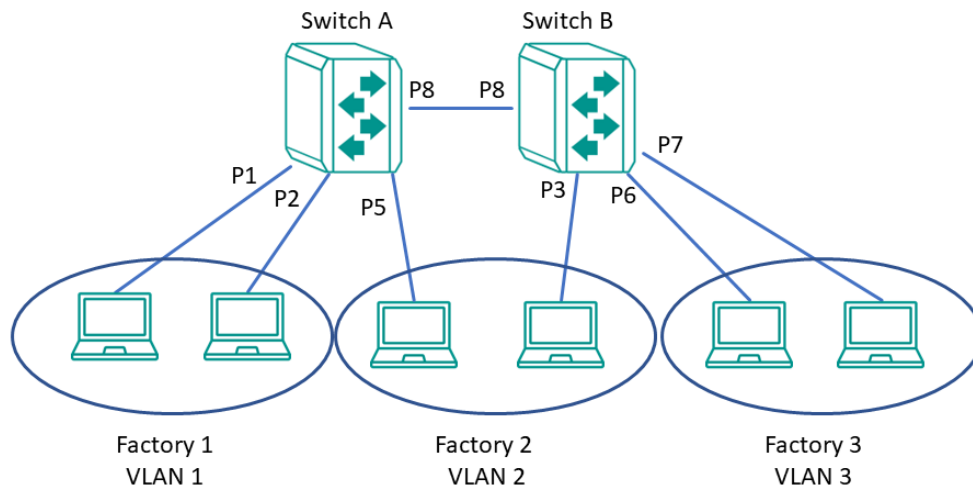
Port	Settings
6	<ul style="list-style-type: none"><li>• <b>PVID: 1</b></li><li>• <b>Mode: Access Mode</b></li></ul>
7	<ul style="list-style-type: none"><li>• <b>PVID: 2</b></li><li>• <b>Mode: Access Mode</b></li></ul>

Port	Settings
------	----------

- |   |   |
|---|---|
| 8 | <ul style="list-style-type: none"> <li>• <b>PVID: 1000</b></li> <li>• <b>Mode: Trunk Mode</b></li> <li>• <b>Tagged VLAN: 1, 2, 3</b></li> </ul> |
|---|---|

**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.

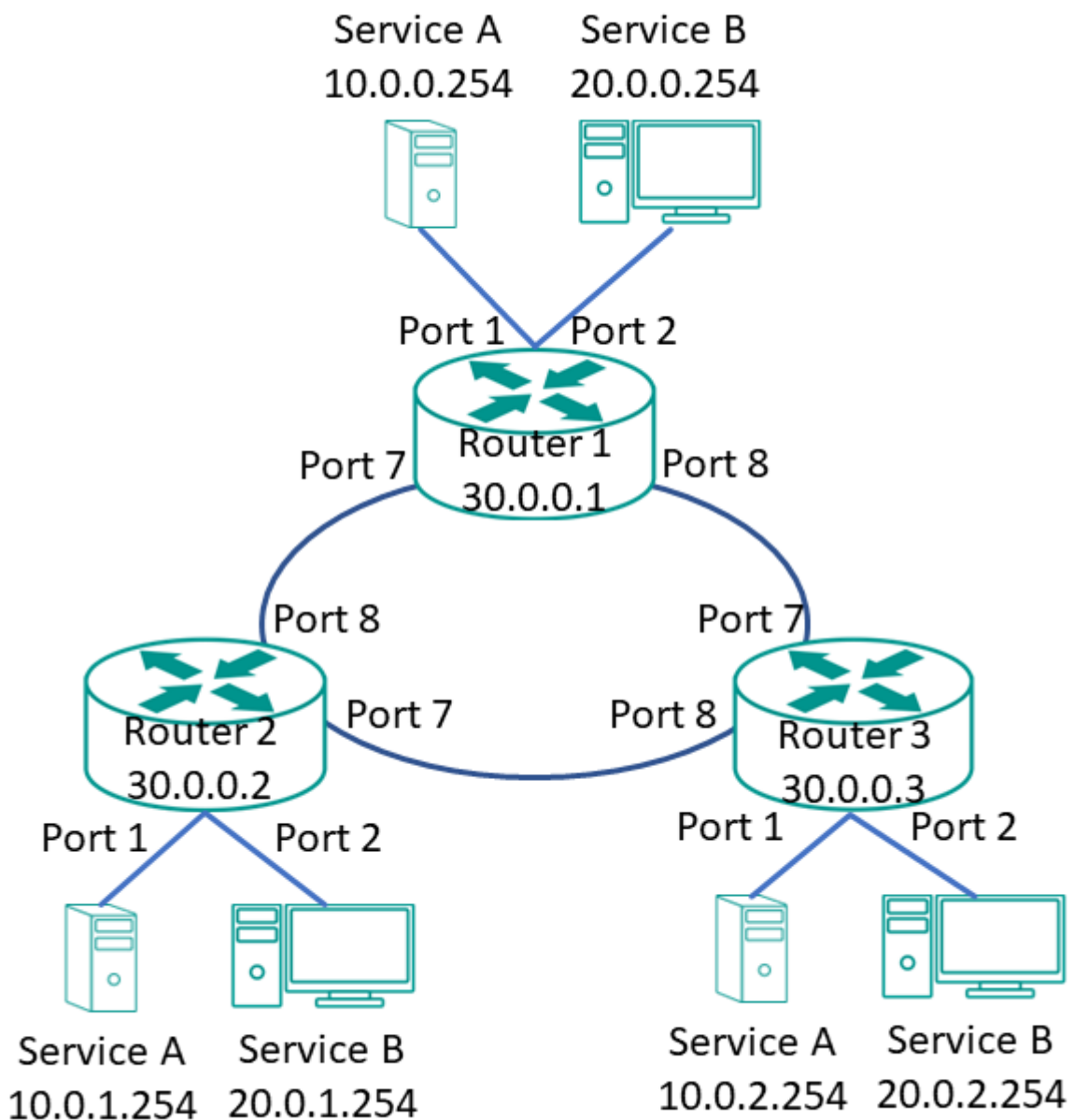
Three routers are used to connect the all of the devices together on the same network, but devices from any factory may be connected to either switch. Each factory has devices running Service A and Service B. Devices need to connect to the corresponding service in other factories, while being isolated 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 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
<b>Name</b>	Service A
<b>VLAN ID</b>	10
<b>IP Address</b>	10.0.1.254
<b>Netmask</b>	<b>8 (255.0.0.0)</b>

**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
<b>Name</b>	Service B
<b>VLAN ID</b>	20
<b>IP Address</b>	20.0.1.254
<b>Netmask</b>	<b>8 (255.0.0.0)</b>

**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
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
<b>Name</b>	Service A Router 2
<b>Status</b>	<b>Enable</b>
<b>Destination Address</b>	<b>10.0.1.254</b> Refers to Production Service A on Router 2.
<b>Subnet Mask</b>	<b>8 (255.0.0.0)</b> Refers to the subnet mask of the destination address.
<b>Next Hop</b>	<b>30.0.0.2</b> Refers to the Router 2 Interface as the next hop on the network.
<b>Metric</b>	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
<b>Name</b>	<b>Service B Router 2</b>
<b>Status</b>	<b>Enable</b>
<b>Destination Address</b>	<b>20.0.1.254</b> Refers to Production Service A on Router 2.
<b>Subnet Mask</b>	<b>8 (255.0.0.0)</b> Refers to the subnet mask of the destination address.

Item	Value
<b>Next Hop</b>	30.0.0.2 Refers to the Router 2 Interface as the next hop on the network.
<b>Metric</b>	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
<b>Appears On</b>	Routers 2/3	Routers 2/3	Routers 1/3	Routers 1/3	Routers 1/2	Routers 1/2
<b>Name</b>	Service A Router 1	Service B Router 1	Service A Router 2	Service B Router 2	Service A Router 3	Service B Router 3
<b>Status</b>	<b>Enable</b>	<b>Enable</b>	<b>Enable</b>	<b>Enable</b>	<b>Enable</b>	<b>Enable</b>
<b>Destination Address</b>	10.0.0.25 4	20.0.0.25 4	10.0.0.25 4	20.0.1.25 4	10.0.0.25 4	20.0.2.25 4
<b>Subnet Mask</b>	<b>8</b> <b>(255.0.0.0)</b>	<b>8</b> <b>(255.0.0.0)</b>	<b>8</b> <b>(255.0.0.0)</b>	<b>8</b> <b>(255.0.0.0)</b>	<b>8</b> <b>(255.0.0.0)</b>	<b>8</b> <b>(255.0.0.0)</b>
<b>Next Hop</b>	30.0.0.1	30.0.0.1	30.0.0.2	30.0.0.2	30.0.0.3	30.0.0.3
<b>Metric</b>	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.

## About Redundancy

Redundancy in industrial networks refers to averting the impact of unexpected shutdowns. If a service becomes unavailable, it can cause interruptions to productivity and services, resulting in potentially significant losses for businesses. Therefore, it is crucial to establish a redundancy protocol to quickly recover from any abnormalities and maintain productivity.

## What kinds of redundancy protocols are there?

Moxa network devices support a variety of network redundancy protocols for both OSI Layer 2 and Layer 3.

- Layer 2: Moxa devices have redundancy protocol support for RSTP, MSTP, Turbo Ring v2, Turbo Chain, Ring Coupling, and Dual Homing for pathway redundancy. These mechanisms establish alternative paths that can be used to reach a destination if the primary connection fails.
- Layer 3: Moxa devices use Virtual Router Redundancy Protocol (VRRP) to ensure that the default gateway function can switch to a backup device in case the primary device fails. This ensures that routing functions remain available even if the primary device goes offline.

By implementing redundancy mechanisms at both Layer 2 and Layer 3, you can help ensure that your networks are reliable and available, even in the event of a failure or outage.

## About Layer 2 Redundancy Protocols

Selecting the appropriate Layer 2 redundancy protocol for your network depends on several factors, including:

- The topology and size of your network
- The applications and services you are running
- Your availability and performance requirements

Suggestions for protocol selection will be mentioned in later chapters. Here's a brief summary of each protocol to help you make an informed decision.

Category		RSTP	Turbo Ring v2	Turbo Chain
<b>Specification needs</b>	Diameter	40 pcs	<b>V</b> 250 nodes per ring	<b>V</b> 250 node per chain
	Recovery Time		<b>V</b> Fast Ethernet: 20ms Gigabit Ethernet: 50ms	<b>V</b> Fast Ethernet: 20ms Gigabit Ethernet: 50ms

Category		RSTP	Turbo Ring v2	Turbo Chain
	Link Health Check (Packet Detection Mechanism)	<b>V</b> 2 sec/1 RSTP BPDU (default)	<b>O</b> Gigabit Ethernet: 10ms/LHC pkt.	<b>O</b> Gigabit Ethernet: 10ms/LHC pkt.
<b>Application needs</b>	Multi-Vendor Support	<b>V</b> Public Standard	Moxa proprietary	Moxa proprietary
	Easy-Deployment	Mesh	<b>V</b> Ring Topology	<b>V</b> Chain Topology
	Flexible Scalability		<b>O</b> Turbo Ring + Ring Coupling	<b>V</b> Directly connected to existing network without any changes.
<b>Supported Models</b>		Managed switch: EDS series, IKS series, ICS series, TN series, PT series, RKS series, MDS series. Router: EDR series, TN series.	Managed switch: EDS series, IKS series, ICS series, TN series, PT series, RKS series, MDS series. Router: EDR series, TN series.	Managed switch: EDS series, IKS series, ICS series, TN series, PT series, RKS series, MDS series. Router: EDR series.

**V:** Most appropriate

**O:** Partially applicable

## About Scenarios for Turbo Chain and Turbo Ring

### Large Semiconductor Network

A semiconductor factory plans to construct a new facility to increase chip production capacity for future electric vehicles. They require a large automated network (100+ switches) with redundant mechanisms to prevent unexpected downtime that could impact production lines. Additionally, their network must balance traffic across multiple links to prevent congestion and improve overall performance.

#### Analysis

- This is a new project with no existing infrastructure.
- A redundancy protocol is required and must support a network with at least 100 switches.

- Link aggregation is needed to increase total throughput beyond what a single connection can sustain.

### **Solution: Turbo Ring v2**

Turbo Ring v2 is suitable in situations where extremely fast failover times are required, such as in mission-critical industrial control systems. Turbo Ring v2 facilitates easy ring topology deployment. With Moxa Turbo Ring technology, networks can recover within 20 ms (Fast Ethernet/fiber) or 50ms (gigabit copper) on a network with up to 250 nodes.

### **Legacy Rapid Transit Network**

A Phase II Metro project needs to build 15 new metro stations in an existing transit system, each requiring networking infrastructure. This project not only establishes its own system with a redundant topology but also ensures compatibility with the Phase I system. The Phase I system comprises a mesh topology with RSTP protocol, consisting of over 30 switches, with cabling that is outdated and no longer replaceable. Nevertheless, Phase II must be interconnected with Phase I without any modifications to the latter.

#### **Analysis**

5. This is a rebuilt project and it should be interconnected with RSTP topology.
6. Redundancy protocol is required and support 100+ switches network.

### **Solution: Turbo Chain**

Turbo Chain is most suitable for this situation. One of the key advantages of Turbo Chain is its simplicity and ease of deployment. It can be directly interconnected to RSTP topology with any change on RSTP network.

Note:

The following two alternative solutions would also work in this scenario:

1. Turbo Ring v2 with Ring coupling to RSTP is also an alternate solution. This would depend on network physical deployment.
2. RSTP could be used to expand an existing RSTP network.

### **Inter-Consist Rail Network**

A well-known railway vehicle manufacturer needs to plan a new on-board network, planning a ring network via Turbo Ring for multiple vehicles to form a consist. The



consists also need to be interconnected with each other when connected as a train, and a redundant backup mechanism should be provided between consists.

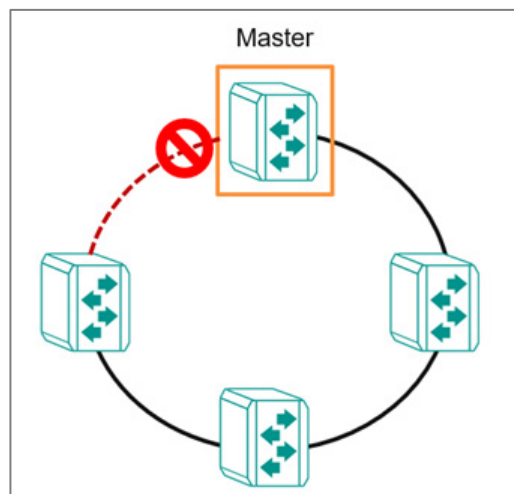
### **Solution: Ring Coupling**

Connection between Turbo Ring networks can be connected with ring coupling. This will allow consists with their own rings to be dynamically uncoupled and recoupled without reconfiguration.

### **About Turbo Ring v2**

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

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



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

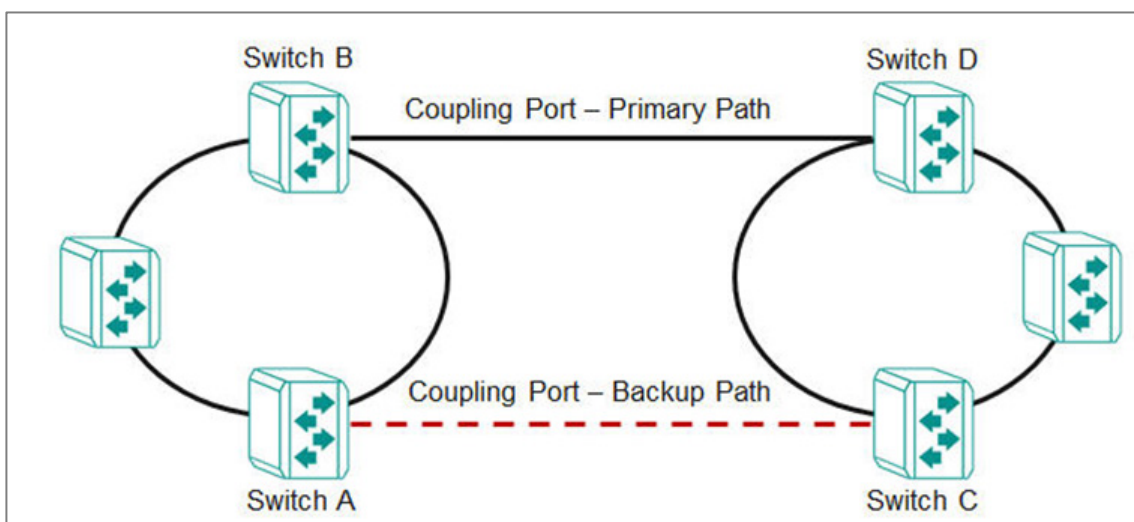
Furthermore, the election mechanism is redundant. If the "master" device itself fails, the network devices detect the failure and automatically elect another. The process occurs quickly, ensuring no interruption.

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

## About Ring Coupling

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

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



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

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

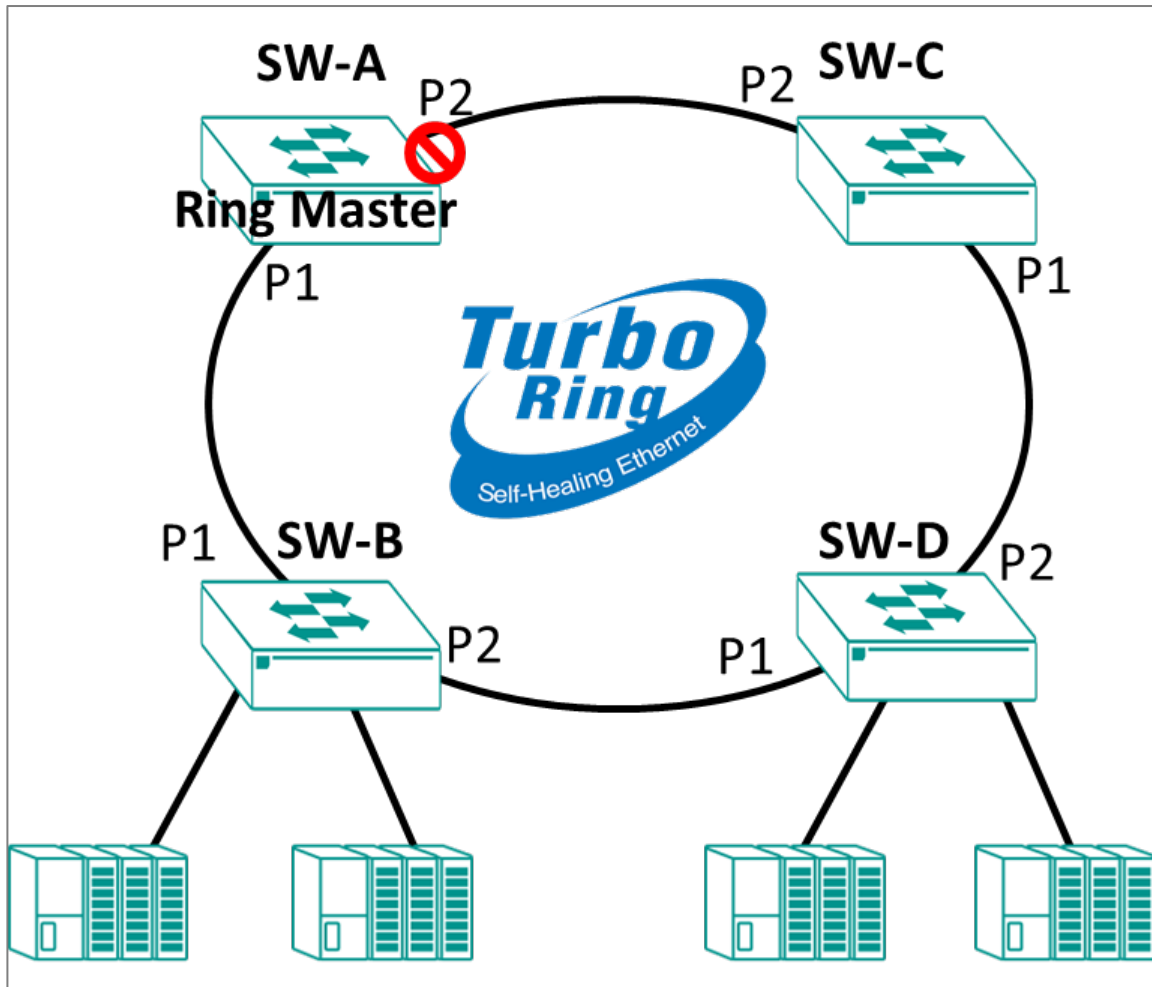
### Note

Only one coupling (primary + backup) per ring pair.

## Scenario: Using Turbo Ring in a Manufacturing Plant

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

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



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

Ensure that switches are installed and powered. Wait to connect them until the end. To configure this scenario, do the following:


- Configure the settings each network device for Turbo Ring v2. See the subsequent sections for details about how to configure each device.
- Connect the network devices in a ring topology, using ports 1 and 2 for ring segments.

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

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

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

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

- Sign in to the device with administrator credentials.
- Go to **Redundancy > Layer 2 Redundancy > Turbo Ring V2**, and then click **General**.
- Set **Status** to **Enabled**.
- Under Ring Settings, next to **Ring 1**, click  **[Add]**.

The Ring 1 Settings screen appears.

- Configure all of the following:

Option	Value
<b>Status</b>	<b>Enabled</b>
<b>Master</b>	<b>Enabled</b>
<b>Ring Port 1</b>	<b>1</b>
<b>Ring Port 2</b>	<b>2</b>

Setting **Master** on multiple devices (or no devices) will have the following effects:


Master Setting	Result
<b>Multiple devices set to Enabled</b>	Ring election based on MAC addresses of <b>Enabled</b> devices
<b>No devices set to Enabled</b>	Ring election based on MAC addresses of all devices
<b>Single device set to Enabled</b>	<b>Enabled</b> device always master, failure of <b>Enabled</b> device results in ring election

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

Repeat this step on devices SW-B, SW-C, and SW-D, but with the **Master** setting set to **Disabled**. This process is outlined in the subsequent section.

## Example: Configuring non-Master devices for Turbo Ring v2 in an On-board Rail Application

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

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

The Ring 1 Settings screen appears.

- Configure all of the following:

Option	Value
<b>Status</b>	<b>Enabled</b>
<b>Master</b>	<b>Disabled</b>
<b>Ring Port 1</b>	<b>1</b>
<b>Ring Port 2</b>	<b>2</b>

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
<b>Multiple devices set to Enabled</b>	Ring election based on MAC addresses of <b>Enabled</b> devices
<b>No devices set to Enabled</b>	Ring election based on MAC addresses of all devices
<b>Single device set to Enabled</b>	<b>Enabled</b> device always master, failure of <b>Enabled</b> device results in ring election

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

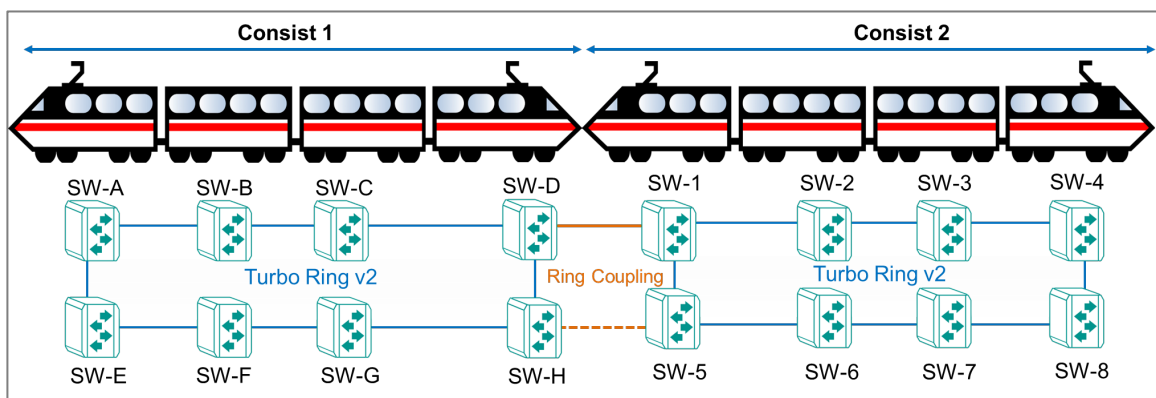
Once all devices in the ring are configured and enabled, you can connect the ring ports.

Continue to the next section to see how to configure ring coupling. Do not connect coupling ports until network devices have been configured.

## Scenario: Using Turbo Ring in an On-board Train Application

In this scenario, we describe setting up Turbo Ring v2 with ring coupling between train consists.

A railway vehicle manufacturer needs to plan a new on-board network with redundancy and flexible inter-consist communication. The customer plans a ring network with Turbo Ring v2 between multiple vehicles to form one ring per consist. Multiple consists will then use ring coupling for inter-consist communication.



This structure allows for easy administration as consists are coupled and uncoupled.


To configure this scenario, do the following:

- Configure the settings each network device for Turbo Ring v2. See the subsequent sections for details about how to configure each device.
- Connect the network devices SW-A through SW-H in a ring topology, using ports 1 and 2 for segments of the ring. Do the same for SW-1 through SW-8. Do not connect the ring coupling yet.
- Configure the Primary Coupling Path path on SW-D. See the subsequent sections for details about how to configure ring coupling.
- Configure the Backup Ring Coupling on SW-H. See the subsequent sections for details about how to configure ring coupling.

Once all devices have been configured, you can connect the ring ports and coupling ports.

## Example: Configuring non-Master devices for Turbo Ring v2 in an On-board Rail Application

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

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

The Ring 1 Settings screen appears.

- Configure all of the following:

Option	Value
<b>Status</b>	<b>Enabled</b>
<b>Master</b>	<b>Disabled</b>
<b>Ring Port 1</b>	<b>1</b>
<b>Ring Port 2</b>	<b>2</b>

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
<b>Multiple devices set to Enabled</b>	Ring election based on MAC addresses of <b>Enabled</b> devices
<b>No devices set to Enabled</b>	Ring election based on MAC addresses of all devices
<b>Single device set to Enabled</b>	<b>Enabled</b> device always master, failure of <b>Enabled</b> device results in ring election


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

Once all devices in the ring are configured and enabled, you can connect the ring ports.

Continue to the next section to see how to configure ring coupling. Do not connect coupling ports until network devices have been configured.

## Example: Configuring non-Master devices for Turbo Ring v2 in an On-board Rail Application

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

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

The Ring 1 Settings screen appears.

- Configure all of the following:

Option	Value
<b>Status</b>	<b>Enabled</b>
<b>Master</b>	<b>Disabled</b>
<b>Ring Port 1</b>	<b>1</b>
<b>Ring Port 2</b>	<b>2</b>

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
<b>Multiple devices set to Enabled</b>	Ring election based on MAC addresses of <b>Enabled</b> devices
<b>No devices set to Enabled</b>	Ring election based on MAC addresses of all devices
<b>Single device set to Enabled</b>	<b>Enabled</b> device always master, failure of <b>Enabled</b> device results in ring election

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

Once all devices in the ring are configured and enabled, you can connect the ring ports.

Continue to the next section to see how to configure ring coupling. Do not connect coupling ports until network devices have been configured.




## Example: Configuring the Primary Ring Coupling Between Consists

Both network devices that make up the ring coupling must be configured as coupling devices.

4. Make sure that you have configured both rings in the scenario.
5. Do not connect the coupling ports until completing setup on both devices. Our scenario assumes port **5** will serve as coupling port.
6. Couplers should only be configured on one ring. Our example uses SW-D as the primary and SW-H as the backup. Do not configure SW-1 or SW-5 as couplers.

To configure SW-D as the primary ring coupler:

- Sign in to the device with administrator credentials.
- Go to **Redundancy > Layer 2 Redundancy > Turbo Ring V2**, and then click **General**.
- Under Ring Coupling Settings, click  **[Edit]**.

The Ring Coupling Settings screen appears.

- Configure all of the following:

Option	Value
Status	Enabled
Coupling Mode	Primary Path
Coupling Port	5

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

The device has been configured as a primary ring coupling.

Connect the ring coupling ports. Once both devices are connected, you can move on to configuring the backup coupling.


## Example: Configuring the Backup Ring Coupling Between Consists

Both network devices that make up the backup ring coupling must be configured as coupling devices.

- Make sure that you have configured both rings in the scenario.

- Do not connect the coupling ports until completing setup on both devices. Our scenario assumes port **5** will serve as coupling port.
- Couplers should only be configured on one ring. Our example uses SW-D as the primary and SW-H as the backup. Do not configure SW-1 or SW-5 as couplers.

To configure SW-H as the backup coupler:

- Sign in to the device with administrator credentials.
- Go to **Redundancy > Layer 2 Redundancy > Turbo Ring V2**, and then click **General**.
- Under Ring Coupling Settings, click  **[Edit]**.

The Ring Coupling Settings screen appears.

- Configure all of the following:

Option	Value
Status	Enabled
Coupling Mode	Backup Path
Coupling Port	5

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

The device has been configured as a backup ring coupling.

Once the device has been configured, connect the ring coupling ports. Your coupling configuration will be complete.

## About RSTP

Rapid Spanning Tree Protocol (RSTP) is an IEEE 802.1w network protocol that enhances the speed and stability of the Spanning Tree Protocol (STP).

RSTP promotes high availability and a "loop-free" topology, similar to STP, but more quickly within Ethernet networks. It provides faster convergence and is backward compatible with STP. While STP takes 30-50 seconds to converge, RSTP can achieve sub-second convergence.

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

## How RSTP Works

Based on the original concept of the STP mode, the RSTP tree also grows from root to leaf to build a loop-free topology. This means that RSTP ensures that there is only a single active path between any two devices on an active connection. The remaining disabled connections serve as backup paths in case an active connection fails.

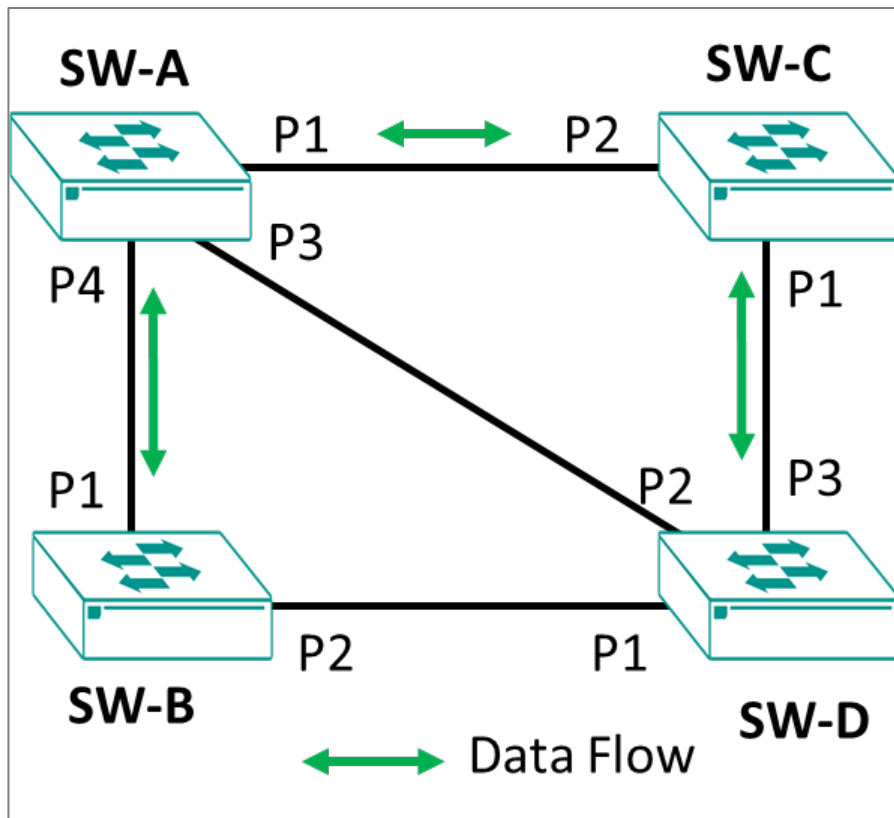
If you are new to STP, please refer to the IEEE 802.1D standard. As an enhancement of STP, RSTP speeds up network convergence. Rapid Spanning Tree Protocol (RSTP) includes additional information in the Bridge Protocol Data Units (BPDUs) that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connect through point-to-point links allow a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally, rather than network-wide. This allows RSTP to carry out automatic configuration and restore a links faster than STP. Additionally, as RSTP is a widely used protocol, Moxa equipment supports connections with switches from various vendors which support RSTP to form a redundant network architecture.

When RSTP is enabled on a network, the spanning tree algorithm automatically determines the configuration of the spanning tree. RSTP's algorithm follows these general procedures:

- **Determining the root bridge:** The switch with the lowest bridge priority is considered the root bridge through priority competition. In case of a tie, a tiebreaker based on the MAC address is used to determine the root bridge. Specifically, the switch with the lowest MAC address is considered the root bridge. All other switches are automatically designated as non-root switches.
- **Selecting the root port for non-root switches:** The root port is selected as the best path to the root bridge based on the root cost, which is typically determined by the bandwidth of the link. Each non-root switch has only one root port.
- **\*\*Assigning designated ports:\*\***Each connection (segment) must have a port assigned as the designated port for forwarding traffic. The designated port is the one that sends the best BPDU on its segment.
- **\*\*Remaining ports in blocking state:\*\***All remaining ports, including alternate ports or backup ports, are in a blocking state. These ports do not transmit data to other switches or learn MAC addresses.

## Scenario: RSTP on 4 Network Devices

In this scenario, we configure 4 network devices with RSTP.




SW-A will serve as the RSTP root. SW-B, C, and D will be connected to all other devices, but use the green arrow paths as their primary data path.

Ports are configured as follows:

	Device SW-A	Device SW-B	Device SW-C	Device SW-D
<b>Connects to SW-A</b>	N/A	P1	P2	P2
<b>Connects to SW-B</b>	P4	N/A	N/A	P1
<b>Connects to SW-C</b>	P1	N/A	N/A	P3
<b>Connects to SW-D</b>	P3	P2	P1	N/A

### Example: Configuring SW-A for RSTP


Here's how to configure SW-A as the root device for RSTP in our example.

- Sign in to the device with administrator credentials.
- Go to **Redundancy > Layer 2 Redundancy > Spanning Tree**, and then click **General**.
- Set **Status** to **Enabled**.
- Set **Bridge Priority** to **28672** to ensure that SW-A will always be set as the root.
- Click **Apply** to save changes.
- Locate **Port 1** on the list, and then click  **[Edit]**.

The Edit Port Settings screen appears.

- Set **Status** to **Enabled**.
- Click **Apply** to save changes.


The port settings will be reflected in the table.

- Locate **Port 3** on the list, and then click  **[Edit]**.

The Edit Port Settings screen appears.

- Click **Apply** to save changes.

The port settings will be reflected in the table.

- Locate **Port 4** on the list, and then click  **[Edit]**.

The Edit Port Settings screen appears.

- Click **Apply** to save changes.

The port settings will be reflected in the table.


SW-A is now configured for RSTP.

Continue to configure SW-B.

### **Example: Configuring SW-B and SW-C for RSTP**

Here's how to configure SW-B and SW-C for RSTP in our example.

- Sign in to the device with administrator credentials.
- Go to **Redundancy > Layer 2 Redundancy > Spanning Tree**, and then click **General**.
- Set **Status** to **Enabled**.
- Click **Apply** to save changes.

- Locate **Port 1** on the list, and then click  **[Edit]**.

The Edit Port Settings screen appears.

- Set **Status** to **Enabled**.
- Click **Apply** to save changes.

The port settings will be reflected in the table.

- Locate **Port 2** on the list, and then click  **[Edit]**.

The Edit Port Settings screen appears.

- Click **Apply** to save changes.


The port settings will be reflected in the table.

SW-B is now configured for RSTP.

Repeat this procedure on SW-C, and then proceed to configure SW-D.

### **Example: Configuring SW-D for RSTP**

Here's how to configure SW-D for RSTP in our example.

- Sign in to the device with administrator credentials.
- Go to **Redundancy > Layer 2 Redundancy > Spanning Tree**, and then click **General**.
- Set **Status** to **Enabled**.
- Click **Apply** to save changes.
- Locate **Port 1** on the list, and then click  **[Edit]**.

The Edit Port Settings screen appears.

- Set **Status** to **Enabled**.
- Click **Apply** to save changes.

The port settings will be reflected in the table.

- Locate **Port 2** on the list, and then click  **[Edit]**.

The Edit Port Settings screen appears.

- Set **Status** to **Enabled**.
- Click **Apply** to save changes.

The port settings will be reflected in the table.

- Locate **Port 3** on the list, and then click  **[Edit]**.

The Edit Port Settings screen appears.

- Set Path Cost to 150000

This will ensure that this path will be preferred over the other two ports.

- Click **Apply** to save changes.

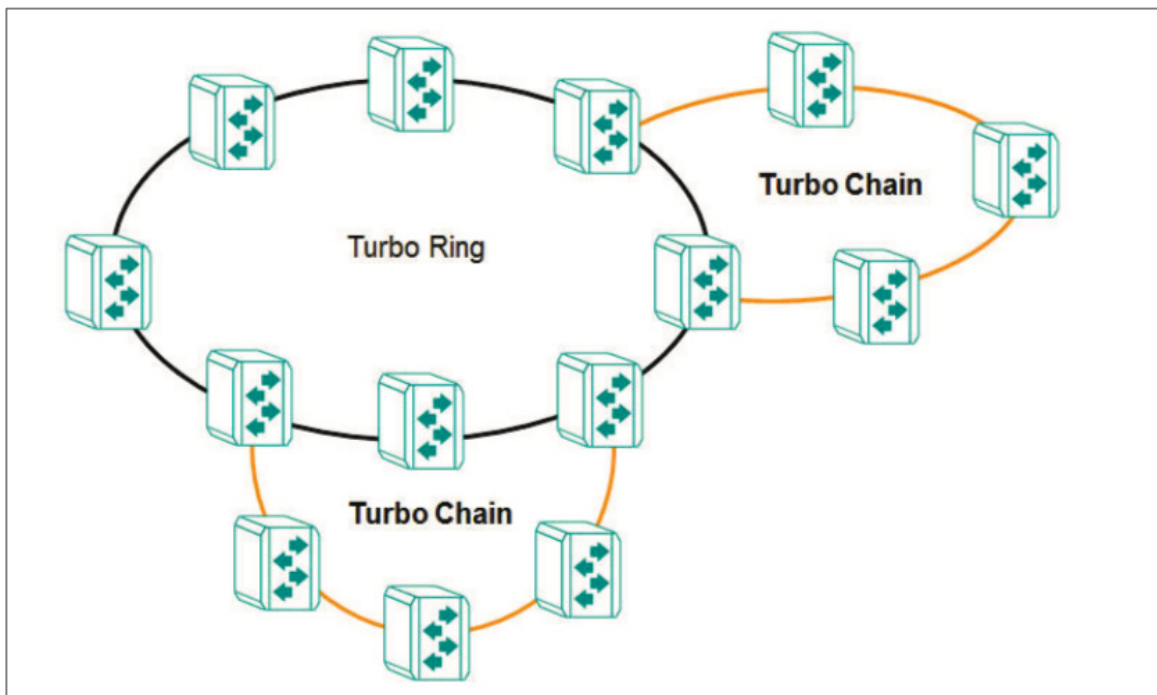
The port settings will be reflected in the table.

SW-D is now configured for RSTP. Now that all network devices are configured, in the event that one link is severed, data will automatically flow over backup paths.

## About Turbo Chain

Turbo Chain allows flexible expansion on top of an existing topology

This allows for flexible, cost-effective expansions. This allows you to grow existing networks without replacement the main ring while still maintaining reliability and redundancy.



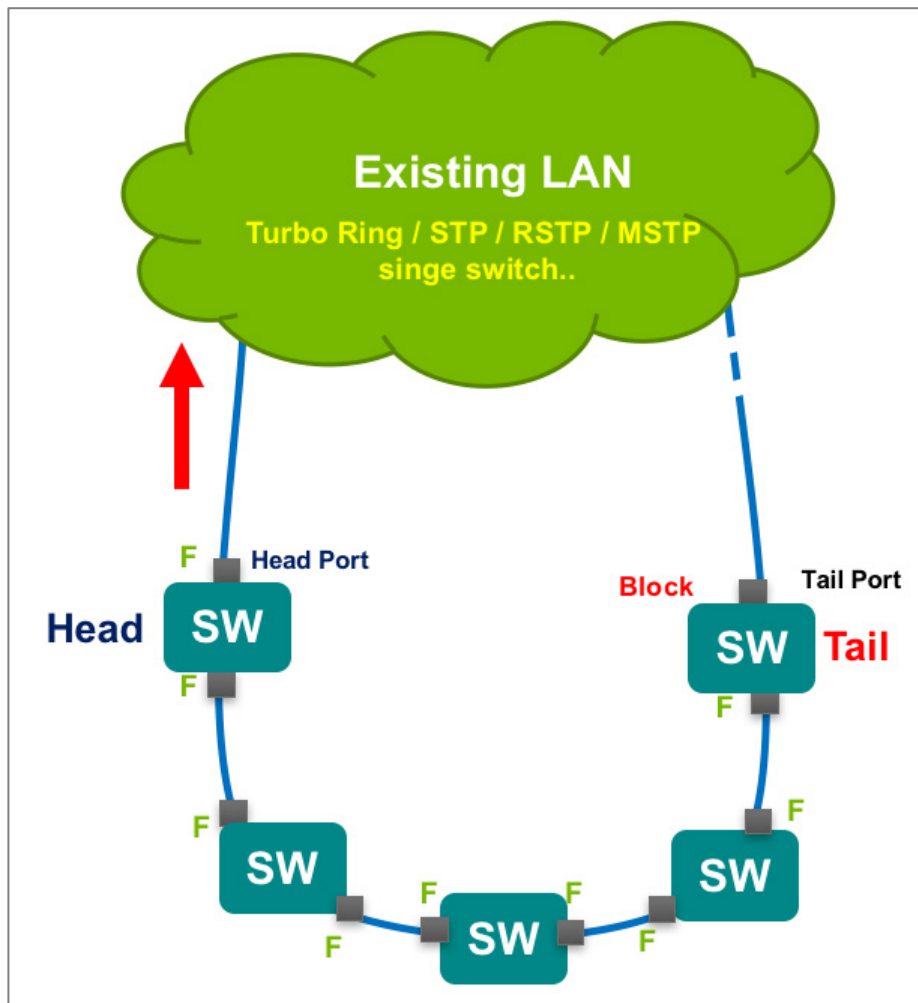
Turbo Chain is a proprietary redundancy technology developed by Moxa, designed for use in widely distributed networks. It enables Ethernet switches to be connected in a daisy-

chain configuration, where each switch serves as a backup path for connected devices. Turbo Chain supports system recovery times of under 20 ms for Fast Ethernet and 50 ms for Gigabit Ethernet in member port link environments.

Turbo Chain is suitable for industrial networks with complex topologies, particularly those utilizing multi-ring architectures. It allows the creation of flexible and scalable topologies with rapid media recovery.

In a typical Turbo Chain setup, each Ethernet switch is connected to two others in a daisy-chain configuration. The switches are categorized into three types: Head, Tail, and Member switches. The Head switch connects the chain to the external network, while the Tail switch provides redundancy. If the Head port is disconnected, the Tail port immediately assumes the role of data transfer, ensuring continuous communication.

This technology ensures that in the event of a link or switch failure, Turbo Chain quickly reroutes traffic to an available backup path, minimizing network downtime and maintaining uninterrupted communication.





Turbo Chain is often used in industrial automation, transportation, and surveillance applications where network reliability is critical. It is compatible with other Moxa networking technologies, such as Turbo Ring, and other Redundancy protocols like STP/RSTP, MSTP etc, to provide further redundancy and resilience for industrial networks.

To sum up, here are some of the features of Turbo Chain technology:

- **Topology:** Turbo Chain uses a daisy-chain topology to connect Ethernet switches in a loop-free configuration.
- **Redundancy:** Turbo Chain provides a backup path on the tail switch to ensure network availability and reduce downtime in the event of a switch or link failure.
- **Fast failover:** Turbo Chain has a fast failover mechanism that can detect and activate backup paths in a matter of milliseconds (< 20 ms) to ensure uninterrupted communication between devices.
- **Compatibility:** Turbo Chain is compatible with other redundancy technologies, such as Turbo Ring and RSTP, to provide even greater redundancy and resilience for industrial networks.

## Example: Configuring Turbo Chain

In this example, we will configure network devices for Turbo Chain.

- Determine which devices will be the head, tail, and members of the chain. The head and tail must connect to the main LAN.
- Do not connect any of the chain devices until configuration of all devices is complete.
- Do not use any of the chain ports until configuration is completed. Do not use these ports for administration, as applying the chain configuration to these ports will disconnect you from the web GUI.

You can configure the head, tail, and member devices in any order as long as you do not connect them until after all devices are configured. Choose a device to configure and do the following:

- Sign in to the device with administrator credentials.
- Go to **Redundancy > Layer 2 Redundancy > Turbo Chain**, and then click **Settings**.
- Set **Turbo Chain** to **Enabled**.

- For **Chain Role**, specify one of the following:
  - **Head** - specify only one head of the chain. This will be the primary connection to the rest of the network.
  - **Tail** - specify only one tail of the chain. This device will be the backup connection to the rest of the network.
  - **Member** - specify one or more member devices. Member devices make up the "links" between the head and the tail of the chain. Make sure that there are no loops in the chain.
- Specify the following Ports based on the **Chain Role**:

Head Chain Role Option	Port Value
------------------------	------------

<b>Head Port</b>	<b>1</b>
<b>Member Port</b>	<b>2</b>

Member Chain Role Option
--------------------------

<b>Member Port 1</b>	<b>1</b>
<b>Member Port 2</b>	<b>2</b>

Tail Chain Role Option
------------------------

<b>Tail Port</b>	<b>1</b>
<b>Member Port</b>	<b>2</b>

- Click **Apply** to save changes.
- Repeat this procedure to configure all devices in the chain. Once all devices have been configured, connect the devices in the chain.

Once all devices are configured and connected, packets are transmitted through the Head Port to the LAN network. If any Turbo Chain path is disconnected, the Tail Port will be activated so that packet transmission can continue.

## About VRRP

The Virtual Router Redundancy Protocol (VRRP) is a layer 3 redundancy protocol enabling multiple routers to collaborate as a group and share a virtual IP address.

The main purpose of VRRP is to provide redundancy for the default gateway utilized by hosts on a LAN or VLAN.

In a VRRP setup, a single router is designated as the "master" while the other routers are "backup" routers. The master router is responsible for forwarding packets sent to the virtual IP address. Additionally, backup routers supervise the master router and take over its tasks in case of failure. This enables automatic failover and redundancy, guaranteeing network connectivity—even in the event of a router failure.

## Benefits of VRRP

- **Increased Network Reliability:** VRRP enables multiple routers to work together in a group, sharing a virtual IP address. This provides redundancy for the default gateway, ensuring that network connectivity is maintained even if one of the routers fails. This increases the overall reliability of the network and helps prevent downtime.
- **Automatic Failover:** VRRP facilitates automatic failover, where backup routers take over the tasks of the master router in case of a failure. This ensures that there is no disruption to network services and users can continue to access resources without any interruption.
- **Easy Network Management:** VRRP simplifies network management by allowing multiple routers to work together as a group, sharing a virtual IP address. This eliminates the need for complex routing protocols and reduces the risk of misconfiguration.

## About VRRP States

With VRRP, routers are assigned different roles and states to ensure seamless failover and improved network availability.

The three primary states of VRRP are:

- **Init State:** This is the initial state when a VRRP router starts up. The router initializes its VRRP configuration and has not yet determined whether it should become a Master or a Backup router. The router remains in the Init state until it

starts receiving VRRP advertisements from other routers in the same VRRP group or until it begins sending advertisements itself.

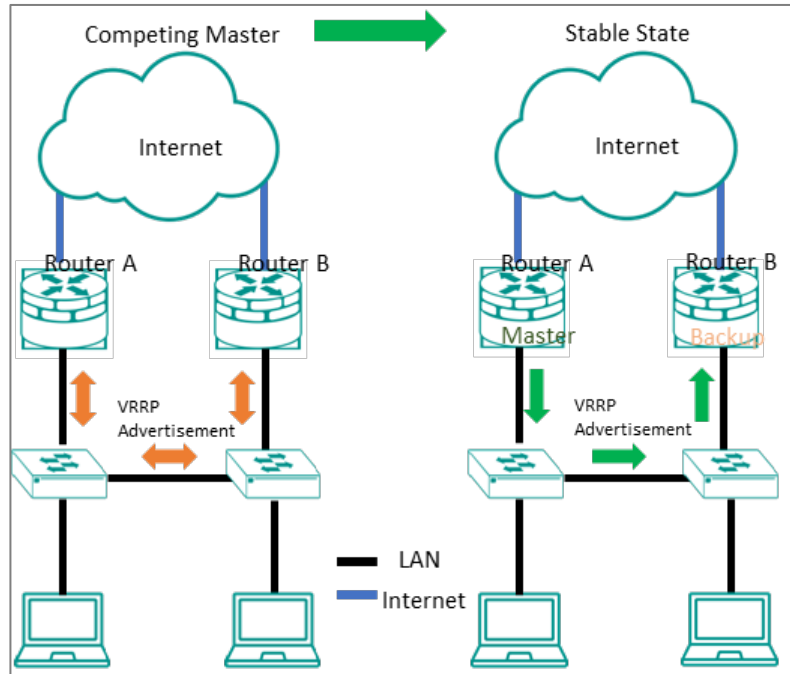
- **Master State:** In this state, the router is responsible for forwarding packets sent to the virtual IP address and acts as the default gateway for the devices in the network. The router with the highest priority (or lowest IP address in case of a tie) becomes the Master router. The Master router periodically sends VRRP advertisements to the other routers in the VRRP group to maintain its role. If the Master router fails, one of the Backup routers will take over the role based on priority.
- **Backup State:** Routers in the Backup state are waiting to take over the Master role if the current Master router fails. Backup routers listen for VRRP advertisements from the Master router and update their timers accordingly. If a Backup router stops receiving VRRP advertisements from the Master router for a certain period (typically three times the advertisement interval), it assumes that the Master router has failed and attempts to transition to the Master state based on its priority.

The VRRP states ensure that the network has a functioning default gateway at all times, providing redundancy and improving network availability in case of router failure. By implementing VRRP, network administrators can achieve increased network reliability, automatic failover, and easier network management.

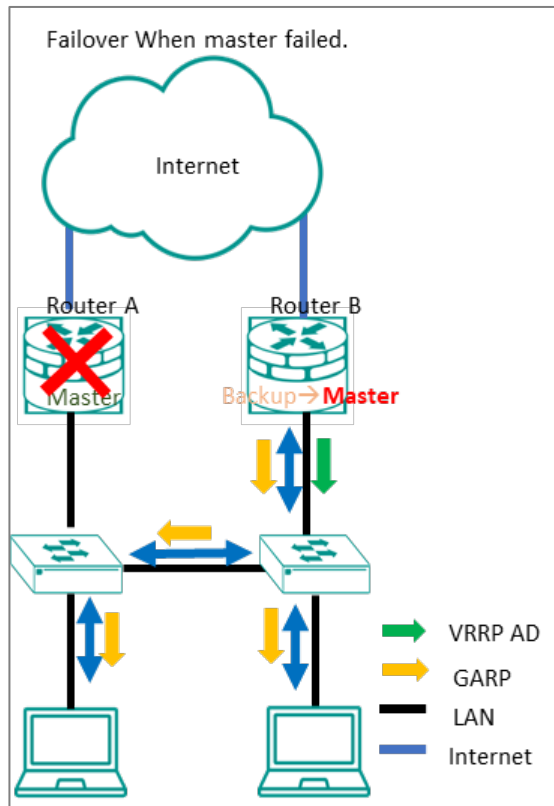
## VRRP in Depth

VRRP group routers select a master router based on priority, with the highest priority being the master.

To accomplish this, Each router in the group announces its priority, and the master router regularly sends out VRRP advertisements to the other routers to update its status.



The virtual IP address is linked with the VRRP group, and the master router forwards network packets using the virtual IP address as the source address. The backup routers stay inactive, listening to the VRRP messages from the master and ready to take over if the master fails. The Master Router sends advertisement packets to the backup routers to inform them that it is still operational. The advertisement interval is manually configured, with a default value of 1 second. If the master router fails, the Backup Router is unable to receive advertisement packets from the Master. Once the advertisement down timer expires, backup router will realize that the Master is experiencing issues or has powered down and one of the backup routers with a higher priority takes over as the new master, ensuring there is no disruption in network connectivity.



VRRP can also be set up to use preemption, which allows a higher-priority router to take over as the master even if the current master router is still functional. This can be useful when the higher-priority router is available again after a period of downtime.

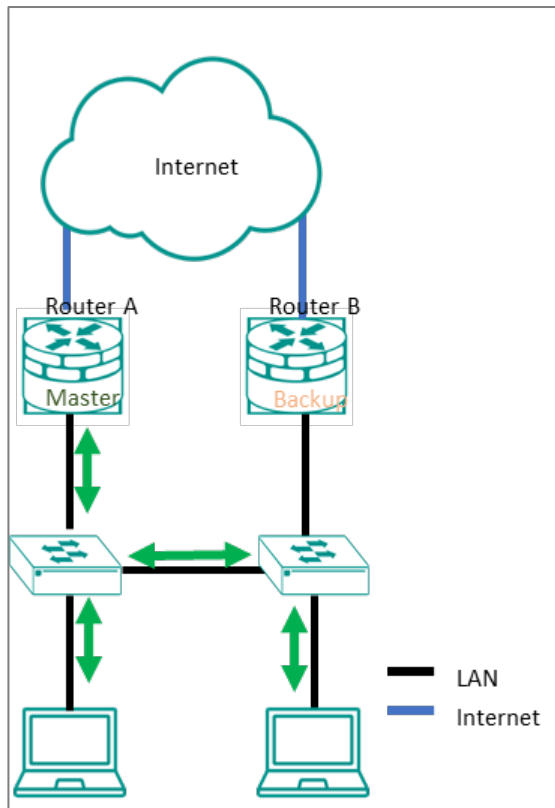
In summary, VRRP is a valuable protocol that provides redundancy in network environments where high availability is critical. It enables multiple routers to act as a single virtual router, ensuring network traffic continues to flow in the event of a router failure.

### Scenario: VRRP on Two Routers

In this scenario, we'll configure two routers connected to the same LAN (Local Area Network). We will configure VRRP to ensure that if one of the routers fails, the other router will continue to forward traffic to the LAN.

For example, suppose Router A (LAN interface IP: 192.168.127.1) is initially configured as the master and Router B (LAN interface IP: 192.168.127.2) as the backup in the VRRP group. Router A is responsible for forwarding packets to the LAN. The master should keep tracking the interface by ping the device (IP 192.168.127.100) in order to make sure of the LAN communication.

If Router A were to fail by ping lost or any link down event, Router B would detect this and assume the role of the master. It would then begin forwarding packets to the LAN, ensuring that there is no disruption in network connectivity. Once Router A becomes available, it can take over as the master, and Router B reverts to its backup role.



### Example: Configuring VRRP on Router A

This task assumes that each device has already configured an interface called LAN1 with the following IP addresses:

- Router A: 192.168.127.1
- Router B: 192.168.127.2

To configure Router A, do the following:

- Sign in to the device with administrator credentials.
- Go to **Redundancy** > **Layer 3 Redundancy** > **VRRP**, and then click **Settings**.
- On the lower table of the screen, click **+ [Add]**.

The Create Virtual Router screen appears.

- Configure the following, and then click **Create**.

Option	Value
Interface	LAN1
Virtual IP	192.168.127.3
Priority	200
Preemption	Enabled
Target IP	192.168.127.100

The **Virtual Router** settings appear in the list.

- Under the Virtual Router list, click **Apply**.
- At the top of the page, under **VRRP**, select **Enabled** from the dropdown list, and then click **Apply**.

Router A is now configured for VRRP.

Continue to configure Router B.

### Example: Configuring VRRP on Router B

This task assumes that each device has already configured an interface called LAN1 with the following IP addresses:

- Router A: 192.168.127.1
- Router B: 192.168.127.2

To configure Router B, do the following:

- Sign in to the device with administrator credentials.
- Go to **Redundancy > Layer 3 Redundancy > VRRP**, and then click **Settings**.
- On the lower table of the screen, click **+ [Add]**.

The Create Virtual Router screen appears.

- Configure the following, and then click **Create**.

Option	Value
Interface	LAN1



Option	Value
<b>Virtual IP</b>	192.168.127.3
<b>Priority</b>	100
<b>Preemption</b>	<b>Enabled</b>
<b>Target IP</b>	192.168.127.100

The **Virtual Router** settings appear in the list.

- Under the Virtual Router list, click **Apply**.
- At the top of the page, under **VRRP**, select **Enabled** from the dropdown list, and then click **Apply**.

Both routers are now configured for VRRP. In the event of a failure of one router, the other can take over using the same virtual IP address, ensuring continued function without reconfiguration.

## 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
<b>Static</b>	Manual Configuration	Manual Configuration
<b>Dynamic</b>	<ul style="list-style-type: none"><li>• <b>RIP</b></li><li>• <b>OSPF</b></li></ul>	<b>PIM</b>

**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.

## About Multicast Routing

**Multicast routing** is an efficient method for transmitting network traffic to a group of devices simultaneously. This approach helps conserve network resources, improve performance, and reduce congestion by sending only one copy of a message to all interested devices in the group.

A **Static Multicast Route** is a manually configured network path used to deliver multicast traffic to a specific group of devices on a network. It is a type of multicast route that is manually created and configured by a network administrator, rather than dynamically established by a multicast routing protocol. Static multicast routes are typically used in small networks where the multicast group membership is known and does not change frequently. They can also be used in situations where the multicast traffic needs to be routed through a specific path in the network, or when multicast traffic needs to be constrained to a specific set of network interfaces.

### Note

While enabling the static multicast routing, it is crucial to regularly review and adjust your configurations in response to any alterations in the network topology or multicast group memberships.


## About Selecting a Routing Protocol

**Short Description:** There are several factors to consider when selecting a routing protocol.

1. **Network Size:** In a small network with only a few L3 devices with two or three interfaces, static routing is often the simplest and most efficient option. Dynamic routing, on the other hand, is more suitable for multiple Layer 3 interfaces with many devices and complex interconnections.
2. **Topology Stability:** If the network topology is relatively stable and changes infrequently, static routing can be a reliable and predictable choice. In contrast, dynamic routing protocols like **RIP** and **OSPF** are designed to adapt to changes in

the network, making them better suited for networks that are constantly changing.

3. **Operational Cost:** Static routing requires manual configuration of each router, which can be time-consuming and error-prone in large networks. Dynamic routing protocols can automate this process, making it easier to manage and scale the network.
4. **Number of Receivers:** Unicast is a one-to-one communication method, while multicast is a one-to-many communication method. Unicast is typically used for sending data to a specific recipient, while multicast is used for delivering data to multiple recipients who have expressed interest in receiving data for a specific multicast group.

 **Note**

Dynamic routing can be vulnerable to attacks that manipulate routing information.

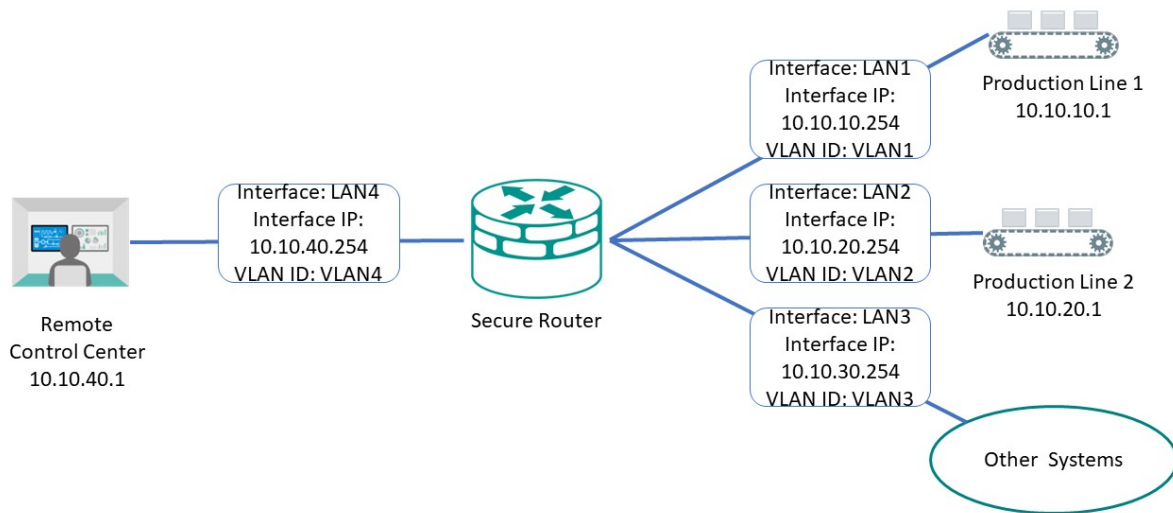
A combination of both static and dynamic routing may also be appropriate in some cases, such as when you have a core network that uses static routes and branch networks that use dynamic routing protocols.

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

Item	Value
<b>Metric</b>	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 <b>Metric</b> 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.

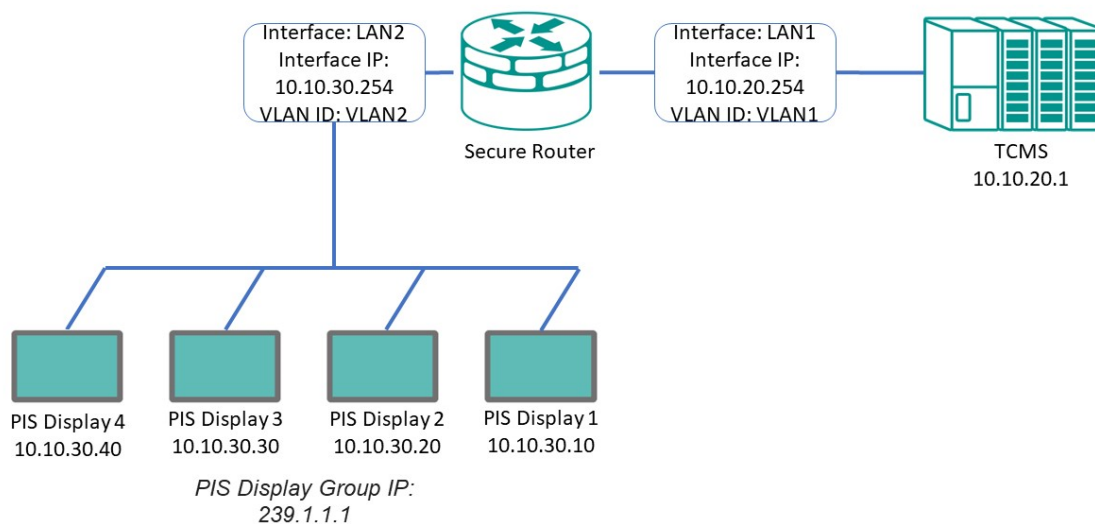
### **Example: Adding Static Multicast Route for Passenger Speed Display**

A train operator wants to display current train speed on the PIS (Passenger Information System), requiring the TCMS (Train Control Management System) to share speed information with the PIS. There are multiple displays in multiple cars throughout the train. Multicast static routing allows the TCMS to send a single packet to multiple displays across the train, minimizing traffic congestion and processing overhead. The reduction in the total number of packets on the network can make it easier to manage quality of service and allocate network resources effectively.

**Before you begin:** Make sure you have correctly configured:

- Each device with an IP address.

- Each display device to join the multicast group (239.1.1.1 in this example). Consult your PIS system documentation for details.
- VLANs for each subnet. Refer to VLAN for more information.
- VLAN assignment to an Interface. Refer to Network Interfaces for more information.
- IGMP Snooping as Enabled on the VLAN for the PIS displays. Refer to VLAN Settings - Edit VLAN Settings for more information.



To create a static multicast route for the PIS Display Group, do the following:

1. Go to **Routing**→**Multicast Route**→**Multicast Route Settings**, make sure **Mode** is set to **Static Multicast Route**, and then click **Apply**.
2. Go to **Routing**→**Multicast Route**→**Static Multicast Route**, and then click **[Add]**.

**Result:** The **Create Static Multicast Route** panel appears.

3. Specify all of the following:

Item	Value
Status	Enable



Item	Value
<b>Group Address</b>	239.1.1.1 Refers to the group IP used by the PIS displays. Packets sent to this address will be sent to all devices configured to listen on this IP which also share the other parameters specified in this section.
<b>Source Address Type</b>	Choose <b>Specify Source</b> , and then specify 10.10.20.1 This refers to the Control Unit, ensuring that other potential devices on this interface and VLAN do not generate unnecessary packets and traffic.
<b>Inbound Interface</b>	<b>LAN1</b> Refers to the interface connecting the TCMS to the Secure Router. Since the TCMS provides the speed data for the displays.
<b>Outbound Interface</b>	<b>LAN2</b> Refers to the interface connecting the PIS screens to the Secure Router.

4. Click **Create**.

**Result:** The new static routing entry appears in the routing table.

### Results:

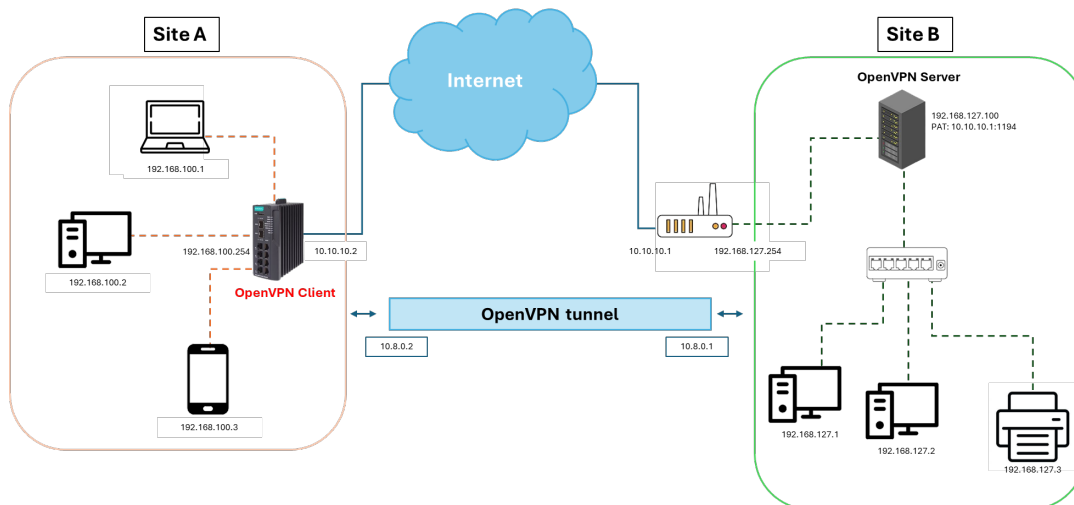
Multicast packets from the TCMS meeting the specified criteria will be sent to PIS screens, allowing them to display speed data without generating duplicate or extra packets that might reduce network performance.

## About OpenVPN Client

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques to create secure point-to-point or site-to-site connections. It can establish a safe and encrypted tunnel between devices and a VPN server, ensuring the internet traffic remains private and secure. OpenVPN can also traverse network address translators (NAT) and firewalls, making it a versatile and powerful solution for secure communication over the Internet.

### Scenario: Using a Site-to-Site OpenVPN Tunnel

Our scenario two locations, Site A and Site B, which need to securely share resources.



Site A has multiple devices that need access to the resources at Site B. Configuring OpenVPN on each device at Site A is complex and time-consuming. To simplify the setup, the user decides to use the router at Site A as an OpenVPN client, facilitating connections from all devices at site A to site B as though they were on the local network.

## Configuring the Router as an OpenVPN Client

Configuring the router as client allows all traffic from devices at Site A to be tunneled over the Internet to Site B as though they were on the same network.

**Before you begin:** Make sure that you have an OpenVPN Profile (.ovpn file) from the VPN server. Additionally, the router at site B must be configured with PAT (Port Address Translation) to forward OpenVPN packets to the OpenVPN server at IP address 192.168.127.100.

### Note

Applying the OpenVPN client will disable the IPSec VPN, which may result in VPN connection loss.

1. Sign in to the device with administrator credentials.
2. Go to **VPN > OpenVPN Client > Settings**.
3. Configure all of the following:

Option	Value
<b>Status</b>	<b>Enabled</b>
<b>Description</b>	Optionally enter a description of up to 40 characters.

Option	Value
<b>Import OpenVPN Profile</b>	Import an OpenVPN profile from the local file system.
<b>Username</b>	Enter a username if required by the OpenVPN server.
<b>Password</b>	Enter a password if required by the OpenVPN server.


4. Click **Apply** to save your settings.

**Results:** After the OpenVPN connection is established, the connection will be visible under **VPN > OpenVPN Client > Status**. Additionally, the routing information for the VPN will be visible in the routing table under **Routing > Unicast Route > Routing Table**.

**What to do next:** If the OpenVPN server cannot identify IPs from site A, it may be necessary to add a NAT rule on the OpenVPN client.

### Example: Configuring NAT to Translate over OpenVPN

For OpenVPN servers that are unable to identify IP addresses from site A, you can add a NAT rule on the OpenVPN client router.

1. Sign into the device with administrator credentials.
2. To configure the inbound rule, go to **NAT**, and then click  **[Add]**.
3. Configure all of the following:

Option	Value
<b>Status</b>	<b>Enabled</b>
<b>Description</b>	Optional: Enter your description here
<b>Index</b>	Specify an index (ID) for the route.
<b>Mode</b>	<b>Advance</b>
<b>Protocol</b>	<b>ICMP, TCP, UDP</b>
<b>Incoming Interface (Original Packet)</b>	<b>LAN</b>
<b>Source IP Mapping Type (Original Packet)</b>	<b>Subnet Mask</b>

Option	Value
Source IP (Original Packet)	192.168.100.0
Subnet Mask (Original Packet)	24 (255.255.255.0)
Source Port mapping Type (Original Packet)	Any
Destination IP Mapping Type (Original Packet)	Any
Destination Port Mapping Type (Original Packet)	Any
Outgoing Interface (Translated Packet)	Any
Source IP Mapping Type (Translated Packet)	Single
Source IP (Translated Packet)	10.8.0.2
Source Port Mapping Type (Translated Packet)	Any
Destination IP Mapping Type (Translated Packet)	Any
Destination Port Mapping Type (Translated Packet)	Any

4. Click **Apply**.

The NAT rule will appear on the list.

The router will now ensure that packets between the local network and the OpenVPN tunnel are translated to the tunnel IP address to facilitate transmission on the remote server.

## About NetFlow

NetFlow collects detailed information about the traffic passing through a network interface.

It provides network administrators with valuable insights into traffic flow within the network, allowing them to monitor and analyze network traffic effectively. This capability is crucial for performance monitoring, capacity planning, troubleshooting, and security analysis.

## NetFlow In Depth

Netflow architecture generally contains three main components.

### NetFlow Exporter

NetFlow exporters are devices that collect and export traffic data, typically a router. The exporter gathers data from the network interface, aggregates packet headers, and sends this information via UDP to the NetFlow collector for analysis.

#### Note

The exporter identifies the flows by at least one of the following features: IP Source, IP Destination, Source Port, Destination Port, Class of Service, Layer 3 Protocol Type, and Interface.

### NetFlow Collector

NetFlow collectors are servers or appliances that receive the aggregated flows transmitted by NetFlow exporters, storing and preprocessing the flow data for the NetFlow analyzer.

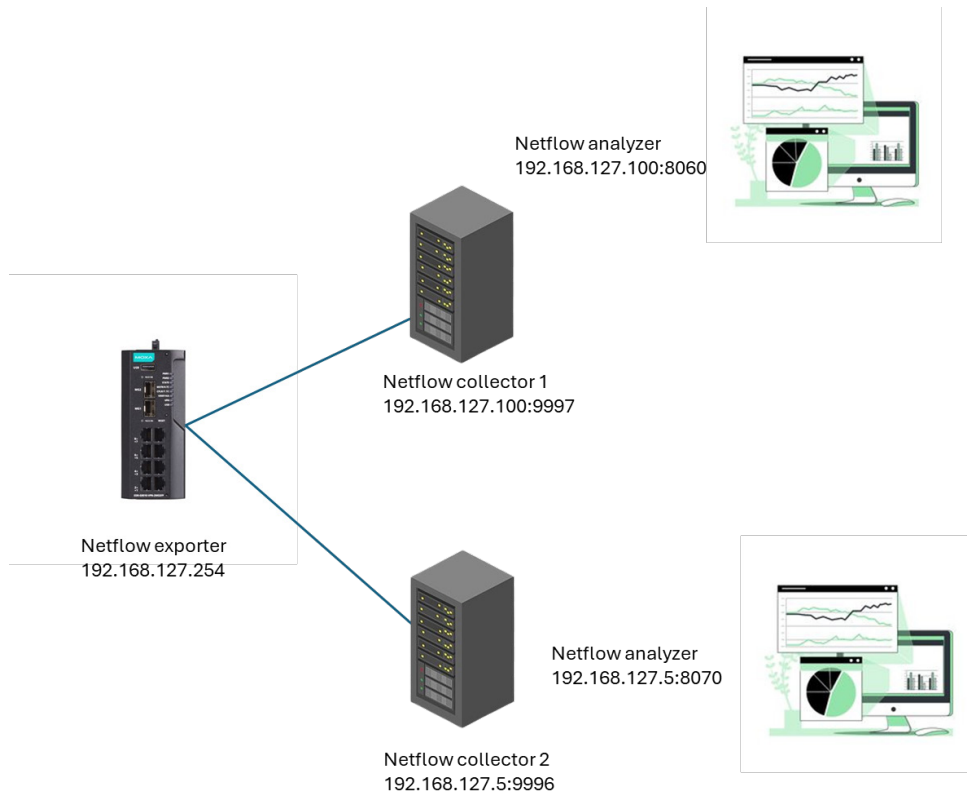
### NetFlow Analyzer

NetFlow analyzers are software tools designed to analyze flow data records stored by NetFlow collectors, transforming them into visual reports to aid network administrators in understanding and optimizing network performance.

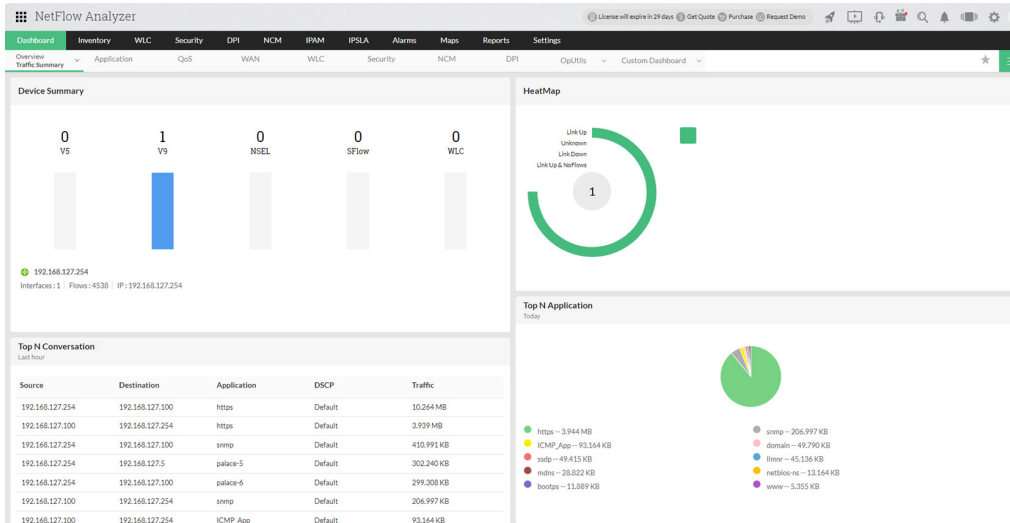
## Scenario: Using NetFlow to Collect LAN Interface Data

See how NetFlow can be used to monitor an enterprise network.

In a large enterprise network, network administrators need to monitor network traffic in real time to ensure stable performance and quickly identify potential security threats. The diagram provided is a simplified example to illustrate the basic concept of NetFlow monitoring and analysis. The system consists of three main components: a NetFlow Exporter, two NetFlow Collectors for redundancy, and a NetFlow Analyzer.

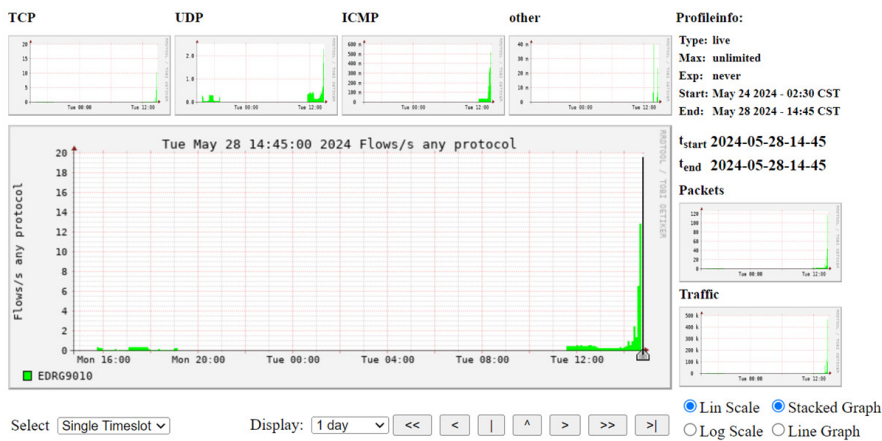


- Netflow Exporter: The router collects network traffic data from the interfaces, and sends it to two Netflow collector servers.
  - 2 NetFlow Collectors (Middle Servers)
- Flows will be sent to both collectors simultaneously. If one collector fails, the other will continue to operate, providing a degree of redundancy.
- NetFlow Analyzers (Software Based):
    - One NetFlow collector running **NetFlow Analyzer on Windows OS**



- One NetFlow collector running **NfSen on Linux**

Profile: live



Statistics timeslot May 28 2024 - 14:45


Channel:	Flows:					Packets:					Traffic:				
all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	
<input checked="" type="checkbox"/> EDRG9010	3.3 /s	1.1 /s	2.2 /s	0.0 /s	0 /s	13.4 /s	7.5 /s	5.8 /s	0.1 /s	0 /s	26.3 kb/s	20.0 kb/s	6.2 kb/s	60.3 b/s	
<b>TOTAL</b>	<b>3.3 /s</b>	<b>1.1 /s</b>	<b>2.2 /s</b>	<b>0.0 /s</b>	<b>0 /s</b>	<b>13.4 /s</b>	<b>7.5 /s</b>	<b>5.8 /s</b>	<b>0.1 /s</b>	<b>0 /s</b>	<b>26.3 kb/s</b>	<b>20.0 kb/s</b>	<b>6.2 kb/s</b>	<b>60.3 b/s</b>	

Display:  Sum  Rate


After collection, the data is sent to an analyzer. The analyzer processes this data and transforms it into visual reports, making it easier to understand and analyze network traffic patterns.

## Example: Configuring the Router as a NetFlow Exporter

To be effective in a NetFlow topology, the device must be configured as a NetFlow Exporter with the correct settings for collectors.

1. Sign in to the device using administrator credentials.
2. Go to **Diagnostics > Tools > NetFlow**.
3. To create Collector entries, next to **Collector Settings**, click  **[Add]** twice.
4. Under **NetFlow Settings**, configure all of the following:

Option	Value
<b>NetFlow</b>	<b>Enabled</b>
<b>Version</b>	<b>V9</b> Selected the correspond NetFlow version for your NetFlow collector.
<b>Collector 1 IP/Host Name</b>	192.168.127.100
<b>Collector 1 Port</b>	9997
<b>Collector 2 IP/Host</b>	192.168.127.5
<b>Collector 2 Port</b>	9996
<b>Active NetFlow Entry Timeout</b>	1
<b>Inactivity Timeout</b>	1

5. Click **Apply** to apply these settings.
6. Above the table on the bottom half of the page, click  **[Add]**.

The Create NetFlow Entry screen appears.

7. Specify all of the following:

<b>Status</b>	<b>Enabled</b>
<b>Interface</b>	<b>LAN</b> Select the network interface to be monitor by NetFlow. In this scenario, "LAN" interface (192.168.127.254/24) is selected.
<b>Traffic Direction</b>	<b>Bidirectional</b>



## Mode

## Basic

**Basic** mode collects all data from the interface. **Filter** mode collects specific data flow according to source IP, source port, destination IP, destination port, and Protocol (TCP, UDP).

## Sampling Rate

1

This parameter defines the sampling rate of NetFlow data. When the user inputs a parameter, the system will automatically sample 1 packet from the specified number of packets as the sampling rate. For example, if the parameter is set to 100, it means that 1 packet will be randomly selected from every 100 packets as the sampling rate. The range of the sampling rate is 0~65535, the default value is 0, which means the sampling function is inactive, the result is same as sampling every packet (sampling rate = 1).

Consider the following guidelines for setting the sampling rate for a production environment:

- Low Traffic Volume: 1 per 100-500 packets
- Medium Traffic Volume: 1 per 1,000-2,000 packets
- High Traffic Volume: 1 per 2,000-4,000 packets

8. Click **Create** to save changes.

## About Loopback Interfaces

Loopback interfaces are dummy IP interfaces to allow otherwise identical subnets to communicate without address conflicts or wasted ports.

Imagine a scenario where you need to enable NAT (Network Address Translation) to traverse a VPN (Virtual Private Network). Currently, the setup requires using a Secondary IP, which needs to be bound to a physical interface. This method, although functional, consumes a physical interface and requires additional configuration. Instead, consider using a virtual interface. A virtual interface is a software-based representation of a network interface that doesn't correspond to a physical port. By using virtual interfaces, you can achieve the same objectives without consuming physical hardware resources.

## Scenario: Connecting Two Subnets

In this network topology, two routers need to establish a VPN tunnel, but their underlying LANs use the same subnet (192.168.127.0/24). This setup typically encounters

difficulties because VPN tunnels cannot usually be established between two identical subnets.

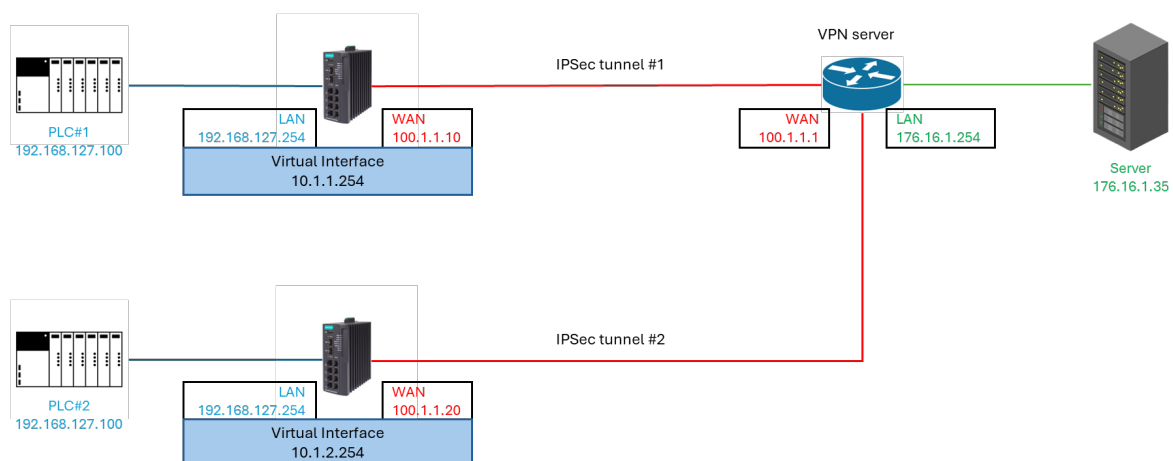
A common solution to this problem is configuring a **secondary IP** address on a physical interface. However, this approach requires binding the secondary IP to an additional physical interface. If the user does not need or cannot use additional physical interfaces, this method becomes impractical.

To solve this problem, we utilized the **loopback interface** feature. Each router is configured with a loopback interface, each with a unique IP address (10.1.1.254 and 10.1.2.254). This way, the two routers can establish VPN tunnels with their respective loopback interfaces without wasting physical ports.

This configuration allows VPN tunnels to be established between two identical LAN subnets (192.168.127.0/24) by using loopback interfaces to isolate and forward internal traffic. Loopback interfaces provide an additional IP layer for the routers, allowing VPN connections to operate normally without changing the internal LAN subnet. This way, PLC#1 and PLC#2 under the LAN can communicate with the remote server (176.16.1.30) through NAT, enabling cross-subnet data exchange.

Using loopback interfaces not only solves the VPN connection issue, but also avoids the need for additional physical interfaces, making it an efficient and flexible solution.

## Sample Topology



In this topology, PLC #1 and #2 both need to communicate with the server over a VPN connection. However, since they have identical local IP addresses and local subnets, their simultaneous connection would ordinarily result in IP address conflicts and routing

problems. With loopback interfaces configured with unique IP addresses, this can be avoided using the loopback interface as a medium for Network Address Translation.

- The VPN tunnel is established between the 176.16.1.0/24 subnet on the server side and the 10.1.1.254/24 and 10.1.2.254/24 loopback interfaces on the routers.
- Internal LAN addresses (192.168.127.0/24) are translated via NAT to communicate through the loopback interfaces. Specifically, PLC#1 at 192.168.127.100 will be translated to 10.1.1.254, and PLC#2 will be translated to 10.1.2.254.
- PLC#1 and PLC#2 use NAT to have their traffic directed through the loopback interface, enabling seamless communication with the server at 176.16.1.254.

By utilizing loopback interfaces and NAT, the architecture ensures that even with identical LAN subnets, VPN connectivity and inter-subnet communication are maintained without the need for additional physical interfaces.


## Setup

To configure this setup, you will need:

- Loopback Interface configuration on both routers (see subsequent section)
- NAT configuration to translate the NAT (see subsequent section)
- IPSec tunnels between the VPN server(WAN IP: 100.1.1.1), Router 1 (WAN IP: 100.1.1.254), and Router 2 (WAN IP: 100.1.2.254) using the loopback interfaces as endpoints.

## Example: Configuring a Loopback Interface for IPSec Tunnel #1

Virtual interfaces need to be defined before they can be translated.

1. Sign into the device with administrator credentials.
2. Go to **Network Configuration > Network Interfaces > Virtual Interface**.
3. Under Loopback Interface, click  **[Add]**.

The Create Loopback Interface Entry screen appears.

4. Configure all of the following:

Option	Value
<b>Name</b>	Specify a name. For our example, we will use VPNLoopback.
<b>Status</b>	<b>Enabled</b>
<b>ID</b>	1
<b>IP Address</b>	10.1.1.254
<b>Netmask</b>	<b>24 (255.255.255.0)</b>

5. Click **Apply**.


The loopback interface appears in the list.

Repeat this procedure on the other router to configure a loopback interface for IPSec tunnel #2 with the following differences:

- **IP Address:** 10.1.2.254

## Example: Configuring NAT to Translate to the Loopback Interface


For the Virtual Interface to be effective, NAT must be configured to correctly translate packets using the interface. Two rules must be configured on each router: an inbound rule and an outbound rule.

1. Sign into the device with administrator credentials.
2. To configure the inbound rule, go to **NAT**, and then click  **[Add]**.
3. Configure all of the following:

Option	Value
<b>Status</b>	<b>Enabled</b>
<b>Description</b>	Optional: Enter your description here
<b>Index</b>	Specify an index (ID) for the route.
<b>Mode</b>	<b>Advance</b>
<b>Protocol</b>	<b>ICMP, TCP, UDP</b>

Option	Value
Incoming Interface (Original Packet)	WAN
Source IP Mapping Type (Original Packet)	Any
Source Port mapping Type (Original Packet)	Any
Destination IP Mapping Type (Original Packet)	Single
Destination IP (Original Packet)	10.1.1.254
Destination Port Mapping Type (Original Packet)	Any
Outgoing Interface (Translated Packet)	Any
Source IP Mapping Type (Translated Packet)	Any
Destination IP Mapping Type (Translated Packet)	Single
Destination IP (Translated Packet)	192.168.127.100 This matches the PLC on our LAN.
Destination Port Mapping Type (Translated Packet)	Any

4. Click **Apply**.

5. To configure the outbound rule, go to **NAT**, and then click  **[Add]**.

6. Configure all of the following:

Option	Value
Status	Enabled
Description	Optional: Enter your description here
Index	Specify an index (ID) for the route.
Mode	Advance
Protocol	ICMP, TCP, UDP
Incoming Interface (Original Packet)	WAN

Option	Value
Source IP Mapping Type (Original Packet)	Any
Source Port mapping Type (Original Packet)	Any
Destination IP Mapping Type (Original Packet)	Single
Destination IP (Original Packet)	192.168.127.100 This matches the PLC on our LAN.
Destination Port Mapping Type (Original Packet)	Any
Outgoing Interface (Translated Packet)	Any
Source IP Mapping Type (Translated Packet)	Any
Destination IP Mapping Type (Translated Packet)	Single
Destination IP (Translated Packet)	10.1.1.254
Destination Port Mapping Type (Translated Packet)	Any

7. Click **Apply**.

Repeat this procedure on the other router to configure NAT binding for IPSec Tunnel #2 and corresponding virtual interface, with the following differences:

- Inbound rule:
  - **Destination IP** (Original Packet) : 10.1.2.254
- Outbound rule:
  - **Destination IP** (Translated Packet) : 10.1.2.254

## Chapter 6

---

# Railway Applications

# Railway Applications

Moxa devices support rail applications through practical implementation of IEC 61375.

## Overview of IEC 61375 for Rail Applications

IEC 61375 helps operators save time and money by standardizing communication throughout a train network while minimizing configuration.

### Ease of Coupling/Decoupling

Adjusting the length of trains by coupling or decoupling consists is a common practice to optimize the economics of revenue-generating rail services. Reduction in complexity and network configuration makes train coupling/decoupling more efficient, reducing downtime of revenue-generating services. IEC 61375 streamlines the train inauguration process with the Train Topology Discovery Protocol (TTDP).

TTDP allows the operational train composition and ETB state to be stored in a Train Topology Database (TTDB), stored on each ETBN router after successful inauguration. Moxa ETBN Routers make this information accessible through a web UI, a command line interface, and Simple Network Management Protocol (SNMP). End Devices (EDs) can further utilize the Train Real-time Data Protocol (TRDP) to retrieve the train's operational status and consist information from the ETBN. TRDP-based control and monitoring service interfaces allow the configuration of leading train direction, as well as access to comprehensive train network details.

### Simplify On-board Device Communication

Train coupling involves connecting either identical or different groups of train cars, known as consists. When using equipment compliant with the IEC 61375 standard, an operational train network configuration is automatically established. This setup ensures essential services, such as TCN-DNS and R-NAT, are configured on the ETBNs (Ethernet Train Backbone Node), regardless of whether the consists are similar or disparate.



This allows onboard EDs to seamlessly send and receive messages across consists using their respective TCN-URIs, without requiring any manual network configuration adjustments within the ECN. This reduction in manual configuration time reduces the need for downtime due to network configuration issues.

## **Failover Supports Redundancy**

IEC 61375 encourages the implementation of redundant communication paths and redundant network components. Redundancy helps ensure that even if one communication path or network component fails, there is an alternative path or component available for data transmission. This enhances the overall reliability of the onboard communication network.

## **Getting to Know IEC 61375**

IEC 61375 is a standard that outlines Train Communication Networks (TCNs).

Issued by the International Electrotechnical Commission, IEC 61375 defines the functional requirements and architecture for Train Communication Networks to ensure interoperability between different media types in an onboard train system. Supported media types include the Multifunction Vehicle Bus (MVB), Ethernet, and wireless, among others.

Rigorous application of the standard ensures standardized communication within and between different train components, contributing to interoperability and seamless integration of systems across the train network.

For the purpose of configuring your device for a rail environment, a basic grasp of the following standards and their terminology is helpful:

- IEC 61375-2-3 - Communication Profiles
- IEC 61375-2-5 - Ethernet Train Backbones
- IEC 61375-3-4 - Ethernet Consist Networks

The following sections provide foundational knowledge of these parts.

- [About Communication Profiles \(IEC 61375-2-3\)](#)

Part 2-3 defines the rules of data exchange between and within consists - known as profiles.

- [About Ethernet Train Backbones \(IEC 61375-2-5\)](#)

Part 2-5 defines the backbone for communication between consists based on Ethernet.

- [About Ethernet Consist Networks \(IEC 61375-3-4\)](#)

Part 3-4 defines networks within consists based on Ethernet.

## **About Communication Profiles (IEC 61375-2-3)**

Part 2-3 defines the rules of data exchange between and within consists - known as profiles.

Onboard application data such as Train Control and Monitoring System (TCMS) or Onboard Multimedia and Telematic Subsystems (OMTS) can take advantage of this communication profile to facilitate interoperability/data exchange. Train Communication Networks (TCN) can leverage the following services:

## **Train Real-time Data Protocol (TRDP)**

The Train Real-time Data Protocol contains two message types:

- Message Data (MD) - Request and Reply
- Process Data (PD) - Periodical Information/Monitoring

Communication Identifiers (ComIDs) are unique identifiers that distinguish between different types of TRDP participants. They are assigned to messages to define the purpose and destination within the communication network. On Moxa devices, attributes like port numbers for PD/MD are set using an XML file loaded onto the router.

## **Train Topology Database (TTDB)**

The Train Topology Database (TTDB) contains the following four data blocks:

- Consist Info
- Train Directory
- Operational Train Directory
- Train Network Directory

Moxa routers feature a TTDB manager that reads the database and displays the current train composition. TTDB-related status can also be retrieved from the TRDP with reserved ComIDs, as well as through the web and Command-line interfaces.

## **ETB Control Service Provider (ECSP) and Client (ECSC)**

The ETB Control Service Provider (ECSP) runs on each ETBN, and controls the ETB. They ensure efficient communication and event handling. ETBs require static consist information, uploaded in the form of an XML file on Moxa ETBN routers. Refer to [Structure and Syntax of Local Consist Info Files](#) for more information about XML configuration files.

The ETB Control Server Client (ECSC) is a consumer or user of the control services provided by the ECSP. Typically, it communicates with the ECSP through TRDP to access ETB control services, enabling actions like train inauguration and setting the leading direction.

## **TCN Domain Name System (TCN-DNS)**

Train Consist Network Domain Name system (TCN-DNS) focuses on domain name resolution and provides a way to help user to get operational train end device IP without pre-configured. It assists in mapping human-readable domain names to machine-readable IP addresses within the train communication environment. It supports multiple domain name resolutions via TRDP. After ECSP is configured correctly, the TCN-URI will be created automatically and available for query.

After the train inauguration process is completed, an operational train topology is established and end-device train network IP addresses are generated automatically. Certain activities—such as changing the train direction or inserting or removing a consist—will trigger dynamic regeneration of end-device train network IP addresses. TCN-

DNS is advantageous because it doesn't require preconfiguration. It can automatically map URLs to IP addresses based on the train operational status.

## TCN Uniform Resource Identifier (TCN-URI)

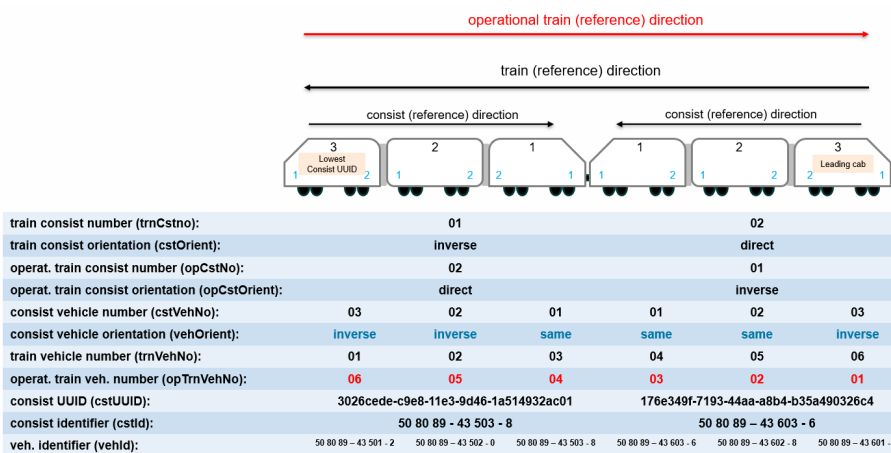
The TCN Uniform Resource Identifier (TCN-URI) defines URIs for resources within the train communication network. This can include addressing schemes, identification of specific resources, or end devices for communication within the train system. TCN-URIs can be resolved by the TCN-DNS on ETB routers.

## Safe Data Transmission (SDTv2)

Safe Data Transmission (SDTv2) is a TRDP mechanism ensuring reliability and safety of data exchanged within the train communication network. SDTv2 offers features such as sink-time supervision, safety codes, and other error detection mechanisms to guarantee the integrity and accuracy of transmitted information.

## IEC 61375-2-3 Terms

IEC 61375-2-3 defines terms such as directions, orientations, and numbers in a train. These concepts can be better understood through the diagram provided below.



## **About Ethernet Train Backbones (IEC 61375-2-5)**

Part 2-5 defines the backbone for communication between consists based on Ethernet. This ensures interoperability among different network architectures. This standard consists of the follow parts:

### **Ethernet Train Backbone Node (ETBN)**

An ETBN is a pivotal element within the TCN, functioning as a network node that facilitates communication between subsystems and end devices within a train.

### **Train Topology Discovery Protocol (TTDP)**

TTDP's primary purpose is to discover the train network topology during train inauguration. TTDP plays a crucial role in maintaining situational awareness within the train communication network, allowing devices to dynamically discover the presence of neighboring devices. This capability is vital for configuring, optimizing, and troubleshooting the network, ensuring that data is transmitted efficiently and reliably between different components within the train.

## **About Ethernet Consist Networks (IEC 61375-3-4)**

Part 3-4 defines networks within consists based on Ethernet. This network utilizes Ethernet technology to enable communication within a train consist, allowing devices and systems within the train to exchange data.

### **Ethernet Device (ED)**

An Ethernet Device (ED) is a networked device that operates within a train communication system.

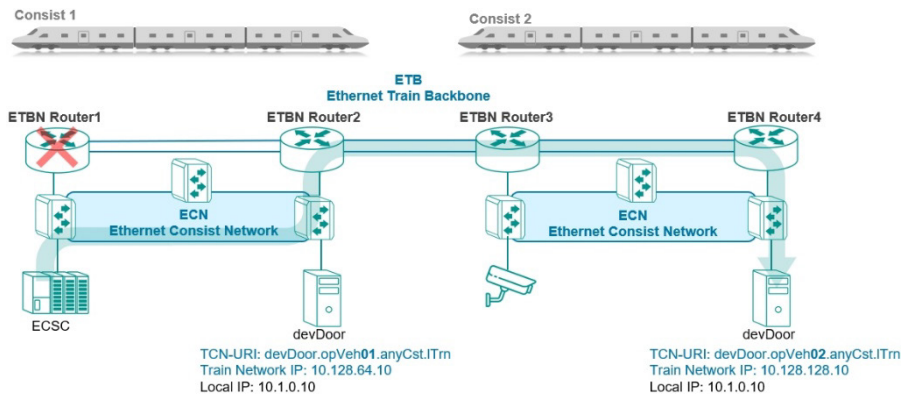
## **Railway-Network Address Translation (R-NAT)**

Railway-Network Address Translation (R-NAT) bridges the gap between internal and external networks. Internal train networks typically use private IP addresses that are not accessible (private, non-routable) outside the train network. R-NAT can translate these addresses to allow the ETB IP address to be used by internal devices to access external network resources. This allows internal devices to communicate with external devices, such as external railway infrastructure.

### **Scenario: 2 Consists, Each with 2 Redundant ETBNs/ECSPs**

In this scenario, we demonstrate an inter-consist network connection with two ETBN in each consist. Having two ETBN routers on each Consist offers enhanced networking reliability.

With the Virtual Router Redundancy Protocol (VRRP) and a redundant router, router failures can be bypassed. In this example with 2 redundant ETBN routers in each consist, in the event ETBN Router 1 fails, the ECSC on Consist 1 can still reach ED (devDoor) on Consist 2 with TCN-URI:devDoor.opVeh02.anyCst.ITrn. ETBN Router 1 will be bypassed, and ETBN router 2 will be used instead. Packets will be relayed to ETBN Router 3 and ETBN Router 4 in turn, before finally reaching the destination train network IP (10.128.128.10).



## About Traffic Flows in ETBNs

A sample of traffic flow over an ETBN using a cross-consist camera connection.

## Network Topology

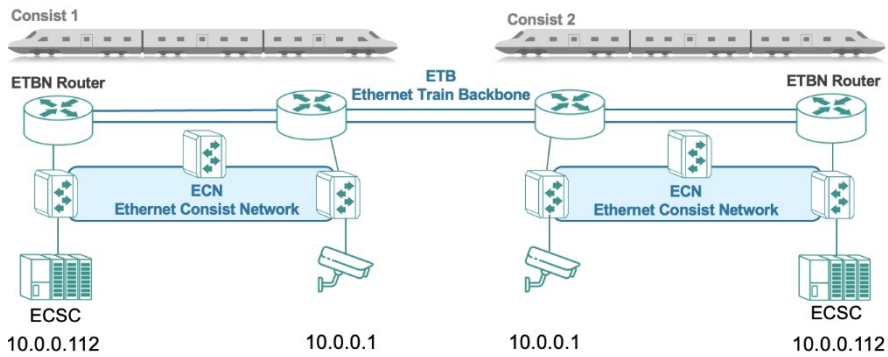
In the example topology below, there are two ETBNs in each consist, and there are two consists coupled together.

The two ETBNs in each consist will negotiate to decide which will serve as primary and backup ECSPs.

The primary ECSP will do two things:

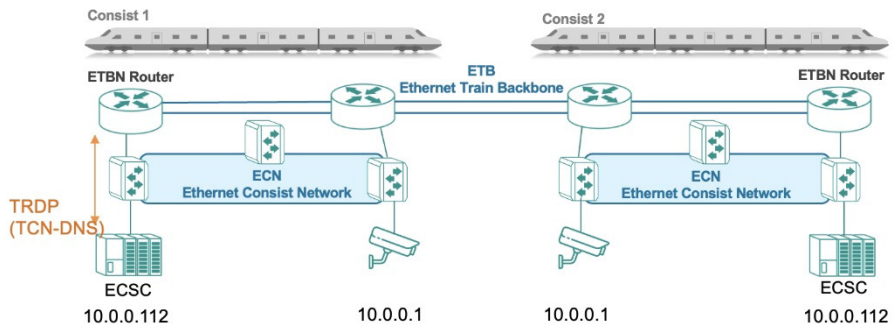
1. Act as the gateway for end device cross-subnet(consist) traffic.
2. Act as the ECSP providing ECSP functions (e.g., respond to TCN-DNS queries from other end devices.)

Let's see how the communication works when the ECSC in consist 1 wants to communicate with the camera in Consist 2.



## T=0 Getting Camera IP

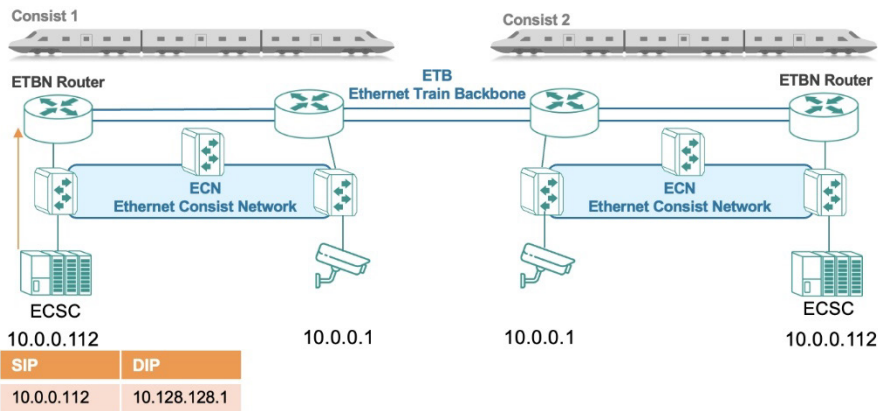
The ECSC in Consist 1 will ask the ECSP (ETBN router) for the Camera IP in consist 2 using TRDP(TCN-DNS). In this case, the master ECSP will respond with the global IP of the camera in consist 2 (10.128.128.1).



## T=1 DIP/SIP

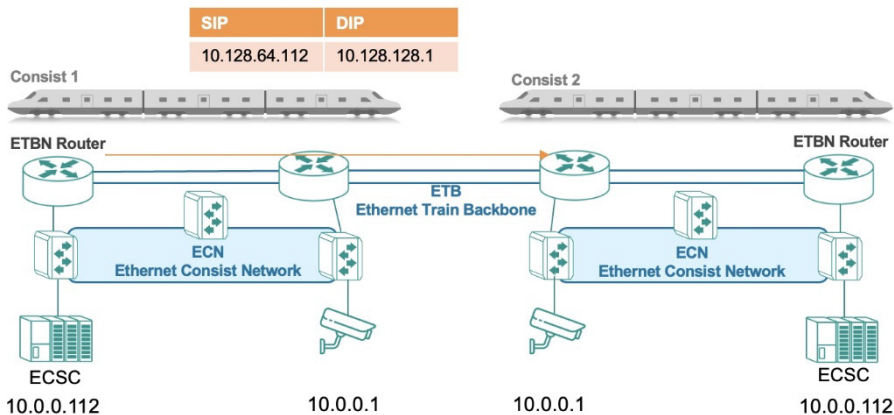
After getting the IP of the consist 2 camera, the ECSC will send out a packet with DIP=camera IP(10.128.128.1), SIP=ECSC local IP(10.0.0.112). Because this is cross-subnet communication, the ECSC will send the packet to the default gateway (10.0.63.254, which is the virtual IP provided by the two ETBNs).





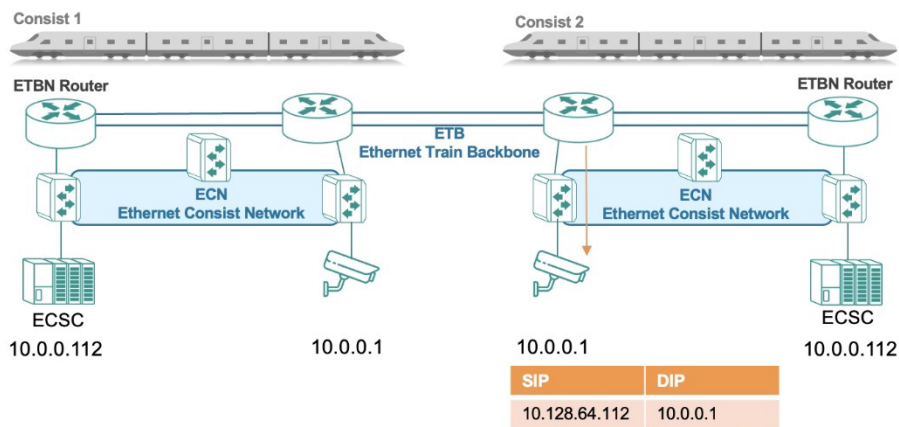
### T=2 R-NAT Translation from Consist 1

After receiving the packet, the ETBN router will translate the source IP address from Consist 1 using R-NAT, and then send it to the corresponding ETBN in Consist 2. In this case, the ETBN in Consist 1 will translate the SIP of the ECSC (10.0.0.112) to the global IP (10.128.64.112).



### T=3 R-NAT Translation to Consist 2

When the ETBN in Consist 2 receives the packets, it translates the destination IP address using R-NAT, and then sends them to the ECN interface. In this case, the ETBN in Consist 2 will translate the DIP of the camera (10.128.128.1) to the local IP (10.0.0.1).



## Example: Configuring 2 Consists with 2 Redundant ETBN Routers Each

Redundant routers in each consist provide an extra layer of reliability.

- Make sure that hardware environment is ready to accommodate this topology and configuration.
- Make sure that you have correctly defined the XML configuration file required for Communication Profiles. While this tutorial provides a sample file, it only covers one consist. Refer to [Structure and Syntax of Local Consist Info Files](#) for more information about XML configuration files.

To configure hardware to match the example configuration with 2 Consists with 2 Redundant ETBN Routers, do the following:

1. Configure Consist 1:
2. Configure TTDP on ETBN router 1.  
Refer to [Example: Configuring TTDP for ETBN Router 1 on Consist 1](#) for detailed instructions.
3. Configure IEC 61375 Communication Profile on ETBN router 1.  
Refer to [Example: Configuring Local Consist Info for ETBNs/ECSPs](#) for detailed

instructions.

4. Configure TTDP on ETBN router 2.  
Refer to [Example: Configuring TTDP for ETBN Router 2 on Consist 1](#) for detailed instructions.
5. Upload a local consist info file to ETBN router 2.  
Refer to [Example: Configuring Local Consist Info for ETBNs/ECSPs](#) for detailed instructions.
6. Configure Consist 2:
7. Configure TTDP on ETBN router 1.  
Refer to [Example: Configuring TTDP for ETBN Router 1 on Consist 2](#) for detailed instructions.
8. Configure IEC 61375 Communication Profile on ETBN router 1.  
Refer to [Example: Configuring Local Consist Info for ETBNs/ECSPs](#) for detailed instructions.
9. Configure TTDP on ETBN router 2.  
Refer to [Example: Configuring TTDP for ETBN Router 2 on Consist 2](#) for detailed instructions.
10. Configure IEC 61375 Communication Profile on ETBN router 2.  
Refer to [Example: Configuring Local Consist Info for ETBNs/ECSPs](#) for detailed instructions.

The TTDP configuration procedure for each ETBN router is similar. The following provides a quick reference of the differences in each configuration:

Table 1. Comparison of 2 Consists with 2 Redundant ETBN Routers Each

	Consist 1		Consist 2	
	ETBN Router 1	ETBN Router 2	ETBN Router 1	ETBN Router 2
<b>Consist UUID</b>	00000000-0000-0000-0000-000000000001		00000000-0000-0000-0000-000000000002	

	Consist 1		Consist 2	
<b>Local ETBN Static ID</b>	<b>1</b>	<b>2</b>	<b>1</b>	<b>2</b>
<b>ECN interface IP address</b>	<b>10.0.0.1</b>	<b>10.0.0.2</b>	<b>10.0.0.1</b>	<b>10.0.0.2</b>

### Example: Configuring TTDP for ETBN Router 1 on Consist 1

Here's how to perform the GUI configuration for a 2 ETBN/ECSP sample train network.

1. Using an account with Admin authority, log in to the network device.
2. Go to **Industrial Application > IEC 61375 > Ethernet Train Backbone > TTDP Settings**.
3. Set **TTDP Enable** to **Enabled**.
4. Under **Local Consist**, configure all of the following:

Option	Description
--------	-------------

**ETB Backbone ID 0**

This field identifies the type of traffic carried by the ETB, and should be the same within the same ETB.

Since both ETBNs are in the same ETB, their ETB backbone IDs are the same.

Option	Description
<b>Consist UUID</b>	00000000-0000-0000-0000-000000000001  The UUID is the same within the same consist. The example UUID is manually assigned, but they can also be randomly generated.
<b>ETBN(s) in Consist</b>	<b>2</b>  Dictated by our sample topology.
<b>ECN(s) in Consist</b>	<b>1</b>  Multi-application consists might have additional ECNs to support additional applications - such as having both TCMS and Media - but our example is limited to 1 for now.

5. Under Local ETBN, configure all of the following:


Option	Description
<b>Local ETBN Static ID</b>	<b>1</b>  Identifies the ETBN when there are multiple ETBNs in the same consist.
<b>Direction 1</b>	<b>Trunk 1</b>  In TN-4908, port 1,2 will be set as trunk 1, and port 5,6 will be set as trunk 2. Important: The direction of all ETBNs in the same consist should be the same.
<b>Direction 2</b>	<b>Trunk 2</b>
<b>ETB Port Speed</b>	<b>Auto</b>

Option	Description
--------	-------------

**ETB Port VLAN ID** 1000

Defines the VLAN ID of the ETB interface. The TTDP function will generate the corresponding ETB and ECN interface.

**Result:** Once the **Local Consist** and **Local ETBN** information is filled out, the  button will be available.

- Click **Add** () to add a Consist Network. The Add ECN screen appears.
- In the Add ECN screen, configure the following:

Option	Description
--------	-------------

**ECN to ETBN** **ETBN 1** and **ETBN 2**

**ECN Port VLAN ID** 1001

For single ECN consists, the value should be shared by all ETBNs, and should be at least 1000. ETBNs on the same VLAN should have different IP addresses.

For multi-application consists with multiple ECNs where each ETBN handles a different ECN, the default value is 1000 + **Local ETBN Static ID**.

**ECN interface IP address** 10.0.0.1

Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP.

Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to [Redundancy > Layer 3 Redundancy > VRRP](#) for more information about VRRP.

Option	Description
--------	-------------

**ECN Ports**      **port3, port4, port7, and port8**

The field is to define which ports on the TN-4900 are the ECN ports. These selected ports will be assigned to the ECN interface.

8. Click **Apply**.

**Results:** You have configured TTDP for ETBN 1 on Consist 1.

To finish configuring of ETBN router, you must configure the Communication Profile by uploading a local consist info file. Refer to [Example: Configuring Local Consist Info for ETBNs/ECSPs](#) for detailed instructions.

After configuring ETBN router 1 on Consist 1, you must configure ETBN router 2 on Consist 1, as well as ETBNs 1 and 2 on Consist 2.

This example uses 4 ETBN routers, 2 on each consist. All ETBN routers in all consists must be correctly configured before the example setup is complete.

### **Example: Configuring TTDP for ETBN Router 2 on Consist 1**

Here's how to perform the GUI configuration for a 2 ETBN/ECSP sample train network.

1. Using an account with Admin authority, log in to the network device.
2. Go to **Industrial Application > IEC 61375 > Ethernet Train Backbone > TTDP Settings**.
3. Set **TTDP Enable** to **Enabled**.
4. Under **Local Consist**, configure all of the following:

Option	Description
--------	-------------

**ETB Backbone ID 0**

This field identifies the type of traffic carried by the ETB, and should be the same within the same ETB.

Since both ETBNs are in the same ETB, their ETB backbone IDs are the same.

**Consist UUID 00000000-0000-0000-0000-000000000001**

The UUID is the same within the same consist. The example UUID is manually assigned, but they can also be randomly generated.

**ETBN(s) in Consist 2**

Dictated by our sample topology.

**ECN(s) in Consist 1**

Multi-application consists might have additional ECNs to support additional applications - such as having both TCMS and Media - but our example is limited to 1 for now.

5. Under Local ETBN, configure all of the following:

Option	Description
--------	-------------


**Local ETBN Static ID 2**

Identifies the ETBN when there are multiple ETBNs in the same consist.



Option	Description
<b>Direction 1</b>	<b>Trunk 1</b>
	In TN-4908, port 1,2 will be set as trunk 1, and port 5,6 will be set as trunk 2. Important: The direction of all ETBNs in the same consist should be the same.
<b>Direction 2</b>	<b>Trunk 2</b>
<b>ETB Port Speed</b>	<b>Auto</b>
<b>ETB Port VLAN ID</b>	1000
	Defines the VLAN ID of the ETB interface. The TTDP function will generate the corresponding ETB and ECN interface.

**Result:** Once the **Local Consist** and **Local ETBN** information is filled out, the  button will be available.

- Click **Add** () to add a Consist Network. The Add ECN screen appears.
- In the Add ECN screen, configure the following:

Option	Description
<b>ECN to ETBN</b>	<b>ETBN 1</b> and <b>ETBN 2</b>

Option	Description
<b>ECN Port VLAN ID</b>	<p>1001</p> <p>For single ECN consists, the value should be shared by all ETBNs, and should be at least 1000. ETBNs on the same VLAN should have different IP addresses.</p> <p>For multi-application consists with multiple ECNs where each ETBN handles a different ECN, the default value is 1000 + <b>Local ETBN Static ID</b>.</p>
<b>ECN interface IP address</b>	<p>10.0.0.2</p> <p>Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP.</p> <p>Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to <a href="#">Redundancy &gt; Layer 3 Redundancy &gt; VRRP</a> for more information about VRRP.</p>
<b>ECN Ports</b>	<p><b>port3, port4, port7, and port8</b></p> <p>The field is to define which ports on the TN-4900 are the ECN ports. These selected ports will be assigned to the ECN interface.</p>

8. Click **Apply**.

**Results:** You have configured TTDP for ETBN 2 on Consist 1.

To finish configuring of ETBN router, you must configure the Communication Profile by uploading a local consist info file. Refer to [Example: Configuring Local Consist Info for ETBNs/ECSPs](#) for detailed instructions.

After configuring ETBN router 2 on Consist 1, you must configure ETBN routers 1 and 2 on Consist 2.

This example uses 4 ETBN routers, 2 on each consist. All ETBN routers in all consists must be correctly configured before the example setup is complete.

## Example: Configuring TTDP for ETBN Router 1 on Consist 2

Here's how to perform the GUI configuration for a 2 ETBN/ECSP sample train network.


1. Using an account with Admin authority, log in to the network device.
2. Go to **Industrial Application > IEC 61375 > Ethernet Train Backbone > TTDP Settings**.
3. Set **TTDP Enable** to **Enabled**.
4. Under **Local Consist**, configure all of the following:

Option	Description
<b>ETB Backbone ID</b>	<b>0</b>  This field identifies the type of traffic carried by the ETB, and should be the same within the same ETB.  Since both ETBNs are in the same ETB, their ETB backbone IDs are the same.
<b>Consist UUID</b>	00000000-0000-0000-0000-000000000002  The UUID is the same within the same consist. The example UUID is manually assigned, but they can also be randomly generated.
<b>ETBN(s) in Consist</b>	<b>2</b>  Dictated by our sample topology.
<b>ECN(s) in Consist</b>	<b>1</b>  Multi-application consists might have additional ECNs to support additional applications - such as having both TCMS and Media - but our example is limited to 1 for now.

5. Under Local ETBN, configure all of the following:

Option	Description
<b>Local ETBN Static ID</b>	<b>1</b>  Identifies the ETBN when there are multiple ETBNs in the same consist.
<b>Direction 1</b>	<b>Trunk 1</b>  In TN-4908, port 1,2 will be set as trunk 1, and port 5,6 will be set as trunk 2. Important: The direction of all ETBNs in the same consist should be the same.
<b>Direction 2</b>	<b>Trunk 2</b>
<b>ETB Port Speed</b>	<b>Auto</b>
<b>ETB Port VLAN ID</b>	1000  Defines the VLAN ID of the ETB interface. The TTDP function will generate the corresponding ETB and ECN interface.

**Result:** Once the **Local Consist** and **Local ETBN** information is filled out, the  button will be available.

- Click **Add** () to add a Consist Network. The Add ECN screen appears.
- In the Add ECN screen, configure the following:

Option	Description
<b>ECN to ETBN</b>	<b>ETBN 1</b> and <b>ETBN 2</b>

Option	Description
<b>ECN Port VLAN ID</b>	<p>1001</p> <p>For single ECN consists, the value should be shared by all ETBNs, and should be at least 1000. ETBNs on the same VLAN should have different IP addresses.</p> <p>For multi-application consists with multiple ECNs where each ETBN handles a different ECN, the default value is 1000 + <b>Local ETBN Static ID</b>.</p>
<b>ECN interface IP address</b>	<p>10.0.0.1</p> <p>Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP.</p> <p>Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to <a href="#">Redundancy &gt; Layer 3 Redundancy &gt; VRRP</a> for more information about VRRP.</p>
<b>ECN Ports</b>	<p><b>port3, port4, port7, and port8</b></p> <p>The field is to define which ports on the TN-4900 are the ECN ports. These selected ports will be assigned to the ECN interface.</p>

8. Click **Apply**.

**Results:** You have configured TTDP for ETBN 1 on Consist 1.2

To finish configuring of ETBN router, you must configure the Communication Profile by uploading a local consist info file. Refer to [Example: Configuring Local Consist Info for ETBNs/ECSPs](#) for detailed instructions.

After configuring ETBN router 1 on Consist 2, you must configure ETBN router 2 on Consist 2.

This example uses 4 ETBN routers, 2 on each consist. All ETBN routers in all consists must be correctly configured before the example setup is complete.

## Example: Configuring TTDP for ETBN Router 2 on Consist 2

Here's how to perform the GUI configuration for a 2 ETBN/ECSP sample train network.

1. Using an account with Admin authority, log in to the network device.
2. Go to **Industrial Application > IEC 61375 > Ethernet Train Backbone > TTDP Settings**.
3. Set **TTDP Enable** to **Enabled**.
4. Under **Local Consist**, configure all of the following:

Option	Description
<b>ETB Backbone ID</b>	<b>0</b>  This field identifies the type of traffic carried by the ETB, and should be the same within the same ETB.  Since both ETBNs are in the same ETB, their ETB backbone IDs are the same.
<b>Consist UUID</b>	<b>00000000-0000-0000-0000-000000000002</b>  The UUID is the same within the same consist. The example UUID is manually assigned, but they can also be randomly generated.
<b>ETBN(s) in Consist</b>	<b>2</b>  Dictated by our sample topology.

Option	Description
--------	-------------

**ECN(s) in Consist**      **1**

Multi-application consists might have additional ECNs to support additional applications - such as having both TCMS and Media - but our example is limited to 1 for now.

5. Under Local ETBN, configure all of the following:

Option	Description
--------	-------------

**Local ETBN Static ID**      **2**

Identifies the ETBN when there are multiple ETBNs in the same consist.

**Direction 1**      **Trunk 1**

In TN-4908, port 1,2 will be set as trunk 1, and port 5,6 will be set as trunk 2. Important: The direction of all ETBNs in the same consist should be the same.


**Direction 2**      **Trunk 2**

**ETB Port Speed**      **Auto**

**ETB Port VLAN ID**      1000

Defines the VLAN ID of the ETB interface. The TTDP function will generate the corresponding ETB and ECN interface.

**Result:** Once the **Local Consist** and **Local ETBN** information is filled out, the  button will be available.

6. Click **Add** () to add a Consist Network.  
The Add ECN screen appears.

7. In the Add ECN screen, configure the following:

Option	Description
<b>ECN to ETBN</b>	<b>ETBN 1</b> and <b>ETBN 2</b>
<b>ECN Port VLAN ID</b>	1001  For single ECN consists, the value should be shared by all ETBNs, and should be at least 1000. ETBNs on the same VLAN should have different IP addresses.  For multi-application consists with multiple ECNs where each ETBN handles a different ECN, the default value is 1000 + Local ETBN Static ID.
<b>ECN interface IP address</b>	10.0.0.2  Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP.  Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to <a href="#">Redundancy &gt; Layer 3 Redundancy &gt; VRRP</a> for more information about VRRP.
<b>ECN Ports</b>	<b>port3, port4, port7, and port8</b>  The field is to define which ports on the TN-4900 are the ECN ports. These selected ports will be assigned to the ECN interface.

8. Click **Apply**.

**Results:** You have configured TTDP for ETBN 2 on Consist 2.

To finish configuring of ETBN router, you must configure the Communication Profile by uploading a local consist info file. Refer to [Example: Configuring Local Consist Info for ETBNs/ECSPs](#) for detailed instructions.

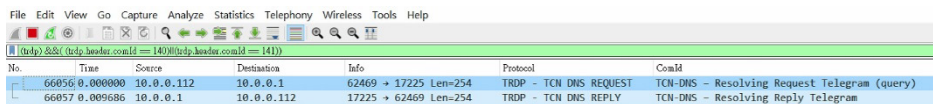


This example uses 4 ETBN routers, 2 on each consist. All ETBN routers in all consists must be correctly configured before the example setup is complete.

## Checking End-Device IPs

There are multiple ways to check the IP addresses of connected devices.

- Use an ECSP (ETB Control Service Provider) or TRDP application to query the end devices' IP with the TRDP protocol.



- Using WireShark to check IP addresses.
- Use the web console to check by opening the web console, and then navigating to **IEC-61375 > Operational Status > TCN-UI Table**.

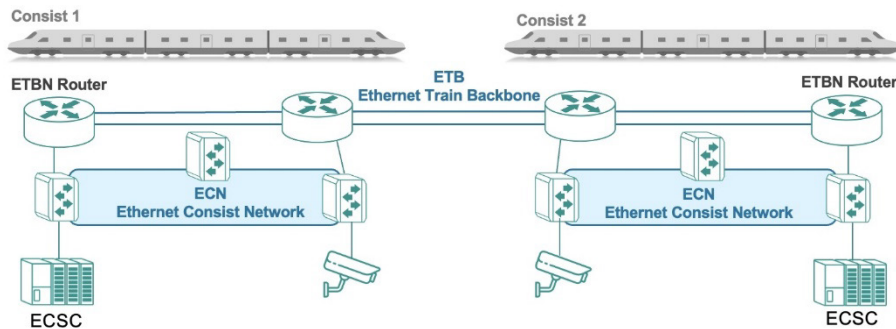
**TCN-URI Table** 1970/01/22 11:03:03

🔍 Search

Index	TCN-URI	Train Network IP	Local IP
1	grpAll.aVeh.aCst.ITrn	239.193.0.0	
2	grpAll.aVeh.ICst.ITrn	239.194.0.0	
3	devECSC.opVeh01.anyCst.ITrn	10.128.64.112	10.0.0.112
4	devsw1.opVeh01.anyCst.ITrn	10.128.64.101	10.0.0.101
5	devsw2.opVeh01.anyCst.ITrn	10.128.64.102	10.0.0.102
6	grpDoor.aVeh.aCst.ITrn	239.193.0.20	
7	grpDoor.aVeh.ICst.ITrn	239.194.0.20	
8	grpDoor.aVeh.opCst01.ITrn	239.194.1.20	
9	devECSC.opVeh02.anyCst.ITrn	10.128.128.111	10.0.0.111
10	devsw3.opVeh02.anyCst.ITrn	10.128.128.103	10.0.0.103
11	devsw4.opVeh02.anyCst.ITrn	10.128.128.104	10.0.0.104

## Getting ECSP Data with a Network Analyzer

Get train orientation, topology, and set leading direction with ECSP using a Network Analyzer.



In our example with 2 consists with 2 ETBNs each, users can use ECSC or the TRDP application to query the ETB information or control the ECSP with the TRDP protocol. Here are some example uses:

- Get train topology information.  
The ECSP (10.0.0.1) periodically sends out TTDB updates on IP 239.194.0.0. Users can use the TRDP application to get TTDB information.

No.	Time	Source	Destination	Info	Protocol	Content
22	0.000000	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
109	1.000452	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
217	0.901593	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
421	1.001417	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
638	1.000402	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
786	1.002041	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
934	0.998213	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
1083	1.000607	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
1228	0.999255	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
1375	1.000908	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
1519	1.000456	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
1667	0.998078	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
1815	1.000913	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
1992	1.000959	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
2142	1.002552	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
2291	0.999227	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
2435	1.001654	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
2584	1.000517	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
2741	0.991411	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
2888	1.000959	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram
3036	1.000401	10.0.0.1	239.194.0.0	33853 + 17224 Len=112	TRDP - TTDB STATUS	TTDB - Operational Train Directory Status Telegram

- Get ECSP information.  
The ECSP (10.0.0.1) periodically sends out the ECSP status to the ECSC (Ethernet Control Service Client, IP=10.0.0.112, configured the IP in the consist info XML file). Users can use the TRDP application to get ECSP status.

No.	Time	Source	Destination	Info	Protocol	Content	InitialSeq	InitialLen
23	0.000000	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
170	1.000452	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
218	0.991593	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
492	1.001417	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
630	1.000452	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
787	1.002041	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
935	0.998623	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
1084	1.000697	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
1229	0.999255	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
1376	1.000900	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
1526	1.000456	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
1668	0.998678	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
1816	1.000793	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
1993	1.000559	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
2143	1.002552	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
2292	0.998227	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
2436	1.001654	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
2585	1.000617	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
2742	0.991411	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
2889	1.000559	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		
3037	1.000441	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram		

- Use the TRDP application as ECSC to control the ECSP. For example, users can change the leading direction by sending the ECSP control packet with a different value in the leadingDir field.

No.	Time	Source	Destination	Info	Protocol	Content	InitialSeq	InitialLen
1	0.000000	10.0.0.112	10.0.0.1	50030 → 17224 Len=80	TRDP - ECSP CTRL	ecsp - Control Telegram		
4	0.317069	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram	False	False
5	0.716556	10.0.0.112	10.0.0.1	50030 → 17224 Len=80	TRDP - ECSP CTRL	ECSP - Control Telegram	False	False
7	0.718761	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram	False	False
8	0.718809	10.0.0.112	10.0.0.1	50030 → 17224 Len=80	TRDP - ECSP CTRL	ECSP - Control Telegram	False	False
10	0.211913	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram	False	False
11	0.812221	10.0.0.112	10.0.0.1	50030 → 17224 Len=80	TRDP - ECSP CTRL	ECSP - Control Telegram	False	False
13	0.187535	10.0.0.1	10.0.0.112	33853 → 17224 Len=80	TRDP - ECSP STATUS	ecsp - Status Telegram	False	False
14	0.846969	10.0.0.112	10.0.0.1	50030 → 17224 Len=80	TRDP - ECSP CTRL	ECSP - Control Telegram	False	False

```

Frame 1: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface vDeviceNPF_{17C338B4-8C5A-40C8-8625-DEEDB1FA1E6}, id 0
  Ethernet II, Src: LFCHeFe_8e:e0:b7 (38:f3:a0:8e:e0:b7), Dst: MoxaTech_96:7f:d0 (00:90:e8:96:7f:d0)
  Internet Protocol Version 4, Src: 10.0.0.112, Dst: 10.0.0.1
  User Datagram Protocol, Src Port: 50030, Dst Port: 17224
  TRDP (Dissector copyrighted by HDMX)
    Header
      sequenceCounter: 0x00000010
      protocolVersion: 1.0
      msgType: PD - PD Data (0x5004)
      ConId: ECSP - Control Telegram (120)
      etsIapCnt: 0x00000000
      opTrnTopoCnt: 0x00000000
      dataSetLength: 40
      replyConId: Hsncp:Find (0)
      replyIpAddress: 0.0.0.0
      headerFcs: 0xaf:7476
    ECSP CTRL
      version: 1.0
      devicName: devECSC
      inhiki: false (0)
      leadingReq: False (0)
      leadingDir: Not relevant (0)
      sncpReq: False (0)
      safetyTrall
        userDatVersion: 0.0
        safesecCnt: 0
        safetyCode: 0
  
```

## Getting ECSP Data with the Web GUI

Get ETB status and Train Network Directory with ECSP using a the web GUI.

1. Using an account with **Admin** authority, log in to the network device.
2. Do any of the following:
  - Choose from:
  - To view **ETB Status**, go to **Industrial Application > IEC 61375 > Ethernet Train Backbone > ETB Status**.
  - To view the **Train Directory**, go to **Industrial Application > IEC 61375 > Operational Status > Train Directory**.

## Viewing ETB Status

ETB Status 11/10/21 10:31:33

Version/Revision: Undefined    Length: False    Direction: False

Connectivity Table  
 ConnTableValid: ConnTableCst2  
 Title: 97025468

Search

Index	Orientation	Mac Address
1	Direct	00:90:82:96:79:20
2	Direct	00:90:82:82:56:12
3	Direct	00:90:82:12:34:65
4	Direct	00:90:82:12:43:56

Items per page: 5    1 - 4 of 4    [ < > ]

## Viewing Train Network Directory

Train Network Directory

ETB Table Valid: True

ETB Table Cst: 98027128    Management: ETB Table Cst: 98027128

Search

Index	CellUID	CN ID	Subnet ID (Train Subnet)	ETBN ID	Calibration
1	00000000-0000-0000-0000-000000000001	1	10.128.64.0/18	1	Direct
2	00000000-0000-0000-0000-000000000001	1	10.128.64.0/18	2	Direct
3	00000000-0000-0000-0000-000000000002	1	10.128.128.0/16	3	Direct
4	00000000-0000-0000-0000-000000000002	1	10.128.128.0/16	4	Direct

Items per page: 5    1 - 4 of 4    [ < > ]

## Scenario: 2 Consists, with 1 ETBN/ECSP Each

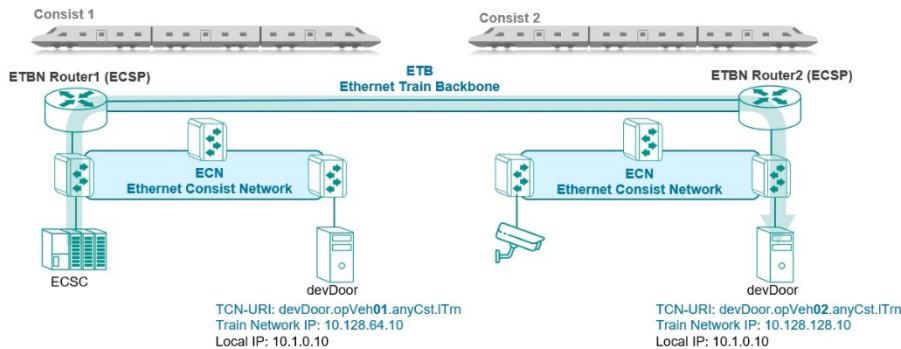
In this example, we demonstrate an inter-consist network connection with a single, non-redundant ETBN in each consist.

The ECSC on Consist 1 wants to send a command to devDoor, located on Consist 2. TCN-DNS and R-NAT make this easy, without requiring unique configuration.

While coupling two consists, as long as the inauguration is not inhibited, the train network is automatically re-established following the IEC 61375 inauguration procedure. The ETBN Router on each consist functions as a TCN-DNS server that can resolve TCN-URI requests. It also serves as a router to route the traffic to other VLAN domains.

In this example, the ECSC on Consist 1 needs to communicate with the ED (devDoor) with a TCN-URI, such as devDoor.opVeh02.anyCst.ITrn on Consist 2. Packets will be

related to ETBN Router 1, then ETBN Router 2, before finally reaching the destination train network IP (10.128.128.10).



## Example: Configuring 2 Consists with 1 ETBN/ECSP Each

Redundant routers in each consist provide an extra layer of reliability.

- Make sure that hardware environment is ready to accommodate this topology and configuration.
- Make sure that you have correctly defined the XML configuration file required for Communication Profiles. While this tutorial provides a sample file, it only covers one consist. Refer to [Structure and Syntax of Local Consist Info Files](#) for more information about XML configuration files.

To configure hardware to match the example configuration with 2 Consists with 1 ETBN Router each, do the following:

1. Configure Consist 1:
2. Configure TTDP on the Consist 1 ETBN router.  
Refer to [Example: Configuring TTDP for ETBN Router on Consist 1](#) for detailed instructions.
3. Upload a local consist file to the Consist 1 ETBN router.  
Refer to [Example: Configuring Local Consist Info for ETBNs/ECSPs](#) for detailed instructions.

4. Configure Consist 2:
5. Upload a local consist file to the Consist 2 ETBN router.  
Refer to [Example: Configuring TTDP for ETBN Router on Consist 2](#) for detailed instructions.
6. Configure IEC 61375 Communication Profile on the Consist 2 ETBN router.  
Refer to [Example: Configuring Local Consist Info for ETBNs/ECSPs](#) for detailed instructions.

The TTDP configuration procedure for each ETBN router is similar. The following provides a quick reference of the differences in each configuration:

Comparison of 2 Consists with 1 ETBN/ECSP Each

Consist 1		Consist 2	
ETBN Router 1		ETBN Router 1	
<b>Consist UUID</b>	00000000-0000-0000-0000-000000000001	00000000-0000-0000-0000-000000000002	

### Example: Configuring TTDP for ETBN Router on Consist 1

Here's how to perform the GUI configuration for a 1 ETBN/ECSP sample train network.

1. Using an account with Admin authority, log in to the network device.
2. Go to **Industrial Application > IEC 61375 > Ethernet Train Backbone > TTDP Settings**.
3. Set **TTDP Enable** to **Enabled**.
4. Under **Local Consist**, configure all of the following:


Option	Description
<b>ETB Backbone ID</b>	<b>0</b>  This field identifies the type of traffic carried by the ETB, and should be the same within the same ETB.
<b>Consist UUID</b>	00000000-0000-0000-0000-000000000001  The UUID is the same within the same consist. The example UUID is manually assigned, but they can also be randomly generated.
<b>ETBN(s) in Consist</b>	<b>1</b>  Dictated by our sample topology.
<b>ECN(s) in Consist</b>	<b>1</b>  Multi-application consists might have additional ECNs to support additional applications - such as having both TCMS and Media - but our example is limited to 1 for now.

5. Under Local ETBN, configure all of the following:

Option	Description
<b>Local ETBN Static ID</b>	<b>1</b>  Identifies the ETBN when there are multiple ETBNs in the same consist.
<b>Direction 1</b>	<b>Trunk 1</b>  In TN-4908, port 1,2 will be set as trunk 1, and port 5,6 will be set as trunk 2. Important: The direction of all ETBNs in the same consist should be the same.

Option	Description
<b>Direction 2</b>	<b>Trunk 2</b>
<b>ETB Port Speed</b>	<b>Auto</b>
<b>ETB Port VLAN ID</b>	1000  Defines the VLAN ID of the ETB interface. The TTDP function will generate the corresponding ETB and ECN interface.

**Result:** Once the **Local Consist** and **Local ETBN** information is filled out, the  button will be available.

- Click **Add** () to add a Consist Network. The Add ECN screen appears.
- In the Add ECN screen, configure the following:

Option	Description
<b>ECN to ETBN</b>	<b>ETBN 1</b>
<b>ECN Port VLAN ID</b>	1001  For single ECN consists, the value should be shared by all ETBNs, and should be at least 1000. ETBNs on the same VLAN should have different IP addresses.  For multi-application consists with multiple ECNs where each ETBN handles a different ECN, the default value is 1000 + <b>Local ETBN Static ID</b> .



Option	Description
<b>ECN interface IP address</b>	<p>10.0.0.1</p> <p>Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP.</p> <p>Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to <a href="#">Redundancy &gt; Layer 3 Redundancy &gt; VRRP</a> for more information about VRRP.</p>
<b>ECN Ports</b>	<p><b>port3, port4, port7, and port8</b></p> <p>The field is to define which ports on the TN-4900 are the ECN ports. These selected ports will be assigned to the ECN interface.</p>

8. Click **Apply**.

**Results:** You have configured TTDP for the ETBN router on Consist 1.

**What to do next:** To finish configuring of ETBN router, you must configure the Communication Profile by uploading a local consist info file. Refer to [Example: Configuring Local Consist Info for ETBNs/ECSPs](#) for detailed instructions.

After configuring the ETBN router on Consist 1, you must configure the ETBN router on Consist 2.

This example uses 2 ETBN routers, 1 on each consist. All ETBN routers in all consists must be correctly configured before the example setup is complete.

## Example: Configuring TTDP for ETBN Router on Consist 2

Here's how to perform the GUI configuration for a 2 ETBN/ECSP sample train network.

1. Using an account with Admin authority, log in to the network device.

2. Go to **Industrial Application > IEC 61375 > Ethernet Train Backbone > TTDP Settings**.
3. Set **TTDP Enable** to **Enabled**.
4. Under **Local Consist**, configure all of the following:


Option	Description
<b>ETB Backbone ID</b>	<b>0</b>  This field identifies the type of traffic carried by the ETB, and should be the same within the same ETB.
<b>Consist UUID</b>	<b>00000000-0000-0000-0000-000000000002</b>  The UUID is the same within the same consist. The example UUID is manually assigned, but they can also be randomly generated.
<b>ETBN(s) in Consist</b>	<b>1</b>  Dictated by our sample topology.
<b>ECN(s) in Consist</b>	<b>1</b>  Multi-application consists might have additional ECNs to support additional applications - such as having both TCMS and Media - but our example is limited to 1 for now.

5. Under Local ETBN, configure all of the following:

Option	Description
<b>Local ETBN Static ID</b>	<b>1</b>  Identifies the ETBN when there are multiple ETBNs in the same consist.

Option	Description
<b>Direction 1</b>	<b>Trunk 1</b>
	In TN-4908, port 1,2 will be set as trunk 1, and port 5,6 will be set as trunk 2. Important: The direction of all ETBNs in the same consist should be the same.
<b>Direction 2</b>	<b>Trunk 2</b>
<b>ETB Port Speed</b>	<b>Auto</b>
<b>ETB Port VLAN ID</b>	1000
	Defines the VLAN ID of the ETB interface. The TTDP function will generate the corresponding ETB and ECN interface.

**Result:** Once the **Local Consist** and **Local ETBN** information is filled out, the  button will be available.

- Click **Add** () to add a Consist Network.  
The Add ECN screen appears.
- In the Add ECN screen, configure the following:

Option	Description
<b>ECN to ETBN</b>	<b>ETBN 1</b>

Option	Description
<b>ECN Port VLAN ID</b>	<p>1001</p> <p>For single ECN consists, the value should be shared by all ETBNs, and should be at least 1000. ETBNs on the same VLAN should have different IP addresses.</p> <p>For multi-application consists with multiple ECNs where each ETBN handles a different ECN, the default value is 1000 + <b>Local ETBN Static ID</b>.</p>
<b>ECN interface IP address</b>	<p>10.0.0.1</p> <p>Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP.</p> <p>Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to <a href="#">Redundancy &gt; Layer 3 Redundancy &gt; VRRP</a> for more information about VRRP.</p>
<b>ECN Ports</b>	<p><b>port3, port4, port7, and port8</b></p> <p>The field is to define which ports on the TN-4900 are the ECN ports. These selected ports will be assigned to the ECN interface.</p>

8. Click **Apply**.

**Results:** You have configured TTDP for the ETBN router on Consist 2.

**What to do next:** To finish configuring of ETBN router, you must configure the Communication Profile by uploading a local consist info file. Refer to [Example: Configuring Local Consist Info for ETBNs/ECSPs](#) for detailed instructions.

This example uses 2 ETBN routers, 1 on each consist. All ETBN routers in all consists must be correctly configured before the example setup is complete.

## Example: Configuring Local Consist Info for ETBNs/ECSPs

ECSPs rely on static XML files that define devices within a consist.

The ETB Control Service Provider (ECSP) runs on each ETBN, and controls the ETB. They ensure efficient communication and event handling. ETBs require static consist information, uploaded in the form of an XML file on Moxa ETBN routers. These files are compiled by the user.

**Before you begin:** Make sure you have compiled an XML file with device information for each consist. Refer to [Structure and Syntax of Local Consist Info Files](#) for more information about XML configuration files.

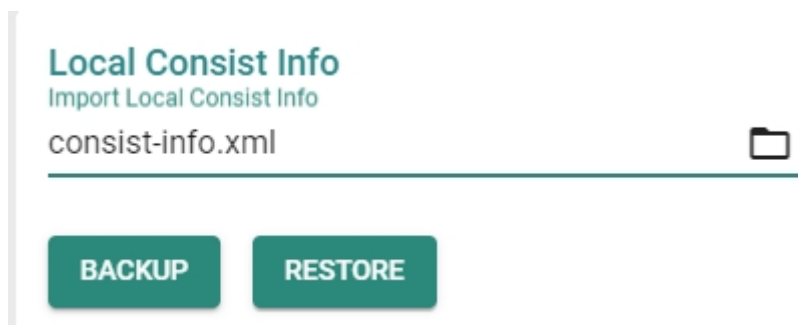
Refer to [Sample Local Consist Info File](#) for a sample file for a single consist.

To upload a configuration file to the ETBN router:

1. Go to **Industrial Application > IEC 61375 > Communication profile > TTDP Settings**.
2. Under **Local Consist Info**, click **Import Local Consist Info**.

**Result:** Your browser's file selection window will appear.

3. Navigate to the configuration file in your file system, and select it.
  - The exact button chosen will vary by operating system and browser. As of April 2024, in Microsoft Edge on Windows, the relevant button is **Open**.



**Result:** The chosen filename appears under **Import Local Consist Info**.

4. Click **Restore** to import the consist info.

**Result: Successfully Updated** appears briefly on the screen.

**What to do next:** You can verify that the correct consist information has been uploaded by going to **Operation Status > Consist Info > Function list** and verifying that the table correctly displays device and consist information.

## Chapter 7

---

# Security Hardening Guide

# Security Hardening Guide

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

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

## Security Best Practices

### Product Security

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

### 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 implement appropriate physical security measures. This may include CCTV surveillance, security guards, locks, and access control systems, among other measures. The specific measures you choose should be based on your environment and the level of risk you face.
- Install a Layer 2 switch within the security perimeter. This perimeter can be established by setting up a firewall at the border, as the switch is not designed to be directly connected to the Internet. Note that the switch should not be classified as zone or boundary equipment. Avoid connecting the device directly to the Internet, as this can leave your network vulnerable to security breaches.
- Follow the Quick Installation Guide included in the package of your device. It contains step-by-step instructions that are easy to follow and will help you set up the device quickly and efficiently.
- Examine and monitor anti-tamper labels applied to the device enclosures. These labels provide a quick and easy way for administrators to determine if the device has been tampered with.



- Deactivate any ports that are not currently in use. Fewer active ports represent fewer avenues of attack. Refer to Network Interfaces for more information.

## Account Management Guidelines

Manage user accounts, set passwords, and restrict access to authorized personnel only.

- Assign the appropriate account privileges.

Limit the number of users with admin privileges to only those who need to perform device configuration or modifications. For other users, read-only access is sufficient. Moxa devices supports both local account authentication and remote centralized mechanisms, including RADIUS and TACACS+. This allows for flexible and secure access control options.

- Implement good password practices. Good password practices include:
  - a. Enabling and configuring a Password Policy to ensure your password meets specified requirements.
  - b. Setting the minimum password length to at least eight characters.
  - c. Require passwords to have at least one uppercase and lowercase letter, a digit, and a special character.
  - d. Setting password expiration.
  - e. Updating passwords regularly.
  - f. Never sharing passwords.

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.

- Generate new SSL certificates and SSH keys for devices prior to using HTTPS or SSH applications. Refer to SSH & SSL for more information.

## **Maintaining Communication Integrity**

Ensure that information sent is accurate, complete, and secure.

Maintaining communication integrity reduces risks risk of data corruption or interception, and associated security breaches, data loss, and other negative effects on networks and their users.

- Use encryption.

Encryption uses mathematical algorithms to convert data into a secret code, making it extremely difficult for people without the correct codes to read or change the data. By using encryption, you can ensure that the data being transmitted is secure and cannot be intercepted by unauthorized users.

- Use digital signatures.

Digital signatures verify the authenticity and integrity of digital documents or messages. Using a digital signature, you can ensure that the message or document came from the expected sender and has not been altered.

- Implement access control.

Access control restricts access to only authorized users to the network and its resources. By implementing access control measures, such as firewalls or access control lists, you can prevent unauthorized access and reduce the risk of data breaches.

## **Communication Integrity Features**

Moxa devices provide support for VPNs and secure versions of protocols to help maintain communication integrity.

### **VPN (Virtual Private Network)**

VPN is a secure network connection allowing users to access a private network. VPNs use encryption and authentication to protect the data in transit, which makes it difficult for anyone to intercept or tamper with the data. VPNs also provide access control features to ensure only authorized users can access the network. VPNs are commonly used to securely connect remote workers to a company network securely or to allow secure access to restricted resources over the internet.

Refer to VPN for more information.

## **HTTPS (Hypertext Transfer Protocol Secure)**

HTTPS is a secure version of the regular HTTP protocol for transmitting data over the internet. HTTPS uses TLS (Transport Layer Security) encryption and digital certificates to protect the data in transit from interception, tampering, or eavesdropping.

Refer to Management Interface for more information.

## **SSH (Secure Shell)**

SSH is a secure protocol for remote terminal login and secure file transfers. SSH uses encryption to protect the data in transit, making it difficult for anyone to intercept or tamper with it. SSH also provides authentication and access control features to ensure only authorized users can access the network.

Refer to Management Interface for more information.

## **SFTP (Secure File Transfer Protocol)**

SFTP is a secure version of FTP (File Transfer Protocol) that uses encryption to protect the data in transit. SFTP also provides authentication and access control features to ensure only authorized users can access the network.

Refer to Management Interface for more information.

## **SNMP v3 (Simple Network Management Protocol version 3)**

SNMP v3 is a secure version of the SNMP protocol used for network management and monitoring. SNMP v3 uses encryption and authentication to protect the data in transit, making it difficult for anyone to intercept or tamper with it. SNMP v3 also provides access control features to ensure only authorized users can access the network.

Refer to SNMP for more information.

## **Device 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:

- 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 trusted access lists. Trusted access lists are authorized devices or users allowed to access a particular network resource. Trusted access lists can be managed at the device, network, or application levels. Network administrators can use trusted access lists to ensure that only authorized devices or users can access sensitive resources. 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. Refer to Firewall for further information.

## **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 creating 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.

## **Denial of Service (DoS) Protection**

In a denial-of-service (DoS) attack, the attacker attempts to overwhelm a target system with a flood of traffic or requests. The deluge of traffic causes the target system to become paralyzed, and also causes disruptions in networks and online services.

Moxa devices can prevent several types of DoS attacks by rejecting requests which ask for a particular network scan, or rejecting too many such requests in a specified period.

Refer to DoS Policy setting for more information.

## **Session Control**

Session control refers to managing communication sessions between network objects, such as IP addresses or ports. The management process involves establishing, maintaining, and terminating sessions to ensure secure and reliable communication between various objects. Session control allows administrators to allocate device resources more efficiently by limiting the number of active sessions, and improving network security by dropping unused sessions.

Refer to Session Control for more information.

## **Recommended Settings for Services and Features**

When prioritizing device security, the first point of assessment is often the network interfaces and services.

By deactivating unneeded interfaces and services, one can reduce potential vulnerabilities and associated security threats. Additionally, activating the appropriate security features enhances early anomaly detection and bolsters the device's defense against cyber attacks.

## **Common Protocols and Ports**

Service Name	Default Port	Default Setting	Security Suggestions
<b>HTTP</b>	TCP 80	Enabled	Disable if possible to avoid leaks from unencrypted traffic.
<b>HTTPS</b>	TCP 443	Enabled	
<b>Telnet</b>	TCP 23	Enabled	Disable if possible to avoid leaks from unencrypted traffic.
<b>SSH</b>	TCP 22	Enabled	
<b>NTP/SNTP</b>	UDP 123	Disabled	Use SNTP to synchronize system time if possible. Enable NTP authentication if possible.
<b>SNMP</b>	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.
<b>Syslog</b>	UDP 514	Disabled	By default, logs are stored in the device, but limited local storage limits the number of saved logs, resulting in missed logs for critical incidence. Sending logs to an external log server can mitigate limitation, decreasing the chance of missing critical logs.
<b>RADIUS</b>	UDP 1812	Disabled	Enabling RADIUS authentication can help administrators manage password changes more efficiently.
<b>Moxa Services</b>	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
<b>Firewall</b>	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.
<b>Password Policy</b>	Disable	Enable password policy to comply enterprise security policies.



Function	Default Setting	Security Suggestions
<b>Login policy</b>	Disable	Enable a login policy to heighten resistance against brute force attacks and terminating any inactive login sessions.
<b>Malformed Packets Filtering</b>	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.
<b>DoS Policy</b>	None	Select a DoS policy according to your network traffic to increase network robustness.
<b>Session control</b>	None	Configure session control policies appropriate for your traffic to improve network reliability.
<b>802.1X over ports</b>	Disable	Enable 802.1X port authentication to block unauthorized LAN access.
<b>Trusted Access</b>	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
<b>Tampering &amp; Information Disclosure</b>	An attacker can read or modify data transmitted over HTTP data flow.	Disable HTTP, and replace HTTP transmission with HTTPS.
<b>Tampering &amp; Information Disclosure</b>	An attacker can read or modify data transmitted over Telnet data flow.	Disable Telnet, and replace HTTP transmission by SSH.
<b>Information Disclosure</b>	Data flowing across TFTP may be sniffed by an attacker.	Use SFTP instead of FTP.
<b>Denial of Service</b>	SNMP Server crashes, halts, stops or runs slowly by excessive quires.	Enable rate limit to stop excessive SNMP requests.
<b>Denial of Service</b>	RADIUS Server crashes, halts, stops or runs slowly by excessive quires.	Enable rate limit to stop excessive RADIUS requests.

Incident Category	Detailed Description	Mitigation Suggestions
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.

## 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.

## **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.

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**

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

## **Using Security Features**

### **Introduction to IPS**

IPS (Intrusion Prevention System) is a network security technology used to detect and prevent potential threats in a network.

IPS analyzes the network traffic and identifies potential attacks, including viruses, worms, malware, and unauthorized access. Once an IPS detects a threat, it takes immediate action to block the attack and protect the security of the network and system. IPS uses signature-based and behavior analysis to identify threats and employs various techniques to protect systems, such as blocking IP addresses and protocols. It is an important component of network security architecture designed to enhance the security of networks and systems, prevent unauthorized access, and protect against data breaches.

## **What is the difference between IDS and IPS?**

IDS (Intrusion Detection System) and IPS are network security systems that help protect against security threats and vulnerabilities.

An IDS monitors network traffic and identifies potential security threats and attacks. When it detects a security threat, it saves logs and generates an alert, which is sent to the security team for further analysis and action. An IDS is a passive security system that only monitors network traffic and does not take any action to prevent or stop an attack.

On the other hand, an IPS monitors network traffic like an IDS, but also takes active measures to prevent security threats and attacks. Additionally, an IPS can block, quarantine, or even terminate network traffic or connections deemed suspicious or malicious. IPS systems often use a set of predefined rules or policies to identify and respond to security threats in real-time.

The main difference between IDS and IPS is that IDS only detects and notifies of potential security threats, while IPS takes action to prevent and stop the security threat. IDS is generally considered a more passive security system, whereas IPS is more proactive and can take immediate action to mitigate security risks.

## **IPS Applications**

IPS is typically used to actively prevent and block unauthorized access or malicious activities on your network.

IPS is typically used when you want to actively prevent and block unauthorized access or malicious activities on your network. It's a proactive security solution that acts in real-time to prevent potential security threats from entering or leaving your network.

Here are some common applications of IPS:

1. **Protecting critical assets:** IPS can protect mission-critical assets or systems, such as PLCs, factory automation, ICS (Industrial Control System), from external and internal security threats.
2. **Resisting zero-day attacks:** IPS can help you detect and block unknown or zero-day attacks that have not yet been identified by traditional anti-virus or intrusion detection systems.
3. **Real-time threat detection:** IPS systems can provide real-time threat detection and prevention, reducing the risk of data breaches and other security incidents.
4. **Virtual patching:** Even devices with outdated OS can receive up-to-date protection without regular security updates and patches.

In summary, IPS should be used when you want to actively prevent and block security threats in real-time and protect critical assets or comply with specific regulations or standards.

## IPS Limitations

The most notable limitation of IPS is that it relies on updated patterns—updated definitions and countermeasures of known threats—to correctly detect and act on threats. To address this issue, Moxa provides regular updates in the form of a security package.

## Example: Updating the Network Security Package via the Web GUI

Download the latest Network Security Package from the Moxa and install via the Web GUI.

**Before you begin:** Make sure you have purchased an activated an IPS license.

This task uses the Moxa EDR-G9010 series as an example product. Replace this product with your product for each step.

1. From the Moxa support website, navigate to **Resources**→**Software Packages**→**Network Security Package for EDR-G9010 Series**

The Moxa support website is located at <https://www.moxa.com/en/support>.

2. Download the latest version of the Network Security Package to your computer.
3. Open the router's web interface and navigate to **System**→**System Management**→**Software Package Management**→**Network Security Package**.

4. Click **Source**, and then choose **Local**.
5. Click **Select Files**, and then choose a file from your local file system.
6. Click **Upgrade** to start the upgrade process.

The upgrade process will begin, and the result appears at the bottom of the interface.

**What to do next:**

Confirm that the Network Security Package has been updated by checking the version information from the Package Information Screen. On the web interface, go to **Firewall→Advanced Protection→Information→Package Information**, and check the version listed.

### **Example: Updating the Network Security Package via MXsecurity**

Download the latest Network Security Package from the Moxa website and install with the MXsecurity web console.

**Before you begin:** Make sure you have purchased an activated an IPS license.

This task uses the Moxa EDR-G9010 series as an example product. Replace this product with your product for each step.

1. From the Moxa support website, navigate to **Resources→Software Packages→Network Security Package for EDR-G9010 Series**

The Moxa support website is located at <https://www.moxa.com/en/support>.

2. Download the latest version of the Network Security Package to your computer.
3. From the MXsecurity web console, go to **Device Deployment→Software Packages→Network Security Packages**.
4. Select the secure routers to update, and then click **Upgrade**.

**Results:** The upgrade process will begin on the selected routers, with the result displayed within seconds.

**What to do next:**

Confirm that the Network Security Package has been updated by checking the version information from the Package Information Screen. On the MXsecurity web console, go to **Device Deployment→Software Packages**, and check the version listed.

## Example: Configuring IPS Rules via MXsecurity

Enable IPS rules and observe the generated event from the MXsecurity, the centralized cybersecurity visualization platform.

**Before you begin:** Make sure you have:

- a configured MXsecurity server
  - an active IPS license that supports MXsecurity
  - at least one Network Security Package uploaded. See Example: Updating the Network Security Package via MXsecurity for upload steps.
1. From the MXsecurity web console, go to **Management**→**Policy Profile**.
  2. Click *[Add]*, and then configure:
    - **Profile Name**
    - **Description** (optional)
  3. Select **IPS**, and then choose one of the **Package Versions** from the list.
  4. Enable one or more IPS rules, then click **Apply**.

You can choose **Select All** to enable all protection.

**Result:** Your new policy profile is visible in the **Policy Profile** table.

5. To apply the profile, go to **Deployment**→**Policy Profile**.
6. Select the IPS profile, and then click **Apply**.

### Results:

If an IPS event is triggered, you can go to **Logging**→**Firewall**→**IPS** to examine the events.

## Example: Configuring IPS rules via WebGUI

Enable and configure IPS rules from device web interfaces.

**Before you begin:** Make sure you have:

- an active IPS license that supports device-based IPS
1. In the device UI, go to **Firewall**→**Advanced Protection**→**IPS**.
  2. Identify rules to configure:

Choose from:



- Choose rules from the list
  - Filter rules by clicking [*Filter*]
  - Type search terms in the search box
3. Edit or enable rules by clicking [*Edit*], then setting **Status** to **Enabled**.

You can toggle multiple rules by selecting them, and then clicking →**Quick Settings**, **and then setting Status to Enabled**.

**Results:** Selected rules will now be enabled.

**What to do next:** You can check the event log to verify to see actions taken by rules by going to **Diagnostics**→**Event Logs and Notifications**→**Event Log**→**Firewall Log**.

## Introduction to Firewalls

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Its primary function is to create a barrier between a private internal network and the public internet, allowing only authorized traffic to pass through and blocking unauthorized access attempts. They use various techniques to filter network traffic, including packet filtering, stateful inspection, and application filtering. Firewalls are an essential component of network security and are used by individuals, small businesses, and large enterprises to protect their networks from various types of cyber threats, such as viruses, malware, hackers, and other malicious attacks.

## Stateful vs. Stateless firewalls

Firewalls can be categorized as either stateful or stateless.

Stateless firewalls, also known as packet filtering firewalls, examine individual packets of data and enforce rules based on information in the packet header, such as source and destination IP addresses or port numbers. Stateless firewalls do not keep track of the state of connections and cannot distinguish between packets belonging to different connections.

Stateful firewalls, on the other hand, keep track of the state of connections and use this information to enforce rules. They can distinguish between packets belonging to different connections and apply more complex security policies. Stateful firewalls maintain a state table that tracks information such as source and destination IP addresses, port numbers, and connection status.

Overall, stateful firewalls offer more advanced security features and are generally more effective at protecting networks from threats. However, they also require more resources and may be more complex to configure and manage. Stateless firewalls are simpler and more lightweight, but may not provide as much protection against advanced threats.

## Categories of Firewall

- Policy (L2,L3~L7) : A policy in firewall function is a set of rules and criteria that are used to determine how traffic is allowed or denied on a network. Firewall policies define the actions that the firewall should take when specific traffic matches the defined criteria.
- Malformed packet: The Malformed Packets function enables the device to record event logs with a user-specified severity whenever malformed packets are dropped by the system.
- Session control: Session control in a firewall is the process of tracking and controlling the flow of network traffic between two endpoints in a network session. Session control to help users protect backend hosts or services and avoid system abnormalities.
- DoS(Denial of Service) policy: The Industrial Secure Router provides 9 different DoS functions for detecting or defining abnormal packet formats or traffic flows. The Industrial Secure Router will drop packets when it either detects an abnormal packet format or identifies unusual traffic conditions.
- Protocol filter policy: The Industrial Secure Router supports industrial protocol filtering, allowing users to inspect network traffic based on specific protocols to detect anomalies and protect your network.

## When to Use Firewalls

Firewalls are a fundamental component of network security and are used to protect networks from unauthorized access and cyber threats. It is a static system that filters traffic based on predefined rules, such as source/destination MAC, IP address or port.

1. Prevent unauthorized access to critical assets: Firewalls are used to prevent unauthorized access to critical assets, such as a controller of a system, central monitor system.
2. Safeguarding sensitive data: Firewalls are used to safeguard sensitive data such as financial information, healthcare records, and production data.

3. Complying with regulations: Many industries are subject to regulations that require the use of firewalls to protect sensitive data.

In summary, firewalls are used to control traffic based on predefined rules and focus on access control. Firewalls are often used in combination with other network security techniques, 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

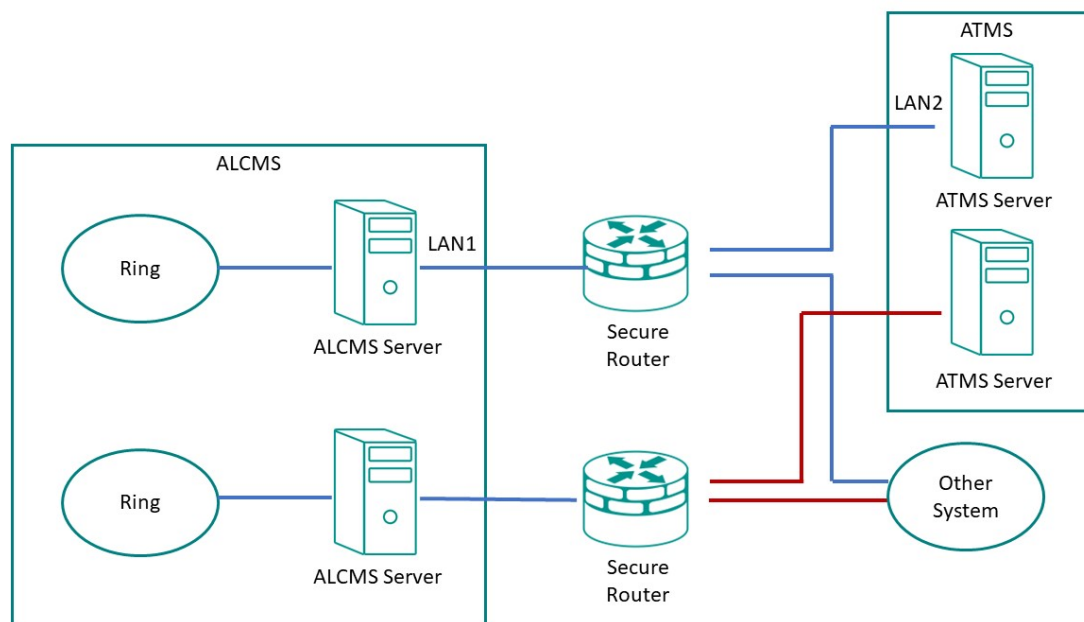
An allowlist is a network configuration that blocks all traffic except those specifically allowed.

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
<b>Action</b>	<b>Allow</b>
<b>Filter Mode</b>	<b>IP and Port Filtering</b>
<b>Source IP Address</b>	<b>LAN2</b> Refers to the ATMS server
<b>Destination IP Address</b>	<b>LAN1</b> 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.

## Scenario: Railway Integrated Solutions

**Short Description:** A network system provider is configuring a network for a railway operator.

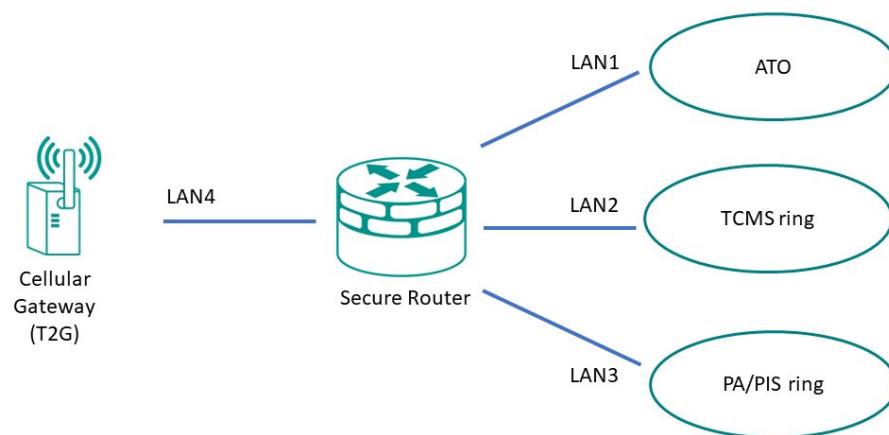
## Understanding Railway Network Topology

A typical railway train network comprises multiple sub-systems working in tandem to ensure smooth operations. These sub-systems communicate crucial information, such as train speed, departure/arrival times, door status, climate control, lighting, and station updates to passengers.

Moxa's secure routers offer firewall functionality that allows seamless integration of these systems. By implementing policy-based firewall rules, these routers can permit authorized traffic and block unauthorized exchanges between the different sub-systems.

For instance, the train operating system might consist of various components:

- T2G system (usually a cellular gateway)
- ATO (Automatic Train Operation) system
- TCMS (Train Control and Management System) ring
- PA (Public Announcement system)/PIS (Public Information System) ring
- Control units for each of these systems



As an example scenario: a network designer might want configure the network such that the TCMS is the gatekeeper for all signals to the ATO, and prevent the ATO from talking

to any other node on the network. We can achieve this kind of network isolation with an allowlist.

## Allowlist Firewall Configuration

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

To apply our example from above, the firewall's rules can be fine-tuned to:

- Allow the TCMS to access the ATO, PA/PIS, and Cellular Gateway.
- Allow the Cellular Gateway to access the TCMS and PA/PIS system.
- Reject all unrelated traffic and connections.

This configuration effectively isolates the ATO from the Cellular Gateway and PA/PIS.

To implement this configuration, set up one or more port filters to allow favorable traffic from recognized devices or ports. Then, set up a "deny all" rule to block any unspecified traffic, allowing the systems coexist securely on a shared network.

Integrating subsystems while preserving security and redundancy requires meticulous design and strategic solutions. With the right tools and approaches, operators can achieve high levels of operational efficiency and safety.

### Example: Allowing TCMS traffic

Create port filtering rules to allow the TCMS to act as a gatekeeper for other devices on the network.

This procedure must be used in tandem with a correctly configured "deny all" policy to correctly implement an allowlist.

**Before you begin:** Make sure that network interfaces have already been configured with static IP addresses.

#### 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
<b>Action</b>	<b>Allow</b>
<b>Filter Mode</b>	<b>IP and Port Filtering</b>
<b>Source IP Address</b>	LAN2 LAN2 should represent the IP address of the TCMS.
<b>Destination IP Address</b>	LAN1 LAN1 should represent the IP address of the ATO.

**Tutorial Info:** In this example, these settings identify the "allowed traffic" by IP address. This requires the IP address to be constant. When configuring in a production environment, make sure the characteristics you choose for your filter clearly distinguish trusted and untrusted network objects, such as IP address, protocol and port, or network interface.

 **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.

Tutorial Info: In this case, we will specifically create a bidirectional or "mirrored" rule for TCMS to Cellular Gateway traffic.

3. Create two more **Allow** rules.

Rule Purpose	Source IP	Destination IP
<b>Allow TCMS to PA/PIS Traffic</b>	LAN2	LAN3
<b>Allow TCMS to Cellular Gateway Traffic</b>	LAN2	LAN4

4. Click **Apply**.

**Results:** Rules have been created that will allow the TCMS to access all network nodes, allowing the TCMS to serve as a gatekeeper. Next, create a rule that will allow the Cellular Gateway to access the TCMS and PA/PIS. Refer to Example: Allowing the T2G to access TCMS and PA/PIS for more information.

## Example: Allowing the T2G to access TCMS and PA/PIS

Create port filtering rules to allow traffic from the Cellular Gateway to the TCMS and PA/PIS.

**Before you begin:** Make sure that network interfaces have already been configured with static IP addresses.

### 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
<b>Action</b>	<b>Allow</b>
<b>Filter Mode</b>	<b>IP and Port Filtering</b>
<b>Source IP Address</b>	LAN4 <b>LAN4</b> should represent the IP address of the Cellular Gateway.
<b>Destination IP Address</b>	LAN2 LAN2 should represent the IP address of the TCMS.

**Tutorial Info:** In this example, these settings identify the "allowed traffic" by IP address. This requires the IP address to be constant. When configuring in a production environment, make sure the characteristics you choose for your filter clearly distinguish trusted and untrusted network objects, such as IP address, protocol and port, or network interface.

**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. To allow the Cellular Gateway to access the PA/PIS, specify all of the following:

Item	Value
<b>Action</b>	<b>Allow</b>
<b>Filter Mode</b>	<b>IP and Port Filtering</b>
<b>Source IP Address</b>	LAN4 LAN4 should represent the IP address of the Cellular Gateway.
<b>Destination IP Address</b>	LAN3 LAN3 should represent the IP address of the PA/PIS.

4. Click **Apply**.

**Results:** Rules have been created that will allow the Cellular Gateway to access the TCMS and PA/PIS.

**What to do next:** Add a policy rule to block all other traffic. Refer to Example: Configuring Blocked Traffic (Rail) for more information.


### Example: Configuring Blocked Traffic (Rail)

Once you have specified "allowed" traffic, block all other traffic so that the ATO will be effectively isolated from all other devices, relying on the TCMS as a gatekeeper.

1. Go to **Firewall** → **Layer 3-7 Policy**, and then click  **[Add]**.

**Result:** The **Layer 3-7 Policy** creation panel appears.

2. In the **Action** field, select **Deny**.
3. In the **Filter Mode** field, select **IP and Port Filtering**.
4. Click **Apply**.
5. Make sure that the "deny all" rule is the last rule on the list, otherwise this rule may override the allow rules.

To reorder rules, click  **[Reorder Priorities]**

**Results:** The TCMS will be able to access all network devices, and the Cellular Gateway will be able to access the TCMS and PA/PIS, but all other traffic will be blocked, effectively isolating these systems from other devices on the network. This helps make sure that even if other systems on the network are compromised, no traffic from these systems will reach the specified systems, effectively isolating them from this vector of attack.

 **Tip**

Instead of configuring a "deny all" rule, you can configure a policy from Global Policy Settings to deny all traffic. To apply the policy,

1. Go to Firewall → Layer 3-7 Policy
2. Specify Status as Enabled.
3. Specify Default Action as Deny All.
4. Click Apply.

Specific rules override generalized policies, effectively making the policy the last rule on the list.

## 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**

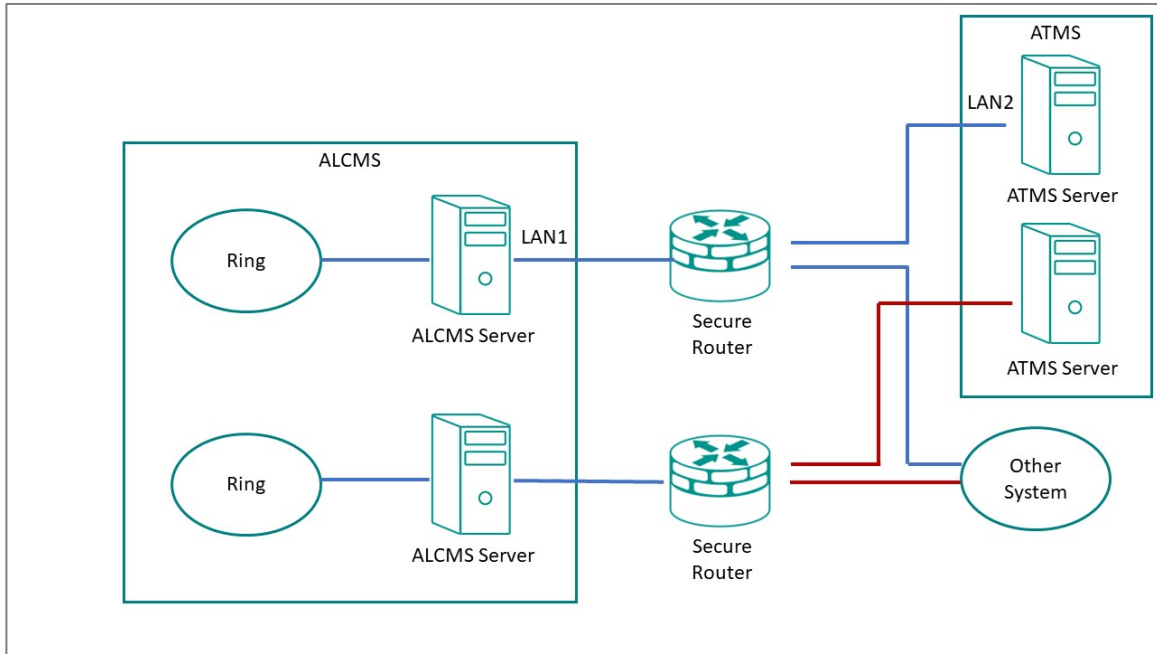
An allowlist is a network configuration that blocks all traffic except those specifically allowed.

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.

- Go to **Firewall** → **Layer 3-7 Policy**, and then click **[Add]**.

**Result:** The **Layer 3-7 Policy** creation panel appears.

- Specify all of the following:

Item	Value
Action	Allow
Filter Mode	IP and Port Filtering

Item	Value
<b>Source IP Address</b>	<b>LAN2</b> Refers to the ATMS server
<b>Destination IP Address</b>	<b>LAN1</b> 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.

- 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.

- Go to **Firewall** → **Layer 3-7 Policy**, and then click  **[Add]**.

**Result:** The **Layer 3-7 Policy** creation panel appears.

- In the **Action** field, select **Deny**.
- In the **Filter Mode** field, select **IP and Port Filtering**.
- Click **Apply**.
- 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.

## **Scenario: Railway Integrated Solutions**

**Short Description:** A network system provider is configuring a network for a railway operator.

### **Understanding Railway Network Topology**

A typical railway train network comprises multiple sub-systems working in tandem to ensure smooth operations. These sub-systems communicate crucial information, such as train speed, departure/arrival times, door status, climate control, lighting, and station updates to passengers.

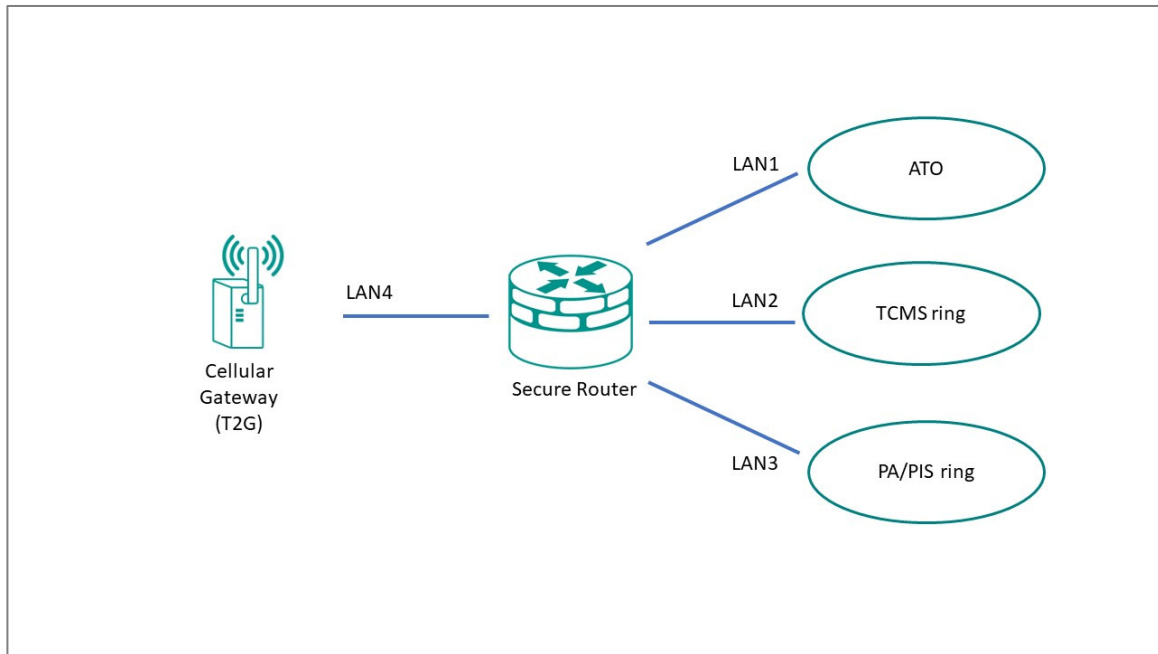
Moxa's secure routers offer firewall functionality that allows seamless integration of these systems. By implementing policy-based firewall rules, these routers can permit authorized traffic and block unauthorized exchanges between the different sub-systems.

For instance, the train operating system might consist of various components:

- T2G system (usually a cellular gateway)
- ATO (Automatic Train Operation) system
- TCMS (Train Control and Management System) ring
- PA (Public Announcement system)/PIS (Public Information System) ring



- Control units for each of these systems



As an example scenario: a network designer might want configure the network such that the TCMS is the gatekeeper for all signals to the ATO, and prevent the ATO from talking to any other node on the network. We can achieve this kind of network isolation with an allowlist.

## Allowlist Firewall Configuration

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

To apply our example from above, the firewall's rules can be fine-tuned to:

- Allow the TCMS to access the ATO, PA/PIS, and Cellular Gateway.
- Allow the Cellular Gateway to access the TCMS and PA/PIS system.
- Reject all unrelated traffic and connections.

This configuration effectively isolates the ATO from the Cellular Gateway and PA/PIS.

To implement this configuration, set up one or more port filters to allow favorable traffic from recognized devices or ports. Then, set up a "deny all" rule to block any unspecified traffic, allowing the systems coexist securely on a shared network.


Integrating subsystems while preserving security and redundancy requires meticulous design and strategic solutions. With the right tools and approaches, operators can achieve high levels of operational efficiency and safety.

### Example: Allowing TCMS traffic

Create port filtering rules to allow the TCMS to act as a gatekeeper for other devices on the network.

This procedure must be used in tandem with a correctly configured "deny all" policy to correctly implement an allowlist.

**Before you begin:** Make sure that network interfaces have already been configured with static IP addresses.

 **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.

- Go to **Firewall** → **Layer 3-7 Policy**, and then click  **[Add]**.

**Result:** The **Layer 3-7 Policy** creation panel appears.

- Specify all of the following:

Item	Value
<b>Action</b>	<b>Allow</b>
<b>Filter Mode</b>	<b>IP and Port Filtering</b>
<b>Source IP Address</b>	LAN2 LAN2 should represent the IP address of the TCMS.
<b>Destination IP Address</b>	LAN1 LAN1 should represent the IP address of the ATO.

**Tutorial Info:** In this example, these settings identify the "allowed traffic" by IP address. This requires the IP address to be constant. When configuring in a production environment, make sure the characteristics you choose for your filter clearly distinguish trusted and untrusted network objects, such as IP address, protocol and port, or network interface.

**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.

Tutorial Info: In this case, we will specifically create a bidirectional or "mirrored" rule for TCMS to Cellular Gateway traffic.

- Create two more **Allow** rules.

Rule Purpose	Source IP	Destination IP
<b>Allow TCMS to PA/PIS Traffic</b>	LAN2	LAN3
<b>Allow TCMS to Cellular Gateway Traffic</b>	LAN2	LAN4

- Click **Apply**.

**Results:** Rules have been created that will allow the TCMS to access all network nodes, allowing the TCMS to serve as a gatekeeper. Next, create a rule that will allow the Cellular Gateway to access the TCMS and PA/PIS. Refer to [Example: Allowing the T2G to access TCMS and PA/PIS](#) for more information.

### Example: Allowing the T2G to access TCMS and PA/PIS

Create port filtering rules to allow traffic from the Cellular Gateway to the TCMS and PA/PIS.

**Before you begin:** Make sure that network interfaces have already been configured with static IP addresses.

**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.

- Go to **Firewall** → **Layer 3-7 Policy**, and then click  **[Add]**.

**Result:** The **Layer 3-7 Policy** creation panel appears.

- Specify all of the following:

Item	Value
<b>Action</b>	<b>Allow</b>
<b>Filter Mode</b>	<b>IP and Port Filtering</b>
<b>Source IP Address</b>	LAN4 <b>LAN4</b> should represent the IP address of the Cellular Gateway.
<b>Destination IP Address</b>	LAN2 LAN2 should represent the IP address of the TCMS.

**Tutorial Info:** In this example, these settings identify the "allowed traffic" by IP address. This requires the IP address to be constant. When configuring in a production environment, make sure the characteristics you choose for your filter clearly distinguish trusted and untrusted network objects, such as IP address, protocol and port, or network interface.

**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.

- To allow the Cellular Gateway to access the PA/PIS, specify all of the following:

Item	Value
<b>Action</b>	<b>Allow</b>
<b>Filter Mode</b>	<b>IP and Port Filtering</b>
<b>Source IP Address</b>	LAN4 LAN4 should represent the IP address of the Cellular Gateway.
<b>Destination IP Address</b>	LAN3 LAN3 should represent the IP address of the PA/PIS.

- Click **Apply**.

**Results:** Rules have been created that will allow the Cellular Gateway to access the TCMS and PA/PIS.

**What to do next:** Add a policy rule to block all other traffic. Refer to [Example: Configuring Blocked Traffic \(Rail\)](#) for more information.


### Example: Configuring Blocked Traffic (Rail)

Once you have specified "allowed" traffic, block all other traffic so that the ATO will be effectively isolated from all other devices, relying on the TCMS as a gatekeeper.

- Go to **Firewall** → **Layer 3-7 Policy**, and then click  **[Add]**.

**Result:** The **Layer 3-7 Policy** creation panel appears.

- In the **Action** field, select **Deny**.
- In the **Filter Mode** field, select **IP and Port Filtering**.
- Click **Apply**.
- Make sure that the "deny all" rule is the last rule on the list, otherwise this rule may override the allow rules.

To reorder rules, click  **[Reorder Priorities]**

**Results:** The TCMS will be able to access all network devices, and the Cellular Gateway will be able to access the TCMS and PA/PIS, but all other traffic will be blocked, effectively isolating these systems from other devices on the network. This helps make sure that even if other systems on the network are compromised, no traffic from these systems will reach the specified systems, effectively isolating them from this vector of attack.

#### Tip

Instead of configuring a "deny all" rule, you can configure a policy from Global Policy Settings to deny all traffic. To apply the policy,

- Go to Firewall → Layer 3-7 Policy
- Specify Status as Enabled.
- Specify Default Action as Deny All.
- Click Apply.

Specific rules override generalized policies, effectively making the policy the last rule on the list.

# Security Standards and Concepts

## Introduction to Defense in Depth

The Defense-in-Depth strategy is used to protect systems from various types of attacks by using multiple independent defense mechanisms.

This involves incorporating multiple layers of security to protect the product against potential attacks and vulnerabilities at various stages of its design, development, and use.

It is crucial to understand that no single protection can guarantee complete security. That's why the Defense-in-Depth approach makes it difficult for attackers to leverage one weakness to attack the product or network as a whole. This approach requires attackers to overcome multiple obstacles undetected, increasing the difficulty level. By leveraging multiple security features and layers of protection in a product, vulnerabilities in any one layer can be mitigated.

## AAA

### About AAA - Authentication, Authorization, and Accounting

Authentication, Authorization, and Accounting (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
<b>Configuration location</b>	Local device	Remote RADIUS server, local as fallback
<b>Number of accounts</b>	Few	Many
<b>Password security requirements</b>	Limited	Many
<b>Allowed services*</b>	Specified locally	Determined by server
<b>Authority types</b>	Admin, User, Supervisor	Admin, User
<b>User feedback on failed login</b>	Custom prompt	Server-defined
<b>Setup effort</b>	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.

The screenshot shows a 'Create New Account' form with the following fields and values:

- Status \*: Enabled
- Username \*: Nick
- Authority \*: User
- New Password \*: [masked]
- Confirm Password \*: [masked]

Character counts are shown below the Username and Password fields: 'At least 4 characters' and '4 / 31' for Username; 'At least 4 characters' and '8 / 16' for both Password fields. 'CANCEL' and 'CREATE' buttons are located at the bottom right of the form.

**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.

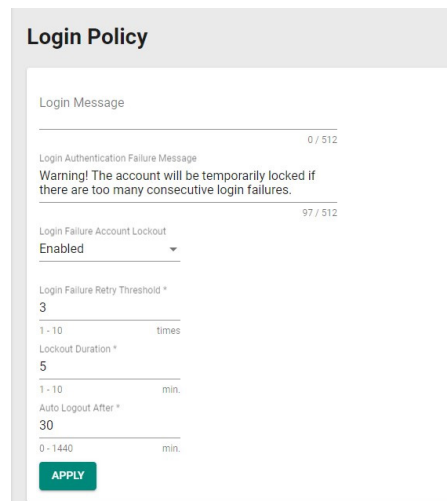
Temporary bans can help prevent password guessing and brute force attacks by preventing attackers from rapidly guessing many passwords.

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.



The screenshot shows a configuration window titled "Login Policy". It contains several fields and a button:

- Login Message:** A text input field with a character count of 0 / 512.
- Login Authentication Failure Message:** A text input field containing the message: "Warning! The account will be temporarily locked if there are too many consecutive login failures." with a character count of 97 / 512.
- Login Failure Account Lockout:** A dropdown menu set to "Enabled".
- Login Failure Retry Threshold \*:** A text input field with the value "3". Below it, the range "1 - 10" and the unit "times" are displayed.
- Lockout Duration \*:** A text input field with the value "5". Below it, the range "1 - 10" and the unit "min." are displayed.
- Auto Logout After \*:** A text input field with the value "30". Below it, the range "0 - 1440" and the unit "min." are displayed.
- APPLY:** A green button at the bottom left.

**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
<b>Authentication Type</b>	<b>PAP</b>
<b>Server Address 1</b>	192.168.127.1
<b>UDP Port</b>	1812
<b>Shared Key</b>	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.

**RADIUS Server**

Authentication Type \*  
PAP

Server Address 1 UDP Port  
1812  
0 / 63 1 - 65535

Shared Key 0 / 60

Server Address 2 UDP Port  
1812  
0 / 63 1 - 65535

Shared Key 0 / 60

**APPLY**

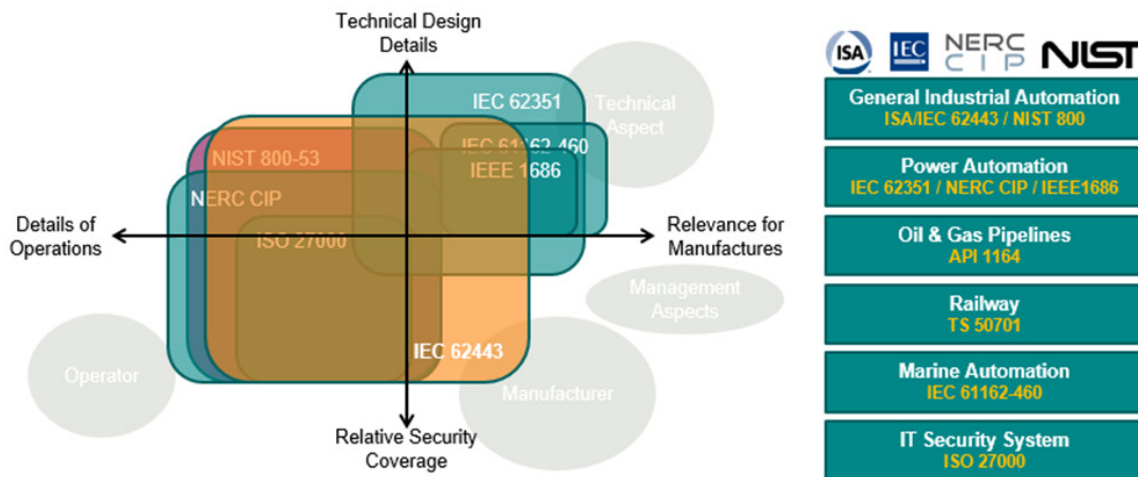
## ISA/IEC 62443 Standards and Architecture

### 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
<b>ISA/IEC 62443-1</b>	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
<b>ISA/IEC 62443-2</b>	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
<b>ISA/IEC 62443-3</b>	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
<b>ISA/IEC 62443-4</b>	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:

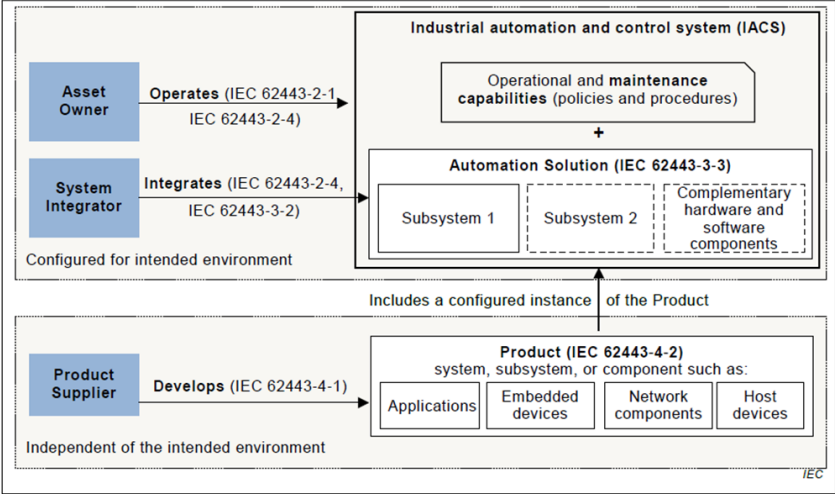
- Determine security zones
- Specify security capability levels for each zone
- Integrate products into an Automation Solution

### Key Parts of ISA/IEC 62443 Standard

Parts of the ISA/IEC 62443 Standard	Technical Security Requirements
<b>General</b> <b>ISA/IEC 62443-1</b>	ISA-/IEC 62443-1-1 Foundational Requirements (FR)
<b>System</b> <b>ISA/IEC 62443-3</b>	ISA-/IEC 62443-3-3 System Requirements (SR)
<b>Component</b> <b>ISA/IEC 62443-4</b>	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 4	Data Confidentiality
FR 5	Restricted Data Flow
FR 6	Timely Response to Events

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

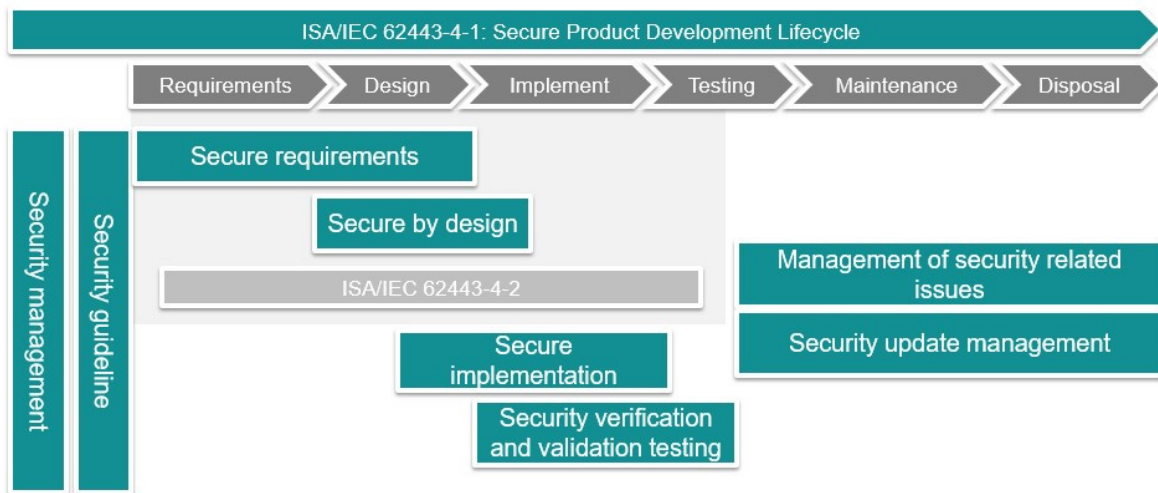
Security Level	Example Threat Actor	Violation Type	Means	Resource Level	Motivation
SL-1	<ul style="list-style-type: none"> <li>Ordinary user</li> </ul>	Coincidental	N/A	N/A	N/A
SL-2	<ul style="list-style-type: none"> <li>Entry-level hacker</li> </ul>	Intentional	Simple	Low	Low
SL-3	<ul style="list-style-type: none"> <li>Terrorist Organization</li> <li>Organized crime</li> </ul>	Intentional	Sophisticated	Moderate	Moderate
SL-4	<ul style="list-style-type: none"> <li>Nation state</li> </ul>	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.

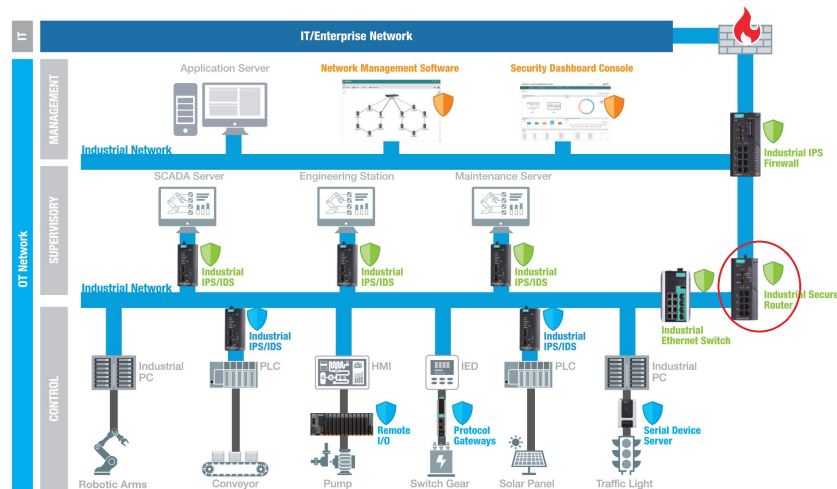
## Component Security with IEC 62443-4-2

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.

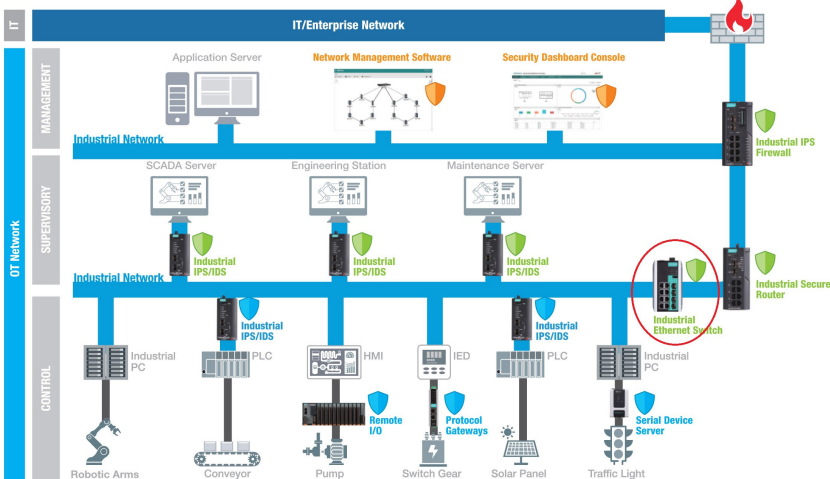
## Security Context of an Industrial Secure Router



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 8

---

# Appendix

# Appendix

This section includes additional reference information for your device.

The following information is included:

- Destination Ports for Layer 3-7 Protocol
- EtherTypes for Layer 2
- Fiber Check Threshold Values
- IEC 61375-2-3 Communication Identifiers
- IEC-104 Cause of Transmission List
- IEC-104 Type Identification List
- LED Behavior
- MIB Groups
- MMS Command Type List
- MMS Service Operation List
- Severity Level List
- Status Codes
- Structure and Syntax of Consist Info Configuration Files
- Supported Features List
- System Event List
- System Log Events
- TRDP Message Type List
- TRDP Protocol Filter Profile List
- User Role Privileges

## Destination Ports for Layer 3 – 7 Protocol

**Network Service**

**Remote-Access**

**Remote-Desktop**

## Network Service

**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**

**moxa-MXview-Request**

## EtherTypes for Layer 2

The following table shows the Layer 2 protocol types commonly used in Ethernet frames.

EtherType Value (Hexadecimal)	Layer 2 Protocol
<b>0x0800</b>	IPv4 (Internet Protocol version 4)
<b>0x0805</b>	X25
<b>0x0806</b>	ARP (Address Resolution Protocol)
<b>0x0808</b>	Frame Relay ARP
<b>0x08FF</b>	G8BPQ AX.25 Ethernet Packet
<b>0x6000</b>	DEC Assigned proto
<b>0x6001</b>	DEC DNA Dump/Load
<b>0x6002</b>	DEC DNA Remote Console
<b>0x6003</b>	DEC DNA Routing
<b>0x6004</b>	DEC LAT
<b>0x6005</b>	DEC Diagnostics
<b>0x6006</b>	DEC Customer use
<b>0x6007</b>	DEC Systems Comms Arch
<b>0x6558</b>	Trans Ether Bridging
<b>0x6559</b>	Raw Frame Relay
<b>0x80F3</b>	Appletalk AARP
<b>0x809B</b>	Appletalk
<b>0x8100</b>	8021Q VLAN tagged frame
<b>0x8137</b>	Novell IPX
<b>0x8191</b>	NetBEUI
<b>0x86DD</b>	IP version 6 (Internet Protocol version 6)
<b>0x880B</b>	PPP
<b>0x884C</b>	MultiProtocol over ATM



EtherType Value (Hexadecimal)	Layer 2 Protocol
<b>0x8863</b>	PPPoE discovery messages
<b>0x8864</b>	PPPoE session messages
<b>0x8884</b>	Frame-based ATM Transport over Ethernet
<b>0x9000</b>	Loopback

## Fiber Check Threshold Values

Model Name	Temperature Threshold (°C)	Max./Min. TX Power (dBm)	Min. RX Power (dBm)
<b>FEMST</b>	120	-11.0/-23.0	-31.0
<b>FEMSC</b>	120	-11.0/-23.0	-31.0
<b>FESSC</b>	120	3.0/-8.0	-34.0
<b>SFP-1FEMLC-T</b>	120	-5.0/-21.0	-37.0
<b>SFP-1FESLC-T</b>	120	3.0/-8.0	-37.0
<b>SFP-1FELLC-T</b>	120	3.0/-8.0	-37.0
<b>SFP-1GSXLC-T</b>	110	-1.0/-12.5	-18.0
<b>SFP-1GLSXLC-T</b>	120	2.0/-12.0	-19.0
<b>SFP-1GLXLC-T</b>	120	0.0/-12.5	-20.0
<b>SFP-1GLHLC-T</b>	120	1.0/-11.0	-23.0
<b>SFP-1GLHXLC-T</b>	120	4.0/-7.0	-24.0
<b>SFP-1GZXLC-T</b>	120	8.0/-3.0	-24.0
<b>SFP-1G10ALC-T</b>	120	0.0/-12.0	-21.0
<b>SFP-1G10BLC-T</b>	120	-5.0/-21.0	-34.0

Model Name	Temperature Threshold (°C)	Max./Min. TX Power (dBm)	Min. RX Power (dBm)
<b>SFP-1G20ALC-T</b>	120	1.0/-11.0	-23.0
<b>SFP-1G20BLC-T</b>	120	-5.0/-21.0	-34.0
<b>SFP-1G40ALC-T</b>	120	5.0/-6.0	-23.0
<b>SFP-1G40BLC-T</b>	120	-5.0/-21.0	-34.0
<b>SFP-1GSXLC</b>	100	-1.0/-12.5	-18.0
<b>SFP-1GLSXLC</b>	100	2.0/-12.0	-19.0
<b>SFP-1GLXLC</b>	100	0.0/-12.5	-20.0
<b>SFP-1GLHLC</b>	100	1.0/-11.0	-23.0
<b>SFP-1GLHXLC</b>	100	4.0/-7.0	-24.0
<b>SFP-1GZXLC</b>	100	8.0/-3.0	-24.0
<b>SFP-1GEZXLC</b>	100	8.0/-3.0	-30.0
<b>SFP-1GEZXLC-120</b>	100	6.0/-5.0	-33.0
<b>SFP-1G10ALC</b>	100	0.0/-12.0	-21.0
<b>SFP-1G10BLC</b>	100	-5.0/-21.0	-34.0
<b>SFP-1G20ALC</b>	100	1.0/-11.0	-23.0
<b>SFP-1G20BLC</b>	100	-5.0/-21.0	-34.0
<b>SFP-1G40ALC</b>	100	5.0/-6.0	-23.0
<b>SFP-1G40BLC</b>	100	-5.0/-21.0	-34.0

## IEC 61375-2-3 Communication Identifiers

This is a list of IEC 61375-2-3 communication identifier ComIDs and their descriptions.

ComID	Description
<b>0</b>	unspecified PDU
<b>1</b>	ETBCTRL telegram
<b>2</b>	CSTINFO notification message
<b>3</b>	CSTINFOCTRL notification message
<b>10</b>	TRDP Echo
<b>31</b>	TRDP - statistics request command
<b>35</b>	TRDP - global statistics data
<b>36</b>	TRDP - subscription statistics data
<b>37</b>	TRDP - publishing statistics data
<b>38</b>	TRDP - redundancy statistics data
<b>39</b>	TRDP - join statistics data
<b>40</b>	TRDP- UDP listener statistics data
<b>41</b>	TRDP - TCP listener statistics data
<b>80</b>	Conformance test- control telegram
<b>81</b>	Conformance test - status telegram
<b>82</b>	Conformance test - confirmation request telegram
<b>83</b>	Conformance test - confirmation reply telegram
<b>84</b>	Conformance test - opTrnDir request telegram
<b>85</b>	Conformance test - opTrnDir reply telegram
<b>86</b>	Conformance test - echo request telegram
<b>87</b>	Conformance test - echo reply telegram
<b>88</b>	Conformance test - echo notification telegram
<b>100</b>	TTDB - operational train directory status telegram

ComID	Description
101	TTDB - operational train directory notification
102	TTDB - train directory information request
103	TTDB - train directory information reply
104	TTDB - consist information request
105	TTDB - consist information reply
106	TTDB - train network directory information request
107	TTDB - train network directory information reply
108	TTDB - operational train directory information request
109	TTDB - operational train directory information reply
110	TTDB - train information complete request
120	ECSP - control telegram
121	ECSP - status telegram
122	ECSP - Confirmation/Correction request
123	ECSP - Confirmation/Correction reply
130	ETBN - control request
131	ETBN - status reply
132	ETBN - train network directory request
133	ETBN - train network directory reply
140	TCN-DNS - resolving request telegram (query)
141	TCN-DNS - resolving reply telegram

## IEC-104 Cause of Transmission List

This is a list of IEC-104 cause of transmission codes and their descriptions.

Cause	Description
<b>0</b>	not used
<b>1</b>	periodic, cyclic
<b>2</b>	background interrogation
<b>3</b>	spontaneous
<b>4</b>	initialized
<b>5</b>	interrogation or interrogated
<b>6</b>	activation
<b>7</b>	confirmation activation
<b>8</b>	deactivation
<b>9</b>	confirmation deactivation
<b>10</b>	termination activation
<b>11</b>	feedback, caused by distant command
<b>12</b>	feedback, caused by local command
<b>13</b>	data transmission
<b>14-19</b>	reserved for further compatible definitions
<b>20</b>	interrogated by general interrogation
<b>21</b>	interrogated by interrogation group 1
<b>22</b>	interrogated by interrogation group 2
<b>23</b>	interrogated by interrogation group 3
<b>24</b>	interrogated by interrogation group 4
<b>25</b>	interrogated by interrogation group 5
<b>26</b>	interrogated by interrogation group 6
<b>27</b>	interrogated by interrogation group 7

Cause	Description
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
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
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
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.

## EDF-G1002 Series LED Behavior

LED	Color	State	Description
<b>PWR1</b>	Amber	On	Power is being supplied to power input PWR1.
	Off	Off	Power is not being supplied to the power PWR1.
<b>PWR2</b>	Amber	On	Power is being supplied to power input PWR2.
	Off	Off	Power is not being supplied to the power PWR2.
<b>STATE</b>	Green	On	The system passed the self-diagnosis test during boot-up and is ready to run.
		Blinking (1 Hz)	The system is ready to do a factory reset after pressing the reset button for 5 seconds.
	Red	On	The system failed the self-diagnosis test during boot-up.
	Off	Off	The system is off.
<b>USB</b>	Green	On	A USB device is connected.
		Blinking (1 sec off, 1 sec on)	USB data is being transmitted.
	Red	On	The USB device is malfunctioning.
	Off	Off	No USB device connected.
<b>Bypass</b>	Amber	On	System-halted bypass or Run-time bypass mode is enabled.
		Blinking (0.5 Hz)	Run-time bypass is enabled and operating
	Off	Off	System-halted bypass or Run-time bypass mode is disabled.
<b>HA</b>	Green	On	Reserved.
	Amber	On	Reserved.
	Off	Off	Reserved.
	Green	On	The port is active, and a link is established at 1000 Mbps.

LED	Color	State	Description
<b>10/100/1000 Mbps</b>		Blinking	Data is being transmitted at 1000 Mbps.
	Amber	On	The port is active, and a link is established at 10/100 Mbps.
		Blinking	Data is being transmitted at 10/100 Mbps.
	Off	Off	The port is inactive, or the link is down.

## EDR-8010 Series LED Behavior

LED	Color	State	Description
<b>PWR1</b>	Amber	On	Power is being supplied to power input P1 on the main module.
		Off	Power is not being supplied to power input P1 on the main module.
<b>PWR2</b>	Amber	On	Power is being supplied to power input P2 on the main module.
		Off	Power is not being supplied to power input P2 on the main module.
<b>STATE</b>	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.
		Red	On
<b>MSTR/H.TC</b>	Green	On	The EDR-8010 is set as the Master of the Turbo Ring, or as the Head of the Turbo Chain.
		Blinking	The Turbo Ring or the Turbo Chain is down.
		Off	The EDR-8010 is not set as the Master of this Turbo Ring or is set as a Member of the Turbo Chain.
<b>CPLR/T.TC</b>	Green	On	The EDR-8010 Series' coupling function is enabled to form a backup path, or the device is set as the Tail of the Turbo Chain.
		Blinking	The Turbo Ring or the Turbo Chain is down.
		Off	The EDR-8010 Series' coupling function is disabled, or the device is set as a Member of the Turbo Chain.
<b>VRRP/HA</b>	Green	On	The EDR-8010 is set as the Master of the VRRP or HA.
		Off	The EDR-8010 is not set as the Master of the VRRP or HA.

LED	Color	State	Description
<b>VPN</b>	Green	On	All VPN tunnels are working normally.
	Amber	On	Only parts of the VPN tunnels are working normally.
		Off	No active VPN connections.
<b>USB</b>	Green	On	USB drive successfully connected.
		Blinking	USB data is being transmitted.
	Red	On	USB dongle malfunction.
<b>1G</b>	Green	On	1G SFP link is up.
		Off	No link or the SFP link is down.
<b>10/100 Mbps</b>	Green	On	10 or 100 Mbps copper link is up.
		Off	No link or the copper link is down.

## EDR-G9004 Series LED Behavior

LED	Color	State	Description
<b>PWR1</b>	Amber	On	Power is being supplied to power input P1 on the main module.
		Off	Power is NOT being supplied to power input P1 on the main module.
<b>PWR2</b>	Amber	On	Power is being supplied to power input P2 on the main module.
		Off	Power is NOT being supplied to power input P2 on the main module.
<b>STATE</b>	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.
	Red	On	The system failed the self-diagnosis test on boot-up.
<b>BYPASS</b>	Amber	On	The bypass redundancy function is enabled.
		Off	The bypass redundancy function is disabled.
<b>WAN/DMZ</b>	Amber	On	The WAN2/DMZ port is set to WAN mode.
	Green	On	The WAN2/DMZ port is set to DMZ mode.

LED	Color	State	Description
		Off	The WAN2/DMZ port is disabled.
<b>VRRP/HA</b>	Green	On	The EDR-G9004 is set as the Master of the VRRP or HA.
		Off	The EDR-G9004 is not set as the Master of the VRRP or HA.
<b>VPN</b>	Green	On	All VPN tunnels are working normally.
	Amber	On	Only parts of the VPN tunnels are working normally.
		Off	No active VPN connections.
<b>USB</b>	Green	On	USB drive successfully connected.
		Blinking	USB data is being transmitted.
	Red	On	USB dongle malfunction.
<b>1G/2.5G</b>	Green	On	2.5G SFP link is up.
	Amber	On	1G SFP link is up.
		Off	No link or the SFP link is down.
<b>10/100/ 1000 Mbps</b>	Green	On	1000 Mbps copper link is up.
	Amber	On	10/100 Mbps copper link is up.
		Off	No link or the copper link is down.

## EDR-G9010 Series LED Behavior

LED	Color	State	Description
<b>PWR1</b>	Amber	On	Power is being supplied to power input P1 on the main module.
		Off	Power is not being supplied to power input P1 on the main module.
<b>PWR2</b>	Amber	On	Power is being supplied to power input P2 on the main module.
		Off	Power is not being supplied to power input P2 on the main module.
<b>STATE</b>	Green	On	The system passed the self-diagnosis test on boot-up and is ready to run.

LED	Color	State	Description
		Blinking	Device reset is in progress, blinking once per second.
	Red	On	The system failed the self-diagnosis test on boot-up.
<b>MSTR/H.TC</b>	Green	On	The EDR-G9010 is set as the Master of the Turbo Ring, or as the Head of the Turbo Chain.
		Blinking	The Turbo Ring or the Turbo Chain is down.
		Off	The EDR-G9010 is not set as the Master of this Turbo Ring or is set as a Member of the Turbo Chain.
<b>CPLR/T.TC</b>	Green	On	The EDR-G9010 Series' coupling function is enabled to form a backup path, or the device is set as the Tail of the Turbo Chain.
		Blinking	The Turbo Ring or the Turbo Chain is down.
		Off	The EDR-G9010 Series' coupling function is disabled, or the device is set as a Member of the Turbo Chain.
<b>VRRP/HA</b>	Green	On	The EDR-G9010 is set as the Master of the VRRP or HA.
		Off	The EDR-G9010 is not set as the Master of the VRRP or HA.
<b>VPN</b>	Green	On	All VPN tunnels are working normally.
	Amber	On	Only parts of the VPN tunnels are working normally.
		Off	No active VPN connections.
<b>USB</b>	Green	On	USB drive successfully connected.
		Blinking	USB data is being transmitted.
	Red	On	USB dongle malfunction.
<b>1G/2.5G</b>	Green	On	2.5G SFP link is up.
	Amber	On	1G SFP link is up.
		Off	No link or the SFP link is down.
<b>10/100/1000 Mbps</b>	Green	On	1000 Mbps copper link is up.
	Amber	On	10/100 Mbps copper link is up.
		Off	No link or the copper link is down.

## 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(1)
| |
| +-- varconfigChangeTrap(1)
| +-- varpower1Trap(2)
| +-- varpower2Trap(3)
| +-- vardi1Trap(4)
| +-- vardi2Trap(5)
| +-- varredundancyTopologyChangedTrap(10)
| +-- varturboRingCouplingPortChangedTrap(11)
| +-- varturboRingMasterChangedTrap(12)
| +-- DisplayString varVRRPStateChangeTrap(13)
| +-- varFiberWarningTrap(28)
| +-- DisplayString varVPNConnectedTrap(40)
| +-- DisplayString varVPNDisconnectedTrap(41)
| +-- DisplayString varFirewallPolicyTrap(50)
| +-- DisplayString varSecurityNotificationTrap(51)
| +-- varLoggingCapacityTrap(52)
| +-- DisplayString varDot1xAuthFailTrap(53)
| +-- varFirmwareUpgradeTrap(54)
```



```

| +-- DisplayString varFirewallConfigChangeTrap(55)
| +-- DisplayString varCellularIpChange(56)
| +-- DisplayString varCellularModuleFail(57)
| +-- DisplayString varCellularSimDetectFail(58)
| +-- DisplayString varCellularPinCodeFail(59)
| +-- DisplayString varCellularSimSwitch(60)
| +-- DisplayString varCellularModuleHighTemperature(61)
| +-- DisplayString varCellularGuaranlinkCellularReconnect(62)
| +-- DisplayString varCellularGuaranlinkTriggerIspReregister(63)
| +-- DisplayString varCellularGuaranlinkTriggerCellularModuleReset(64)
| +-- DisplayString varCellularGuaranlinkTriggerSystemReboot(65)
| +-- DisplayString varCellularPmPowerSavingStart(66)
| +-- DisplayString varCellularPmPowerSavingEnd(67)
| +-- DisplayString varCellularPmSchedulingRuleExpired(68)
| +-- DisplayString varCellularSmsWrongPassword(69)
| +-- DisplayString varCellularSmsWrongCommand(70)
| +-- DisplayString varCellularSmsWrongFormat(71)
| +-- DisplayString varCellularSmsCommandDisabled(72)
| +-- DisplayString varCellularSmsTrustedNumberAuthenticationFail(73)
| +-- DisplayString varWanInterfaceChange(74)
| +-- DisplayString varWanInterfacePingFail(75)
| +-- DisplayString varSerialOpModeStateChange(76)
| +-- DisplayString varSerialDSRStateChange(77)
| +-- DisplayString varSerialDCDStateChange(78)
| +-- DisplayString varLfpOn(79)
| +-- DisplayString varLfpOff(80)
| +-- DisplayString varDeviceLockdownStateChangeTrap(81)
|
+--swMgmt(2)
| |
| | +--basicSetting(2)
| | |
| | | +--systemSetting(1)
| | | |
| | | | +-- DisplayString sysRouterName(1)
| | | |

```

```

| | +--accessibleIP(2)
| | |
| | +-- enableAccessibleIP(1)
| | +-- enableAccessibleLan(2)
| | |
| | +--accessibleIpTable(3)
| | |
| | +--accessibleIpEntry(1) [accessibleIpAddress]
| | |
| | +-- IPAddress    accessibleIpAddress(1)
| | +-- IPAddress    accessibleIpNetMask(2)
| | +-- accessibleIpState(3)
| |
| +--network(3)
| | |
| | +--networkSetting(1)
| | |
| | +--wanSetting(1)
| | | |
| | | +-- wanConnMode(1)
| | | +-- wanConnType(2)
| | | +-- IPAddress    wanStaticIpAddr(3)
| | | +-- IPAddress    wanStaticIpMask(4)
| | | +-- IPAddress    wanStaticDefaultGateway(5)
| | | +-- DisplayString wanAdslName(6)
| | | +-- DisplayString wanAdslHost(7)
| | | +-- wanPptpEnable(9)
| | | +-- IPAddress    wanPptpAddr(10)
| | | +-- DisplayString wanPptpUsrName(11)
| | | +-- IPAddress    wanDnsServer1(13)
| | | +-- IPAddress    wanDnsServer2(14)
| | | +-- IPAddress    wanDnsServer3(15)
| | | +-- IPAddress    ipAddr(16)
| | | +-- IPAddress    ipMask(17)
| | | +-- IPAddress    defaultGateway(18)
| | | +-- directedBroadcast(19)

```

```

| | | +-- sourceIPOverwrite(20)
| | |
| | | +--wan2Setting(2)
| | | |
| | | | +-- wan2ConnMode(1)
| | | | +-- wan2ConnType(2)
| | | | +-- wan2DmzState(3)
| | | | +-- IPAddress wan2StaticIpAddr(4)
| | | | +-- IPAddress wan2StaticIpMask(5)
| | | | +-- IPAddress wan2StaticDefaultGateway(6)
| | | | +-- DisplayString wan2AdslName(7)
| | | | +-- DisplayString wan2AdslHost(8)
| | | | +-- wan2PptpEnable(10)
| | | | +-- IPAddress wan2PptpAddr(11)
| | | | +-- DisplayString wan2PptpUsrName(12)
| | | | +-- IPAddress wan2DnsServer1(14)
| | | | +-- IPAddress wan2DnsServer2(15)
| | | | +-- IPAddress wan2DnsServer3(16)
| | | | +-- IPAddress wan2IpAddr(17)
| | | | +-- IPAddress wan2IpMask(18)
| | | | +-- IPAddress wan2DefaultGateway(19)
| | | | +-- wan2DirectedBroadcast(20)
| | | | +-- wan2SourceIPOverwrite(21)
| | | |
| | | +--lanSetting(3)
| | | |
| | | | +--lanTable(1)
| | | | |
| | | | | +--lanEntry(1) [lanVlanId]
| | | | | |
| | | | | | +-- lanVlanId(1)
| | | | | | +-- lanEnable(2)
| | | | | | +-- DisplayString lanName(3)
| | | | | | +-- IPAddress lanIpAddr(4)
| | | | | | +-- IPAddress lanIpMask(5)
| | | | | | +-- lanDirectedBroadcast(6)

```

```

| | |      +--- lanSourceIPOverwrite(7)
| | |
| | | +---dhcpServer(4)
| | | |
| | | | +---dhcpSrvTable(1)
| | | | |
| | | | | +---dhcpSrvEntry(1) [dhcpSvrEnable]
| | | | | |
| | | | | | +--- dhcpSvrEnable(1)
| | | | | | +---  dhcpSvrLeaseTime(2)
| | | | | | +--- IPAddress  dhcpSvrDns1(3)
| | | | | | +--- IPAddress  dhcpSvrDns2(4)
| | | | | | +--- IPAddress  dhcpIpRangeStart(5)
| | | | | | +--- IPAddress  dhcpIpRangeEnd(6)
| | | | | | +--- IPAddress  dhcpNTP(7)
| | | | | | +--- IPAddress  dhcpDefaultGateway(8)
| | | | | | +--- IPAddress  dhcpNetmask(9)
| | | | |
| | | | +---dhcpStaticTable(8)
| | | | |
| | | | | +---dhcpStaticEntry(1) [dhcpStaticEnable]
| | | | | |
| | | | | | +---  dhcpStaticEnable(1)
| | | | | | +--- DisplayString dhcpStaticName(2)
| | | | | | +--- IPAddress  dhcpStaticIp(3)
| | | | | | +--- MacAddress  dhcpStaticMac(4)
| | | | | | +---  dhcpStaticLeasetime(5)
| | | | | | +--- IPAddress  dhcpStaticDns1(6)
| | | | | | +--- IPAddress  dhcpStaticDns2(7)
| | | | | | +--- IPAddress  dhcpStaticNtp(8)
| | | | | | +--- IPAddress  dhcpStaticDefaultGateway(9)
| | | | | | +--- IPAddress  dhcpStaticNetmask(10)
| | | | |
| | | | +---dhcpSvrPipTable(9)
| | | | |
| | | | | +---dhcpSvrPipEntry(1) [dhcpPipEnable]

```

```

| | | |
| | | +--- dhcpPipEnable(1)
| | | +--- dhcpPipPortNumber(2)
| | | +--- IPAddress dhcpPipIp(3)
| | | +--- IPAddress dhcpPipNetmask(4)
| | | +--- dhcpPipLeasetime(5)
| | | +--- IPAddress dhcpPipDns1(6)
| | | +--- IPAddress dhcpPipDns2(7)
| | | +--- IPAddress dhcpPipNtp(8)
| | | +--- IPAddress dhcpPipGateway(9)
| | |
| | +---dhcpList(5)
| | | |
| | | +---dhcpListTable(1)
| | | | |
| | | | +---dhcpListEntry(1) [dhcpListName]
| | | | |
| | | | +--- DisplayString dhcpListName(1)
| | | | +--- DisplayString dhcpListMac(2)
| | | | +--- IPAddress dhcpListAddr(3)
| | | |
| | +---dhcpServerMode(8)
| | | |
| | | +--- dhcpServerModeStatus(1)
| | | |
| | +---brigdeSetting(9)
| | | |
| | | +--- bridgeEnable(1)
| | | +--- DisplayString bridgeName(2)
| | | +--- IPAddress birdgeIpAddr(3)
| | | +--- IPAddress bridgeIpMask(4)
| | | |
| | +---cellularSetting(10)
| | | |
| | | +--- cellularEnable(1)
| | | +--- cellularConnectionEnable(2)

```

```

| | |
| | | +---cellularSimTable(3)
| | | |
| | | | +---cellularSimEntry(1) [cellularSimIndex]
| | | | |
| | | | | +--- cellularSimIndex(1)
| | | | | +--- cellularSimEnable(2)
| | | | | +--- cellularSimPriority(3)
| | | |
| | | +---guaranlinkSetting(4)
| | | |
| | | | +--- glinkEnable(1)
| | | | +--- glinkCheckTiming(2)
| | | |
| | | +---remoteSmsSetting(5)
| | | |
| | | | +--- remoteSmsEnable(1)
| | | |
| | | +---gnssSetting(6)
| | | |
| | | | +--- gnssEnable(1)
| | | | +--- gnssServerEnable(2)
| | | | +--- gnssClientEnable(3)
| | | | +--- DisplayString gnssSatelliteStatus(4)
| | | | +--- DisplayString gnssLongitudeStatus(5)
| | | | +--- DisplayString gnssLatitudeStatus(6)
| | |
| | +---routeSetting(5)
| | |
| | | +---showRoutingTable(3)
| | | |
| | | | +---rTable(1)
| | | | |
| | | | | +---rEntry(1) [rIndex]
| | | | | |
| | | | | | +--- --- rIndex(1)

```

```

| |         +--- DisplayString rType(2)
| |         +--- DisplayString rDestination(3)
| |         +--- IPAddress      rNextHop(4)
| |         +--- DisplayString rIfsName(5)
| |         +---      rMetric(6)
| |
| | +---natSetting(6)
| | |
| | | +---natTable(1)
| | | |
| | | | +---natEntry(1) [natIndex]
| | | | |
| | | | | +---      natIndex(1)
| | | | | +---      natEnable(2)
| | | | | +--- DisplayString natDesc(3)
| | | | | +---      natMode(4)
| | | | | +---      natProtocolTcp(10)
| | | | | +---      natProtocolUdp(11)
| | | | | +---      natProtocolIcmp(12)
| | | | | +---      natNatLoopback(50)
| | | | | +---      natDoubleNat(51)
| | | | | +---      natVrrpBinding(52)
| | | | | +--- DisplayString natOriIface(100)
| | | | | +--- IPAddress      natOriSrcIp1(110)
| | | | | +--- IPAddress      natOriSrcIp2(111)
| | | | | +--- IPAddress      natOriSrcMask(112)
| | | | | +---      natOriSrcPort1(114)
| | | | | +---      natOriSrcPort2(115)
| | | | | +--- IPAddress      natOriDstIp1(130)
| | | | | +--- IPAddress      natOriDstIp2(131)
| | | | | +--- IPAddress      natOriDstMask(132)
| | | | | +---      natOriDstPort1(134)
| | | | | +---      natOriDstPort2(135)
| | | | | +--- DisplayString natTransIface(150)
| | | | | +--- IPAddress      natTransSrcIp1(160)
| | | | | +--- IPAddress      natTransSrcIp2(161)

```

```

| |      +-- IPAddress    natTransSrcMask(162)
| |      +--    natTransSrcDyn(163)
| |      +--    natTransSrcPort1(164)
| |      +--    natTransSrcPort2(165)
| |      +-- IPAddress    natTransDstIp1(180)
| |      +-- IPAddress    natTransDstIp2(181)
| |      +-- IPAddress    natTransDstMask(182)
| |      +--    natTransDstPort1(184)
| |      +--    natTransDstPort2(185)
| |
| |      +---filterSetting(7)
| |      |
| |      +---firewallPolicy(1)
| |      | |
| |      | | +-- firewallGlobalLogEnable(20)
| |      | | +-- firewallGlobalMalEnable(21)
| |      | | +-- firewallGlobalMalLevel(22)
| |      | | +-- firewallGlobalMalFlash(23)
| |      | | +-- firewallGlobalMalSyslog(24)
| |      | | +-- firewallGlobalMalTrap(25)
| |      | |
| |      +---dosSetting(2)
| |      |
| |      +-- dosNullScanEnable(1)
| |      +-- dosXmasScanEnable(2)
| |      +-- dosNmapXmasScanEnable(3)
| |      +-- dosSynFinScanEnable(4)
| |      +-- dosFinScanEnable(5)
| |      +-- dosNmapIdScanEnable(6)
| |      +-- dosSynRstScanEnable(7)
| |      +-- dosIcmpDeathScanEnable(8)
| |      +--    dosIcmpLimit(9)
| |      +-- dosSynFloodScanEnable(10)
| |      +--    dosSynLimit(11)
| |      +-- dosArpFloodScanEnable(12)
| |      +--    dosArpLimit(13)

```



```

| |   +-- dosNewTCPWithoutSYNScan(14)
| |   +-- dosUdpFloodScanEnable(15)
| |   +-- dosUdpLimit(16)
| |
| +--vpnSetting(8)
| | |
| | | +--vpnIpsec(1)
| | | |
| | | | +--ipsecGlobal(1)
| | | | |
| | | | | +-- ipsecGlobalState(1)
| | | | | +-- ipsecGlobalNatt(2)
| | | | | +-- ipsecGlobalEventLog(3)
| | | | | +-- ipsecGlobalEventLogFlash(4)
| | | | | +-- ipsecGlobalEventLogSyslog(5)
| | | | | +-- ipsecGlobalEventLogSNMPTrap(6)
| | | | |
| | | | +--ipsecSetting(2)
| | | | |
| | | | | +--ipsecSettingTable(1)
| | | | | |
| | | | | | +--ipsecSettingEntry(1) [ipsecSettingEnable]
| | | | | | |
| | | | | | | +-- ipsecSettingEnable(1)
| | | | | | | +-- IpAddress ipsecSettingRemoteEndIp(2)
| | | | | | | +-- ipsecSettingL2tp(4)
| | | | | | | +-- ipsecSettingPfs(5)
| | | | | | | +-- DisplayString ipsecSettingName(6)
| | | | | | | +-- ipsecSettingSecurityLevel(7)
| | | | | | | +-- ipsecConnIfs(8)
| | | | | | | +-- ipsecStartup(9)
| | | | | | | +-- IpAddress ipsecLocalNetwork(10)
| | | | | | | +-- IpAddress ipsecLocalMask(11)
| | | | | | | +-- DisplayString ipsecLocalId(13)
| | | | | | | +-- IpAddress ipsecRemoteNetwork(14)
| | | | | | | +-- IpAddress ipsecRemoteMask(15)

```

```

| | | | +-- DisplayString ipsecRemoteId(17)
| | | | +-- ipsecAuthMode(18)
| | | | +-- DisplayString ipsecPsk(19)
| | | | +-- DisplayString ipsecLocalSelectPem(20)
| | | | +-- DisplayString ipsecRemoteSelectPem(21)
| | | | +-- ipsecExchange(22)
| | | | +-- ipsecP1Encrypt(23)
| | | | +-- ipsecP1Ah(24)
| | | | +-- ipsecP1Dh(25)
| | | | +-- ipsecIKELifetime(27)
| | | | +-- ipsecSaLifetime(30)
| | | | +-- ipsecP2Encrypt(31)
| | | | +-- ipsecP2Ah(32)
| | | | +-- ipsecDpdAction(33)
| | | | +-- ipsecDpdDelay(34)
| | | | +-- ipsecDpdTimeout(35)
| | | | +-- ipsecIdentityType(36)
| | | | +-- ipsecPfsDHGroup(37)
| | | | +-- DisplayString ipsecLocalSubnet(38)
| | | | +-- DisplayString ipsecRemoteSubnet(39)
| | | |
| | | +--ipsecStatus(3)
| | | |
| | | +--ipsecStatusTable(1)
| | | |
| | | +--ipsecStatusEntry(1) [ipsecStatusIndex]
| | | |
| | | +-- --- ipsecStatusIndex(1)
| | | +-- DisplayString ipsecStatusName(2)
| | | +-- DisplayString ipsecStatusLocSubnet(3)
| | | +-- IpAddress ipsecStatusLocGateway(4)
| | | +-- IpAddress ipsecStatusRemGateway(5)
| | | +-- DisplayString ipsecStatusRemSubnet(6)
| | | +-- DisplayString ipsecStatusPhase1(7)
| | | +-- DisplayString ipsecStatusPhase2(8)
| | | +-- ipsecI2tp(9)

```

```

| | |
| | +--vpnL2tp(2)
| | |
| | +-- l2tpModewan1(1)
| | +-- IPAddress l2tpLocalIpWan1(2)
| | +-- IPAddress l2tpOfferIpStartWan1(3)
| | +-- IPAddress l2tpOfferIpEndWan1(4)
| | |
| | +--l2tpTable(9)
| | |
| | +--l2tpEntry(1) [l2tpLoginUserName]
| | |
| | +-- DisplayString l2tpLoginUserName(1)
| |
| +--snmpSetting(9)
| | |
| | +--snmpSetup(1)
| | |
| | +-- snmpVersion(1)
| | +-- snmpAuthType(3)
| | +-- snmpAccessControl1(7)
| | +-- snmpAccessControl2(9)
| | +-- DisplayString trap1ServerAddr(10)
| | +-- DisplayString trap2ServerAddr(11)
| | +-- DisplayString trap3ServerAddr(12)
| | +-- snmpInformEnable(13)
| | +-- DisplayString snmpReadCommunity1(14)
| | +-- DisplayString snmpReadCommunity2(15)
| | +-- DisplayString snmpTrapCommunity(16)
| | +-- snmpTrapMode(17)
| | +-- snmpAdminSecurityLevel(22)
| | +-- snmpUserSecurityLevel(23)
| |
| +--diagnosisSetting(12)
| | |
| | +--lldpSetting(2)

```

```

| | |
| |   +-- lldpEnable(1)
| |   +-- lldpInterval(2)
| |   +-- lldpRingPortBypass(3)
| |
| | +--monitor(13)
| | |
| |   +-- power1InputStatus(7)
| |   +-- power2InputStatus(8)
| | |
| |   +--monitorFiberCheckTable(11)
| | |
| |   +--monitorFiberCheckEntry(1) [portIndex]
| | |
| |     +-- DisplayString fiberPort(1)
| |     +-- DisplayString fiberModelName(2)
| |     +-- DisplayString fiberWaveLength(3)
| |     +-- DisplayString fiberVoltage(4)
| |     +-- DisplayString fiberTemperature(5)
| |     +-- DisplayString fiberTempWarn(6)
| |     +-- DisplayString fiberTxPower(7)
| |     +-- DisplayString fiberTxPowerWarn(8)
| |     +-- DisplayString fiberRxPower(9)
| |     +-- DisplayString fiberRxPowerWarn(10)
| |     +-- DisplayString fiberSN(13)
| |
| | +--systemLog(14)
| | |
| |   +--syslog(2)
| | |
| |     +-- syslogServer1Enable(1)
| |     +-- DisplayString syslogServer1(2)
| |     +-- syslogServer1port(3)
| |     +-- syslogServer2Enable(4)
| |     +-- DisplayString syslogServer2(5)
| |     +-- syslogServer2port(6)

```

```

| |   +--  syslogServer3Enable(7)
| |   +--  DisplayString syslogServer3(8)
| |   +--  syslogServer3port(9)
| |   +--  DisplayString syslogServer1cert(10)
| |   +--  DisplayString syslogServer2cert(11)
| |   +--  DisplayString syslogServer3cert(12)
| |
| |   +--networkMode(15)
| |   |
| |   +--  networkModeSelection(1)
| |   |
| |   +--routingRedundancy(16)
| |   |
| |   +--vrrp(1)
| |   |
| |   +--vrrpInterfaceTable(1)
| |   | |
| |   | +--vrrpInterfaceEntry(1) [vrrpIfIndex]
| |   | |
| |   | |   +-- ---  vrrpIfIndex(1)
| |   | |   +--  DisplayString vrrpIfName(2)
| |   | |   +--  IPAddress    vrrpIfAddr(3)
| |   | |   +--  vrrpIfEnable(4)
| |   | |   +--  IPAddress    vrrpIfVirtualIp(5)
| |   | |   +--  vrrpIfRouterId(6)
| |   | |   +--  vrrpIfPriority(7)
| |   | |   +--  vrrpIfPreemption(8)
| |   | |   +--  vrrpIfStatus(9)
| |   | |   +--  DisplayString vrrpIfTrack(10)
| |   | |   +--  IPAddress    vrrpPingTrackIP(11)
| |   | |   +--  vrrpPingTrackInt(12)
| |   | |   +--  vrrpPingTimeout(13)
| |   | |   +--  vrrpPingTrackSuccess(14)
| |   | |   +--  vrrpPingTrackFailure(15)
| |   | |   +--  vrrpAdvInt(16)
| |   | |   +--  vrrpPreemptDelay(17)

```

```

| | |
| |   +-- vrrpEnable(2)
| |
| +--portSetting(17)
| | |
| |   +--portTable(1)
| |   |
| |     +--portEntry(1) [portIndex]
| |     |
| |       +--   portIndex(1)
| |       +--   DisplayString portDesc(2)
| |       +--   portEnable(3)
| |       +--   portSpeed(4)
| |       +--   portMDI(5)
| |       +--   portFDXFlowCtrl(6)
| |       +--   DisplayString portName(7)
| |       +--   portType(8)
| |
| +--portTrunking(19)
| | |
| |   +--trunkSettingTable(1)
| |   | |
| |     +--trunkSettingEntry(1) [trunkSettingIndex]
| |     | |
| |       +--   trunkSettingIndex(1)
| |       +--   trunkType(2)
| |       +--   PortList   trunkMemberPorts(3)
| |       |
| |     +--trunkTable(2)
| |     |
| |       +--trunkEntry(1) [trunkIndex,trunkPort]
| |       |
| |         +--   trunkIndex(1)
| |         +--   trunkPort(2)
| |         +--   trunkStatus(3)
| |

```

```

| +-commRedundancy(20)
| | |
| | +-spanningTree(3)
| | | |
| | | +- spanningTreeRoot(1)
| | | +- spanningTreeBridgePriority(2)
| | | +- spanningTreeHelloTime(3)
| | | +- spanningTreeMaxAge(4)
| | | +- spanningTreeForwardingDelay(5)
| | | |
| | | +-spanningTreeTable(6)
| | | |
| | | +-spanningTreeEntry(1) [enableSpanningTree]
| | | |
| | | +- enableSpanningTree(2)
| | | +- spanningTreePortPriority(3)
| | | +- spanningTreePortCost(4)
| | | +- spanningTreePortStatus(5)
| | | +- spanningTreePortEdge(6)
| | | |
| | +- activeProtocolOfRedundancy(4)
| | |
| | +-turboRingV2(5)
| | | |
| | | +-turboRingV2Ring1(1)
| | | | |
| | | | +- ringIndexRing1(1)
| | | | +- ringEnableRing1(2)
| | | | +- masterSetupRing1(3)
| | | | +- masterStatusRing1(4)
| | | | +- MacAddress designatedMasterRing1(5)
| | | | +- rdnt1stPortRing1(6)
| | | | +- rdnt1stPortStatusRing1(7)
| | | | +- rdnt2ndPortRing1(8)
| | | | +- rdnt2ndPortStatusRing1(9)
| | | | +- brokenStatusRing1(10)

```

```

| | | |
| | | +--turboRingV2Ring2(2)
| | | | |
| | | | +-- ringIndexRing2(1)
| | | | +-- ringEnableRing2(2)
| | | | +-- masterSetupRing2(3)
| | | | +-- masterStatusRing2(4)
| | | | +-- MacAddress designatedMasterRing2(5)
| | | | +-- rdnt1stPortRing2(6)
| | | | +-- rdnt1stPortStatusRing2(7)
| | | | +-- rdnt2ndPortRing2(8)
| | | | +-- rdnt2ndPortStatusRing2(9)
| | | | +-- brokenStatusRing2(10)
| | | |
| | | +--turboRingV2Coupling(3)
| | | |
| | | +-- couplingEnable(1)
| | | +-- couplingMode(2)
| | | +-- coupling1stPort(3)
| | | +-- coupling1stPortStatus(4)
| | | +-- coupling2ndPort(5)
| | | +-- coupling2ndPortStatus(6)
| | |
| | +--turboChain(6)
| | |
| | +-- turboChainRole(1)
| | +-- turboChainPort1(2)
| | +-- turboChainPort2(3)
| | +-- turboChainPort1Status(4)
| | +-- turboChainPort2Status(5)
| |
| +--vlan(21)
| | |
| | +--vlanPortSettingTable(1)
| | | |
| | | +--vlanPortSettingEntry(1) [portIndex]

```



```

| | | |
| | | +-- portVlanType(1)
| | | +-- portDefaultVid(2)
| | | +-- DisplayString portFixedVid(3)
| | | +-- DisplayString portFixedVidUntag(5)
| | |
| | +--vlanTable(2)
| | | |
| | | +--vlanEntry(1) [vlanId]
| | | |
| | | +-- vlanId(1)
| | | +-- PortList joinedAccessPorts(2)
| | | +-- PortList joinedTrunkPorts(3)
| | | +-- PortList joinedHybirdPorts(4)
| | |
| | +-- managementVlanId(3)
| | +-- vlanType(4)
| |
| +--swMgmtGroup(22)
| | |
| | +-- numberOfPorts(1)
| | +-- DisplayString switchModel(2)
| | +-- DisplayString firmwareVersion(4)
| |
| +--globalStatus(23)
| | |
| | +-- firewallGlobalStatus(1)
| | +-- natGlobalStatus(2)
| | +-- vpnGlobalStatus(3)
| | +-- securityNotificationFirewallStatus(4)
| | +-- securityNotificationDoSAttackStatus(5)
| | +-- securityNotificationAccessViolationStatus(6)
| | +-- securityNotificationLoginFailStatus(7)
| | +-- defaultPasswordChange(8)
| |
| +--interfaceStatus(24)

```

```

| | |
| | +--interfaceStatusTable(1)
| | | |
| | | +--interfaceStatusEntry(1) [interfaceOverallStatus]
| | | |
| | | +-- DisplayString interfaceOverallStatus(1)
| | | +-- interfaceOverallType(2)
| | |
| | +--cellularStatus(2)
| | |
| | +-- DisplayString cellularMode(1)
| | +-- DisplayString cellularCarrier(2)
| | +-- DisplayString cellularRSSI(3)
| | +-- DisplayString cellularIP(4)
| | +-- DisplayString cellularIMEI(5)
| | +-- DisplayString cellularIMSI(6)
| | +-- cellularConnectionStatus(7)
| | +-- DisplayString cellularSim1Status(8)
| | +-- DisplayString cellularSim2Status(9)
| | +-- DisplayString cellularRSRP(10)
| | +-- DisplayString cellularRSRQ(11)
| | +-- DisplayString cellularSINR(12)
| |
| +--securityNotification(25)
| | |
| | +-- eventFirewall(1)
| | +-- eventDoSAttack(2)
| | +-- eventAccessViolation(3)
| | +-- eventLoginFail(4)
| |
| +--mtuAdjustment(28)
| | |
| | +--mtuAdjustmentTable(1)
| | |
| | +--mtuAdjustmentEntry(1) [mtuAdjustmentIndex]
| | |

```

```

| |      +-- ---      mtuAdjustmentIndex(1)
| |      +-- DisplayString mtuAdjustmentIfName(2)
| |      +--      mtuAdjustmentMTUsize(3)
| |      +--      mtuAdjustmentPRPtraffic(4)
| |
| +--poeSetting(40)
| | |
| | | +--poePortTable(3)
| | | |
| | | | +--poePortEntry(1) [poePortIndex]
| | | | |
| | | | | +--      poePortIndex(1)
| | | | | +--      poePortEnable(2)
| | | | | +--      powerLimit(4)
| | | | | +--      pdfailure(5)
| | | | | +-- DisplayString pdipaddr(6)
| | | | | +--      pdPollingInterval(7)
| | | | | +--      poePortLegacyPdDetect(9)
| | | | | +--      pdNoResponseTimeout(10)
| | | | | +--      pdNoResponseAction(11)
| | | | | +--      poePowerOutputMode(12)
| | | |
| | | +--poeStatusTable(6)
| | | |
| | | | +--poeStatusEntry(1) [poePortIndex]
| | | | |
| | | | | +--      poePortStatus(1)
| | | | | +--      poePortConsumption(2)
| | | | | +--      poePortVoltage(3)
| | | | | +--      poePortCurrent(4)
| | | | | +--      poePortPowerOutput(5)
| | | | | +--      poePortClass(6)
| | | | | +--      poePortPdFailCheck(7)
| | | | | +--      poePortPdStatusDescription(8)
| | | |
| | +--poeSystemSetting(9)

```

```

| | |
| | +-- poeSysPowerEnable(1)
| | +-- poeSysPowerThreshold(2)
| | +-- poeSysThresholdCutOff(3)
| | +-- poeSysAllocatedPower(4)
| | +-- poeSysMeasuredPower(5)
| | +-- poeSysPowerBudget(7)
| |
| +--eventlog(46)
| | |
| | +--eventlogSystem(1)
| | | |
| | | +--eventlogSystemTable(1)
| | | | |
| | | | +--eventlogSystemEntry(1) [eventlogSystemIndex]
| | | | |
| | | | +-- eventlogSystemIndex(1)
| | | | +-- DisplayString eventlogSystemTimestamp(2)
| | | | +-- eventlogSystemSeverity(3)
| | | | +-- DisplayString eventlogSystemEvent(4)
| | | |
| | | +-- eventlogSystemClear(2)
| | |
| | +--eventlogVPN(2)
| | | |
| | | +--eventlogVPNTable(1)
| | | | |
| | | | +--eventlogVPNEntry(1) [eventlogVPNIndex]
| | | | |
| | | | +-- eventlogVPNIndex(1)
| | | | +-- DisplayString eventlogVPNTimestamp(2)
| | | | +-- eventlogVPNSeverity(3)
| | | | +-- DisplayString eventlogVPNEvent(4)
| | | |
| | | +-- eventlogVPNClear(2)
| | |

```

```

| | +--eventlogTruseAccess(3)
| | | |
| | | +--eventlogTruseAccessTable(1)
| | | | |
| | | | +--eventlogTruseAccessEntry(1) [eventlogTruseAccessIndex]
| | | | |
| | | | +-- eventlogTruseAccessIndex(1)
| | | | +-- DisplayString eventlogTruseAccessTimestamp(2)
| | | | +-- eventlogTruseAccessSeverity(3)
| | | | +-- DisplayString eventlogTruseAccessEvent(4)
| | | |
| | | +-- eventlogTruseAccessClear(2)
| | |
| | +--eventlogMalformed(4)
| | | |
| | | +--eventlogMalformedTable(1)
| | | | |
| | | | +--eventlogMalformedEntry(1) [eventlogMalformedIndex]
| | | | |
| | | | +-- eventlogMalformedIndex(1)
| | | | +-- DisplayString eventlogMalformedTimestamp(2)
| | | | +-- eventlogMalformedSeverity(3)
| | | | +-- DisplayString eventlogMalformedEvent(4)
| | | |
| | | +-- eventlogMalformedClear(2)
| | |
| | +--eventlogDOS(5)
| | | |
| | | +--eventlogDOSTable(1)
| | | | |
| | | | +--eventlogDOSEntry(1) [eventlogDOSIndex]
| | | | |
| | | | +-- eventlogDOSIndex(1)
| | | | +-- DisplayString eventlogDOSTimestamp(2)
| | | | +-- eventlogDOSSeverity(3)
| | | | +-- DisplayString eventlogDOSEvent(4)

```

```

| | | |
| | | +-- eventlogDOSClear(2)
| | |
| | +--eventlogDevLockdown(6)
| | | |
| | | +--eventlogDevLockdownTable(1)
| | | | |
| | | | +--eventlogDevLockdownEntry(1) [eventlogDevLockdownIndex]
| | | | |
| | | | +-- eventlogDevLockdownIndex(1)
| | | | +-- DisplayString eventlogDevLockdownTimestamp(2)
| | | | +-- eventlogDevLockdownSeverity(3)
| | | | +-- DisplayString eventlogDevLockdownEvent(4)
| | | |
| | | +-- eventlogDevLockdownClear(2)
| | |
| | +--eventlogL3Policy(7)
| | | |
| | | +--eventlogL3PolicyTable(1)
| | | | |
| | | | +--eventlogL3PolicyEntry(1) [eventlogL3PolicyIndex]
| | | | |
| | | | +-- eventlogL3PolicyIndex(1)
| | | | +-- DisplayString eventlogL3PolicyTimestamp(2)
| | | | +-- eventlogL3PolicySeverity(3)
| | | | +-- DisplayString eventlogL3PolicyEvent(4)
| | | |
| | | +-- eventlogL3PolicyClear(2)
| | |
| | +--eventlogProtocolFilterPolicy(8)
| | | |
| | | +--eventlogProtocolFilterPolicyTable(1)
| | | | |
| | | | +--eventlogProtocolFilterPolicyEntry(1)
[eventlogProtocolFilterPolicyIndex]
| | | | |

```

```

| | | | +-- eventlogProtocolFilterPolicyIndex(1)
| | | | +-- DisplayString eventlogProtocolFilterPolicyTimestamp(2)
| | | | +-- eventlogProtocolFilterPolicySeverity(3)
| | | | +-- DisplayString eventlogProtocolFilterPolicyEvent(4)
| | | |
| | | +-- eventlogProtocolFilterPolicyClear(2)
| | |
| | +--eventlogADP(9)
| | | |
| | | +--eventlogADPTable(1)
| | | | |
| | | | +--eventlogADPEntry(1) [eventlogADPIndex]
| | | | |
| | | | +-- eventlogADPIndex(1)
| | | | +-- DisplayString eventlogADPTimestamp(2)
| | | | +-- eventlogADPSeverity(3)
| | | | +-- DisplayString eventlogADPEvent(4)
| | | |
| | | +-- eventlogADPClear(2)
| | |
| | +--eventlogIPS(10)
| | | |
| | | +--eventlogIPSTable(1)
| | | | |
| | | | +--eventlogIPSEntry(1) [eventlogIPSIndex]
| | | | |
| | | | +-- eventlogIPSIndex(1)
| | | | +-- DisplayString eventlogIPSTimestamp(2)
| | | | +-- eventlogIPSSeverity(3)
| | | | +-- DisplayString eventlogIPSEvent(4)
| | | |
| | | +-- eventlogIPSClear(2)
| | |
| | +--eventlogSessionControl(11)
| | | |
| | | +--eventlogSessionControlTable(1)

```

```

| | | | |
| | | | +--eventlogSessionControlEntry(1) [eventlogSessionControlIndex]
| | | | |
| | | | +-- eventlogSessionControlIndex(1)
| | | | +-- DisplayString eventlogSessionControlTimestamp(2)
| | | | +-- eventlogSessionControlSeverity(3)
| | | | +-- DisplayString eventlogSessionControlEvent(4)
| | | |
| | | +-- eventlogSessionControlClear(2)
| | |
| | +--eventlogL2Filter(12)
| | |
| | | +--eventlogL2FilterTable(1)
| | | |
| | | | +--eventlogL2FilterEntry(1) [eventlogL2FilterIndex]
| | | | |
| | | | +-- eventlogL2FilterIndex(1)
| | | | +-- DisplayString eventlogL2FilterTimestamp(2)
| | | | +-- eventlogL2FilterSeverity(3)
| | | | +-- DisplayString eventlogL2FilterEvent(4)
| | | |
| | | +-- eventlogL2FilterClear(2)
| | |
| +-- cpuLoading5s(53)
| +-- cpuLoading30s(54)
| +-- cpuLoading300s(55)
| +-- totalMemory(56)
| +-- freeMemory(57)
| +-- usedMemory(58)
| +-- memoryUsage(59)
| |
| +--managementInterface(63)
| | |
| | +-- httpEnable(1)
| | +-- httpPort(2)
| | +-- sslEnable(3)

```



```

| | +--      sslPort(4)
| | +--      telnetEnable(5)
| | +--      telnetPort(6)
| | +--      sshEnable(7)
| | +--      sshPort(8)
| | +--      mgmtInterfaceAutoLogout(9)
| | +-- DisplayString moxaUtilityServicePort(13)
| | +--      httpMaxLoginUsers(14)
| | +--      telnetMaxLoginUsers(15)
| | +--      moxaUtilityServiceEnable(16)
| | |
| | +--pingResponseIfTable(18)
| | |
| |     +--pingResponseIfEntry(1) [pingResponseIf]
| |     |
| |         +-- DisplayString pingResponseIf(1)
| |
| +--passwordPolicy(70)
| | |
| | +--      pwdMinLength(1)
| | +--      pwdComplexityCheckEnable(2)
| | +--      pwdComplexityCheckDigitEnable(3)
| | +--      pwdComplexityCheckAlphabetEnable(4)
| | +--      pwdComplexityCheckSpecialCharEnable(5)
| |
| +--loginLockout(71)
| | |
| | +--      loginFailureLockoutEnable(1)
| | +--      loginFailureLockoutRetrys(2)
| | +--      loginFailureLockoutTime(3)
| |
| +--systemNotifyMessage(72)
| | |
| | +--      DisplayString httpLoginMessage(1)
| | +--      DisplayString httpLoginFailureMessage(2)
| |

```

```

| +-- DisplayString serialNumber(78)
| +--  configEncryptEnable(79)
| |
| +--security(80)
| | |
| | +--portAccessControl(2)
| | |
| | +--dot1x(2)
| | |
| | +-- dataBaseOption(1)
| | +-- dot1xReauthEnable(5)
| | +--  dot1xReauthPeriod(6)
| | |
| | +--dot1xSettingTable(7)
| | | |
| | | +--dot1xSettingEntry(1) [portIndex]
| | | |
| | | +-- enableDot1X(1)
| | | |
| | | +--dot1xReauthTable(8)
| | | | |
| | | | +--dot1xReauthEntry(1) [dot1xReauthPortIndex]
| | | | |
| | | | +--  dot1xReauthPortIndex(1)
| | | | +-- dot1xReauth(2)
| | | |
| | | +--dot1xRadius(9)
| | | |
| | | +-- DisplayString dot1x1stRadiusServer(2)
| | | +--  dot1x1stRadiusPort(3)
| | | +-- DisplayString dot1x1stRadiusSharedKey(4)
| | | +-- DisplayString dot1x2ndRadiusServer(5)
| | | +--  dot1x2ndRadiusPort(6)
| | | +-- DisplayString dot1x2ndRadiusSharedKey(7)
| | |
| | +--powerMgmtSetting(81)

```

```

| | |
| | +-- powerMgmtEnable(1)
| |
| +--serialSetting(82)
| | |
| | +-- serialPort(1)
| | +-- serialPortIfType(2)
| | +-- serialPortOpMode(3)
| | +-- serialDataLog(4)
| | +-- serialPortBuffer(5)
| |
| +--linkFaultPassthrough(83)
| | |
| | +-- lfpState(1)
| | +-- lfpPort1(2)
| | +-- lfpPort2(3)
| |
| +--softLockdownModeStatus(84)
| | |
| | +-- softLockdownModeStatusStatus(1)
| | +-- softLockdownModeStatusTr2(2)
| | +-- softLockdownModeStatusDhcpSvr(3)
| | +-- softLockdownModeStatusDhcpRelayAgent(4)
| | +-- softLockdownModeStatusSnmpSvr(5)
|
+--mibNotificationsPrefix(3)
|
+--configChangeTrap(1) [varconfigChangeTrap]
|
+--power1Trap(2) [varpower1Trap]
|
+--power2Trap(3) [varpower2Trap]
|
+--di1Trap(4) [vardi1Trap]
|
+--di2Trap(5) [vardi2Trap]

```

```

|
+--redundancyTopologyChangedTrap(10) [varredundancyTopologyChangedTrap]
|
+--turboRingCouplingPortChangedTrap(11)
[verturboRingCouplingPortChangedTrap]
|
+--turboRingMasterChangedTrap(12) [verturboRingMasterChangedTrap]
|
+--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

Command Type	Command Name
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

Service Operation	Service Operation Name
<b>15</b>	deleteEventAction
<b>16</b>	deleteEventCondition
<b>17</b>	deleteEventEnrollment
<b>18</b>	deleteJournal
<b>19</b>	deleteNamedType
<b>20</b>	deleteNamedVariableList
<b>21</b>	deleteProgramInvocation
<b>22</b>	deleteSemaphore
<b>23</b>	deleteVariableAccess
<b>24</b>	downloadSegment
<b>25</b>	eventNotification
<b>26</b>	fileClose
<b>27</b>	fileDelete
<b>28</b>	fileDirectory
<b>29</b>	fileOpen
<b>30</b>	fileRead
<b>31</b>	fileRename
<b>32</b>	getAlarmEnrollmentSummary
<b>33</b>	getAlarmSummary
<b>34</b>	getCapabilityList
<b>35</b>	getDomainAttributes
<b>36</b>	getEventActionAttributes
<b>37</b>	getEventConditionAttributes

Service Operation	Service Operation Name
38	getEventEnrollmentAttributes
39	getNamedTypeAttributes
40	getNamedVariableListAttributes
41	getNameList
42	getProgramInvocationAttributes
43	getScatteredAccessAttributes
44	getVariableAccessAttributes
45	identify
46	informationReport
47	initializeJournal
48	initiateDownloadSequence
49	initiateUploadSequence
50	input
51	kill
52	loadDomainContent
53	obtainFile
54	output
55	read
56	readJournal
57	relinquishControl
58	rename
59	reportActionStatus
60	reportEventActionStatus

Service Operation	Service Operation Name
61	reportEventConditionStatus
62	reportEventEnrollmentStatus
63	reportJournalStatus
64	reportPoolSemaphoreStatus
65	reportSemaphoreEntryStatus
66	reportSemaphoreStatus
67	requestDomainDownLoad
68	requestDomainUpload
69	reset
70	resume
71	start
72	status
73	stop
74	storeDomainContent
75	takeControl
76	terminateDownloadSequence
77	terminateUploadSequence
78	triggerEvent
79	unsolicitedStatus
80	uploadSegment
81	write
82	writeJournal



## Severity Level List

This is a list of severity levels and descriptions, which are based on CVSS vulnerability classifications.

Severity	Description
<b>Emergency</b>	System is unusable
<b>Alert</b>	Action must be taken immediately
<b>Critical</b>	Critical conditions
<b>Error</b>	Error conditions
<b>Warning</b>	Warning conditions
<b>Notice</b>	Normal but significant condition
<b>Infomational</b>	Informational messages
<b>Debug</b>	Debug-level messages

## Status Codes

This page shows the different status codes for your device.

 **Note**

Available settings and options will vary depending on the product model.

## PoE Status Codes

### Classification

Classification	Max Power (watts) by PSE Output
<b>0</b>	15.4
<b>1</b>	4
<b>2</b>	7
<b>3</b>	15.4

Classification	Max Power (watts) by PSE Output
----------------	---------------------------------

4	30
---	----

## Device Type

Item	Description
------	-------------

<b>Not Present</b>	There are no active connections to the port.
--------------------	--

<b>802.3at</b>	An IEEE 802.3at PD is connected to the port.
----------------	--

<b>802.3af</b>	An IEEE 802.3af PD is connected to the port.
----------------	--

<b>NIC</b>	A NIC is connected to the port.
------------	---------------------------------

<b>Unknown</b>	An unknown PD is connected to the port.
----------------	---

<b>N/A</b>	The PoE function is disabled.
------------	-------------------------------

## Configuration Suggestion

Item	Description
------	-------------

<b>Disable PoE power output</b>	A NIC or unknown PD was detected; you may want to disable PoE power output for the port.
---------------------------------	--

<b>Select Force Mode</b>	A higher/lower resistance or higher capacitance was detected; you may want to select <b>Force Mode</b> for the port.
--------------------------	--

<b>Select high power output</b>	An unknown classification was detected; you may want to select High Power output.
---------------------------------	---

<b>Raise the external power supply voltage to greater than 46 VDC</b>	When the external supply voltage is detected at less than 46 V, the system suggests raising the voltage.
---	--

<b>Enable PoE function for detection</b>	The system suggests enabling the PoE function.
--	--

<b>Select IEEE 802.3at auto mode</b>	When detecting an IEEE 802.3at PD, the system suggests selecting 802.3at Auto mode.
--------------------------------------	---

<b>Select IEEE 802.3af auto mode</b>	When detecting an IEEE 802.3af PD, the system suggests selecting 802.3af Auto mode.
--------------------------------------	---

## Structure and Syntax of Local Consist Info Files

A local consist info file uses XML syntax to represent consist information. It is composed of the physical vehicle information and the network device information within each vehicle.

The basic file structure is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<consistinfo>
  <vehicleinfo>
    <functioninfo>
    </functioninfo>
  </vehicleinfo>
</consistinfo>
```

### consistinfo

The consistinfo element represents consist info. There must be only one consistinfo element per configuration file.

### Attributes

There are no attributes for this element.

### Child Elements

Name	Description	Valid Range
<b>cstId</b>	Required. Specifies a unique ID for a consist. This is different than the Consist UUID.  The suggested naming convention for using a UIC for the cstId is: <i>"UIC" + (numerical part of UIC)</i>  For example, the suggested cstId for UIC 508089-43503-8 would be <i>UIC508089435038</i> .	Valid XML element name that is 3 to 15 characters. A hyphen cannot be used as the last character.
<b>cstType</b>	Optional. Specifies the type of the consist.	Valid XML element name that is 3 to 15 characters. A hyphen cannot be used as the last character.
<b>cstOwner</b>	Optional. Specifies the owner of the consist.	Valid XML element name that is 3 to 15 characters. A hyphen cannot be used as the last character.
<b>vehicleinfo</b>	Required. List of vehicle information that belongs to the consist. Refer to vehicleinfo for more information.	The numbers of the vehicle information, ranges from 1 to 32

## vehicleinfo

The vehicleinfo element represents vehicle information in the consist. There should be 1 to 32 vehicleinfo elements within a consistinfo element.

### Attributes

Name	Value	Valid Range
<b>leading</b>	Required. Boolean that indicates whether ECSC is attached to this vehicle.	true / false
<b>tractVeh</b>	Optional. Boolean that indicates whether a vehicle has traction.	true / false

### Child Elements

Name	Description	Valid Range
<b>vehId</b>	Required. Specifies a unique ID for a vehicle. The suggested naming convention for using a UIC as for the vehId is: <i>"UIC" + (numerical part of UIC)</i> For example, suggested vehId for <i>UIC 508089-43501-2</i> would be <i>UIC508089435012</i> .	Valid XML element name that is 3 to 15 characters. A hyphen cannot be used as the last character.
<b>vehType</b>	Optional. Specifies the type of vehicle.	Valid XML element name that is 3 to 15 characters. A hyphen cannot be used as the last character.
<b>vehOrient</b>	Required. Specifies the vehicle orientation with respect to the consist direction. <b>same:</b> Indicates that vehicle has the same direction with respect to the consist direction. <b>inverse:</b> Indicates that the vehicle is in the opposite direction with respect to the consist direction.	same / inverse
<b>cstVehNo</b>	Required. Specifies the index of the vehicle within the consist. Indexing starts from consist direction 1 to direction 2. The first vehicle in consist direction 1 is assigned index 1. The second vehicle (next vehicle in direction 2 of first vehicle) has index 2, and so on.	Integer from 1 to 32
<b>functioninfo</b>	Required. List of devices/functional groups information within the vehicle. Refer to functioninfo for more information. Number of devices/function group information ranges from 0 to 1024	Integer from 0 to 1024

## functioninfo

The functioninfo element represents device or functional group information in the vehicle. There can be 0 to 1024 functioninfo elements within a vehicleinfo element.

### Attributes

There are no attributes for this element.

### Child Elements

Name	Description	Valid Range
<b>fctName</b>	Required. Specifies a unique name for the device/functional group.  For devices, we suggest using "dev" or "fct" as a prefix for the fctName. Examples: fctDoorCtrl, fctBrake, devHMI  For functional groups, which represent multicast addresses, fctName should use "grp" as the prefix. Examples: grpDoorCtrl, grpBrake, grpETBN, grpECSC	Valid XML element name that is 3 to 15 characters. A hyphen cannot be used as the last character.
<b>cnId</b>	Required. Specifies the static CN ID of the ECN this device/functional group connects to. Set this to 0 for functional groups.	Integer from 0 to 32
<b>fctId</b>	Required. Specifies the numeric ID for the device/functional group. Must be different from the Host ID of the ECN.  There should be no duplicate combinations of fctId and cnId within a single consist.	Integer from 1 to 32767

## 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	EDR Series	EDF Series	OnCell Series
Device Summary		YES	YES	YES

Configuration Section	Function	EDR Series	EDF Series	OnCell Series
<b>Setup Wizard</b>		YES	-	-
<b>System</b>		YES	YES	YES
	System Management	YES	YES	YES
	Information Settings	YES	YES	YES
	Firmware Upgrade	YES	YES	YES
	Software Package Management	YES	YES	YES
	Configuration Backup and Restore	YES	YES	YES
	Account Management	YES	YES	YES
	User Accounts	YES	YES	YES
	Password Policy	YES	YES	YES
	License Management	YES	YES	YES
	Management Interface	YES	YES	YES
	Out of Band Management	-	YES	-
	User Interface	YES	YES	YES
	Hardware Interface	YES	YES	YES
	SNMP	YES	YES	YES
	Moxa Remote Connect	-	-	YES
	MXsecurity	YES	YES	YES
	Time	YES	YES	YES
	System Time	YES	YES	YES
	NTP/SNTP Server	YES	-	YES
	Power Management	-	-	YES

Configuration Section	Function	EDR Series	EDF Series	OnCell Series
	SMS	-	-	YES
	GNSS	-	-	YES
	Setting Check	YES	YES	YES
<b>Cellular</b>		-	-	YES
<b>Serial</b>		-	-	YES
<b>Network Configuration</b>		YES	YES	YES
	Ports	YES	YES	YES
	Port Settings	YES	YES	YES
	Link Aggregation	YES	-	-
	PoE	-	-	-
	Link Fault Passthrough	YES	YES	-
	LAN Bypass Gen3	YES	YES	-
	Layer 2 Switching	YES	-	YES
	VLAN	YES	-	YES
	MAC Address Table	YES	-	YES
	QoS	YES	-	-
	Rate Limit	YES	-	-
	Multicast	YES	-	YES
	IGMP Snooping	YES	-	-
	Static Multicast Table	YES	-	YES
	Network Interfaces	YES	YES	YES
<b>Redundancy</b>		YES	-	-

Configuration Section	Function	EDR Series	EDF Series	OnCell Series
	Layer 2 Redundancy	YES	-	-
	Spanning Tree	YES	-	-
	Turbo Ring V2	YES	-	-
	Turbo Chain	YES	-	-
	Layer 3 Redundancy	YES	-	YES
	VRRP	YES	-	YES
	WAN Redundancy	YES	-	YES
<b>Network Service</b>		YES	-	YES
	DHCP Server	YES	-	YES
	Dynamic DNS	YES	-	YES
<b>Routing</b>		YES	-	YES
	Unicast Route	YES	-	YES
	Static Routes	YES	-	YES
	RIP	YES	-	-
	OSPF	YES	-	-
	Routing Table	YES	-	YES
	Multicast Route	YES	-	YES
	Multicast Route Settings	YES	-	YES
	Static Multicast Route	YES	-	YES
	Multicast Forwarding Table	YES	-	YES
	Broadcast Forwarding	YES	-	YES
<b>NAT</b>		YES	-	YES



Configuration Section	Function	EDR Series	EDF Series	OnCell Series
<b>Object Management</b>		YES	YES	YES
<b>Firewall</b>		YES	YES	YES
	Layer 2 Policy	YES	YES	YES
	Layer 3-7 Policy	YES	YES	YES
	Malformed Packets	YES	YES	YES
	Session Control	YES	YES	YES
	DoS Policy	YES	YES	YES
	Soft Lockdown Mode	-	-	YES
	Advanced Protection	YES	YES	YES
	Dashboard	YES	YES	YES
	Configuration	YES	YES	YES
	Protocol Filter Policy	YES	YES	YES
	ADP	YES	YES	YES
	IPS	YES	YES	-
<b>VPN</b>		YES	-	YES
	IPSec	YES	-	YES
	L2TP Server	YES	-	-
	OpenVPN Client	YES	-	-
<b>Certificate Management</b>		YES	YES	YES
	Local Certificate	YES	YES	YES
	Trusted CA Certificate	YES	YES	YES
	Certificate Signing Request	YES	YES	YES

Configuration Section	Function	EDR Series	EDF Series	OnCell Series
<b>Security</b>		YES	YES	YES
	Device Security	YES	YES	YES
	Login Policy	YES	YES	YES
	Trusted Access	YES	YES	YES
	SSH & SSL	YES	YES	YES
	Network Security	YES	YES	-
	IEEE 802.1X	YES	-	-
	Authentication	YES	YES	YES
	Login Authentication	YES	YES	YES
	RADIUS	YES	YES	YES
	TACACS+ Server	YES	YES	YES
	MXview Alert Notification	YES	YES	YES
<b>Diagnostics</b>		YES	YES	YES
	System Status	YES	YES	YES
	Utilization	YES	YES	YES
	Fiber Check	YES	-	-
	Network Status	YES	YES	YES
	Network Statistics	YES	YES	YES
	LLDP	YES	YES	YES
	ARP Table	YES	YES	YES
	Event Log and Notifications	YES	YES	YES
	Event Log	YES	YES	YES

Configuration Section	Function	EDR Series	EDF Series	OnCell Series
	Event Notifications	YES	YES	YES
	Syslog	YES	YES	YES
	SNMP Trap/Inform	YES	YES	YES
	Email Settings	YES	YES	YES
	SMS Settings	-	YES	YES
	Tools	YES	YES	YES
	Port Mirroring	YES	-	-
	Ping	YES	YES	YES
	Diagnostic Support	-	-	YES
	Netflow	YES	YES	-

## System Event List

This is a list of system events and their descriptions.

System Event	Description
<b>Cold Start</b>	Power was cut off and then reconnected.
<b>Warm Start</b>	The Moxa industrial secure router was rebooted, such as when network parameters are changed (IP address, netmask, etc.).
<b>Power 1 Transition (On-&gt;Off)</b>	The Moxa industrial secure router's power 1 is powered down.
<b>Power 1 Transition (Off-&gt;On)</b>	The Moxa industrial secure router's power 1 is powered up.
<b>Power 2 Transition (On-&gt;Off)</b>	The Moxa industrial secure router's power 2 is powered down.
<b>Power 2 Transition (Off-&gt;On)</b>	The Moxa industrial secure router's power 2 is powered up.

System Event	Description
<b>Digital Input Transition (On-&gt;Off)</b>	The Moxa industrial secure router's input is turning off.
<b>Digital Input Transition (Off-&gt;On)</b>	The Moxa industrial secure router's input is turning on.
<b>Configuration Changed</b>	A configuration setting was changed.
<b>Login Failure</b>	An incorrect password was entered.
<b>802.1X Authentication Failure</b>	An 802.1X authentication failure occurred.
<b>Firmware Upgrade Success</b>	Firmware upgrade was successful.
<b>Firmware Upgrade Failure</b>	An error occurred during the firmware upgrade.
<b>Log Service Ready</b>	Log service is ready.
<b>Ring/RSTP Topology Changed</b>	The Ring/RSTP topology was changed.
<b>Master Mismatch</b>	A Turbo Ring Master mismatch occurred.
<b>Coupling Topology Changed</b>	The Coupling topology was changed.
<b>VRRP State Change</b>	The VRRP state was changed.
<b>VPN Connected</b>	VPN has been connected.
<b>VPN Disconnected</b>	VPN has been disconnected.
<b>Firewall Policy</b>	A firewall policy failure occurred.
<b>PoE PD On</b>	PoE
<b>PoE PD Off</b>	Port#N PD power on.
<b>Over Measured Power limitation</b>	Port#N PD power off.
<b>PoE FETBad</b>	PD Port#N MOSFET is bad.

System Event	Description
<b>PoE Over Temperature</b>	The temperature of the environment exceeds the maximum operating temperature of the router.
<b>PoE VEE Uvlo</b>	VEE (PoE input voltage) under Voltage Lockout. The voltage of the power supply has dropped below 44V DC.
<b>PoE PD Over Current</b>	Current of Port#N has exceeded the safety limit.
<b>PoE PD Check Fail</b>	The router does not receive a PD response from Port#N after the defined period for specific time cycles.
<b>Over Allocated Power limitation</b>	The total PD power consumption exceeds the total allocated power.

## System Log Events

This table shows the related names, descriptions, and tag/program categories of different system log events.

Event	Log Description	Tag/Program
<b>COLD_START</b>	System has performed a cold start.	System
<b>WARM_START</b>	System has performed a warm start.	System
<b>POW_OFF</b>	Power {{index}} has turned off.	System
<b>POW_ON</b>	Power {{index}} has turned on.	System
<b>DI_ON</b>	Digital Input {{index}} has turned on.	System
<b>DI_OFF</b>	Digital Input {{index}} has turned off.	System
<b>AP_CONFIG</b>	Configurations {{modules}} have been changed by [Account:{{user_name}}].	System
<b>AP_ENABLE</b>	Configurations {{modules}} have been Enabled by [Account:{{user_name}}].	System

Event	Log Description	Tag/Program
<b>AP_DISABLE</b>	Configurations {{modules}} have been Disabled by [Account:{{user_name}}].	System
<b>LINK_ON</b>	Port {{number}} link up.	System
<b>LINK_OFF</b>	Port {{number}} link down.	System
<b>IP_CHG</b>	Network Interface IP have been changed by [Account:{{user_name}}].	System
<b>AUTH_FAIL</b>	[Account:{{user_name}}] log in failed.	System
<b>AUTH_OK_LOGIN_SUCCESS</b>	[Account:{{user_name}}] successfully logged.	System
<b>AUTH_CHANGE</b>	Device SSL & SSH Key/Cert Change(re-generate)	System
<b>TOPOLOGY_CHANGE</b>	Topology has been changed	TurboRingV2
<b>MASTER_MISMATCH</b>	Ring {{Index}} master setting does not match.	TurboRingV2
<b>MRR_COUPLING_TC</b>	Coupling path status has changed.	TurboRingV2
<b>FW_UPGRADE_SUCCESS</b>	Firmware Successfully Upgraded.	System
<b>FW_UPGRADE_FAIL</b>	Firmware Upgrade Fail.	System
<b>CONFIG_IMPORT_FAIL</b>	Configuration import has {{'failed'}} by [Account:{{user_name}}].	System
<b>CONFIG_EXPORT_SUCCESS</b>	Configuration export {{successful}} by [Account:{{user_name}}].	System
<b>CONFIG_IMPORT_SUCCESS</b>	Configuration import has {{'successful'}} by [Account:{{user_name}}].	System
<b>VRRP_STATE_CHANGE</b>	VRRP Virtual Router state change	System
<b>DOT1X_AUTH_FAIL</b>	{{mac address}} authentication failed on port {{number}}.	IEEE802.1X

Event	Log Description	Tag/Program
<b>FIREWALL_POLICY</b>	Firewall Rule Hit Log(Firewall, Trust Access, DOS)	
<b>AUTH_OK_BUT_SESSION_FULL</b>	[Account:{{user_name}}] locked due to {{session_number}} failed login attempts.	System
<b>AUTH_OK_BUT_LOCKOUT</b>	[Account:{{user_name}}] locked due to {{failed_times}} failed login attempts.	System
<b>OOM_OCCURRED</b>	Kernel OOM Occurred	System
<b>FIBER_CHECK</b>	Fiber Check Warning	Port
<b>SYSLOG_NG_LEAK</b>	Clear memory cache (syslog agent)	System
<b>IEC61375_TTDP_STATUS_CHANGE</b>	TTDP Status Change	IEC61375
<b>IEC61375_ECSP_STATUS_CHANGE</b>	ECSP Status Change	IEC61375
<b>POE_PD_ON</b>	Port#N PD power on.	PoE
<b>POE_PD_OFF</b>	Port#N PD power off.	PoE
<b>POE_EXCEED_SYSTEM_THRESHOLD</b>	The total PD power consumption exceeds the total measured power limit.	PoE
<b>POE_FETBAD</b>	PD Port#N MOSFET bad.	PoE
<b>POE_OVER_TEMPERATURE</b>	The temperature of the environment exceeds the maximum operating temperature of the router.	PoE
<b>POE_VEE_UVLO</b>	VEE (PoE input voltage) under Voltage Lockout. The voltage of the power supply has dropped below 44V DC.	PoE
<b>POE_PD_OVER_CURRENT</b>	Current of Port#N has exceeded the safety limit.	PoE
<b>POE_PDCHECK_FAIL</b>	The router does not receive a PD response from Port#N after the defined period for specific time cycles.	PoE
<b>POE_EXCEED_POWER_BUDGET</b>	The total PD power consumption exceeds the total allocated power.	PoE

Event	Log Description	Tag/Program
<b>ROOT_CHANGE</b>	New Root has been elected in topology.	RSTP
<b>SECURITY_NOTIFICATION_DEVICELOCKDOWN</b>	Hit Device Lockdown Rule	System
<b>DEVICE_LOCKDOWN_STATE_CHANGE</b>	Configurations {{Device Lockdown State(on/off)}} have been changed by [Account:{{user_name}}].	System
<b>VPN_LOG</b>	IPSec connection log	VPN
<b>LFP_ON</b>	Link Fault Passthrough is triggered.	LFP
<b>LFP_OFF</b>	Link Fault Passthrough is cleared.	LFP
<b>WAN_INTERFACE_CHANGE</b>	The selected WAN interface in WAN Backup is changed, it means the default gateway is also changed.	WAN Backup
<b>WAN_INTERFACE_PING_FAIL</b>	The ping check of the WAN interface in WAN Backup is failed.	WAN Backup

## TRDP Message Type List

### Configuration attribute requirements - msgType

This is a list of TRDP msgTypes and their descriptions.

msgType	Description
<b>Pr</b>	PD Request
<b>Pp</b>	PD Reply
<b>Pd</b>	PD Data
<b>Pe</b>	PD Data (Error)
<b>Mn</b>	Notification (Request without reply)
<b>Mr</b>	MD Request with reply
<b>Mp</b>	MD Reply without confirmation



msgType	Description
<b>Mq</b>	MD Reply with confirmation
<b>Mc</b>	MD Confirm
<b>Me</b>	MD error

## Configuration attribute requirements - msgType Profile

This is a list of TRDP msgType profiles and their descriptions.

Profile	Description
<b>PD-PDU</b>	A collection of "Pr, Pp, Pd, Pe"
<b>MD-PDU</b>	A collection of "Mn, Mr, Mp, Mq, Mc, Me"

## TRDP Protocol Filter Profile List

This is a list of the different built-in protocol filter profiles for common applications and their corresponding message types and communication identifiers.

Protocol Filter Profile	Message Type	Communication Identifier (ComID)
<b>PD-PDU</b>	0x5072: PD Request, 0x5070: PD Reply, 0x5064: PD Data, 0x5065: PD Data (Error)	All
<b>MD-PDU</b>	0x4D6E: Notification (Request without reply), 0x4D72: MD Request with reply, 0x4D70: MD Reply without confirmation, -x4D71: MD Reply with confirmation, 0x4D63: MD Confirm, 0x4D65: MD error	All
<b>Communication Framework and ETB Control Service</b>	All	1-29, 50-79, 150-199
<b>TRDP statistics data</b>	All	30-41
<b>Conformance test</b>	All	80-99
<b>TTDB</b>	All	100-119
<b>ECSP</b>	All	120-129

Protocol Filter Profile	Message Type	Communication Identifier (ComID)
ETBN	All	130-139
TCN-DNS	All	140-149

## User Role Privileges

This page shows the privilege levels granted to the different authority levels: Admin, Supervisor, and User. Refer to System > Account Management > User Accounts for more information on user accounts.

Privileges are indicated as follows:

- **R/W**: Read and write access granted for the relevant settings
- **R**: Read-only access granted for the relevant settings
- **-**: No access granted for the relevant settings

### Note

Available settings and options will vary depending on the product model.

## System

Settings	Admin	Supervisor	User
<b>System Management</b>			
Information Settings	R/W	R/W	R
Firmware Upgrade	R/W	-	-
Software Package Management	R/W	-	-
Configuration Backup and Restore	R/W	-	-
<b>Account Management</b>			
User Account	R/W	-	-

Settings	Admin	Supervisor	User
<b>Password Policy</b>	R/W	-	-
<b>License Management</b>	R/W	R	R
<b>Management Interface</b>			
<b>Out of Band Management</b>	R/W	R/W	R
<b>User Interface</b>	R/W	R/W	R
<b>Hardware Interface</b>	R/W	R/W	R
<b>SNMP</b>	R/W	-	-
<b>Moxa Remote Connect</b>	R/W	-	-
<b>MXsecurity</b>	R/W	R/W	-
<b>Time</b>			
<b>System Time</b>	R/W	R/W	R
<b>NTP/SNTP Server</b>	R/W	R/W	R
<b>Power Management</b>	R/W	R/W	R
<b>SMS</b>	R/W	R/W	R
<b>GNSS</b>	R/W	R/W	R
<b>Setting Check</b>	R/W	R/W	R

## Cellular

Settings	Admin	Supervisor	User
<b>Cellular</b>	R/W	R/W	R

## Serial

Settings	Admin	Supervisor	User
<b>Serial</b>	R/W	R/W	R

## Network Configuration

Settings	Admin	Supervisor	User
<b>Ports</b>			
Port Settings	R/W	R/W	R
Link Aggregation	R/W	R/W	R
PoE	R/W	R/W	R
Link Fault Passthrough	R/W	R/W	R
LAN Bypass Gen3	R/W	R/W	R
<b>Layer 2 Switching</b>			
VLAN	R/W	R/W	R
MAC Address Table	R/W	R/W	R
QoS	R/W	R/W	R
Rate Limit	R/W	R/W	R
Multicast	R/W	R/W	R
Network Interfaces	R/W	R/W	R

## Redundancy

Settings	Admin	Supervisor	User
<b>Layer 2 Redundancy</b>			
Spanning Tree	R/W	R/W	R
Turbo Ring V2	R/W	R/W	R
Turbo Chain	R/W	R/W	R
<b>Layer 3 Redundancy</b>			
VRRP	R/W	R/W	R

Settings	Admin	Supervisor	User
----------	-------	------------	------

<b>WAN Redundancy</b>	R/W	R/W	R
-----------------------	-----	-----	---

## Network Service

Settings	Admin	Supervisor	User
----------	-------	------------	------

<b>DHCP Server</b>	R/W	R/W	R
--------------------	-----	-----	---

<b>Dynamic DNS</b>	R/W	R/W	R
--------------------	-----	-----	---

## Routing

Settings	Admin	Supervisor	User
----------	-------	------------	------

### Unicast Routing

<b>Static Routes</b>	R/W	R/W	R
----------------------	-----	-----	---

<b>RIP</b>	R/W	R/W	R
------------	-----	-----	---

<b>OSPF</b>	R/W	R/W	R
-------------	-----	-----	---

<b>Routing Table</b>	R	R	R
----------------------	---	---	---

### Multicast Route

<b>Multicast Route Settings</b>	R/W	R/W	R
---------------------------------	-----	-----	---

<b>Static Multicast Route</b>	R/W	R/W	R
-------------------------------	-----	-----	---

<b>Multicast Forwarding Table</b>	R	R	R
-----------------------------------	---	---	---

<b>Broadcast Forwarding</b>	R/W	R/W	R
-----------------------------	-----	-----	---

## NAT

Settings	Admin	Supervisor	User
----------	-------	------------	------

<b>NAT</b>	R/W	R/W	R
------------	-----	-----	---

## Object Management

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

## Firewall

Settings	Admin	Supervisor	User
Layer 2 Policy	R/W	R/W	R
Layer 3 - 7 Policy	R/W	R/W	R
Malformed Packets	R/W	R/W	R
Session Control	R/W	R/W	R
DoS Policy	R/W	R/W	R
Soft Lockdown Mode	R/W	R/W	R
Advanced Protection			
Dashboard	R/W	R/W	-
Configuration	R/W	R/W	-
Protocol Filter Policy	R/W	R/W	-
ADP	R/W	R/W	-
IPS	R/W	R/W	-

## VPN

Settings	Admin	Supervisor	User
IPsec	R/W	R/W	R
L2TP Server	R/W	R/W	R
OpenVPN Client	R/W	R/W	-

## 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
<b>Device Security</b>			
Login Policy	R/W	R	R
Trusted Access	R/W	R/W	R
SSH & SSL	R/W	R/W	-
<b>Network Security</b>			
IEEE 802.1X	R/W	R/W	R
<b>Authentication</b>			
Login Authentication	R/W	-	-
RADIUS	R/W	-	-
TACACS+	R/W	-	-
MXview Alert Notification	R/W	R/W	R

## Diagnostics

Settings	Admin	Supervisor	User
<b>System Status</b>			
Utilization	R/W	R/W	R
Fiber Check	R/W	R/W	R

Settings	Admin	Supervisor	User
<b>Network Status</b>			
<b>Network Statistics</b>	R	R	R
<b>LLDP</b>	R/W	R/W	R
<b>ARP Table</b>	R	R	R
<b>Event Log &amp; Notifications</b>			
<b>Event Log</b>	R/W	R/W	R
<b>Event Notifications</b>	R/W	R/W	R
<b>Syslog</b>	R/W	R	R
<b>SNMP Trap/Inform</b>	R/W	-	-
<b>Email Settings</b>	R/W	R	R
<b>SMS Settings</b>	R/W	R/W	R
<b>Tools</b>			
<b>Port Mirroring</b>	R/W	R/W	R
<b>Ping</b>	R/W	R/W	R
<b>Diagnostic Support</b>	R/W	R/W	R
<b>NetFlow</b>	R/W	R/W	R



**MOXA<sup>®</sup>**

**Moxa Inc.**

Copyright © 2024 Moxa, Inc. All rights reserved. Reproduction without permission is prohibited. Trademarks and logos are copyrights of their respective owners.

[www.moxa.com/products](http://www.moxa.com/products)