EDR-G9010 Series User Manual

Version 2.0, September 2022

www.moxa.com/products

EDR-G9010 Series User Manual

Copyright Notice

Trademarks

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction

Welcome to the Moxa EDR-G9010 Industrial Secure Router Series. These all-in-one Firewall/NAT/VPN secure routers are designed for connecting Ethernet-enabled devices with network IP security.

Overview

As the world's network and information technology becomes more mature, the trend is to use Ethernet as the major communications interface in many industrial communications and automation applications. In fact, an entirely new industry has sprung up to provide Ethernet products that comply with the requirements of demanding industrial applications.

Moxa's Industrial Secure Router series is a Gigabit speed, all-in-one Firewall/VPN/Router for Ethernet security applications in sensitive remote control and monitoring networks.

The Quick Automation Profile function of the Industrial Secure Router's firewall supports most common Fieldbus protocols, including EtherCAT, EtherNet/IP, FOUNDATION Fieldbus, Modbus/TCP, and PROFINET. Users can easily create a secure Ethernet Fieldbus network from a user-friendly web UI with a single click. In addition, wide temperature models are available that operate reliably in hazardous, -40 to 75°C environments.

The EDR-G9010 Series is a set of highly integrated industrial multi-port secure routers with firewall/NAT/VPN and managed Layer 2 switch functions. These devices are designed for Ethernet-based security applications in critical remote control or monitoring networks. These secure routers provide an electronic security perimeter to protect critical cyber assets including substations in power applications, pump-and-treat systems in water stations, distributed control systems in oil and gas applications, and PLC/SCADA systems in factory automation.

Package Checklist

The Industrial Secure Routers are shipped with the following items. If any of these items are missing or damaged, please contact your customer service representative for assistance.

- 1 Moxa Industrial Secure Router
- USB-C-to-DB9 cable
- Protective caps for unused ports
- DIN-rail mounting kit (attached to the Industrial Secure Router's rear panel by default)
- Quick installation guide (printed)
- Warranty card

Features

- 10-port Gigabit all-in-one firewall/NAT/VPN/router/switch
- Industrial-grade Intrusion Prevention/Detection System (IPS/IDS)
- Visualize OT security with the MXsecurity management software
- Secure remote access tunnel with VPN
- Examine industrial protocol data with Deep Packet Inspection (DPI) technology
- Easy network setup with Network Address Translation (NAT)
- RSTP/Turbo Ring redundant protocol enhances network redundancy
- Security features based on IEC 62443/NERC CIP
- Supports secure boot for checking system integrity
- -40 to 75°C operating temperature range (-T model)

Defend Against Malicious Threats With Advanced Cybersecurity Features

The EDR-G9010 Series' embedded firewall uses policy rules to control network traffic between trusted zones while Network Address Translation (NAT) shields the internal network from unauthorized access by outside hosts. The Virtual Private Networking (VPN) functionality further provides users with secure communication tunnels when accessing the private network from the public Internet. To help protect your OT assets from cyberattacks, the EDR-G9010 Series supports Deep Packet Inspection (DPI) to examine the data portion of network packets for various OT-specific protocols.

Simplify Configurations With the User-friendly Interface and Quick Settings

The EDR-G9010 Series' "Interface Type Quick Settings" provide an easy way for users to set up WAN, LAN, and Bridge ports for routing functionality in just four steps. In addition, the "Quick Automation Profile" feature gives engineers a simple way to configure the firewall filtering function for general automation protocols, including EtherNet/IP, Modbus TCP, EtherCAT, FOUNDATION Fieldbus, and PROFINET.

Industrial-grade Design to Ensure Uninterrupted Network Connectivity

The EDR-G9010 Series' rugged hardware makes these secure routers ideal for harsh industrial environments, featuring wide-temperature models that are built to operate reliably in hazardous conditions and extreme temperatures of -40 up to 75°C. Moreover, the EDR-G9010 Series supports comprehensive Layer 2 and Layer 3 redundancy mechanisms to ensure that your network stays connected at all times.

Virtual Patching and Intelligent Threat Protection

Patching remains a major challenge in OT environments because OT applications cannot afford interrupting operations by shutting down systems to apply patches. Virtual patching technology can help complement existing patch management processes by shielding known and unknown vulnerabilities. In addition, the EDR-G9010 features intelligent IPS functionality for continuous protection against cyberthreats which uses pattern-based detection to identify and block known attacks.

2. Getting Started

This chapter explains how to access the Industrial Secure Router for the first time. There are three ways to access the router: (1) serial console, (2) Telnet console, and (3) web browser. The serial console connection method, which requires using a short serial cable to connect the Industrial Secure Router to a PC's COM port, can be used if you do not know the Industrial Secure Router's IP address. The Telnet console and web browser connection methods can be used to access the Industrial Secure Router over an Ethernet LAN, or over the Internet. A web browser can be used to perform all monitoring and administration functions, but the serial console and Telnet console only provide basic functions.

RS-232 Console Configuration (115200, None, 8, 1, VT100)

ATTENTION

We strongly suggest that you do NOT use more than one connection method at the same time. Following this advice will allow you to maintain better control over the configuration of your Industrial Secure Router.

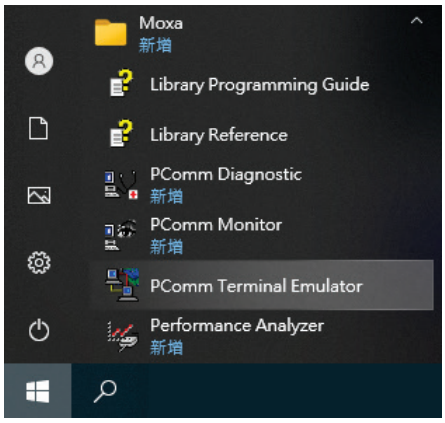
NOTE

We recommend using Moxa PComm Terminal Emulator, which can be downloaded free of charge from Moxa's website.

Before running PComm Terminal Emulator, use a USB-C-to-DB9-F (or USB-C-to-DB25-F) cable to connect the Industrial Secure Router's RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).

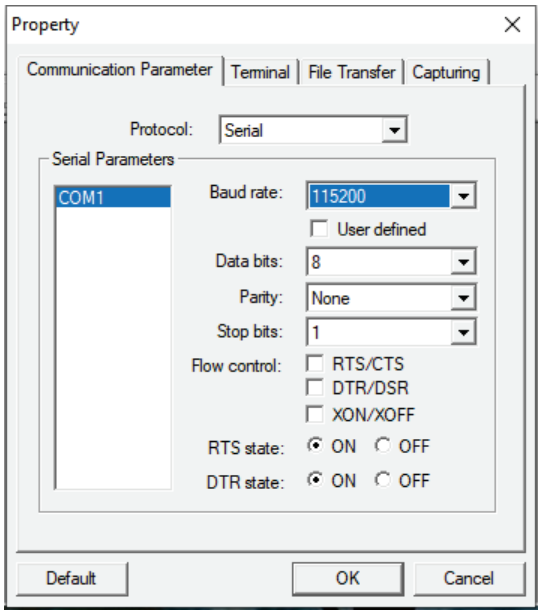
After installing PComm Terminal Emulator, perform the following steps to access the RS-232 console utility.

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

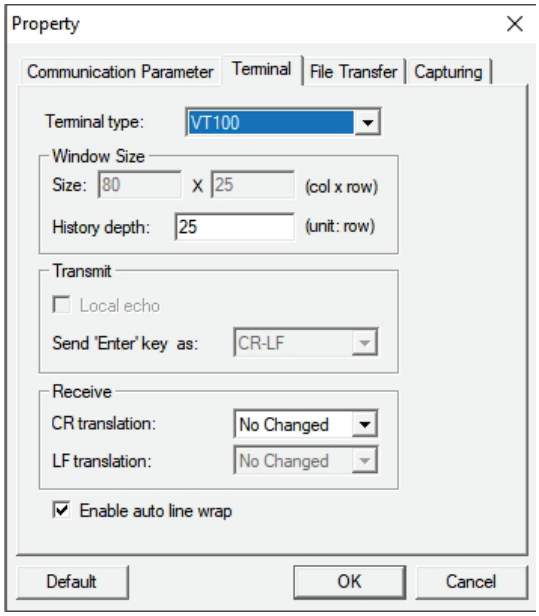


2. Click **Open** in the Port Manager menu to open a new connection.

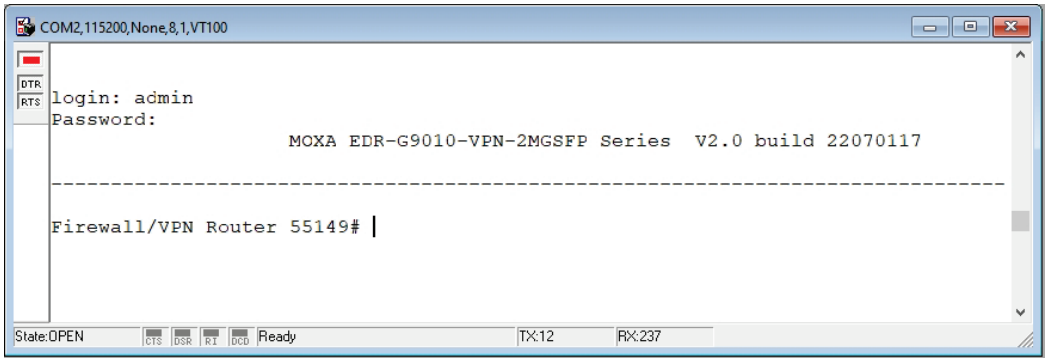
3. The **Communication Parameter** page of the **Property** window will appear. Select the appropriate COM port from the **Serial Parameters** list and configure the following values:
Baud Rate: 115200
Data Bits: 8,
Parity: None
Stop Bits: 1.



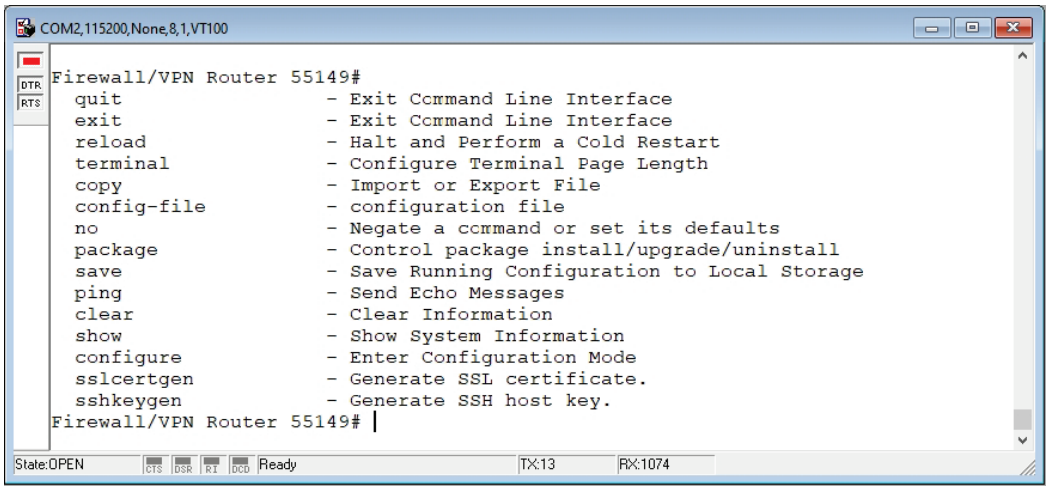
4. Click the **Terminal** tab, select **VT100** for Terminal Type, then click **OK** to continue.



5. The **Console** screen will appear. Press **Enter** to input the login account (**admin** or **user**) and press **Enter** again to jump to the **Password** field. Enter the console password, or if no password has been configured before, enter the default password "**moxa**" and press **Enter**.



6. Enter a question mark (**?**) to display the command list.



The following table lists the commands that can be used when the Industrial Secure Router is in console (serial or Telnet) mode:

Admin Account Commands

Command	Description
quit	Exit the Command Line Interface
exit	Exit the Command Line Interface
reload	Halt and perform a cold restart
terminal	Configure the terminal page length
copy	Import or export a file
config-file	Configure a file
no	Negate a command or reset to its defaults
save	Save the running configuration to flash
ping	Send echo messages
tcpdump	Dump traffic on a network
clear	Clear information
show	Show system information
configure	Enter Configuration Mode
sslcertgen	Generate a SSL certificate
sshkeygen	Generate a SSH host key

Using Telnet to Access the Industrial Secure Router's Console

You may use Telnet to access the Industrial Secure Router's console utility over a network. To access the EDR's functions over the network (by either Telnet or a web browser) from a PC host that is connected to the same LAN as the Industrial Secure Router, you need to make sure that the PC host and the Industrial Secure Router are on the same logical subnet. To do this, check your PC host's IP address and subnet mask. By default, the LAN IP address is 192.168.127.254 and the Industrial subnet mask is 255.255.255.0 (for a Class C subnet). If you do not change these values, and your PC host's subnet mask is 255.255.0.0, then its IP address must have the form 192.168.xxx.xxx. On the other hand, if your PC host's subnet mask is 255.255.255.0, then its IP address must have the form, 192.168.127.xxx.

NOTE

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

NOTE

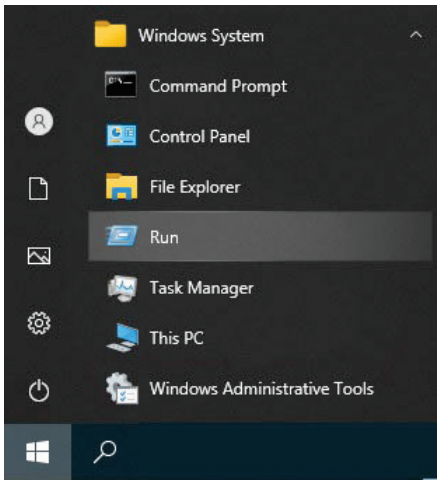
Before accessing the console utility via Telnet, first connect one of the Industrial Secure Router's RJ45 Ethernet LAN ports to your Ethernet LAN, or directly to your PC's Ethernet card (NIC). You can use either a straight-through or cross-over Ethernet cable.

NOTE

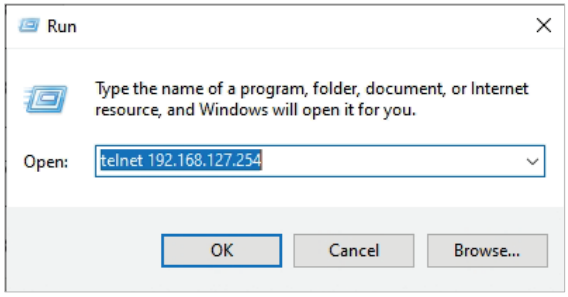
The Industrial Secure Router's default LAN IP address is 192.168.127.254.

Perform the following steps to access the console utility via Telnet.

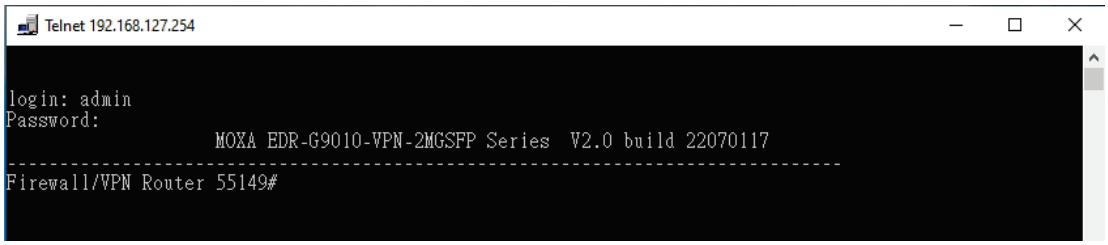
1. Click **Start > Windows System > Run** from the Windows desktop.



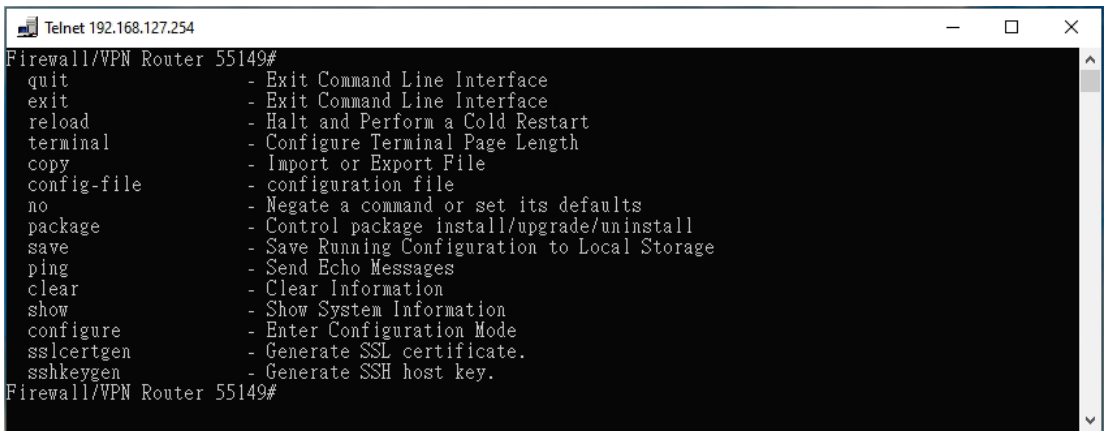
2. Enter "telnet 192.168.127.254" and click **OK** to connect to the Industrial Secure Router's IP address. You may also issue the Telnet command from the MS-DOS prompt.



3. The **Console** login screen will appear. Enter the login account (**admin** or **user**) and press **Enter** to jump to the **Password** field. Enter the console password, or if no password has been configured before, enter the default password "**moxa**" and press **Enter**.



4. Enter a question mark (**?**) to display the command list.



Using a Web Browser to Configure the Industrial Secure Router

The Industrial Secure Router's web browser interface provides a convenient way to modify the router's configuration and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft Internet Explorer 6.0 with JVM (Java Virtual Machine) installed.

NOTE

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

NOTE

Before accessing the Industrial Secure Router's web browser, first connect one of the Industrial Secure Router's RJ45 Ethernet LAN ports to your Ethernet LAN, or directly to your PC's Ethernet card (NIC). You can use either a straight-through or cross-over Ethernet cable.

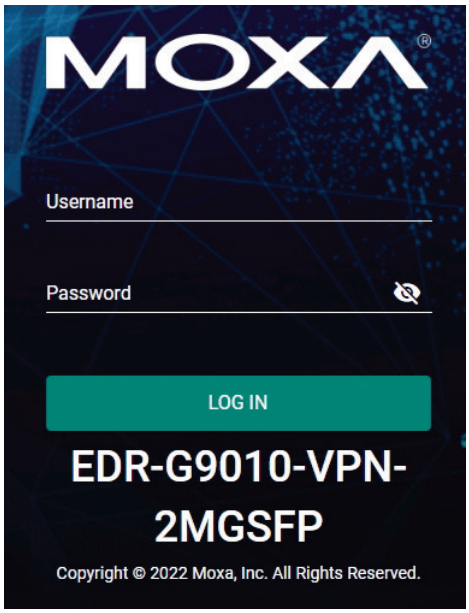
NOTE

The Industrial Secure Router's default LAN IP address is 192.168.127.254.

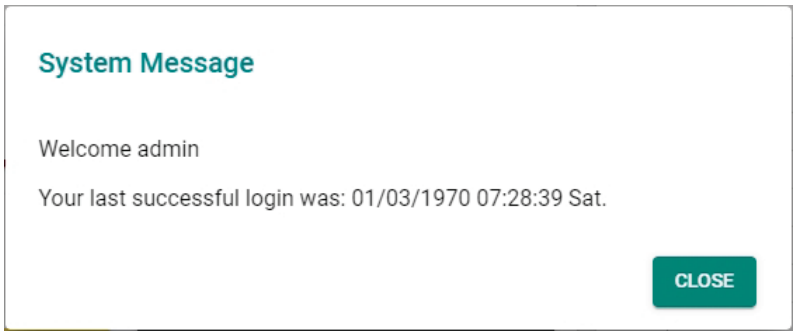
Perform the following steps to access the Industrial Secure Router's web browser interface.

1. Open a web browser and type the Industrial Secure Router's LAN IP address (**192.168.127.254**) in the address bar and press **Enter**.

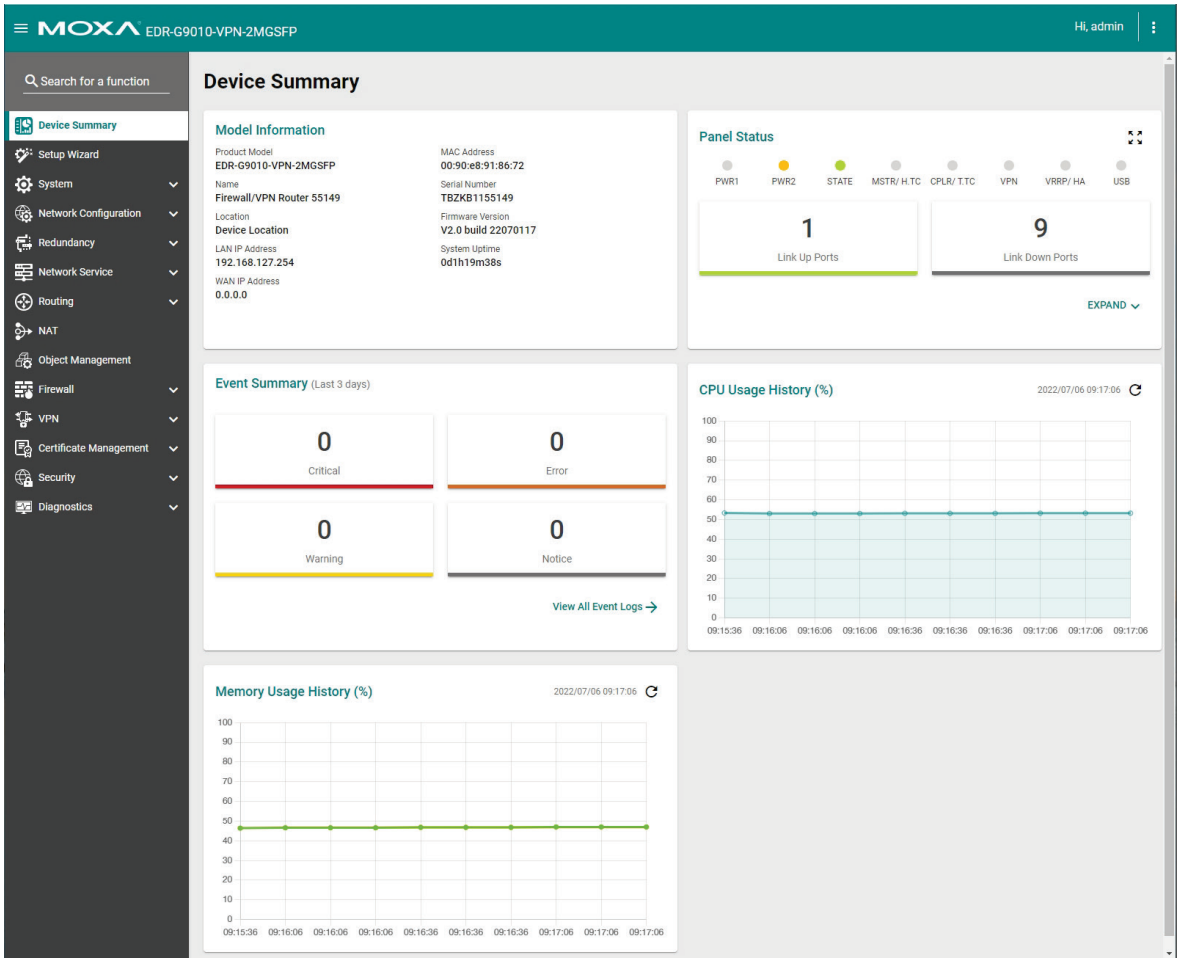
2. The web login page will open. Enter the username (**Admin** or **User**) and password (the same as the Console password) and click **LOG IN** to continue. Enter the default password "**moxa**" if a password has not been set yet.



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.



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.

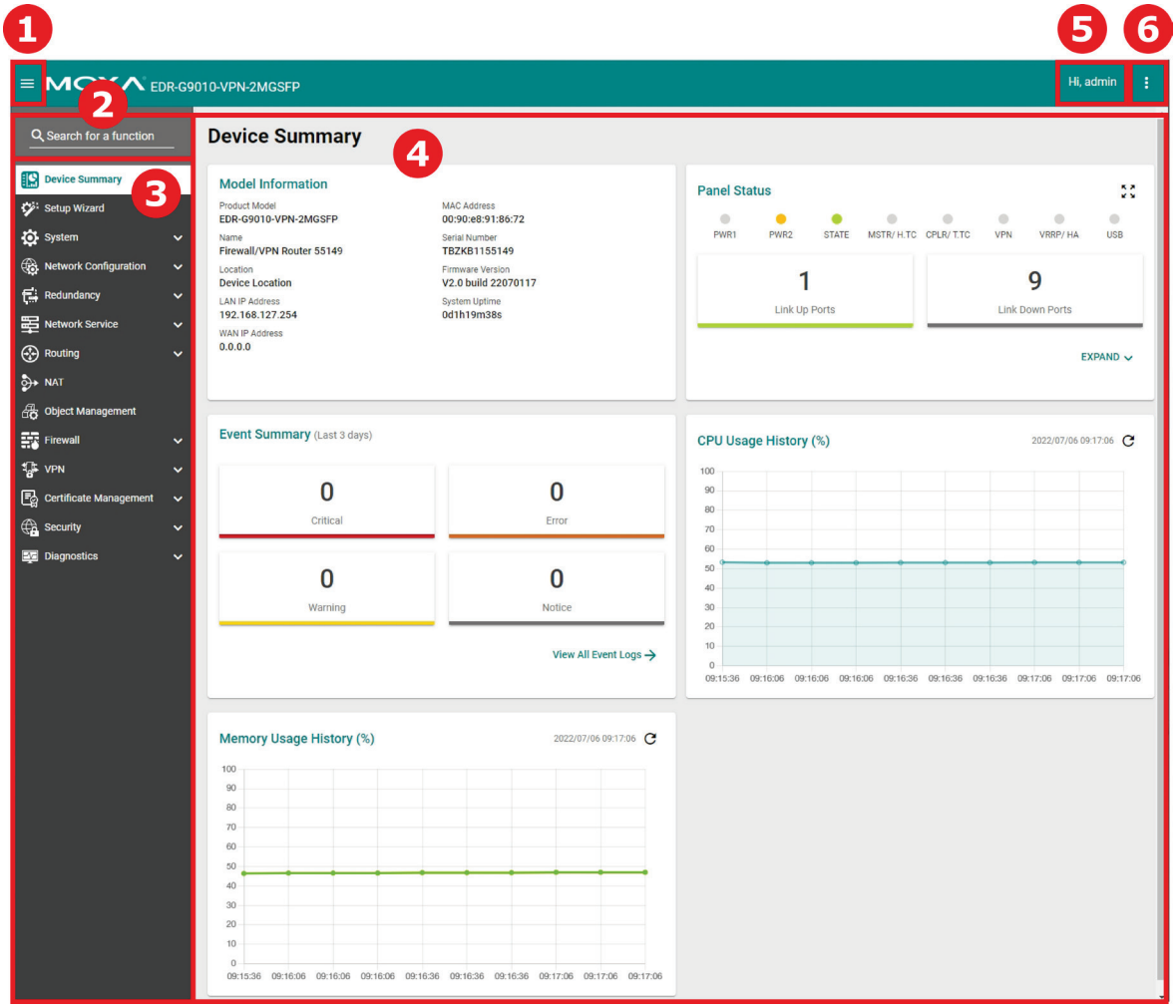


3. Device Summary and Setup Wizard

In this chapter, we explain how to access the Industrial Secure Router's configuration options, perform monitoring, and use administration functions. There are three ways to access these functions: (1) RS-232 console, (2) Telnet console, and (3) web browser.

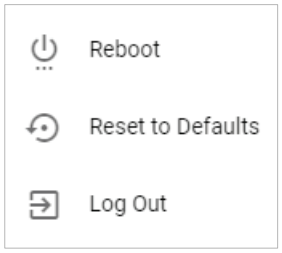
The web browser is the most user-friendly way to configure the Industrial Secure Router since you can both monitor the Industrial Secure Router and use administration functions from the web browser. An RS-232 or Telnet console connection only provides basic functions. In this chapter, we use the web browser to introduce the Industrial Secure Router's configuration and monitoring functions.

Function Introduction

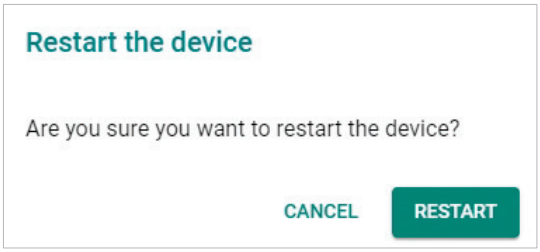


1. Clicking  in the top-left will close or expand the function menu.
2. Enter the name of a function in the **Search Bar** to quickly find a specific function.
3. Click on a function name in the **Function Menu** on the left-hand side to view or configure the function.
4. All the configuration options and information of the selected function will be shown here.
5. This shows the name of the logged in user.

6. Clicking in the top-right will expand the drop-down menu shown below.

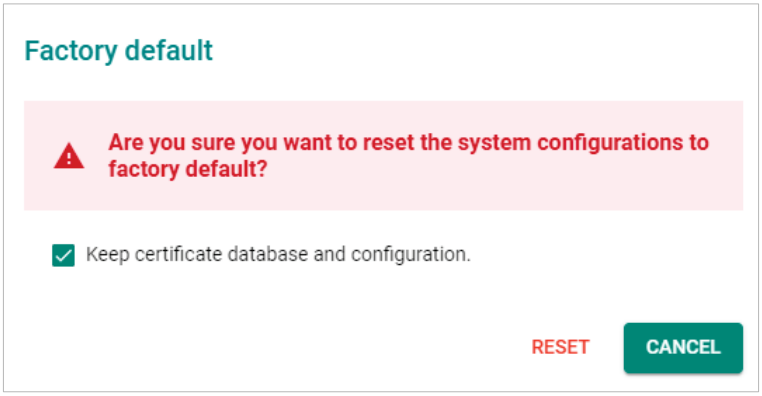


Reboot



Click **RESTART** to reboot the Industrial Secure Router.

Reset to Defaults



The **Reset to Defaults** option gives users a quick way of restoring the Industrial Secure Router's configuration settings to their factory default values. This function is available in both the console utility (serial or Telnet) and the web browser interface.

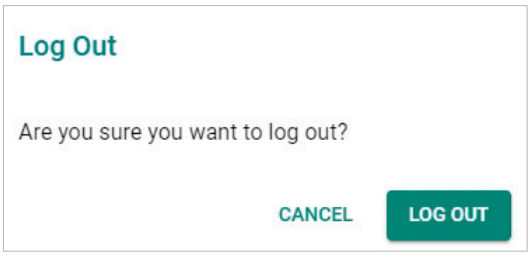
Check the **Keep certificate database and configuration** option to keep certificate database and configuration information. Leaving this option unchecked will delete all information on the device and reset everything to its factory default value.

Click **RESET** to reset the Industrial Secure Router to the factory default settings. Be aware that all your configuration settings will be permanently deleted.

NOTE

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

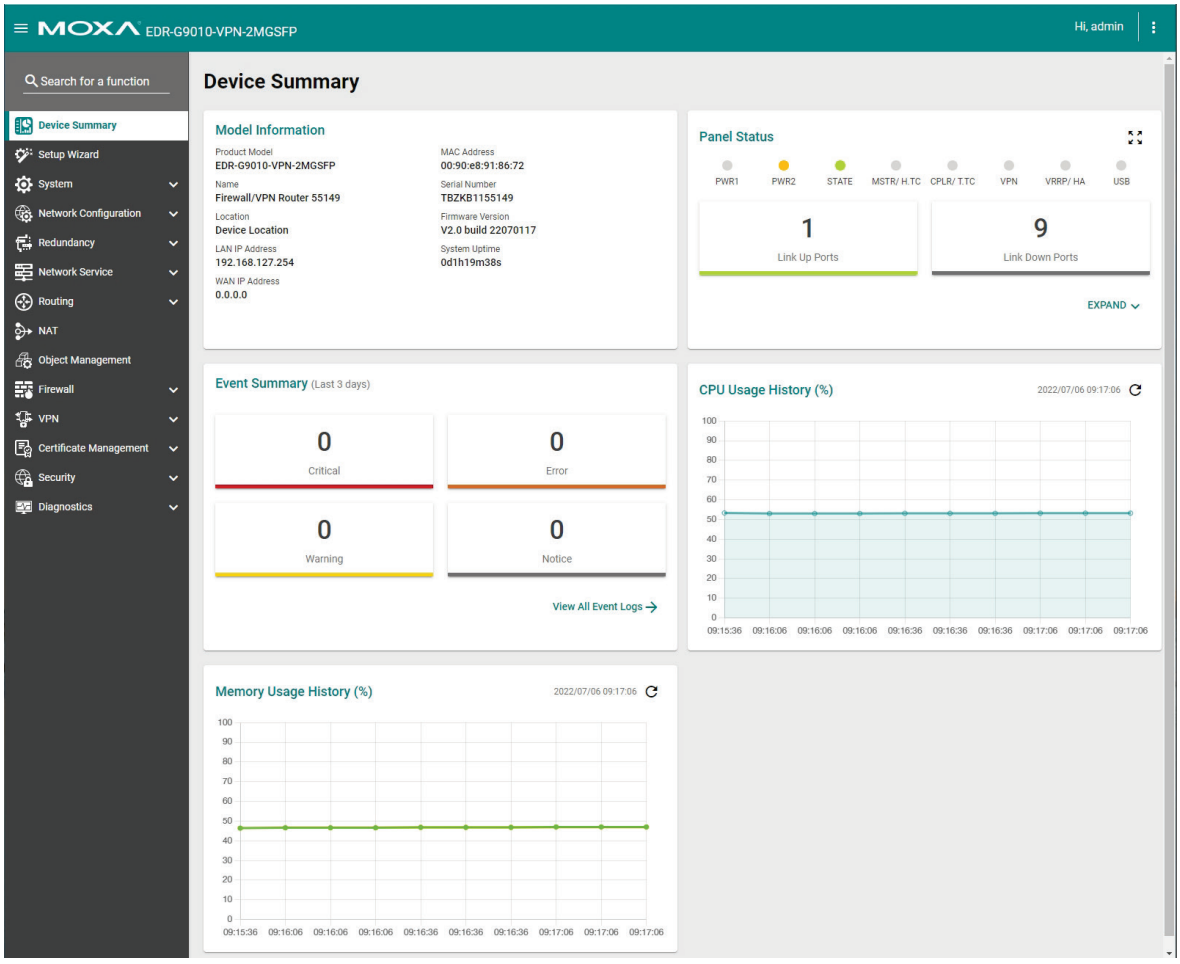
Log Out



Click **LOG OUT** to log out of the Industrial Secure Router.

Device Summary

When logging in to the Industrial Secure Router, you will be presented with the **Device Summary** page. This overview page contains basic activity and performance information of the device. If you are on another configuration page, click **Device Summary** from the Function Menu to jump to the summary page.



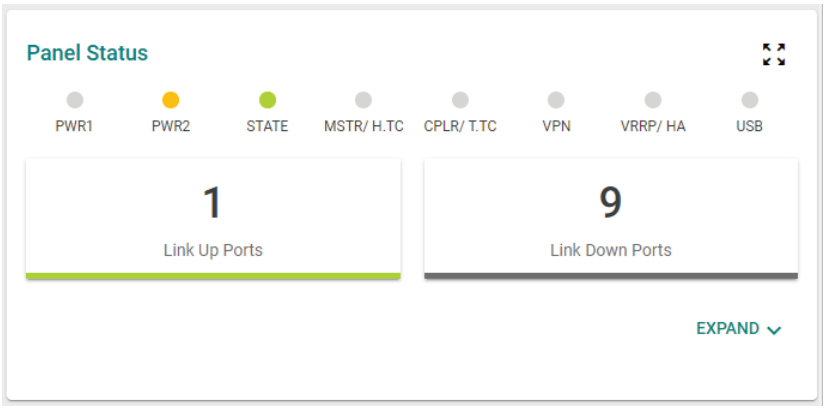
See the following sections for a more detailed description of each widget on the summary page.

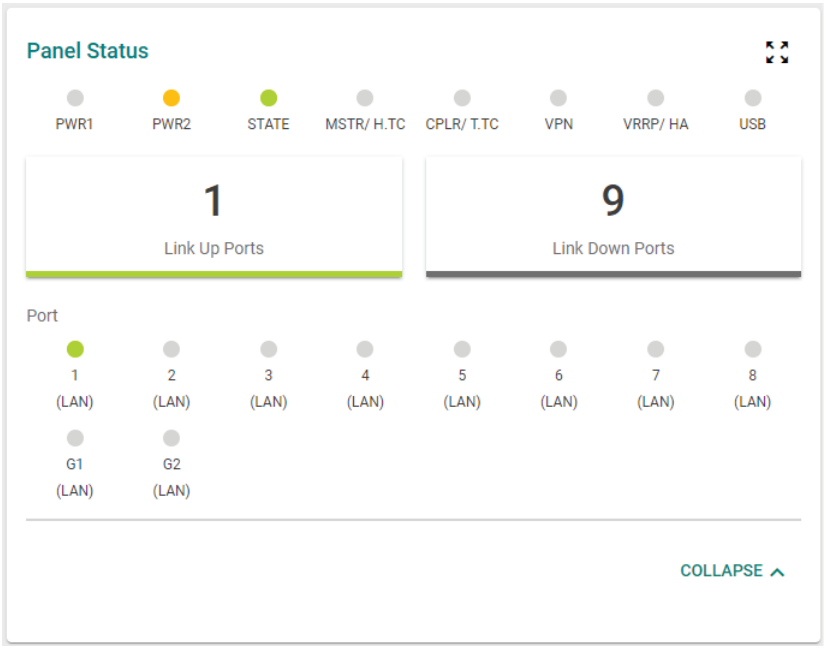
Model Information

This panel shows basic information for the Industrial Secure Router, including product model name, serial number, firmware version, system uptime, etc.

Panel Status

This panel illustrates the panel status. For example, the connecting ports will be shown in green, while the disconnected ports will be shown in gray. Click EXPAND to view more detailed information. Click COLLAPSE to hide the details.





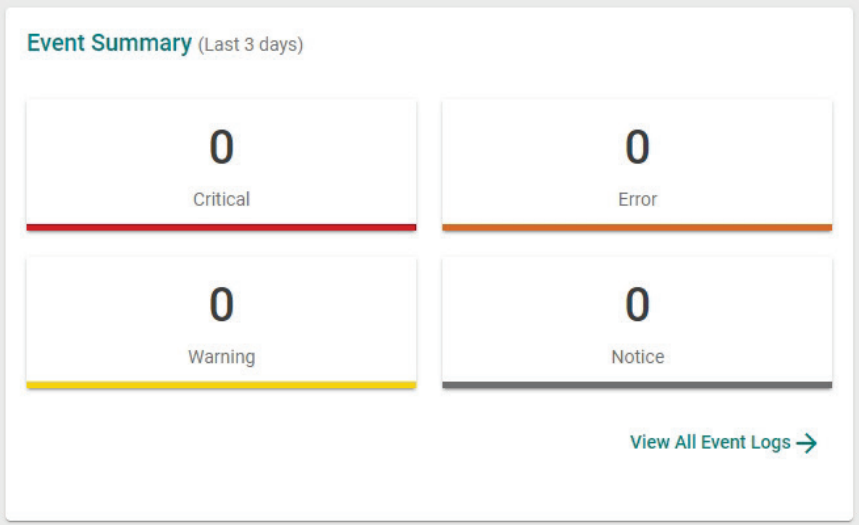
Panel View

Click the ⛶ icon in the Panel Status widget to view the device port status on a representative image of the device. Click the ✕ icon in the upper-right corner to close the panel view.

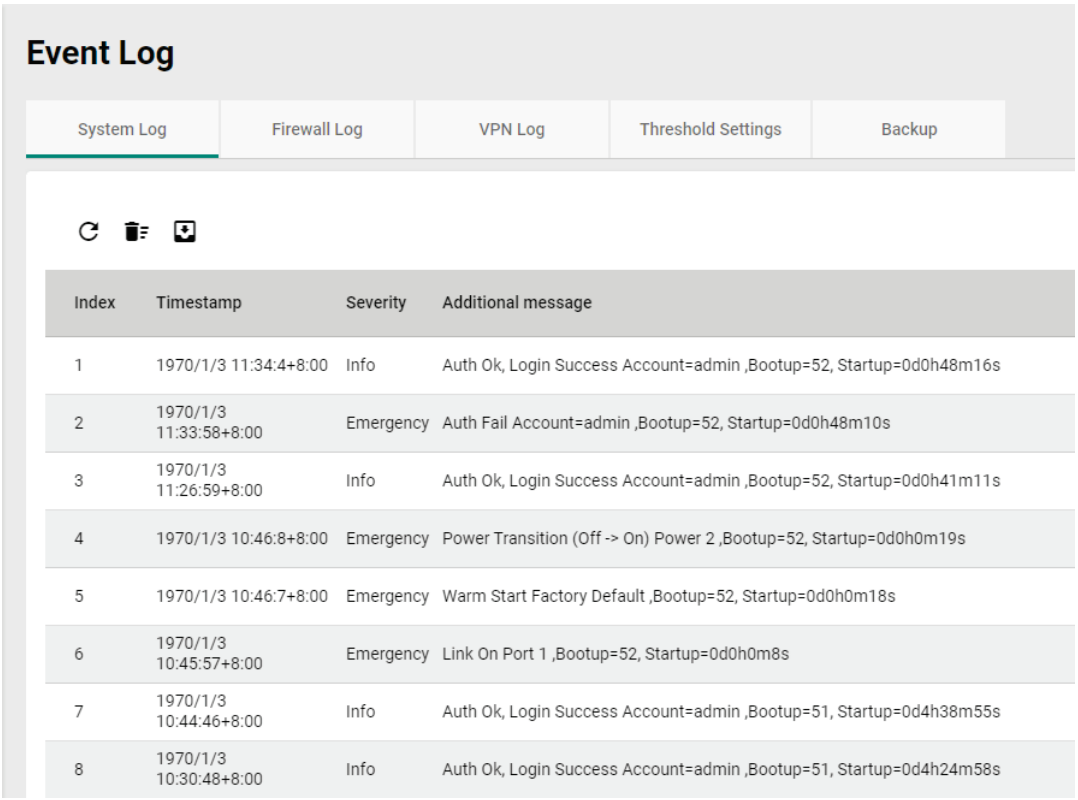
The panel view figure varies depending on the product model you are using.

Event Summary (Last 3 Days)

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



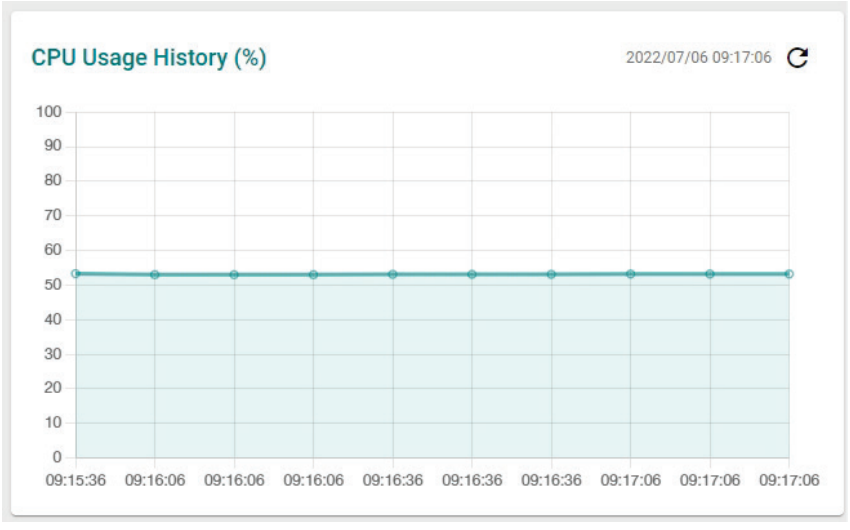
Click View All Event Logs → to go to the Event Log page, where you can view all event logs in more detail.



For Event Log settings, refer to the Event Log section.

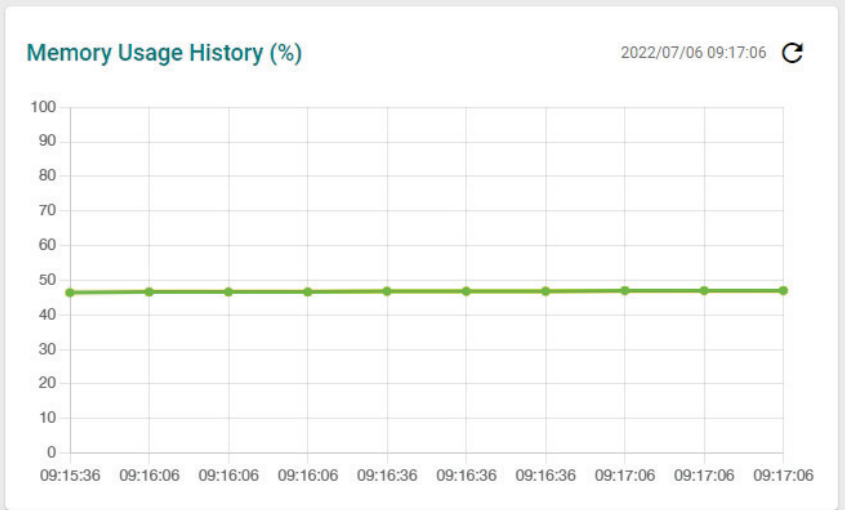
CPU Usage History (%)

This panel shows the device's CPU usage. The data will be shown as a percentage over time. Click the icon to refresh the graph.



Memory Usage History (%)

This panel shows the device's memory usage. The data will be shown as a percentage over time. Click the icon to refresh the graph.

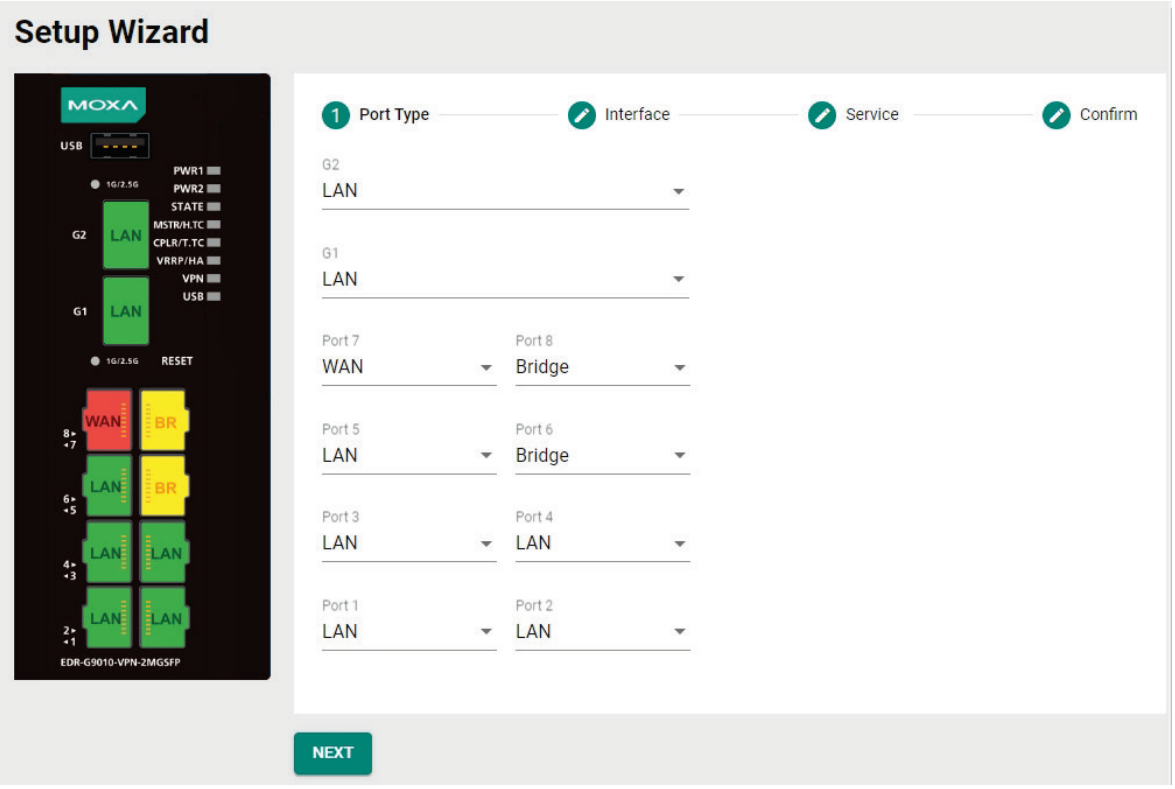


Setup Wizard

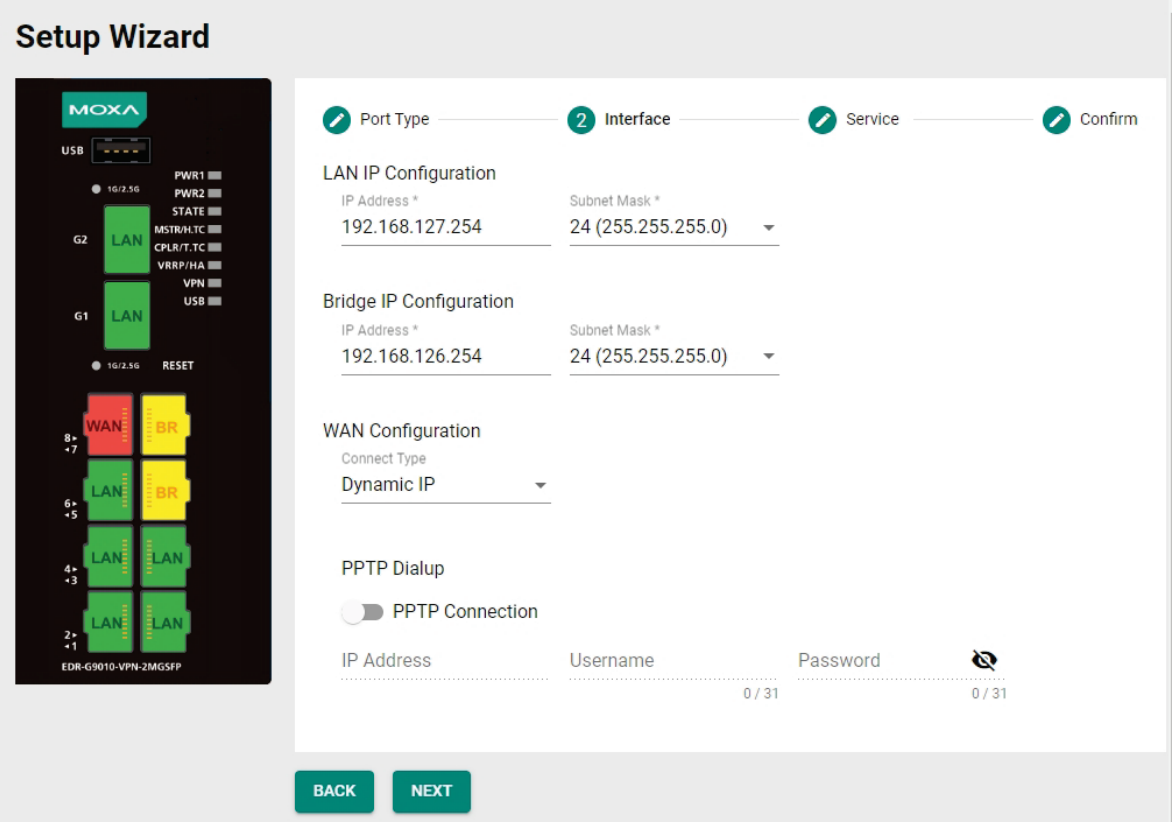
The EDR-G9010 Series supports a Setup Wizard to help you quickly set up routing functionality between the user-defined LAN, WAN, and Bridge ports.

Step 1: Port Type

Select the port type (LAN, WAN, Bridge) for each port from the corresponding drop-down menu.



Step 2: Interface



LAN IP Configuration

Configure the LAN IP address to define the subnet of the LAN ports on the secure router. The default IP address on the LAN side is 192.168.127.254, and the default subnet address is 255.255.255.0.

Bridge IP Configuration

Configure the Bridge LAN Interface IP address to define the subnet of the Bridge LAN ports on the secure router. The default IP address on the Bridge LAN side is 192.168.126.254, and the default subnet address is 255.255.255.0.

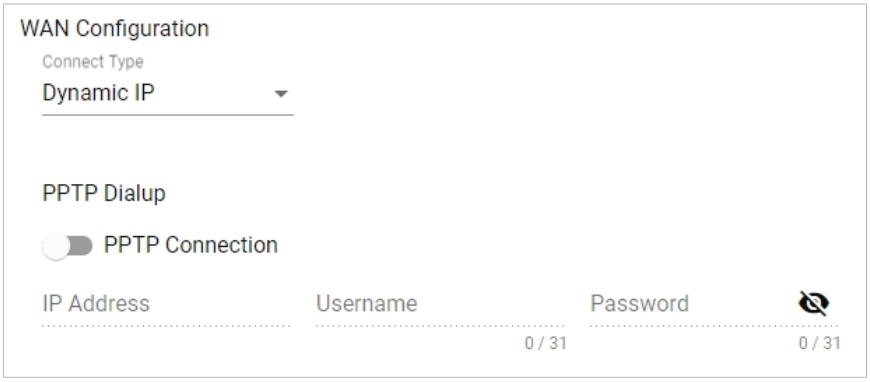
WAN Configuration

Configure the WAN port type to define how the secure router connects to the WAN.

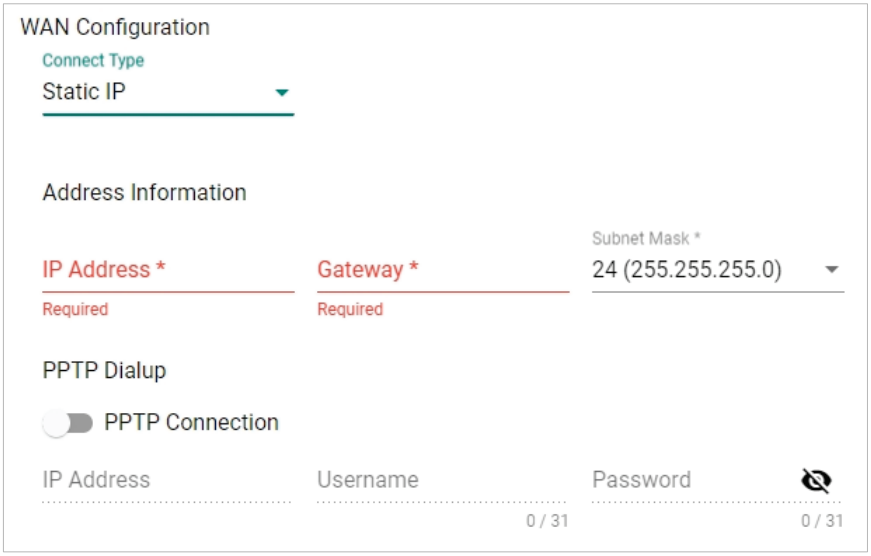
Connect Type

Setting	Description	Factory Default
Dynamic IP	Get the WAN IP address from a DHCP server or via a PPTP connection.	Dynamic IP
Static IP	Specify a static WAN IP address or create a connection to a PPTP server with a specific IP address.	
PPPoE	Get the WAN IP address via PPPoE Dialup.	

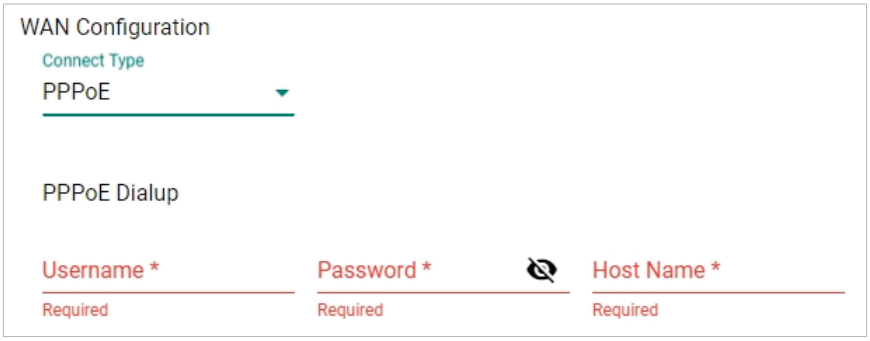
Dynamic IP



Static IP

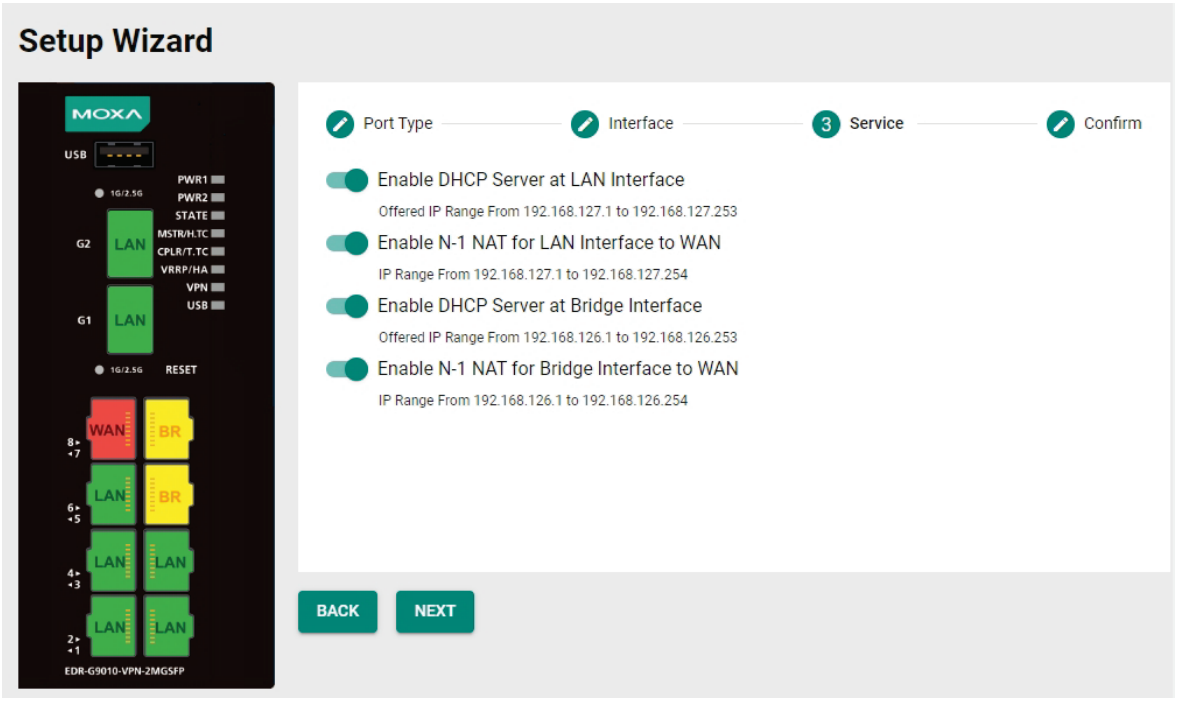


PPPoE



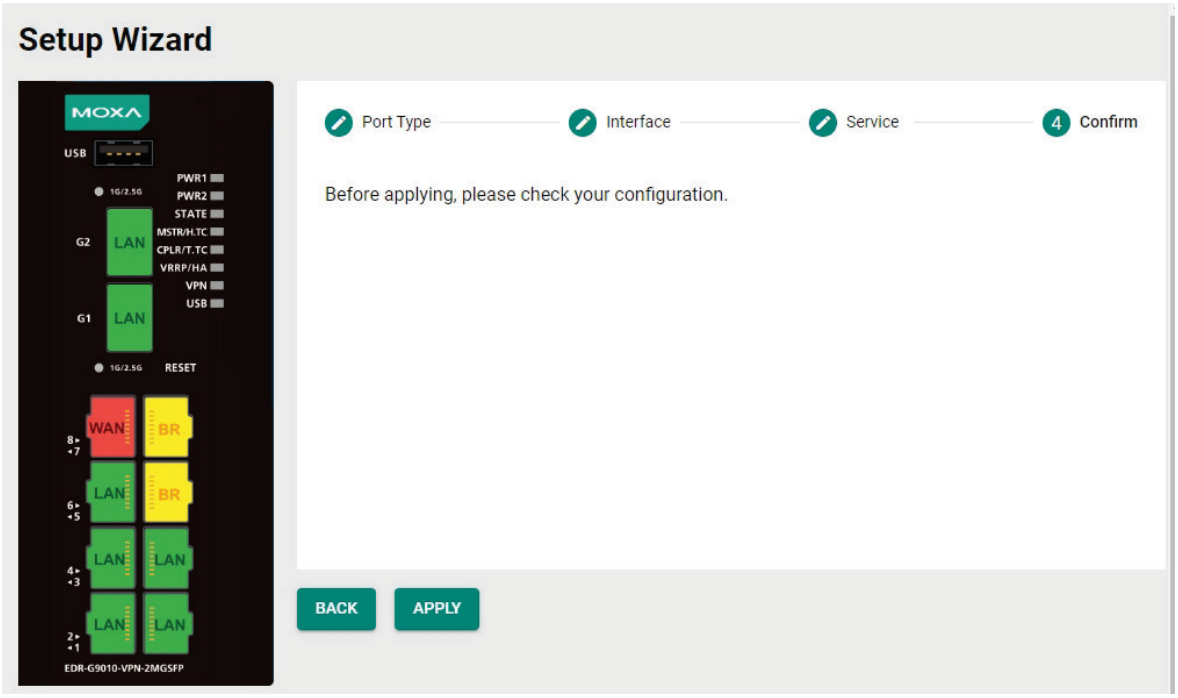
Step 3: Service

Use the toggle buttons to enable or disable the corresponding services. The **Enable DHCP Server** and **Enable N-1 NAT** are enabled by default. The default IP address range will be set automatically. To modify the IP range, refer to the DHCP Server section.



Step 4: Confirm

Click **APPLY** to apply the settings or click **BACK** to modify the settings.



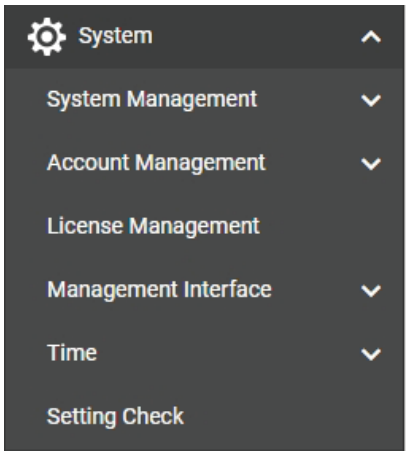
NOTE

The settings configured in the Setup Wizard will override any existing configuration.

4. System

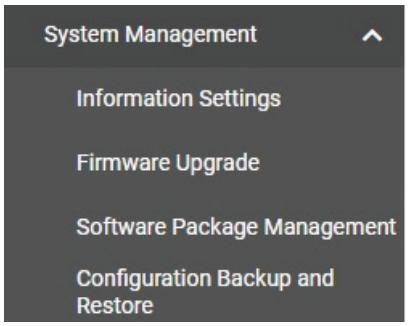
The **System** section includes the most common settings required by administrators to maintain and control the Moxa Industrial Secure Router.

From the **System** menu, you can access the **System Management, Account Management, License Management, Management Interface, Time,** and **Setting Check** configuration pages.



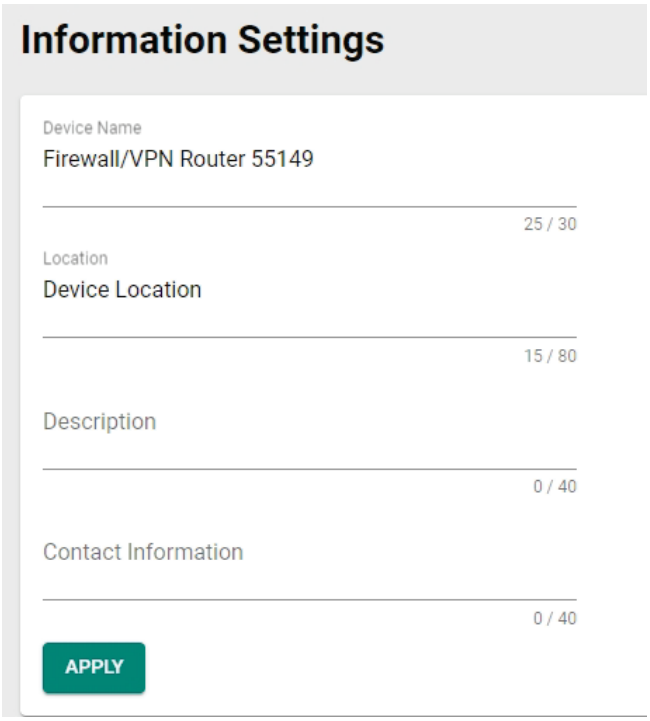
System Management

From the **System Management** menu, the following functions can be configured: **Information Settings, Firmware Upgrade, Software Package Management,** and **Configure Backup and Restore**.



Information Settings

The **Information Settings** screen lets you edit the basic device information to make it easier to identify the device on the network.



Device Name

Setting	Description	Factory Default
Max. 30 characters	Enter a name for the device. This is useful for differentiating between the roles or applications of different units on the network. For example, "Factory Router 1".	Firewall/VPN Router

Location

Setting	Description	Factory Default
Max. 80 characters	Enter a location for the device. This is useful for quickly identifying the location of different units. For example, "Production line 1".	Device Location

Description

Setting	Description	Factory Default
Max. 40 characters	Enter a description for the device.	None

Contact Information

Setting	Description	Factory Default
Max. 40 characters	Enter the contact information for the person in charge of the device. This is useful for providing information on who is responsible for maintaining this unit and how to contact this person.	None

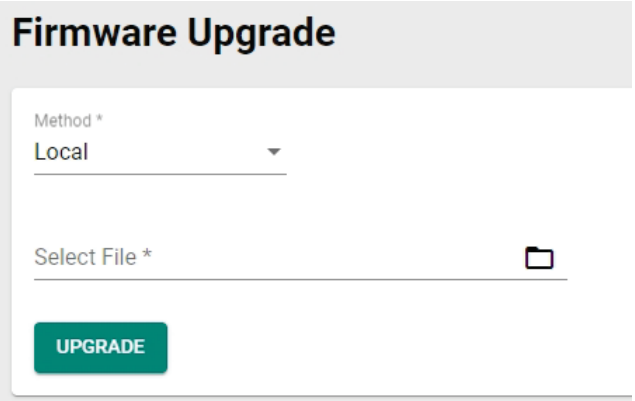
When finished, click **APPLY** to save your changes.

Firmware Upgrade

There are three ways to update your Moxa router's firmware: from a local *.rom file, by remote TFTP server, and via a USB tool.

Local

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



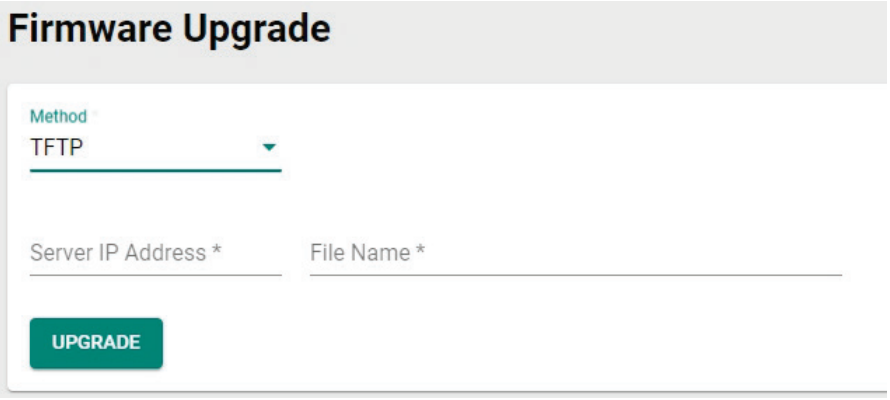
Select File

Before performing the firmware upgrade, download the firmware (*.rom) file from the Moxa website (www.moxa.com).

Click 🗀 to select the firmware file stored locally on the host computer. With the firmware selected, click **UPGRADE** to start the upgrade process. This procedure will take several minutes to complete.

TFTP Server

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



Server IP Address

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

File Name

Setting	Description	Factory Default
Firmware file name	Enter the file name of the target firmware file.	None

When finished, click **UPGRADE** to start the firmware upgrade process.

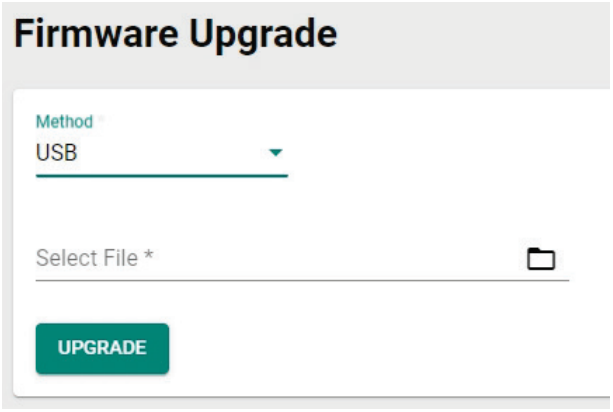
USB

On large-scale networks, administrators need to configure many network devices. This is a time-consuming process and errors often occur. By using Moxa's Automatic Backup Configurator (ABC-02), the administrator can easily duplicate the system configurations across many systems in a short period of time.

Administrators only need to set up the configuration in a system once including the firewall rules and certificates and export the configuration file to the ABC-02. Then, the administrator can plug the ABC-02-USB into other systems to sync the configuration of these devices with the configuration files stored in the ABC-02-USB. For more details about the ABC-02-USB, please visit: https://www.moxa.com/product/Automatic_Backup_Configurator_ABC-02-USB.htm

Moxa's Automatic Backup Configurator (ABC-02-USB)

To use the Moxa USB-based ABC-02 configuration tool to upgrade the firmware, connect the ABC-02-USB to the router and select **USB** from the drop-down list under **Method**.



Select File

Before performing the firmware upgrade, download the firmware (*.rom) file from the Moxa website (www.moxa.com).

Click 🗀 to select the firmware file stored on the ABC-02-USB. With the firmware selected, click **UPGRADE** to start the upgrade process. This procedure will take several minutes to complete.

NOTE

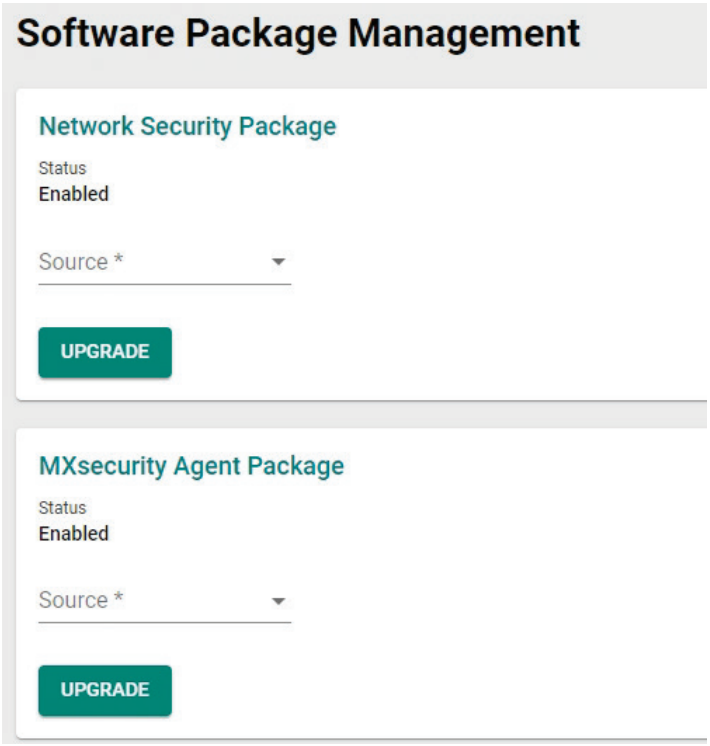
The ABC-02 USB is an optional accessory and must be purchased separately.

NOTE

If you have difficulties using the ABC-02 configuration tool, check if the USB Function has been enabled in the Hardware Interface section.

Software Package Management

The Industrial Secure Router supports two package types: a **Network Security Package** and a **MXsecurity Agent Package**. You can install or upgrade these packages to expand the security features of the Industrial Secure Router with advanced functions.



Status

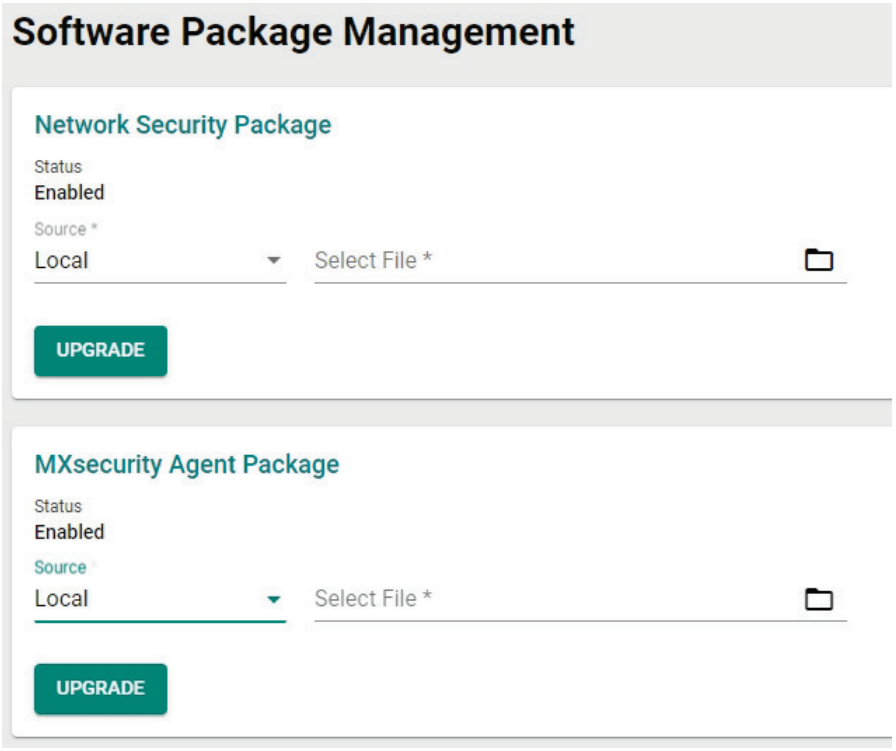
Setting	Description	Factory Default
Enabled	The package is installed and is working normally.	Enabled
Disabled	The package is installed but was abnormally terminated.	
Uninstalled	No package is installed.	

Source

Select the source for installing or upgrading the security package. There are two ways to install or upgrade security packages: using a local file or through a firmware file. Refer to the following sections.

Local

Before performing the package upgrade, download the package (*.pkg) file from the Moxa website (www.moxa.com).



Source

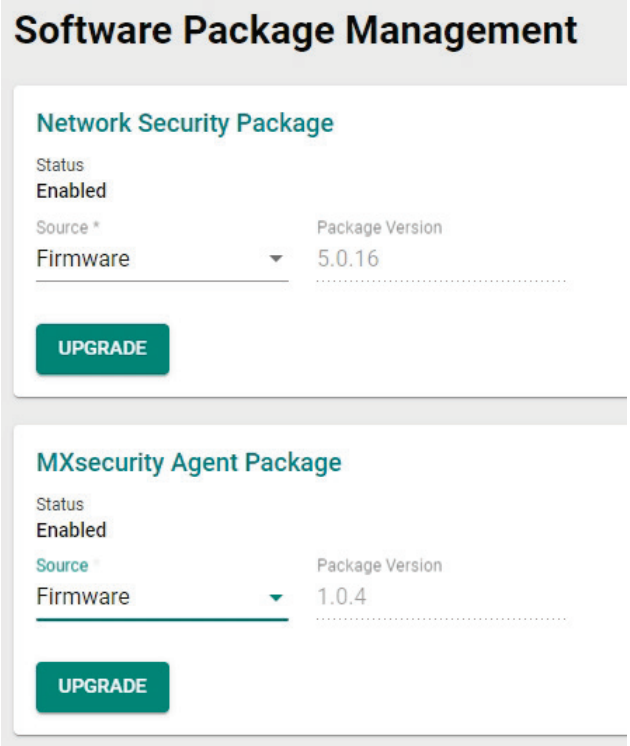
Select **Local** from the drop-down menu under **Source** to update an existing package using a local file.

Select File

Click 🗀 to select the package file stored locally on the host computer. With the package selected, click **UPGRADE** to start the upgrade process. This procedure will take several minutes to complete.

Firmware

This requires the firmware containing the package file is already installed on the device. Refer to the Firmware Upgrade section on how to install firmware.



Source

Select **Firmware** from the drop-down menu under **Source** to install or update a package through firmware.

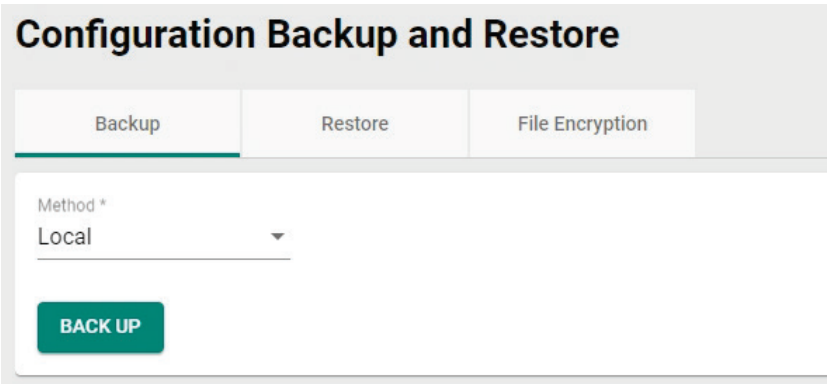
Package Version

This shows the target firmware version. Click **UPGRADE** to start the upgrade process. This procedure will take several minutes to complete.

Configuration Backup and Restore

Backup

From the **Backup** screen, you can export the device's configuration.



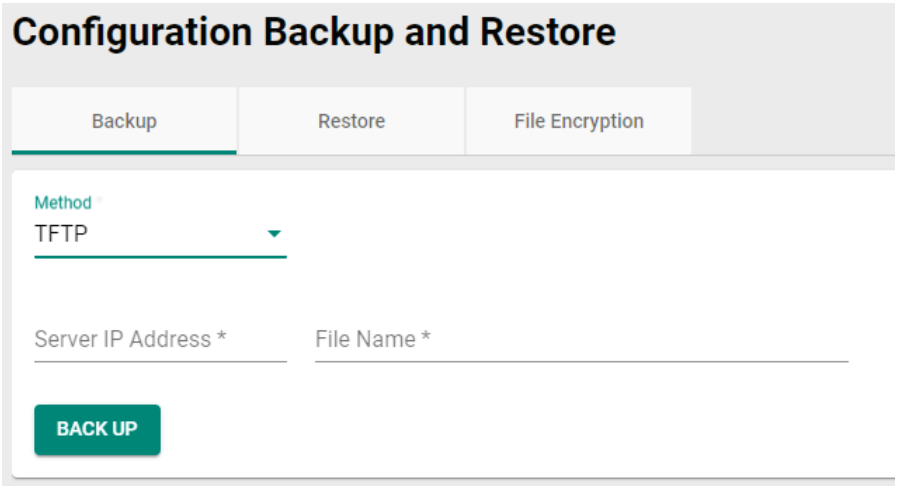
There are three ways to back up the configuration of your Industrial Secure Router: to the local host computer, to a remote TFTP server, or to a Moxa ABC-02 USB tool.

Local

Select **Local** from the drop-down list under **Method**, then click **BACK UP** to back up the system configuration file to the local host machine.

TFTP

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



Server IP Address

Setting	Description	Factory Default
IP address	Enter the IP address of the TFTP server.	None

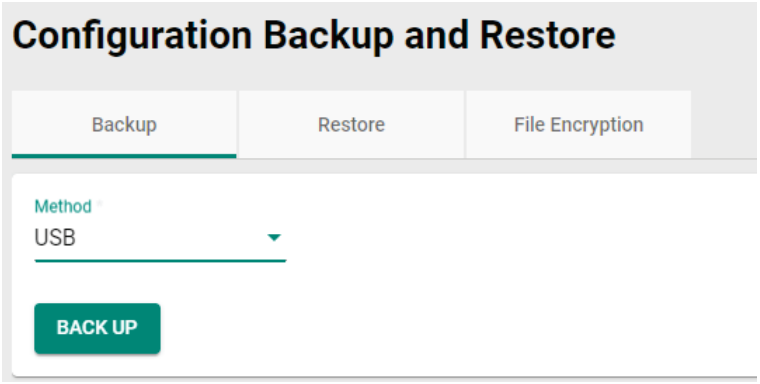
File Name

Setting	Description	Factory Default
Backup file name	Enter the file name of the configuration backup file.	None

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

USB

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



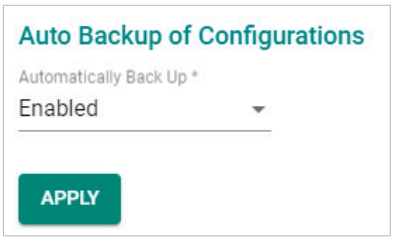
Insert the Moxa ABC-02 USB-based configuration tool into the USB port of the Industrial Secure Router and click **BACK UP** to back up the system configuration file to the tool.

NOTE

If you have difficulties using the ABC-02 configuration tool, check if the **USB Function** has been enabled in the Hardware Interface section.

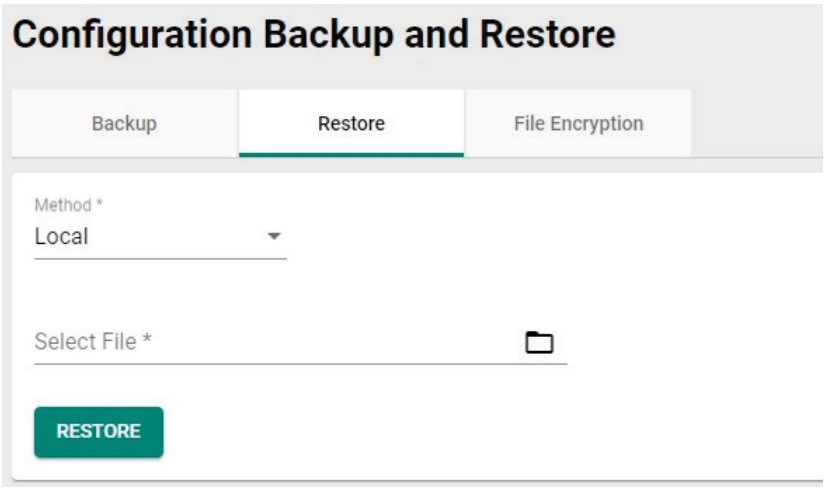
Auto Backup of Configurations

To enable automatic configuration backups, select **Enabled** from the drop-down list. Click **APPLY** to have the device automatically back up the system configuration.



Restore

From the **Restore** screen, you can restore the device's configuration using a previously back up configuration file.



There are three ways to restore the configurations of your Industrial Secure Router: from a local configuration file, by remote TFTP server, or using a Moxa ABC-02 USB tool.

Local

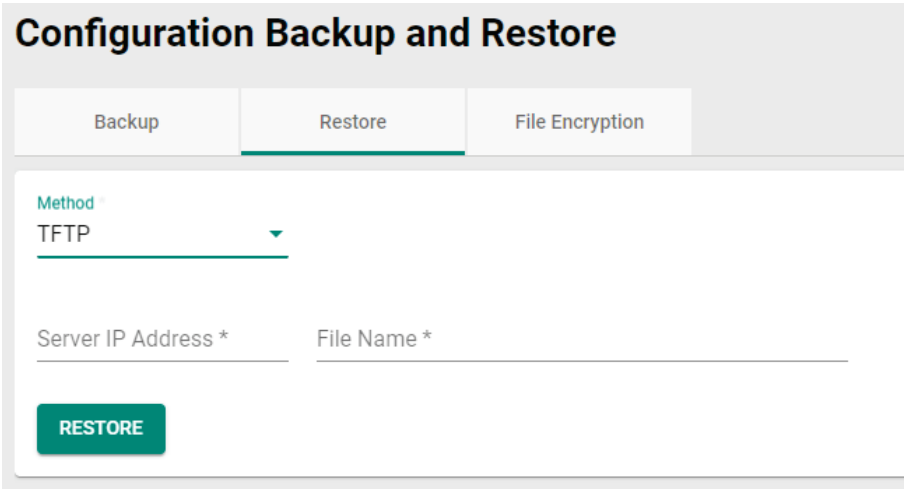
Select **Local** from the drop-down list under **Method**

Select File

Click 🗀 to select a configuration file stored locally on the host computer. With the configuration file selected, click **RESTORE** to restore the system configuration. This procedure will take several minutes to complete.

TFTP

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



Server IP Address

Setting	Description	Factory Default
IP address	Enter the IP address of the TFTP server.	None

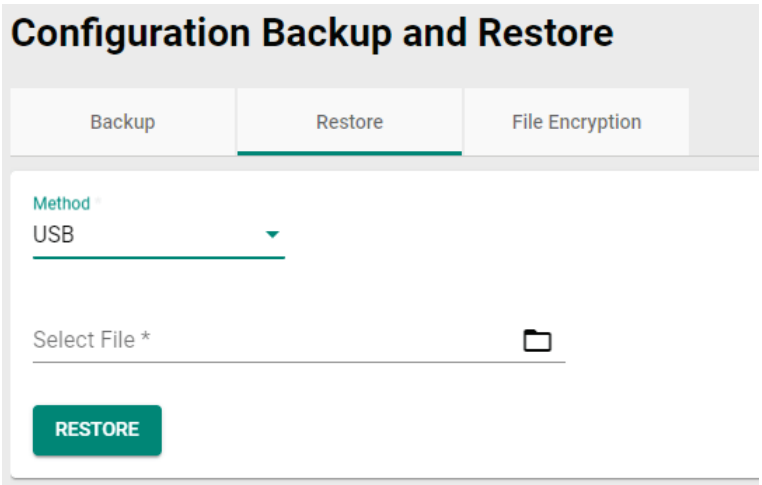
File Name

Setting	Description	Factory Default
Configuration file name	Enter the file name of the configuration restore file.	None

When finished, click **RESTORE** to restore the system configuration.

USB

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



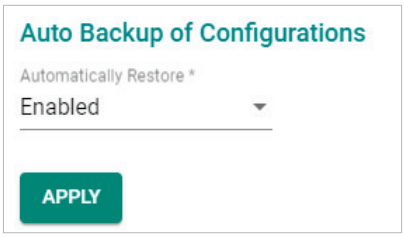
Insert the Moxa ABC-02 USB-based configuration tool into the USB port of the Industrial Secure Router and click **RESTORE** to restore the system configuration.

NOTE

If you have difficulties using the ABC-02 configuration tool, check if the **USB Function** has been enabled in the Hardware Interface section.

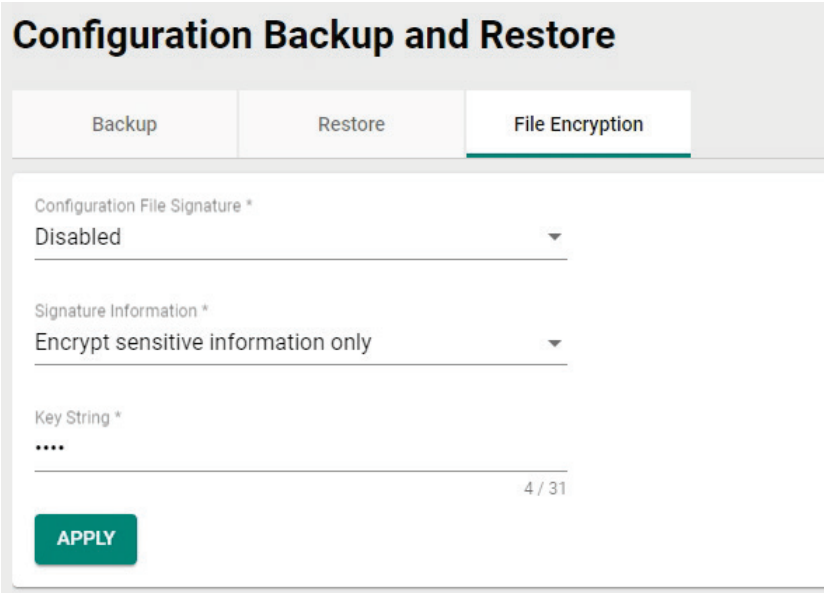
Auto Backup of Configurations

To enable automatic configuration restoration, select **Enabled** from the drop-down list and click **APPLY** to have the device automatically restore the system configuration.



File Encryption

You can export the configuration as an encrypted text-based (command line type) configuration file and specify an encryption key string. The key string is also used for decrypting when importing an encrypted configuration file.



Configuration File Signature

Setting	Description	Factory Default
Enabled or Disabled	Enables or disables the use of a digital signature for checking the configuration file integrity.	None

Signature Information

Setting	Description	Factory Default
Encrypt sensitive information only	Only encrypt password-related sensitive information in the exported configuration file.	Encrypt sensitive information only
Encrypt all information	Encrypt all information in the exported configuration file.	

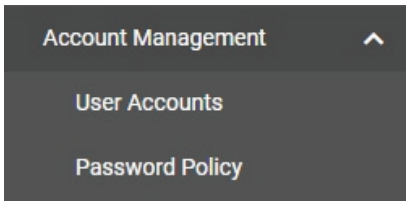
Key String

Setting	Description	Factory Default
Max. 31 characters	Enter an encryption key string. This key string is also used to decrypt encrypted configuration files.	moxa

When finished, click **Apply** to apply the changes.

Account Management

Click **Account Management**, two functions can be configured under this section: **User Accounts,** and **Password Policy**.

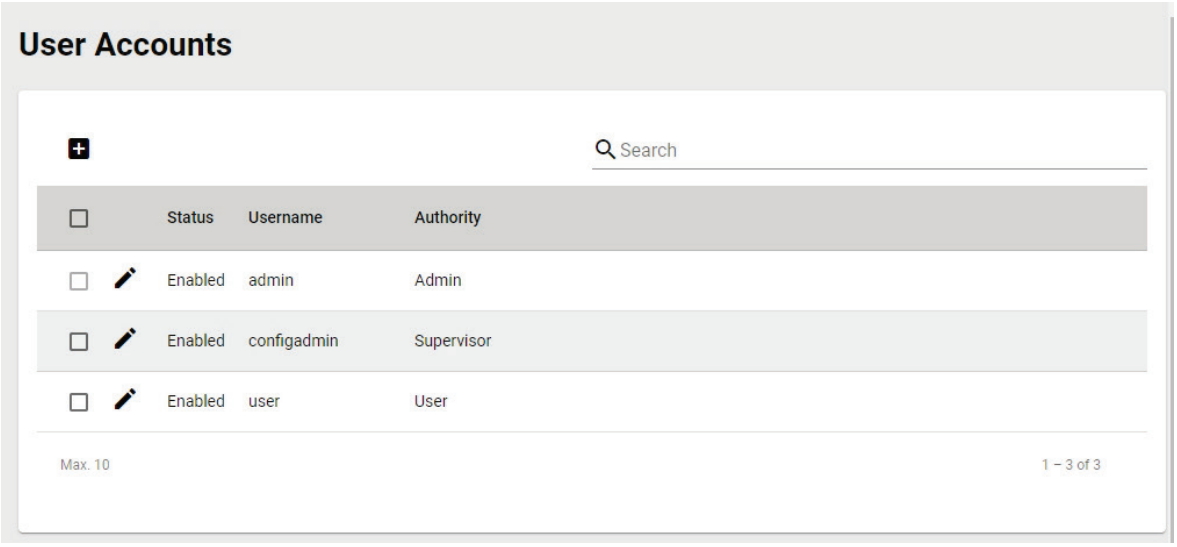


User Accounts

The Moxa Industrial Secure Router's account management function allows you to create, manage, modify, and remove user accounts. There are three levels of configuration access: Admin, Supervisor, and User. The admin accounts have read/write access to all configuration parameters. Supervisors have full editing rights but cannot create, modify, or delete accounts. User-level accounts have read-only access and can only view configurations.

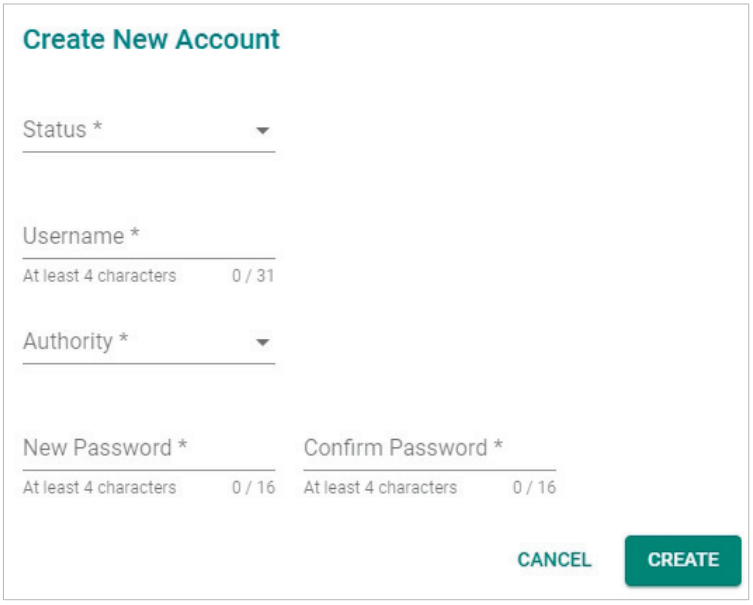
NOTE

1. We strongly recommend changing the default password after logging in for the first time.
2. The default 'admin' account cannot be deleted and is enabled by default.



Create a New Account

Click the ⊞ icon to create a new user account. Enter a username and password, assign the status and the authority to the new account, and click **CREATE**. Once created, the new account will appear in the Account List table.



Status

Setting	Description	Factory Default
Enabled	The Industrial Secure Router can be accessed by this account.	None
Disabled	The Industrial Secure Router cannot be accessed by this account.	

Username

Setting	Description	Factory Default
4 to 31 characters	Enter a username for the account.	None

Authority

Setting	Description	Factory Default
Admin	The account has read/write access to all configuration parameters.	None
Supervisor	The account has read/write access to all configuration parameters except create, delete, and modify accounts.	
User	The account can only view configurations and cannot make any modifications.	

NOTE

Refer to User Role Privileges for a detailed description of read/write access privileges for the admin, supervisor, and user authority levels.

New Password

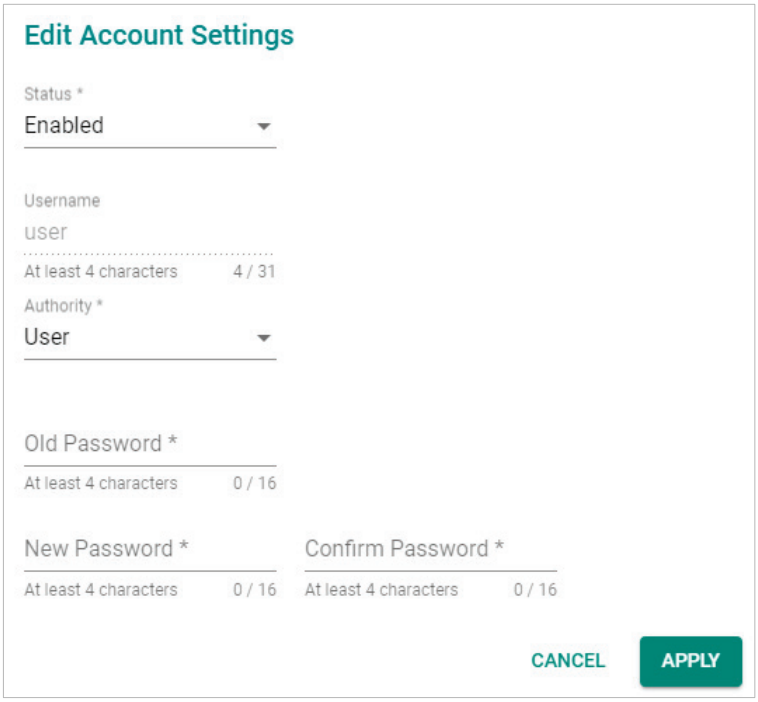
Setting	Description	Factory Default
4 to 16 characters	Enter a password for the account.	None

Confirm Password

Setting	Description	Factory Default
4 to 16 characters	Re-enter the password for the account to confirm.	None

Modify an Existing Account

In the Account List table, click the icon next to the account you want to modify the account.



Status

Setting	Description	Factory Default
Enabled	The Industrial Secure Router can be accessed by this account.	None
Disabled	The Industrial Secure Router cannot be accessed by this account.	

Username

Setting	Description	Factory Default
4 to 31 characters	Enter a username for the account.	None

Authority

Setting	Description	Factory Default
Admin	The account has read/write access to all configuration parameters.	None
Supervisor	The account has read/write access to all configuration parameters except create, delete, and modify accounts.	
User	The account can only view configurations but cannot make any modifications.	

Old Password

Setting	Description	Factory Default
4 to 16 characters	If you want to change the account password, enter the current password of the account.	None

New Password

Setting	Description	Factory Default
4 to 16 characters	Enter a new password for the account.	None

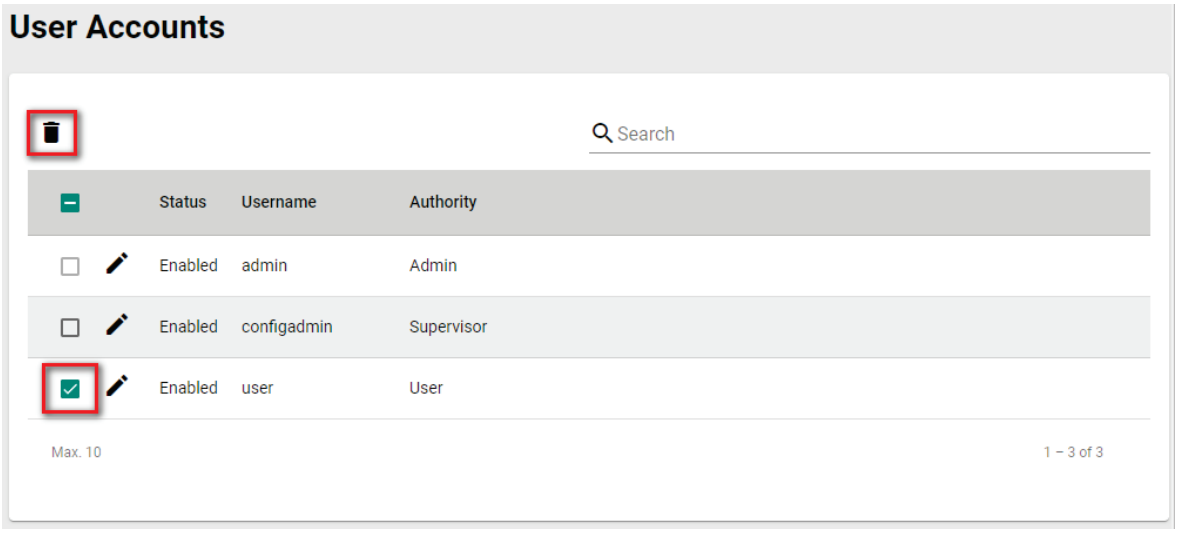
Confirm Password

Setting	Description	Factory Default
4 to 16 characters	Re-enter the new password for the account to confirm.	None

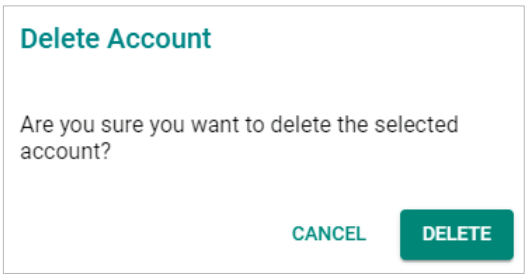
When finished, click **APPLY** to save your changes.

Delete an Existing Account

To delete existing accounts, select one or multiple accounts from the Account List table and click the icon.

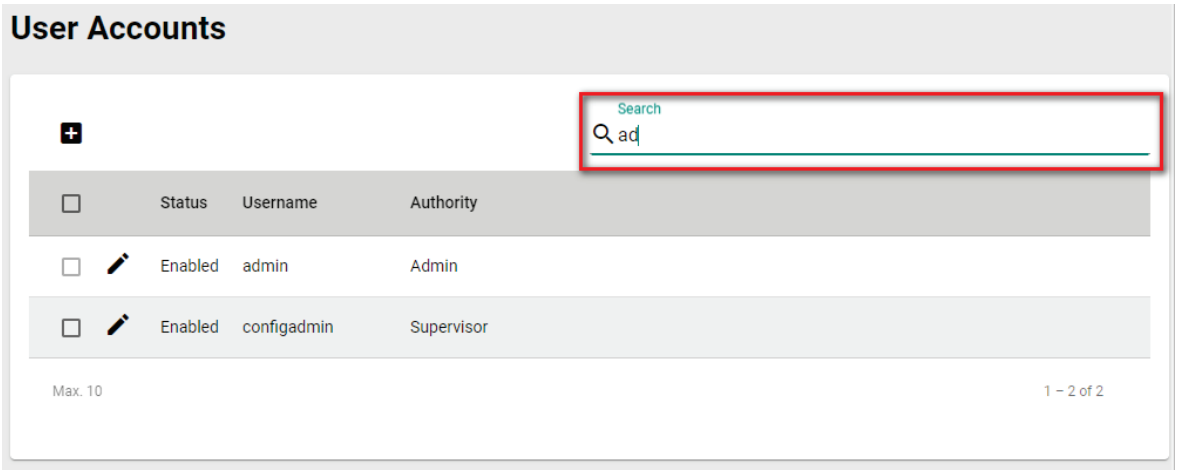


Click **DELETE** to delete the account



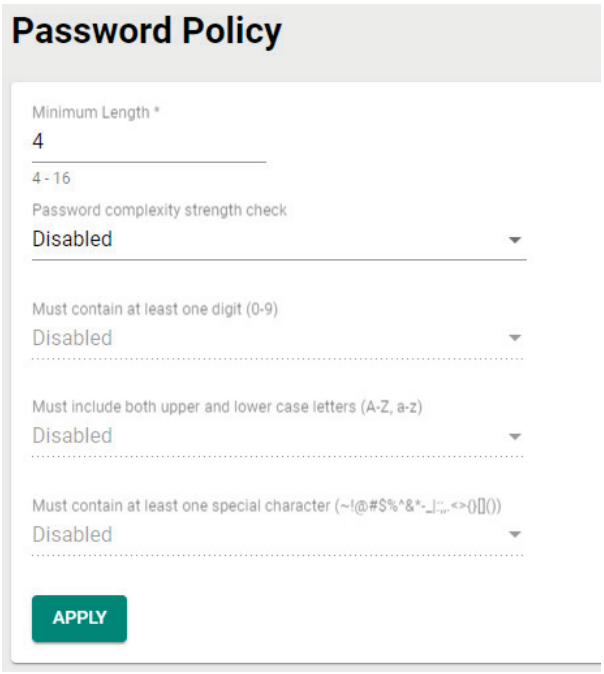
Search for an Existing Account

Enter the full or partial account username in the Search field. Any user accounts matching the search criteria will be shown in the Account List table.



Password Policy

Using the Password Policy function, administrators can force more complex login passwords to improve the overall security of the system. At the same time, administrators can configure an account login failure lockout time to avoid unauthorized users from gaining access.



Minimum Length

Setting	Description	Factory Default
4 to 16 characters	Enter the minimum required password length.	4

Password complexity strength check

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the password complexity strength check.	Disabled

Must contain at least one digit (0-9)

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the requirement of the password to contain at least one digit.	Disabled

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

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the requirement of the password to include both upper- and lower-case letters.	Disabled

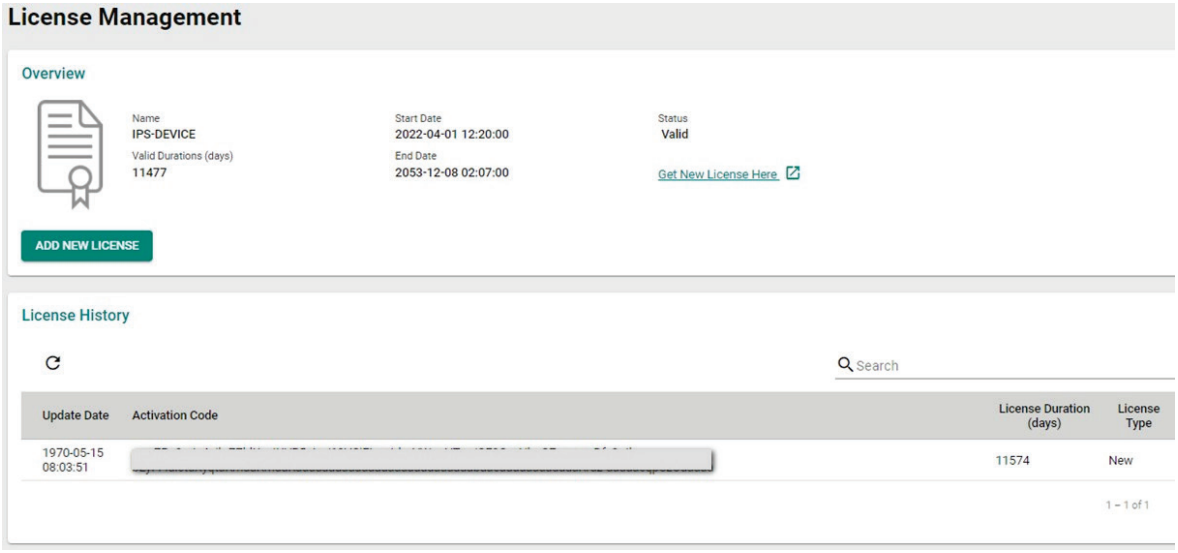
Must contain at least one special character (~!@#$%^&*- \|:;,.<>{}[]())

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the requirement of the password to contain at least one special character.	Disabled

License Management

The Industrial Secure Router supports additional software licenses to enable specific functions and services. To add a new license, you will need to activate the product license using a registration code.

Click the Get New License Here link to go to the Moxa license management portal. Refer to the **Moxa Software License Portal User Manual** for more information on how to activate product licenses.



Overview

The Overview section displays the license name, the valid duration (in days), the start date, the end date, and the status of the current license.

License History

The license history section shows more detailed license information.

- **Updated Date:** The date when the license was updated by entering the activation code.
- **License Duration:** The duration the license is valid for (in days).
- **License Type:** The type of license.

Click the icon to refresh the license information.

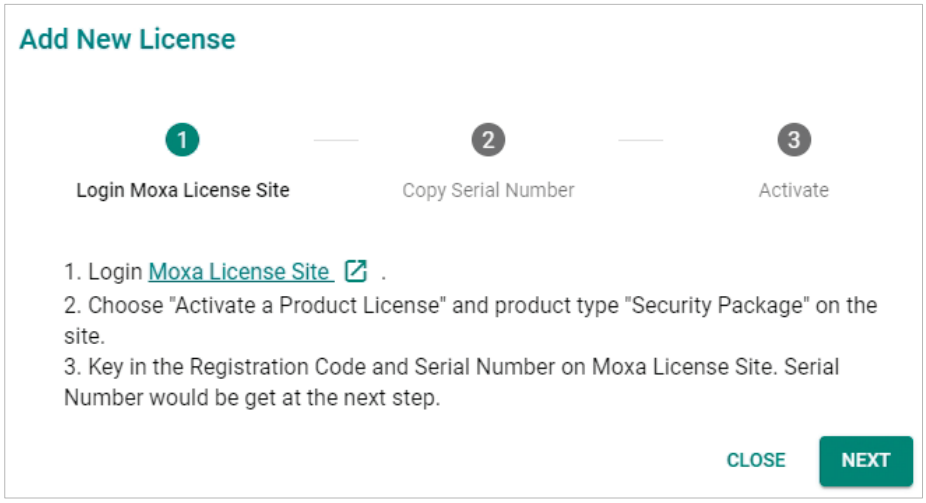
Enter the full or partial license number in the Search field. Any licenses matching the search criteria will be shown in the License List table.

Add a New License

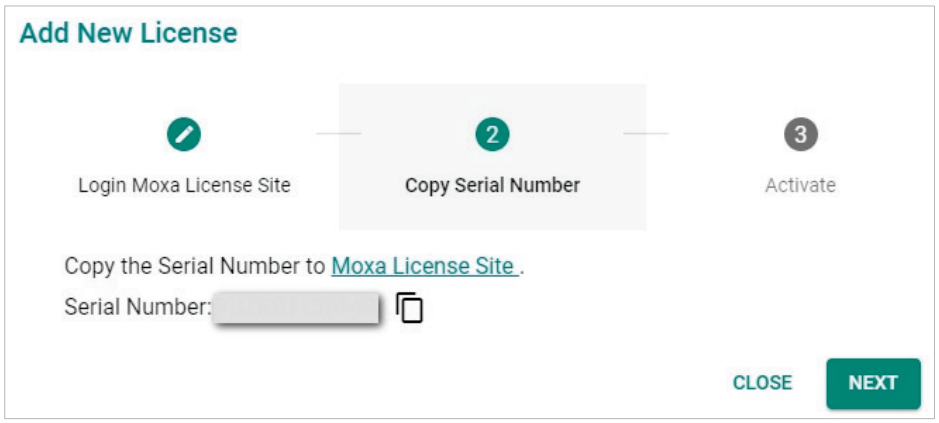
Whenever a new Industrial Secure Router license is activated in the license management portal, the system will generate an activation code that can be used to activate the license on the Industrial Secure Router.

1. Go to **System > License Management**.
2. Click the **ADD NEW LICENSE** button in the Overview section.

   The **Add New License** screen appears.

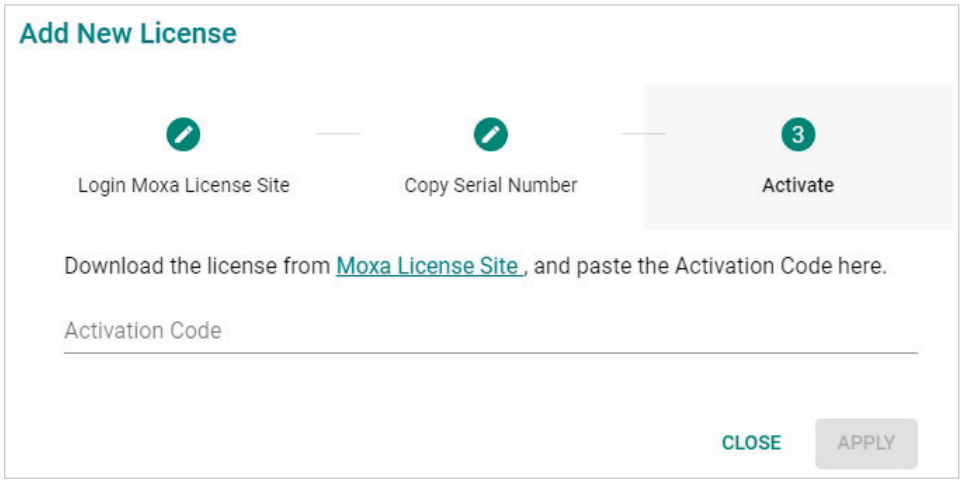


3. Click **Next**.
4. Click the icon to copy the serial number and store it somewhere where it can be easily copied from. Use the serial number to activate the license in the Moxa license management portal.



5. Click **Next**.

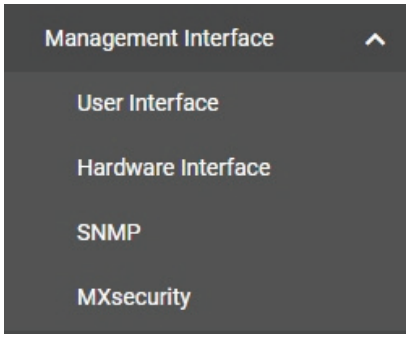
6. Enter the activation code from the email you have received after activating the license in the license management portal.



7. Click **APPLY**.
   The license is now activated on the Industrial Secure Router.

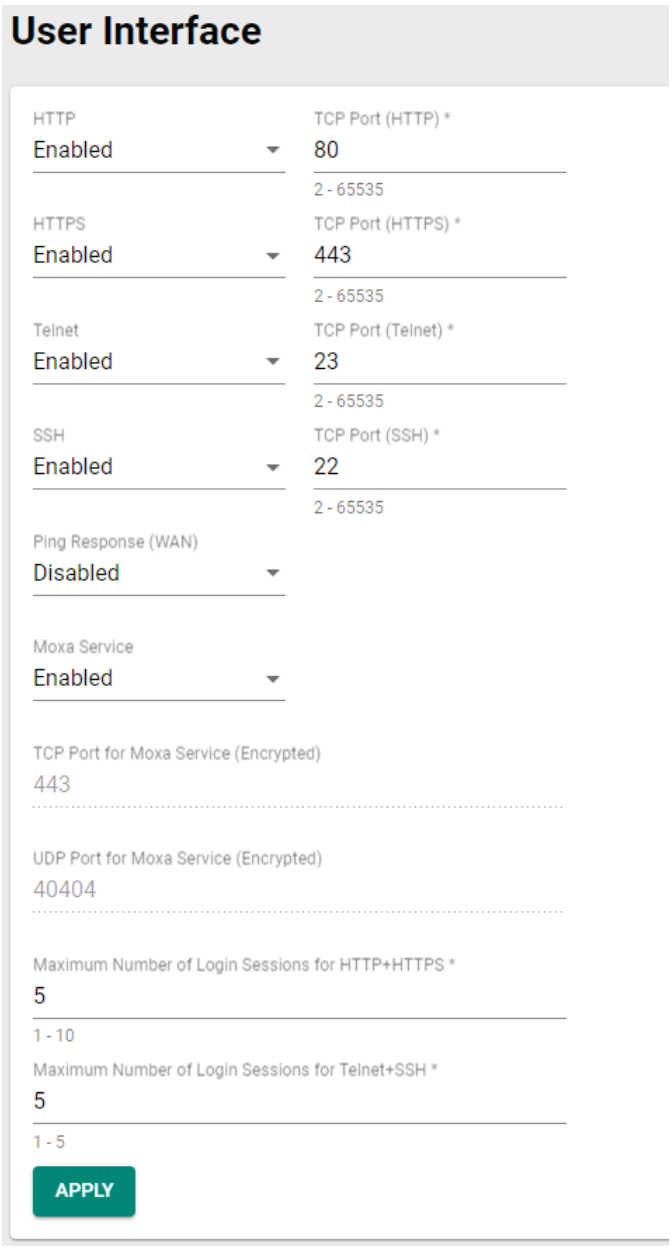
Management Interface

From the **Management Interface** section, four functions can be configured: **User Interface, Hardware Interface, SNMP,** and **MXsecurity**.



User Interface

From the User Interface screen, users can configure which interfaces can be used to access the device.



HTTP

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable HTTP connections.	Enabled

TCP Port (HTTP)

Setting	Description	Factory Default
2 to 65535	Enter the TCP port number for HTTP.	80

HTTPS

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable HTTPS connections.	Enabled

TCP Port (HTTPS)

Setting	Description	Factory Default
2 to 65535	Enter the TCP port number for HTTPS.	443

Telnet

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable Telnet connections.	Enabled

TCP Port (Telnet)

Setting	Description	Factory Default
2 to 65535	Enter the TCP port number for Telnet.	23

SSH

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable SSH connections.	Enabled

TCP Port (SSH)

Setting	Description	Factory Default
2 to 65535	Enter the TCP port number for SSH.	22

Ping Response (WAN)

Setting	Description	Factory Default
Enabled or Disabled	If a WAN connection has been established, enable this feature to have the WAN port respond to ping requests.	Disabled

NOTE

To ping the WAN port, make sure the "Ping Response (WAN)" function is enabled, and the ping sender IP is in the Trusted Access list or the "Accept All LAN Port Connections" option is enabled in Trusted Access.

MOXA Service

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the MOXA Service.	Enabled

NOTE

Moxa Service is only used for Moxa network management software.

TCP Port for Moxa Service (Encrypted)

Setting	Description	Factory Default
443 (read only)	The TCP port number for Moxa Service.	443

UDP Port for Moxa Service (Encrypted)

Setting	Description	Factory Default
40404 (read only)	The UDP port number for Moxa Service.	40404

Maximum Number of Login Sessions for HTTP+HTTTPS

Setting	Description	Factory Default
1 to 10	Specify the maximum combined number of users that can be logged in to the Industrial Secure Router using HTTP and HTTPS. The maximum is 10.	5

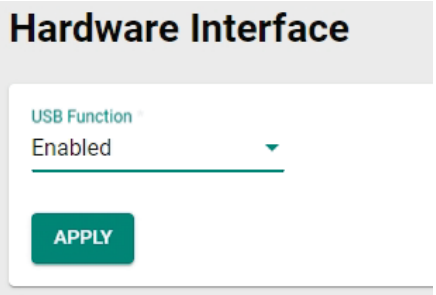
Maximum Number of Login Sessions for Telnet+SSH

Setting	Description	Factory Default
1 to 5	Specify the maximum combined number of users that can be logged in to the Industrial Secure Router using Telnet and SSH. The maximum is 5.	5

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

Hardware Interface

The **Hardware Interface** allows you to enable or disable the USB interface, which is used by the Moxa ABC-02 configuration tool.



USB Function

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the USB function on the Industrial Secure Router.	Enabled

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

SNMP

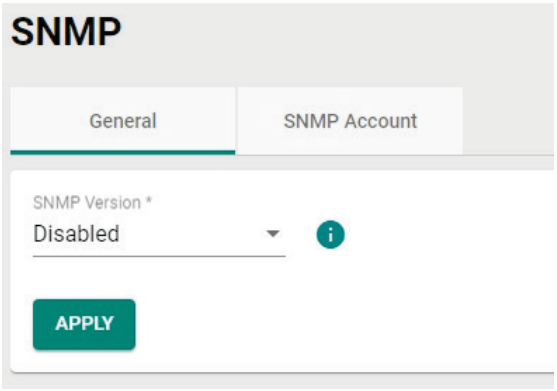
The Industrial Secure Router supports SNMP V1/V2c/V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only permissions using the community string public (default value). SNMP V3, which requires the user to select MD5 or SHA authentication, is the most secure protocol. You can also enable data encryption to enhance data security.

SNMP security modes and security levels supported by the Industrial Secure Router are listed in the following table.

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

General Settings

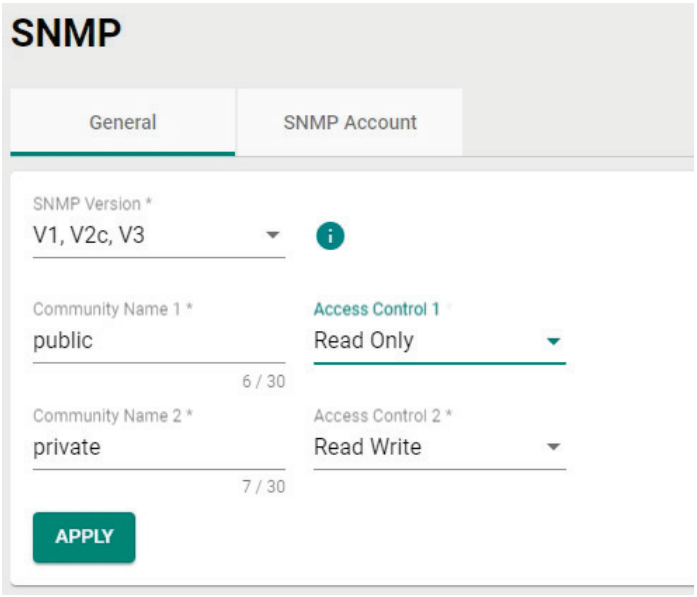
The SNMP page is used to enable or disable SNMP. Depending on the selected SNMP version, additional configuration parameters will become available.



SNMP Version

Setting	Description	Factory Default
Disabled, V1, V2c, V3, or V1, V2c, or V3 only	Select the SNMP protocol version used to manage the secure router.	Disabled

If you selected an SNMP version, configure the following settings:



Community Name 1/2

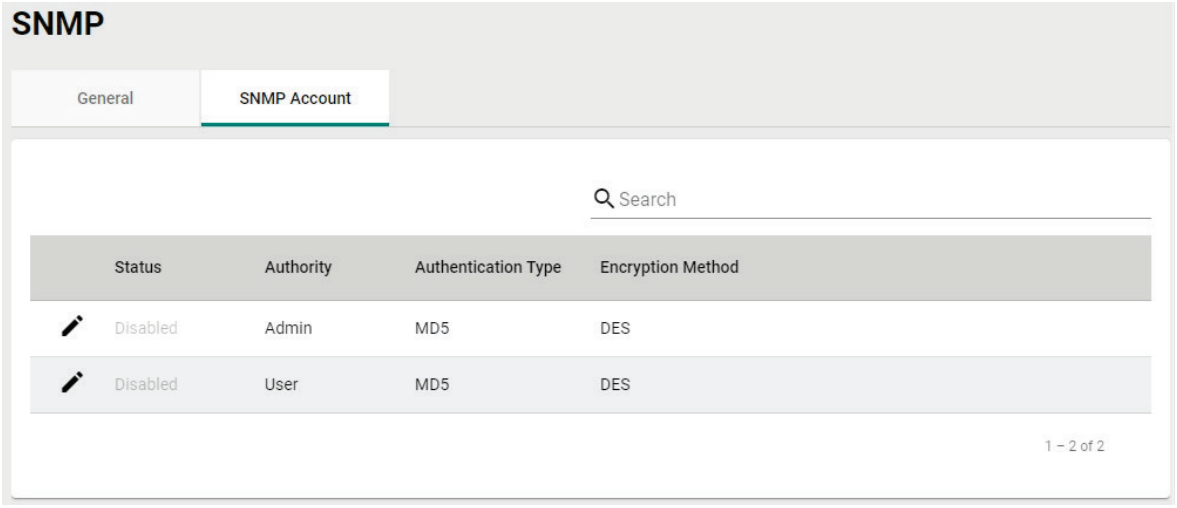
Setting	Description	Factory Default
Max. 30 Characters	Use a community string match for authentication	public/private

Access Control 1/2

Setting	Description	Factory Default
Read Write, or Read only, or No Access	Select the access control type for when the community string is matched	Read Only/Read Write

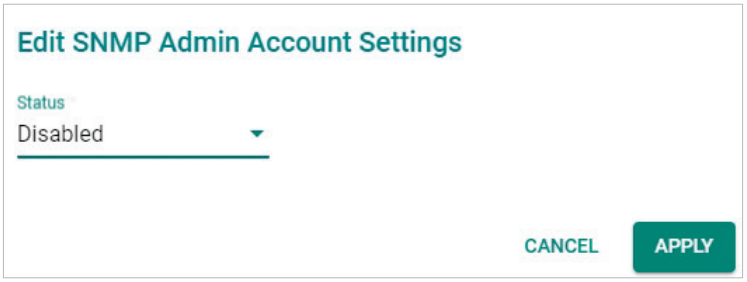
SNMP Account

The Industrial Secure Router comes with two preconfigured SNMP Accounts which are disabled by default.

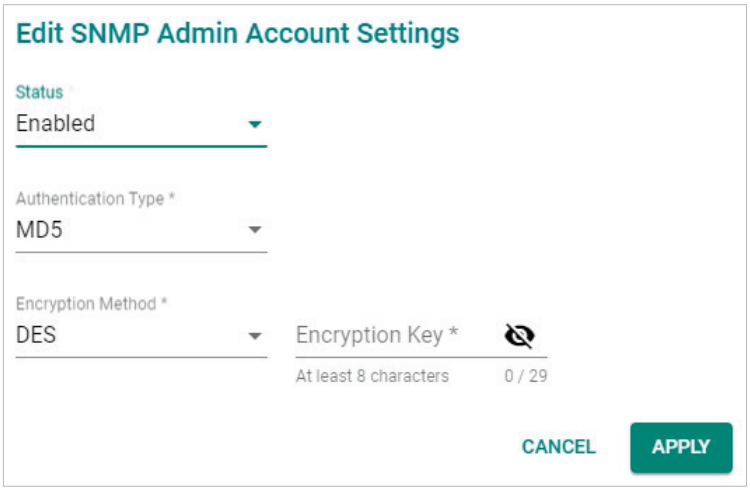


Modify an Existing SNMP Account

In the SNMP Account list, click the icon next to the SNMP account you want to modify.



Select **Enabled** from the Status drop-down menu and configure the following settings:



Authentication Type

Setting	Description	Factory Default
MD5	Provides authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	MD5
SHA	Provides authentication based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	
None	Do not use any authentication.	

Encryption Method

Setting	Description	Factory Default
DES/AES	Select an encryption method.	DES

Encryption Key

Setting	Description	Factory Default
Max. 29 Characters	Specify the encryption key. The key must be at least 8 characters long.	None

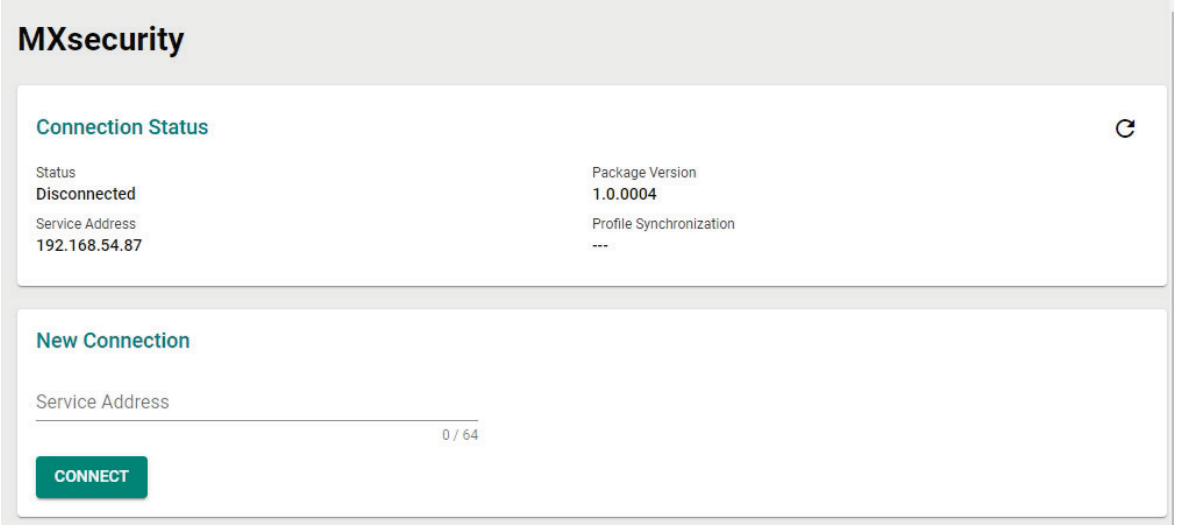
When finished, click **APPLY** to save your changes.

MXsecurity

The Industrial Secure Router supports management of firmware, software package, firewall policy, threat signature, and other functions through the MXsecurity centralized security management software.

NOTE

To manage the EDR-G9010 functions through MXsecurity, the MXsecurity Agent Package must be installed and enabled first. Refer to the Software Package Management section for how to install the MXsecurity Agent Package.



Connection Status

This section shows the current connection status to MXsecurity, the installed MXsecurity Agent package version, and the profile sync status.

Click the **Refresh** ( ) icon in the upper-right corner to refresh the connection status information.

Status

- **Disconnected:** Not connected to MXsecurity.
- **Connected:** A connection has been established with MXsecurity.
- **Connecting:** Connecting to MXsecurity.

Profile Synchronization

- **---:** No synchronization data available.
- **Sync:** The EDR-G9010 and MXsecurity configurations are synced.
- **Un-sync:** MXsecurity has configuration changes that are not synced to the EDR-G9010 device.
- **Out-of-sync:** There are configuration changes on the local EDR device that are not synced to MXsecurity.

New Connection

Use this function to establish a connection to the MXsecurity software.

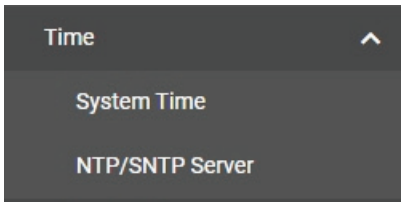
Service Address

Setting	Description	Factory Default
0 to 64 characters	Enter the MXsecurity server IP address or domain name address.	None

Click **CONNECT** to connect to the MXsecurity service.

Time

From the **Time** section, the following functions can be configured: **System Time,** and **NTP/SNTP Server**.



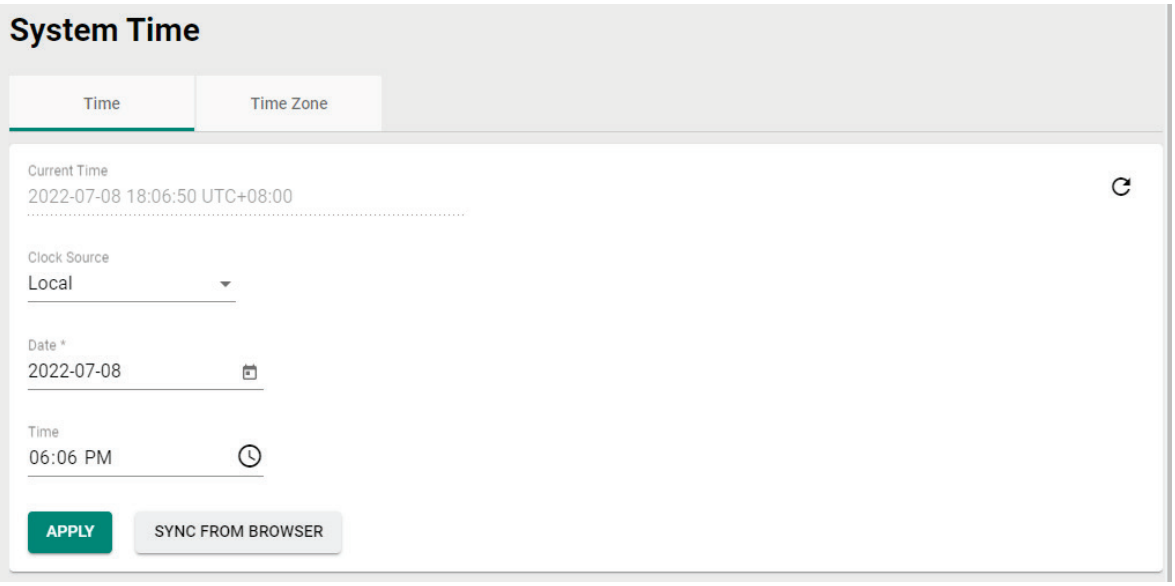
System Time

The Moxa Industrial Secure Router's system time can be synced with an NTP/SNTP server or can be user-specified. The system time is also used for time stamps in functions such as automatic warning emails.

NOTE

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

Time



Current Time

This shows the current date, time, and time zone.

NOTE

Click **SYNC FROM BROWSER** to synchronize the router's clock with the browser time. Click the icon in the upper right corner to refresh all the information on the page.

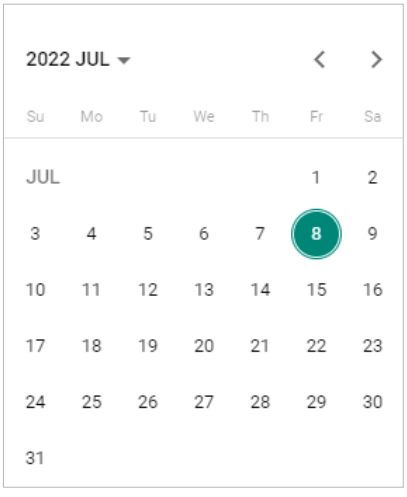
Clock Source

Setting	Description	Factory Default
Local	Set the clock source to local time. This will require you to manually specify the time and date.	Local
SNTP	Set the clock source to SNTP.	
NTP	Set the clock source to NTP.	

Local

Date

Setting	Description	Factory Default
Date	Manually set the date in YYYY-MM-DD format.	Current date

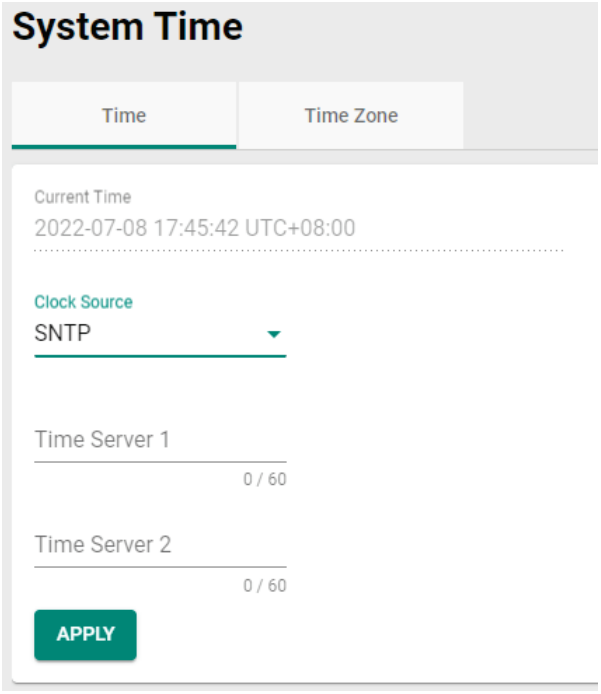


Time

Setting	Description	Factory Default
Time	Manually set the time in HH:MM AM/PM format.	Current time

NTP/SNTP Server

If SNTP or NTP is selected as the clock source, configure the following settings:



Time Server 1

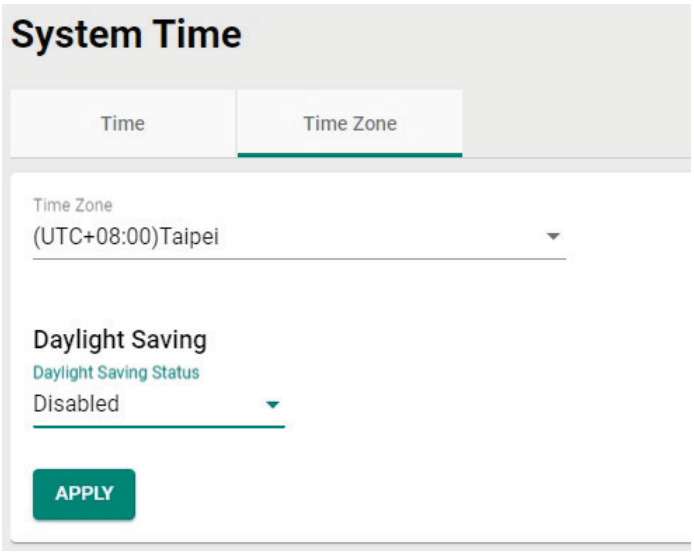
Setting	Description	Factory Default
0 to 60 characters	Specify the IP or domain address of the primary time server (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	None

Time Server 2

Setting	Description	Factory Default
0 to 60 characters	Specify the IP or domain address of the secondary time server. The Moxa Industrial Secure Router will use the secondary NTP server if it cannot connect to the primary NTP server.	None

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

Time Zone



Time Zone

Setting	Description	Factory Default
Select from the drop-down list	Select the time zone, which is used to determine the local time offset from UTC (Coordinated Universal Time).	UTC (Coordinated Universal Time)

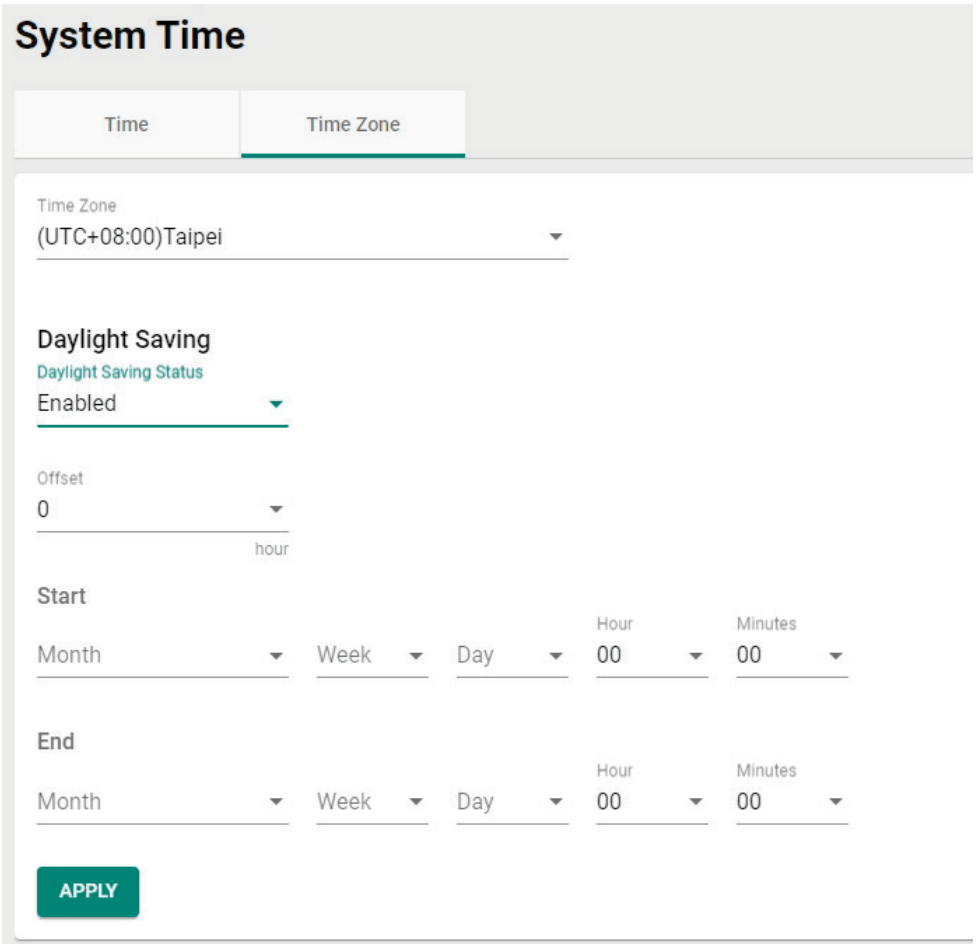
Daylight Saving

The Daylight Saving settings are used to automatically set the Moxa router's time forward according to national standards.

Daylight Saving Status

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

If Daylight Saving time is enabled, configure the following settings:



Offset

Setting	Description	Factory Default
User-specified hour	Specify the offset time (in hours) for Daylight Saving time.	0

Start

Month

Setting	Description	Factory Default
User-specified month	Specify the month the Daylight Saving time begins.	None

Week

Setting	Description	Factory Default
User-specified week	Specify the week the Daylight Saving time begins.	None

Day

Setting	Description	Factory Default
User-specified day	Specify the day the Daylight Saving time begins.	None

Hour

Setting	Description	Factory Default
User-specified hour	Specify the hour the Daylight Saving time begins.	00

Minutes

Setting	Description	Factory Default
User-specified minutes	Specify the minute(s) the Daylight Saving time begins.	00

End

Month

Setting	Description	Factory Default
User-specified month	Specify the month the Daylight Saving time ends.	None

Week

Setting	Description	Factory Default
User-specified week	Specify the week the Daylight Saving time ends.	None

Day

Setting	Description	Factory Default
User-specified day	Specify the day the Daylight Saving time ends.	None

Hour

Setting	Description	Factory Default
User-specified hour	Specify the hour the Daylight Saving time ends.	00

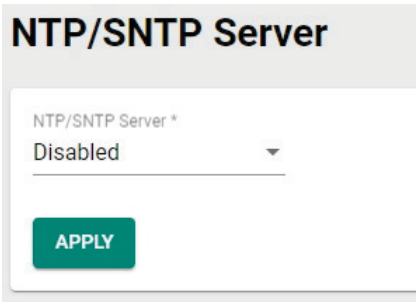
Minutes

Setting	Description	Factory Default
User-specified minutes	Specify the minute(s) the Daylight Saving time ends.	00

NOTE

Changing the time zone will automatically adjust the current time. Be sure to set the time zone before setting the time.

NTP/SNTP Server

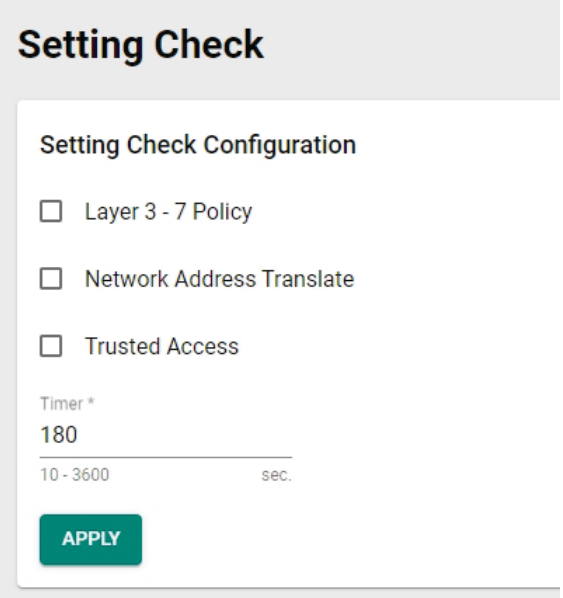


NTP/SNTP Server

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable NTP/SNTP server functionality for clients.	Disabled

Setting Check

Setting Check is a safety function which provides a double confirmation mechanism when a remote user changes the security policies, such as **Layer 3 – 7 Policy**, **Network Address Translate**, and **Trusted Access**. When a remote user changes these security policies, Setting Check allows you to block the remote user's connection to the EDR device. In the event of a misconfiguration, often the only way to correct a wrong setting is to get help from the local operator or go on-site and physically connect to the device through the console port, which takes up time and resources. Enabling the Setting Check function will execute these new policy changes temporarily until confirmed by the user. If not confirmed, the Industrial Secure Router will revert the changes.



Setting Check Configuration

Layer 3 – 7 Policy

Enable or disable the Setting Check function for Layer 3 - 7 policies changes.

Network Address Translate

Enable or disable the Setting Check function for NAT policies changes.

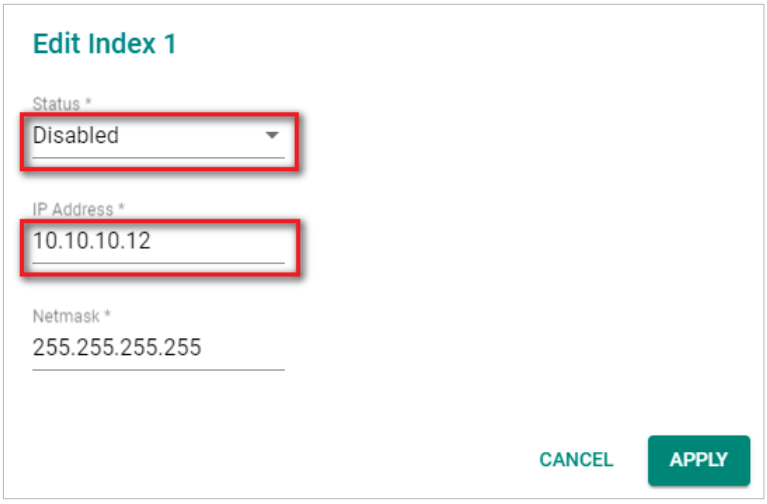
Trusted Access

Enable or disable the Setting Check function for Trusted IP address changes.

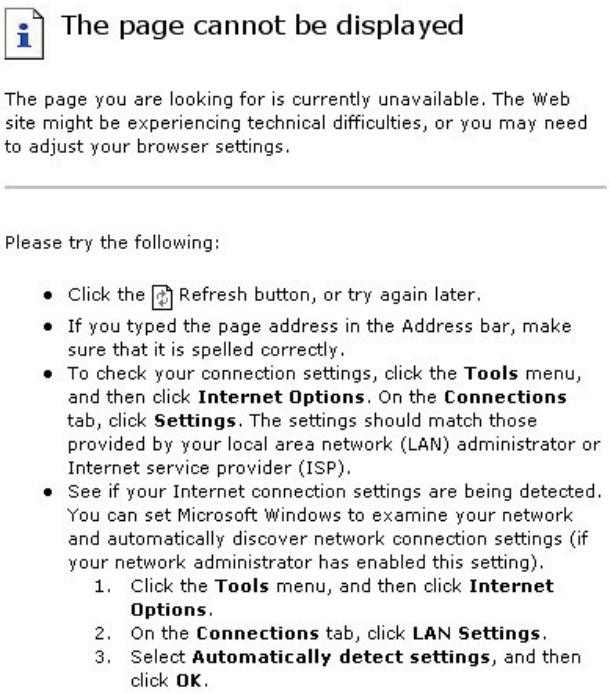
Timer

Setting	Description	Factory Default
10 to 3600 seconds	Specify the time (in seconds) the user has to confirm the changes. If the timer expires and the changes were not confirmed, the system will automatically revert to the previous settings.	180 (seconds)

For example, if a remote user (IP: 10.10.10.10) connects to the Industrial Secure Router and changes the Trusted IP address to 10.10.10.12, or accidentally disables the Trusted IP entry and applies the changes, the connection to the Industrial Secure Router will be lost because the IP address is no longer in the Industrial Secure Router's Trusted IP list.



If the user enables the Setting Check function for Trusted IP list changes and the confirm Timer is set to 15 seconds, when the user clicks the **APPLY** button on the Trusted IP list page, the Industrial Secure Router will execute the configuration change and the web browser will attempt to go to the Setting Check Confirmed page automatically. Because the remote user's IP address is not in the new Trusted IP list, the remote user cannot connect to the Setting Check Confirmed page. After 15 seconds, the timer will expire and the Industrial Secure Router will roll back to the original Trusted IP List settings, allowing the remote user to reconnect to the Industrial Secure Router.

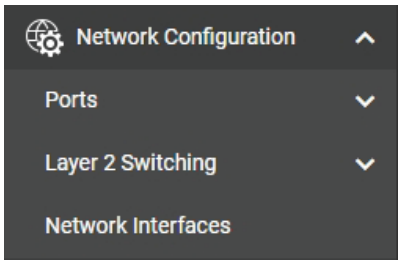


If the new configuration does not block the remote user's connection to the Industrial Secure Router, the user will see the Setting Check Confirmed page. Click **CONFIRM** to save and apply the changes.

5. Network Configuration

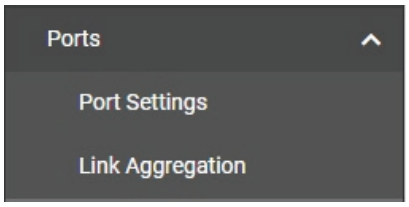
This chapter describes how to configure the physical ports and network interfaces of the Industrial Secure Router.

From the **Network Configuration** section, you can configure the **Ports**, **Layer 2 Switching**, and **Network Interfaces** settings.



Ports

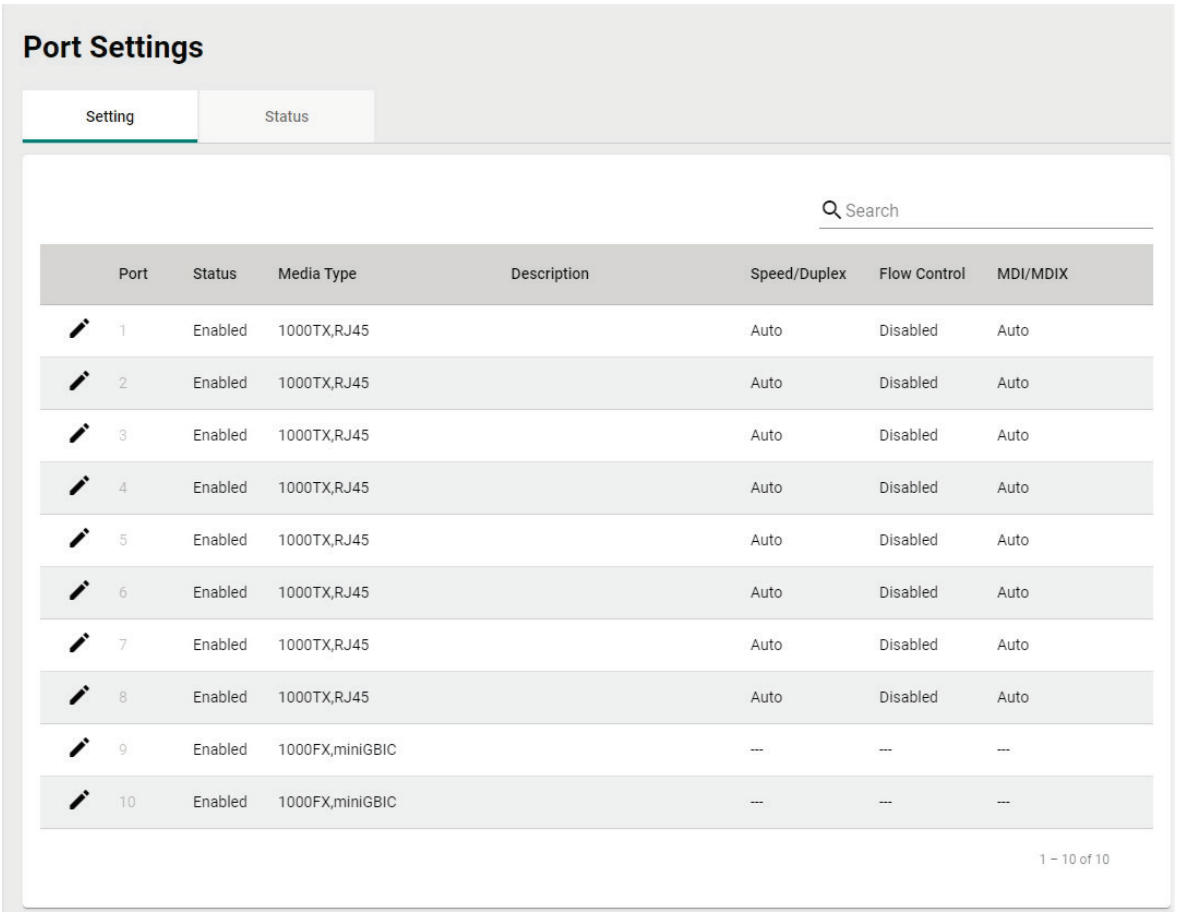
From the **Ports** section, the following functions can be configured: **Port Settings,** and **Link Aggregation**.



Port Settings

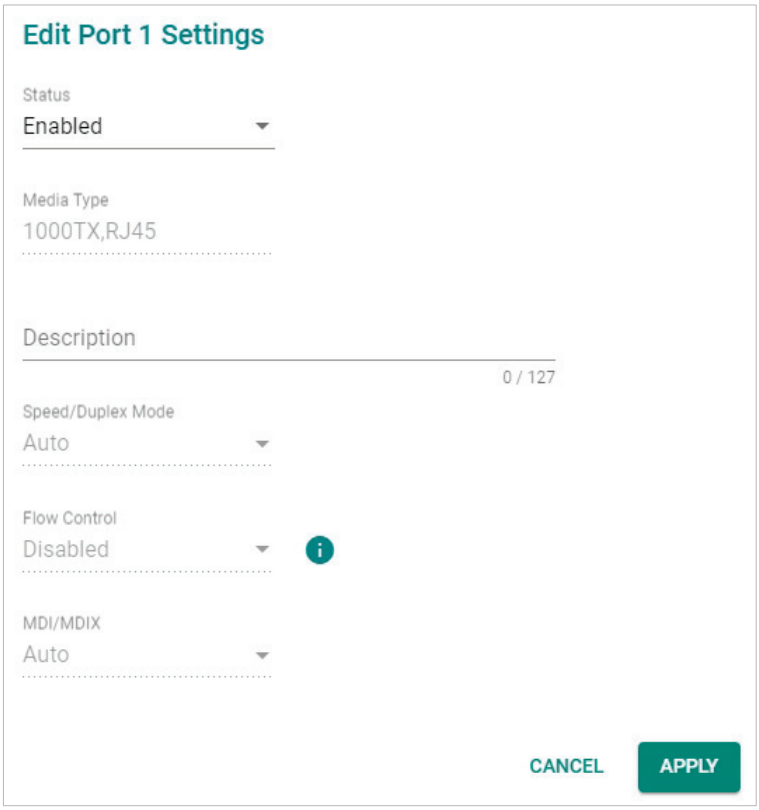
Port settings let you manage port access, port transmission speed, flow control, and port type (MDI or MDIX). The EDR-G9010 Series has eight RJ45 Ethernet ports and two mini GBIC fiber ports.

Setting



Modify Port Settings

Click the ✎ icon to modify the settings of the corresponding port.



Configure the following settings:

Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the port.	Enabled

Media Type

Setting	Description	Factory Default
Media type	Displays the port's media type.	Current media type

Description

Setting	Description	Factory Default
Max. 127 characters	Enter a description for the port. This helps administrators differentiate between different ports more easily. Example: PLC 1	None

Speed/Duplex Mode

Setting	Description	Factory Default
Auto	Allow the port to use the IEEE 802.3u protocol to negotiate the port speed and duplex mode with the connected device. The port and connected device will determine the best speed for that connection.	Auto
1G Full	Select a fixed speed and duplex mode if the connected Ethernet device has trouble auto-negotiating the line speed.	
100M-Full		
100M-Half		
10M-Full		
10M-Half		

Flow Control

The Flow Control setting allows you to enable or disable the flow control feature for the port when the port's Speed is set to Auto. Flow control helps manage the data transfer rate between the router and the connected Ethernet device.

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable flow control for this port when the port's Speed is set to Auto.	Disabled

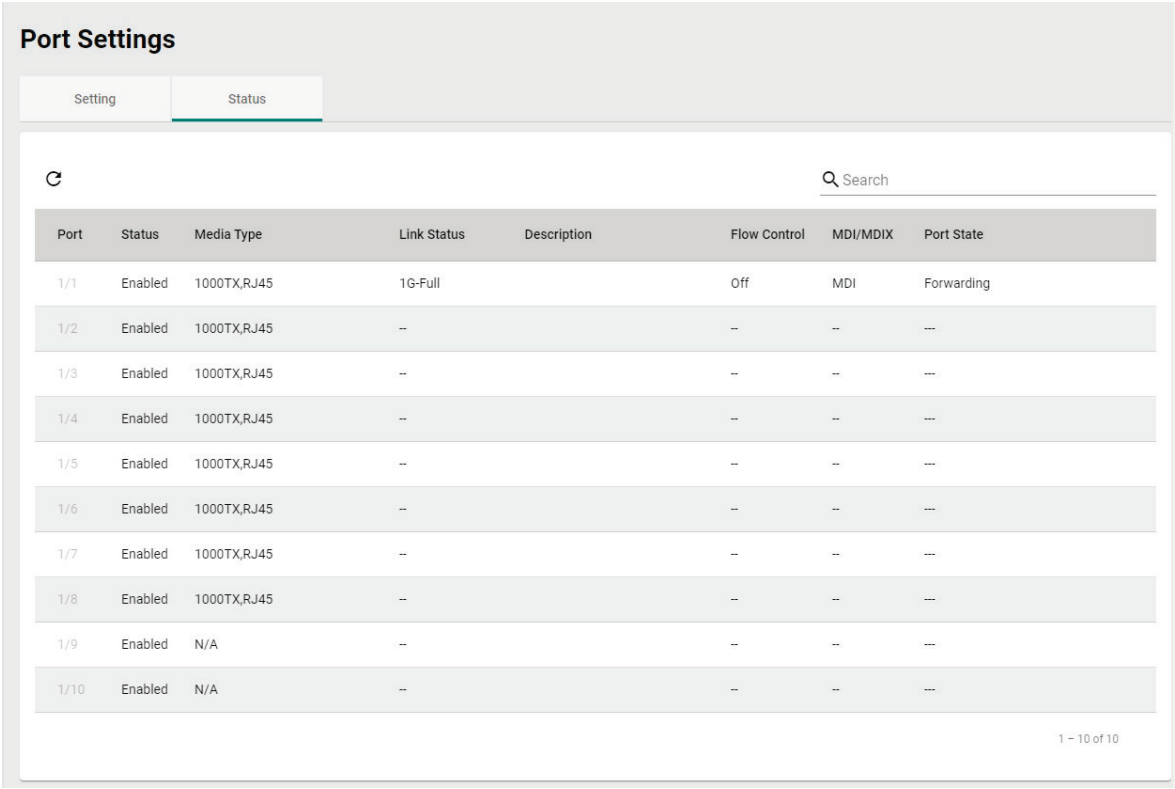
MDI/MDIX

Setting	Description	Factory Default
Auto	Allow the port to auto-detect the port type of the connected Ethernet device and change the port type accordingly.	Auto
MDI	Choose MDI or MDIX if the connected Ethernet device has trouble auto-negotiating the port type.	
MDIX		

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

Status

The Status page shows the current status of the Ethernet ports including the port transmission speed, flow control, and port type (MDI or MDIX).

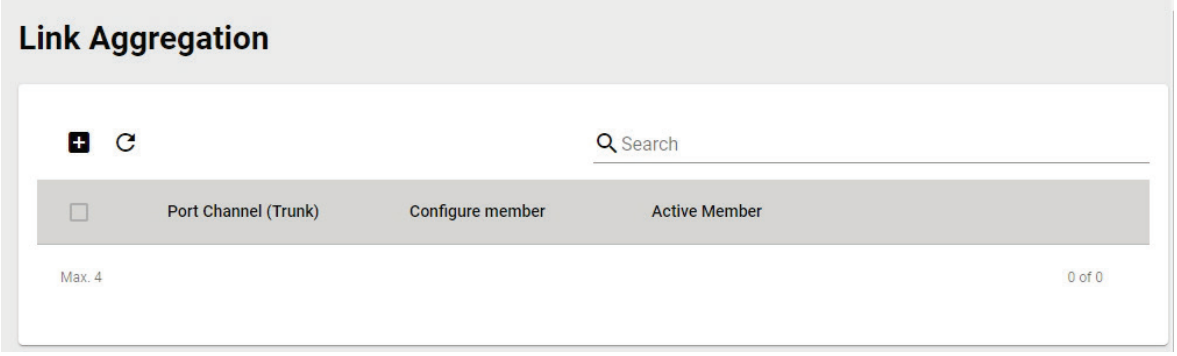


Link Aggregation

Link aggregation involves grouping links into a link aggregation group. A MAC client can treat link aggregation groups as if they were a single link.

The Moxa Industrial Secure Router's port trunking feature allows devices to communicate by aggregating up to 4 trunk groups, with a maximum of 8 ports for each group. If one of the 8 ports fails, the other seven ports will automatically provide backup and share the traffic.

Port trunking can be used to combine up to 8 ports between two Moxa switches or industrial secure routers. If all ports on both switches are configured as 1000BaseTX and they are operating in full duplex, the potential bandwidth of the connection will be 16 Gbps.



The Port Trunking Concept

Moxa has developed a port trunking protocol that provides the following benefits:

- Greater flexibility in setting up your network connections, since the bandwidth of a link can be doubled, tripled, or quadrupled.
- Redundancy—if one link is broken, the remaining trunked ports share the traffic within the trunk group.
- Load sharing—MAC client traffic can be distributed across multiple links.

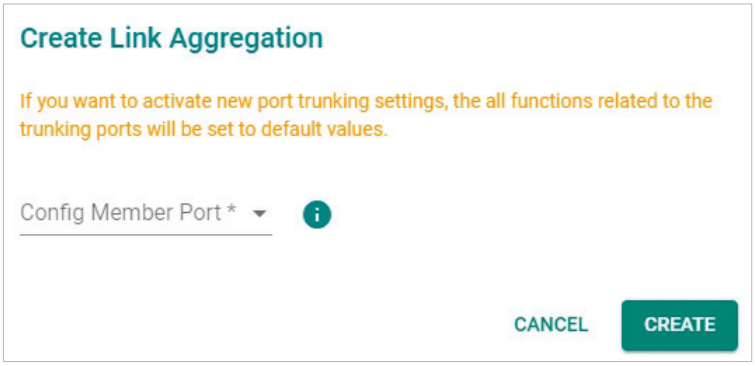
To avoid broadcast storms or loops in your network while configuring a trunk, first disable or disconnect all ports that you want to add to the trunk or remove from the trunk. After you finish configuring the trunk, enable or reconnect the ports.

Each Moxa industrial secure router can set a maximum of 4 port channel (trunking) groups. When you activate port trunking, certain settings on each port will be reset to factory default values or will be disabled:

- Communication redundancy will be reset
- 802.1Q VLAN will be reset
- Multicast Filtering will be reset
- Port Lock will be reset and disabled.
- Set Device IP will be reset
- Mirror will be reset

Create a Link Aggregation

Click the ⊞ icon on the Link Aggregation page.



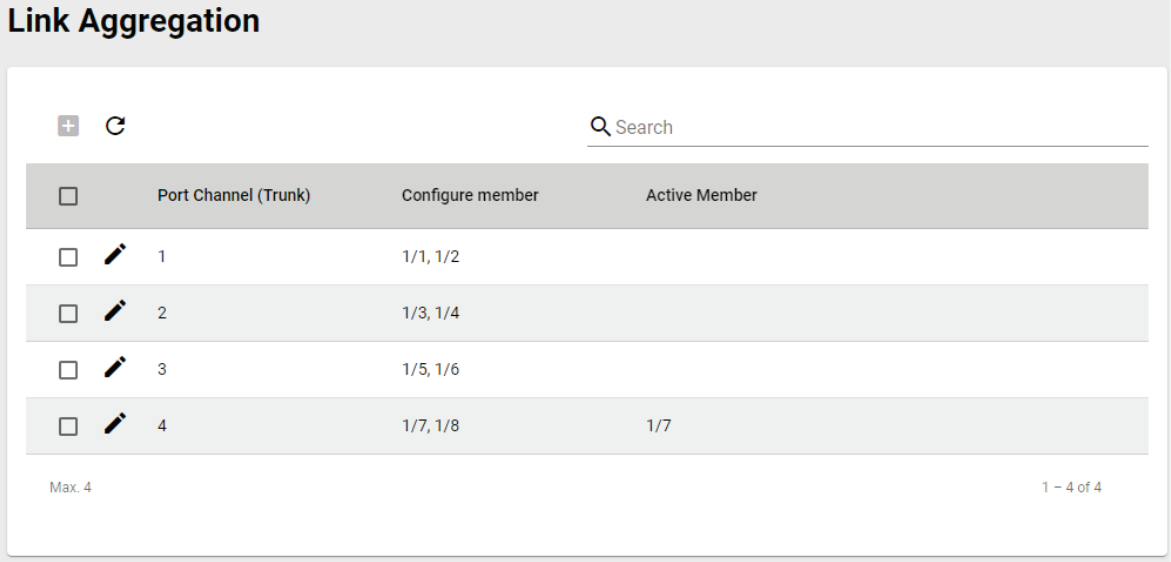
Config Member Port

Setting	Description	Factory Default
Port drop-down menu	Select the ports you want to add to the link aggregation group.	None

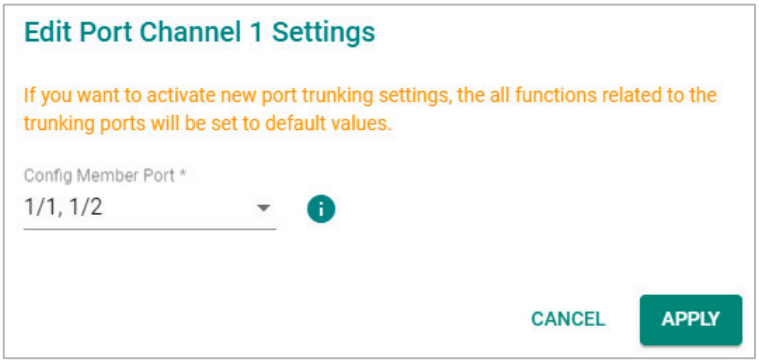
When finished, click **CREATE** to save your configuration.

Edit Existing Link Aggregation

Click the ✎ icon to modify the settings for each trunking port.

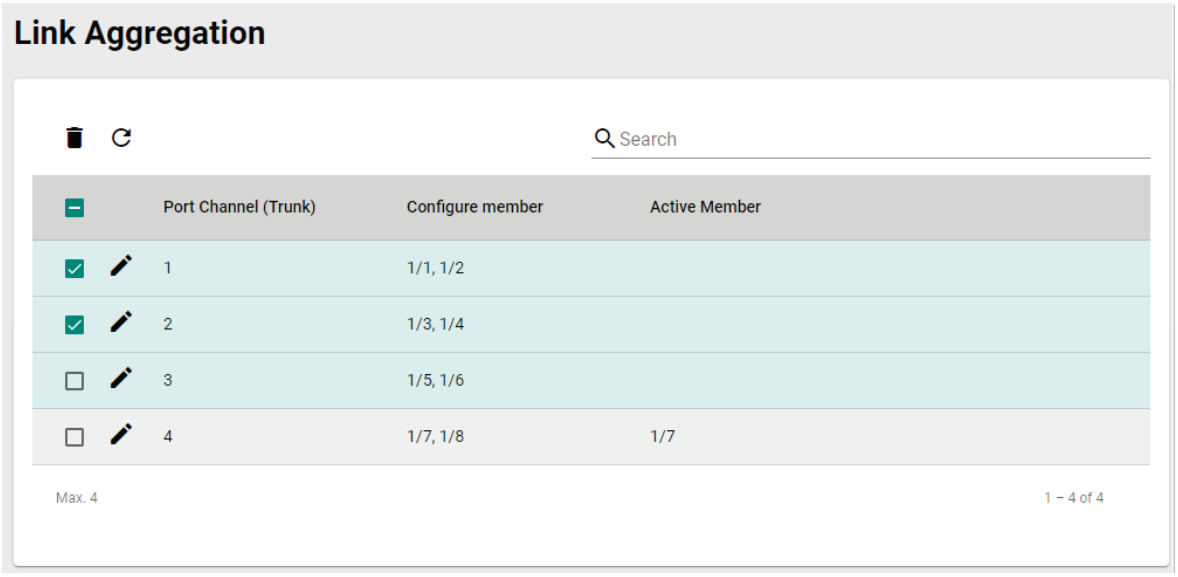


Select the ports you want to add to the link aggregation group and click **APPLY**.

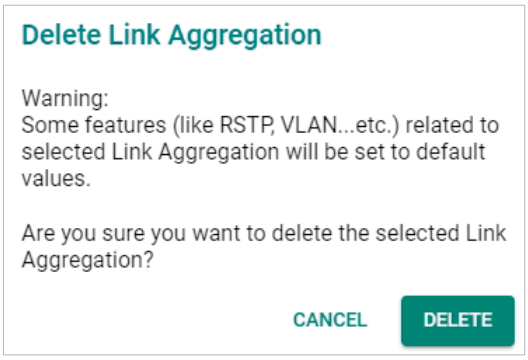


Delete a Link Aggregation

Select the link aggregation groups you want to delete in the Link Aggregation list and click the icon.

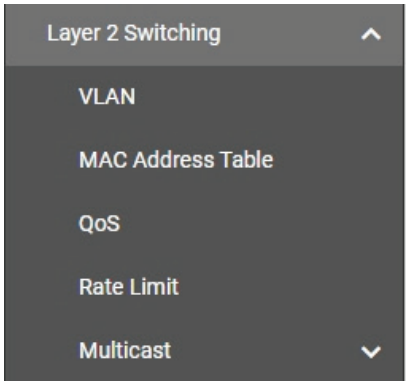


Click **DELETE** to delete the selected items.



Layer 2 Switching

From the **Layer 2 Switching** section, the following functions can be configured: **VLAN**, **MAC Address Table**, **QoS**, **Rate Limit**, and **Multicast**.



VLAN

Using Virtual LAN

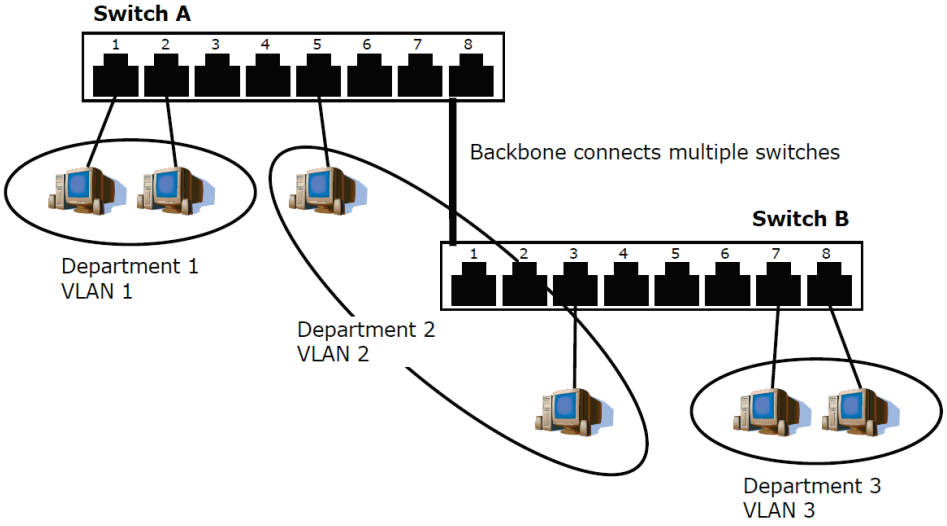
Setting up Virtual LANs (VLANs) on your Moxa industrial secure router increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

The VLAN Concept

What is a VLAN?

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

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



Benefits of VLANs

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

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

VLANs and the Moxa switch

- Your Moxa switch includes support for VLANs using IEEE Std 802.1Q-2005. This standard allows traffic from multiple VLANs to be carried across one physical link. The IEEE Std 802.1Q-2005 standard allows each port on your Moxa switch to be placed as follows:
- On a single VLAN defined in the switch
- On several VLANs simultaneously using 802.1Q tagging
- The standard requires that you define the 802.1Q VLAN ID for each VLAN on your Moxa switch before the switch can use it to forward traffic:

Managing a VLAN

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

- Management VLAN ID 1 can be changed
- 802.1Q VLAN default ID 1 cannot be deleted

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

Communication Between VLANs

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

VLANs: Tagged and Untagged Membership

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

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

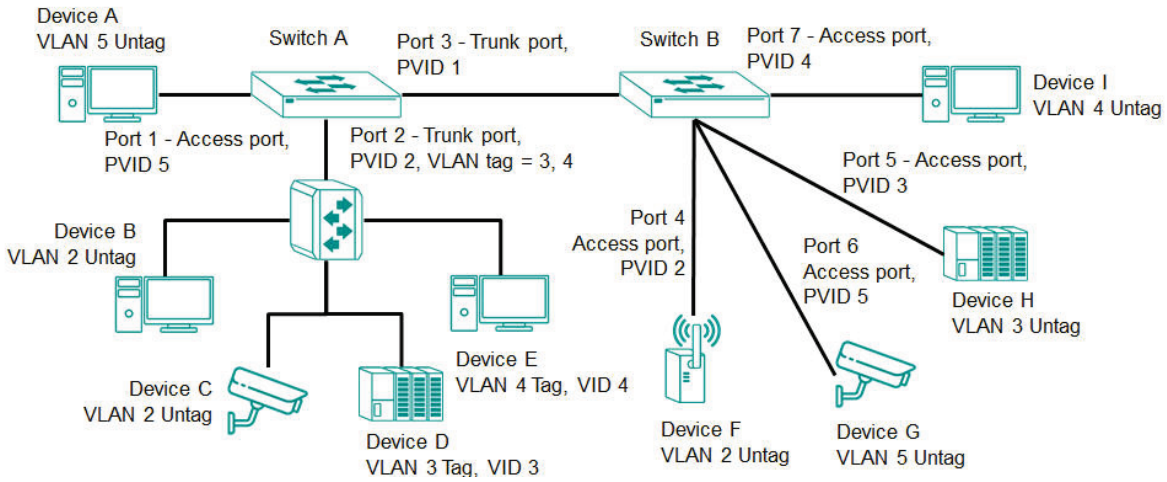
The IEEE Std 802.1Q-2005 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine which VLAN the port belongs to. If a frame is carrying the additional information, it is known as a tagged frame.

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

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

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

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



In this application:

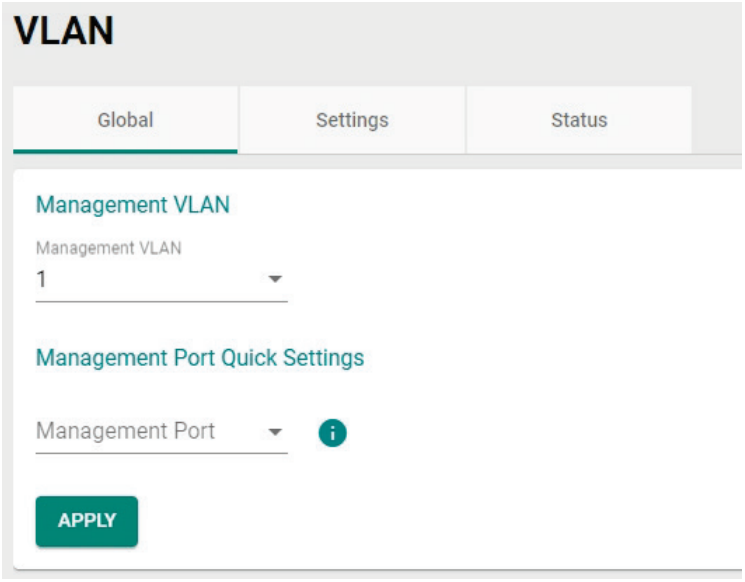
- Port 1 connects a single untagged device and assigns it to VLAN 5; it should be configured as an **Access Port** with PVID 5.
- Port 2 connects a LAN with two untagged devices belonging to VLAN 2. One tagged device with VID 3 and one tagged device with VID 4. It should be configured as a **Hybrid Port** with PVID 2 for untagged device and Fixed VLAN (Tagged) with 3 and 4 for tagged device. Since each port can only have one unique PVID, all untagged devices on the same port must belong to the same VLAN.
- Port 3 connects with another switch. It should be configured as a **Trunk Port**. GVRP protocol will be used through the Trunk Port.
- Port 4 connects a single untagged device and assigns it to VLAN 2; it should be configured as an **Access Port** with PVID 2.
- Port 5 connects a single untagged device and assigns it to VLAN 3; it should be configured as an **Access Port** with PVID 3.
- Port 6 connect a single untagged device and assigns it to VLAN 5; it should be configured as an **Access Port** with PVID 5.
- Port 7 connects a single untagged device and assigns it to VLAN 4; it should be configured as an **Access Port** with PVID 4.

After the application is properly configured:

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

Global

From the **Global** tab, you can configure management VLAN and port settings.



Management VLAN

Management VLAN

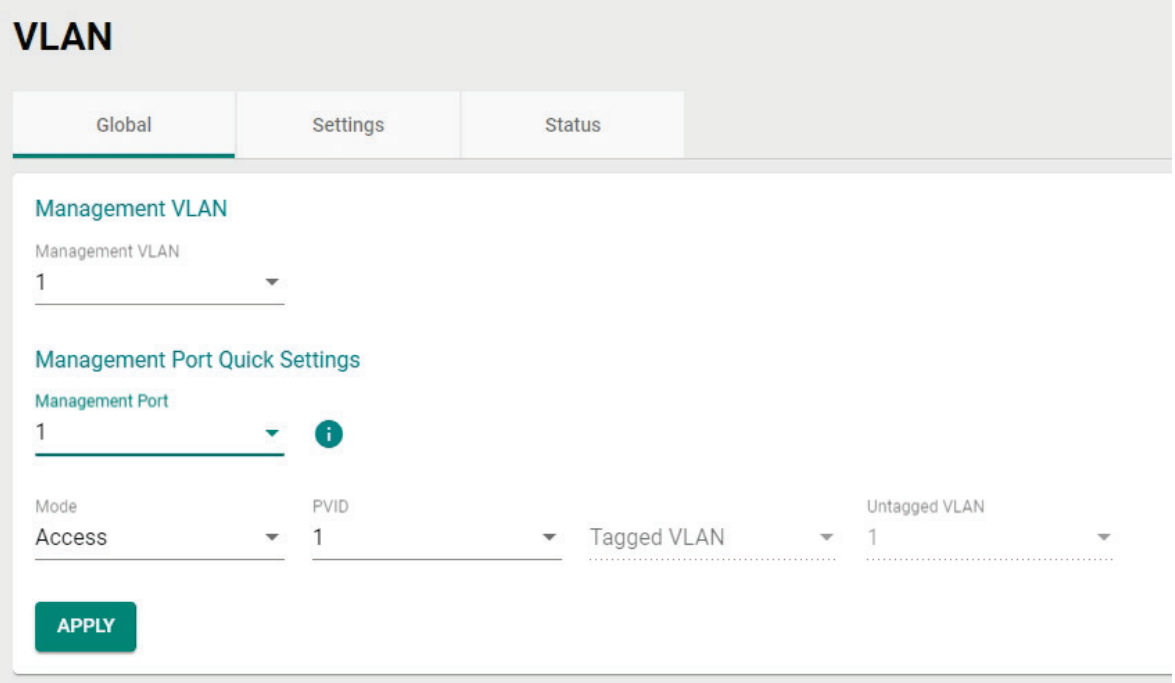
Setting	Description	Factory Default
1 to 16	Select the management VLAN ID from the drop-down menu.	1

Management Port Quick Settings

Use this for quick and easy configuration of VLAN settings for multiple ports at once.

Management Port

Setting	Description	Factory Default
1 to 10	Select the management port of this Moxa Industrial Secure Router for quick and easy configuration of VLAN settings for multiple ports at once. Set the Mode, PVID, Tagged VLAN ID, and Untagged VLAN ID and click **APPLY** button to create the VLAN ID configuration table.	None



Mode

Setting	Description	Factory Default
Access	Define the port as an Access port. This is used when connecting to single devices without tags.	Access
Trunk	Define the port as a Trunk port. This is used when connecting to another 802.1Q VLAN aware the Industrial Secure Router.	
Hybrid	Define the port as a Hybrid port. This is used when connecting tp another Access 802.1Q VLAN aware Industrial Secure Router or another LAN that combines tagged and/or untagged devices and/or other routers/hubs.	

PVID

Setting	Description	Factory Default
1 to 16	Set the default VLAN ID for untagged devices that connect to the port.	1

Tagged VLAN

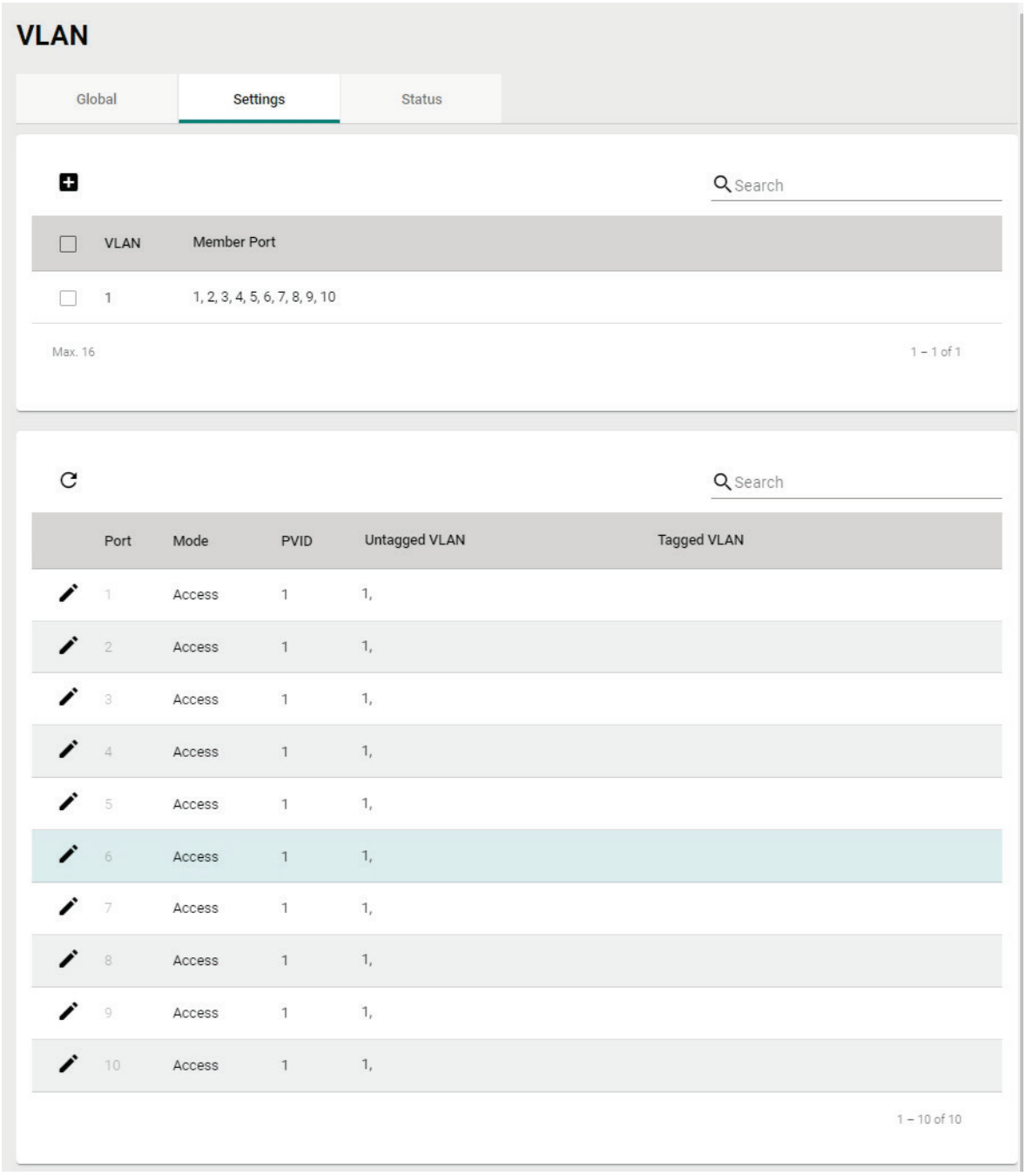
Setting	Description	Factory Default
All Member VIDs, 1 to 16	If the Mode is set to Trunk or Hybrid, set the other VLAN ID for tagged devices that connect to the port. Use commas to separate different VIDs.	Access mode: None Trunk or Hybrid mode: 1

Untagged VLAN

Setting	Description	Factory Default
All Member VIDs, 1 to 16	If the Mode is set to Trunk or Hybrid, set the other VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets. Use commas to separate different VIDs.	Access mode: 1 Trunk or Hybrid mode: None

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

Settings


VLAN
Global
Settings
Status
Search
VLAN
Member Port
1
1, 2, 3, 4, 5, 6, 7, 8, 9, 10
Max. 16
1 – 1 of 1
Search
Port
Mode
PVID
Untagged VLAN
Tagged VLAN
1 Access 1 1,
2 Access 1 1,
3 Access 1 1,
4 Access 1 1,
5 Access 1 1,
6 Access 1 1,
7 Access 1 1,
8 Access 1 1,
9 Access 1 1,
10 Access 1 1,
1 – 10 of 10

Create a VLAN

Click the icon to create a VLAN.

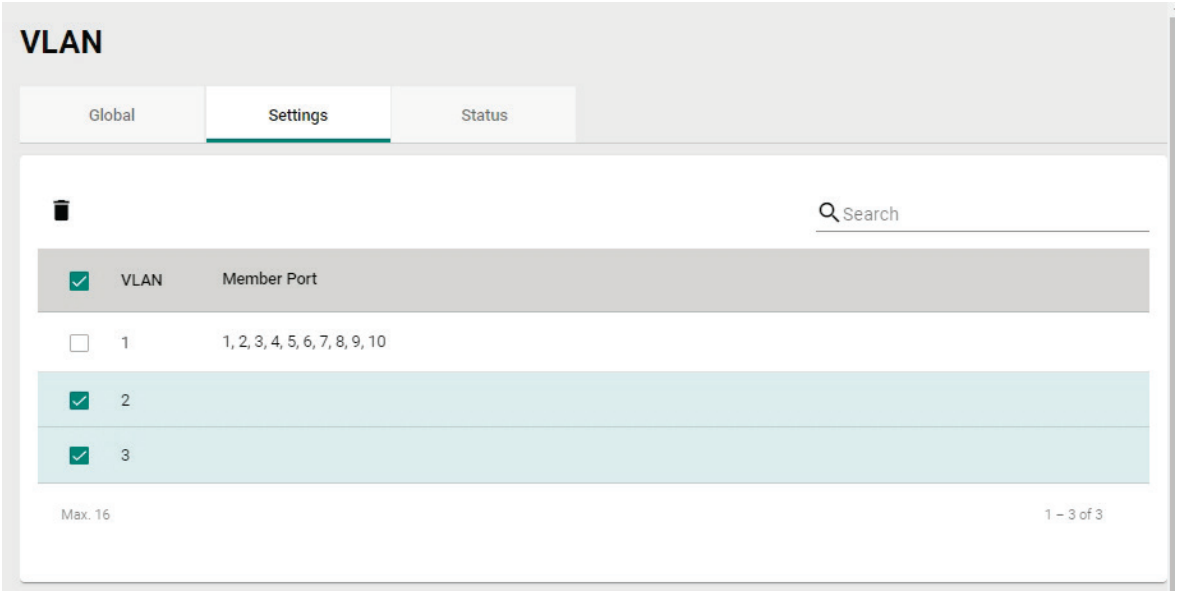
VID

Setting	Description	Factory Default
VLAN ID, max. 16 VLANs	Specify the VLAN ID. You can create multiple VLANs at once by entering single VLAN IDs or a range of IDs. For example, 2, 4-8, 10-13.	None

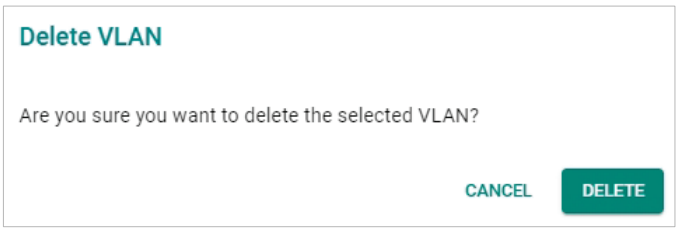
When finished, click **CREATE** to create the VLAN.

Delete a VLAN

Select the VLAN you want to delete from the list and click the icon.

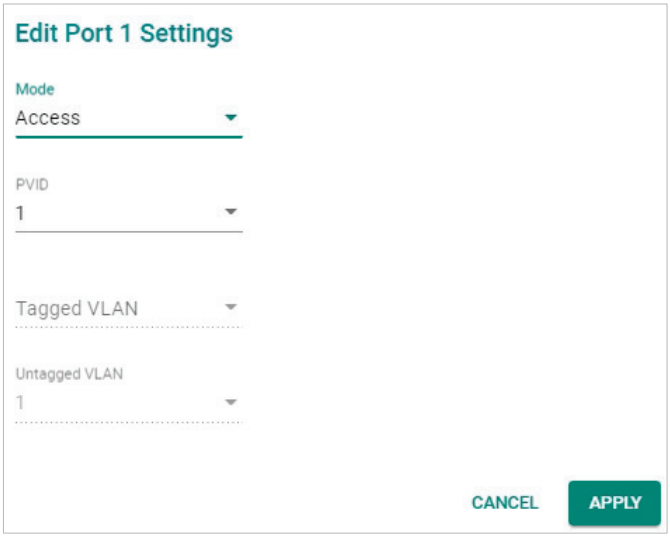


Click **DELETE** to delete the selected items.



Modify the Port Settings

Click ✎ to modify the settings of the corresponding VLAN entry.



Mode

Setting	Description	Factory Default
Access	Define the port as an Access port. This is used when connecting to single devices without tags.	Access
Trunk	Define the port as a Trunk port. This is used when connecting to another 802.1Q VLAN aware the Industrial Secure Router.	
Hybrid	Define the port as a Hybrid port. This is used when connecting to another Access 802.1Q VLAN aware Industrial Secure Router or another LAN that combines tagged and/or untagged devices and/or other routers/hubs.	

PVID

Setting	Description	Factory Default
1 to 16	Set the default VLAN ID for untagged devices that connect to the port.	1

Tagged VLAN

Setting	Description	Factory Default
All Member VIDs, 1 to 16	If the Mode is set to Trunk or Hybrid, set the other VLAN ID for tagged devices that connect to the port. Use commas to separate different VIDs.	Access mode: None Trunk or Hybrid mode: 1

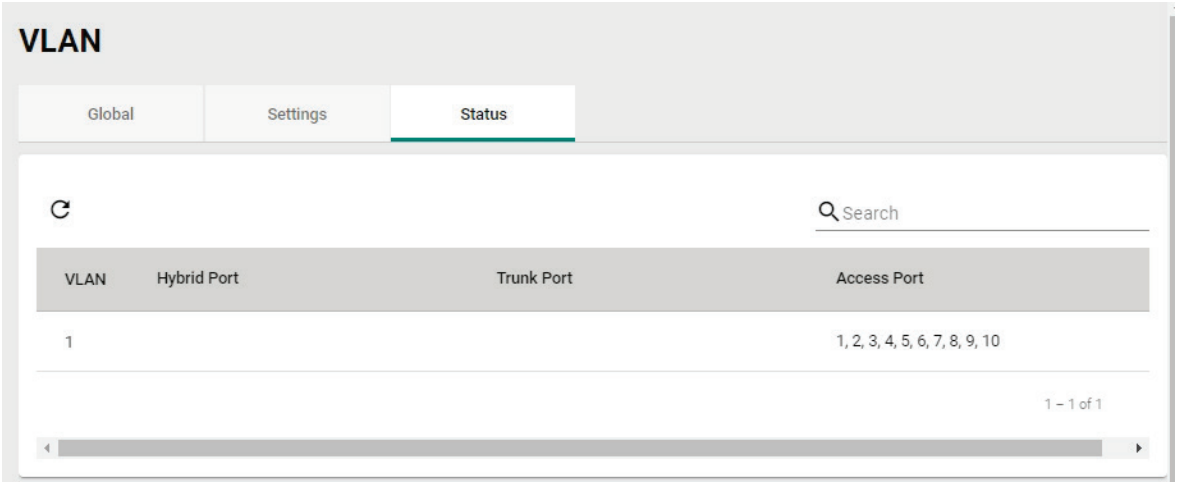
Untagged VLAN

Setting	Description	Factory Default
All Member VIDs, 1 to 16	If the Mode is set to Trunk or Hybrid, set the other VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets. Use commas to separate different VIDs.	Access mode: 1 Trunk or Hybrid mode: None

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

Status

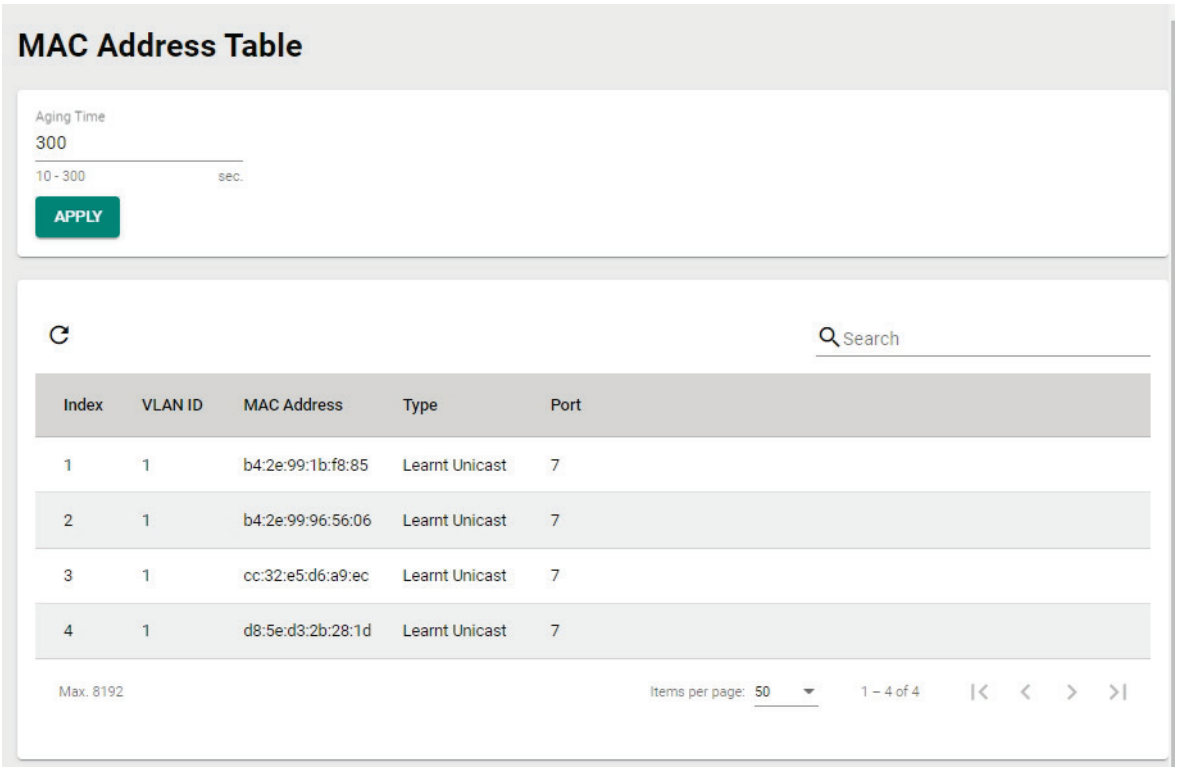
From the **Status** tab, you can review created VLAN groups, joined access ports, trunk ports, and hybrid ports. Click the icon to refresh the information in the VLAN Status Table.



MAC Address Table

The MAC Address Table shows the MAC address of devices that go through the Moxa industrial secure router. The Aging Time (10 to 300 seconds) is the duration that a MAC address entry can remain in the Moxa router's MAC Address Table before it is removed. Once a MAC address is removed, the Industrial Secure Router will no longer forward frames originating from this MAC address.

To modify the Aging Time, specify the duration (in seconds) and click **Apply**.



You can quickly filter MAC addresses by entering one of the following criteria into the Search field.

Learnt Unicast	Show all learnt Unicast MAC addresses.
Static	Show all Static, Static Lock, and Static Multicast MAC addresses.
Multicast	Show all Static Multicast MAC addresses.
Port x	Show all MAC addresses associated with a specific port.

The table displays the following information:

VLAN ID	This field shows the VLAN ID.
MAC Address	This field shows the MAC address.
Type	This field shows the type of this MAC address.
Port	This field shows the port that this MAC address belongs to.

QoS

This section describes how Quality of Service (QoS) works and how to configure the relevant settings. There are three main functions in this section: **CoS Mapping**, **DSCP Mapping**, and **Port Classification**.

QoS Overview

The switch's traffic prioritization capability provides Quality of Service (QoS) to your network by making data delivery more reliable. You can prioritize traffic on your network to ensure that high priority data is transmitted with minimum delay. Traffic can be controlled by a set of rules to obtain the required Quality of Service for your network. The rules define different types of traffic and specify how each type should be treated as it passes through the switch. The switch can inspect both IEEE 802.1p/1Q Layer 2 CoS (Class of Service) tags, and even Layer 3 DSCP (Differentiated Services Code Point) information to provide consistent classification of the entire network. The switch's QoS capability improves the performance and determinism of industrial networks for mission-critical applications.

The Traffic Prioritization Concept

Traffic prioritization allows you to prioritize data so that time-sensitive and system-critical data can be transferred smoothly and with minimal delay over a network. The benefits of using traffic prioritization are:

- Improve network performance by controlling a wide variety of traffic and by managing congestion.
- Assign priorities to different categories of traffic. For example, set higher priorities for time-critical or mission-critical applications.
- Provide predictable throughput for multimedia applications, such as video conferencing or voice over IP, and minimize traffic delay and jitter.
- Optimize the network utilization depending on application usage and usage needs. Hence, asset owners do not always need to expand their backbone bandwidth as the amount of traffic increases.

Traffic prioritization uses eight traffic queues to ensure that higher priority traffic can be forwarded separately from lower priority traffic, which guarantees Quality of Service (QoS) to your network.

Moxa switch traffic prioritization is based on two standards:

- **IEEE 802.1p**—a Layer 2 QoS marking scheme
- **Differentiated Services (DiffServ)**—a Layer 3 QoS marking scheme.

IEEE 802.1p Class of Service

The IEEE Std 802.1D 2005 Edition marking scheme, which is an enhancement to IEEE Std 802.1D, enables Quality of Service on the LAN. Traffic service levels are defined in the IEEE 802.1Q 4-byte tag, which is used to carry VLAN identification as well as IEEE 802.1p priority information. The IEEE 802.1p occupying 3 bits of the tag follows the destination MAC address and Source MAC address.

The IEEE Std 802.1D 2005 Edition priority marking scheme assigns an IEEE 802.1p priority level between 0 and 7 to each frame, which specifies the level of service that the associated packets will be handled with. The table below shows an example of how different traffic types can be mapped to the eight IEEE 802.1p priority levels.

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

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

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

Differentiated Services (DiffServ) Traffic Marking

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

The advantages of DiffServ over IEEE 802.1Q are as follows:

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

Traffic Prioritization

Moxa switches classify traffic based on Layer 2 of the OSI 7 Layer model, and the switch prioritizes outbound traffic according to the priority information defined in the received packet. Incoming traffic is classified based upon the IEEE 802.1p service level field and is assigned to the appropriate egress priority queue. The traffic flow through the switch is as follows:

- A packet received by the Moxa switch may or may not have an 802.1p tag associated with it. If it does not, then it is given a default CoS value (according to the port settings in the classification section). Alternatively, the packet might be marked with a new 802.1p value, which will result in all knowledge of the previous 802.1p tag being lost.
- Each egress queue has associated 802.1p priority levels, and can be defined by users, the packet will be placed in the appropriate priority queue. When the packet reaches the head of its queue and is about to be transmitted, the device determines whether or not the egress port belongs to the VLAN group. If it is, then the new 802.1p tag is used in the extended 802.1D header.

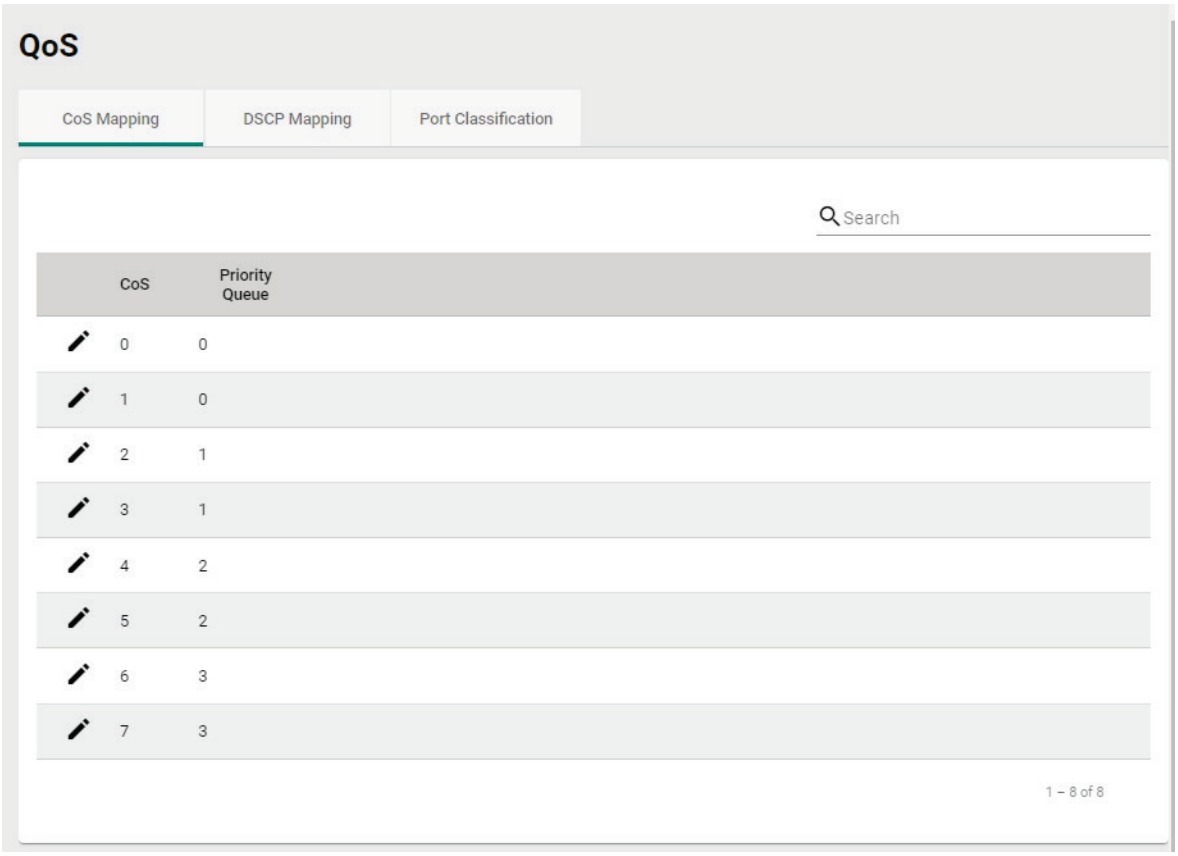
Traffic Queues

The hardware of Moxa switches has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the Moxa switch without being delayed by lower priority traffic. As each packet arrives in the Moxa switch, it undergoes ingress processing (which includes classification, marking/re-marking), and is then sorted into the appropriate queue. The switch then forwards packets from each queue.

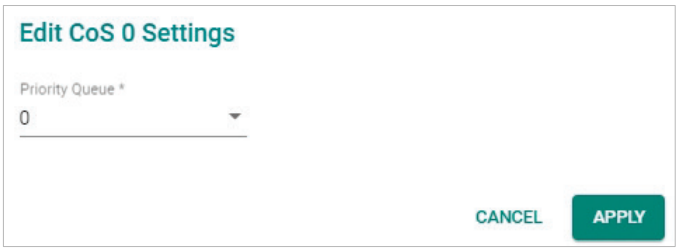
Moxa switches support two different queuing mechanisms:

- **Weight Fair:** This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, the Weight Fair method gives high priority precedence over low priority, but in the event that high priority traffic does not reach the link capacity, lower priority traffic is not blocked.
- **Strict:** This method services high traffic queues first; low priority queues are delayed until no more high priority data needs to be sent. The Strict method always gives precedence to high priority over low priority.

CoS Mapping



Click the ✎ icon to configure the priority queue settings of the corresponding CoS level.

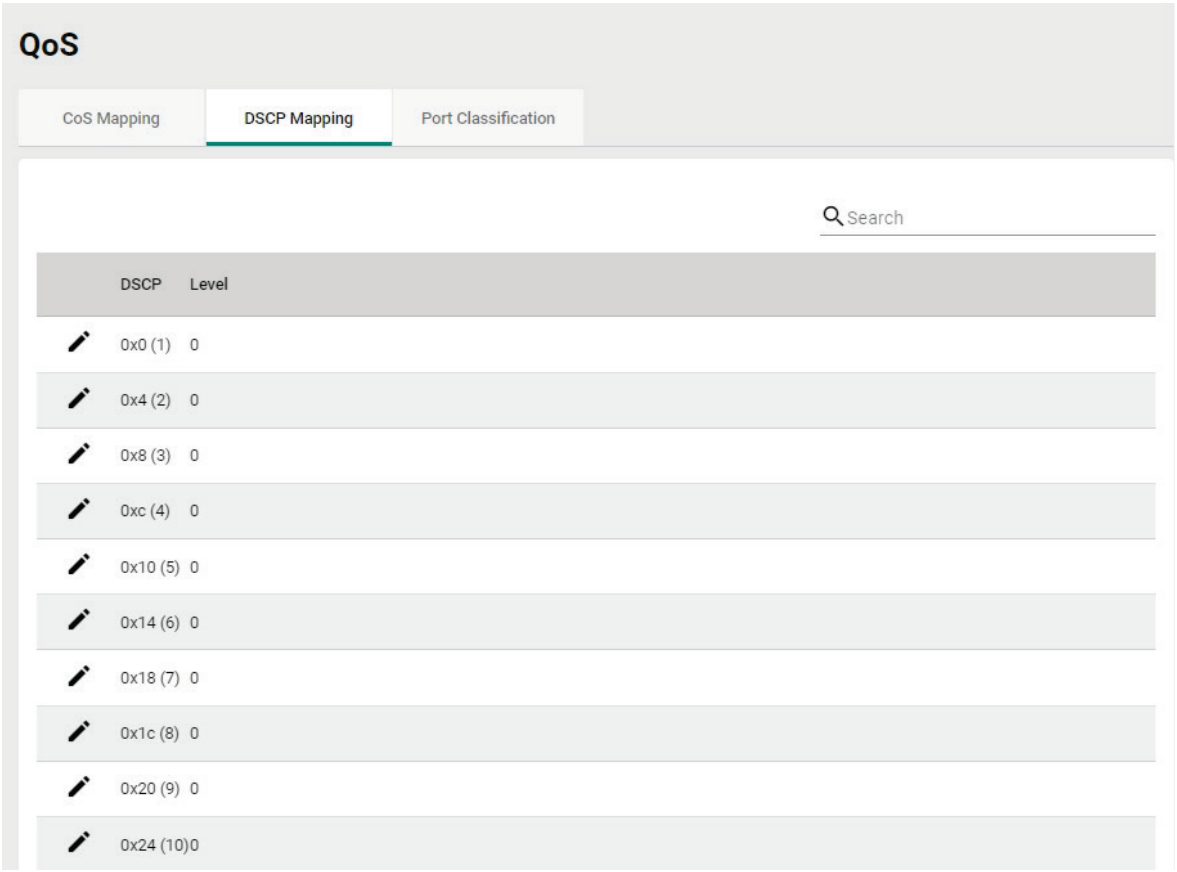


Priority Queue

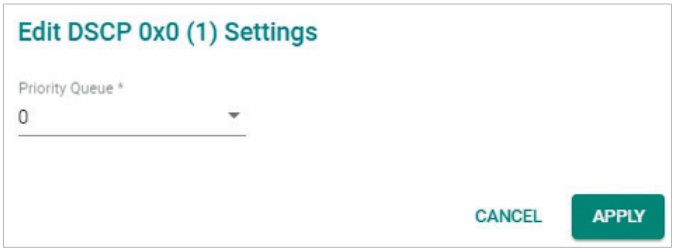
Setting	Description	Factory Default
0 to 3	Select the priority queue to map to the CoS level.	0 to 3

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

DSCP Mapping



Click the ✎ icon to configure the priority queue settings of the corresponding DSCP value.

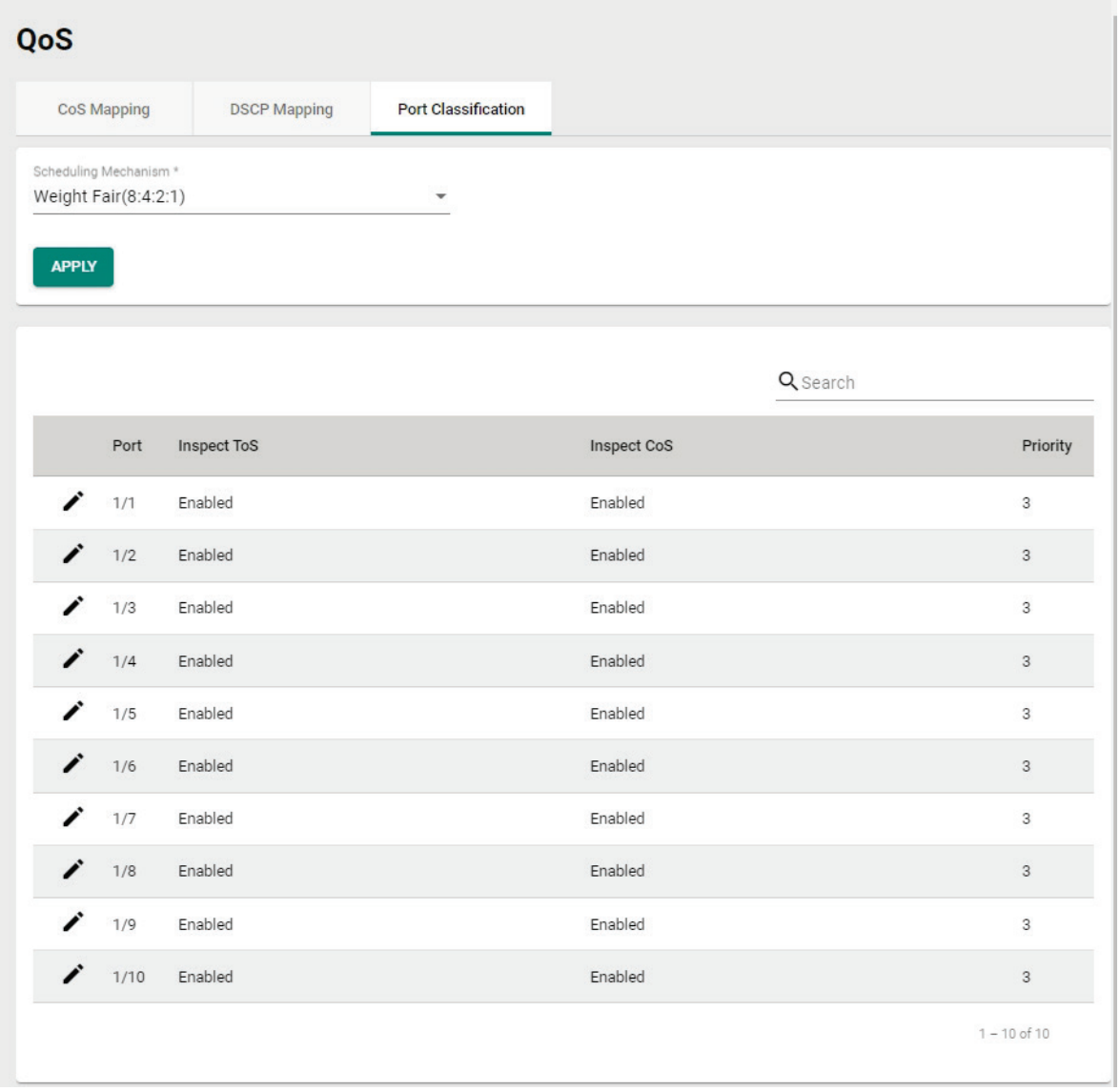


Priority Queue

Setting	Description	Factory Default
0 to 3	Select the egress queue to map to the ToS value.	0 to 3

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

Port Classification



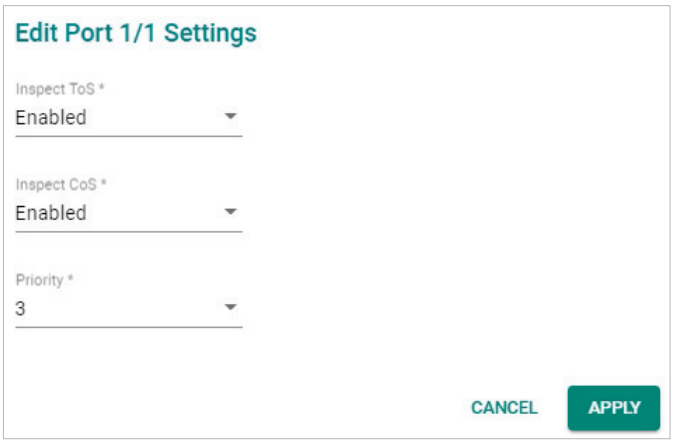
The Moxa switch supports inspection of Layer 3 ToS and/or Layer 2 CoS tag information to determine how to classify traffic packets.

Scheduling Mechanism

Setting	Description	Factory Default
Weight Fair(8:4:2:1)	The Moxa industrial secure router has 4 priority queues. In the weight fair scheme, an 8, 4, 2, 1 weighting is applied to the four priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.	Weight Fair(8:4:2:1)
Strict(High Priority First Always)	In the Strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures that all high priority frames will egress the switch as soon as possible.	

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

Click the icon to configure the Inspect type and Queue priority for the corresponding port.



Inspect ToS

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable inspection of Type of Service (ToS) bits in the IPV4 frame to determine the priority of each frame.	Enabled

Inspect COS

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable inspection of 802.1p CoS tags in the MAC frame to determine the priority of each frame.	Enabled

Priority

Setting	Description	Factory Default
0 to 7	Specify the priority. The port priority ranges from 0 (lowest) to 7 (highest).	3

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

NOTE

The priority of an ingress frame is determined in the following order:

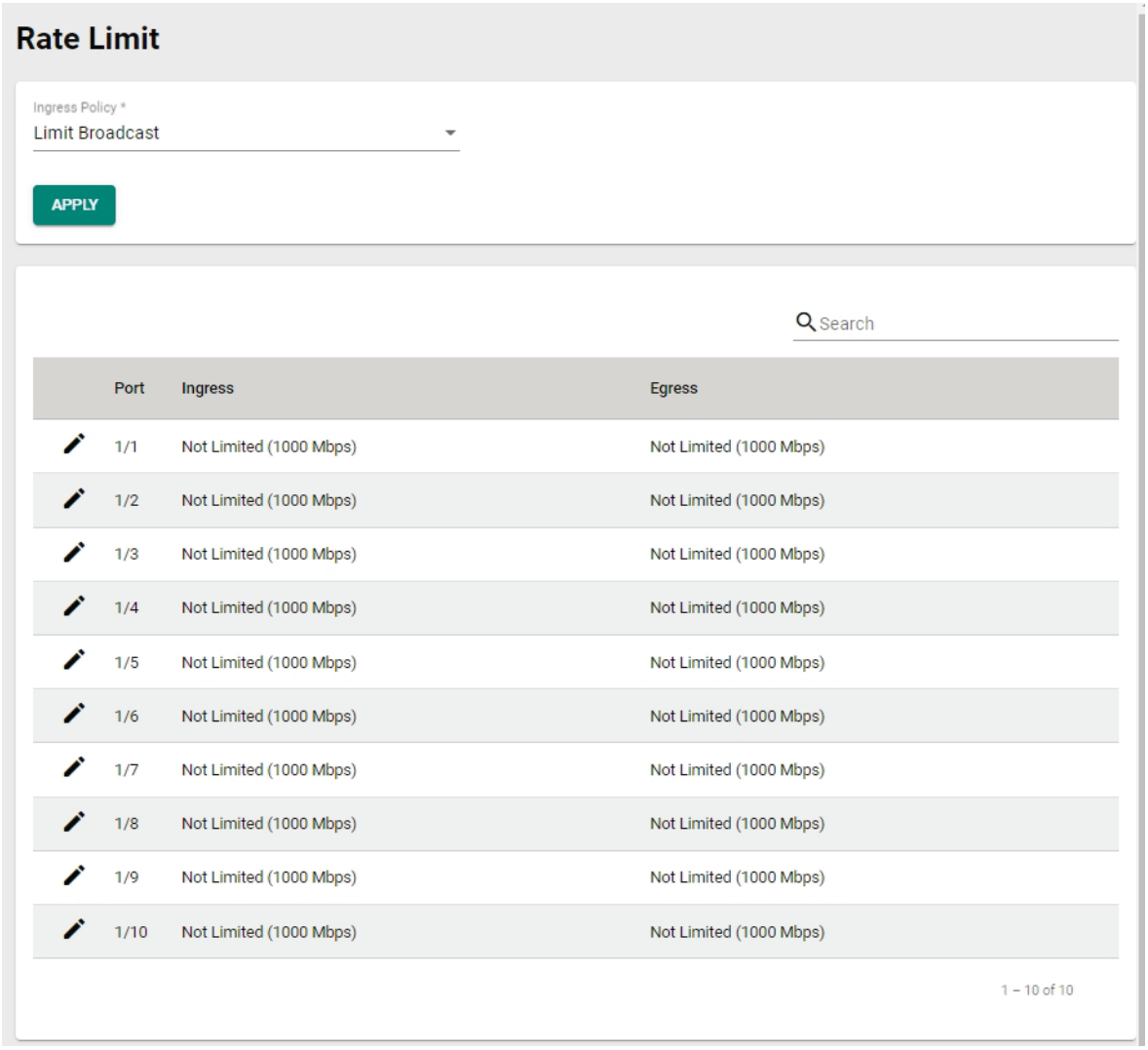
1. Inspect CoS
2. Inspect ToS
3. Port Priority

NOTE

These classifications can be enabled individually or as a combination. For instance, if a "hot" higher priority port is required for a network design, **Inspect TOS** and **Inspect CoS** can be disabled. This setting leaves only port default priority active, which results in all ingress frames being assigned the same priority on that port.

Rate Limiting

In general, one host should not be allowed to occupy unlimited bandwidth, particularly when the device malfunctions. For example, so-called "broadcast storms" could be caused by an incorrectly configured topology, or a malfunctioning device. Moxa industrial secure routers not only prevent broadcast storms but can also be configured to have a different ingress rate for all packets, giving administrators full control of their limited bandwidth to prevent undesirable effects caused by unpredictable faults.

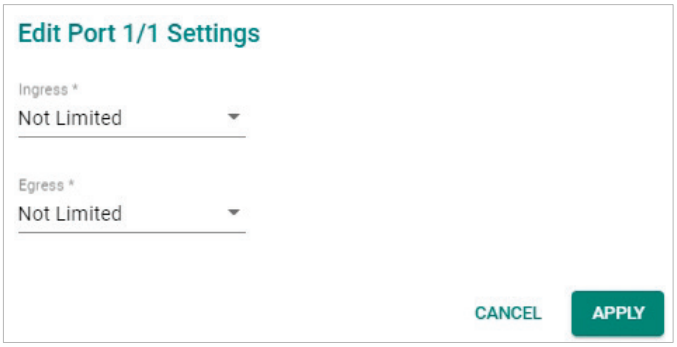


Ingress Policy

Setting	Description	Factory Default
Limit All	Select the ingress rate limit for different packet types.	Limit Broadcast
Limit Broadcast, Flooded Unicast		
Limit Broadcast, Multicast		
Limit Broadcast		

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

Click the ✎ icon to configure the Ingress and Egress rate for the corresponding port.



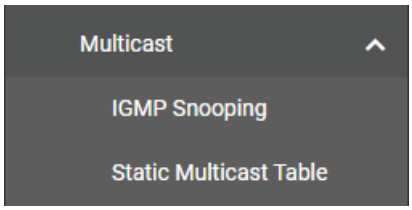
Ingress/Egress

Setting	Description	Factory Default
Not Limited, 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%	Select the ingress/egress rate limit (% of max. throughput) for all packets.	Not Limited

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

Multicast

Multicast filtering improves the performance of networks that carry multicast traffic. This section covers the IGMP Snooping and Static Multicast Table pages, and explains how multicast filtering can be implemented on your Moxa industrial secure router.



The Concept of Multicast Filtering

What is an IP Multicast?

A *multicast* is a packet sent by one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. If the network is set up correctly, a multicast can only be sent to an end-station or a subset of end-stations on a LAN or VLAN that belong to the multicast group. Multicast group members can be distributed across multiple subnets, so that multicast transmissions can occur within a campus LAN or over a WAN. In addition, networks that support IP multicast send only *one* copy of the desired information across the network until the delivery path that reaches group members diverges. To make more efficient use of network bandwidth, it is only at these points that multicast packets are duplicated and forwarded. A multicast packet has a multicast group address in the destination address field of the packet's IP header.

Benefits of Multicast

The benefits of using IP multicast are:

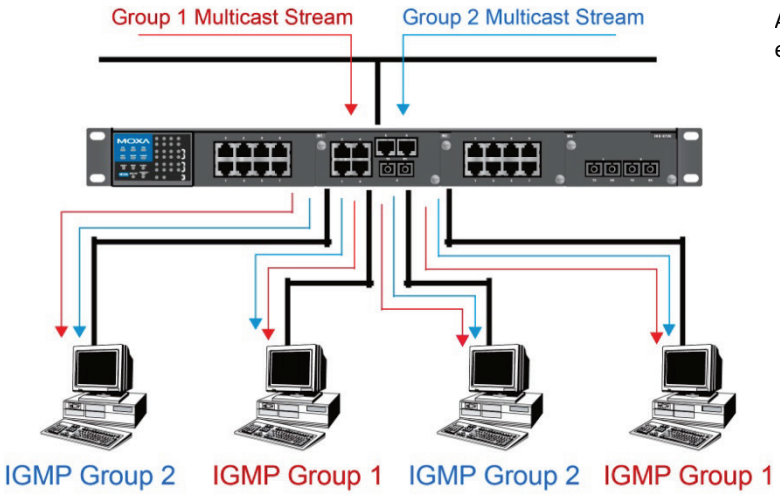
- It uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- It reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- It makes efficient use of network bandwidth and scales well as the number of multicast group members increases.
- Works with other IP protocols and services, such as Quality of Service (QoS).

Multicast transmission makes more sense and is more efficient than unicast transmission for some applications. For example, multicasts are often used for video-conferencing, since high volumes of traffic must be sent to several end-stations at the same time, but where broadcasting the traffic to all end-stations would cause a substantial reduction in network performance. Furthermore, several industrial automation protocols, such as Allen-Bradley, EtherNet/IP, Siemens Profibus, and Foundation Fieldbus HSE (High Speed Ethernet), use multicast. These industrial Ethernet protocols use publisher/subscriber communications models by multicasting packets that could flood a network with heavy traffic. IGMP Snooping is used to prune multicast traffic so that it only travels to those end destinations that require the traffic, reducing the amount of traffic on the Ethernet LAN.

Multicast Filtering

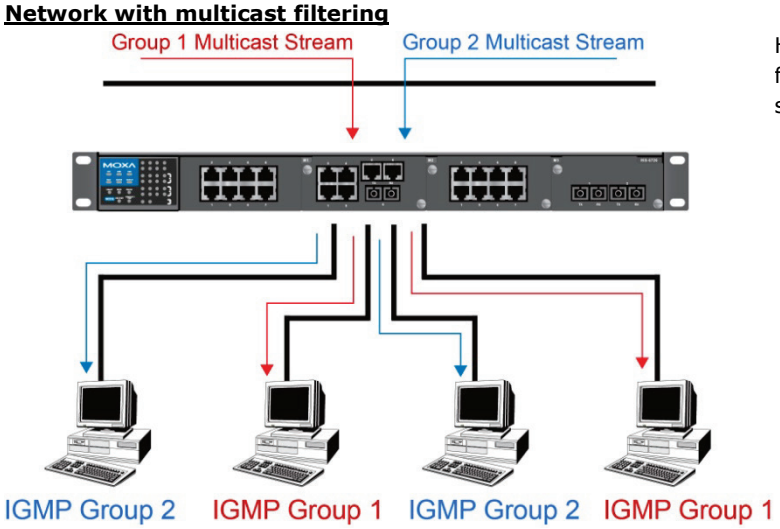
Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following two figures illustrate how a network behaves without multicast filtering, and with multicast filtering.

Network without multicast filtering



All hosts receive the multicast traffic, even if they don't need it.

Network with multicast filtering



Hosts only receive dedicated traffic from other hosts belonging to the same group.

Multicast Filtering and Moxa's Industrial Secure Routers

The Moxa industrial secure router has two ways to achieve multicast filtering: IGMP (Internet Group Management Protocol) Snooping and adding a static multicast MAC manually to filter multicast traffic automatically.

Snooping Mode

Snooping Mode allows your industrial secure router to forward multicast packets only to the appropriate ports. The router **snoops** on exchanges between hosts and an IGMP device to find those ports that want to join a multicast group, and then configures its filters accordingly.

Query Mode

Query Mode allows the Moxa router to work as the Querier if it has the lowest IP address on the subnetwork to which it belongs.

IGMP querying is enabled by default on the Moxa router to ensure proceeding query election. Enable query mode to run multicast sessions on a network that does not contain IGMP routers (or queriers). Query mode allows users to enable IGMP Snooping by VLAN ID. The Moxa industrial secure router supports IGMP Snooping Version 1, Version 2, and Version 3. Version 2 is compatible with version 1. The default setting is IGMP V1/V2.

IGMP Multicast Filtering

IGMP is used by IP-supporting network devices to register hosts with multicast groups. It can be used on all LANs and VLANs that contain a multicast-capable IP router, and on other network devices that support multicast filtering. Moxa switches support IGMP Version 1, 2, and 3. IGMP Version 1 and 2 work as follows:

- The IP router (or querier) periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IP router, the router with the lowest IP address is the querier. A switch with an IP address lower than the IP address of any other IGMP queriers connected to the LAN or VLAN can become the IGMP querier.
- When an IP host receives a query packet, it sends a report packet back that identifies the multicast group that the end-station would like to join.
- When the report packet arrives at a port on a switch with IGMP Snooping enabled, the switch knows that the port should forward traffic for the multicast group, and then proceeds to forward the packet to the router.
- When the router receives the report packet, it registers that the LAN or VLAN requires traffic for the multicast groups.
- When the router forwards traffic for the multicast group to the LAN or VLAN, the switches only forward the traffic to ports that received a report packet.

IGMP Version 3 supports "source filtering," which allows the system to define how to treat packets from specified source addresses. The system can either allow-list or deny-list specified sources.

IGMP version comparison

IGMP Version	Main Features	Reference
V1	a. Periodic query	RFC-1112
V2	Compatible with V1 and adds: a. Group-specific query b. Leave group messages c. Resends specific queries to verify leave message was the last one in the group d. Querier election	RFC-2236
V3	Compatible with V1, V2 and adds: a. Source filtering • Accept multicast traffic from a specified source • Accept multicast traffic from any source except the specified source	RFC-3376

Static Multicast MAC

Some devices may support multicast packets, but not support IGMP Snooping. The Moxa industrial secure router supports adding multicast groups manually to enable multicast filtering.

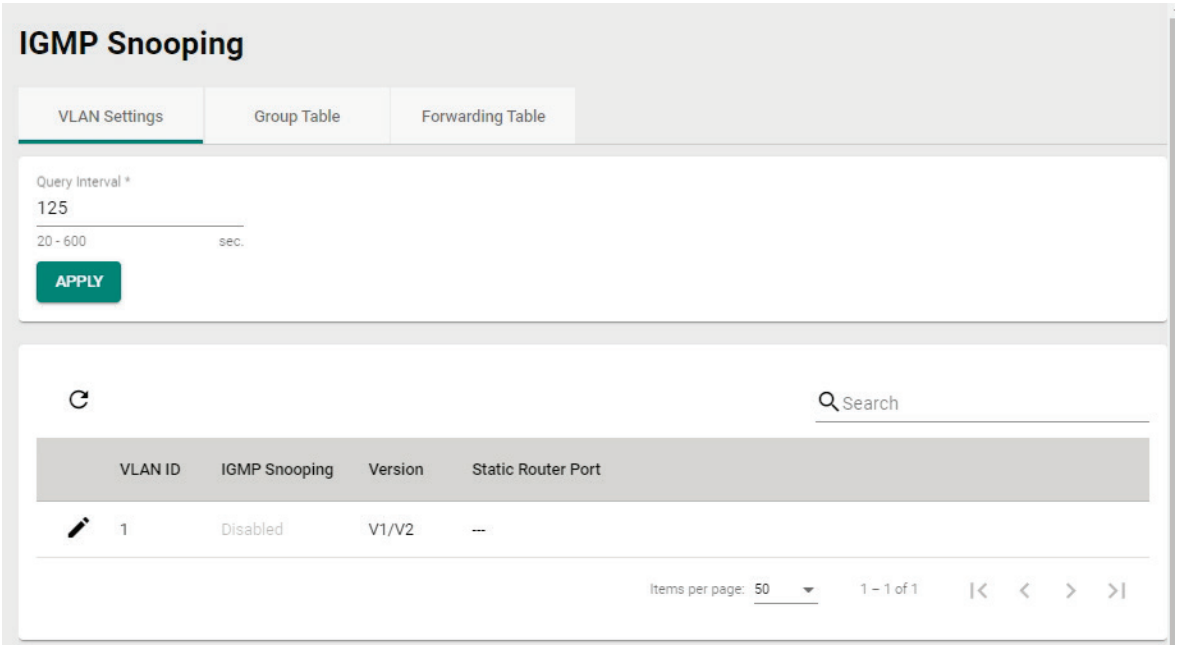
Enabling Multicast Filtering

Use the USB console or web interface to enable or disable IGMP Snooping and IGMP querying. If IGMP Snooping is not enabled, then IP multicast traffic is always forwarded, flooding the network.

IGMP Snooping

IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic, thereby reducing the amount of traffic on the Ethernet LAN.

VLAN Settings



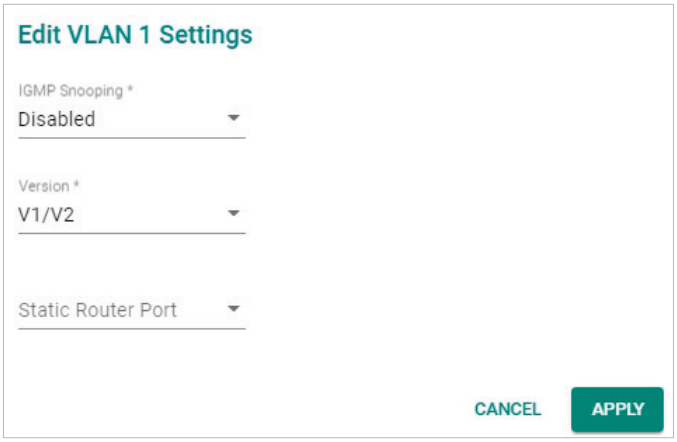
Query Interval

Setting	Description	Factory Default
20 - 600 seconds	Sets the query interval of the Querier function globally.	125 seconds

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

Modify Existing VLAN Settings

Click the ✎ icon to modify the settings of the corresponding VLAN.



IGMP Snooping

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the IGMP Snooping function for that particular VLAN.	Disabled

Version

Setting	Description	Factory Default
V1/V2, V3	If IGMP Snooping is enabled, select the IGMP Snooping version. V1/V2: Enable the Moxa Industrial Secure Router to send IGMP Snooping Version 1 and 2 queries. V3: Enable the Moxa Industrial Secure Router to send IGMP Snooping Version 3 queries.	V1/V2

Static Router Port

Setting	Description	Factory Default
1/1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 1/9, 1/10 checkbox	If IGMP Snooping is enabled, select the ports that will connect to the multicast routers. These ports will receive all multicast packets from the source.	None

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

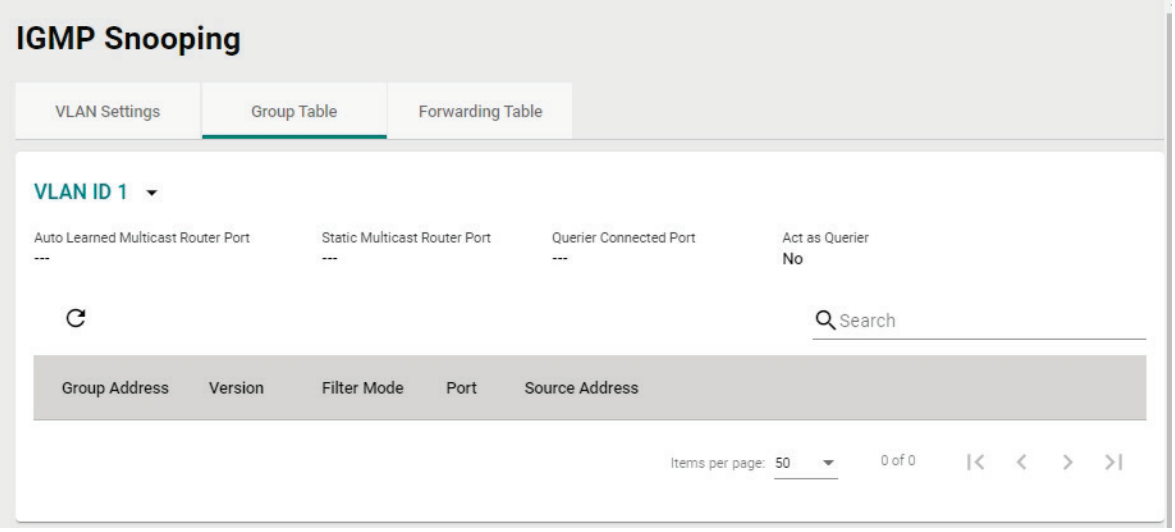
NOTE

If a router or Layer 3 switch is connected to the network, it will act as the Querier. Consequently, this Querier option will be disabled on all Moxa Layer 2 switches.

If all switches on the network are Moxa Layer 2 switches, then only one Layer 2 switch will act as Querier.

Group Table

The IGMP Snooping Group Table displays the currently active IGMP groups that were detected for each VLAN.

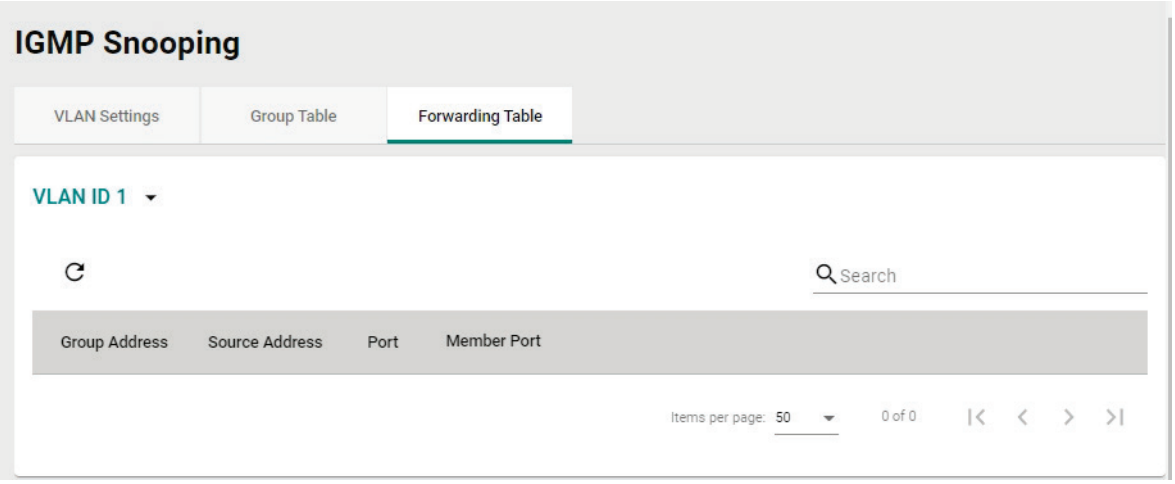


The information shown in the table includes:

- **Auto Learned Multicast Router Port:** This indicates that a multicast router connects to/sends packets from these port(s).
- **Static Multicast Router Port:** Displays the static multicast querier port(s).
- **Querier Connected Port:** Displays the port which is connected to the querier.
- **Act as a Querier:** Displays whether or not this VLAN is a querier (winner of an election).
- **Group Address:** Displays the multicast group addresses.
- **Version:** Displays the IGMP Snooping version.
- **Filter Mode:** Indicates the multicast source address is included or excluded. Displays Include or Exclude when IGMP v3 is enabled.
- **Port:** Displays the port which receives the multicast stream/the port the multicast stream is forwarded to.
- **Source Address:** Displays the multicast source address when IGMP v3 is enabled.

Forwarding Table

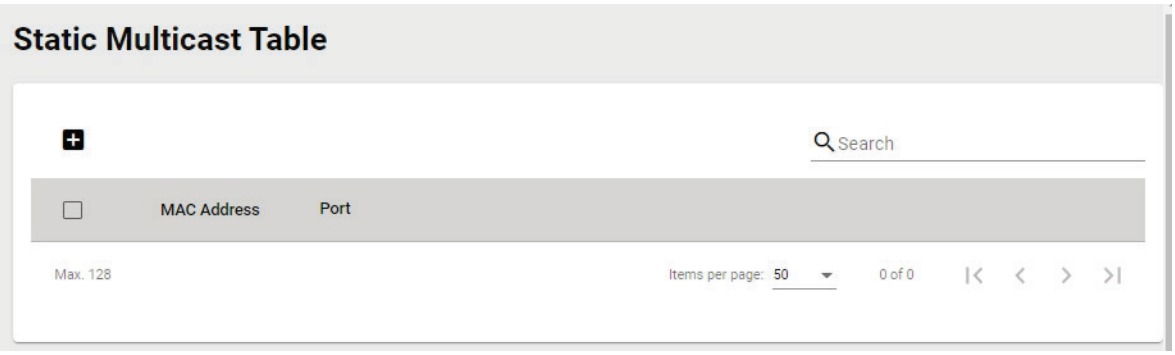
The Forwarding Table shows the multicast stream forwarding status for each VLAN. Select a VLAN ID from the drop-down menu to view the forwarding table for that VLAN ID.



- **Group Address:** Displays the multicast group IP address.
- **Source Address:** Displays the multicast source IP address.
- **Port:** Displays the port which receives the multicast stream.
- **Member port:** Displays the port the multicast stream is forwarded from.

Static Multicast Table

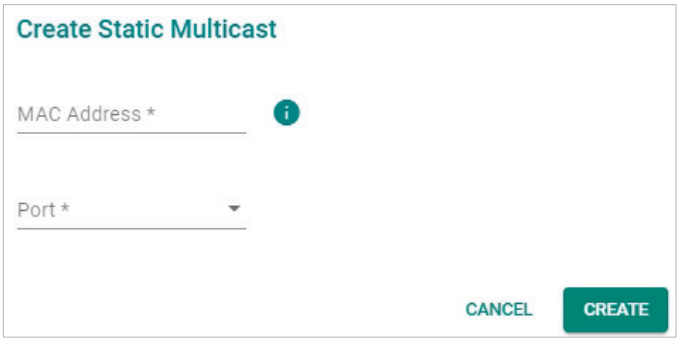
From the Static Multicast Table, you can create static multicast entries.



NOTE

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

Click the ⊞ icon to create a new static multicast entry.



MAC Address

Setting	Description	Factory Default
Integer	Enter the Static Multicast MAC address.	None

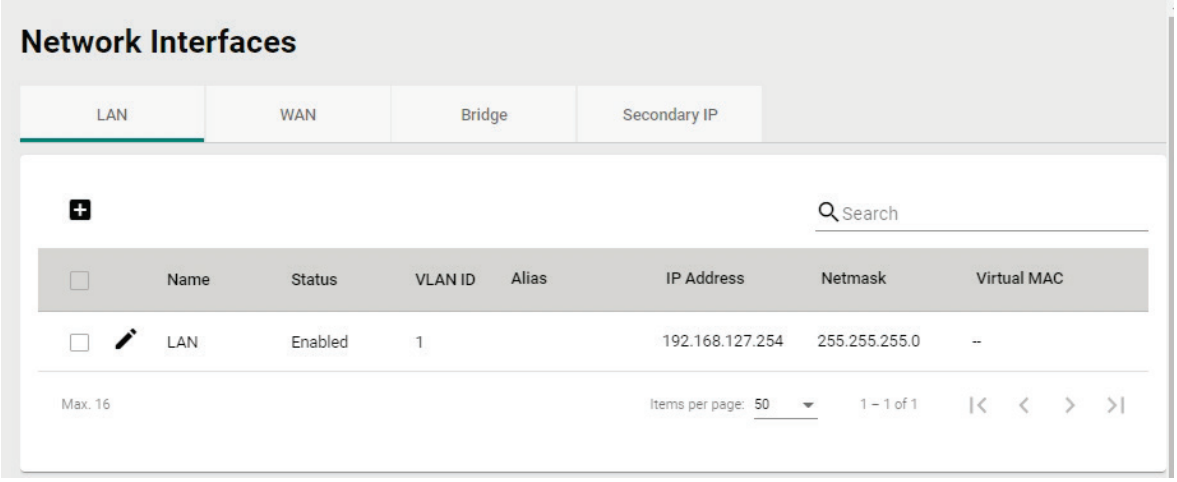
Port

Setting	Description	Factory Default
1/1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 1/9, 1/10 checkbox	Check the boxes to add the corresponding ports to the static multicast group.	None

When finished, click **CREATE** to create the static multicast entry.

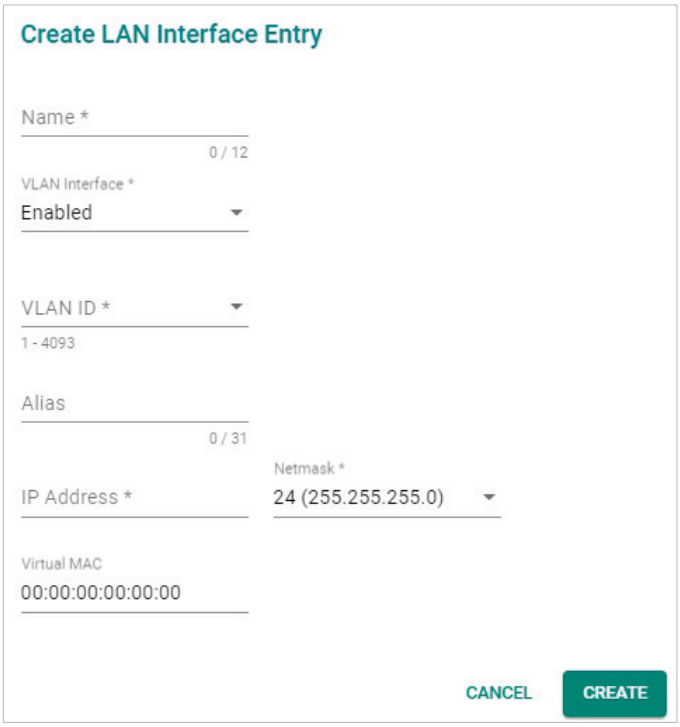
Network Interface

LAN



Create a LAN Interface

Click the ⊞ icon to create a LAN interface.



Configure the following settings:

Name

Setting	Description	Factory Default
Max. 12 characters	Enter a name for the interface.	None

VLAN Interface

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

VLAN ID

Setting	Description	Factory Default
1 to 4093	Enter the VLAN ID.	None

Alias

Setting	Description	Factory Default
Max. 31 characters	Enter an alias for the VLAN interface.	None

IP Address

Setting	Description	Factory Default
IP address	Specify the IP address of the interface.	None

Netmask

Setting	Description	Factory Default
Subnet mask	Specify the subnet mask of the interface.	24 (255.255.255.0)

Virtual MAC

Setting	Description	Factory Default
Virtual MAC	Enter the virtual MAC address of the interface.	00:00:00:00:00:00

When finished, click **CREATE** to create the new interface.

NOTE

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

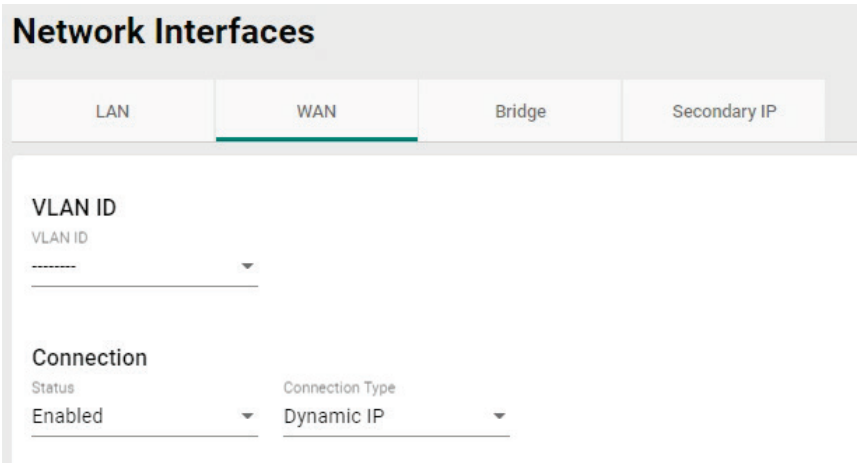
Delete a LAN Interface

Select the item(s) you want to delete in the LAN Interface List, click the icon. When prompted to confirm, click **DELETE** to delete the selected item(s).

Modify a LAN Interface

In the LAN Interface List, click the icon of the entry you want to modify. When finished editing the attributes, click **APPLY** to save and apply your changes.

WAN



VLAN ID

VLAN ID

The Moxa Industrial Secure Router's WAN interface is configured by VLAN group. Ports with the same VLAN ID can be configured as one WAN interface.

Setting	Description	Factory Default
VLAN ID	Select a VLAN ID. The Moxa Industrial Secure Router's WAN interface is VLAN-based. All ports associated with the selected VLAN ID will act as a single WAN interface.	None

Connection

There are three different connection types for the WAN interface: **Dynamic IP**, **Static IP**, and **PPPoE**. A detailed explanation of the configuration settings for each type is given below.

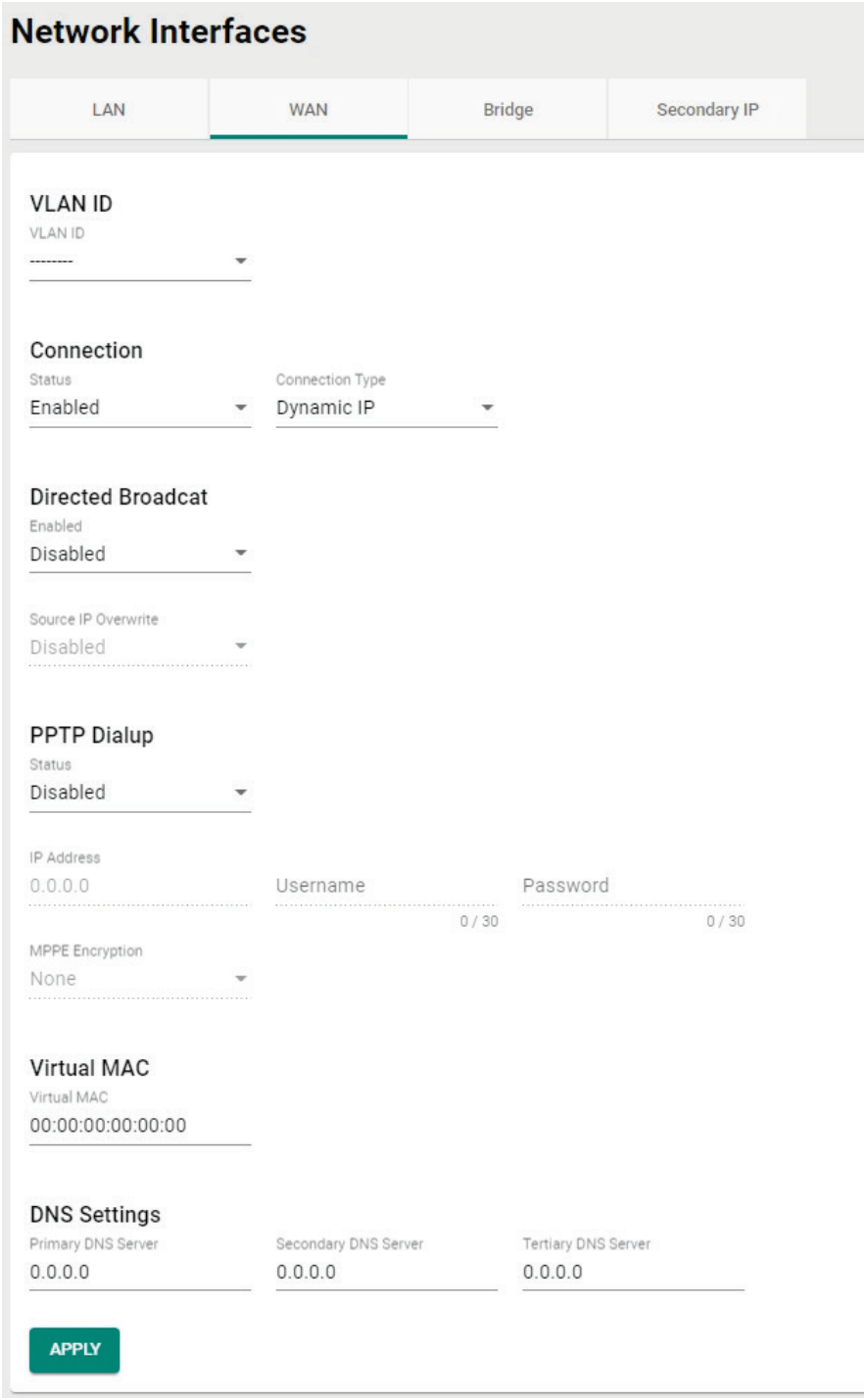
Status

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

Connection Type

Setting	Description	Factory Default
Static IP, Dynamic IP, PPPoE	Choose the connection type. For more details and configuration settings for each type, refer to: Dynamic IP Connection Static IP Connection PPPoE Connection.	Dynamic IP

Dynamic IP Connection



Directed Broadcast

Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the directed broadcasting.	Enabled

Source IP Overwrite

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable source IP overwriting.	Enabled

PPTP Dialup

The Point-to-Point Tunneling (PTP) protocol is used for Virtual Private Networks (VPN). Remote users can use PPTP to connect to private networks from public networks.

PPTP Connection

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the PPTP connection.	None

IP Address

Setting	Description	Factory Default
IP Address	Specify the PPTP service IP address.	0.0.0.0

Username

Setting	Description	Factory Default
Max. 30 Characters	Enter the username used for dialing in to the PPTP service.	None

Password

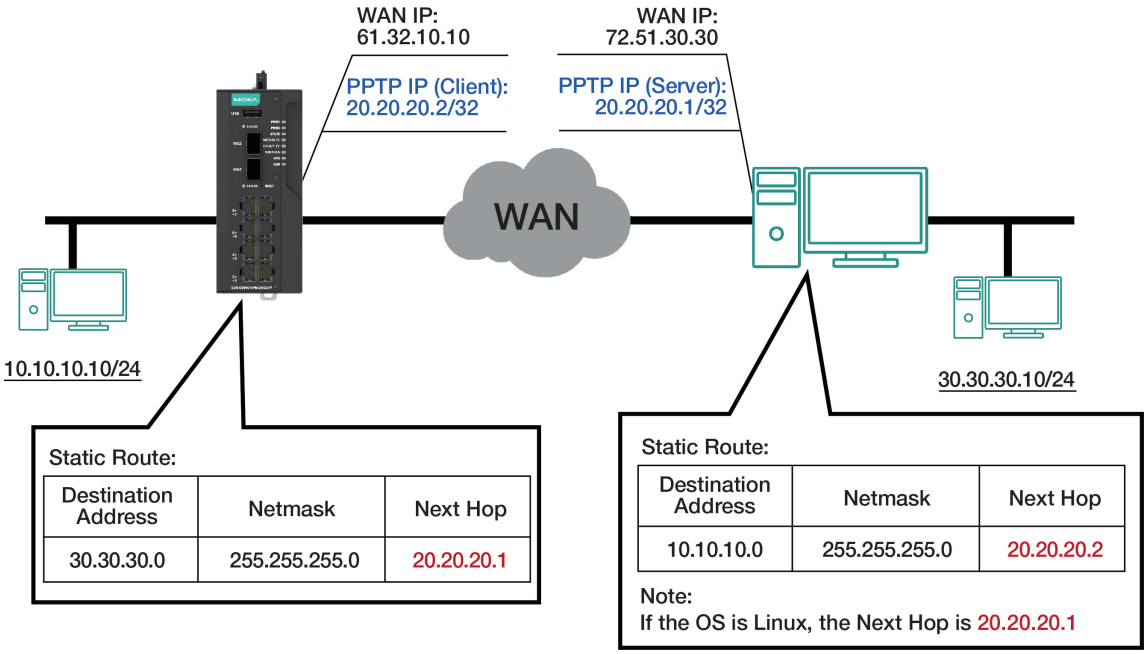
Setting	Description	Factory Default
Max. 30 characters	Enter the password used for dialing in to the PPTP service.	None

MPPE Encryption

Setting	Description	Factory Default
None/Encrypt	Enable or disable MPPE encryption.	None

Example

In this scenario, a remote user (IP: 10.10.10.10) wants to connect to the internal server (private IP: 30.30.30.10) via the PPTP protocol. The IP address of the PPTP server is 20.20.20.1. The necessary configuration settings are shown in the following figure:



Virtual MAC

Virtual MAC

Setting	Description	Factory Default
Virtual MAC Address	Specify the virtual MAC address.	00.00.00.00.00.00

DNS Settings

When using Dynamic IP or PPPoE as the Connection Type, you can also configure optional DNS servers.

Primary DNS Server

Setting	Description	Factory Default
IP Address	Enter the primary DNS IP address.	0.0.0.0

Secondary DNS Server

Setting	Description	Factory Default
IP Address	Enter the secondary DNS IP address.	0.0.0.0

Tertiary DNS Server

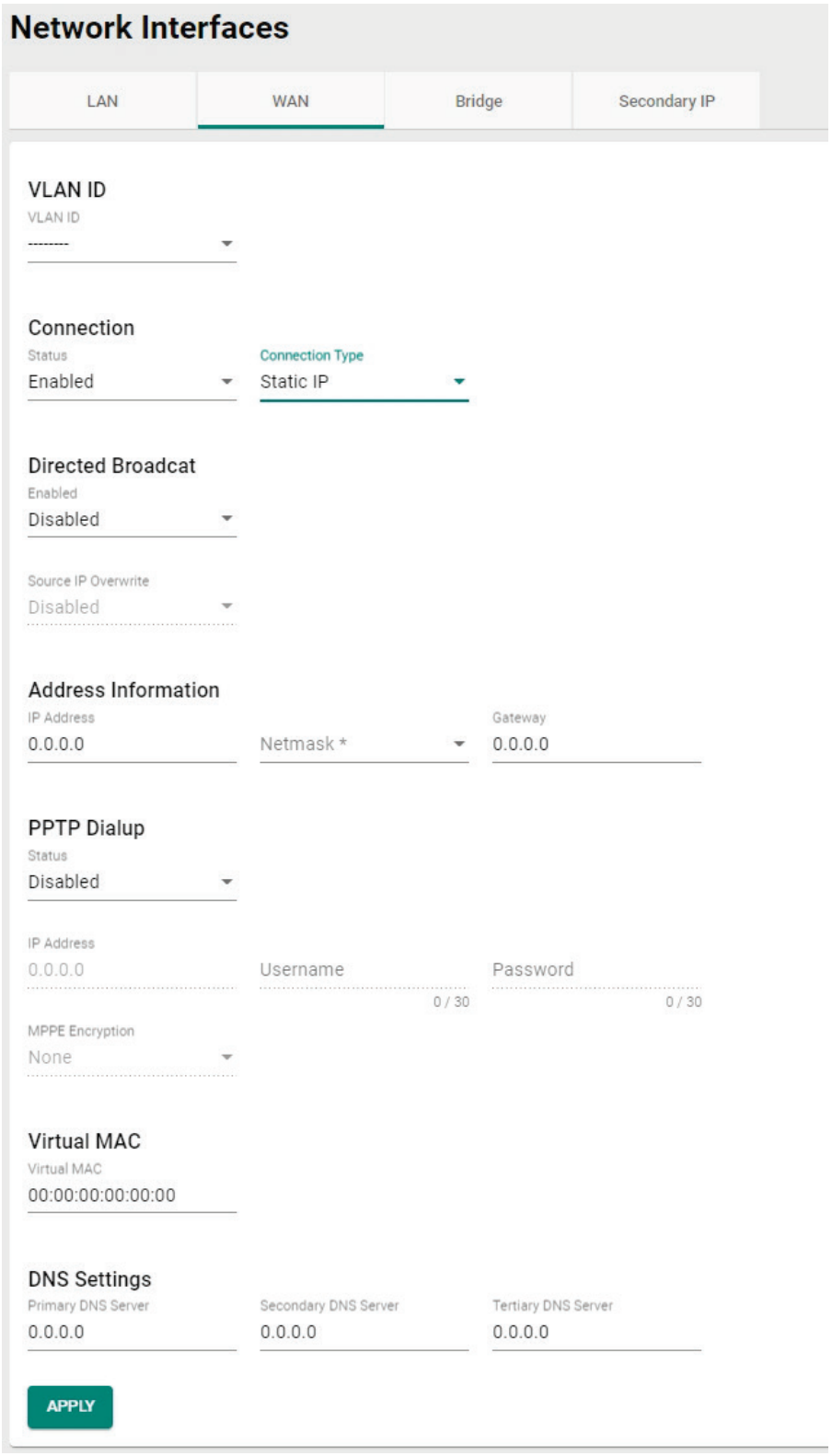
Setting	Description	Factory Default
IP Address	Enter the tertiary DNS IP address.	0.0.0.0

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

NOTE

Manually configured DNS servers will have a higher priority than DNS servers from the PPPoE or DHCP server.

Static IP Connection



Directed Broadcast

Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the directed broadcasting.	Enabled

Source IP Overwrite

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable source IP overwriting.	Enabled

Address Information

IP Address

Setting	Description	Factory Default
IP Address	Specify the interface IP address.	0.0.0.0

Subnet Mask

Setting	Description	Factory Default
IP Address	Specify the subnet mask.	None

Gateway

Setting	Description	Factory Default
IP Address	Specify the gateway IP address.	0.0.0.0

PPTP Dialup

The Point-to-Point Tunneling (PTP) protocol is used for Virtual Private Networks (VPN). Remote users can use PPTP to connect to private networks from public networks.

PPTP Connection

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the PPTP connection.	None

IP Address

Setting	Description	Factory Default
IP Address	Specify the PPTP service IP address.	0.0.0.0

Username

Setting	Description	Factory Default
Max. 30 Characters	Enter the username used for dialing in to the PPTP service.	None

Password

Setting	Description	Factory Default
Max. 30 characters	Enter the password used for dialing in to the PPTP service.	None

MPPE Encryption

Setting	Description	Factory Default
None/Encrypt	Enable or disable MPPE encryption.	None

Virtual MAC

Virtual MAC

Setting	Description	Factory Default
Virtual MAC Address	Specify the virtual MAC address.	00.00.00.00.00.00

DNS Settings

When using Dynamic IP or PPPoE as the Connection Type, you can also configure optional DNS servers.

Primary DNS Server

Setting	Description	Factory Default
IP Address	Enter the primary DNS IP address.	0.0.0.0

Secondary DNS Server

Setting	Description	Factory Default
IP Address	Enter the secondary DNS IP address.	0.0.0.0

Tertiary DNS Server

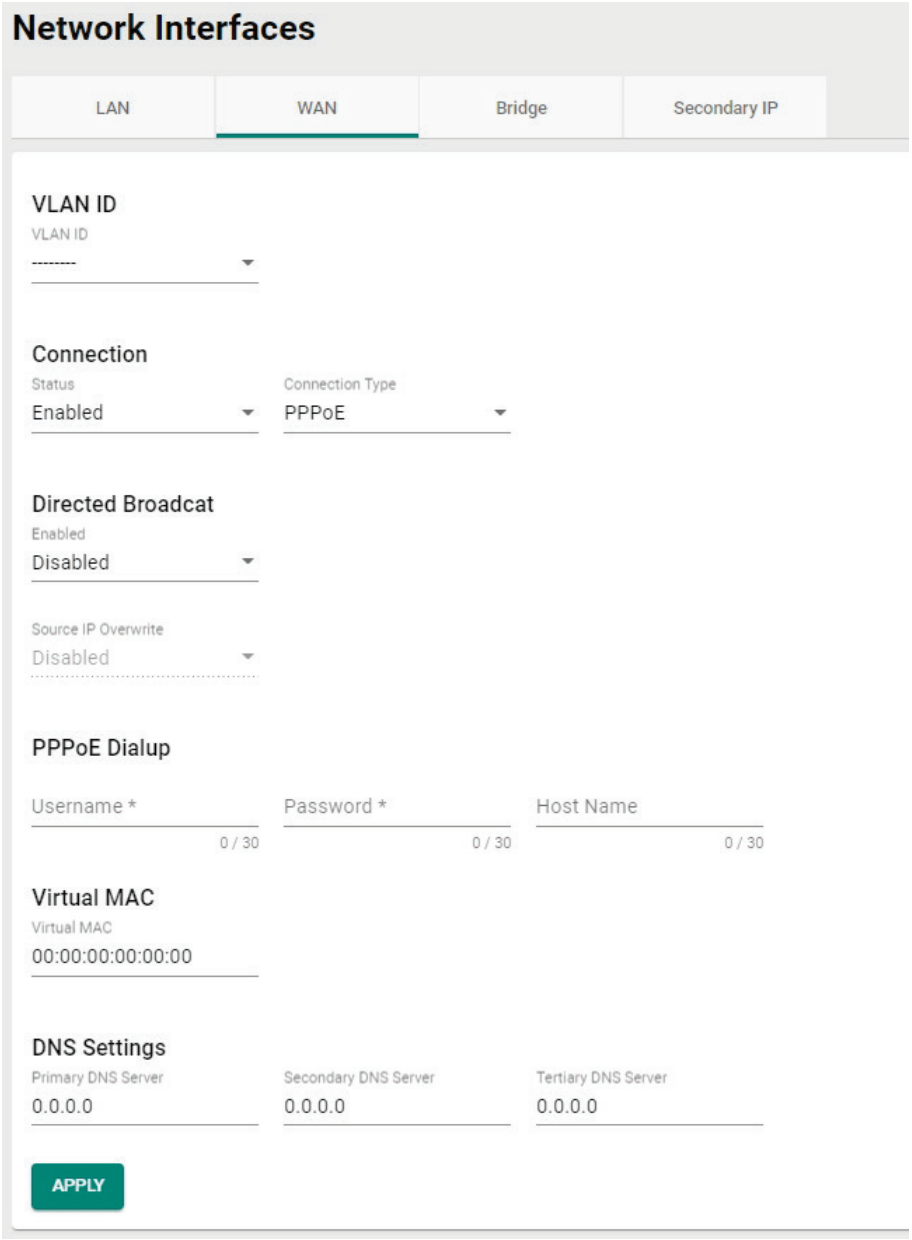
Setting	Description	Factory Default
IP Address	Enter the tertiary DNS IP address.	0.0.0.0

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

NOTE

Manually configured DNS servers will have a higher priority than DNS servers from the PPPoE or DHCP server.

PPPoE Connection



Directed Broadcast

Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the directed broadcasting.	Enabled

Source IP Overwrite

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable source IP overwriting.	Enabled

PPPoE Dialup

Username

Setting	Description	Factory Default
Max. 30 characters	Enter the username used for logging in to the PPPoE server.	None

Password

Setting	Description	Factory Default
Max. 30 characters	Enter the password used for logging in to the PPPoE server.	None

Host Name

Setting	Description	Factory Default
Max. 30 characters	Enter the user-defined hostname of the PPPoE server.	None

Virtual MAC

Virtual MAC

Setting	Description	Factory Default
Virtual MAC Address	Specify the virtual MAC address.	00.00.00.00.00.00

DNS Settings

When using Dynamic IP or PPPoE as the Connection Type, you can also configure optional DNS servers.

Primary DNS Server

Setting	Description	Factory Default
IP Address	Enter the primary DNS IP address.	0.0.0.0

Secondary DNS Server

Setting	Description	Factory Default
IP Address	Enter the secondary DNS IP address.	0.0.0.0

Tertiary DNS Server

Setting	Description	Factory Default
IP Address	Enter the tertiary DNS IP address.	0.0.0.0

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

NOTE

Manually configured DNS servers will have a higher priority than DNS servers from the PPPoE or DHCP server.

Bridge Group Interface

When ports are set in the VLAN, the packets transmitted within these ports will be forwarded by the switching chip without being filtered by the firewall. However, in some scenarios, it is required to filter specific packets transmitted within the VLAN. By selecting ports as Bridge port, the packets transmitted between these ports will be checked by the firewall.

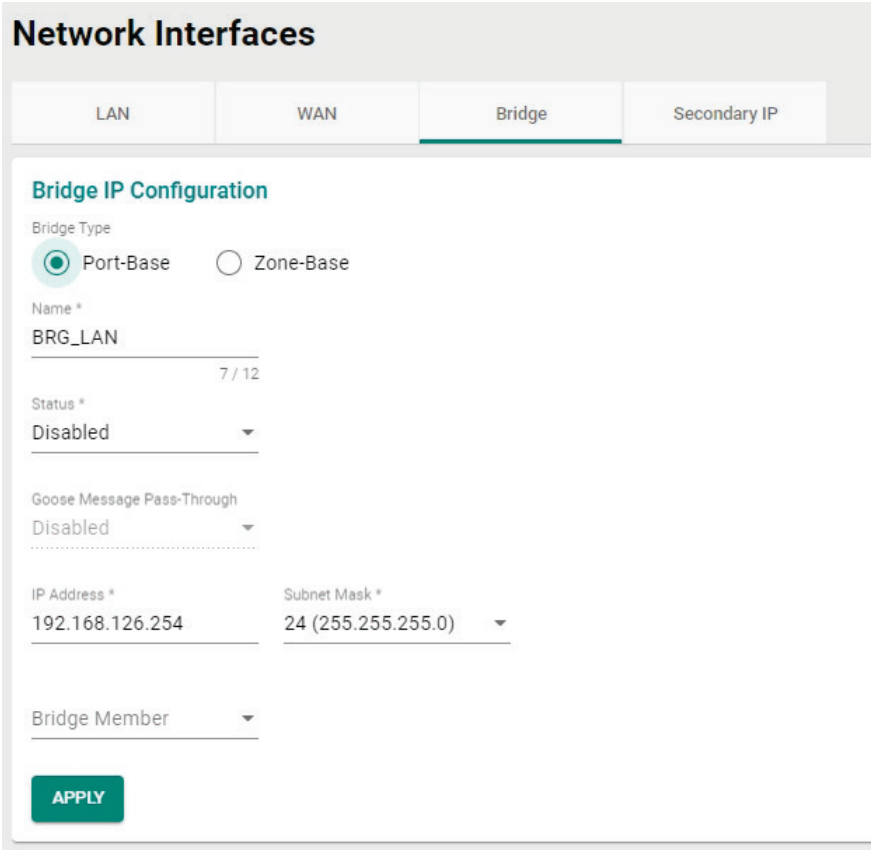
Similarly, when ports are associated with different VLANs, the packets transmitted within these VLANs will be routed by the switching chip locally, without being inspected by the firewall. However, in some scenarios, it is required to filter specific packets transmitted between VLANs. By adding VLANs to a Bridge Zone, the packets transmitted between these two zones will be checked by the firewall.

Adding Ports/VLANs to the Bridge Interface

Port Base

Port-based bridge ports allow the router firewall to filter traffic moving between the assigned bridge ports.

Select **Port-Base** as the Bridge type to create a port-based bridge.



Name

Setting	Description	Factory Default
Max. 12 characters	Enter a name for the bridge interface.	None

Status

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

Goose Message Pass-Through

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable GOOSE message passthrough.	Disabled

IP Address

Setting	Description	Factory Default
IP Address	Enter the IP address of the interface.	None

Subnet Mask

Setting	Description	Factory Default
Subnet Mask	Enter the subnet mask of the interface.	None

Bridge Member

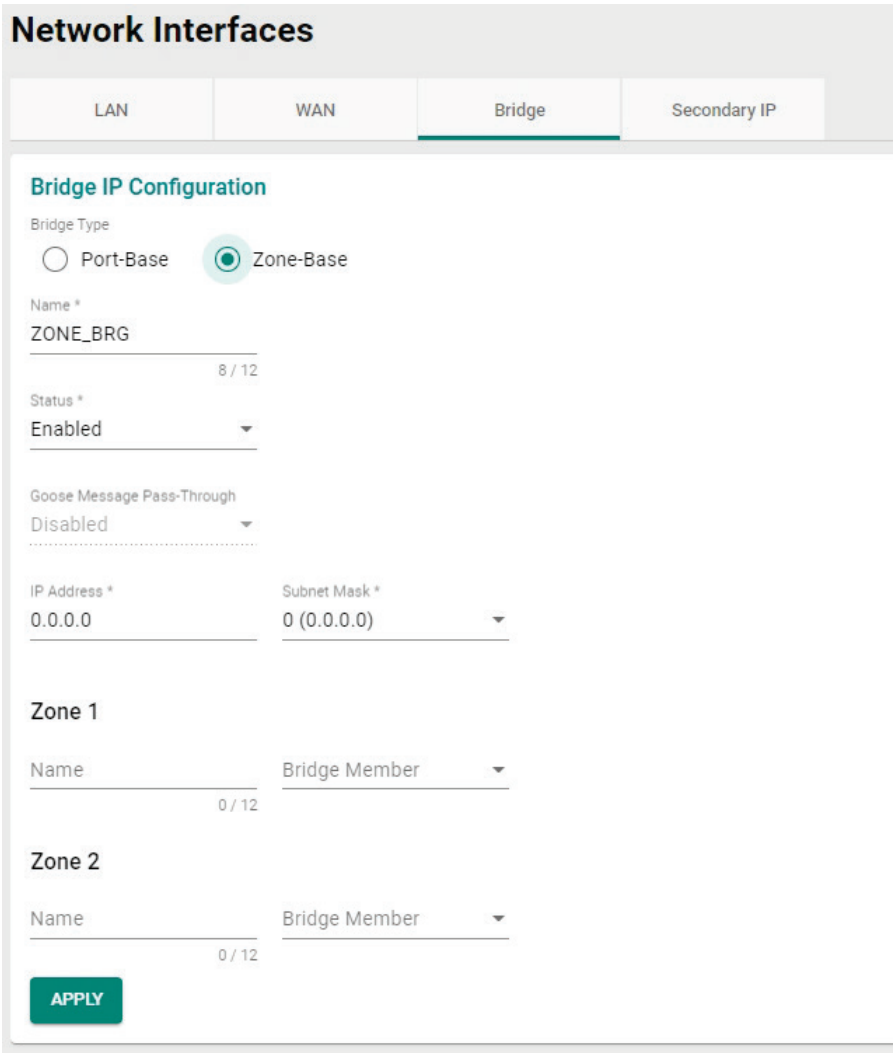
Setting	Description	Factory Default
Port	Select the port that will act as the bridge port.	None

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

Zone base

A zone-based bridge allows the router firewall to filter traffic moving between all ports associated with the bridge zone.

Select **Zone-Base** as the Bridge type to create a zone-based bridge.



Name

Setting	Description	Factory Default
Max. 12 characters	Enter a name for the bridge zone interface.	None

Status

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

Goose Message Pass-Through

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable GOOSE message passthrough.	Disabled

IP Address

Setting	Description	Factory Default
IP Address	Enter the IP address of the interface.	None

Subnet Mask

Setting	Description	Factory Default
Subnet Mask	Enter the subnet mask of the interface.	None

Zone 1/2

Name

Setting	Description	Factory Default
Max. 12 characters	Enter a name for the bridge zone.	None

Bridge Member

Setting	Description	Factory Default
VLAN	Select the VLAN to assign to the corresponding bridge zone.	None

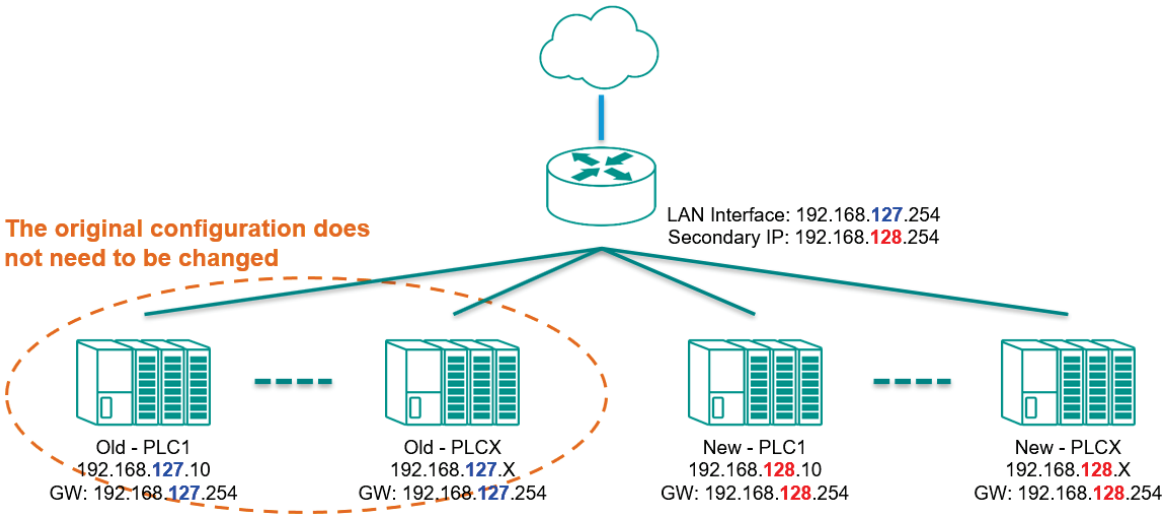
When finished, click **APPLY** to save your changes.

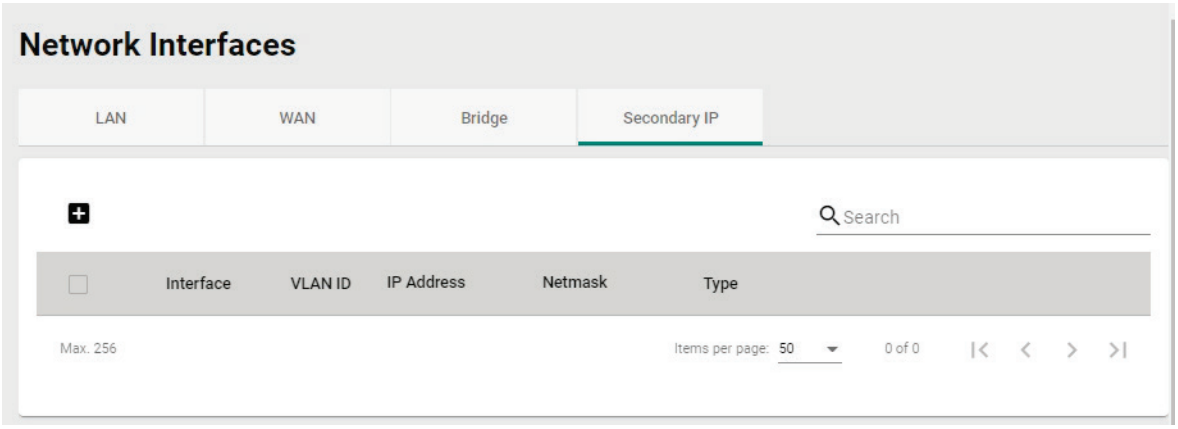
NOTE

Even when the Bridge IP function is disabled (e.g. the bridge interface is disabled), the bridge interface will still exist in the system. Even if no ports are assigned to it, you can view the VLAN ID of the bridge interface in the VLAN table. To fully remove or disable the bridge interface, modify the PVID in the VLAN settings.

Secondary IP

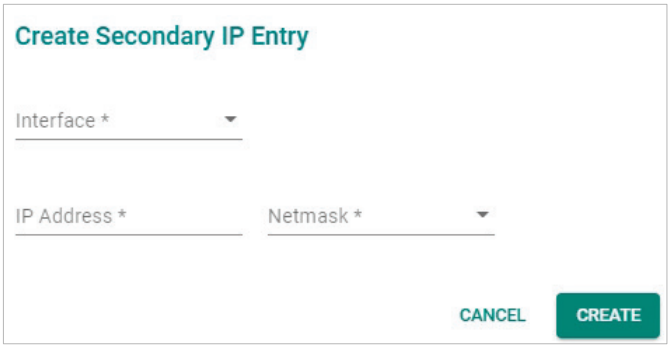
The Layer 3 interface can also act as a secondary IP. As shown in the example below, if the user needs additional IP addresses in the LAN segment but does not want to change the settings of the original interface IP/device, the secondary IP can be used to create a new network segment.





Create a Secondary IP

Click ➕ to create a secondary IP.



Configure the following settings:

Interface

Setting	Description	Factory Default
Interface	Select the interface to create a secondary IP for.	None

IP Address

Setting	Description	Factory Default
IP Address	Specify the IP address of the secondary interface.	None

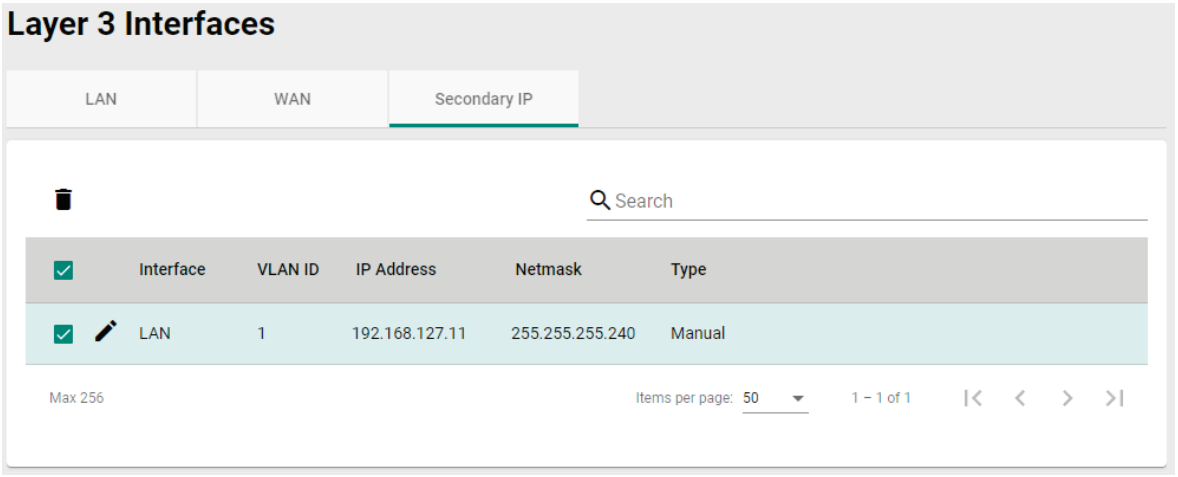
Netmask

Setting	Description	Factory Default
Subnet Mask	Specify the subnet mask of the secondary interface.	None

When finished, click **CREATE** to activate the secondary interface.

Delete a Secondary IP

Select the interface from the Secondary IP List and click 🗑 to delete it.

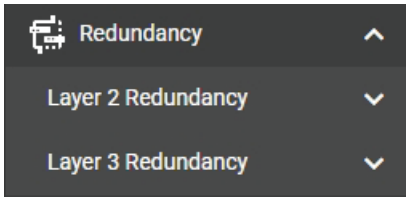


Modify a Secondary IP

Click ✎ to modify the secondary IP entry. When finished, click **APPLY** to save and apply your changes.

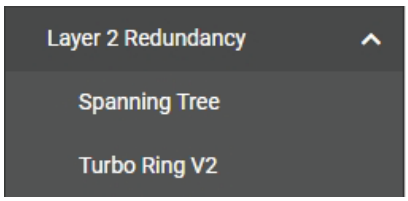
6. Redundancy

From the **Redundancy** section, you can configure the **Layer 2 Redundancy**, and **Layer 3 Redundancy** settings.



Layer 2 Redundancy

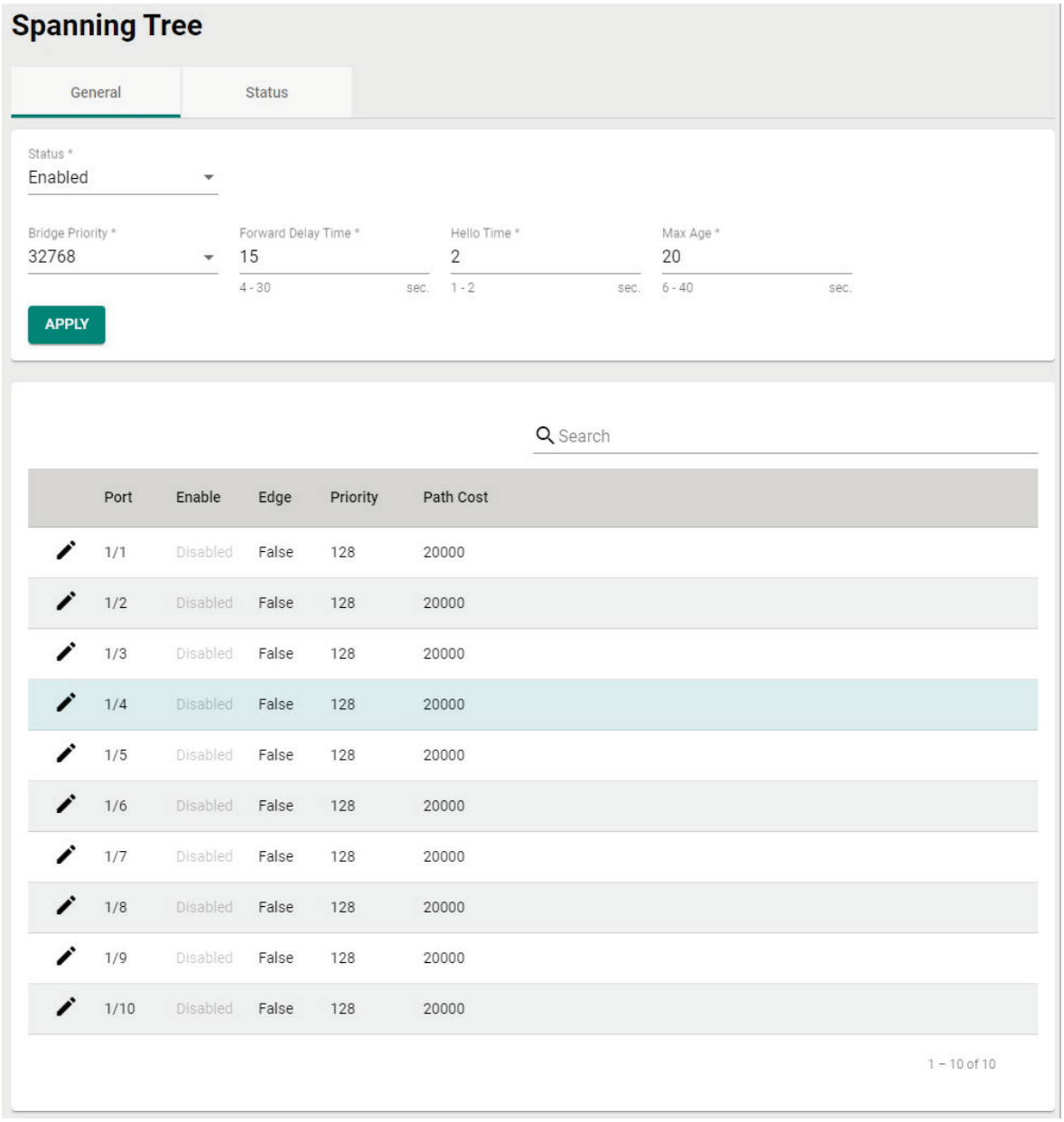
From the **Layer 2 Redundancy** section, the following functions can be configured: **Spanning Tree,** and **Turbo Ring V2**.



Spanning Tree

From the Spanning Tree screen, you can configure general Spanning Tree settings and view the status of the current Spanning Tree configuration.

General Settings



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the Spanning Tree Protocol.	Enabled

Bridge priority

Setting	Description	Factory Default
0 to 61440, multiples of 4096	Specify the bridge priority. A lower number represents a higher priority. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Forwarding Delay Time

Setting	Description	Factory Default
4 to 30 seconds	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.	15

Hello time

Setting	Description	Factory Default
1 to 2 seconds	Specify the interval at which the device will send out "hello" messages. The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy.	2

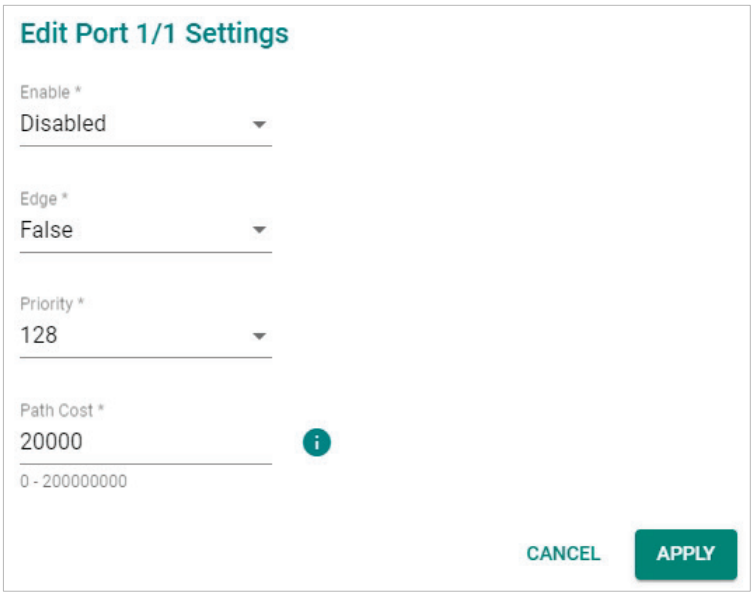
Max. Age

Setting	Description	Factory Default
6 to 40 seconds	Specify the maximum age duration. If the device is not the root, and it has not received a hello message from the root within the specified "Max. Age" time, the device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate to set up a new Spanning Tree topology.	20

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

Editing Spanning Tree for a Port

To edit the Spanning Tree settings for a specific port, click the ✎ icon next to the port you want to modify.



Enable

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the port as a node in the Spanning Tree topology.	Disabled

NOTE

It is recommended to disable Spanning Tree Protocol on the port if it is connected to a device (PLC, RTU, etc.) as opposed to network equipment, as this may cause unnecessary negotiation.

Edge

Setting	Description	Factory Default
Force Edge	The port is fixed as an edge port and will always be in the forwarding state.	False
False	The port is not an edge port.	

Priority

Setting	Description	Factory Default
0 to 240, multiples of 16	Specify the port priority. A lower number indicates a higher priority.	128

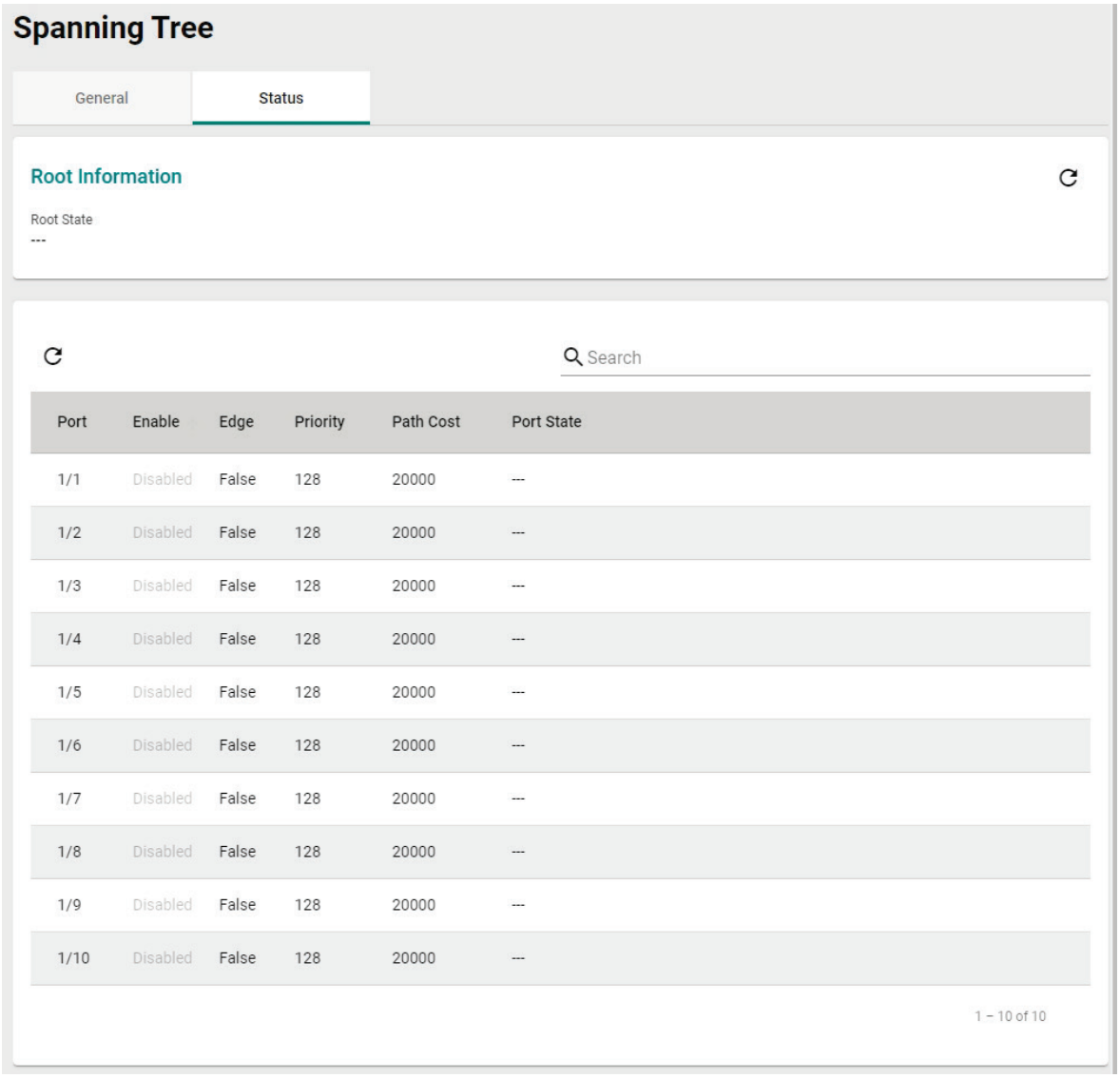
Path Cost

Setting	Description	Factory Default
0 to 200000000	Specify the path cost. A higher cost indicates 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.	20000

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

Status

The Status page shows the Spanning Tree root and port information.



At the top of the page, the user can check the **Root Information** of this function. You will see:

Root State

This shows if this switch is the Root of the Spanning Tree (the root is determined automatically).

At the bottom of the page, the user can check the **Status** of this function.

Port State

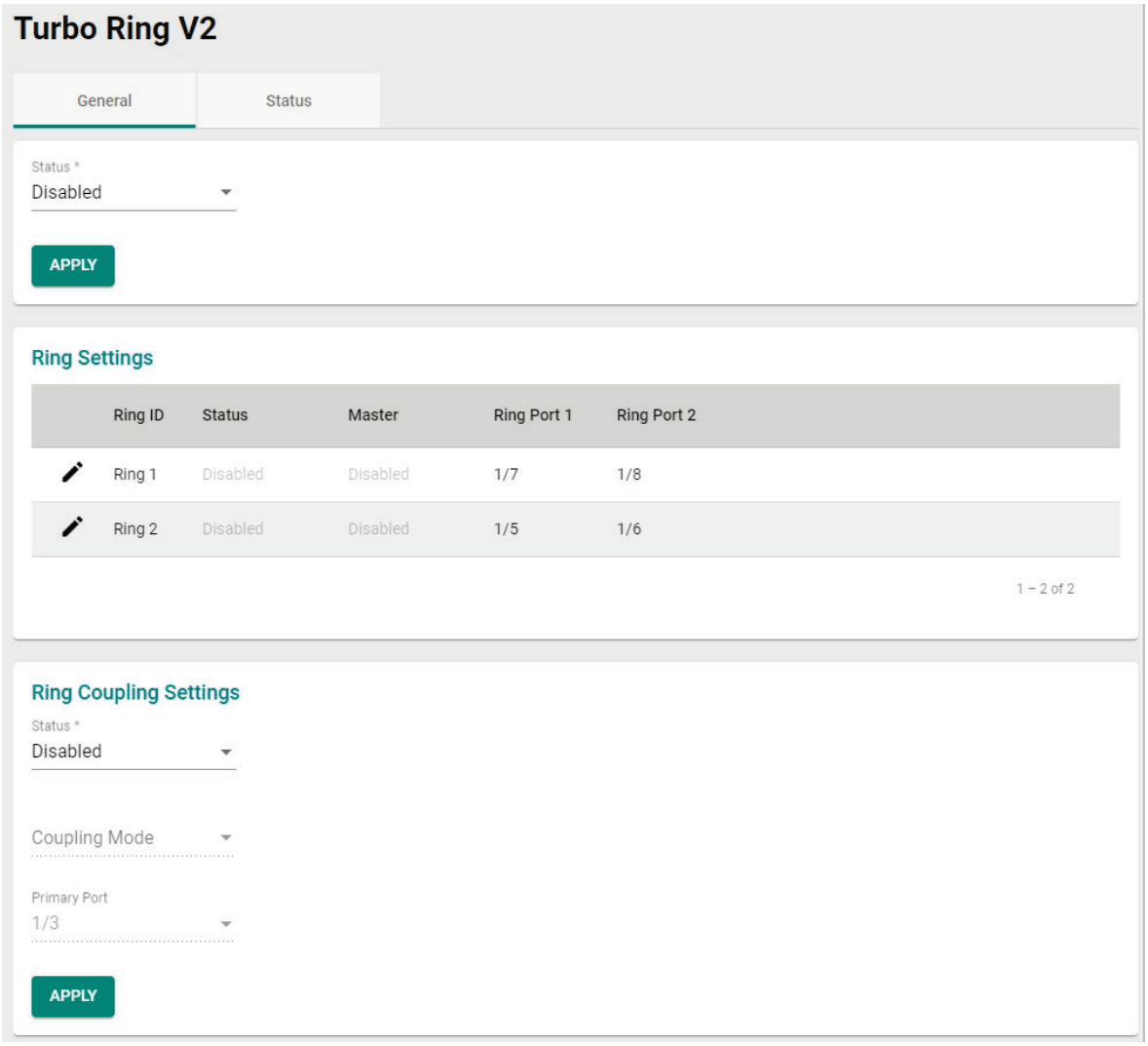
Indicates the current Spanning Tree status of the port. **Forwarding** for normal transmission or **Blocking** to indicate the port is blocking transmissions.

Click the icon to refresh the Spanning Tree status of each port.

Turbo Ring V2

From the Turbo Ring V2 screen, you can configure general Turbo Ring V2 settings and view the status of the current Turbo Ring V2 configuration.

General Settings



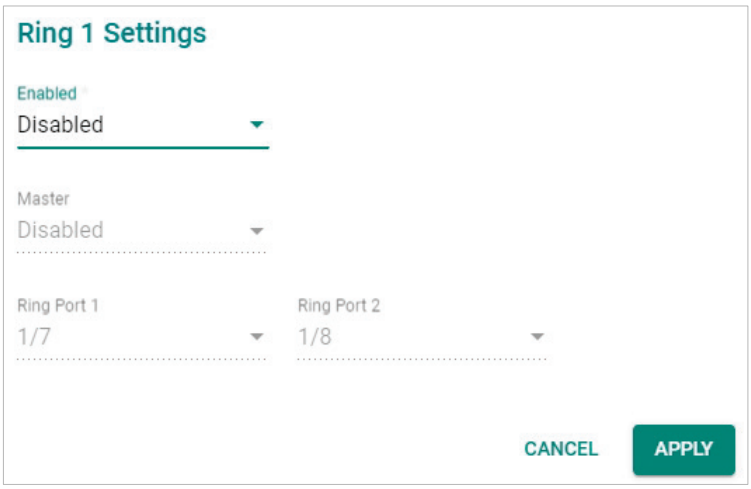
Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable Turbo Ring V2.	Disabled

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

Ring Settings

In the Ring Settings table, click the ✎ icon of the entry you want to modify.



Enabled

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable this Turbo Ring.	Disabled

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

Master

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable this Ring as the Master ring.	Disabled

Ring Port 1

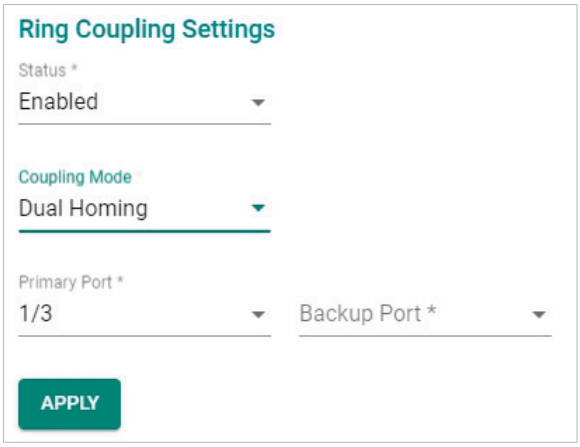
Setting	Description	Factory Default
Select the port from the drop-down list	Select the port to act as the 1st redundant port.	1/7

Ring Port 2

Setting	Description	Factory Default
Select the port from the drop-down menu	Select the port to act as the 2nd redundant port.	1/8

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

Ring Coupling Settings



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable this device as a Ring Coupler.	Disabled

Coupling Mode

Setting	Description	Factory Default
Dual Homing	Set the Coupling mode to Dual Homing.	Dual Homing
Backup Path	Set the Coupling mode to Backup Path.	
Primary Path	Set the Coupling mode to Primary.	

If the Coupling Mode is set to Dual Homing, configure the following settings:

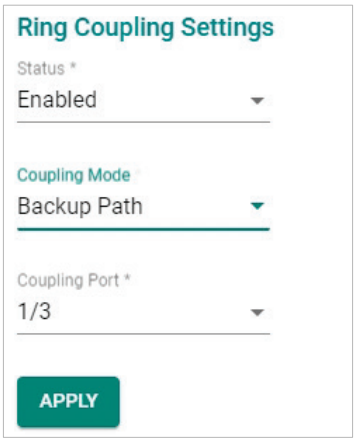
Primary Port

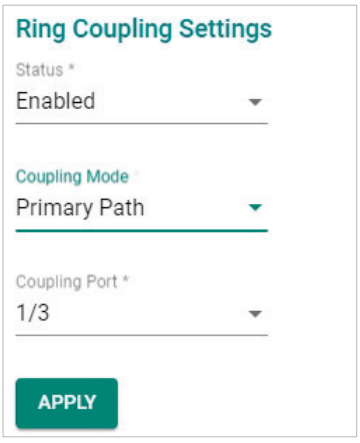
Setting	Description	Factory Default
Select the port from the list	Select the port that will act as the backup port.	1/3

Backup Port

Setting	Description	Factory Default
Select the port from the list	Select the port that will act as the backup port.	None

If the Coupling Mode is set to Backup Path or Primary, configure the following settings:





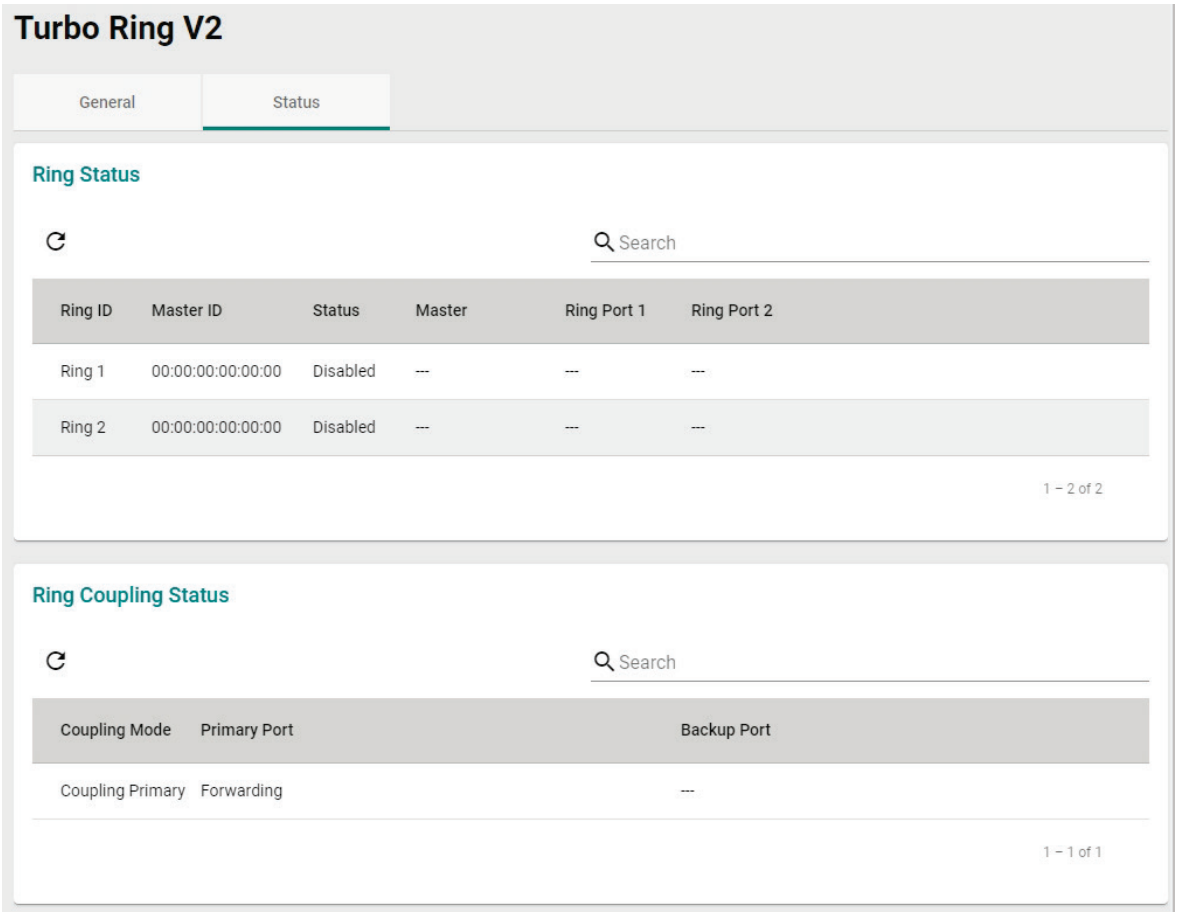
Coupling Port

Setting	Description	Factory Default
Select the port from the list	Select the port that will act as the coupling port.	1/3

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

Status

From the **Status** tab, you can view the current Ring settings and the Ring Coupling Status.



Ring Status

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

Item	Description
Ring ID	The ID number of the Ring.
Master ID	The MAC address of the Ring Master.
Status	Healthy: The Ring and the ports are working properly. Break: One or more Rings are broken.
Master	The device is the Master/Slave in this Ring.
Ring Port 1	The first Ring port.
Ring Port 2	The second Ring port.

Ring Coupling Status

Refer to the following table for a detailed description for the status of Coupling Mode and Coupling Port.

Item	Description
Coupling Mode	Primary: The main path of Ring Coupling. Backup: The backup path of Ring Coupling.
Coupling Port	The port of the Ring Coupling.

Click the icon to refresh the Turbo Ring V2 status.

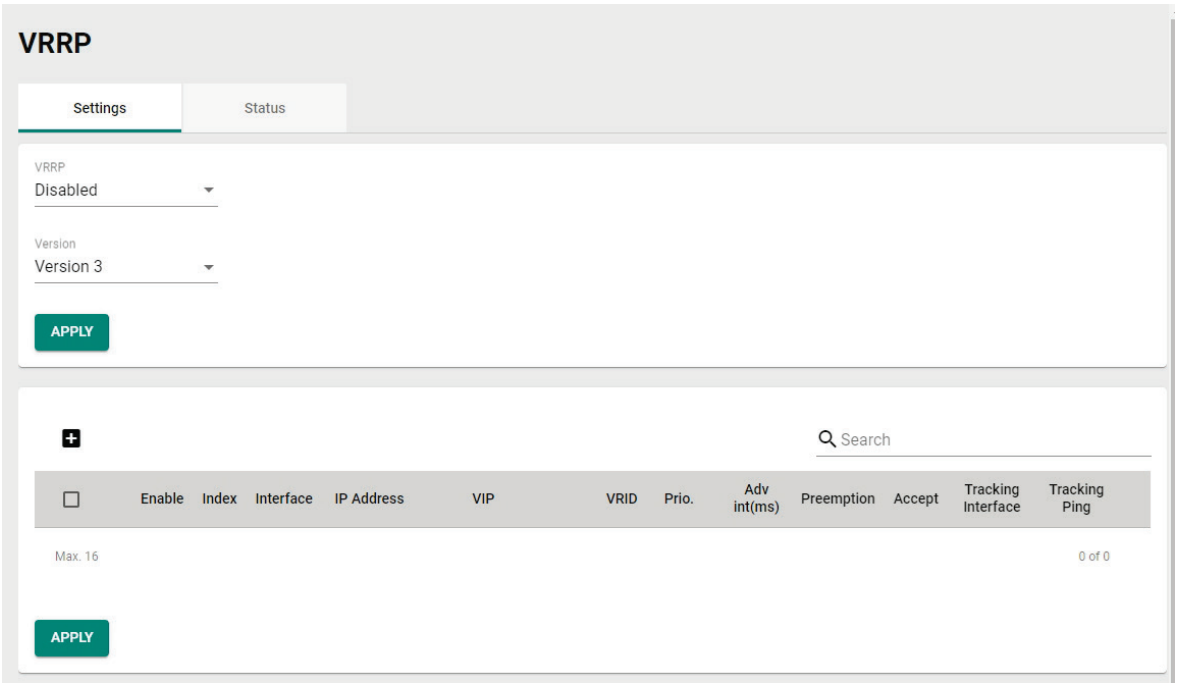
Layer 3 Redundancy

From the Layer 3 Redundancy section you can configure VRRP Settings.

VRRP

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.

Settings



VRRP

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable VRRP functionality.	Disabled

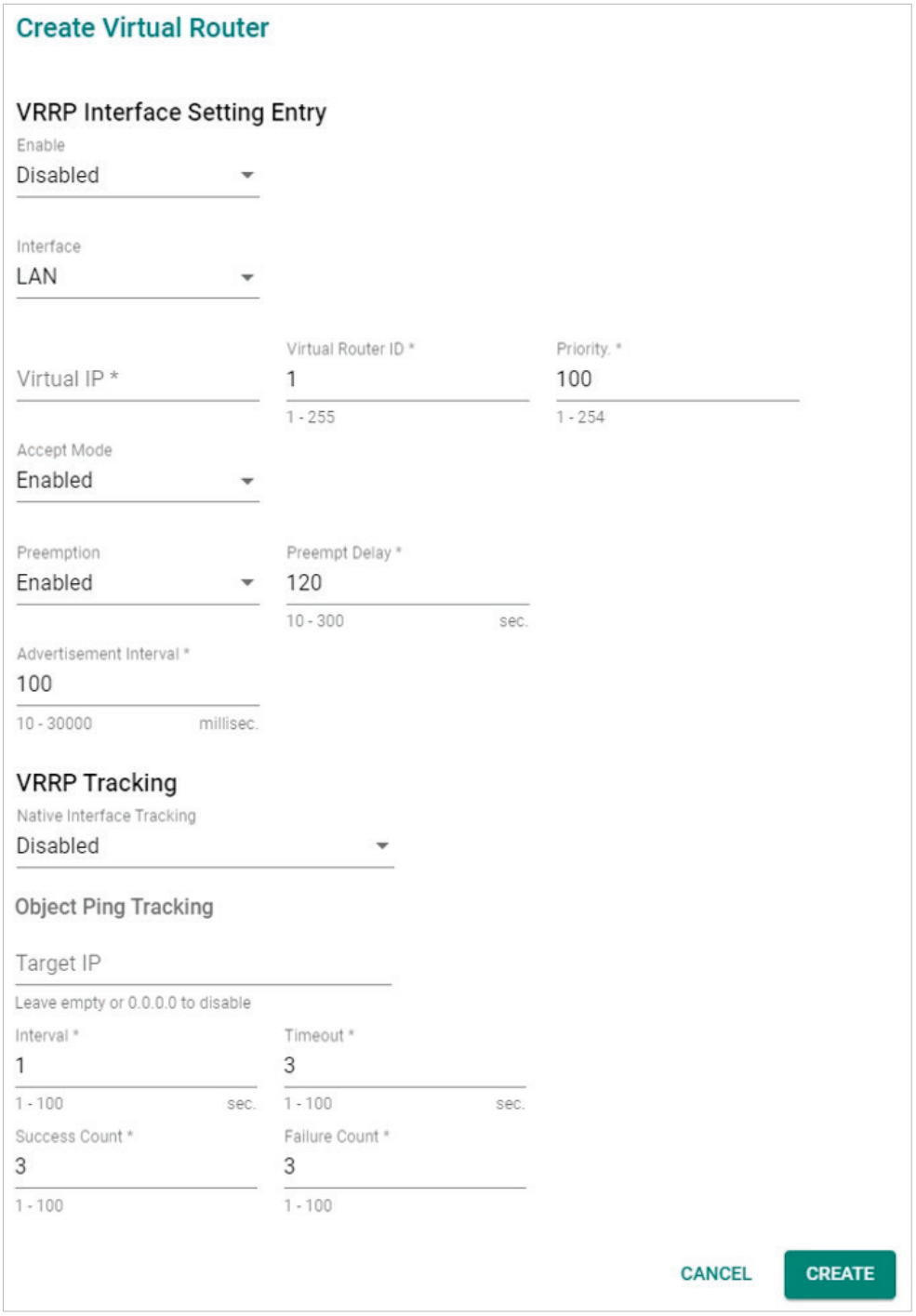
Version

Setting	Description	Factory Default
Version 2, Version 3	Select the VRRP version.	Version 3

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

Create a Virtual Router

Click the ➕ icon to create a new virtual router.



VRRP Interface Setting Entry

Enable

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the virtual router	Disabled

Interface

Setting	Description	Factory Default
LAN, WAN	Select the interface to enable VRRP for, either the LAN or WAN interface.	LAN

Virtual IP

Setting	Description	Factory Default
IP Address	Specify the virtual router IP address. The virtual IP must be the same subnet as the real IP address. Industrial secure routers in the same VRRP group must be in the same subnet.	None

Virtual Router ID

Setting	Description	Factory Default
1 to 255	Specify the virtual router ID, which is used to assign the router to a VRRP group. The Industrial secure routers that operate as master/backup should have the same ID. Each interface supports one virtual router ID.	1

Priority

Setting	Description	Factory Default
1 to 254	Specify the VRRP interface priority. A higher number represents a higher priority, with 254 being the highest. If multiple industrial secure routers have the same priority, the router with the highest IP address will have priority.	100

Accept Mode

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable Accept Mode. When enabled, the virtual router with the role of Master will allow others to access its own virtual IP address.	Enabled

Preemption

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable preemption. If enabled, preemption will decide if the master will retake authority or not after being unavailable.	Enabled

Preempt Delay

Setting	Description	Factory Default
10 to 300 seconds	If Preemption is enabled, specify the preemption delay. If enabled, the master will wait for the specified period of time before retaking authority back in order to prevent the master from acting before the network connection is ready.	120

Advertisement Interval

Setting	Description	Factory Default
10 to 30000 seconds	Specify the advertisement interval. This determines the interval (in seconds) at which the master will send packets to all slave device to inform them who the master device is.	100

VRRP Tracking

Native Interface Tracking

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the Native Interface Tracking function.	Disabled

NOTE

Make sure the WAN IP is configured correctly before enabling the “Native Interface Tracking” function.

Object Ping Tracking

Target IP

Setting	Description	Factory Default
IP Address	Specify the Target IP to verify if the connection to the destination (e.g. control center) is working. Leave this blank or enter 0.0.0.0 to disable this function.	None

Interval

Setting	Description	Factory Default
1 to 100 seconds	Specify the interval at which the router will ping the target.	1

Timeout

Setting	Description	Factory Default
1 to 100	Specify the timeout duration. This indicates the time the router will wait for a response before timing out.	3

Success Count

Setting	Description	Factory Default
Enabled or Disabled	Specify the success count. This indicates how many responses the router must receive to consider the connection working.	3

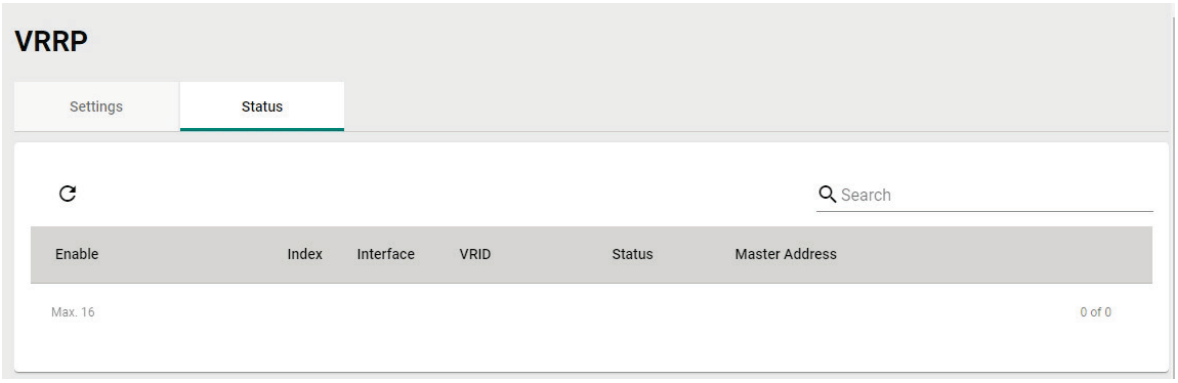
Failure Count

Setting	Description	Factory Default
Enabled or Disabled	Specify the failure count. This indicates how many times the target can fail to respond before the router considers the connection not working.	3

When finished, click **CREATE** to save and apply your configuration.

VRRP Status

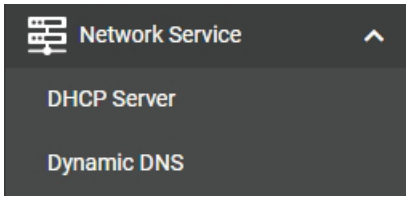
The Status screen shows a table with the current VRRP settings status.



Click the icon to refresh the information.

7. Network Service

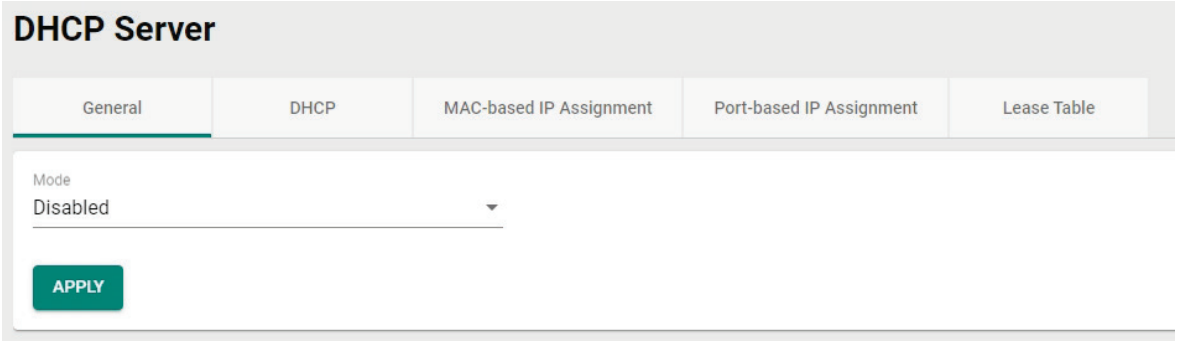
From the **Network Service** section the following functions can be configured: **DHCP Server,** and **Dynamic DNS**.



DHCP Server

From the DHCP Server screen, you can enable the DHCP and configure the various DHCP Server modes.

General Settings



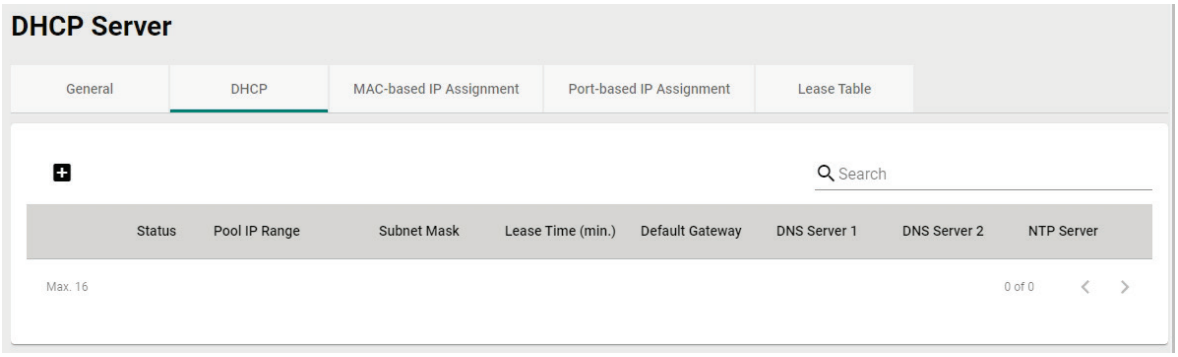
DHCP Server Mode

Setting	Description	Factory Default
Disabled, DHCP/MAC-based assignment, Port-based IP assignment	Select the DHCP Server Mode. Each mode has its own configuration settings. Refer to the following sections for more information: DHCP MAC-based IP Assignment Port-based IP Assignment	Disabled

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

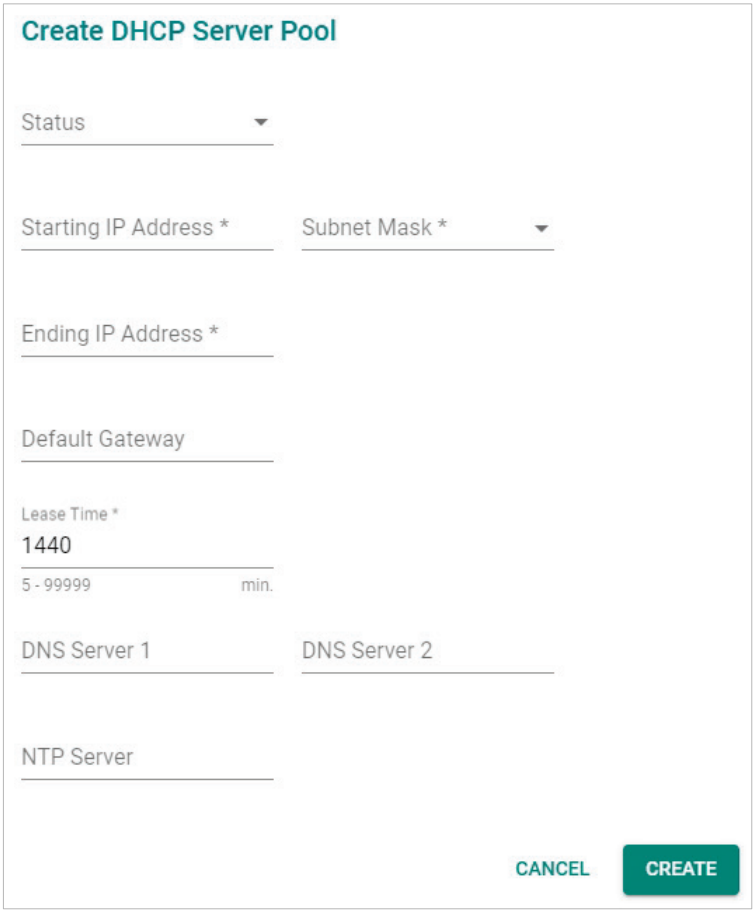
DHCP

The Industrial Secure Router provides DHCP (Dynamic Host Configuration Protocol) server functionality for LAN interfaces. When configured, the Industrial Secure Router will automatically assign an IP address from a user-configured IP address pool to connected Ethernet devices.



Create a DHCP Server Pool

Click ⊞ to create a new DHCP Server Pool.



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable DHCP server functionality.	Disabled

Starting IP Address

Setting	Description	Factory Default
IP Address	Specify the starting IP address of the DHCP IP pool.	None

Subnet Mask

Setting	Description	Factory Default
Subnet Mask	Specify the subnet mask for DHCP clients.	None

Ending IP Address

Setting	Description	Factory Default
IP Address	Specify the ending IP address of the DHCP IP pool.	None

Default Gateway

Setting	Description	Factory Default
IP Address	Specify the default gateway for DHCP clients.	None

Lease Time

Setting	Description	Factory Default
5 to 99999 minutes	Specify the lease time for IP addresses assigned by the DHCP server.	1440

DNS Server 1

Setting	Description	Factory Default
IP Address	Specify the IP address for the first DNS server for DHCP clients.	None

DNS Server 2

Setting	Description	Factory Default
IP Address	Specify the IP address for the second DNS server for DHCP clients.	None

NTP Server

Setting	Description	Factory Default
IP Address	Specify the NTP server for DHCP clients.	None

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

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.

Delete a DHCP Server Pool

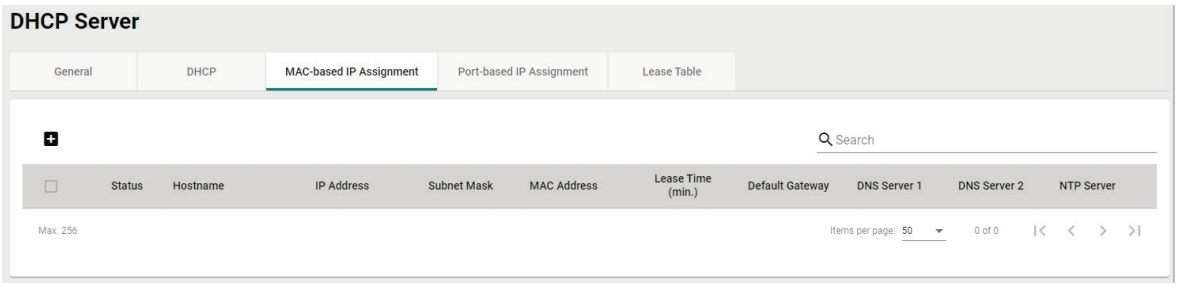
Click  next to the DHCP Server pool entry you want to delete.

Modify a DHCP Server Pool

Click  to next to the DHCP Server Pool you want to modify. When finished, click **APPLY** to save your changes.

MAC-based IP Assignment

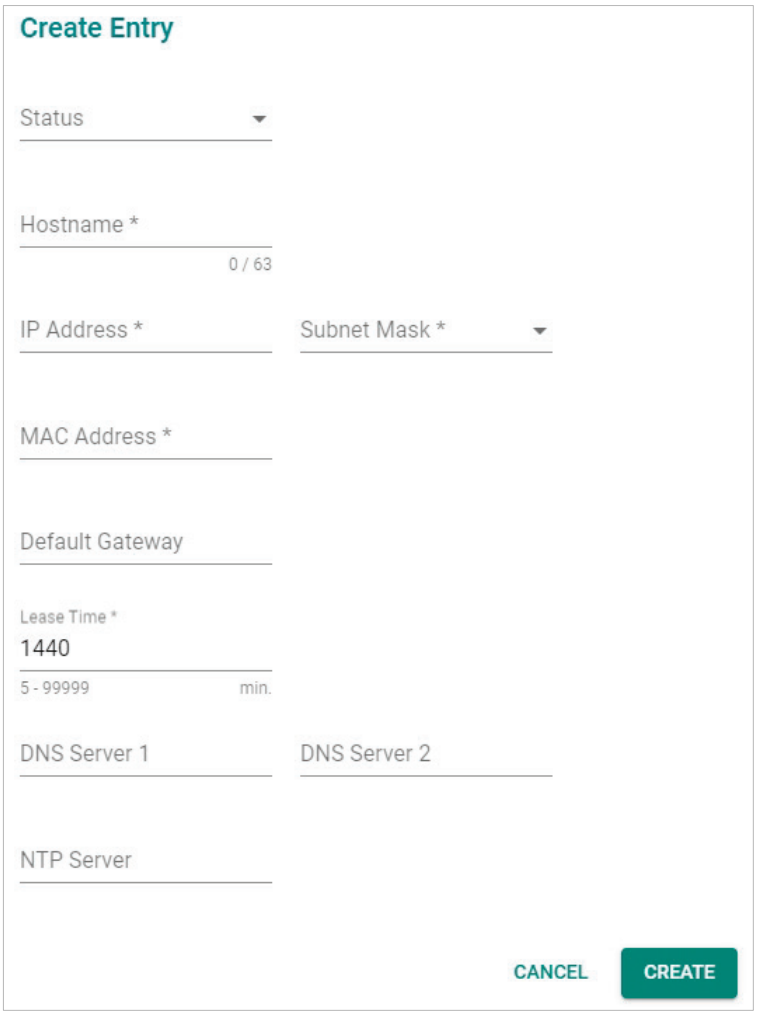
Use the Static DHCP list to ensure that devices connected to the Industrial Secure Router always use the same IP address. The static DHCP list matches IP addresses to MAC addresses.



For example, a device named "Device-01" was added to the Static DHCP list, with a static IP address set to 192.168.127.101 and MAC address set to 00:09:ad:00:aa:01. When a device with a MAC address of 00:09:ad:00:aa:01 is connected to the Industrial Secure Router, the Industrial Secure Router will offer the IP address 192.168.127.101 to this device.

Create a MAC-based IP Entry

Click ⊞ to create a new MAC-based IP entry. The hostname, IP address, and MAC address must be different from any existing MAC-based IP entries.



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable MAC-based IP assignment functionality.	None

Hostname

Setting	Description	Factory Default
Max. 63 characters	Enter a hostname for the device.	None

IP Address

Setting	Description	Factory Default
IP Address	Specify the IP address of the device.	None

Subnet Mask

Setting	Description	Factory Default
Subnet Mask	Specify the subnet mask of the device.	None

MAC Address

Setting	Description	Factory Default
MAC Address	Specify the MAC address of the device.	None

Default Gateway

Setting	Description	Factory Default
IP Address	Specify the default gateway of the device.	None

Lease Time

Setting	Description	Factory Default
5-99999 minutes	Specify the lease time for IP addresses assigned by the DHCP server.	1440

DNS Server 1

Setting	Description	Factory Default
IP Address	Specify the IP address for the first DNS server for DHCP clients.	None

DNS Server 2

Setting	Description	Factory Default
IP Address	Specify the IP address for the second DNS server for DHCP clients.	None

NTP Server

Setting	Description	Factory Default
IP Address	Specify the IP address for the NTP server for DHCP clients.	None

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

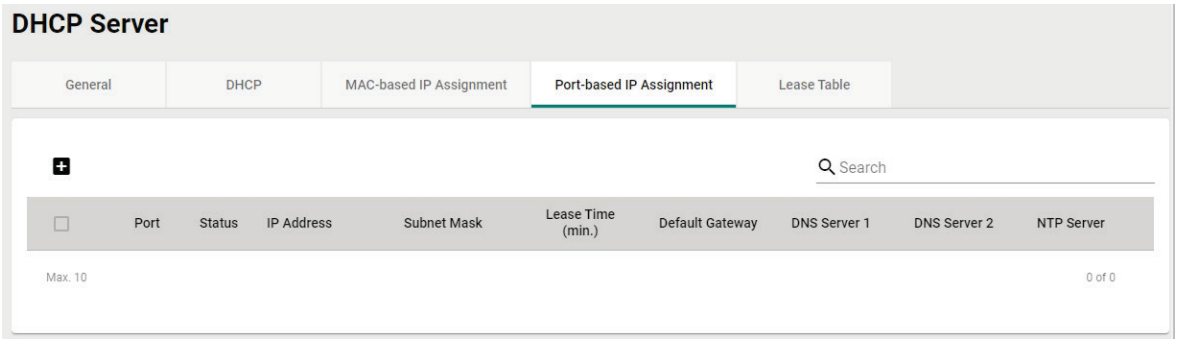
Delete a MAC-based IP Entry

Select the entry from the list and click .

Modify a MAC-based IP Entry

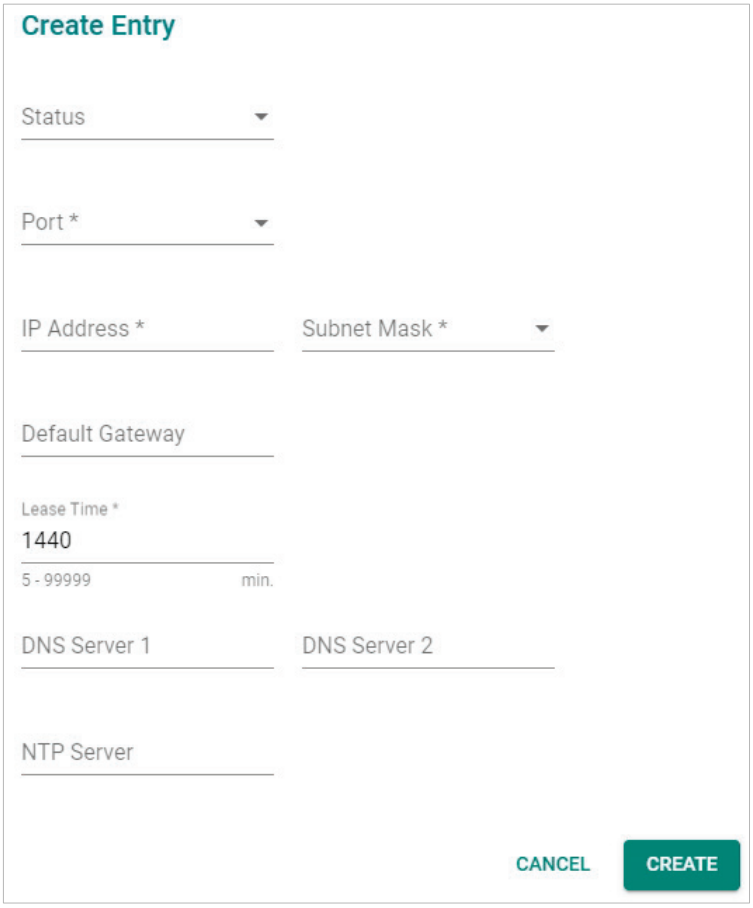
Click next to the MAC-based IP entry you want to modify. When finished, click **APPLY** to save your changes.

Port-based IP Assignment



Create a Port-based IP Entry

Click ⊞ to create a new port-based IP entry.



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable Port-based IP assignment functionality.	None

Port

Setting	Description	Factory Default
Port	Select the physical port on the device to associate the IP with.	None

IP Address

Setting	Description	Factory Default
IP Address	Specify the IP address of the connected device.	None

Subnet Mask

Setting	Description	Factory Default
Subnet Mask	Specify the subnet mask for the connected device.	None

Default Gateway

Setting	Description	Factory Default
IP Address	Specify the default gateway for the connected device.	None

Lease Time

Setting	Description	Factory Default
5-99999 minutes	Specify the lease time for IP addresses assigned by the DHCP server.	1440

DNS Server 1

Setting	Description	Factory Default
IP Address	Specify the IP address for the first DNS server for the connected device.	None

DNS Server 2

Setting	Description	Factory Default
IP Address	Specify the IP address for the second DNS server for the connected device.	None

NTP Server

Setting	Description	Factory Default
IP Address	Specify the IP address for the NTP server for the connected device.	None

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

Delete a Port-based IP Entry

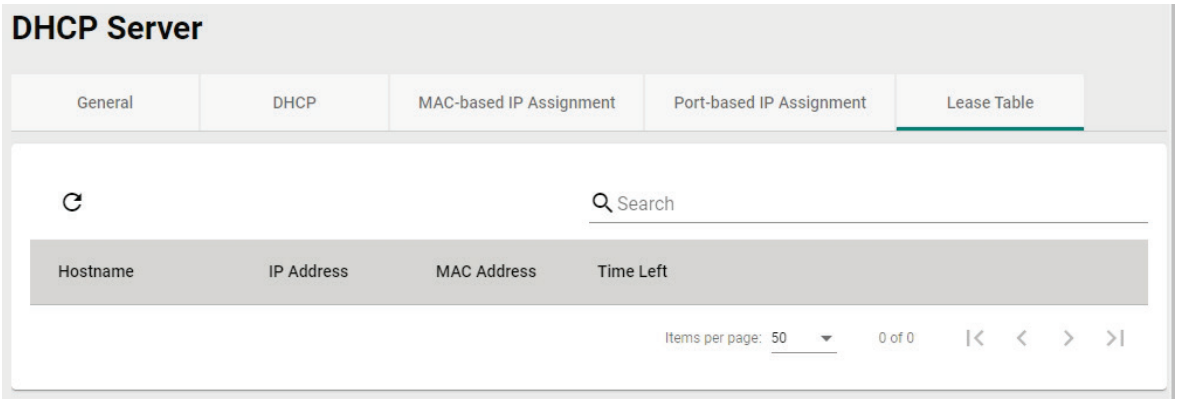
Select the entry from the list and click .

Modify a Port-based IP Entry

Click to next to the Port-based IP entry you want to modify. When finished, click **APPLY** to save your changes.

Lease Table

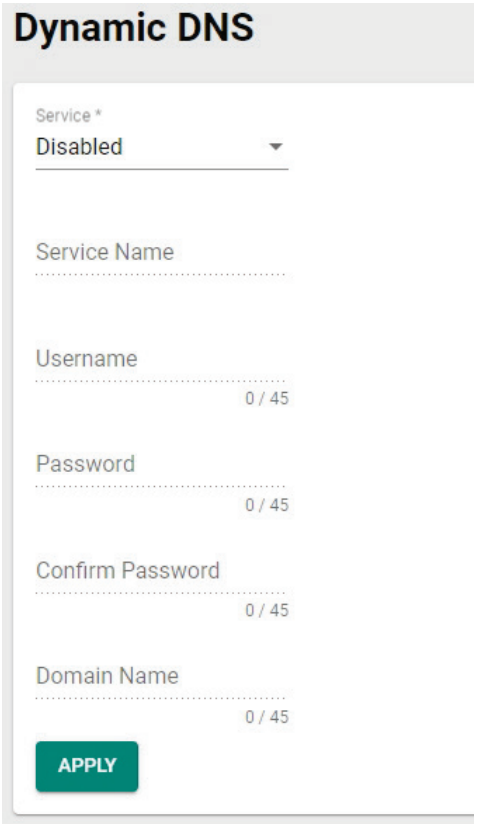
The Lease Table provides an overview of the current DHCP clients.



Click the icon to refresh the table.

Dynamic DNS

Dynamic DNS (Domain Name Server) allows you to use a domain name to connect to the Industrial Secure Router. The Industrial Secure Router can connect to four free DNS servers and register a domain name on these servers.



Service

Setting	Description	Factory Default
Disabled, freedns.afraid.org, www.3322.org, DynDns.org, NO-IP.com	Disable or select a DNS server.	Disabled

Service Name

Setting	Description	Factory Default
Max. 45 characters	The DNS server's name.	None

Username

Setting	Description	Factory Default
Max. 45 characters	Enter the DNS server username.	None

Password

Setting	Description	Factory Default
Max. 45 characters	Enter the DNS server password.	None

Confirm Password

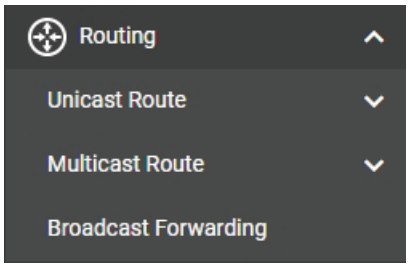
Setting	Description	Factory Default
Max. 45 characters	Confirm the DNS server password.	None

Domain name

Setting	Description	Factory Default
Max. 45 characters	Enter the DNS server's domain name	None

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

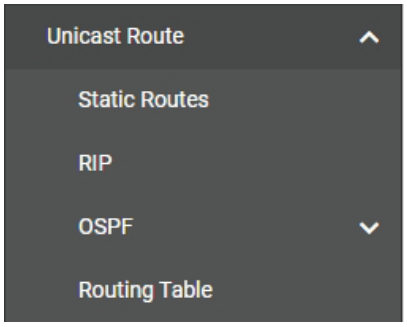
From the **Routing** section, you can configure the **Unicast Route**, **Multicast Route**, and **Broadcast Forwarding** settings.



Unicast Route

The Industrial Secure Router supports two routing methods: static routing and dynamic routing. Dynamic routing makes use of RIP V1/V1c/V2. You can either choose one routing method or combine the two methods to establish your routing table. A routing entry includes the following items: the destination address, the next hop address (which is the next router along the path to the destination address), and a metric that represents the cost to access a different network.

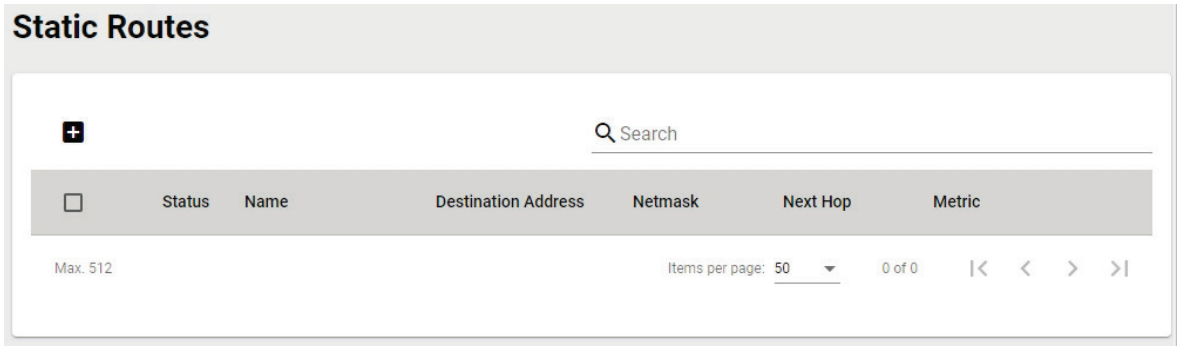
From the **Unicast Route** section, the following functions can be configured: **Static Routes, RIP, OSPF,** and **Routing Table**.



Static Routes

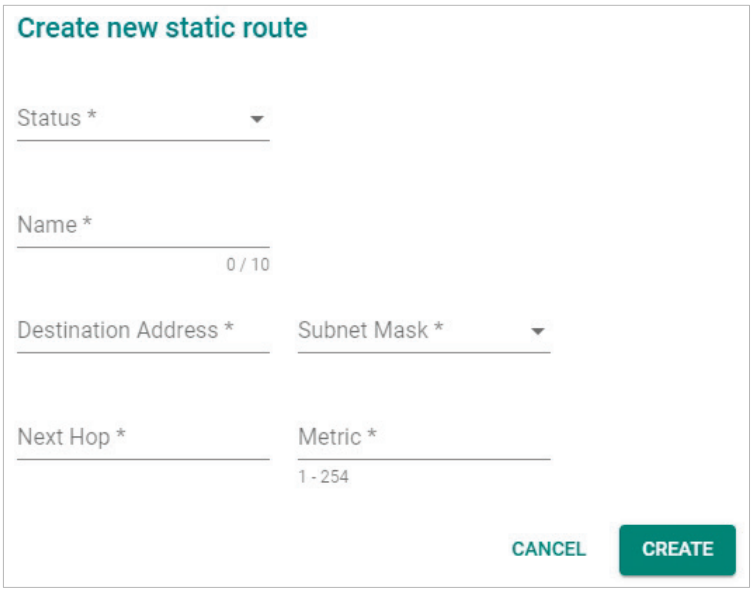
The Static Routing page is used to configure the Industrial Secure Router's static routing table.

Static routes allow you to specify the next hop (or router) that the Industrial Secure Router forwards data to for a specific subnet. The Static Route settings will be added to the routing table and stored on the Industrial Secure Router.



Create a Static Route

Click ➕ to create a new static route.



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the static route.	None

Name

Setting	Description	Factory Default
Max. 10 characters	Enter a name for the static route.	None

Destination Address

Setting	Description	Factory Default
Destination address	Specify the destination IP address.	None

Subnet Mask

Setting	Description	Factory Default
Subnet mask	Specify the subnet mask for this IP address.	None

Next Hop

Setting	Description	Factory Default
Next hop IP address	Specify the next router on the path to the destination IP.	None

Metric

Setting	Description	Factory Default
1 to 254	Specify the metric value for the route.	None

Click **CREATE** to add the entry to the Static Routing Table.

Delete a Static Route

Select the entry from the list and click 🗑.

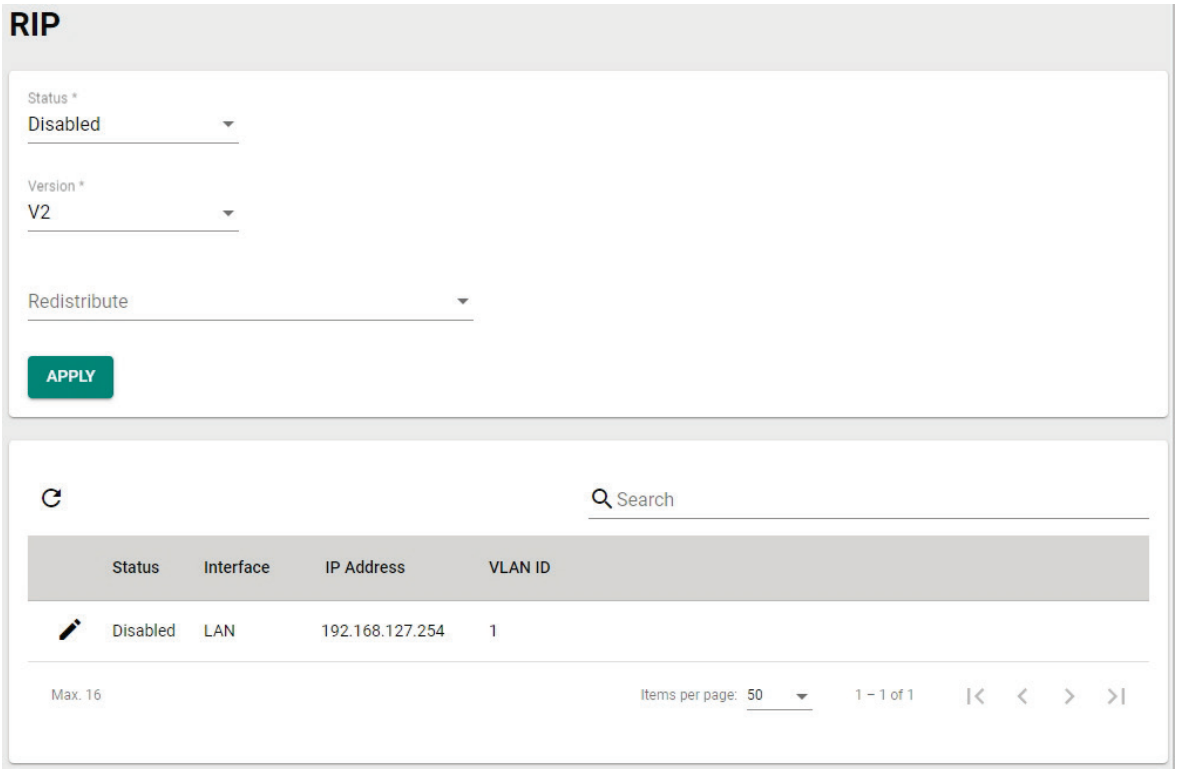
Modify an Existing Static Route

Click ✎ next to the entry you want to modify. When finished, click **APPLY** to save your changes.

RIP (Routing Information Protocol)

RIP is 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.

The **RIP** page is used to set up the RIP parameters.



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the RIP protocol.	Disabled

Version

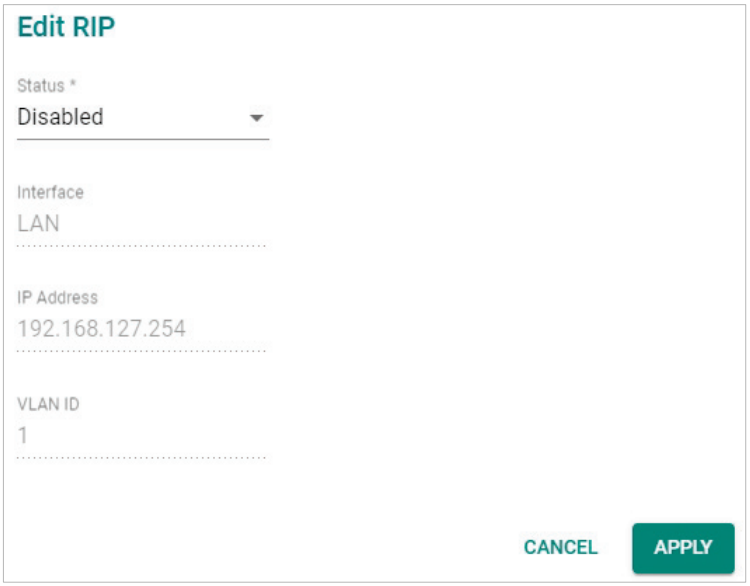
Setting	Description	Factory Default
V1/V2	Select the RIP protocol version.	V2

Redistribute

Setting	Description	Factory Default
Connected	Enable the Redistributed Connected function.	None
Static	Enable the Redistributed Static Route function. The entries that are set in a static route will be re-distributed if this option is enabled.	
OSPF	Enable the Redistributed OSPF function.	

Modify an Existing RIP Entry

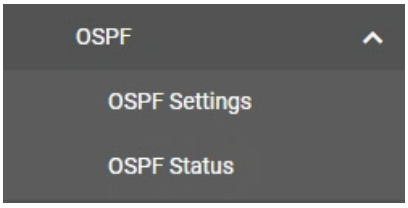
Click the ✎ icon next to the entry you want to modify. When finished, click **APPLY** to save your changes.



OSPF (Dynamic Routing With Open Shortest Path First)

Open Shortest Path First (OSPF) is a dynamic routing protocol for use on Internet Protocol (IP) networks. Specifically, it is a link-state routing protocol, and falls into the group of interior gateway protocols, operating within a single autonomous system. As a link-state routing protocol, OSPF establishes and maintains neighbor relationships in order to exchange routing updates with other routers. The neighbor relationship table is called an adjacency database in OSPF. OSPF forms neighbor relationships only with the routers directly connected to it. In order to form a neighbor relationship between two routers, the interfaces used to form the relationship must be in the same area. An interface can only belong to a single area. With OSPF enabled, Industrial Secure router is able to exchange routing information with other L3 switches or routers more efficiently in a large system.

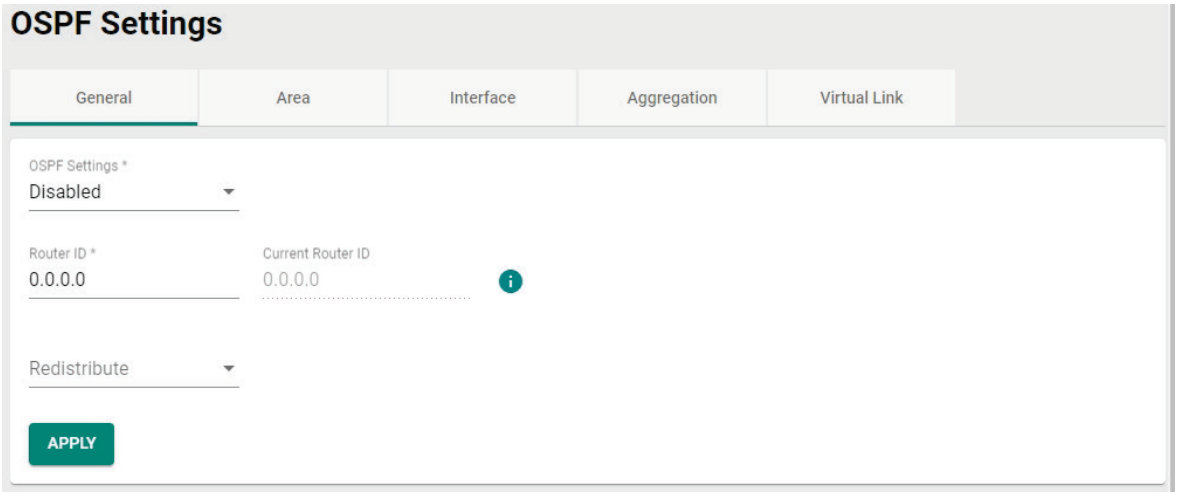
This section describes the configurations for **OSPF Settings** and **OSPF Status**.



OSPF Settings

General Settings

The Industrial Secure router has an OSPF router ID, written in the dot-decimal format (e.g., 1.2.3.4) of an IP address. This ID must be established for every OSPF instance. If not explicitly configured, the default ID (0.0.0.0) will be regarded as the router ID. Since the router ID is an IP address, it does not need to be part of any routable subnet on the network.



OSPF Settings

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the global OSPF function.	Disabled

Router ID

Setting	Description	Factory Default
Router ID	Specify the router ID.	0.0.0.0

Current Router ID

Setting	Description	Factory Default
Current Router ID	Shows the current ID of the Industrial Secure Router.	0.0.0.0

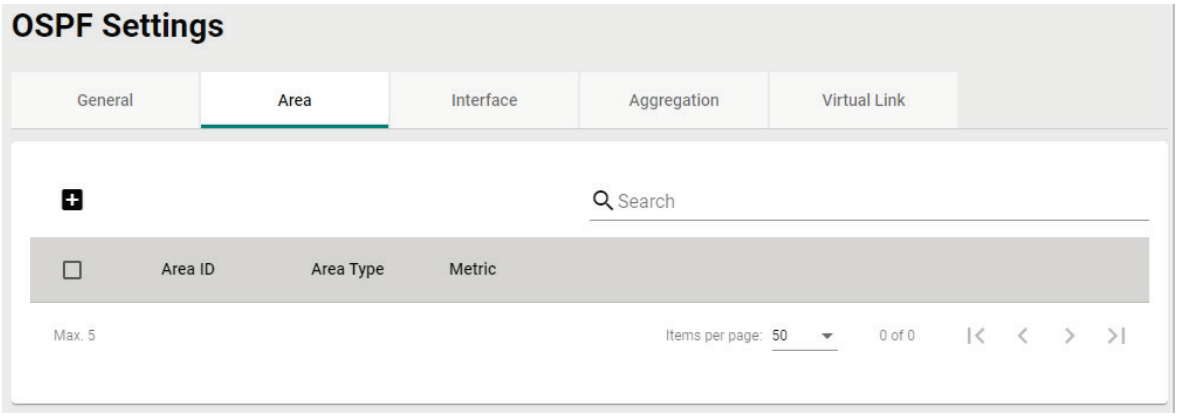
Redistributed

Setting	Description	Factory Default
Connected	Entries learned from the directly connected interfaces will be redistributed.	None
Static	Entries set in a static route will be redistributed.	
RIP	Entries learned from through RIP will be redistributed.	

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

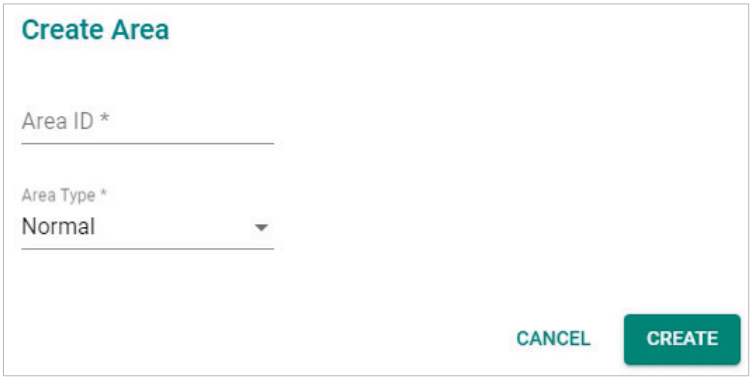
Area Settings

An OSPF domain is divided into areas that are labeled with 32-bit area identifiers, commonly written in the dot-decimal notation of an IPv4 address. Areas are used to divide a large network into smaller network areas. They are logical groupings of hosts and networks, including the routers connected to a particular area. 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.



Create a New Area

Click the icon to create a new area.



Area ID

Setting	Description	Factory Default
Area ID	Specify the Area ID which defines the areas that this Industrial Secure Router connects to.	None

Area Type

Setting	Description	Factory Default
Normal, Stub, NSSA	Select the area type.	Normal

Metric

Setting	Description	Factory Default
1 to 65535	If the Area Type is Stub or NSSA, specify the metric.	1

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

Modify an Existing Area ID

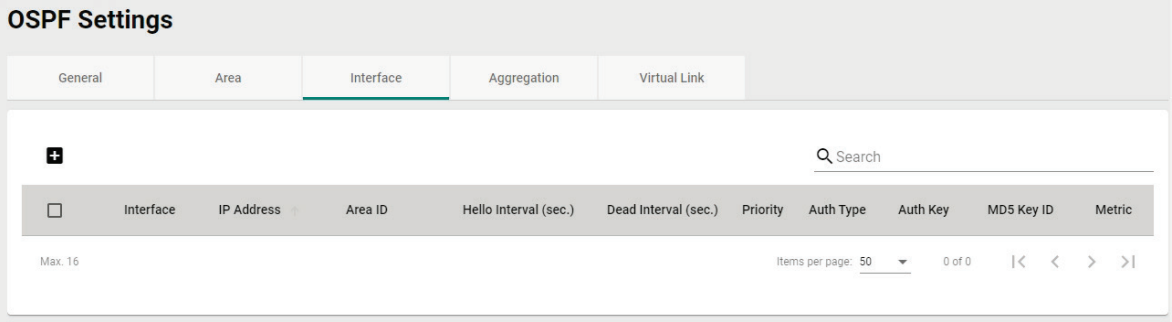
Click the icon next to the area you want to modify. When finished, click **APPLY** to save your changes.

Delete an Existing Area ID

Select the item(s) in the Area ID List, click the icon and then click **DELETE** to delete the item(s).

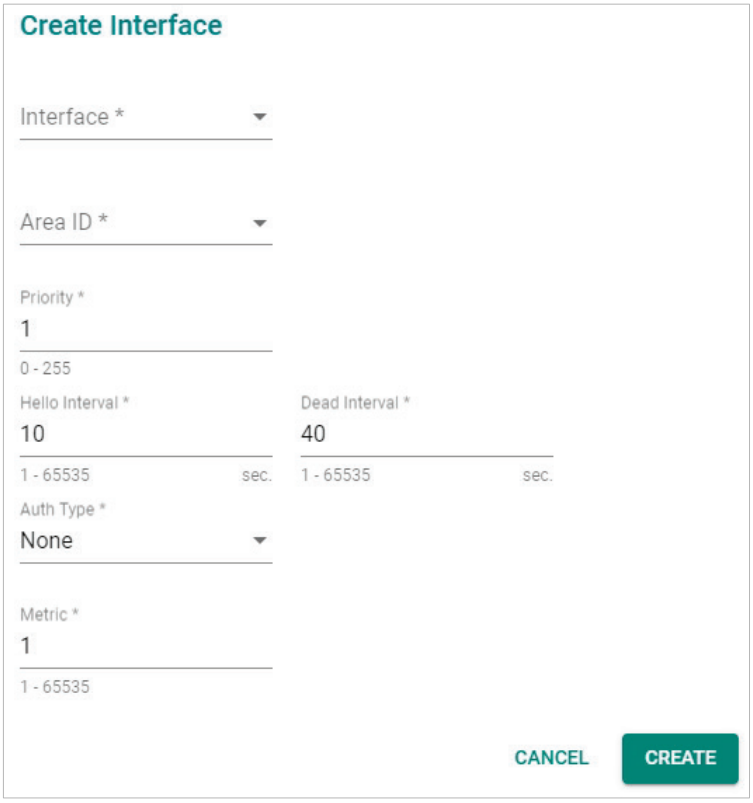
Interface Settings

Before using OSPF, you need to assign an interface for each area.



Create a New Interface

Click the ⊞ icon to create a new OSPF Interface.



Interface

Setting	Description	Factory Default
LAN, WAN	Select an interface to assign to the area.	None

Area ID

Setting	Description	Factory Default
Area ID	Specify the Area ID.	None

Priority

Setting	Description	Factory Default
0 to 255	Specify the priority.	1

Hello Interval

Setting	Description	Factory Default
1 to 65535 seconds	Specify the Hello message interval. Hello packets are packets that an OSPF process sends to its OSPF neighbors to maintain connectivity with those neighbors. The hello packets are sent at a configurable interval (in seconds). The value of all hello intervals must be the same within a network.	10

Dead Interval

Setting	Description	Factory Default
1 to 65535 seconds	Specify the Dead interval. The dead interval is a configurable interval (in seconds), and defaults to four times the value of the hello interval.	40

Auth Type

Setting	Description	Factory Default
None, Simple, MD5	Select an authentication method. OSPF authentication provides the flexibility of authenticating OSPF neighbors. Users can enable authentication to exchange routing update information in a secure manner. OSPF authentication can either be none, simple, or MD5. Authentication does not need to be configured. If it is configured, all Industrial Secure Routers on the same segment must have the same password and authentication method.	None

Auth Key

Setting	Description	Factory Default
0 to 8	Specify the authentication key. If the Auth Type is Simple the auth key is a pure-text password. If the Auth Type is MD5 the auth key is encrypted password.	None

MD5 Key ID

Setting	Description	Factory Default
1 to 255	MD5 authentication provides higher security than plain text authentication. This method uses the 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.	None

Metric

Setting	Description	Factory Default
1 to 65535	Manually set Metric value /Cost of OSPF.	1

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

Modify an Existing Interface

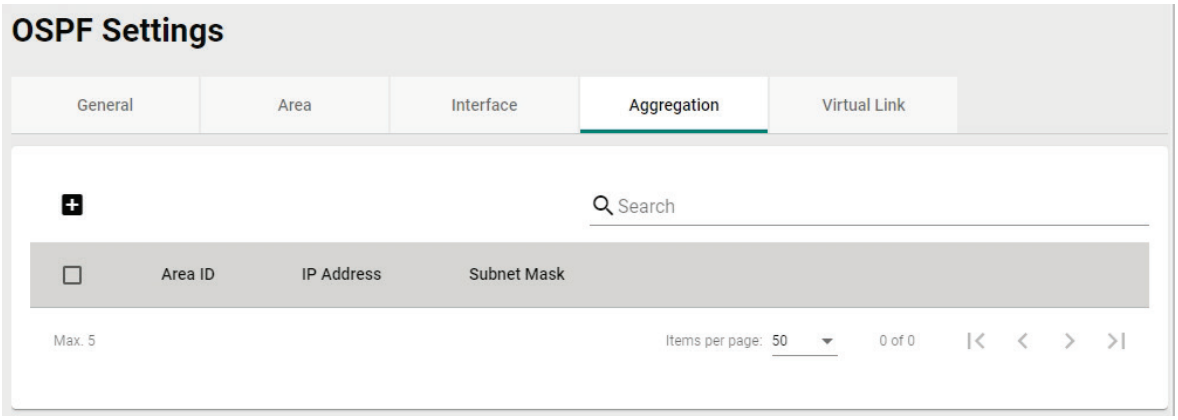
Click the icon next to the entry you want to modify. When finished, click **APPLY** to save your changes.

Delete an Existing Interface

Select the item(s) in the Interface List, click the icon and click **DELETE** to delete the item(s).

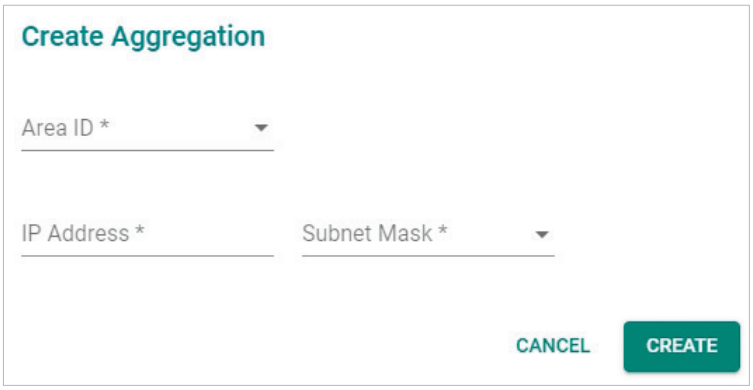
Aggregation Settings

Each OSPF area, which consists of a set of interconnected subnets and traffic, is handled by routers attached to two or more areas, known as Area Border Routers (ABRs). With the OSPF aggregation function, users can combine groups of routes with common addresses into a single routing table entry. The main purpose of this function is to reduce the size of routing tables.



Create a New OSPF Aggregation

Click the icon to create a new OSPF Area Aggregation.



Area ID

Setting	Description	Factory Default
Area ID	Select the Area ID that you want to configure.	None

IP Address

Setting	Description	Factory Default
IP address	Specify the IP address of the area.	None

Subnet Mask

Setting	Description	Factory Default
1 (128.0.0.0) to 31 (255.255.255.254)	Select the network subnet mask.	None

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

Modify an Existing Aggregation

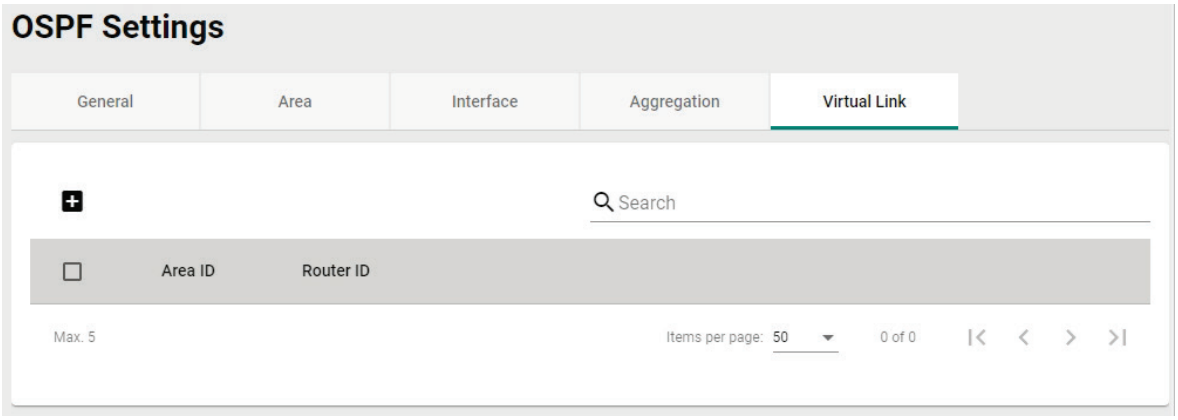
Click the icon next to the entry you want to modify. When finished, click **APPLY** to save your changes.

Delete an Existing Aggregation

Select the item(s) in the Aggregation List, click the icon and click **DELETE** to delete the item(s).

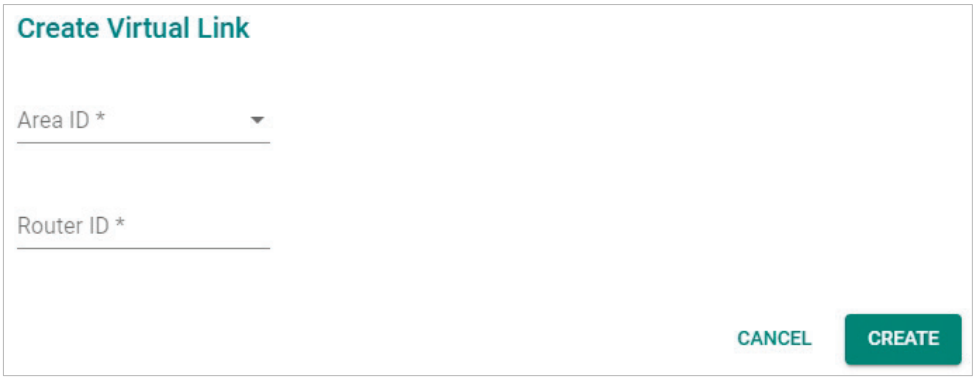
Virtual Link Settings

All areas in an OSPF autonomous system must be physically connected to the backbone area (Area 0.0.0.0). However, this is impossible in some cases. For those cases, users can create a virtual link to connect to the backbone through a non-backbone area or to connect two parts of a partitioned backbone through a non-backbone area.



Create a Virtual Link

Click the icon to create a new virtual link.



Area ID

Setting	Description	Factory Default
Area ID	Select the Area ID which defines the areas that this Industrial Secure Router connect to.	None

Router ID

Setting	Description	Factory Default
Router ID	Specify the Industrial Secure Router's ID.	None

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

Modify an Existing Virtual Link

Click the icon next to the entry you want to modify. When finished, click **APPLY** to save your changes.

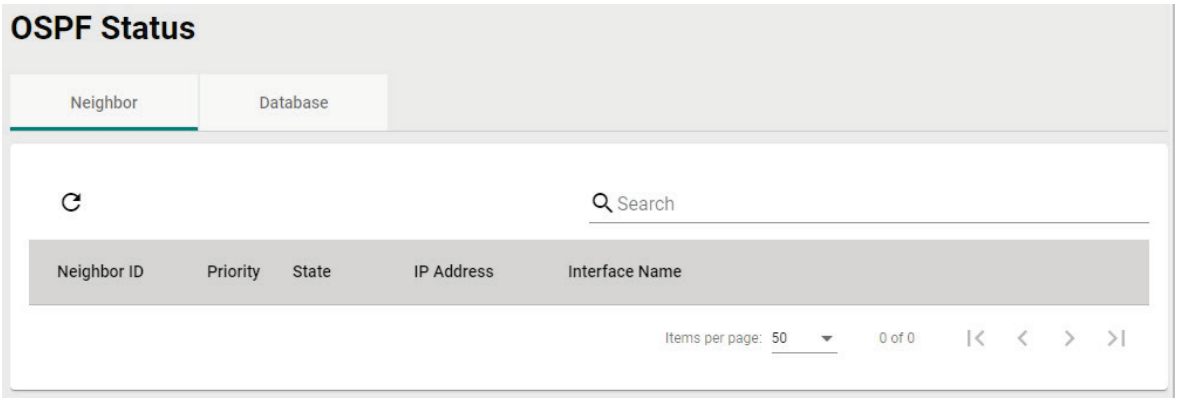
Delete an Existing Virtual Link

Select the item(s) in the Virtual Link List, click the icon and click **DELETE** to delete the item(s).

OSPF Status

Neighbor

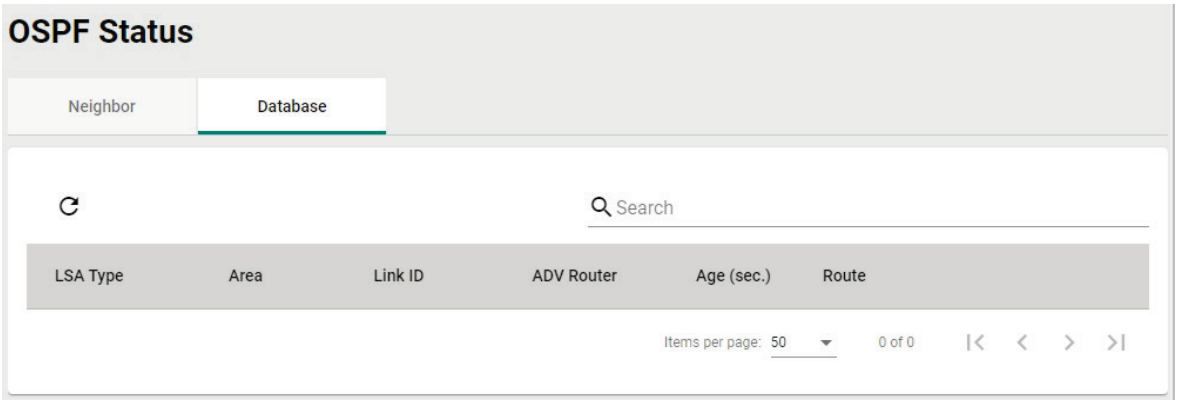
The Neighbor table shows all current OSPF neighbors.



Click the icon to refresh the table.

Database

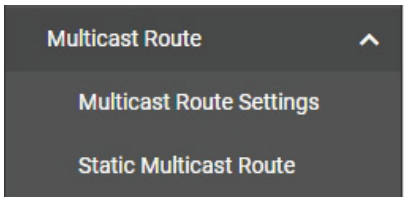
The Database table shows the current OSPF LSA information.



Click the icon to refresh the table.

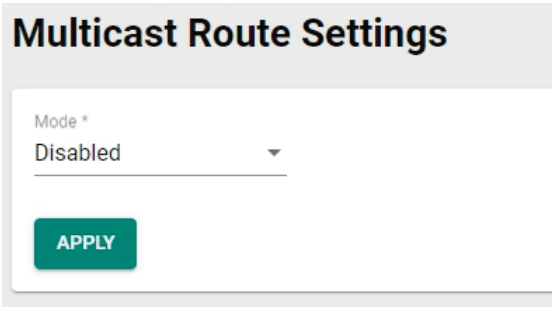
Multicast Route

From the **Multicast Route** section, the following functions can be configured: **Multicast Route**, and **Static Multicast Route**.



Multicast Route Settings

The industrial secure router supports one multicast routing protocol: **Static Multicast Route**.



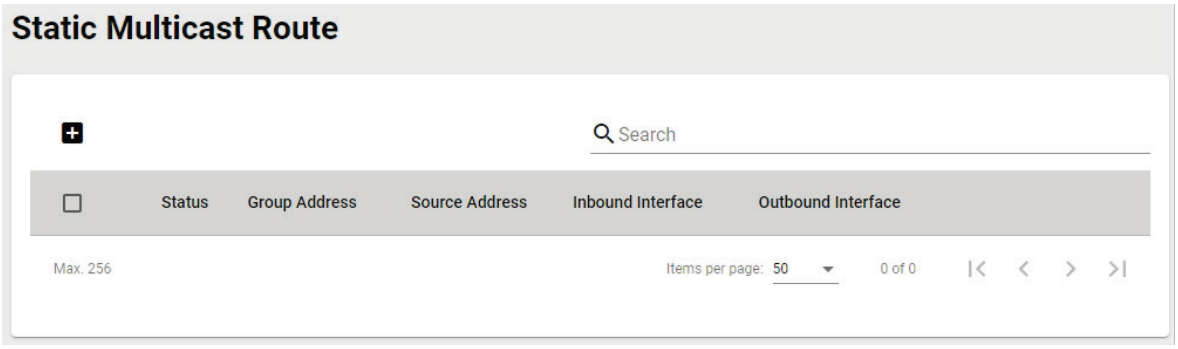
Mode

Setting	Description	Factory Default
Static Multicast Route, Disabled	Disable multicast routing or select which multicast routing protocol to use (Static multicast route).	Disabled

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

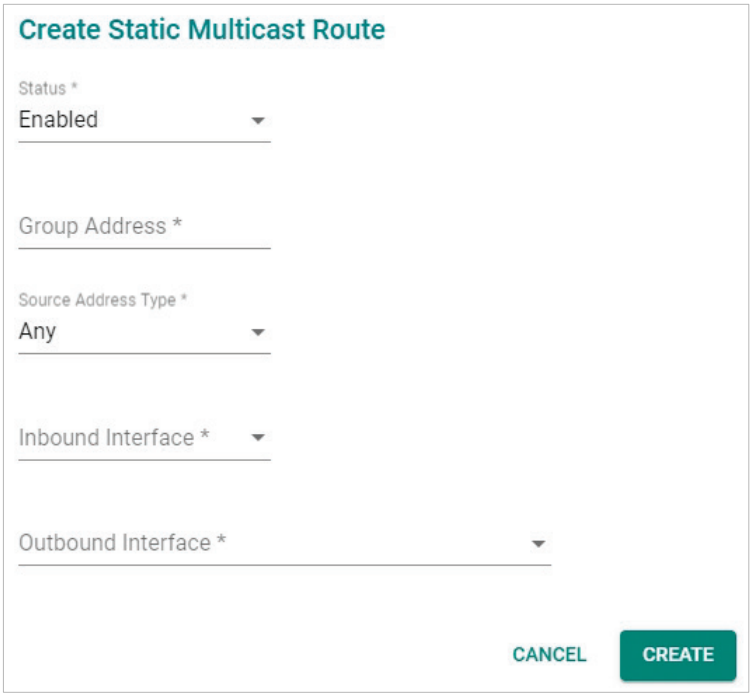
Static Multicast Route

The Static Multicast Route table shows all static multicast entries.



Create a Static Multicast Route

Click the icon to create a new Static Multicast Route.



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the static multicast route.	Enabled

Group Address

Setting	Description	Factory Default
IP address	Specify the group IP address	None

Source Address Type

Setting	Description	Factory Default
Any	Set the source to any IP address.	Any
Specify Source	Set the source to a specified IP address only.	

Source Address

Setting	Description	Factory Default
IP address	If the Source Address Type is Specify Source, enter the source IP address.	None

Inbound Interface

Setting	Description	Factory Default
LAN, WAN	Select which interface the broadcast packet will come from.	None

Outbound Interface

Setting	Description	Factory Default
LAN, WAN	Select which interface the broadcast packet will pass through.	None

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

Modify an Existing Static Multicast Route

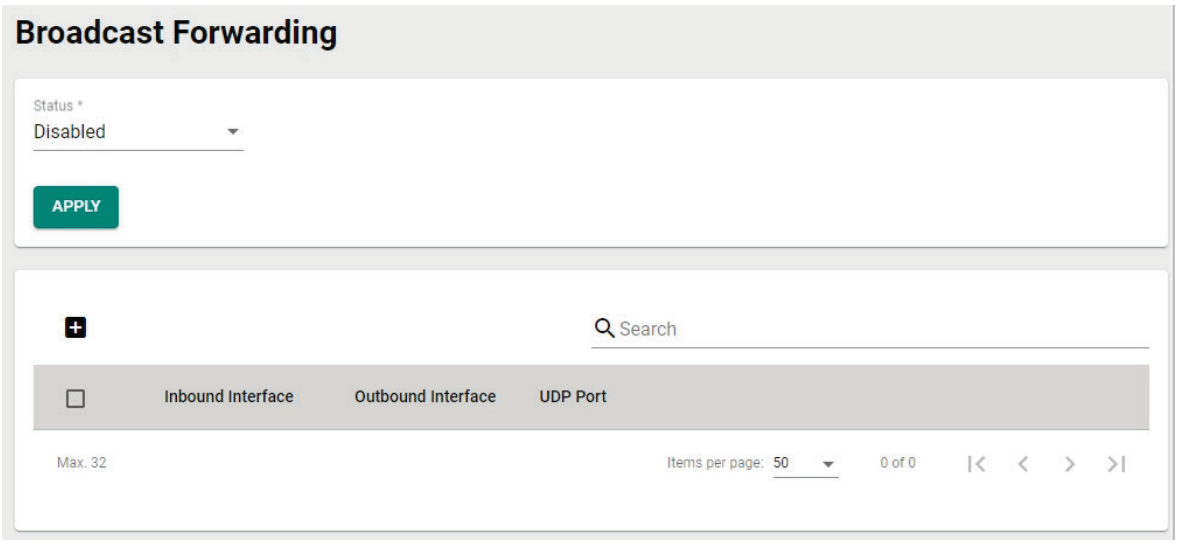
Click the icon next to the entry you want to modify. When finished, click **APPLY** to save your changes.

Delete an Existing Static Multicast Route

Select the item(s) in the Static Multicast Route List, click the icon and then click **DELETE** to delete the item(s).

Broadcast Forwarding

In some scenarios, users may have to issue broadcast packets to query all the devices on the network for data collecting, such as Modbus devices. However, normally, broadcast packets cannot pass through the router. Broadcast Forwarding allows users to configure which interface and UDP port numbers broadcast packets will pass through.



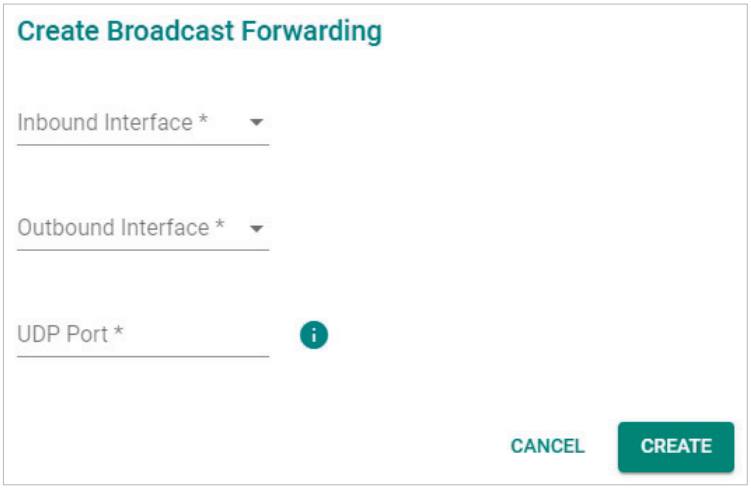
Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable Broadcast Forwarding. Enable this function to allow broadcast packets to pass through the Industrial Secure Router.	Disabled

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

Create a Broadcast Forwarding Entry

Click the icon to create a new Broadcast Forwarding entry.



Inbound Interface

Setting	Description	Factory Default
LAN, WAN	Select which interface the broadcast packet will come from.	None

Outbound Interface

Setting	Description	Factory Default
LAN, WAN	Select which interface the broadcast packet will pass through.	None

UDP Port

Setting	Description	Factory Default
UDP Port Number	Specify the service port number. You can enter multiple port numbers up to a total of 8 ports. For example, entering "67, 68, 520, 1701" means the device will listen on UDP ports 67, 68, 520, and 1701.	None

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

Modify the Existing Broadcast Forwarding

Click the icon next to the entry you want to modify. When finished, click **APPLY** to save your changes.

Delete the Existing Broadcast Forwarding

Select the item(s) in the Broadcast Forwarding List, click the icon and click **DELETE** to delete the item(s).

9. NAT (Network Address Translation)

NAT Concept

NAT (Network Address Translation) is a common security function for changing the IP address during Ethernet packet transmission. When the user wants to hide the internal IP address (LAN) from the external network (WAN), the NAT function will translate the internal IP address to a specific IP address, or an internal IP address range to one external IP address. The benefits of using NAT include:

- The N-1 or port forwarding NAT function to hide the internal IP address of a critical network or device to increase the level of security of industrial network applications.
- The Industrial Secure Router uses the same private IP address for different, but identical, groups of Ethernet devices. For example, 1-to-1 NAT makes it easy to duplicate or extend identical production lines.

NOTE

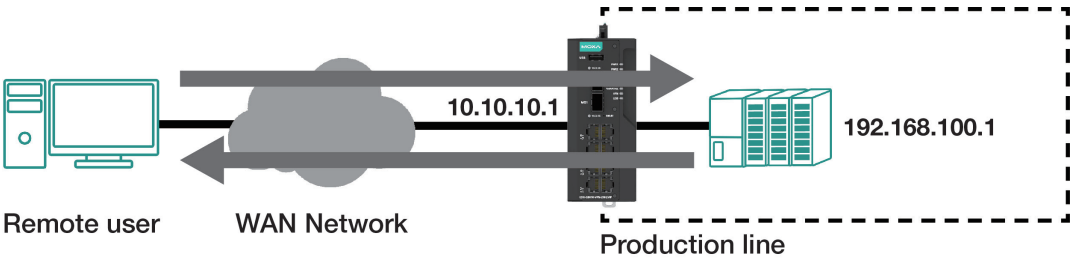
The NAT function will check if incoming or outgoing packets match the policy. It starts by checking the packet against the first policy (Index=1); if the packet matches this policy, the Industrial Secure Router will translate the address immediately and then start checking the next packet. If the packet does not match this policy, it will check with the next policy.

NOTE

The Industrial Secure Router supports a maximum of 512 NAT policies.

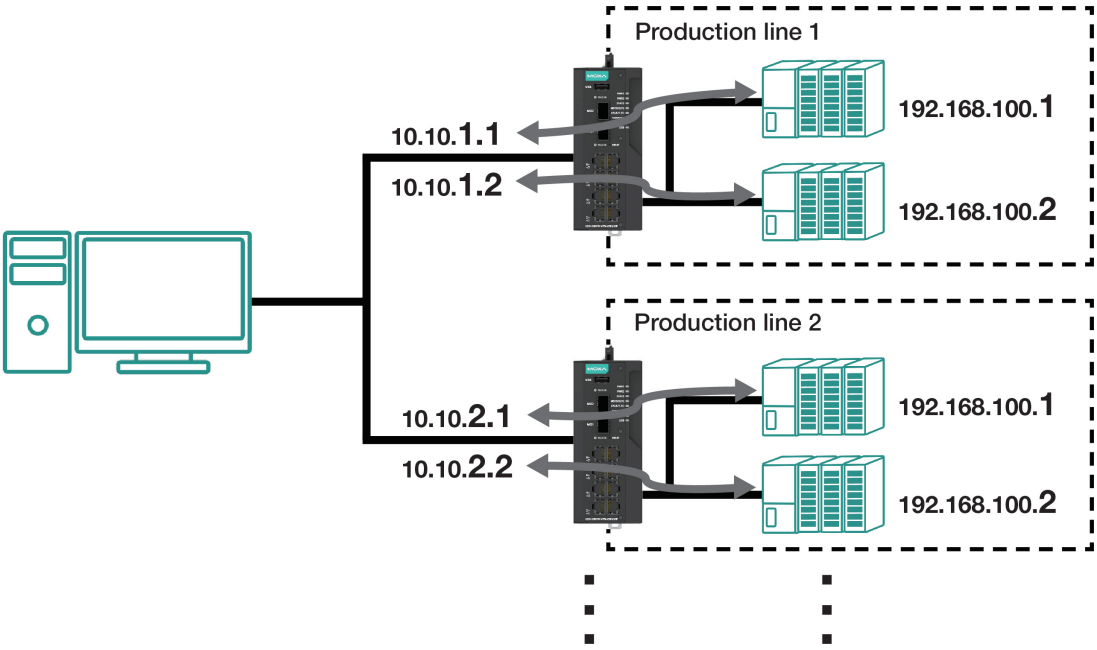
1-to-1 NAT Overview

If the internal device and external device need to communicate with each other, choose 1-to-1 NAT, which offers bi-directional communication (N-to-1 and Port forwarding are both single-directional communication NAT functions).



1-to-1 NAT is usually used when you have a group of internal servers with private IP addresses that must connect to the external network. You can use 1-to-1 NAT to map the internal servers to public IP addresses. The IP address of the internal device will not change. 1-to-1 NAT will also create a corresponding secondary IP address (10.10.10.1) if the device is in the same subnet as the incoming interface.

The figure below illustrates how a user could extend production lines and use the same private IP addresses of internal devices in each production line. The internal private IP addresses of these devices will map to different public IP addresses. Configuring a group of devices for 1-to-1 NAT is easy and straightforward.



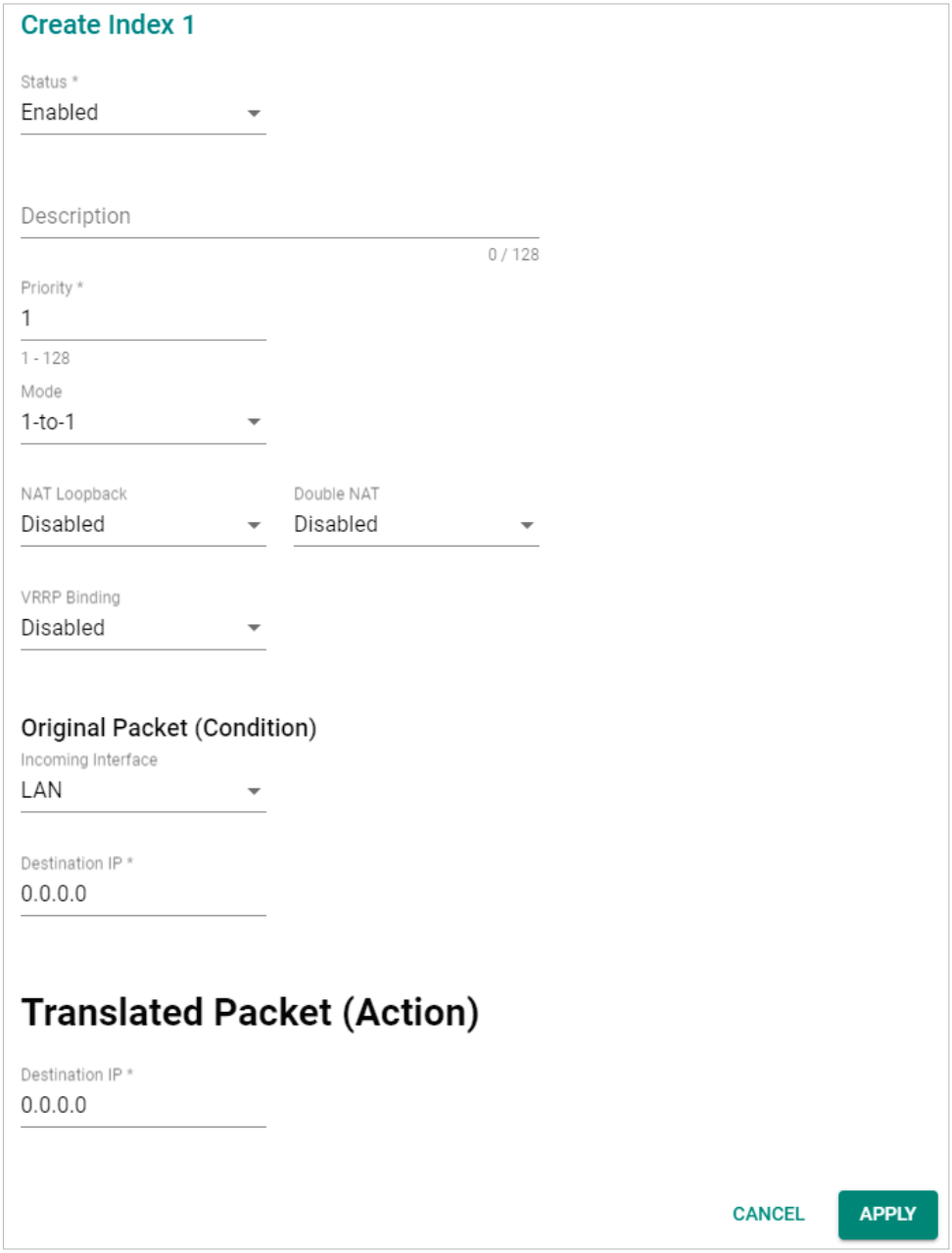
1-to-1 NAT Setting in Production Line 1

	Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)
☐	Enabled	1-to-1_production_line_1-1	1	1-to-1		WAN	Any:Any	10.10.1.1:Any	All	Any:Any	192.168.100.1:Any
☐	Enabled	1-to-1_production_line_1-2	2	1-to-1		WAN	Any:Any	10.10.1.2:Any	All	Any:Any	192.168.100.2:Any

1-to-1 NAT Setting in Production Line 2

	Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)
☐	Enabled	1-to-1_production_line_2-1	1	1-to-1		WAN	Any:Any	10.10.2.1:Any	All	Any:Any	192.168.100.1:Any
☐	Enabled	1-to-1_production_line_2-2	2	1-to-1		WAN	Any:Any	10.10.2.2:Any	All	Any:Any	192.168.100.2:Any

1-to-1 NAT



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the NAT policy.	Enabled

Description

Setting	Description	Factory Default
Description	Enter a name for the NAT rule.	None

Priority

Setting	Description	Factory Default
1 to 128	Specify the index of the NAT rule.	1

NAT Mode

Setting	Description	Factory Default
1-to-1 N-to-1 PAT Advance	Select 1-to-1 as the NAT type. For other NAT modes, refer to: N-to-1 PAT Advance	1-to-1

NAT Loopback

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the NAT Loopback function. Refer to NAT Loopback for more information.	Disabled

Double NAT

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the Double NAT function. Refer to Double NAT for more information.	Disabled

VRRP Binding

Setting	Description	Factory Default
VRRP Index No	Select which VRRP settings the 1-to-1 NAT rule should use.	Disabled

NOTE

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, the1-to-1 NAT rule will be valid regardless of if the system is the master or backup.

Original Packet (Condition)

Incoming Interface

Setting	Description	Factory Default
All LAN WAN	Select the incoming interface for the NAT rule.	LAN

Destination IP

Setting	Description	Factory Default
IP Address	Set the public IP address which the internal IP will be translated into.	0.0.0.0

Translated Packet (Action)

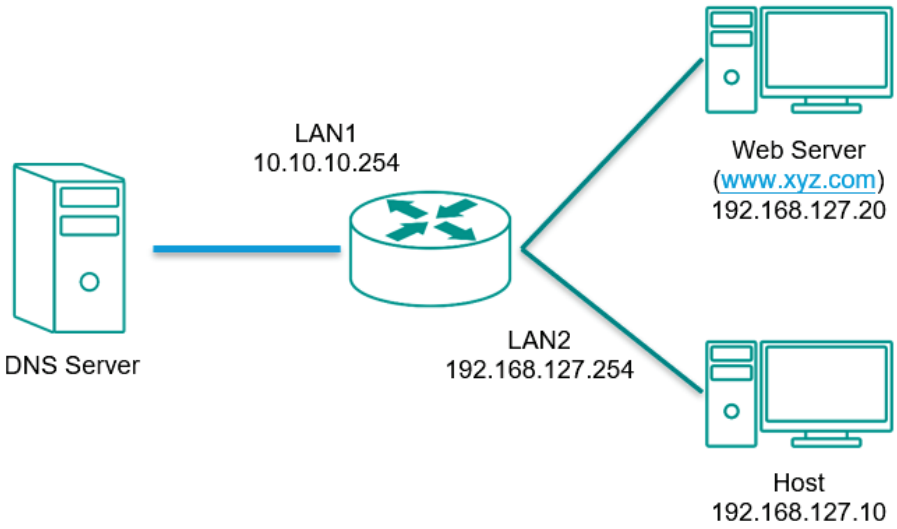
Destination IP

Setting	Description	Factory Default
IP Address	Specify the internal IP address on the LAN.	0.0.0.0

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

NAT Loopback

NAT Loopback is designed to facilitate communication with service servers which have external IP translation within the same LAN segment. Consider the following scenario:



1. Host tries to access the web server via www.xyz.com.
2. The DNS server returns the Web Server IP: 10.10.10.20.
3. Host will start to send the request packets to 10.10.10.20.

With NAT Loopback disabled:

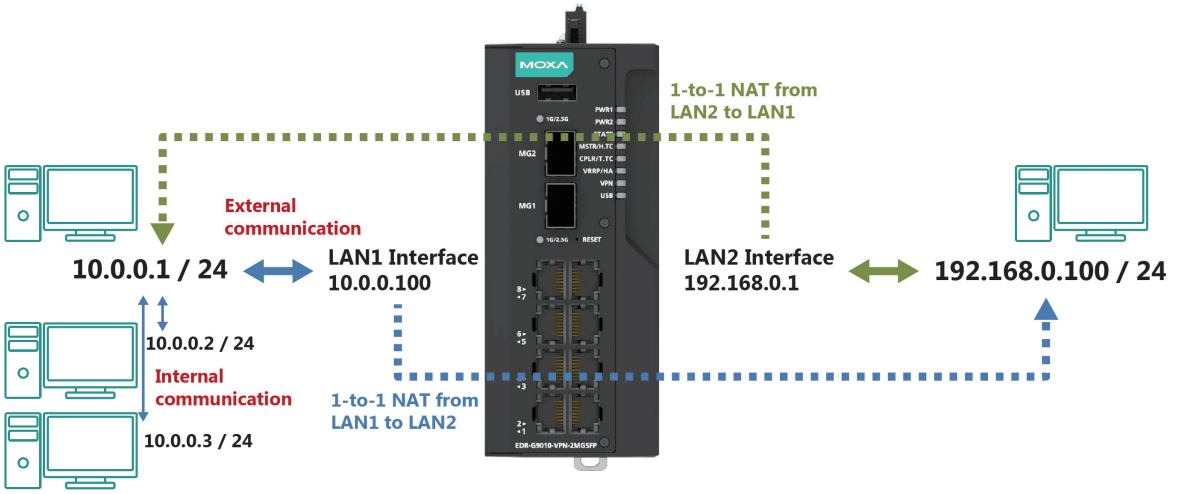
- Because the request packet comes from Host, the incoming interface does not match any NAT rule.
- The EDR-G9010 will receive the request packet because the NAT rule has created a secondary IP: 10.10.10.20.
- The EDR-G9010 sends the response packet to Host itself.
- Host will access the EDR-G9010's web page via www.xyz.com.

With NAT Loopback enabled:

- The EDR-G9010 will forward the request packet from Host to the Web Server with Destination (from 10.10.10.20 to 192.168.127.20) and Source (from 192.168.127.10 to 10.10.10.20) IP translation.
- The Web Server sends the response packet to the EDR-G9010. The EDR-G9010 then forwards it to Host with Destination (from 10.10.10.20 to 192.168.127.10) and Source (from 192.168.127.20 to 10.10.10.20) IP translation.
- Host will correctly access the Web Server via www.xyz.com.

	Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)
☐	Enabled		1	1-to-1		LAN	Any:Any	10.10.10.20:Any	All	Any:Any	192.168.127.20:Any

Bidirectional 1-to-1 NAT



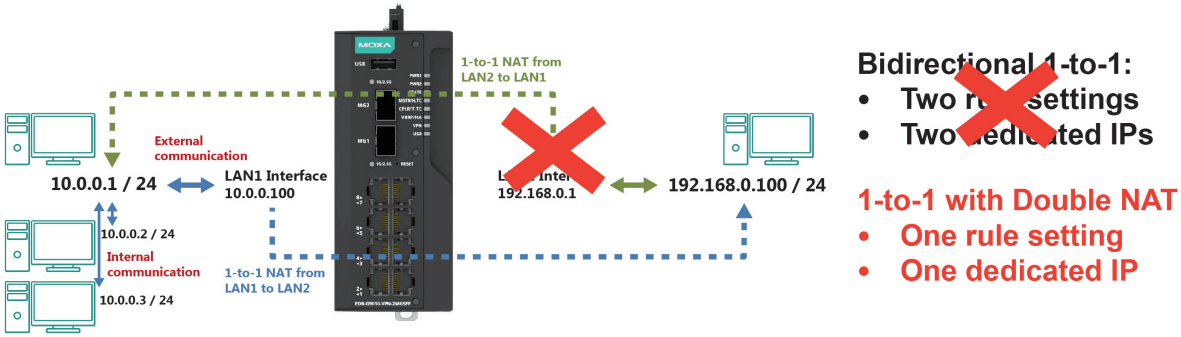
Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)
Enabled		1	1-to-1		LAN	Any:Any	192.168.0.1:Any	All	Any:Any	10.0.0.1:Any
Enabled		2	1-to-1		WAN	Any:Any	10.0.0.100:Any	All	Any:Any	192.168.0.100:Any

For some applications, devices need to talk to both internal and external devices without using a gateway. Bidirectional 1-to-1 NAT can do Network Address Translation in both directions without needing a gateway.

Double NAT

The traditional bidirectional 1-to-1 NAT concept uses two 1-to-1 rules to facilitate two-way communication, as in the example below. With Double NAT, only 1-to-1 rule is necessary. The EDR-G9010 will automatically translate the incoming and outgoing addresses as if it was handling two separate rules, one for inbound and one for outbound. The main advantage of Double NAT is that it reduces the number of NAT rules and necessary IP addresses.

Example



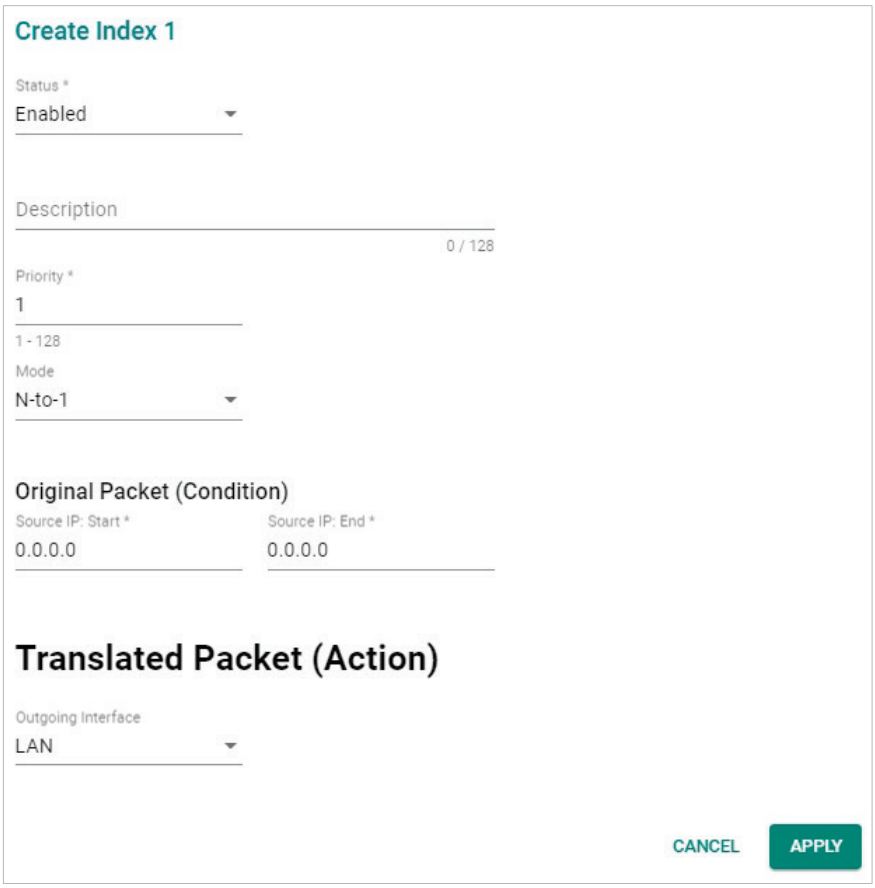
Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)
Enabled		1	1-to-1		LAN	Any:Any	10.0.0.100:Any	All	Any:Any	192.168.0.100:Any

NOTE

The Industrial Secure Router can obtain an IP address via DHCP or PPPoE. However, if this dynamic IP address is the same as the WAN IP for 1-to-1 NAT, then the 1-to-1 NAT function will not work. For this reason, we recommend disabling the DHCP/PPPoE function when using the 1-to-1 NAT.

N-to-1 NAT

If the user wants to hide the internal IP address from users outside the LAN, the easiest way is to use the N-to-1 (or N-1) NAT function. N-1 NAT replaces the source IP address with an outgoing interface IP address and adds a logical port number to identify the connection of this internal/external IP address. This function is also called "Network Address Port Translation" (NAPT) or "IP Masquerading".



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the NAT policy.	Enabled

Description

Setting	Description	Factory Default
Description	Enter a name for the NAT rule.	None

Priority

Setting	Description	Factory Default
1 to 128	Specify the index of the NAT rule.	1

NAT Mode

Setting	Description	Factory Default
1-to-1 N-to-1 PAT Advance	Select N-to-1 as the NAT type. For other NAT modes, refer to: 1-to-1 PAT Advance	1-to-1

Original Packet (Condition)

Source IP: Start

Setting	Description	Factory Default
IP address	Specify the starting IP address of the source IP range.	0.0.0.0

Source IP: End

Setting	Description	Factory Default
IP address	Specify the ending IP address of the source IP range.	0.0.0.0

Translated Packet (Action)

Outgoing Interface

Setting	Description	Factory Default
All LAN WAN	Select the outgoing interface for the NAT rule.	LAN

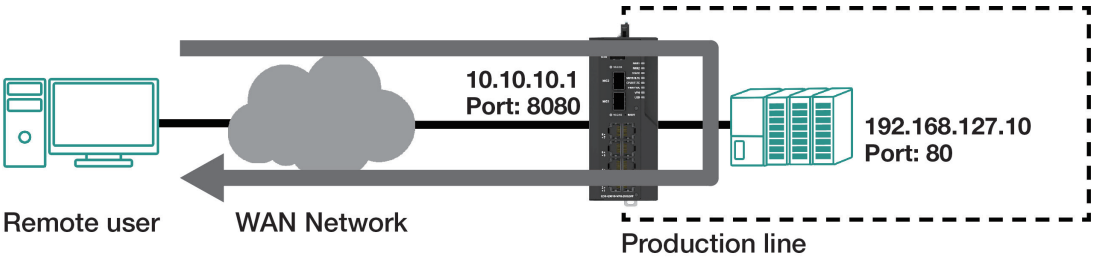
When finished, click **APPLY** to save your changes.

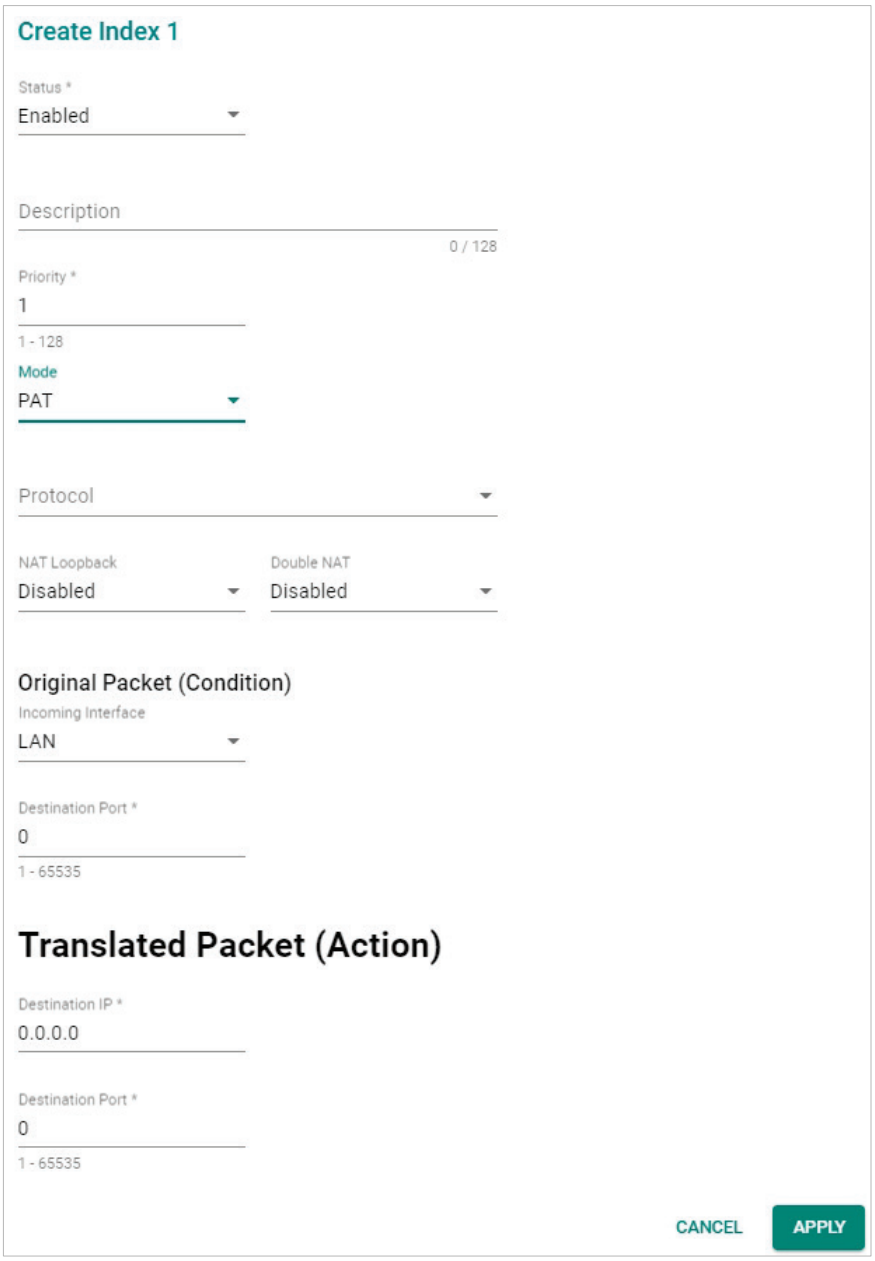
PAT (Port Address Translation)

If the initial connection is from outside the LAN, but the user still wants to hide the internal IP address, one way to do this is to use the PAT NAT function.

The user can specify the port number of an external IP address (WAN1 or WAN2) in the Port Forwarding policy list. For example, if the IP address of a web server in the internal network is 192.168.127.10 with port 80, the user can set up a Port Forwarding policy to let remote users connect to the internal web server from external IP address 10.10.10.10 through port 8080. The Industrial Secure Router will transfer the packet to IP address 192.168.127.10 through port 80.

The PAT NAT function is one way of connecting from an external non-secure area (WAN) to an internal secure area (LAN). The user can initiate the connection from the external network to the internal network, but not the other way around.





Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)
Enabled		1	PAT	TCP	WAN	Any:Any	Dynamic:8080	All	Any:Any	192.168.127.10:80

Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the NAT policy.	Enabled

Description

Setting	Description	Factory Default
Description	Enter a name for the NAT rule.	None

Priority

Setting	Description	Factory Default
1 to 128	Specify the index of the NAT rule.	1

NAT Mode

Setting	Description	Factory Default
1-to-1 N-to-1 PAT Advance	Select PAT as the NAT type. For other NAT modes, refer to: 1-to-1 N-to-1 Advance	1-to-1

Protocol

Setting	Description	Factory Default
ICMP TCP UDP	Select the NAT policy protocol.	None

NAT Loopback

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the NAT Loopback function. Refer to NAT Loopback for more information.	Disabled

Double NAT

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the Double NAT function. Refer to Double NAT for more information.	Disabled

Original Packet (Condition)

Incoming Interface

Setting	Description	Factory Default
All LAN WAN	Select the interface for the NAT policy.	LAN

Destination Port

Setting	Description	Factory Default
1 to 65535	Specify the destination port number.	0

Translated Packet (Action)

Destination IP

Setting	Description	Factory Default
IP Address	Specify the translated IP address on the internal network.	0.0.0.0

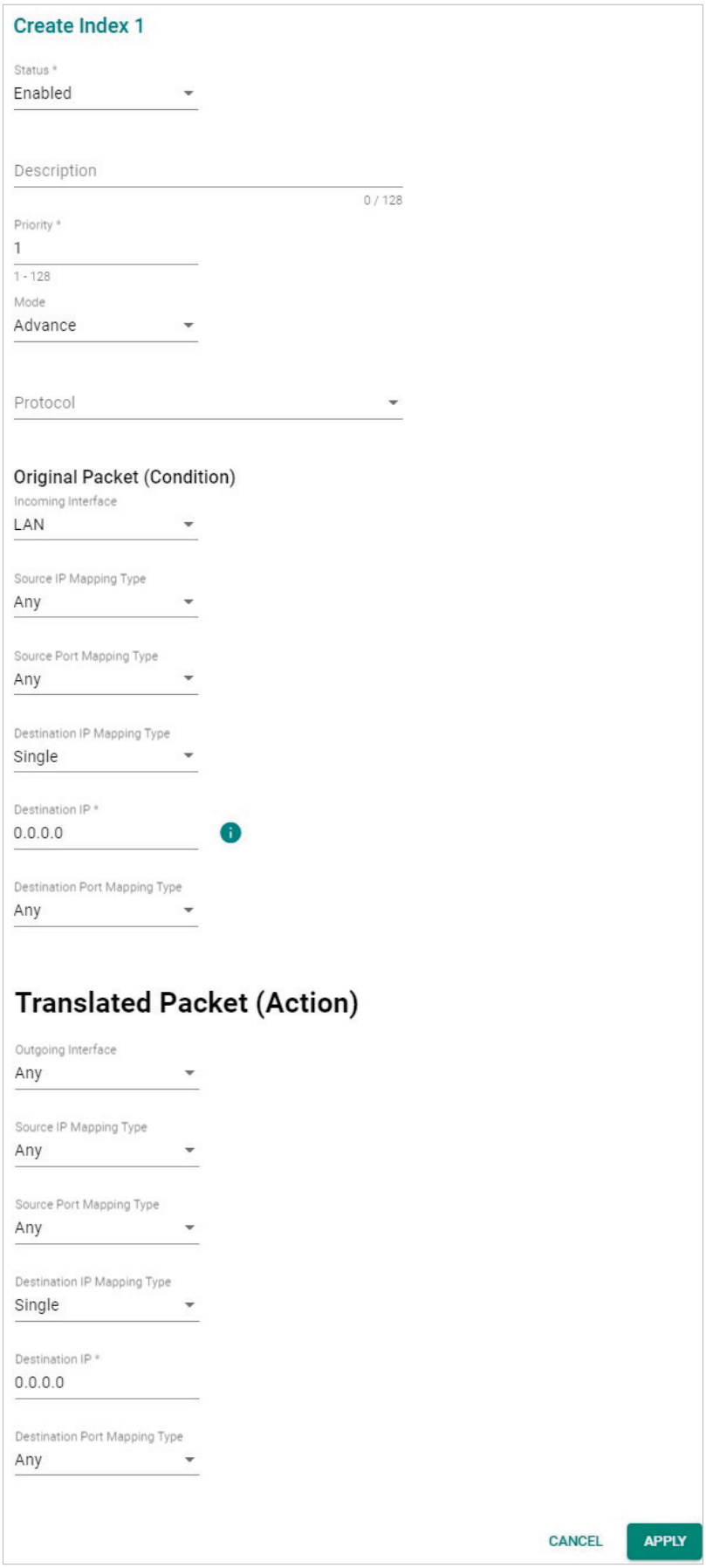
Destination Port

Setting	Description	Factory Default
1 to 65535	Specify the translated port number on the internal network.	0

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

Advance

The Advance NAT function opens up all available options to advanced users to customize their own settings.


Create Index 1
Status *
Enabled
Description
0 / 128
Priority *
1
1 - 128
Mode
Advance
Protocol
Original Packet (Condition)
Incoming Interface
LAN
Source IP Mapping Type
Any
Source Port Mapping Type
Any
Destination IP Mapping Type
Single
Destination IP *
0.0.0.0
Destination Port Mapping Type
Any
Translated Packet (Action)
Outgoing Interface
Any
Source IP Mapping Type
Any
Source Port Mapping Type
Any
Destination IP Mapping Type
Single
Destination IP *
0.0.0.0
Destination Port Mapping Type
Any
CANCEL
APPLY

Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the NAT policy.	Enabled

Description

Setting	Description	Factory Default
Description	Enter a name for the NAT rule.	None

Priority

Setting	Description	Factory Default
1 to 128	Specify the index of the NAT rule.	1

NAT Mode

Setting	Description	Factory Default
1-to-1 N-to-1 PAT Advance	Select Advance as the NAT type. For other NAT modes, refer to: 1-to-1 N-to-1 PAT	1-to-1

Protocol

Setting	Description	Factory Default
ICMP TCP UDP	Select the NAT policy protocol.	None

Original Packet (Condition)

Incoming Interface

Setting	Description	Factory Default
All LAN WAN	Select the interface for the NAT policy.	LAN

Source IP Mapping Type

Setting	Description	Factory Default
Any Single Range Subnet mask Dynamic	Select the source IP mapping type.	Any

Source Port Mapping Type

Setting	Description	Factory Default
Any Single Range	Select the source port mapping type.	Any

Destination IP Mapping Type

Setting	Description	Factory Default
Any Single Range Subnet mask	Select the destination IP mapping type.	Any

Destination IP

Setting	Description	Factory Default
IP Address	Specify the translated IP address on the internal network.	0.0.0.0

Destination Port Mapping Type

Setting	Description	Factory Default
Any Single Range	Select the destination port mapping type.	Single

Translated Packet (Action)

Outgoing Interface

Setting	Description	Factory Default
All LAN WAN	Select the interface for the NAT policy.	Any

Source IP Mapping Type

Setting	Description	Factory Default
Any Single Range Subnet mask Dynamic	Select the source IP mapping type.	Any

Source Port Mapping Type

Setting	Description	Factory Default
Any Single Range	Select the source port mapping type.	Any

Destination IP Mapping Type

Setting	Description	Factory Default
Any Single Range Subnet mask	Select the destination IP mapping type.	Single

Destination IP

Setting	Description	Factory Default
IP Address	Specify the translated IP address on the internal network.	0.0.0.0

Destination Port Mapping Type

Setting	Description	Factory Default
Any Single Range	Select the destination port mapping type.	Single

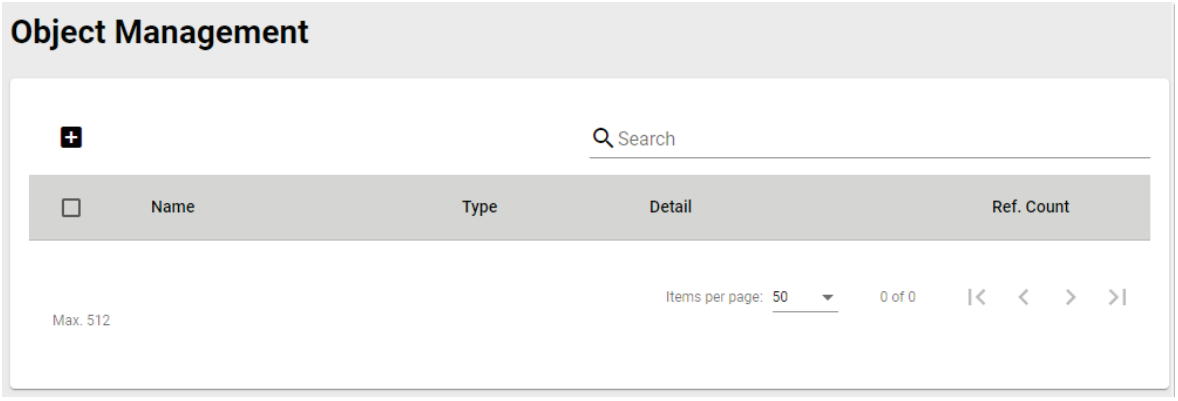
When finished, click **APPLY** to save your changes.

10. Object Management

Overview

The EDR-G9010 Industrial Secure Routers support object-based firewall management to help protect your network on a granular level. From the Object Management screen, you can create, modify, and edit the objects you need based on your security requirements. These objects are used in firewall policies that can be configured on the Firewall function page.

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, saving users time having to update individual policies one by one.



NOTE

The EDR-G9010 supports a maximum of 512 objects.

Create a New Object

The EDR-G9010 Series supports several types of objects, depending on the security requirements for your network.

On the **Object Management** page, click the ⊞ icon to create a new object.

Name

Setting	Description	Factory Default
0 to 32 characters	Enter a name for the object.	None

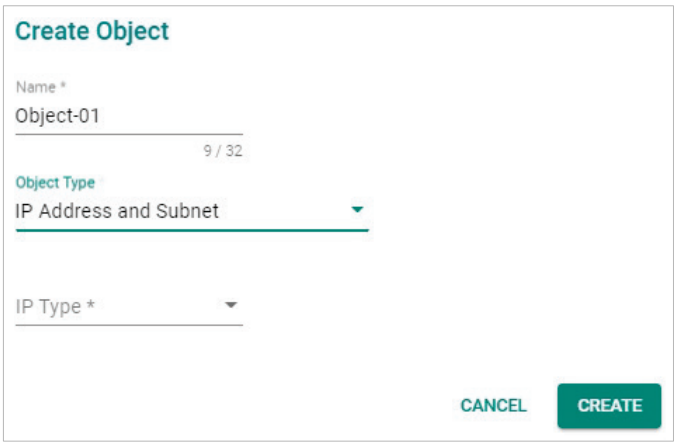
Object Type

Setting	Description	Factory Default
IP Address and Subnet, Network Service, Industrial Application Service, User-Defined Service	Select the type of object. Refer to the following sections for more information about each object type: • Create an IP Address and Subnet Object • Create a Network Service Object • Create an Industrial Application Service Object • Create a User-defined Service Object	None

Create an IP Address and Subnet Object

IP address/subnet-based objects allow traffic filtering for a single IP, an IP range, or a subnet.

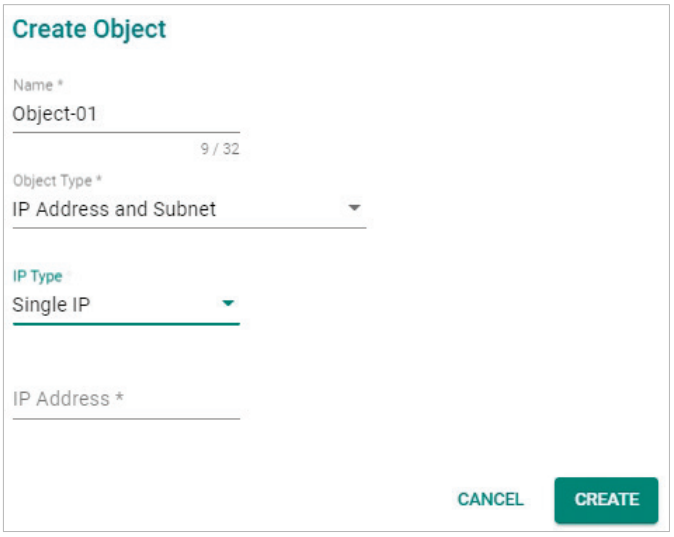
On the **Object Management** page, click the ⊞ icon to create a new object and select **IP Address and Subnet** as the Object Type.



IP Type

Setting	Description	Factory Default
Single IP, IP Range, Subnet	Select the IP type. Refer to the following sections for more information about each option.	None

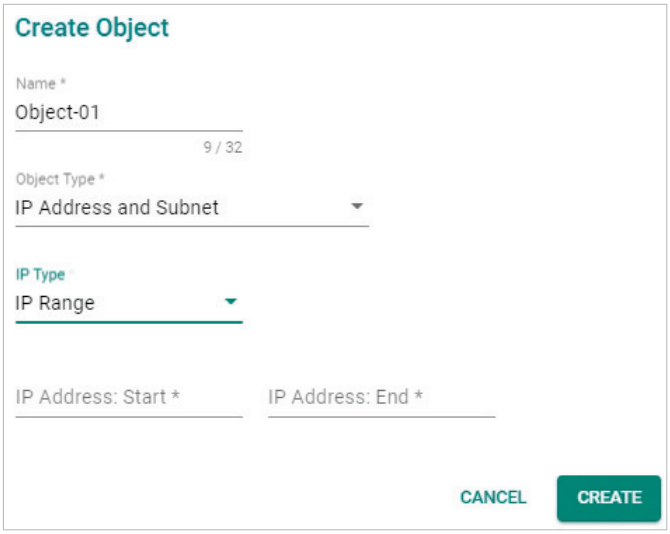
Single IP



IP Address

Setting	Description	Factory Default
IP address	Enter a valid IP address.	None

IP Range



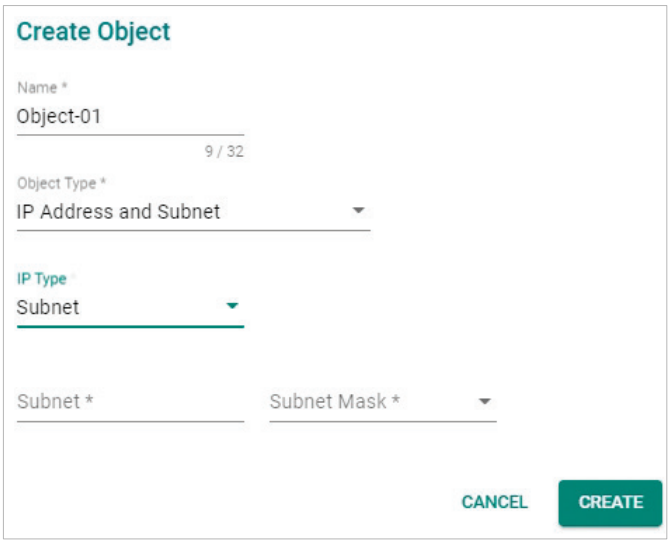
IP Address: Start

Setting	Description	Factory Default
IP address	Specify the starting IP address of the IP range.	None

IP Address: End

Setting	Description	Factory Default
IP address	Specify the ending IP address of the IP range.	None

Subnet



Subnet

Setting	Description	Factory Default
IP address	Specify the subnet IP address.	None

Subnet Mask

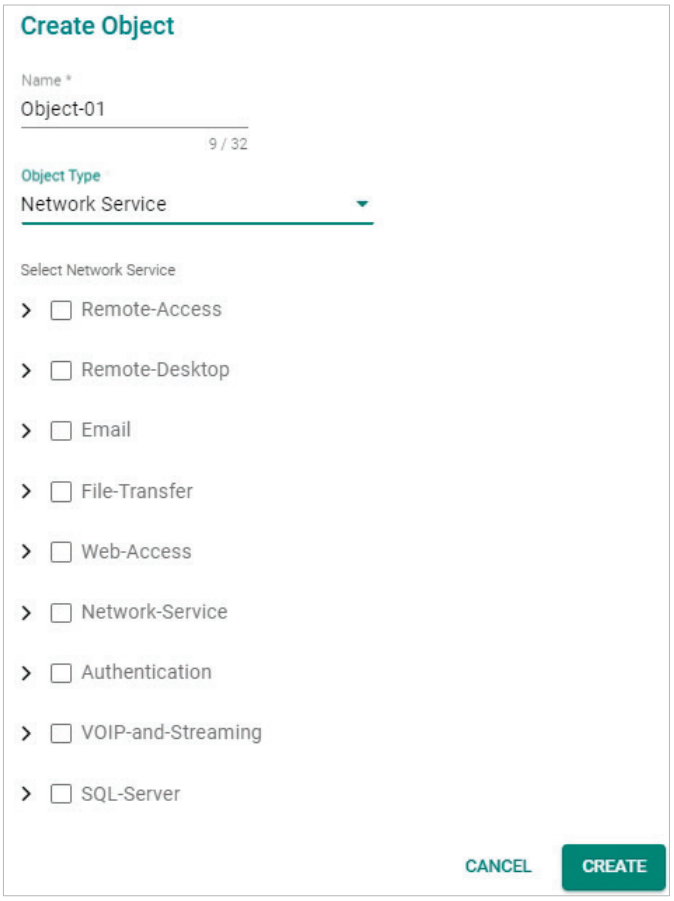
Setting	Description	Factory Default
IP address	Select the subnet mask for this IP address.	None

When finished, click **CREATE** to create the object.

Create a Network Service Object

Service-based objects allow for traffic filtering based on specific network services.

On the **Object Management** page, click the ⊞ icon to create a new object and select **Network Service** as the Object Type.



Select Network Service

Select the network service(s) you want to enable. Refer to the table below for more details about each service.

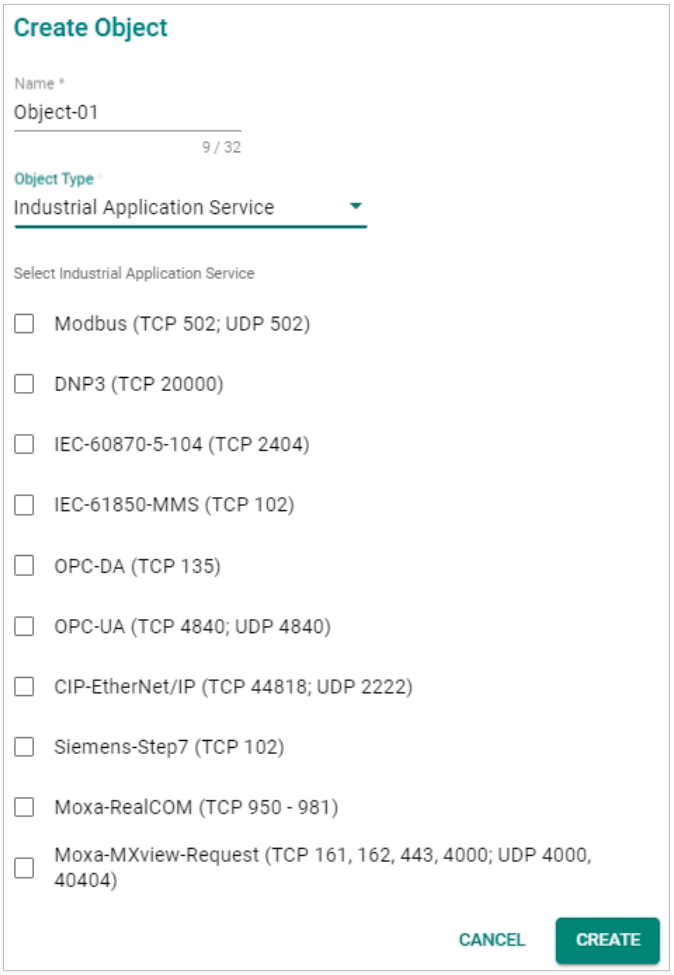
Service Name	Protocol (Port Number)
Remote-Access	WINS (TPC 1512; UDP 1512)
	TELNET (TCP 23)
	SSH (TCP 22)
Remote-Desktop	PC-Anywhere (TCP 5631; UDP 5632)
	Chrome-Remote-Desktop (UDP 5222)
	AnyDesk (TCP 6568, 7070; UDP 50001 - 50003)
	Teamviewer (TCP 5938)
	RDP (TCP 3389)
	VNC (TCP 5900)
	X-WINDOW (TCP 6000 - 6063)
Email	IMAP (TCP 143)
	IMAPS (TCP 993)
	POP3 (TCP 110)
	POP3S (TCP 995)
	SMTP (TCP 25)
	SMTPS (TCP 465)
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)
Web-Access	HTTP (TCP 80)
	HTTPS (TCP 443)
Network-Service	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)
Authentication	LDAP (TCP 389; UDP 389)
	LDAPS (TCP 636; UDP 636)
	RADIUS (UDP 1812 – 1813)
	TACACS+ (TCP 49; UDP 49)
VOIP-and-Streaming	SIP (TCP 5060; UDP 5060)
	RSTP (TCP 554, 7070, 8554; UDP 554)
SQL-Server	MS-SQL (TCP 1433 - 1434)
	MYSQL (TCP 3306)

When finished, click **CREATE** to create the object.

Create an Industrial Application Service Object

Industrial application service-based objects allow for traffic filtering based on specific industrial application protocols.

On the **Object Management** page, click the ⊞ icon to create a new object and select **Industrial Application Service** as the Object Type.



Select Industrial Application Service

Select the industrial application service(s) you want to enable. Refer to the table below for more details about each service.

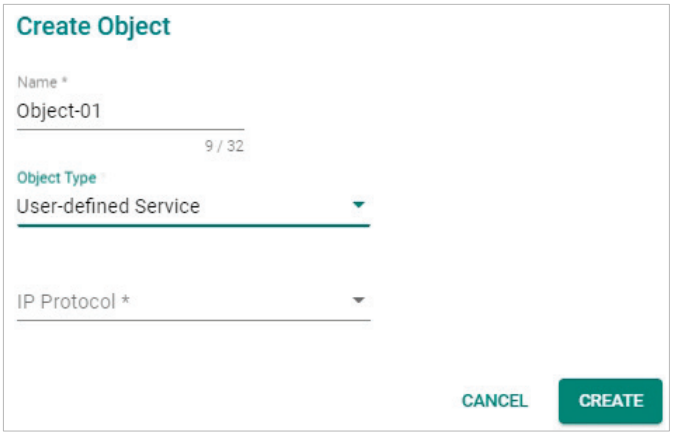
Service Name	Port Number
Modbus	TCP 502; UDP 502
DNP3	TCP 20000
IEC-60870-5-104	TCP 2404
IEC-61850-MMS	TCP 102
OPC-DA	TCP 135
OPC-UA	TCP 4840; UDP 4840
CIP-EtherNet/IP	TCP 44818; UDP 2222
Siemens-Step7	TCP 102
Moxa-RealCOM	TCP 950 – 981
Moxa-MXview-Request	TCP 161, 162, 443, 4000; UDP 4000, 40404

When finished, click **CREATE** to create the object.

Create a User-defined Service Object

User-defined service-based objects allow for traffic filtering based on user-defined communication protocols.

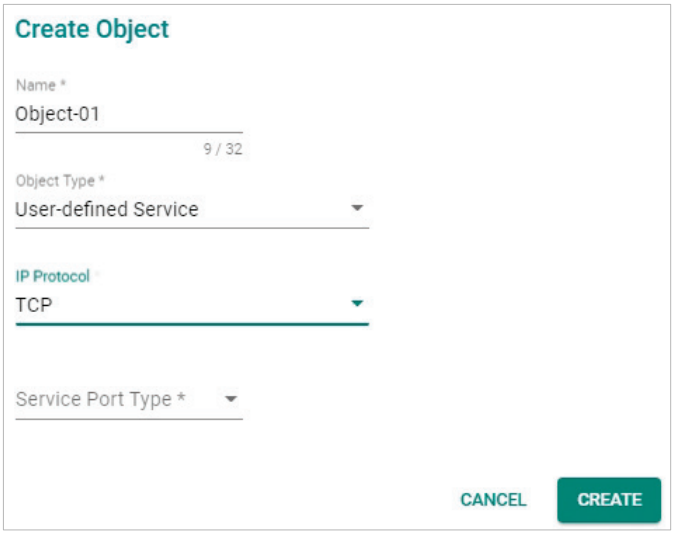
On the **Object Management** page, click the ⊞ icon to create a new object and select **User-defined Service** as the Object Type.



IP Protocol

Setting	Description	Factory Default
TCP, UDP, TCP and UDP, ICMP, Custom IP Protocol	Select a protocol. Refer to the following sections for more information about each option.	None

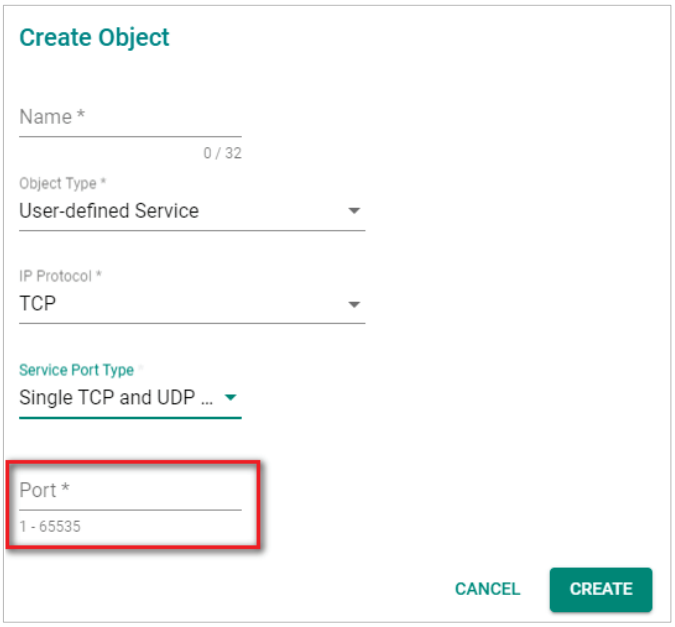
TCP, UDP, TCP and UDP



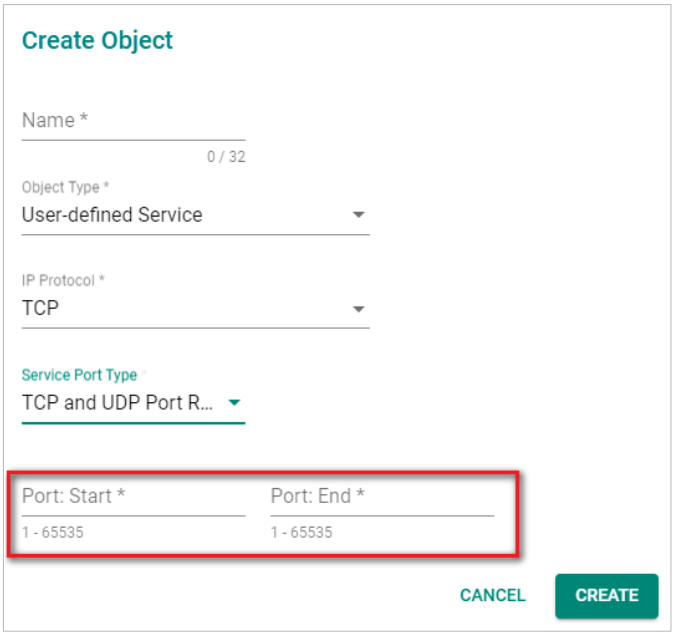
Service Port Type

Setting	Description	Factory Default
Any, Single TCP and UDP Port, TCP and UDP Port Range	Select a port type for the protocol.	None

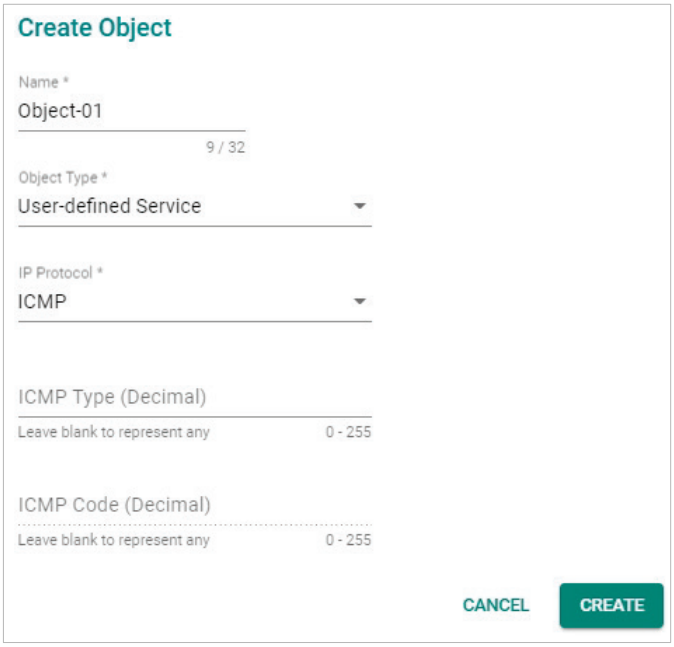
If you selected **Single TCP and UDP Port** as the port type, you also need to specify a port number. The port number range is between 1 to 65535.



If you selected **TCP and UDP Port Range** as the port type, you also need to specify the starting and ending port number. The port number range is between 1 to 65535.



ICMP



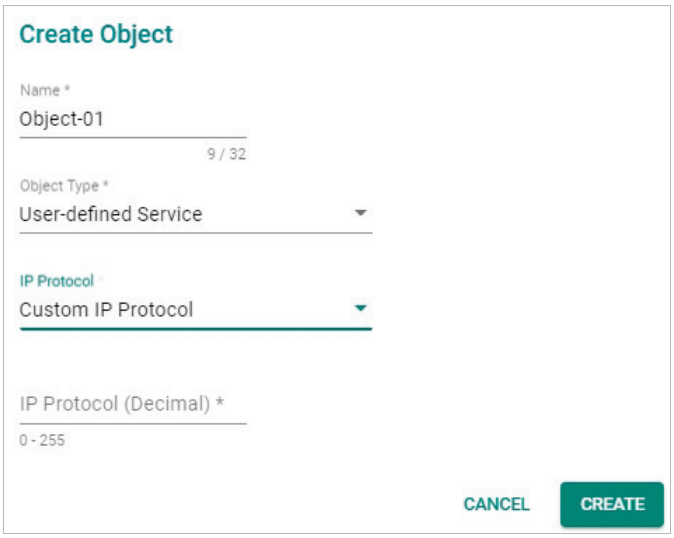
ICMP Type (Decimal)

Setting	Description	Factory Default
Blank, 0 to 255	Specify the ICMP type value.	None

ICMP Code (Decimal)

Setting	Description	Factory Default
Blank, 0 to 255	Specify the ICMP code value.	None

Custom IP protocol



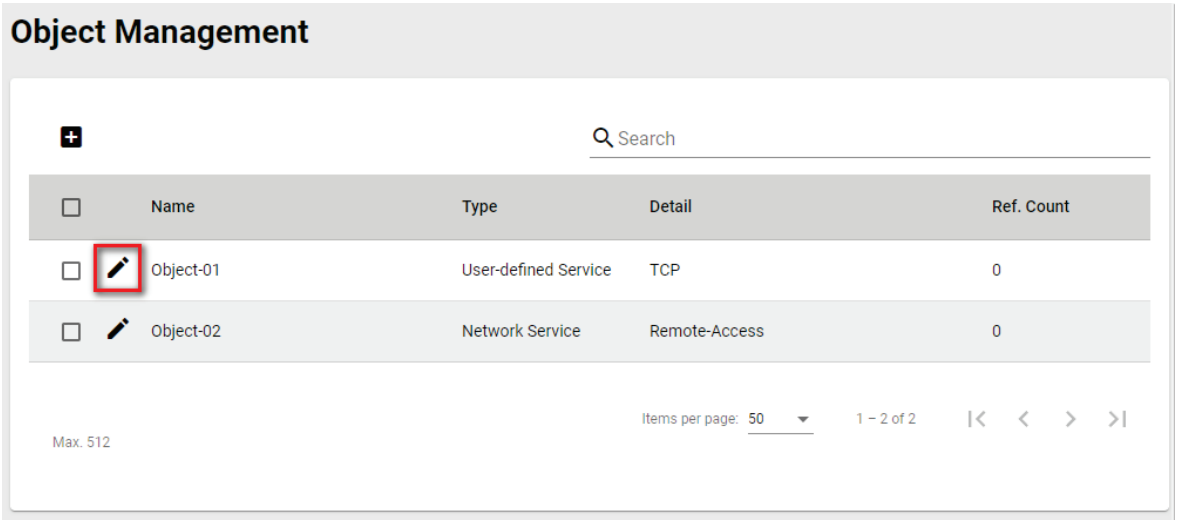
IP Protocol (Decimal)

Setting	Description	Factory Default
0 to 255	Specify the IP protocol value.	None

When finished, click **CREATE** to create the object.

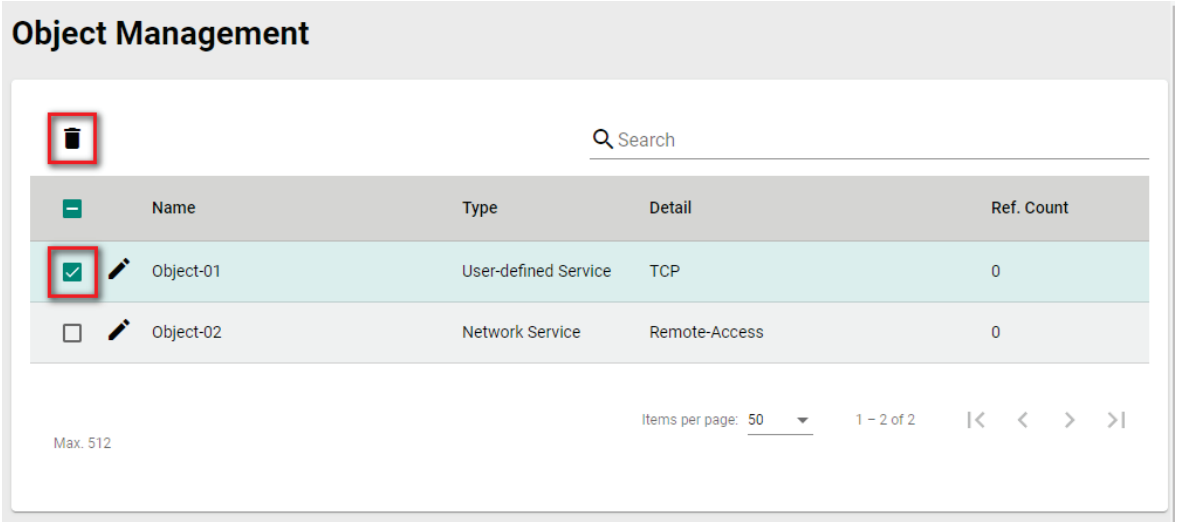
Modify an Existing Object

In the object list, click the **Edit** (✎) icon next to entry you want to modify. When finished, click **APPLY** to save your changes.



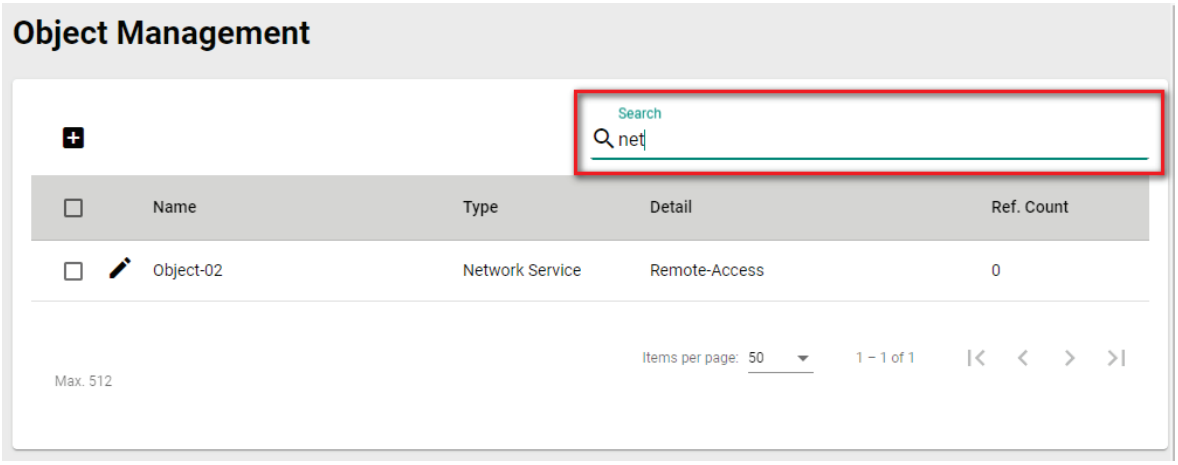
Delete an Object

Select the item(s) in the object list, click the **Delete** (🗑) icon. When prompted to confirm, click **DELETE** to delete the object(s).



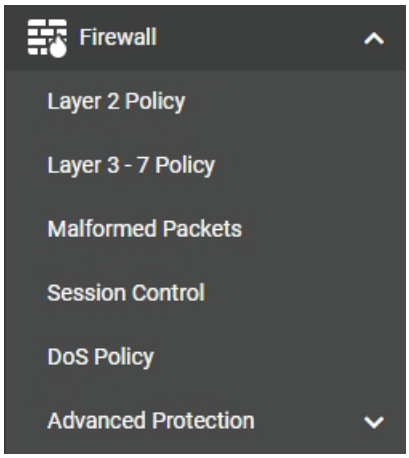
Search for an Object

Enter a search term in the Search field. Any object matching the search criteria will be shown in the object list.



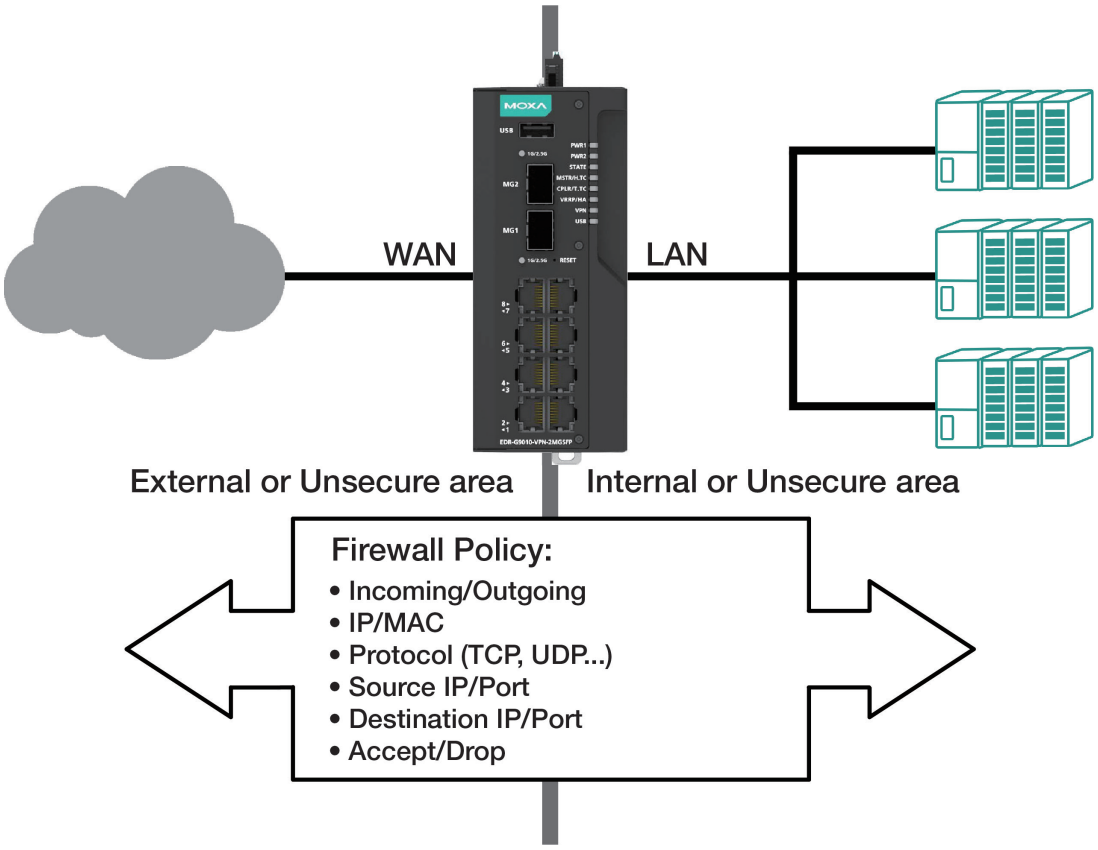
11. Firewall

From the **Firewall** section you can configure the **Layer 2 Policy**, **Layer 3 – 7 Policy**, **Malformed Packets**, **Session Control**, **DoS Policy**, and **Advanced Protection** settings.



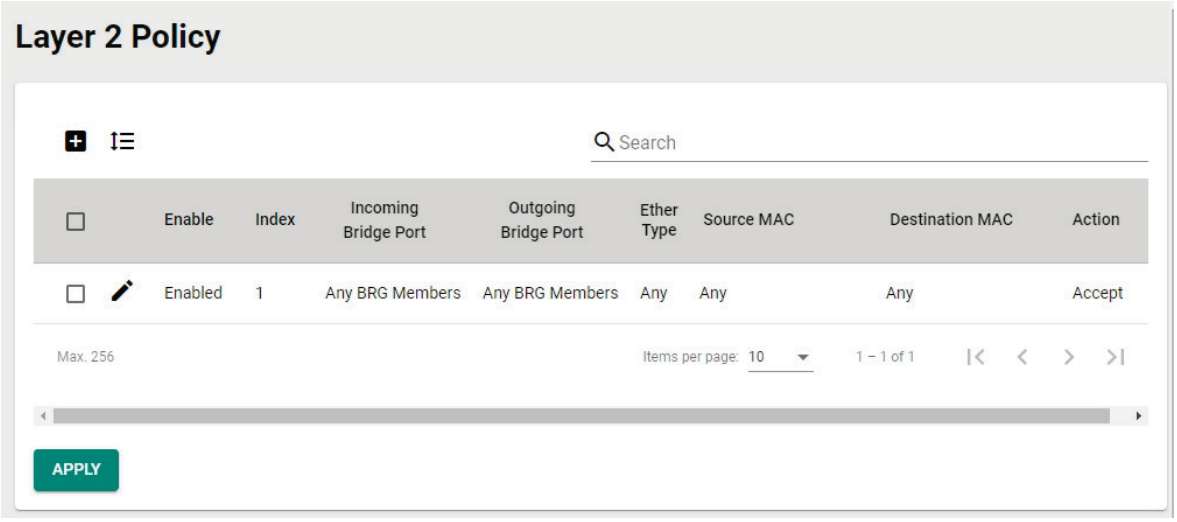
Policy Concept

A firewall device is commonly used to provide secure traffic control over an Ethernet network, as illustrated in the following figure. Firewall devices are deployed at critical points between an external network (non-secure) and an internal network (secure).



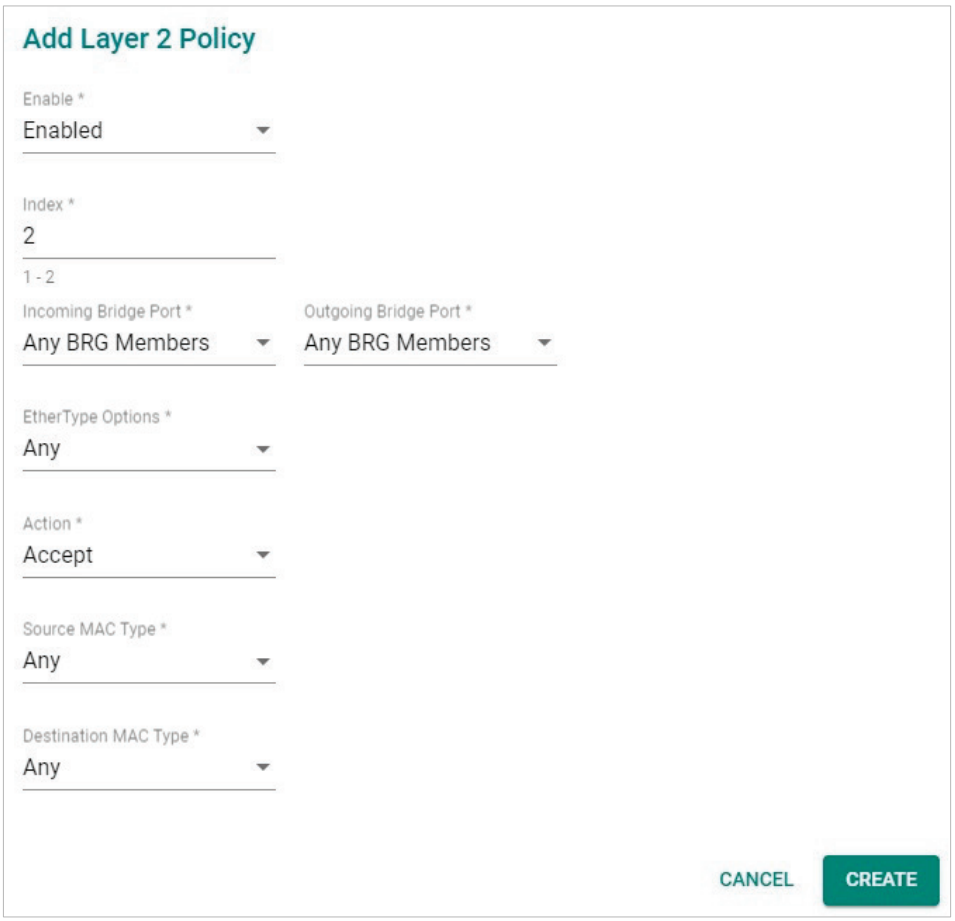
Layer 2 Policy

The EDR-G9010 supports advanced Layer 2 firewall policies for secure traffic control. Layer 2 firewall policies can filter packets from bridge ports and have a higher priority than L3 policies.



Create a New Layer 2 Policy

Click the ⊞ icon to create a new Layer 2 Policy.



Enable

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the Layer 2 policy.	Enabled

Index

Setting	Description	Factory Default
Max. 256	The index number is generated automatically.	1

Incoming/Outgoing Bridge Port

Setting	Description	Factory Default
Any BRG Members	Select the Incoming and Outgoing bridge port.	Any BRG Members

EtherType Options

Setting	Description	Factory Default
Any, Manual	Select the Layer 2 protocol for this policy. If set to "Manual", you can specify the EtherType. Refer to EtherType for Layer 2 Protocol for a list of all types.	Any

Action

Setting	Description	Factory Default
Accept	The Firewall will accept the packet if it matches the policy.	Accept
Drop	The Firewall will drop the packet if it matches the policy.	

Source MAC Type

Setting	Description	Factory Default
Any	The Firewall will check all source MAC addresses of the packet.	Any
Single	The Firewall will only check the specified source MAC address of the packet.	00:00:00:00:00:00

Destination MAC Type

Setting	Description	Factory Default
Any	The Firewall will check all destination MAC addresses of the packet.	Any
Single	The Firewall will only check the specified destination MAC address of the packet.	00:00:00:00:00:00

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

Modify an Existing Layer 2 Policy

Click the icon of the entry you want to modify. When finished, click APPLY to save your changes.

Delete an Existing Layer 2 Policy

Select the item(s) in the Layer 2 policy list, click the icon and click DELETE to delete the item(s).

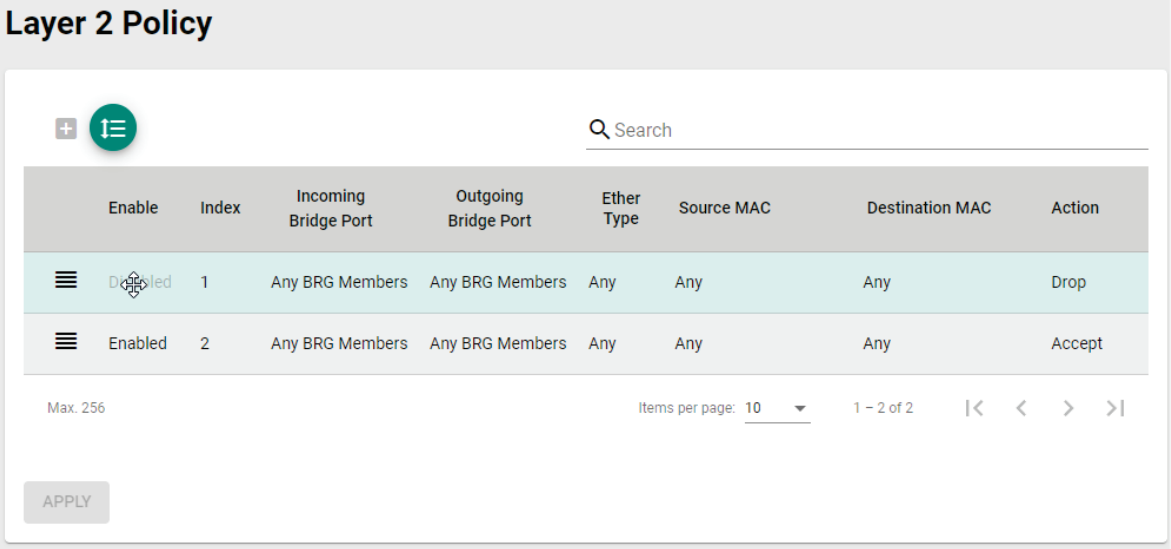
Search for a Existing Layer 2 Policy

Enter the words you want to search in the **Search** field. Anything matching the search criteria will be shown in the Layer 2 Policy list.

Reorder Layer 2 Policies

If necessary, the priority of Layer 2 policies can be changed by reordering policies. the priority of Layer 2 policy.

1. Click the icon.
2. Move the cursor to the policy you want to reorder. The cursor will change to .
3. Click and drag the policy into the desired position and release.
4. When finished reordering the policies, click the icon.



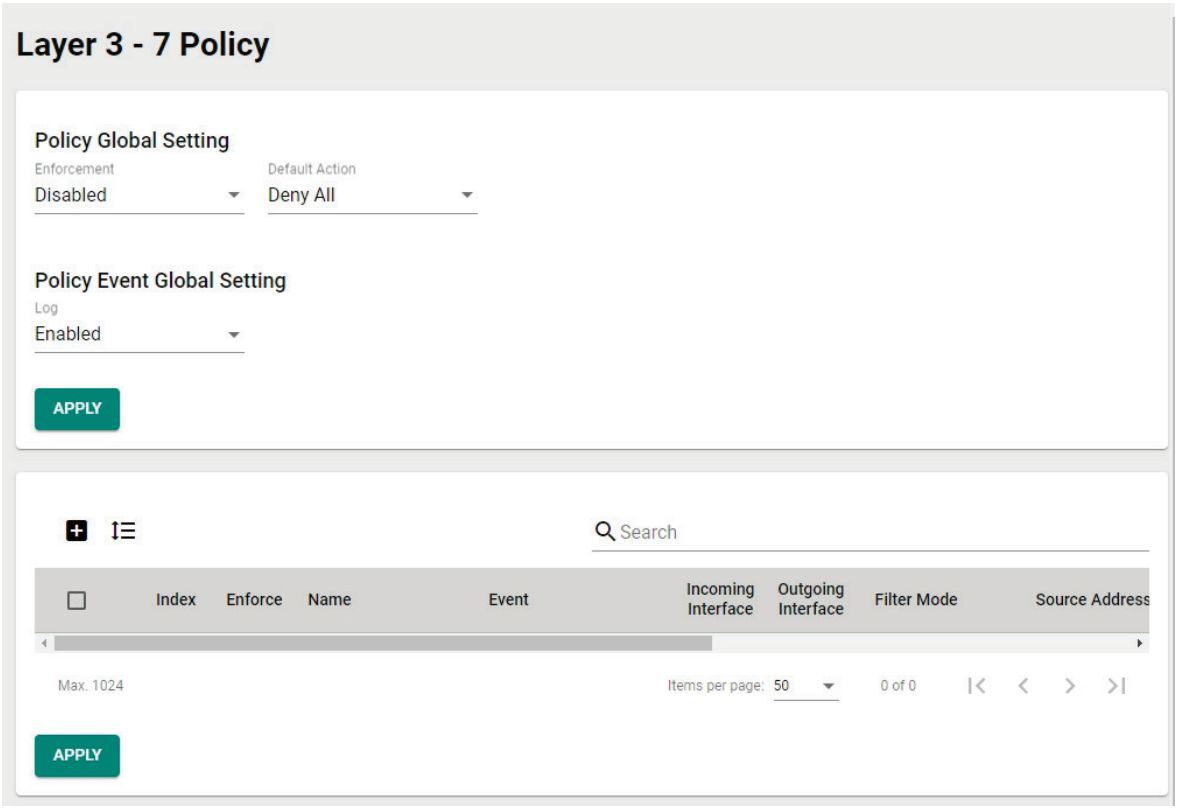
EtherType for Layer 2 Protocol

The following table shows the Layer 2 protocol types commonly used in Ethernet frames.

Type	Layer 2 Protocol
0x0800	IPv4 (Internet Protocol version 4)
0x0805	X25
0x0806	ARP (Address Resolution Protocol)
0x0808	Frame Relay ARP
0x08FF	G8BPQ AX.25 Ethernet Packet
0x6000	DEC Assigned proto
0x6001	DEC DNA Dump/Load
0x6002	DEC DNA Remote Console
0x6003	DEC DNA Routing
0x6004	DEC LAT
0x6005	DEC Diagnostics
0x6006	DEC Customer use
0x6007	DEC Systems Comms Arch
0x6558	Trans Ether Bridging
0x6559	Raw Frame Relay
0x80F3	Appletalk AARP
0x809B	Appletalk
0x8100	8021Q VLAN tagged frame
0x8137	Novell IPX
0x8191	NetBEUI
0x86DD	IP version 6 (Internet Protocol version 6)
0x880B	PPP
0x884C	MultiProtocol over ATM
0x8863	PPPoE discovery messages
0x8864	PPPoE session messages
0x8884	Frame-based ATM Transport over Ethernet
0x9000	Loopback

Layer 3 - 7 Policy

The Industrial Secure Router's Firewall policy provides secure traffic control, allowing users to control network traffic.



Policy Global Setting

The Policy Global Setting section lets users enable and configure the default action if the traffic doesn't match any of the configured rules on the router.

Enforcement

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the global Policy Enforcement feature.	Disabled

Default Action

Setting	Description	Factory Default
Allow All	Allow all network traffic that does not match any rule.	Deny All
Deny All	Block all network traffic that does not match any rule.	

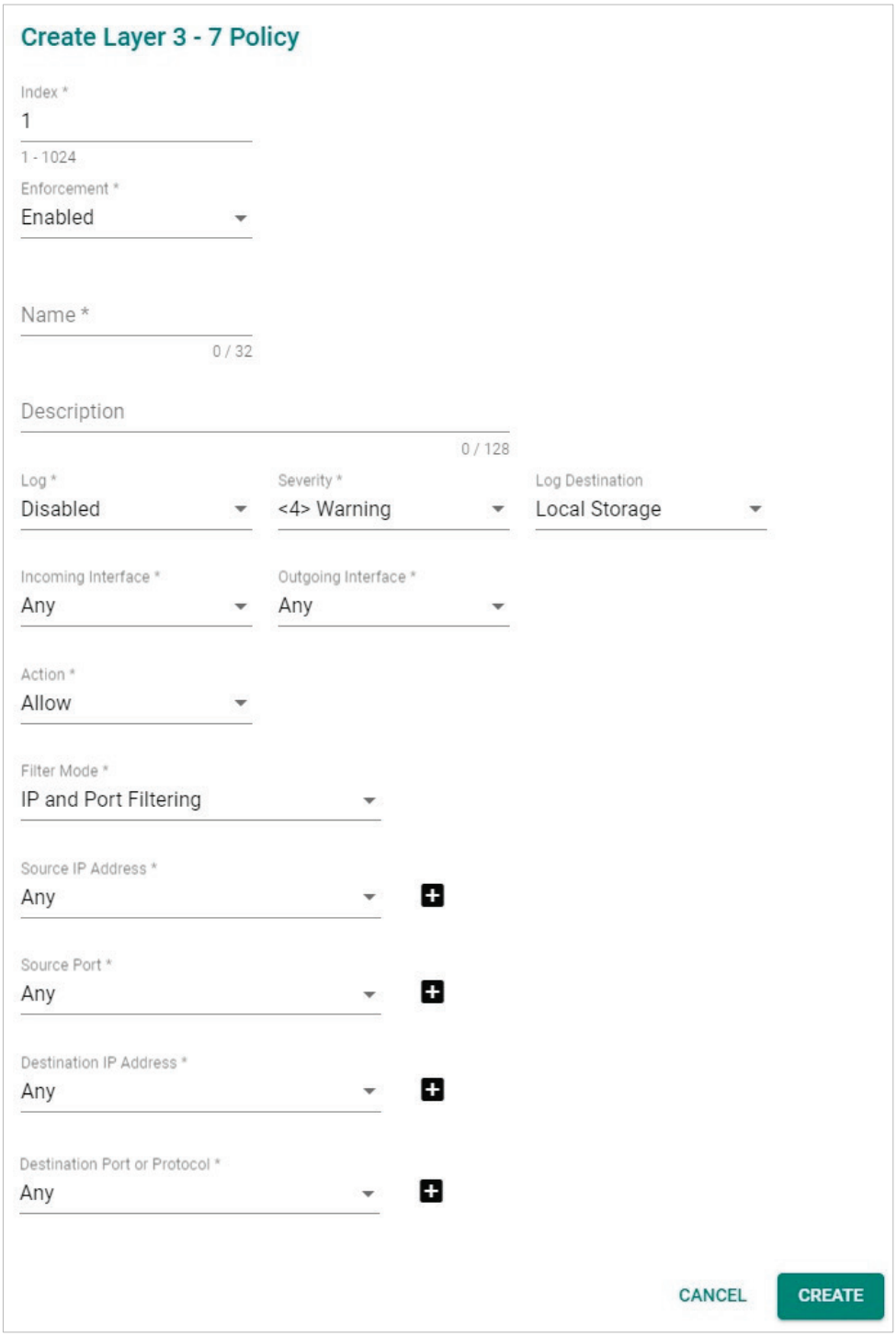
Policy Event Global Setting

Log

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable global policy event logs.	Disabled

Create a New Layer 3 - 7 Policy

Click ⊞ to create a new Layer 3 – 7 policy.



Index

Setting	Description	Factory Default
Max. 1024	The index number is generated automatically.	1

Enforcement

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the Policy Enforcement feature.	Enabled

Name

Setting	Description	Factory Default
Custom string (0 to 32 characters)	Enter a name for the firewall rule.	None

Description

Setting	Description	Factory Default
Custom string (0 to 128 characters)	Enter the description for the firewall rule.	None

Log

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the firewall event logging.	Disabled

Severity

Setting	Description	Factory Default
<0> Emergency <1> Alert <2> Critical <3> Error <4> Warning <5> Notice <6> Informational <7> Debug	Select the severity of firewall events.	<4> Warning

Log Destination

Setting	Description	Factory Default
Local Storage	The firewall event logs are stored on the local storage and will show in the Event Log table.	Local Storage
Syslog	The firewall event logs are sent to a Syslog server.	
Trap	The firewall event logs are sent to a SNMP Trap.	

Incoming Interface

Setting	Description	Factory Default
Any, WAN, LAN	Select the incoming interface.	Any

Outgoing Interface

Setting	Description	Factory Default
Any, WAN, LAN	Select the outgoing interface.	Any

Action

Setting	Description	Factory Default
Allow	Allow network traffic that matches this rule.	Allow
Deny	Block network traffic that matches this rule.	

Filter Mode

Setting	Description	Factory Default
IP and Port Filtering	The firewall policy will filter based on IP address and port.	IP and Port Filtering
IP and Source MAC Binding	The firewall policy will filter based on IP address and check the source MAC address in the packet.	
Source MAC Filtering	The firewall policy will filter based on source MAC address.	

Source MAC Address

Setting	Description	Factory Default
MAC Address	If the Filter Mode is set to "IP and Source MAC Binding" or "Source MAC Filtering", specify the source MAC address. The firewall policy will check the source MAC address in the packet.	None

Source IP Address

Setting	Description	Factory Default
Any	Select Any to have the firewall policy check any source IP addresses in the packet or pre-defined objects, or click the ⊞ icon to Create an IP Address and Subnet Object.	Any

Source Port

Setting	Description	Factory Default
Any	Select Any to have the firewall policy check any source port numbers in the packet or pre-defined objects, or click the ⊞ icon to Create a User-defined Service Object.	Any

Destination IP Address

Setting	Description	Factory Default
Any	Select Any to have the firewall policy check any destination IP addresses in the packet or pre-defined objects, or click the ⊞ icon Create an IP Address and Subnet Object.	Any

Destination Port

Setting	Description	Factory Default
Any	Select Any to have the firewall policy check any destination port numbers in the packet or pre-defined objects, or click the ⊞ icon to Create an IP Address and Subnet Object. Refer to Destination Port for Layer 3 – 7 Protocol for a list of all destination ports.	Any

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

NOTE

The Industrial Secure Router's firewall function will check if incoming or outgoing packets match the firewall policy. It starts by checking the packet with the first policy (Index=1); if the packet matches this policy, it will accept the packet immediately and then check the next packet. If the packet does not match this policy it will check against the next policy.

NOTE

The maximum number of Firewall policies for the EDR-G9010 is 1024.

Modify an Existing Layer 3 – 7 Policy

Click the ✎ icon next to the entry you want to modify. When finished, click **APPLY** to save your changes.

Delete an Existing Layer 3 – 7 Policy

Select the item(s) in the Layer 3 – 7 policy list, click the 🗑 icon and click **DELETE** to delete the item(s).

Search for an Existing Layer 3 – 7 Policy

Enter the words you want to search in the **Search** field. Any matching the search criteria will be shown in the Layer 3 – 7 policy list table.

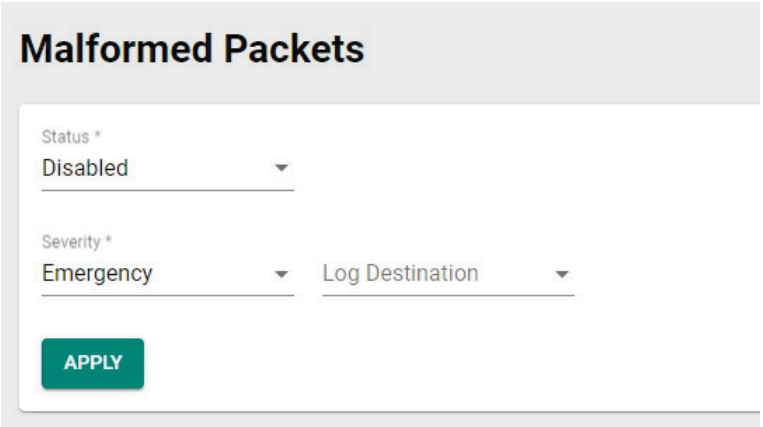
Reorder Existing Layer 3 – 7 Policy

If necessary, the priority of Layer 3 – 7 policies can be modified by reordering rules. Refer to the instructions in the Reorder Layer 2 Policies section.

Destination Port for Layer 3 – 7 Protocol

Network Service	Industrial Application Service
Remote-Access	Modbus
Remote-Desktop	DNP3
Email	IEC-60870-5-104
File-Transfer	IEC-61850-MMS
Web-Access	OPC-DA
Network-Service	OPC-UA
Authentication	CIP-EtherNet/IP
VOIP-and-Streaming	Siemens-Step7
SQL-Server	Moxa-RealCOM
Authentication	moxa-MXview-Request

Malformed Packets



Enable Malformed Packets

The Malformed Packets function enables the device to record event logs with a user-specified severity whenever malformed packets are dropped by the system.

Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the system to record event logs when malformed packets are dropped.	Disabled

Severity

Severity	Description	Factory Default
Emergency	System is unusable	Emergency
Alert	Action must be taken immediately	
Critical	Critical conditions	
Error	Error conditions	
Warning	Warning conditions	
Notice	Normal but significant condition	
Info	Informational messages	
Debug	Debug-level messages	

Log Destination

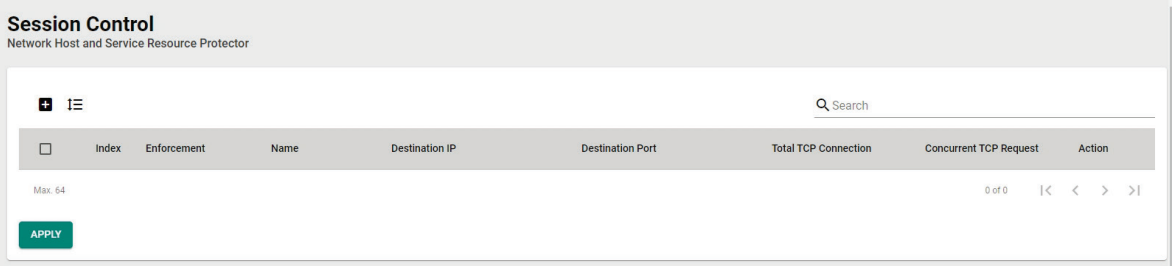
Setting	Description	Factory Default
Local Storage	The malformed packets event logs are stored in the local storage and will show in the Event Log table.	None
Syslog	The malformed packets event logs are sent to a Syslog server.	
Trap	The malformed packets event logs are sent by SNMP Trap.	

Session Control

EDR-G9010 supports session control to help users protect backend hosts or services and avoid system abnormalities.

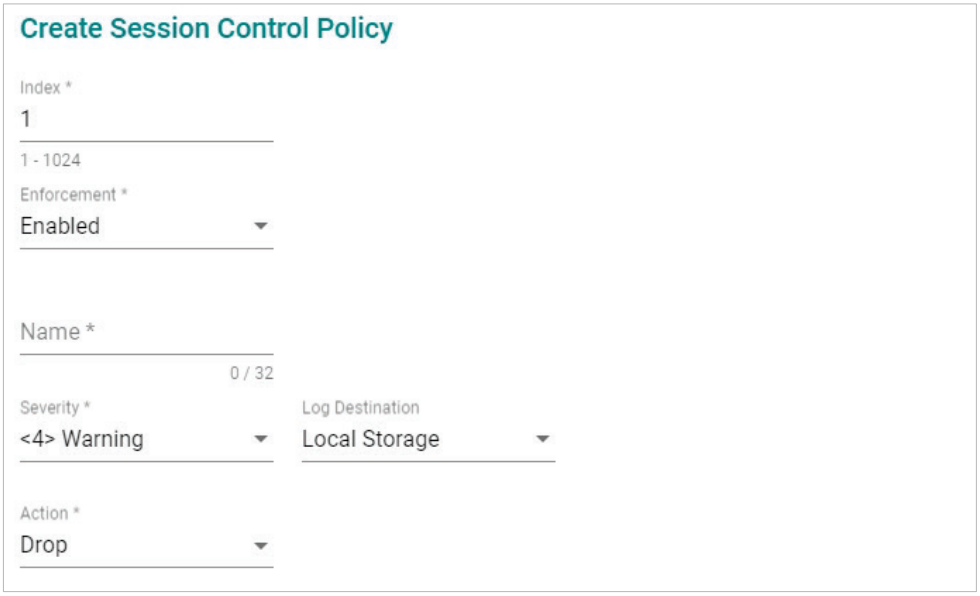
NOTE

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 on the connection exceeds 300 seconds, the connection will also be released.



Create a New Session Control Policy

Click ⊞ to create a new Session Control policy.



Index

Setting	Description	Factory Default
Max. 1024	The index number is generated automatically.	1

Enforcement

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the control policy rule.	Enabled

Name

Setting	Description	Factory Default
0 to 32 characters	Enter a name for this policy.	None

Severity

Setting	Description	Factory Default
<0> Emergency <1> Alert <2> Critical <3> Error <4> Warning <5> Notice <6> Informational <7> Debug	Select the severity of the session control event.	<4> Warning

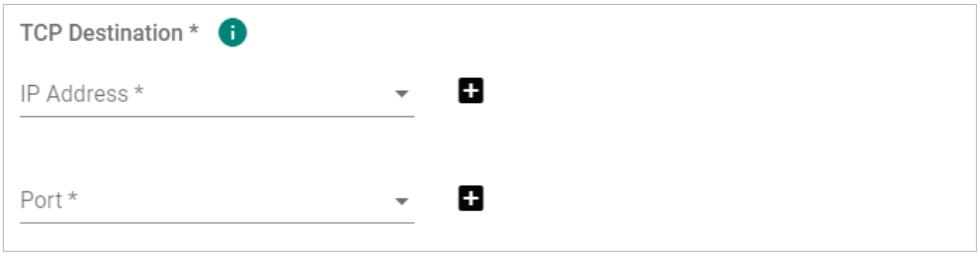
Log Destination

Setting	Description	Factory Default
Local Storage	The session control event logs will be stored in the local storage and will show in the Event Log table.	Local Storage
Syslog	The session control event logs will be sent to a Syslog server.	
Trap	The session control event logs will be sent by SNMP Trap.	

Action

Setting	Description	Factory Default
Monitor	Monitor the network traffic that matches this rule.	Drop
Drop	Drop the network traffic that matches this rule.	

TCP Destination



NOTE

IP Address and Port cannot both be Any.

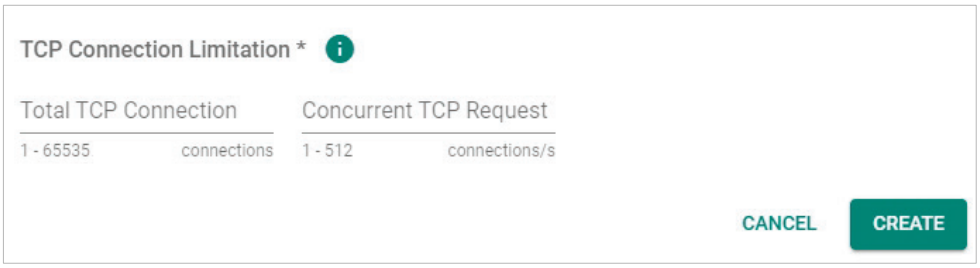
IP Address

Setting	Description	Factory Default
Any	Select Any to have the session control policy check any IP addresses in the packet or pre-defined objects, or click the + icon to Create an IP Address and Subnet Object.	None

Port

Setting	Description	Factory Default
Any	Select Any to have the session control policy check any port numbers in the packet or pre-defined objects, or click the + icon to Create a User-defined Service Object.	None

TCP Connection Limitation



NOTE

At least one limitation is required.

Total TCP Connection

Setting	Description	Factory Default
1 to 65535	Specify the total allowed number of TCP connections.	None

Concurrent TCP Request

Setting	Description	Factory Default
1 to 512	Specify the total allowed number of concurrent TCP requests.	None

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

NOTE

The maximum number of session control policies is 64.

Modify an Existing Session Control Policy

Click the icon next to the entry you want to modify. When finished, click **APPLY** to save your changes.

Delete an Existing Session Control Policy

Select the item(s) in the Session Control policy list, click the icon and click **DELETE** to delete the item(s).

Search for an Existing Session Control Policy

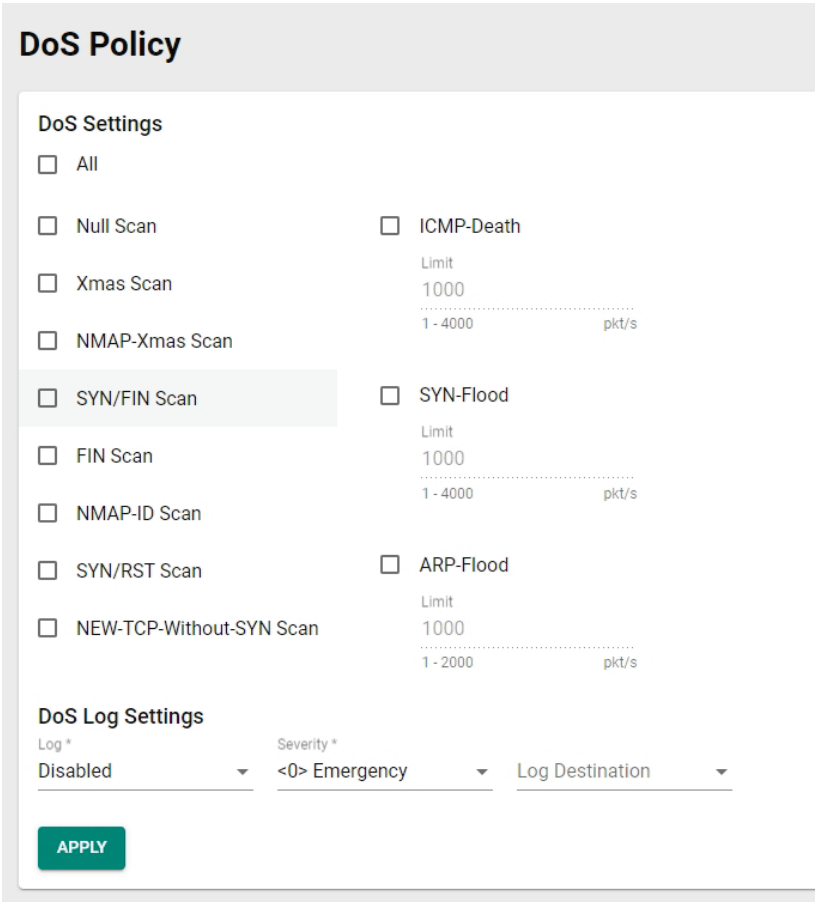
Enter the search term in the **Search** field. Anything matching the search criteria will be shown in the Session Control policy list table.

Reorder Session Control Policies

If necessary, the priority of Session Control policies can be modified by reordering rules. Refer to the instructions in the Reorder Layer 2 Policies section.

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.



DoS Settings

All

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable the DoS policy for all types.	Unchecked

Null Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable Null Scan.	Unchecked

Xmas Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable Xmas Scan.	Unchecked

NMAP-Xmas Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable NMAP-Xmas Scan.	Unchecked

SYN/FIN Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable SYN/FIN Scan.	Unchecked

FIN Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable FIN Scan.	Unchecked

NMAP-ID Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable NMAP-ID Scan.	Unchecked

SYN/RST Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable SYN/RST Scan.	Unchecked

NEW-TCP-Without-SYN Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable NEW-TCP-Without-SYN Scan.	Unchecked

ICMP-Death

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable the ICMP-Death protection.	Unchecked
Limit (1 to 4000 Packets/Second)	If enabled, specify the limit that will trigger ICMP-Death protection.	1000

SYN-Flood

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable SYN-Flood protection.	Unchecked
Limit (1 to 4000 Packets/Second)	If enabled, specify the limit that will trigger SYN-Flood protection.	1000

ARP-Flood

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable ARP-Flood protection	Unchecked
Limit (1 to 2000 Packets/Second)	If enabled, specify the limit that will trigger ARP-Flood protection.	1000

DoS Log Settings

Log

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable DoS event logs.	Disabled

Severity

Setting	Description	Factory Default
<0> Emergency <1> Alert <2> Critical <3> Error <4> Warning <5> Notice <6> Informational <7> Debug	Select the severity of DoS events.	<0> Emergency

Log Destination

Setting	Description	Factory Default
Local Storage	The DoS event logs are stored in the local storage and will show in the Event Log table.	Disabled
Syslog	The DoS event logs are sent to a Syslog server.	
Trap	The DoS event logs are sent by SNMP Trap.	

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

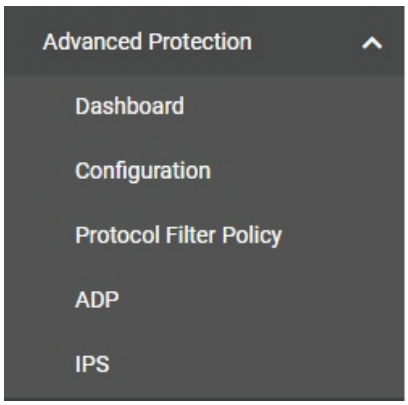
Advanced Protection

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.

NOTE

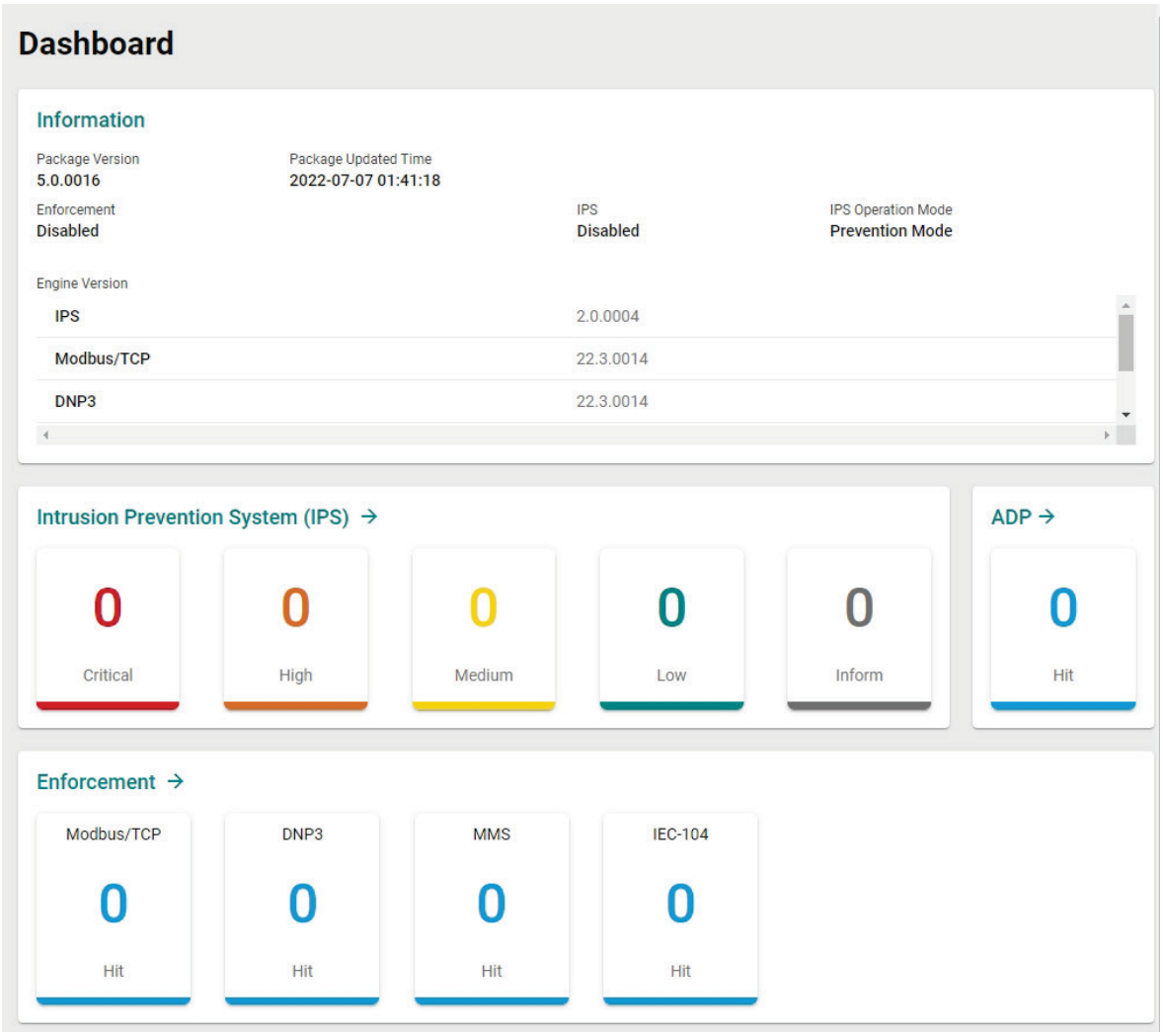
The application firewall requires a security package to be installed. Refer to Software Package Management for more information and instructions.

From the **Advanced Protection** section, the following functions can be configured: **Dashboard, Configuration, Protocol Filter Policy, ADP,** and **IPS**.



Dashboard

The application firewall's dashboard provides an overview with package information and real-time event counters. Click **Refresh** to renew the information on the dashboard.



Information

This section shows the version of the firewall engines and the security package currently installed on the Industrial Secure Router.

Intrusion Prevention System (IPS)

This section shows the current number of intrusion prevention system (IPS) events.

ADP (Anomaly Detection & Protection)

This section shows the current number of anomaly detection & prevention (ADP) events.

Enforcement

This section shows the current number of Modbus/TCP, DNP3, MMS, and IEC-104 industrial protocol events.

Click the → icon in each section to see all event logs or click any of the cards to view event logs for that specific type.

Configuration

From the Configuration section, you can modify settings for the application firewall including global settings, protocol filtering objects and profiles, and firewall policy settings.

Global Settings

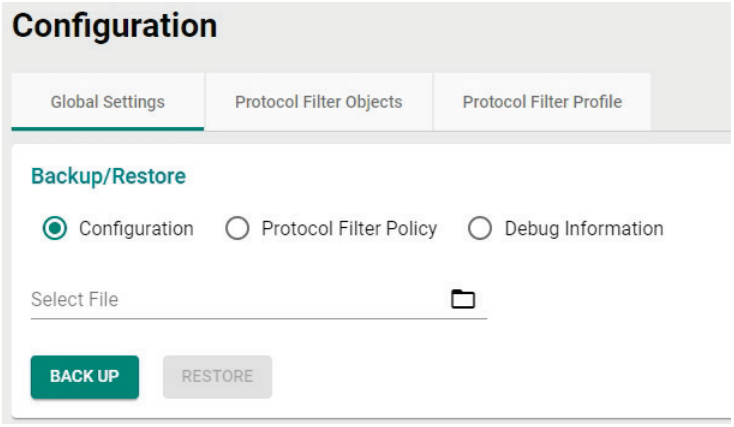
Backup/Restore

Configuration

On the Global Settings tab, select **Configuration** in the **Backup/Restore** section.

Click **BACK UP** to export the Industrial Secure Router's configuration settings as a file to the local host.

To restore the device's configuration using a backup file, click the 🗀 icon and navigate to the configuration backup file on the local host and click **RESTORE**.

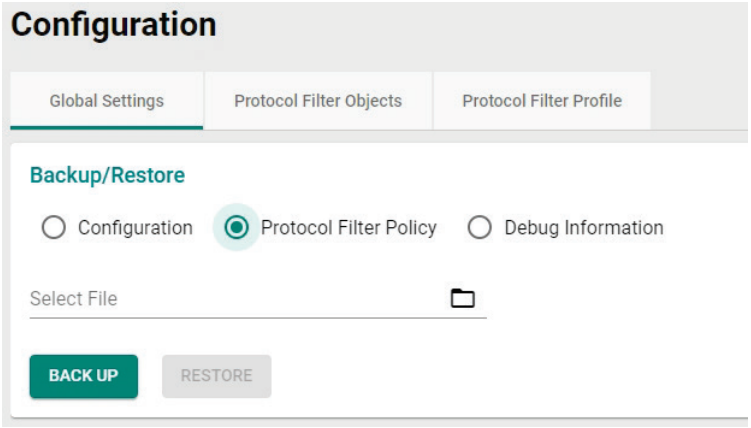


Protocol Filter Policy

On the Global Settings tab, select **Protocol Filter Policy** in the **Backup/Restore** section.

Click **BACK UP** to export the Industrial Secure Router's protocol filter policy settings as a file to the local host.

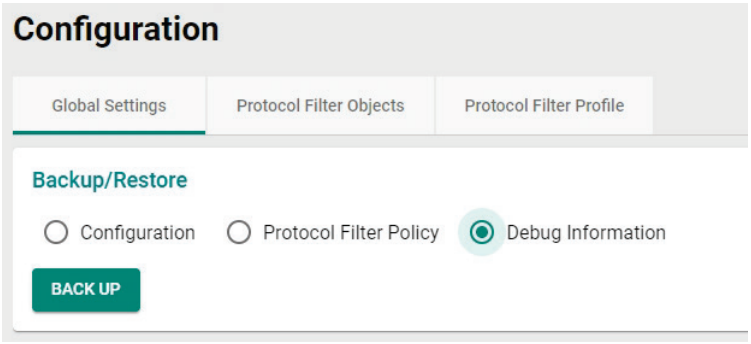
To restore the device's policy settings using a backup file, click the 🗀 icon and navigate to the policy backup file on the local host and click **RESTORE**.



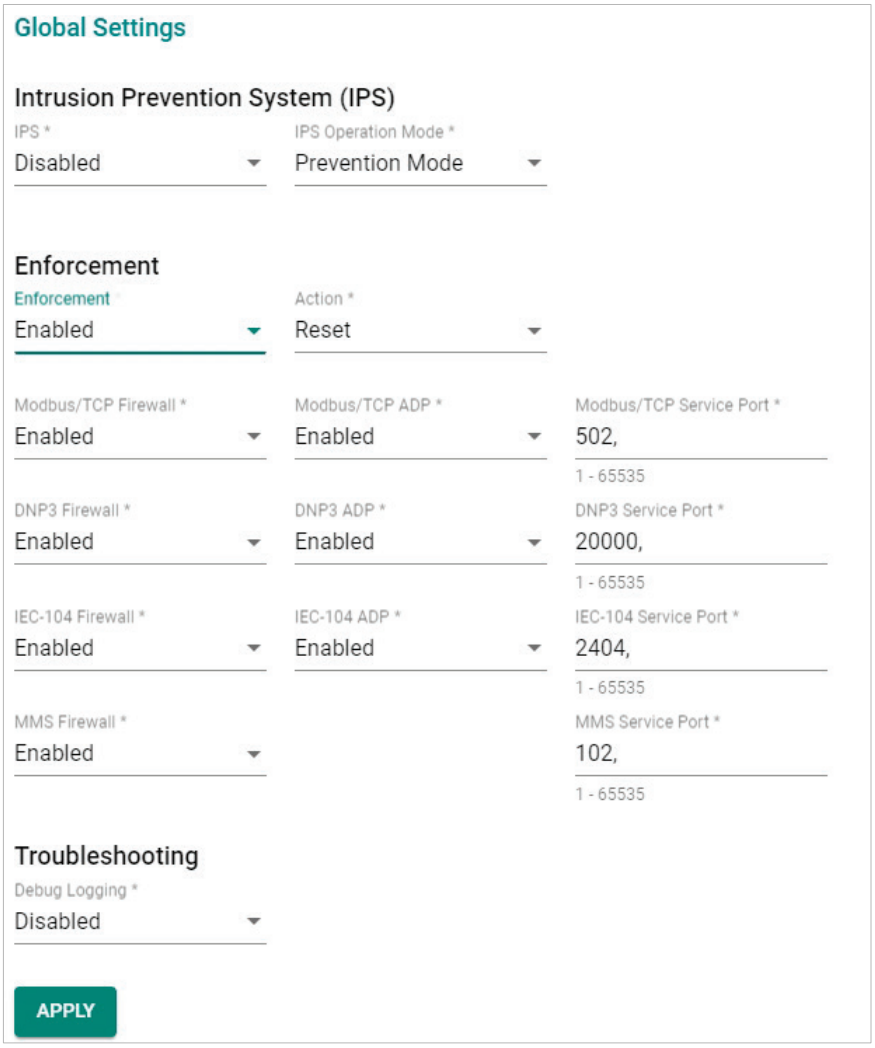
Debug Information

On the Global Settings tab, select **Debug Information** in the **Backup/Restore** section.

Click **BACK UP** to export the Industrial Secure Router's debug information as a file to the local host.



Global Settings



Intrusion Prevention System (IPS)

IPS

Setting	Description	Factory Default
Enables or Disabled	Enable or disable intrusion prevention system (IPS) functionality.	Disabled

IPS Operation Mode

Setting	Description	Factory Default
Prevention Mode, Detection Mode	Select the IPS operation mode.	Prevention Mode

Enforcement

Enforcement

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the default global rule.	Disabled

Action

Setting	Description	Factory Default
Accept, Monitor, Reset	Select the default action of the protocol filter.	Reset

Modbus/TCP Firewall

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the Modbus/TCP protocol filter engine.	Enabled

Modbus/TCP ADP

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the Modbus/TCP protocol filter engine and corresponding ADP function.	Enabled

Modbus/TCP Service Port

Setting	Description	Factory Default
1 to 65535	If Modbus/TCP Firewall is enabled, specify the service port for Modbus/TCP traffic.	502

DNP3 Firewall

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the DNP3 protocol filter engine.	Enabled

DNP3 ADP

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the DNP3 protocol filter engine and corresponding ADP function.	Enabled

DNP3 Service Port

Setting	Description	Factory Default
1 to 65535	If DNP3 Firewall is enabled, specify the service port for DNP3 traffic.	20000

IEC-104 Firewall

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the IEC-104 protocol filter engine.	Enabled

IEC-104 ADP

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the IEC-104 protocol filter engine and corresponding ADP function.	Enabled

IEC-104 Service Port

Setting	Description	Factory Default
1 to 65535	If IEC-104 Firewall is enabled, specify the service port for IEC-104 traffic.	102

MMS Firewall

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the MMS protocol filter engine.	Enabled

MMS Service Port

Setting	Description	Factory Default
1 to 65535	If MMS Firewall is enabled, specify the service port for MMS traffic.	2404

Troubleshooting

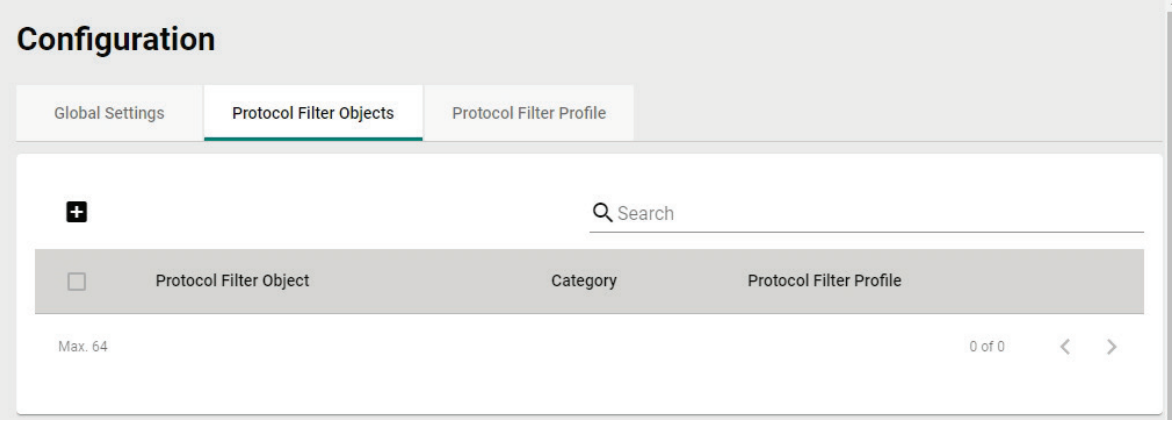
Debug Logging

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable debug logging. If enabled, the system will create debug logs for troubleshooting.	Disabled

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

Protocol Filter Objects

The application firewall's protocol filter uses objects to configure firewall policies. Objects simplify rule composition and maintenance.



Create a New Protocol Filter Object

On the **Protocol Filter Objects** tab, click the ⊞ icon to create a new filter object. The configuration settings depend on the selected Category.

Refer to the following sections for more details on each category:
Create a Modbus/TCP Object
Create a DNP3 Object
Create an IEC-104 Object
Create a MMS Object

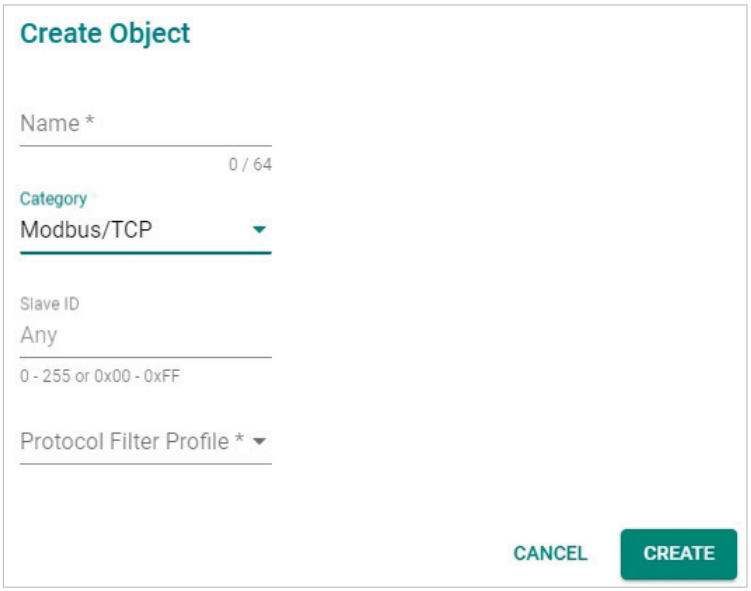
Modify an Existing Protocol Filter Object

Select the item in the Protocol Filter Object Table and click the ✎ icon next to the entry you want to modify. When finished, click **APPLY** to save your changes.

Delete an Existing Protocol Filter Object

Select the item(s) in the Protocol Filter Object Table. Click the 🗑 icon and click **DELETE** to delete the protocol filter object(s).

Create a Modbus/TCP Object



Name

Setting	Description	Factory Default
0 to 64 characters	Enter a name for the protocol filter object.	None

Category

Setting	Description	Factory Default
Modbus/TCP	Select the Modbus/TCP protocol.	None

Slave ID

Setting	Description	Factory Default
0 to 255, 0x00 to 0xFF)	Specify the slave ID. Leave this field blank to represent any ID.	Any

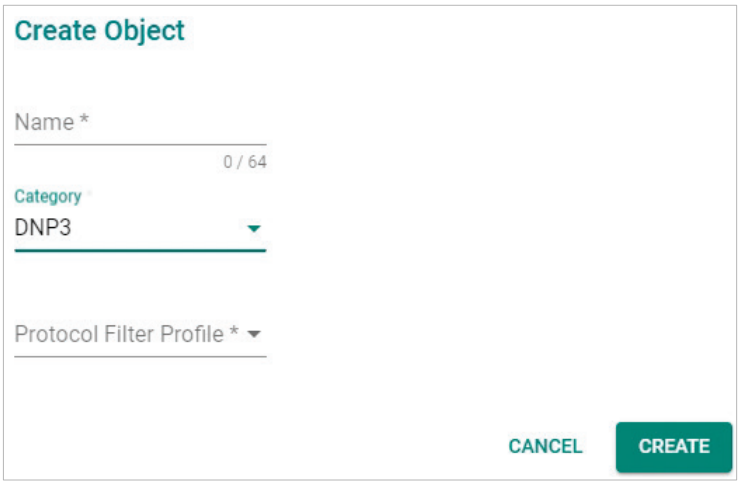
The Slave ID is used to identify Modbus devices. This ID can be used to communicate via devices such as bridges and gateways which use a single IP address to support multiple independent end units.

Protocol Filter Profile

Setting	Description	Factory Default
Read Only, Write Only, Read/Write, Manual	Select a preset or user-configured protocol filter profile for this protocol filter object. Refer to Protocol Filter Profile for more information about user-configured profiles. Select Manual to manually configure the profile parameters.	None

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

Create a DNP3 Object



Name

Setting	Description	Factory Default
0 to 64 characters	Enter a name for the protocol filter object.	None

Category

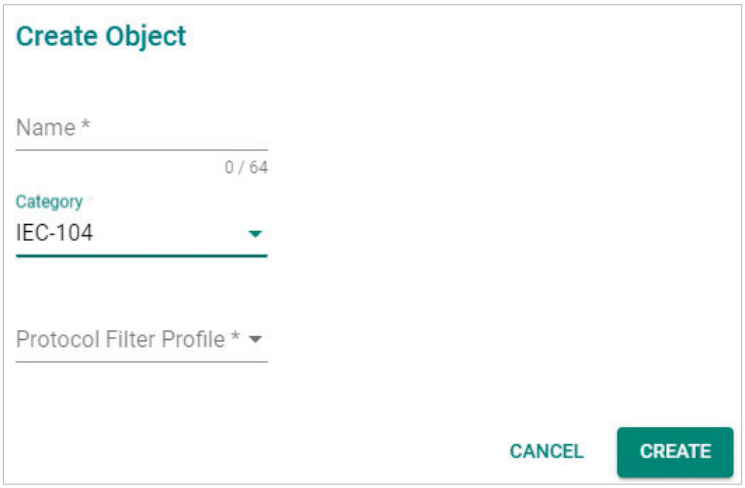
Setting	Description	Factory Default
DNP3	Select the DNP3 protocol.	None

Protocol Filter Profile

Setting	Description	Factory Default
Manual	Select a preset or user-configured protocol filter profile for this protocol filter object. Refer to Protocol Filter Profile for more information about user-configured profiles. Select Manual to manually configure the profile parameters.	None

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

Create an IEC-104 Object



Name

Setting	Description	Factory Default
0 to 64 characters	Enter a name for the protocol filter object.	None

Category

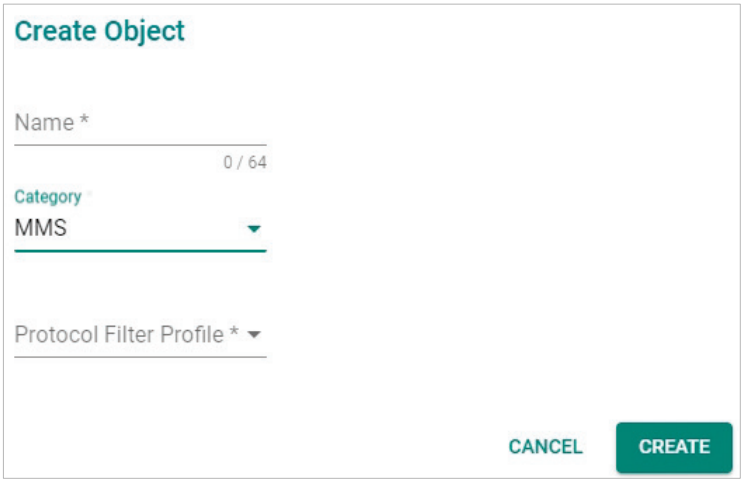
Setting	Description	Factory Default
IEC-104	Select the IEC-104 protocol.	None

Protocol Filter Profile

Setting	Description	Factory Default
Manual	Select a preset or user-configured protocol filter profile for this protocol filter object. Refer to Protocol Filter Profile for more information about user-configured profiles. Select Manual to manually configure the profile parameters.	None

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

Create a MMS Object



Name

Setting	Description	Factory Default
0 to 64 characters	Enter a name for the protocol filter object.	None

Category

Setting	Description	Factory Default
MMS	Select the MMS protocol.	None

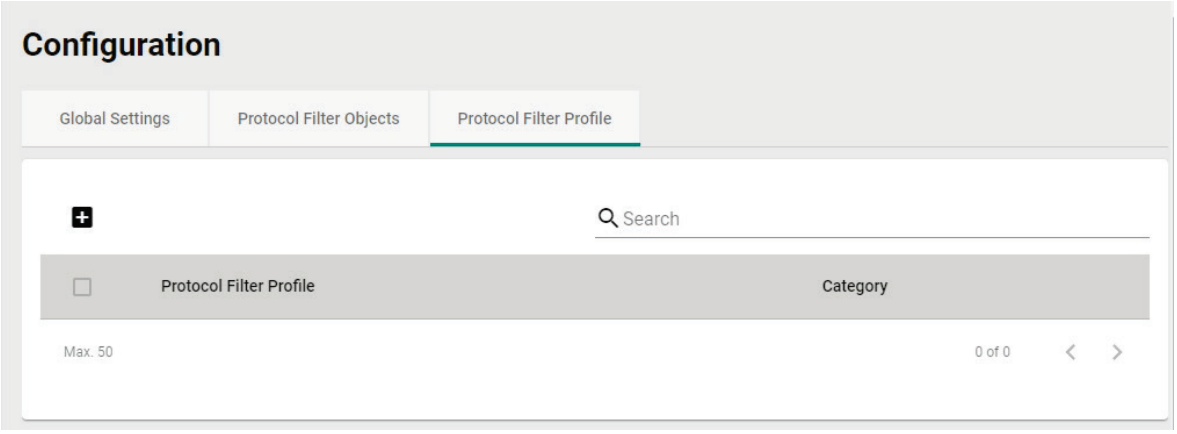
Protocol Filter Profile

Setting	Description	Factory Default
Identity Service, Read Service, Write Service, Report Service, File Operation Service, Journal Service, Manual	Select a preset or user-configured protocol filter profile for this protocol filter object. Refer to Protocol Filter Profile for more information about user-configured profiles. Select Manual to manually configure the profile parameters.	None

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

Protocol Filter Profile

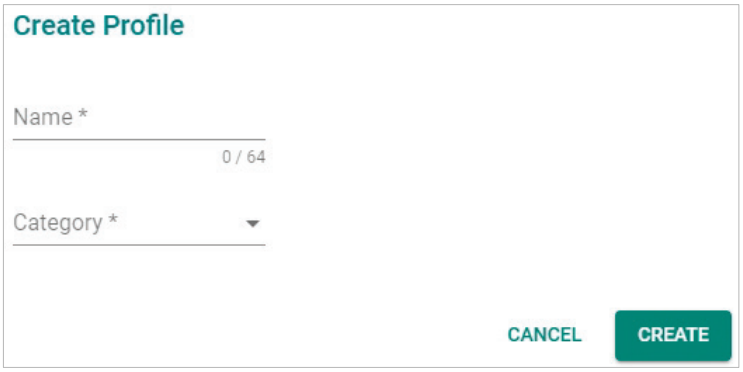
Protocol filter profiles provide a way to quickly group protocol-related settings. Protocol filter profiles can then be used in protocol filter objects.



Create a New Protocol Filter Profile

On the **Protocol Filter Profile** tab, click the icon to create a new filter profile. The configuration settings depend on the selected Category.

Refer to the following sections for more details on each category:
Create a Modbus/TCP Profile
Create a DNP3 Profile
Create an IEC-104 profile
Create a MMS Profile



Modify an Existing Protocol Filter Profile

Select the item in the Protocol Filter Profile Table and click the icon next to the entry you want to modify. When finished, click the **APPLY** button to save your changes.

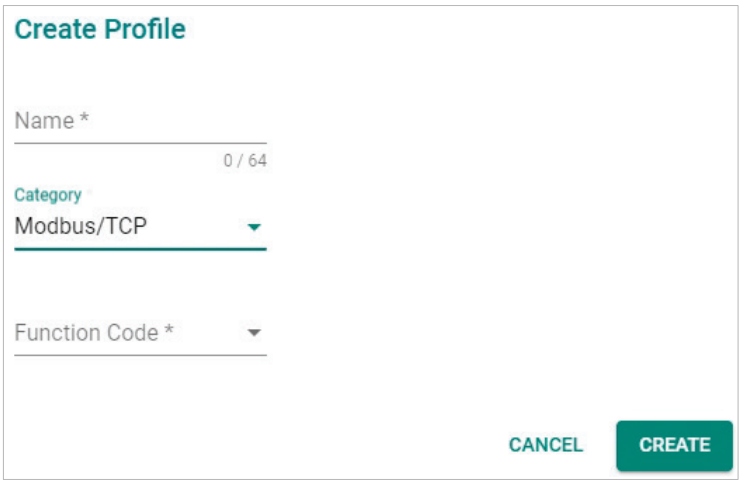
Delete an Existing Protocol Filter Profile

Select the item(s) in the Protocol Filter Profile Table. Click the icon and click **DELETE** to delete the protocol filter profile(s).

Create a Modbus/TCP Profile

Modbus/TCP is a Modbus protocol used for communications over TCP/IP networks, connecting over port 502 by default. Modbus has also been experimentally used over UDP on IP networks, which removes the overheads required for TCP. The following table shows the Modbus TCP frame format:

Modbus/TCP Frame Format		
Description	**Length**	**Function**
Transaction Identifier	2 bytes	Synchronization between messages of the server and client
Protocol Identifier	2 bytes	The value is 0 for Modbus TCP protocol
Length Field	2 bytes	Number of remaining following bytes in this frame
Unit Identifier	1 byte	Slave Address (255 is used for device broadcast information)
Function code	1 byte	Defines the message type
Data bytes	n bytes	Data block with additional information



Name

Setting	Description	Factory Default
0 to 64 characters	Enter a name for the protocol filter profile.	None

Category

Setting	Description	Factory Default
Modbus/TCP	Select the Modbus/TCP protocol.	None

Function Code

Setting	Description	Factory Default
All, blank, common function code	Select the function code or manually specify the function code. The function code format is 0 to 255 and allows commas. Refer to the Common Function Codes table for a full list of function codes.	None

Common Function Codes:

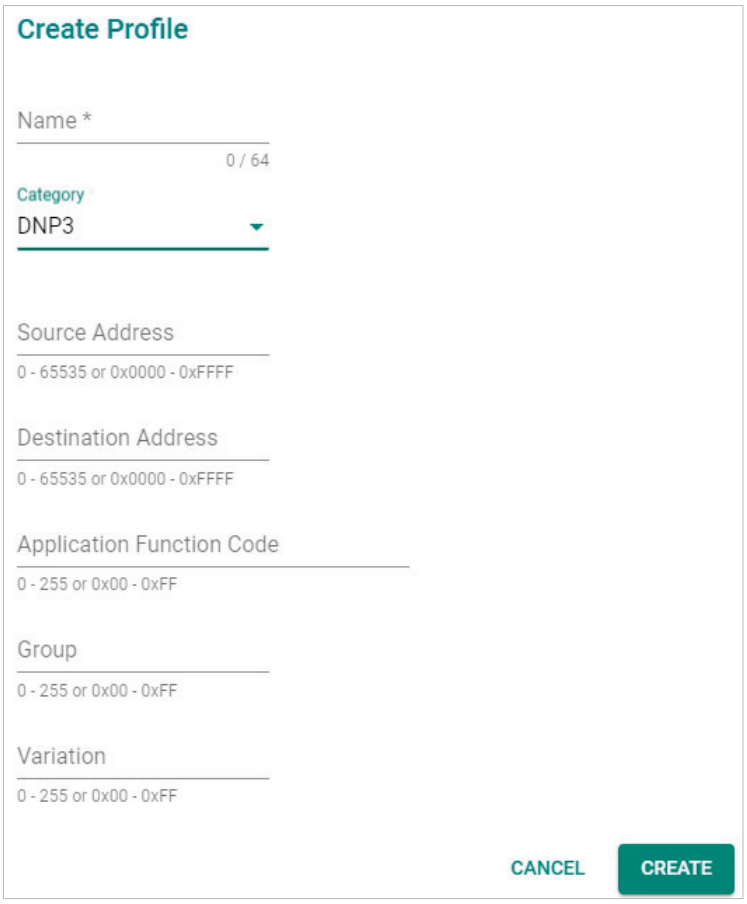
			Function Name	Function Code
Data Access	Bit Access	Physical Discrete Inputs	Read Discrete Inputs	2
		Internal Bits or Physical Coils	Read Coils	1
			Write Single Coil	5
			Write Multiple Coils	15
	16-bit Access	Physical Input Registers	Read Input Register	4
		Internal Registers or Physical Output Registers	Read Holding Registers	3
			Write Single Register	6
			Write Multiple Registers	16
			Read/Write Multiple Registers	23
			Mask Write Register	22
			Read FIFO Queue	24
	File Record Access		Read File Record	20
			Write File Record	21
Diagnostics			Read Exception Status	7
			Diagnostic	8
			Get Com Event Counter	11
			Get Com Event Log	12
			Report Slave ID	17
			Read Device Identification	43

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

Create a DNP3 Profile

Distributed Network Protocol 3 (DNP3) is a set of communications protocols used between components in process automation systems, connecting over port 20000 by default. Its main use is in utilities such as electric and water companies. The following table shows the DNP3 frame format:

DNP3 Frame Format		
Description	**Length**	**Function**
Application Header	4 bytes	Includes application control, function code and internal indications information.
Object Header	4 bytes	Includes object type field, qualifier field, and range field information.
DNP3 Objects	n bytes	Encoded representation of data from a point, or other structure, that is formatted according to its group and variation number for transport in a message.



Name

Setting	Description	Factory Default
0 to 64 characters	Enter a name for the protocol filter profile.	None

Category

Setting	Description	Factory Default
DNP3	Select the DNP3 protocol.	None

Source Address

Setting	Description	Factory Default
0 to 65535, 0x0000 to 0xFFFF	Specify the source address, which will be checked in the DNP3 packet.	None

Destination Address

Setting	Description	Factory Default
0 to 65535, 0x0000 to 0xFFFF	Specify the destination address, which will be checked in the DNP3 packet.	None

Application Function Code

Setting	Description	Factory Default
0 to 255, 0x00 to 0xFF	Specify the function code.	None

The application function code indicates the purpose, or requested operation, of the message. While DNP3 allows multiple data types in a single message, it only allows a single requested operation on the data types within the message. The following table shows the reading, writing, and other operations.

	Function Name	Function Code
Requests	Confirm	0
	Read	1
	Write	2
	Select	3
	Operate	4
	Dir operate	5
	Dir operate – No resp	6
	Freeze	7
	Freeze – No resp	8
	Freeze clear	9
	Freeze clear – No resp	10
	Freeze at time	11
	Freeze at time – No resp	12
	Cold restart	13
	Warm restart	14
	Initialize data	15
	Initialize application	16
	Start application	17
	Stop application	18
	Save configuration	19
	Enable unsolicited	20
	Disable unsolicited	21
	Assign class	22
	Delay measurement	23
	Record current time	24
	Open file	25
	Close file	26
	Delete file	27
	Get file information	28
	Authenticate file	29
	Abort file	30
	Activate config	31
	Authenticate request	32
	Authenticate request – No ack	33
Responses	Response	129
	Unsolicited response	130
	Authentication resp	131

Group

Setting	Description	Factory Default
0 to 255, 0x00 to 0xFF	Specify the group. This classifies the type or types within a message.	N/A

Variation

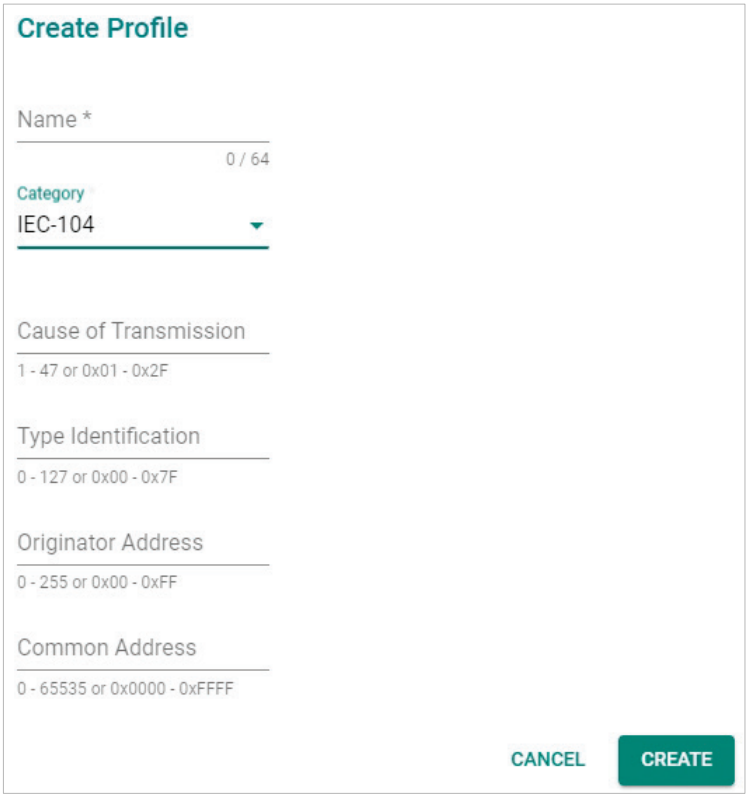
Setting	Description	Factory Default
0 to 255, 0x00 to 0xFF	Specify the variation. This represents a choice of encoding formats for many of the data types.	N/A

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

Create an IEC-104 Profile

The IEC 60870-5-104 (IEC-104) protocol is an extension of the IEC-101 protocol with changes in transport, network, link, and physical layer services to suit complete network access, connecting over port 2404 by default. The protocol can be used to provide TCP/IP communication between a Controlling Station and Controlled Station (Outstation). The following table shows the IEC-104 Application Service Data Unit (ASDU) frame format:

IEC-104 ASDU Frame Format		
Description	**Length**	**Function**
Type Identification	1 byte	Number that identifies the ASDU followed by its format and its content.
Variable Structure Qualifier	1 byte	Describes how the information objects are organized.
Cause of Transmission	1-2 bytes	Includes the reason for sending the ASDU and one byte with an identifier of the control center.
Common Address	1-2 bytes	The application address used to identify the data in the system.
Information Object	n bytes	Includes the content of the requested service or the notified information.



Name

Setting	Description	Factory Default
0 to 64 characters	Enter a name for the protocol filter profile.	None

Category

Setting	Description	Factory Default
IEC-104	Select the IEC-104 protocol.	None

Cause of Transmission

Setting	Description	Factory Default
1 to 47, 0x01 to 0x2F	Specify the number that identifies the reason for sending the ASDU. Refer to the table below for an overview of all causes and corresponding description.	None

Cause	Description
1	periodic, cyclic
2	background interrogation
3	spontaneous
4	initialized
5	interrogation or interrogated
6	activation
7	confirmation activation
8	deactivation
9	confirmation deactivation
10	termination activation
11	feedback, caused by distant command
12	feedback, caused by local command
13	data transmission
14-19	reserved for further compatible definitions
20	interrogated by general interrogation
21	interrogated by interrogation group 1
22	interrogated by interrogation group 2
23	interrogated by interrogation group 3
24	interrogated by interrogation group 4
25	interrogated by interrogation group 5
26	interrogated by interrogation group 6
27	interrogated by interrogation group 7
28	interrogated by interrogation group 8
29	interrogated by interrogation group 9
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

Type Identification

Setting	Description	Factory Default
0 to 127 or 0x00 to 0x7F	Specify the number that identifies the ASDU, its format, and its content. Refer to the table below for an overview of all types and corresponding description.	None

	Type	Description
Process information in monitor direction	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)	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	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)	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	70	End of initialization

	Type	Description
System information in control direction	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
	100	(General-) Interrogation command
Parameter in control direction	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	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

Original Address

Setting	Description	Factory Default
0 to 255, 0x00 to 0xFF	Specify the address that identifies the control center.	None

Common Address

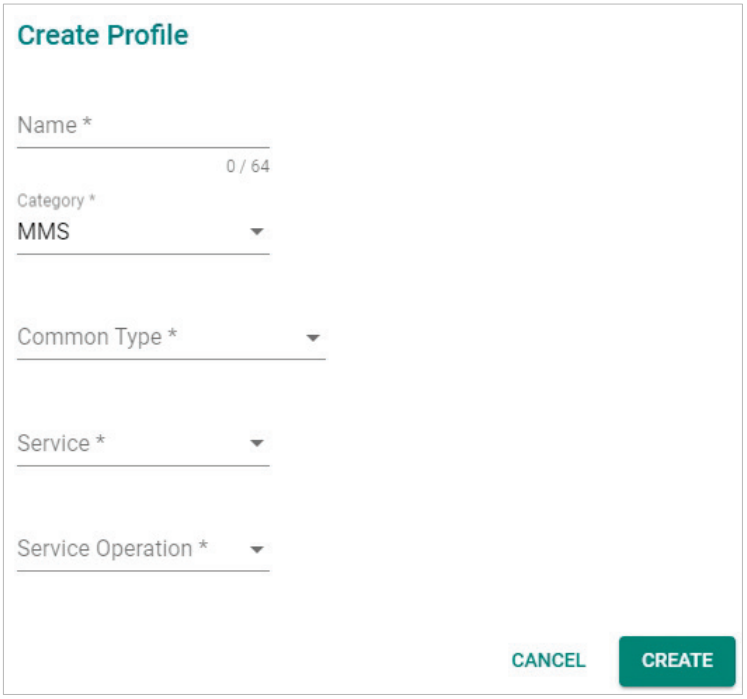
Setting	Description	Factory Default
0 to 65535, 0x0000 to 0xFFFF	Specify the common address of the ASDU.	None

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

Create a MMS Profile

MMS (Manufacturing Message Specification) is a messaging system for modeling real devices and functions and for exchanging information about the real device and process data in real-time, and supervisory control information between networked devices and/or computer applications. MMS connects over port 102 by default.

MMS communicates using a client-server model. A client is a network application or device (e.g., monitoring system, control center) that asks for data or an action from the server. A server is a device or application that contains a Virtual Manufacturing Device (VMD) and its objects (e.g., variables) that the MMS client can access. The VMD object represents a container in which all other objects are located. The client issues MMS service requests and the server responds to these requests.



Name

Setting	Description	Factory Default
0 to 64 characters	Enter a name for the protocol filter profile.	None

Category

Setting	Description	Factory Default
MMS	Select the MMS protocol.	None

Command Type

Setting	Description	Factory Default
Command type code	Select the type of MMS PDU. Refer to the table below for an overview of all command types.	None

	Command Type		Command Type
1	confirmed_RequestPDU	8	cancel_ErrorPDU
2	confirmed_ResponsePDU	9	initiate_RequestPDU
3	confirmed_ErrorPDU	10	initiate_ResponsePDU
4	unconfirmed_PDU	11	initiate_ErrorPDU
5	rejectPDU	12	conclude_RequestPDU
6	cancel_RequestPDU	13	conclude_ResponsePDU
7	cancel_ResponsePDU	14	conclude_ErrorPDU

Service

Setting	Description	Factory Default
Any, Confirmed Request, Confirmed Response, Unconfirmed	Select the service.	None

Service Operation

Setting	Description	Factory Default
Service operation code	Select the MMS service operation. Refer to the table below for an overview of all service operations.	None

	Service Operation		Service Operation
1	acknowledgeEventNotification	42	getProgramInvocationAttributes
2	alterEventConditionMonitoring	43	getScatteredAccessAttributes
3	alterEventEnrollment	44	getVariableAccessAttributes
4	createJournal	45	identify
5	createProgramInvocation	46	informationReport
6	defineEventAction	47	initializeJournal
7	defineEventCondition	48	initiateDownloadSequence
8	defineEventEnrollment	49	initiateUploadSequence
9	defineNamedType	50	input
10	defineNamedVariable	51	kill
11	defineNamedVariableList	52	loadDomainContent
12	defineScatteredAccess	53	obtainFile
13	defineSemaphore	54	output
14	deleteDomain	55	read
15	deleteEventAction	56	readJournal
16	deleteEventCondition	57	relinquishControl
17	deleteEventEnrollment	58	rename
18	deleteJournal	59	reportActionStatus
19	deleteNamedType	60	reportEventActionStatus
20	deleteNamedVariableList	61	reportEventConditionStatus
21	deleteProgramInvocation	62	reportEventEnrollmentStatus
22	deleteSemaphore	63	reportJournalStatus
23.	deleteVariableAccess	64	reportPoolSemaphoreStatus
24	downloadSegment	65	reportSemaphoreEntryStatus
25	eventNotification	66	reportSemaphoreStatus
26	fileClose	67	requestDomainDownLoad
27	fileDelete	68	requestDomainUpload
28	fileDirectory	69	reset
29	fileOpen	70	resume
30	fileRead	71	start
31	fileRename	72	status
32	getAlarmEnrollmentSummary	73	stop
33	getAlarmSummary	74	storeDomainContent
34	getCapabilityList	75	takeControl
35	getDomainAttributes	76	terminateDownloadSequence
36	getEventActionAttributes	77	terminateUploadSequence
37	getEventConditionAttributes	78	triggerEvent
38	getEventEnrollmentAttributes	79	unsolicitedStatus
39	getNamedTypeAttributes	80	uploadSegment
40	getNamedVariableListAttributes	81	write
41	getNameList	82	writeJournal

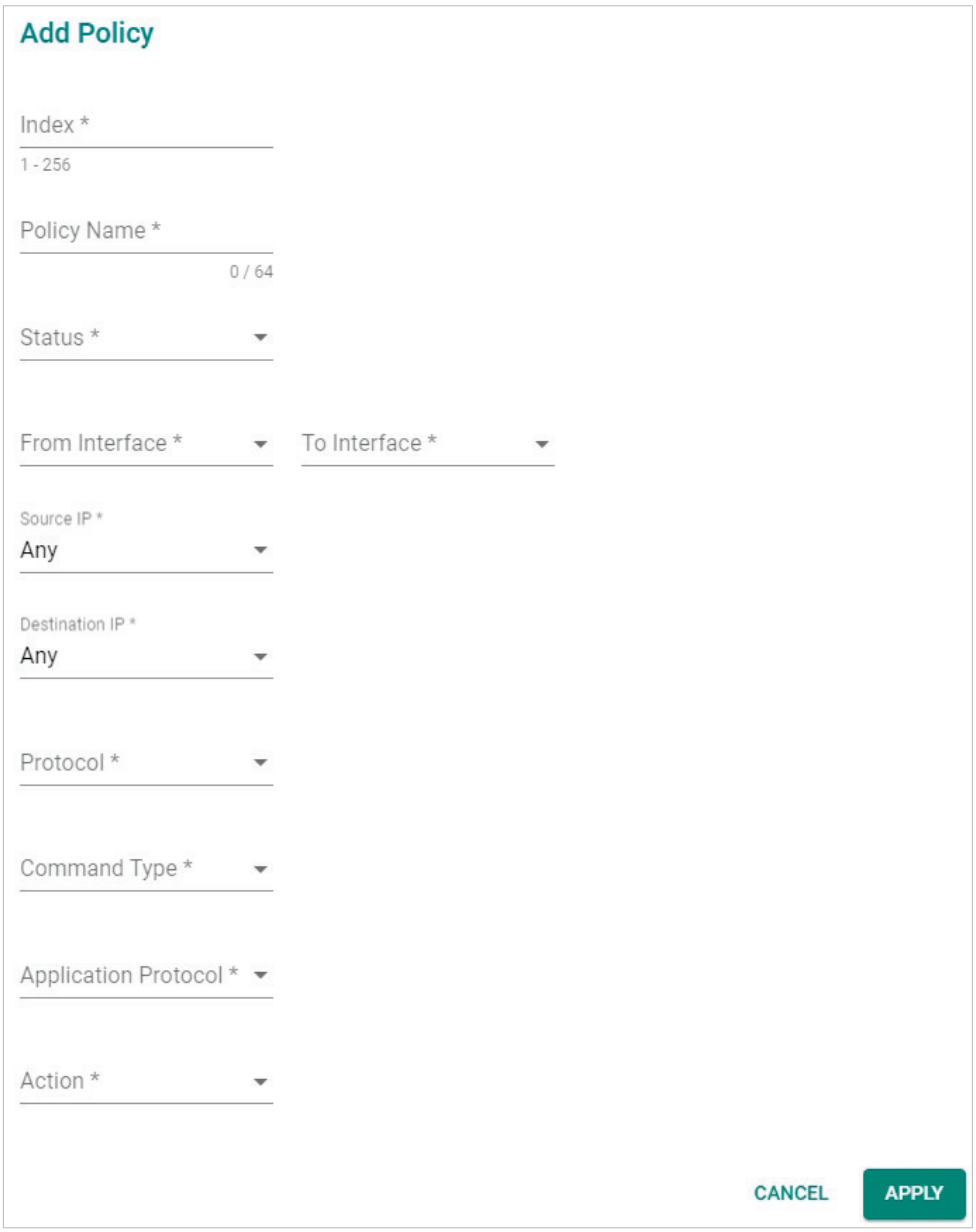
When finished, click **CREATE** to save your configuration.

Protocol Filter Policy

The application firewall policies provide inspection of industrial protocol packets, which allows users to control protocol traffic based on the configured policy and Anomaly Detection & Protection (ADP) settings. Refer to the Add a New Protocol Filter Policy and ADP (Anomaly Detection & Protection) sections.

Add a New Protocol Filter Policy

Click the ⊞ icon to create a new protocol filter policy.



Index

Setting	Description	Factory Default
1 to 256	Specify the index of the policy.	None

Name

Setting	Description	Factory Default
0 to 64 characters	Enter a name for the policy.	None

Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the policy.	None

From/To Interface

Setting	Description	Factory Default
Any, LAN, WAN	Select the From Interface and To Interface.	None

Source IP

Setting	Description	Factory Default
Any	The policy will check all source IP addresses in the packet.	Any
Single	The policy will only check for the specified source IP address in the packet.	
Range	The policy will check all source IP addresses in the packet within the specified IP range.	
Subnet	The policy will check for source IP addresses in the packet that are within the specified subnet mask.	

Destination IP

Setting	Description	Factory Default
Any	The policy will check all destination IP addresses in the packet.	Any
Single	The policy will only check for the specified destination IP address in the packet.	
Range	The policy will check all destination IP addresses in the packet within the specified IP range.	
Subnet	The policy will check for destination IP addresses in the packet that are within the specified subnet mask.	

Protocol

Setting	Description	Factory Default
Any, TCP, UDP	Select the protocol for this policy.	None

Command Type

Setting	Description	Factory Default
Master Query, Slave Response	Select the packet transmission direction for this policy.	None

Application Object

Setting	Description	Factory Default
Custom object	Select the application object for this policy.	None

Action

Setting	Description	Factory Default
Accept	The packet will be allowed through the firewall when it matches this policy.	None
Monitor	The packet will be allowed through the firewall when it matches this policy, and an event log will be recorded.	
Reset	The packet will by dropped by the firewall when it matches this policy. The session will also be disconnected.	

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

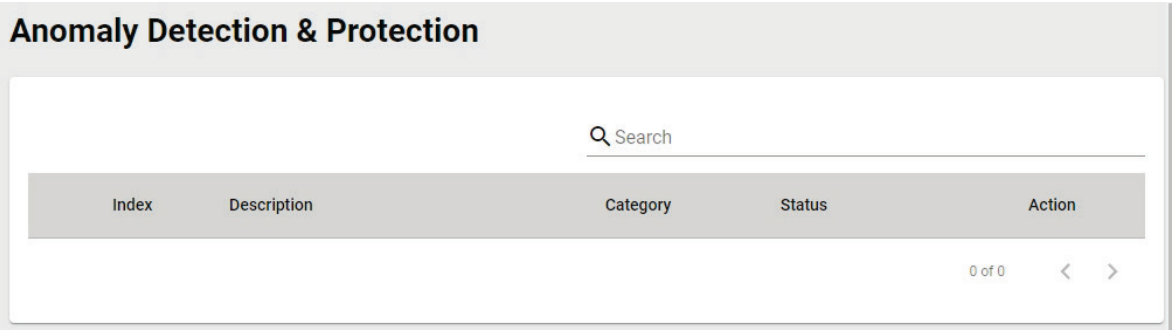
Modify an Existing Policy

Select the item in the Policy Table. Click the icon next to the entry you want to modify. When finished, click **APPLY** to save your changes.

Delete an Existing Policy

Select the item(s) in the Policy Table, click the icon and then click **DELETE** to delete the item(s).

ADP (Anomaly Detection & Protection)



Modify an Existing ADP Entry

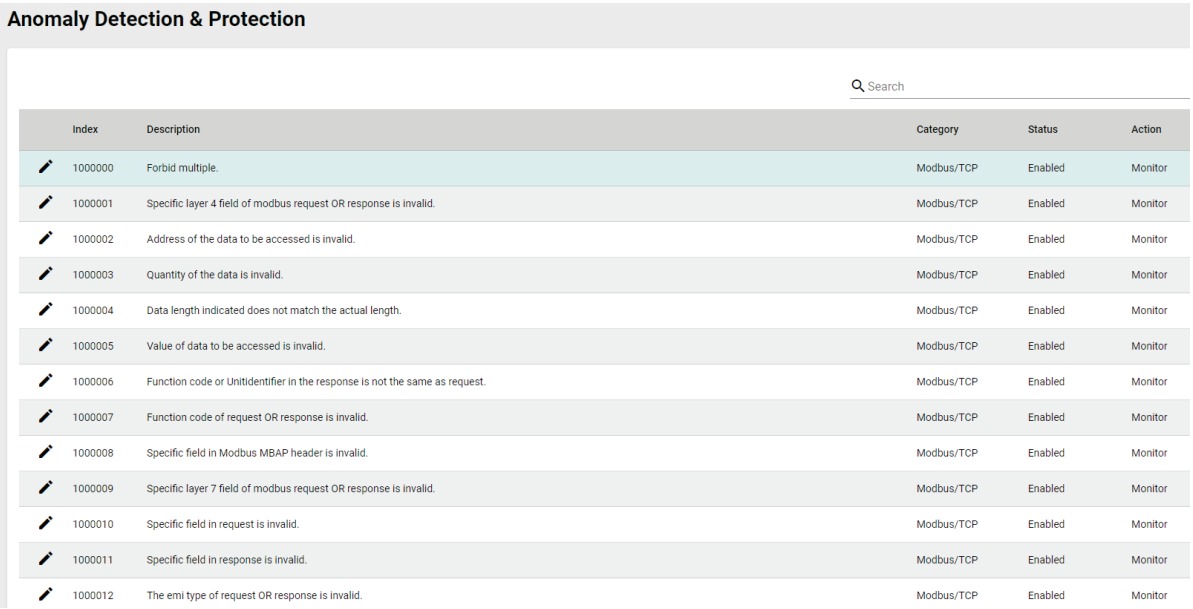
Click the icon to modify the Anomaly Detection & Protection (ADP) parameters.

Index

Setting	Description	Factory Default
ADP setting index	The number of the ADP setting.	1000000

Description

The following table provides a description for each ADP setting, listed by index.



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
1000005	Value of data to be accessed is invalid.	Modbus/TCP	Enabled	Monitor
1000006	Function code or Unitidentifier in the response is not the same as request.	Modbus/TCP	Enabled	Monitor
1000007	Function code of request OR response is invalid.	Modbus/TCP	Enabled	Monitor
1000008	Specific field in Modbus MBAP header is invalid.	Modbus/TCP	Enabled	Monitor
1000009	Specific layer 7 field of modbus request OR response is invalid.	Modbus/TCP	Enabled	Monitor
1000010	Specific field in request is invalid.	Modbus/TCP	Enabled	Monitor
1000011	Specific field in response is invalid.	Modbus/TCP	Enabled	Monitor
1000012	The emi type of request OR response is invalid.	Modbus/TCP	Enabled	Monitor

Category

Setting	Description	Factory Default
Modbus/TCP, DNP3, IEC-104	Select the protocol for the ADP settings.	Modbus/TCP

Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the selected ADP setting.	Enabled

Action

Setting	Description	Factory Default
Accept	The packet will be allowed through the firewall when it matches this ADP setting.	Monitor
Reset	The packet will by dropped by the firewall when it matches this ADP setting. The session will also be disconnected.	
Monitor	The packet will be allowed through the firewall when it matches this ADP setting and an event log will be recorded.	

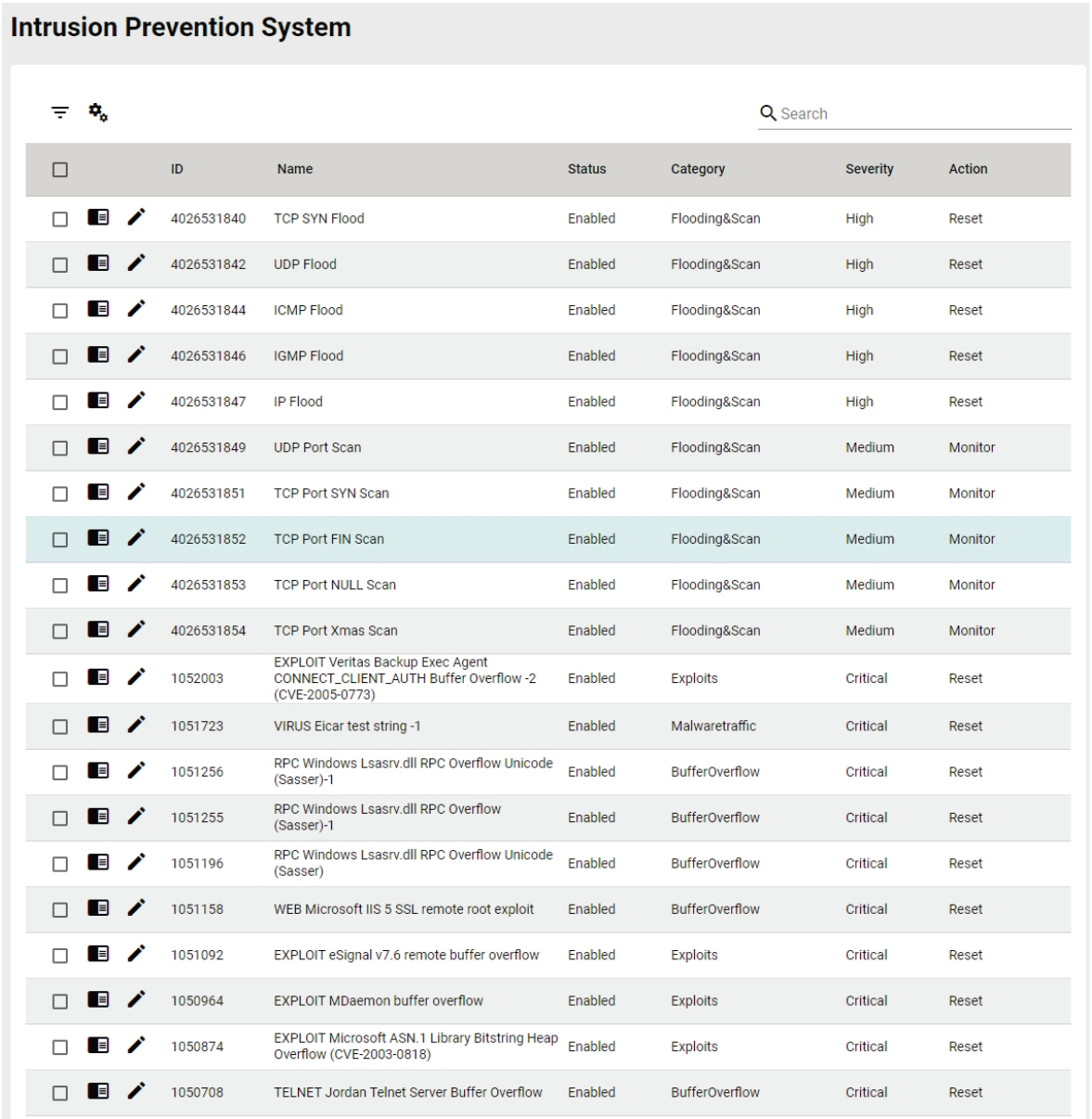
When finished, click **APPLY** to save your changes.

IPS (Intrusion Prevention System)

To combat ever-changing cyberthreats, the EDR-G9010 Series supports intelligent IPS features that perform pattern-based detection and block known attacks.

NOTE

A separate license is required to enable IPS functionality on the device.



ID	Name	Status	Category	Severity	Action
4026531840	TCP SYN Flood	Enabled	Flooding&Scan	High	Reset
4026531842	UDP Flood	Enabled	Flooding&Scan	High	Reset
4026531844	ICMP Flood	Enabled	Flooding&Scan	High	Reset
4026531846	IGMP Flood	Enabled	Flooding&Scan	High	Reset
4026531847	IP Flood	Enabled	Flooding&Scan	High	Reset
4026531849	UDP Port Scan	Enabled	Flooding&Scan	Medium	Monitor
4026531851	TCP Port SYN Scan	Enabled	Flooding&Scan	Medium	Monitor
4026531852	TCP Port FIN Scan	Enabled	Flooding&Scan	Medium	Monitor
4026531853	TCP Port NULL Scan	Enabled	Flooding&Scan	Medium	Monitor
4026531854	TCP Port Xmas Scan	Enabled	Flooding&Scan	Medium	Monitor
1052003	EXPLOIT Veritas Backup Exec Agent CONNECT_CLIENT_AUTH Buffer Overflow -2 (CVE-2005-0773)	Enabled	Exploits	Critical	Reset
1051723	VIRUS Eicar test string -1	Enabled	Malwaretraffic	Critical	Reset
1051256	RPC Windows Lsasrv.dll RPC Overflow Unicode (Sasser)-1	Enabled	BufferOverflow	Critical	Reset
1051255	RPC Windows Lsasrv.dll RPC Overflow (Sasser)-1	Enabled	BufferOverflow	Critical	Reset
1051196	RPC Windows Lsasrv.dll RPC Overflow Unicode (Sasser)	Enabled	BufferOverflow	Critical	Reset
1051158	WEB Microsoft IIS 5 SSL remote root exploit	Enabled	BufferOverflow	Critical	Reset
1051092	EXPLOIT eSignal v7.6 remote buffer overflow	Enabled	Exploits	Critical	Reset
1050964	EXPLOIT MDaemon buffer overflow	Enabled	Exploits	Critical	Reset
1050874	EXPLOIT Microsoft ASN.1 Library Bitstring Heap Overflow (CVE-2003-0818)	Enabled	Exploits	Critical	Reset
1050708	TELNET Jordan Telnet Server Buffer Overflow	Enabled	BufferOverflow	Critical	Reset

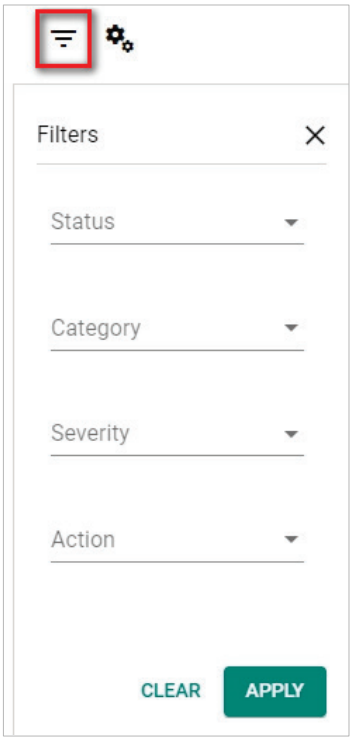
Refer to the table below for a description of each field.

Field	Description
ID	The pattern rule ID
Name	The pattern name of the intrusion
Status	The operational status of the pattern rule
Category	The threat category of the intrusion
Severity	The assigned security level for the intrusion
Action	The preset action when responding to the intrusion

Filter IPS Rules

Use the filter function to quickly narrow down IPS pattern rules based on the set criteria.

Click the icon to expand the filter menu.



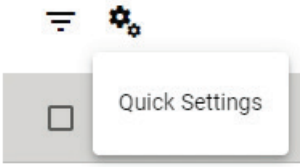
Select the criteria for one or more fields and click **APPLY**. Any pattern rules matching the filter criteria will be shown in the table.

Click **CLEAR** to reset all filter criteria.

Quick Settings

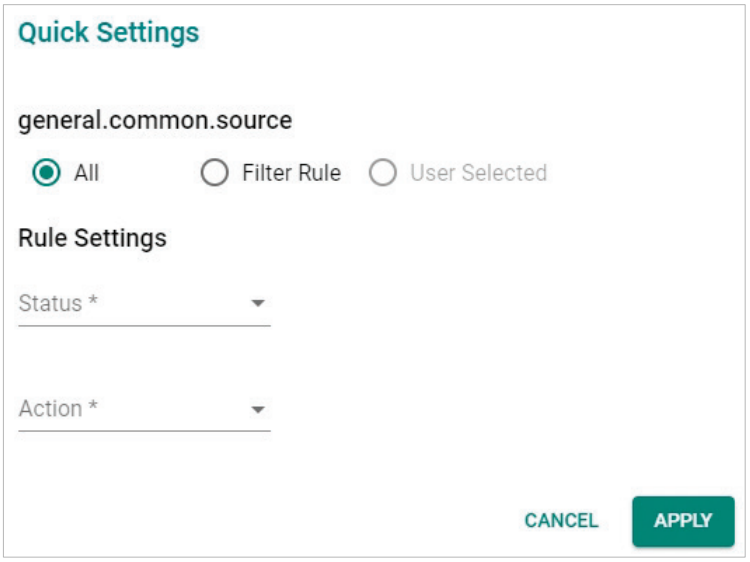
Quick Settings is used to easily configure multiple IPS rules at once. Users can choose to configure all IPS rules, based on filter criteria, or selected IPS rules.

Click the icon and click **Quick Settings**.



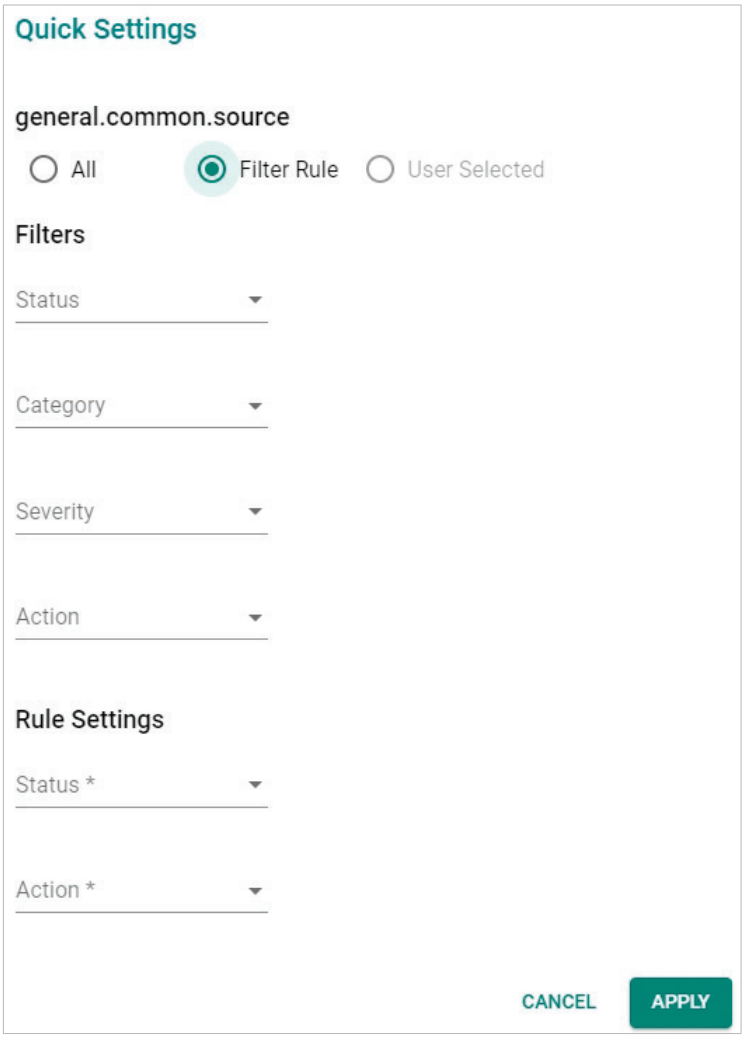
Modify Settings for All IPS Pattern Rules

1. Select **All** under general.common.source.
2. Select the **Status** and **Action** in the Rule Settings section.
3. Click **APPLY** to save your changes. The changes will be applied to all IPS pattern rules.



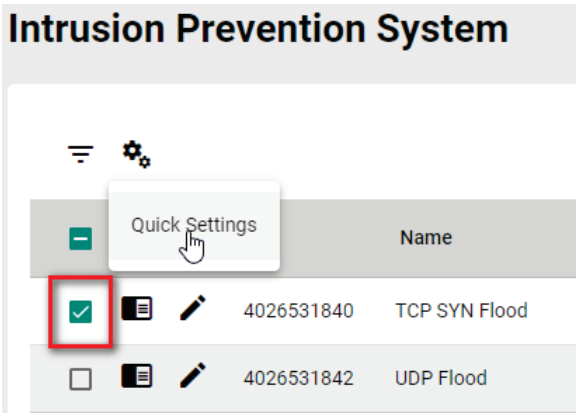
Modify Settings for Filtered Pattern Rules

1. Select **Filter Rule** under general.common.source.
2. Select the filter criteria in the Filters section.
3. Select the **Status** and **Action** in the Rule Settings section.
4. Click **APPLY** to save your changes. The changes will be applied to all IPS pattern rules that match the filter criteria.

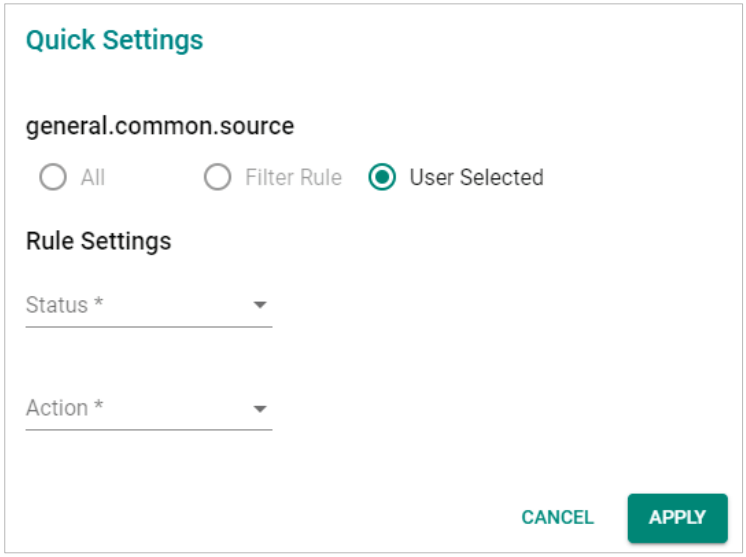


Modify Settings for User-selected IPS Pattern Rules

1. In the IPS rules table, check the box of the IPS pattern rule(s) you want to modify.
2. Click the icon and click Quick Settings.

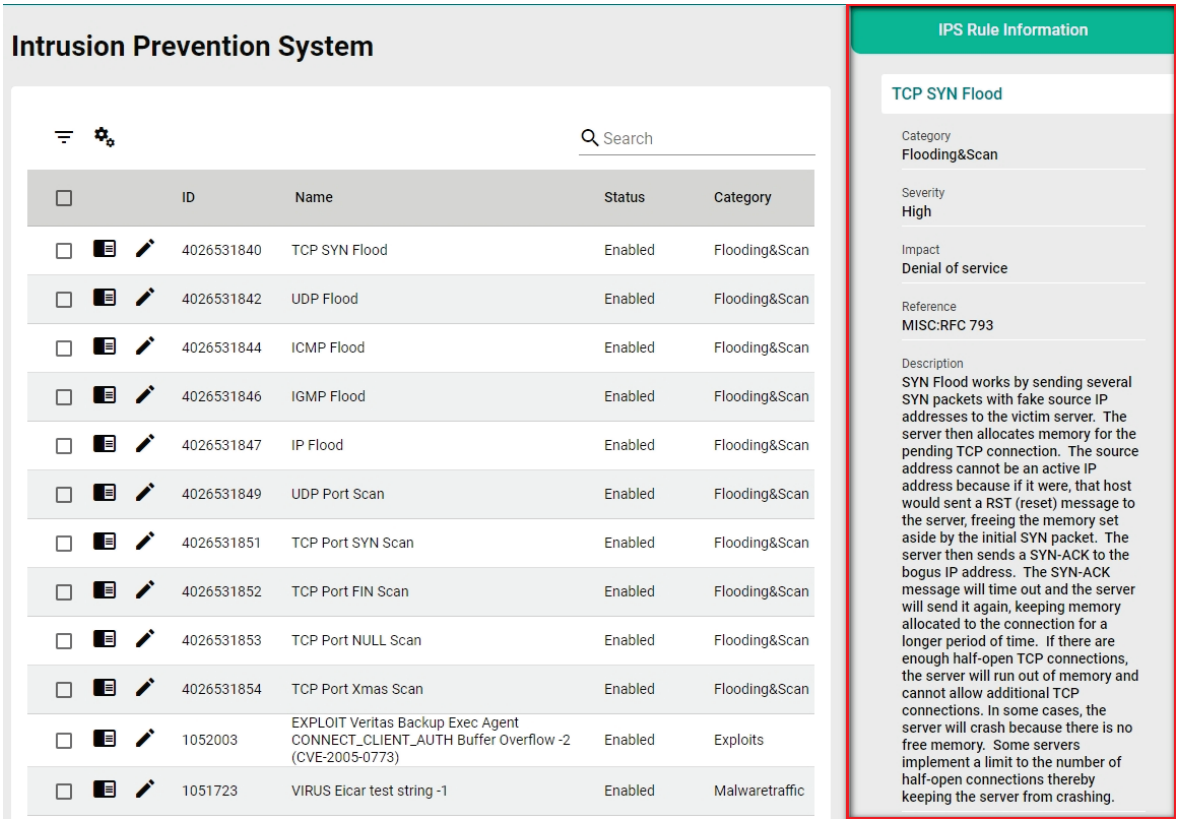


3. **User Selected** will selected by automatically.
4. Select the **Status** and **Action** in the Rule Settings section.
5. Click **APPLY** to save your changes. The changes will be applied to all selected IPS pattern rules.



Detailed Information

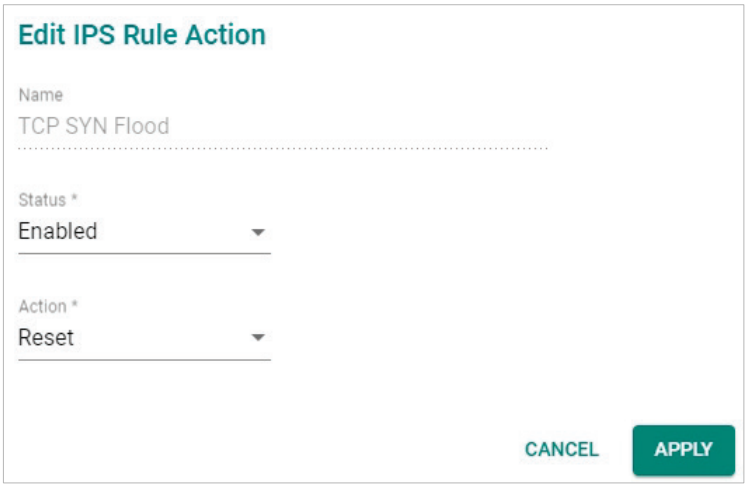
Click the icon next to any rule to bring up a panel with detailed information about the IPS rule.



Click the icon again to close the panel.

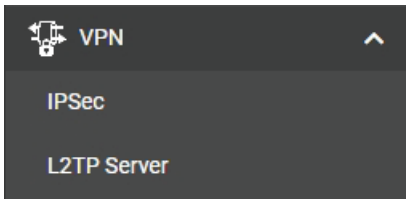
Modify an Existing IPS Rule Action

1. Click the icon next to the rule you want to modify.
2. Select the **Status** and **Action**.
3. Click **APPLY** to save your changes.



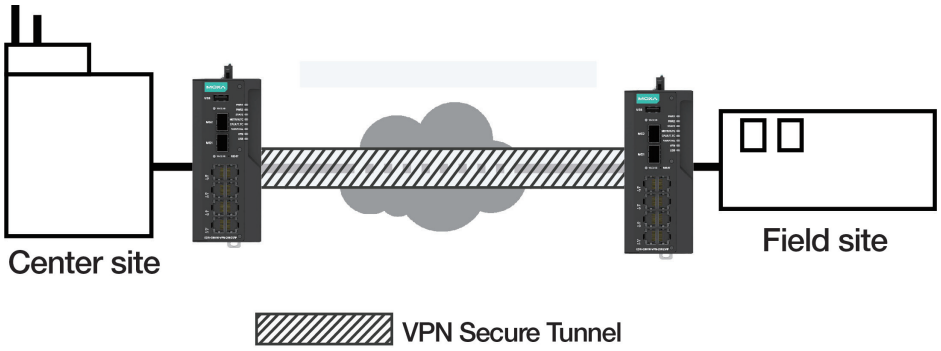
12. VPN (Virtual Private Network)

From the **VPN** section, you can configure **IPSec,** and **L2TP Server** settings.



Overview

In this section we describe how to use the Industrial Secure Router to build a secure remote automation network with the VPN (Virtual Private Network) feature. A VPN provides a highly cost-effective solution for establishing secure communication tunnels so that data can be exchanged safely.



There are two common applications for secure remote communication in an industrial automation network:

IPsec (Internet Protocol Security) VPN for LAN-to-LAN Security

IPsec is often used for data communication between two different LAN segments that is limited to a predefined IP range.

IPsec uses the IKE (Internet Key Exchange) protocol for Authentication, Key exchange and provides a way for the VPN gateway data to be protected by different encryption methods.

There are 2 phases for IKE when negotiating the IPsec connections between 2 VPN gateways:

Key Exchange (IPsec Phase 1): The 2 VPN gateways will negotiate how IKE should be protected. Phase 1 will also authenticate the two VPN gateways by the matched Pre-Shared Key or X.509 Certificate.

Data Exchange (IPsec Phase 2): In Phase 2, the VPN gateways negotiate to determine additional IPsec connection details, which include the data encryption algorithm.

L2TP (Layer 2 Tunnel Protocol) VPN for Remote Roaming Users

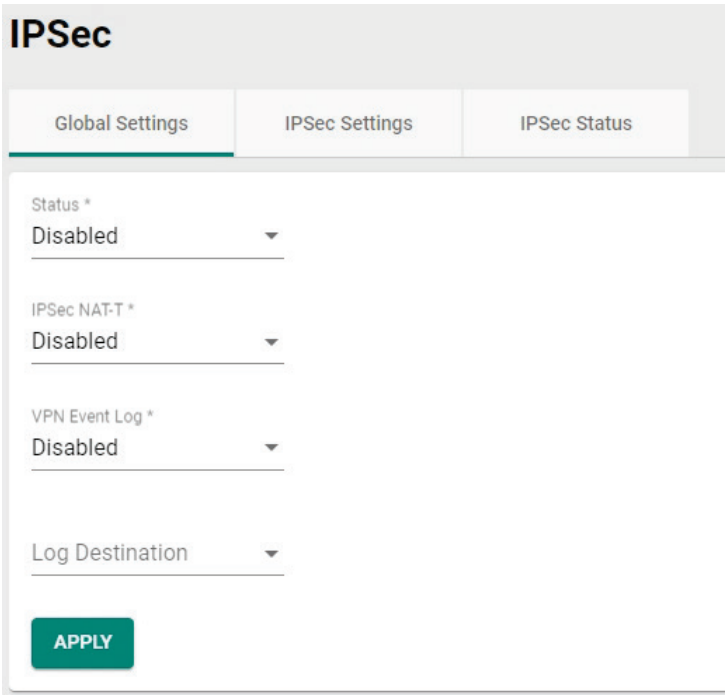
L2TP is suitable for VPN environments with dynamic IPs for remote, roaming users. L2TP is a popular choice for VPN applications with remote roaming users because the protocol is already built into the Microsoft Windows operating system.

IPsec Configuration

IPsec configuration consists of 5 parts:

- **Global Setting:** Enable or disable all IPsec tunnels and NAT-Traversal (NAT-T) functionality
- **Tunnel Setting:** Set up the VPN connection type and the VPN network plan
- **Key Exchange:** Authentication for 2 VPN gateways
- **Data Exchange:** Data encryption between VPN gateways
- **Dead Peer Detection:** The mechanism for VPN Tunnel maintenance

Global Settings



The Industrial Secure Router provides 3 Global Settings for IPsec VPN applications.

Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable all IPsec VPN services.	Disabled

NOTE

IPsec VPN is disabled by default. Make sure to enable this option if you want to use the IPsec function.

IPsec NAT-T

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable IPsec NAT-T (NAT-Traversal). This option should be enabled if there an external Industrial Secure Router located between VPN tunnels.	Disabled

VPN Event Log

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

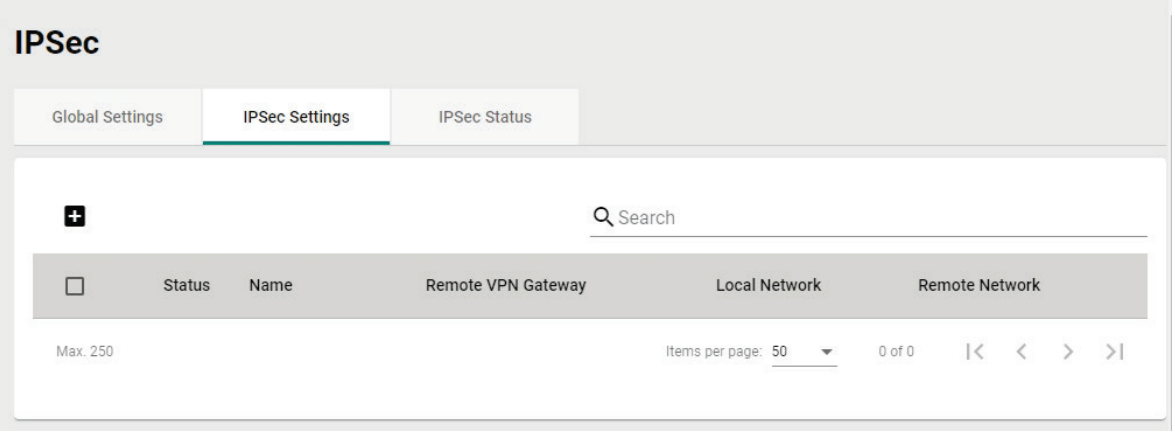
Severity

Setting	Description	Factory Default
Log severity	If VPN Event Log is enabled, select the severity for the VPN event logs.	None

Log Destination

Setting	Description	Factory Default
Local Storage, Syslog, Trap	If VPN Event Log is enabled, select the VPN event log storage location.	Disabled

IPsec Settings

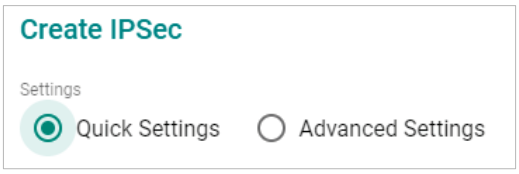


Create an IPsec Entry

Click the ⊞ icon to create a new IPsec entry. IPsec supports two types of settings. Refer to the IPsec Quick Settings and Advanced Settings sections for more information.

IPsec Quick Settings

The Industrial Secure Router's **Quick Settings** mode can be used to easily set up a site-to-site VPN tunnel between two Industrial Secure Router units.

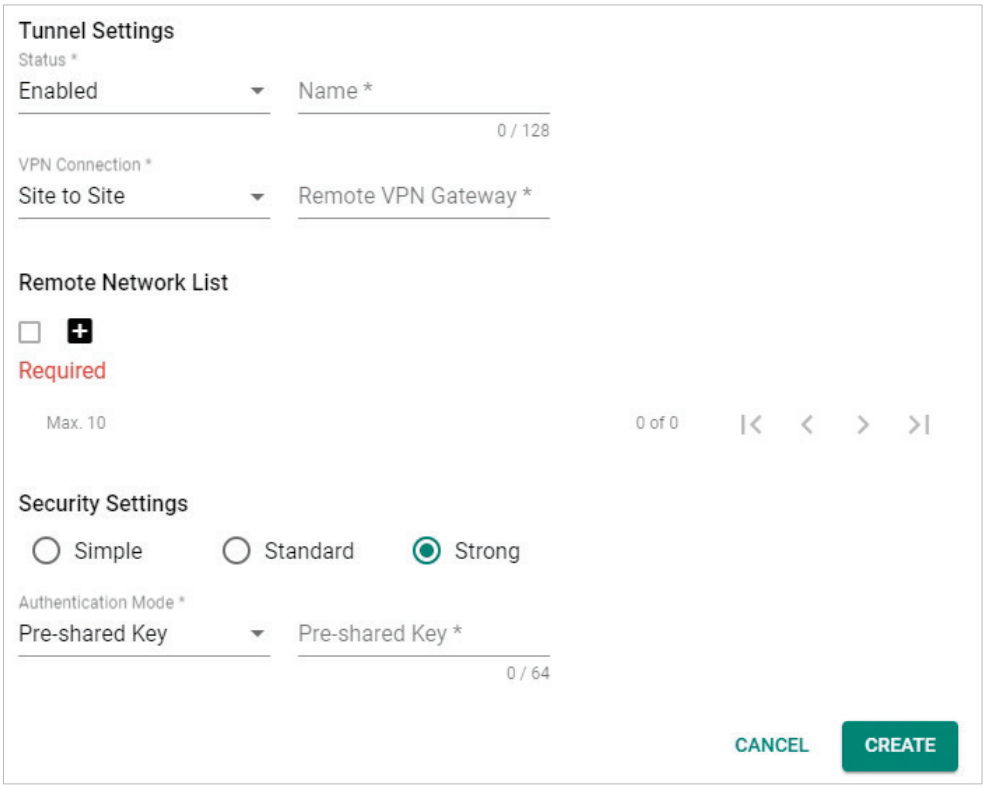


When choosing the Quick Settings mode, the user just needs to configure the following:

- Tunnel Settings
- Remote Network List

  Click the ⊞ icon to configure the remote VPN network.

  - Remote Network: The IP address of the remote VPN network.
  - Netmask: The netmask of the remote VPN network.
- Security Settings
  - Encryption Strength: Simple (AES-128), Standard (AES-192), or Strong (AES-256)
  - Authentication Mode: Pre-shared Key, X.509, or X.509 With CA
  - Pre-shared Key: The password of Pre-Shared Key

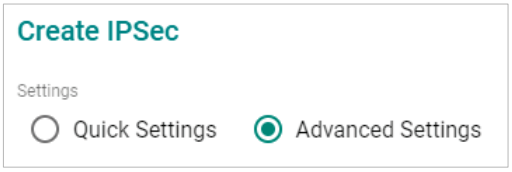


NOTE

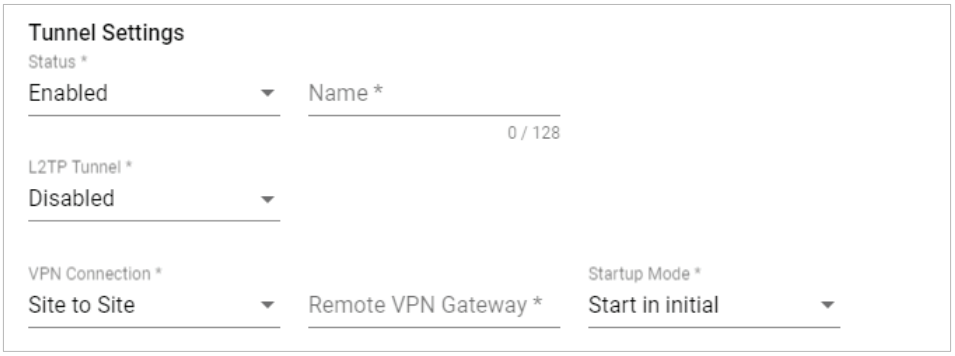
The Encryption Strength, Authentication Mode, and Pre-Shared Key configuration should be identical for both Industrial Secure Router units.

IPsec Advanced Settings

Select **Advanced Settings** to manually configure the full range of VPN settings.



Tunnel Settings



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the VPN tunnel.	Enabled

Name

Setting	Description	Factory Default
Max. 128 characters	Enter a name for this VPN tunnel.	None

> **NOTE**
>
> The name cannot start with a number.

L2TP Tunnel

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable L2TP over IPsec.	Disabled

VPN Connection

Setting	Description	Factory Default
Site to Site	The VPN tunnel for the Local and Remote subnets is fixed.	Site to Site
Site to Site(Any)	The VPN tunnel for the Remote subnet area is dynamic and is fixed for the Local subnet.	

Remote VPN Gateway

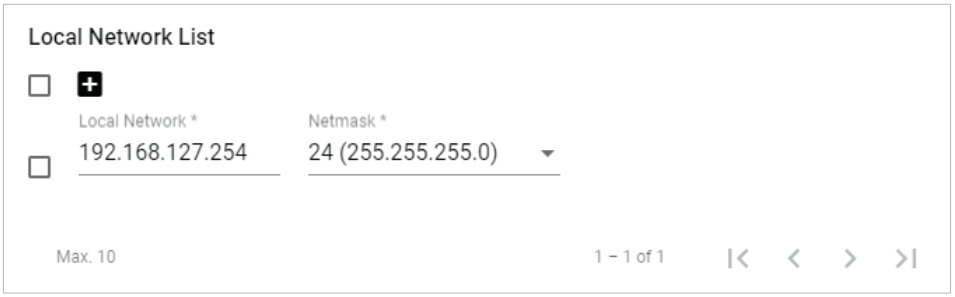
Setting	Description	Factory Default
IP Address	Specify the IP address of the remote VPN gateway.	None

Startup Mode

Setting	Description	Factory Default
Start in Initial	The VPN tunnel will actively initiate the connection with the remote VPN gateway.	Start in Initial
Wait for Connecting	The VPN tunnel will wait for the remote VPN gateway to initiate the connection.	

> **NOTE**
>
> The maximum number of **Starts** in the initial VPN tunnel is 30. The maximum number of **Waits** for connecting to a VPN tunnel is 100. This cannot be changed.

Local Network List

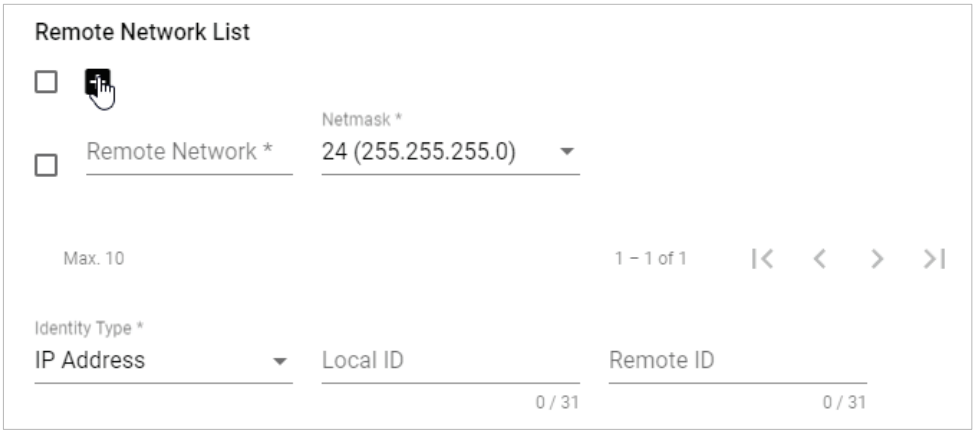


Local Network/Netmask

Setting	Description	Factory Default
IP Address (max. 10 local VPN networks)	Specify the IP address and subnet mask of the local VPN network. Users can configure multiple local networks to create an IPsec connection to the remote network. For example, if the user configures two local networks (192.168.127.254/24 and 192.168.126.254/24), these two networks will build an IPsec connection to the remote network.	192.168.127.254/ 24 (255.255.255.0)

Remote Network List

Click the ⊞ icon to configure the remote VPN network.



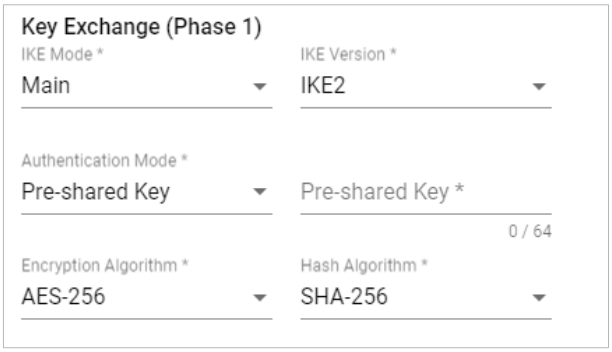
Remote Network/Netmask

Setting	Description	Factory Default
IP address (max. 10 remote VPN network)	Specify the IP address and subnet mask of the remote VPN network. Users can configure multiple remote networks to create an IPsec connection to the local network. For example, if the user configures two remote networks (10.10.100.254/24 and 10.10.110.254/24), these two networks will build an IPsec connection to the local network.	None/ 24 (255.255.255.0)

Identity

Setting	Description	Factory Default
Type	Select an ID type. There are four ID types: IP address, FQDN, Key ID, and Auto(with Cisco). Key ID is a user-defined string. Auto(with Cisco) is for used establishing connections to Cisco systems.	IP address
Local ID (max. 31 characters)	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.	None
Remote ID (max. 31 characters)	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.	None

Key Exchange (Phase 1)



IKE Mode

Setting	Description	Factory Default
Main	In 'Main' IKE Mode, 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.	Main
Aggressive	In "Aggressive" Mode, the Remote and Local VPN gateway will not negotiate the algorithm and will only use the user-defined configuration.	

IKE Version

Setting	Description	Factory Default
IKE1	Use the IKE Version 1 protocol	IKE2
IKE2	Use the IKE Version 2 protocol	

Authentication Mode

Setting	Description	Factory Default
Pre-Shared Key	Pre-Shared Key is a user-defined authentication string used by two systems to establish an IPsec VPN connection.	Pre-Shared Key
X.509	In this mode, two systems authenticate the VPN connection using certificates imported in advance by the user on the Local Certificate page. Refer to User Scenario 1 and 2 in the IPsec Use Case Demonstration section for more details.	N/A
X.509 With CA	In this mode, two systems authenticate the VPN connection using certificates imported in advance by the user on the Local Certificate page and a CA certificate imported on the Trusted CA Certificate page. Refer to User Scenario 3, 4, and 5 in the IPsec Use Case Demonstration section for more details.	N/A

NOTE

Certificates are a time-based form of authentication. Before processing certificates, please ensure that the industrial secure router is synced with the local device. For more information about syncing device time, please refer to the Time section.

Encryption Algorithm

Setting	Description	Factory Default
DES 3DES AES-128 AES-192 AES-256	Select the encryption algorithm for Key Exchange.	AES-256

Hash Algorithm

Setting	Description	Factory Default
MD5 SHA-1 SHA-256	Select the encryption algorithm for Key Exchange.	SHA-256

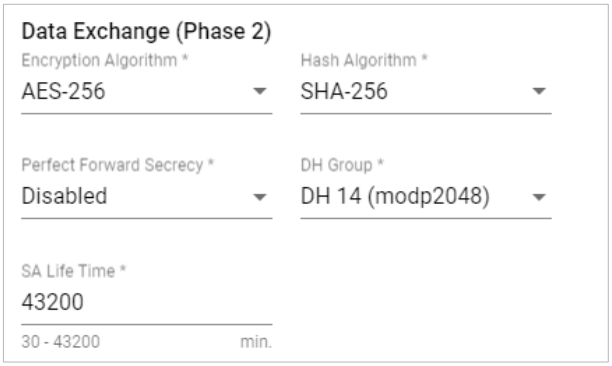
DH Group

Setting	Description	Factory Default
DH 1(modp768) DH 2(modp1024) DH 5(modp1536) DH 14(modp2048)	Select the Diffie-Hellman group. This is the Key Exchange group between the remote and VPN gateways.	DH 14(modp2048)

IKE Lifetime

Setting	Description	Factory Default
30 to 43200 (minutes)	Specify the lifetime (in minutes) for IKE SA.	43200 (minutes)

Data Exchange (Phase 2)



Encryption Algorithm

Setting	Description	Factory Default
DES 3DES AES-128 AES-192 AES-256	Select the encryption algorithm for data exchange	AES-256

Hash Algorithm

Setting	Description	Factory Default
MD5 SHA-1 SHA-256	Select the Hash Algorithm for data exchange.	SHA-256

Perfect Forward Secrecy

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable Perfect Forward Secrecy. When enabled, different security keys are used for different IPsec phases in order to enhance security.	Disabled

DH Group

Setting	Description	Factory Default
DH 1 (modp768) DH 2 (modp1024) DH 5 (modp1536) DH 14 (modp2048)	Select the Diffie-Hellman group. This is the Key Exchange group between the remote and VPN gateways.	DH 14 (modp2048)

SA Lifetime

Setting	Description	Factory Default
30 to 43200 (minutes)	Specify the lifetime (in minutes) for Phase 2 IKE SA.	43200 (minutes)

Dead Peer Detection

Dead Peer Detection is a mechanism to detect whether the connection between a local secure router and a remote IPsec tunnel has been lost.

Action

The action the system will take when a dead peer is detected.

Setting	Description	Factory Default
Hold	Maintain the VPN tunnel.	Restart
Restart	Reconnect the VPN tunnel.	
Clear	Clear the VPN tunnel.	
Disabled	Disable Dead Peer Detection.	

Retry Interval

Setting	Description	Factory Default
0 to 3600 (seconds)	Specify the interval (in seconds) at which Dead Peer Detection messages are sent.	30 (seconds)

Confidence Interval

Setting	Description	Factory Default
0 to 3600 (seconds)	Specify the interval (in seconds) at which the system will check if the connection is alive or not.	120 (seconds)

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

Modify an Existing IPsec Entry

Select the item in the IPsec VPN List and click the icon next to the entry you want to modify. When finished, click **APPLY** to save your changes.

Delete an Existing IPsec Entry

Select the item(s) in the IPsec VPN List. Click the icon and click **DELETE** to delete the item(s).

IPsec Use Case Demonstration

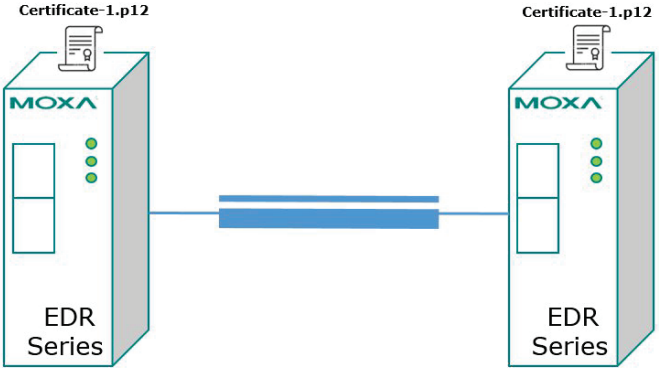
In the following section, we will consider five common user scenarios. The purpose of each example is to give a clearer understanding of two authentication modes 'X.509' and 'X.509 with CA'.

NOTE

Certificates are a time-based form of authentication. Before processing certificates, please ensure that the industrial secure router is synced with the local device. For more information about syncing device time, please refer to the Time section.

Scenario 1: X.509 Mode-One Certificate

Users will sometimes use certificates generated from a server or from the Internet. If users only get one certificate, they can import this certificate into a system. This system can then use the same certificate to identify other certificates and establish a VPN connection. In this case, users have to import certificates (.p12) into both systems. Refer to the instructions in the diagram below to learn how to install certificates and build an IPsec VPN connection.



EDR Security Router (A)

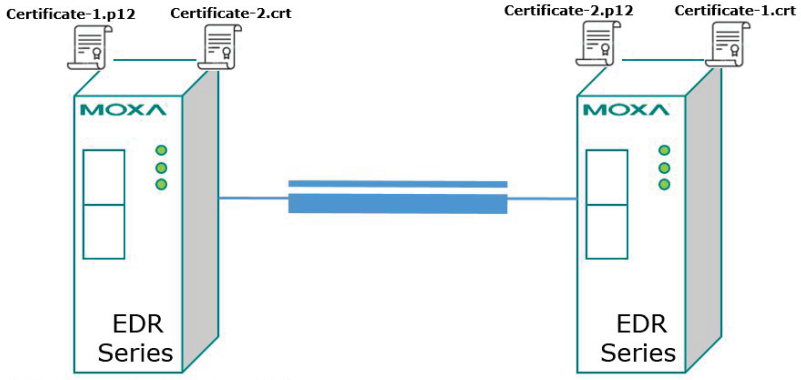
1. Import **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.
2. Enter "IPSec setting", and in "Advanced Setting", select X.509 authentication mode.
3. In "Local", select No.1
4. In "Remote", select No.1

EDR Security Router (B)

1. Import **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.
2. Enter "IPSec setting", and in "Advanced Setting", select X.509 authentication mode.
3. In "Local", select No.1
4. In "Remote", select No.1

Scenario 2: X.509 Mode-Two Certificates

Users will sometimes use certificates generated from a server or from the Internet. If users get different certificates for different systems, users can import these certificates into the systems accordingly. However, systems require all of these certificates to identify trusted systems before establishing a IPsec VPN connection. Take the following two systems as an example: System A has certificate-1 (.p12) and System B has certificate-2 (.p12). To establish an IPsec VPN connection, System A and B have to exchange certificates (.crt) with each other. Next, Systems A and B need to install certificates (.crt). Refer to the instructions in the diagram below to learn how to install certificates and build an IPsec VPN connection.



EDR Security Router (A)

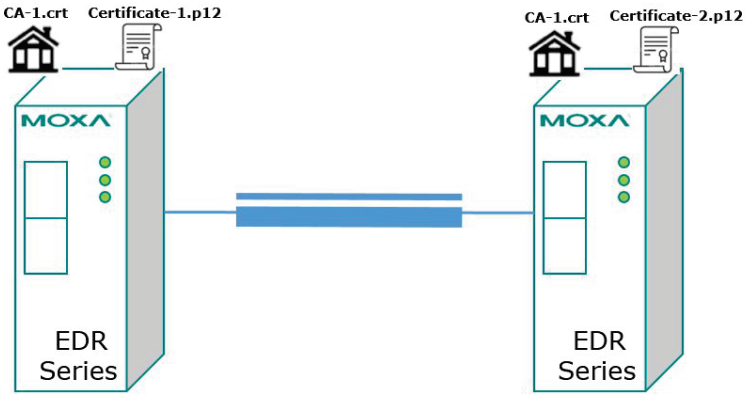
1. Import **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.
2. Import **Certificate-2.crt** file or **Certificate-2.p12** file in "Local Certificate", and label it a number. Here take No.2 as an example.
3. Enter "IPSec setting", and in "Advanced Setting", select X.509 authentication mode.
4. In "Local", select No.1
5. In "Remote", select No.2

EDR Security Router (B)

1. Import **Certificate-2.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.
2. Import **Certificate-1.crt** file or **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.2 as an example.
3. Enter "IPSec setting", and in "Advanced Setting", select X.509 authentication mode.
4. In "Local", select No.2
5. In "Remote", select No.1

Scenario 3: X.509 with CA Mode-One CA

In X.509 mode, users have to install all certificates in all systems. To simplify this process, users can obtain the certificate from the CA (Certificate Authority). When using certificates from the CA, each system needs to install the same CA (.crt) to allow each system to identify different certificates from different systems. Every certificate must be issued by the same CA. Refer to the instructions in the diagram below to learn how to install the CA and build an IPsec VPN connection.



EDR Security Router (A)

1. Import **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.

2. Import **CA-1.crt** file in "Trusted CA Certificate".

3. Enter "IPSec setting", and in "Advanced Setting", select X.509 With CA authentication mode.

4. In "Local", select No.1

EDR Security Router (B)

1. Import **Certificate-2.p12** file in "Local Certificate", and label it a number. Here take No.2 as an example.

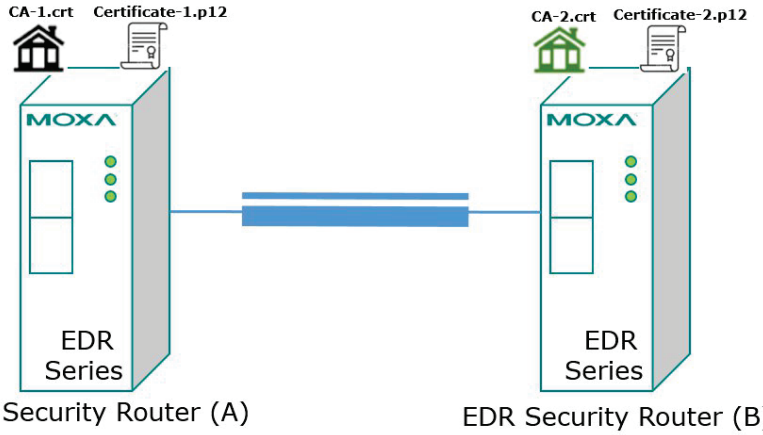
2. Import **CA-1.crt** file in "Trusted CA Certificate".

3. Enter "IPSec setting", and in "Advanced Setting", select X.509 With CA authentication mode.

4. In "Local", select No.2

Scenario 4: X.509 with CA Mode-Two CAs

In some large-scale systems, users may find it difficult to get certificates from one CA and therefore need to get certificates from different CAs. This scenario applies to the X.509 CA mode. Users have to install all CAs (.crt) into all systems to enable every system to recognize certificates from different CAs and subsequently allow identification of all the different systems. Refer to the instructions in the diagram below to learn how to install the CA (.crt) and certificates (.p12) to build an IPsec VPN or OpenVPN connection.



EDR Security Router (A)

1. Import **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.

2. Import **Import CA-1.crt file and CA-2.crt file** in "Trusted CA Certificate".

3. Enter "IPSec setting", and in "Advanced Setting", select X.509 With CA authentication mode.

4. In "Local", select No.1

EDR Security Router (B)

1. Import **Certificate-2.p12** file in "Local Certificate", and label it a number. Here take No.2 as an example.

2. **Import CA-1.crt file and CA-2.crt file** in "Trusted CA Certificate".

3. Enter "IPSec setting", and in "Advanced Setting", select X.509 With CA authentication mode.

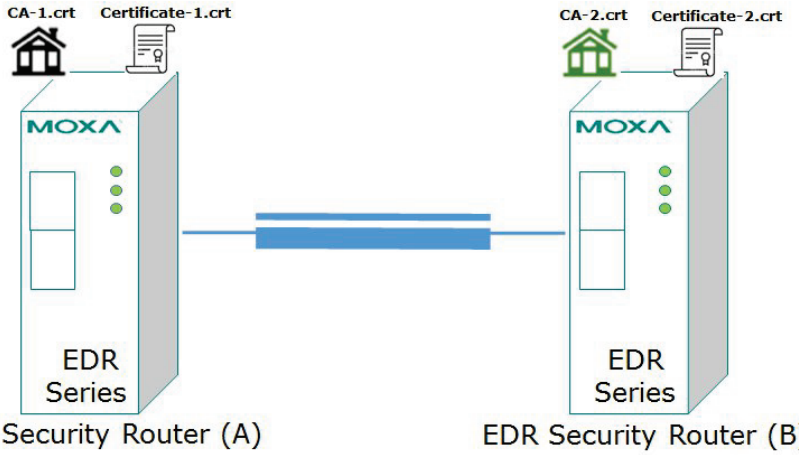
4. In "Local", select No.2

Scenario 5: X.509 with CA Mode-Certificate from CSR

For the previous four user scenarios, even when systems use certificates to identify each other before establishing a VPN connection, there is still a risk that someone can steal the certificate and pretend to be part of the trusted system.

The Certificate Signing Request (CSR) function in X.509 with CA mode is designed to minimize this risk. CSR is a request issued by a single system for certificates issued by the CA. Through CSR, the certificate belongs only to one system and cannot be installed on other systems. By following this method, CSR significantly reduces the risk of certificates being used illegitimately.

Consider the following example using System A and System B. The CSR working model is System A or B issues a CSR (.csr) to the CA and then the CA updates the system with the certificate (.crt) and the CA file (.crt). Next, System A or B updates the other system with the CA file (.crt). System A or B installs certificates and the CA file in the system in order to establish a VPN connection. Refer to the instructions in the diagram below to learn how to install the CA (.crt) and certificates (.crt) to build an IPsec VPN or OpenVPN connection.



EDR Security Router (A)

1. Generate Key in "Key Pair Generate", and give it a name. Here take One as an example.
2. Generate CSR in "CSR Generate". Select One in "Private Key". Name this CSR in "Common Name". Here name this CSR as Certificate-1 as an example.
3. Export **Certificate-1.csr** file and send it to CA-1.
4. Download **Certificate-1.crt** and **CA-1.crt** from CA-1.
5. Import **Certificate-1.crt** file in "Local Certificate. In "Import Identity Certificate" select "Certificate From CSR". In "CSR Common Name" select **Certificate-1.csr**.
6. Import **CA-2.crt** file in "Trusted CA Certificate.
7. Enter "IPSec setting", and in "Advanced Setting", select X.509 With CA authentication mode.
8. In "Local", select No.1

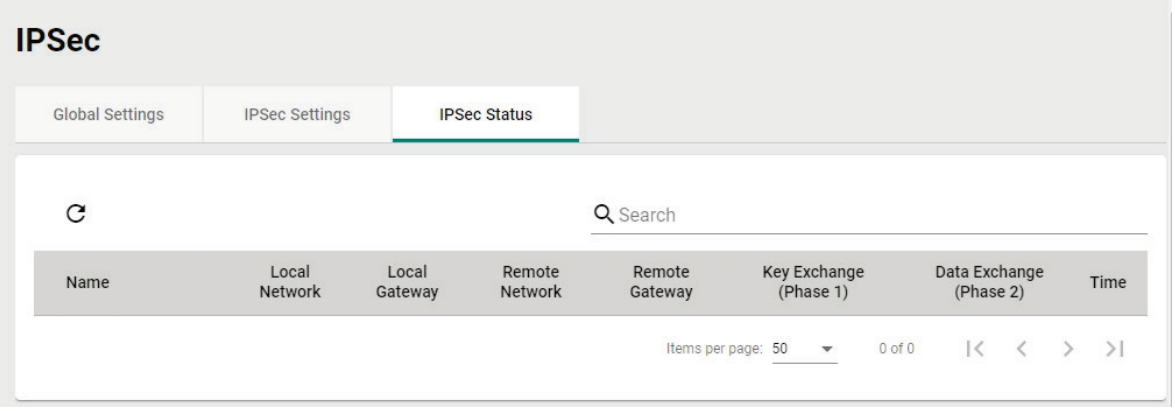
EDR Security Router (B)

1. Generate Key in "Key Pair Generate", and give it a name. Here take Two as an example.
2. Generate CSR in "CSR Generate". Select Two in "Private Key". Name this CSR in "Common Name". Here name this CSR as Certificate-2 as an example.
3. Export **Certificate-2.csr** file and send it to CA-2.
4. Download **Certificate-2.crt** and **CA-2.crt** from CA-1.
5. Import **Certificate-2.crt** file in "Local Certificate. In "Import Identity Certificate" select "Certificate From CSR". In "CSR Common Name" select **Certificate-2.csr**.
6. Import **CA-1.crt** file in "Trusted CA Certificate.
7. Enter "IPSec setting", and in "Advanced Setting", select X.509 With CA authentication mode.
8. In "Local", select No.2

IPsec Status

From the **IPsec Status** table, users can check the VPN tunnel status.

This list shows the name of the IPsec tunnel, the IP address of the Local and Remote Network/Gateway, and the status of the Key Exchange and Data Exchange phases.

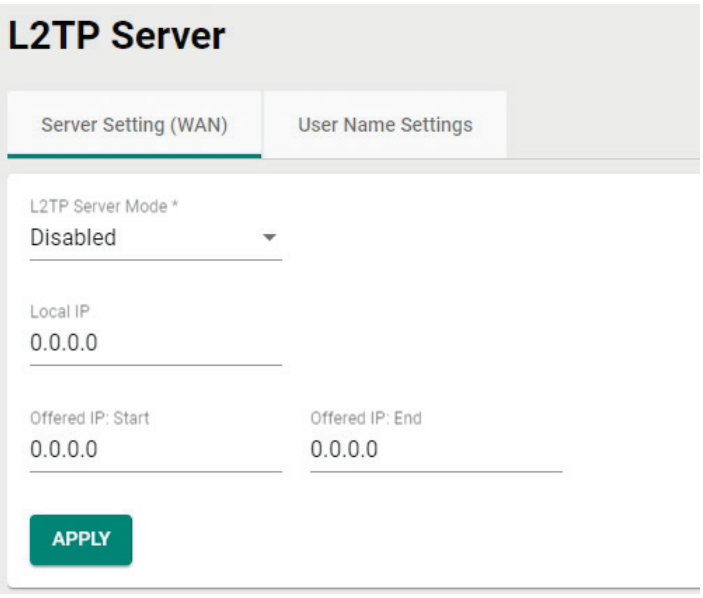


Click the icon to refresh the information.

L2TP Server (Layer 2 Tunnel Protocol)

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.

L2TP Server Setting (WAN)



The Industrial Secure Router supports up to 10 accounts with different usernames and passwords.

L2TP Server Mode

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the L2TP function on the WAN1 or WAN2 interface.	Disabled

Local IP

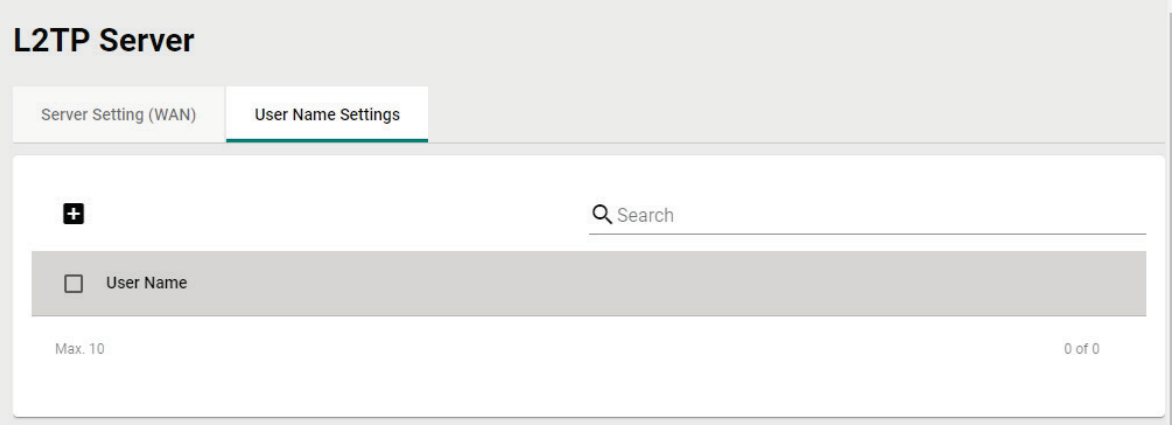
Setting	Description	Factory Default
IP Address	Specify the IP address of the local subnet.	0.0.0.0

Offered IP: Start/Offered IP: End

Setting	Description	Factory Default
IP Address	Specify the starting and ending IP address of the Offered IP range, used for L2TP clients.	0.0.0.0

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

L2TP User Name Settings



Create a New Account for L2TP

Click the ➕ icon to create a new L2TP account.

Username

Setting	Description	Factory Default
Max. 32 characters.	Enter a username for the L2TP connection.	None

New Password

Setting	Description	Factory Default
Max. 32 characters.	Enter the password for the L2TP connection.	None

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

Modify an Existing L2TP Account

Select the item in the L2TP Account List and click the ✎ icon next to the entry you want to modify. When finished, click **APPLY** to save your changes.

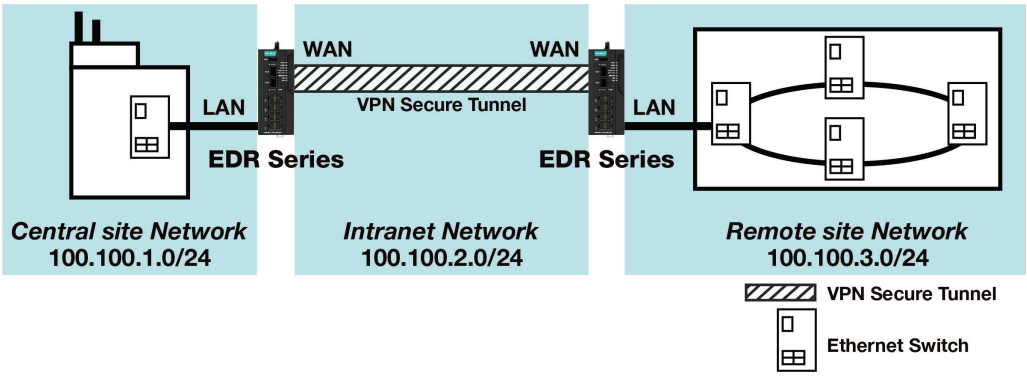
Delete an Existing L2TP Account

Select the item(s) in the L2TP Account List. Click the icon and click **DELETE** to delete the item(s).

Examples of Typical VPN Applications

Site-to-site IPsec VPN tunnel with Pre-Shared Key

The following example shows how to create a secure LAN-to-LAN VPN tunnel between a Central and Remote site via an intranet network.



VPN Plan

- All communication from the Central site network (100.100.1.0/24) to the Remote site Network (100.100.3.0/24) needs to pass through the VPN tunnel.
- The Intranet Network is 100.100.2.0/24.
- The configuration of the WAN/LAN interface for the 2 Industrial Secure Routers is shown in the following table.

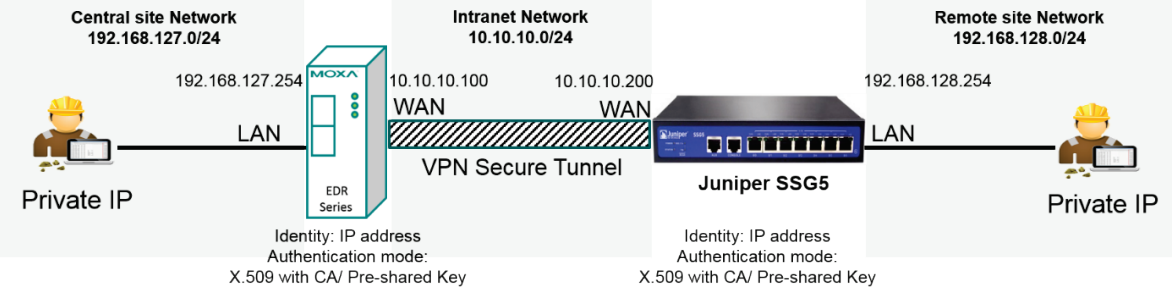
	Configuration	Industrial Secure Router (1)	Industrial Secure Router (2)
Interface Setting	WAN IP	100.100.2.1	100.100.2.2
	LAN IP	100.100.1.1	100.100.3.1

Based on the requirements and VPN plan, the recommended configuration for the IPsec VPN connection is shown in the following table:

	Configuration	Industrial Secure Router (1)	Industrial Secure Router (2)
Tunnel Setting	Connection Type	Site to Site	Site to Site
	Remote VPN gateway	100.100.2.2	100.100.2.1
	Startup mode	Wait for Connection	Start in Initial
	Local Network/ Netmask	100.100.1.0/ 255.255.255.0	100.100.3.0/ 25.255.255.0
	Remote Network/ Netmask	100.100.3.0/ 25.255.255.0	100.100.1.0/ 255.255.255.0
Key Exchange	Pre-Shared Key	12345	12345
Data Exchange	Encryption/Harsh	3DES/SHA-1	3DES/SHA-1

Site-to-site IPsec VPN tunnel with Juniper systems

In this example, in order to establish a VPN tunnel, the central site router and remote site router have to know the identity of each other and use the same authentication mechanism to verify each other. Here we use a Juniper SSG5 as an example to elaborate how the Industrial Secure Router can build an IPsec VPN connection with Juniper systems.



VPN Plan

- All communication from the Central site network (192.168.127.0/24) to the Remote site Network (192.168.128.0/24) needs to pass through the VPN tunnel.
- The Intranet Network is 10.10.10.0/24.
- The configuration of the WAN/LAN interface for the Industrial Secure Routers and Juniper SSG5 is shown in the following table.

	Configuration	EDR Series	Juniper SSG5
Router Setting	WAN IP	10.10.10.100	10.10.10.200
	LAN IP	192.168.127.254	192.168.128.254

Based on the requirements and VPN plan, the recommended configuration for the IPsec VPN connection is shown in the following table:

	Configuration	EDR Series	Juniper SSG5
Tunnel Setting	Connection Type	Site to Site	Site to Site
	Remote VPN gateway	10.10.10.200	10.10.10.100
	Startup mode	Wait for Connection	Start in Initial
	Local Network/ Netmask	192.168.127.0/ 255.255.255.0	192.168.128.0/ 25.255.255.0
	Remote Network/ Netmask	192.168.128.0/ 25.255.255.0	192.168.127.0/ 255.255.255.0
	Identity	IP address Local ID: 10.10.10.100 Remote ID: 10.10.10.200	IP address Local ID: 10.10.10.200 Remote ID: 10.10.10.100
Key Exchange	Authentication mode	Pre-Shared Key or X.509 with CA	Pre-Shared Key or X.509 with CA
Data Exchange	Encryption / Harsh	3DES/SHA-1	3DES/SHA-1

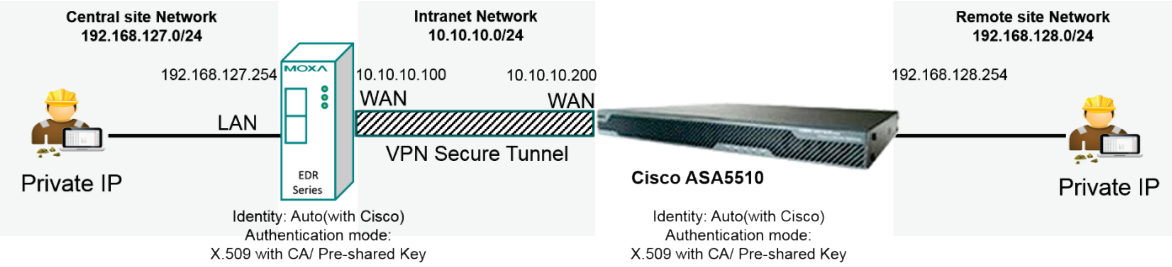
Note that to establish a VPN connection with Juniper systems, the Identity should set to "**IP Address**" and the authentication mode should set to "**Pre-Shared Key**" or "**X.509 with CA**". During the EDR Series compliance test with the Juniper SSG5, all Identity modes except "IP Address" and all authentication modes except "X.509 with CA" did not work with the Juniper SSG5. A summary of settings for VPN connections with Juniper systems is listed in the table below.

EDR Series VPN settings for compatibility with Juniper systems		Authentication mode		
		Pre-shared Key	X.509	X.509 With CA
Identity	IP Address	Supported	Not supported	Supported
	FQDN	Not supported		
	Key ID			
	Auto(with Cisco)			

Site-to-site IPsec VPN tunnel with Cisco systems

To build up a VPN tunnel, the central site router and remote site router have to know the identity of each other and use the same authentication mechanism to verify each other. Here we take Cisco's ASA5510 as example to elaborate how the Industrial Secure Router builds an IPsec VPN connection with Cisco systems.

In this example, in order to establish a VPN tunnel, the central site router and remote site router have to know the identity of each other and use the same authentication mechanism to verify each other. Here we use a Cisco ASA5510 as an example to elaborate how the Industrial Secure Router can build an IPsec VPN connection with Cisco systems.



VPN Plan

- All communication from the Central site network (192.168.127.0/24) to the Remote site Network (192.168.128.0/24) needs to pass through the VPN tunnel.
- The Intranet Network is 10.10.10.0/24
- The configuration of the WAN/LAN interface for the Industrial Secure Routers and Cisco ASA5510 is shown in the following table:

	Configuration	EDR Series	Cisco ASA5510
Router Setting	WAN IP	10.10.10.100	10.10.10.200
	LAN IP	192.168.127.254	192.168.128.254

Based on the requirements and VPN plan, the recommended configuration for the IPsec VPN connection is shown in the following table:

	Configuration	EDR Series	Cisco ASA5510
Tunnel Setting	Connection Type	Site to Site	Site to Site
	Remote VPN gateway	10.10.10.200	10.10.10.100
	Startup mode	Wait for Connection	Start in Initial
	Local Network / Netmask	192.168.127.0/ 255.255.255.0	192.168.128.0/ 25.255.255.0
	Remote Network / Netmask	192.168.128.0/ 25.255.255.0	192.168.127.0/ 255.255.255.0
	Identity	Auto(with Cisco)	
Key Exchange	Authentication mode	Pre-Shared Key or X.509 With CA	Pre-Shared Key or X.509 With CA
Data Exchange	Encryption/Harsh	3DES/SHA-1	3DES/SHA-1

Note that when establishing a VPN connection with Cisco systems, all authentication modes except "**X.509**" are supported.

When using Pre-shared Key authentication, the Identity can be set to "**IP Address**", "**FQDN**", "**Key ID**", or "**Auto (with Cisco)**". When using X.509 with CA authentication, the Identity must be set to "**Auto (with Cisco)**".

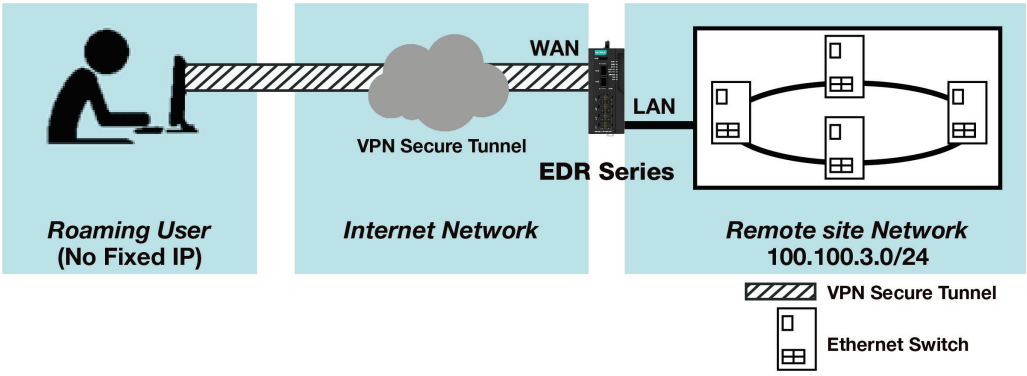
To simplify the VPN configuration, the Industrial Secure Router supports an identity called **"Auto(with Cisco)"** which can be used alongside Pre-shared Key and X.509 with CA authentication.

A summary of settings for VPN connections with Cisco systems is listed in the table below.

EDR Series VPN Settings for compatibility with Cisco systems		Authentication mode		
		Pre-shared Key	X.509	X.509 With CA
Identity	IP Address	Supported	Not supported	Not supported
	FQDN	Supported		
	Key ID	Supported		
	Auto(with Cisco)	Supported		Supported

L2TP for Remote User Maintenance

The following example shows how roaming users can use L2TP over IPsec to connect to the remote site network.



VPN Plan

- All communication from the Roaming user (no fixed IP) to the Remote site Network (100.100.3.0/24) needs to pass through the VPN tunnel.
- Communication goes through the Internet.
- The configuration of the WAN/LAN interface for the Industrial Secure Router is shown in the following table.

	Configuration	Industrial Secure Router (1)
Interface Setting	WAN IP	100.100.2.1
	LAN IP	100.100.3.1

Based on the requirements and VPN plan, the recommended configuration for the IPsec VPN connection is shown in the following table:

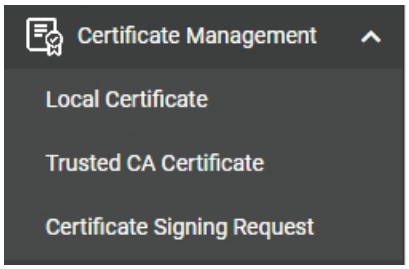
	Configuration	Industrial Secure Router (1)
L2TP Server Setting	L2TP Server Mode (WAN1)	Enable
	Local IP (L2TP Server IP)	100.100.4.1
	Offer IP Range	100.100.4.1 ~ 100.100.4.100
	Login User/Password	User01/12345
Tunnel Setting	Connection Type	Site to Site(Any)
	L2TP Tunnel	Enable
	Local Network	100.100.3.1/24 (Same as LAN Interface)
	Startup mode	Wait for Connection
Key Exchange	Pre-Shared Key	12345
Data Exchange	Encryption Algorithm Harsh Algorithm	3DES SHA-1

13. Certificate Management

For the purposes of this document, certificate management refers to the X.509 SSL certificate. X.509 is a digital certificate method commonly used for IPsec, OpenVPN, and HTTPS authentication. The Industrial Secure Router can act as a Root CA (Certificate Authority) and issue a trusted Root Certificate. Alternatively, users can import certificates from other CAs into the Industrial Secure Router.

Certificates are a time-based form of authentication. Before processing certificates, please ensure that the industrial secure router is synced with the local device. For more information about syncing device time, please refer to the Time section.

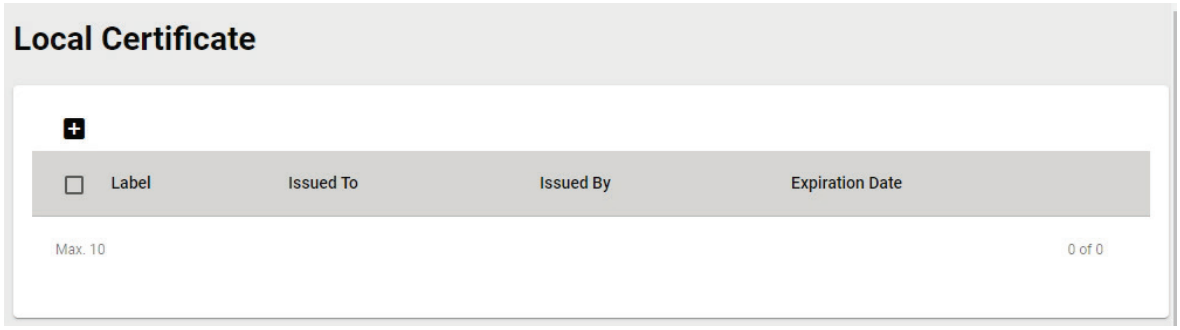
From the **Certificate Management** section, you can configure **Local Certificate, Trusted CA Certificate,** and **Certificate Signing Request** settings.



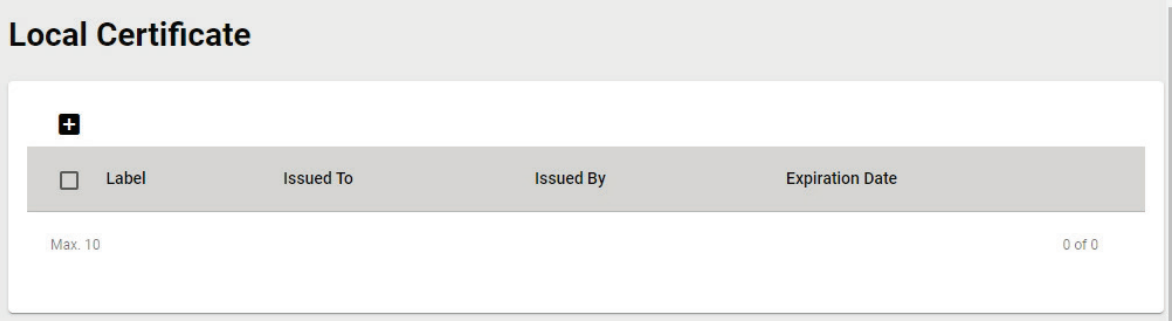
Local Certificate

From the **Local Certificates** screen, users can import certificates issued by the CA into the Industrial Secure Router.

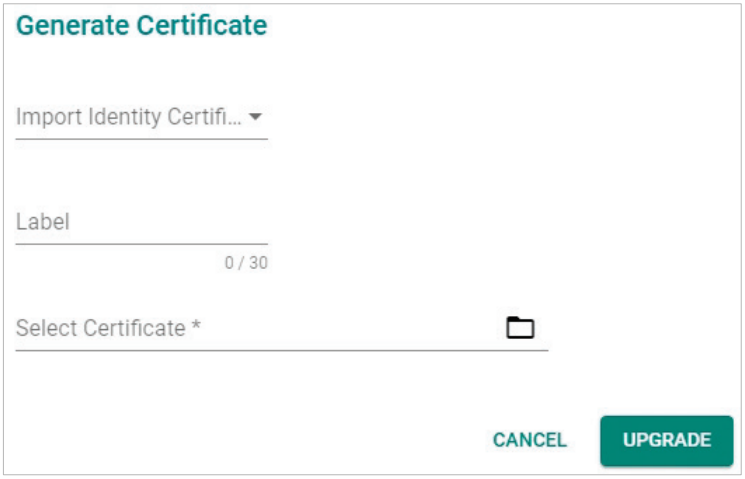
Depending on the selected certificate, some settings may differ. Refer to the following sections:
Import a Certificate
Import a Certificate From CSR
Import a Certificate from PKCS#12



Import a Certificate



Click the ⊞ icon to add a certificate.



Import Identity Certificate

Setting	Description	Factory Default
Certificate, Certificate from CSR, Certificate from PKCS#12	Select Certificate as the certificate type.	Certificate

Label

Setting	Description	Factory Default
0 to 30	Specify the certification number.	None

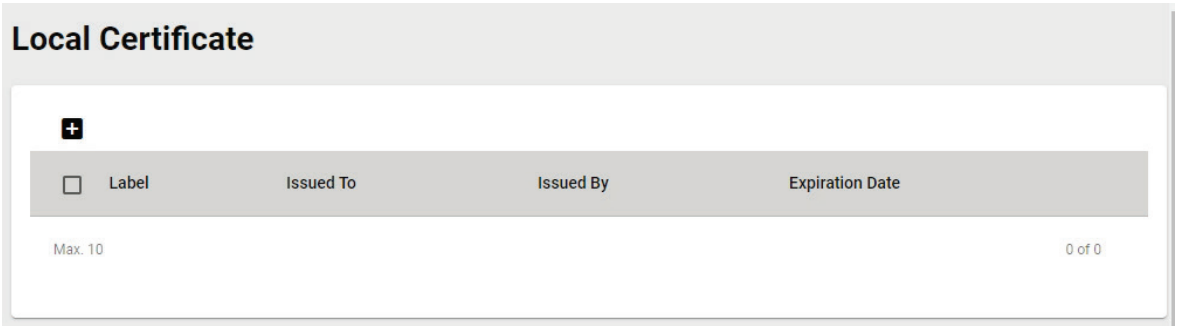
Select Certificate

Setting	Description	Factory Default
Click the 🗀 icon to select a certificate file	Upload a certificate from the local computer. **Certificat**e uses the .crt file extension. **Certificate from CSR** is a certificate issued by another CA. **Certificate from PKCS#12** uses the .p12 file extension.	None

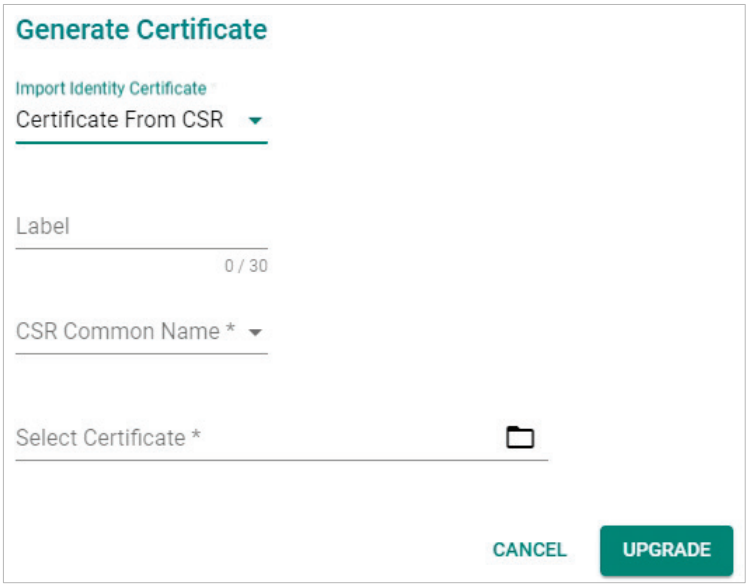
When finished, click **UPGRADE** to import the selected certificate.

Import a Certificate From CSR

When importing a Certificate From CSR, you must browse to the certificate file before selecting the CSR Common Name.



Click the ⊞ icon to add a certificate.



Import Identity Certificate

Setting	Description	Factory Default
Certificate, Certificate from CSR, Certificate from PKCS#12	Select **Certificate From CSR** as the certificate type.	Certificate

Label

Setting	Description	Factory Default
0 to 30	Specify the certification number.	None

CSR Common Name

Setting	Description	Factory Default
Domain name	Select the CSR Common Name. This is the domain name the certificate will apply to.	None

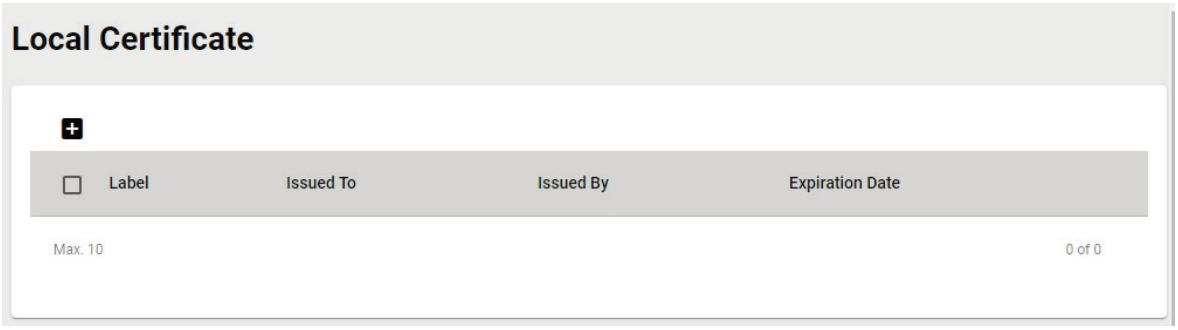
Select Certificate

Setting	Description	Factory Default
Click the 🗀 icon to select a certificate file	Upload a certificate from the local computer. **Certificate** uses the .crt file extension. **Certificate from CSR** is a certificate issued by another CA. **Certificate from PKCS#12** uses the .p12 file extension.	None

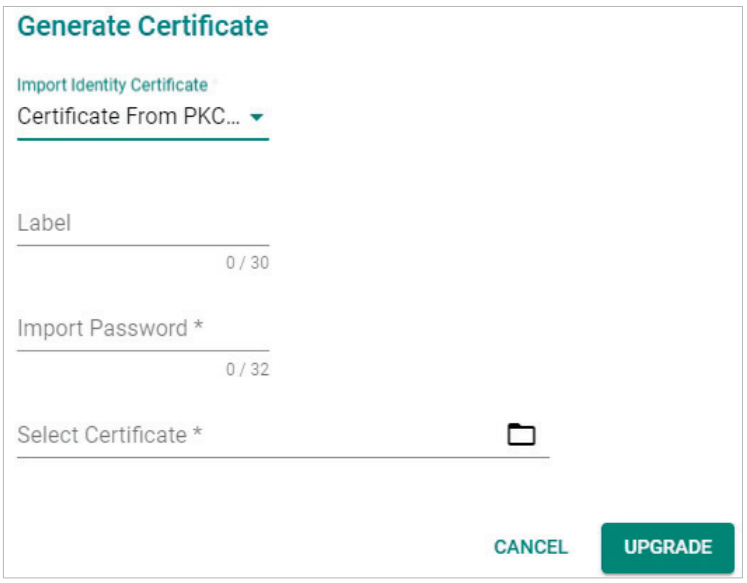
When finished, click **UPGRADE** to import the selected certificate.

Import a Certificate from PKCS#12

When importing the Certificate from PKCS#12, you must browse to the certificate file before entering the Import Password.



Click the ⊞ icon to add a certificate.



Import Identity Certificate

Setting	Description	Factory Default
Certificate, Certificate from CSR, Certificate from PKCS#12	Select **Certificate From PKCS#12** as the certificate type.	Certificate

Label

Setting	Description	Factory Default
0 to 30	Specify the certification number.	None

Import Password

Setting	Description	Factory Default
Max. 32 characters	Enter the import password.	None

Select Certificate

Setting	Description	Factory Default
Click the 🗀 icon to select a certificate file	Upload a certificate from the local computer. **Certificate** uses the .crt file extension. **Certificate from CSR** is a certificate issued by another CA. **Certificate from PKCS#12** uses the .p12 file extension.	None

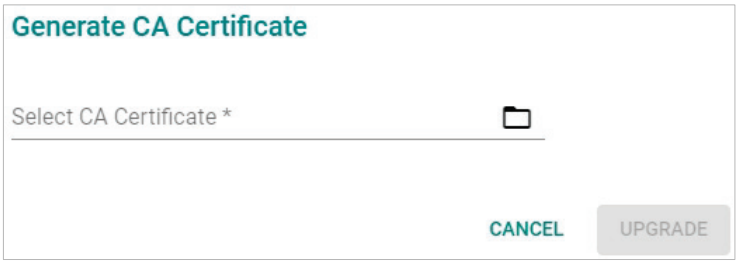
When finished, click **UPGRADE** to import the selected certificate.

Trusted CA Certificate

Import a CA Certificate

From the **Trusted CA Certificate** screen, users can import a trusted CA into the Industrial Secure Router. It is recommended that the user imports a trusted CA in advance. Otherwise, the Industrial Secure Router may not recognize the certificate and reject the connection.

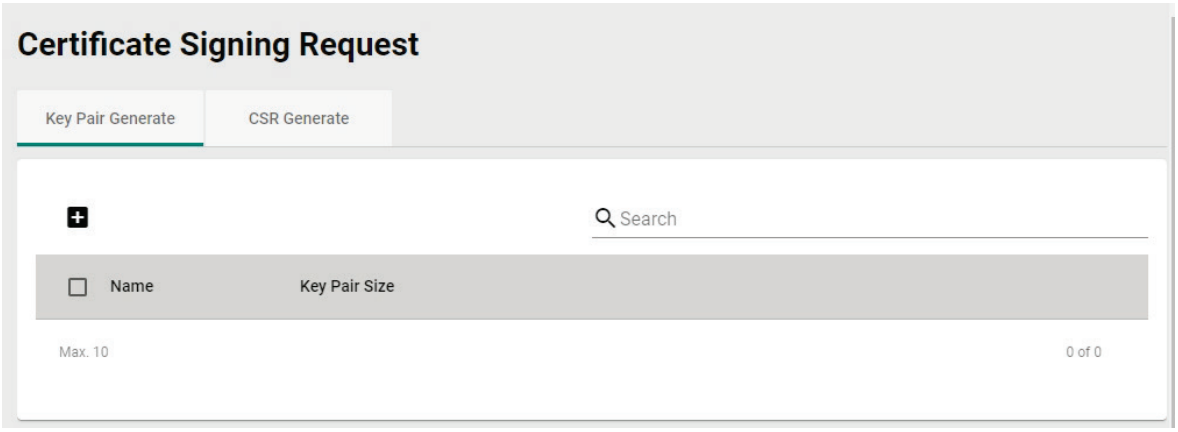
Click the icon to add a CA Certificate.



Click the icon to select a CA certificate file, then click **UPGRADE** to import the certificate.

Certificate Signing Request

From the Certificate Signing Request screen, users can generate key pairs and the CSR.



To get a certificate from the CA for connection purposes, users must follow the two-step process below.

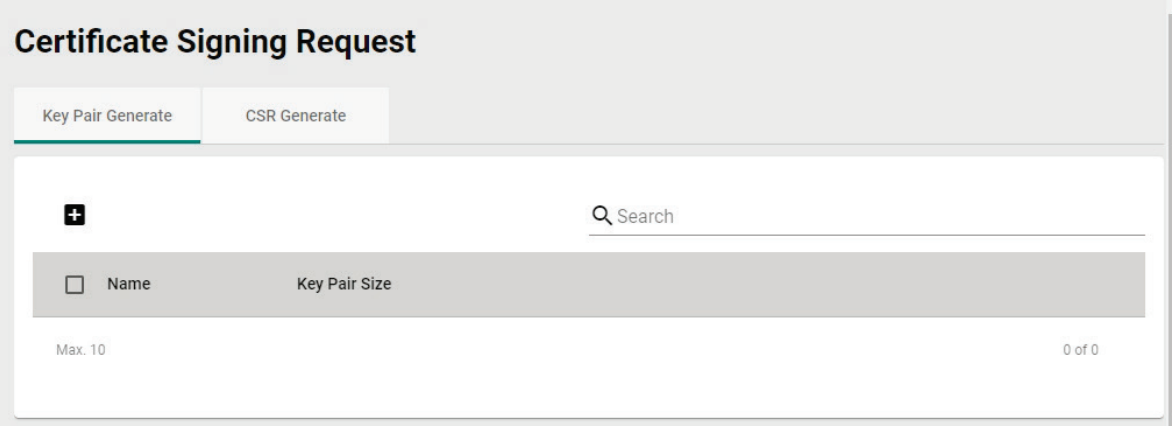
Step 1: Generate a Private Key

Step 2: Generate the CSR

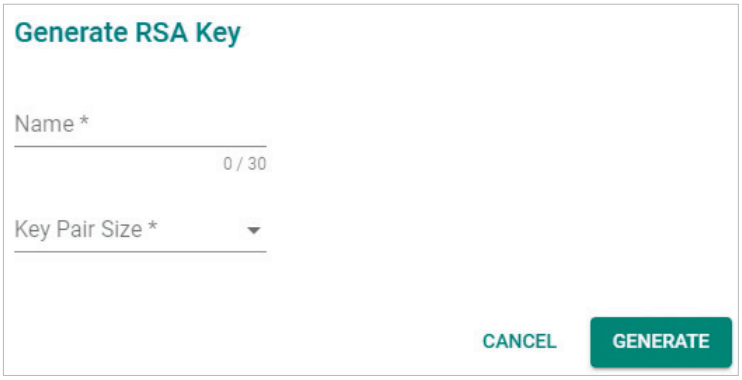
Key Pair Generate

Step 1: Generate a Private Key

Before sending the Certificate Signing Request (CSR) to the CA, the CSR must include a public key that can be generated together with a private key. The user can use the private key to encrypt data while the receiver can use the public key to decrypt the data.



Click the ⊞ icon to generate a RSA key.



Name

Setting	Description	Factory Default
0 to 30 characters	Enter a name for the RSA key.	None

Key Pair Size

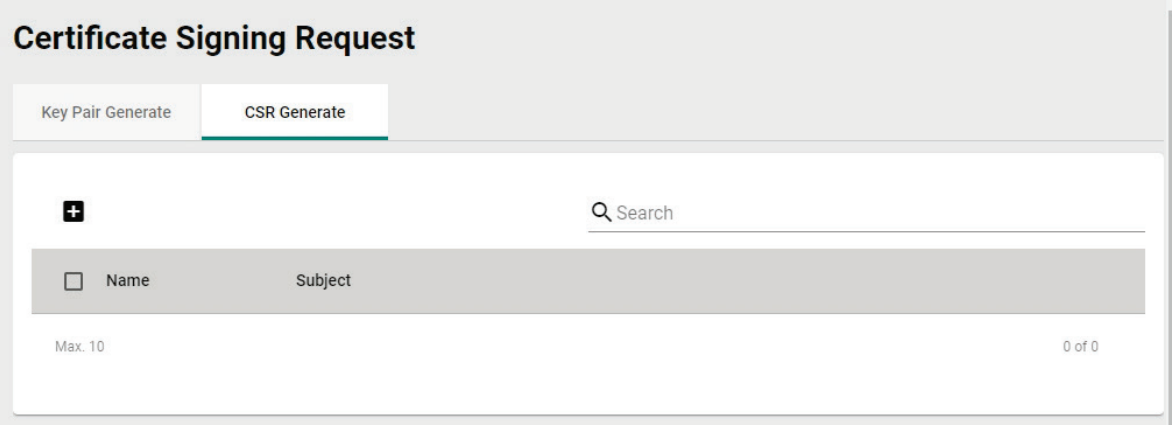
Setting	Description	Factory Default
1024 Bit or 2048 Bit	Select the key pair size of each private key.	None

When finished, click **GENERATE** to generate the RSA key.

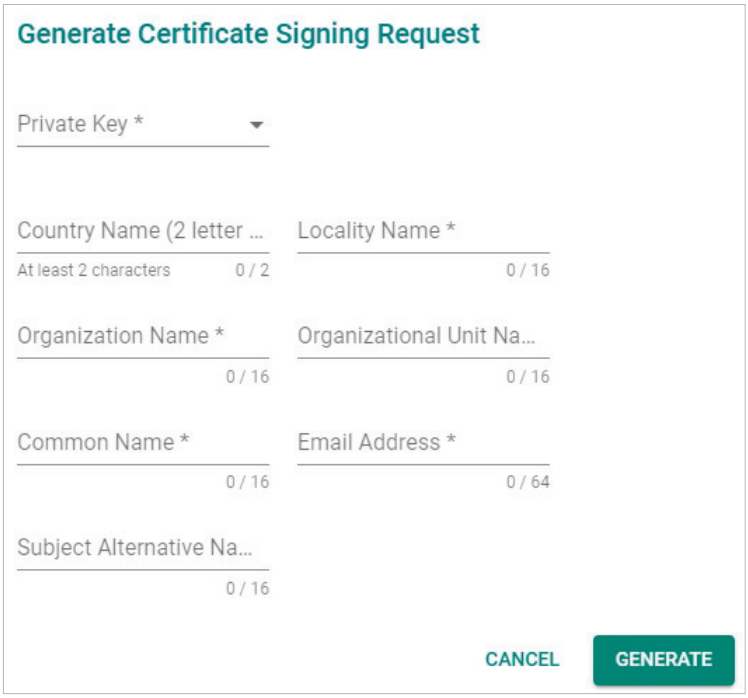
To delete the RSA key, select the RSA key in the RSA key List and click the 🗑 icon, then click **DELETE** to delete the RSA key.

CSR Generate

Step 2: Generate the CSR



After generating the private key, click the + icon to generate the CSR.



Private Key

Setting	Description	Factory Default
Private Key	Select the private key generated on the Key Pair Generate tab. If you have not generated a private key yet, refer to Step 1: Generate a Private Key.	None

Country Name (2 letter code)

Setting	Description	Factory Default
At least 2 characters	Enter the country code for the CSR.	None

Locality Name

Setting	Description	Factory Default
Max. 16 characters	Enter the locality name for the CSR.	None

Organization Name

Setting	Description	Factory Default
Max. 16 characters	Enter the organization name for the CSR.	None

Organization Unit Name

Setting	Description	Factory Default
Max. 16 characters	Enter the organization unit name for the CSR.	None

Common Name

Setting	Description	Factory Default
Max. 16 characters	Enter the common name for the CSR.	None

Email Address

Setting	Description	Factory Default
Max. 64 characters	Enter the email address for the CSR.	None

Subject Alternative Name

Setting	Description	Factory Default
Max. 16 characters	Enter the subject alternative name for the CSR.	None

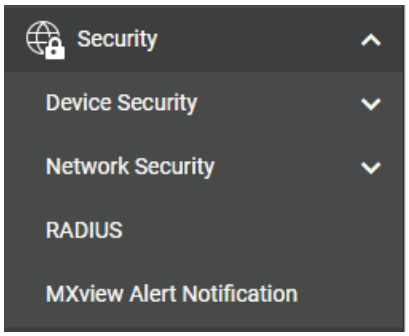
When finished, click **GENERATE** to generate the CSR.

To export the CSR, select the CSR in Certificate List and click the icon.

To delete the CSR, select the CSR in Certificate List and click the icon, then click **DELETE** to delete the CSR.

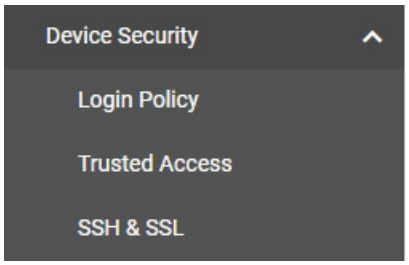
14. Security

From the **Security** section, you can configure **Device Security**, **Network Security**, **RADIUS**, and **MXview Alert Notification** settings.

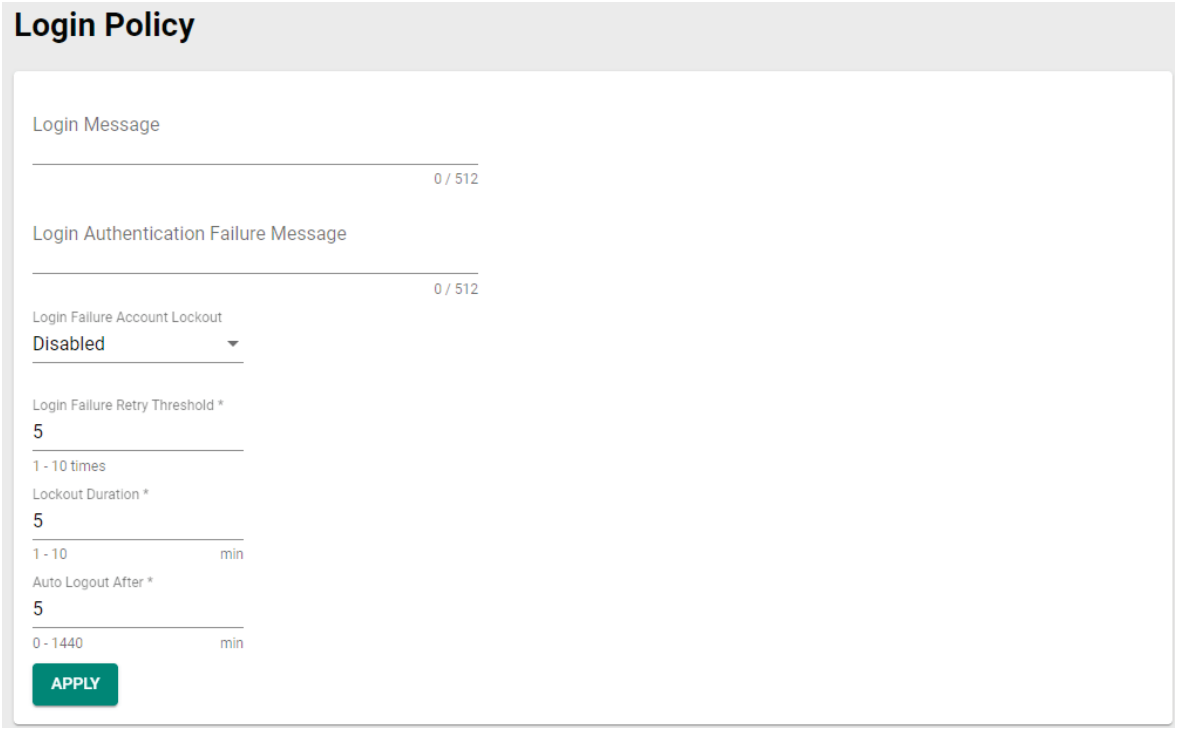


Device Security

From the **Device Security** section, the following functions can be configured: **Login Policy**, **Trusted Access**, and **SSH & SSL**.



Login Policy



Login Message

Setting	Description	Factory Default
Max. 512 characters	Enter a welcome message that will appear when users log in to the device.	None

Login Authentication Failure Message

Setting	Description	Factory Default
Max. 512 characters	Enter the message that will appear if the user failed to log in.	None

Login Failure Account Lockout

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the lockout function which will temporarily prevent users from logging in after several failed login attempts.	Disabled

Login Failure Retry Threshold

Setting	Description	Factory Default
1 to 10 times	Specify the number of login retry attempts before the user is locked out.	5

Lockout Duration

Setting	Description	Factory Default
1 to 10 minutes	Specify the lockout duration (in minutes). During this time, the locked-out user will be unable to log in.	5

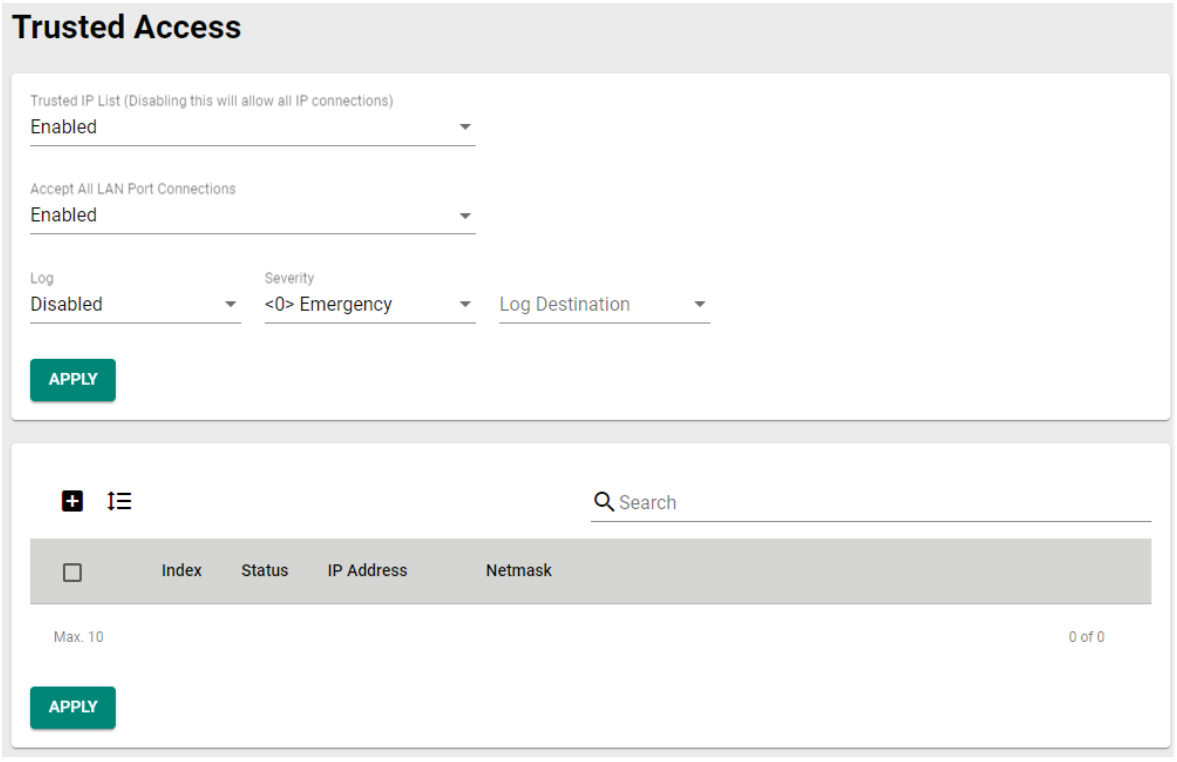
Auto Logout After

Setting	Description	Factory Default
Max. 1440 minutes	When the user is idle for the specified duration, the user will be automatically logged out from the device. The default duration is 5 minutes.	5

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

Trusted Access

The EDR-G9010 Series uses an IP address-based filtering method to control access to the device.



Trusted IP List

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the Trusted IP list. If enabled, only IP addresses in the Trusted IP table can access the device. Refer Create a Trusted Access Entry for more information. If this option is disabled, any IP address can access the device.	Enabled

Accept All LAN Port Connections

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the device to accept all connections on the LAN interface.	Enabled

Log

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable Trusted Access event logs.	Disabled

Severity

Setting	Description	Factory Default
<0> Emergency <1> Alert <2> Critical <3> Error <4> Warning <5> Notice <6> Informational <7> Debug	Select the severity of the Trusted Access event.	<0> Emergency

Log Destination

Setting	Description	Factory Default
Local Storage, Syslog, Trap	If Log is enabled, select the Trusted Access event log storage location.	None

Create a Trusted Access Entry

You can control which IP addresses can have access to the Moxa Industrial Secure Router by adding them to the Trusted Access list. If enabled, only addresses on the list will be allowed access to the Moxa Industrial Secure Router.

Click ⊞ to add an IP address to the Trusted Access list.

Each IP address and netmask entry can be tailored to different situations:

- **Grant access to one host with a specific IP address**
  For example, enter IP address 192.168.1.1 with netmask 255.255.255.255 to allow access to 192.168.1.1 only.
- **Grant access to any host on a specific subnetwork**
  For example, enter IP address 192.168.1.0 with netmask 255.255.255.0 to allow access to all IPs on the subnet defined by this IP address/Netmask combination.
- **Grant access to all hosts**
  Disable the Trusted Access list. Select **Disabled** in **Trusted IP List (Disabling this will allow all IP connections)**.

The following table shows additional configuration examples:

Hosts That Need Access	Input Format
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the Trusted Access entry.	None

IP Address

Setting	Description	Factory Default
IP Address	Specify the IP address of the Trusted host(s).	None

Netmask

Setting	Description	Factory Default
Netmask	Specify the subnet mask of the Trusted host(s).	None

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

Modify a Trusted Access Entry

Click the ✎ next to the entry you want to modify. When finished, click **APPLY** to save your changes.

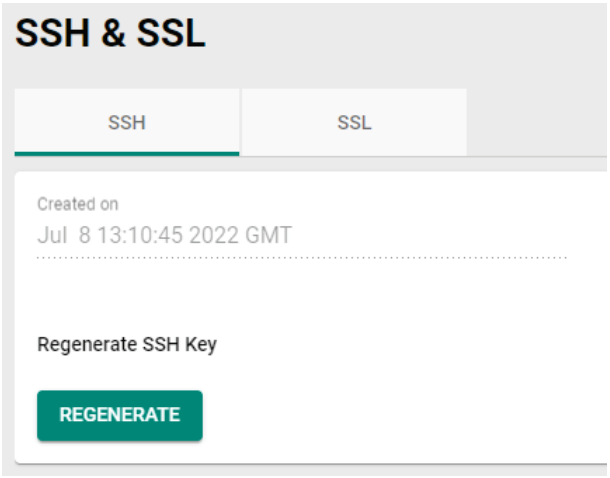
Delete a Trusted Access Entry

Select the entry from the Trusted Access List and click the icon, then click **DELETE** to delete it.

SSH & SSL

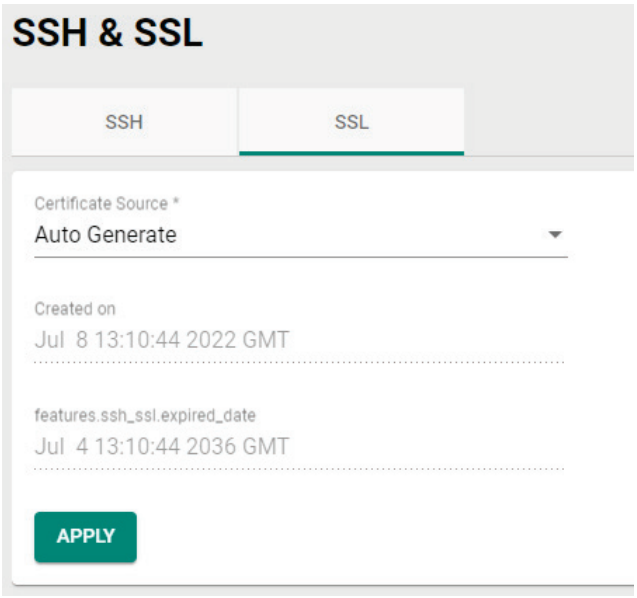
SSH

The Industrial Secure Router will generate a SSH certificate automatically by default. If not, click **REGENERATE** to regenerate the SSH host key.



SSL

On the SSL page, you can generate an SSL certificate.



Certificate Source

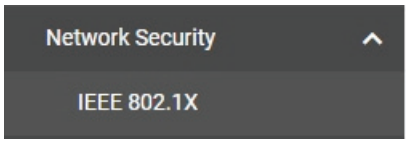
Setting	Description	Factory Default
Auto Generate	The Industrial Secure Router will generate a certificate automatically.	Auto Generate

Setting	Description	Factory Default
Local Certificate Database	Select the certificate you want to import into the Local Certificate Database. The certificate that can be loaded here is limited to "Certificate from CSR" and "Certificate From PKCS#12".	

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

Network Security

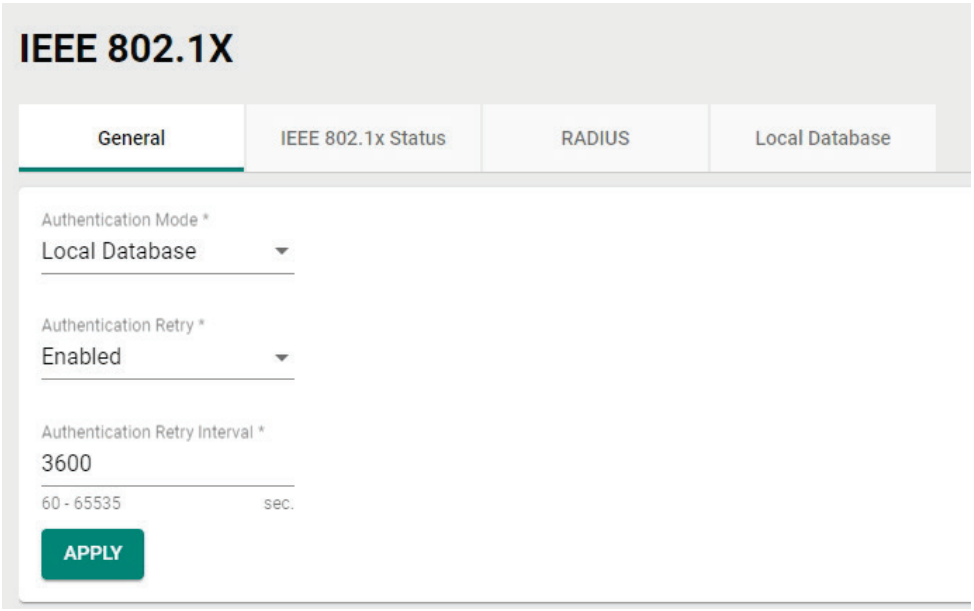
The Industrial Secure Router supports IEEE 802.1X network security authentication.



IEEE 802.1X

IEEE 802.1X provides an authentication mechanism to prevent unauthorized access to the LAN. Without this mechanism, users can access the LAN by simply physically connecting to any LAN device on the network. IEEE 802.1X enhances network security by providing a procedure to authenticate and authorize users who attempt to access the network.

General Settings



Authentication Mode

Setting	Description	Factory Default
RADIUS, Local Database, or both RADIUS, Local	Select the authentication server user account database.	Local Database

Authentication Retry

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable reauthentication.	Enabled

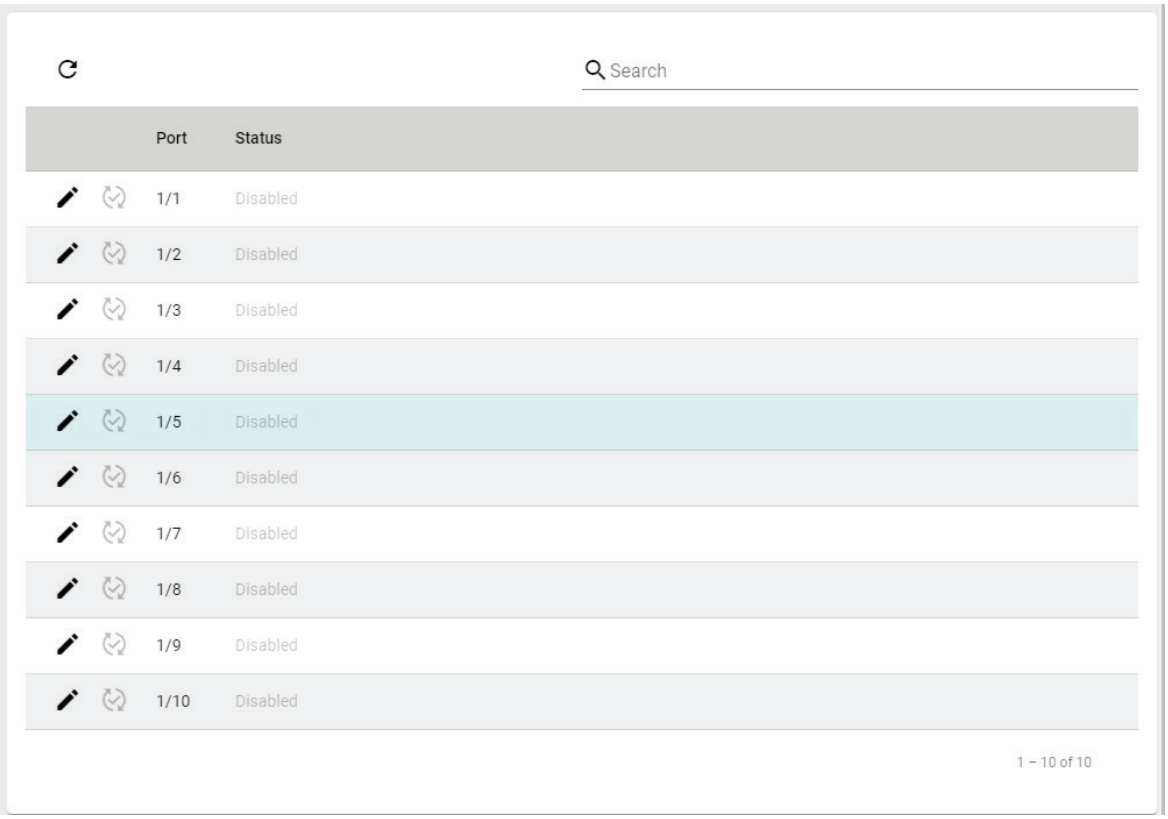
Authentication Retry Interval

Setting	Description	Factory Default
60 to 65535 seconds	If Authentication Retry is enabled, specify the authentication retry interval (in second).	3600

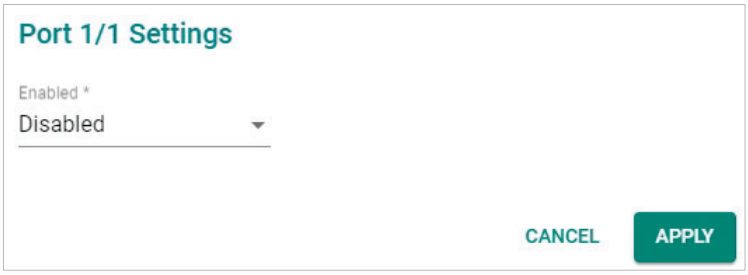
When finished, click **APPLY** to save your changes.

Modify IEEE 802.1X Port Settings

Click the icon to refresh the port status.



To configure the IEEE 802.1X settings for a specific port, click the icon next to the port.

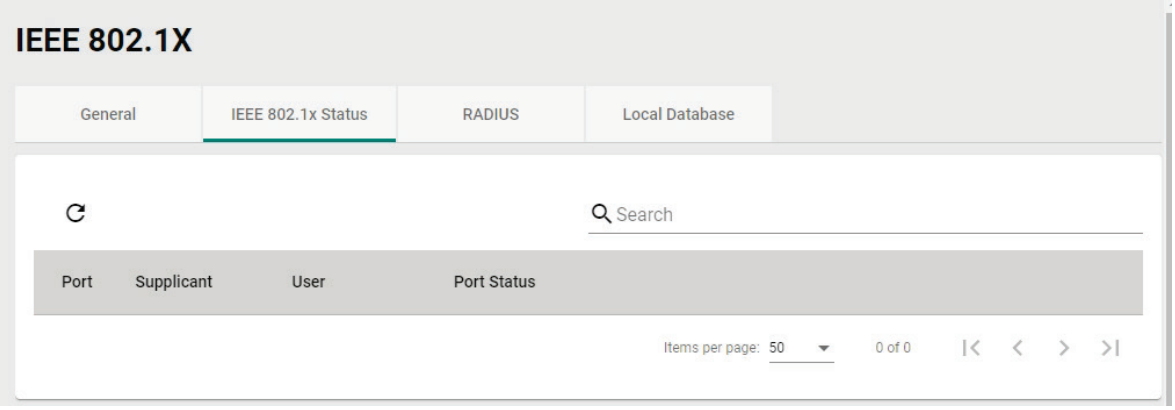


Enabled

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable IEEE 802.1X port access control for this port.	Disabled

IEEE 802.1x Status

This page shows the IEEE 802.1X status of each port, supplicant, user, and port status information.

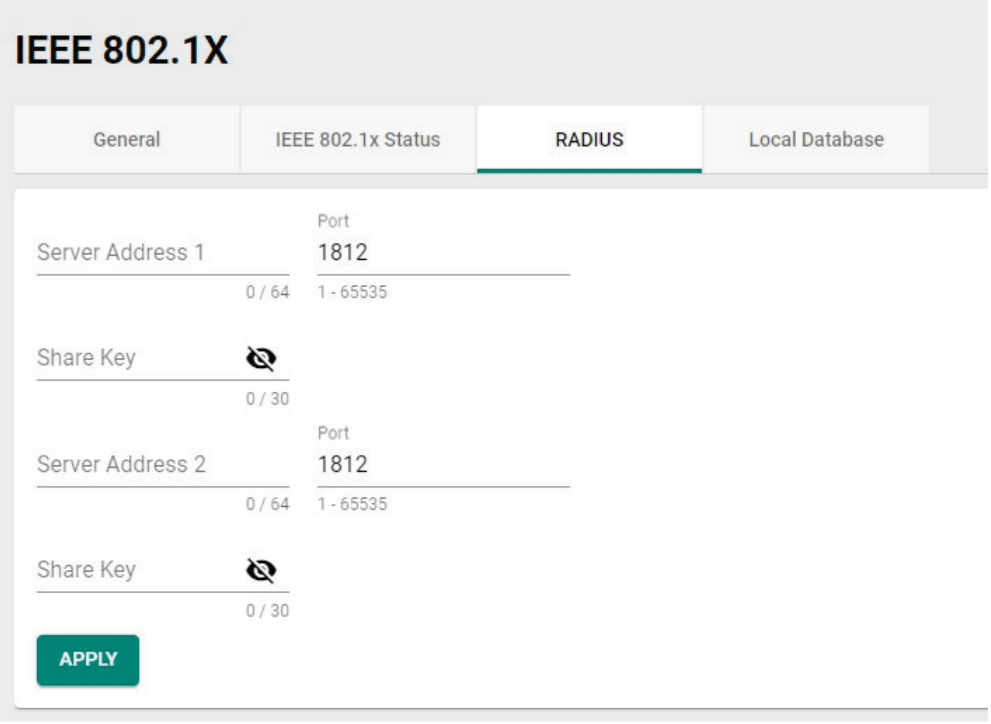


Click the icon to refresh the information.

RADIUS

RADIUS **Remote Authentication Dial in User Service** is a protocol that involves three services in one network protocol: Authentication, Authorization, and Accounting (AAA). The protocol operates on port 1812, and the AAA management for users connecting to a network service.

RADIUS is based on a client/server protocol that runs in the application layer and can use either TCP or UDP as the mode of transport. The network access servers that contain the RADIUS protocol can allow the client to communicate with the RADIUS server. Through Authentication, Authorization, and Accounting, RADIUS is used to monitor access to the network.



RADIUS Server Settings

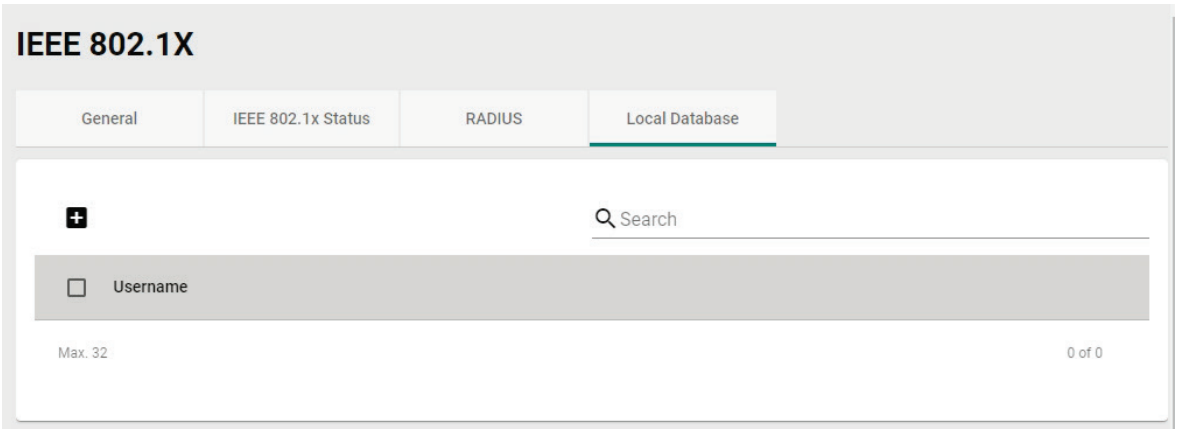
Setting	Description	Factory Default
Server Address 1/2 (0 to 64)	Specify the first and second RADIUS authentication server IP address or server name.	None
UDP Port (1 to 65535)	Specify the first and second RADIUS server port number.	1812

Setting	Description	Factory Default
Shared key (max. 60 characters)	Specify the shared key for the first and second RADIUS server.	None

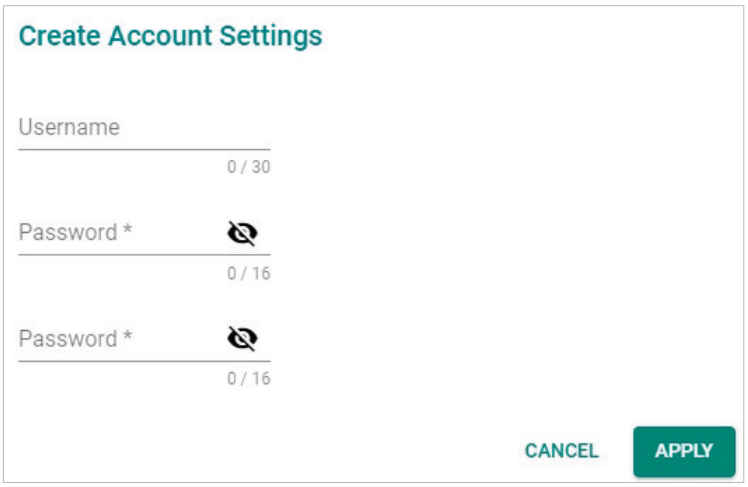
When finished, click **APPLY** to save your changes.

> **NOTE**
>
> The system will use the primary RADIUS server by default. If the primary RADIUS is unavailable, it will use the secondary RADIUS server.

Local Database



Click the ⊞ icon to create add a user account to the local database.



Username

Setting	Description	Factory Default
Max. 30 characters	Enter the username for this account.	None

Password

Setting	Description	Factory Default
Max. 16 characters	Enter the password for this user account. Confirm the password.	None

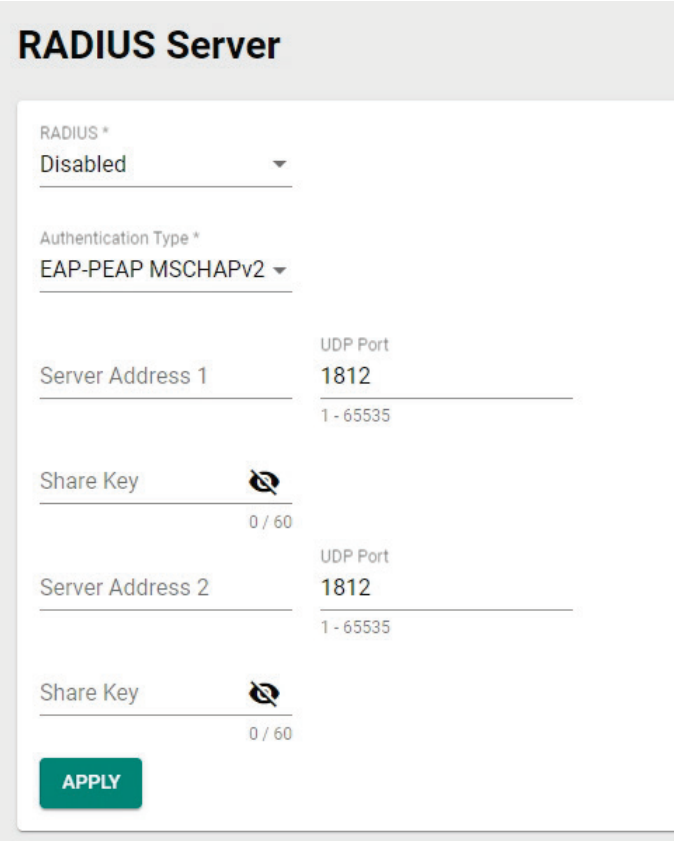
When finished, click **APPLY** to save your changes.

Delete an Existing Local Database Entry

Select the user account(s) in the Account List. Click the icon and click **DELETE** to delete the selected user account(s).

RADIUS

Users can set up two RADIUS servers, one primary and one secondary backup server. When the primary RADIUS server becomes unavailable, the EDR-G9010 Series will switch to the backup RADIUS server.



RADIUS

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable RADIUS login authentication.	Disabled

Authentication Type

Setting	Description	Factory Default
PAP	Select the authentication type for the RADIUS server.	EAP-PEAP MSCHAPv2
CHAP		
EAP-PEAP MSCHAPv2		

RADIUS Server Setting

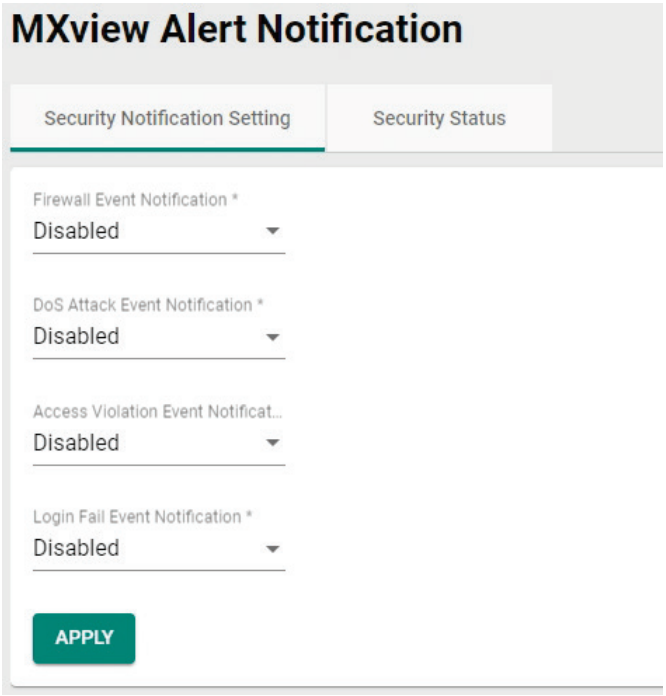
Setting	Description	Factory Default
Server Address 1/2 (0 to 64)	Specify the first and second RADIUS authentication server IP address or server name.	None
UDP Port (1 to 65535)	Specify the first and second RADIUS server port number.	1812
Shared key (max. 60 characters)	Specify the shared key for the first and second RADIUS server.	None

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

MXview Alert Notification

Security Notification Setting

If event notifications are enabled, the EDR-G9010 will send an SNMP Trap to notify the server.



Firewall Event Notification

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable notifications for Firewall events.	Disabled

DoS Attack Event Notification

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable notifications for DoS attack events.	Disabled

Access Violation Event Notification

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable notifications for Access Violation events.	Disabled

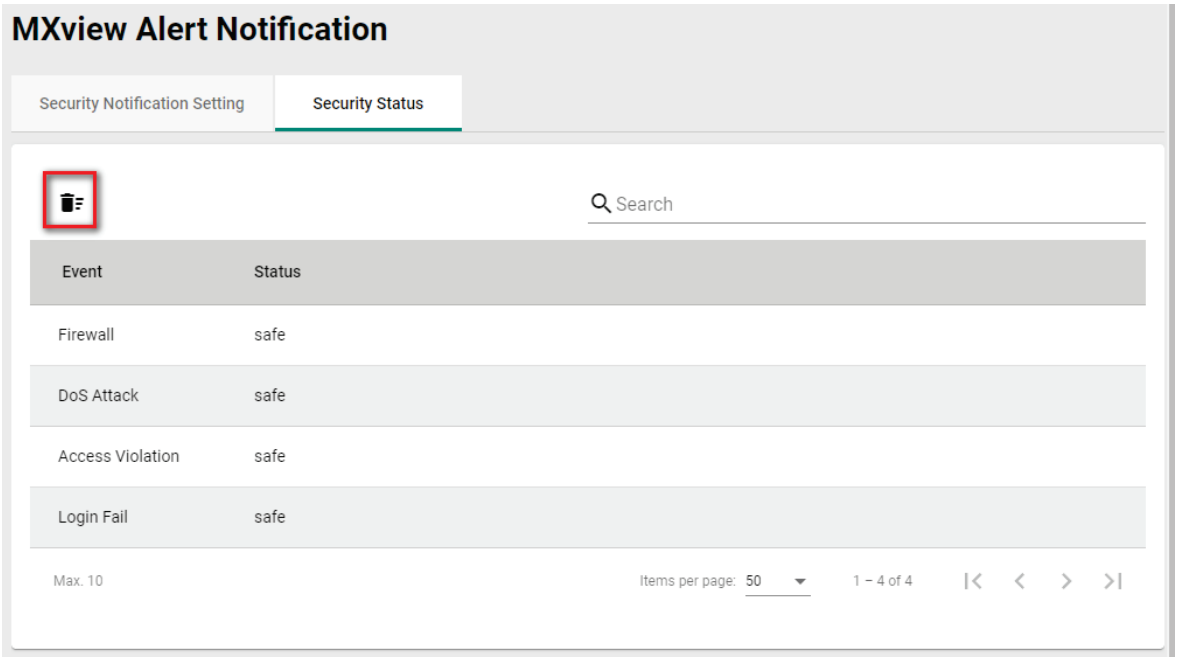
Login Fail Event Notification

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable notifications for Login Fail events.	Disabled

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

Security Status

The Security Status screen shows the status of all event types. Click the icon to clear all event statuses.

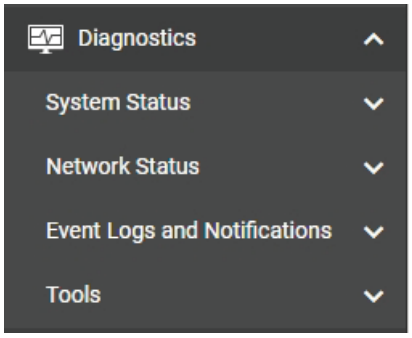


15. Diagnostics

Through the Diagnostics section, you can keep track of the system and network performance, consult event logs, and check the status of the port connectors.

The Industrial Secure Router also provides **Port Mirror** and **Ping** tools for administrators to diagnose network systems.

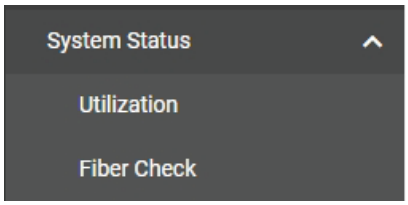
From the **Diagnostics** section, you can configure the **System Status, Network Status, Event Logs and Notifications,** and **Tools** configurations.



System Status

Users can monitor the data transmission activity of all the Industrial Secure Router ports from two perspectives, **Bandwidth Utilization** and **Packet Counter**. The graph displays data transmission activity by showing Utilization/Sec or Packet/Sec (i.e., packets per second, or pps) versus Min:Sec. (Minutes: Seconds). The graph is updated every 5 seconds, allowing the user to analyze data transmission activity in real-time.

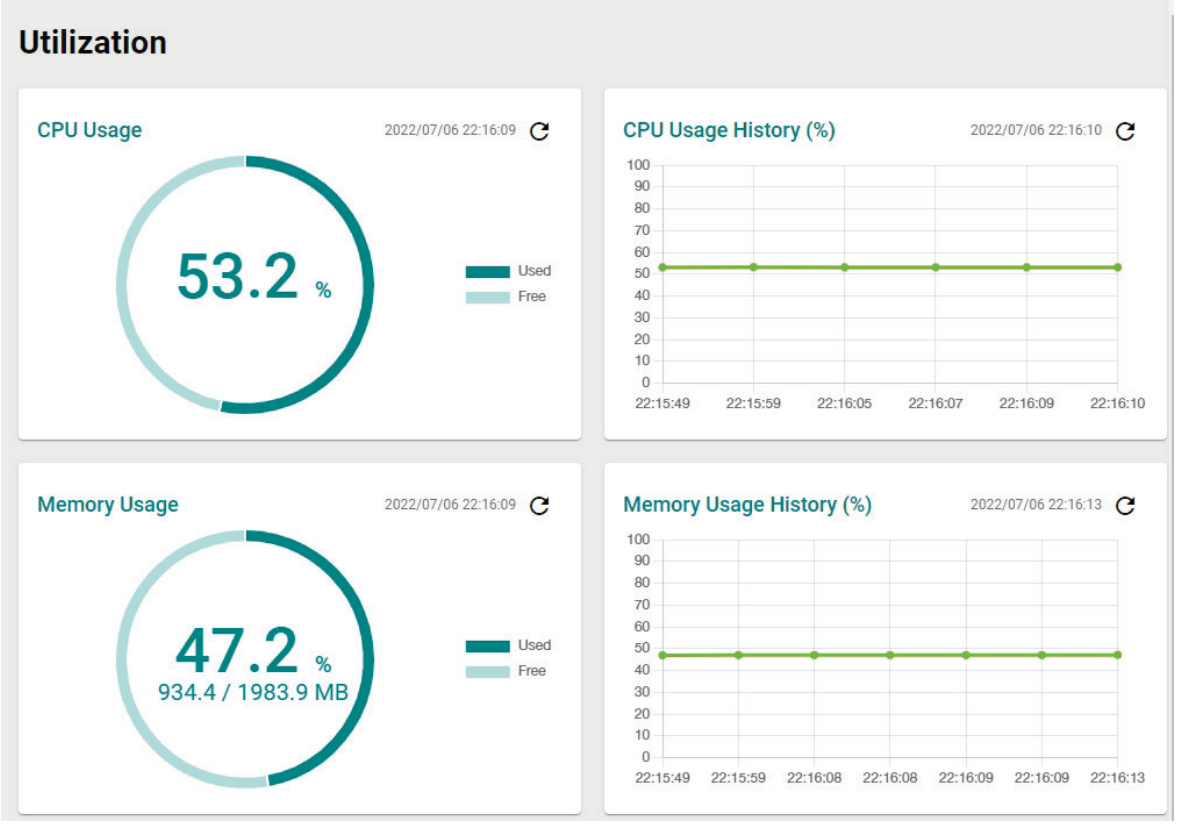
From the **System Status** section, the following functions can be configured: **Utilization,** and **Fiber Check**.



Utilization

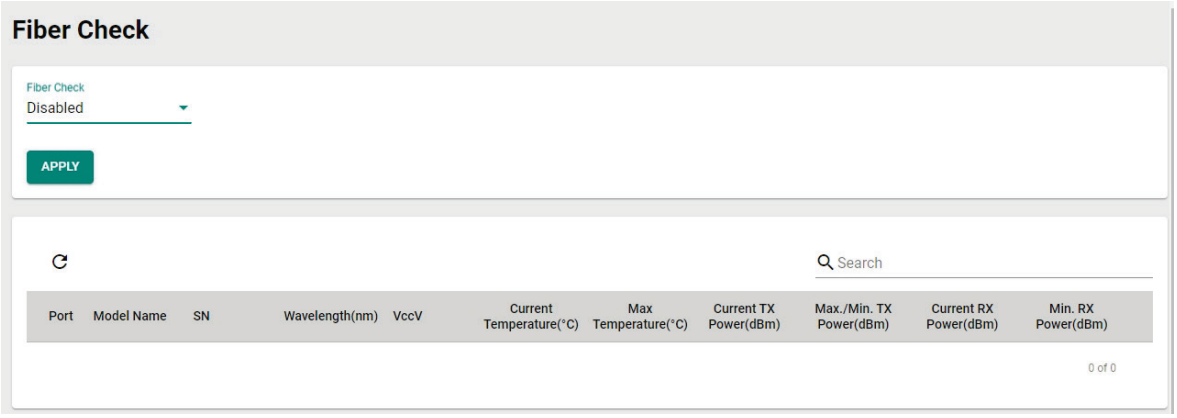
On the **Utilization** page, you can view the system resource utilization history, including the current and historical CPU and memory usage.

Click the icon on the upper-right corner of each graph to refresh the data.



Fiber Check

Fiber Check is used to diagnose the link status of fiber connectors, including SFP and fixed type (Multi-mode SC/ST and Single-mode SC) connectors. Fiber Check allows you to monitor the temperature, TX/RX power, and other parameters on fiber ports to determine if the ports are working properly. Enable the trap, email warning, and/or relay warning functions on the System Event Settings page to receive an alarm or relay if one of the fiber ports exceeds the threshold for that port.



Fiber Check

Setting	Description	Factory Default
Enabled or disabled	Enable or disable the Fiber Check function.	Disabled

Fiber Check table

The Fiber Check table displays the following information:

Field	Description
Port	The switch port number hosting the fiber connection.
Model Name	The name of the SFP module.
SN	The serial number of the SFP module.
Wavelength (nm)	The wavelength of the fiber connection.
VccV	The voltage supply to the fiber connection.
Current Temperature (°C)	The current temperature of the fiber connection.
Max. Temperature (°C)	The maximum temperature threshold the fiber connection supports.
Current TX Power(dBm)	The current amount of light transmitted over the fiber-optic cable.
Max./Min. TX Power(dBm)	The maximum/minimum amount of light the fiber optic cable can transmit.
Current RX Power(dBm)	The current amount of light received over the fiber optic cable.
Min. RX Power(dBm)	The minimum amount of light the fiber optic cable can receive.

Fiber Check Threshold Values

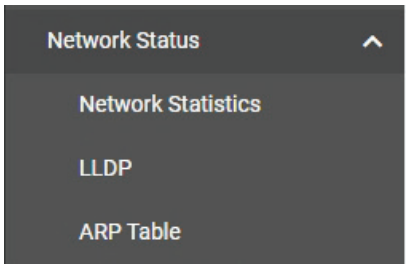
Model Name	Temperature Threshold (°C)	Max./Min. Tx Power (dBm)	Min. Rx Power (dBm)
FEMST	120	-11.0/-23.0	-31.0
FEMSC	120	-11.0/-23.0	-31.0
FESSC	120	3.0/-8.0	-34.0
SFP-1FEMLC-T	120	-5.0/-21.0	-37.0
SFP-1FESLC-T	120	3.0/-8.0	-37.0
SFP-1FELLC-T	120	3.0/-8.0	-37.0
SFP-1GSXLC-T	110	-1.0/-12.5	-18.0
SFP-1GLSXLC-T	120	2.0/-12.0	-19.0
SFP-1GLXLC-T	120	0.0/-12.5	-20.0
SFP-1GLHLC-T	120	1.0/-11.0	-23.0
SFP-1GLHXLC-T	120	4.0/-7.0	-24.0
SFP-1GZXLC-T	120	8.0/-3.0	-24.0
SFP-1G10ALC-T	120	0.0/-12.0	-21.0
SFP-1G10BLC-T	120	-5.0/-21.0	-34.0
SFP-1G20ALC-T	120	1.0/-11.0	-23.0
SFP-1G20BLC-T	120	-5.0/-21.0	-34.0
SFP-1G40ALC-T	120	5.0/-6.0	-23.0
SFP-1G40BLC-T	120	-5.0/-21.0	-34.0
SFP-1GSXLC	100	-1.0/-12.5	-18.0
SFP-1GLSXLC	100	2.0/-12.0	-19.0
SFP-1GLXLC	100	0.0/-12.5	-20.0
SFP-1GLHLC	100	1.0/-11.0	-23.0
SFP-1GLHXLC	100	4.0/-7.0	-24.0
SFP-1GZXLC	100	8.0/-3.0	-24.0
SFP-1GEZXLC	100	8.0/-3.0	-30.0
SFP-1GEZXLC-120	100	6.0/-5.0	-33.0
SFP-1G10ALC	100	0.0/-12.0	-21.0
SFP-1G10BLC	100	-5.0/-21.0	-34.0
SFP-1G20ALC	100	1.0/-11.0	-23.0
SFP-1G20BLC	100	-5.0/-21.0	-34.0
SFP-1G40ALC	100	5.0/-6.0	-23.0
SFP-1G40BLC	100	-5.0/-21.0	-34.0

NOTE

Certain tolerances exist between real data and measured data.

Network Status

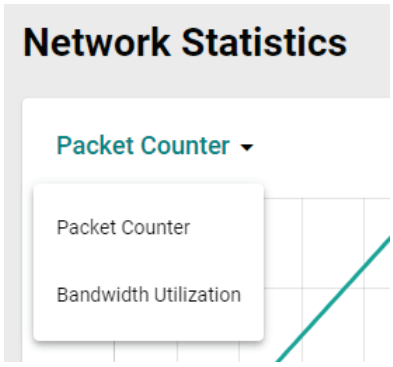
From the **Network Status** section, the following functions can be configured: **Network Statistics, LLDP,** and **ARP Table**.



Network Statistics

The **Network Statistics** page shows the Packet Counter status by default.

To switch views, click the **Packet Counter** drop-down menu and select **Bandwidth Utilization** to see the current bandwidth usage.

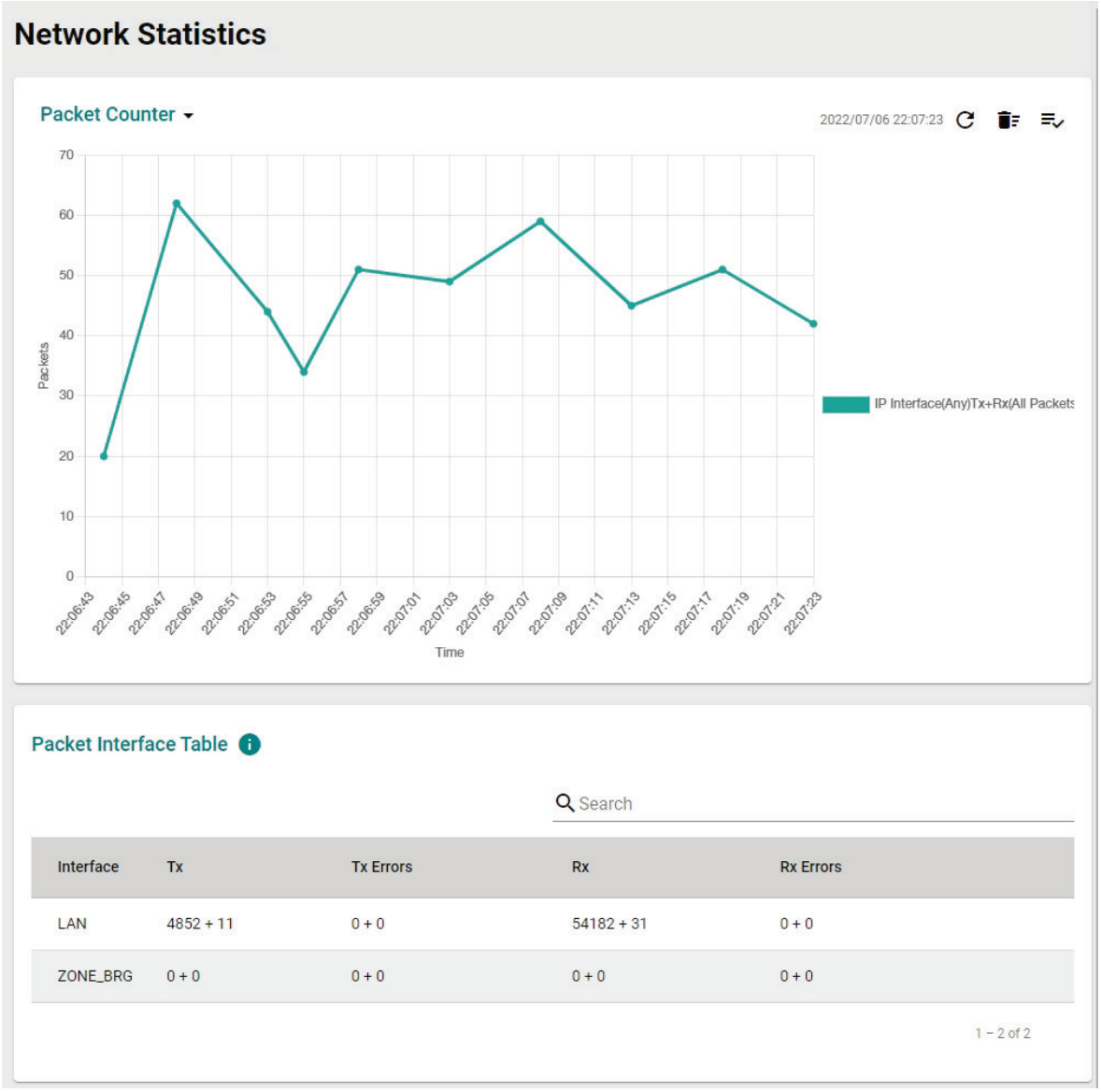


Display Mode

Setting	Description	Factory Default
Packet Counter, Bandwidth Utilization	Select which statistics to show. Refer to the following sections for more information: Packet Counter Bandwidth Utilization	Packet Counter

Packet Counter

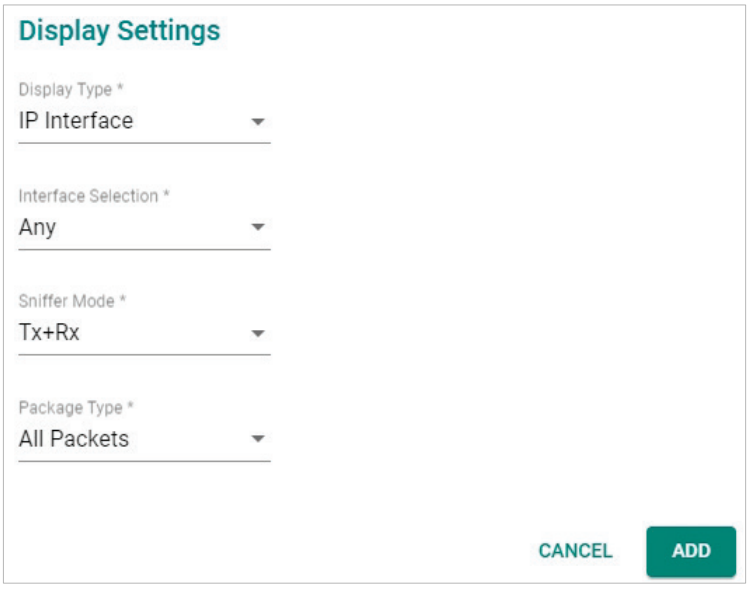
In the **Packet Counter** view, users can monitor the total amount of packets per second for each interface (**IP Interface)**, each port, or port group (**Ports**). Users can choose which packet flows to monitor, **TX Packets**, **RX Packets**, or both (**TX/RX**). **TX Packets** are packets sent out from the Industrial Secure Router while **RX Packets** are packets received from connected devices. Additionally, users can also choose which packet types to monitor, including unicast, broadcast, multicast, and error.



There are three function icons in the upper-right corner of the page. The table below provides a description for each function.

Icon	Name	Description
	Refresh	Refresh all statistical data immediately.
	Reset Statistics Graph	Click this icon, then click CLEAR to clear the packet counter and reset the graph.
	Display Settings	Configure which information is shown on the graph. Refer to Display Settings for more information.

Display Settings



Display Type

Setting	Description	Factory Default
Port	Monitor the total traffic per port or port group (FE Ports/GbE ports).	IP Interface
IP Interface	Monitor the total traffic per interface, e.g. LAN, WAN, Bridge.	

Interface Selection

Setting	Description	Factory Default
Any, LAN, WAN, Bridge LAN	If Display Type is set to IP Interface, select which interface to monitor traffic for.	Any

Port Selection

Setting	Description	Factory Default
All ports, FE Ports, GE Ports, Port 1, Port 2, Port 3, Port 4, Port 5, Port 6, Port 7, Port 8, Port G1, Port G2	If Display Type is set to Port, select which port or port group to monitor traffic for.	All ports

Sniffer Mode

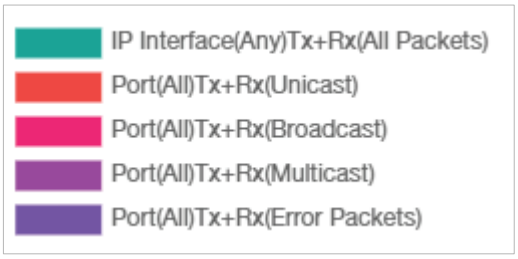
Setting	Description	Factory Default
TX+RX, TX, RX	Select which packet flow to monitor.	TX+RX

Packet Type

Setting	Description	Factory Default
All Packets, Unicast, Broadcast, Multicast, Error Packets	Select which packet type to monitor.	All Packets

When finished, click **ADD** to save your display settings.

Each type of data is represented by a different color, as shown below:

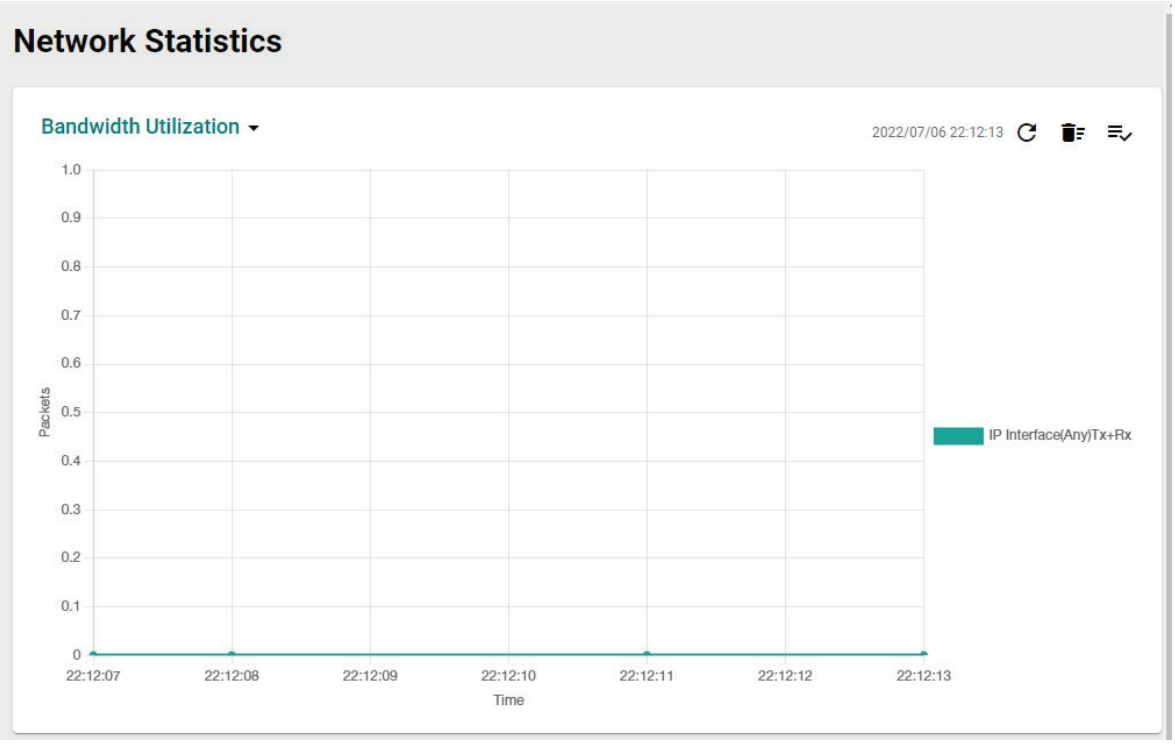


Packet Interface Table

The packet flow format is Total Packets + Packets in the past 5 seconds. The data is updated every 5 seconds.

Bandwidth Utilization

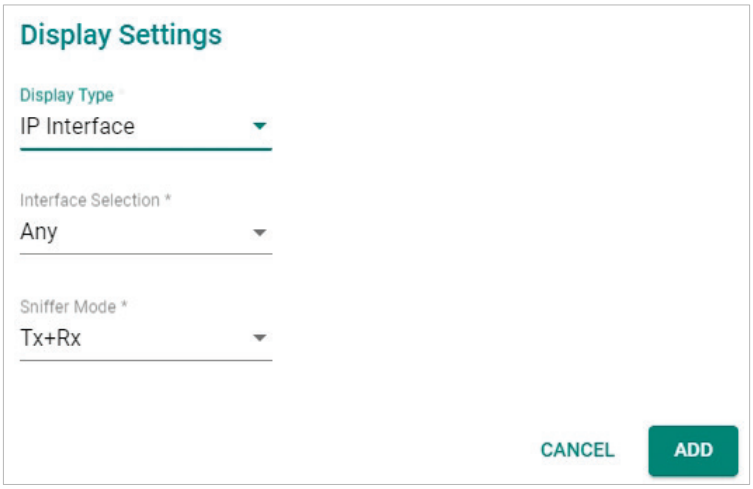
Select **Bandwidth Utilization** from the drop-down menu in the **Network Statistics** page to view the current bandwidth usage.



There are three function icons in the upper-right corner of the page. The table below provides a description for each function.

Icon	Name	Description
	Refresh	Refresh all statistical data immediately.
	Reset Statistics Graph	Click this icon, then click CLEAR to clear the bandwidth usage data and reset the graph.
	Display Settings	Configure which information is shown on the graph. Refer to Display Settings for more information.

Display Settings



Display Type

Setting	Description	Factory Default
Port	Monitor the total traffic per port or port group (FE Ports/GbE ports).	IP Interface
IP Interface	Monitor the total traffic per interface, e.g. LAN, WAN, Bridge.	

Interface Selection

Setting	Description	Factory Default
Any, LAN, WAN, Bridge LAN	Select which interface to monitor traffic for.	Any

Sniffer Mode

Setting	Description	Factory Default
TX+RX, TX, RX	Select which packet flow to monitor.	TX+RX

When finished, click **ADD** to save your display settings.

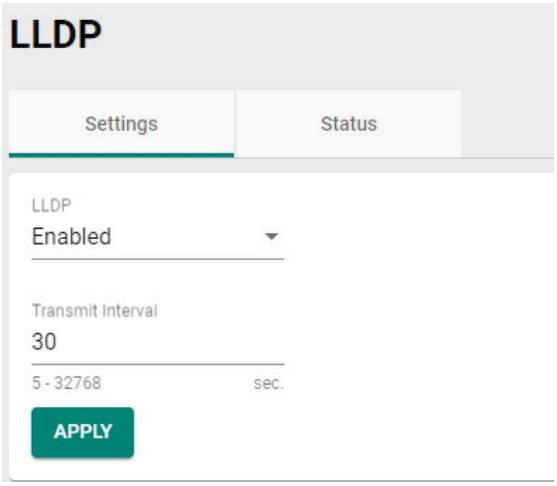
LLDP

LLDP Function Overview

Defined by IEEE 802.11AB, Link Layer Discovery Protocol (LLDP) is an OSI Layer 2 protocol that standardizes the methodology of self-identity advertisement. It allows each networking device, such as a Moxa managed switch/router, to periodically inform its neighbors about itself and its configuration. This way, all devices are aware of each other.

LLDP can be enabled or disabled. Additionally, users can configure the interval at which LLDP packets are sent and view each switch's neighbor-list, which is reported by its network neighbors.

LLDP Settings



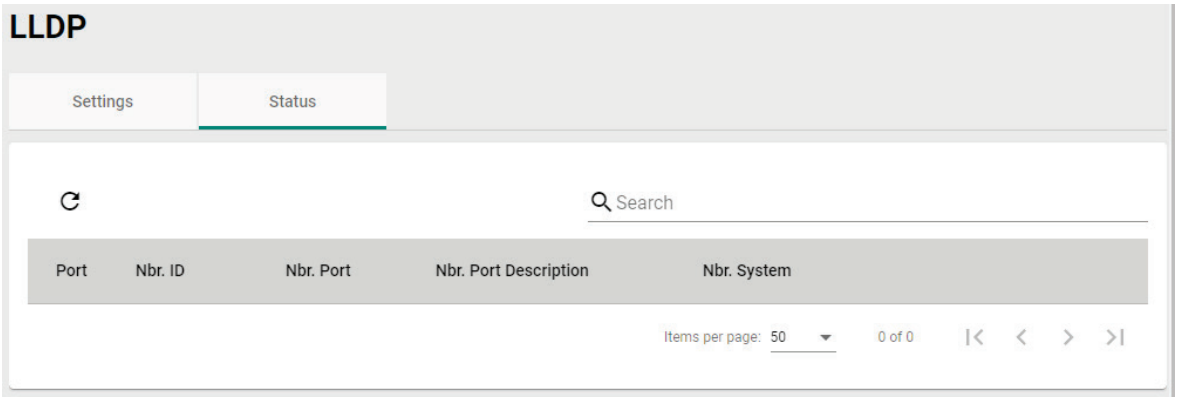
LLDP

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

Transmit Interval

Setting	Description	Factory Default
5 to 32768 seconds	Specify the interval (in seconds) at which LLDP messages are sent.	30 (seconds)

LLDP Status



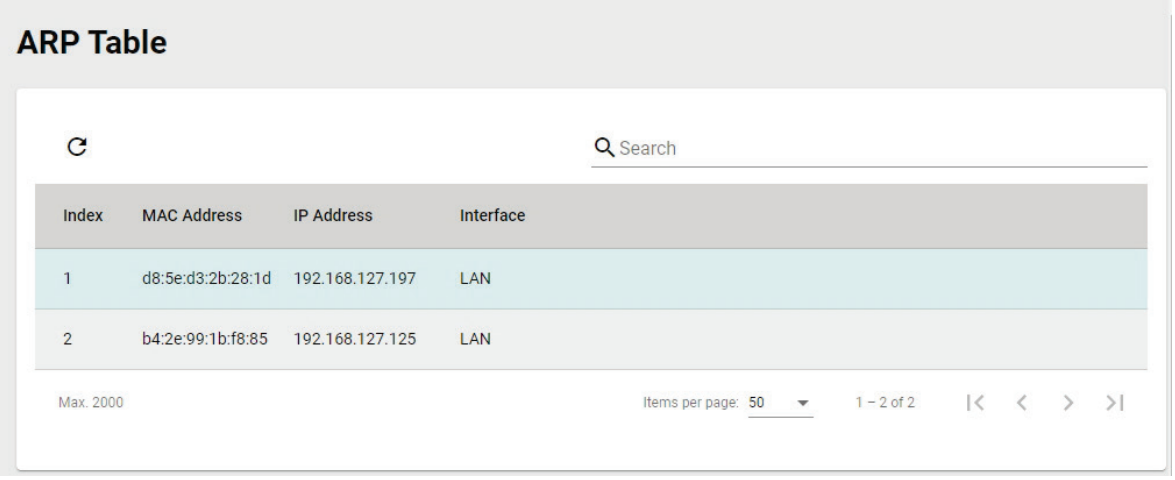
The LLDP table displays the following information:

Field	Description
Port	The port number that connects to the neighbor device.
Neighbor ID	A unique identifier (typically the MAC address) that identifies the neighbor device.
Neighbor Port	The port number of the connecting neighbor device.
Neighbor Port Description	The description of the neighbor device's interface.
Neighbor System	The hostname of the neighbor device.

Click the icon to refresh the table.

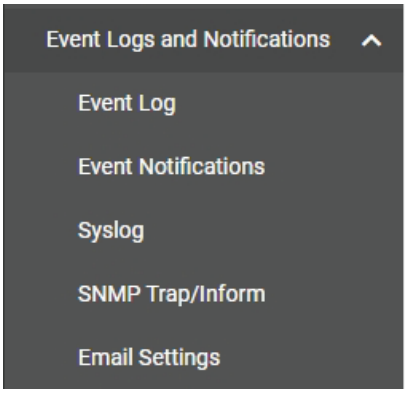
ARP Table

The ARP table shows the device's Address Resolution Protocol (ARP) information.



Event Logs and Notifications

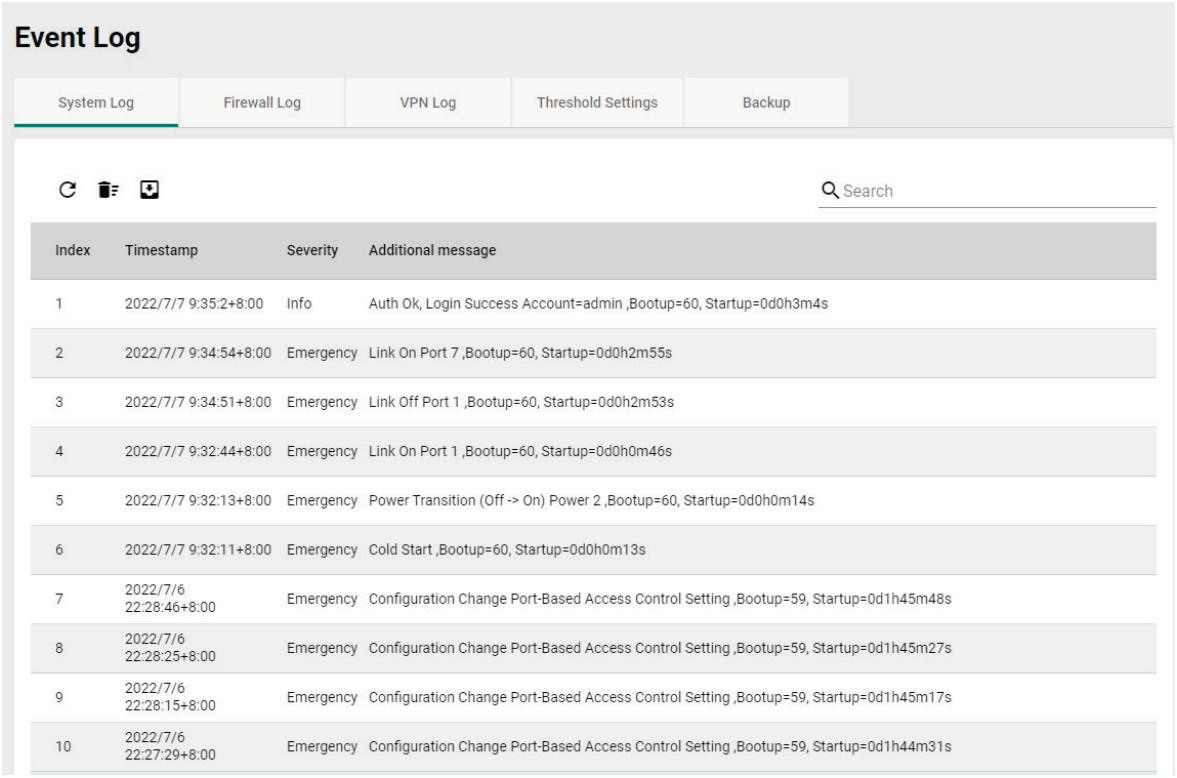
From the **Event Logs and Notifications** section, the following functions can be configured: **Event Log, Event Notification, Syslog, SNMP Trap/Inform,** and **Email Settings**.



Event Log

System Log

By default, the **System Log** shows details of all system-related event logs.



Click the icon to refresh the system logs.

Click the icon to delete all system logs.

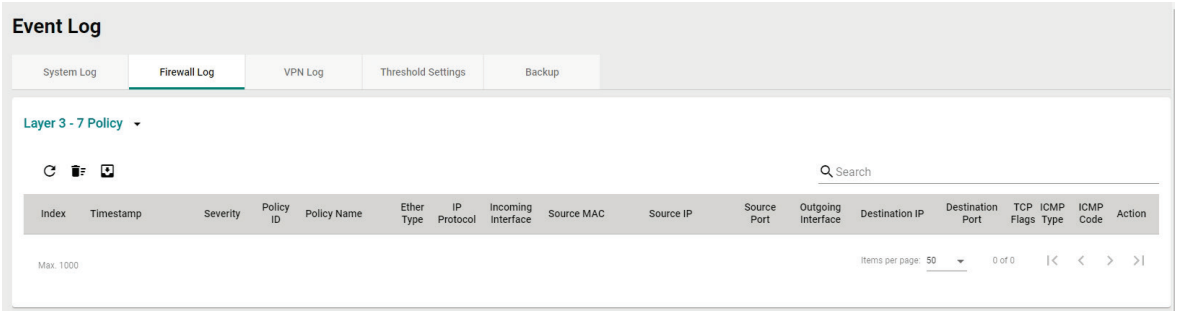
Click the icon to export all system logs to a file.

Firewall Log

From the **Firewall Log** page, you can check the various types of firewall event logs. By default, the firewall logs of the Layer 3–7 Policy will be displayed.

Click the **Layer 3–7 Policy** drop-down menu to select and show the firewall logs for other policy patterns, including:

- Trusted Access
- Malformed Packets
- DoS Policy
- Layer 3 – 7 Policy
- Protocol Filter Policy
- ADP
- IPS
- Session Control



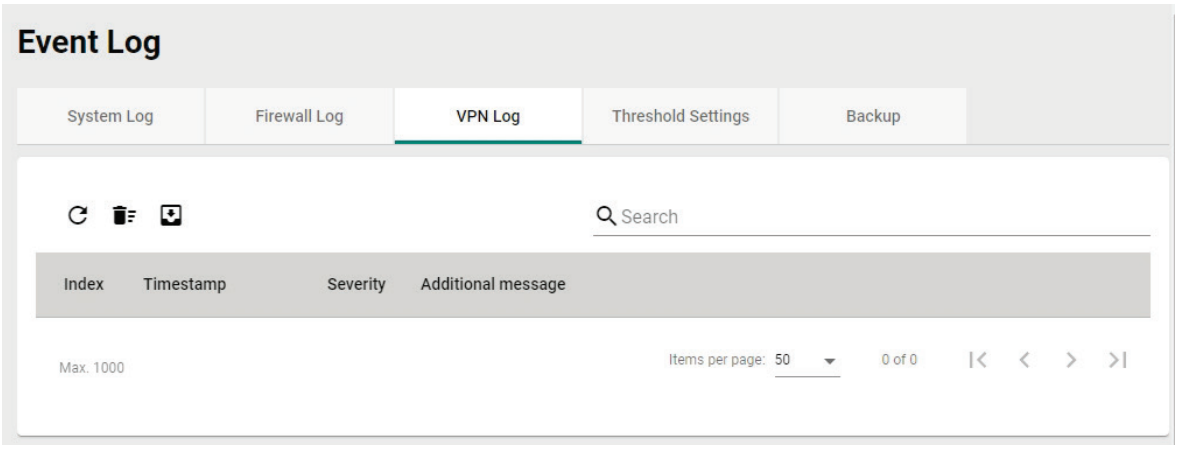
Click the icon to refresh the firewall logs.

Click the icon to delete all firewall logs.

Click the icon to export all firewall logs to a file.

VPN Log

The **VPN Log** table shows details for all VPN-related event logs.



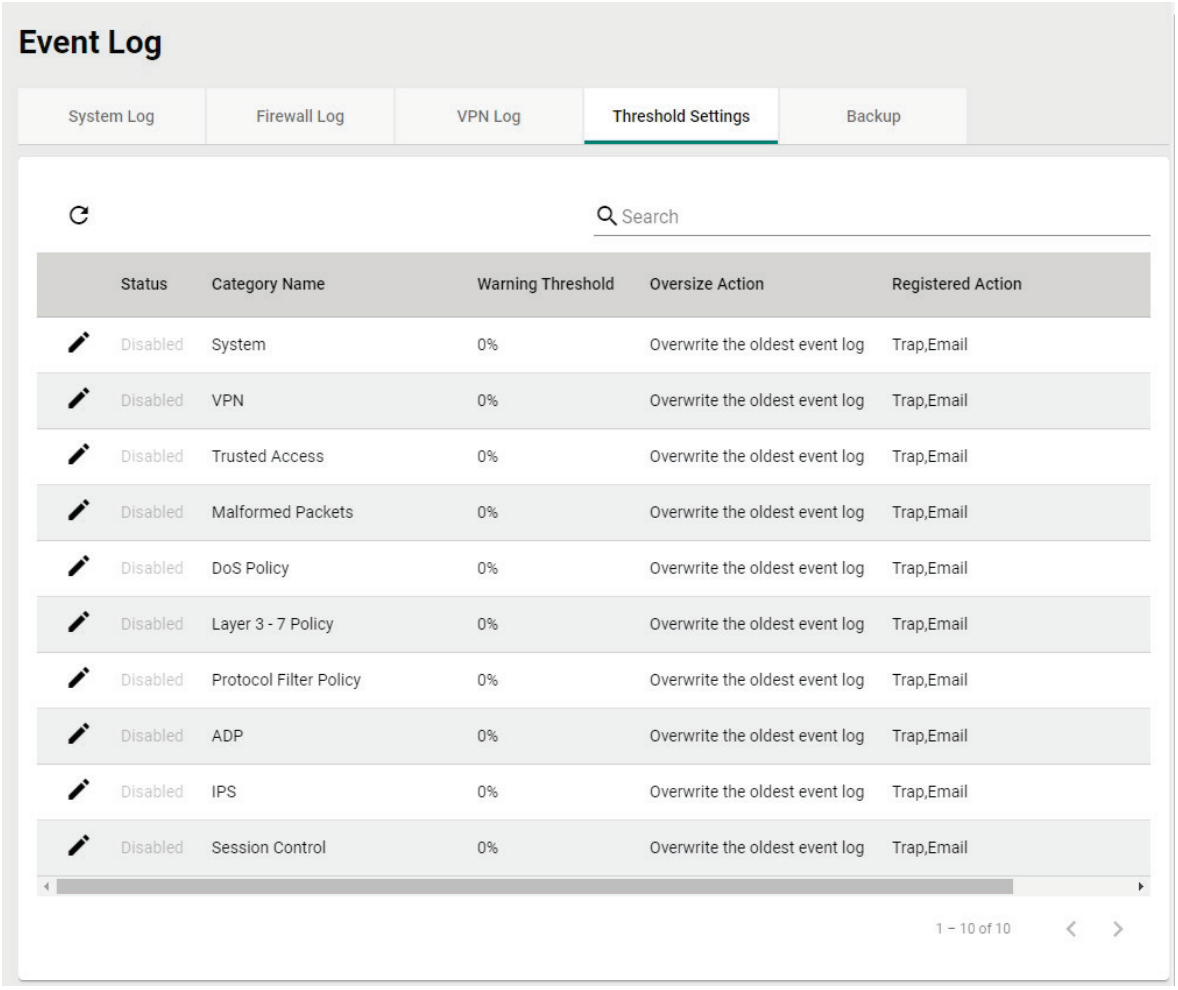
Click the icon to refresh the VPN logs.

Click the icon to delete all VPN logs.

Click the icon to export all VPN logs to a file.

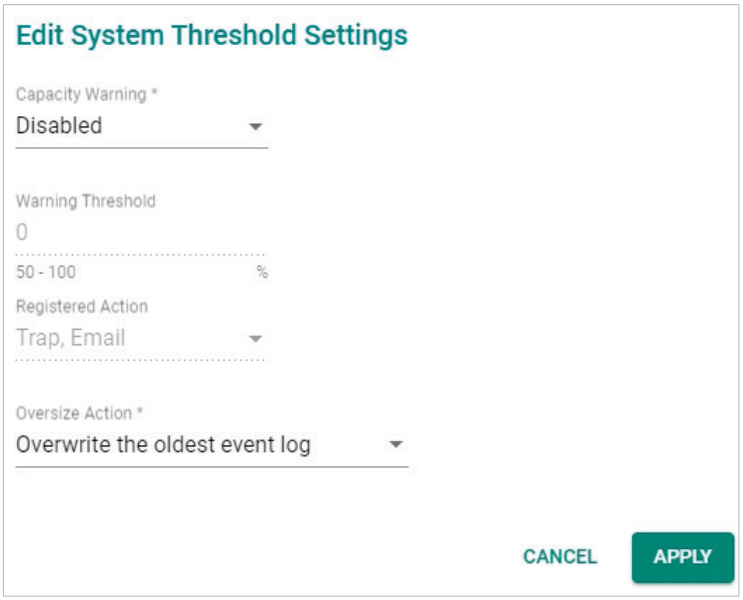
Threshold Settings

On the **Threshold Settings** screen, users can set up capacity warnings and oversize actions that trigger when the log storage has exceeded the specified storage threshold.



Click the icon to refresh the threshold settings.

Click the icon next to the entry you want to modify.



Capacity Warning

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable capacity warnings. The Registered Action can be configured for individual events by editing the event on the Event Notifications page.	Disabled

Warning Threshold

Setting	Description	Factory Default
50 to 100 %	Specify the threshold percentage of the current storage. Once the storage exceeds this value, the warning will trigger.	0

Registered Action

Setting	Description	Factory Default
Trap, Email	Select how the warning is sent.	Trap, Email

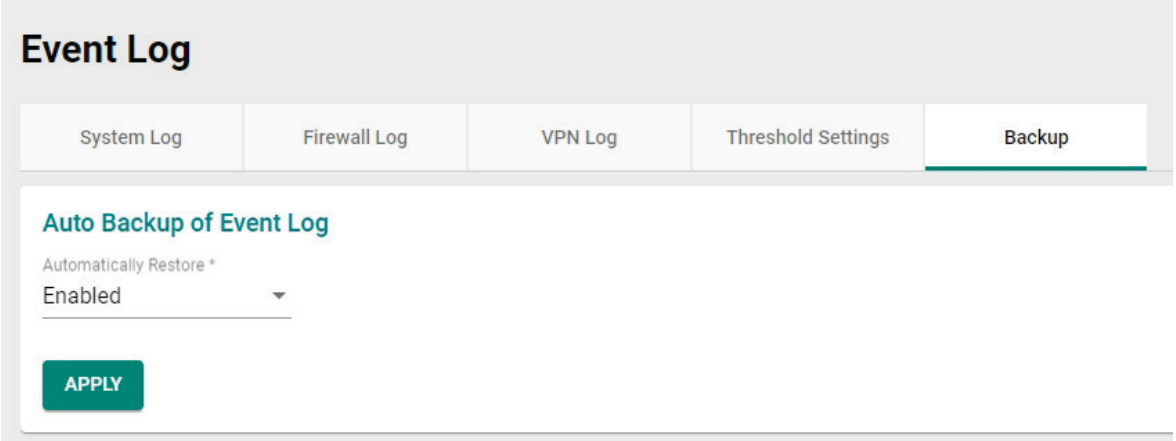
Oversize Action

Setting	Description	Factory Default
Overwrite the oldest event log, Stop recording event logs	Select the oversize action when the log storage is full.	Overwrite the oldest event log

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

Backup

From the **Backup** screen, users can enable automatic event log backups.



Automatically Restore

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable automatic event log backups.	Enabled

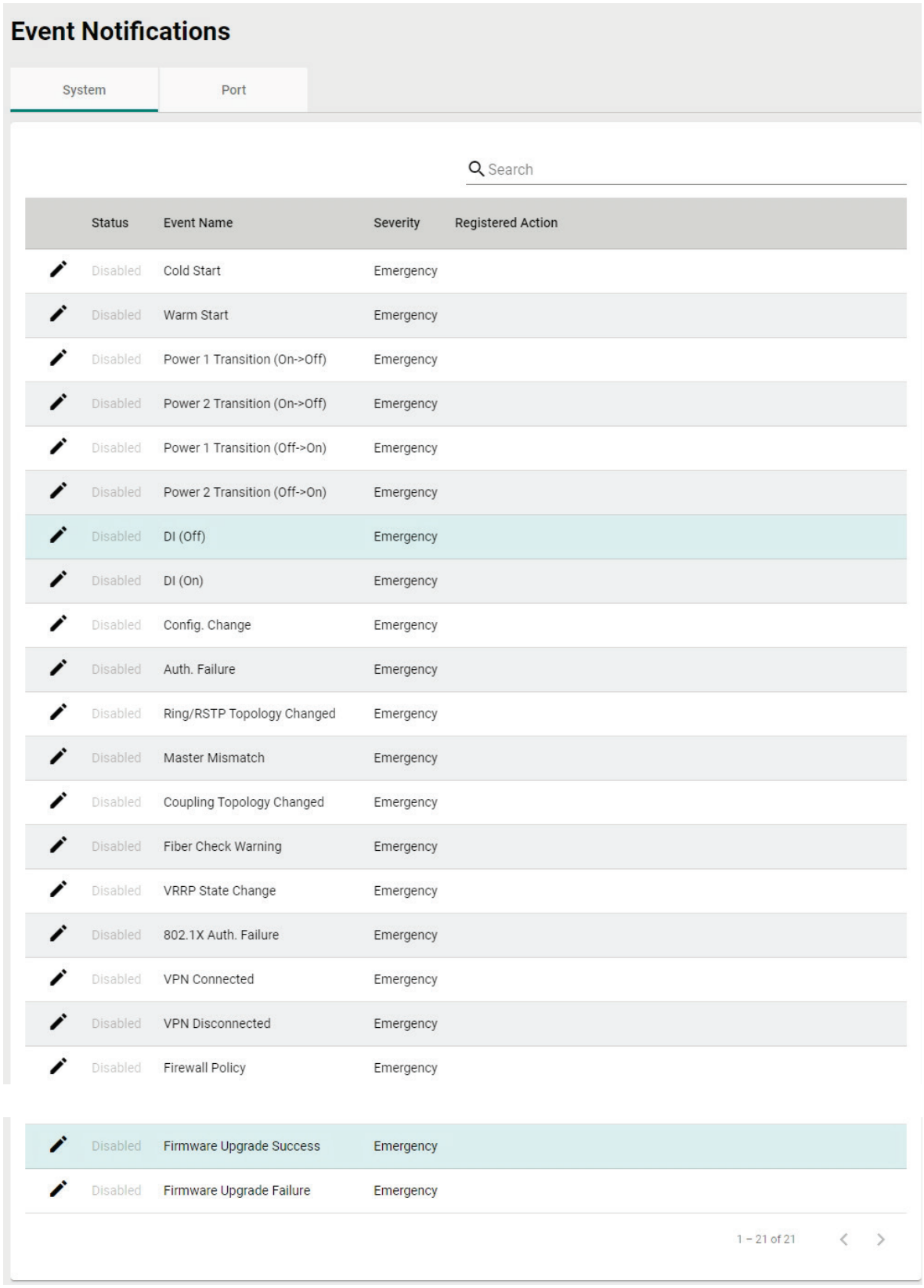
When finished, click **APPLY** to save your changes.

Event Notifications

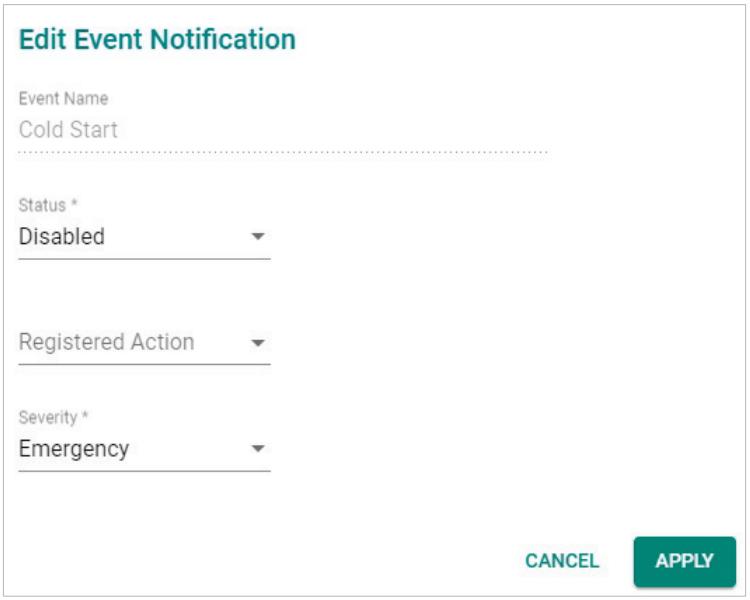
Since industrial Ethernet devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that an industrial secure router that connects to these devices must provide system maintainers with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of devices almost instantaneously when exceptions occur. The Moxa industrial secure router supports different methods to warn engineers automatically, such as email, trap, syslog and relay output. It also supports one digital input to integrate sensors into your system to automate alarms by email and relay output.

System Event Settings

System Events are related to the overall functions of the device. Each event can be activated independently with different warning methods. Administrator also can decide the severity of each system event.



Click the ✎ icon next to the entry you want to modify.



Event Name

System Events	Description
Cold Start	Power was cut off and then reconnected.
Warm Start	The Moxa industrial secure router was rebooted, such as when network parameters are changed (IP address, netmask, etc.).
Power 1 Transition (On->Off)	The Moxa industrial secure router's power 1 is powered down.
Power 2 Transition (On->Off)	The Moxa industrial secure router's power 2 is powered down.
Power 1 Transition (Off->On)	The Moxa industrial secure router's power 1 is powered up.
Power 2 Transition (Off->On)	The Moxa industrial secure router's power 2 is powered up.
DI (Off)	The digital input state is "0"
DI (On)	The digital input state is "1"
Config. Change	A configuration setting was changed.
Auth. Failure	An incorrect password was entered.
Ring/RSTP Topology Changed	The Ring/RSTP topology was changed.
Master Mismatch	A Turbo Ring Master mismatch occurred.
Coupling Topology Changed	The Coupling topology was changed.
Fiber Check Warning	The fiber port threshold has been exceeded.
VRRP State Change	The VRRP state was changed.
802.1X Auth. Failure	An 802.1X authentication failure occurred.
VPN Connected	VPN has been connected.
VPN Disconnected	VPN has been disconnected.
Firewall Policy	A firewall policy failure occurred.
Firmware Upgrade Success	Firmware upgrade was successful.
Firmware Upgrade Failure	An error occurred during the firmware upgrade.

Status

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

Registered Action

There are four response actions available on the Industrial Secure Router when events are triggered.

Setting	Description	Factory Default
Trap	The notification is sent to the Trap server when the event is triggered.	None
Email	The notification is sent to the email server defined in the Email Settings section.	
Syslog	The event log is recorded to a Syslog server defined in the Syslog section.	
Relay	The industrial secure router supports digital inputs to integrate sensors. When event is triggered, the device will automate alarm notifications through the relay output.	

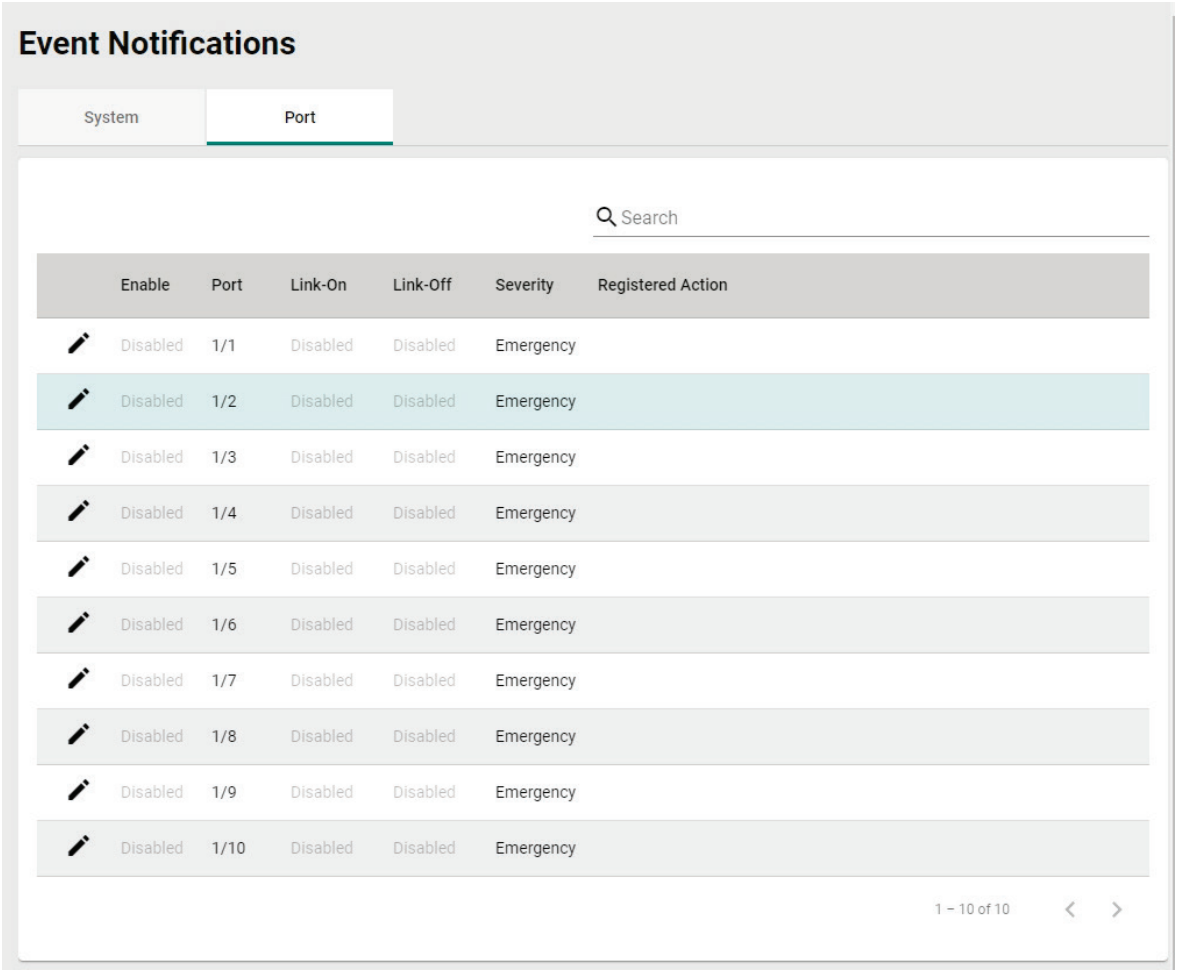
Severity

Setting	Description	Factory Default
Emergency	System is unusable	Emergency
Alert	Action must be taken immediately	
Critical	Critical conditions	
Error	Error conditions	
Warning	Warning conditions	
Notice	Normal but significant condition	
Info	Informational messages	
Debug	Debug-level messages	

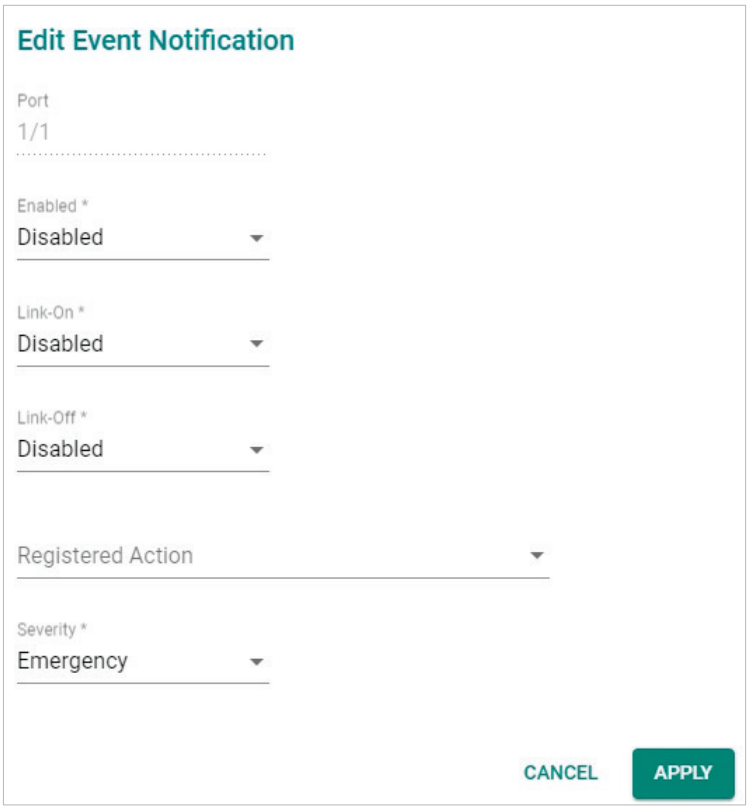
When finished, click **APPLY** to save your changes.

Port Event Settings

Port Events are related to the activity of a specific port.



Click the icon next to the entry you want to modify.



Port

This is the physical port (1/1 to 1/10) on the Industrial Secure Router.

Enabled

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

Link-On

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable Link-On events. If enabled, an event is triggered when the port is connected to another device.	Disabled

Link-Off

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable Link-Off events. If enabled, an event is triggered when the port is disconnected (e.g., the cable is unplugged, or the connected device is shut down).	Disabled

Registered Action

There are four response actions available on the Industrial Secure Router when events are triggered.

Setting	Description	Factory Default
Trap	The notification is sent to the Trap server when the event is triggered.	None
Email	The notification is sent to the email server defined in the Email Settings section.	
Syslog	The event log is recorded to a Syslog server defined in the Syslog section.	
Relay	The industrial secure router supports digital inputs to integrate sensors. When event is triggered, the device will automate alarm notifications through the relay output.	

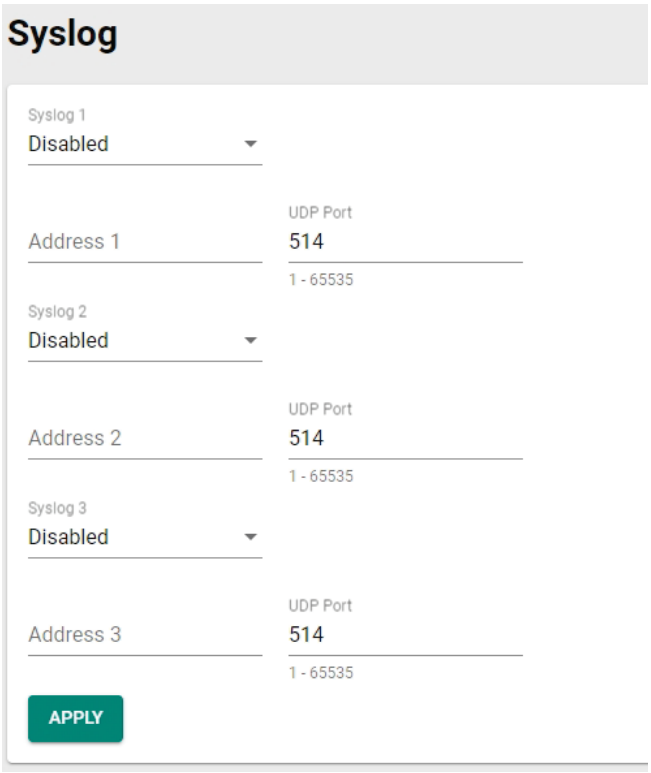
Severity

Setting	Description	Factory Default
Emergency	System is unusable	Emergency
Alert	Action must be taken immediately	
Critical	Critical conditions	
Error	Error conditions	
Warning	Warning conditions	
Notice	Normal but significant condition	
Info	Informational messages	
Debug	Debug-level messages	

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

Syslog

The Syslog function is used to set up Syslog servers for storing event logs. Up to three Syslog servers can be set up. When an event occurs, the event will be sent as a syslog UDP packet to the specified Syslog servers. Each Syslog server can be enabled individually.



Syslog 1/2/3

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

Address 1/2/3

Setting	Description	Factory Default
Address 1/2/3	Enter the IP address of the Syslog server.	None

UDP Port

Setting	Description	Factory Default
1 to 65535	Specify the UDP port of the Syslog server.	514

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

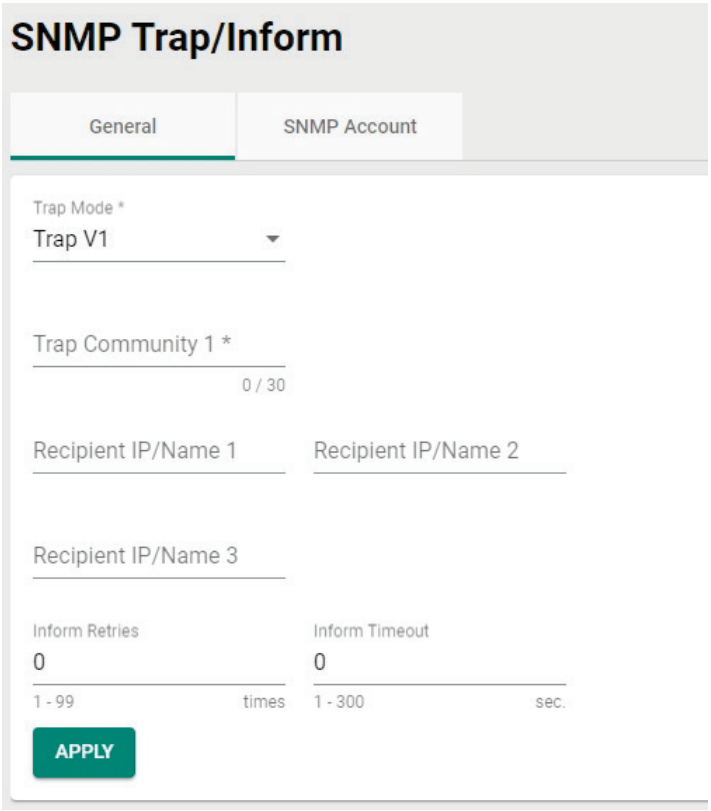
NOTE

The following events will be recorded into the Moxa industrial secure router's Event Log table, and will then be sent to the specified Syslog Server:

- Cold start
- Warm start
- Configuration change activated
- Power 1/2 transition (Off (On), Power 1/2 transition (On (Off))
- Authentication fail
- Port link off/on
- Ring/RSTP Topology Change activated
- Master Mismatch
- Coupling Topology Change activated
- Fiber Check Warning
- VRRP State Change activated
- 802.1X Auth. fail
- VPN connected/disconnected
- Firewall policy
- Firmware upgrade success/failure

SNMP Trap/Inform

General Settings



Trap Mode

Setting	Description	Factory Default
Trap V1	Set the Trap version to Trap V1.	Trap V1
Trap V2	Set the Trap version to Trap v2.	
Inform V2	Set the Inform version to Inform V2.	
Trap V3	Set the Trap version to Trap V3.	
Inform V3	Set the Inform version to Inform V3.	

Trap Community 1

Setting	Description	Factory Default
max. 30 characters	Specify the community string that will be used for authentication.	None

Recipient IP/Name 1/2/3

Setting	Description	Factory Default
Recipient IP or name	Specify the name of the primary Trap server used by your network.	None

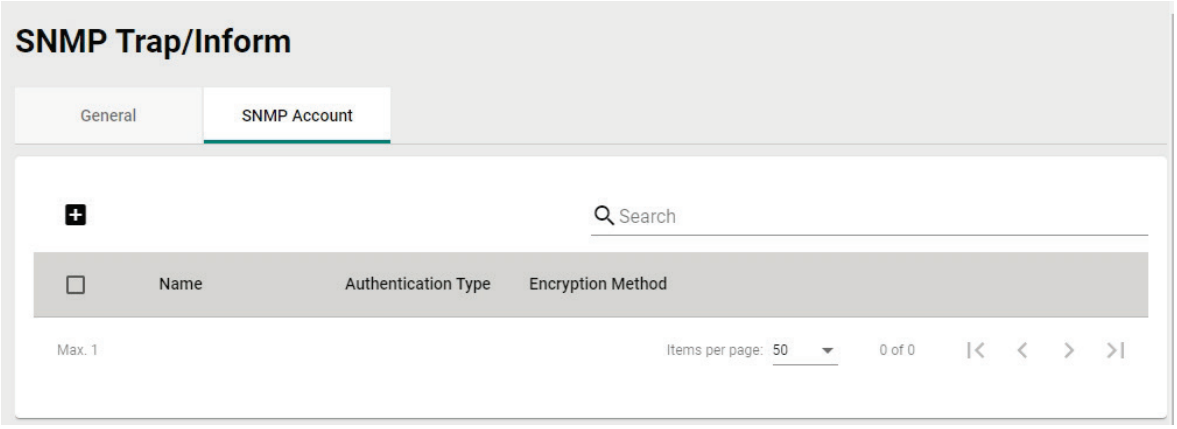
Inform Retries

Setting	Description	Factory Default
1 to 99 times	Specify the allowed number of retries for attempting to reconnect to a server.	0

Inform Timeout

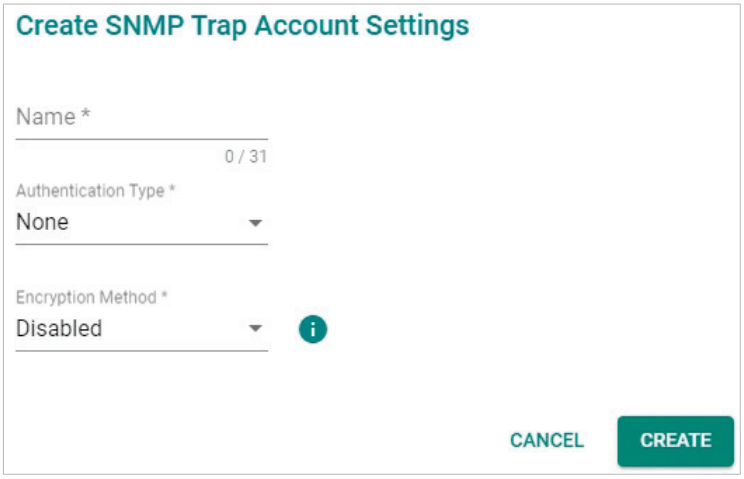
Setting	Description	Factory Default
1 to 300 seconds.	Set the retry interval when trying to reconnect to a server.	0

SNMP Account



Create a SNMP Trap Account

Click the + icon to create a SNMP Trap account.



Name

Setting	Description	Factory Default
max. 31 characters	Enter a name for the account.	None

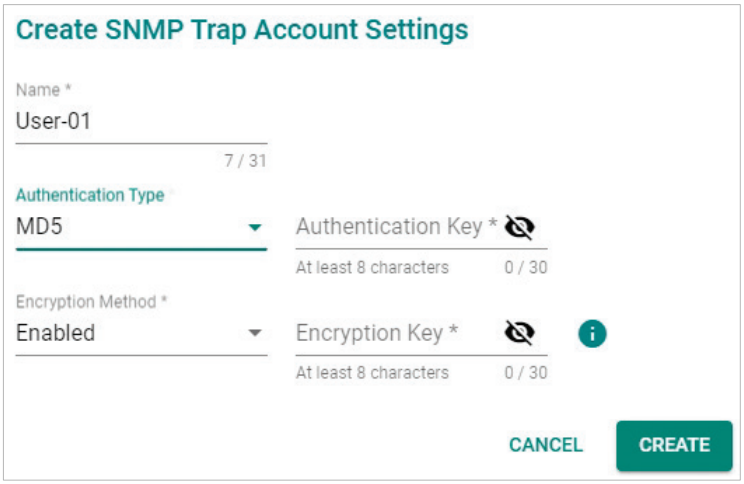
Authentication Type

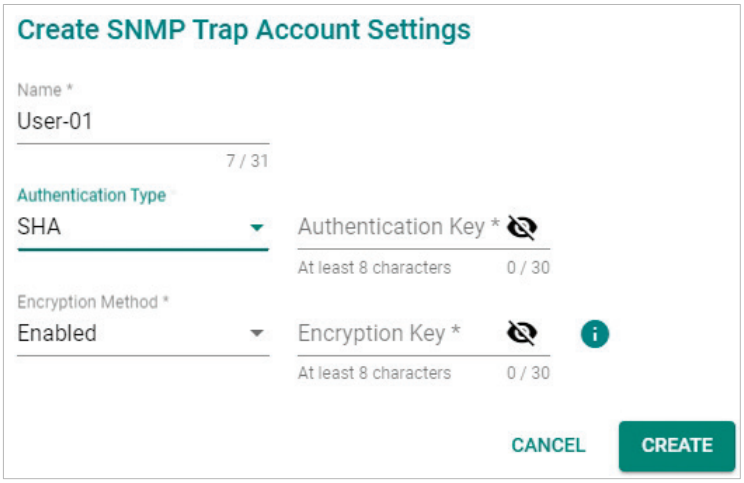
Setting	Description	Factory Default
None	No authentication type will be used.	None
MD5	Use MD5 authentication.	
SHA	Use SHA authentication.	

Encryption Method

Setting	Description	Factory Default
Disabled	Disable the encryption method.	None
DES	Use DES encryption.	
AES	Use AES encryption.	

If the Authentication Type is set to **MD5** or **SHA**, and the Encryption Method is set to **Enabled**, also configure the following settings:





Authentication Key

Setting	Description	Factory Default
8 to 30 characters	Enter the authentication password.	None

Encryption Key

Setting	Description	Factory Default
8 to 30 characters	Enter the data encryption password.	None

When finished, click **CREATE** to create the SNMP Trap account.

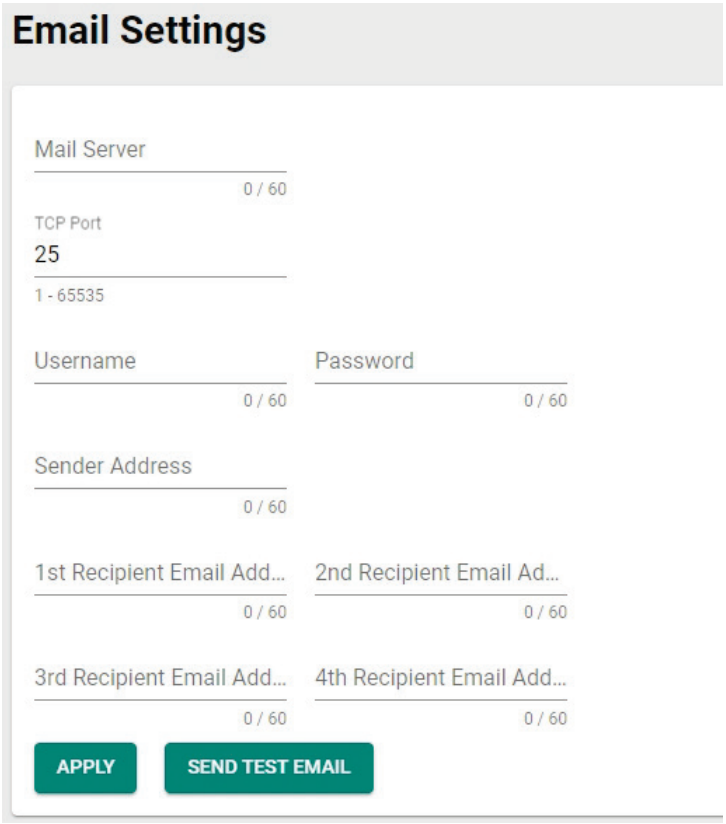
Modify an Existing SNMP Trap Account

Click the ✎ icon next to the entry you want to modify. When finished, click **APPLY** to save your changes.

Delete an Existing SNMP Trap Account

Select the item(s) in the SNMP Trap account List. Click the icon and click **DELETE** to delete the item(s).

Email Settings



Mail Server

Setting	Description	Factory Default
Max. 60 characters	Enter the email server address.	None

TCP Port

Setting	Description	Factory Default
1 to 65535	Specify the TCP port of the email server.	25

Username

Setting	Description	Factory Default
Max. 60 characters	Enter the username used to log in to the email server.	None

Password

Setting	Description	Factory Default
Max. 60 characters	Enter the password used to log in to the email server.	None

Sender Address

Setting	Description	Factory Default
Max. 60 characters	Enter the sender's email address.	None

1st/2nd/3rd/4th Recipient Email Address

Setting	Description	Factory Default
Max. 60 characters	Enter the recipient address. You can set up to 4 email addresses to receive alarm emails from the Industrial Secure Router.	None

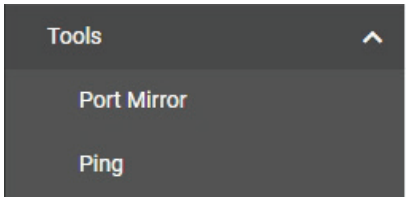
Send Test Email

After configuring the email settings, click **APPLY** to apply the settings. Press **SEND TEST EMAIL** to verify that the settings are working correctly.

> **NOTE**
>
> Auto warning e-mail messages will be sent through an authentication-protected SMTP server that supports the CRAM-MD5, LOGIN, and PAIN methods of SASL (Simple Authentication and Security Layer) authentication mechanism.
>
> 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.

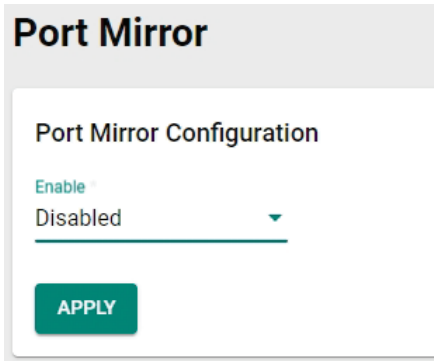
Tools

From the **Tools** section, the following functions can be configured: **Port Mirror,** and **Ping**.



Port Mirror

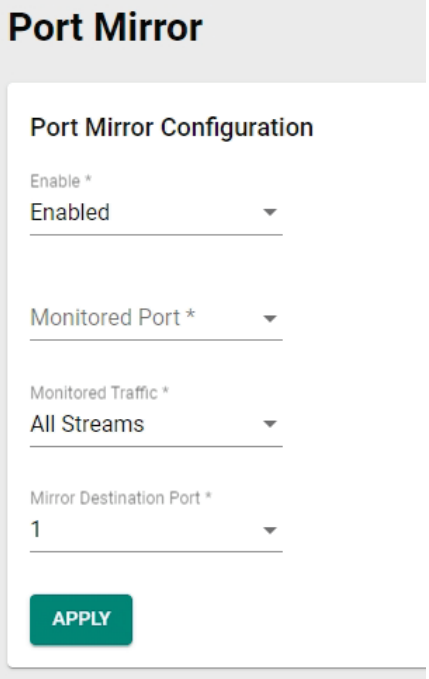
The **Port Mirror** function can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the mirror port) to receive the same data being transmitted from, or both to and from, the port under observation. Using a mirror port allows the network administrator to sniff the observed port to keep tabs on network activity.



Enable

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the port mirror function.	Disabled

If enabled, also configure the following settings:



Monitored Port

Setting	Description	Factory Default
1 to 10	Select the number of the port(s) whose network activity will be monitored. Multiple port can be selected.	Disabled

Monitored Traffic

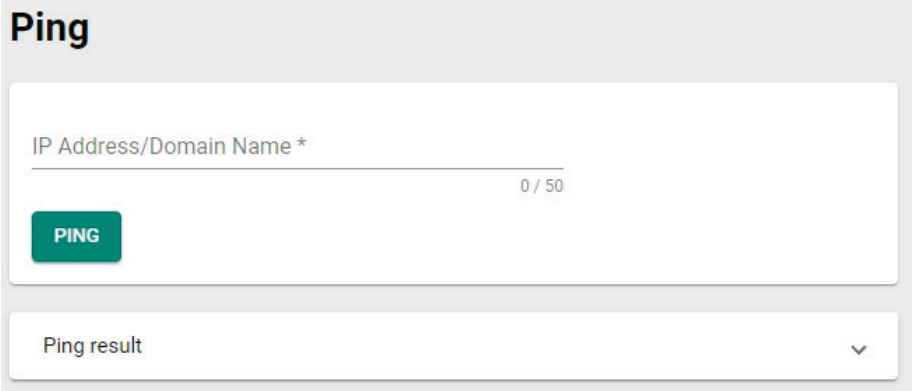
Setting	Description	Factory Default
Ingress Stream, Egress Stream, All Streams	Select the type of traffic that will be monitored. • Ingress Stream Select this option to monitor only those data packets coming into the Moxa industrial secure router's port. • Egress Stream Select this option to monitor only those data packets being sent out through the Moxa industrial secure router's port. • All Streams Select this option to monitor data packets both coming into and being sent out through the Moxa industrial secure router's port.	Disabled

Mirror Destination Port

Setting	Description	Factory Default
1 to 10	Select the number of the port that will be used to monitor the activity of the monitored port.	Disabled

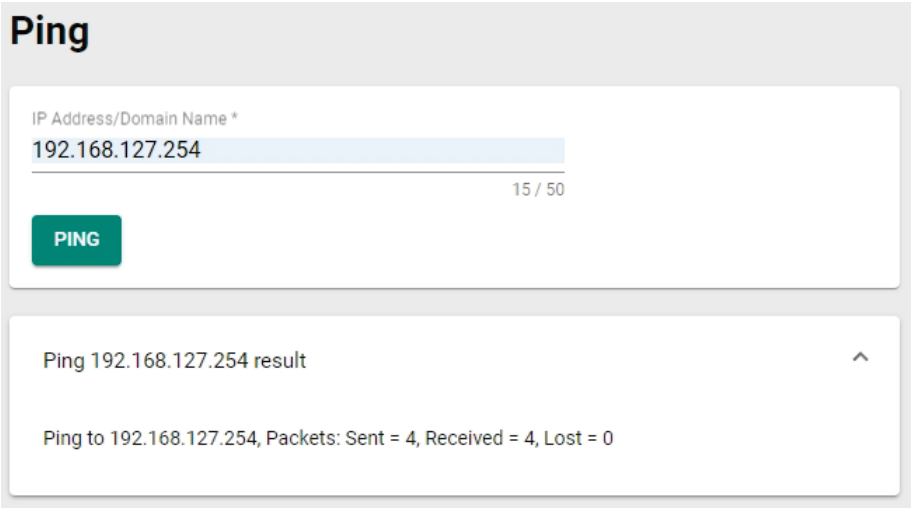
When finished, click **APPLY** to save your changes.

Ping



The Ping function uses the ping command to give users a simple but powerful tool 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 Industrial Secure Router itself. In this way, the user can essentially control the Industrial Secure Router and send ping commands out through its ports.:

Type in the desired IP address and click **Ping**. The result of the ping will be displayed in the section below.



A. MIB Groups

The Industrial Secure Router comes with built-in SNMP (Simple Network Management Protocol) agent software that supports cold start trap, line up/down trap, and RFC 1213 MIB-II. The standard MIB groups that the Industrial Secure Router series support are:

MIB II.1 – System Group

sysORTable

MIB II.2 – Interfaces Group

ifTable

MIB II.4 – IP Group

ipAddrTable

ipNetToMediaTable

IpGroup

IpBasicStatsGroup

IpStatsGroup

MIB II.5 – ICMP Group

IcmpGroup

IcmpInputStatus

IcmpOutputStats

MIB II.6 – TCP Group

tcpConnTable

TcpGroup

TcpStats

MIB II.7 – UDP Group

udpTable

UdpStats

MIB II.11 – SNMP Group

SnmpBasicGroup

SnmpInputStats

SnmpOutputStats

Public Traps

1. Cold Start
2. Link Up
3. Link Down
4. Authentication Failure

Private Traps:

1. Configuration Changed
2. Power On
3. Power Off
4. DI Trap

B. Account Privileges List

This appendix lists the privileges for the different account roles.

User Role Privileges

The following table lists the privileges of the different user roles for the functions of the device.

The table uses the follow letter designations:

- **R**: Read-only privilege
- **W**: Write privilege
- **R/W**: Read/write privilege

Function	Account Privilege		
System	**Admin**	**Supervisor**	**User**
System Management			
- Information Settings	R/W	R/W	R
- Firmware Upgrade	R/W	R/W	R
- Software Package Management	R/W	R/W	R
- Configuration Backup and Restore	R/W	R/W	R
Account Management			
- User Account	R/W	R	R
- Password Policy	R/W	R/W	R
License Management	R/W	R/W	R
Management Interface			
- User Interface	R/W	R/W	R
- Hardware Interface	R/W	R/W	R
- SNMP	R/W	R/W	R
- MXsecurity	R/W	R/W	R
Time			
- System Time	R/W	R/W	R
- NTP/SNTP Server	R/W	R/W	R
Setting Check	R/W	R/W	R
Network Configuration	**Admin**	**Supervisor**	**User**
Port			
- Port Settings	R/W	R/W	R
- Link Aggregation	R/W	R/W	R
Layer 2 Switching			
- VLAN	R/W	R/W	R
- MAC Address Table	R/W	R/W	R
- QoS	R/W	R/W	R/W
- Rate Limit	R/W	R/W	R
- Multicast	R/W	R/W	R
Network Interface	R/W	R/W	R
Redundancy	**Admin**	**Supervisor**	**User**
Layer 2 Redundancy			
- Spanning Tree	R/W	R/W	R
- Turbo Ring V2	R/W	R/W	R
Layer 3 Redundancy			
- VRRP	R/W	R/W	R
Network Service	**Admin**	**Supervisor**	**User**
DHCP Server	R/W	R/W	R
Dynamic DNS	R/W	R/W	R

Function	Account Privilege		
Routing	**Admin**	**Supervisor**	**User**
Unicast Routing			
- Static Routes	R/W	R/W	R
- RIP	R/W	R/W	R
- OSPF	R/W	R/W	R
- Routing Table	R	R	R
Multicast Route			
- Multicast Route Settings	R/W	R/W	R
- Static Multicast Route	R/W	R/W	R
Broadcast Forwarding	R/W	R/W	R
NAT	**Admin**	**Supervisor**	**User**
NAT Setting	R/W	R/W	R
Object Management	**Admin**	**Supervisor**	**User**
Object Management	R/W	R/W	R
Firewall	**Admin**	**Supervisor**	**User**
Layer 2 Policy	R/W	R/W	R
Layer 3 - 7 Policy	R/W	R/W	R
Malformed Packets	R/W	R/W	R
Session Control	R/W	R/W	R
DoS Policy	R/W	R/W	R
Advanced Protection			
- Dashboard	R/W	R/W	R
- Configuration	R/W	R/W	R
- Protocol Filter Policy	R/W	R/W	R
- ADP	R/W	R/W	R
- IPS	R/W	R/W	R
VPN	**Admin**	**Supervisor**	**User**
IPsec	R/W	R/W	R
L2TP Server	R/W	R/W	R
Certification Management	**Admin**	**Supervisor**	**User**
Local Certificate	R/W	R/W	R
Trusted CA Certificate	R/W	R/W	R
Certificate Signing Request	R/W	R/W	R
Security	**Admin**	**Supervisor**	**User**
Device Security			
- Login Policy	R/W	R/W	R
- Trusted Access	R/W	R/W	R
- SSH & SSL	R/W	R/W	R
Network Security			
- IEEE 802.1X	R/W	R/W	R
RADIUS	R/W	R/W	R
MXview Alert Notification	R/W	R/W	R
Diagnosis	**Admin**	**Supervisor**	**User**
System Status			
- Utilization	R/W	R/W	R
- Fiber Check	R/W	R/W	R
Network Status			
- Network Statistics	R	R	R
- LLDP	R/W	R/W	R
- ARP Table	R	R	R
Event Log & Notifications			
- Event Log	R/W	R/W	R
- Event Notifications	R/W	R/W	R
- Syslog	R/W	R/W	R
- SNMP Trap/Inform	R/W	R/W	R
- Email Settings	R/W	R/W	R
Tools			
- Port Mirror	R/W	R/W	R

Function	Account Privilege		
- Ping	R/W	R/W	R